International Journal of Software Engineering and Computer Systems (IJSECS)
ISSN: 2289-8522, Volume 4 Issue 2, pp. 62-79, August 2018

DOI: https://doi.org/10.15282/ijsecs.4.2.2018.5.0049

MULTI-FACTOR ATTENDANCE AUTHENTICATION SYSTEM

Yew Kwang Hooi, Khairul Shafee Kalid and Serdarmammet Tachmammedov

Department of Computer and Information Sciences
Universiti Teknologi PETRONAS
Bandar Seri Iskandar, 31750 Perak, Malaysia
Email: yewkwanghooi@utp.edu.my, khairulshafee_kalid@utp.edu.my,
tachserdar@gmail.com

ABSTRACT

Taking attendance in classes is a cumbersome task which can benefit from smartphone innovation. This study identifies the vulnerabilities of the technology and proposes a technique to identify cheating. Several smartphone features are proposed for collective use to improve the reliability. The first measure is by using Quick Response (QR) code as a unique token; the second measure is by using International Mobile Equipment Identity (IMEI) number as a unique identification; the third measure is by checking timestamp; and the fourth measures is by checking Global Positioning System (GPS) location of the student. Algorithm matches attendee with event using QR, identifies identify using IMEI and verify attendance using timestamp and GPS. Use cases conducted have shown feasibility in practical aspect and user acceptance. This paper evaluates reliability of the approach and inherent issues.

Keywords: attendance logging, mobile applications, educational administrative data processing, office automation.

INTRODUCTION

Taking attendance is common in many educational institutions to instil discipline. Some institutions impose strict rules to ensure attainment of good student attendance. This include punitive approach such as barring students from the final examination. For international students studying in some countries, the governments require universities to systemize tracking of attendance. The Malaysian Immigration Department for instances, requires a good record as a pre-requisite for renewal of international student visas.

Typical attendance-taking is done manually by educators. This could be done by calling names or by circulating the attendance form among students who attend. Manual attendance-taking is time-consuming (Čisar, Pinter, Vojnić, Tumbas, & Čisar, 2016; Lukas, Mitra, Desanti, & Krisnadi, 2016) and prone to cheating. Studies have shown that as many as 15.8% of the class have admitted to cheating (Bjorklund & Wenestam, 1999). Furthermore, the records can be unclear, tampered or even lost(M. B. Khan, Prashanth, Nomula, Pathak, & Muralidhar, 2017).

As an alternative, technologies such as biometrics, Radio Frequency Identification (RFID), Quick Response (QR) have been proposed and tested. Besides taking attendance, the common features include detection of cheating and generation of report.

However, these solutions require special hardware to be purchased and installed in venues, which make the implementation more costly but less flexible. Furthermore, users need to queue up thus making the process less efficient.

The goal of this study is to propose a cost-efficient and flexible alternative that would improve attendance-taking through ubiquitous technologies such as the smart phone. The focus of the study is to improve accuracy of attendance-taking by detecting and eliminating fake attendance. The proposed solution uses software strategy that exploits existing and common smart phone features.

LITERATURE REVIEW

There are some existing studies to improve attendance-taking using technology. Saraswat & Kumar (2010) proposed biometric attendance system that uses fingerprint verification. Xiao & Yang (2009) also use biometric as the technology to authenticate and validate the attendance of students. They developed a real-time authentication that made use of facial recognition technology. A non-biometric device can be seen in the work (Čisar et al., 2016). The authors proposed the use of mobile application that can register attendance to an Arduino device using Bluetooth connection. Biometric approach requires special hardware and thus cumbersome.

More recently, attendance system has also incorporated sensors. (Chew et al., 2015) has proposed NFC-based attendance system to minimize human involvement and errors in attendance-taking. The paper has also evaluated the technology against RFID and concluded both can increase the efficiency. However, there is a concern over setup cost and infrastructure. NFC is more cost-efficient than RFID. The use of mobile phone sensor is a promising cost-effective alternative to dedicated sensor devices and infrastructure. However, NFC is not a permanent feature available in most phones, unlike the camera.

QR code takes advantage of the phone camera. Baban (2014) described implementation of a basic attendance-taking system that uses QR code scanning via students' smart phones. The system generated attendance reports. The design is generic for reimplementation but did not address issues of cheating in attendance. Deugo (2015) proposed a system wherein, students are to generate their unique QR codes and bring them into class for their lecturers to scan them through a special application. However, using the system may not offer time efficiency as it is the lecturers that need to scan the student QR codes.

Cleveland (2012) proposed a simpler QR-based attendance in which the lecturer generates the QR code for the students to scan and confirm attendance. The QR code is generated using a web form (e.g. Google Docs) link. Then, the QR code is scanned by attendees during attendance taking. This will trigger the link to a new attendance form for the attendees to fill up. The idea is by placing the link to the form in a third party QR code generator website. Attendees then scan the QR code using smart phones to confirm attendance on the retrieved form.

The use of QR code has advantage over biometrics due to ease of implementation. QR code can be generated easily and scanned using smartphones, which reduces the need for special hardware. However, QR code is less safe compared to biometrics approach when dealing with cheating. QR code can be shared and identity can be tampered. The use of QR code is still insufficient in deterring attendance cheating. Survey conducted with 125 students from 3 different lectures/tutorials reveal a high percentage (39%) being aware of the work-around.

Masalha & Hirzallah (2014) proposed the design of an attendance system that uses QR code with multiple security factors to eliminate false registration. The additional factors are biometrics on a selfie photo and analysis of GPS location. GPS seemed to be a popular non-biometric approach apart of QR code. M. Y. Khan, Ram, & others (2015) proposed system that tracks employee through GPS by keeping an active login session on the smart phone. The approach requires registration of the phone's IMSI number with user identity. The solution requires continuous tracking by the server.

Literature review has shown preference for QR compared to biometrics because of economic and scalability reasons. QR code is not cheat-proof, therefore additional checks are conducted using IMEI and GPS features of the smart phone. None of the work, to the best of our knowledge, investigates and explains how the information is processed to detect potential cheating within the system. This work investigates measures that can be used to cheat-proof QR code.

