NEAR FIELD COMMUNICATION FOR SECURE APPLICATION USING ANDROID MOBILE PHONE

[1]Vishwajeet Rajendra Nikam
[1]Student of Master of Engineering
[1]Electronics & telecommunication (communication group)
[1]D N Patel college of engineering, shahada, India

Abstract—- Development in technology bring digital world to be border-less. It's proven through a developed technology, when trade and transaction can be done not only using real money but also virtual one. Shopping process using virtual money has even more supported by existed Near Field Communication (NFC) device. This particular device works using radio frequency. In the year of 2011, Google was integrating this device into a Android-based cell phone, which made transactions using virtual money gradually developed. Online shopping is one of the utmost services in online trading. Online shopping is basically a paper-less electronic document, which commonly used for Petrol pump, Mall, Toll Plaza. One of the aims in using NFC in daily life can be implemented within public services application.

Index Terms— Android, e-Ticket, Near Field Communication, NFC, Mobile Computing.

I. INTRODUCTION

A key application of Near Field Communication (NFC) can be found in the Online shopping in this project we are implementing a shopping for Petrol pump, Mall, Toll Plaza using the concept of (NFC) near field communication. It can radically change existing system of isolated interoperable Online shopping. Online shopping system consists of of transactions. Moreover. By simplifying the online shopping process and transforming ticket physical form to virtual one, then the NFC technology development will not limited only for payment transaction. This paticular technology can also be implemented as one of the way to substitute current shopping .

Within the development of technology, problems in banking transaction have been solved by integration among customer's bank accounts to the internet. It can be seen from the existence of iBanking and mBanking as main features of banking services. The ability to establish transaction anytime and anywhere isn't only beneficial for Bank's management, but also several service providers and sellers which also make use of banking features to cycling an amount of transactions happened. Proven by viral development of online shops that take advantages from payment feature to shop's bank account. Technology will never stops expanding. Online shopping is one of commonly used by people. Everyday, Petrol pump, Mall, Toll Plaza establish huge number of transactions.

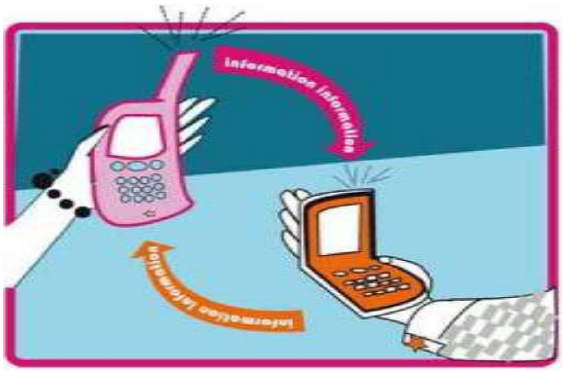
II. LITERATURE SURVEY

NFC enables users to exchange information by holding their mobile phones within 20 centimeters of NFC logos. Due to the fact that the communication range sis so small, the user – in principle, at least – initiates all forms of communication. NFC technology integrates three functions with which consumers are already familiar: smart cards (such as ID-, debit- or access cards); the accessing of digital content (such as clicking with a mouse); and the establishment of communication between two devices (Bluetooth, for example).

Bluetooth. The NFC Forum's promotional presentations envisage this technology being used to transfer files such as photos or meeting agendas between NFC-equipped devices. Another potential use would be transferring funds from one electronic purse to another

