Mobile Attendance using Near Field Communication and One-Time Password

John Jacob
Computer Engineering Department
MPSTME, NMIMS
Mumbai, India
johnjacob.nmims@gmail.com

Kavya Jha
Computer Engineering Department
MPSTME, NMIMS
Mumbai, India
kavyajha.nmims@gmail.com

Paarth Kotak
Computer Engineering Department
MPSTME, NMIMS
Mumbai, India
paarthkotak.nmims@gmail.com

Shubha Puthran
Assistant Professor
Computer Engineering Department
MPSTME, NMIMS
Mumbai, India
shubha.puthran@nmims.edu

***Abstract*— This paper introduces a Near Field Communication (NFC) supported College M-Attendance system for University Students. Near Field Communication (NFC) is one of the latest technologies in radio communications and being a subset of RFID technology, it is growing at an enormous pace. NFC technology provides the fastest way to communicate between two devices and it happens within a fraction of a second. It has several applications in Mobile Communications and transactions. An NFC-supported College M-Attendance system for University Students is discussed as one potential use of this technology. The proposed framework replaces manual roll calls and hence, making it resilient to forgery. It gives parents and professors information about the students' attendance. The marking of attendance is quick, unsupervised, and makes use of a One Time Password (OTP) to enhance the security of the system and takes away the possibility of proxy attendance. This paper discusses NFC as a technology that is more secure and convenient than the prevalent technology of Bluetooth, and also elaborates on the proposed framework of the M-Attendance system that makes use of this advantage that NFC has over other technologies.**

Keywords—Near Field Communication, One Time Password, and M-Attendance, Bluetooth

I. INTRODUCTION

This paper proposes a Near Field Communication (NFC) and One-Time Password (OTP) supported M-Attendance framework for Universities. Traditionally, professors conduct pupils' attendance, monitoring it at the start of every lecture with manual roll calls or by recording their signatures on a piece of paper which, later, they use to manually enter the attendance in the backend system. This routine requires time and effort, compromising on the teaching time. In addition to this, some students take advantage of the low-security attendance system and mark the attendance of the students who aren't present in the lectures, i.e., proxy cases. The proposed school attendance supervision system has been designed to simplify and optimize attendance monitoring. It replaces the traditional attendance-marking system and makes it faster, more secure and completely digital.

Elakiyaselvi [1] provides us with the framework of implementing an Android application using NFC. NFC is a short-range and high frequency wireless communication technology that enables the exchange of data between devices within a range of 10 cm from each other. It is an upgrade of the existing proximity card standard (RFID) that combines the interface of a smartcard and a reader into a single device. It allows users to seamlessly share content between digital devices. Shorter set-up time is a big advantage that NFC has on its side. Instead of performing manual configurations to identify devices, the connection between two NFC devices is established at once (under 1/10 a second). Due to this short range, NFC provides a higher degree of security than Bluetooth and makes NFC suitable for crowded areas where correlating a signal with its transmitting physical device might otherwise prove impossible. NFC can also work when one of the devices is not powered by a battery (e.g. on a phone that may be turned off, a contactless smart credit card, etc.).

A one-time password (OTP) is a password that is valid for only one login session or transaction, on any digital device. OTPs avoid a number of shortcomings that are associated with the traditional password based authentication systems. [2] The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. OTP systems also aim to ensure that a session cannot be easily intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus, reducing the attack surface further.