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.

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

A. Abbreviations and Acronyms

TABLE I. ABBREVIATIONS AND DESCRIPTION

Abbreviation	Description
NFC	Near Field Communication
OTP	One Time Password
RF	Radio Frequency
SMS	Short Message Service
RFID	Radio-Frequency Identification

II. RELATED WORK

In the last decades we have witnessed an enormous increase in the end user acceptance of mobile communications. The appearance of mobile platforms based on the open source software has rapidly increased the interest into mobile applications development. [3] Shanbhag discusses Mobile Based Attendance Marking System Using Android and Biometrics. Android mobile phone application development is based on an open source software and open source development environment. For achieving portability, they aimed to have wireless communication of the biometric scanner with the server. Development of software should be more real, user friendly, compatible with system and cost effective. The use of software by user must be simple and should not require much training to use software. Their system primarily focuses on building an efficient and user friendly Android mobile application for an Attendance Monitoring. The application will be installed on the professor's phone as well as student's phone which runs android OS. It intends to provide an interface to the professor who will require minimal details to input for marking of attendance of a particular class of students. Apart from that, the application would support strong user authentication and quick transmission of data. Another noticeable feature of the entire application is to give options to the user such as feedback provision, attendance retrieval in a very convenient way, messaging between user and professor and campus notifications like low attendance reminder, lecture amendments to name a few. The application thus build would also help to avoid the chance of a proxy as the system has biometric scanning which will serve the purpose of authentication

Near Field Communication allows for simplified transactions, data exchange, and wireless connections between two devices in proximity to each other, usually by no more than a few centimeters. [4] NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity. Simple tags offer just read and write semantics, sometimes with one- time-programmable areas to make the card read-only. More complex Tags offer math operation and have cryptographic hardware to authenticate access to a sector.

NFC and Bluetooth were compared and fastest connection can be established with the help of NFC. It takes only <0.2 second for setting up a connection. [5] Benefits of Android OS over iOS were also studied and android being Open Source was concluded to be better for the implementation of the system. Android Application framework enabling reuse and replacement of components, Dalvik virtual machine optimized for mobile devices, Integrated browser based on the open source WebKit engine, Optimized graphics powered by a custom 2D graphics library; 3D graphics based on the OpenGL ES 1.0 specification SQLite for structured data storage, Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF), rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE were the major advantages.

Further they describe the Learning system which is implemented using mobile equipment that can be used either by the student or the teacher. The Mobile Equipment has the DIAD NFC framework installed on it along with the student or teacher application. The teacher uses the mobile equipment for taking attendance, editing mark and maintaining curriculum. The students' mobile equipment to register their presence in particular place. An attendance module consist three separate functions; they are mobile attendance, mobile mark editor and mobile curriculum. This three let to ease the work of teachers.

From mobile attendance they can take attendance and can be update to sever at the moment. It avoids the malfunction in attendance system. Mobile Mark Editor also has the same function as mobile attendance. It saves the mark details of the student and saved in server. Mobile curriculum which is developed to maintain course plan and teaching plan in mobile. A gamified Activity module is also implemented and in this part gamified activity is implemented and this also used for registering the attendance. NFC reader or smart poster will be used for this. This smart poster or NFC reader should be placed the specified place. When the student wave their NFC enabled mobile or tablet in-front of the poster connection will be created and data exchange will be started in single click. Poster confirms the student verification and points will be given for their presence. These points will be saved in sever and at the end of the semester or the year lead scorer will be awarded. This framework will encourages student to take part particular activity.

III. TECHNOLOGY USED

A. *Near-Field Communication*

a. *Summary and Applications*

NFC is a wireless communication interface [6]. It has various working distances and the maximum working distance is limited to approximately 10 cm. There are various modes in which NFC can operate. These modes are distinguished based

on whether a device creates its own RF field or whether a device retrieves the power from the RF field generated by another device. If the device generates its own field, then it is called an active device. Otherwise, it is called a passive device. Active devices usually have a power supply; passive devices don't (e.g. contactless Smart Card). There are various configurations possible for communication as shown in Table II.

