THE INTERNATIONAL JOURNAL OF
SCIENCE & TECHNOLEDGE

Android Application for E-Card Transaction Using NFC

A. Saranya
B.Tech. Student, Department of Information Technology,
AVC College of Engineering, Tamil Nadu, India
S. Vishnupriya
B.Tech. Student, Department of Information Technology,
AVC College of Engineering, Tamil Nadu, India
S. Sathyapriya
B.Tech. Student, Department of Information Technology,
AVC College of Engineering, Tamil Nadu, India
B. Pradeepa
B.Tech. Student, Department of Information Technology,
AVC College of Engineering, Tamil Nadu, India
N. Rajganesh
Assistant Professor, Department of Information Technology,
AVC College of Engineering, Tamil Nadu, India

Abstract:
People continuously try to improve their quality of life with respect to modern trends. Payment method using physical credit card is bored and it is not comfortable to undertake at all time. Modern technology computerizes everything and reduces the usage cost with the maximum user satisfaction. For the sophisticated usage of credit card, we have to computerize it in our smartphone using Near Field Communication (NFC). The NFC is a new secures short-range wireless connectivity technology, can play an important role on this kind of issues. It uses secure element and hence it stores the data in a secure manner. NFC technology can store multiple virtual credit cards in secure element and prevent skimming, loss of credit card. In this paper, an android application which performs credit card transaction between NFC enabled devices [Mobile–credit card machine]. It enable users to securely store their multiple virtual credit card and allows to perform transaction with NFC enabled POS terminal.

Keywords: *virtual card, secure element, NFC*

1. Introduction

Android provides a service application framework that allows the users to build innovative applications and games. Android application is built as a combination of distinct components that can be invoked individually. For instance, an individual activity provides a single screen for a user interface and a service independently performs works in the background. Android provides an adaptive application framework that allows you to provide unique resources for different device configuration. We can also query the availability of device features at run time if any application features require specific hardware. Now-a-days, people uses credit card for many reasons such as internet purchase, emergency money transaction, rewards for purchases, keep tracking history of purchases, convenience etc. There may be some little bit problems arises while using credit card physically. Problems include damage of credit card, missing / loss of credit card, difficult to undertake multiple credit cards at a time. People always like to computerize everything. For convenient and sophisticated usage of credit card, we propose a concept for creation of android application which performs transaction between NFC enabled mobile phone and POS terminal. Here, we can store our credit card virtually in our mobile phone using NFC technology; transaction can be performed between mobile phone and POS terminal. NFC (Near Field Communication) is one of the radio technologies that enable communication between units (Devices) without direct physical touch. NFC is an open-platform technology, which is being standardized in NFC-Forum. It is based on and extends on RFID (Radio Frequency Identification). It operates on 13.56 MHZ frequency. Its communication range is up to 10cm.
NFC supports two communication modes

- Active: In this mode, the target and the initiator devices have power supplies and communication done by alternate signal transmission.
- Passive: In this mode, the initiator device generates radio signals and a target device gets powered by this electromagnetic field.

- Operation Modes:
- Read/write: In this mode, the NFC enabled phone can read or write data to any of the supported tag types in a standard NFC data format.
- Peer to peer: In this mode, two NFC enabled devices can exchange of data.
- Card Emulation: An NFC enabled phone acts as a reader when in contact with tags. In this mode, the phone act as a tag or contactless for existing readers.

2. Existing System and Their Related Works

Credit transfer using NFC technology plays a vital role in the current market. The concept of this application is money transfer from one mobile to another. This process uses two devices, one is NFC chip and another is Bluetooth, these two technologies have separate specific function. This application is based on client-client system. Once the sender opens an application, they have to need on the NFC touch and Bluetooth and wait for connection. Then they made network requests and send the money to receiver SIM card. Receiver receives the money and at last transaction is completed.

