A Robust Student Attendance Monitoring System using NFC Technology and Biometrics

Sanjana Ekbote
Department of Information Technology
SSN College of Engineering
Chennai, India
sanjanaekbote@gmail.com

Valarmathi P
Department of Information Technology
SSN College of Engineering
Chennai, India
valarmathi414@gmail.com

Abstract**—**In most of the colleges across the globe, an efficient and authenticated attendance monitoring system for students has not been developed yet. In this paper, we are proposing a non-intrusive system wherein students can record their attendance by providing their fingerprint while they are seated in their places. This system makes use of NFC enabled smart phones, NFC tags, a biometric fingerprint scanner App and Wi-Fi for storing the attendance online. It provides authentication of students and security of data. Secure session is maintained by NFC tags using encryption. The lecture time can be saved since no manual attendance is required.

Keywords- *NFC enabled smartphone; NFC tags; Biometric; Fingerprint; Session.*

*****

I. Introduction

Due to globalization and easy availability of almost all information on the internet these days, students are less motivated to come to the lecture rooms or laboratory. There is often a clear co-relation between student's attendance and overall academic performance. Moreover, attending classes greatly contributes to a personally and professionally beneficial experience. This demands for an equally important attendance monitoring system, one where records are managed with ease and accuracy as well as removing the communication gap between college authorities and parents.

Various types of modern attendance monitoring systems are available in the market - using smartcards, RFID tags on ID cards and biometric scanners.The most traditional way and commonly practiced method of taking attendance till date is the roll call method. In this, the teacher maintains a physical attendance register and calls out roll numbers or names of the students. This method has several flaws such as, (a) High probability of giving proxies (b) Consumes the lecture time (c) Manual entry of attendance into the computer (d) Prone to human errors (e) Risk of losing the attendance register, etc. Fixing scanners in class rooms will require students to move from their respective places, which might disturb the flow of the lecture. These issues can be overcome using this system in the following ways:

- The input is the student's fingerprint, hence proxies can't be given
- Lecture time in taking attendance manually is saved
- Attendance is automatically stored in the database.
- Manual entry into the computer is not needed.
- Sessions is maintained by the NFC tag so that attendance can be recorded only during the particular class hour
- Free from human errors.
- Backup is maintained and monthly reports can be generated.

This system is based on NFC technology [1] with MIFARE DESFire EV1 and biometrics [2].

Near Field Communication (NFC) is a standard for very short range (10cm) radio transmission. It allows communication between two active devices or between on active and passive device. Now a days, many mobile consumer electronics like mobile phones, PDAs etc are coming with NFC reader/writer. In a few years time, almost all the hand held devices will have NFC functionality. This paper addresses the scenario in future.NFC tags are cheap and easily available.

Authentication of the student is done using finger print scan. Online comparison of fingerprint is done in the server.

II. PRE-REQUISITES FOR THIS SYSTEM

- The college must allow the teachers and students to carry cell phones to class.
- The college must have WIFI connectivity and must have a concurrent server that can handle 2000-5000 clients concurrently.
- At the beginning of the semester, the fingerprints of each student's left and right index fingers' fingerprint must be stored in the database of the server.
- The teachers and students must possess NFC enabled Smartphones.
- Every teacher must have a unique id and password stored in the server.

- There must be a specific link to the database of each subject and for each class that is accessible by the subject teacher. These links must be stored in all the NFC tags for a particular class.
- Subject-wise NFC tags must be stuck near the classroom's entrance. It must be coded such that it authenticates the subject teacher and switches the link "on/off" to receive data.
- NFC tags must be stuck on the benches(for students).They must be coded such that the fingerprint data is sent to the server for online matching in the server with whichever database link is active or "on" for that particular session.
- Server data must be accessible only to the Admin and must be protected by one time passwords.

III. SYSTEM FLOW DIAGRAM

Step 1**:** The Teacher enters the classroom with his/her NFC enabled Smartphone
Step 2: The Mobile Application will log in with teacher's ID(we can map the subject based on teacher log-in).Now the teacher "taps" on the tag of his/her subject to "open" the link to attendance database(See Figure 1(a))
Step 3: Students put their fingerprint on the Mobile App of their own phones and "tap" the phone on the tags stuck on their benches to record attendance (See Figure 1(b)). Online fingerprint comparison is done in the server (See Figure 1(c)).
Step 4: At the end of the class, teacher taps on the subjects tag to "close" the link. By then, the attendance is uploaded to server with a unique session key and time stamp (See Figure 1(d)).

