GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

IMPLEMENTATION OF RELIABLE ATTENDENCE SYSTEM USING ANDROID AND NEAR FIELD COMMUNICATION TECHNOLOGY

VIJAY KAKANI
Department of Electronic and Computer Engineering, University of Limerick, Ireland

Abstract

Technology is an outcome of education, but in this modern technological era time has come to education to get benefits from technology. Student attendance monitoring system is a system that will take students attendance by using android and NFC technology. This system mainly comprises of active NFC device (Mobile Device) which is used as a reader, passive NFC tags which are embedded to the students ID cards and Server machine with database and application server. Android application installed in active NFS device will read student‘s NFC tag embedded card and identify the unique identifier assign to student and that will be transfer to application server with other details in a encrypted secured message over wireless network and stored in the database .Interfaces will be provided to access and analyze data in a secured way to administration staff to look in to daily attendance and to create timely reports. This System will replace old and inefficient paper based systems. This paper discusses the framework implementation of the system with corresponding software designing diagrams. On the other hand, the results are illustrated from the implemented procedure using the Samsung NFC tag with the android implemented NFC code.

Keywords: NFC technology, Student Attendance system, Android SDK, NFC tags

1. Introduction

Near Field Communication (NFC) is an integration of contactless smart card communication technology in mobile devices such as mobile phones. NFC Technology offers three modes of operation and each mode differs from the others in terms of communication and data processing model. Each mode has properties that can distinguished, advantages and disadvantages; so that each one of them offers different business opportunities and different perspectives of value added. In this work we study NFC applications currently available, as well as its application prototypes. Subsequently, we analyze the applications in order to find the features that offer. The central idea of this work is to implement some of the emerging technologies such as computing, mobile smart card technology and near field communications. The concept of Near Field Communication (NFC) is indeed a short range high frequency wireless technology which facilitates the users to exchange data between the devices at certain limited range of distance (10 centimeters). The concept of NFC is based on the wireless communication between the two entities making the protocol more commonly called as the peer-to-peer communication protocol. Here the two parties participating in the wireless communications are the computer peripherals and the customer electronic. This communications in the wireless mode operates at the reasonable radio frequencies like 13.56 MHz [1] [2] which indeed don’t require any sort of permissions or licenses. But each and every country has its limitations on the use of RF frequency ranges. In this project point of view, the usage of operating distance is set up between 0~20 cm. In this mode of wireless transfer the communicating entities share the single RF channel making the communication scenario as half duplex – listen before talk policy. The device must talk or transmit the signal after listening to the signal transmitted by the other device and making the confirmation that the other devices aren’t transmitting. This indeed has the two entities mentioned with certain terminology like Initiator and the Target. As the name indicates, the initiator makes the initial communication and controls the data exchange and the Target responds to the Initiator by answering to the requests sent by Initiator. Thereby using android in this project could have the capability of gaining more access and having more flexibility with the recent technologies.

In the perspective of the use cases for the NFC, initially there are 3 main use cases:

- **Card emulation:** In this the NFC device acts as if an existing card with contactless in practice [3].
- **Reader mode:** In this mode, the NFC device will be active and also reads the passive RFID tag for interactive advertising and other initial issues [3].
- **Peer-to-Peer mode:** In this mode, the NFC devices communicate with each other in the way by exchanging information. In this scenario, the usage of android beam is done in order to communicate with each other [3].

The NFC communication also supports the active and passive mode of communications:

- **Active mode:** In this mode, the both devices generate the RF fields of their own to carry the data. As such the name says the devices acting in the communication are in the active mode [4].
- **Passive mode:** In this mode, only one device acts as a generator of the RF field and the other will use the load modulation to transfer the data. In such cases, the protocol itself specifies the device that is responsible for the generation of RF field is “Initiator” [4].

