Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 5; April-June, 2015 pp. 429-435
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Adoption of Near Field Communication (NFC) Technology and Possible Security Challenges

Satyakam Rahul

Kebbi State University of Science &Technology, Nigeria
E-mail: satyakam_rahul@yahoo.co.in

Abstract—*Near Field Communication (NFC) Technology is a short wave radio communication technology for allowing devices to communicate with each other. NFC working is based on RFID technology, RFID meaning Radio Frequency identification is a communication technology that is used for tracking and identification of item by a reader through the information stored on a tag.*

Currently the application of NFC is mainly focused on mobile contactless payment, any devices capable of making payment using radio-frequency identification technology is using contactless payment technology i.e. "wave to pay "credit cards, transit system passes or ticketing, and secure building entry. Passport or other identity means mayuse embedded NFC tags for additional security .industrial applications include inventory management and tracking. NFC is said to be inherently secure since two physical devices must be brought together to such a short range

Other application of NFC is peer- to-peer communication that will enable NFC enabled devices to exchange contact information, trading characters, items, or other bit related game.

The objective of this paper is to describe some of the applications in detail and give examples of how they have been implemented in other technologically advanced countries, and offer suggestions on how NFC can be used to enhance services, promote commercial industries or companies such as Banks, Hotels, supermarket and SMEs companies, also promoting the economic growth of a country.

How adoption of NFC technology can reduce the rapidly increasing cyber crime ranging from hacking, interception threat, eavesdropping, cyber theft, identity theft, credit card theft, and ATM Fraud etc.

Keyword: *NFC, Cyber Crime, Contactless Payment, RFID*

1. INTRODUCTION

Near Field Communication is a wireless technology that has a range of only a few inches. It is based on the magnetic field induction between readers and tags in radio frequency identification (RFID) system. With an operating frequency of 13.56 MHz NFC supports data transfer up to 424 Kbits/second using three different modes of operation: card emulation, reader/writer, and peer- to-peer, which enables the exchange of data between devices over about a 10 centimetre (around 4 inches) distance. Two major specifications exist for NFC technology: ISO/IEC 14443 and ISO/IEC 18000-3. The first defines the ID cards used to store information, such as that found in NFC tags. The latter specifies the RFID communication used by NFC devices.

NFC allow two device to communicate, using complex protocols, however the device receiving data switch to passive mode which prevent interception attacks

NFC working is based on RFID technology, RFID meaning Radio Frequency identification is a communication technology that used for tracking and identification of item by a reader through the information stored on a tag. One of the main goals of NFC technology has been to make the benefits of short-range contactless communications available to consumers globally.

NFC offers the best of the both worlds. Smartphone's equipped with NFC enable customers or users to store multiple credit cards and other payment methods all in one device that the customer is likely to carry everywhere with them like a wallet, your Smartphone will do all for you by touching of passing by your Smartphone through the NFC payment terminals devices.

2. EVOLUTION OF NFC

NFC traces its origin back to RFID radio frequency identification. RFID allow a reader to transmit radio wave to a passive electronic tag for tracking, identification and authentication.

NFC is a subset of radio frequency identification (RFID). NFC was design and marketed by the NFC forum. NFC forum is a non-profit industry association which was established by Nokia, Philips and Sony in 2004, to advance the use of NFC technology by developing specifications, interoperability among devices and services, and educating the market about NFC technology. The forum now has 190 members. Manufacturers, applications developers, financial services institutions and others all work together to promote the use of NFC technology in consumer electronics, mobile devices, Pcs, and more

The goals of the NFC Forum are to:

- Develop standards-based Near Field Communication specifications that define a modular architecture and interoperability parameters for NFC devices and protocols.
- Encourage the development of products using NFC Forum specifications.
- Work to ensure that products claiming NFC capabilities comply with NFC Forum specifications.
- Educate consumers and enterprises globally about NFC

In June 2006, only 18 months after its founding, the Forum formally outlined the architecture for NFC technology. The Forum has released 16 specifications to date. The specifications provide a “road map” that enables all interested parties to create powerful new consumer driven products.

