A Secure Smart Posters in Android using NFC

K. Nagargoje,S. Bhailume, A. Kanade, A. Gupta

[1]*Kiran Nagargoje, Computer Engg, MMIT Lohgaon, Maharastra, India*
[2] *Sachin Bhailume, Computer Engg, MMIT Lohgaon, Maharastra, India*
[3] *Akshay Kanade, Computer Engg, MMIT Lohgaon, Maharastra, India*
[4] *Aanchal Gupta, Computer Engg, MMIT Lohgaon, Maharastra, India*

ABSTRACT

A Smart posters are a promising new use case for NFC-enabled mobile devices, but to date there has been a general lack of security mechanisms for NFC smart posters. We present a secure smart poster system consisting of three parts: an administrative web interface for managing posters, a backend server for storing and serving data, as well as an Android application for end-users. Smart Poster enforces confidentiality and integrity of smart poster data as well as authentication, authorization of administrators and end-users, thus ensuring that only authorized users can access the content.

Keyword : - *Near Field Communication , NFC Card, Security, Smart Poster*

1. INTRODUCTION

A Smart posters posses businesses or other organizations to shared private information to end-users in a more interactive fashion in standard posters, are an increasingly popular application of NFC tags. A typical NFC smart posters is to provide users of NFC-enabled smart phones with quick access to a URL related to the poster content. Smart posters used for NFC enabled mobile devices, there has been a general lack of security mechanisms for NFC smart posters. The confidentiality and integrity of smart poster data as well as authentication and authorization of administrators and users is not checked. NFC tags are vulnerable to spoofing and wireless channel, is susceptible to data modification or man-in the-middle attacks. the presence of a digital signature. There are also situations that call for smart posters to contain sensitive information only privacy to specific users

Example :- A museum may wish to use NFC smart posters in tandem with a custom smart phone application, to provide additional information about exhibits on the condition that the content should only be available to users who have paid for admission on a given day.

1.1 Communication Mode

In NFC communication. These technique is based on a message and reply concept. This means one device A sends a message to another device B and device B sends back a reply to device A.It is not possible for device B to send any data to device A without first receiving some message from device A.

NFC devices support two communication modes.

1.1.1   Active Mode –

In this mode, the target and the initiator devices have power supplies and can communicate with one another by signal transmission.

1.1.2   Passive Mode –

In this mode, the initiator device generates radio signals and the target device gets powered by this electromagnetic field.

1.2 Near Field Communication

In NFC, the communication occurs when two NFC compatible devices are brought together less than four centimeters, or simply by touching themselves. It operates at 13.56 MHz and can transfer data up to 424 Kbits per second. In an NFC model two devices are involved in the communication, which are called initiator and target. Initiator is an active NFC device which is responsible for starting the communication. Also it has an embedded energy component whereas target can be either a tag, RFID card or an NFC device which responses the initiators requests.

Parameter	Bluetooth	Zigbee	NFC
Range	10-100 m	10-100 m	4-10 cm
Data	0.8-2.1 Mbps	0.02-0.2 Mbps	0.02-0.4 Mbps
Cost	Low	Low	Low
Power Cosumption	High	Medium	Low
Spectrum	2.4 GHz	2.4 GHz	13.56 MHz
Security	Low	Low	High
Network Topology	Piconets, Scatternets	Star, Tree, Mesh	One to One
Devices per Network	8	2 to 65000	2
Usability	Moderate, Data Centric	Easy, Data Centric	Easy, Human Centric
Personalization	Medium	Low	High
Flexibilty	High	High	High
Setup Time	Approx. 6 sec	Approx. 0.5 sec	Less Than 0.1 sec

Table -1: Comparison of WPAN technologies

One of the advantages of NFC technology is that mobile devices can be used both as information storage or an NFC reader. They can read information from NFC tags and display that information on the screen with an ability to make additional processing. Also they can be used as a digital storage.
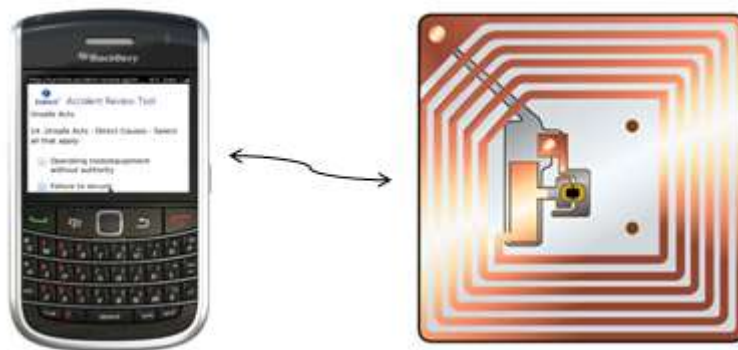
Fig-1 :- Magnetic Field between Readers and Tags RFID

