International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 09 | Sep -2017 www.irjet.net p-ISSN: 2395-0072

Android Application for Mobile Attendance Using NFC

Pallavi M V[1], S B Mallikarjuna[2]

[1]Student , Dept. Of Computer Science And Engineering, BIET college, Karnataka , India
[2]Associate Professor , Dept. Of Computer Science And Engineering, BIET college, Karnataka , India

---

Abstract – *Near Field Communication (NFC) upheld organization Mobile Attendance (Attendence) framework for representative in an organization. NFC is one of the most recent advancement in radio correspondences and being a subset of RFID innovation, it is developing at a immense pace. NFC innovation gives the quickest approach to convey between two devices and it happens inside a small amount of a second. It has a few applications in portable correspondences and exchanges. A NFC- reinforced organization M-Attendance framework for organization worker is one potential utilization of this development. The proposed structure replaces manual move calls and thus, making it versatile to imitation. The stamping of cooperation is smart, unsupervised, and makes use of a One Time Password (OTP) to redesign the security of the system and takes away the probability of mediator investment. NFC as an innovation that is more secure and advantageous than the common innovation of bluetooth, furthermore explains on the proposed structure of the M-Attendance framework that makes utilization of this preferred standpoint that NFC has over different advances.*

Key Words: *Near filed communication, NFC tag, RFID.*

1. INTRODUCTION

Near Field Communication (NFC) and one time password (OTP) upheld M- Attendance structure for little scale association. Traditionally employee needs to maintain the enrollment records for participation. This routine requires time and exertion, compromising on the working time. Expansion to this, a few employees exploits the benefit of low-security attendance framework and test the participation of the representative who is not available in the office [8]. The proposed M-Attendance framework has been intended to design to simplify streamlines attendance monitoring. It replaces the standard attendance checking framework and makes it faster, more secure and totally advanced.

It gives with the structure of executing an android application utilizing NFC. NFC is a short-range and high remote correspondence innovation that empowers the exchanging for majority of the data between gadgets inside a scope of 10cm from each other. It may be a update of the current closeness card standard that consolidates those interface of a smartcard and reader into a solitary device. It permits clients to continuously share content material among advanced gadgets.

Shorter set-up time is a significant preferred point of view that NFC has on its side. Rather than performing manual setups to distinguish gadgets, the association between two NFC device is built up without a moments delay (under 111 0 a second) due to this short range, NFC offers a better stages of protection than Bluetooth makes NFC affordable for swarmed zones in which connecting a flag with its transmitting physical gadget may somehow or another show impossible

1.1 RELTED WORK

The purpose of SRS report is to list the customer or client requirement in a systematic way. It characterizes all the constraints and software requirement that are necessary to understand the application and documentation.

Functional Requirements

A functional requirement characterizes quality of a framework or its part. A Characteristic is described as arrangement of input, behaviour, and output. Functional requirements are supported by non-functional necessities which force limitation on the plan or execution [12].
This framework system having two applications one is a web application in MVC architecture. Another application is android application which is developed with android SDK tools. The web application has following applications.

1. **Admin Application:** It is responsible to store the data on the server by providing employee details
2. **Android User Application**: Authorized user can login and write the employee details on NFC tag with encryption using key.
3.**NFC Writing Application:** Admin write the employee details into the NFC tag which will be encrypted using the NFC writing algorithm.
4.**NFC Reading Application:** When an employee taps the NFC tag to the device it decrypts the employee data.
5.**OTP Send Message Service:** If employee is an authenticated user OTP message will be sent to the user.

Non Functional Requirements

The non-functional requirements of the proposed system are as follows:

1.Performance:
The framework will be utilized by many employees simultaneously. Since the framework will be facilitated on a solitary web server with a single database server in the background, Performance turns into a major concern.

2. Scalability:
The framework is sufficiently versatile to include new functionalities at later stages. There should be a typical channel, which can accommodate the new functionalities.

3. Reliability:
The proposed framework will be reliable; it will not give false positive results and the fake user such that one cannot rely on it.

4.Flexibility:
The proposed system will be flexible to the user with less complexity and user friendliness.

1.2 SYSTEM DESIGN

The system design includes various phases of project design which consist of description of project, algorithms and some high level diagram such as data flow diagram (DFD), sequence diagram, use case diagram and class diagram .