Nokia 6131 first NFC phone released on February 2006. In 2011, handset vendors released more than 40 NFC-enabled handsets such as, Google Nexus S, Black Berry Bold 9790, Bold 9900/9930 and more others. Between 2012 and 2013 many more Smartphone equipped with NFC were released, e.g. Motorola Photon Q, Razr 1 and Razr D3 HTC 1xl, Google Nexus 5, Samsung Galaxy Note 3 e.t.c Smartphone’s equipped with NFC Technology that are available in the market today are highly increasing. HTC among several other companies such as LG, RIM, Samsung Mobile, Windows Phone 8 operating system and more, has begun developing devices based on NFC technology

Other devices that are equipped compatible with NFC Technology are Tablet computers e.g Nexus 7, Nexus 10 and AccerIconia W510 and Think Pad Tablet 2 e.t.c and video game controller such as Wii U GamePad. Smartphones outfitted with near-field communications could see a jump in shipments from 416 million this year to 1.2 billion in another four years, says research firm IHS Technology

For those who want to use near field communication technology but don’t currently have an NFC compatible Smartphone, there are other ways to enable NFC on your phone without trading it in for an expensive new model. Both SIM and SD cards can be equipped with NFC chips, and some companies currently offer or are preparing to offer these options so more customers can start using NFC technology.

Once you’ve purchased an SD or SIM card for your Smartphone, turn off your phone and insert the card. Turn the phone back on and search your Smartphone’s marketplace for apps compatible with NFC technology. To work you’ll need to wave the area with the SD or SIM card over the card reader, which can prove a little trickier to hit than with Smartphone’s that come preinstalled with NFC chips. Removing the card will disable your NFC access.

On April 16, 2014 the NFC Forum announced the public availability of new versions of nine technical specifications, following approval by the Board of Directors. The new versions deliver greater interoperability, faster read and write performance, mediated handover, and lower power consumption, as well as additional functionality for products incorporating NFC technology. The revised specifications comprise an integrated and streamlined set designed to be used together, bringing greater efficiency to the process of developing standards-based NFC products. Currently, devices such as Nexus S, Galaxy Nexus, Samsung Galaxy Note, Sony Xperia ZR, Nokia 6131 NFC etc. provide NFC facility to its users. Some applications of NFC are Google Wallet (US), A Little World (India) for mobile payments, China Unicom for mobile transport ticketing (China) etc.

To date, the NFC Forum has completed 21 technical specifications, as the momentum for Near Field Communication devices and services continues to grow. ABI Research estimates that over 500 million NFC-enabled devices will reach the market this year.

3. MODE OF OPERATION

NFC enabled devices and tags are designed just like an RFID enabled device and tag to be used at 13.56 MHz with a bandwidth of almost 2 MHz [COCHIN UNI.] and therefore the device and tag designs are similar. At this frequency range, RFID tags mostly use the theory of Strongly Coupled Magnetic Resonance. This is basically where two nearby loop antennae provide strong electromagnetic mutual induction resonance. This effect is also known as inductive coupling. During operation, other communication frequencies are disabled which allows very fast communication between coupled resonances [KFUPM].

The Fig. bellow depicts how NFC technology works

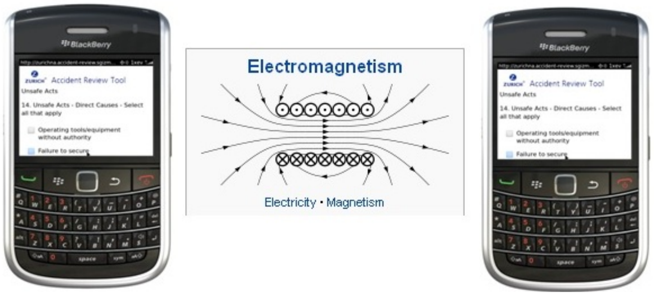
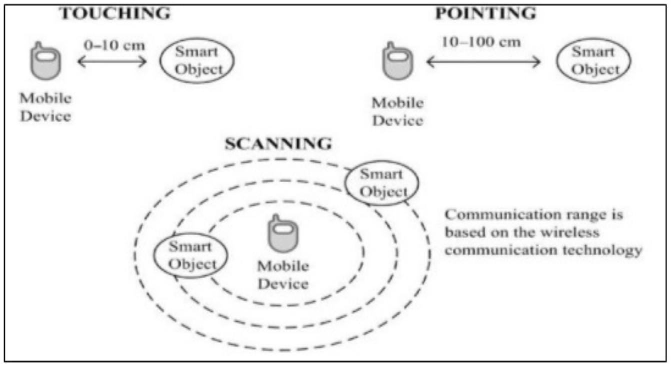


