# Technical Report

Mobile application for secure and private file sharing on the cloud

Team App+

27-5-2022

# Table of Contents

# System Requirements

## Introduction

The system requirements include Roles and Responsibilities, Project Scope Statement, Work Breakdown Structure (WBS) ,WBS Dictionary and Iteration Management.This project is to design, program and test a new software that will be used for file transfer between users as well as simple chat function and keep files safe in the cloud.

## Roles and Responsibilities

Clients, project leaders and team members will all play a key role in the scope management of the project. Therefore, all need to understand their responsibilities to ensure the stability of the project. The following table shows the roles and responsibilities of each member.

| Name | Role | Responsibilities |
|---|---|---|
| Pairat Thorncharoensri | Client | Approve or reject project change requests as appropriate;<br>Assess the completion of the project. |
| Ziming Mao | Project leader | Measure and verify project scope<br>Develop a project plan and modify the project plan according to various changes;<br>Regular project evaluation meetings are held;<br>Communicate clear goals to team members; |
| Tianchi He | Team member | Participate in meetings regularly;<br>Assess the need for project changes;<br>Ask the project manager or leader in time when encountering problems. |
| Cheng Zhang | Team member | Participate in meetings regularly;<br>Assess the need for project changes;<br>Ask the project manager or leader in time when encountering problems. |

| | | |
|---|---|---|
| Yanchao Yu | Team member | Participate in meetings regularly; Assess the need for project changes; Ask the project manager or leader in time when encountering problems. |
| Zhiyong Jian | Team member | Participate in meetings regularly; Assess the need for project changes; Ask the project manager or leader in time when encountering problems. |
| Bohong Sun | Team member | Participate in meetings regularly; Assess the need for project changes; Ask the project manager or leader in time when encountering problems. |

## Project Scope Statement

The project includes designing, programming and testing mobile applications for users to securely share photos on the cloud.
We will conduct segmented tests according to each function or requirement of the project; on this basis, new functions will be added. We divide the main functions of the project into the following four points:

Function 1: User interface
Goal: Allow users to add personal information, pictures, etc. while satisfying the user's ability to view the friend list and add friends

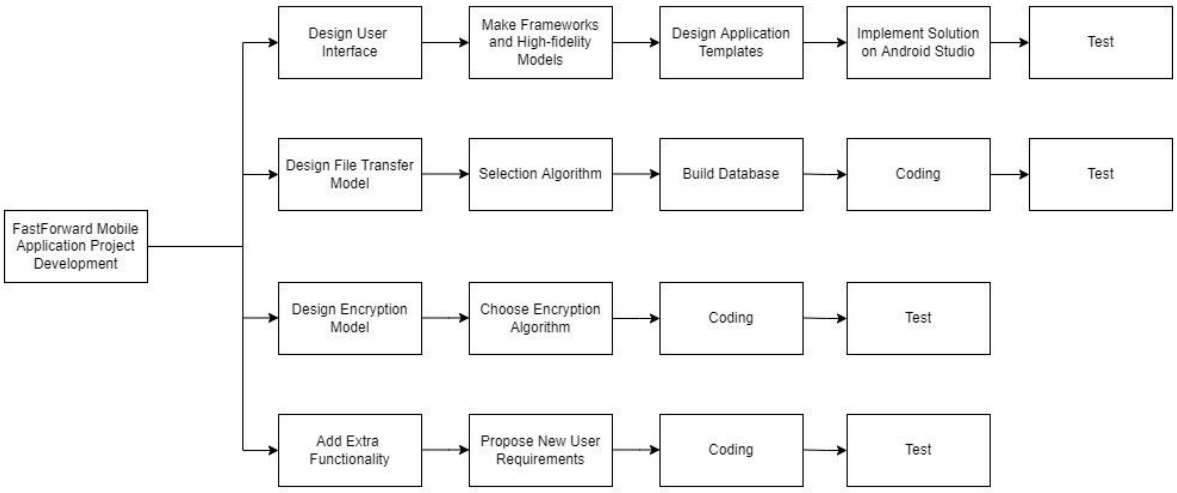
Function 2: File transfer
Goal: After the user clicks, automatically filter out the photos that they want to share, and share them with other users

Function 3: Encryption
Goal: to ensure the security of the file in the process of sharing the file, and simultaneously, the key of the file can only be known by two users.

