Indian Journal of Science and Technology, Vol 8(19), DOI: 10.17485/ijst/2015/v8i19/77134, August 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

NFC based Smart Campus Payment System

Uday Kiran Ruttala*, M. S. Balamurugan and M. Kalyan Chakravarthi

School of Electronics Engineering, VIT University, Chennai - 600127, Tamil Nadu, India;
ruttala.udaykiran2013.vit.ac.in, balamurugan.ms@vit.ac.in, maddikerakalyan@vit.ac.in

Abstract

Background/Objectives: Near Field Communication (NFC) technology follows traditional Radio Frequency Identification (RFID) standard that enables the communication using radio frequency between the devices that are separated by distance less than 10 cm. **Methods/Statistical Analysis:** The present work is a secured campus payment system that uses near Field Communication (NFC) technology and RFID integrated campus ID cards to make payments automatically within the organization or campus. The work is developed using an Arduino Microcontroller with PN532 based NFC controller shield and LabView. **Findings:** The system in implementation provides a convenient facility to act as a smart payment system in place of cash transactions with an added layer of authentication with no extra tags attached to it. **Conclusion/ Improvements:** The smart campus payment system in implementation can be further enhanced to include the mobile NFC as the payment authentication system with banking features attached to the mobile NFC gateway.

Keywords: Authentication System, NFC, RFID

1. Introduction

Near Field Communication follows traditional RFID standards including ISO/IEC 14443 and FeliCa used for short distance radio communication. TodayNFC has been integrated in mobile phones and has a wide range of applications associated with it. Now a days there exists multiple applications like smart payment systems, access control, ticketing system etc. developed using NFC incorporated in the mobile devices which can be used within an organization or campus. These applications are short go in a single device which makes the day to day life easy. Present work deals with the secured, low cost, less complex smart campus payment system developed using NFC technology along with the RFID integrated personal identity cards of individuals within the campus. The work replaces the use of mobile phones for smart payments as an application of NFC. The proposed work doesn't use mobile phones which reduces the cost of the system largely. Authentication through password is developed in the system which provides ATM type secure environment with the ID card for making the payment. This work can be implemented in schools, organizations, college campus etc. The proposed work is developed using PN532 NFC/RFID controller shield V2.0 of seed studio, Arduino UNO, Lab View and Microsoft access.

In recent years, various mobile terminals equipped with NFC (Near Field Communication) are free. The mixture of NFC with sensible devices has widened the deployment categories of NFC. It's expected to overtake credit cards in electronic payment. During this regard, security problems got to be addressed to vitalize NFC electronic payment. The NFC security standards need the utilization of user's public key at a hard and fast price within the method of key agreement[1]. With the increasing handiness of good handsets, the mobile is probably going to become the device of selection for accessing refined services and applications in an exceedingly convenient however secure manner. This can be very true with the introduction of close to Field Communication (NFC), that provides the phone with varying degree of interface permitting it to act as good, sensible wise card reader or

*Author for correspondence

to emulate smart cards[2]. An approach for NFC utilization has been put forward to make use of it in cell phones or any Context based Applications Invocation (CAI) by Einwich. The code implementation is performed with the improvements occurring in the environment. In the similar way the same methodology can be made use in mobiles where the response of telephone is set according to the token of the client[3]. Arriens described about the advancements in the applications related to the portable business, where the developments made it easy for the clients for transferring the money throughout the world instead of wandering from place to place[4]. Martens proposed a method of NFC integration with the android there by making the payment easy at the time of shopping which lead the world wide norms focused on the innovations of NFC[5]. Using ISO/IEC 14443 sort A/B standard and Felica schemes[6] flexible read/write functions are described and for measuring information by combining with the object. The NFC customary by itself doesn't give intrinsically safety features. This implies that each and every developer would wish to implement safety features in his NFC application on his own. This successively leads to users being as secure from NFC-based security vulnerabilities because the developer chooses to implement[7]. The instructions and commands can be made use to operate the gadgets according to the requirement by passing through it. Type1, Type2, Type3 and Type4 are some commonly used tags. SystemC and SystemC-Ams can be displayed by making use of two techniques which focus around the closeness.

2. System Architecture

The proposed work includes a PN532 based NFC shield v2.0 of seed studio, RFID integrated ID cards, Arduino UNO Microcontroller, LabView and Microsoft access database. In a campus every individual is provided with a RFID which is integrated in the identity card. A database associated with the unique RFID is maintained for every individual. During the payment one should authenticate by tapping the ID card to NFC antenna and enter the password. Then the respective amount is debited from the account and data base is updated with the remaining balance. The amount is credited in the same way after successful authentication. The architectural overview is shown in the Figure 2.