Kay et al. [1] proposed a method for financial transaction which initiates using mobile communication device. Here user needs to give the type of functionality, PIN and amount. Based on this nearest financial terminal with needed functionality is provided. In this method, NFC is attached to mobile device. Location of mobile device is determined using GPS.

Monterio et al. [2] proposed a paper for credit transfer among mobile phones it's used for credit transfer among mobile devices. Here uses a NDEF format specification for exchange information with two NFC presented device. Bluetooth is also needed. Emir Husni et al. [3] proposed a method to perform cashless payment for shopping payment system which allows customer to pay for shopping with their NFC enabled phone.

Frank Morgner et al. [4] discussed mobile smart card reader using NFC enabled smart phones in which smart phone is connected to computer device and used as a secure input and output device. For contactless smart cards, mobile phones are used as card reader, transaction can be authorized securely and perform authentication. By introducing reader mode on mobile phones user can block the attacker and management is also used for security purpose.

Gowri et al. [5] proposed a paper for conditional privacy preserving security protocol to perform the interaction between an android phone and computer with integrated NFC, more uses NFC device connected to the existing web service enabled infrastructure standard technology.

Keith L. Paulsen [6] proposed a paper for transmission of data between two NFC enable smart phones, one act as a smart card and other act as a POS terminal. It is performed by scanning QR codes in smart phones chip and pin method is used here.

Koby Levy et al. [7] discussed multiple NFC card application in multiple execution environment may be coupled to a NFC controller and each execution environment is communicating with remote reader via NFC. Timing synchronization for multiple NFC application during polling that is initially all NFC technologies are enables and granted, no poll to other technologies are re-enables, no response allowing other technologies slot.

Lishoy Francis et al. [8] proposed a paper for enhancing NFC transaction which allows an NFC enabled mobile phone to access and use over a contactless interface device or contact based interface. M Fisher [9] proposed a paper for transmission of data between mobile communication device and server for secure NFC payment transaction and it is performed by using mobile application running in mobile communication device.

M Fisher and Jackson [10] discussed scheduling and paying for a banking transaction using the NFC enabled mobile device automatically access available network, the NFC controller automatically upload the task and complete transaction. The personal details are securely store in NFC mobile device and it can't hack on any execution environment.

Michal Rolard et al. [11] proposed a paper for evaluate the feasibility of the software based relay attack in mobile payment system. Analysis of Goggle wallet, here use an android secure element is established between NFC enabled mobile phone and POS terminal.

Marc Pasquet [12] proposed a method to perform contactless payment securely with NFC mobile phones. It does not use physical connection. Omkar Ghag and Saket Hedger [13] proposed a method which allows customer to perform prepaid transaction between NFC enabled mobile communication device like mobile phones and POS terminal. But NFC provides wide entry point to several attacks like eavesdropping, data corruption.

Poonguzhali et al. [14] present detail study of storing of data and text/files on android mobile device in secure manner, store and also study about various threats on mobile device. Threats on mobile device based on loss or theft, unwanted data storage, other network problem. Encrypted data store only in kernel not external storage. Storing password as part of platform, namely Android Key store, support complete encryption of device.

Roelverdult and Francois kooman [15] proposed a method for practical attacks on NFC enabled cell phones show a communication between phone and NFC tag. S. Goldth Waite and William [16] proposed a paper for contactless smart card reader/writer which enable mobile communication device to access wireless network with both SIM card slot and smart card slot. It transmits data between mobile device and POS terminal.

Subhasini Dwivedi et al. [17] proposed a method for secured green payments using NFC device, to perform the secure transaction between NFC based android mobile phone and server site using the IP address of vendor site. For contact less payment, HCE (Host Card Emulation) is the basis, virtual but exact presentation of smart card in software using the vendor Wi-Fi, IP address the transaction can be done securely.

3. Work Flow Diagram

Customer applies credit card to the bank then the bank stores the customer details in database and provide the E-card link to customer through Mail or SMS. User downloads the E-Card and store in our application and it verifies the user details from database for authentication. User performs transaction between NFC enabled mobile device and POS terminal.

