Near Field Communication

Conference Paper · January 2015

CITATION
1

READS
6,688

1 author:

Devharsh Trivedi
Nirma University
12 PUBLICATIONS **2** CITATIONS

SEE PROFILE

Near Field Communication

Submitted By

Devharsh Trivedi

14MCEI25

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

April 2015

Near Field Communication

Seminar

Submitted in partial fulfillment of the requirements

for the degree of

Master of Technology in Computer Science and Engineering

Submitted By

Devharsh Trivedi

(14MCEI25)

Guided By

Dr Sharada Valiveti

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

April 2015

Certificate

This is to certify that the major project entitled **"Near Field Communication"** submitted by **Devharsh Trivedi (Roll No: 14MCEI25)**, towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering of Nirma University, Ahmedabad, is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr. Sharada Valiveti
Guide & Associate Professor,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
Professor and Head,
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad

Acknowledgements

I would like to thank Dr Sharada Valiveti for guiding me to explore NFC to produce some working application which I have done at some extent. I would also like to thank Prof Vipul Chudasama for letting me use Akash Tablet provided by IIT Bombay and Mr Paras Jain for allocating RFID tags when I needed. At last I would like to thank my classmate Ms. Nidhi Trivedi (14MCEI27) for providing me her NFC enabled Samsung android smart phone to test the application.

- Devharsh Trivedi

14MCEI25

Abstract

Near Field Communication (NFC) is a special category or a case of RFID (Radio Frequency Identification) Technology. The modern age NFC was introduced in 2004 and since 2014 after 10 years of invention it has picked popularity mainly because of cheap hardware, extensive use of smart phones and boom in Internet of Things technology. I have explained in this report about NFC and the implementation that I have done and at last some future work that can be done to extend the use of my application.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 NFC

Near Field Communication (NFC) as its name suggests is a shorter range subset of RFID (Radio Frequency Identification) technology. It has gained popularity as the rising development in todays technical world. What this wireless communication technology offers is a low bandwidth with high frequency allowing data transfer in range of centimeters.

13.56 MHz is the frequency where NFC operates. It can provide speed up to 424 kbps. NFC tags communication and data exchanges are based on standards like ISO 14443 A, MIFARE and FeliCa. It provides high comfort level and ease of use as there are no further configuration steps required to initiate a session to share data. [1]

Reading from NFC tags is very easy as you just need to bring NFC tag closer to NFC reader and it will start reading from it without providing any connection details. Concept of inductive coupling is used in this architecture. It is also compatible with Bluetooth and Wi-Fi.

1.2 RFID

RFID emerged somewhere around in 1980s. Charles Walton invented an object using RFID in 1983. It basically enables a one-way wireless communication that is typically between two devices, i.e. a powerless RFID tag and a powered RFID reader. RFID reader

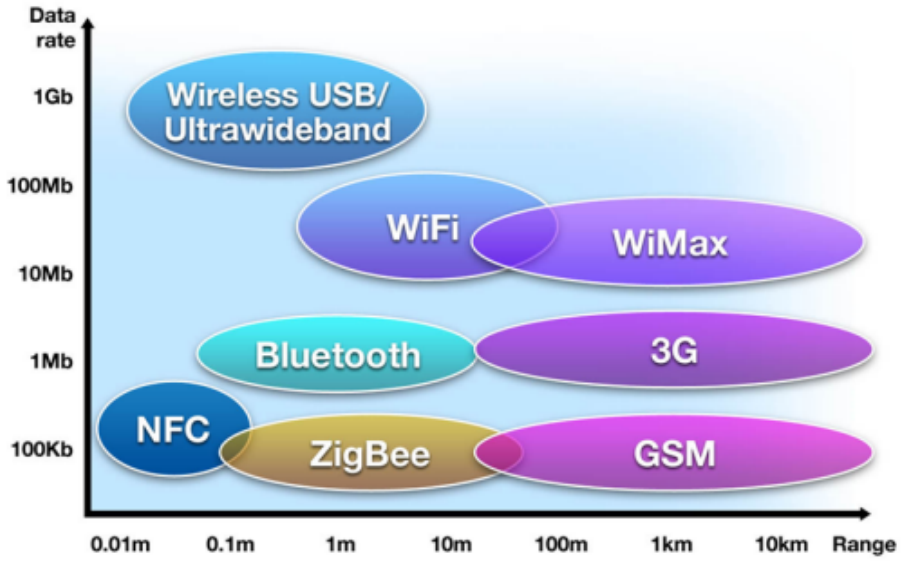

Figure 1.1: Comparisons of various wireless standards

which is enabled with battery supply is responsible for generating long-distance Radio frequency waves using which RFID tag will get induced and generates its own electricity based on the strength of electromagnetic field received. [1]

