ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (309-316), Month: January - March 2015, Available at: www.researchpublish.com

A Secure NFC Application for Credit Transfer among Mobile Phones

[1]Prof. N.B. Kadu, [2]Mr. Akshaykumar B. Tilekar, [3]Mr. Avinash D. Kanawade, [4]Mr. Shiril Y. Pathak, [5]Mr. Harshit R. Gandhi

[1]Professor, [2,3,4,5] Students, Pravara Rural Engineering College, Loni.

***Abstract*: Since the late 1990s, people have enjoyed a comfortable lifestyles. Mobile devices supported by the development of wireless networks have spread throughout the world and mobile commerce applications become the most popular application for mobile device users those who want to do business and financial transactions are available anytime, anywhere. Today the use of physical cash is experiencing a decline in popularity in the business world, because it is being acquireded by e-money. An important technology behind mobile payments is now called Near Field Communication (NFC). As it indicates that the NFC has tremendous business potential, leading companies Microsoft, Nokia and Visa Inc. is actively engaged on them. Payment processing integrated with NFC technology based mobile operating system that is a trend today. The prototype Android application is designed to pay for the user side as consumer and the merchant side as a trader or seller by using the handset that already have NFC technology is Google Nexus S. This application also implements the concept of security in e-commerce transactions by using the protocol Tag-to-Tag so thatthe user needs for security and comfort during the financial transaction are met.**

***Keywords*: Android Platform, Java Programming Language, Credit Transfer Application, Social Engineering.**

1. 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. This can also be defined as the transfer of money from one party to another through the exchange of information. Mobile devices can 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 like Interoperability, Usability, Simplicity, Security, Universality, Privacy, Cost Speed and Cross border Payments. 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. 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.

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. 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 and allowing wireless transactions only over a distance of up to 10 centimetres. The rest of the paper is organized as follows: In the next Section we review previous related work on mobile payment and technology. Then, bellowed sections describes the overview of mobile payments systems,details of NFC technology along its operating modes, architecture, standards and services, the proposed payment model where NFC technology is used for P2P transactions. Later on conclusion and future work.

2. LITERATURE SURVEY

The complexity of mobile payments for customers and merchants are strong barriers to usability and adoption. The usage of SMS for mobile payment services is criticized because the message formats are often complicated and slow to key in. The mobile paymentprocedures need to be simpler and faster includingbiometrics 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. 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.

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.

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.

3. OVERVIEW OF THE MOBILE PAYMENT CONCEPTS

MOBILE PAYMENT:

Mobile payments are also defined as the Method of exchanging financial value between two entities using mobile devices to pay for a product or service. As shown in Figure 1, alternative payment options that consumers able to pay for products or services anywhere and anytime with the convenience of using mobile devices such as mobile phones, or smartphone. The system is designed to operate using wireless technology such as Infrared, Bluetooth, Wi-Fi (802.11), WiMAX (802.16) and the latest technology that is Near Field Communication (NFC).

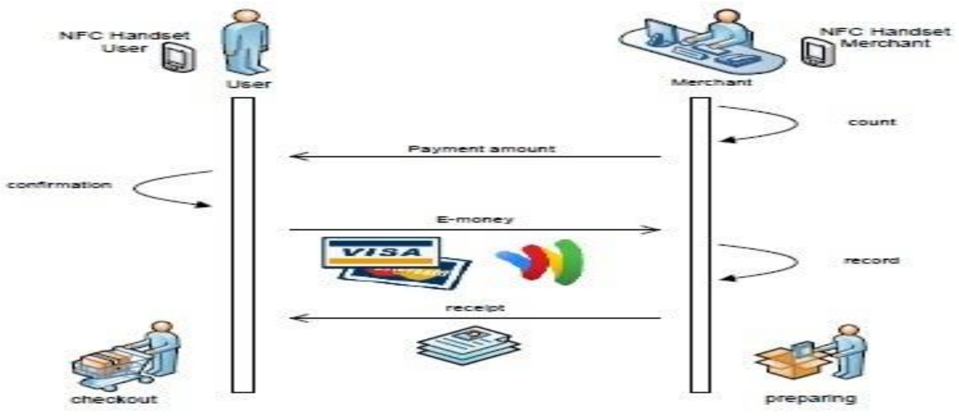

fig : The Process Of paying

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.

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 Personal Digital Assistants. Such a 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, ISO 15693, FeliCa and Mifare Standard .Further details on the potential of NFC technology can be found in .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.

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.