Function 4: Add Extra Functionality
Goal: Provide some basic controls and settings for users to share files or send messages, and allow users to customize privacy settings, and finally send a notification to the user after the user has successfully shared.

## Work Breakdown Structure

In order to improve work efficiency and facilitate the monitoring of progress, we divide the project development into 4 stages, and subdivide each stage into multiple small tasks and set up milestones. As the tasks of each phase are completed, the team checks the completion of all work and confirms whether revisions and iterations are required.




## WBS Dictionary

| Element Name | Description work | Deliverables | Budget |
|---|---|---|---|
| Design User Interface | Design a clean and beautiful user interface for mobile application | User interface is easy to use and meets user needs | 0 |
| Design File Transfer Model | Design functional modules that allow users to share files | Files can be transferred correctly | 0 |

| | | | |
|---|---|---|---|
| Design Encryption Model | Encrypt user-transferred files and user's personal information | Documents and information can be securely encrypted | 0 |
| Add Extra Functionality | Add extra functionality to the mobile application to meet the needs of different users | Added functionality works fine | 0 |

## Iteration Management

In the development of this mobile phone software project, our team has gone through many iterations of design, and the main iterative content of our team is the iteration of UI. When our team was developing a function, because the project had just started, there was no information and UI template, so we carried out several iterations in UI design. In the beginning, we used figma to simulate our entire UI, as shown in Figure 1. In the initial design, we wanted to make all the available features visible to the user.

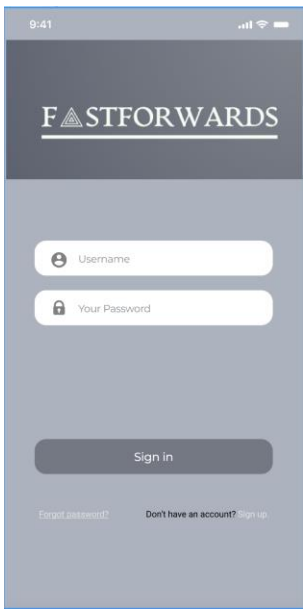



Figure1. The first generation UI (figma)

However, due to the limitation of figma, we cannot make more detailed modifications, and we cannot be sure that all functions can be implemented. So we made a second design, as shown in Figure 2, we used Android Studio for the new design, typing and text boxes can work normally, but there are some problems with the jump.

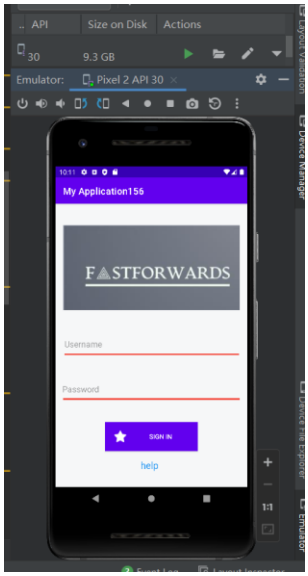



Figure 2. Android Studio version UI

So we carried out the third iteration of the design, as shown in Figure 3, and our idea was to create a second interface to realize the jump of the screen touch. We have added more content on the basis of the second version of the code. In order to improve the user's physical examination and ease of use, we have also adjusted and beautified the program to allow users to use it better.