RFID can be scanned from a distance of 100 meters without being in line of sight and thats why it is being used everywhere for asset tracking such as in a warehouse or airport and wild animal movement tracker or livestock identification. As shown in the figure RFID is categorized in various frequency ranges from 120 kHz to 10 GHz spectrum.

NFC works at High Frequency RFID band that is 13.56 MHz. The reason why this spectrum is accepted globally is because it is unlicensed and hence anyone can use it freely for transmitting and intercepting data.

1.3 NFC vs. RFID

RFID uniquely identifies using radio waves. NFC is a subset of RFID technology. NFC is a branch of High-Frequency RFID. Both RFID and NFC operate on 13.56 MHz frequency. NFC is designed to be a secure form of data exchange, and an NFC device is capable of being both an NFC reader and an NFC tag. This unique feature allows NFC devices to communicate peer-to-peer.

RFID Frequency Band	Scan Distance
120-150 kHz (Low Frequency, LF)	Up to 10 cm
13.56 MHz (High Frequency, HF)	Up to 1 m
433 MHz (Ultra High Frequency, UHF)	1-100 m
865-868 MHz & 902-928 MHz (Ultralight High Frequency, UHF)	1-2 m
2450-5800 MHz (Microwave)	1-2 m
3.1-10 GHz (Microwave)	Up to 200 m

Figure 1.2: Classification of RFID Frequency Band

	NFC	RFID	IRDA	BLUETOOTH
Set-up time	<0.1ms	<0.1ms	~0.5s	~6s
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy,Intuitive ,fast	Item centric Easy	Data Centric Easy	Data Centric medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access,share,initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchanga,headset
Consumer experience	Touch,wave,simply connect	Get information	Easy	Configuration needed

Figure 1.3: Comparison of NFC, RFID, Infrared and Bluetooth

1.4 NFC Forum

It was launched in 2004 by leading companies in the field of semiconductors, communication and electronics as a non-profit organization. The forum educates market about NFC and promotes its usage. They build specifications, standards and maintain interoperability between devices and services. They have around 200 global partner companies who are working towards modular NFC device architecture and much more.

The NFC Forum's Sponsor members are: Intel, NXP Semiconductors, Qualcomm, Samsung, MasterCard Worldwide, NEC, Sony Corporation, Broadcom Corporation, Google, Inc., STMicroelectronics, and Visa Inc.

Figure 1.4: Sponsors of NFC Forum

Chapter 2

Literature Survey

2.1 Problem Definition

Near Field Communications (NFC) is a short-range wireless technology that allows mobile devices to actively interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users. RFID is a powerful enabling technology that is being applied in an astonishing range of applications and uses, from supply chain management and product inventory control to identity authentication and access control. As RFID technologies become widely deployed, the possibility of unwanted identification, tracking and surveillance may increase, as may the likelihood of data interception, cloning and misuse.

2.2 Objectives

NFC has become an attractive research area for many academics due to its exploding growth and its promising applications and related services. Due to its nature, large proportion of the NFC research can be represented as a design science research which aims to propose an innovative design artifact and has a problem relevance and rigorous nature. As we shall present, for the last few years, there has been a considerable amount of increase in the number of research papers and activities concerning NFC. However, understanding the current status of NFC research area is necessary to maintain the advancement of knowledge in NFC.