Teacher's Smartphone

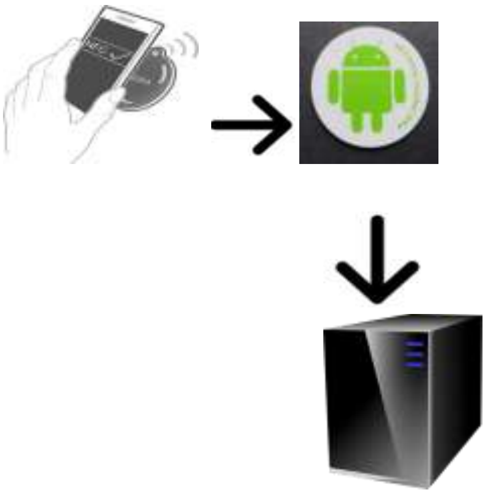


Figure 1(a). Proposed Design of the System (Teacher's end)

Student's Smartphone

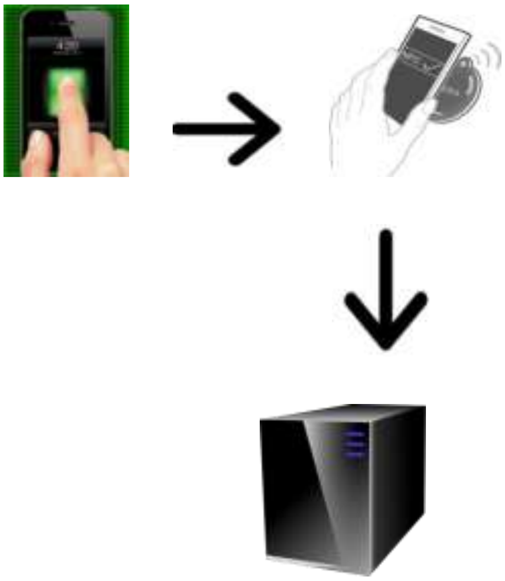


Figure 1(b). Proposed Design of the System (Student's end)

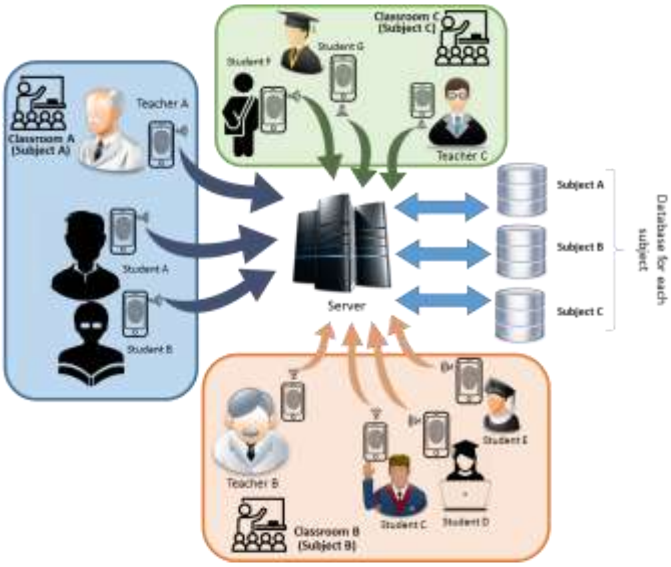


Figure 1(c) Overall functioning of the System

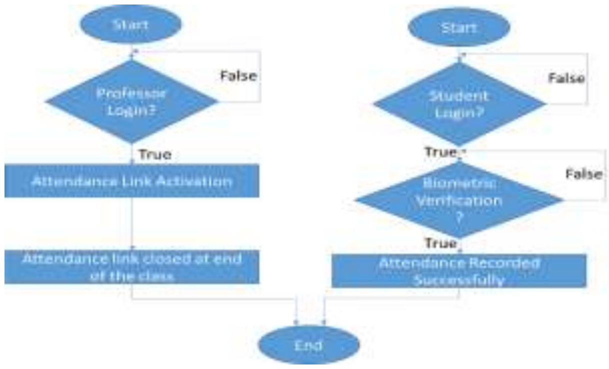

Start
Professor Login?
False
True
Attendance Link Activation
Attendance link closed at end of the class
Start
Student Login?
False
True
Biometric Verification ?
False
True
Attendance Recorded Successfully
End

Figure 1(d)Flow chart of the System

IV. EXPERIMENTAL SETUP

In this system, three parties involved are the subject teacher, the student and the server. For the system to work continuously, the server is running during the college time. The sequences of activities are as follows

A. Teacher

The teacher switches on her dedicated link to a particular class for a particular subject by tapping on the NFC tag attached near the entrance of the classroom. The teacher turns it off when the class is over.

