

A Secure Application For Shopping in Mall using NFC

Monika S. Borkar
(Student)
ZCOER, Pune

Piyusha . Kadam
(Student)
ZCOER, Pune

Nikita P. Pagar
(Student)
ZCOER, Pune

Aboli G. More
(Student)
ZCOER, Pune

Akshada Deokar
(Asst. Prof)
ZCOER, Pune

Trupti Suryawanshi
(Asst Prof.)
SCSCOE, Pune

Abstract- Now a days, technology has reached up to an extent that everything has become advanced its an age of new and immersing technologies which also plays an important role in enhancing quality of life. Money transaction between mobile devices is bored and a difficult operation to perform since there is not a simple and safe way to do it. Near Field Communication (NFC), an emerging short-range wireless point to point interconnection technology, with the combination of handheld electronic device has become a potential tool for the two devices to exchange various information when in close range. It provides high level of comfort to users as it can communicate without any further configuration steps when two devices brought very close to each other and to enjoy the privilege for accessing the content services in an intuitive way just by simply “touching” smart objects. The major advantage of NFC compared to other wireless technology is its simplicity. NFC enabled mobile device establish a wireless transaction system to make payment. By using NFC this paper proposed a secure NFC payment application which is introduced in paper to demonstrate its use in shopping malls to make the payment system more easier and queue-less.

Index Terms— Near Field communication, handheld electronic device, NFC enabled mobile device.

I. INTRODUCTION

Near Field Communication (NFC) [1] is a new short range (maximum 10cm) wireless communication technology with security support. It emerged from the combination of contactless identification (Radio Frequency Identification - RFID), interconnection technologies (ISO14443A/MIFARE/FeliCa) and mobile phone devices[1],[2]. A potential application of NFC, contactless payments using NFC-enabled mobile phone enables secure and convenient purchases in a wide range of transactions [2]. Near Field Communication can be used in various fields and its application in medical field is more considerable now a days [3]. When we go for shopping in malls there is a long queue for payment, we need to wait for a long time to pay bill which is very boring and time consuming. To overcome these constraints, existing systems need to be changed, so that payment process will become easy. For solving this problem we propose a model based on NFC which will also include QRcode (Quick Response Code). QR code is can be easily scanned by integrated cameras which are present in smart phones. QR code is a two dimensional bar code invented by Japanese corporation Denso Wave where information is coded in

both vertical and horizontal direction, thus holding up to several hundred times more data than that of a traditional barcode [4]. We present the methodologies and the Software Application Program Interfaces (API's) associated with these technologies for their use in mobile phones. After scanning QR code bill will get generated and for paying payment NFC terminal will be used. The rapidly growing number of wireless communication users had lead to increasing demand for security measures and devices to protect user data transmission over wireless channels [5]. Symmetric cryptography is more suitable for encryption of large amount of data. The AES(Advanced Encryption Standard) is a symmetric block cipher that is used in model for providing security for payment transaction.

II. LITERATURE REVIEW

A proposed NFC payment application proposed by Pardis Pourghomi, Muhammad Qasim Saeed, Gheorghita Ghinea [8] is a transactional protocol that provides a secure and trusted communication channel to the communication parties. The disadvantage is that this method of payment is a micropayment where people can only use this payment method to pay for cheap products.

Nagashree R N et.al.[2] stated that NFC is being most prominent technology for contactless system seems to be fulfilling the growing demands of mobile contactless communication. The paper also gives comparison of NFC with other existing popular technologies.

Mabel Vazquez-Briseno et.al.[7] explained the use of mobile phones for linking physical objects with digital world using AIDC techniques. And also described API's required for implementing mobile applications with QR code and NFC technologies.

Ritu Pahal and Vikas Kumar [5] presented a new AES model having bigger block size which is 200 bits rather than conventional 128 bits AES. And also compared the throughput of various AES standards and concluded that the throughput at encryption end of AES – 200 is 15% more than AES – 128.

David M. Monteiro et.al.[1] explored the capabilities of the novel NFC technology for enabling secure mobile application and demonstrate it through the proposal of a NFC peer-to-peer mobile application, founded on NFC Forum rules and Android NFC API's. And also stated that with a simple touch of two NFC enabled devices it is possible to create reliable, safe and trusted operation for money exchange.

III. PROPOSED SYSTEM

The aim of this system is a try to create a wireless payment system for shopping malls. The payment should be free of credit /debit cards, hard cash, etc. This is always time consuming and needs queue architecture. The users need not to worry about the cash or cards being theft. We are going to build a queue-less payment system which can be used by people from anywhere within mall to pay for their purchase.