4. SYSTEM ARCHITECTURE

A. *NFC Architecture:*

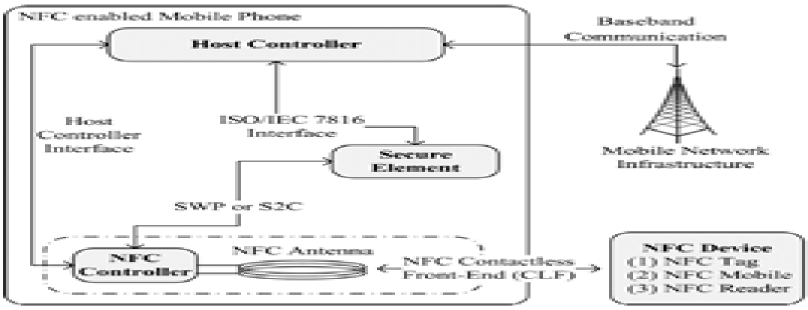

Figure1. Architecture of NFC integrated in a mobile device

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 credentials, and secure execution of NFC enabled services such as contactless payments and more than one SE can be directly connected to the NFC controller system. The supported common interfaces between SE's and the NFC controller system are the Single Wire Protocol (SWP) and the NFC Wired Interface (NFC-WI). The SE can be accessed and controlled by the host controller for 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 and host controller. And host controller sets the operating modes of the NFC controller through the HCI, processes on data that are sent and received, and creates a connection between the NFC controller and the SE. Also, host controller is able to exchange data with the secure element (internal mode for e.g. the 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 the services such as remote tracking 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.

4.1 Description:

B. NFC standards and specifications:

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

4.2 Protocol Technical Specifications:

4.2.1 NFC Logical Link Control Protocol (LLCP) Technical Specifications:

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

LLCP is a compact protocol, based on the industry standard IEEE 802.2, is designed to support both small applications with limited data transport requirements, like as minor file transfers, or network protocols, like OBEX and TCP/IP, which in turn provide a more robust service environment for applications. Hence NFC LLCP delivers a solid foundation for peer-to-peer applications, enhancing the basic functionality which is offered by ISO/IEC 18092, but by not impacting the interoperability of legacy NFC applications and chipsets.

4.2.2 NFC Digital Protocol Technical Specification:

This specification addresses the digital protocol for NFC-enabled device communication, by providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards. Also, harmonizes the integrated technologies, specifies the implementation options and limits the interpretation of the standards; in essence of showing developers how can we use NFC, ISO/IEC 14443 and JIS X6319-4 standards together to ensure global interoperability between different NFC devices, and in between NFC devices and existing contactless type of infrastructure.

4.3 NFC Activity Technical Specifications:

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 building blocks, called Activities, for setting the communication protocol. The Activities can be used as defined in this specification or can be modified to define other ways of setting up the communication protocol, covering same or different use cases. Activities may be combined in Profiles. Each Profile is having a specific Configuration Parameters and covers a particular use case. The document defines Profiles polling for the NFC device and establishment of Peer to Peer communication, polling for and reading the NFC Data Exchange Format (NDEF) data from a NFC Forum tag, and polling for a NFC tag or a NFC device in the combination. The combination of Activities and Profiles define a predictable behavior for NFC Forum device. This does not limit to NFC Forum devices from implementing other building blocks or defining other Profiles – for other use cases – on top of the existing ones.

NFC Simple NDEF Exchange Protocol (SNEP) Specification:

The Simple NDEF Exchange Protocol (SNEP) allows the application on a 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 the use of the Logical Link Control Protocol (LLCP) connection-oriented.

4.4 Data Exchange Format Technical Specification:

4.4.1 NFC Data Exchange Format (NDEF) Technical Specification

Specifies a common data format used by NFC Forum-compliant devices and NFC Forum-compliant tags.

4.5 NFC Forum Tag Type Technical Specifications:

The NFC Forum has mandated the four tag types to be operable with NFC devices. This is backbone of interoperability between different NFC tag providers and the NFC device manufacturers to ensure a consistent user experience. The operation specifications for NFC Forum Type 1/2/3/4 Tags provides the technical information needed for the implementation of 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 they are commercially available.

4.5.1 NFC Forum Type 1 Tag Operation Specification

Type 1 Tag is always based on ISO/IEC 14443A. Tags are capable of read and re-write; users configure the tag to become read-only. Memory availability starts from 96 bytes and expandable to 2 Kbytes.

4.5.2 NFC Forum Type 2 Tag Operation Specification:

Type 2 Tag is mainly based on ISO/IEC 14443A. Tags are capable of read and re-write; users can configure tag to be read-only. Memory availability starts from 48 bytes and expandable to 2 Kbytes.

4.5.3 NFC Forum Type 3 Tag Operation Specification:

Type 3 Tag mainly based on the Japanese Industrial Standard (JIS) X 6319-4, also called as FeliCa. Tags can be pre-configured at manufacture to be both read and re-writable, or read-only. Memory availability may vary, theoretically limits to 1MByte per service.

4.5.4 NFC Forum Type 4 Tag Operation Specification 2.0:

Type 4 Tag is always fully compatible with the ISO/IEC 14443 standard series. Tags can be pre-configured at manufacture to be either read and re-writable or read-only. The memory availability may vary, up to 32 Kbytes per services; the communication of interface is either Type A or Type B compliant.

4.6 Record Type Definition Technical Specifications:

Technical specifications of Record Type Definitions (RTDs) and four specific RTDs: Text, URI, Smart Poster, and Generic Control.

4.6.1 NFC Record Type Definition (RTD) Technical Specification:

The specification specifies the format and rules for building standard record types using NFC Forum application definitions and third parties that may base on the NDEF data format. The RTD specifications provide way to efficiently define record formats for new applications and giving the users opportunity to create their own applications based on NFC Forum specifications.