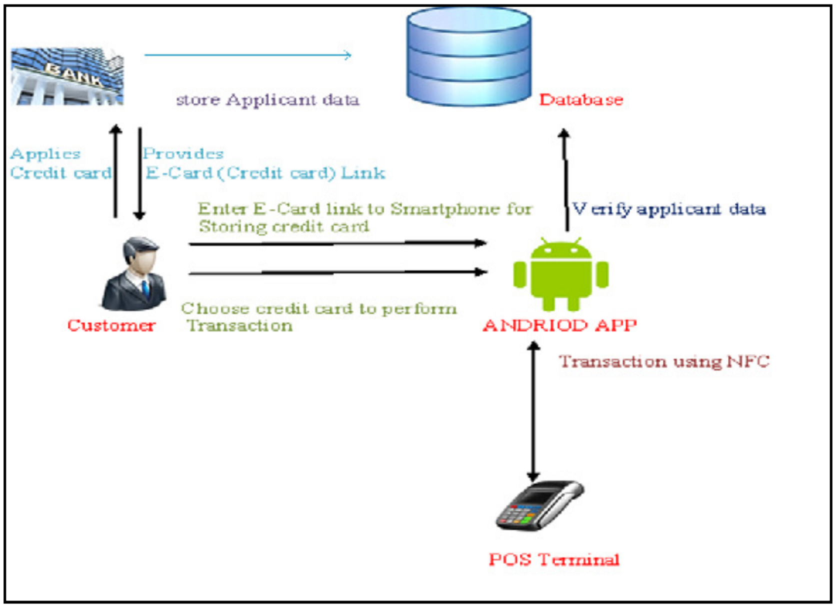
BANK
store Applicant data
Database
Applies Credit card
Provides E-Card (Credit card) Link
Enter E-Card link to Smartphone for Storing credit card
Verify applicant data
Customer
Choose credit card to perform Transaction
ANDRIOD APP
Transaction using NFC
POS Terminal

Figure 1: Workflow diagram for E-Card transaction

4. Proposed Approach

Now-a-days computerizing everything as per the technology is the emerging trend. It is usual to use credit card by swiping but it is not sophisticated to undertake it physically or to handle multiple credit card at every time. Smartphone is a mobile phone that performs many of the functions of compiler, typically having a touch screen interface, Internet access and an operating system. Smartphone technology is so successful and most of the people have double imagining a day without them. Hence if we store the credit card into the smartphone as the virtual card, it is sophisticated to use credit card.

Our approach represented in Figure.1 is to perform transaction between NFC enabled mobile phone and POS terminal. It enables the users to perform transaction without directly holding the credit card. For that user needs to open the application and perform login, then they are allowed to add a new credit card (or) perform transaction using already stored credit card. There are two options are available. First one is Add card; it is used to store multiple credit card in NFC enabled mobile device. Second one is choose card, it is used to choose the already stored credit for transaction and further process is going on as usual.