2.3 List of Research Papers Referred

No.	Paper	Journal	Year	Author	Findings height
1	Mobile Near Field Communications (NFC) Tap n Go Keep it Secure and Private	Information and Privacy Commissioner, Ontario, Canada	2011	CanadaAnn Cavoukian, Ph.D.	Applying Privacy by Design to Mitigate Risks
2	White Paper Near Field Communication	NOKIA	2007		Key factors for the success of NFC
3	A design research exploration of Near Field Communication technology	University of Gothenburg	2012	Magnus Bergqvist Ali Issa Kristoffer Morsing	Building and evaluating an NFC-ticket prototype extending an existing system
4	Near Field Communication (NFC)	IJCSNS International Journal of Computer Science and Network Security	2012	HUSSEIN AHMAD AL-OFEISHAT, MOHAMMAD A.A.AL RABABAH	NFC Modes of Operation, NFC Usage Models
5	Near Field Communication	International Journal of Advanced Research in Computer Science and Software Engineering	2014	Chetna Bajaj	Protective Measures For Securing Near Field Communication
6	Strengths and Weaknesses of Near Field Communication (NFC) Technology	Global Journal of Computer Science and Technology	2011	Mohamed Mostafa Abd Allah	NFC Applications Threats

No.	Paper	Journal	Year	Author	Findings height
7	Contactless Communication through Near Field Communication	International Journal of Advanced Research in Computer Science and Software Engineering	2012	K.Preethi, Anjali Sinha, Nandini	Contactless Communication API
8	Touch and Run with Near Field Communication (NFC)	Computer Science Department Stanford University	2010	Ben Dodson Hristo Bojinov Monica S. Lam	P2P APPLICATIONS WITH JUNCTION
9	Near Field Communication: an assessment for future payment systems	Springer	2008	Jan Ondrus, Yves Pigneur	NFC As A Payment System
10	NFC Research Framework: A Literature Review And Future Research Directions	14th IBIMA Conference	2010	Bra ZDENZC, Mehmet AYDIN, Vedat COKUN, Kerem OK	Results and Analysis of NFC Framework
11	Conditional Privacy Preserving Security Protocol for NFC Applications	IEEE	2013	Hasoo Eun, Hoonjung Lee, and Heekuck Oh	Proposed key agreement and confirmation protocol using self-updatable pseudonym based method
12	Practical Secret Key Agreement for Full-Duplex Near Field Communications	ASIA CCS14	2014	Rong Jin, Xianru Du, Zi Deng, Kai Zeng, Jing Xu	Proposed key agreement method working on two active NFC devices

Table 2.1: Literature Survey

Chapter 3

NFC Operating Characteristics

As discussed earlier being a wireless communication technology it operates on short-range radio frequency. It is capable to form a peer-to-peer network for data communication. 13.56 MHz band is unlicensed in all the countries.

The technology works when NFC enabled devices brought within close proximity i.e. a small distance around 4 to 20 cm. It can provide transfer data rate of up to 424 Kbps. It also allows data transfer in the chunks of 106 Kbps and 212 Kbps. It can provide a bandwidth of approximately 2 MHz.[2]

Data Rate (Kbps)	Active Device	Passive Device
106	Modified Miller, 100%, ASK	Manchester, 10%, ASK
212	Manchester, 10%, ASK	Manchester, 10%, ASK
424	Manchester, 10%, ASK	Manchester, 10%, ASK

Figure 3.1: NFC RF Signal Coding and Data rates

Chapter 4

NFC Standards

ISO (18092), ECMA (340) and ETSI are popular NFC standards. It supports smart cards like Mifare and Felica. NFC has two standards: NFCIP-1 and NFCIP-2. NFCIP-1 is defined in the ECMA-340 standard. This mode is intended for peer-to-peer data communication between devices which is divided into two variants: active and passive mode. NFCIP-2 is specified in ECMA-352 which defines how to automatically select the correct operation mode when starting communications.[3]

4.1 Modes of Operations

4.1.1 Active Mode

NFC device operating in active mode generates its own carrier frequency, resulting its own RF field for transmission purpose. It is equipped with a power supply for operation. Active NFC device act as an initiator in communication. Two active NFC devices can alternatively generate RF field to form a two-way communication link to transfer data. NFC device operating in passive mode would not be able to generate its own carrier frequency.

4.1.2 Passive Mode

Passive device acts as a target. Initiator device produces RF field for communication and Target device use inductive coupling for responding them back. Target device modulates to initiator's RF field, for replying back to initiator. Target device uses power from ini-

tiator's generated RF electromagnetic field and saves energy. Resultant, Passive device can be provided a small battery for its operation to restrict energy sources consumption.

