International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

EasyKey - Multipurpose RFID Card based IoT System

Abhinav[1], Abhinav Kumar[2], Akshari Nidugala[3], Mridul Ganga[4]

[1,2,3,4]*B.E., Department of Information Science and Engineering, The National Institute of Engineering, Mysuru, India*

Abstract - *We often find our wallets overloaded with many different cards that serve various purposes. The handling and monitoring of all these cards becomes a very cumbersome task. We end up misplacing one or the other card, or we end up forgetting a particular card at home. Our project aims to solve this issue that we face. This project proposes the use of a single card that will perform the operations of some of the cards that we possess. Basically, we are promoting the use of a single card in place of some cards. This way, we can easily keep track of a single multipurpose card instead of keeping tab of multiple cards. This project proposes a system called EasyKey that uses RFID (Radio Frequency Identification Reader) cards, which can be used along with a wide range of applications. The project provides Two Factor Authentication using a mobile device and allows the user to list all the authentication requests on a mobile application.*

Key Words: EasyKey, multipurpose card, RFID, Two Factor Authentication

1. INTRODUCTION

Our project EasyKey proposes the use of a single RFID (Radio Frequency Identification Reader) card to perform the operations of Authentication and Payment cards. This is how the EasyKey card can be used- when the user visits a store he/she can make payments using the card, when the user visits a hospital he/she can register using the same RFID card all the operations must go through the mobile device for authentication. The authentication will be two factor authentication for privacy and security purposes.

Radio-frequency identification (RFID) uses electromagnetic fields to identify and track tags attached to objects automatically. Electronically stored information is maintained in the tags. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source and may operate from several meters from the RFID reader. The tag need not be within the line of sight of the reader unlike a barcode, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture.

Two-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two pieces of factors to complete and authentication. It is a method of confirming identities claimed by users by using a mixture of two different factors: 1) something they know, 2) something they have, or 3) something they are. An example of two-factor authentication is withdrawing of money from an ATM machine; only the correct combination of a bank card (something the user has) and a PIN (something the user knows) allows the transaction to be carried out.

2. SYSTEM DESCRIPTION

The system comprises of the following components-

- Application at user end
- A device on the vendor's end
- Vendor database
- API Server
- EasyKey database

The user swipes his/her card at a vendor's machine device. The vendor's device receives a RFID code. The system uses a Two Factor Authentication for confirmation. The first factor of authentication is met when the vendor device makes an authentication request to EasyKey server. The EasyKey receives the request and puts it into its database. The EasyKey server then sends a authentication request to the user's mobile device. This satisfies the second authentication factor. The user then reviews and performs action accordingly. The user either accepts or declines the transaction. If the transaction is accepted, the vendor device is notified of a "Successful transaction". If the transaction is declined, the vendor device is notified of an "Unsuccessful transaction".

3. EXISTING SYSTEM

There have been numerous systems designed that make use of RFID cards.

- RFID technology has been used to simulate smart trolleys that can be used in supermarkets, in order to alleviate the time consuming process of a bar code scanner at the cash counter.
- RFID technology has also been used in development of a smart library management system in order to allow fast transactions like issue and return of books by reducing manual intervention as far as possible.
- RFID tags have also been used alongwith ZigBee and NFC systems to bring about smart shopping experiences for user by helping new users in

selecting shopping items according to popularity and demand.

4. PROPOSED APPROACH

4.1 Block Diagram

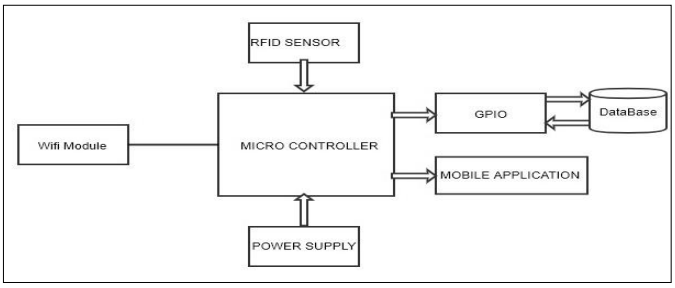


Fig 1- Block diagram of system

4.2 Hardware design

The Hardware Design contains Raspberry pi, RFID reading sensor and few RFID cards. With this system, the user will be able to authenticate himself/herself to places like hospitals. Users can also make payments to vendors at shops. At first, the user will have to register himself/herself by filling all the necessary details.