Fig. 1

1. Coil in the first smart phone sets up a current that is picked up a second smart phone or reader.
2. The second smart phone receives the “induced current” from the first, recognizes it as a valid signal and offers a connection.
3. The first cell phone accepts the connection and begins the transaction.

When mobile devices are used to interact with smart objects in the environment, additional components are required where when a user interacts with a smart object using an interaction technique. Fig. 2shows the available interaction techniques that the mobile devices use, which are called mobile interaction techniques, they are touching, pointing, and scanning [2]. The NFC technology interaction technique is touch based



The touching action is taken as the triggering condition for NFC communication. The NFC application is designed so that when the mobile touches some NFC device with the expected form of data, it boots up immediately.

We can classify the NFC devices in the communication based on two parameters. The first parameter is the energy supply which results in active and passive devices. The second one is initiating the communication and leads to initiator and target devices.

There are two modes of communication:

1. Passive Communication Mode: The Initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the Target device may draw its operating power from the Initiator-provided electromagnetic field, thus making the Target device a transponder.
2. Active Communication Mode: Both Initiator and Target device communicate by alternately generating their own field. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically need to have a power supply.
3. Having a mobile phone fitted with an NFC chip will enable users to send and exchange data just by touching, or bringing together the two devices. Fig 3 shows the NFC-related elements on Mobile Handsets.

NFC tags contain data and are typically read-only, but may be rewriteable. They can be custom-encoded by their manufacturers or use the specifications provided by the NFC Forum, an industry association charged with promoting the technology and setting key standards. The tags can securely store personal data such as debit and credit card information, loyalty program data, PINs and networking contacts, among other information. The NFC Forum defines four types of tags that provide different communication speeds and capabilities in terms of configurability, memory, security, data retention and write endurance. Tags currently offer between 96 and 4,096 bytes of memory.