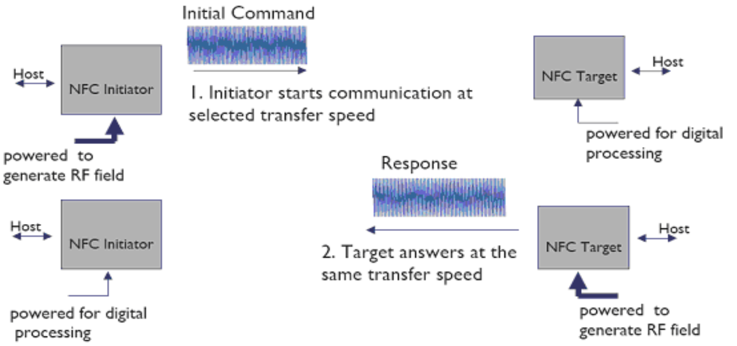

Initial Command
Host
NFC Initiator
1. Initiator starts communication at selected transfer speed
NFC Target
Host
powered for digital processing
powered to generate RF field
Response
Host
NFC Initiator
2. Target answers at the same transfer speed
NFC Target
Host
powered for digital processing
powered to generate RF field

Fig. 1 Active mode

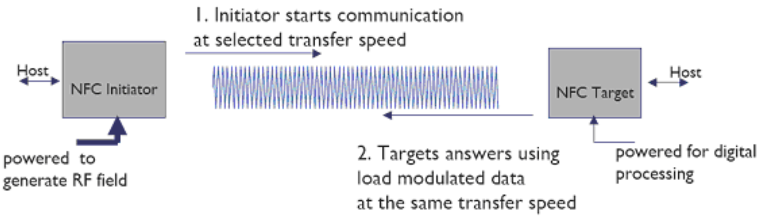

1. Initiator starts communication at selected transfer speed
Host
NFC Initiator
NFC Target
Host
powered to generate RF field
2. Targets answers using load modulated data at the same transfer speed
powered for digital processing

Fig. 2 Passive mode

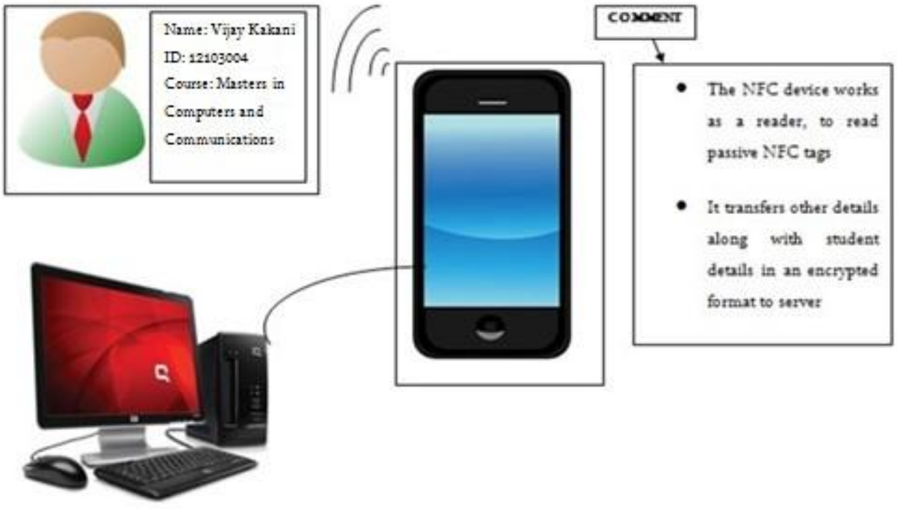
2. System Analysis

2.1. Existing System

Presently we are implementing some manual registers to enter the student attendants and for other details which lead to lot of time consuming process and it was very complicated work to retrieve the student details from older days to check his attendants. After this we implemented barcode readers to give authentication to the users (students) but it was quite unsecured process where the barcode can be corrupted. So for more secured authentication fingerprint readers were implemented but it was a very expensive process.

2.2. Proposed System

In the proposed system implementing a very simple NFC (Near Field Communication) System with an android application device to track the attendance details of the student and providing some access permissions to the student in the campus. The system implemented in NFC was highly secured. Although the higher-layer cryptographic protocols (e.g., SSL) are used to establish a secure channel in order to overcome General Security Threats like Eavesdropping, Data modification, Relay attack, and Lost property and Walk-off.


