Research Article Impact Factor: 0.621 ISSN: 2319-507X
Snehal Kuche, IJPRET, 2014; Volume 2 (9): 170-180 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY IN NEAR FIELD COMMUNICATION(NFC) AND SECURE MOBILE HEALTHCARE SYSTEM

SNEHAL H. KUCHE, STEFFI H.POPLI

Assistant Professor, IBSS College of Engineering, Amravati, Maharashtra, India

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Near field communication (NFC) is a set of standards for Smartphone and similar devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than a few inches. Present and anticipated applications include contactless transactions, data exchange, and simplified setup of more complex communications such as Wi-Fi. Communication is also possible between an NFC device and an unpowered NFC chip, called a "tag". NFC is the descendant or an evolved form of Radio Frequency Identification (RFID). Although technically its working principal is based on RFID, it is more similar to Bluetooth in applications since it allows communication between active devices. Currently, it has applications mostly in the field of contactless electronic payment. One of the largest IT challenges in the health and medical fields is the ability to track large numbers of patients and materials. As mobile phone availability becomes ubiquitous around the world, the use of Near Field Communication (NFC) with mobile phones is emerging as a promising solution to this challenge. The decreasing price and increasing availability of mobile phones and NFC allows us to to apply these to developing countries in order to overcome patient identification and disease surveillance limitations, and permit improvements in data quality, patient referral and emergency response. Mobile phone based patient terminals require an easy-to use and versatile design to facilitate collecting of various kinds of data relevant for therapy optimization. To meet these requirements a user interface concept based on mobile phones and medical sensor devices enabled with Near Field Communication (NFC) technology was developed, linked to a web-based telemonitoring system and evaluated in clinical field trials with patients suffering from different chronic diseases like diabetes and heart failure. Simple touch of NFC enabled mobile devices can benefit both the patient as well as the medical doctors by providing a robust and secure health flow. It can also provide portability of devices and usability for health management in emergency situation, overpopulated hospitals and remote locations.

Keywords: Near field communication (NFC), Security, Radio Frequency Identification (RFID).

PAPER-QR CODE

Corresponding Author: MS. SNEHAL H. KUCHE

Access Online On:

www.ijpret.com

How to Cite This Article:

Snehal Kuche, IJPRET, 2014; Volume 2 (9): 170-180

INTRODUCTION

Near Field Communication (NFC) is a wireless connectivity technology that enables convenient short-range communication between electronic devices. NFC offers the ultimate in convenience for connecting all types of consumer devices and enables rapid and easy communications. It is the perfect solution for controlling data in our increasingly complex and connected world. NFC builds upon RFID systems by allowing two-way communication between endpoints, where earlier systems such as contactless smart cards were one-way only. It has been used in devices such as Google Nexus, running Android 4.0 Ice Cream Sandwich, named with a feature called "Android Beam" which was first introduced in Google Nexus. Currently, NFC has applications mostly in the field of contactless electronic payment. Examples include Electronic Point of Sales (EPOS) terminals at shopping centers and ticketing systems in public transport such as buses and trains. NFC has also shown promise in being used for data transfer or 'data beaming' in applications such as smart posters or simplifying the setup of more complex communication methods such as Wi-Fi or Wi-Max. The inability to record visits or a brief medical history precludes continuity of care, not only as patients move across providers but frequently at the same clinic or hospital. Patients can be observed carrying old prescriptions, laboratory test results, and radiographs, and the information in these is not easily accessible and is often ignored. Additionally, since health care centres' are understaffed, providers often see a large number of patients in a short period of time, and may not have the time to counsel or refer patients appropriately.

In order to overcome these challenges and facilitate pneumonia detection in young children, we have developed tools which utilize NFC-capable mobile phones to allow electronic patient identification and tracking across multiple providers. These tools allow patients to be identified by a unique RFID tag on their person when they visit a clinic. By using a cell phone to send a patient ID and diagnosis to a central server, the physician will be able to report pneumonia in real time.