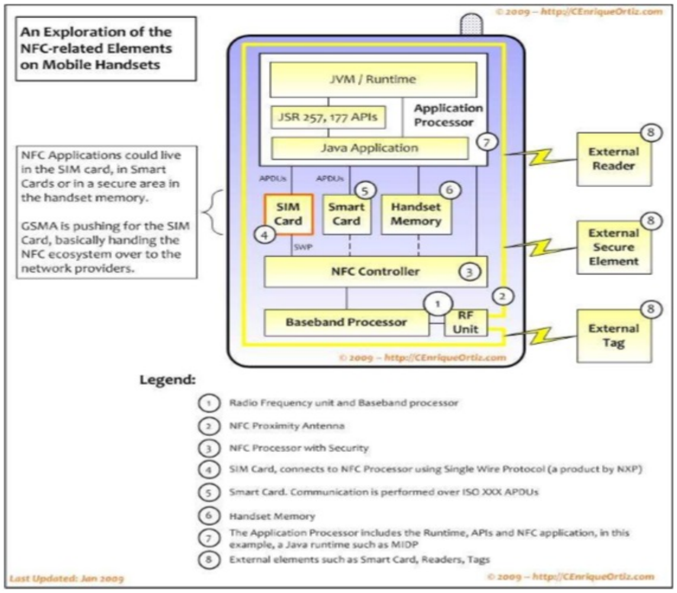

© 2009 – http://CEnriqueOrtiz.com
An Exploration of the NFC-related Elements on Mobile Handsets
NFC Applications could live in the SIM card, in Smart Cards or in a secure area in the handset memory.
GSMA is pushing for the SIM Card, basically handing the NFC ecosystem over to the network providers.
JVM / Runtime
JSR 257, 177 APIs
Application Processor
Java Application
7
APDUs
APDUs
5
6
SIM Card
4
Smart Card
Handset Memory
SWP
NFC Controller
3
2
1
Baseband Processor
RF Unit
© 2009 – http://CEnriqueOrtiz.com
8
External Reader
8
External Secure Element
8
External Tag
Legend:
1 Radio Frequency unit and Baseband processor
2 NFC Proximity Antenna
3 NFC Processor with Security
4 SIM Card, connects to NFC Processor using Single Wire Protocol (a product by NXP)
5 Smart Card. Communication is performed over ISO XXX APDUs
6 Handset Memory
7 The Application Processor includes the Runtime, APIs and NFC application, in this example, a Java runtime such as MIDP
8 External elements such as Smart Card, Readers, Tags
Last Updated: Jan 2009
© 2009 – http://CEnriqueOrtiz.com

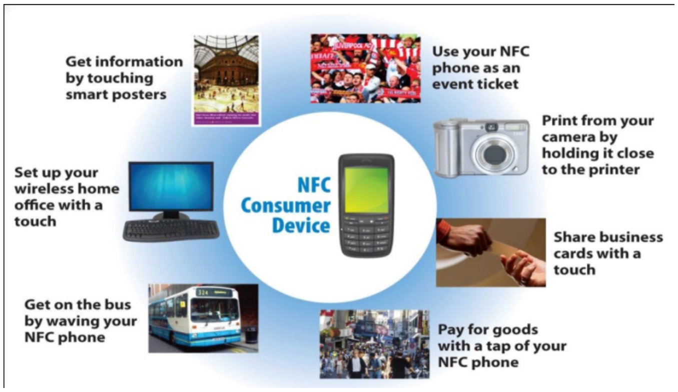
Fig. 3

- As with proximity card technology, near-field communication uses magnetic induction between two loop antennas located within each other's near field, effectively forming an air-core transformer. It operates within the globally available and unlicensed radio frequency ISM band of 13.56 MHz Most of the RF energy is concentrated in the allowed ±7 kHz bandwidth range, but the full spectral envelope may be as wide as 1.8 MHz when using ASK modulation.[3]
- Theoretical working distance with compact standard antennas: up to 20 cm (practical working distance of about 4 cm)
- Supported data rates: 106, 212 or 424 kbit/s (the bit rate 848 kbit/s is not compliant with the standard ISO/IEC 18092)
- NFC employs two different codings to transfer data. If an active device transfers data at 106 kbit/s, a modified Miller coding with 100% modulation is used. In all other cases Manchester coding is used with a modulation ratio of 10%.
- NFC devices are able to receive and transmit data at the same time. Thus, they can check for potential collisions, if the received signal frequency does not match with the transmitted signal's frequency.

4. APPLICATION OF NFC

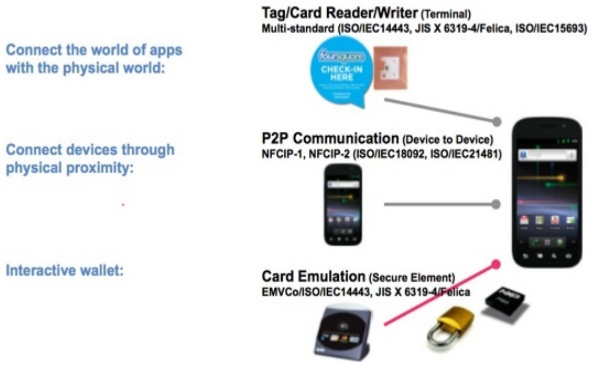
Near Field Communication (NFC) technology makes life easier and more convenient for consumers around the world by making it simpler to complete transactions, exchange digital content and connect electronic devices. Because of NFC’s inherent business benefits including security advantages, interoperability with existing contactless card technologies, applicability to a broad variety of industries and uses, and ease of use NFC is a vitally important technology helping to drive the burgeoning mobile commerce (M-Commerce) space. [10]

NFC technology harmonizestoday’s diverse contactless technologies, enabling solutions in areas such as information collection and exchange, Access Control, healthcare, loyalty and coupons, transportation, payments, and consumer electronics[4]. NFC technology is supported by the world's leading communication device manufacturers, semiconductor producers, network operators, IT and services companies, and financial services organizations. NFC is compatible with hundreds of millions of contactless cards and readers already deployed worldwide.


