DETI Access Control System

Group 8:

- Rui Lameiras 102817
- Rafael Santos 98466
- Vladyslav Mysnyk 97548
- Gonçalo Sousa 98152
- Leandro Rito 92975

Coordinators:

- Pedro Fonseca
- André Zúquete

Projeto de Engenharia de Computadores e Informática

Index

- Context
- Problems
- Goals
- Project Timeline
- Tasks
- Solution
- Expected Results
- Scope and Related Work
- Communication Plan

Context

- Keycards are one of the most used systems in the world.
- But like everything it has its flaws…
- What about your phone?

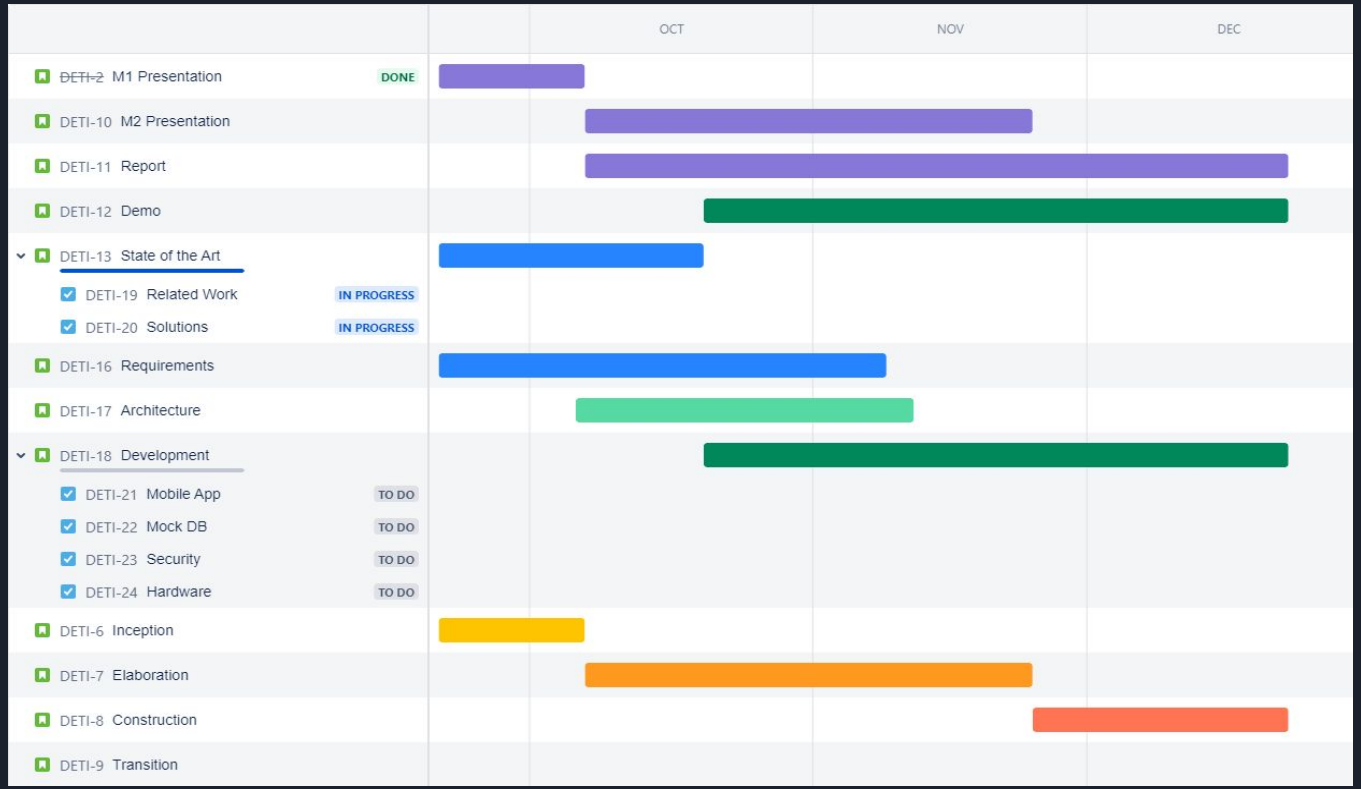
Problems

- Hardware Costs
- Human Factors
- Ease of Use
- Implementation Efficiency
- System Weaknesses

Goals

- Mobile app for interacting with the door's hardware and the back-end (our group).
- Having a functional door access control system (project as a whole)