1.3 NFC Tag

The NFC tag is battery less and is charged by an electromagnetic field generated by the mobile phone. One of the advantages of NFC over other wireless technologies is simplicity. Transactions are initialized automatically after touching a reader, another NFC device or an NFC compliant transponder. NFC is short range wireless technology with range of 10 cm theoretically ,practically being 4cm. NFC standard supports different data transmission rates such as 106kbps, 212 kbps, and 424 kbps. NFC requires no discovery and pairing. Another advantage of installing NFC software in your cell phone is that it consumes less power than Bluetooth. Smart phone users are greatly attracted to NFC technology as they can get another latest application in their NFC Phones that can bring more convenience in the way they operate things. A tag stores data in a standard manner called the NFC Data Exchange Format (NDEF) and each NDEF message contains a number of records that identify the type of stored data.

1.4 Near Field Communication Smart Posters

An NFC Smart Poster. It can be Magazine, a newspaper, and of course a poster. The NFC smart poster will hold one or more NFC tags that will interact with any reader. When any user moves an NFC enable phone close to a smart poster, then phone reads the contents of the tag and executes an action e.g. opens a browser pointing to the URL or displays the text. Figure1. Shows that an example of user interaction with department smart poster.

Fig-2 :- User interaction with department smart poster

The main advantage NFC technology offers, emerge the idea of providing to users access to university information and services using Smart Posters. The location of Smart Posters in anywhere on the campus or university or organisation building, allows that anyone (students, teachers, or people not related with the university) with a NFC enabled device may access to this information and services at any time.

2. LITERATURE REVIEW

In NFC, the communication occurs when two NFC compatible devices are brought together less than four centimeters, or simply by touching themselves. In an NFC model two devices are involved in the communication, which are called initiator and target. Initiator is an active NFC device which is responsible for starting the communication. Also it has an embedded energy component whereas target can be either a tag, RFID card or an NFC device which responses the initiator's requests. One of the advantages of NFC technology is that mobile devices can be used both as information storage or an NFC reader. They can read information from NFC tags and display that information on the screen with an ability to make additional processing. Also they can be used as a digital storage e.g. storing credit card information.

Other most important advantages of NFC technology include;
• The technology is compatible with existing RFID structures, existing RFID tags and contactless smart cards.
• It is easy to use and familiar to people because users don't need to have any knowledge about the technology. All a user has to do is to start communication by bringing two devices together. International Journal of Advance Research in Engineering, Science & Technology (IJAREST) Volume 4, Issue 5, April 2017, e-ISSN: 2393-9877, print-ISSN: 2394-2444 All Rights Reserved, @IJAREST-2017 526
• The transmission range is so short that, when the user separates two devices, the communication is cut. This brings inherent security. If there isn't any other device close, there is no other communication.

There are several short range communication technologies such as RFID, Bluetooth, Bluetooth ULP (Ultra low power, known also as a Wibree), Zigbee which provide flexible communication for several applications depending on which kind of communication is required. From these technologies, RFID is one of the promising technologies to be used with a human operator.
NFC is an promising growth technology and thus has become a topic of interest for academic research. The entire research framework has been divided into four categories.

1. NFC Theory and development

Author : Mauricio A. Valle , Samuel Varas , Gonzalo A. Ruz The most fundamental aspects related with the development of NFC falls under this section."Overviews, Context and Foundations" deals with general introductions, assessment, reviews and standards etc. "Policy, Legal and Ethical Issues" includes legal requirements, security and privacy issues etc. Such kind of paper focuses on behavioural aspects..