The issue with device-to-device communications is security, especially over extended ranges. NFC has been designed for communications within a close range: ten or less centimeters. Holding the device (of whatever form factor) containing the payment details close to the reader addresses the security concern. The possibility of any person or device coming within range to eavesdrop on the messaging traffic is minimized.
Although many see NFC as a payments standard this is not the case. Payment is only one use of the technology. NFC can be used to configure and initiate other wireless network connections such as Bluetooth and Wi-Fi. In the payment context NFC is starting to be considered more than a communications protocol. It is being seen more as a proximity payment method, bundled with ISO14443, the proximity standard and EMV. with a contactless chip. The contactless chip may support the EMV security standard, or the chip may just hold a magnetic strip image. This enables proximity payments where the card and device generates a standard purchase transaction under the request and response payment model. The advantages of this technology are reflected in the MasterCard Pay pass and Visa Wave solutions. These two payment methods are based on lower value proximity payments without the need for either signature or PIN. The business justification is based on increasing the customer throughput per cashier, resulting in a higher retail sale volume at a lower cost for merchants while improving the consumer experience. Removing cash reduces handling costs and shrinkage. The EMV application of Wave and Pay pass does perform two-way card-to-device authentication. But obviously the cardholder is not authenticated. It will be interesting to see if the business case stacks up once a high market penetration rate of Wave and Pay pass capable cards is reached and the merchant acceptance base expands. From a payment perspective, unauthenticated transactions represent a payment risk. Keeping proximity fraud levels within budgeted limits is the key. The risk is intended to be carried by the issuer, although merchants will inevitably pay indirectly through the interchange rates. More importantly NFC technology removes the need for a payment instrument to make contact with a payment device to initiate a payment request. Removing this physical contact means the chip can be supported from a variety of form factors. The ability to communicate back to the cardholder's issuing bank introduces the ability for both cardholders and issuers to communicate unobtrusively with each other on an event-by-event basis, in real time. This completes the communications link in a way that is impossible for payment cards.

Figure 1 Card Emulation mode



Specification of NFC:

- Short range contactless communication available to consumers globally.
- Based on RFID Card magnetic field induction to enable the communication.
- Bidirectional data communication.
- It operates within the globally available radio frequency ISM band of 13.56 MHz.
- Working distance with compact standard antennas: up to 20 cm.
- Supported data rates: 106, 212, 424 or 848 kb/s
- The devices implement the ―listen before talk‖ policy – any device must first listen on the carrier and start transmitting a signal only if no other device can be detected transmitting

Tag - The tag is a thin simple device containing antenna and small amount of memory. It is a passive device, powered by magnetic field. Depending on the tag type the memory can be read only, re-writable, and writable once. The Initiator, as follows from the name, is the device that initiates and controls the exchange of data. The Target is the device that answers the request from the Initiator.

NFC protocol also distinguishes between two modes of operation: Active mode and Passive mode. All devices support both communication modes.

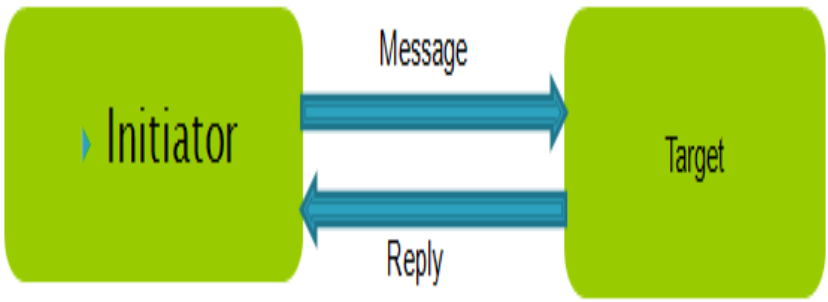
The distinction is as follows:

In the Active mode of communication both devices generate their own RF field to carry the data. NFCIP-1 uses different modulation and bit encoding schemes depending on the speed. While establishing the communication, the Initiator starts the communication in a particular mode at a particular speed. The Target determines the current speed and the associated low-level protocol automatically and answers accordingly. The communication is terminated either on the command from the application or when devices are out of range.

In the Passive mode of communication only one device generates the RF field while the other device uses load modulation to transfer the data. The protocol specifies that the Initiator is the device responsible to generate the RF field. The application chooses the initial communication speed from the set of 106, 212 and 424 Kbit/s.