Get information by touching smart posters
Use your NFC phone as an event ticket
Print from your camera by holding it close to the printer
Set up your wireless home office with a touch
NFC Consumer Device
Share business cards with a touch
Get on the bus by waving your NFC phone
Pay for goods with a tap of your NFC phone

NFC, or Near Field Communication, allows consumers pay for goods and services on the go through their mobile phones simply by touching or passing them over another NFC-equipped device such as a register or terminal. The funds themselves are transferred from the user‘s credit card account stored through the mobile phone.

NFC-enabled devices are unique in that they can support three modes of operation: card emulation, peer-to-peer, and reader/writer


Connect the world of apps with the physical world:
Connect devices through physical proximity:
Interactive wallet:
Tag/Card Reader/Writer (Terminal)
Multi-standard (ISO/IEC14443, JIS X 6319-4/Felica, ISO/IEC15693)
foursquare CHECK-IN HERE
P2P Communication (Device to Device)
NFCIP-1, NFCIP-2 (ISO/IEC18092, ISO/IEC21481)
Card Emulation (Secure Element)
EMVCo/ISO/IEC14443, JIS X 6319-4/Felica

Card emulation mode enables NFC-enabled devices to act like smart cards, allowing users to perform transactions such as purchases, ticketing, and transit access control with just a touch.

Peer-to-peer mode enables two NFC-enabled devices to communicate with each other to exchange information and share files, so that users of NFC-enabled devices can quickly share contact information and other files with a touch. For example, users can share Bluetooth or Wi-Fi link set-up parameters or exchange data such as virtual business cards or digital photos.

Reader/writer mode enables NFC-enabled devices to read information stored on inexpensive NFC tags embedded in smart posters and displays, providing a great marketing tool for companies.

In reader/writer mode, the NFC-enabled device is capable of reading NFC Forum-mandated tag types, such as a tag embedded in an NFC smart poster.

Smartphones and other devices are not the only object that can be embedded with NFC technology, the MJ Bale power suit in collaboration with Australia Heritage bank and Visa pay wave unveil a technology to embed contactless payment chip and antenna to the sleeve of the suit so that you can pay by swiping the sleeve at the contactless POS terminals [5].

Personal health monitoring can be read by an NFC reader/Writer, which could be patient mobile phone by simply touching the reader to the health devices, Doctors equipped with NFC-capable tablet computers can call up all the information on a patient within seconds, without any chance of data getting mixed up. Chemists and pharmacists can also quickly check medicines in order to further diminish the risk of side-effects or to identify counterfeits if any doubt arises, heart rate could also be continuously monitored using heart rate monitors using NFC. The design droppler unit is embedded in a sort of clothing such as garment and the unit is directly placed on patient’s body [7].

NFC technology integrated in a mobile device typically consists of two integrated circuits. The NFC controller is required for the analog digital conversion of the signals transferred over the proximity connection. An HCI (host controller interface) allows the host controller to set the operating modes of the NFC controller, process data sent and received and establish a connection between the NFC Modem and the secure element.

The second IC, a secure smartcard chip also referred to as the secure element, is used for the tag emulation mode. The secure element is connected to the NFC controller for proximity transactions (external mode e. g. for payment at point of sale) through the Single-Wire Protocol (SWP). The host-controller as well is able to exchange data with the secure element (internal mode e. g. for top up of money into the secure element over the air).

