Phone to Phone

In this category two cell phones equipped with NFC communicate with each other. They can transfer music files or pictures by just touching each other.

Figure 3: Phone to Phone NFC Transaction [8]

Phone to Device

Here NFC equipped cell phone can communicate with any device. For example, by just touching phone with NFC equipped printer can print the pictures stored in cell phone. Or by touching payment device can perform payment transaction.

Figure 4: Phone to Device Transaction [10]

Phone to Tag

Tag contains data. Normally tags are embedded on posters for marketing purpose. Cell phone is touched with tag and data from tag is transferred to cell phone. For example there is a tag on bus terminal which by touching cell phones transfers bus timings and other details.

Figure 5: Phone to Tag Transaction [10]

Phone to Reader

We can purchase and store electronic tickets on our cell phones. Cell phone can communicate with external reader by just touching it with reader. So one can purchase ticket easily instead of standing and waiting in a long queue

Figure 6: Phone to Reader Transaction [8]

2.7 NFC Application

NFC fall under three different categories upon its usage in different fields.

1- Service initiation category
2- Peer-to-Peer category
3- Payment and Ticketing category

Service Initiation

In this scenario functioning of NFC is the same as of RFID. NFC device reads some data from a tag and uses this information in several different ways. In this case tag serves as transponder, it could be a turned off cell phone. NFC device can read the data even if the cell phone is powered off. Example of such scenario can be the advertisement or information poster [12]. In this application NFC tag is fixed near information desk, user touches its NFC device with tag and retrieves the information. Suppose this tag is placed in university for guidance regarding study schedule of students. Whenever student wants to know his course schedule, he brings his NFC device close to NFC course tag and retrieves the information of his course schedule

Peer-to-Peer

In this application direct link between two devices is set up to transfer data. Amount of data may not be too large. If user wants to transfer large amount of data, Wi-Fi or Bluetooth connection can be set up, but that is invisible to user [12].

Figure 7: Peer-to-Peer data transfer [12]

Payment and Ticketing

In this scenario cell phone is used as electronic wallet. Nowadays we are using cards only for payments. But with NFC equipped device multiple functions could be collected under the same platform. Virtual money can be loaded in the cell phone that can be used to pay travelling tickets or parking fee [12].

Figure 8: Presenting e-ticket to machine [14]

3. NFC in Data Entry Tool

3.1 Proposed System

The architecture diagram with necessary components to obtain information of a particular product is shown in figure 9. The detail of how the real-time information from the product is acquired is explained below.

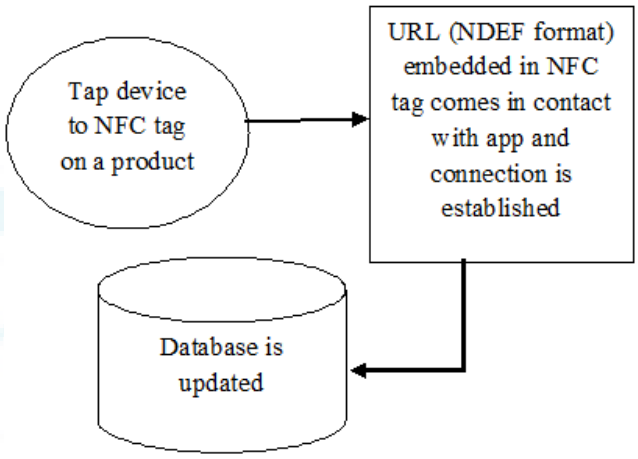

Figure 9: Process Flow

The URL of the user interface is embedded in the NFC tag using the NFC writer, we can use any phone having NFC to write and read the information from the NFC tag. The URL has to be stored in NDEF format to enable data exchange between NFC devices. After the encoding is done, the NFC tag is ready to be embedded to a product.

The data stored in the NFC tag has to be NDEF To encode our URL in to NDEF format and store it in a tag we use the NXP Tag writer android application. NXP Tag writer application fully supports the NFC Forum Type 1 Tag, Type 2 Tag, Type 3 Tag as well as Type 4 Tag portfolio. The application has to be downloaded and installed in the Smartphone. The following steps has to be followed to encode the URL in to the NFC tag

1) Open the NXP Tag writer application on your android device.
2) From the main menu select, create, write and store.
3) Type the URL that has to be stored in the NFC tag and click done button.
4) Select confirm overwrite from the list of options.
5) Just tap the NFC writer on the tag and the information is stored in the passive tag.

Just by doing a simple touch, NFC tag on the Product with the NFC enabled mobile phone, NFC device is initiating the connection with the passive NFC tag and the tag responds with a URL stored on it. This way connection is established. It is very simple, easy and convenient. The NFC enabled device is connected to the user interface and the user interface displays the information of the product

3.2 Advantages & Disadvantages

The implementation of this system would lead to easy data entry of product information into the web application instead of manually entering all the details of a product, it can now be done easily by just tapping a device to a tag.

NFC has several advantages over QR codes because to use a QR code, a business decides what they want the code to link to and uses a computer program to generate the image.