With regard to cheat prevent technology, (Noguchi, Niibori, Zhou, & Kamada, 2015) has implemented an Android personal scanner that allows students to scan their ID cards using their own phone. To prevent cheating, the researchers employed a Bluetooth Low Energy (BLE) beacon device to transmit a secret code that enables proper registration of attendance but only within the range of the beacon.

METHODOLOGY

Figure 1 shows the methodology of the project. It contains three major phases: Phase 1 Preliminary Investigation, Phase 2 System Development and Phase 3 User Acceptance.

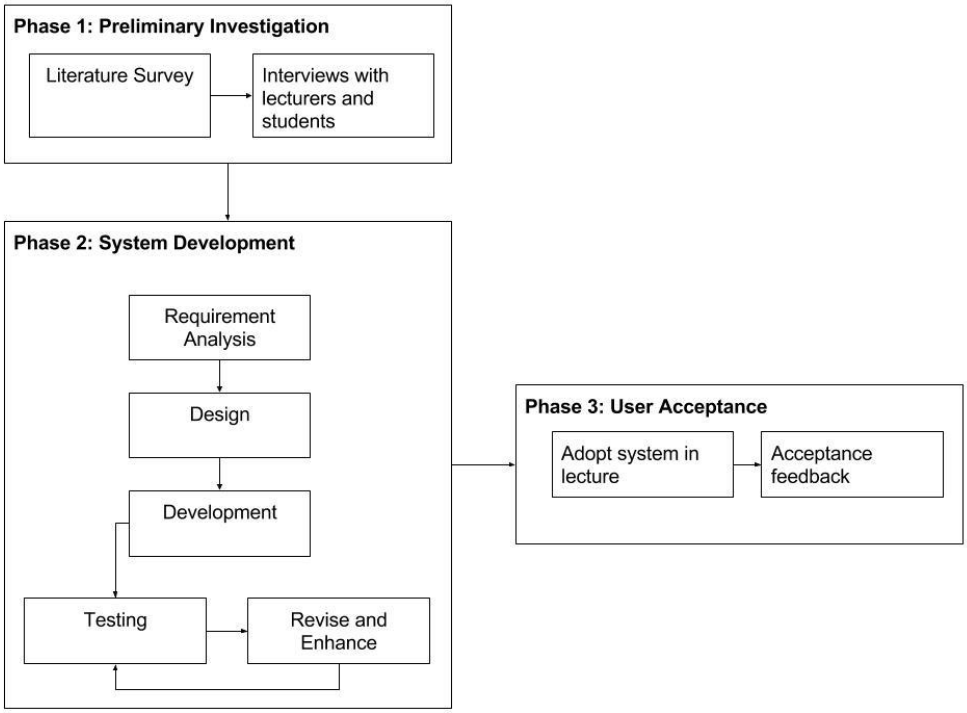

Figure 1 Research methodology.

Preliminary investigation is conducted in phase 1. The goal is to understand the problem and what have been done so far to curb the problem. Phase 1 activities include literature review and fieldworks.

The goal of literature survey is to identify the issues in attendance taking and the state of the art. Existing techniques were investigated by reviewing literature recently published in Google Scholar, IEEE, ACM and commercial websites. 75% of the studied systems are not more than 3 years ago. Inclusion criteria are "attendance cheating", "attendance logging", "mobile application", "QR code application", "attendance-taking technology" and "authentication". Search results are prioritized according to articles that fulfil most of the inclusion criteria.

The goal of fieldworks is to investigate the current methods of attendance taking at the university. Formal and informal interviews as well as observation were conducted throughout a period of a year involving 20 lecturers and 100 over students for feedbacks on their thoughts about attendance taking, the issues of the current attendance mechanism in their classes and the effectiveness of the current attendance mechanism. Attendance cheating is an issue with the current attendance mechanism thus information on the methods of cheating and suggestions on prevention were obtained.

Data are collected through questionnaire survey and semi-structured interviews. Student feedbacks are collected through online form during the use of the proposed application. Interviews with lecturers are done in semi-structure format.

a. Questionnaire - Survey questionnaire collects students' opinions and knowledge about attendance taking, the significance, the method used and safety issues. Questions also polls for student's history of attempted cheating. The surveys were done two times. The second questionnaire survey was dispensed after students were given opportunity to use the developed smart app. The objective is to collect the usability opinions.
b. Interview – Interviews were done with lecturers. Interview contains two parts. The first part of the interview is structured by giving questions which require objective answers. These questions are mainly about the techniques that have been used to collect attendance and measures to detect cheating. The second part of the interview is open-ended. Questions allow space for interview to elaborate on concerns and ideas.

In Phase 2, findings from literature review and fieldworks are combined and analysed. The state of the art mentioned in literature is matched with requirements and existing approach in fieldworks. Different techniques have different strengths and weaknesses. The analysis of this study focuses on curbing attendance cheating using ubiquitous technologies to minimize cost and to increase flexibility of implementation. This affects the design and development of the idea which will be elaborated in the following sections. Analysis using Unified Modelling Language (UML) diagrams help with analysis of structure and behaviour of the design. The resulting prototype is developed using rapid prototyping approach in order to gain quick feedbacks from end-users and to identify hidden issues.

Phase 3 is about testing activities to ensure the proposed technique is working and users can accept and perceive if the proposal is both useful and user-friendly. The techniques apply multiple measures to capture data essential for authentication of an attendance. It is important that the techniques work collectively and smoothly.

Tests was conducted on multiple lecture and lab cohorts of various sizes. A total of 18 different locations inside and outside of the premises were tested using the smart app that implements the proposal. A student familiar with the attendees was implanted

to simulate cheating. Several scenarios involving attempted cheating were re-enacted during actual lecture or laboratory to see if the proposed technique could cheat-proof those attempts. The results captured by the software were compared with manual attendance.

MANUAL ATTENDANCE TAKING - A UNIVERSITY CASE STUDY

Various methods may have been used to take attendance in Malaysian universities. This case study is based on a Malaysian private university. Various approaches have been used, from manual attendance to phone-based attendance.

A common manual approach will have an attendance form passed around and students put their initials on the form. Some lecturers prefer use a single attendance form for the whole semester, and some on session basis. Cheating occurs when students put initials on the days that they had not attended; or signing for others. Detecting this cheating is cumbersome and finding the proof is even more burdensome. Manual approach is prone to cheating.

