www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

A Study on Mobile Attendance using Near Field Communication

[1]Mr. Narayana, [2]Prof. B. Sakthivel

[1]PG Student, [2]HOD

Department of Computer Science & Engineering, PSV College of Engineering & Technology, Krishnagiri

Abstract:

A Near Field Communication (NFC) upheld College M-Attendance framework for University Understudies. Close to Field Communication (NFC) is one of the most recent advances in radio correspondences and being a subset of RFID innovation, it is developing at a colossal pace. NFC innovation gives the quickest method to impart between two gadgets and it occurs inside a small amount of a second. It has a few applications in Mobile Communications and exchanges. An NFC-bolstered College M-Attendance framework for University Understudies is examined as one possible utilization of this innovation. The proposed system replaces manual move calls and thus, making it tough to phony. It gives guardians and teachers data about the understudies' participation. The stamping of participation is speedy, unaided, and utilizes a One Time Secret word (OTP) to upgrade the security of the framework and takes away the chance of intermediary participation. This paper talks about NFC as an innovation that is safer and helpful than the predominant innovation of Bluetooth, and furthermore explains on the proposed structure of the M-Attendance framework that makes use of this favorable position that NFC has over different advances.

Keywords: Near Field Communication, RFID, M-Attendance

I. Introduction

Wireless Technology is fast replacing the wired technology. A gain of 128 percent in the shipments of phones equipped with wireless technology rose from 120 million to 275 million in 2013. According to Information Handling Service (IHS), from 2013 through the end of 2018 shipments could grow 325 percent. End users now expect that a single device can be used to access variety of services, such as communication, entertainment and commerce. This has brought huge improvements in the field of contactless technology; NFC being one of them. NFC has many applications including contactless payments usually referred to as NFC

Payments. NFC Payments are being accepted by retailers in developed/developing countries giving an option, that may prove convenient to people. NFC-enabled devices lie in a close proximity.

A. RFID

RFID is a form of wireless communication that uses radio waves to identify and track objects. This system has readers and tags that communicate with each other by radio frequency. An RFID System is made up of three components: Antenna, Transceiver and Transponder (the tag). A signal is transmitted in the form of radio frequency waves using the antenna that activates the transponder. The data is transmitted back to the antenna by the tag when activated. A programmable logical controller is notified of any action that has occurred via the data. This action could represent a work as simple as opening a door or as complicated as interfacing with a database to carry out a monetary transaction. Low-frequency RFID systems have short transmission ranges. High-frequency RFID systems offer longer transmission ranges.

B. Magnetic Induction

In magnetic induction: A small electric current that creates a magnetic field around it is emitted by the reader. Another coil in the client device receives this field and turns it back into electrical impulses for the communication of data. Fig. 1 explains this concept. On activation of NFC, a signal is sent to the NFC chip inside the smartphone. Electricity flows through the circuitry of this chip that generates a magnetic field. At this stage, it is the smartphone that uses power to generate a magnetic field. Due to this a magnetic field is induced in the transponder or a device that does not have its own power supply. This results in the creation of radio field by the transponder that interacts with the electromagnetic field generated by the smartphone.

II. Methodology

NFC is a wireless short-range communication technology based on existing standards of the RFID infrastructure. NFC operates in a short range of four to ten centimeters for communication. For a communication, an NFC device generates a radio frequency in 13.56 MHz spectrum. The principle of magnetic inductive coupling is used to send and receive data within close proximity. NFC supports data rate of 106 Kbps, 212 Kbps and 424 Kbps.

A. Communication Ways

Communication in NFC is either in active mode or passive mode. Active device is the one that generates RF and has its own power supply. The passive device is powered by another active device. Following are the two communication ways:

Two-Way Communication

Devices that are capable of reading and writing to each other. For example, using NFC, you can touch both Android devices together to transfer data like contacts, links, or photos.

One-Way Communication

One-way communication: Reading and writing to an NFC chip is done by a powered device (like a phone, credit card reader, or commuter card terminal). Hence, when a commuter card is tapped on the terminal, money is subtracted from the balance by the NFC-powered terminal.

B. Operating Modes

NFC devices can be in any one of the modes which are reader/writer mode, peer-to-peer mode or card emulation mode. These operating modes are based on ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 standards.