NFC phones contain special hardware-

Secure Element: Stores sensitive data (e.g. payment card information)

NFC Controller: Manages traffic and RF signals

NFC Antenna: Collects & transmits the RF

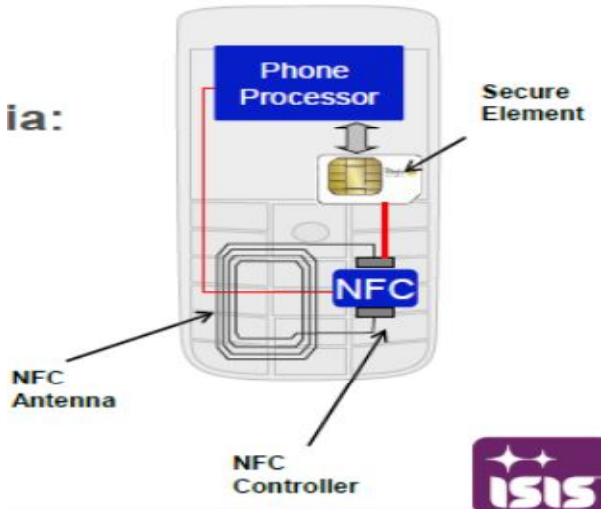

Fig.1. Secure elements of NFC

NFC devices can be used in contactless payment systems, similar to those currently used in credit cards and electronic ticket smartcards, and allow mobile payment to replace or supplement these systems.

II. LITURATURE REVIEW

Near Field Communication (NFC) is a wireless interface increasingly available in current and future mobile phones and Smartphone's. It is a short range (<10cm) wireless technology evolving from radio frequency identification (RFID). Although NFC based applications run in a similar manner to Bluetooth on mobile devices, the working principal behind Near Field Communication is based on RFID. The RFID reader is also called an interrogator or an initiator. It is a device that continuously propagates Radio Frequency (RF) signals and waits for a tag to response. NFC is a descendant or an evolved form of Radio Frequency Identification (RFID). Before studying NFC, certain features and specifications of RFID must be studied. RFID involves tracking or identifying objects by a 'reader' through information stored on electronic 'tags' using special RFID software called middleware. For communication, RFID technology uses frequencies in the radio range of the Electromagnetic (EM) spectrum; which are in the range of 3 kHz – 300 GHz. RFID can trace its roots back to World War II where a Russian inventor developed a covert audio spying device for the Soviet army in 1945. However, it wasn't until 1970's that the first true RFID device was invented which was a radio transponder with memory. From 1973 and onwards, real competition developed for research in the field of RFID. The term RFID was first used in a patent that was awarded to Charles Walton in 1983 for a

"Portable radio frequency emitting identifier". From then on, many applications have been found for RFID. NFC offers a low-speed connection with extremely simple setup, and can be used to bootstrap more capable wireless connections.

For example, the Android Beam software uses NFC to complete the steps of enabling, pairing and establishing a Bluetooth connection when doing a file transfer. Nokia, Samsung, BlackBerry and Sony have used NFC technology to pair Bluetooth headsets, media players, and speakers with one tap in its NFC-enabled devices. NFC can be used in social networking situations, such as sharing contacts, photos, videos or files, and entering multiplayer mobile games.

Acting as a secure gateway to the connected world, tomorrow's NFC-enabled mobile devices will allow consumers to store and access all kinds of personal data – at home or on the move. Simply by bringing two NFC-enabled devices close together, they automatically initiate network communications without requiring the user to configure the setup. NFC-enhanced consumer devices can easily exchange and store your personal data – messages, pictures, MP3 files, etc.

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
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 exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Table 1: Comparison between NFC and other technologies

Smart key access:

NFC is fully compatible with both Philips' MIFARE® and Sony's Felica contactless smart card platforms. These proven systems provide a solid foundation for the introduction of NFC-enabled devices. This enables NFC devices, like your mobile phone or PDA, to act as an electronic key to access your home, office, or car, or to pay for – as well as to act as – your transport ticket.