Manual approach is also less efficient for both collecting initials and analysing the attendance. Paper-based attendance has another drawback: M. B. Khan et al (2017) mentioned that attendance forms can be lost easily which leads to loss of data.

To address the limitation of paper-based attendance, the University has also attempted phone-based technology. Any generic QR code scanner can be installed on student's phone. During class, attendance is taken by requiring student to scan a unique QR code displayed by the lecturer. The QR code provides a link to a Microsoft Form. Students open the link, fill and submit the attendance form. The advantage is instant report generation. However, it does not address attendance cheating. User survey has revealed that the approach does not eliminate cheating as the QR code can be captured as an image and sent to another phone for QR scanning.

MULTI-FACTOR AUTHENTICATION ATTENDANCE SYSTEM

Figure 2 depicts the multi-factor authentication attendance system architecture. The system architecture uses client-server architecture. The client is a thin Android application, an Android Package Kit (APK) file downloadable from Google Play Store. It contains simple user interface for one time registration of user and phone; and a function to scan QR code each time the user intends to sign for an attendance.

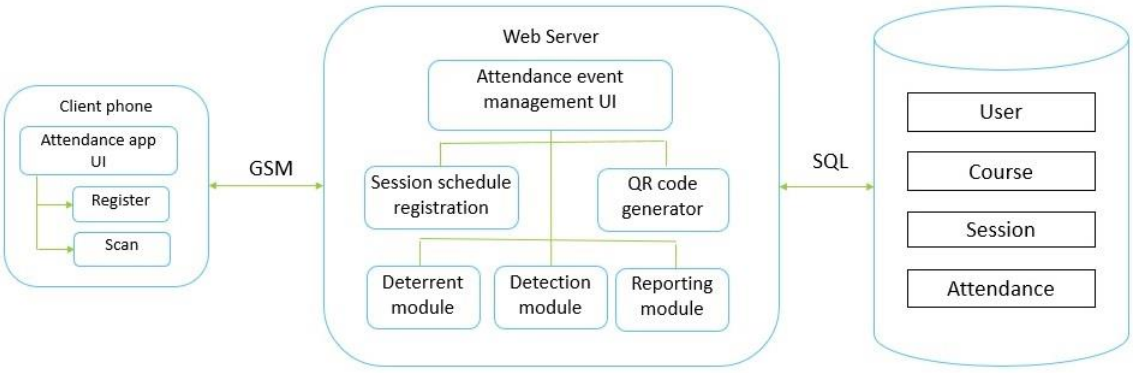

Figure 2 System architecture

The web server provides GSM connection to clients that are logged into the system. One-time device registration is needed with the server for mapping user identity with device (smart phone) unique 15-digit IMEI. The server-side system is using 3-tier architecture.

The front-tier provides access to the system through client's smartphone application to end-user and through web forms for administrator and course creator. The design focuses on minimalist and intuitive use. Data required for authentication and validation are captured through user input and detecting client system's unique identification.

The second tier contains the essential business functions: - registration, QR code generator, reporting and multi-factor attendance analytics sub-functions. The analytics sub-functions will be elaborated in the following sections.

The third-tier of the server is data tier. It is implemented in MySQL Relational Database Management System and designed through MySQL Workbench. It contains multiple relational tables which are designed for ease of scalability and flexibility. A user can create or sign into a course/event. A participant needs only to register once to sign attendance for any events. An event can have multiple sessions, each with its attendance list.

Framework Using Multi-Factor Attendance Cheat-Proofing Analytics

The Multi-Factor Attendance Authentication System adopts a framework that uses a combination of deterrent and detection approach. The two approaches provide two level of attendance checking are the deterrent approach and the detection approach. The deterrent approach makes logging a fake attendance difficult. Detection approach helps administrator to identify potential fake attendance using analytics of the logging data statistics. Figure 3 shows the multi-factor conceptual framework.

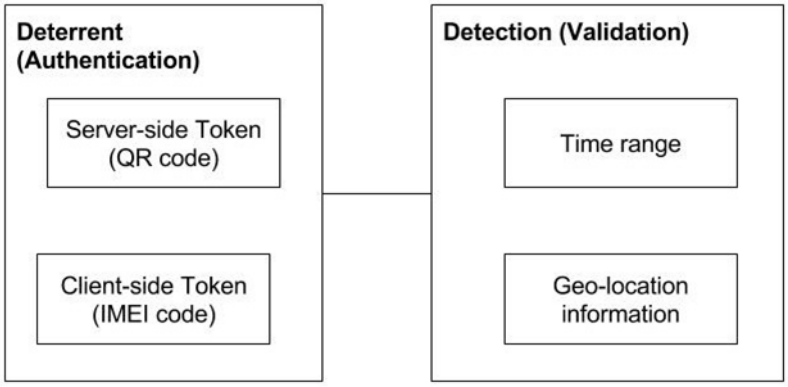

Figure 3 Multi-factor Conceptual Framework

In deterrent approach, tokens are introduced as a measure to authenticate a genuine attendance. The use of tokens makes forging identity more difficult. There are two-sided tokens used in this work: server-side and client-side token. The server-side token uses unique QR code generated by server for each lecture/laboratory or session. The client-side token uses a unique 15-digit International Mobile Equipment Identifier (IMEI) code of each phone is mapped to the identity of the user during first-time registration. The use of two unique tokens create a unique attendance identifier in the database to be used for authentication.

It is still possible to identify the unique digits of the QR code and IMEI thus, a second level of security to curb forged attendance. This second level acts as detection stage by validating that the student's actual location when the attendance is taken. The detection stage uses time range and space parameters for validation. Time range parameter indicates that attendance logging should occur within the start and end time of the event. Space parameter. Space parameter indicates that attendance logging should occur at the venue of the event within the time range parameter.

Factor 1 – QR Code

The use of the QR code is to provide student the access to a lecture session. A lecturer registers the event in the system by entering the name and running time. The server attaches a unique QR code. This code is displayed on screen as a small window during the lecture session. A unique number based on name and time of event is encoded. Figure 4 shows the activity diagram for the lecturer to generate the QR code for the lecture session.

