NFC Attendance Application
Functional Specification

Amy Leitch - 14531977

24/11/2017

Functional Specification Contents

0. Table of contents

1. Introduction

1.1 Overview

Keeping track of attendance can be very useful in a number of scenarios. Some college lecturers take student attendance into account when grading. Secondary schools have mandatory attendance and need to be aware of truancy. Keeping record of meetings and the names of attendees is important in any educational or work environment.

The system in this project would be used to keep attendance at particular events, such as lectures or project supervisor meetings, with zero configuration other than the user's name and email address. It is made up an NFC chip, an android mobile application and a web interface. For example, a lecturer would own a personal NFC tag, be that a keyring or card, and students would use the mobile app to scan the tag and record their attendance with that lecturer at that particular time slot.
It can be assumed that if 10 people scan the tag at the same time period, they were all at the same event. This info would be recorded and stored in a database. This information can then be viewed by the lecturer on a timetable web interface. Time slots where the tag had been scanned will be highlighted on the lecturer own timetable, showing how many students were in attendance at that event. Clicking into the event will show more detail such as individual student names.

This application stores information about the attendance at an event and removes the need of individual times, timetables, locations, lists of names and numbers, and any other configuration that may had needed to be set up or known previously .

1.2 Glossary

- ***Android* -** Mobile operating system developed by Google.
- ***Android SDK* -** Android Software Development Kit, developer tool used to create applications for Android devices.
- ***NFC*** - Near Field Communication, a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a mobile phone, to pass data to one another by touching them or putting them very close together.
- ***Public/Private key pair*** accomplishes two functions: authentication, which is when the public key is used to verify that a holder of the paired private key sent the message, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key.
- ***URL* -** Uniform Resource Locator, a reference to a web source that specifies its location on a computer network and a mechanism for retrieving it.
- ***Web Server*** - A computer system that processes requests via the basic network protocols to distribute information on the internet.

2. General Description

2.1 Product / System Functions

The product is aimed at those who want a simpler way of taking attendance at an event. It is made up an NFC chip, an android mobile application and a web interface, with minimal configuration necessary. In a college situation, the lecturer will own an NFC chip, students will scan the chip with their mobile device, and the data will be stored and displayed for the lecturer on a visual web interface.

2.2 User Characteristics

- Basic IT knowledge for initial installation of mobile application.
- Knowledge of how to use mobile NFC technology.
- Ability to enter user details such as student name and student number.
- It can be assumed, and confirmed in practice, that a student's phone is set up with their personal email address, not their DCU email address. Therefore they must enter their DCU email address rather than the application retrieving it automatically from the device.

2.3 User Objectives:

- A simplified way of taking attendance in lectures and meetings.
- Easy to use and aesthetically pleasing UI.
- Straightforward process of verifying user via email.
- Ability to store user details to device to prevent multiple sign-ins. **(wish-list)**
- Ability for lecturers to personalise web interface timetable **(wish-list)**