4.2 Modes of Communications

4.2.1 Peer-to-peer

Peer-to-Peer mode is defined for device to device link-level communication. This mode is not supported by the Contactless Communication API. Peer-to-peer mode is a simple or classic mode of NFC operation. It allows data transfer at a rate of up to 424Kbps. It works on NFCIP-1 protocol, whose protocol's detail and electromagnetic properties are standardized in ISO 18092 and ECMA 320/340.

4.2.2 Reader-writer

Read/Write mode allows applications for the transmission of NFC Forum-defined messages. This mode is not secure and supported by the Contactless Communication API. NFC device can also operate as Reader/Writer for tags and smart cards. In Reader/Writer mode, NFC active device act as an initiator and passive tag act as target. This mode allows data transfer rate of 106 Kbps.

4.2.3 Card emulation

NFC Card Emulation mode allows the NFC-handset behave as a standard smartcard. This mode is secure and is supported by the Contactless Communication API. In emulation mode, NFC device emulates ISO 14443 smart card chip. These smart chips are integrated in mobile devices and get connected to NFC module for communication to occur.

Chapter 5

NFC Applications

Now-a-days most of the high range smart phone provides NFC chips. This has created an unprecedented interest for application developers to take advantage of it and make it useful in many domains. Some of the most popular ones are ecommerce and security. Peer to peer transfer has also found its usages. Some of the applications are as listed below:

- Mobile Payments (m-payments)
- Credit Cards Replacement
- Advertising
- Educational purpose
- Electronic Ticketing
- Visiting Cards
- Parking Lots
- Key less Entry
- Device Pairing

Figure 5.1: Bihar Smartcards

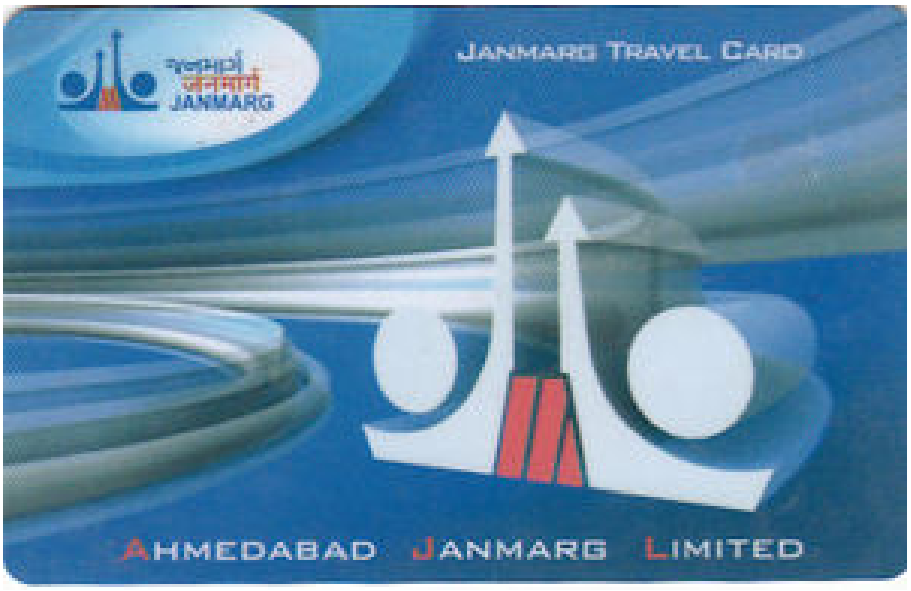

Figure 5.2: Janmarg Travel Card

5.1 eShakti cards in Bihar

5.2 Janmarg (BRTS) cards in Ahmedabad

5.3 Security Applications

In cases where authentication is needed for physical access such as starting a vehicle or to enter a room or turn on a machine it can be useful.

5.4 Google Wallet

1. Unlock / Wake up phone. No need to start application.
2. Hold the back of your phone against the payment terminal.
3. If asked for a PIN on the terminal or your phone use Wallet PIN.
4. The terminal might flash or beep to show your payment was made.

Chapter 6

Implementation

As a part of this seminar I made an android application using Xamarin framework which converts C code to native APIs. This application can read and write from NFC tags. Though there are many applications available on play store to read and write data but they are not open source. I made another lightweight apk file which simply checks whether the phone has NFC hardware or not which was made in eclipse and that is coded in Java.

The idea was to read and write tag and then process that read data to perform some operation like opening the door, turning on any appliance or just manipulating data with web service. I have completed the first part which was to read and write data but havent completed second part that is to perform some action based on that data.

