DISPOSABLE NFC BRACELETS AND READER

ECE 445 Project Proposal

Team 42

Brennan Eng, Edson Alpizar, Ege Gunal

1. Introduction

1.1 Problem

Waterparks have an issue with optimizing their security, sales, and customer experience. The first example of a problem is customers who manage to sneak past staff and get in for free. There is no easy way to discern between a paying customer and someone who has just snuck in with a fake or old paper armband and even then there is always human error in identifying them. Another problem is if a consumer is currently in the water and becomes hungry they must travel back to their locker/chair to get their card/cash, go to the food stands to purchase the food, go back to their locker/chair to safely re-stash their belongings after eating, and only then can they finally go back to the water. Another niche example of a problem is if a parent loses their child within the park; usually there is no log of where to narrow down the search for the kid or any way to determine their last known location beyond observation.

Security and authenticated entry to events should always be a top priority for businesses for the safety of their customers as well as ensuring that they do not have a loss in profits. On top of this concern, there are not many comprehensive systems that combine both security, payment, and consumer data collection to optimize the experience for the consumer as well as streamline operations for the business.

1.2 Solution

Our solution involves constructing a system that uses cheap, disposable, and reprogrammable NFC bracelets that can be scanned with an NFC chip reader. The solution has two purposes: user-sided actions (to improve user customer experience), and

business-sided actions (to optimize profits and security). The purpose of the NFC bracelets for the user is to integrate a seamless low-latency experience for the consumer which takes care of access, payment, and other services if requested. On the other hand, the purpose of the NFC bracelet for the business is that invaluable data that is received from each interaction of the user. Depending on the use case, the NFC chip reader will then access a custom built consumer database that will carry out authenticated user-sided actions. The applications from a business perspective go so far as to use big data to determine localized traffic and popularity of events in a quantitative manner.

In addition to the reader and the bracelets, the goal is to create a display of utility by attaching the ultrasonic sensor system onto a door frame ensuring that the count of users entering the site in the database ends up matching that of the ultrasonic sensor.

1.3 Visual Aid

Our project consists of three primary systems, the user, server and board systems. The user system consists of a band with a NFC Tag.

Figure 1: Silicon band with area to insert NFC tag

The server system will use a raspberry pi to host a local server with databases containing user accounts and traffic. It will also be used to write to the user bands. When a new user is added, this information will be transmitted to each reader microcontroller through Wi-Fi.

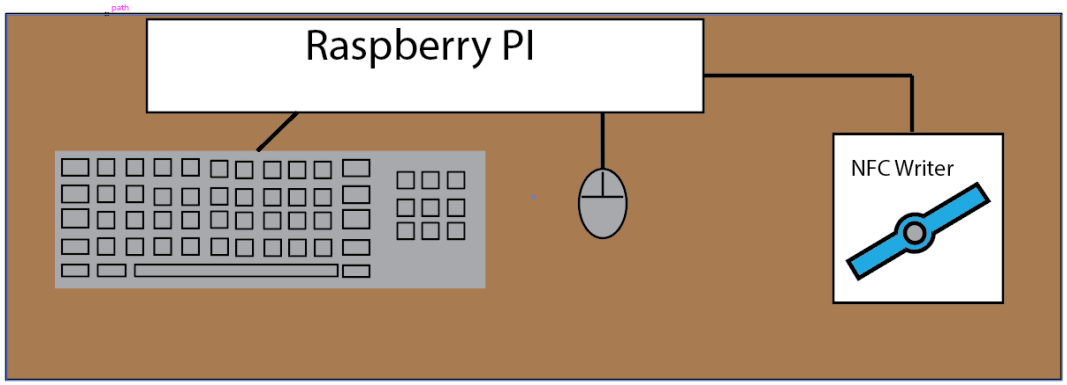

Figure 2: Example setup of server subsystem in the process of writing to NFC Band

The user will then approach the board system and tap their NFC band to the reader.