B. Student

The student opens the fingerprint scanner App on his/her Smartphone and applies impression on his finger. After it is scanned, he/she taps on the NFC tag attached on the bench. Now the fingerprint goes to the server for verification.

C. Server

The server verifies the fingerprints of the students by looking into the database of only the active link for a particular session. The link which the teacher opens and the link through which the student sends the fingerprint is the same. So it looks for a match only in the database which has the current link. The server must be able to handle multiple requests concurrently and must give accurate results.

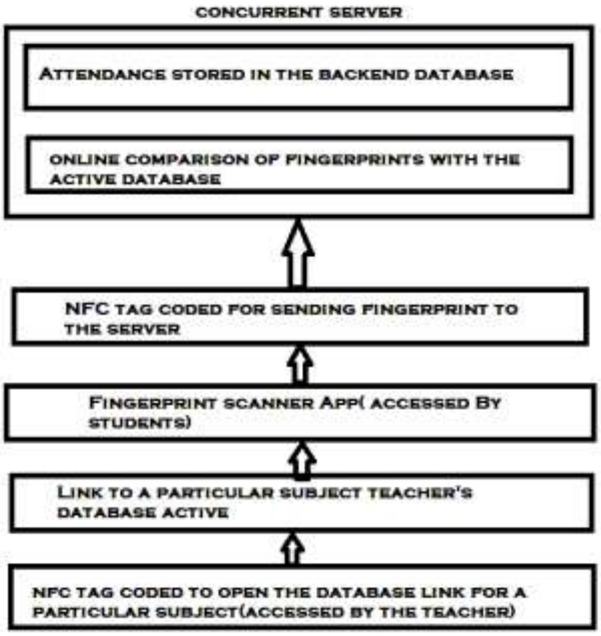

CONCURRENT SERVER
ATTENDANCE STORED IN THE BACKEND DATABASE
ONLINE COMPARISON OF FINGERPRINTS WITH THE ACTIVE DATABASE
NFC TAG CODED FOR SENDING FINGERPRINT TO THE SERVER
FINGERPRINT SCANNER APP(ACCESSED BY STUDENTS)
LINK TO A PARTICULAR SUBJECT TEACHER'S DATABASE ACTIVE
NFC TAG CODED TO OPEN THE DATABASE LINK FOR A PARTICULAR SUBJECT(ACCESSED BY THE TEACHER)

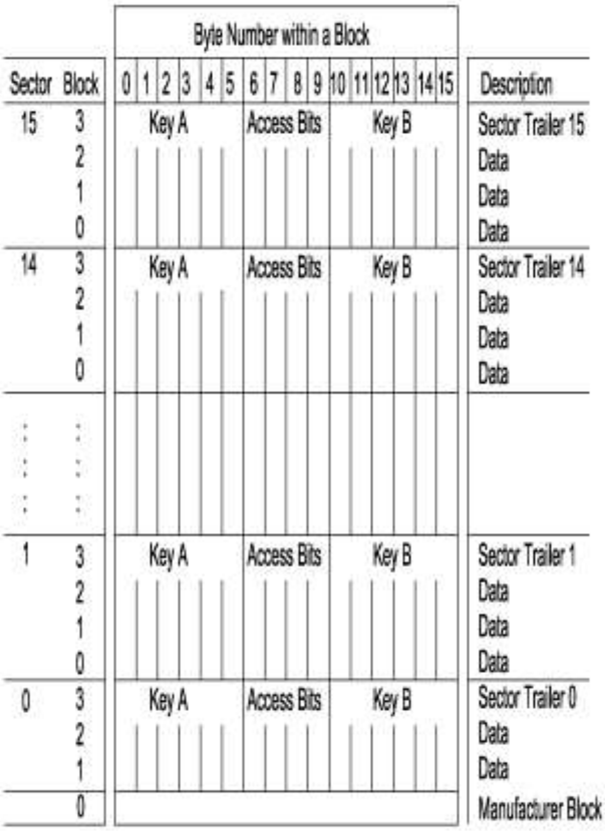
Figure 2. Process Flow Diagram of the concurrent server

If the fingerprint is verified, the server sends the message “Attendance Recorded Successfully” and maps it to the backend database for future reference (See Figure 2). This can be viewed or changed only by the system administrator.