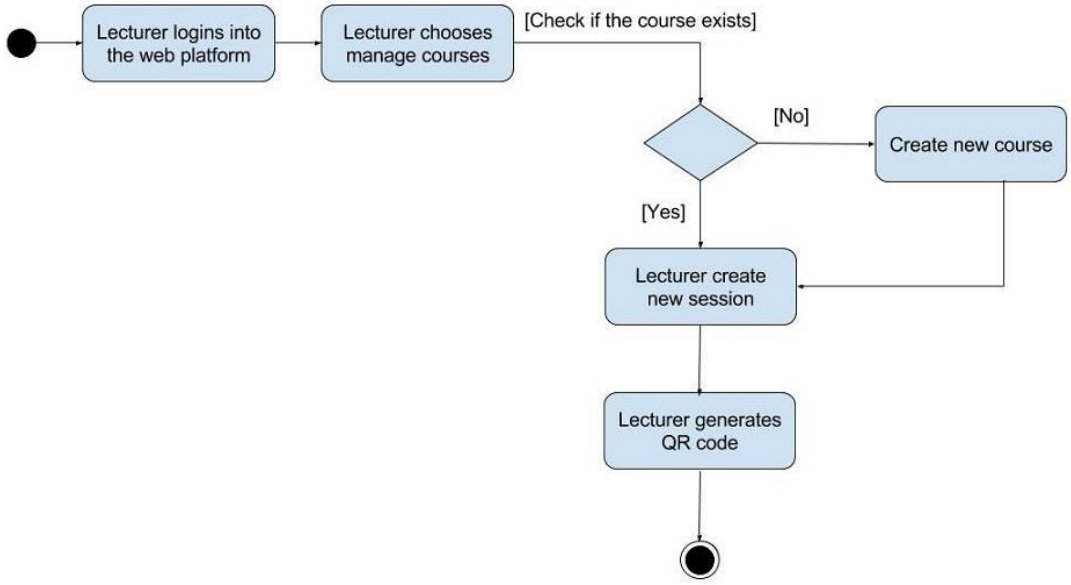

Figure 4 Activity Diagram: Lecturer Generates QR Code.

Figure 5 shows the activity diagram for students to record their attendance. Before the class begins, the lecturer will display the QR code via a projector. The students need to download the Multi-factor attendance authentication mobile application and access the mobile application. For a first-time user, the student needs to register their details. Once logged in, the student can scan a QR code each time for attendance record.

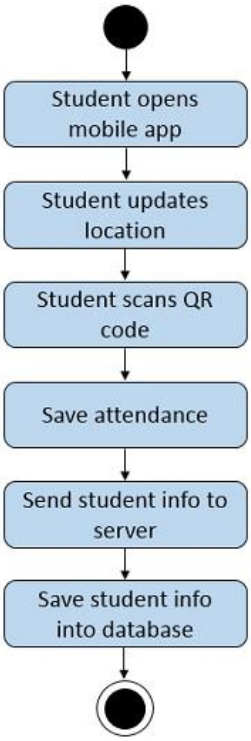

Figure 5 Activity Diagram: Students Record their Attendance

When student downloads and installs the smart app, they are prompted for personal details. The phone number is mapped to the registered name. Apart of phone number, the smart app will also register the unique IMEI number of the smartphone device. This information is stored in the database. The database contains five entities: Students, lecturers, courses, sessions and attendance. One of the attributes in Students class is the IMEI number which indicates that a mobile phone is attached to one student only. The QR code is generated based on the Session class. When the students record their attendance using the QR code, the QR unique identifier, scan time and attendee geo-location are sent to server for cheat-proofing analysis. The data will be analysed by comparing the data using some assumptions against known information in the database.

Factor 2: IMEI Code

The second deterrent factor is the IMEI code. IMEI code is a unique 15-digit code that uniquely identifies a valid mobile phone. An IMEI code is attached to a user. When a student registers first time, the system stores the IMEI code of the phone used for registration into the database. This maps student identity with IMEI. However, a limitation is that the student needs to update the registration in case he or she plans to use a different phone. During authentication, IMEI of the attendee will be checked against the stored IMEI number. Figure 6 presents the algorithm to check whether the student uses a registered phone when recording the attendance.

```
START
    CAPTURE IMEI NUMBER OF A PHONE
    SEND IMEI NUMBER TO SERVER
    PERFORM IMEI NUMBER CHECK
    IF IMEI NUMBER = REGISTERED IMEI NUMBER THEN
        PRINT MESSAGE "ATTENDANCE SAVED SUCCESSFULLY"
    ELSE
        PRINT MESSAGE "UNABLE TO SAVE ATTENDANCE"
    ENDIF
END
```

Figure 6 Pseudocode for IMEI Number Check.

Factor 3: Time and Space Parameters

The third factor is about the validation of the user's time of attendance and location. Students needs to be at the right date, time and location to considered as present. Multi-Factor Attendance Authentication System checks for both time and location parameters. The time parameter is based on server time of when a new attendance record is created in the database. This is compared with the registered time of the event. In case the attendance time was not within the event's expected time window, the attendance would not be recorded. Next, the system identify determines location of attendee. Attendance logging should take place inside the premise. For this purpose, latitudes and longitudes coordinates of a student smart phone will be captured automatically when the student snaps the QR code. The longitudes and latitudes become the coordinates of each authenticated attendees. Each event will have a list of recorded attendees, each row represents an attendee. The assumption is that majority of the attendees are genuine and there may be a small minority of forged attendance if any. Figure 7 shows the pseudocode to identify forged attendance by processing the geo-location of the user.

```
START
    CAPTURE PHONE LOCATION
    SEND LOCATION INFORMATION TO SERVER
    INCLUDE IN THE ATTENDANCE REPORT
    SORT IN ASCENDING ORDER BASED ON LATITUDE COORDINATES
END
```

Figure 7 Pseudocode for Geolocation Processing.

In the report, the coordinates are sorted in ascending order. All coordinates are expected to be very close. In our observation, all the digits up to thousandths decimal place is typically similar in both latitude and longitude coordinates. Using the sample in Table 1 below, note that attendees have similar digits up to thousandth decimal places for latitude 4.381 and longitude 100.968 respectively with reasonable distances among one another (especially with the session creator). Thus, the mod value can be determined from the thousandth decimal precision. Any record falling out of the mod (outlier) is a potential defaulter.