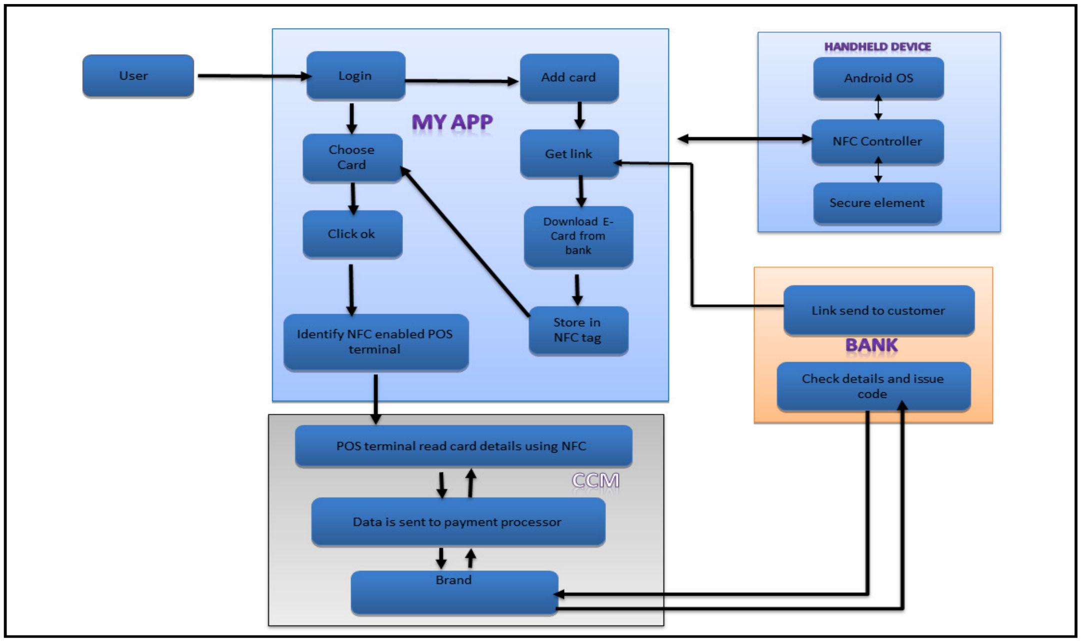
User
Login
Add card
MY APP
Choose Card
Get link
Click ok
Download E-Card from bank
Identify NFC enabled POS terminal
Store in NFC tag
HANDHELD DEVICE
Android OS
NFC Controller
Secure element
Link send to customer
BANK
Check details and issue code
POS terminal read card details using NFC
CCM
Data is sent to payment processor
Brand

Figure 2: E-Card Transaction diagram

4.1. Module Description

As per the above Figure.1, we frame the system with the following modules to do the NFC enabled transaction process. Each module is expressed and a detailed work plan is also given in the bellow subsections.

4.1.1. My app

This module is the first stage to initialize transaction. The first step is login. User has to login with their passwords. Two options are available for the user.

- Add card
- Choose card

If he/she chooses add card, then the following actions are performed. Give the link which is sent from bank. Then it downloads the virtual card and stores it in NFC chip in the device.

If he/she chooses choose card, then the following actions are performed user has to Select card for transaction. Then Click ok. It automatically Identify NFC enabled POS terminal.

4.1.2. Credit Card Machine (CCM)

As per the input from the MYAPP module, POS terminal read card details using NFC. Data from the virtual card is received by the payment processor. Payment processor sends the details to the payment brand. Brand forwards it to the issuing bank.

4.1.3. Corporate Section Process

Bank send virtual card link i.e., a link where the virtual credit card for the particular user in available] to the credit card applied customer. Bank verifies the credit card details from the brand and generates authorization number, then routes the number to card brand and agree to pay. Finally, brand forwards the number to the payment processor. This is as per the usage of physical credit card.

4.1.4. NFC enabled Handheld Device

A user supporting device with the enabling of the application termed MYAPP for the transaction processing. These are equipped with the built in NFC and are configured to co-operate with the proposed system as per the architecture diagram illustrated in the figure.1.

5. Secure Element

While not all NFC applications require security, those that involve financial transactions or certain mobile marketing applications (e.g., coupons and loyalty) require a “secure element” within the phone to securely store applications and/or credentials (e.g., financial account numbers) and provide for secure execution of applications. The secure element (secure memory and execution environment) is a dynamic environment in which application code and application data can be securely stored and administered and in which secure execution of applications occur. The element resides in highly secure crypto chips (usually a smart card chip). The element provides delimited memory for each application and other functions that can encrypt, decrypt, and sign the data packet.

