Ind Jour Math & Comp Sc. Jhs, Vol. I-II, 2011 Pg. 49 - 57

Use of Mobile Transactions Payment Model in Customer Oriented Payment System using NFC Technology

Vibha Kaw Raina[1], U.S Pandey [2,] Munish Makkad[3]
Department of Computer Science Birla Institute of Technology, Noida, India.
School of Open Learning Delhi University, India.
Department of Management, Birla Institute of Technology, Noida, India.

Received on 26/2/2012

Abstract--**Mobile payment is an application of mobile commerce which facilitates mobile commerce transactions by providing the mobile customer with a convenient means to pay. Many mobile payment methods have been proposed and implemented like user friendly, customer centric, merchant centric where security concerns are highly addressed. This paper proposes a mobile payment model with a Near Field Communications that provides a platform for many applications for peer to peer transactions and other security features where confidentiality and trust are main concerns. Near Field Communication (NFC) provides means to close-range contactless identification and communications for mobile phones and other devices Also, use of NFC for short range communication allows the possible integration with existing Point-of-Sale equipment and the payment process from the customers and merchants perspective.**

Keywords**:** - Mobile payments, P2P transactions, NFC, Security.

I. INTRODUCTION

Mobile payments are defined as the payments carried on the mobile devices. A mobile payment is the process of two parties exchanging financial value using mobile device in return for goods and services. It can also be defined as the transfer of money from one party to another through the exchange of information. Mobile devices may include mobile phones, PDA's, wireless tablets and any other device that can be connected to mobile telecommunications network for making payments. For any mobile payment to be widely accepted and adopted it is important to overcome the following challenges. Interoperability, Usability, Simplicity, Universality, Security, Privacy, Cost, Speed and Cross border Payments. [1] The existing wireless payment systems can be classified into three types: account based payment systems, token-based payment systems, mobile POS (point of sale) payment, and mobile wallets payment systems [2]. The combination of the mobile device with the latest wireless technology NFC (Near Field Communication) makes possible variety of payment applications like ticketing, access control, content distribution, smart advertising, and peer-to-peer data/money transfer. NFC is a short-range wireless connectivity technology that evolved from the combination of existing contact less identification and interconnection technologies [3].
NFC is a standard based, short range wireless technology supporting the two way interactions among electronic devices. A cellular phone having a NFC device is able to communicate not only with internet via wireless connections but also with smart card readers.[4] NFC technology brings the user experience, convenience and security of contactless technology to the mobile devices, and is enabling quick transactions and services in our day-to-day lives. NFC has revolutionized the mobile payments. The major advantage of NFC over other wireless communication technologies is its simplicity: transactions are initialized automatically, simply by touching the reader, another NFC device or an NFC compliant transponder. NFC is a proximity technology relying on the smart card standard ISO 14443[5] and allowing wireless transactions only over a distance of up to 10 centimetres. [6]
The rest of the paper is organized as follows: In the next Section we review previous related work on mobile payment and technology. Then, Section 3 describes the overview of mobile payments systems. Section 4 gives the details of NFC technology along its operating modes, architecture, standards and services. Section 5 describes the proposed payment model where NFC technology is used for P2P transactions. Section 6 conclusion and Section 7 future work.

II. RELATED WORK

The complexity of mobile payments for customers and merchants are strong barriers to usability and adoption. In[7,8] the usage of SMS for mobile payment services is criticized because the message formats are often complicated and slow to key in. The mobile payment procedures need to be simpler and faster including biometrics and keystrokes and possibly another technology to replace SMS. Another study [9], deals with mobile banking in Germany argue, that a lot of German banks cancelled their m-banking services. As a cause, among other things the ease of operations and the impoverished WAP sites were mentioned. Dahlberg et al. [10] pointed out: "the social and cultural factors on mobile payments, as well as comparisons between mobile and traditional payment services are entirely uninvestigated issues. Especially, the NFC technology is deemed as easy to use and as an enabler for mobile payment. Ondrus and Pigneur presented an assessment of NFC for future mobile payment systems in Switzerland [11]. Their result from expert interviews shows that NFC is a popular technology for payment. It is illustrated that the, contact less technology has shown to be more efficient than cash for payment transaction. In expert opinion, NFC is with regard to the speed a good choice for m-payment.

