A Secure Near Field Communication (NFC)-enabled Attendance on Android Mobile for Higher Education

David Ong Da Wei, and Manmeet Mahinderjit Singh
Universiti Sains Malaysia, Malaysi, dodwei.dev@gmail.com; manmeet@usm.my

ABSTRACT

Today, many universities evaluate the performance of students in a semester based on the student's attendance to class to make sure that they do not miss out any important class. This lead to taking attendance system is an important issue in universities. In this work, a sensor based attendance system is proposed. This approach adopts sensing technology, which is Near Field Communication (NFC). Besides that, this system also includes face detection and recognition function to identify the person that taking attendance is currently being the owner of the NFC tag. This multi-factor identification system will be designed to cater the limitation of the conventional attendance system. The final results demonstrate that the proposed system thwart against replaying events leading to duplications recording and cheating by legitimate and illegitimate users have due to the added randomization effect in generating sessions for each event recorded within the web-service database. The overall system provides an efficient, accurate and portability solution and work well for the real-life attendance environment within the university.

Keywords: Attendance system, near field communication, cloud-based face detection and recognition

I INTRODUCTION

Successful schools begin by engaging students and making sure that they will come to school regularly, so the attendance rate becomes very important. The attendance rate will be calculated based to the average percentage of students attending school in every class of the course. The attendance rate is important because students are more likely to succeed in academics when they attend class consistently. It's difficult for the lecturer and the class to build their skills and progress if a large number of students are frequently absent. Moreover, the students have given the right to have their own time management at university. This will cause the attendance rate of the class become a major problem because some student may choose to absent from the class. Therefore, students from university in Malaysia are required to attend the class not less than 80% per semester, otherwise a student will be barred from taking any examinations.

The main aim of this paper is to present a sensor-based attendance system designed for recording university students attendance. The objectives of this proposed prototype are : i) to provide a secure student's attendance capturing and tracking processes by enhancing NFC sensor primitive commands and ii) to increase the efficiency and effectiveness of taking student's attendance procedure by using multi-factor authentications concept. In ensuring high accuracy, identification and verification, biometric features such as face identifier has been added together. By adding dual-factor authentication factors; the overall security is enhanced. In this paper, the implementation and architecture of a proposed attendance system known as Multi-factor Identification Authentication System (MIDAS) are presented. The outline of the paper is as follows. Section II focuses on the background studies. Section III provides comprehensive information on the methodology of the system. Nest, section IV and section V present the implementations and the evaluations of the system. Finally, section VI presents the discussion and followed by the conclusion an future work in section VII.

II BACKGROUND STUDY

There have some researches that develop technology-based attendance system. Basically technology-based attendance system can divide into two groups:

- Biometric-based Attendance System
- Sensor-based Attendance System

A. Biometric-based Attendance System

Biometric-based attendance system recognize a person's identity based on the biological characteristic such as fingerprint, hand geometry, voice, retina, iris and face recognition, which reliably distinguishes one person from another or used to recognize the identity. They have five subsystems: data collection, signal process, matcher, storage and transmission. However, the biometric system is suitable for highly secured system and mostly the biometric system is expensive (Meng and Mahinderjit Singh, 2015). Kadry and Smaili (2007) implement an attendance system based on iris recognition. The system takes attendance as follows:

A digital image of one person's eyes to be verified is captured. A feature extracting algorithm is carried out Minutiae are extracted and stored as a template for verifying later. People to be verified place his eye on the iris recognition sensor. A matching algorithm is applied to match minutiae. Talaviya et.al (2013), implement a system that takes attendance of student by using fingerprint sensor module. When the student enrolls his/her finger on the finger print sensor module, his/her fingerprint will matched with database to mark the attendance. Chintalapti and Raghunadh (2013), implement an automated attendance management system based on face detection and recognition algorithm. Every time the student enter the class, his / her images will be capture by the camera placed in the entrance. The images will retrieve the identity of the student and take attendance for that student. They use Viola-Jones algorithm for the face detection part. There are five performance evaluation conditions used by them for the face recognition part, which are PCA + Distance Classifier, LDA + Distance Classifier, PCA + SVM, PCA + Bayes, LBPH + Distance Classifier.