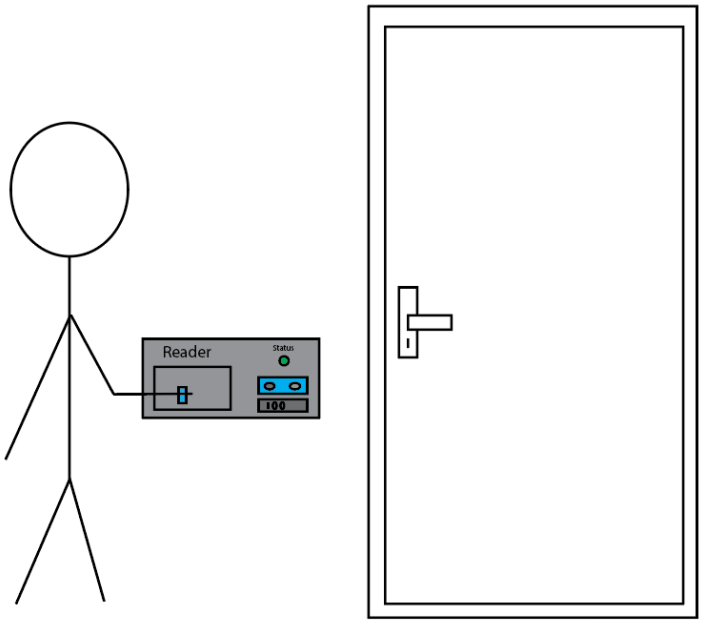

Figure 3: A different implementation of our nfc door opening mechanism, where it is used to open an office door rather than a pool turnstile

The board system will store user logs, and send them to the server through Wi-Fi on a regular basis.

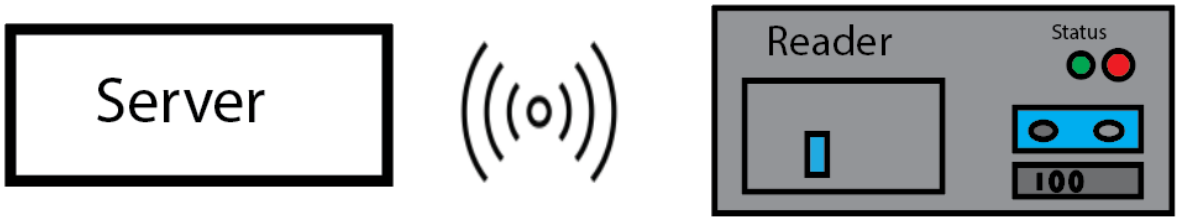

Figure 4: Wireless communication between server and microcontroller

If the user is recognized, the status LED will turn green. After the user passes through the ultrasonic sensor, causing the distance reading to fluctuate, the LED display counter will increment.

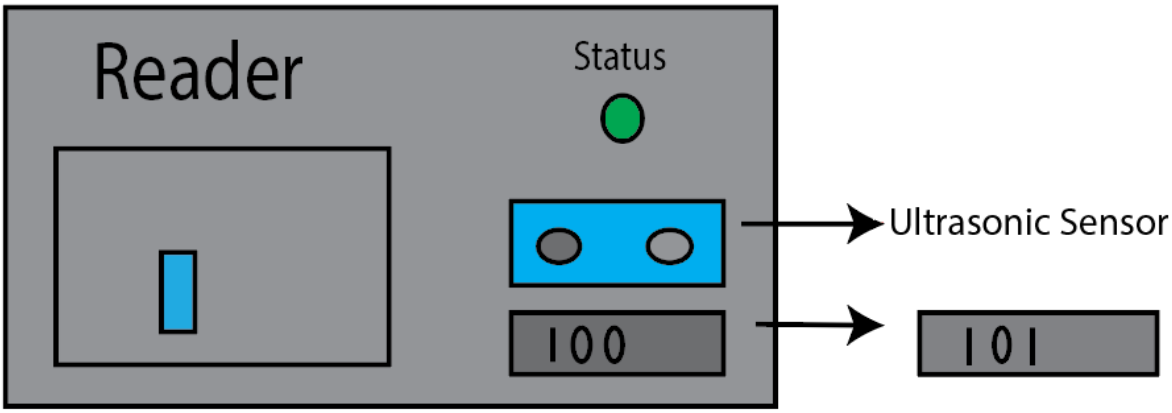

Figure 5: Incrementing person counter after a user gets access and ultrasonic sensor verifies a single person is passing through