Name: Vijay Kakani
ID: 12103004
Course: Masters in Computers and Communications

- The NFC device works as a reader, to read passive NFC tags
- It transfers other details along with student details in an encrypted format to server

Fig. 3 Proposed system schematic

3. Flow Schematic of the Proposed System

3.1 System Modules

The following are the modules used in the project to accomplish the task, there are hereby very important stages of the total implementation.

- NFC reader
- Data Transfer
- Data Maintenance

3.1.1 NFC Reader:

In this module the active NFC device read the passive NFC tags to authenticate the student. This module consists of passive mode of communication and then the whole picture of transferring data to the database comes next to this stage. In this stage, the NFC tags which has its significant information stored as the encrypted data could later be read by the reader (NFC enabled phone in this case) to decrypt and send the information to the server as well store in the database. This is the initial module that is to be implemented using NFC tag and a reader which can read it.

3.1.2 Data Transfer:

In this module the student details which were retrieved from the passive tag were used as a reference of the particular student and his/her in time when he entered and his/her out time when leave the campus wear updated to the server in secured manner. The security provided to the data while transferring from NFC device to the server in wireless medium by implementing the higher-layer cryptographic protocols (e.g., SSL) to establish a secure channel and need to overcome General Security Threats like Eavesdropping, Data modification, Relay attack, and Lost property and Walk-off. Data security will be provided though application server and Database management system. This step is very important in terms of the security aspects, being involved with some techniques to prevent the attacks on the system information that is transferred to the server from the reader device.

3.1.3 Data maintenance:

In data maintenance process the data received from the active NFC device was decrypted and use the student id and name as reference and updates the student details like in time, out time, late time and absent in the database and send the report to the student and the parents about the student status report And the data was not supposed to be modified other than the administrator. Maintaining such system requires exact accessibility and errorless storage facilities.

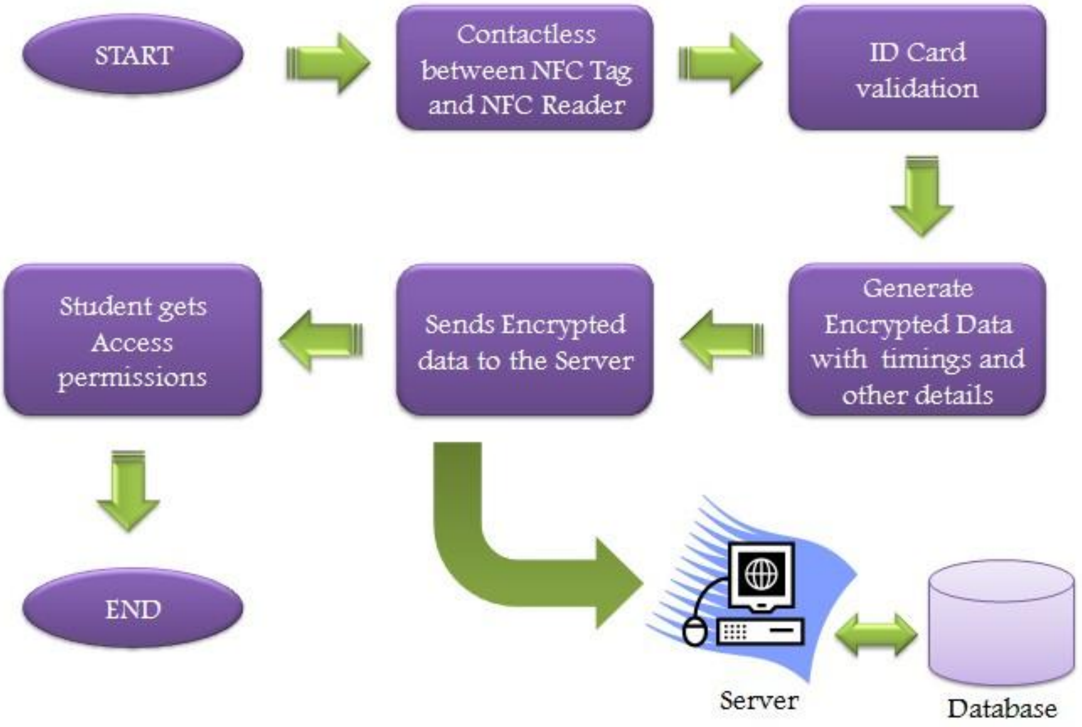

START
Contactless between NFC Tag and NFC Reader
ID Card validation
Generate Encrypted Data with timings and other details
Sends Encrypted data to the Server
Student gets Access permissions
END
Server
Database