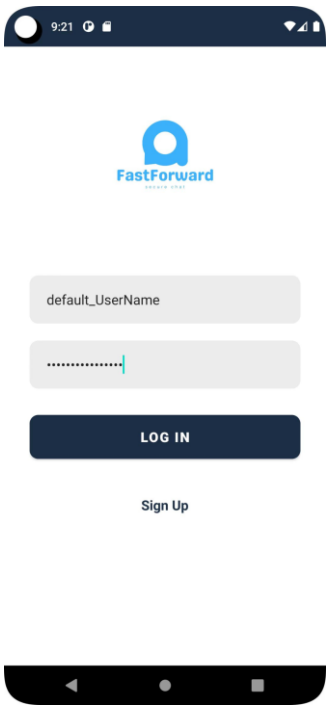



Figure 3. Latest version of UI

The fourth iteration of the design is to add new features, in order to make the product more "full", we will focus on the functional aspects. As shown in Figure 4 and 5, we completed the registration function on the basis of the login interface, established a database, realized a series of functions to meet the needs such as adding friends, and optimized and updated the UI design of each interface.

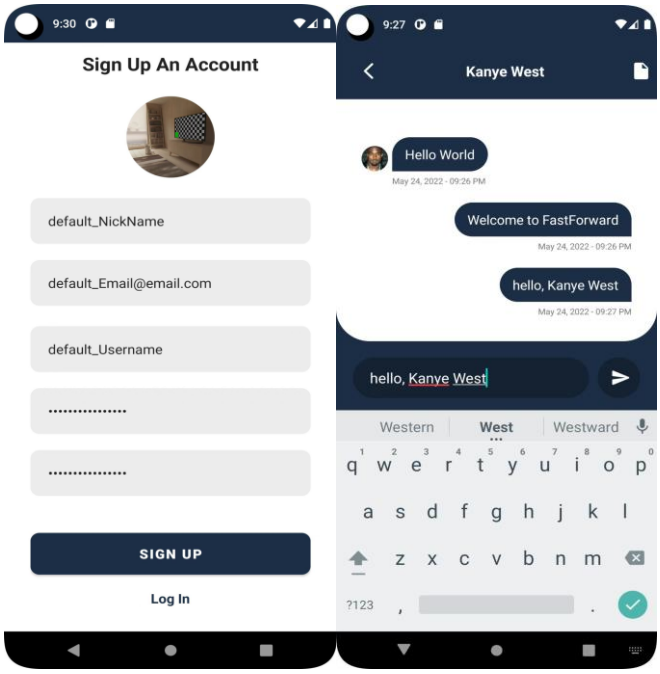


Figure 4 and 5. Feature update and UI beautification

# Project summary

## Executive Summary

The purpose of this report is to provide the client with a summary of the completion of all parts of the project and the technologies used in development. The project started on August 19, 2021 and ended on May 27, 2022, and lasted 9 months.The main goal of this project is to develop an independent application by using data transmission, data encryption and other technologies. With the efforts of all team members, we completed the development of the application and conducted multiple rounds of testing.
This report mainly includes the following contents: project summary, project status report, changes in project requirements, key milestones of the project, requirements traceability matrix, and project budget report, etc.The report provides a comprehensive overview of all key details of project development, not only to help team members draw lessons learned, but also to help clients understand the status and development context of the project more quickly.

## Work Summary

The team's work tasks are mainly mobile application development, the core functions of which are file sharing and file encryption. According to the meeting discussions within the team, we divided the project into four parts: user interface design, file transfer module design, file encryption module design, and adding additional features. According to the priority of the requirements, we divided the team into two parts, and started to develop the

user interface and the file transfer module at the same time. Our team chose a semi-agile development model. When designing the user interface, we collected a lot of relevant resources and materials, and continued to iterate until it met customer needs. When writing code for file sharing and file encryption, we are constantly learning algorithms and logic from related websites. When development hits a bottleneck, teams meet to discuss solutions or whether to change work assignments. We recorded in detail the content of each meeting and the final conclusions. In the table below, we also recorded the time, money, and human level resource consumption for each stage of the work period. In the project developed by the team, all members strictly abide by the rules and regulations set by the team, which allows our work to proceed smoothly. In the follow-up work, we also continue to summarize and reflect, and find some potential problems and details that need to be improved.
The table below is some detailed data in the development of the project and the working status of the team.