TABLE II. COMMUNICATION CONFIGURATIONS

Device A	Device B	Description
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF filed is generated by Device B only

NFC finds its usage in various areas of life, some of them mentioned as follows:

- Public transportation: NFC tags and cards allow you to pay with the tap of your phone. It comes under the umbrella of Mobile Payments with NFC being the enabling technology for the payments. It removes the need to buy tickets and stand in queues.
- Ticketing: Any kind of ticketing can be done through NFC enabled devices or tags. Concerts, conferences, sporting events, theme parks, checking into a flight and boarding.
- Keys: NFC Technology in your phone or a small NFC tag can replace your keychain. It could help one tap their way into apartments, offices or hotel rooms. They could also be used as keys to vehicles and automobiles.
- Comparison-shopping: This could be done with barcode scanning but NFC makes the whole process faster. Whether you are doing groceries, buying clothes or getting something from the local electronics store, with a wave of your phone you could have access to reviews, additional product information, or prices from other stores.
- Check-ins and venue reviews: You can check-in to a location just by waving your NFC Enabled Mobile device at the location. In addition you can easily rate places or read reviews so you have an idea what the place offers before going in. In this research paper we explain how students can use it to mark Attendance in Classrooms.

b. Comparison of NFC with Bluetooth

In this paper, we have also elaborated on the technical differences between NFC and Bluetooth and why we chose NFC over Bluetooth for our M-Attendance framework.

To start with, Bluetooth works on short-wavelength radio waves in the ISM band from 2.4 to 2.485 GHz. NFC, too, works on radio waves, but the range on NFC is limited to 20 cm. Also, NFC is designed for limited data transfer (maximum of 424 Kb/s) and a quick handshake, of about 0.1 second. Power consumption in an NFC-enabled communication is very less as compared to that in a Bluetooth-enabled communication. There is no pairing required in NFC-based transactions, which saves a lot of time, whereas pairing is imperative in Bluetooth-based transactions. Data transfer in NFC is much faster than in Bluetooth, NFC being easier and more convenient to use. The parameters where Bluetooth overpowers NFC is the cost-effectiveness and Multi-device connectivity, Bluetooth being cheaper than NFC and Bluetooth being capable of connecting up to 8 devices at the same time where NFC being capable of connecting a maximum of 2 devices concurrently.

NFC transmits data across much smaller distances, typically between 4 and 10 centimeters, compared to Bluetooth's 10-meter range, or in the case of some RFID implementations even kilometers. [7] This by-design limitation reduces the likelihood of unwanted interception and makes NFC particularly suitable for crowded areas where correlating a signal with its transmitting physical device becomes difficult. Its short-range nature may significantly reduce the risk of eavesdropping but that alone does not guarantee secure communications.

Another differentiating factor is that NFC sets up connections faster than standard Bluetooth and its low-power variant, Bluetooth 3.0. Instead of performing manual configurations to identify devices, the connection between two NFC devices is automatically established quickly in less than a tenth of a second. In fact, NFC could even be used to speed up the process of pairing two Bluetooth devices, acting as an initiator by simply bringing them close to each other. Lastly, their data throughput capacity makes them fit for different applications. NFC operates within the globally available and unlicensed radio frequency ISM band of 13.56 MHz and can go up to a maximum data rate of 424Kb/s, whereas Bluetooth operates in the 2.4GHz frequency and can reach maximum data rate of 2.1Mb/s. These properties make NFC the suitable choice for a Mobile Attendance system over Bluetooth.

c. Shortcomings of NFC

Whenever radio frequencies are involved, there's a potential security risk. It could be possible for an unscrupulous person to eavesdrop on communications between NFC devices. With the right antenna, hardware and software, it's possible to snoop on transactions. Even though NFC transmissions must take place over very short ranges (with the maximum distance of transmission being 10 centimeters), it is possible to pick up transmissions from much further away. Defining exactly how far away an eavesdropper can be isn't easy. It relies on several factors, including whether the information is being sent in active or passive mode, the type of antenna and receiver the eavesdropper is using and how much power the active

component pours into the transmission. It's possible that someone trying to listen in on an active component could get a signal as far away as 10 meters.

[6] Another potential problem with NFC is that someone could attempt to disrupt communications by broadcasting radio signals in the NFC spectrum during transactions. While this isn't the same as eavesdropping, it could be a source of disruption.

B. *One-Time Password*

a. *Summary*

A One-Time Password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates the user for a single transaction or session.

[8] An OTP is more secure than a fixed password, especially a user-created password, which might get prone to attacks after a certain period of time. OTPs may replace authentication login information or may be used in addition to it, to add another layer of security. OTPs can either be time-synchronized or be based on mathematical algorithms, time-synchronized OTPs being the more famous type.

For time-synchronized OTPs, the tokens are usually pocket-size fobs with a small screen that displays a number. The number changes every 30 or 60 seconds, depending on how the token is configured. [9] For two-factor authentication, the user enters his user ID, PIN and the OTP to access the system.