Fig. 4 Flow schematic of the proposed system

The system flow starts with the user making a contactless communication using his/her NFC enabled device towards the NFC tag; a passive RFID card in which the details of the student is stored and also the reader can also be used in the another context making the user to access to the services on campus.

Firstly, the user initiates the communication between the reader and the card, thereby the information present in the card, i.e.; name and ID details of the student are sensed by the reader (NFC enabled device) and then these are sent to the server or processing unit of the whole institute or organization to prepare a data log and to acquire the access permissions. Here at this point of system flow, the very crucial issue comes to play regarding the security for the data transferred from the reader device to the processing system using wireless networks etc. Here in the proposed system, some of the algorithms and high end cryptographic security systems are used such as secure socket layer protocols in order to present the security aspect and to prevent the data from attackers.

Finally, the student or the staff in that organization gets the access to the services provided and also the records are stored in the data base about the user using the service at that point of time. Later on the records can be cross checked or retrieved if needs and these retrieving access permissions are also limited to the users, staff and the parents. For instance, the student is willing to see his record of attendance this month, and then he/she can log into the system with their data information and see the details. The admin will have full access to the system and can control each and every record up-to-date. Here ends the flow schematic making the system more user friendly in nature.

4. System Design using UML diagrams

4.1 Use Case Diagrams

A use case diagram in the unified modeling language is a form of behavioral diagram shaped from a Use-case analysis. This presents a pictorial overview functionality of the system in terms of actors, their goals and any dependencies between them.

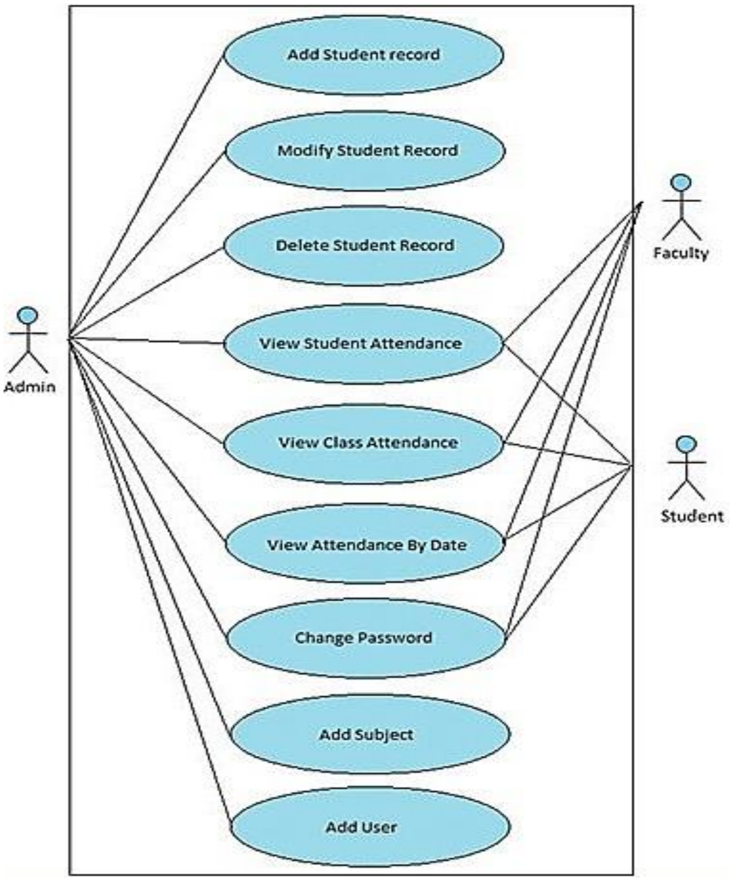


Fig. 5 Use case diagram of the NFC system

4.2. Data Flow Diagram:

The data flow is explained between the staff and the system controller and the students data with the server and thereby the admin data etc.