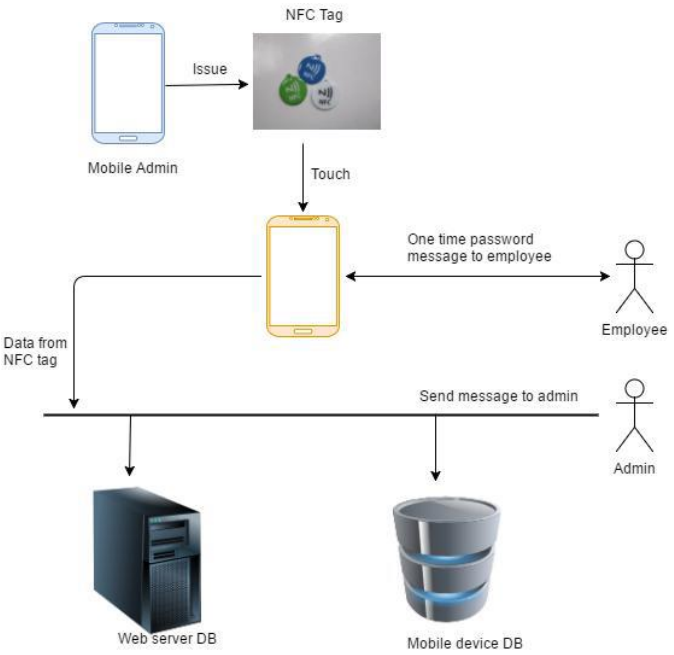


Fig -1: Architecture Diagram

Description:

The system design is a conceptual model which describes the structure, behaviour of a system. The above 4.1 shows the system architecture which has the following steps.

Step 1: Admin uses his ID and password for his login. Once the login is successful then he write the employee details like employee name , employee number , employee e-mail id , employee id , employee manager number etc., into the NFC tag . Tag now will contain the details of the employee.

Step 2: Employee/user tap the NFC tag to NFC enabled mobile device for the attendance purpose. One time password will be generated for each employee.

Step 3: Generation of one time password message and employee /user enters those OTP in the user's application, if password matches than user is an authenticated employee/user .If wrong OTP is entered or password entered doesn't match then user is not an authenticated employee/user.

Step 4: Once verification is successful it sends the time-in or time-out details to Admin. Admin gets time-in or time-out details of an employee. If the verification is not successful it displays invalid user.

2.1 MODULES

Writing the data into NFC tag Module
Once the key is generated admin has to collect each employee details from web application like (emp_id,emp_mobile number etc) this details has to be written into NFC card.

Reading the Data from NFC tag Module
User can get the NFC card from the admin of an office, Once the employee has entered into the office he has to tap the NFC tag into NFC enabled mobile device. Once User can get the NFC card from the admin of an office, Once the employee has entered into the office he has to tap the NFC tag into NFC enabled mobile device. Once the card is tapped, data is read from the NFC card. Below shows the psuedocode for reading the data from NFC tag.

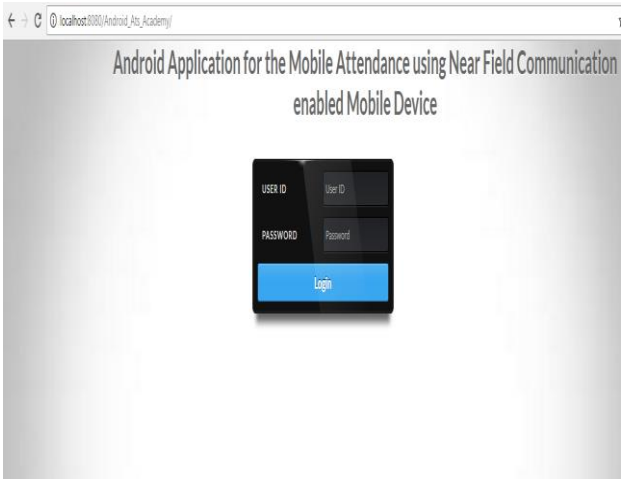
NFC Attendance System Module
Once Writing of the data with encryption and reading of the data with decryption is successful .To ensure the user or employee is an authenticated person the one time password will be sent to the emp mobile number. If the OTP is matching then get the current date , time and emp details insert emp attendance details into the mobile database. Once the inserting the details is successful send an emp attendance details to the appropriate manager mobile .If the entered OTP is incorrect then displays "entered OTP is incorrect try again" then stop .