I have also made use of android apps available on play store to read and write data to NFC tags which supports variety of tags from different manufacturers and can write variety of data to perform many different applications. Following section represents the screenshots of those applications.

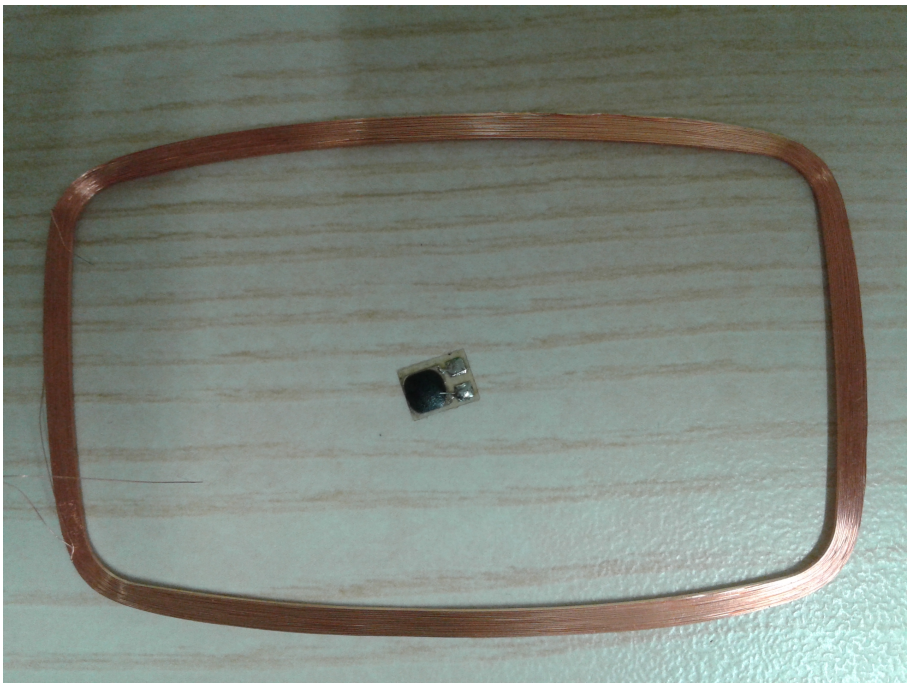