Project Timeline



Tasks

- Task 1 (all) - Define the project timeline
- Task 2 (all) - Search and propose solutions
- Task 3 (all) - Search related works
- Task 4 (2/3) - Program the hardware
- Task 5 (2/3) - Create a mobile app
- Task 6 (2/3) - Create a mock database

NFC

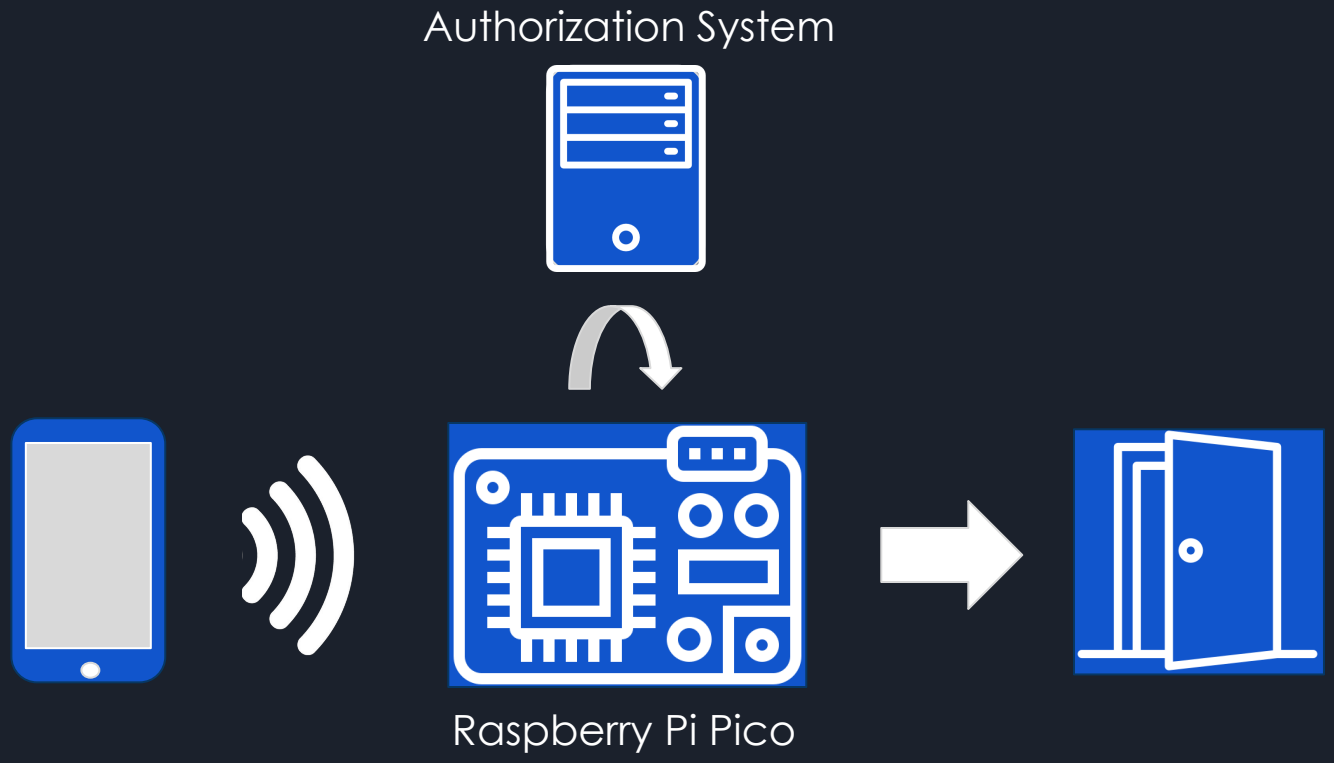
Pros

- Low Cost
- Easy to Use
- Efficient

Cons

- Availability

NFC



Wi-fi (backup)