2.5 Constraints

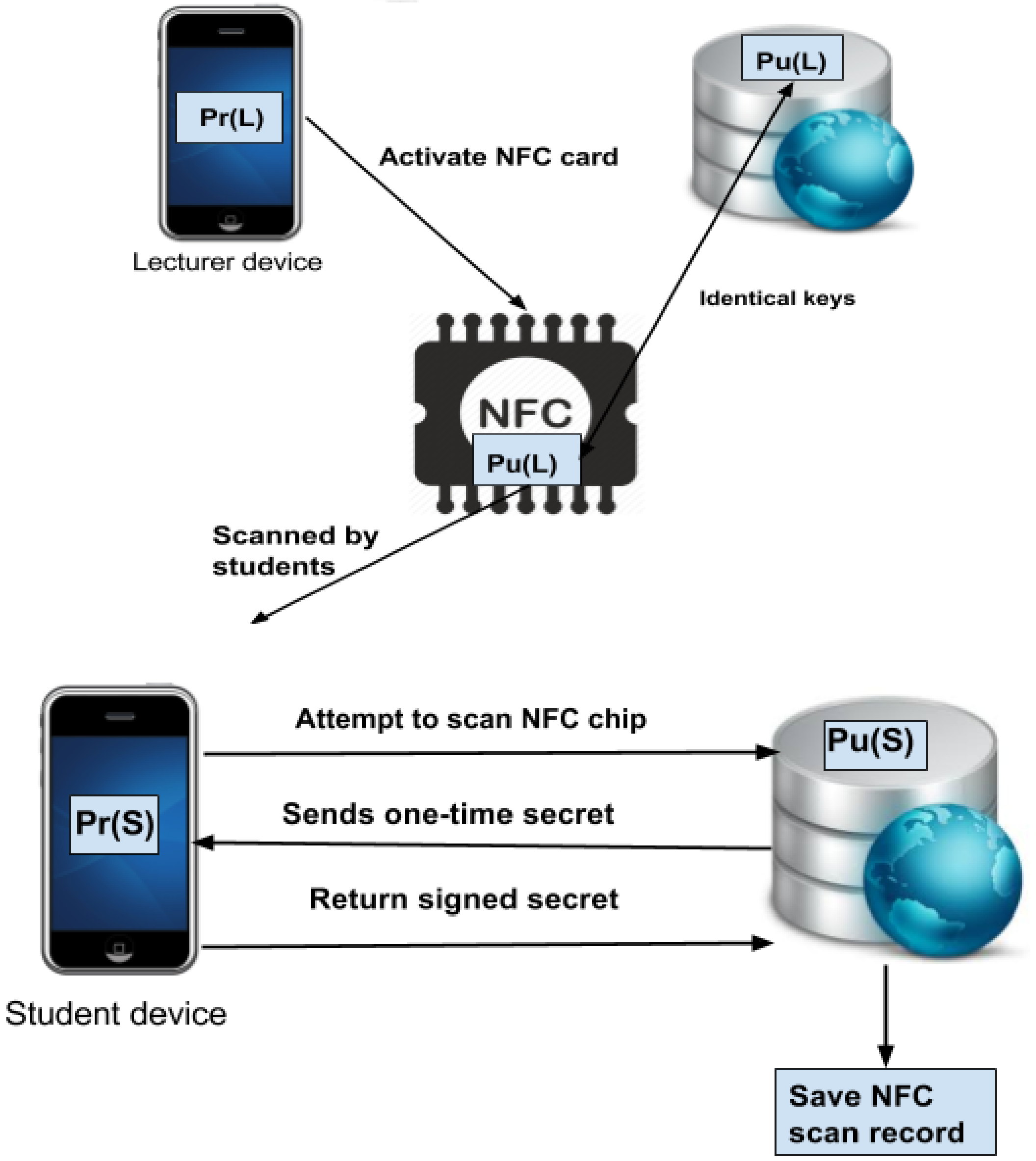
1. **IOS NFC technology**. Apple does not allow access to their devices NFC technology. This would suggest creating an Android only mobile application. A stretch feature would be another version of the app where the user scans a QR code found on the NFC card**.**
2. **Time.** The functional specification deadline is the 24th of November, and the project deadline is 21st of May. These deadlines of course limit the time to work on the project and any documentation to go with it.
3. **Internet connection.** Slow or no internet connection will affect the applications ability to send both verification data and NFC scan data to and from the application and the database. It will also affect the ability to create and test the system also.
4. **Cryptography.** This application will use private and public key generation for verification and security, but it is a new area of development and will need to be researched and attempted with trial and error.

2.6 Security and Authentication

It is intended to use public and private key generation in order to verify and authenticate users. Students will need to verify via DCU email that they are registered students of DCU. When they are verified, the student's public key is stored in the database.

The lecturer activates the NFC card via the application, the lecturers public key is stored on the NFC and in the database.

Key: Pr = Private Key, Pu = Public key, L = Lecturer, S = Student



The student has to prove who they are and that they have seen the lecturers NFC card. When they scan the NFC card, the database is alerted that a user is attempting to save data to the database. The database sends a piece of secret data for the users device to sign with the NFC chips unique code, the lecturers public key. This secret data is different each time to prevent a user from trying to replicate the message at another time. The user returns the signed secret, which proves the user has seen this NFC chip, the students private key is checked with their public key and their NFC scan can be recorded on the database.

2.4 Operational Scenarios

1. **Student signs up**	
Action	● Student installs and opens the app. ● The app prompts the student to enter their name and their DCU email address. ● An email is sent to this address with a URL which the student clicks on to verify themselves and the app is assigned to that name and email address.
Success	● A public/private key pair is created for when the student uses the app to scan tags. ● Student's name and DCU email address are saved to database. ● Student will now be able to scan NFC chips and their attendance will be recorded with their details
Failure	● User is not verified. ● User details are not stored in database ● Student cannot scan NFC chips

2. Scan NFC tag	
Action	● Student opens mobile app and scans lecturers NFC chip by holding tag close or against phone's NFC antenna. ● The public key online is checked with the students private key
Success	● User details (name, email) are saved to the database and the time and date is recorded. ● App indicates the NFC chip was read
Failure	● App indicates that scan had failed ● User details are not stored in database

3 .Lecturer signs up	
Action	● Goes to interface URL and enters name and email address.