B. Sensor-based Attendance System

Sensor based attendance system are becoming popular nowadays. Barcode technology is a method of identification, which is used to retrieve in a shape of symbol generally in bar, vertical, space, square and dots which have different width with each one A reader of scanners are required to identify the data that represent by each barcode by using light beam and scan directly to barcode. Smart card can use as individual identification, building access and network access are part of a multi-tiered program that is in the final stages of rolling out.

Meng and Mahinderjit Singh (2015), implement an attendance, which take attendance by using RFID. RFID can be categorized into three categories, which are low frequency (LF) RFID, high frequency (HF) RFID, and ultra-high (UHF) RFID. LF have 120-150 kHz, HF have 13.56MHz, and UHF have 433 MHz. RFID is an automatic identification method, whereby identification data are stored in electronic devices, called RFID tags (Transponders), and RFID readers (interrogators) retrieve these data.Student only need to place their RFID tags which contains a unique id number on the reader and their attendance will be taken immediately. Every time the student enter / leave the class, they need to scan their RFID tags with RFID reader. The RFID reader will read the identification code in the RFID tags and transfer the code to the PC, which connected with USB. A program in PC will retrieve the student's identity from database using the identification code that received and take attendance for that student. Figure 1 shows the system architecture of the RFID attendance system.

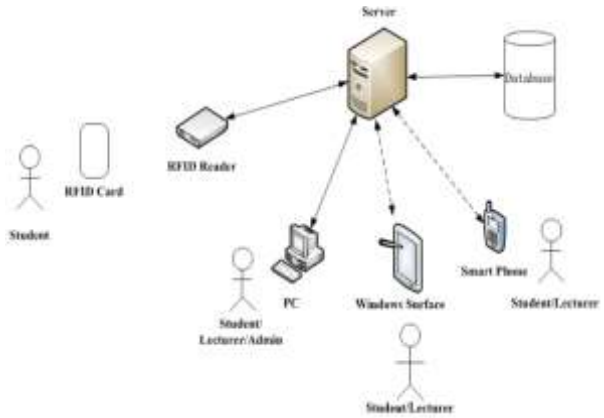

Figure 1. System Architecture for RFID attendance system (Ayu and Ahmad, 2014)

Ayu and Ahmad (2014), implement NFC supported attendance system in a University Environment named as TouchIn. Before the class start, the lecturer will run a mobile application on his/her own NFC-enabled smartphone, student that want to take the attendance will run another mobile application which will fetch the student ID from file, read the device ID and beam (send) it to the lecturer's device by simply touching the device. The attendance of the student will be taken.

III NFC-ENABLED ATTENDANCE SYSTEM

Figure 2 shows the system architecture of Multifactor Identifications System (MIDAS). The system consists of client application (web application and mobile application) that will use by the users of the system. The web application will serve as the main platform to be used by any of the system, whereas student and lecturer use the mobile application to view the class attendance information or status. The mobile application also has an additional feature for the student when taking attendance for the class. The web services will act as a medium agent between the view layer (Web application and mobile application) and data layer (Database).

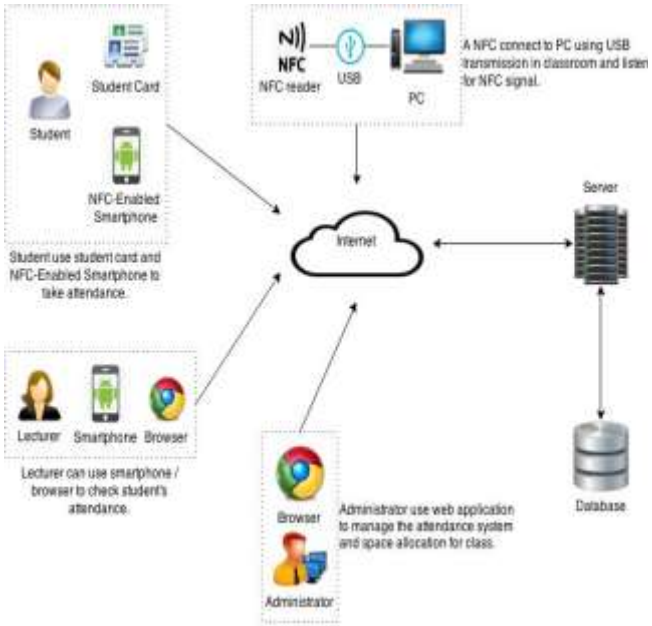

Figure 2. System Architecture Diagram for MIDAS.