2.2 EXPERIMENTAL RESULTS

Web Application

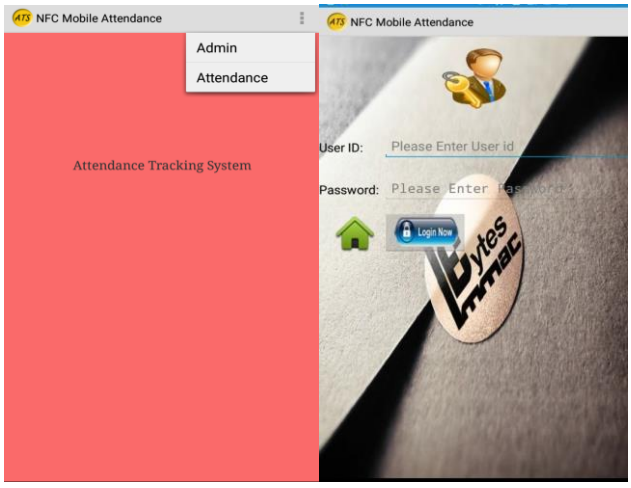
This section shows snapshots of a web application.

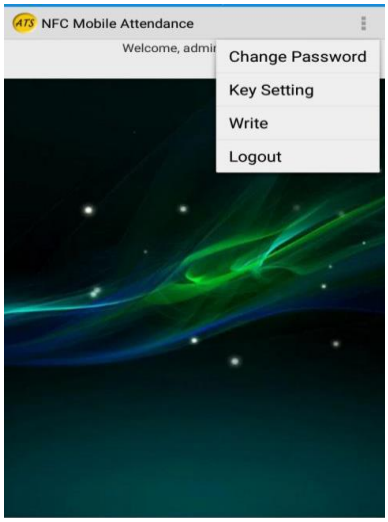
The fig shows the login form where a username and Password has to be entered to login into homepage.



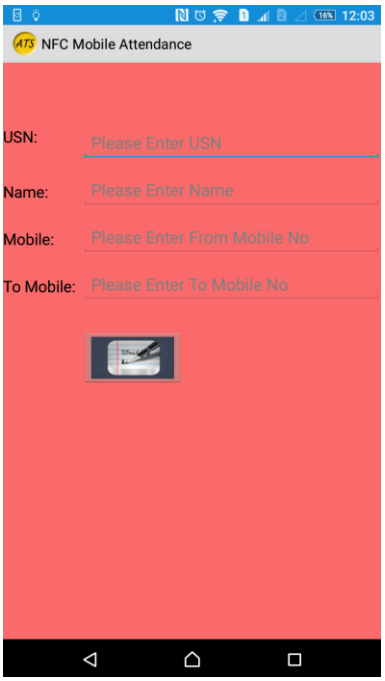
Android Application

This section contains the snapshots of an android application. The fig displays the sign in page of the application. By clicking sign in button its get navigated to login page. The fig shows the admin login page. With user id and password the admin login to homepage.

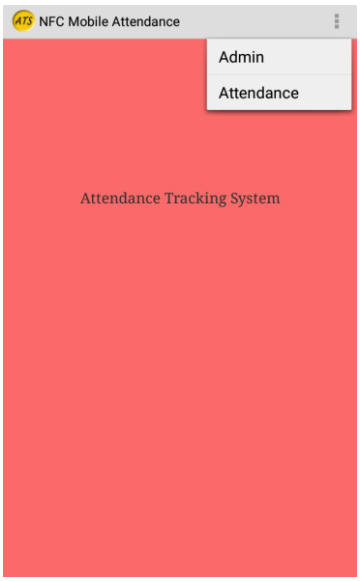




The admin has entered the correct user id and password the home page will be displayed which consist of four options they are change password, Key setting, write and logout.

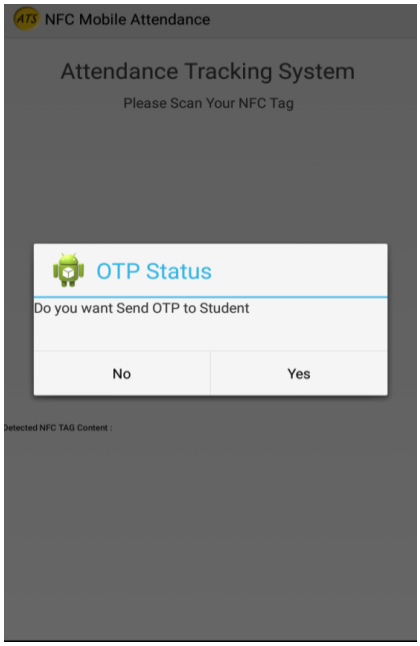


Writing the data into the NFC tag. Once the writing of data is complete then an message will be displayed “I have written your Encryption data into the tag!!”

