Project Semester 5 (IoT)

Socio-Technical Analysis Report

Project Title:	Smart Locker System with QR-Code Authentication
Student Name:	Loti Ibrahimi
Student Id:	20015453

1. Project Outline and Objectives

The QR Locker holds its purpose simply as a safe holding for personal items. Many places use standard lockers that make use of keys/locks, which by no means is a bad idea, however QR Lockers are another more appropriate means of identifying one's self.

The idea came about after a class discussion about having lockers for your personal belongings i.e. mobile phones etc. to store whilst in an exam hall. Due to multiple users, keys can be misplaced and lost, hence why having QR code lockers would be more suitable & convenient but also cheaper!

QR Codes are in use nowadays in a variety of ways & are becoming quite popular, be it for identity authentication (which is what I'll be looking at in this project) or as a way of sending mobile users to online content.

2. Functional Requirements

The QR Code Locker would be required to firstly access user accounts in an appropriate cloud database, containing user information as follows – Name, D.O.B, Phone, Personal Pin, QR Code.

This would mean registration is required in order to be eligible for locker use.

The QR Locker would make use of a standard lock (possibly controlled by a servo motor) which is triggered via built in camera. This camera is used for reading QR codes and verifying identification. Users are not only prompted to scan their QR code but to also input a pin (which would have been set during registration).

Make use of LEDs for identifying usage – Green: Available | Red: Occupied.

[Note: for this artefact demonstration purposes I will only be conceptually demonstrating the functionality above.]

3. Technologies Used

Below is a list of the software & hardware components that I intend to use for my project:

Hardware

- Raspberry Pi 3 Model B
- Servo Motor (Lock demonstration)
- Green/Red LEDs.
- Breadboard.
- Standard clip-on Webcam

Software

- QR Code generator
- OpenCV & ZBar (for scanning and decoding QR Codes)
- Python (Programming Language for this project)

4. Social Analysis and Issues

In this section I will be discussing the possible social, human, legal and ethical issues which may pertain to my project/artefact.

4.1. Privacy Issues

Possible security & privacy issues need to be taken into consideration, especially with this project. The whole objective of this artefact is to make sure it carries out its duty, keep users personal belongings SAFE! If there's a breach in that, we've got a big problem.

Although this artefact would primarily look towards possible security issues, there is also an element of privacy with when it comes to the use of QR codes.

Security is a key factor, as authentication needs to be carried out appropriately and effectively, especially if QR Codes are being used. Therefore two-factor authentication would be an important feature to prevent malicious use & copy of others QR codes.

4.2. Data Protection Issues

The 1980 OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" specifies 8 principles which one must adhere to. Regarding this project, data protection may primarily become an issue with QR Codes and data associated with them.

Possible data protection issues may result from QR codes storing personal information, as they can be scanned not only by the locker itself but also other users. Appropriate data needs to be stored on these QR codes in order to identify registered users but also to restrict exposure of personal information if scanned by another source.

To take care of this possible data protection issue, QR codes will only store a user ID. This ID would in turn be linked to a locker database of registered users, containing the associated user details & personal pin number.

Registered users would mainly be of an associated organisation/company, such as a school, college or gym etc. Only details necessary for proper identification should be collected, such as student number (if part of a college). This focusses on the 'Collection limitation principle' of OECD.

Personal user data must be relevant to the purpose they tend to be used for. In this case for identity authentication. User data needs to be only obtained for this use (locker identity authentication) only unless informed otherwise.

Registered user information (users eligible for locker use) that may be stored in an online database, may not be disclosed or used for other purposes unless stated otherwise & the user is informed/consents with changes.

4.3. Intellectual Property

All software and hardware components, that I intend to use for this project are not restricted by IPR, which may affect the creation of this artefact. QR code generators are open to public use and may be used in any personal apps/products, likewise with Raspberry Pi's & OpenCV/Zbar.

I don't think this project would infringe on copyrights if marketed, as there are many companies out there that deal with smart lock systems, in various forms, not only with QR codes. An example is Ubilock. They make smart security systems that work with – Card, Pin code, App, Iris Scan, Fingerprint, Bluetooth & NFC (Near-Field Communication). However, smart lockers are built by different companies worldwide.

The actual methods/forms of smart locking are not copyrighted, however, the ways in which these forms are implemented would be. (Coding, hardware builds etc.)

Fair use is in place as there are many different companies who deal with similar methods of smart locking. My personal project only deals with one of those methods (QR-Code Authentication) which is used widely in many different forms.

4.4. Stakeholder and Risk Analysis

The stakeholders of this project would be the likes of colleges, gyms, businesses, clubs etc. This project would be more so aimed towards these types of organisations due to it primarily being suitable for a larger user base & one that may find greater benefits with its uses.

Loss/theft of items whilst in use of this artefact would be impactful on the stakeholders, therefore security is a key and needs to be taken into consideration greatly.

