International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:6, 2013

An Efficient Mobile Payment System Based On NFC Technology

Shafiq ur Rehman and Jane Coughlan

***Abstract*—**The work we have accomplished in implementing a Mobile Payment mechanism that enables customers to pay bills for groceries and other purchased items in a store through the means of a mobile phone, specifically a Smartphone. The mode of transaction, as far as communication between the customer's handset and the merchant's POS is concerned, we have decided upon NFC (Near Field Communication). This is due to the fact that for the most part, Pakistani Smartphone users have handsets that have Android mobile OS, which supports the aforementioned platform, IOS, on the other hand does not.

***Keywords*—**Usability, mobile payment system, NFC technology, payment process, customer.

I. Introduction

TODAY the world is moving towards mobile computing. Tasks done through mobile phones/devices are increasing the easiness of doing everyday tasks. Important tasks of daily life revolve around payments which can be cash or through bank transfers. To make this process easy for consumers several institutes are working on mobile payment of which the major part is on security of mobile payment. There have been many extensive studies on this topic. Mobile phones have revolutionized the lives by bring mobility. The use of mobiles phones has been increased with the passage of time. The mobile phones are today used for the payment of money. In the beginning it was only used for the small transactions and the medium was IVR or SMs but today mobile phones can be trusted with the bigger transactions and other mediums like WLAN and NFC are also used. The mobile phone where have provided its user's with the facility have also exposed them to several issues like security. The people need their transaction to be secure and trustworthy. The information of the users must be confined to the concerned departments and no third party should be involved.

The sensitive information like passwords and account numbers must be kept secure. There is a special term for this "M-Commerce". The mobile phones are currently being used for the purchasing of the music, pictures, and software applications. The market of mobile phone is now entering in to the new dimensions and being used in the replacement of credit cards. The rapid increase and growth of the mobile payment is also leading to several threats like security, trust, privacy and reliability. The success of mobile payment is lies only if the users are provided with the above mentioned features. Therefore research has been conducted on the feasibility of mobile payments methods and how they can be made more secure, reliable and useable for the consumers so that they can use it without any hassle.

Shafiq Rehman is a PhD Student at Department of Information System and Computing, Brunel University, West London, UK.
Jane Coughlan is a lecturer at Department of Information System and Computing, Brunel University, West London, UK.

II. Literature Review

The authors (Istrefi & Cico 2005) [1] have explained the essence of mobile payment through integrated NFC module on smart-phones. They have highlighted the issues that mobile payment methods face, both generic and some of them specific to NFC and their solutions are also discussed. Some of the prominent issues include security, supply and demand, and user experience. The solution presented adds another software layer (agent) to the NFC hardware, through which we can customize the mobile payment and solve the problems which we are currently facing. Software agents will also gather the relevant information about the product and present it to user, minimizing the errors.

This article discusses the research being done on biometric security for mobile payments. This article is based on the patent, filed in February 2006, registered by Universal Secure Registry [2]. It is their proprietary technology for secure mobile financial transactions. This authentication can be used/ integrated with NFC and ZigBee. The security system USR proposed uses three identification factors (token, Secret, Biometric) adding on that an additional layer of biometric, a photo of the purchaser.

In this paper, (Hsu-Chen Cheng et al, ICACT 2009) [3], discussed the various issue and advantages of using NFC technology for mobile commerce. They propose a generic model for employing NFC in mobile commerce; called NMC (NFC based Mobile commerce). This model comprises of six phases namely: Initialization, order, payment/collection, services and loyalty management. They go onto to elaborate that these stages/phases can be implemented independently with the exception of initialization phase and may occur in various permutations of sequences according to the need of the scenario they serve. In the initialization phase there are four steps, these are: back-end services, terminal services, tags and handsets. This phase is typically followed by order phase, payment phase and finally shipping collection phase. This model was implemented in a restaurant successfully, which goes onto show that, while there are security and other issue at the heart of this technology, with a little improvement and tweaking, NFC based mobile commerce can not only aid

different businesses, it can lend much needed ease of use to them.

This mobile payment method has been proposed in (Devendra Mani et al, 2012) [4] in this paper the process is aimed at reducing the cost and time of generating public key operation and registration process in Mobile payment. They proposed a system that includes three stakeholders namely: The client (customer), the Merchant and the Issuer. The client exchanges messages with the issuer through the merchant to satisfy integrity and other aspects of mobile transactions and complete a successful transaction. Once the client has bought a product, the client sends a message to the issuer through the merchant in return of which the client gets confirmation message via the payment gateway of a successful transaction. The payment gateway, while confirming the transaction for the customer also sends a message to the merchant indicating that the correct amount for the transaction has been sent to their account. This proposed method, is intended to ease mobile payment procedures for owners of low-end mobile handsets that cannot support other resource demanding methods such as NFC and RFID transactions.