According to an evaluation of wireless technologies for payments, Zmijewska outlines in that NFC is a promising technology for ticketing as well as payments. He explains that the contactless technology has high ease of use in comparison to other technologies. [12]

Transaction speed and convenience have often been cited as the main advantage of cashless payment. Therefore the advantages of this payment solution for consumers are obvious. NFC allows transaction convenience and speed due to the use of a single ubiquitous device and interface. To, increase adoption, m-payments must demonstrate clear advantages in terms of speed and convenience over traditional payment options to consumers [13].

In Japan there are already several contactless systems in use which are quite well accepted. In order to use them a DoCoMo's handset is required. With regard to trust it is also mentioned, that the operator can lock the handset in case of loss or theft.

III. OVERVIEW OF THE MOBILE PAYMENT CONCEPTS

It consists of a web server, IVR server and a database. The SMS gateway is provided by another company allowing access over SMPP.

The IVR application uses a uses the basic GSM mobile telephone technology to call a consumer and ask for a PIN. Also, SMS application sends a short message to the consumer asking for authorizing a payment by replying to the message with: "yes".

The WAP application sends a WAP push message containing a customized URL to the consumer. The consumer opens the message which loads the WAP browser loading a web page asking for authorizing a payment with the PIN.

The OTP application uses time synchronization between server and a mobile application to generate one time passwords. The consumer starts the OTP application on the mobile phone and enters the PIN. A hash is being built, using the PIN and other information to identify the consumer on the server side.

The NFC application uses the NFC technology build in some mobile phones. This technology allows the phone to read an RFID tag which contains a Point of Sale ID. As soon as the phone touches the RFID tag an application is started which contacts a server and retrieves the payment data. The consumer will be asked for the PIN to authorize the payment.

IV. NFC TECHNOLOGY

NFC is a short range and standardised (ISO 18092)[14] wireless communication technology that adds contact less functionality to mobile devices including mobile phones and PDA's (Personal Digital Assistants). Such devices can act both as a "contactless card" (based on its secure element and as a "contactless reader" and also operate in P2P mode with peer devices. These devices support various contactless communication standards, such as ISO 14443[15], ISO 15693 [16], FeliCa [17] and Mifare Standard [18].Further details on the potential of NFC technology can be found in [19].

The NFC driven payment model has a potential to evolve from the traditional payment model (where the consumer pays the merchant for the goods using mobile phone) into a new model where the consumer pays the merchant for the goods using mobile phone) into a new model where consumer can also act as a merchant.

The technology used in NFC is compatible with existing contactless infrastructure and NFC device offers three operating modes.

a). Reader/Writer mode: In this mode the NFC device can read or write information such as URLs, SMS's in a tag or smart card e.g. Smart posters applications. Here, users touch the device or a cell phone with the tag embedded in the poster, which triggers the transmission of a URL to the phone. The URL could be used to open the web browser without any human intervention.[20]

b).Card Emulation mode: In this mode the NFC enabled device emulates a contactless smartcard (ISO 14443). In this case there is a secure element embedded in the device where sensitive data can be stored in a safe place and value added services requiring a high level of

security such as payment applications can be made available to the customers.

c). Peer-to-Peer mode: In this mode a connection is established between two NFC enabled devices and data can be exchanged between them. The NDEF (NFC Data Exchange format) is used to transmit data. This mode is standardized on ISO 18092.[21]

A. NFC Architecture

NFC technology integrated in a mobile device consists of two integrated circuits. SE's and an NFC interface. The NFC interface is composed of a contactless; analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an IC called an NFC controller to enable NFC transactions. The NFC Controller is required for the analog digital conversion of the signals transferred over the proximity connection. Apart from an NFC controller, an NFC enabled mobile phone has at least one SE which is connected to the NFC controller for performing secure proximity transactions with external NFC devices (e.g. payment at POS) through Single-Wire Protocol (SWP). The SE provides a dynamic and secure environment for programs and data. The secure element is also called as tag emulation operating mode. It enables secure storage of valuable and private data such as the user's credit card information, and secure execution of NFC enabled services such as contactless payments. Also, more than one SE can be directly connected to the NFC controller. The supported common interfaces between SE's and the NFC controller are the Single Wire Protocol (SWP) and the NFC Wired Interface (NFC-WI). The SE can be accessed and controlled from the host controller internally as well as from the RF field externally. The host controller (baseband controller) is the heart of any mobile phone. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The host controller sets the operating modes of the NFC controller through the HCI, processes data that are sent and received, and establishes a connection between the NFC controller and the SE. Also, host controller is able to exchange data with the secure element (internal mode e.g. for top up of money into the secure element over the air. NFC is closely related to RFID (Radio Frequency Identification). RFID is mainly used for remote tracking, tracing and identification of goods and persons without a line of sight while as NFC is used for more sophisticated and secure transactions like contactless access or payments. Both technologies have several layers and protocol concepts and are therefore open for the same attacks. [22, 23, 24]