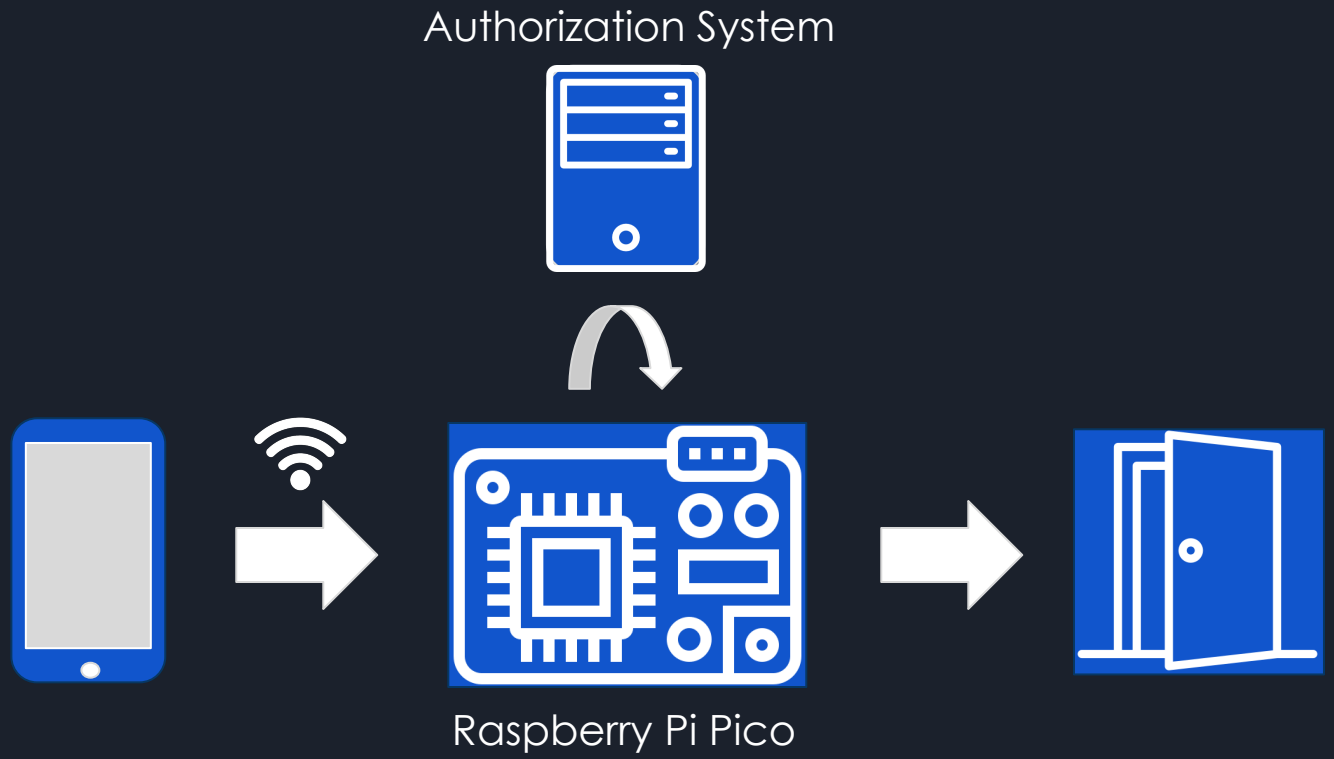
Pros

- No Cost
- Availability

Cons

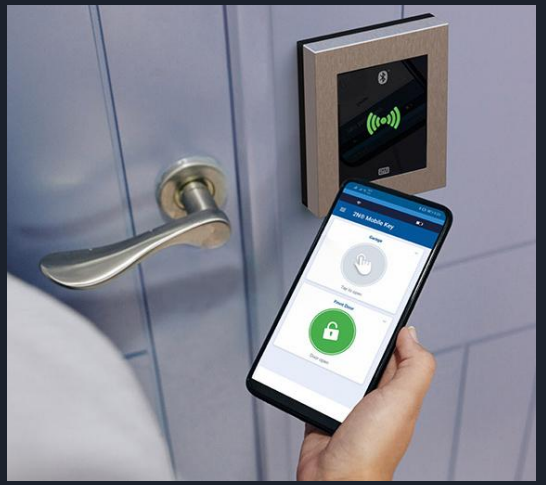
- Has more steps
- Less secure

Wi-fi (backup)