D. Processes

The NFC target/passive tag for each subject teacher is stuck near the entrance i.e. on the wall beside the door. The teacher carries an NFC enabled smart phone/smart device and taps it on his/her NFC sticker. This on tap makes the link for that database active for that session. Now the database is ready to receive attendance entries. A session’s key is generated.

This NFC tag is the “master “tag as it has control over the whole session. There is a mobile application for authenticating fingerprints. The students use their NFC enabled Smartphone to put his/her finger on the screen. Since it is a capacitive screen, only touch of the finger can be taken as input. This is sent to the server via the active database link. If the match is successful, authentication is done. Now the attendance is recorded into the current database link and the student is notified by a “success” message. After leaving the class, the teacher again taps her phone on the same tag to “switch off” the link/session. Here, the readers memory is used only for authentication, the attendance recording doesn`t need memory on the smart phone/ smart device as it is getting stored in the link directly (See Figure 3 and Table 1). A separate link is given for different subjects. If a teacher teaches say, subject A to one class and subject B to another class, a different link must be given to different classes as databases are different. i.e., student names are different. The reader automatically detects which link the attendance must go into on tapping.



		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 3.Organisation of blocks in the NFC tag

TABLE I. NFC tag and its Blocks after assigning Links to different subjects

Sector	Block-2	Block-1	Block-0
Sector-1	Teacher(1) details	Subject (a)details	Last Class Attendance Status
Sector-2	Teacher(2) details	Subject (b)details	Last Class Attendance Status
Sector-3	Teacher(3) details	Subject (c)details	Last Class Attendance Status
Sector-4	Teacher(4) details	Subject (d)details	Last Class Attendance Status
Sector-5	Teacher(5) details	Subject (e)details	Last Class Attendance Status

V. SCALABLITY

Production of cell phones equipped with Near Field Communication (NFC) will expand by nearly a factor of 10 from 2013 to 2017, reaching 1.2 billion units as the majority of Smartphone makers are increasingly adopting the wireless communications technology in their products as a de facto standard [9].The server must be able to handle an average of 2000 to 5000 requests for comparison of fingerprints concurrently. The concurrency of the server can be scaled up or down depending on the strength of the college. Since NFC tags are cheap, they can be used in large numbers. They can be coded using Java or C language. It can be coded using the Smartphone itself.

VI. CONCLUSION AND FUTURE WORK

This proposed system might play vital role in the future educational institutions, as technology becomes more than a part in a human's life. This system makes the attendance taking process and the maintenance easier. A smarter report can be generated based on the requirements. This system also discourages the proxies given during the attendance entry and reduces the manual mistakes and saves time, which is very essential. Though, it has many merits, this system must take care of some security issues such as spoofing attacks, stealing of data, scanner sensitivity, support for 360 degree data input, SQL injection of main database. These security issues can be handled and resolved by adapting suitable techniques in the future.

ACKNOWLEDGMENT

The authors would like to thank Poornima.S and Sivamurgan.V of SSN College of Engineering, Chennai (India) for their helpful suggestions.

REFERENCES

[1] International Organization for Standardization (ISO).ISO/IEC 18092: Information technology-Telecommunications and information exchange between systems-Near Field Communication-Interface and Protocol, April, 2004.

[2] M.Feldhofer,S.Dominikus, and J.Wolkerstorfer.Strong Authentication for RFID Systems using AES Algorithm.In M.Joyce and J.-J Quisquater, editors, *Cryptographic Hardware and Embedded Systems-CHES 2004,6th International Workshop, Cambrige, MA, USA, August 11-13,2004,Proceedings* ,volume 3156 of *Lecture Notes in Computer Science*, pages 357-370.Springer,August 2004.

[3] National Institute of Standards and Technology(NIST).FIPS-197:Advanced Encryption Standard, November 2001.Available online at hhttp://www.itl.nist.gov/fipspubs

[4] Manfred Aigner, Sandra Dominikus and Martin Felhofer, "A System of Secure Virtual Coupons Using NFC Technology", *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops,2007*

[5] Anil K. Jain, Arun Ross and Salil Prabhakar" An Introduction to Biometric Recognition" *Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.*

[6] How NFC Works Available at[3] National Institute of Standards and Technology(NIST).FIPS-197:Advanced Encryption Standard, November 2001.Available online at hhttp://www.itl.nist.gov/fipspubs

[7] NFC and RFID differences Available at http://www.differencebetween.net/technology/difference-between-rfid-and-nfc/

[8] http://electronics.howstuffworks.com/difference-between-rfid-and-nfc.htmhttp://www.differencebetween.com/difference-between-rfid-and-vs-nfc/

[9] About Mifare cards specs Available at http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/