## Current Project Status Report

| Report Date | Project Name | Prepare By |
|---|---|---|
| 27/5/2022 | Mobile application for secure and private file sharing on the cloud | APP+ Team |

### Status Summary

Below is a summary of the section, which contains information on the project's Current Status, cost consumption, project's risk history, and key milestones. This information will help clients understand the specifics of our project content.

### Project Overview

| Task | Done ( % ) | Due Date | Main in-charge |
|---|---|---|---|
| User interface | 100 | October 17,2021 | Tianchi He, Cheng Zhang, Bohong Sun,Yanchao Yu |
| File transfer | 100 | March 5, 2022 | Ziming Mao, Cheng Zhang, Bohong Sun, Zhiyong Jian |

| | | | |
|---|---|---|---|
| Encryption | 95 | May 27,2022 | Ziming Mao,Yanchao Yu, Bohong Sun, Zhiyong Jian, |
| Add Extra Functionality | 100 | May 27,2022 | Tianchi He, Cheng Zhang, Bohong Sun, Ziming Mao |

## Budget Overview

| Category | Spent ( $ ) | Note |
|---|---|---|
| User interface | 0 | The UI interface uses Figma and Android Studio, which are both free and self-contained products. |
| File transfer | 0 | The code is modified on existing material, so there is no cost |
| Encryption | 0 | This code content needs to be done on the second function, so it doesn't cost anything |
| Add Extra Functionality | 0 | This content needs to be implemented after the second and third are completed, so there is no need to add new assets. |

## Risk and Issue History

| Issue | Assigned To | Date | Comment |
|---|---|---|---|
| User interface design dissatisfaction | Cheng Zhang | October 2 ,2021 | Not satisfied with the UI model of the first version, and there are problems with the design ideas. |
| Database build problem | Bohong Sun, Yanchao Yu | April 4 ,2022 | Having difficulty creating the database and unable to complete the task on time. |
| Encryption method is not applicable | Ziming Mao, Zhiyong Jian | May 1,2022 | Unable to successfully connect wit |

| | | | |
|---|---|---|---|
| | | | h the existing code due to the limitation of the encrypted code |

## Key Project Milestones

| Milestones | Target Date | Actual Date | Status | Comment |
|---|---|---|---|---|
| Project start | August 19,2021 | August 19,2021 | Completed | First Zoom meeting with client to identify project requirements and tasks. |
| User interface Design | October 17,2021 | October 17,2021 | Completed | The UI design is completed, and the first part of the task is over. |
| File transfer | March 5, 2022 | March 5, 2022 | Completed | Successful file sharing on a simulated phone. |
| Encryption | May 27, 2022 | May 27, 2022 | Completed | Function realization |
| Add Extra Functionality | May 27, 2022 | May 27, 2022 | Completed | Summarize the front-end and back-end content, and add a series of additional operations |

## Conclusion/Recommendation

The above chart shows the details of the team in the development of the project. During the development of the project, the team has been communicating with customers, and user needs have undergone subtle changes. Our team has always developed around the core features of file sharing and encryption. In order to increase market competitiveness, we refer to a large number of

similar applications in the Apple and Android stores, and learn from their advantages to make up for their shortcomings.
The project was completed by only 6 people, and did not require a lot of resources and budget. The above forms record the team's budget statistics, risk history, and key milestones. These forms allow customers to have a better understanding of the project, and also facilitate us to better arrange work in the subsequent development process.