Table 1 Sample Student Attendance Records

Name	Matrix	IMEI	Latitude (°N)	Longitude (°E)	Distance (m)
Yew Kwang Hooi (Session creator)	11580	355320072988898	4.3812785	100.96810	0
Serdarmammet Tachmammedov	15777	356381063227320	4.381269	100.96828	19.98
M Khairul Shafee	11679	356381153127891	4.3812784	100.96812	2.22

Figure 8 shows the pseudocode to identify the outliers:

```
START
    DOWNLOAD REPORT
    START CHECKING COORDINATES
    CHECK COORDINATES THAT HAVE SAME 3 DECIMAL PLACES, CHANGES
     ONLY IN LAST 3 DIGITS AND APPEAR MOST FREQUENT
        ATTENDANCE CAPTURED INSIDE THE CLASSROOM
    CHECK REMAINING COORDINATES IF ANY
    IF BOTH LATITUDE AND LONGITUDE HAVE CHANGES IN 3 DECIMAL PLACES
     FROM MOST FREQUENT APPEARED COORDINATES
        DETECT SIGN OF CHEATING
        PERFORM FURTHER INVESTIGATION
    ELSE IF ONLY EITHER LATITUDE OR LONGITUDE HAVE CHANGES IN 3
     DECIMAL PLACES FROM MOST FREQUENT APPEARED COORDINATES
        DETECT SIGN OF CHEATING
        PERFORM FURTHER INVESTIGATION
    ENDIF
END
```

Figure 8 Pseudocode for Geolocation Outlier Analysis.

The algorithm carries out analysis automatically by using the following logical expression on the coordinates for each row of the list*:*

```
IF ((latitude_row(?) <> latitude_mod) OR (longitude_row(?) <> longitude_mod))
THEN
        OUTCOME(?) = "Outside"
ELSE
        OUTCOME(?) = "Inside", WHERE ? is ROW
END IF
```

As a prerequisite, the algorithm needs to know the mode of the longitude and latitude. The assumption is attendees flock together, thus the values of longitude and latitude are very similar. Based on our study, within an average lecture hall, the longitude and latitude values are similar up to the 3rd decimal place. Thus, the mode can be determined by checking for similar values up to 3rd decimal places.

Algorithm to determine cheating is implemented as finding the row of data with attribute that is distant from the mode value. The above algorithm compares every longitude and latitude in records with the mode longitude and mode latitude. Difference after the 3rd decimal place is negligible. Any other dissimilarity before the 3rd decimal indicates possibility of the device being in a different location.

Both algorithms above are of O(n) complexity, where n is the number of records. Since n is reasonably small, the complexity is negligible.

Mobile Application User Interface

The user interface of Multi-Factor Attendance Authentication System consists of a client smart phone application and server web application user interface. Figure 9 shows the user interface for the Multi-factor attendance authentication mobile application.

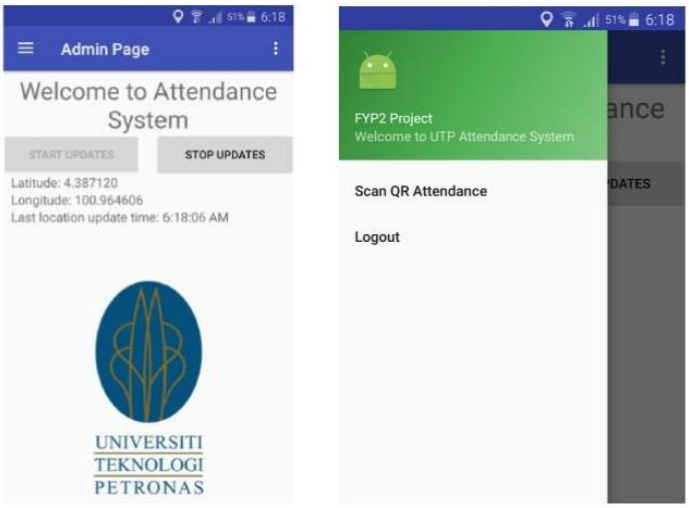

Figure 9 Student User Interface: Mobile Application

The mobile application requires one-time registration of new user to map user identity with IMEI. Then, attendance checking is done by having the device scanning a QR code.

The client mobile application does not analyse authentication. The role is as a sensor to capture values needed for multi-factor authentication analysis on the server side. The values captured are summarized in Table 2:

Table 2 Factors for attendance authentication.

Factor	Purpose	Data type
1	Which event?	QR code
2	Which device?	Device IMEI
3	Which location?	Device longitude and latitude
4	What time?	Timestamp

Figure 10 shows the user interface for the lecturer to manage courses. This user interface includes all created courses with their details by lecturer and reports button on the left. Moreover, the page includes actions such as adding new course, creating session and editing or deleting the course itself. A lecturer can create more than one courses. For each course, the lecturer can create the sessions.