Figure 6.1: Inside the tag

Figure 6.2: RFID tags used by me

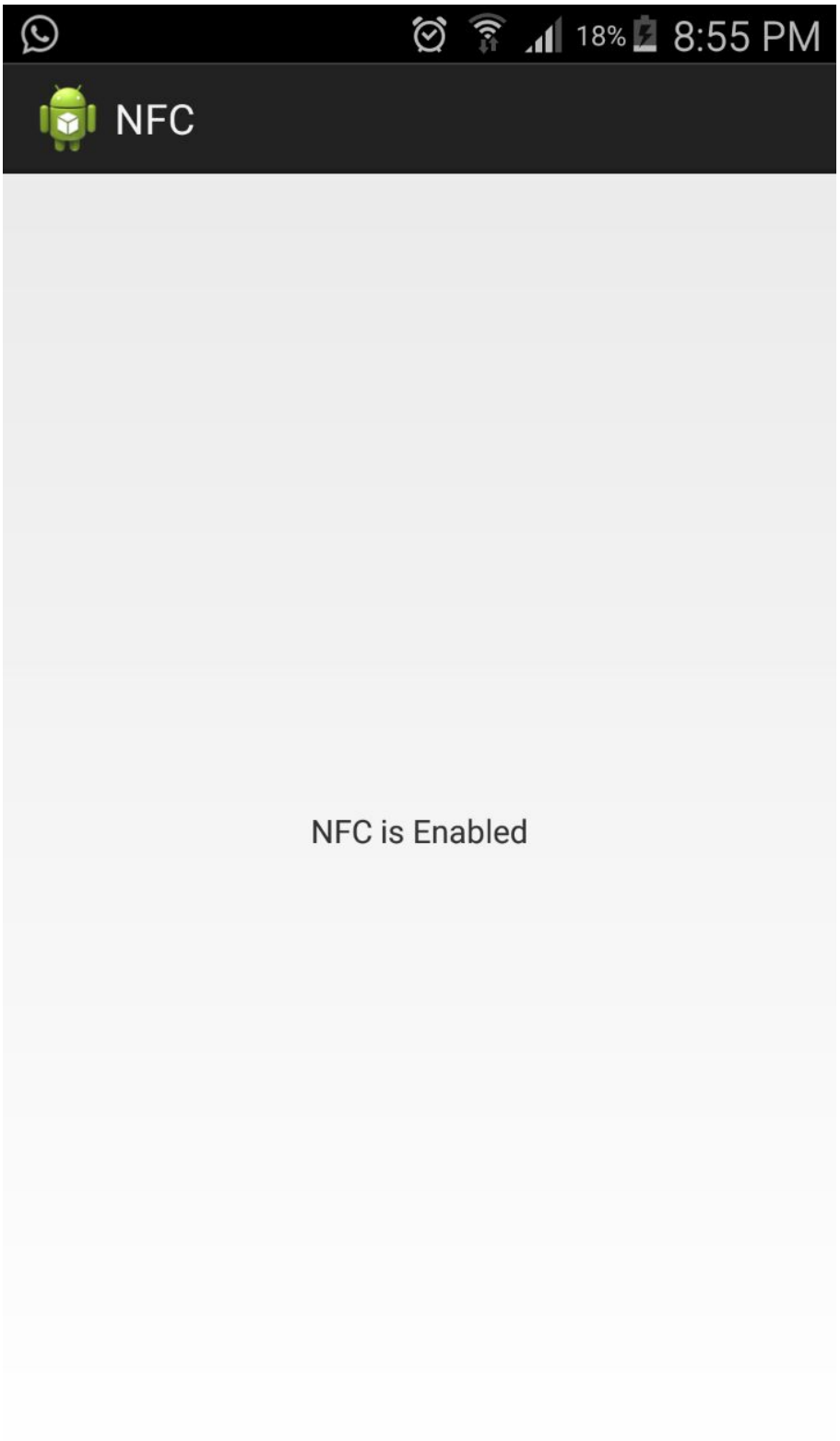

Figure 6.3: Application to check whether NFC is supported

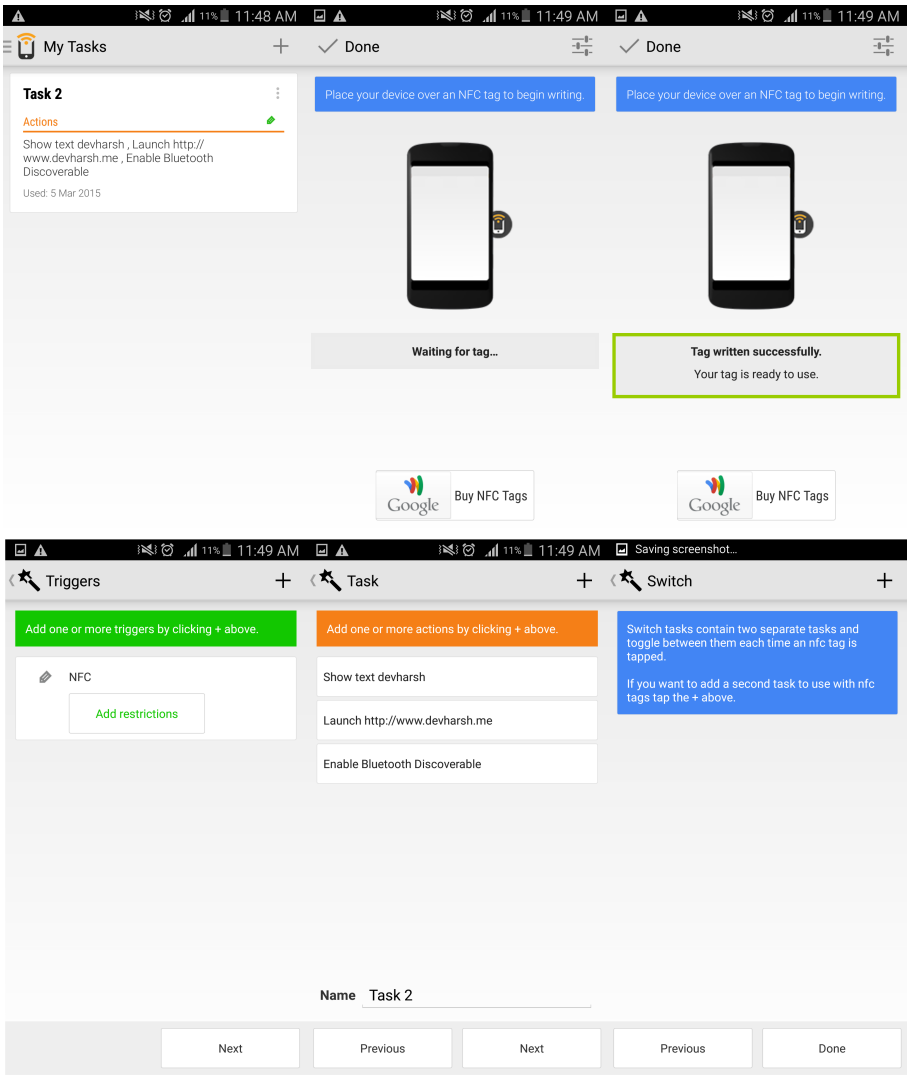

Figure 6.4: Triggers application is used here to write three actions: 1) Display text devharsh 2) Enable Bluetooth 3) Open website www.devharsh.me

