

Fraud Mitigation in Attendance Monitoring Systems using Dynamic QR Code, Geofencing and IMEI Technologies

Augustine Nwabuwe, Baljinder Sanghera, Temitope Alade, Funminiyi Olajide
Department of Computer Science, Nottingham Trent University, Nottingham, NG11 8NS UK

Abstract—Attendance monitoring is a vital activity in several organizations. Due to its importance, many attendance monitoring systems have been developed to automate this process. Despite several advancements in automated attendance management solutions, attendance fraud remains an issue as some end users can manipulate known vulnerabilities, such as proxy attendance, buddy-punching, early departure, and so on. In this paper, a fraud-resistant attendance management solution is developed by harnessing technologies such as geofencing, dynamic QR code and IMEI Checking. The proposed solution is comprised of a single-page web application where QR code can be enabled for attendance registration, and a mobile application, where end-users can scan generated QR code to register their attendance. Attendance cheating via QR code sharing is prevented by encoding the polygonal coordinates of the event venue in the QR code to determine if the user is within the venue. The proposed system solves the problem of proxy attendance by registering and verifying the end user's device IMEI number. Results obtained from testing indicate that attempts at committing a variety of attendance frauds are effectively mitigated.

Keywords—Attendance management systems; fraud prevention; dynamic QR code; geofencing; IMEI verification; software algorithms; mobile application

I. INTRODUCTION

Mobile technologies have changed the way attendance is monitored. Whether it is in schools, colleges, universities or organisations, attendance monitoring systems play a vital role in effective student or staff management. Certain metrics and statistics from attendance data can reveal vital information that can help management identify underlying problems that otherwise may not have been discovered [1]. Attendance monitoring has become ever more important in higher education institutes due to evidence of a positive correlation between attendance, engagement, and academic achievement [2]. Moreover, the UK visas and immigration (UKVI) require UK universities to ensure that all international student visa holders are engaging satisfactorily with their courses. Poor attendance or failure to engage with programmes could lead to being withdrawn from the university and the student visa being curtailed [3]. Despite the importance of attendance, high levels of student non-attendance continues to be a problem in schools and universities [4]. It is also worth noting that with a large student population, effective monitoring of attendance is a problematic task as users constantly look for ways to manipulate attendance monitoring systems, leading to inaccurate and false records. Current electronic techniques for attendance monitoring include the use of quick response (QR) code scan [5], radio frequency identification (RFID) [6], near field communication

(NFC) [7], biometrics technology [8], and global positioning systems (GPS) [9]. Each method has its own pros and cons such as cost, power, ease of deployment and operation, communication, privacy and accuracy, and attendance cheating. For instance, QR code attendance management systems which involve users using their smartphone to scan a QR code are vulnerable to fraud as the generated code can be easily shared amongst colleagues to commit attendance fraud. RFID-based attendance systems where attendance is completed by placing an RFID card on an RFID reader is a common approach. However, a crucial challenge with RFIDs is that students are unable to mark their attendance on days when they have lost or forgotten their ID cards, as RFID tags are embedded in the user's ID card. RFIDs are relatively expensive, and susceptible to buddy-punching, as users can fraudulently help their colleagues mark their attendance [6]. Biometric-based solutions such as face recognition, fingerprint recognition, and voice recognition are convenient as there are no lost cards and replacement problems given that users are essentially their own authentication. Face recognition technology uses image processing techniques to extract features and match a human face from a digital image or video against a database of faces. However, they are prone to the issue of false rejects, mismatch errors, and may not work if a user has an injury or scar [8]. There are also ways to invalidate face recognition systems, such as using a prepared photo or recorded video [10]. Biometric-based solutions are relatively costly and may also expose students' privacy. Furthermore, none of the above techniques effectively capture the problem of early exits and lateness. Tracking and maintaining accurate attendance records remains a challenge. Consequently, it is vital to understand the benefits and challenges of various approaches in order to effectively develop and deploy an attendance monitoring system that is highly resistant to attendance fraud and manipulation. This paper proposes to combine multiple fraud-prevention techniques including geofencing, dynamic QR code and international machine equipment identity (IMEI) checking to increase the reliability of attendance data and significantly reduce the possibility of committing attendance fraud. The main contributions are as follows:

- 1) A mobile application is built to allow users to be authenticated and carry out QR code scanning.
- 2) A single-page web application is developed to generate QR code, manage end user devices and user access, monitor and track attendance activities.
- 3) Geofencing around an area of interest, such as lecture venue or company location is implemented to prevent

end users from registering their attendance outside a specified virtual geographic boundary.

- 4) IMEI checking feature is implemented to ensure that end-users can only register their attendance from their own personal mobile device.
- 5) A new algorithm is created as a final layer of fraud prevention to ensure that generated QR code changes dynamically at set intervals.

The rest of the paper is organised as follows: Relevant related work is presented and analysed in Section II. Details of the system architecture and the core functionality of the proposed attendance monitoring system are discussed in Section III. The system performance under different scenarios of attendance fraud is examined in Section IV, and conclusions are presented in Section V.