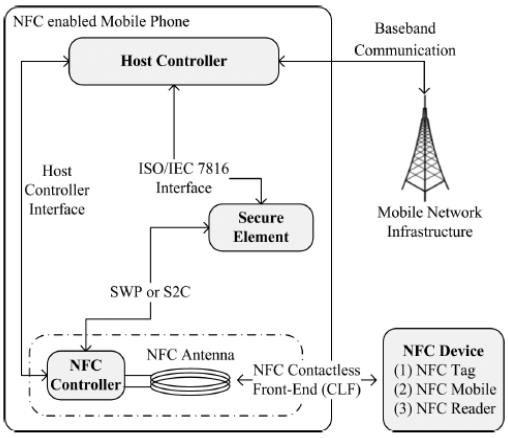


Figure1. Architecture of NFC integrated in a mobile device

B. NFC standards and specifications:

The different standards and specifications given for NFC technology are as follows:

B.a) Protocol Technical Specifications:

B.a.1 NFC Logical Link Control Protocol (LLCP) Technical Specification:

This specification defines an OSI layer-2 protocol to support peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications. The specification defines two service types, connectionless and connection-oriented, organized into three link service classes: connectionless service only; connection-oriented service only; and both connectionless and connection-oriented service. The connectionless service offers minimal setup with no reliability or flow-control guarantees (deferring these issues to applications and to the reliability guarantees offered by ISO/IEC 18092 and ISO/IEC 14443 MAC layers). The connection-oriented service adds in-order, reliable delivery, flow-control, and session-based service layer multiplexing.

LLCP is a compact protocol, based on the industry standard IEEE 802.2, designed to support either small applications with limited data transport requirements, such as minor file transfers, or network protocols, such as OBEX and TCP/IP, which in turn provide a more robust service environment for applications. The NFC LLCP thus delivers a solid foundation for peer-to-peer applications, enhancing the basic functionality offered by ISO/IEC 18092, but without impacting the interoperability of legacy NFC applications or chipsets.

B.a.2 NFC Digital Protocol Technical Specification:
This specification addresses the digital protocol for NFC-enabled device communication, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards. It harmonizes the integrated technologies, specifies implementation options and limits the interpretation of the standards; in essence, showing developers how to use NFC, ISO/IEC 14443 and JIS X6319-4 standards together to ensure global interoperability between different NFC devices, and between NFC devices and existing contactless infrastructure.

B.a.3 NFC Activity Technical Specification
The specification explains how the NFC Digital Protocol Specification can be used to set up the communication protocol with another NFC device or NFC Forum tag. It describes the building blocks, called Activities, for setting up the communication protocol. These Activities can be used as defined in this specification or can be modified to define other ways of setting up the communication protocol, covering the same or different use cases. Activities are combined in Profiles. Each Profile has specific Configuration Parameters and covers a particular use case. This document defines Profiles polling for an NFC device and establishment of Peer to Peer communication, polling for and reading NFC Data Exchange Format (NDEF) data from an NFC Forum tag, and polling for a NFC tag or NFC device in combination. The combination of Activities and Profiles define a predictable behaviour for an NFC Forum device. This does not limit NFC Forum devices from implementing other building blocks or defining other Profiles – for other use cases – on top of the existing ones.

B.a.4 NFC Simple NDEF Exchange Protocol (SNEP) specification:
The Simple NDEF Exchange Protocol (SNEP) allows an application on an NFC-enabled device to exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device when operating in NFC Forum peer-to-peer mode. The protocol makes use of the Logical Link Control Protocol (LLCP) connection-oriented.