(Pirker and Slamanig 2012) [5] Presented a solution to the privacy issues faced by mobile payment methods, in this paper targeted at highlighting privacy problems and their solutions when it comes to smart-phone usage for mobile commerce. The core focus of the paper is to elaborate privacy checks as implemented in the T&T system, the system has been targeted as an example to highlight privacy loop holes and subsequently they've proposed a solution wherein privacy is preserved in mobile payment through recent advancements in ARM processor platform and resource payment. Payment is largely based on prepaid mechanisms in this approach, the system works on the assumption that a client owns a state of the art smart-phone; the smart-phone's platform integrates ARM's trust-zone technology. Through this a platform partition is achieved that provides a secure passage into a secure space, logically, where security and privacy sensitive data can be stored, furthermore, for traditional OS and other application tasks a separate normal environment is provisioned. For this to work the smart-phone must have NFC based capabilities for Bi-directional communication.

(Jhe-Yi-Hu et al 2012) [6] Present the premise that android based mobile E-commerce can perform up to the required standards of security and serviceability. In the approach put forth in (Jhe-Yi-Hu et al 2012), the concept centre's around provision of a counter reader and a payment client on an android enabled smart-phone. The 3 factor authentication method mixes PIN code authentication, USIM card authentication and facial recognition through biometric procedures. For the transactions to take place in a low risk environment, 3 factor authentications is both effective and secure. Biometric measure is the most important and key element of this technology and the built in camera has become almost a must in a cell phones, expensive and cheap therefore the objective of facial recognition can be easily achieved.

In this article, (Kiran Kadambi et al, 2009) [7] the research put forth sponsored by HP suggests that NFC based mobile payment can be made secure through the introduction of a collection of software agents. The interaction of a user mobile with a point of sale terminal has been established through issuing a token to the specific mobile device, this eliminates that need for exchange of personal information such as PIN numbers and user passwords. The software agent layer provides a secure environment for communication by introducing two modules namely: The adaptive bank an abstraction of banking services tailored to the needs of the transaction at hand and a Retail store assistant (RSA) software agent that intermediates the transaction being done at a particular point of sale terminal (POST).

The idea proposed in (Riti Chowdhury and Debashish De, 2011) [8] is that secure mobile payment can be achieved in global markets using NFC enabled mobile wallets. The mechanism behind the protocol floated is that each user has a session dedicated to them. From a pool of cryptography algorithms, an algorithm is chosen and the stipulation that the chosen hadn't been chosen for any previous transaction is checked. Once the condition is verified, a key is allotted to the session. A dedicated server is maintained for storing the cryptography algorithms and an intermediary known as the trusted party is responsible for communication between the mobile wallet of the user and the crypto server. Secure communication is achieved through employing wireless protocols such as WTLS (Wireless Transfer Layer Security) and WTP (Wireless Transfer Protocol). A function named as Ranf() is used to alternate between various disparate algorithm for any particular transaction of a session established for the user. The differentiating factor being that no two transaction should use the same cryptography algorithm for encryption of user information.

In this article, (Geoffrey Ottoy et al, 2011) [9] have presented an alternative hardware approach to the security problem posed by NFC. The pitfalls of NFC are that it doesn't provide a robust mechanism of secure communication; due to this the technology has not been able to garner the kind of reception that had been initially estimated. For this purpose, as has been discussed in (Geoffrey Ottoy et al, 2011) an alternative hardware approach seems to be the best course to take. In a multiprocessor environment the tasks of testing a secure communication channel and encryption of enclosed messages have been delegated to two cores one labeled a crypto core and the other as CPU. For the purpose of testing they have implemented remote monitoring system within the environment. Unlike traditional approach they haven't used microcontroller based system instead they have gone for FPGA with two power PC cores.

In this research paper (Mia Olsen, Jonas Hedman et al, 2012) [10] have conducted a Design inquiry of m-wallet based on contribution of the exist research by conducting a m-wallet design survey based analysis .Four Focused groups were targeted young teenagers, young Adults ,mothers and Businessmen, prior to that a survey and comparison analysis of the existing mobile payment was conducted, the result shows that many existing solution failed to be adopted by the public , one of the reason behind was the usability and design

factor raised from lack of user involvement when designing m- wallet. The research involves identification of m-wallet properties (design properties and technical properties) with focus of user interaction in the designing m-wallet system to have deep insight of user level issue while using m-wallet system. Designing process being followed in this research divided into a number of phases.