	● An email is sent to this address with a URL which the lecturer clicks on to verify themselves.
Success	● This creates a private/public key pair that is used to log the lecturer into the interface. ● User details saved to database. ● Lecturer now has access to timetable interface .
Failure	● User is not verified. ● User details are not stored in database. ● Lecture cannot access web interface.

4. Lecturer accesses web interface	
Action	● Lecturer uses email address to sign into web interface. ● Private/public key pair linked to email is used for access.
Success	● A timetable is displayed, slots where the tag had been scanned are highlighted on the timetable.
Fail	● Interface alerts user sign-in was unsuccessful.

5. Activating NFC chip	
Action	● Lecturer access only. ● User hits “Activate NFC card” button. ● Tap NFC card to device.
Success	● Lecturer’s public key written and locked to the card. ● Card is now owned by the lecturer who activated the NFC card. ● Further taps of the NFC scan attendance.
Failure	● Card has already been written and locked. ● App indicates it cannot write to card.

3. Functional Requirements

3.1 Generate Public/Private Keys

- **Description -** Generating keys to
- **Criticality -** Very important. This cryptography will be used to authenticate verified users when they attempt to use the system.
- **Technical issues -** This is a new area of development and will involve research, trial and error.
- **Use Case Dependencies -** 1,2,3,4,5

3.2 Storing User Information

- **Description -** Storing the collected data in an online database.
- **Criticality -** Very Important. Product is useless if it cannot store data
- **Technical issues -** Unsure of what type of online database to use. The data could potentially build up to large amounts. The database could be wiped at the end of every semester or academic year.
- **Use Case Dependencies -** 1, 2, 3, 4