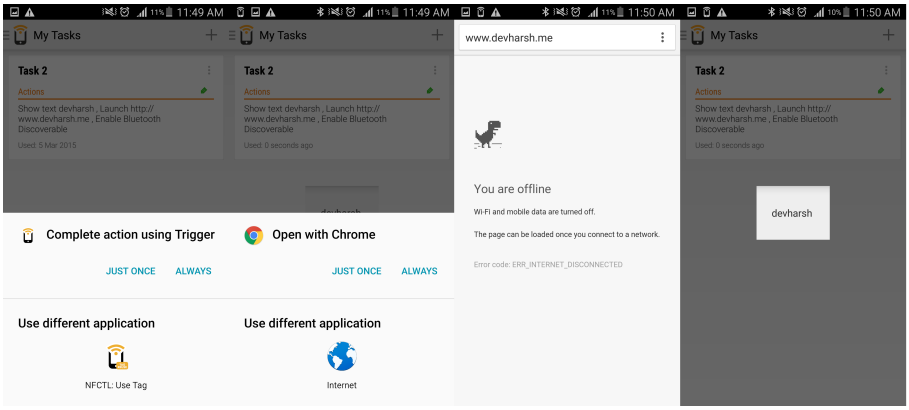

Figure 6.5: Triggers application to launch action by reading tag

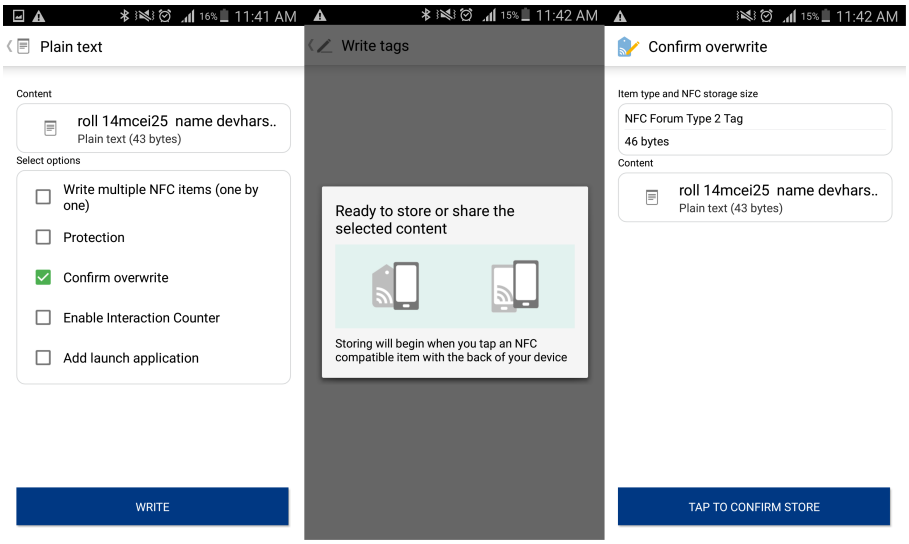

Figure 6.6: TagWriter by NXP is used for writing text data

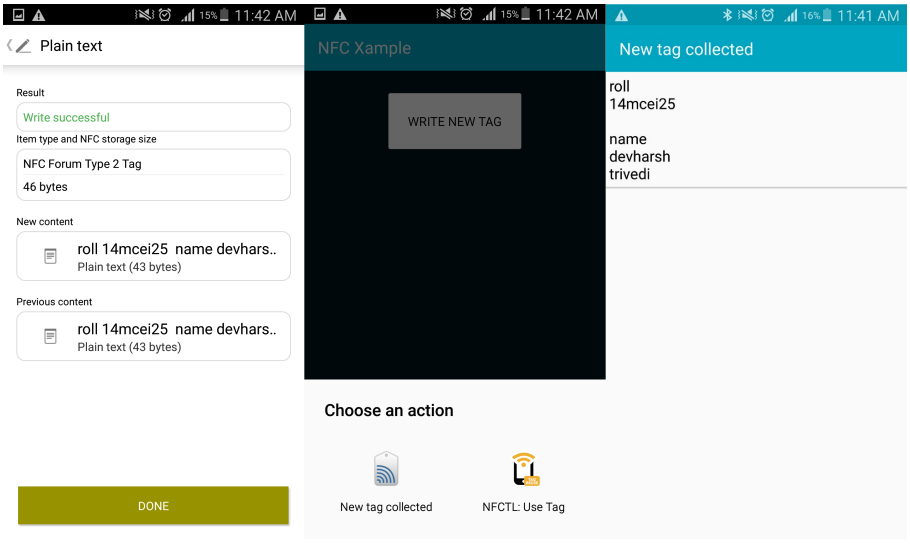

Figure 6.7: My application that reads data

Chapter 7

Security threats and solutions

7.1 Eavesdropping

It is a wireless communication interface so eavesdropping is a big issue. A secure channel must be established. Diffie-Hellman can be used for key exchange to generate a symmetric key which further can be used with AES or 3DES encryption. [4]

7.2 Data corruption

Instead of eavesdropping an attacker may disturb the transmitted data. This can be detected by checking RF field as the power needed for corrupting data is higher than detected by NFC.

7.3 Data modification

It is different from data corruption as in this case attacker wants receiver to get the malicious data. It can be prevented by regularly checking RF field by active sending device or a secure channel should be used as described in 6.1.

7.4 Data insertion

Attacker sends his own data along with the data transmitted by both parties. The best solution is to minimize the delay. The attacker cannot be faster than the active device

in this case. A secure channel can also be used as remedy.

7.5 Man-in-the-middle attack

Attacker can easily implement this attack by generating his own electromagnetic field to induce the receiver. Practically this attack is not possible but it is good habit by sender to listen to RF field before sending data to check for any disturbance present in the channel.