## Requirements traceability matrix

| Id | Functional requirement | | | Status |
|---|---|---|---|---|
| | Main Requirements | Category | Description | |
| 1 | User interface | Required | Create a personal information interface for each user. Through this function, users can add personal information, add friends, view the list of friends, and chat. | Complete |
| 2 | File transfer | Required | Users can transfer files through this application, and the software has the authority to find the location of the files in the user's device | Complete |
| 3 | Encryption | Required | The encryption is performed by the AES algorithm, which is symmetric encryption. The keys of both parties are the same, which is fast and secure.Then the distribution key and the initial communication use the | Complete |

| | | | | |
|---|---|---|---|---|
| | | | RSA algorithm, which is an asymmetric algorithm. | |
| 4 | Add Extra Functionality | Required | Management of user data, such as file transfer, modification, and deletion, user permission settings, etc. | Complete |

# System Design

## Information architecture

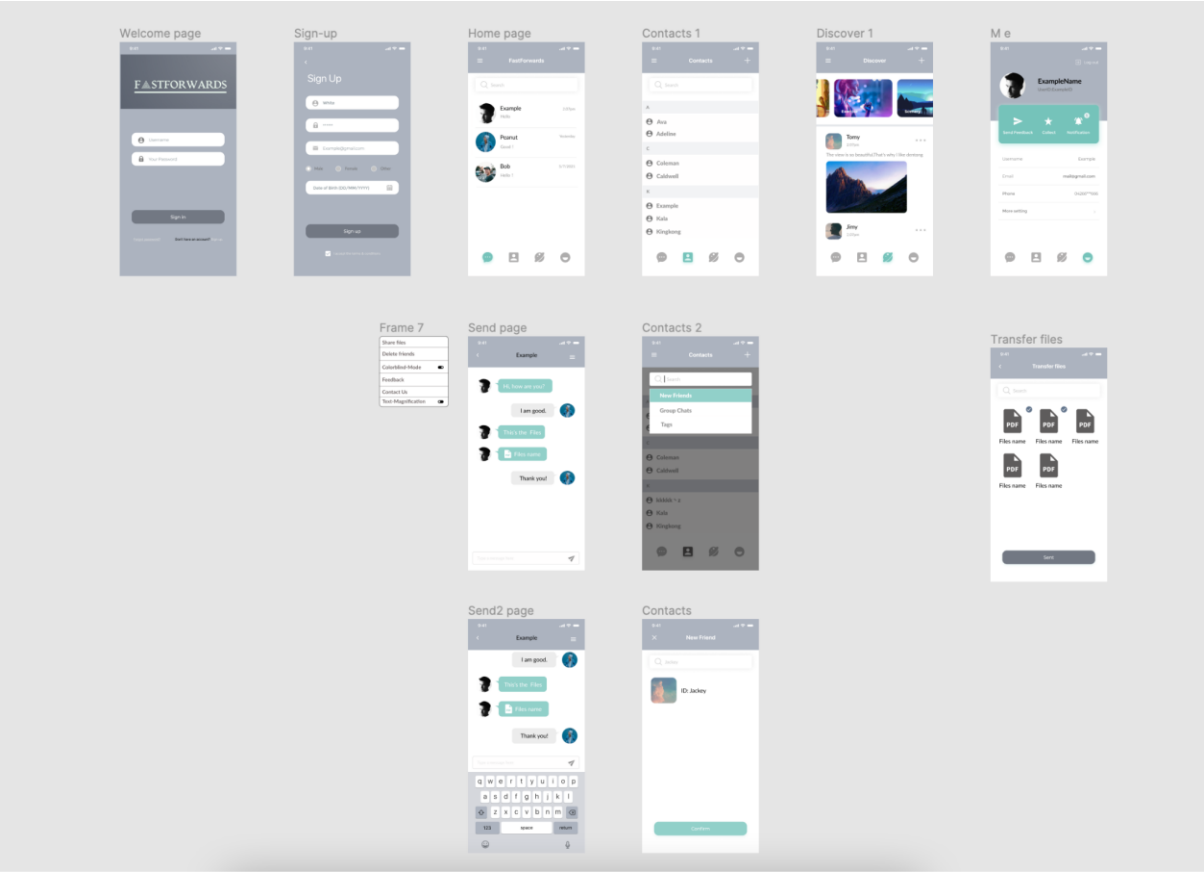



Figure 6. Final version UI design in figma

## Encryption Method

The encryption is performed by the AES algorithm, which is a symmetric encryption. The keys of both parties are the same, which is fast and secure. Th

en the distribution key and the initial communication use the RSA algorith m, which is an asymmetric algorithm.