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices located a few centimeters apart. The technology can be used for a wide variety of mobile applications

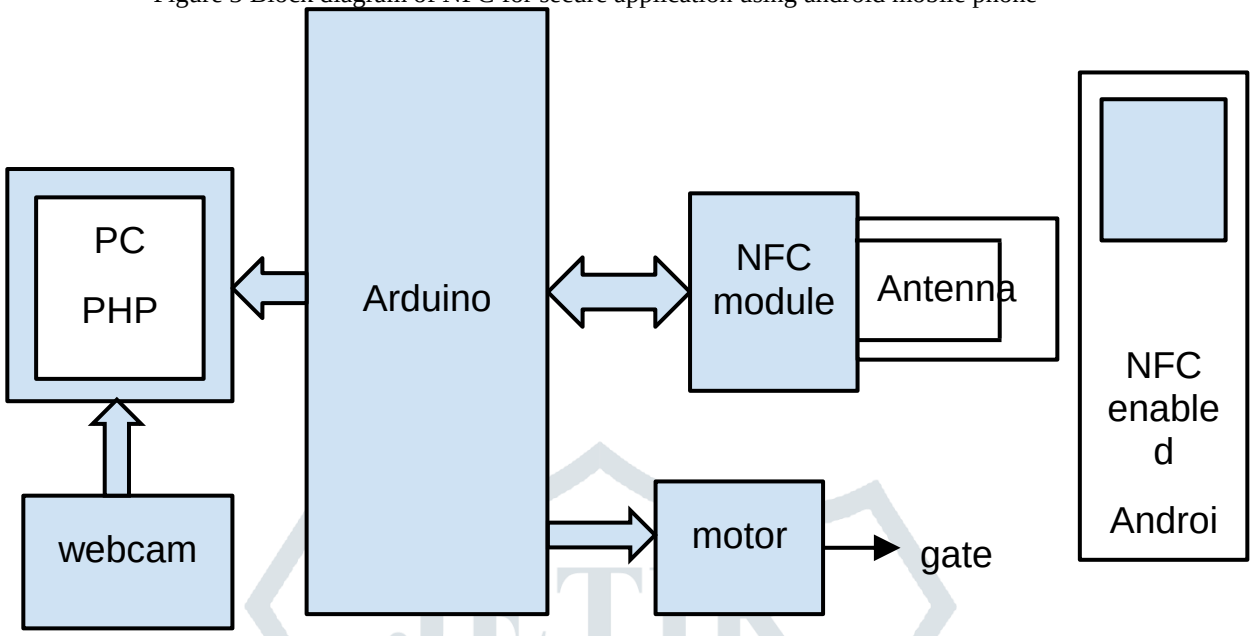
Figure2 Two way communication



An NFC-enabled device can operate in reader/writer, peer-to-peer, or card emulation mode. For mobile contactless payments, the NFC-enabled mobile device operates in card emulation mode and appears to an external reader to be a traditional contactless smart card. Payment information is stored in the mobile phone in a secure element, which is a smart card chip that protects stored data and enables secure transactions. Contactless payments and ticketing using NFC devices can be enabled without changing the existing acceptance infrastructure. The NFC Forum25 has developed and released implementation specifications and has also launched a certification program that checks devices for compliance with NFC Forum specifications. Compliant devices behave consistently, facilitating an interoperable infrastructure.

III. SYSTEM DEVELOPMENT

Figure 3 Block diagram of NFC for secure application using android mobile phone



Deploying NFC mobile contactless payment applications requires an ecosystem in which stakeholders cooperate to deliver different functions and capabilities. Stakeholders in the NFC ecosystem. As the figure illustrates, the secure element in the NFC-capable device (discussed in the following section) is provided to the consumer by one of the ecosystem stakeholders. Which secure element is chosen and who provides it has critical implications for usability, portability, ubiquity of handsets, and control. The ST21 NFCA system-on-chip combines a complete hardware capability for 13.56 MHz contactless communication with an useful embedded firmware which handles:

- ISO/IEC 14443 A&B, Calypso V1 Radio Protocol (B'), ECMA340 (NFCIP-1), ISO/IEC 15693, ISO/IEC18000-3Mod1 in card emulation modes as well as reader modes
- Switch modes between operating modes and RF modes
- Host Controller Interface functions (HCI based on the ETSI specification) In addition, the embedded firmware and associated microcells support handling and protocol for the various interfaces:
- Single Wire Protocol (SWP) interface fully compliant with ETSI TS 102 613 Release 7
- C Slave interface fully compliant with NXP specification
- SPI Slave interface fully compliant with Free-Scale specification
- Asynchronous Receiver Transmitter in master configuration supporting ISO/IEC 781 6-3 T=0 and T=1 protocols

The PN532 is a highly integrated transmission module for contactless communication at 13.56 MHz including microcontroller functionality based on an 80C51 core with 40 Kbytes of ROM and 1 Kbytes of RAM.

