

# A Survey on Near Field Communication Based Smart Posters in Android

<sup>1</sup>K. Bankar<sup>2</sup>S. Choudhari<sup>3</sup>V. Bele<sup>4</sup>S. Gore<sup>1</sup> Ketaki Bankar, Computer, SRESCOE Kopergaon, Maharashtra, India<sup>2</sup> Surekha Choudhari, Computer, SRESCOE Kopergaon, Maharashtra, India<sup>3</sup> Vidya Bele, Computer, SRESCOE Kopergaon, Maharashtra, India<sup>4</sup> Supriya Gore, Computer, SRESCOE Kopergaon, Maharashtra, India

## ABSTRACT

Near Field Communication (NFC) is a short range wireless communication technology. The concept of NFC technology in a holistic approach including College assignments for students. NFC smart poster system in Colleges for assignments purpose consisting of three models: an administrative interface for managing smart posters, a backend server for storing and serving data to user, as well as an Android application for end-users. The system enforces to check authentication/authorization of administrators and end-users, thus ensuring that only authorized users can access the content. Near Field Communication released Signature Record Type Definition to provide integrity and authenticity for the NFC Data Exchange Format (NDEF). The Signature Record Type Definition add digital signature to the NDEF which is the standard format for storing the data on NFC device and transport the data between the NFC devices. .

**Keyword:** *NFC, smart posters, NFC enable smart phone, security*

---

## 1. INTRODUCTION

A Smart Poster can be any useful surface such as a magazine, a newspaper, and of course a poster. NFC is a new Radio Frequency (RF) technology used for short-range communication. It is an extension of Radio Frequency Identification (RFID) Technology [1]. It allows a bidirectional communication and an exchange of data between devices over a distance of about less than 20 centimeters. it operates at the frequency of 13.56 MHz's The maximum data transfer rate is 424kbit/s. NDEF is a binary message format that can be used to encapsulate information in NFC tag called NDEF message used to storing data on NFC device [3].

NFC technology is now available on smart mobile phones. It makes life easier for consumers around the world by making it simpler to make transactions, exchange digital content, and connect to electronic devices with a touch [2]. The application data stored inside an NFC Tag is encapsulated firstly into an NDEF message and then into a data structure specified by the NFC Tag Platform [3]. Such tags store small amounts of read-only metadata data. When user bring their NFC enabled smartphones close to smart poster, the phone reads the contents of the tag and execute an action.

NFC can operate in two modes. The modes are Active mode and passive mode. If the device generates its own RF field and has a power supply, it is called an active device; otherwise device is called a passive device. When two devices communicate can be done by three different configurations are (Active-Active, Active-Passive, and Passive-Active). These configurations are important because the data is transmitted depends on whether the device is in active or passive mode. There are two different roles for the active and passive mode, In NFC communication. NFC 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. The role of the device A which starts the data exchange is called initiator, the role of the other device i.e. device B is called target. The important thing is that NFC communication is not limited to a pair of only two devices, one initiator device can pair with multiple target devices [5].

On the security Analysis, NFC tags are very low-cost and have no processing power, so smart posters containing sensitive information and based on NFC tags must be carefully designed with security in mind. System is designed to overcome Tag Spoofing, Tag Cloning, Eavesdropping attacks. At the core of the application is the authentication framework used to authentication/authorization of one must be 'logged in.' our approach to eliminating tag spoofing and cloning is to store no information other than a string of random bytes in the tag. This is different from the conventional approach of storing the complete resource in the tag itself. Thus, if an attacker attempts to clone our tag, then he gets a bunch of random numbers, from which no information store in tag. These random numbers function as the tag ID, every tags has its own tag ID. HTTPS is used to secure communication between the server which browse data on mobile phone, so it avoid any possibility of eavesdropping. The role of administrator, whose only responsibility is to register the tags, has access to the audit logs of the posters and can revoke any poster and responsible for the user registration. A framework for secure active-passive pairings between NFC tags and Android devices in a smart poster setting is NFC smart poster secure itself because of transmission range which is less than 20cm [5].

This paper presents our work in developing an NFC supported College assignment system. The presentation in this paper is organized as follows: Section II presents a review on works done by some researches. We referred those researches to develop system in colleges for assignments purpose. All India campaign which is declared by government of India can be accessed using technologies like NFC smart posters, NFC enable mobile phone etc. Section III Discussed about the complete architecture and working of the system is explained. Finally, the last part presents the how it works and conclusion.

## 2. LITERATURE SURVEY

### 2.1 Near Field communication

NFC technology developed by Sony and Philips in late 2002. It is extension of Radio Frequency Identification (RFID) technology Short Range Radio Communication Technology with Frequency 13.56 MHz and Max. Bandwidth 424Kbits/sec.