To put it simply, the user publishes his key on the Internet, and everyone can get my public key. If anyone needs to send a message to the user, he wi ll package the data and send it to the user. The user also has a private ke y. Only the private key can be unlocked (the user's public key belongs to t he encrypted data).

The process of passing AES through RSA is such a process. The RSA public ke y of the server is public, and the user now wants to communicate with the s erver, then the user encrypts the AES key generated locally by the user wit h the RSA public key of the server, and the transmission process It doesn't matter if it is intercepted in the middle, because the garbled code cannot be opened. After the server receives it, it opens it with his private key, finds the AES key generated by the client, and then both the server and the client use this AES. key for transmission. AES key, the same key is used fo r encryption and decryption.
Then if the user wants to communicate with other users, such as adding frie nds, then the server knows my RSA public key, and will push my RSA public k ey to the friend, and the friend generates an AES key for communication bet ween us. , the friend encrypts this key with the user's RSA public key, and then sends it. After the user receives it, he knows the AES KEY used for co mmunication between the two of us, and every time the user sends a message to that friend, or the friend sends a message to When users are using this AES key for encryption and decryption.

At the same time, when the user needs to send a file, it is not through the server, but through a storage platform, such as Amazon. If the user wants t o send a file to You, the user can encrypt the file with AES, and then uplo ad it to the file server. Send an address back. Then send this address to a friend. After receiving it, download it and decrypt it with AES that we neg otiated.

So the complete process is, if the user wants to send a message to a frien d, the user must first perform the AES encryption between the user and the friend of the actual message or file download address he wants to send. The message also has other information, such as the recipient or something. . P ack and encrypt the entire message again, use the AES key negotiated by the user and the server, and then send it to the server. After the server recei ves it, it first decrypts it with AES negotiated by the user and the serve r, and then knows who the user needs to send the message to, such as to a f riend, and then the server encrypts it with the AES key used by the server to communicate with the friend, and then sends the message to a friend. To friends. After receiving the message, use the AES between the friend and th

e server to decrypt it, and then know that it was sent to you by someone el se, and then use the AES key between us to decrypt the message content twic e. The content of the message to send to a friend or where to download the file.

So, the reason we use AES is that it is fast and secure, RSA is secure, but very slow, so RSA is used to pass some short messages, such as the work of distributing AES.

# Project Closeout

## Project Acceptance

This section establishes the formal acceptance of all deliverables for the < Mobile application for secure and private file sharing on the cloud > pro ject. < Mobile application for secure and private file sharing on the clou d > This project has met all acceptance criteria defined in the requirement s document and project scope statement. At the same time, the project docum ents are handed over to the customer to check compliance with product requi rements and functionality. In addition, an evaluation of the software proje ct will be carried out and all requirements will be ensured to the quality required by the client.

## Lessons learned

### Android database learning summary

In order to allow us to use the database conveniently, android provides us with a SQLiteOpenHelper helper class

It is an abstract class, so we need to customize a class to inherit this cl ass to implement the logic of our database creation

Implement logic

Create and update

Let's talk about his constructor first, we generally rewrite the first (with four parameters) constructor

The four parameters mean respectively (context, database name, null (a custom Cursor is also allowed here, which will be returned after querying the data), the version number of the current database)

Let's talk about the **two methods** we need to override

onCreate(), create database method, call internally, create a database

onUpgrade(), the upgrade database method, is also an internal call

There are also **two methods** we generally use (both get a database instance)

getReadableDatabase(), get a database instance by reading

getWritableDatabase(), open a database instance for writing

Note: When the database is not writable, the former returns a writable database, while the latter reports an exception

Logic of creation

When we go to the new database, we only get the operation handle of this database. Regarding the specific data inventory that does not exist, this is not what we do here.