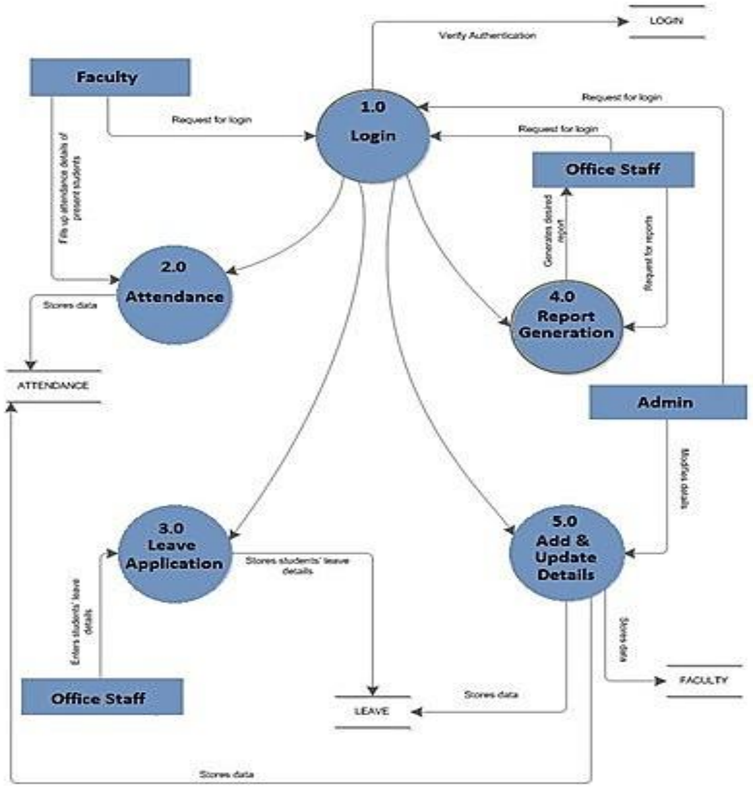


Fig. 6 First level DFD diagram

4.3. Entity Relationship Diagram:

An entity-relationship diagram is a modeling language diagram that creates a graphical representation of the entities, and the relationships between entities, and also creates a clear picture of all the entities involved and each action performed via system.