Chapter 8

Conclusions

NFC is a short range version of RFID which makes it immune to few attacks by default. It is highly interoperable with existing technologies and cheaper hardware has made its use more popular. Many applications are being used for payment and physical access. NFC does not provide protection against threats itself so encryption should always be used.

Chapter 9

List of useful websites

i. http://www.nearfieldcommunication.org/history-nfc.html

ii. http://www.nfcnearfieldcommunication.org/history.html

iii. http://nfc-forum.org/what-is-nfc

iv. http://www.nxp.com/products/identification$_a nd_s ecurity/smart_c ard_i cs/mifare_s mart_c ard_i cs$

$v.http : //www.netcard.com.au/products/what - is - mifare$

$vi.https : //support.google.com/wallet/answer/2466137?hl = en$

$vii.http : //www.google.co.in/wallet/faq.html$

$viii.http : //blog.atlasrfidstore.com/rfid - vs - nfc$

$ix.http : //rapidnfc.com/blog/72/the_d iff erence_b etween_n fc_a nd_r fid_e xplained$

$x.http : //www.nfc - phones.org/nfc - enabled - phones - in - india$

References

[1] V. SHARMA, P. GUSAIN, and P. KUMAR, "Near field communication," 2013.

[2] R. Nagashree, V. Rao, and N. Aswini, "Near field communication," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 4, no. 2, p. 20, 2014.

[3] K. Curran, A. Millar, and C. Mc Garvey, "Near field communication," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 2, no. 3, pp. 371–382, 2012.

[4] E. Haselsteiner and K. Breitfu, "Security in near field communication (nfc)," pp. 12–14, 2006.