Reader/Writer Mode

In Reader/Writer modern NFC enabled device reads NFC tags like contact less smart cards and RFID tags.[9]. A tag if in close proximity is immediately detected. Once detected, it can either read data from or write data to the detected tag. Important application for this mode is smart posters.

Peer-To-Peer Mode

Two devices that are powered can engage in peer-to-peer mode, that is NFC specific. This mode lets the two devices converse as though networked together

Card Emulation Mode

In Card emulation mode, the NFC device itself acts as a NFC card placing the device in passive communication mode. The smartphone does not generate its own RF field; the NFC reader creates this field instead. The emulated NFC card can then be accessed by an external NFC reader, such as an NFC point-of-sale terminal (POS).

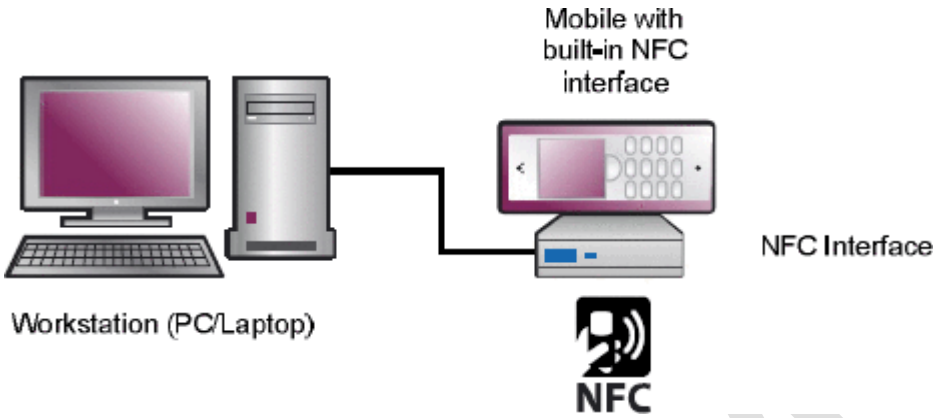

Fig. 1. The physical working environment of the implemented applications

III. Architecture

A. NFC (Forum Specification Architecture)

NFC Forum Specifications is a technology standard that in tunes and extends existing contactless standards unlocking the full potential of NFC technology across the different contactless operating modes as explained above. Refer Fig. 2[24]. The different types of NFC Forum Technical Specifications [11] are explained below:

A. Protocol Technical Specification

Logical Link Control Protocol (LLCP) Specification

OSI layer-2 protocol is designed to support peer-to-peer transmission between two NFC enabled devices in LLCP. The specification defines two service types, connectionless and connection-oriented that is essential for any NFC applications to involve bi-directional communications.

Digital Protocol Specification

NFC-enabled device Communicate, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards. The specification defines the common feature set that can be used consistently and without further modification. The specification covers the digital interface and the half-duplex transmission protocol of the NFC-enabled device in its four roles as Initiator, Target, Reader/Writer and Card Emulator.

Activity Specification

This NFC Digital Protocol Specification can be used to set up the communication protocol with another NFC device or NFC Forum tag. The building blocks called Activities are described here, for setting up the communication protocol.

Simple NFC Data Exchange Format (NDEF) Exchange Protocol (SNEP) Specification

When operating in peer-to-peer mode SNEP lets an application on an NFC-enabled device to exchange NDEF messages with another NFC Forum device.

Analog Specification

Analog characteristics of RF interface of NFC enabled devices are addressed. The main reason of this specification is to describe and specify the distinct features of the externally observable signals for NFC enabled device without having to specify the design of the antenna of an NFC-Enabled Device. Meant to be used by manufacturers for implementation of NFC-enabled device.