In this research paper (Wei Dai, Shou, Zhou et al, 2011) [11] have analyzed different site charge mobile payment technology current available in use the market. Based on their research survey site charge mobile payment shows potential growth in the market, particular RFID based mobile payment system which offers security convenience. Research highlight brief work description of RFID based mobile payment system, intro of different RFID based includes SIM pass RFID system, near field communication system RF-SIM. Comparison analysis based on a number of evaluating factors includes working range, reading speed, security, reliability and compatibly lead to a point that NFC which involves better security, compatibility, range and affordability is the most appropriate choice of system for the Chinese market, apart from that research also indicates that effort should be put in toward promotion of this technology in the corporate sectors and up gradation of POS system in order to make this technology successfully adopted in the market.

III. Recommended Architecture

The Fig. 1 shows the complete architecture of the application and describes how it works.

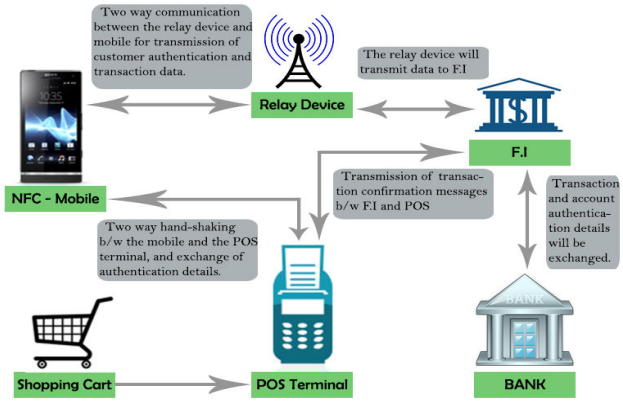

Fig. 1 Architecture

A. Main Success Scenario

- The user enters their username and password in the corresponding fields in the application interface.
- The user enters the merchant's, from whom the purchase is being made, merchant Id which would be assigned to them by the financial services institution.
- Both the user's and the customer's ID's are verified by the financial institution and they allowed to proceed further.
- The user checks the price for individual items in the corresponding fields in the application interface and confirms the net total.
- The user selects the pay bill option on the application interface; the financial services institution verifies that the required amount is present in the user's account via the corresponding bank.
- Once the validation has been performed, application performs the payment and the financial services institution sends confirmation of the said payment to both the user and the merchant.

B. Payment Process

The aforementioned process deals with the abstract concept payment and describes how the payment will be handled.

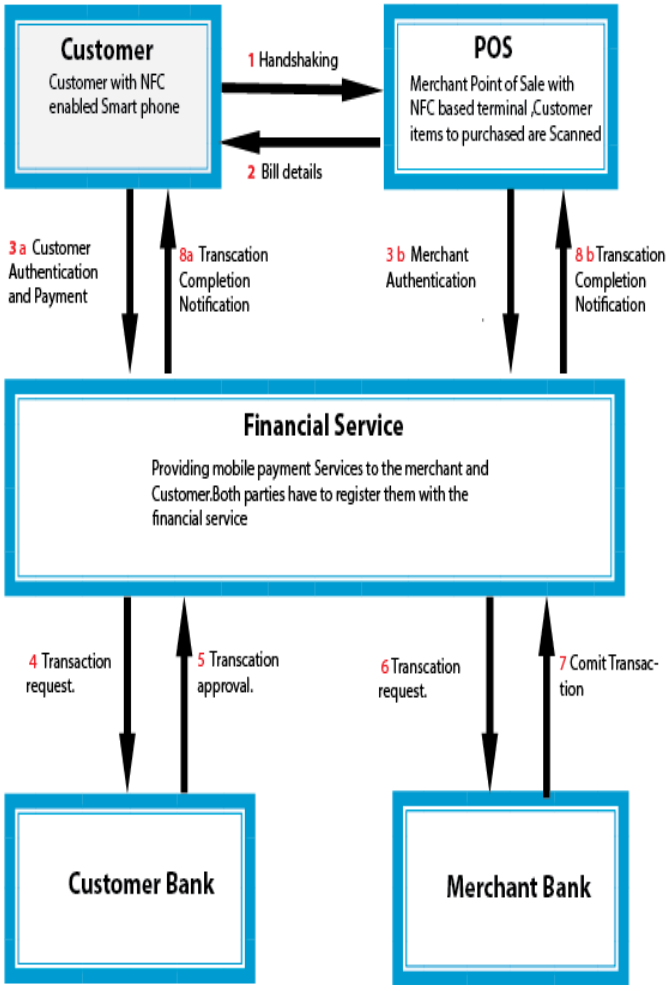

Fig. 2 Payment Process

1. Assumption and Dependencies:

Assuming Customer has NFC based Smart phone. NFC receiver is installed in the shop's point of sale counter. Information exchange between two devices is encrypted.

Constraints

2. Payment through Multiple accounts not possible:

Both applications are provided by the same financial service.