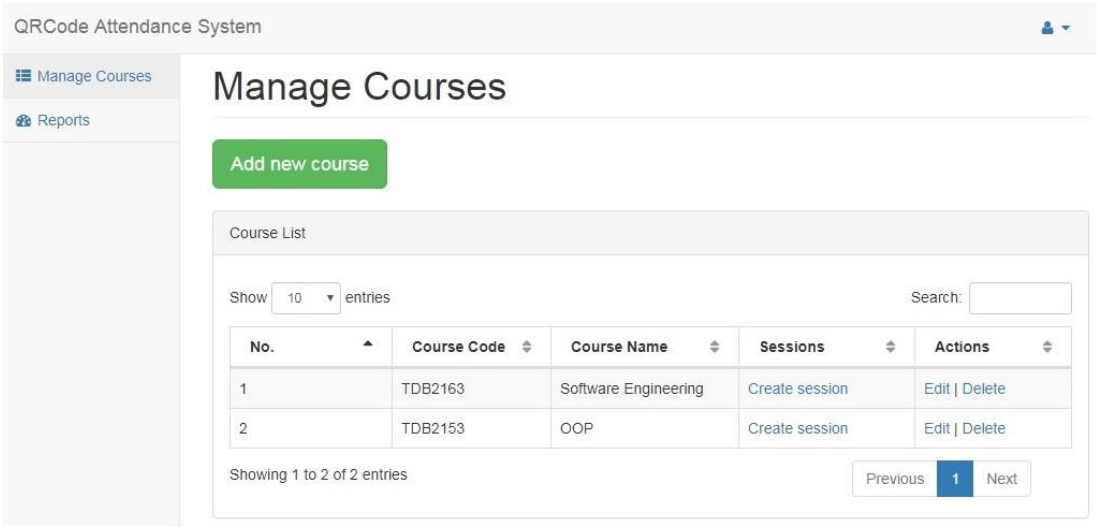

Figure 10 Lecturer User Interface: Manage Courses

Figure 11 shows the user interface for the lecturers to create a session for a course. Sessions can be lecture slots, tests slots and presentation slots. Each session has a specific date and time duration. If the user clicks the "Create Session" link, it will create a new event session. QR code is generated by clicking the “Display QR Code” button. The QR code will be scanned by the students as means to record their attendance.

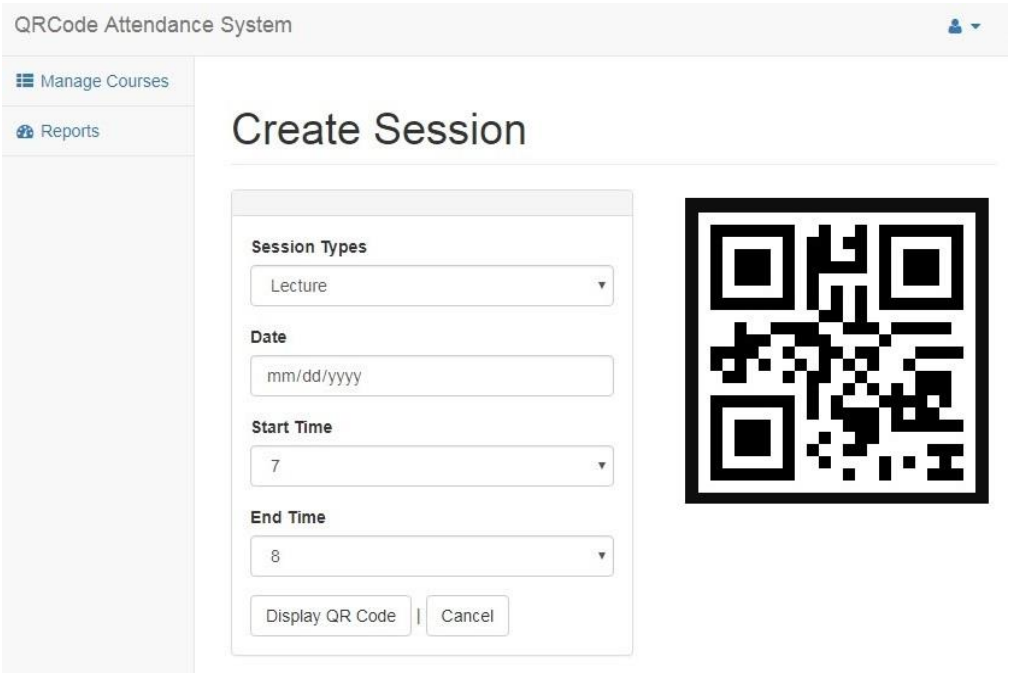

Figure 11 Lecturer User Interface: Creating New Session.

The reporting features of Multi-Factor Attendance Authentication System provides documentation to the lecturers and the university. Users can select the courses that they want to view or download the report. Figure 12 shows user interface for users to download the attendance report. The downloaded report will be in CSV file format.

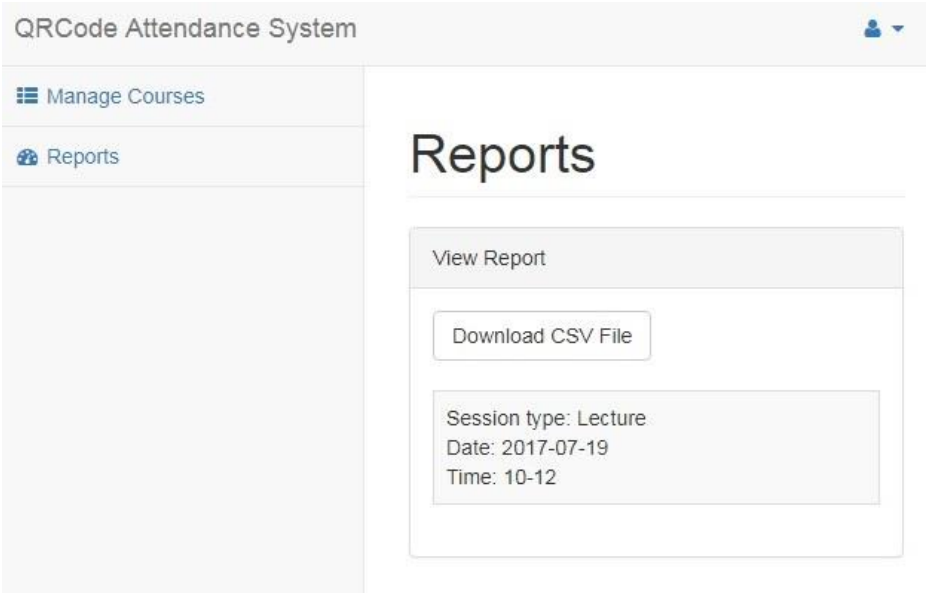

Figure 12 Lecturer User Interface: Report Download.

SYSTEM TESTING

The system has successfully detected QR and IMEI code in most situations. First-time installation and usage of the system's smart app has shown to be taking a longer time than usual due to participant's lack of familiarity with the procedure. The experiment was deliberately done in a candid manner to see how attendees could use the system with zero or minimal instruction.

It is also noted that scanning QR code is straightforward and easy. However, if the room is large, the screen may become warped for students who sat on the edges. They found the scanner to be less effective in detecting the screen.

Table 3 presents a sample record from the experiment conducted for geo-location analysis. The actual location of the subject is already known, as depicted by column "Expected outcome" in Table 3 below. The system will generate values recorded under "Actual test outcome". Conclusion is consistent if both expected value and actual value are similar.