2. NFC Infrastructure

These are intermediate level. "Network and communications" deals with new protocols, data and communication aspects. "Tags, Antennae, Readers and NFC Chip" deals with the hardware aspects. "Security and Privacy" deals with CIA principles, Non Repudiation and other possible vulnerabilities.

3. NFC Application and Services

Author: Yasin Uzun These include various NFC applications or services that can be developed from NFC infrastructure available. Industry and developers around world focus more on this part. The 3 modes of NFC communication fall under this category. "Read/Write" to read and write data from/to NFC tags. "Peer-to- peer" mode allows establishing communication link between two active devices. "Card-emulation" mode which makes smart phones behaves like credit cards or smart cards etc..

4. NFC Ecosystem

This is the highest level NFC Research framework. "NFC Economics and Strategy" and "NFC Business Models and Processes" deal with the business requirements and managerial aspects of the NFC Technology. "NFC Stakeholders, Structure and Culture" deals with more of social aspects. They deal with User Acceptance, Reliability and maintainability etc.

3. PROPOSED SYSTEM

Smart posters, which allow businesses or other organizations to disseminate information to end-users in a more interactive fashion than standard posters, are an increasingly popular application of NFC tags. Such tags store small amounts of read-only (or less commonly, rewriteable) data. A typical use case for NFC smart posters is to provide users of NFC-enabled smartphones with quick access to a URL related to the poster content. Smart posters are a promising new use case for NFC enabled mobile devices, but to date there has been a general lack of security mechanisms for NFC smart posters. The confidentiality and integrity of smart poster data as well as authentication/authorization of administrators and end-users is not checked. NFC tags are vulnerable to spoofing as well as cloning, and the RF channel, like any wireless channel, is susceptible to data modification or man-in the-middle attacks. Furthermore, the NFC protocol as currently defined has some weaknesses, e.g. the standardized NFC Data Exchange Format (NDEF) does not guarantee integrity and authenticity, even in the presence of a digital signature. There are also situations that call for smart posters to contain sensitive information only privacy to specific users.
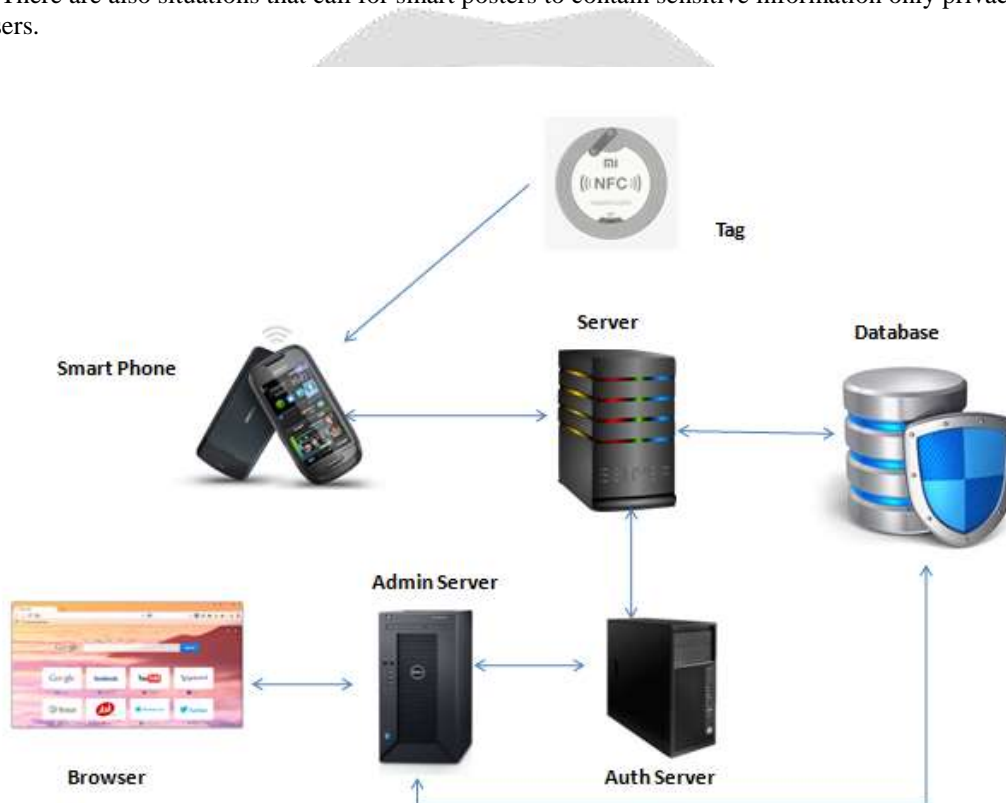
Fig-3 : Application Artitecture Block Diagram