Parameter	Bluetooth	Zigbee	NFC
Range	10-100 m	10-100 m	4-10 cm
Data Rate	0.8-2.1 Mbps	0.02-0.2 Mbps	0.02-0.4 Mbps
Cost	Low	Low	Low
Power Consumption	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
Flexibility	High	High	High
Setup Time	Approx. 6 sec	Approx. 0.5 sec	Less than 0.1 sec

Table 1. Comparison of WPAN technologies

Communication can establish when two NFC-compatible devices brought together less than 20cm [7]. NFC technology has been used in a number of applications such as ticketing and payment, retrieving information from information kiosks or setting up connections between devices (so called *device pairing*) [2].

### 2.1.1 NFC Tag

The NFC tag is battery less and is charged by an electromagnetic field generated by the mobile phone. The same field is used to establish communications between the NFC tag and the phone. A tag typically stores data in a standardized manner called the NFC Data Exchange Format (NDEF) and each NDEF message contains a number of records that identify the type of stored data. For example, the data may be a URL pointing to a website. When a user moves an NFC enable mobile phone close to a smart poster, the phone reads the contents of the tag and executes an action e.g. opens a browser pointing to the URL or displays the text. In principle an NFC tag could store 1Mbyte of data [6].

### 2.1.2 NFC smart posters

An advertising and provide service access means that is enabled by NFC technology, is the NFC Smart Poster. A Smart Poster 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 [6]. Figure 1. Shows that an example of user interaction with department smart poster.



Fig1. User interaction with department smart poster

The main advantage of features and NFC technology offers, emerge the idea of providing to the university users access to university information and services using Smart Posters. The location of Smart Posters in anywhere on the campus or university 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 [3].

## 3. PROPOSED SYSTEM

NFC Smart Posters have been created and used for many purposes, College assignments for student or notice. Whenever the student wants the information about their assignments or any notice, then corresponding to user's poster will display the contents to student. Student will get UserID and password via SMS notification. He/she just have to take his/her mobile near to the smart poster, after scanning he/she will get the detail info about poster.

### 3.1 Backend Server

The backend server for the NFC 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 user 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. If the administrator discovers that a poster contains undesirable content or simply wishes to stop using a particular poster, she can use the web interface to manually disable the poster so that users of the mobile app will no longer be able to access the content. 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, each NFC tag having its own tag ID. Tag IDs are never reused so as to prevent accidental or malicious reuse of an old, possibly disabled, poster to point to new content. 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 [4].



Fig. 1. Application architecture block diagram

### 3.2 Authentication Server

All pages and scripts on our backend server are protected, so the Smart Poster app must check the user's authentication status on each request to the server. To perform this check, the app takes advantage of the fact that will automatically redirect requests with invalid provide credentials to a login page; if the check fails, then the app asks the user to once again provide credentials [4].

### 3.3 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. When a user scans an NFC tag, the app calls `get poster` with the poster/tag identifier stored on the tag. The main API request, `get poster`, takes a tag ID for a particular poster and returns an XML file containing the poster content. If the tag ID is not in the database

or the poster has already been disabled, then the XML file instead contains an error code. The mobile app can appropriately parse the XML file to retrieve the poster contents and display them to the user [4].

#### 4. CONCLUSION

In recent years, NFC has become an attractive research area for many researchers and practitioners due to its exploding growth and its promising applications and related services. NFC in general is a very promising technology. With this study, NFC technology and its use cases in campaign by Government of India system. The Government schemes that provides to user using NFC smart poster. When user move their NFC enabled mobile phone near to smart posters then user get quick access to URL which stored in NFC tag, before access to URL administrator check the authentication/authorization of user.

#### 5. REFERENCES

- [1] Liam Church and Maria Moloney Escher Group Ltd, Ireland “State of the Art for Near Field Communication: security and privacy within the field” May 10th, 2012.
- [2] Muhammad Qasim Saeed, Colin D. Walter “An Attack on Signed NFC Records and Some Necessary Revisions of NFC Specifications”.
- [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.
- [5] By Mohamed Mostafa Abd Allah “Strengths and Weaknesses of Near Field Communication (NFC) Technology” Volume 11 Issue Version 1.0 March 2011.
- [6] “Keith E. Mayes, Lazaros Kyrrillidis, Konstantinos Markantonakis “A Brief Comparison of NFC Smart Posters and Quick Response Codes” keith.mayes, lazaros.kyrrillidis.2011.
- [7] Vedat Coskun · Busra Ozdenizci · Kerem OkA “Survey on Near Field Communication (NFC) Technology”.
- [8] “NFC Forum smart poster white poster”, April 2011.

#### BIOGRAPHIES

**Bankar Ketaki** is pursuing B.E Computer Engg in SRESCO, Kopargaon. Her areas of research interests include Information Security, Android.



**Choudhari Surekha** is pursuing B.E Computer Engg in SRESCO, Kopargaon. Her areas of research interests include Information Security; Android.



**Bele Vidya** is pursuing B.E Computer Engg in SRESCOE, Kopargaon. Her areas of research interests include Information Security; Android.



**Gore Supriya** is pursuing B.E Computer Engg in SRESCOE, Kopargaon. Her areas of research interests include Information Security; Android.