Enabling mcommerce:

Mobile ecommerce or mcommerce is a vast area of activity, covering any transactions involving monetary value conducted via an electronic device such as a mobile phone or PDA. Offering consumers the possibility to make any sort of electronic payment wirelessly, NFC-enabled mobile devices are well placed to become the heart of ecommerce.

III. TECHNOLOGY OVERVIEW

3.1 Wireless short range communication technology

NFC is designed for short distance wireless communication

•Allows intuitive initialization of wireless networks

•NFC is complementary to Bluetooth and 802.11 with their long distance capabilities

•NFC also works in dirty environment

•NFC does not require line of sigh

•Easy and simple connection method

•Provides communication method to non-self powered devices.

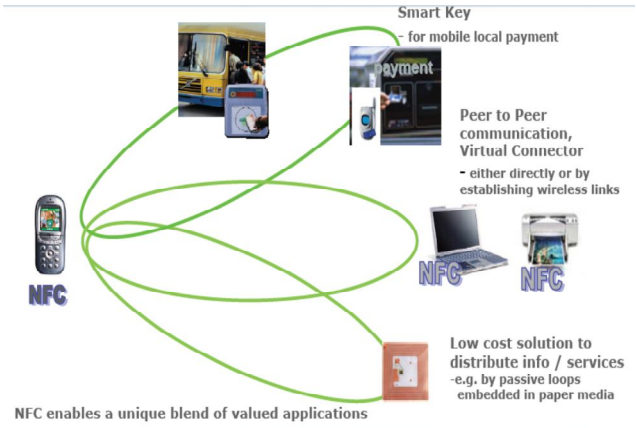

Fig.2 Wireless short range communication technology

NFC is a short-range wireless technology for distances measured in centimeters. It is optimized for intuitive, easy and secure communications between various devices without requiring user configuration. To make two devices communicate, users simply bring them close together. The devices' NFC interfaces will automatically connect and configure themselves to form a peer-to-

peer network. NFC can also bootstrap other wireless protocols like Bluetooth or Wireless Ethernet (WiFi) by exchanging configuration and session data.

Wireless short-range communication technology

- Based on RFID technology operating at 13.56 MHz
- Typical operating distance of 10 cm
- Compatible with today's field proven contactless MIFARE and FeliCa smart cards
- Data exchange rate today up to 424 kbit/s.

NFC communication modes NFC-enabled devices can operate in active or passive modes. Mobile devices operating primarily in passive mode can achieve significant power savings, extending precious battery time. Active NFC devices can supply all the power needed for communication with passive devices through their internally generated RF field. This is exactly the same way that contactless smart cards are powered and ensures that data remains accessible even when the mobile device is switched off.

3.2 Communication Modes: Active and Passive

The NFC interface can operate in two different modes: active and passive. An active device generates its own radio frequency (RF) field, whereas a device in passive mode has to use inductive coupling to transmit data. For battery-powered devices, like mobile phones, it is better to act in passive mode. In contrast to the active mode, no internal power source is required. In passive mode, a device can be powered by the RF field of an active NFC device and transfers data using load modulation. Hence, the protocol allows for card emulation, e.g., used for ticketing applications, even when the mobile phone is turned off. This yields to two possible cases, which are described in Table 3.1. The communication between two active devices case is called active communication mode, whereas the communication between an active and a passive device is called passive communication mode.

Communication Mode	Description
Active	Two active devices communicate with each other. Each device has to generate its own RF field, if it wants to send data. The RF field is alternately generated by one of the two devices.
Passive	In this mode the communication takes place between an active and a passive device. The passive device has no battery and uses the RF field generated by the active device.

Table 2: Communication Configurations

The system architecture can be seen in Figure 1. It features two components: a cell phone and a centralized web server.