The raspberry pi is connected to the RFID sensor and wifi. The RFID card is scanned through the sensor. The unique ID of the card will be stored in the database and the user will be asked to fill in personal credentials like Name, Email, Phone number, Aadhar number, PAN number and billing and communication address. The user will also be asked to enter payment details like UPI ID.

Now, when the user scans the RFID card at any vendor,'s device the ID will be matched to the database and the user will get a notification on his/her registered mobile number to authenticate the request. The request will then be authenticated. For payments, the user will get a notification on mobile for either accepting or declining the payment.

The Raspberry pi is connected to the web server via the wireless network. The web server is connected to the database as shown in the block diagram.

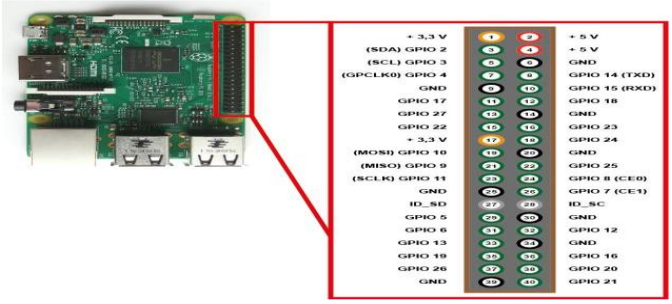


Fig 2- Raspberry pi setup

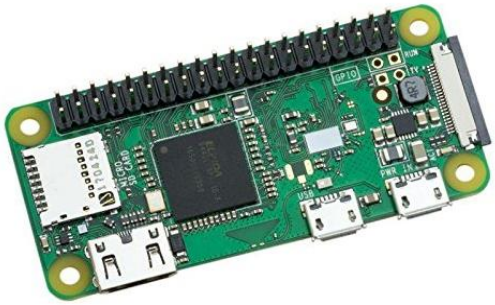


Fig 3- Raspberry pi setup

Fig 4-RFID Sensor

4.3 Software design

The mobile application will have the following design-

THE HOME PAGE:

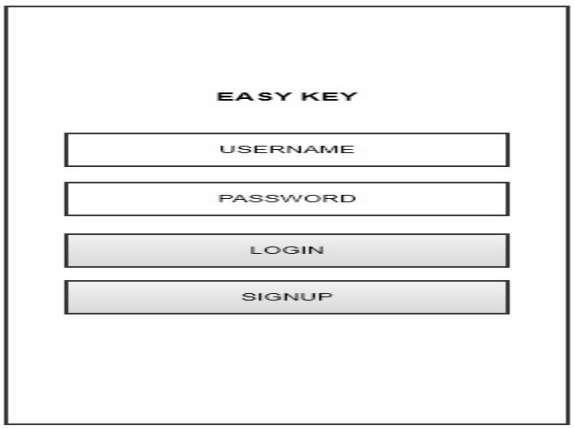
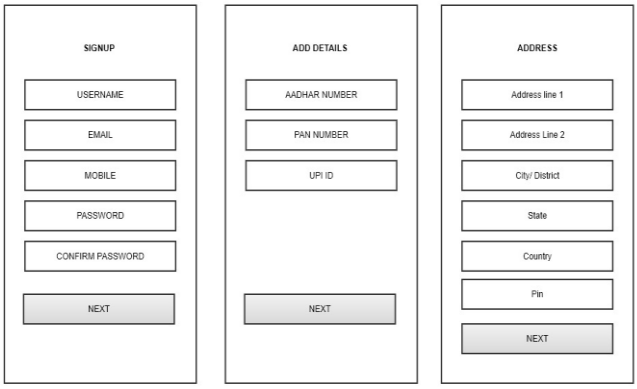