A. MIDAS modules

The system consists of four different modules, which are web application, mobile application, Restful Web Services, and Windows Application integrate with NFC.The user of this system divided into three groups, which are:

i) Administrator

An administrator is a user who has the highest privileges and authorization. An administrator can enroll a new student and lecturer, create a class for course in specific academic year, semester, date and time, register course for student and lecturer and user management for the system.

ii) Lecturer

A lecturer is a user who has enrolled by administrator. The lecturer can create a class for course in a specific academic year, semester, date and time, check the class attendance's statistic, check the students' attendance and movement.

iii) Student

A user is a student who has lowest privileges and authorization. The student can check his attendance and movement for a particular class only.

Web Application is to be used by the administrator, lecturer and student. It have five main functions, which are:

i) Login/Logoff Function
ii) Registration
iii) Class Management
iv) Course Registration Management
v) Class Attendance & Movement Mangement

A web service contains a set of methods or functions that made visible and accessible on the server in order to be called or invoked by mobile application. Currently, the web services are implemented using Microsoft's ASP.NET Web API, deployed using Windows's Internet Information Service (IIS). The web services are coded in C#. The web protocol used to communicate and access to ASP.NET web services is REST (Representational State Transfer). REST is an architectural pattern that creating an API by uses HTTP as its underlying communication method. The mobile device is connected to the internet uses HTTP. HTTP is a request and response system. The client (Browser, Mobile) sends a request to the endpoint, which is web services and the endpoint, will reply to the client. The window application plays an important role in the system. It is responsibilities for:

i) Check the NFC card is authorized or not.

If the student failed to authorize the NFC card and take attendance by using the unauthorized NFC card, the system will not allow the student take attendance and alert him for authorized the NFC card. However, if the student takes attendance by using the authorized NFC card, the system will allow the student to take attendance and record the student's attendance and movement in the database.

ii) Take student attendance when student scanned the NFC card.

The application has the logic implemented inside and it is able to identify the following condition:

- The student is the first time enters the class.
- The student is out from the class in the middle of class.
- The student enters the class after the student out from the class.
- The student leaves the class after the class is ended.

iii) Classify the student attendance status

Calculate the total time of the student stay in the class. The application has the logic implemented inside and it is able to identify the different scenario, such as Attend, Attend & Incomplete, Incomplete and Absent.

Figure 3 shows some user interface of application and NFC reader/tag that used for this project.

Figure 3. NFC Reader and Tag

Mobile application is to be used by the lecturer and student. The student uses the mobile application for takes and check attendance. The lecturer uses it to view the class statistics and student attendance.

B. Case-scenario of NFC-Attendance System

There are four case scenarios will be discussed in this section whereby the student using the system to sign attendance. In these four cases, three assumptions will be made below.

- If the student scans the card when he/she enters in class time, the system will recognize the student as entering the classroom.
- If the student scans the card in leave class time, the system will recognize the student as leaving the classroom.
- Besides all the assumptions above, the system will recognize the student as out from class or enter class by checking the last movement of the student. If the student scan the card and the last movement of the student is enter class, then the system will recognize the student move out from the class. If the student scan the card and last movement of the student is out from the class, then the system will recognize the student move in to the class. The total duration of time the student leave the class will be calculated based on the time differences between the times move in to the class and last movement, which is the time move out from the class.
- Total time of the student stay in the class should be 80% of the total class time.

Case 1: Student's attendance status is "attend"

If the total time of the student stay in the class is more than 80% of the actual class time, the system will recognize the student as attend to the class.