The PN532 combines a modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocols at 13.56 MHz with an easy-to-use firmware for the different supported modes and the required host controller interfaces. This document describes the firmware embedded in the PN532 chip, in particular the global behavior in the system depending if the PN532 device is used as initiator or target. The PN532 is a highly integrated transmission module for contactless communication at 13.56 MHz including microcontroller functionality based on an 80C51 core with 40 Kbytes of ROM and 1 Kbytes of RAM.

This document describes the firmware embedded in the PN532 chip, in particular the global behavior in the system depending if the PN532 device is used as initiator or target. The PN532 is a highly integrated transmission module for contactless communication at 13.56 MHz including microcontroller functionality based on an 80C51 core with 40 Kbytes of ROM and 1 Kbytes of RAM. The PN532 combines a modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocols at 13.56 MHz with an easy-to-use firmware for the different supported modes and the required host controller interfaces. This document describes the firmware embedded in the PN532 chip in particular the global behavior in the system depending if the PN532 device is used as initiator or target.

A better way for the host controller is to use the P70_IRQ pin that indicates when the PN532 is ready to send its frame. In that case, the host controller can wait for this line to be asserted by the PN532 and has no more need to read the status byte. As a consequence, the overall traffic on the SPI bus is reduced.

The PN532 combines a modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocols at 13.56 MHz with an easy-to-use firmware for the different supported modes and the required host controller interfaces. This document describes the firmware embedded in the PN532 chip, in particular the global behavior in the system depending if the PN532 device is used as initiator or target. The PN532 is a highly integrated transmission module for contactless communication at 13.56 MHz including microcontroller functionality based on an 80C51 core with 40 Kbytes of ROM and 1 Kbytes of RAM. The PN532 combines a modulation and demodulation concept completely integrated for different kinds of contactless communication methods and protocols at 13.56 MHz with an easy-to-use firmware for the different supported modes and the required host NFC technology integrated in a mobile device typically consists of two integrated circuits. The NFC controller is required for the analog digital conversion of the signals transferred over the

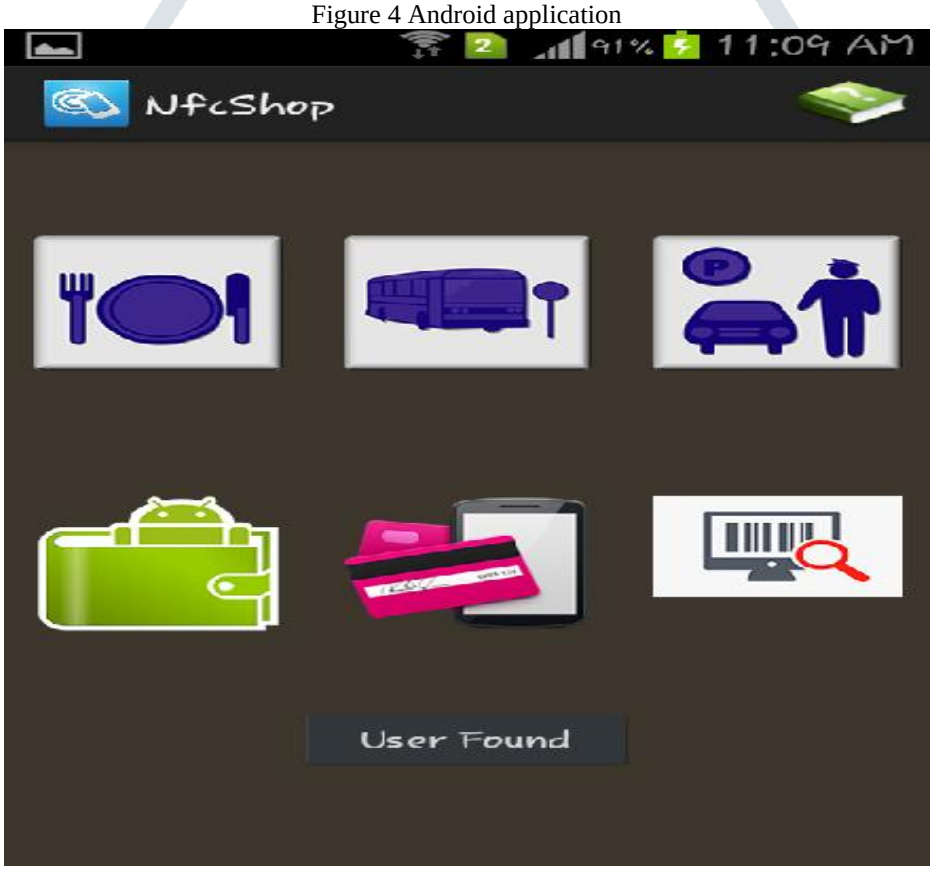
proximity connection. An HCI (host controller interface) allows the host controller to set the operating modes of the NFC controller, process data sent and received and establish a connection between the NFC Modem and the secure element. The second IC, a secure smartcard chip also referred to as the secure element, is used for the tag emulation mode. Basically, the technologies Radio Frequency Identification and Near Field Communication use the same working standards. However, the essential extension of RFID is the communication mode between two active devices.