1.4 High-level requirements list

- Our NFC bands need to check if a user has access with a millisecond-level latency.
- Our NFC bands need to detect when someone with/without access attempts to pass through checkpoints via LEDs, and store this information in a central database that gets cleared on a semi-regular basis.
- Our entry checking mechanism needs to accurately count people who enter, and alert when someone follows another person without tapping their NFC band, this will be done via ultrasonic sensors.
- Our NFC bands need to be linked to a central database linked to user accounts, to which food stalls can send the appropriate billing.

2. Design

2.1 Block Diagram

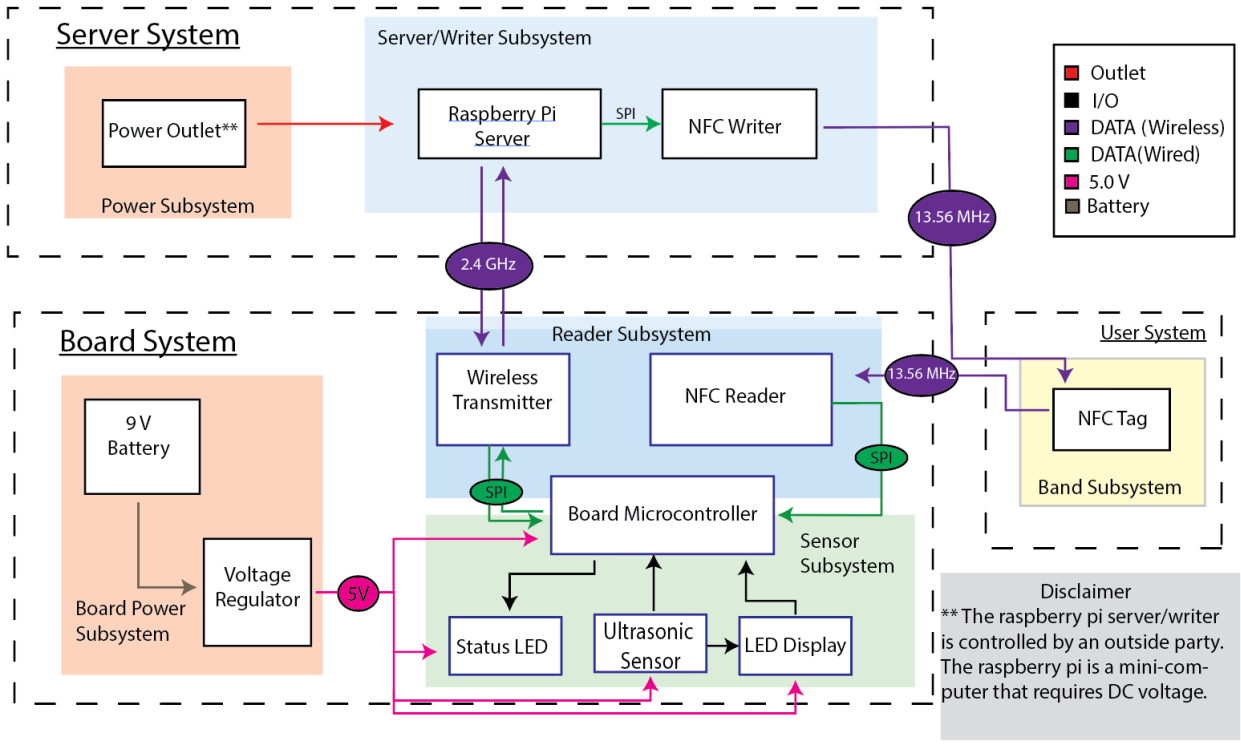

Figure 6: Block Diagram

2.2 Subsystem Overview

2.2.1 Board Power/Server Power

The power subsystem will only be used to power the Raspberry Pi. The raspberry pi will be connected to a power outlet. The board power subsystem is different since this component will power up both the Reader and Sensor Subsystems. We will accomplish this by using a 9V battery and voltage regulator to channel appropriate voltages.