Fig 5- Home page of application

THE SIGN UP PROCESS



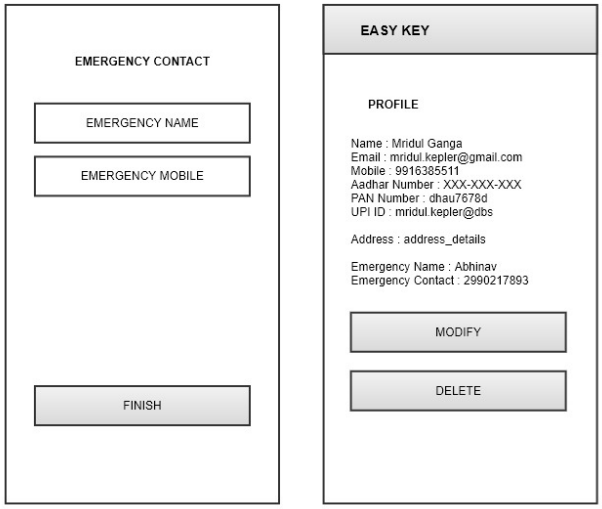


Fig 6- Sign Up Process

AFTER LOGIN

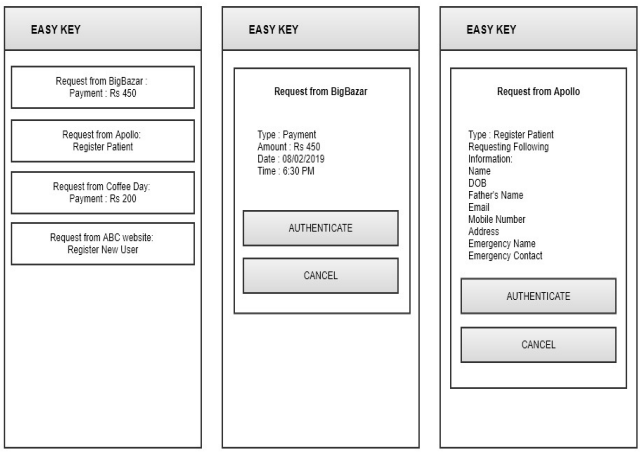


Fig 7- Login and payment

AFTER TRANSACTION

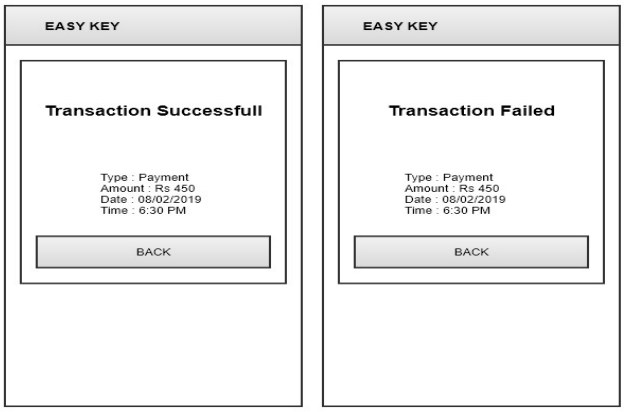


Fig 8- Transaction success or failure

CODE SNIPPET FOR SERVER THAT CONNECTS TO DATABASE

4.4 Database

The entity relationship of the database used in this system is shown below:

```
This is the code for server that connects the database.
The code is written in python.

from flask import Flask, g, render_template, request, redirect
import pyrebase

config = {
  "apiKey": "AIzaSyDsoYLse6FrkbClDm-C0BoLg_m7U0yyBps",
  "authDomain": "easykey-160212.firebaseapp.com",
  "databaseURL": "https://easykey-160212.firebaseio.com",
  "storageBucket": "easykey-160212.appspot.com"
}
app = Flask(__name__)
firebase = pyrebase.initialize_app(config)
db = firebase.database()

def add_firebase_entry(source,uid):
    db.child("auths").child(source).child(uid).set("none")
    return 'added'

def remove_firebase_entry(source,uid):
    db.child("auths").child(source).child(uid).remove()
    return 'removed'

def get_firebase_entry(source,uid):
    return db.child("auths").child(source).child(uid).get().val()


@app.route('/')
def index():
    return '''<pre>

        use
        /login/website/email
        to make Request
        and check the response at
        /check/website/email
        </pre>
    '''

# Here goes the code for the rest of the pages

@app.route('/login/<source>/<uid>')
def login(source="",uid=""):
    add_firebase_entry(source,uid)
    #send notification to app
    return 'Request Made goto check url now'


@app.route('/check/<source>/<uid>')
def check(source="",uid=""):
    #check firebase
    return get_firebase_entry(source,uid)


@app.errorhandler(404)
def page_not_found(e):
    return render_template('error.html', errorcode=404)

if __name__ == "__main__":
    app.run(host='0.0.0.0', port=8080, debug=True, threaded=True)
```