B.b) Data Exchange Format Technical Specification

B.b.1NFC Data Exchange Format (NDEF) Technical Specification
Specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags.

B.c) NFC Forum Tag Type Technical Specifications:
The NFC Forum has mandated four tag types to be operable with NFC devices. This is the backbone of interoperability between different NFC tag providers and NFC device manufacturers to ensure a consistent user experience. The operation specifications for the NFC Forum Type 1/2/3/4 Tags provide the technical information needed to implement the reader/writer and associated control functionality of the NFC device to interact with the tags. Type 1/2/3/4 Tags are all based on existing contactless products and are commercially available.

B.c.1 NFC Forum Type 1 Tag Operation Specification
Type 1 Tag is based on ISO/IEC 14443A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability is 96 bytes and expandable to 2 Kbytes.

B.c.2 NFC Forum Type 2 Tag Operation Specification
Type 2 Tag is based on ISO/IEC 14443A. Tags are read and re-write capable; users can configure the tag to become read-only. Memory availability is 48 bytes and expandable to 2 Kbytes.

B.c.3 NFC Forum Type 3 Tag Operation Specification
Type 3 Tag is based on the Japanese Industrial Standard (JIS) X 6319-4, also known as FeliCa. Tags are pre-configured at manufacture to be either read and re-writable, or read-only. Memory availability is variable, theoretical memory limit is 1MByte per service.

B.c.4 NFC Forum Type 4 Tag Operation Specification 2.0
Type 4 Tag is fully compatible with the ISO/IEC 14443 standard series. Tags are pre-configured at manufacture to be either read and re-writable, or read-only. The memory availability is variable, up to 32 Kbytes per service; the communication interface is either Type A or Type B compliant.

B.d) Record Type Definition Technical Specifications:
Technical specifications for Record Type Definitions (RTDs) and four specific RTDs: Text, URI, Smart Poster, and Generic Control.

B.d.1 NFC Record Type Definition (RTD) Technical Specification
This specification specifies the format and rules for building standard record types used by NFC Forum application definitions and third parties that are based on the NDEF data format. The RTD specification provides a way to efficiently define record formats for new applications and gives users the opportunity to create their own applications based on NFC Forum specifications.

B.d.2 NFC Text RTD Technical Specification
This specification provides an efficient way to store text strings in multiple languages by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.

B.d.3 NFC URI RTD Technical Specification
This specification provides an efficient way to store Uniform Resource Identifiers (URI) by using the RTD mechanism and NDEF format. An example of using this specification is included in the Smart Poster RTD.

B.d.4 NFC Smart Poster RTD Technical Specification
This Specification defines an NFC Forum Well Known Type to put URLs, SMS's or phone numbers on an NFC tag, or to transport them between devices. The Smart Poster RTD builds on the RTD mechanism and NDEF format and uses the URI RTD and Text RTD as building blocks.

B.d.5 NFC Generic Control RTD Technical Specification
This Specification provides a simple way to request a specific action (such as starting an application or setting a mode) to an NFC Forum device (destination device) from another NFC Forum device, tag or card (source device) through NFC communication.

B.d.6 NFC Signature RTD Technical Specification
This specification specifies the format used when signing single or multiple NDEF records. Defines the required and optional signature RTD fields, and also provides a list of suitable signature algorithms and certificate types that can be used to create the signature. Does not define or mandate a specific PKI or certification system, or define a new algorithm for use with the Signature RTD. Specification of the certificate verification and revocation process is out of scope.

B.e. NFC Forum Connection Handover Technical Specification
This specification defines the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies. Connection Handover combines the simple, one-touch set-up of NFC with high-speed communication technologies, such as Wi-Fi or Bluetooth. The specification enables developers to choose the carrier for the information to be exchanged. If matching wireless capabilities are revealed during the negotiation process between two NFC-enabled devices, the connection can switch to the selected carrier. With this specification, other communication standards bodies can define information required for the connection setup to be carried in NFC Data Exchange Format (NDEF) messages. The specification also covers static handover, in which the connection handover information is stored on a simple NFC Forum Tag that can be read by NFC-enabled devices. Static mode is used in applications in which the negotiation mechanism or on-demand carrier activation is not required. [25, 26, 27, 28, 29, 30, 31]

C. NFC Services
Services provided by NFC technology are as follows:

C.1Connectionless Transport
An unacknowledged data transmission service with minimal protocol complexity.