Expected Results

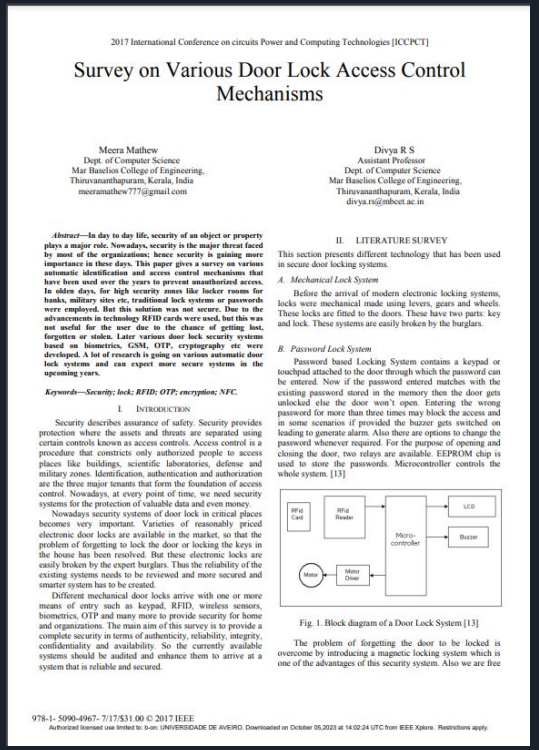
- Functional mobile app
- Mock Database
- Safety measures



Scope and Related Work

- https://ieeexplore.ieee.org/abstract/document/8074187 - Door Lock Access Control Survey
- https://ieeexplore.ieee.org/document/9213475 - DES encrypted QR Code Access Control System
- https://ieeexplore.ieee.org/document/7009188 - NFC Access Control System

Scope and Related Work



2017 International Conference on circuits Power and Computing Technologies [ICCPCT]

Survey on Various Door Lock Access Control Mechanisms

Meera Mathew
Dept. of Computer Science
Mar Baselios College of Engineering,
Thiruvananthapuram, Kerala, India
meeramathew777@gmail.com

Divya R S
Assistant Professor
Dept. of Computer Science
Mar Baselios College of Engineering,
Thiruvananthapuram, Kerala, India
divya.rs@mbcet.ac.in

***Abstract*—In day to day life, security of an object or property plays a major role. Nowadays, security is the major threat faced by most of the organizations; hence security is gaining more importance in these days. This paper gives a survey on various automatic identification and access control mechanisms that have been used over the years to prevent unauthorized access. In olden days, for high security zones like locker rooms for banks, military sites etc, traditional lock systems or passwords were employed. But this solution was not secure. Due to the advancements in technology RFID cards were used, but this was not useful for the user due to the chance of getting lost, forgotten or stolen. Later various door lock security systems based on biometrics, GSM, OTP, cryptography etc were developed. A lot of research is going on various automatic door lock systems and can expect more secure systems in the upcoming years.**

Keywords—Security; lock; RFID; OTP; encryption; NFC.

I. Introduction

Security describes assurance of safety. Security provides protection where the assets and threats are separated using certain controls known as access controls. Access control is a procedure that constricts only authorized people to access places like buildings, scientific laboratories, defense and military zones. Identification, authentication and authorization are the three major tenants that form the foundation of access control. Nowadays, at every point of time, we need security systems for the protection of valuable data and even money.

Nowadays security systems of door lock in critical places becomes very important. Varieties of reasonably priced electronic door locks are available in the market, so that the problem of forgetting to lock the door or locking the keys in the house has been resolved. But these electronic locks are easily broken by the expert burglars. Thus the reliability of the existing systems needs to be reviewed and more secured and smarter system has to be created.

Different mechanical door locks arrive with one or more means of entry such as keypad, RFID, wireless sensors, biometrics, OTP and many more to provide security for home and organizations. The main aim of this survey is to provide a complete security in terms of authenticity, reliability, integrity, confidentiality and availability. So the currently available systems should be audited and enhance them to arrive at a system that is reliable and secured.

II. Literature Survey

This section presents different technology that has been used in secure door locking systems.

A. Mechanical Lock System

Before the arrival of modern electronic locking systems, locks were mechanical made using levers, gears and wheels. These locks are fitted to the doors. These have two parts: key and lock. These systems are easily broken by the burglars.