The secure element could be implemented either by a separate secure smart card chip (currently implemented in most of the NFC-enabled mobile phone pilots), in the SIM/UICC (which is used by GSM mobile phone operators to authenticate subscribers on their networks and maintain personalized subscriber information and applications), or in an SD card that can be inserted in the mobile phone. The secure element implementation approach will be selected by the mobile operator implementing the service and/or by the payment service provider (for SD card implementations).

6. Expected Results

The following are the expected results in our project. For that user has to download the application and to open it. Two options are available for the user as shown in fig. a. When they click the New user button. Then the layout in Fig. b will display to the user. User needs to fill the details and to click the request for password button. A One Time Password (OTP) will sent to the mobile number of user when the details are verified. Then user has to enter the OTP in the Fig. c and click set password button. Now the user is allowed to set password as shown in Fig.d.

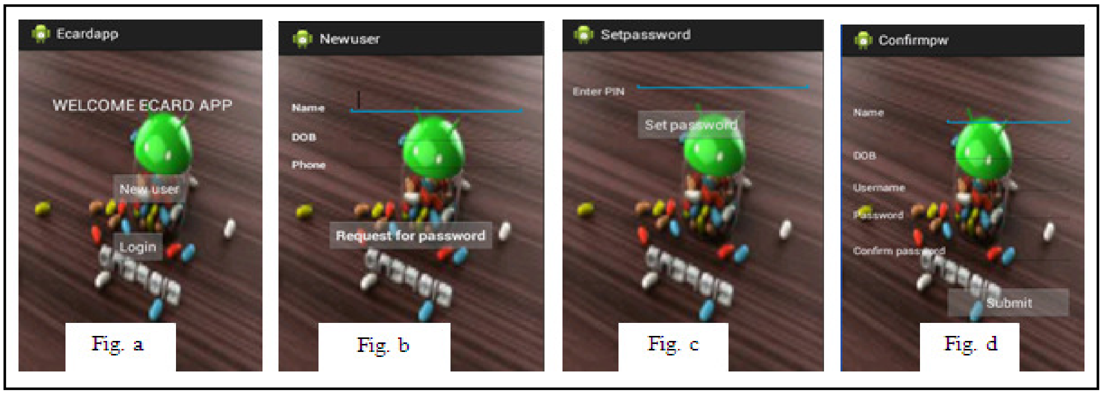

Fig. a Fig. b Fig. c Fig. d

Figure 3

Once the User completes the verification process and sets the password, then they are direct to first layout as shown in Fig.a. Now they need to click Login button.The layout shown in Fig. e will display to the user. User has to login with their username and password. Then layout in Fig. f shown to the user.If they click the add card button then it display the layout as shown in Fig. g. They need to type the link which was sent from bank and to click the download button for download the virtual credit card.