C.2 Connection-oriented Transport
A data transmission service with sequenced and guaranteed delivery of service data units.

C.3Data link connection
A unique combination of source and destination service access point address used for numbered information transfer.

C.4 Logical Link Control (LLC)
It forms a part of the data link layer that supports the logical link control functions of one or more logical links. It includes interpreting message packets (PDUs) received on a network and generating appropriate response and acknowledgement data (PDUs).

C.4.1Logical Link Control Protocol (LLCP)
It provides a reliable communication channel between the local and the remote LLC that provides the transport for all data link connections and logical data links.

C.4.2 NFC Data Exchange Format (NDEF)
It defines a message encapsulation format to exchange information, for example, between an NFC device and another NFC device or an NFC tag.

C.4.3 NFC Tag
An NFC tag is a small object, such as an adhesive sticker, that can be attached to or incorporated into a product. It can store data in NDEF format. [32, 33].The following figure illustrates the NFC Services architecture. It works on client-server architecture and has four main components - NFC applications, NFC client, NFC server and NFC libraries:

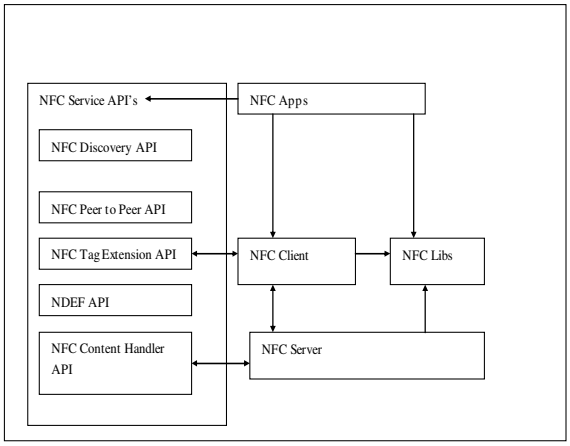
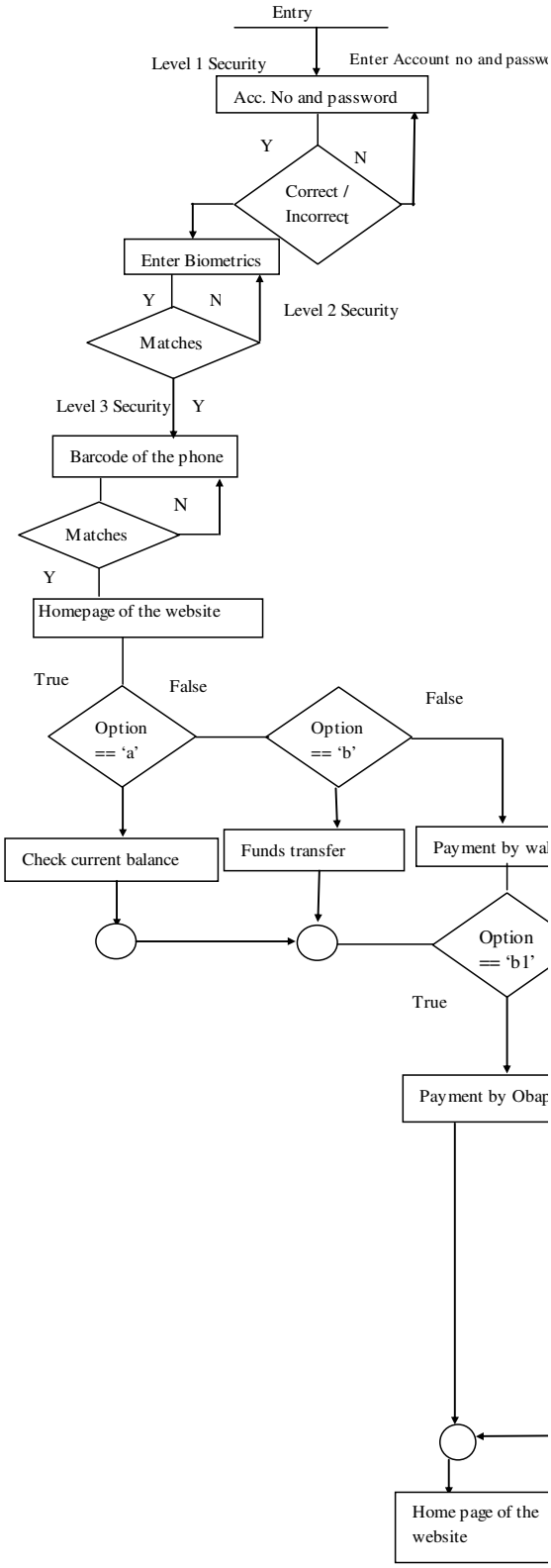
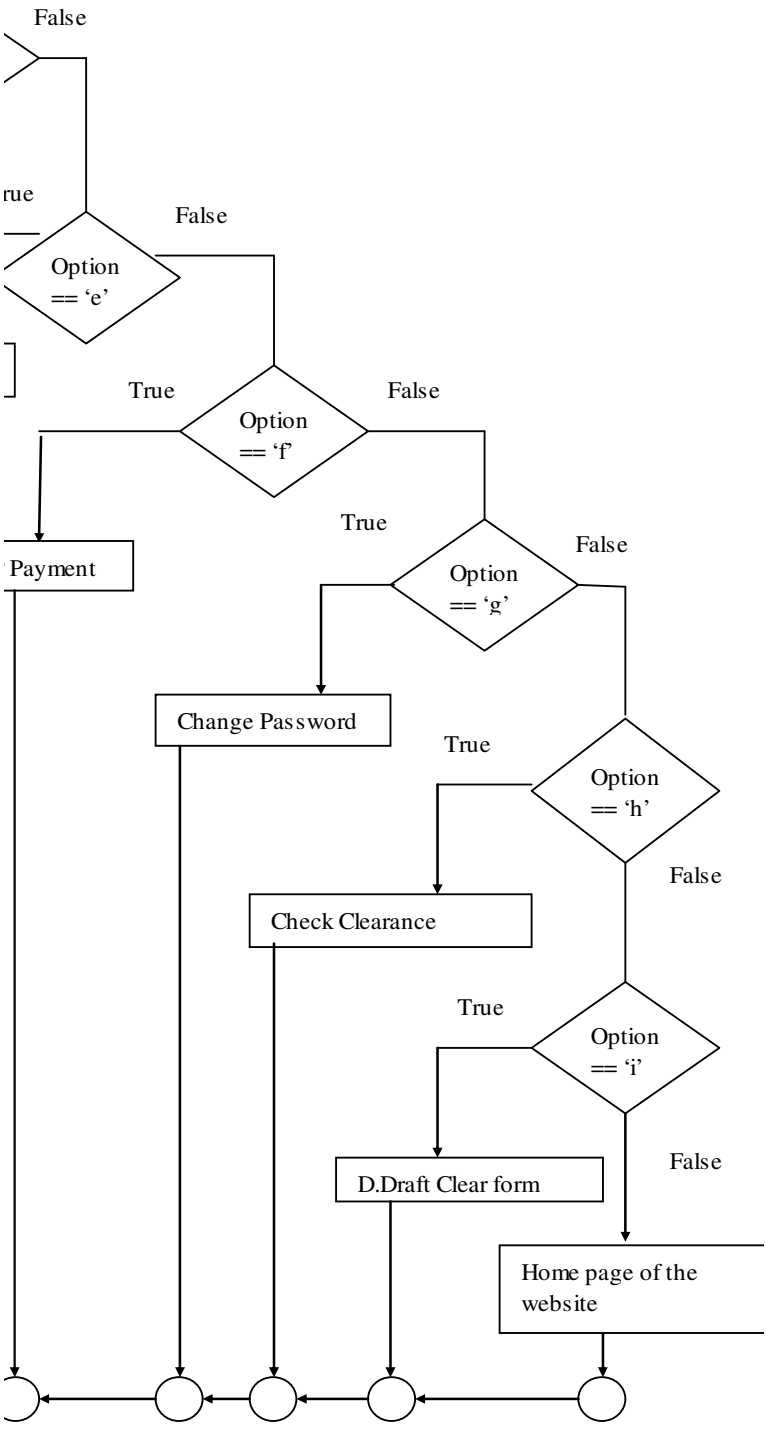