C. Application Types

The following are the types of application used during the

Payment process:

Mobile app used by customer

Desktop Application installed on the Point of Sale used by shop personnel's

D. The Process – Payment Process

Step 1: Handshaking

Customer arrives at point of sale counter after picking up groceries .Customer place it NFC enabled smart phone in front of the point of Sale NFC receiver with physical shopping mobile application being open. A hand shake (communication link formation) between. Customer application id and shop id is exchange between the two devices.

Step 2 Bill Details

Customer Items are scanned on the POS and Customer application display list of items to be purchased by the customer along with total amount of the Bill.

Step 3 Authentication

Customer and Merchant authentication is performed by the financial institution. Customer and merchant are authenticated via pin authentication number, which is verified at the financial institution.

Step 4 Transaction Request

A transaction with the customer's authentication details shall be sent to the bank for account related matters.

Step 5 Transaction Approval

Once it has been verified that the transaction can be made as per account details and bill requirements, the transaction is made and preserved.

Step 6 Transaction Request

Same as step 4.

Step 7 Transaction Commit and Notification:

Once the transaction is committed and preserved, the relevant notifications are relayed to the customer and the merchant.

E. Sequence Diagram

1. Login

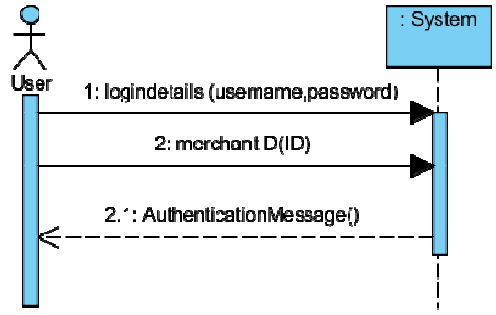

Fig. 3 Login

2. Payment Confirmation

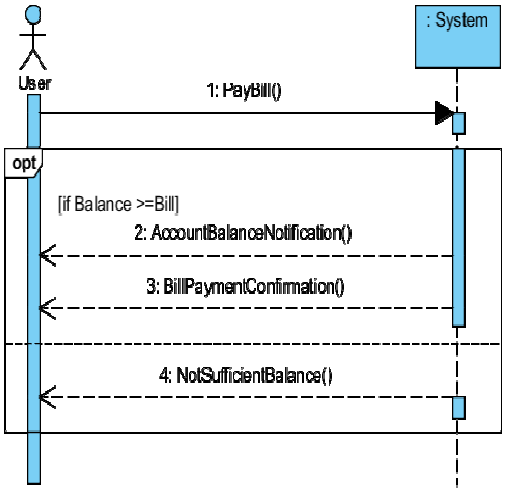

Fig 4 Payment

IV. Conclusion

The proposed designed allays most of the issues faced by the masses in their daily purchases and that the application provides the necessary groundwork for further development in the field of mobile payment system. The intended architecture is designed by keeping interface interactive and simple and very much similar to normal mobile application so that user can easily grasp idea out of it, so as to increase the user learning curve by introducing short procedural steps to make transaction.

References

[1] Dashmir Istrefi & Betim Cico, 2012. NFC Based Mobile Payment MECO Bar, Montenegro.
[2] Biometric Technology Today, September 2011, Elsevier, Amsterdam.
[3] Hsu-Cheng-Chen,Jen-Wel-Chen, Tain-Yow-Chi and Pin-Hun-Chen A Generic Model for NFC based Mobile E-commerce, 2009.
[4] Devandra Mani Tripathi and Aparajita Ojha, An Efficient Lightweight Protocol for Mobile Payment, 2012.

[5] Martin Parker and Daniel Slamanig, A Framework for Privacy Preserving Mobile Payment through Enhanced ARM Trustzone Platforms, 2012.
[6] Jhe-Yi-Hu, Chien-Chen-Sueng, Wei_Hsiang-Lioa & Chian C.Ho, Android Based Mobile Payment Service prtotected by 3 Factor Authentication and Virtual Private Ad-hoc Networking, IEEE 2012.
[7] Kiran S. Kadambi, Jun Li, & Alan H. Karp, Near-Field Communication-Based Secure Mobile Payment Service.
[8] Riti Chowdhury and Debashis De, Secure Money Transaction in NFC Enabled Mobile Wallet Using Session Based Alternative Cryptographic Techniques, 2011.
[9] Geoffrey Ottoy, Jeroen Martens, Nick Saeys, Bart Preneel, Lieven De Strycker, Jean-Pierre Goemaere, and Tom Hamelinckx, A Modular Test Platform for Evaluation of Security Protocols in NFC Applications, IFIP International Federation for Information Processing 2011.
[10] Mia Olsen, Jonas Hedman, and Ravi Vatrapu, Designing Digital Payment Artifacts, Association for Computing Machinery, 2012.
[11] Wei Dai, Shuo Zhou, Guangjun Luo, Zongxing] Chen, and Ling Xie, Analyze on Mobile Payment Based on RFID, 2011