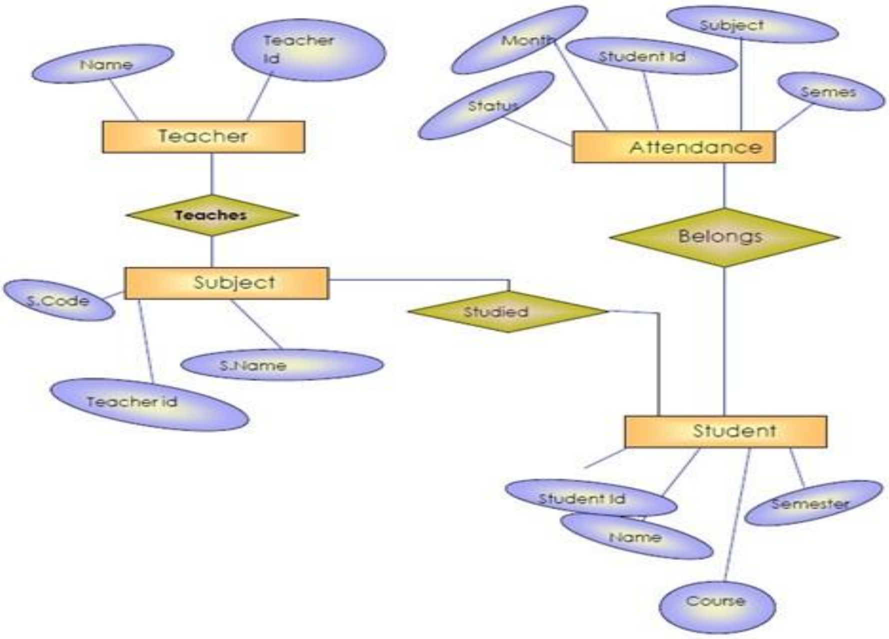


Fig. 7 Entity Relationship Diagram

5. Results and Discussions

1. Stick the TechTile (NFC Tag) to a non-metal surface.

Fig. 8 Samsung NFC tag used in the practical session

2. Enable NFC in the Samsung Galaxy S3 through settings menu.

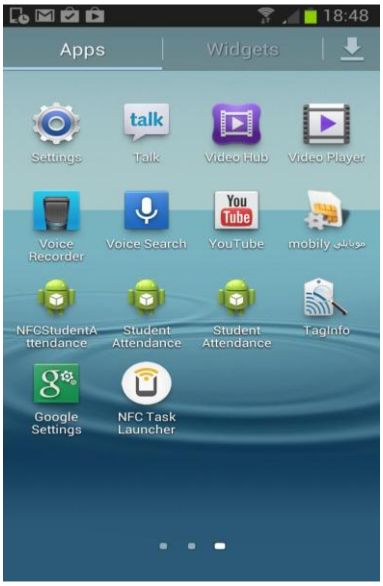


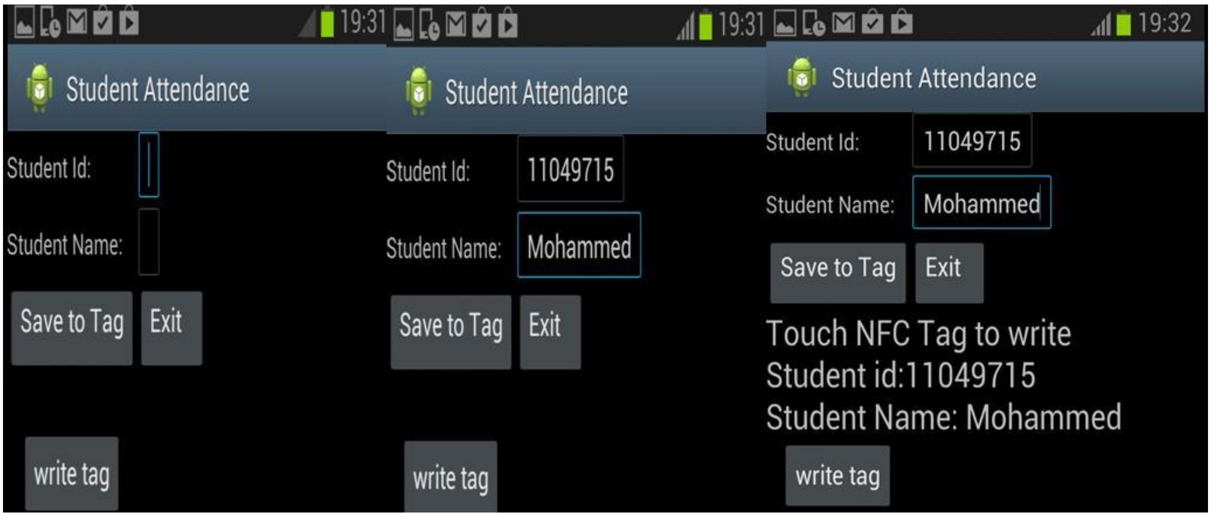
Fig. 9 Screenshot of NFC enabled device with android program apps.

3. Open the NFC writer application:

a. Input Student ID and Student Name

b. Save information temporarily in the memory using button ‘Save to Tag’

c. Tap the tag with the phone and the display should read Message to tag written.