A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement.

b. *Shortcomings of OTP*

Although most SMS text messages are transmitted in seconds, it is common to find them delayed when networks are congested. SMS traffic is not sent point to point; it is queued and then sent on to the required network cell where it is again queued and finally sent to the end user's phone. Irrespective of delay to delivery or non-usage of the SMS OTP, each and every SMS OTP will be charged.

OTP over text messaging may be encrypted using an A5/x standard, which several hacking groups report can be successfully decrypted within minutes or seconds or the OTP over SMS might not be encrypted by one's service-provider at all. [10] In addition to threats from hackers, the mobile phone operator becomes part of the trust chain. In the case of roaming, more than a single mobile phone operator has to be trusted. Anyone using this information may mount a man-in-the-middle attack.

IV. SYSTEM AND USERS

The M-Attendance system is setup for use in classrooms. Each Professor and Student can use their NFC enabled Mobile devices to mark attendance and the Admin carries out the necessary maintenance and upkeep of the system as a whole. The main components of the system are Android Devices, Student NFC Tags and a Web Portal to view and carry out various other activities for Admin, Professors and Students. The users of the system and their functions are explained as follows:

- Administrator: Administrator (Admin) has complete control on the application and is responsible for governing vital functionalities in the application. The admin role is mainly in the web interface.

TABLE III. RIGHTS BESTOWED ON THE ADMINISTRATOR

Rights	Description
Registration of Teachers and Parents	Creating entries for the teachers and parents in the application
Registration of Students	Each student studying a course needs to be added into the system by the admin. The Students will be given a registration number or a username equivalent. Once a student is enrolled, he can start using the system. The Students use the Android Application primarily.
Display Notices and Add Events	Any Event that needs to be added can be done by the admin through the web module.
Take Backup	Regular Periodic backup of the system needs to be taken and this can be performed by the admin.
Attendance Marking	The android mobile phone acts as an attendance machine in our application. It is using this mobile through which the student will be marked in the class. The teacher will have the NFC enabled mobile phone on which he/she will run the application. On successful validation, the teacher would trigger the feature of Start attendance. It is during this phase that students need to come forward to mark their attendance.
Student Verification	The student needs to place his NFC tag near the mobile phone. The application retrieves the information saved in the tag and verifies the student.
Attendance Confirmation	On successful validation of the student, the application marks the attendance of the student in the application. This attendance is mark on the central server. Likewise, notification is also sent to the parents of the students for their reckoning.
Managing the Web Module	Using this module, the parents can see the attendance of their children in the application. They can view the attendance of their children through one single interface. Using this Web Analytics module, the parents can compare the attendance of their children with other students in the class or the average attendance.

- Professor: Each Professor will have multiple courses assigned to him/her. The professor uses the NFC-enabled device to take the attendance. The web portal can be used to add notes and notices.

TABLE IV. RIGHTS BESTOWED ON THE PROFESSOR

Rights	Description
Add Notes	Study Material, Presentations and Documents.
Add Notices	Any message/Notice to be conveyed is broadcasted.

- Parents: The students' parents can see the attendance of their children in the application and on the web portal.

- Students: The students can view their attendance, download notes uploaded on the web portal and on the Android application.

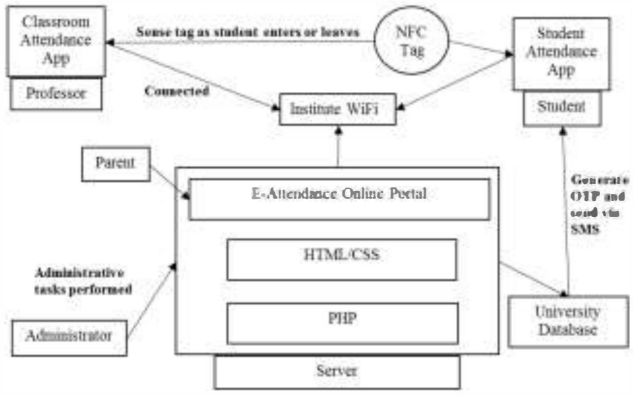

Fig. 1. System Diagram

V. METHODOLOGY

The proposed procedure for this system is explained in the following steps.

Step 1: Student walks into class with his NFC Tag/ID Card with NFC Tag.

Step 2: Teacher sets Attendance Application, selects Lecture and Time and starts M-Attendance.

Step 3: Students' Tag is detected and his ID is added to queue as soon as he walks into the class and taps his phone/NFC tag to the teacher's phone or a classroom phone. (He is still considered absent at this stage. His Tag ID is recognized but his identity needs to be verified.)

Step 4: Student runs the student application and verifies his Tag and receives OTP as SMS on his registered Mobile Number.

