*Impact Factor (SJIF): 3.632*

**International Journal of Advance Research in Engineering, Science & Technology**

*e-ISSN: 2393-9877, p-ISSN: 2394-2444*

***Volume 4, Issue 5, May-2017***

# S-SPAN: Secure Smart Posters in Android using NFC

**Komal Chandrakant Kante[1], Mayuri Rajendra Shewale[2], Megha Rajkumar Sawarkar[3], Prof. S. N. Firame[4],**

[1]*Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune*

[2]*Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune*

[3]*Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune*

[4]*Associate Professor, Department of Information Technology, Sinhgad Institute of Technology and Science, Narhe, Pune*

***Abstract — —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 S-SPAN - 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. S-SPAN 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.***

***Keywords- NFC, Smart posters, Smart phone, Security, Android***

## I. INTRODUCTION

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; for example, a user interested in a product advertisement might swipe her phone over the ad poster to open a webpage containing detailed specifications and a link to purchase the item. There are also situations that call for smart posters to contain sensitive information only privy to specific users. For example, a museum may wish to use NFC smart posters in tandem with a custom smartphone 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. S-SPAN aims to provide a framework for secure active-passive pairings between NFC tags and Android devices in a smart poster setting. This project was motivated by the Report on Smart Posters by the NFC Forum: "The benefit of signing tags is that they become secure - they can't be changed to direct users to other content" . Like any security analysts, our group recoiled in horror, when we read that the caretakers of NFC believe that signing tags make it secure. In particular, 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.Within this context, 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 . The main goal of S-SPAN is to secure smart posters against attacks on tags, end-user devices, the RF communication channel, as well as the NFC protocol, thus ensuring confidentiality and integrity of poster data as well as authentication of poster administrators and end-users.

## II. LITERATURE REVIEW

In NFC, the communication occurs when two NFC compatible devices are brought together less than four centimeters, or simply by touching themselves. It operater 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 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.

- 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 and Ir DA 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 emerging technology because of its promising growth 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.

## III. 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 privy to specific users. For example, a museum may wish to use NFC smart posters in tandem with a custom smartphone 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.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, all he gets is a bunch of random numbers, from which no information can be gleaned about the resource. These random numbers function as the tag ID, and an authenticated user queries the database using an HTTPS connection, thereby thwarting any possibility of eavesdropping.

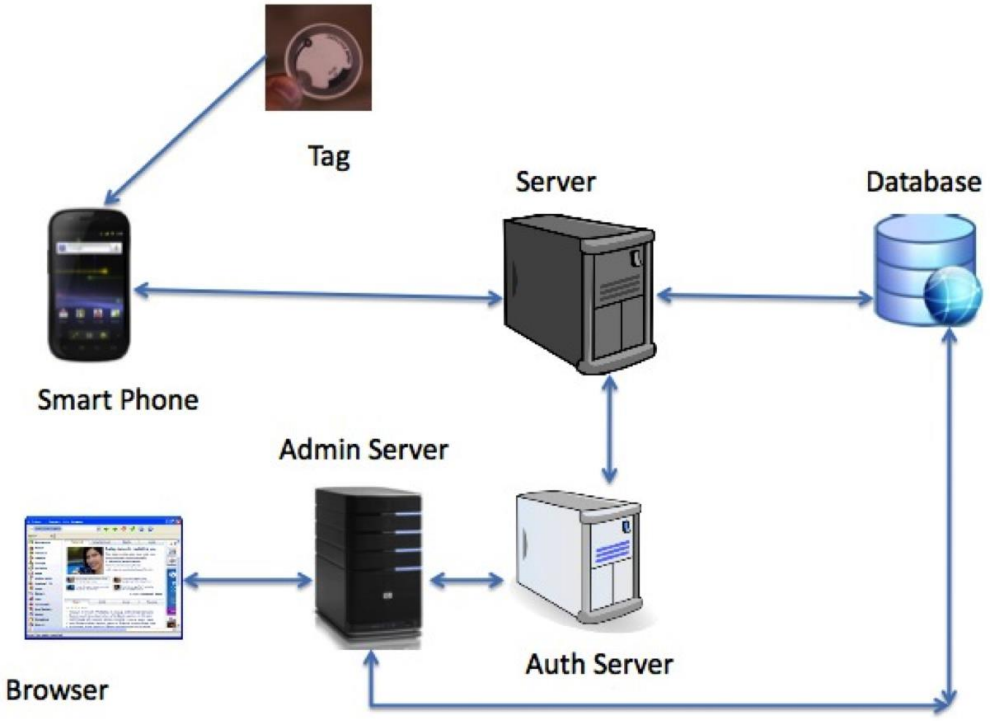



Figure: Proposed system architecture

**Advantages of projected System:**

NFC is a perfect source of convience because it merges a mobile device with wallet(s). 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.

## V. MATHEMATICAL MODEL

Let S is the Whole System Consist of

S= {I, P, O}

I = Input.

I = {U, Q, D}

U = User

U = {u1,u2….un}

Q = Query Entered by user

Q = {q1, q2, q3…qn}

D = Dataset.

P = Process:

P = {Topic Modeling, K-Means, SVM}

K-Means= K-Means Clustering Algorithm:

K-means algorithm will creates clusters of user searched query.