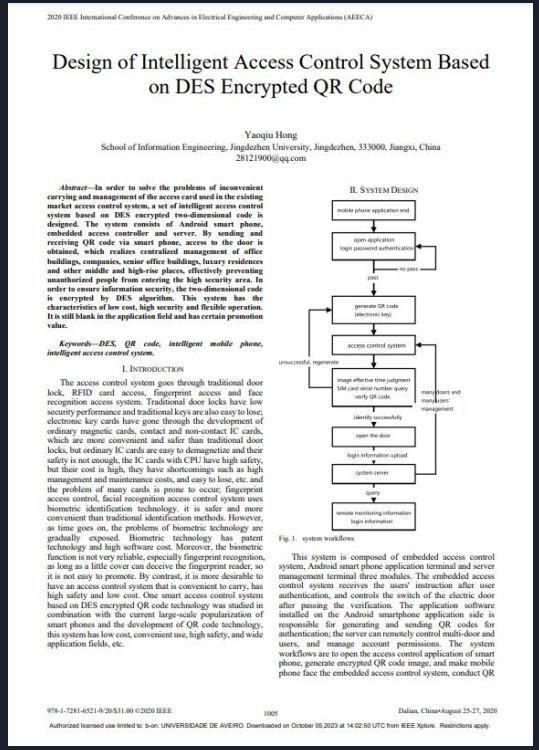
B. Password Lock System

Password based Locking System contains a keypad or touchpad attached to the door through which the password can be entered. Now if the password entered matches with the existing password stored in the memory then the door gets unlocked else the door won't open. Entering the wrong password for more than three times may block the access and in some scenarios if provided the buzzer gets switched on leading to generate alarm. Also there are options to change the password whenever required. For the purpose of opening and closing the door, two relays are available. EEPROM chip is used to store the passwords. Microcontroller controls the whole system. [13]

Fig. 1. Block diagram of a Door Lock System [13]

The problem of forgetting the door to be locked is overcome by introducing a magnetic locking system which is one of the advantages of this security system. Also we are free

978-1- 5090-4967- 7/17/$31.00 © 2017 IEEE



2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)

Design of Intelligent Access Control System Based on DES Encrypted QR Code

Yaoqiu Hong
School of Information Engineering, Jingdezhen University, Jingdezhen, 333000, Jiangxi, China
28121900@qq.com

***Abstract*—In order to solve the problems of inconvenient carrying and management of the access card used in the existing market access control system, a set of intelligent access control system based on DES encrypted two-dimensional code is designed. The system consists of Android smart phone, embedded access controller and server. By sending and receiving QR code via smart phone, access to the door is obtained, which realizes centralized management of office buildings, companies, senior office buildings, luxury residences and other middle and high-rise places, effectively preventing unauthorized people from entering the high security area. In order to ensure information security, the two-dimensional code is encrypted by DES algorithm. This system has the characteristics of low cost, high security and flexible operation. It is still blank in the application field and has certain promotion value.**

Keywords—DES, QR code, intelligent mobile phone, intelligent access control system.

I. Introduction

The access control system goes through traditional door lock, RFID card access, fingerprint access and face recognition access system. Traditional door locks have low security performance and traditional keys are also easy to lose; electronic key cards have gone through the development of ordinary magnetic cards, contact and non-contact IC cards, which are more convenient and safer than traditional door locks, but ordinary IC cards are easy to demagnetize and their safety is not enough, the IC cards with CPU have high safety, but their cost is high, they have shortcomings such as high management and maintenance costs, and easy to lose, etc. and the problem of many cards is prone to occur; fingerprint access control, facial recognition access control system uses biometric identification technology. it is safer and more convenient than traditional identification methods. However, as time goes on, the problems of biometric technology are gradually exposed. Biometric technology has patent technology and high software cost. Moreover, the biometric function is not very reliable, especially fingerprint recognition, as long as a little cover can deceive the fingerprint reader, so it is not easy to promote. By contrast, it is more desirable to have an access control system that is convenient to carry, has high safety and low cost. One smart access control system based on DES encrypted QR code technology was studied in combination with the current large-scale popularization of smart phones and the development of QR code technology, this system has low cost, convenient use, high safety, and wide application fields, etc.

II. System Design

Fig. 1. system workflows

This system is composed of embedded access control system, Android smart phone application terminal and server management terminal three modules. The embedded access control system receives the users' instruction after user authentication, and controls the switch of the electric door after passing the verification. The application software installed on the Android smartphone application side is responsible for generating and sending QR codes for authentication; the server can remotely control multi-door and users, and manage account permissions. The system workflows are to open the access control application of smart phone, generate encrypted QR code image, and make mobile phone face the embedded access control system, conduct QR

978-1-7281-6521-9/20/$31.00 ©2020 IEEE

Dalian, China•August 25-27, 2020

Scope and Related Work

NFC-enabled Access Control and Management System

Nurbek Saparkhojayev
Department of Information Technology
Almaty Management University
Almaty, Kazakhstan
nursp81@gmail.com