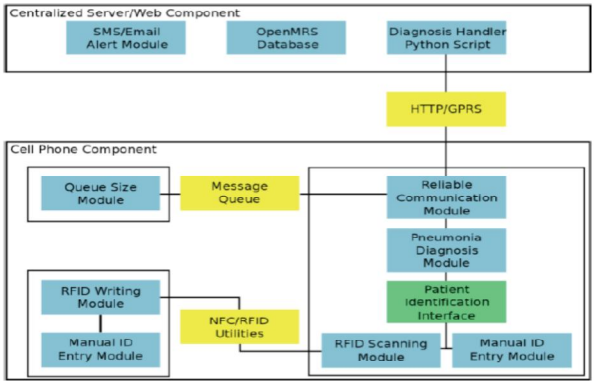

Fig. 3. System architecture. Web server side (top), Nokia 6131 NFC cell phone side (bottom).

A dynamic interpretation of the operation of the system architecture of our implementation is presented in the interaction diagram in Figure 2**.**

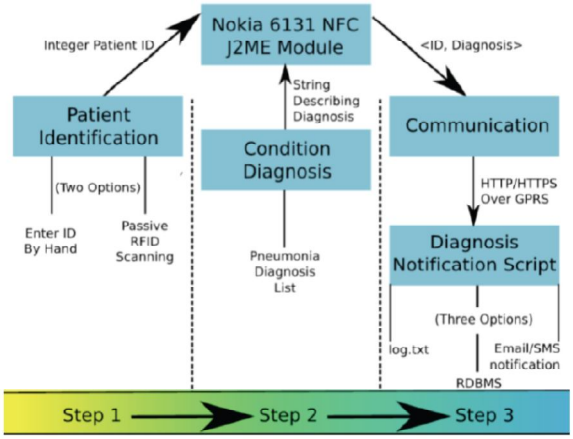

Fig. 4. The dynamic architecture of the developed system.

J2ME - Java Micro Edition, HTTP/S - Hypertext Transfer Protocol (over Secure Socket Layer),

GPRS - General Packet Radio Service, SMS - Short Message Service, RDBMS - Relational Database Management System

3.3 Combining communications and identification Near Field Communication

• The advantages of NFC • Combining communications and identification • Putting the user in control NFC enables connected consumer applications NFC technology Press releases NFC Forum Contact us Evolving from a combination of contactless radio frequency identification

(RFID) and networking technologies, NFC is a unique wireless connectivity technology that enables convenient short-range communication between electronic devices. It allows fast and automatic set-up of wireless networks, providing a virtual connector for existing cellular, Bluetooth and wireless 802.11 devices. This touch-and-go convenience enables rapid and easy communication between all types of consumer devices, making NFC the perfect solution for controlling data in our increasingly complex and connected world. Smart card security NFC combines connectivity with smart card security. NFC devices can read information from contactless cards. This makes smart cards the ideal solution for bringing information and electronic coupons into the NFC world. They can also operate like a contactless card – even when switched off – and are compatible with the huge installed infrastructure of Philips' MIFARE and Sony's Felicia contactless card systems. Virtual connector. NFC can be used as a virtual connector for quickly establishing other types of wireless communication between devices. By bringing two devices close together, it can automatically confi gure and initialize other wireless protocols such as WiFi and Bluetooth. This enables communications at longer ranges and higher data rates. In an environment rich with wireless-enabled devices, NFC is the easy way to set up connections without needing to go through complicated selection menus.

IV. SECURITY ASPECTS

There are different possibilities to attack the Near Field Communication technology. On the one hand the different used devices can be manipulated physically. This may be the removal of a tag from the tagged item or wrapping them in metal foil in order to shield the RF signal. Another aspect is the violation of privacy. If proprietary information is stored on a tag it is important to prevent from unauthorized read and write access. For detecting errors, NFC uses the cyclic redundancy check (CRC). This method allows devices to check whether the received data has been corrupted. NFC offers no protection against eavesdropping and can be vulnerable to data modifications. Applications may use higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel.

4.1 Eavesdropping

RF waves for the wireless data transfer with an antenna enables attackers to pick up the transmitted Monitoring data. In practice a malicious person would have to keep a longer distance in order not to get noticed. The short range between initiator and target for a successful communication is no significant problem, since attackers are not bound by the same transmission limits.