K-means algorithm will creates clusters of user searched query.
Let
X = fx1; x2; x3; :::; xng be the set of data points and V = fv1; v2; :;
Vcg be the set of centers.
1) Randomly select c cluster centers.
2) Calculate the distance between each data point and cluster centers.
3) Assign the data point to the cluster center whose distance from the cluster center is minimum of all the cluster centers.
4) Recalculate the new cluster center using: where, ci represents the number of data points in ith cluster.

$$v_i = (1/c_i) \sum_{j=1}^{c_i} x_i$$

5) Recalculate the distance between each data point and new obtained cluster centers.
6) If no data point was reassigned then stop, otherwise repeat from step 3).

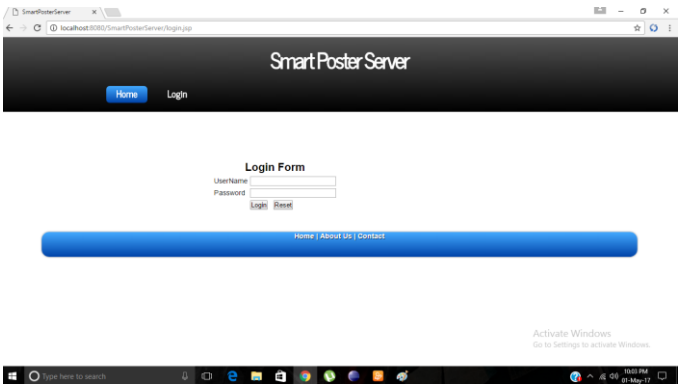
SVM=SVM Algorithm

SVM Algorithm will apply classification of created clusters

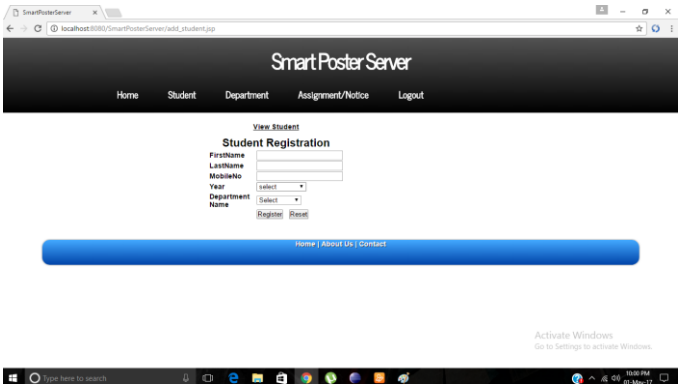
OUTPUT: The output will be the response of the user query.

## IV. RESULT AND DISCUSSION

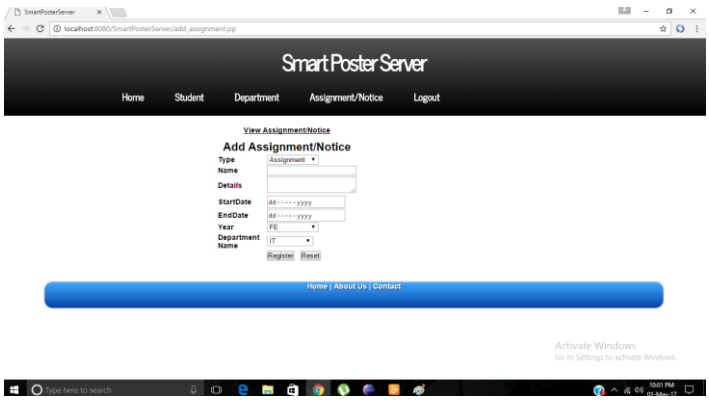
1. Result Screen Shot 1:



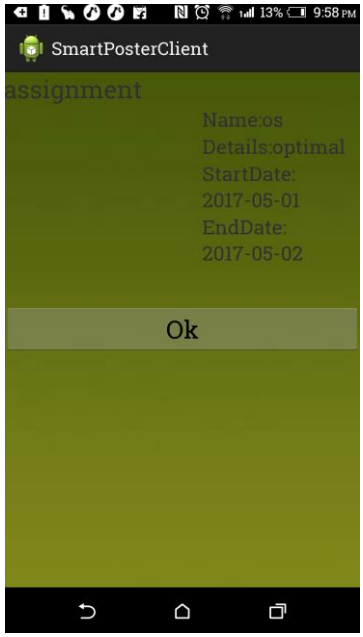

2. Result Screen Shot 2:



3 Result Screen Shot :




4 Result Screen Shot 4:



5 Result Screen Shot 5:


## V. CONCLUSION

The idea of "Smart poster" will help user to changes they way of communication. This will be a very good example of "HCI" domiain. an administrative web interface for managing posters. 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/authorization of administrators and end-users, thus ensuring that only authorized users can access the content.

## ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

## REFERENCES

[1]."Smart posters," White Paper, NFC Forum, Apr. 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]. 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.

[4]. M. Roland, J. Langer, and J. Scharinger, "Security vulnerabilities of the ndef signature record type," 2011 Third International Workshop on Near Field Communication (NFC), pp. 65–70, Feb. 2011.

[5] Ankit Lodha, Clinical Analytics – Transforming Clinical Development through Big Data, Vol-2, Issue-10, 2016

[6] Ankit Lodha, Agile: Open Innovation to Revolutionize Pharmaceutical Strategy, Vol-2, Issue-12, 2016

[7] Ankit Lodha, Analytics: An Intelligent Approach in Clinical Trail Management, Volume 6 ,Issue 5 , 1000e124