Figure 2: NFC Service Architecture

V. PROPOSED PAYMENT MODEL FOR P2P TRANSACTIONS




False
rue
False
Option
== ‘e’
True
False
Option
== ‘f’
Payment
True
False
Option
== ‘g’
Change Password
True
Option
== ‘h’
False
Check Clearance
True
Option
== ‘i’
False
D.Draft Clear form
Home page of the
website

The proposed model gives the flexibility to perform any payment or transaction, where no external entity is involved other than bank. This model is based on customer centric and bank centric approach which is useful for both the bank as well as the user. The model has the three levels of security to authenticate the user. The first step in the proposed model is to check the first level of security i.e. in the form of account number and password. After entering the account number and password the system checks the validity of the user credentials. If the user enters the right account number and password the system enters into second level of security otherwise again asks for the account number and password. After authenticating the first level the system asks for the second level of security which is the biometric template of the user. The system verifies the biometric template of the user with the stored biometric template in the database. If the user enters the valid biometric template then the system enters the third level of security i.e. barcode. The system asks for the scanning of the barcode of the phone through which the transaction takes place. After the scanning of the barcode of the phone the system asks for the type of transaction. Then, the system proceeds and enters in to the mode of transactions/payments otherwise it will continue asking the valid set of credentials till the loop ends (three times). Since, this model is also used for P2P transactions and it uses mobile wallet it becomes necessary to ask for the security of mobile device. After entering the security credentials the model gets activated and the user can perform any kind of payment or transaction. For P2P transactions or POS transactions this model is to implement the NFC technology as discussed above. The proposed model is to be implemented in J2ME.

a) The first option provided in the model is to check the current balance of the account holder. By this option the user is able to check the details of the balance in the account.
b) The second option is for transferring the funds from existing account to another account in any of the banks (money transfer).
c) The third option is the payments with the help of mobile wallets. This option is further having different choices that include payment with Pay Pal, M-check, Obapay, Pay mate. These payment options are useful for P2P transactions providing the facility to do transactions with electronic money.
d) The fourth option will be updating of the account. [34, 35]

VI. CONCLUSION This paper proposes an NFC enabled payment model that is customer centric and bank centric. The model developed provides not only the opportunity for to create ease and user friendliness for the customers but also makes possible to implement the business logic and user interface. NFC standard has impact at the system design level, application level, user interface level with multimodal features. This model should be easy to integrate into existing networks and deployed POS systems.

VII. FUTURE WORK It includes the potential security issues that may arise in the practical deployment of the proposed model. Also, OTA platforms with application deployment onto a secure element which could be the SIM or an independent chip. Some other areas of research in NFC development platforms include NFC location based, context based profile based App store, and robust web services NFC architectures and NFC application measurement platform and Tag management platforms.

References:

[1] Praveen Chandrahas, Deepti Kumar, Ramya Karthik, Timothy Gonsalvis, Ashok Jhunjhunwala and Gaurav Raina " Mobile Payment Architectures for India", National Conference on Communications,2010.

[2] Y.Lin, M.Chang, and H.Rao, "Mobile prepaid phone services", IEEE Personal Communications,vol. 7, pp 4-14, 2000.

[3] H.Aziza, "NFC technology in Mobile Phone next Generation Services", IEEE Second International Workshop on Near Field Communication 2010.

[4] Jungha Woo, Abhilasha Bhagav-Spantzel ,Anna Cinzia Squicciarini ,Elisa Bertino, " Verification of Receipts from M-Commerce Transactions on NFC Cellular Phones" IEEE Conference on E-Commerce Technology and the fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services 2008.

[5] Gerald Madlmayr, Josef Langer, "Managing an NFC Ecosystem", IEEE 7th International Conference on Mobile Business ICMB 2008.

[6] International Organization for Standardization. Near Field Communication – Interface and Protocol (NFCIP-1).ISO/IEC 14443,2009.

[7] Micheal Massoth and Thomas Bingel, "Performance of different mobile payment serviceconcepts compared with a NFC based solution" IEEE Fourth International Conference on Internet and Web Applications and Services.ICIW.2009.