IV. FLOW OF WORKING

Based on test that has been done in previous chapter, we can conclude several point as what written below.

1. Application created is a prototype which can be implemented in train company, and still has wide chance of development based on the needs.
2. NFC technology can be used to simplify train ticket purchase process and electronic ticket distribution, especially cell phone electronic ticket.
3. Based on beta testing, created application has work properly, proven by 53% of correspondents confession said that the application has run smoothly, moreover 56% correspondents confess that this application has attractive display. Respond time needed for TrainNFC is relatively faster, proven by 56% correspondents confession and 100% correspondents confess that TraiNFC can ecomeone of the way in train ticket purchasing.
4. Average process time needed for each activity existed within application, need less than 1 minute. Only "beliTiket" activity needs longer time which is around 3 minutes. It's because data should be requested to database server and it needs longer time based on the respond speed fromthe server itself.
5. Process time needed to run "beliTiket" activity became 162,97% longer when there is traffic in internet access compared to burdenless internet access. Nevertheless process time using celular network (3G) takes 115,378% longer compared to burdenless internet access

Figure 4 Android application



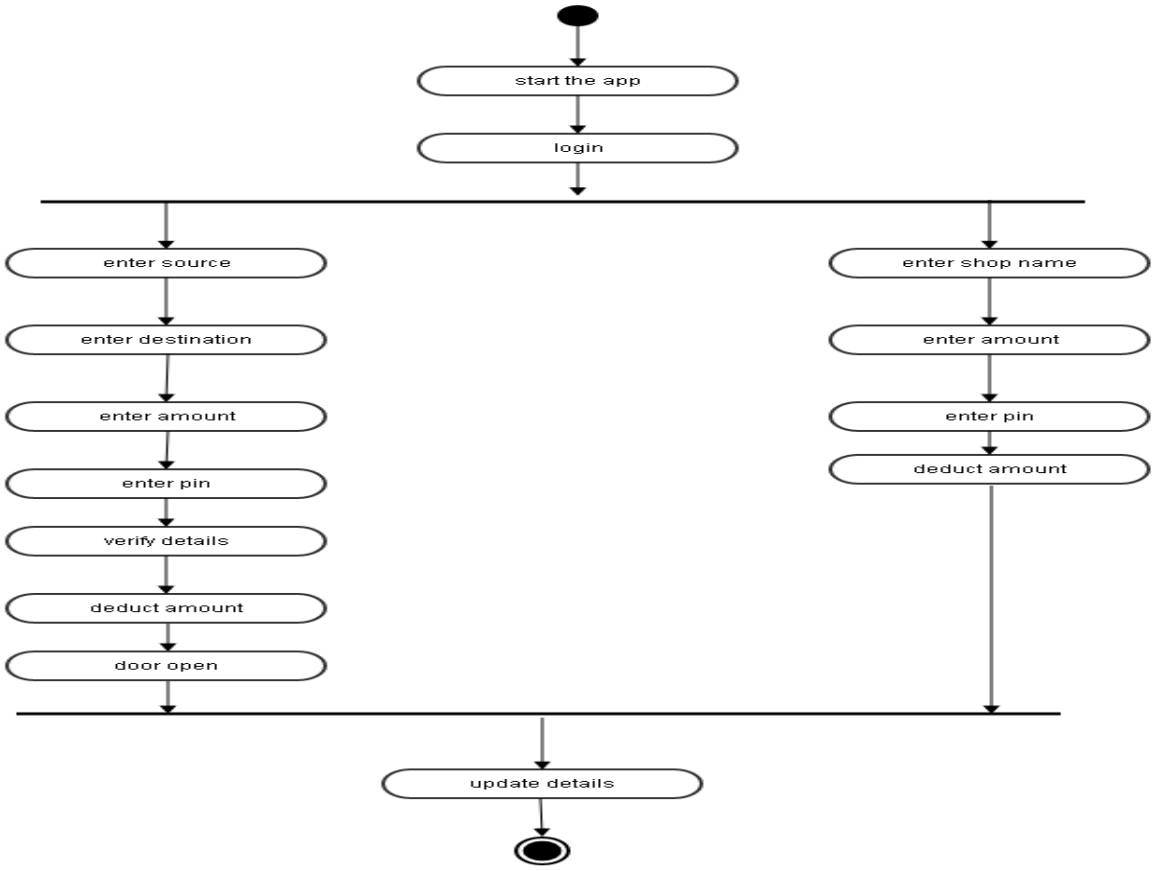
a) Metro

- User will login on the app.
- User will enter source, destination and amount.
- After submitting details, app will ask for pin.
- User will tap on the system.
- Server will verify the details and deduct the amount from user account.
- Gate will open on Successful transaction

b) Shopping

- User will login on the app
- User will enter shop name and amount.
- After submitting details, app will ask for pin.
- User will tap on the system.
- Server will verify the details and deduct the amount from user account.