3. Near Field Communication (NFC)

Near Field Communication is a secured and short distance communication procedure which works in less than 10 cm range. NFC utilizes radio frequency of 13.56 MHz with a transmitting range of 1Mbps.

There are two modes of NFC for correspondence:

3.1 Active Mode

Same radio frequency is used by initiator and target for their communication in this secured mode.

3.3 Passive Mode

Target responds to the command given by the initiator in this mode

The proposed work uses PN532 based NFC shield v2.0 of seed studio as the hardware which should be interfaced to the base system for implementation. This NFC shied has access to UART, SPI and I2C communication protocols. The present work uses SPI protocol for communicating between NFC and the Base system. Figure 1 shows the NFC shield used in the work.

The final design is developed using LabView which performs password authentication after ID card is tapped to the NFC antenna.

The database is accessed only after proper authentication of the user. Figure 3 shows the final design developed using sub vi designs VISA and Database. VISA sub vi is a design developed using VISA modules in the LabView for reading the serial data from the Base system. Sub vi

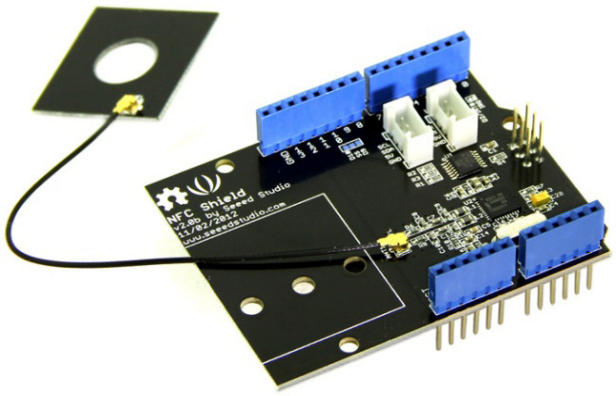


Figure 1. Seed studio NFC shield V2.0.

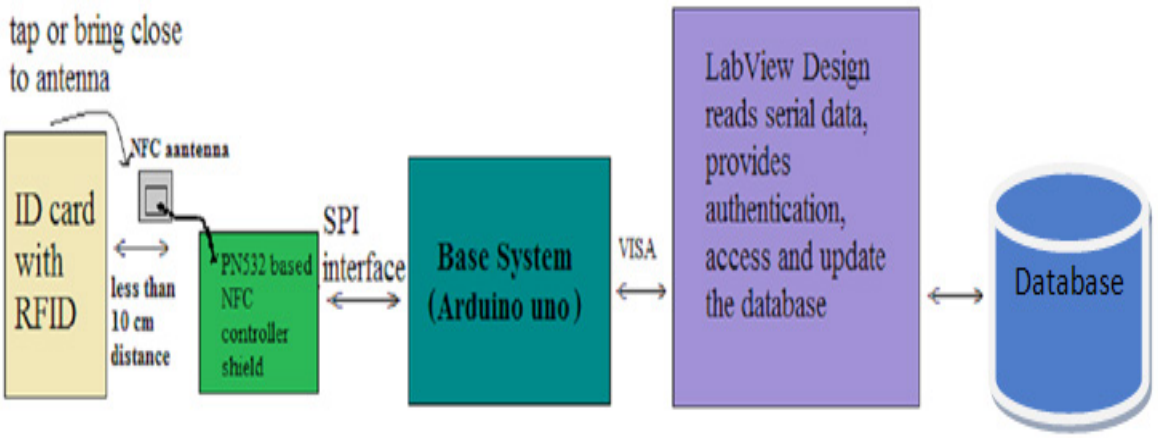


Figure 2. Architectual overview of smart campus payment.

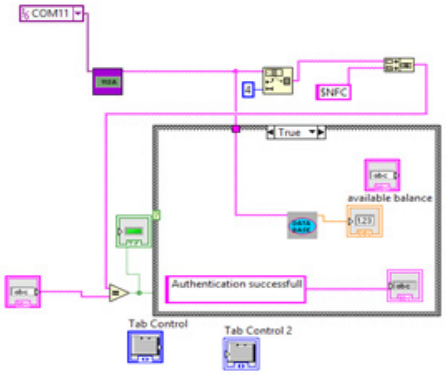


Figure 3. Block diagram of final system in LabVIEW.

named Database is a design developed for accessing database depending on the RFID read by the VISA module. A dynamic SQL syntax is generated every time when an RFID is read and this syntax plays role in accessing respective data of the user. This data Base can be accessed only after proper authentication through password.

4. System Implementation

Even though NFC has been integrated into mobile phones in the current technology, a cost effective smart payment system is developed using the RFID integrated identity cards instead of mobile phones which reduces the cost of the total system. The following steps describe the implementation of the overall system.