3.1 Backend-Server

The backend for the smart poster application consists of two major components, namely a web interface for administrators as well as an API for the mobile application. Only specific authorized users are allowed to access the administrative web interface. Once logged in, an administrator can add two types of smart posters: link posters or poll posters. A link poster contains a brief description and a URL to the web version of the poster or a related webpage. A poll poster contains a question as well as up to ten choices, from which the user can choose. These responses are sent to a URL that the administrator specifies. When adding a poster, the administrator also has the option to set an expiration date; the poster will be automatically disabled after that date. In addition, for auditing and accountability reasons, all actions performed on the administrative web interface are logged. After an administrator

adds a poster, the server generates a pseudorandom 39-byte (312-bit) tag identifier for that poster. The administrator should write the tag ID into an NFC tag and affix it onto the poster so that users of the smart poster app can see the additional content.

3.2 Mobile Application

Our API provides the mobile app with read-only access to the database of tag IDs. For security reasons, all API requests must be made via HTTPS, and all input is validated before being acted on. The main API request, get poster, takes a tag ID for a particular poster and returns an XML le containing the poster content. If the tag ID is not in the database or the poster has already been disabled, then the XML le instead contains an error code. The mobile app can appropriately parse the XML le to retrieve the poster contents and display them to the user.

3.3 Authentication Server

Our All pages and scripts on our backend server are protected, so the Smart Poster app must check the users authentication status on each request to the server. To perform this check, the app takes advantage of the fact that will automatically redirect re-quests with invalid credentials to a login page; if the check fails, then the app asks the user to once again provide credentials.

Advantages of projected System:
NFC is a perfect source of convience because it merges a mobile device with wallet. NFC is also quite intuitive; all it takes is a simple touch when using NFC for payments. NFC can be well adapted for all kinds of situations ranging from bank cards to transit passes, movie passes, reward systems and even keys. Ideally, NFC is suited for a broad range of industries and uses because this innovation allows users to manipulate through the development of softwares.

4. CONCLUSIONS

The idea of "Secure Smart poster" will help user to changes they way of communication medium. A backend server for storing and serving data, as well as an Android application for end-users. We will enforces confidentiality and integrity of. Smart poster data as well as authentication and authorization of administrators and end-users, thus ensuring that only authorized users can access the content. It is a very good example of "HCI" domain. in administrative web interface for managing posters.

5. ACKNOWLEDGEMENT

6. REFERENCES

[1]. M. M. A. Allah, "Strengths and weaknesses of near field communication nfc technology," Global Journal of Computer Science and Technology, vol. 11, no. 3, Mar. 2011.

 [2].] A. J. Jara, A. F. Alcolea, M. A. Zamora, and A. F. G. Skarmeta, "Evaluation of the security capabilities on nfcpowered devices," 2010 European Workshop on Smart Objects: Systems, Technologies and Applications (RFID Sys Tech), pp. 1–9, Jun. 2010.

[3]. Pilar Castro Garrido, Guillermo Matas Miraz, Irene Luque Ruiz and Miguel Ángel Gómez-Nieto "A NFC Tool for Building Intelligent Environment using Smart Posters." Issue 1, Volume 4, 2010

[4]. Jason Wu, Lin Qi, Nishant Kumar, Ram Shankar Siva Kumar, and Patrick Tague S-SPAN: Secure Smart Posters in Android using NFC.

BIOGRAPHIES

	Name - Prof. Kiran B. Nagargoje Mail-Kiran.nagargoje@mmit.edu.in Phone No - 9763677613
	Name - Sachin A. Bhailume Mail-sachin.bhailume@mmit.edu.in Phone No - 8149524655
	Name - Akshay J. Kanade Mail-akshay.kanade@mmit.edu.in Phone No - 9561190419
	Name - Aanchal S. Gupta Mail-aanchal.gupta@mmit.edu.in Phone No - 8149691237