Flowchart 1 System flow



V. CONCLUSION

We aim to implement a Train Ticketing System using NFC Technology. The system is implemented to generate NFC tickets, thus reducing human effort and making the process completely automated. NFC tickets helps in identifying people travelling in the train providing security. The Passengers only need to carry their NFC enabled android phone and recharge their account when the balance is below the required fare price. They are much more convenient compared to the current ticketing system as it eliminates wastage of papers. Any unwanted events can be avoided as all the person carrying NFC tickets are monitored every time they travel as their details are recorded.

VI. ACKNOWLEDGMENT

We would firstly like to acknowledge my guide Mr .N C PATIL, who have helped us a lot right from selection of our seminar topic to its fulfillment. We are really thankful to him for his kind guidance and creating our interests in "Digital Signal Processing designing for FPGA Architecture " without which our work would not have been completed.We are also thankful to Mr. V K PATIL, Head of E & TC Department for providing us necessary facilities for completion of our Seminar work.

REFERENCES

[1] EcmaInternational,‖Nearfield communication—White paper‖, 2005,Ecma/TC3TG19/2005/012,Available:http://www.ecma international.org/

[2] Mehmet AYDIN vedat COSKUN kerem OK information dept ISIK university,Istambul Turkey‖NFC research Framework.A literature review and future reaserch directios‖june 10

[3] Shyamal pampattiwar ―literature survey on NFC ,applications ‖IJSER feb-2012.

[4] Florian Michahelles, Frederic Thiesse, Albrecht Schmidt, and John R. Williams.―pervasive RFID and NFC technology‖ IEEE 2007

[5] NFC Forum: www.nfc-forum.org

[6] NFC World: www.nfcworld.com

[7] NFC Nokia: http://europe.nokia.com/nfc

[8] Urgen Morak, Hannes Kumpusch, Dieter Hayn‖ Design and Evaluation of aTelemonitoring Concept Based on NFC-Enabled Mobile Phones and Sensor Devices‖IEEE Jan 2012