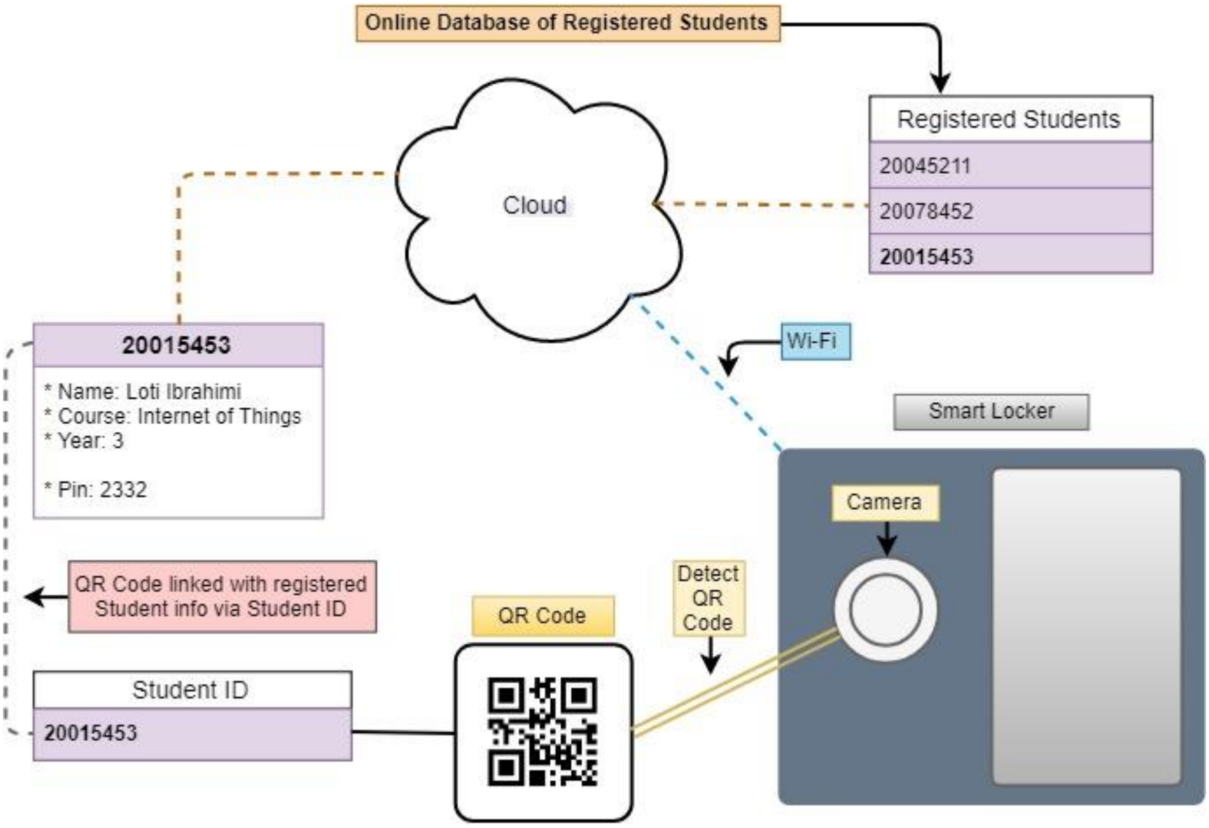
One positivity of this artefact being implemented, especially in a gym for example is that you do not need to carry a key around on you. Keys can also be lost/forgotten. QR Codes can be easily copied/retrieved.

5. Technical Analysis and Design

In this section I will present a technical analysis and design of my project.

5.1. Functional Design and Non-Functional Requirements

Visual Design Concept



The QR code locker is a smart lock system which may be implemented in different organisations such as schools, colleges, gyms, sports clubs or general clubs for that matter, businesses and workplaces.

It makes use of a cloud database which stores registered users that are eligible to make use of these lockers. Each user would have necessary personal details, including personal pin number associated with their accounts. Each user will receive a unique user ID, which is also assigned to a unique QR code.

For the purpose of this project I will be aiming this artefact primarily towards college use. Therefore, a unique ID is not necessary, as a student's number can be utilised instead.

The lockers are equipped with a motorised lock (servo motor) which is triggered by an authentication system that is implemented, in this case a camera for detecting QR codes.

Once a valid QR code is detected, the user is prompted to enter their pin – this two-factor authentication is simply an increased security precaution, that touches on the privacy issues previously mentioned.

5.2. Data Requirements and Design

The data for the smart locker database would be gathered via a web app or mobile app of the associated organisation. Users would need to be part of that establishment in order to register for a smart lock account.

Once they have registered with their personal details, pin, and generated a QR code, the data is then sent and stored in the cloud, possibly through mLabs. The smart lockers would read in this data via Wi-Fi, and process QR code requests accordingly.

This ties in with the data protection issues mentioned above previously, as those terms need to be taken into consideration.

6. Professional Conduct and Ethics

Even though there are many smart lock systems out there, if I were to develop this artefact into a fully marketable product, I would need to ensure a high degree of ethical professional conducts and behaviour.

In order to ensure these principles, I would start with the consumer or stakeholders of which my artefact is aimed towards. Respect for privacy is very important & one needs to also honour the confidentiality of others involved. In order for the system to be at its highest quality I must strive to achieve high quality in both the processes and products of professional work. Products, with regard to information that pertains to a consumer good, namely its price, quality, safety and security!

To achieve that high degree of ethical professional conduct I would also need to design and implement the system whereby it would be robustly and useably secure. All possible risks/cons of a certain system would need to be taken into consideration for it to become a fully marketable product.

I would finally also need to know and respect existing rules pertaining to the professional work in the area – smart safety systems/locks & possibly aim towards an ISO certification (a series of frameworks that help run a business effectively), to have that proof that this product complies with an ISO management standard.