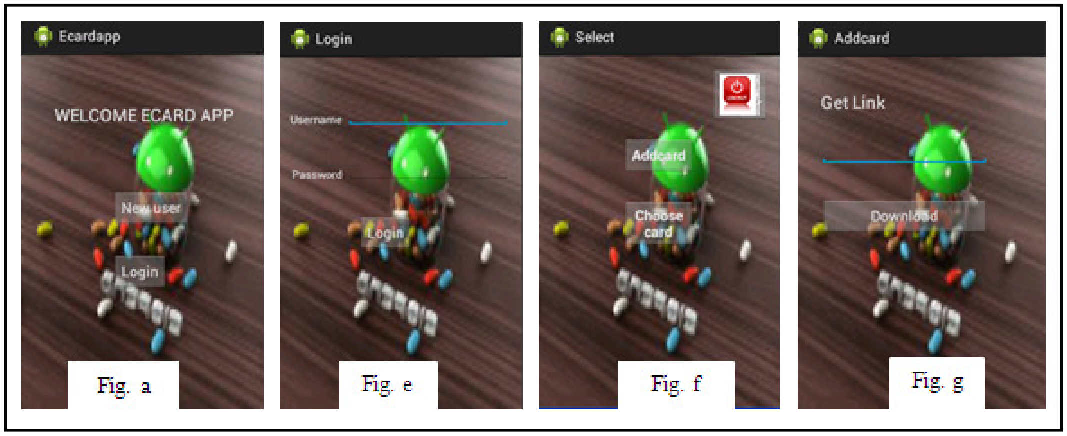

Figure 4

Fig. h display show after successful downloading of virtual credit card. If the user chooses Choose card button from the layout shown in Fig. f then they will direct to Fig. i where the downloading credit card are stored. They have to choose the credit card and to click OK button.In the next layout shown in Fig.j they have to enter the amount for transaction and to click OK button. Then the layout in Fig.k will display and it indicates the completion of transaction.After the completion of transaction, user needs to click the Finish button and then they will direct to layout in Fig. f.From there they are allowed to log out from the application.