4.1 SPI Communication Protocol

The Serial communication between Base system (Arduino UNO) and NFC is implemented using Serial peripheral interface (SPI) Protocol. Arduino libraries are developed for SPI such that RFID read by NFC antenna is sends the data serially to the base system. When the code is executed in the Base system, the data read by the NFC is transmitted to the Base system in serial form.

4.2 Transmitting Data from Base System to LabView using VISA Port

The serial data from the base system is fetched by the LabView using the design developed with VISA modules. Appropriate COM port and baud rate should be selected. Figure shows the front panel when the data is fetched by VISA port.

4.3 Accessing the Database through LabView

A database is created using Microsoft access and a design is developed in the LabView by generating the SQL syntax for accessing the database. The SQL syntax comprises of the RFID which plays a vital role in reading the data of respective person. A dynamic SQL syntax is generated whenever NFC antenna reads the RFID from the ID card.

NFC shield is activated by uploading the code in the Arduino IDE after making proper hardware connections. Once the NFC starts reading the data the LabView design

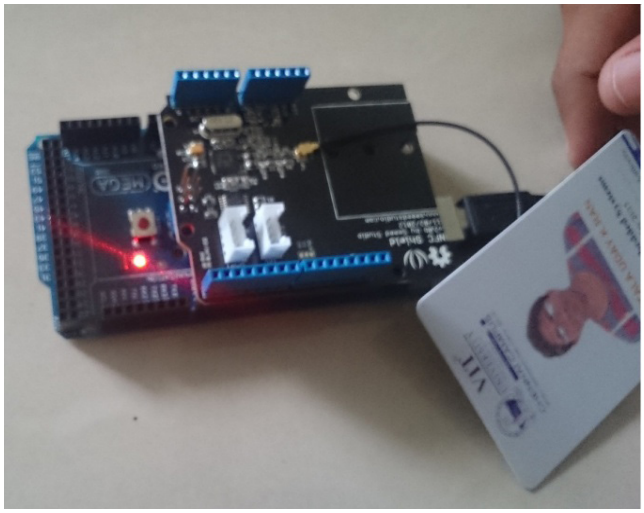


Figure 4. Hardware set up used in this work for passive communication.

should be executed. In addition, performs authentication with the password and then process the payment. After the payment is done the database is updated with available balance. The balance can be credited in the same way after proper authentication Figure 4 shows the hardware setup of the work.

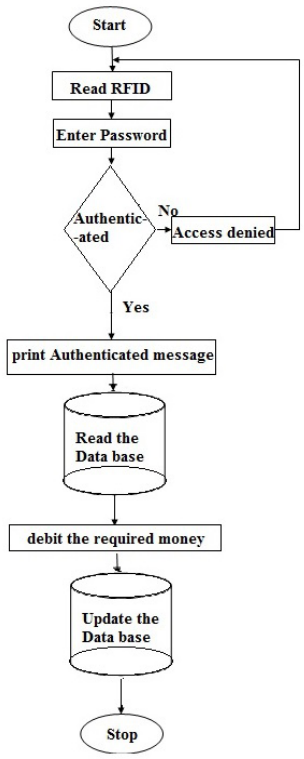
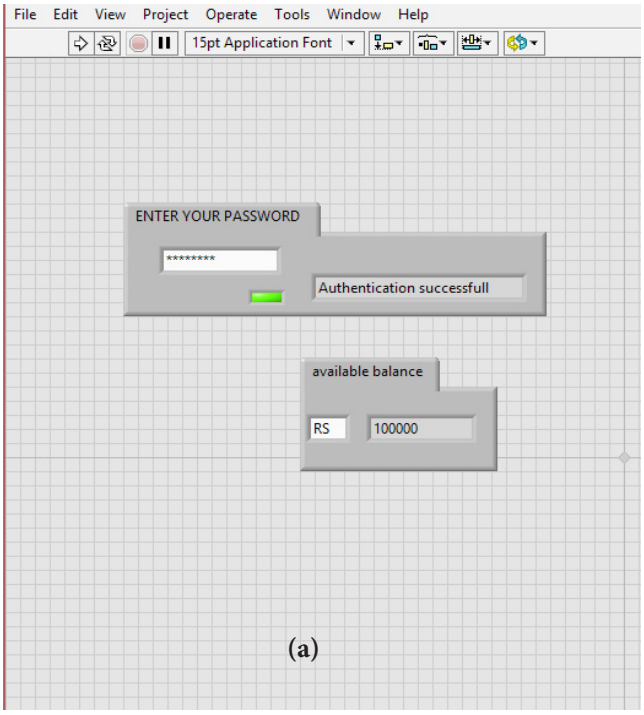


Figure 5. Flow chart for authentication process.