[8] Mallat, N.2007. Exploring consumer adoption of mobile payments-A quantative study.J.Strateg.Inf.Syst.16,4(Dec.2007,413-432.DOI= **http://dx.doi.org/10.1016/j.jsis.2007.08.00120.02.2009**.

[9] Scornavacca, E. and Hoehle,H.2007. Mobile Banking in Germany: a strategic perspective. Int .J. Electron. Financ. 1, 3 (Mar.2007),304-320.DOI= **http://dx.doi.org/10.1504/IJEF.2007.0115012 0.02.2009**.

[10] Tomi Dahelberg, Nina Millat, Ondrus J., Zmijewska A. 2007. "Mobile Payment Market and Research Past, Present and Future: A Literature review", Proceedings of Helsinki Mobility Round table. Sprouts: Working Papers on Information Systems, 6(48). **http://sprouts'aisnet.org/6-48**.

[11] Ondrus, J. and Pigneur, Y.2007. An assessment of NFC for future Mobile Payment Systems. IEEE International Conference on the Management of Mobile Business(ICMB 2007).

[12] A. Zmijewska. "Evaluating Wireless Technologies in Mobile Payments-A Customer Centric Approach." IEEE International Conference on Mobile Business (ICMB'05) .

[13] Chen, L.2008. A model of consumer acceptance of mobile payment. Int J.Mob. Comm6,1(Jan 2008)32-52.

[14] ISO/IEC 18092 (ECMA-340), "Information technology Telecommunications and information exchange between systems Near Field Communication Interface and Protocol (NFCIP-1)", http://www.iso.org/.

[15] ISO/IEC 14443, "Identification cards-Contactless integrated circuits cards-Proximity cards", http://www.iso.org/.

[16] ISO/IEC 15693, "Identification cards-Contactless integrated circuits cards-Vicinity cards", http://www.iso.org/.

[17] Sony, "FeliCa",http://www.sony.net/Products/felica/. Cited20 December 2011.

[18] NXP Semiconductor. "Mifare Standard Specification", **http://www.nxp.com/acrobat_download/other/identification/.** Cited20 December 2011.

[19] "Near Field Communication (NFC) Forum",http://www.nfc-forum.org/,Cited 20 December 2011.

[20] C.I. Electronics, "NFC:choosing the right tag for the job."2008 **http://www.cieonline.co.uk**.

[21] Marie Reveilhac and Mar c Pasquet, "Promising Secure Element Alternatives for NFC Technology." IEEE International Workshop on Near Field Communication 2009.

[22] Mobile NFC technical guidelines,1st ed.,GSMA London Office, Ist Floor,Mid City Place,71 High Holborn, LondonWCIV 6EA,United Kingdom, 042007, Ist Revision.

[23] C.Bishwajit and R.Juha,Mobile Device Security Element, obey Forum, Satamaradanketu 3, 3rd floor 00020 Nordea,Helsinki/Finland,2005.

[24] Gerald Madlmayr,Josef Langer, Christian Kantner,Josef Scharinger, "NFC Devices: Security and Privacy" IEEE Proc. Intl. Conf. on availability, reliability and Security.2008.

[25] **www.nfc-forum.org/Technical_Architecture.pdf** Cited 20 December 2011.

[26] **www.nfc-forum.org/news/june06_architecture_schematic/** Cited 20 December. 2011.

[27] **www.rfifjournal.com/article/view/2407/2** Cited 20 December 2011

[28] **www.Nearfieldcommunication.com/developers/architecture/** Cited 20 December 2011.

[29] **www.nfc-forum.org/specs/**

[30] **www.nfc-forum.org/specs/spec_list/**

[31] **www.nfc.gov.in/eng10931-ts.pdf**

[32] **www.library.developer.nokia.com/**

[33] **www.gsmworld.com/documents/nfc-services-0207.pdf**

[34] Vibha Kaw Raina, "Integration of Biometric authentication procedure in customer oriented payment system in trusted mobile devices. **http://airccse.org/journal/ijitcs/currentissue.html**

[35] Vibha Kaw Raina & U.S Pandey. Research Objectives and an overview of wireless Technologies in payment systems. Proceedings of International Conference on Reliability, InfoCom, Technology and Optimization (Trends and Future direction). Pp .469- 476 2010.