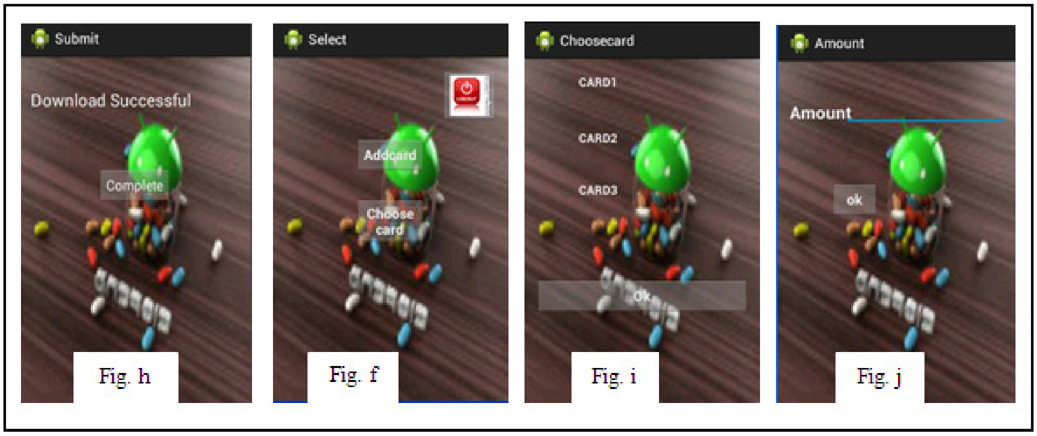

Figure 5

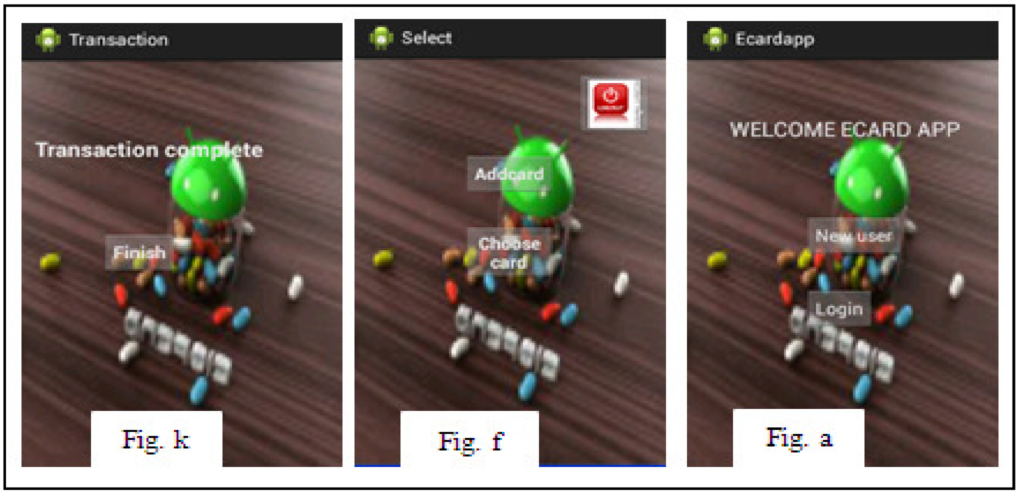

Figure 6

7. Conclusion

With suitable to modern computing world and developing (increase) technology people tries to computerize everything payment method using physical credit card is not comfortable since needs swiping and physical undertaking Hence (in this paper) we proposed a method for creating android application which stores credit card virtually and perform transaction with NFC enabled mobile phone and POS terminal. it uses NFC, which is short range radio technology that enable communication between devices without direct touch Hence this method reduces manual undertaking of credit card and allows user to store more one credit card in our application. It is easy of use and convenient for card holder. It also reduces the workload of bank (reduce generating plastic credit card and issuing to customer).

8. References

i. Christopher Eric Kay and Palo Alto, “System and Method for Conducting a transaction at a financial transaction terminal using a mobile device” United States Patent publication 8972297, No.3, 2015.

ii. D. Monteiro, Joel J. P. C. Rodrigues and Jaime Lloret, “A Secure NFC Application for Credit Transfer Among Mobile Phones”, International Conference on Computer, Information and Telecommunication Systems (CITS), 2012.

iii. EmirHusni and Sugeng Purwantoro, “Shopping Application System With Near Field Communication”, International Conference on System Engineering and Technology (ICSET), 2012 .

iv. FrankMorgner, Dominik Oepen, Wolf Müller and Jens-Peter Redlich, “Mobile smart card reader using NFC-enabled smartphones”, ICST Institute for Computer Science, Social Informatics and Telecommunications Engineering,2013.

v. Gowri and F.W. Jesudas, “conditional privacy preserving security protocol for NFC application”, International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 2, 2014, pg.248 – 254.

vi. Keith L. Paulsen, “method for protecting cardholder data in a mobile device that performs secure payment transactions and which enables the mobile device to function as a secure payment terminal” United States Patent Application Publication Pub. No.: US 2014/0195429, issue 10, 2014.

vii. Koby Levy, Bat-Yam and Ran Katz, “Multiple NFC card applications in multiple execution environment” Publication US 2012/0178366 A1issue 10, 2015.

viii. Lishoy Francis, Gerhard Hancke, Keith Mayes and Konstantinos Markantonakis, “A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions”, Conference on Telecommunications (AICT), 2010.

ix. M.Fisher, “Conducting an online payment transaction on NFC enabled mobile communication devices”, United States Patent Application Publication, publication number US8352323 B2, 2013.

x. M Fisher and Jackson, “Scheduling and paying for banking transaction using NFC enabled mobile communication device” United States Patent Application Publication issue 29, 2012 .

xi. Michael Roland, Josef Langer and Josef Scharinger, “Applying Relay Attacks to Google Wallet”, 5th International Workshop on 5,2013 .

xii. Marc Pasquet, Joan Reynaud and Christophe Rosenberger, “Secure Payment With NFC Mobile Phones In The Smart Touch Project”, International symposium on collaborative technologies and system, 2008.

xiii. Omkar Ghag and SaketHegde, “A Comprehensive Study of Google Wallet as an NFC Application”, International Journal of Computer Applications (0975 – 8887) Volume 58– No.16, 2012.

xiv. Poonguzhali P, Prajyot Dhanokar, M.K. Chaithanya, and Mahesh U. Patil, “Secure Storage of Data on Android Based Devices” issue 15, 2014.

xv. Roel Verdult and Francois Kooman, “Practical Attacks on NFC Enabled Cell Phones” International Workshop on Near Field Communication, International Workshop on 2011, pg. 77-82.

xvi. Scott Goldthwaite and William Graylin, “mobile device equipped with a contactless smart card” United States Patent Publication, 20040127256 A1, issue 1, 2004.

xvii. Subashini Dwivedi, Shraddha Panbude and Rama Rao, “Secured Green Payments using NFC Device” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 issue 11, 2014.