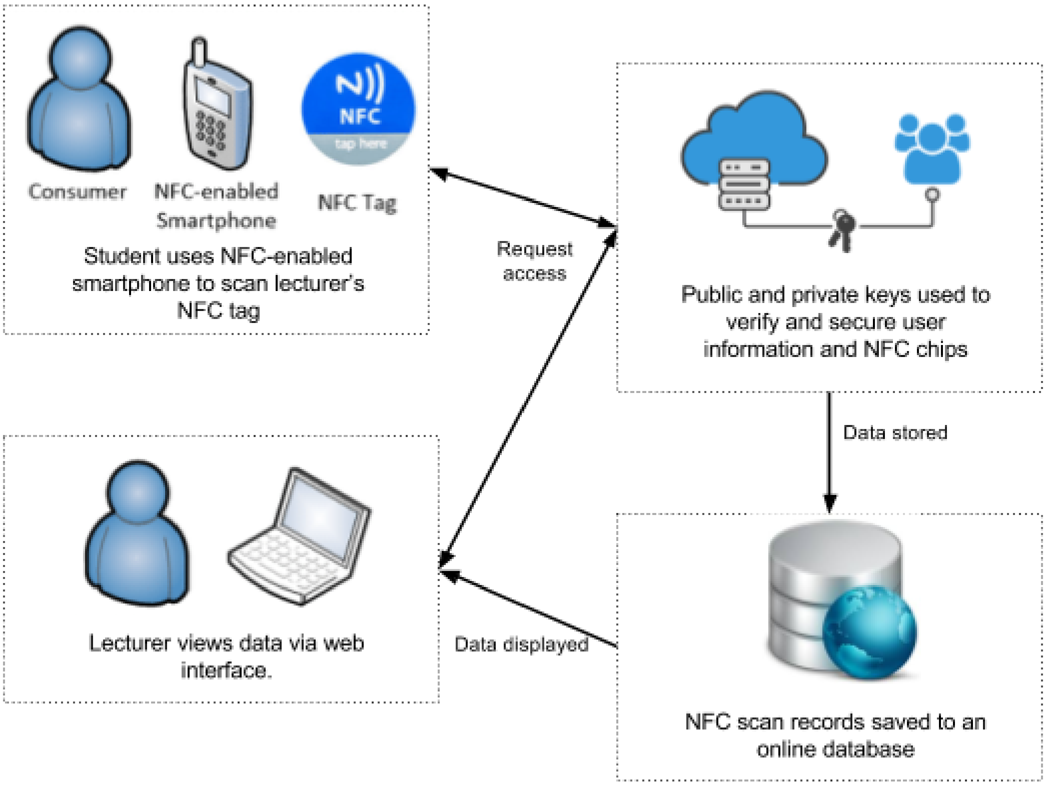
3.3 Validating user

- **Description -** This is the process of a student signing into the app for the first time. The user enters their DCU email address. A verification email is sent to the address, which contains a URL. Clicking this URL will send (something) back to the app to confirm the user is a DCU student. A public/private key is generated which will allow the user to scan the NFC chip with their details with no more configuration.
- **Criticality -** Important. Verifies and saves the user so no more configuration needed.
- **Technical issues -** User must use a DCU email, not personal email. The verification URL must send data back to the app.
- **Use Case Dependencies -** 1, 3

3.4 Display Data on Web Interface

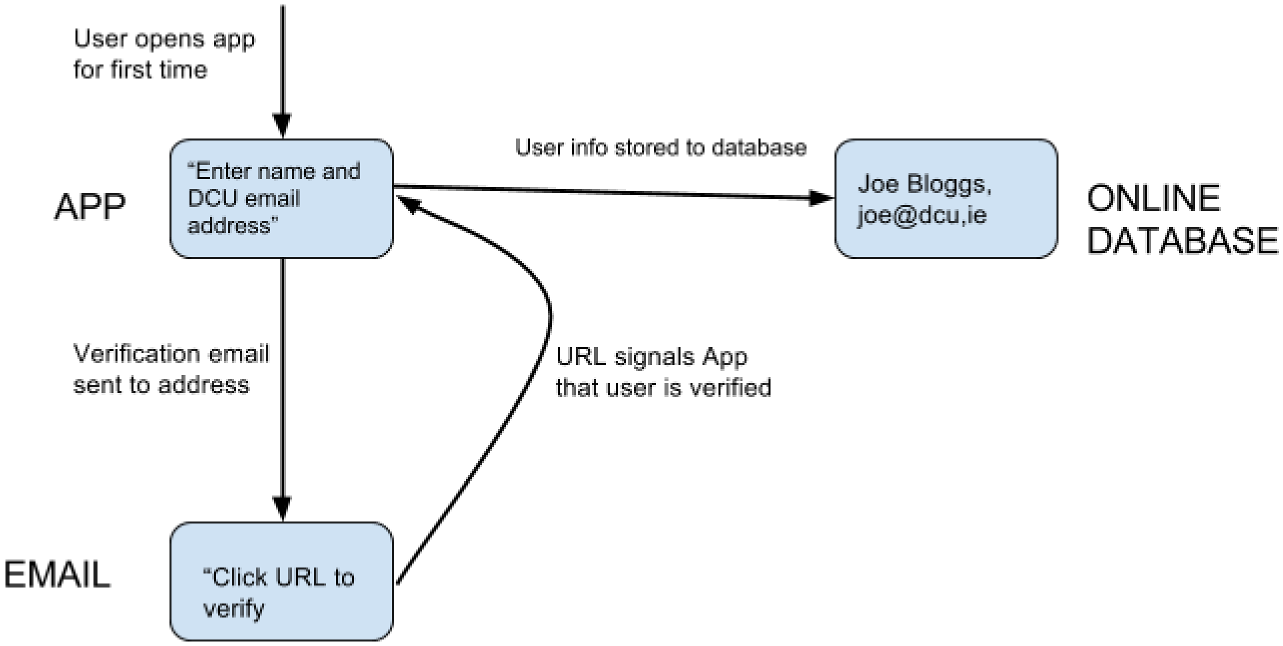
- **Description -** Keeping record of NFC scans is no use without somewhere to view the data. The stored data is taken and displayed in a visually timetable-styled format so that NFC card holders can view the attendance of their classes and meetings.
- **Criticality -** Important. Visual representation of the data collected.
- **Technical issues -** Unsure of what type of online database to use, as the data could potentially build up to large amounts. The database could be wiped at the end of every semester or academic year.
- **Use Case Dependencies -** 2, 3, 4