Majority recorded coordinates are similar. The MOD coordinates are determined by counting similar coordinates up to thousandth place. In the example, the MOD latitude and MOD longitude are 4.381 and 100.968 respectively.

However, highlighted rows have different coordinates from the MODs and thus requires further validation. It could be seen that for Max, the difference is in the longitude coordinate. For both John and Conor, the difference is in the latitude coordinate. As for Jeff, difference is found in both latitude and longitude.

Table 3 Sample Attendance Record

	A	B	C	D	E	F	G	H
1	Session ID	Session Type	Date	Start Time	End Time			
2	55	Lecture	7/19/2017	10	12			
3	Name	Matrix	IMEI	Latitude	Longitude	Expected outcome	Actual test outcome	Conclusion
4	John	19215	35964545784	4,380975	100,968806	Outside	Outside	Consistent
5	Max	19216	39638547451	4,381236	100,967863	Outside	Outside	Consistent
6	Amir	19205	36859802017	4,381466	100,968348	Inside	Inside	Consistent
7	Azri	19207	36646343463	4,381468	100,968151	Inside	Inside	Consistent
8	Ben	19202	46346364646	4,381506	100,968261	Inside	Inside	Consistent
9	Ridhwan	19212	34255465464	4,381526	100,968238	Inside	Inside	Consistent
10	Mohammad	19209	59476272527	4,381527	100,968262	Inside	Inside	Consistent
11	Nasr	19203	96278875754	4,381542	100,968266	Inside	Inside	Consistent
12	Alex	19214	43436436434	4,381561	100,968272	Inside	Inside	Consistent
13	Joshua	19204	69685274425	4,381565	100,968304	Inside	Inside	Consistent
14	Jeniffer	19213	45454545423	4,381571	100,968244	Inside	Inside	Consistent
15	Mark	19211	23452344532	4,381604	100,968304	Inside	Inside	Consistent
16	Stephannie	19210	78784568969	4,381642	100,968271	Inside	Inside	Consistent
17	Sara	19206	56765734545	4,381655	100,968297	Inside	Inside	Consistent
18	Shafiq	19208	98656878456	4,381656	100,968138	Inside	Inside	Consistent
19	Sharon	19201	56789234234	4,381674	100,968305	Inside	Inside	Consistent
20	Jeff	19218	86474256598	4,382011	100,969534	Outside	Outside	Consistent
21	Conor	19217	36598745454	4,382133	100,968164	Outside	Outside	Consistent
22								

Figure 13 illustrates number of detected attendance cheatings against attempted cheatings using two methods of attendance taking. The blue line represents the proposed attendance system whereas orange dashed line represents manual attendance-taking.

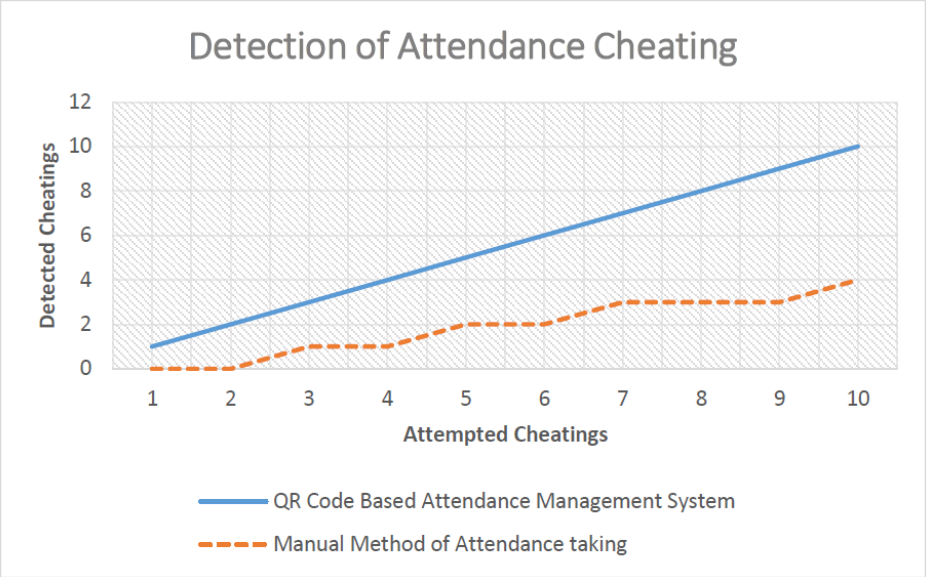

Figure 13 Detection of Attendance Cheating

Several repeated tests of the system have produced consistent and positive outcomes. On the other hand, manual attendance does not reliably detect all cheating attempts. With a bigger number of attendees and more cheating attempts, manual approach does not effectively catch up.

USER ACCEPTANCE TESTING

User acceptance testing has been conducted with a total of hundred undergraduate students spanning over three lectures and two labs. These students were familiar with manual attendance as well as QR code scanning. A facilitator guided them to install, register identity, scan QR code to register the attendance and to fill up the feedbacks.

The general perception (90% of respondents) is in favor of the technology for effective record-keeping. The proposed technique introduces a new hassle which is requiring registration for a new event and scanning of QR code for every session of the event. Respondents, however, did not see this as being more of a hassle compared to manual attendance taking. On the Likert Scale of 1 to 10, where higher number indicates higher perceived hassle, the average hassle score for manual attendance and the proposed multi-factor approach are 9 and 2 respectively.

Respondents were unable to distinct the difference between the conventional QR code application and the proposed QR code with multiple-factor authentication. This is unsurprising because the multi-factor authentication is a server-side processing. The mobile phone is only used for collecting contextual information about the user, which is location and time. A few users are aware that Location feature of the phone is being used when the application prompted them to turn on the feature.

Survey has also been conducted with a few lecturers. Two of them tested the technique with students in real lecture and lab settings. The rest of the lecturers are interviewed after being shown the system's interface and demonstration. Feedbacks indicate good acceptance because all the lecturers are familiar with attendance-taking using QR code. All agreed that QR code itself does not prevent cheating in a way better than manual attendance. In fact, manual attendance provides an advantage when the student's signature can be analyzed.