User having NFC enabled Android mobile will have an Android application for shopping in a particular mall. As the user will enter mall, he/she has to login app and then just click pictures of QR Code on the products, which he/she wants to purchase. The selected products will get added to cart and bill will get generated.

For payment the user has to just “touch” NFC Terminal with his/her Android enabled NFC phone and the bill will get paid automatically through bank server.

A. Block Diagram of System

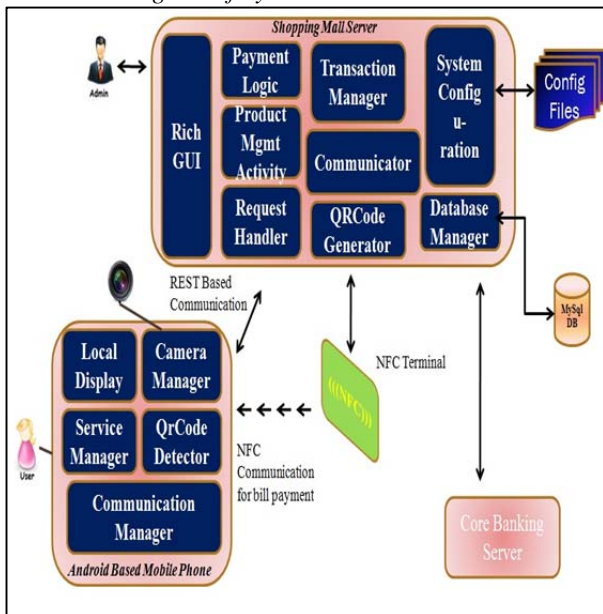


Figure 1 : Architecture Design

The architecture of the system will mainly consist of three modules and two users.

1. Shopping mall server
2. NFC enabled Android based mobile phone
3. Core Banking server
4. NFC tag

1) *Shopping mall server:* First user, Admin will have access to this server. Administrator will be able to do following activities:

- I. Add/Update product information
- II. Generate QRCode for products
- III. Set offer/discount
- IV. View daily/Monthly/Yearly reports
- V. Connected to NFC Terminal.

Including above operations mentioned, to perform them the shopping mall server will be composed with or will have following components:

Rich GUI: A rich graphical user interface will be there to perform these operations consistently.

Payment Logic: When the user will do payment i.e., touch NFC terminal, what actions will be take place at that time i.e., starting from checking account balance to bill payment will be involved in payment logic.

Product Management Activity: This module will facilitate to manage different products, like checking stock, programming analysis of products, if users delete some products from his/her cart it will also be deleted by admin. **Request Handler:**

Request Handler: There will be different types of request like log-in and authentication, adding/deleting products, request for payment. These types of request will be handled by the request handler module.

Transaction Manager: When a customer will do payment using NFC the transaction must take place in between user-bank server, bank server-mall server, to perform money transactions **Transaction manager** module is there which will also monitor them.

Communication: Communicator will act as a communication module.



Figure 2 : QR Code

QRCode generator: Generally, now a day every product has its own QR Code, then also there will exist a separate QRCode generator which will generate QRCode for products with change in selling price or discounts.

System Configuration: It will contain the configuration files required for the system.

Database Manager: We will using MySQL database, therefore to perform various operations on database, there exists a database manager.

2) *NFC enabled Android based Mobile phone:*

The second user i.e., customer will have an Android based mobile phone which will be NFC enabled. This is the second main component of our system.

Using these the user will be able to perform following operations:

- I. Scan QR Code
- II. Add/Delete items
- III. View item details

IV. NFC PAYMENT SUPPORT

The user mobile camera will be used for detecting QR Code.

QR Code detector: To detect the QR Code captured by camera there will be a module named QR Code detector.

Local Display: There will an Android based application for shopping, it will have a display which will contain cart, adding /deleting the facility etc.

Communication Manager: It will manage the communication between the mobile phone and the shopping mall server.

Core Banking Server:

The core banking server is for transactions between customer and shopping mall. It will transfer money from customers account to malls account. Firstly, it will check for the available balance, if balance is not sufficient the payment will not be done.

NFC Terminal:

NFC Terminal is nothing but a NFC tag which is a replacement of outage counter or billing counter. The customer will just touch the NFC terminal with mobile phone and bill will get paid.