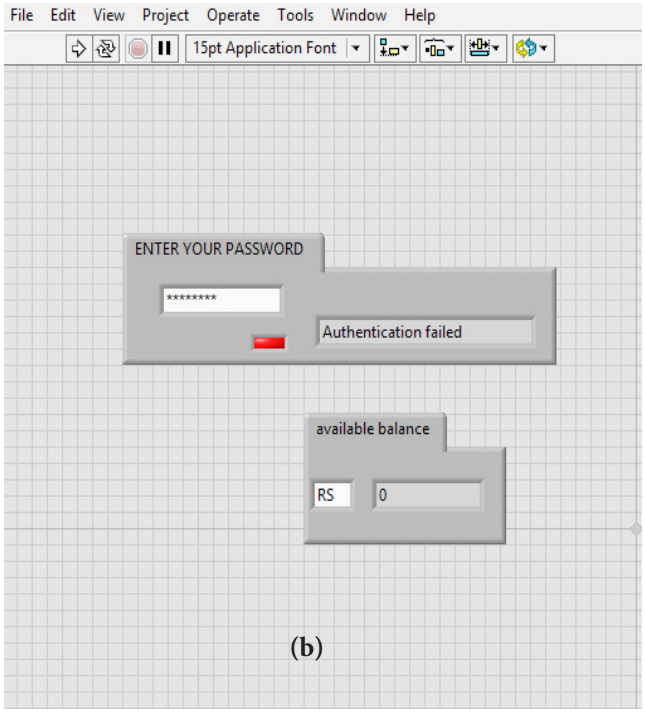


Figure 6. (**a**) Front panel of overall design when authentication successful and (**b**) Front panel of overall design when authentication unsuccessful.

The flow chart for authentication process is shown in Figure 5. Access will be granted only when the password is correct. Once authentication becomes successful it will allow access to the database which shows the available balance and after required amount is debited the database will update with remaining balance.

5. Results

Usage methodology and implementation of this work just utilizes present NFC technology on the smart cards accordingly actualizing the procedure completed. The Arduino UNO board is interfaced with PN532 NFC/RFID controller shield utilizing the libraries developed for SPI protocol. An RFID integrated campus ID card is tapped to the NFC antenna in order to launch the correspondence. NFC follows the RFID standards that include ISO14443-A/B and Felica. Figures 6 (a) and 6 (b) shows the front panel of overall design after concatenating the individual modules. Thus a smart campus payment system is developed using PN532 NFC/RFID controller shield.

6. Conclusion

An application which uses RFID integrated campus ID card instead of mobile phones to communicate with NFC shield has been made for smart campus payment system which reduces the cost of the system which are available today and complexity of the design. The system is hacking free as it is impossible to hack from distance more than 10cm, without ID card. In addition it is password protected which overcomes the issue in case of ID card missing or stolen. Since it doesn't need any keying or encryption techniques, design complexity is reduced. Since the work is developed using individual identity cards valid within the campus, it is flexible for every individual to use the payment system effectively and easily. No extra gadgets are required for authenticating and making the payment. This work adds feature to the existing systems which uses ID card scanning for granting access into an organization or a campus. The proposed work is successfully developed using PN532 based NFC shield V2.0 of seed studio.

7. Refernces

1. Eun H, Lee H, Oh H. Conditional privacy preserving security protocol for NFC applications. IEEE Transactions on Consumer Electronics. 2013 Feb; 59(1):153–60.
2. Chen WD, Mayes KE, Lien YH, Chiu JH. NFC mobile payment with Citizen Digital Certificate. The 2nd International Conference on Next Generation Information Technology (ICNIT); 2011 Jun 21-23. p. 120–6.
3. Einwich K. Introduction to the System C AMS extension standard. Proceedings of IEEE Int Symp Design Diagnost Electron Circuits Syst; 1998 Nov.
4. Open System C Initiative. System C AMS extension user's guide; 2010. Available from: http://www.accellera.org/downloads/standards/systemC/ams
5. Martens ESJ, Gielen GGE. Analyzing continuous-time modulators with generic behavioral models. IEEE Trans Computer-Aided Design Integr Circuits Syst. 2006 May; 25(5):924–32.
6. Agostinelli M, Priewasser R, Huemer M, Marsili S, Straeussnigg D. System C-AMS modeling and simulation of digitally controlled DC-DC converters. Proceedings of IEEE Appl Power Electron Conf Exp; 2010 Feb. p. 170–5.
7. Hameed S, Hameed B, Hussain SA, Khalid W. Lightweight security middleware to detect malicious content in NFC tags or smart posters. 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); Beijing. 2014 Sep 24-26. p. 900–5. DOI: 10.1109/TrustCom.2014.118.