4. System Architecture

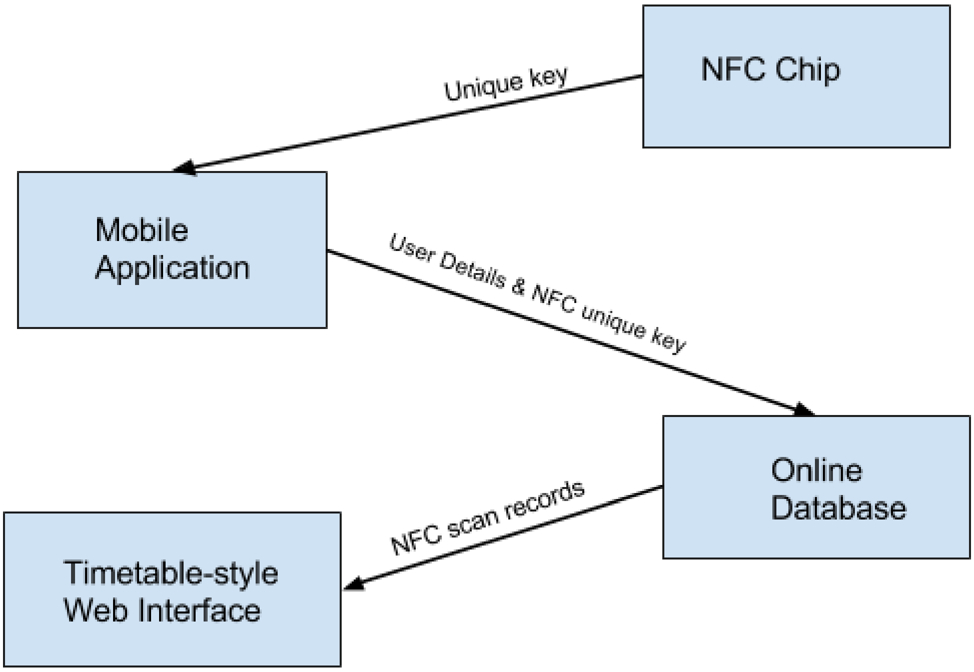

Consumer
NFC-enabled Smartphone
NFC Tag
N)) NFC tap here
Student uses NFC-enabled smartphone to scan lecturer's NFC tag
Request access
Public and private keys used to verify and secure user information and NFC chips
Data stored
Lecturer views data via web interface.
Data displayed
NFC scan records saved to an online database

5.High-Level Design

5.1 Verifying a new user


User opens app for first time
APP
"Enter name and DCU email address"
User info stored to database
Joe Bloggs, joe@dcu,ie
ONLINE DATABASE
Verification email sent to address
URL signals App that user is verified
EMAIL
"Click URL to verify

5.2 DFD of movement of data message when NFC is scanned



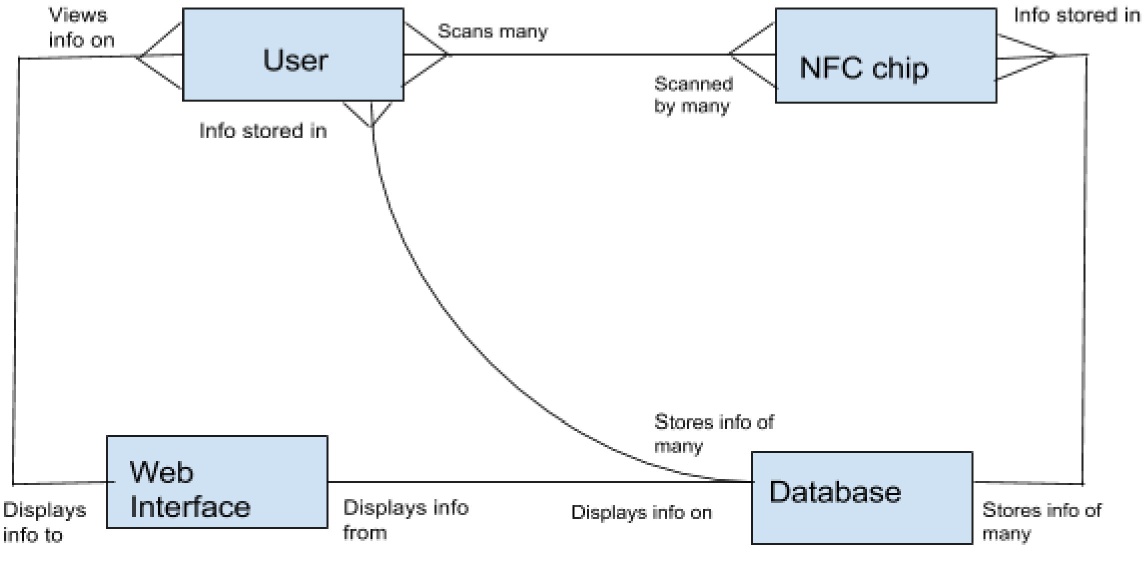
NFC Chip: A unique key is saved onto the NFC chip when activated by owner.