Case 2: Student's attendance status is "attend & incomplete"

If the total time of the student stay in the class is less than 80% of the actual class time, the system will recognize the student's attendance status as attend & incomplete.

Case 3: Student's attendance status is "incomplete"

The student scans the card when he/she first time enter the class. After that, the student moves out from the class during the class on going. Next time, the class entered the leave class time already when the student enters again into the class. The system will recognize the student's attendance status as incomplete.

Case 4: Student's attendance status is "absent"

The student didn't scan his/her NFC card during the system class time.

IV. EVALUATION AND TESTING FOR THE MIDAS

The system is tested for usability, security and evaluated the system on the cost and compare with other similar system.

i) Usability

In order to do the system's function testing, user will log in as the administrator, lecturer and student. Web Application, mobile application, web services and window application were fully tested. Below are the results of the function testing for web application.

Table 1. Web Application Function Testing.

No.	Function	Working
1	User Login	✓
2	Admin Register Student	✓
3	Admin Register Lecturer	✓
4	Admin Register Course for Student	✓
5	Admin Register Course for Lecturer	✓
6	Admin Setting Class Time	✓
7	Lecturer Checking Student Attendance	✓
8	Lecturer Checking Student Movement	✓
9	Class Statistic	✓
10	Student Checking Attendance	✓
11	Student Checking Movement	✓
12	User Forgetting Password	✓
13	User Changing Password	✓

Based on Table 1, we demonstrate that all the functions work successfully. The role of the administrator could register student and lecturer, register course for student and lecturer, and setting the class time and location. The role of lecturer can check student's attendance status, movement and class statistics. The role of student can check his/her own attendance status and movement.

ii) Security

ITU-T Recommendation X.800 uses as references to systematically evaluate and define security requirements. In this section, we will evaluate our system with the X.800 Security Standards.

Authentication ensures that entities do communication is the correct entity. This service is ensuring there is no interference from the third of the communication is done. The users of MIDAS need to provide the correct username and password in order to access into the system. The student need to provide his/her own card when record attendance. If he / she failed to do it, he / she is not allowed to proceed the record attendance process.

Access Control is the ability to limit and control access to the host system and applications. Its implementation is done by early identification of the entity that will enter the lines of communication. Prevent users not authorized to access the resource. MIDAS is using role-based access control approach that assigns the users into three roles, which are an Administrator, Lecturer and Student, based on their responsibilities.

Data Confidentiality is the protection of data from unauthorized disclosure. The private data should not disclose to unauthorized individuals. Private record (the images and database record) is protected and administrator is the user who has the privileges to access all the private record.

Data Integrity is the assurance that the data received is really from the data sent from the correct sender. The sensor-biometric approach that using is ensure that the record or any data that send from the legitimate student.

Non-repudiation is providing protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. The student's image will be save into database when he / she is completed the record attendance process.

iii) Comparison between Systems

Table 2 shows the comparison between MIDAS and other attendance system in term of effectiveness, security and cost.

Table 2. MIDAS to Other Attendance Systems.

Attendance System	Effective	Security	Cost
RFID-enabled Attendance System (Meng and Mahinderjit Singh, 2015)	High	Low	Low
TouchIn (Ayu and Ahmad, 2014)	High	Low	Low
NFC-Attendance System	High	High	Medium

The effectiveness of three systems that stated above is same because they can record student's attendance by using different approaches. However, the security of MIDAS is greater than the other two attendance systems because it is using multifactor authentication which using NFC and biometric via face. Besides that, NFC commands are extended to add the randomization effect in generating sessions for each event recorded within the web-service database. It has higher security on against replaying events leading to duplications recording and cheating by legitimate and illegitimate users. It is costly than other two attendance systems because of the including of biometric approaches.