The NFC market is still in its infancy, but analysts project rapid growth, and several hundred NFC initiatives are under way. The total market value of NFC globally is projected to increase by a 118 percent compound annual growth rate over five years, reaching $145 billion in 2015. By then, 863 million NFC-enabled mobile phones are projected to be in use, representing more than 53 percent of the total mobile phone market[10]

A variety of industry players have kicked off their own efforts to tap into the potential of NFC. Japan's three major mobile operators had sold nearly 14 million standard NFC-enabled Smartphones and tablets as of January this year as the country countries continues to be among the leaders in rolling out NFC enabled phones and Sims.

This will be a new business opportunities for Nigerian banks because the RFID infrastructure already exist in the ICT industry USA, Asia, Europe and some African countries, and their customers with NFC enabled phones will take full advantage of the situation where the banks don‘t have to rely on the mobile service operators for the payment services, the NFC enabled mobile acts as a credit card. The banks will not have to rely on the terms and conditions of any mobile service provider in order to provide mobile payment services, thus banks will have their own independent mobile payment service.

NFC is good business opportunity and a strategy for telecoms to have a competitive advantage over banks because with the ease of using NFC enabled phones customers will be able to purchase hard goods such as items bought from a supermarket or rental services over-and-above purchasing digital and services .

5. COMPARISION OF NFC WITH OTHER WIRELESS TEHNOLOGIES

Table 1 shows the comparison of various existing wireless technologies with NFC and Its benefits over the others.

Table 1: NFC provides a range of benefits to consumers and businesses through its inherent advantageous characteristics:

S/No	Concept	Bluetooth	RFID	NFC
1.	Setup time	~ 6sec	<0.1ms	<0.1ms
2.	Range	Up to30m	Up to 3m	Up to 10cm
3.	Userabilty	Data centric medium	Item centric easy	Human centric easy, intuitive, fast
4.	Selectivity	Who are you?	Partly giving	High given security
5.	Use cases	Control and exchange data	Item tracking	Pay, get access, share, initiate services, easy setup
6.	Consumers experience	Configuration needed	Get information	Touch, wave, simply connect
7.	Bit rate	2.1 Mbit/s		424kb/s

- **Intuitive**: NFC interactions require no more than a simple touch
- **Versatile**: NFC is ideally suited to the broadest range of industries, environments, and uses
- **Open and standards-based**: The underlying layers of NFC technology follow universally implemented ISO, ECMA, and ETSI standards
- **Technology-enabling**: NFC facilitates fast and simple setup of wireless technologies, such as Bluetooth, WiFi, etc.)
- **Inherently secure**: NFC transmissions are short range (from a touch to a few centimeters)
- **Interoperable**: NFC works with existing contactless card technologies
- **Security-ready**: NFC has built-in capabilities to support secure applications

6. NFC TECHNOLOGY VERSUS CYBER CRIME

With emergence of Information and communication Technology (ICT) in Nigeria, her economy is rapidly growing and the advent of mobile telephony on the Nigerian market played a major role and continues to be a key driver of advancements. But however, Nigeria's image as a country has been seriously tarnished, by various species of cyber crime that result from use of Internet and ranges of global wireless connection such as Wi-Fi, wireless USB/ Ultra wideband, Wimax, 3G, Bluetooth and GSM.

Cyber crime refers to the series of organized crime attacking cyberspace and cyber security, cyber crime varieties include cyber stalking, identity theft, hacking, interception threat, piracy, ATM fraud and among others. Cyber attacks that steal money, intellectual property, or launch political attacks that can destroy trusted relationships with customers and partners, which is your lifeblood. Cybercrime, which costs the world $300 billion to $1 trillion [7] estimated cost from cyber activites. Cybercrime, which costs the world hundreds of millions of dollars every year, had also led to the loss of sensitive business information, including possible stock market manipulation, the loss of intellectual property and business confidential information and reputational damage to the hacked company. Developed countries are also facing cyber security challenges, cyber crime activities in USA have cost her about $24 billion to $120 billion [12]. Millions of dollars are lost annually by consumers who have credit card and calling card numbers stolen from on-line databases. Cyber crime activities has led to the estimated Nigerian consumer loss of N2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012[13].ATM fraud is perpetrated through the ATM machine and e-transaction system. The current rise in ATM fraud has made the public to lose confidence in this technology that is meant to provide convenience and comfort while making cash withdrawal or while shopping. Cases of ATM frauds have made some banks and their customers lose millions of Naira yearly in Nigeria.Hackers can gain access to a phone's information by setting up a free wifi hotspot in a public place, or by tricking a user into clicking on an unsecured link that contains malicious code. This would give the hacker a backdoor entry into a phone and all the information on it including emails and bank details even if the phone looked as though it was on standby. The code can also be used to record all conversations conducted on a phone including those where a bank's security questions are answered or to take photos of a person and their home without them knowing [21].The growth of mobile and digital payments further highlights vulnerabilities within the smartphone system.