Step 5: Student Enters OTP through college Wi-Fi and verifies his Identity and Presence in class. Attendance Status changed to 'O', i.e., Verified State. Attendance is not yet marked Present.

Step 6: After the lecture is done, teacher ends class on the Attendance Application.

Step 7: As students leave, their tags are detected again and their attendance is marked 'P' i.e. Present. This ensures that students who leave in between lectures do not get marked Present.

VI. SECURITY FEATURES

The server in this system is the XAMPP server with PHP at its back-end. XAMPP needs to be configured to port number 80 so that the Apache server is able to receive requests from the localhost URL. The PHP code along with the SQL DDL command need to be added inside the htdocs folder. The exact location is "C:\xampp\htdocs". The back-end database should be intranet because admins located in the premises should be able to access the database as there is confidential information at stake. [11] Once the Tag ID is detected when student enters the class, the server is responsible for generating a random four digit number as OTP. As this number is a 4 digit random number, there is no way it could be guessed. It also generates a different random number each time ensuring that the OTP or PIN cannot be reused, memorized or misused. [12] The system sends the OTP as an SMS to the students registered Mobile Number or through college Wi-Fi in case there is no network. Once this OTP is entered by the student, he needs to be connected to college Wi-Fi to submit the OTP after tapping their tag on the student device. This extra measure ensures that students who are at home or outside the class won't be able to verify the OTP through their Student Application as their devices need to be connected to the institutions Wi-Fi and Tag needs to be inside Class. Those who have verified the OTP have also verified their presence in class as the device is connected to the Local Wi-Fi Network. The OTP method was proposed in order to make the system fool proof and prevent proxies.

[13] What makes the system more secure is the OTP verification that takes place. Consider the student has swiped his tag against the sensor device and receives his OTP, there comes a scenario where if a student sends his tag with a colleague and forwards the SMS he received containing the OTP from home. Now the colleague can enter the OTP within the expiry time and the proxy attendance is marked. Therefore, to counter this, a feature was introduced which allowed OTP verification only when the Tag is in proximity of the students own mobile phone. This is possible because each student logs into the app on his/her device using their own credentials only. Hence, when we bring the Tag in proximity of the device the application recognizes that the tag number and credentials belong to the same person, hence the dual- verification takes place. Attendance is logged into the database as soon as the lecture ends.

VII. Conclusion

Traditional Attendance Systems tend to be insecure due to lack of verification. In the proposed system, we leverage the benefits of using NFC (Near Field Communication) tags and OTP for verification of student identity and registration of attendance in a fool proof manner. Each student's NFC tag will be used along with his Mobile Device which would be used for automating the process of marking attendance.

In the future, this framework could be supported on various Operating Systems, and various software environments. Also, Biometrics could be incorporated in the proposed framework to ensure more security.

Acknowledgment

For this study, we would like to thank our mentor, Professor Shubha Puthran, who has guided and encouraged us to take this research study up and has helped us overcome the difficulties that we faced during implementation. We would like to thank her for her positive and encouraging feedback. We would also like to thank our families for their continuous support and faith in us.

References

[1] P Elakiyaselvi, "A framework for implementing M-Attendance system using near field communication in android OS", *Int. J. Computer Technology & Applications, Vol 3 (2).*

[2] M. Viju Prakash, P. Alwin Infant, and S. Jeya Shobana, "Eliminating Vulnerable Attacks Using One-Time Password and Pass Text – Analytical Study of Blended Schema", *Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, ISSN: 2219-2158, November 2010.*

[3] G. Shanbhag, H. Jivani, and S. Shahi, *"*Mobile Based Attendance Marking System using Android and Biometrics", *IJIRST–International Journal for Innovative Research in Science & Technology, Vol. 1, Issue 1, ISSN: 2349-6010, June 2014.*

[4] W. Yi, W. Jia, and J. Saniie, "Mobile Sensor Data Collector using Android Smartphone", *Circuits and Systems (MWSCAS), 2012 IEEE 55th International Midwest Symposium, IEEE, August 2012.*

[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.*

[7] B. Özdenizci, M. Aydin, V. Coşkun, and K. OK, "NFC Research Framework: A Literature Review and Future Research Directions", *14th IBIMA Conference, June 2010.*

[8] E. Haselsteiner and K. Breitfuß, "Security in Near Field Communication (NFC) Strengths and Weaknesses".

[9] K. G. Paterson, and Douglas Stebila, "One-time-password-authenticated key exchange" *September 4, 2009.*

[10] 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.*

[11] 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.*

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

[13] A. 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.*