Student Id:
Student Name:

Student Id: 11049715
Student Name: Mohammed

Student Id: 11049715
Student Name: Mohammed

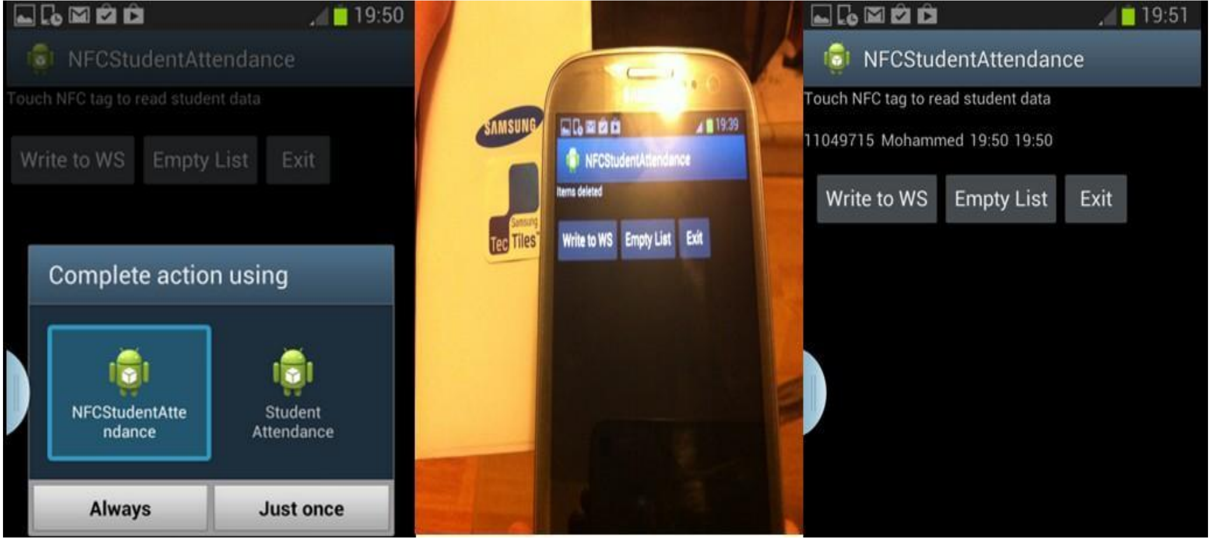
Touch NFC Tag to write
Student id:11049715
Student Name: Mohammed

Fig. 10 Sequence of screenshots showing the tag writing process

4. Open the NFC reader application:

a. Tap the tag with the phone and the display should read the student details of all the students registered in the tag.

b. Delete button may be used to empty the NFC tag and freeing the memory.



Touch NFC tag to read student data

Items deleted

Touch NFC tag to read student data
11049715 Mohammed 19:50 19:50

Fig. 11 Sequence of screenshots showing the tag reading process

6. Conclusion

This “NFC Attendance System using Android” focuses on the elements like the user friendly system which is capable of having the student records in an organization with secured manner. The NFC system used in this project is carried by the virtual android elements like NFC tag and NFC reader as the emulator. This android virtual device enables the system to view the graphical user interface thereby creating the real android device functioning with the NFC tag. The system efficiency and handling costs are also some of the factors that are discussed in the feasibility study; explaining the easy access to the system and cost efficiency in the user’s point of view. Coming to the other very important aspect is the error probability and technical aspects, which are also discussed during the feasibility study; these are the vital features of the system making this NFC system as a user friendly and efficient system. In the results and discussions section, the programming code fragments are executed in the ellipse tool kit and android sdk tool kit to get the output as the practical NFC tag-reader communication is demonstrated in a great way.

References

1. C. Patauner1, H. Witschnig1, D. Rinner2, A. Maier3, E. Merlin1, E. Leitgeb2 “High Speed RFID/NFC at the Frequency of 13.56 MHz”, 1.NXP Semiconductors 2.Institute of Broadband Communications, Graz University of Technology 3.Fachhochschule Technikum K¨arnten
2. Yang, B., & Sun, J. (2011). Near field communication technology. Linkopings Universitet,
3. Cavoukian, A. (2012). Near Field Communications.
4. Haselsteiner, E., & Breitfuß, K. (2006, July). Security in near field communication (NFC). In Workshop on RFID Security RFIDSec.