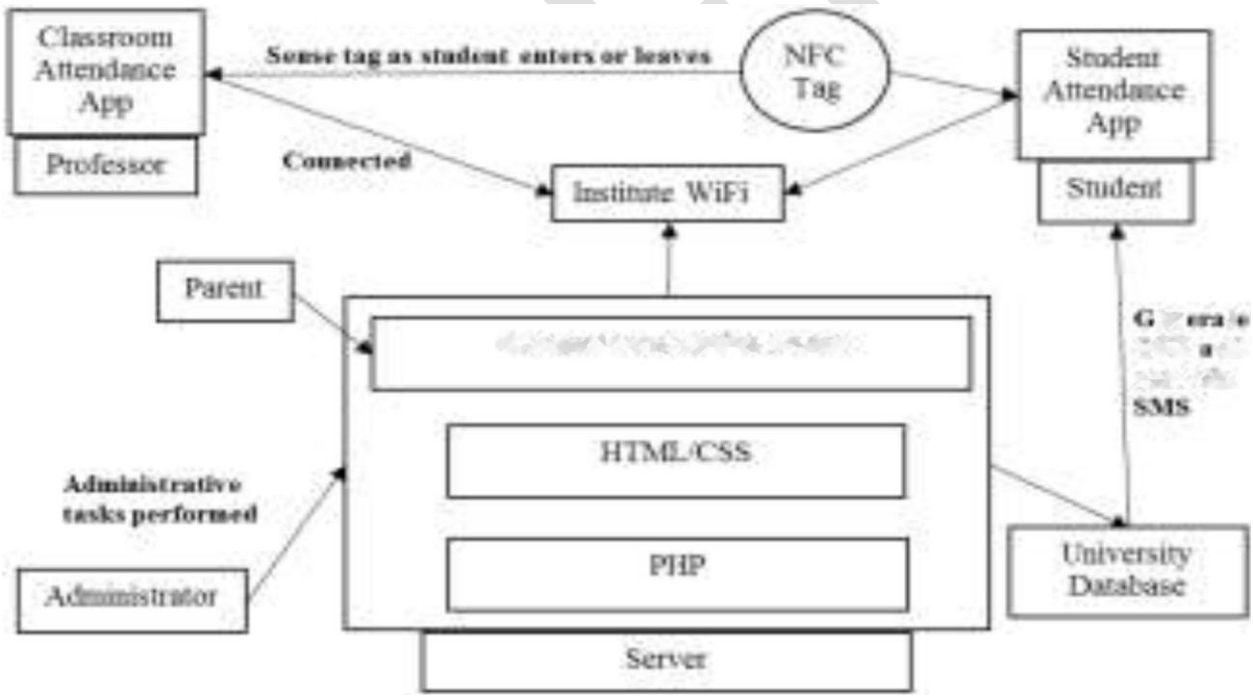

Fig. 2 Architecture Diagram

B. Data Exchange Specification

NFC Data Exchange Format (NDEF) - Specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags.

NFC Forum Tag Type Technical Specification

NFC Tags store a small amount of information for transfer to another NFC device, these are microchips with an antenna. There's a whole set of various data types to can store on an NFC tag. The information stored in NFC tags is stored in a specific data format (NDEF), it can be reliably read by most devices. The amount of data varies depending on the type of NFC tag used - different tags have different memory capacities as explained below:

Record Type Definition Technical Specification

States the format and rules for building standard record types based on NDEF data format that are used by NFC Forum application definitions and third parties.