Then we take this instance to get the instance of reading the database. When it is here, he will judge that if the database does not exist, it will onCreate(), and if it exists, it will judge whether the version is the current version. If we are in new When the incoming version is higher than the existing database version, the onUpgrade() method will be called to update the database, so the logic of updating the database needs to be written by ourselves

CRUD

Four methods are provided for us,

insert:

Takes three parameters:

First: table name

The second: it is used to automatically assign NULL to some nullable columns without specifying the addition of data. Generally, it is not used, and null is passed directly.

The third: is a ContentValues object, this object is used to wrap the data we want to add, it provides a series of put key-value pair methods, let us set the data we want to pass in

update:

four parameters

First: table name

The second: ContentValues object, wrapping the new data to be

The third and fourth are used to constrain the update of a row or rows of data. If not specified, the default is to change all rows

delete:

three parameters

First: table name

The third and second are used to constrain the deletion of a row or rows of data. If not specified, the default is to delete all rows

query:

This method is more complicated, there are several overloaded methods, and the method has many parameters, but it is actually a constraint on the query data. Let's take a look at the meaning of some parameters.

table : Specifies the table name for the query

columns : specify the column names of the query

selection : specify the constraints of where

selectionArgs : Provide specific parameters for the placeholder of the previous parameter

groupBy : Specify the columns that need groupBy

having : Further constraints on the result after groupBy

orderBy: Specifies the ordering method of query results

## Learn from Project Management

Since this project is an initial project, our team is also doing project development for the first time, without any historical experience as a reference. At first, the project was in the exploratory stage, and encountered many problems and did not know how to solve them. After two semesters of rese

arch and exploration, we finally handed in the complete finished product and learned a lot from it. Our team summarizes the following experiences, including communication, project resource management, confirmation of the core strengths of the team, and project processes.

Communication

Communication is a critical step in project management. After the test plan is developed, it is necessary to communicate with the customer in a timely manner, and at the same time communicate with the team members and make suggestions. Before the project started testing, we just made a test plan by ourselves without communicating with the customer, resulting in many functions that were not supported and deviated from the customer's expectations, resulting in us doing a lot of useless work. After that, we discussed and communicated with the client after we made the decision, and we also communicated frequently within our team, which ensured the efficient execution of the project and also accelerated the progress of our entire project.

Project Resource Management

Project resource management is to determine project requirements. This step is very important, because project management resources are a key factor and play a crucial role in the success of the project. Team leaders need to clarify project roles and allocate tasks reasonably according to project requirements.

Core advantages

When developing a project, it is also important to recognize the strengths of each team member and make those strengths the main area of focus. This makes it easier for the team leader to assign everyone's work. This way everyone can contribute their best effort and the project progress will be accelerated.

Project Milestones and Workflow

Setting key nodes (milestones) in the entire project process will help us complete the project effectively. Establish a key milestone at key stages such as project initiation, planning, execution, and closure. This way, it can be well used for staged checks, and at the end of each stage, a real evaluation test can be carried out, discovering Deficiencies in the project are dealt with in a timely manner, so that the process of the next task will not be delayed.

The development of workflow can also help us understand the status of the project, eliminate redundant links in the work process, merge similar activities, make the workflow more reasonable and convenient, and improve work efficiency.

# Post project review

## Project name and summary

Our APP+ team completed the development of the project < Mobile application for secure and private file sharing on the cloud > in the two semesters of 2021-2022. The project has been successfully handed over to the client for inspection.The main content of this project is to implement a mobile phone software that allows users to transfer files and encrypt them in the cloud.