Printing the image onto advertisements or displays makes it available to the public. That's all there is to it. Yet if the business wants to change the link, they must generate and reprint a new QR code. The major advantage of NFC is its flexibility. Storing different types of information and changing it on a whim is possible without every creating a new NFC tag. The owner can simply overwrite the information currently on the tag and create new info. The second major advantage of NFC is its ease of use. With a QR code, the user must open a scanner app on their smartphone, hover over the QR code, and wait for the phone to analyze it and react to the code. With NFC technology, the user waves the phone near the NFC tag area and the information is transferred instantly. No need to open an app or wait for analysis. The tag and reader communicate with each other to complete complex transactions quickly and securely.

Some of the risks involved are Eavesdropping, Data Corruption and Manipulation, Interception Attacks, Theft. These can be reduced by ensuring use of secure channels; 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 and lastly by installing a password or other type of lock that appears when the smartphone screen is turned on, a thief may not be able to figure out the password and thus cannot access sensitive information on the phone.

4. Conclusion

The paper describes NFC and its functioning in detail and a rough architecture required for enabling data entry into a web portal by just touching a device to a product with NFC tag or sticker on it. NFC compared to QR codes is cheaper and hassle free, because in order to change the content on the NFC tag reprinting of image is not required, a simple overwrite will do the job. Using this method of data entry even an illiterate person can save product information on to the database. A significant advantage of using this technique is the compatibility with existing RFID infrastructures. It would bring benefits to the setup of longer range wireless techniques such as Bluetooth. Though security concerns are present, they can be overcome through the use of various schemes such as setting up a secure channel that can provide confidentiality, integrity and authenticity, or having password based locks on your phone to prevent from thefts.

References

[1] Near Field Communication, White paper, ECMA international, December 2003
[2] Päivi Jaring, Vili Törmänen, Erkki Siira, and Tapio Matinmikko, "Improving Mobile Solution Workflows and Usability Using Near Field Communication Technology", Technical Research Center of Finland Oulu, Finland, Springer-Verlag Berlin Heidelberg, pp. 358–373, 2007
[3] Eamonn O'Neill, Peter Thompson, Stavros Garzonis, and Andrew Warr," Reach Out and Touch: Using NFC and 2D Barcodes for Service Discovery and Interaction with Mobile Devices", UK, 2007
[4] ECMA-340 Standard, Near Field Communication Interface and Protocol (NFCIP-1), 2nd edition, December 2004
[5] Collin Mulliner," Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", Fraunhofer Institute for Secure Information Technology (SIT),2008
[6] Gauthier Van Damme and Karel Wouters, "Practical Experiences with NFC Security on Mobile Phones, Belgium, 2008
[7] Renee Montes, "Examining the technology, security and application of NFC and Evaluating the possible success of near field communication application in US Markets", Master thesis , Bowie State University, May 2009
[8] Ernst Haselsteiner and Klemens Breitfu, "Security in Near Field Communication (NFC) - Strengths and Weaknesse", Philips Semiconductors, Mikronweg , Gratkorn, Austria, 2006
[9] Gerald, Josef, Christian and Josef Scharinger, "NFC Devices: Security and Privacy, ARES 08 proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computing Society, Washington, DC, USA, 2008
[10] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis," Practical NFC Peer-to-Peer Relay Attack using Mobile Phones",UK,2010
[11] Renee Montes, "Examining the technology, security and application of NFC and Evaluating the possible success of near field communication application in US Markets", Master thesis , Bowie State Univerity, May 2009
[12] Matija Bumbak," Analysis of potential RFID security problems in supply chains and ways to avoid them", Master thesis, May 2005
[13] Rhys Williams, "NFC and RFID: Data security and privacy issues", Bird & Bird United Kingdom, USA, April 3, 2007
[14] Eamonn O'Neill, Peter Thompson , Stavros Garzonis and Andrew Warr," Reach out and touch: using NFC and 2D barcodes for service discovery and interaction with mobile devices", UK, 2006
[15] NFC Forum Specification, "NFC Record Type Definition (RTD) Technical Specification". Version 1.0, July 2006.

Author Profile

Mrs. Dhanamma Jagli is an Assistance professor in V.E.S Institute of Technology, Mumbai, currently Pursuing Ph.D in Computer Science and Engineering and received M.Tech in Information Technology from Jawaharlal Nehru Technological University, Hyderabad and Andhra Pradesh. She has around 9 years teaching experience at the post graduate and under graduate level. She had published and presented papers in referred international journals and conferences. Her areas of research interest are Data Mining, Cloud Computing, Software Engineering, Data base Systems and Embedded Real time systems. She has been associated with Indian Society of Technical Education (ISTE) as a life member.

Ms. Annora Rodrigues is a final year student of Master of Computer Application (M.C.A) from Vivekanand Education Society's Institute of Technology (V.E.S.I.T), Mumbai University, Annora has completed her B.Sc. in Computer-science from SIES college of Arts, Science & Commerce; Mumbai University. She is an ardent programmer with an abiding interest in web application development and programming languages like C++, Java, PHP and .Net technologies.