The lecturers agreed however QR code used with other prevention factors introduced in this work can effectively help to authenticate an attendance and possibly make cheating very inconvenient. One advantage of the system is the real-time recording of attendance, time-stamp and GPS location. A lecturer can access the dashboard to track the attendance, identify the suspicious IMEI device using GPS location that is not similar to the mode values statistically, and use the mapped phone number to call the student.

SIGNIFICANCE AND LIMITATIONS OF THE STUDY

Significance

The significance of this study is the implementation of multi-factor attendance authentication which requires no special hardware setup but providing reliable detection. It is naïve to say that it is totally cheat-proof, but the algorithm makes cheating less appealing: -

- Factor 1 – are you at the right event?
- Factor 2 – do you have the unique token?
- Factor 3 – are you there within the event time range?
- Factor 4 – are you (your token) there physically?

Limitations

The design and test had been done using android phone technologies. Thus, the result may not be applicable to some phone models in the market. iPhone for instance, does not use android operating system. However, User Acceptance Test (UAT) had been conducted on generic functions across all phone models and had revealed some limitations, see Table 2.

Table 2 Limitations and Recommendations

Limitations	Recommendations
Skewed QR code on projector screen is challenging for a good scan by students sitting at the corners of the premise.	Instead of projecting QR code on screen, print and display it at entrance.
QR code has to be displayed at intervals.	Instead of projecting QR code on screen, print and display it at entrance.
Requires GPS location detection to be turned on smartphones.	Client application to prompt user to turn on GPS location.

It is important to put a note here that QR code is just one of the factors of authentication. It is not used to identify user identity but to identify the event. QR code is not cheat-proof as it can be captured as an image and shared or reused. In fact, QR code can be replaced by bar code or by a secret number. A more secured alternative is to have QR code replaced by Bluetooth Low Level Energy beacon, as elaborated in (Noguchi et al., 2015)'s work. However, that solution requires special hardware setting.

Another issue is privacy as IMEI is a unique identifier of the device and hence can be used for tracking when used in combination with GPS. There are many tracking applications that make use of both IMEI and GPS. Thus, good faith is required between user and service provider in that the IMEI mapping is not shared and used without the knowledge of the device owner.

IMEI is only useful for identifying the device, thus it does not exactly confirm the bearer of the device is the registered owner. Furthermore, IMEI may not be available in some android devices. CDMA device for instance, uses Mobile Equipment Identifier (MEID) hexadecimal digits which serves the same function as IMEI. Less common is Electronic Serial (ESN) number which is used in some older phone models.

Another limitation is the use of smart phone may be prohibitive in some situations. Some locations may have poor GSM bandwidth. Students from economically disadvantaged background may not have telephone with the required specification. In situations where there are only a few students who are affected, the lecturer can revert to manual attendance for these students.

CONCLUSION

This study has investigated attendance cheating and proposed manipulating common smartphone features as prevention. The proposed method requires combination of multiple factors: - QR code (unique event identifier), IMEI code (unique token), timestamp (time constraint) and GPS location (space constraint) as data for authentication of attendance. Implementation has shown promising efficiency and feasibility for attendance taking. It is also a very promising cost-effective approach for detecting anomaly in attendance automatically and real-time, thus making cheating very unappealing and easily detectable.

ACKNOWLEDGEMENT

The authors wish to thank Universiti Teknologi PETRONAS (UTP) and department of Computer and Information Sciences for the opportunities and supports throughout the project duration. Moreover, authors are thankful to fellow lecturers and students who have participated in the project.

REFERENCES

Baban, M. H. M. (2014). Attendance checking system using quick response code for students at the university of sulaimaniyah. *Journal of Mathematics and Computer Science (JMCS)*.

Bjorklund, M., & Wenestam, C.-G. (1999). Academic cheating: frequency, methods, and causes. In *European Conference on Educational Research*. Lahti, Finland: Education-line. Retrieved from http://www.leeds.ac.uk/educol/documents/00001364.htm

Chew, C. B., Sing, M. M., Chiang, K., Tan, W., Sheng, W., Husin, H., . . . Malim, N. (2015). Sensors-enabled Smart Attendance Systems Using NFC and RFID Technologies. *International Journal of New Computer Architectures and their Applications (IJNCAA), 5*(1), 19-28.

Čisar, S. M., Pinter, R., Vojnić, V., Tumbas, V., & Čisar, P. (2016). Smartphone application for tracking students' class attendance. In *Intelligent Systems and Informatics (SISY), 2016 IEEE 14th International Symposium on* (pp. 227–232).

Cleveland, N. (2012). Take Attendance or RSVPs with a QR code. Retrieved April 13, 2018, from https://nataliecleveland.wordpress.com/2012/02/28/attendance-with-qr-code/

Deugo, D. (2015). Using qr-codes for attendance tracking. In *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)* (p. 267).

Khan, M. B., Prashanth, N. M., Nomula, N., Pathak, P., & Muralidhar, A. M. (2017). Auto Student Attendance System Using Student ID Card via Wi-Fi. Retrieved from https://scholarworks.bridgeport.edu/xmlui/handle/123456789/1912

Khan, M. Y., Ram, S. P. A., & others. (2015). GPS enabled employee registration and attendance tracking system. In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2015 International Conference on* (pp. 62–65).

Lukas, S., Mitra, A. R., Desanti, R. I., & Krisnadi, D. (2016). Student attendance system in classroom using face recognition technique. In *Information and Communication Technology Convergence (ICTC), 2016 International Conference on* (pp. 1032–1035).

Masalha, F., & Hirzallah, N. (2014). A students attendance system using QR code. *International Journal of Advanced Computer Science and Applications*, *5*(3), 75–79.

Noguchi, S., Niibori, M., Zhou, E., & Kamada, M. (2015). *Student Attendance Management System with Bluetooth Low Energy Beacon and Android Devices*. Paper presented at the Proceedings of the 2015 18th International Conference on Network-Based Information Systems.

Saraswat, C., & Kumar, A. (2010). An efficient automatic attendance system using fingerprint verification technique. *International Journal on Computer Science and Engineering*, *2*(2), 264–269.

Xiao, Q., & Yang, X. D. (2009). A facial presence monitoring system for information security. In *Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, 2009. CIB 2009. IEEE Workshop on* (pp. 69–76).