V. SYSTEM DISCUSSION

The Multifactor Identifications Attendance System (MIDAS) is implemented based on the requirement that discuss during the analysis stage. However, it still has some weakness and threats.

i) Strength

This system implemented and meet the requirements of the system design, and the strength of the system. The portability of the system increases because it includes a web application and mobile application. A session ID is generated using complex algorithm based on time and computer's MAC address and assigned to each of the student when the student authorizes his/her NFC card with the server. The system's security increase.The NFC card store a session ID and does not store any student's private information, it is protects user privacy. The accuracy of the system increases because the system combines sensor technology, which is NFC with the biometric authentication, which is face. The cheating issue has been eliminated. NFC commands are extended to add the randomization effect in generating sessions for each event recorded within the web-service database. Globally Unique Identifier (GUID) used to provide randomness based on time is designed using MD5 for data hashing purposes. MIDAS thwart against replaying events leading to duplications

recording and cheating by legitimate and illegitimate users.

ii) Weakness

Same like other system, the system still has some challenges and limitations to be improved.
The system is developed by using the cloud-based face detection and recognition API, so the system will not work if the network failure happens. The accuracy of the face detection and recognition depends heavily on the lighting of the surroundings. For instances, the accuracy of the face detection system will be reduced if the student snaps the photo in the low light condition.The performance of the system relates closely to the action done by the students in recording their attendance themselves. If a student forgets to scan his/her NFC card according to the procedure in case if he has left the class before the class ends, the system will fail to calculate his attendance record correctly. There have different screen resolution for the Android smartphone. The mobile application UI can present perfectly in Samsung Galaxy Note 3 only. If the mobile application install in the android smartphone, which have smaller screen resolution, the UI components will not aligned on the original position in the screen.

iii) Opportunities

There have some opportunities the can let the system become more perfect and advance. The system can combine with subway entrance guard machine, to make the system become more perfect. If the student wants to enter or leave the classroom, they must scan the card, otherwise the door will not open, and the door permits only one student pass for each opening. Nowadays, biometric become more and more popular in the mobile device, such as fingerprint and face. The cost of implement and employment of the system will become cheaper because the system will not rely on the third party for the face detection and recognition.

iv) Threats

The system has some threats. Card cloning is the biggest threat to the system. Although each of the card has a unique ID and it is only readable. The card very difficult to be duplicated because the card has some limitation at some important fields and it is not writeable. However, there still has some software or machine could clone a same card in the market. The server does not own any certificate for its secure socket layer. Certificate is important to ensure the integrity of data transferred in and out from the server (to prevent man-in-middle attack). In order to get a legal certificate, it must be purchased from any known certificate authority (CA) such as VeriSign.

VI. CONCLUSION AND FUTURE WORK

Multifactor IDentifications Attendance System (MIDAS) is a system, which can help lecturer to take the student's attendance. The system is integrating the face detection and recognition function into NFC. The main outcome for this project especially the important of Multifactor Identification System can stand as an extension to the existing student card currently used in University. In addition, the lack of automated attendance system in the University is the main motivation for implementing this system.The system can combine with subway entrance guard machine. If the student want to enter or leave the classroom, they must scan the card, otherwise the door will not open, and the door permits only one student pass for each opening. This can make the system accuracy on getting the student's attendanceand movement become higher

REFERENCES

S,Kadry; K.Smaili , "A Design and Implementation of A Wireless Iris Recognition Attendance Management System", ISSN 1392 – 124X Information Technology and Control, 2007, Vol.36, No.3.

G.Talaviya; R.Ramteke; A.K.Shete, "Wireless Fingerprint Based College Attendance System Using Zigbee Technology", International Journal of Engineering and Advance Technology (IJEAT), ISSBN: 2249-8958, Volume-2, Issue-3, February 2013.

S.Chintalapati; M.V. Raghunadh, "Automated attendance management system based on face recognition algorithms," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,5, 26-28 Dec. 2013, doi: 10.1109/ICCIC.2013.6724266.

Z.Meng, M.Mahinderjit-Singh, "RFID-enabled Smart Attendance Management System" 2014, Lect. Notes Electrical Eng.,Vol. 329, James J. (Jong Hyuk) Park et al. (Eds): Future Information Technology - II, 978-94-017-9557-9, 328439_1_En.

M. Ayu and B. Ahmad, 'TouchIn: An NFC Supported Attendance System in a University Environment', *International Journal of Information and Education Technology*, vol. 4, no. 5, pp. 448-453, 2014.