Risks include programs that eavesdrop on phone calls and text message, access to cooperate email and files, data corruption and manipulation, interception threat e.t.c.Cyber-attack risks continue to rise, cyber attacks are out of their control and will increase exponentially in the next 10 years. The negative cost of each attack will also increase. The Ponemon 2013 Cost of Cyber Crime Study, sponsored by HP, pegs the average annual cost of cyber crime for organizations at $7.2 million in 2013, up 30% from 2012[21].

New capabilities, such as Near Field Communication (NFC) technology is continuously on rise and this may increase the opportunities for cyber criminals to exploit weaknesses. NFC technology which is based on RFID allows for Smartphones to communicate with each other by simply touching another Smartphone or passing by a device by another device being in close proximity range of 4cm to another Smartphone with NFC capabilities or NFC devices. This technology is being in used for contactless payment i.e. payment of transaction such as purchase & ticketing.

7. NFC SECURITY CHALLENGES

New users of near field communication, especially for payment purposes such as storing credit card information, are understandably concerned at first about the security and safety of their private information. Possible security attacks include eavesdropping, data corruption or modification, interception attacks, and physical thefts. Below we cover the risks and how NFC technology works to prevent such security breaches from occurring.

- **Eavesdropping:** Eavesdropping is when a criminal "listens in" on an NFC transaction. The criminal does not need to pick up every single signal to gather private information. Two methods can prevent eavesdropping. First there is the range of NFC itself. Since the devices must be fairly close to send signals, the criminal has a limited range to work in for intercepting signals. Then there are secure channels. When a secure channel is established, the information is encrypted and only an authorized device can decode it. NFC users should ensure the companies they do business with use secure channels.
- **Data Corruption and Manipulation**: Data corruption and manipulation occur when a criminal manipulates the data being sent to a reader or interferes with the data being sent so it is corrupted and useless when it arrives. To prevent this, secure channels should be used for communication. Some NFC devices "listen" for data corruption attacks and prevent them before they have a chance to get up and running.
- **Data Insertion:** Data insertion is only possible if the answering device is slow in response to the message sent by the active device. The attacker inserts messages into the data exchanged between the two devices, but if the messages overlap, then the data becomes corrupt and the communication fails.
- **Interception Attacks:** Similar to data manipulation, interception attacks take this type of digital crime one step further. A person acts as a middleman between two NFC devices and receives and alters the information as it passes between them. This type of attack is difficult and less common. To prevent it, devices should be in an active-passive pairing. This means one device receives info and the other sends it instead of both devices receiving and passing information.
- **Walk Off:** Walk offs are when the device user lifts the device and walks away from the transaction while leaving the transaction connection open. Usually, when the connections are idle for a period of time the connection terminates automatically, but the time window where the connection is still open, it can be exploited.
- **Theft**: No amount of encryption can protect a consumer from a stolen phone. If a smartphone is stolen, the thief could theoretically wave the phone over a card reader at a store to make a purchase. To avoid this, smartphone owners should be diligent about keeping tight security on their phones. By installing a password or other type of lock that appears when the Smartphones screen is turned on, a thief may not be able to Fig. out the password and thus cannot access sensitive information on the phone.