For providing security to money transaction between user and bank server there will be used an encryption algorithm i.e. AES algorithm will be used for it. AES is Advanced Encryption Standard, uses an identical key for the sender and receiver, both to encrypt the message text and decrypt the cipher text. Asymmetric cryptography, such as in the Rivest-Shamir-Adleman (RSA) uses different keys for encryption and decryption, eliminating the key exchange problem. Symmetric cryptography is more suitable for the encryption of a large amount of data. The AES algorithm defined by the National Institute of Standards and Technology (NIST) of the United States has been widely accepted to replace DES as the new symmetric encryption algorithm [5]. The AES algorithm is a symmetric block cipher that processes data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. Each data block consists of a 4×4 array of bytes called the *state*, on which the basic operations of the AES algorithm are performed.

IV. CONCLUSION

In this paper we have designed and developed a NFC based application for credit transfer which can be mainly used for paying payments in shopping malls. An user sign-in into android based application and clicks pictures of QR code of products which are needed. Automatically bill gets generated and user can pay the bill at just one touch to NFC terminal, user will select bank account details and the bill will get paid. The AES algorithm is used for providing security to user's bank details i.e. bank details will be encrypted and then sent to server. As compared to barcode QR codes are more store data in both the vertical and horizontal direction. Thus QR code can hold up to several hundred times more data than a traditional bar code. Thus we aim to build a queue-less payment system, such that it will be time saving and there will be no risk and fear of pick pocket or money theft. There will be no need to carry any hard cash or debit/credit cards.

REFERENCE

- [1] David M Monterio¹, Joel J. P. C. Rodrigues¹, and Jaime Lioret², "A Secure NFC Application for Credit Transfer Among Mobile Phones", ¹ *Instituto de Telecomunicacoes, University of Beira Interior, Portugal.* ² *Integrated Management Coastel Research Institute, University Politecnica de Valencia, Spain.* david.monteiro@it.ubi.pt, joeljr@ieee.org, jlloret@dcom.upv.es
- [2] Ashwini N, Nagashree R N, Vibha Rao, "Near Field Communication", *IJ Wireless Technologies*, 2014, 2, 20-30. Published online March 2014 in MECS (<http://www.mecs-press.net>) DOI: 10/5815/ijwmt.2014.02.03
- [3] G. Gopichand, T. Krishna Chaitanya, R. Ravi Kumar, "Near Field Communication And Its Applications in Various Fields", ISSN : 2231-5381, *International Journal of Engineering and Technology (IJETT) – Volume4 Issue4- April 2013*
- [4] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schittwieser, Mayank Sinha, Edgar Weippi, "QR Code Security", *SBA Research*
- [5] Ritu Pahal, Vikas kumar, "Efficient Implementation of AES", ISSN : 2277-128X, *International Journal of Advanced Research in Computer Science and Software Engineering – Volume 3 Issue 7- July 2013*
- [6] Kevin Fiscus, "Base64 Can Get You Pwned", *GIAC (GCIA) Gold Certification*, April 13th 2011
- [7] Mabel Vazquez-Briseno, Francisco I. Hirata*, Juan de Dios Sanchez-Lopez, Elitania Jimenez-Garcia, Christian Navarro-Cota and Juan Ivan Nieto-Hipolito, "Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World", *Autonomous University of Baja California,*CICESE, Mexico*
- [8] Pardis Pourghomi; Muhammad Qasim Saeed; Gheorghita Ghinea, "A Proposed NFC Payment Application", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 8, 2013
- [9] HUSSEIN AHMAD AL-OFEISHAT, MOHAMMAD A.A.AL RABABAH, "Near Field Communication(NFC)", *IJCSNS International Journal of Computer Science and Network Security*, VOL.12 No.2, February 2012
- [10] Raju Kumar, K. Gopalakrishna, K. Ramesha, "Intelligent Shopping Cart", *International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 4, July 2013*
- [11] Surapaneni Pujitha, B Veera Mallu, "SMS Based Mobile Banking", *International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue4- April 2013*
- [12] Nitika Rai, Anurag Ashok, Janhvi Chakraborty, Prajakta Arolker, Saumeel Gajera, "M-Wallet : An SMS based payment System", *International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 National Conference on Emerging Trends in Engineering & Technology (VNCET-30 Mar'12)*
- [13] Satish Kamble, Sachin Meshram, Rahul Thokal, Roshan Gakre, "Developing a Multitasking Shopping Trolley Based On RFID Technology", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-6, January 2014*
- [14] Giridhar D. Mandyam, Mike Milikich, "Mobile Web and Payments: Challenges and Ways Forward"
- [15] Mircea Moisoiu, Andrei Negrău, Robert Györödi, Cornelia Györödi, George Pecherle, "QR Code Scanning app for Mobile Devices", *IJCSMC, Vol. 3, Issue. 6, June 2014, pg.334 – 340*