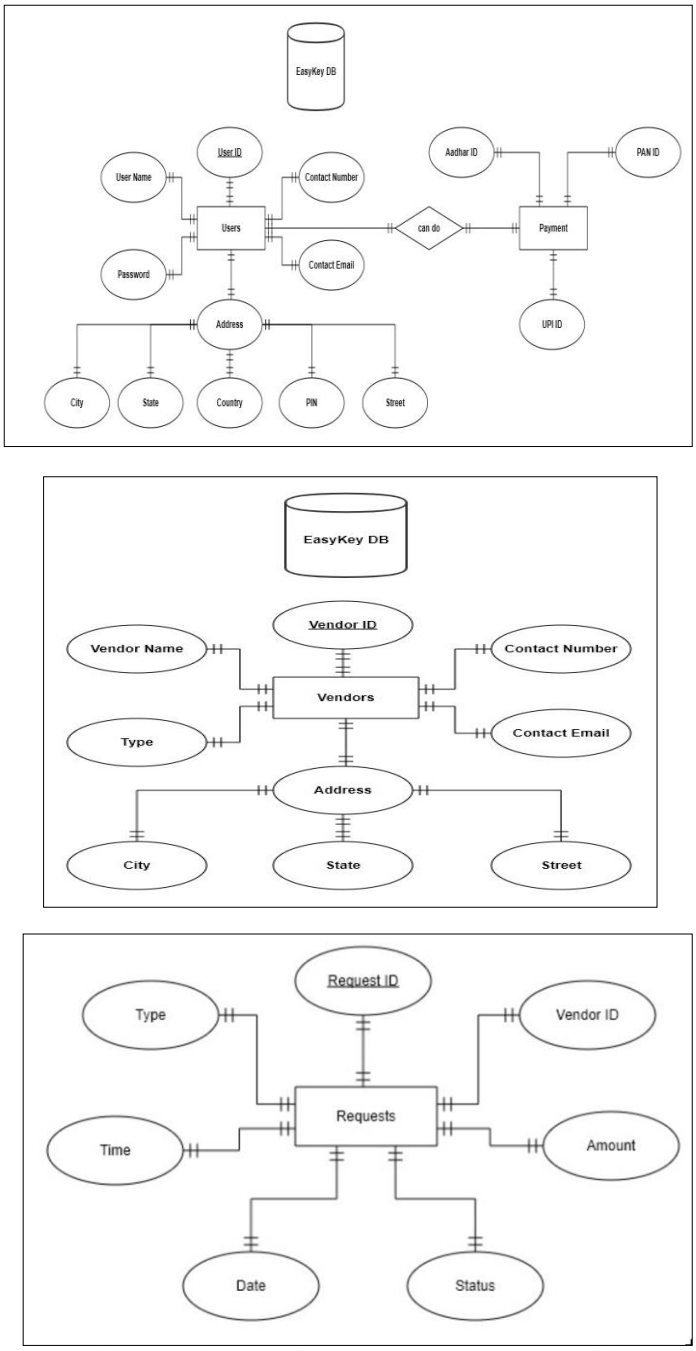


Fig 9- Entity relationship

5. SYSTEM FLOW

The system flow is shown below in Fig. 10

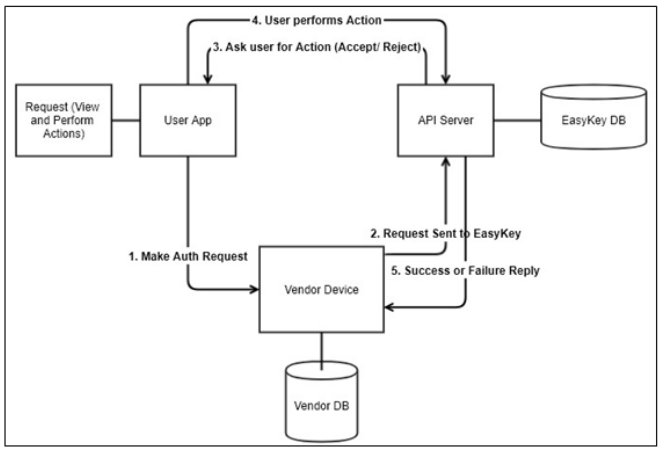


Fig 10 – System Flow

6. PROGRAM FLOWCHART

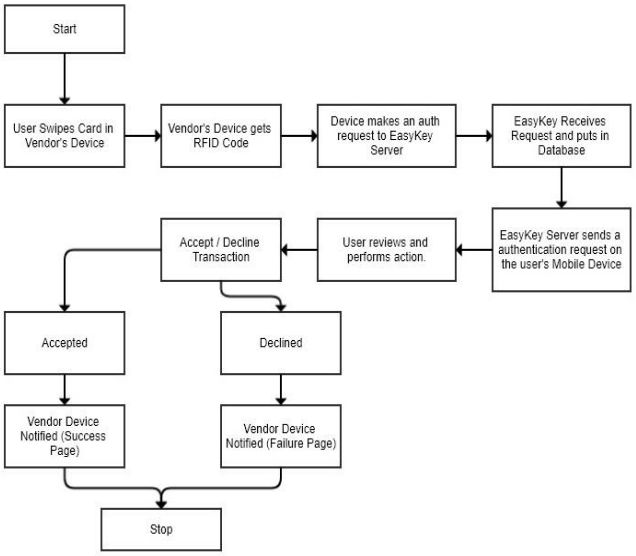


Fig 11- Program flowchart

7. FUTURE ENHANCEMENTS

The fact that the scope of the project is large cannot be denied. After analyzing from various different angles, one prospect which we can work upon is security. In this growing radius of Internet, we come across threats to personal data and security related issues. Most of the data and privacy issues have been taken care of in this project. However, minor concerns will be taken care of in the further versions. Moreover we aim to collaborate with the currently existing UPI payment and identification applications in order to expand the scope of the overall project. Linking the account of the user with various other platforms will give him/her the independence to sync all the data at once and create a single login which will work for rest of the applications. Adjusting with the current infrastructure will

become easy with further improvisations which will credit the user to access data and services more easily.

CONCLUSION

In this paper, we have shown the implementation of a single multipurpose RFID card that can be used to make payments and for authentication purposes. This multipurpose card eliminates the need of carrying various cards that