4.6.2 NFC Text RTD Technical Specification:

The specification provides a way to store text strings in multiple languages by using the RTD mechanism and NDEF format. An example of using the specification is to include the Smart Poster RTD.

4.6.3 NFC URI RTD Technical Specification:

The specification provides an efficient way to store Uniform Resource Identifiers (URI) by using the RTD mechanism and NDEF format. Example of using this specification is included in the Smart Poster RTD.

4.6.4 NFC Smart Poster RTD Technical Specification:

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

4.6.5 NFC Generic Control RTD Technical Specification:

The Specification provides a simple way to request the specific action (such starting an application or setting a mode) to a NFC Forum device (destination device) from another NFC Forum device, tags or cards (source device) through NFC communication.

4.6.6 NFC Signature RTD Technical Specification:

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

4.6.7 NFC Forum Connection Handover Technical Specification

The specifications define the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies. Connection Handovers the combine’s simple, one-touch set-up of NFC with very high-speed communication technologies, such as Wi-Fi and Bluetooth. The specification enables developers to choose the carrier for information to be exchanged. If matching the wireless capabilities revealed during the negotiation process between two NFC-enabled devices, the connection can be switch to the selected carrier. With the specification, other communication standards bodies can also define information required for the connection setup to be carried in NFC Data Exchange Format (NDEF) messages. The specifications are also covering static handover, in which connection handover information is stored on a simple NFC Forum Tag that can be read by NFC-enabled devices. Static modes are used in applications in which the negotiation mechanism or on-demand carrier activation is not required.

4.7 NFC Services:

The Services provided by NFC technology are as:

Connectionless Transport:

An unacknowledged of data transmission services with minimal protocol complexity.

Connection-oriented Transport:

A data transmission of services with sequenced and guaranteed delivery of service data units.

Data link connection:

It is a unique combination of source and destination service access point address used for numbered information transfer.

Logical Link Control (LLC):

It forms a part of the data link layer which supports the logical link control functions of one or more logical links. It includes the interpreting message packets (PDUs) received by a network and generating appropriate responses and acknowledgement data (PDUs).

Logical Link Control Protocol (LLCP):

It is providing a reliable communication channel between the local and remote LLC that provides the transport for all data link connections and logical data links.

NFC Data Exchange Format (NDEF):

This defines the message encapsulation format to exchange information, for example, between an NFC device and another NFC device or an NFC tag.

4.8 NFC Tag:

NFC tag is a small object, such as adhesive sticker, that can be attached or incorporated into product. It can also store data in NDEF format. The following figure is illustrating the NFC Services architecture. It is working on client-server architecture and has four main components - NFC applications, NFC client, NFC server and NFC libraries.

The layer of protection. We refer to this as passive anti-phishing approach. This is only because the approach only attempts to locally protect individual from a phishing attack, but does not actively make any kind of effort to remove or shut down the Phisher at source. In effect, the Phisher is a free to continue with his/her operation and can be potentially accrue the further victims. Many several spam filters, browser tools, anti-spyware and anti-virus software are available to protect online of computers from various attacks. However, there were very less research efforts have been entirely focused to protect online users from phishing attacks in past. Existing anti-phishing and anti-spam techniques may suffer from one or more limitations and they are not 100% effective at stopping all spam and phishing attacks.

The intuition of the clustering is to separate points at different groups according to their similarities. For data given in the form of a similarity graph, the problem can be restated as follows: we want to find partition of the graph like the edges between different groups have a very low weight (which means that points in different clusters are dissimilar from each other) and the edges which are within a group have high weight (which means that points within the same cluster are similar to each other).

Embedding is used in an unnormalized spectral clustering is related to the commute time embedding, but is not identical. In spectral clustering, we map vertices of graph on the rows yi of matrix U, while to commute time embedding maps the vertices on the rows zi of the matrix (_†)1/2U. That is, compared to entries of yi, the entries of zi will additionally scaled by the inverse eigenvalues of L. Moreover, in spectral clustering we can only take the first k columns of matrix, while commute time embedding takes all columns. Several authors will try to justify why yi and zi are not so different after all and state a bit of hand-waiving that the fact that spectral clustering constructs clusters based on Euclidean distances between the yi and can be interpreted as building clusters of the vertices in the graph based on commute distance. However, note that both the approaches can differ considerably.

Phishers may be able to find ways to bypass existing rule-based and statistical-based filters without having much difficulty. Many e-mail service providers such as Yahoo, Hotmail, Gmail, and AOL filter all the incoming emails separating them into Inbox (legitimate email) and junk (illegitimate email) email folders. However, these are the e-mail service providers do not actually attempt to remove the phishing pages associated with the illegitimate email. Furthermore, Phishers have the readily available tools to bypass the spam filters.

5. 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.

6. FUTURE SCOPE

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

[2] 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.

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

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

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

[6] 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.2007.08.001 20.02.2009**.**

[7] 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.2007.01150120.02.2009**.**