Mobile Application: User information stored on the application is taken with the NFC unique key when the chip is scanned with the device, and sent to an online database.

Online Database: This database has records of which NFC chips have been scanned, the time and date of the scan, which users device scanned the chip, etc.

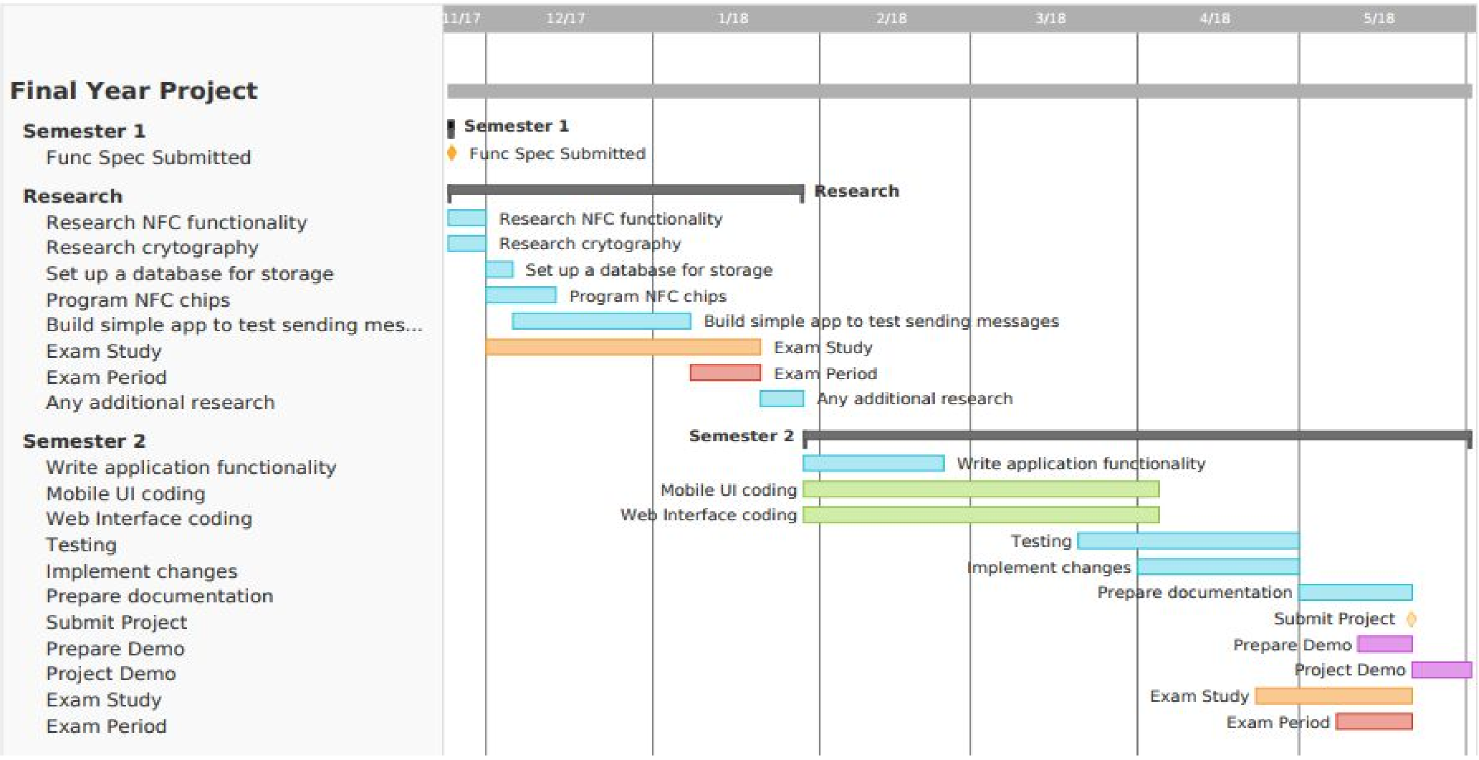
Web Interface: The information from the database is used to be displayed in a simple visual representation of the NFC chip owners timetable.

5.3 Logical Data Structure



6. Preliminary Schedule

6.1 Gannt Chart



7. Appendices

https://en.wikipedia.org/wiki/Near-field_communication
https://en.wikipedia.org/wiki/Public-key_cryptography
https://developer.android.com/training/articles/keystore.html