are used for authentication and payment usages. We have kept in mind the privacy and security aspects of the users, and hence have instilled a Two Factor authentication. This two factor authentication reduces the risk of transactions being performed when the card falls into wrong hands. Decisively, this application may reduce the number of cards that a person carries in his/her wallet. Also, the many number of cards may be replaced by this single multipurpose RFID card.

REFERENCES

[1] J. C. Michael Melton, Theodore Arnold "Managing RFID tags using an RFID-enabled cart," 2005. Available:https://patents.google.com/patent/US20060163350A1/fr#patentCitations.

[2] A. X. Liu and L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," Comput. Commun., vol. 32, pp. 1194-1199, 2009.

[3] Cheng Feng, Research for Application of RFID in Library, 978-1-4244-6947-5/10 ©20l0 IEEE

[4] Paul Golding and Vanesa Tennant, Performance and Reliability of Radio Frequency Identification (RFID) Library System, 0-7695-2777-9/07 © 2007 IEEE.

[5] Tim Good · Mohammed Benaissa, "A holistic approach examining RFID design for security and privacy," JSupercomput 64, pp. 664–684, 2013.

[6] Mirza, Zainab Rasheed Fahad and M.N. Brohi, "Integrating radio frequency identification technology in academic management system," J. Comput. Sci., vol. 10, issue 2, pp. 361-365, 2014.

[7] Dawes A.T. (2004),"Is RFID Right for Your Library",Journal of Access Services, Volume 2(4), pp 7-13.