Connection Handover Specification

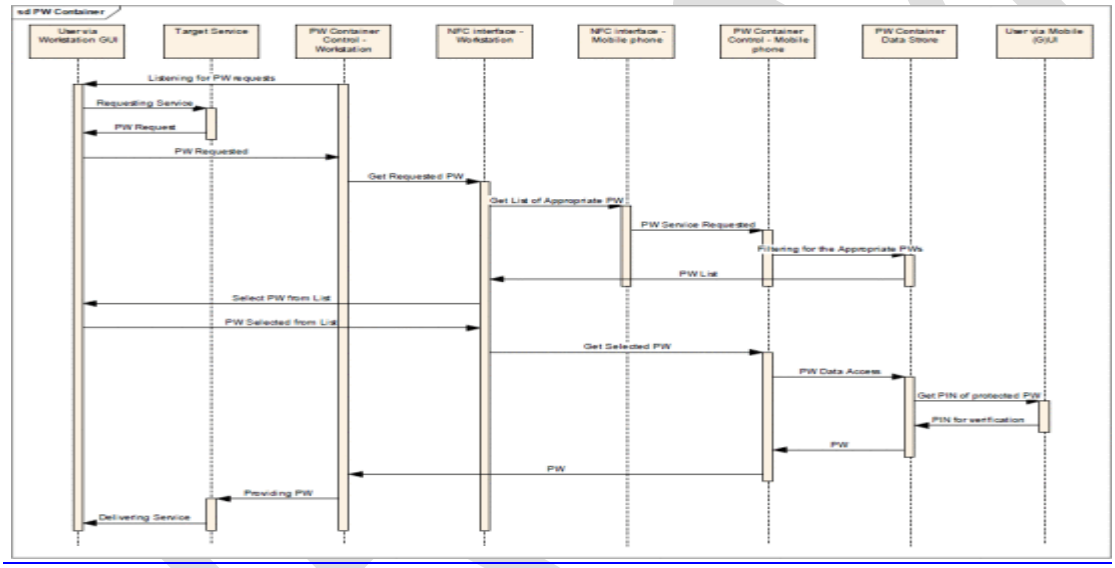

Fig. 3. Data flow diagram: Password Container

It defines the structure and sequence of interactions that enable two NFC-enabled devices to create a connection using other wireless communication technologies. During the negotiation process the connection can switch to the selected carrier between two NFC-enabled devices if the matching wireless capabilities are revealed.

SE

A SE is a tamper proof device, providing a secure storage and execution environment for sensitive data is prepared. It gives both physical and logical protection against attacks, ensuring integrity and confidentiality of its content. SE's are micro controllers that may come in different form factors, such as:

Smart Cards, the chip are embedded in a plastic card that is size of a typical credit card. The card may show physical contacts to transmit with the chip, or the chip may support NFC, in which case the plastic card embeds an antenna. Some cards also support both communication methods.

IV. System and Users

Authentication: Instead of a user name and password, access to an online service may be protected by a strong authentication mechanism, based on credentials stored and processed in a SE. Digital Signature: Applications may use the SE to digitally sign a document or any data with a key stored in this SE. Payment: Online commerce may widely use smart credit cards, or specific payment applications, to enforce the security of online transactions. On mobile telephony environment, the on-card payment application may be hosted on the SIM card, Lightens the need for the user to handle multiple physical devices.

B. Copy Protection and Secure Licensing

This solution is designed to help addressing software and multimedia piracy by providing software publishers with strong copy protection and secure licensing. This use case is a special case of the Password Container application, where the PW Container Control is replaced by a Licence Key Control application.

C. Virtual NFC tag embedded in to applications

The solution allows the content and application providers to put virtual NFC tag information into the application or service. NFC gives the opportunity to implement an intelligent component (plug-in, application extension), that enables the application to place virtual NFC tags on to the web-pages or application GUI, and transfer application data via the NFC data exchange into the mobile device. Later the NFC data can be used and transferred from the mobile device back to any other application. Application areas: ticketing, loyalty, discount, gambling, etc.

D. GPS coordinates in NFC tag

The application helps the users to easily pickup and transfer route information. It supports services where the customer and/or merchant geographical position is relevant. NFC gives the opportunity to implement intelligent navigation data exchange into the NFC enabled mobile devices. This use case is a special case of the Virtual Tag application, where the

Virtual Tag Issuer delivers navigation data to applications. Otherwise, the Virtual Tag data flow applies.

V. Conclusion

NFC is a wireless technology for short range data transmission. It operates in three modes via two types of communication. RFID and magnetic induction are the key factors in implementing NFC. Few forms of implementing this technology is through NFC tags and NFC payment. Through NFC Payments transactions are secure and carried out with just a tap. The SE is responsible for security, authenticity and data confidentiality with respect to payments. Although this technology has its drawback, it is being widely used in the field of payment. The global market of smartphones equipped with this technology is expanding at a fast pace making it popular.

References:

1. K. G. Paterson, and Douglas Stebila, "One-time-password authenticated, key exchange" September 4, 2009.
2. T. Chang-Lung, C. Chun-Jung, and Z. Deng-Jie, "Secure OTP and Biometric Verification Scheme for Mobile Banking", Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, IEEE, 2012.
3. 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. 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. A. Khan, "Preventing Phishing Attacks using One Time Password and User Machine Identification", International Journal of Computer Applications (0975 - 8887), Volume 68- No. 3, April 2013.
5. V. Kostakos and E. O'Neill, "NFC on mobile phones: issues, lessons and future research".
6. K. Preethi, A. Sinha, and Nandini, "Contactless Communication through Near Field Communication, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012, ISSN: 2277 128X.