Aigul Dauitbayeva
Department of Computer Engineering and Information Systems
Korkyt Ata Kyzylorda State University
Kyzylorda, Kazakhstan
aicos@mail.ru

Aybek Nurtayev
Department of Computer Science and Software Engineering
International IT University
Almaty, Kazakhstan
nur4i@mail.ru

Gulnaz Baimenshina
Department of Applied Physics
K.I. Satpayev Kazakh National Technical University
Almaty, Kazakhstan
baimenshina@mail.ru

***Abstract*— In today's world, we always carry all sorts of keys and addition to them, we use pass cards as well. Moreover, we keep all of them in our pockets or wallets; they occupy a lot of space and weigh a lot. In addition to this, we carry gadgets (smart phones, tablets, smart watches, etc.) which are essential in today's life. After thinking all these issues, authors came up to the idea of replacing usual keys by smartphones to use for opening/closing and locking/unlocking doors. Smartphones have already used as mobile payments. Most of the modern mobile devices are equipped with NFC module, and by using such devices, it is possible to get rid of carrying heavy, metal keys, pass-cards, etc. People often forget keys at home and they are relatively small and easy to lose. Instead of carrying all these keys, we present an NFC- enabled Access Control and Management System, which by the help of mobile devices, NFC technology and HCE mode, introduced in Android 4.4, makes possible for people to use only one single key. ISO 7816-4 smart card standard is used for emulation a smart card and the data exchange between the mobile device and NFC-reader.**

***Index Terms*— NFC- technology, smart phones, Android, Access control and management system;**

I. Introduction

In today's fast- growing technology world, most of mobile devices are equipped with wireless modules, which are potential way of solving the problems with keys. Almost all of them are equipped with Bluetooth and infrared technologies, latest ones have NFC installed on-board. Compared to other short-range technologies, NFC has the following advantages:

- Slow speed and short range: this allows NFC to consume as little power as possible so it can be left on at all times and not affect the phone's battery by that much (vs. Bluetooth);
- hassle-free approach to connections: with NFC, bringing the two devices within range is enough to facilitate the communication between the two (vs. Bluetooth);
- free-line of sight: no direct line of sight is required to establish connection (vs. Infrared) [1].

NFC-enabled Access Control System will let the people lock/unlock doors just by tapping mobile device to NFC reader. It will also perform all the functionality that other ACMS's do, such as logging entrance time, controlling access privileges, etc. This system can be used as:

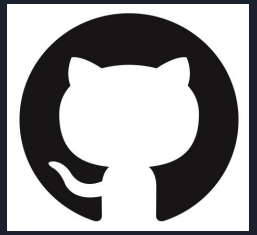
- Independent and complete ACMS (Access Control and Management System;
- The system for checking attendance of students in educational institutions, as well as observation of student's location within the institution;
- Small ACMS for home, as an addition to "smart house" system.

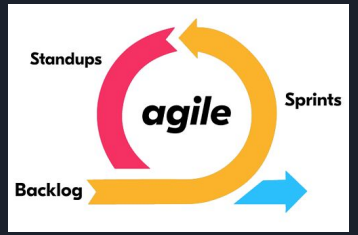
NFC is one of the popular latest wireless communication technologies. The big advantage of the short transmission range is that it inhibits eavesdropping on NFC-enabled transactions. NFC technology opens up exciting new usage scenarios for mobile devices [2]. Until recently, payments using smart phones were possible using NFC card emulation combined with secure elements (see Figure 1). Traditionally, you would have to store security information, for example the security keys from debit card (which are stored in the tamper resistant card chip) in a similarly tamper resistant chip on your device – the Secure Element. The Secure Element emulates the card and can be found either on the SIM card or in a chip embedded in the phone handset. When NFC card emulation is provided using a secure element, the card to be emulated is provisioned into the secure element on the device through an application. Then, when the user holds the device over an NFC

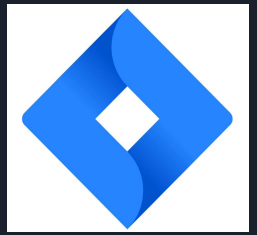
978-1-4799-5739-2/14/$31.00 ©2014 IEEE

Communication Plan

- Discord
- Github
- Agile
- Jira







Thanks for your attention!

and

Q&A