While it may seem like NFC would open up a world of new security risks, it may actually be safer than a credit card. If a user loses her credit card, a criminal can read the card and find out the owner's information. If that same person loses her smartphone and has it password protected the criminal cannot access any private info. Through data encryption and secure channels, NFC technology can help consumers make purchases quickly while keeping their information safe at the same time.By using cyber security practice, users and organizations can strengthen readiness and response to help defend against the myriad of challenges and mitigate potential impacts of incidents;

- Enable encryption and password features on your Smartphones and other mobile devices.

- Disable wireless, Bluetooth, and NFC when not in use.
- Do not share your devices if used for a purpose
- Devices should be in active –passive pairing. This means one device receives info and the other sends it instead of both devices receiving and passing information.
- The Smartphones should be provided with tight security. By installing a password or other type of lock that appears when the Smartphone screen is turned on.

Near field communication technology has become a reality for many companies and users, and is poised for takeoff with other smartphone manufacturers. With Apple planning to incorporate NFC into the iPhone and a handful of NFC compatible smartphones already on the market, this branch of technology is changing rapidly. Hence, NFC has good speed of operation for close proximity. It is suitable for crowded areas. It uses ISM band of frequency which is available worldwide. NFC is affordable, has good throughput and low latency. Since transactions are done at a small range at which signals are not much susceptible to interception, NFC is highly

8. CONCLUSION AND RECOMMENDATION

As the general population becomes increasingly refined in their understanding and use of computers and Smartphones devices, the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. NFC technology has come to its maturity with big ICT and telecom industry players such as Google, Samsung and Nokia having embraced the technology. We are headed to an era of Mobile Wallet where cash value that can be stored on a card, phone or other electronic device may be topped up.

With over 114 million mobile subscribers amidst poor service and Nigeria‘s population is 166.2 million as last recorded in 2012, it shows that more than half of the population owns a mobile phone. Over half of the Nigerian population will benefit from the NFC technology if implemented by banks and the telecommunication companies. It will be easy for NFC to be implemented because banks already have the VISA card and MasterCard infrastructure in place. Also Implementation of NFC in hotels and airport terminal for domestic or International flights. As for NFC, we saw how it offers more benefits than drawbacks compared to existing technologies. At the end, we suggested how in the future NFC can be used in the country to improve the customers experience.

9. ACKNOWLEDGEMENT

Author is thankful to Kebbi State University of Science &Technology, Nigeria for providing necessary support for this research work.

REFFERENCE

[1] NFC Forum Publishes Comprehensive Set of Technical Specifications;NFC Forum

[2] Rukzio E., Callaghan V., Leichtenstern K., and Schmidt A. (2006), “An Experimental Comparison of Physical Mobile Interaction Techniques: Touching, Pointing and Scanning”, Proc. of Eighth International Conference on Ubiquitous Computing, CA, USA, 17–21 September 2006, pp. 7–104.

[3] Published on 16 April 2014; http://www.gisuser.com/content/view/32748/2/#sthash.eJqX5x9f.dpuf; Retrieved on 18 April 2014.

[4] Patauner, C. "High Speed RFID/NFC at the Frequency of

[5] "Wii U GamePad". Ign.com. Retrieved 30-04-2014

[6] By Lance Whitney @lancewhit; February 12, 2014 9:20 AM PST;NFC-enabled cell phones to hit 416 million shipments – report; http://www.cnet.com/news/nfc-enabled-cell-phones-to-hit-416-million-shipments-report; Retrieved on 30-04-2014

[7] Bank develops NFC suit that lets customers pay by swiping a sleeve; By RianBoden23 April 2014, 12:28; https://nfcworld.com/2014/04/23/328835/bank-develops-nfc-suit-lets-customers-pay-swiping-sleeve/; Retrieved on 2-05-2014, 23:27.

[8] The economic impact of cybercrime and cyber espionage;center for strategic and international studies July 2013

[9] JKSC, New Field Communication White Paper

[10] IJECE, vol 2, no. 3, june 2012, pp.375-376, kevin Curran, Amanda millar, conorMcGarvey

[11] SPRING 2013, NFC Implementation model;new science transaction Security,ul.com/newscience; Retrieve on 12-05-2014 23:08