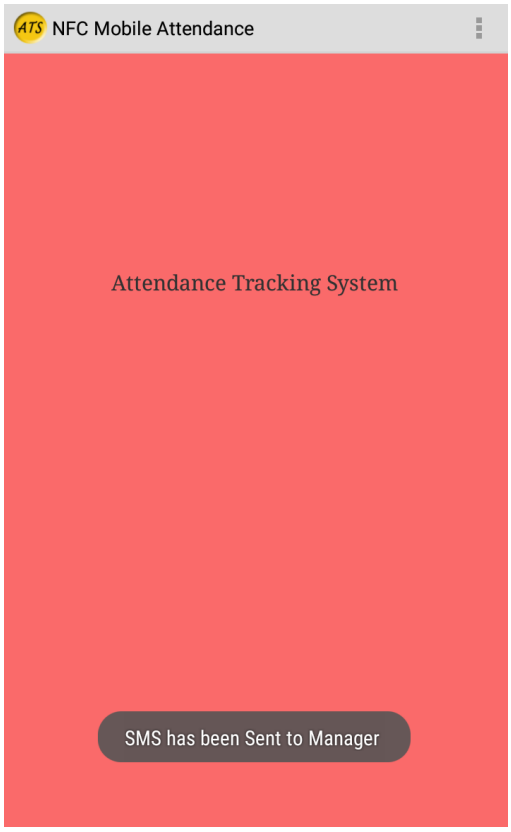


The android application attendance login page where the employee can enter the one time password.

The android application attendance home page where the NFC tag has to be scanned in order to get the one time password



Once the NFC is scanned or detected the One time password will be generated to the employee to verify that he/ she is an authenticated user.



Conformation message about the employee log in and log out details to admin.

3. CONCLUSIONS

The traditional attendance system have a tendency to be insecure due to absence of verification. In the proposed framework, we are utilizing Near Field Communication tags or cards and one time password for verification of employee and enlistment of participation in a systematic and secured way .Every employee near field communication tag will be utilized along with mobile device which would be utilized for automating the way of marking attendance.

The mobile device attendance framework can reduce unnecessary manual work by enabling administrator to get real time information about attendance of an employee. The advantages for the administrator are that to maintain all the data about employee attendance and keeping log record for future reference.

REFERENCES

1. T. Saini, "One Time Password Generator System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, ISSN:2277 128X, March 2014.

2. K. Preethi, A. Sinha, and Nandini, "Contactless Communication through Near Field Communication.

3. D. Florencio and C. Herley, "One-Time Password Access to Any Server without Changing the Server", Springer-Verlag,pp. 401-420, Berlin, Heidelberg, 2008.

4. G. Shanghai, H. Jivani, and S. Shahi, "Mobile BasedAttendance Marking System using Android and Biometrics",IJIRST-International Journal for Innovative Research inScience &Technology, Vol. 1, Issue 1, ISSN: 2349-6010, June2014.

5. S.K.Jain ,U.Joshi .B.K Sharma “Smart touch NFC innovation”.

6. T. Chang-Lung, C. Chun-Jung, and Z. Deng-Jie, "SecureOTP and Biometric Verification Scheme for Mobile Banking",Third FTRA International Conference on Mobile, Ubiquitous,and Intelligent Computing, IEEE, 2012.

7. K. G. Paterson, and Douglas Stebila, "One-time-password authenticated key exchange" September 4, 2009.

8. P Elakiyaselvi, "A framework for implementing M-Attendance system using near field communication in android OS".

9. V. Kostakos and E. O'Neill, "NFC on mobile phones issues, lessons and future research".

10. B. Ozdenizci, M. Aydin, V. Co□kun, and K. OK, "NFC Research Framework: A Literature Review and Future Research Directions", 14th IBIMA Conference, June 2010.

11. E. Haselsteiner and K. Breitfub, "Security in Near FieldCommunication (NFC) Strengths and Weaknesses".

12. https://en.wikipedia.org/wiki/Software_requirements_specification

13. https://en.wikipedia.org/wiki/Systems_design