2.2.2 Server/Writer

The Server/Writer subsystem contains the raspberry pi and the NFC writer. The server will be stored locally onto the raspberry pi. Since the pi is a computer we will connect the writer to it so we can program the NFC tags with the necessary information. The server system will also communicate with the reader system wirelessly to update readers' local databases and to receive customer traffic information.

2.2.3 Reader

The reader subsystem contains the wireless transceiver, NFC reader and microcontroller. This subsystem interacts with the user system when the NFC tag comes into contact with the NFC reader. That information will be sent to the server system wirelessly to determine if the user is eligible to enter a particular location. The eligibility information will then affect the output of the sensor subsystem.

2.2.4 Sensor

This is the physical access portion of the project where users will access a door if given access by the reading subsystem. The sensor will use an LED indicator that will light up green if the eligibility information from the reading subsystem is true and light up red if it is false. Once a person walks through a door the ultrasonic will pick up that interference and send that information back to the microcontroller for further security purposes, also incrementing the counter on the display.

2.3 Subsystem Requirements

2.3.1 Board Power/Server Power

2.3.1.1 Server Power

- Standard Raspberry pi power adapter

2.3.1.2 Board Power

- Down convert 9V battery input to 5V and fix it there using a Zener Diode
- Buffer some energy in a large capacitor to ensure safe microcontroller shutdown when battery runs out/is taken out

2.3.2 Server/Writer

- Store user information in a database
- Generate a unique UIDs and write that UID onto NFC tags
- Send new users to each reader subsystem through Wi-Fi
- Receive entry logs from reader subsystems and store them in a central database

2.3.3 Reader

- Receive new user information from Wi-Fi and send them to the board microcontroller via SPI
- Receive NFC UID from user arm bands and share it with the board microcontroller via SPI
- Determine if user is eligible to enter for sensor subsystem to act on

2.3.4 Sensor

- Count people passing through and send that information to the microcontroller

- Display whether someone has access on LEDs, as determined by the microcontroller
- Display the number of people who entered on LED Display

2.4 Tolerance Analysis

A potential risk to the completion of the project would be the failure to read/write the NFC bands with the unique ID in order for the security system to read them correctly to perform a specific task. The issue at hand is ensuring the bands are reprogrammed and overwritten correctly so when the reader scans the band, the system accesses the ID without any issues and performs the task. With this issue, ensuring that the bands are reprogrammed correctly requires our group to heavily research which NFC bands are the best at being reprogrammed as well as a device that can write the values that we require onto the band itself. Wireless components are sometimes a risk due to it being susceptible to interference. That being said, the risk should be mitigated by ensuring our systems optimize the range and accuracy from which we scan these bands in order to reduce the risk of failure.

Some potential risks to the widespread use of our project is working with wireless protocols and ensuring that reader microcontrollers will always get necessary updates to their local user databases. We will be researching how wireless protocols operate to reduce our system's susceptibility to wireless connectivity issues, as well as potentially encrypting each signal to reduce malicious attempts to replicate our NFC arm bands.

3. Ethics and Safety

One potential exposure in our project is the data aggregation of user interactions within the premise of a business. It is a concern because it presents the risk of exposure of customer privacy if not handled correctly. These factors may pose a threat to the privacy of others as well as the mishandling of financial data if payment systems are involved. While these devices pose no physical threat to a user or its customer, the database records and stores all interactions of consumers for the business to make more sound decisions based on the business intelligence it has gathered. That being said, while the data belongs to the business, the release of that data may pose a threat to those involved. To reduce the risk of data breaches, a comprehensive cybersecurity system is necessary as well as vetting of businesses who intend to use these products for malicious purposes. We will also need to ensure anonymity of long-term stored data and further investigate privacy concerns over data we store, such as California State Law that has a strict emphasis on data privacy.