## Team members

The Mobile application for secure and private file sharing on the cloud pr oject consists of 6 members, and the member information is as follows:

| Name | Project Role | Title | Contact |
|---|---|---|---|
| Ziming Mao | Developer, Testing Engineer | Team Leader, Testing Tech | zm783@uowmail.edu.au |
| Zhiyong Jian | Developer, Testing Engineer | Testing Tech | zj536@uowmail.edu.au |
| Bohong Sun | Developer, Database Designer | Data Tech | bs382@uowmail.edu.au |
| Yanchao Yu | Developer, Database Designer | Data Tech | yry345@uowmail.edu.au |
| Tianchi He | Developer, UI/UX Designer | Design Tech | th144@uowmail.edu.au |
| Cheng Zhang | Developer, UI/UX Designer | Design Tech | cz960@uowmail.edu.au |

## Expected outcomes vs. Actual outcomes

In expected outcomes, from the UI perspective, it contains file sharing windows with communication functions. For the data storage, it should be designed to connect with a MySQL database directly with JDBC implementations. Truing to the encryption part, the file needs to be shared securely with the RSA algorithm which is much more solid and reliable.

Turning to actual outcomes, from a UI perspective, more functions include account profit viewing and provide users with choices whether to accept a friend request. The database in software used sqlite and sp storage. In the server, it used MySQL and redis. Turning to the encryption part, both RSA and AES algorithms are used. The server will send the RSA key from sender to receiver. Then the receiver will create an AES key for communication. Meanwhile the file is not stored in the server but the storage platform. Receiver will use the previous AES key to reveal the website address and download.

## Project Cost

The main task of our team in the development of the Mobile application for secure and private file sharing on the cloud project is to make a mobile phone software that can be encrypted in the cloud, and to design UI/UX for it. During the development process, our team members searched a lot of materials, and most of the content was designed by our team members themselves, so the project did not consume any cost.

## Project Schedule

The Mobile application for secure and private file sharing on the cloud project started on August 19th and ended on May 27th, taking a total of 9 months.
The table below shows the various phases of our completed projects.

| Project Phase | Scheduled Completion | Actual Completion |
|---|---|---|
| Project start | August 19,2021 | August 19,2021 |
| Function 1: User interface Design | October 17,2021 | October 17,2021 |
| Function 2 : File transfer | March 5, 2022 | March 5, 2022 |
| Function 3 : Encryption | May 27, 2022 | May 27, 2022 |
| Function 4 : Add Extra Functionality | May 27, 2022 | May 27, 2022 |

| | | |
|---|---|---|
| Project end | May 27, 2022 | May 27, 2022 |

## Transition plan

Project 1: Mobile application development
Project Description: Develop a file sharing mobile application that can encrypt files.
Status: The development phase has ended.
Deadline: 2022/5/27
Resources: Human resources include 6 team members, as well as materials from the Internet and GITHUB.
Next step: Testing

Project 2: Testing
Project description: Install the application on an Android phone and test if all functions work properly.
Status: Two rounds of testing have been conducted and the team is working on fixing bugs.
Deadline: 2022/5/27
Source: Two Android phones
Next step: Marketing

Project 3: Marketing
Project Description: Shoot an advertising video for this mobile app and promote the app on campus.
Status: Advertising video production completed. The team sends out questionnaires to students and invites interested students to try it out.
Deadline: 2022/5/27
Resources: Camera used for filming and 50 questionnaires
Next up: Tradeshow

# System installation process

FastForward is a software on Android phones, and all his installation methods require a computer to operate.

First, we need to find the required apk file on the computer and connect your Android device to the computer. At this point, System Difficulty will ask you if you want to charge your phone or connect it as a "media device".

The second step, find your phone's folder on your computer, it will be in "My Computer" or "Computer" on Windows (PC). Copy the APK file from your computer to a folder of your choice on your Android device.

The third step, open your Android phone, go to "My Files", search for the location of the APK file you just copied.

The fourth step, open the file manager, find the APK file, click on it, and then click "Install". Wait for the installation to complete and you are ready to use the software.

Note: If you use the file manager to install the APK file for the first time, the Android device will prompt you to authorize the application to install unknown applications, then you can click Allow.

If you can't open the software, you can go to the Android settings, click "Security", activate the "Unknown sources" option, and try again.

If the operating system on your Android device is running a version lower than Android 8.0, you will need to change the system settings to install apps not downloaded from the Play Store.