4.2Data modification

It is easy to destroy data by using a jammer. There is no way currently to prevent such an attack. However, if NFC devices check the RF field while they are sending, it is possible to detect attacks.

It is much more difficult to modify data in such a way that it appears to be valid to users. To modify transmitted data, an intruder has to deal with the single bits of the RF signal.

4.3 Data Destruction

An attacker who aspires data destruction intends a corruption of the communication. The effect is that a service is no longer available. Still, the attacker is not able to generate a valid message. Instead of eavesdropping this is not a passive attack. This attack is relatively easy to realize. One possibility to disturb the signal is the usage of a so called RFID Jammer.

There is no way to prevent such an attack, but it is possible to detect it. NFC devices are able to receive and transmit data at the same time. That means, they can check the radio frequency field and will notice the collision.

4.4 Data Insertion

This attack can only be implemented by an attacker, if there is enough time to send an inserted message before the real device starts to send his answers. If a collision occurs the data exchange would be stopped at once.

4.5 Man-in-the-Middle-Attack

In order to show that NFC is secure against a Man-in-the-Middle-Attack to survey both, the active and the passive communication mode. In the following distinguish between device A and device B that are exchanging data. In passive mode the active device (A) generates the RF field in order to send data to a passive device (B). The aim of an intruder is to intercept this message and prevent device B from receiving it.

4.6 Lost property

Losing the NFC RFID card or the mobile phone will open access to any finder and act as a single-factor authenticating entity. Mobile phones protected by a PIN code acts as a single authenticating factor. A way to defeat the lost-property threat requires an extended security concept that includes more than one physically independent authentication factor.

4.7 Secure Element

- **Java Card Operating Platform**

- **Secure memory**
- **Contact and contactless interfaces** ISO7816 and Single Wire Protocol (SWP)
- **Implements Global Platform** Smart card specification that defines card components, command sets, transaction sequences. Systems specification that standardizes back end systems for personalization, security, key management and application loading. Supports multiple security domains - One bank can have its own separate domain for secure credentials and Java applets.

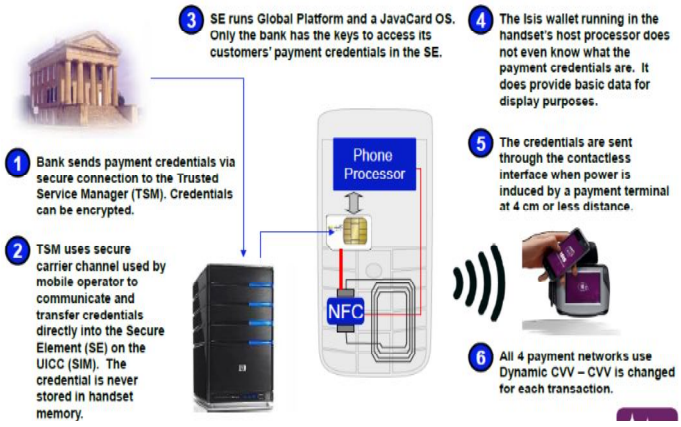

Fig.5 End to End Security

V.CONCLUSION

In summary, Near Field Communication is an efficient technology for communications with short ranges. It offers an intuitive and simple way to transfer data between electronic devices. A significant advantage of this technique is the compatibility with existing RFID infrastructures. Additionally, it would bring benefits to the setup of longer-range wireless technologies, such as Bluetooth. With a secure channel NFC provides confidentiality, integrity and authenticity.

REFERENCES

1. L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones." IACR Cryptology ePrint Archive, vol. 2011, p. 618, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/iacr/iacr2011.html#FrancisHMM11

2. ETSI TS 102 190 V1.1.1: Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1) 2003-03, URL:

http://www.etsi.org.

3. Yang, B., & Sun, J. (2011). Near field communication technology. Linkopings Universitet,

4. Near field communication. (2012, January 28). In Wikipedia, The Free Encyclopedia. Retrieved 23:49, January 31, 2012

5. The RFID Knowledgebase - Sample Case Studies. http://www.idtechex. com/pdfs/en/k3807f3934.pdf