II. BACKGROUND AND RELATED WORK

A. Radio Frequency Identification (RFID) based Solutions

Various approaches have been widely explored in literature to automate attendance monitoring in educational settings and organisations. Among these, radio frequency identification (RFID) based attendance monitoring systems [11] – [13], which utilize RFID Tags, also known as a transponder, attached to the identity (ID) card of the individual to be tracked is a popular approach. Students complete their attendance monitoring by placing their RFID card on a RFID reader. In [11], a RFID-based attendance monitoring system is proposed where each student record, and lecture schedules is electronically linked to the RFID tag of the student ID card. The RFID readers are then connected to a server for the information to be stored and processed in a database. Authors in [12] proposed and developed a RFID-based attendance management system with additional functionalities such SMS and email that notify stakeholders including parents and managers when specific metrics are triggered. More recently, RFID-based attendance monitoring systems that combine Internet of things (IoT) technology have also been proposed [13], where IoT devices are used to log, track and fetch attendance data on the cloud and made available for the user anytime and anywhere. Although RFID-based solutions can greatly improve attendance monitoring, the drawbacks are also obvious including but not limited to queuing problems during peak periods, recognition distance, lost or forgotten student ID cards. The cost of deploying RFID readers is relatively high. More critically, RFID-based solutions are susceptible to fraud via buddy-punching, as users could help their colleagues clock in and out of events [14]. As attendance is recorded and checked once, it is not possible to respond to the problem of early departure from scheduled events.

B. Near-Field Communication (NFC) based Solutions

The near-field communication (NFC) empowered attendance system similar in concept to RFID-based solution is proposed in [15], where a strategically located reading device exists to capture access attempts of users with embedded NFC devices, like phones and ID cards. Face identification was incorporated into the NFC-based attendance solution proposed in [16] to create a much more robust system. To enhance the security of NFC-based attendance system, the one-time

passwords (OTP) technology was integrated in [17]. NFC-based solutions are a more cost-effective alternative to RFIDs and are better optimised for power consumption. However, they are also susceptible to the problem of fake attendance or buddy-punching by students and employees.

C. Biometric based Solutions

To overcome the prolonged process of attendance marking associated with ID-based attendance management systems, biometric-based attendance methods are preferred. Biometric-based attendance management systems use users' distinct biological or physiological characteristics such as face, fingerprint, and iris to verify their requests [18]. A typical biometric system will include a reader, software for converting the scanned biometric data into a digital format and a database to store biometric data for future comparison. In [19], images of the user's fingertips are captured, and characteristics such as whorls, arches and loops are recorded. A major challenge with fingerprint-based attendance system is that it cannot recognise a wet or dirty finger [20]. An Iris recognition-based attendance system that utilizes biometric entropy was proposed in [21], where specific eye highlights peculiar to each user were extracted and transformed into a 512-digit Iris Code number. This code was stored as a unique identifier in a database and used to identify users. Face recognition technology is one of the most widely used in biometric-based attendance management systems due to its advantages of greater security, improved accuracy, and capability to easily integrate with other systems [22]. The underlying technologies in face recognition system are based on artificial intelligence and machine learning [23]. A face recognition attendance management system that utilizes the local binary pattern (LBP) algorithm and techniques like bilateral filtration and histogram equalization was proposed in [24]. The technique helped to address some of the issues associated with face recognition accuracy, like varying lighting conditions, image background, and noise in face images. This improved the recognition efficiency to as much as 95%. Biometric-based solutions are convenient; however, they are prone to the issue of false rejects (mismatch errors) and may not work if a user gets injured or scarred [9]. There are also ways to invalidate face recognition system such as using a prepared photo or recorded video [10]. Biometric-based solutions are relatively costly and may expose students' privacy [25].

D. QR Code based and Geolocation based Solutions

In recent years, QR code technology has significantly improved the efficiency and cost of deploying attendance monitoring systems. With the increasing popularity of mobile devices, attendance checking-related applications are deployed on mobile devices, and users can complete attendance checking by scanning a QR code. In [26], a QR code-based attendance management system was proposed which allows users to log on to a web-based application with their mobile phones and complete their attendance by scanning a QR Code generated by the class tutor using the QR code scanner on the web application. Mobile support for QR code makes it cost-effective as no special reading devices or ID cards are required but the problem of an imposter signing in remains. A user can bring the mobile phones of others into the classroom

to complete the attendance checking for them. Furthermore, given that QR code is unencrypted [27], the generated code can be easily shared amongst colleagues to commit attendance fraud. Aiming at solving this problem, location aware QR code attendance management systems have been proposed in [28], where users are required to scan a static QR code generated by the event organizer with a mobile application. Event details and the user’s location are stored in a remote database. Users are not allowed to register their attendance outside a specified virtual geographic boundary, known as a geofence. In [29], a mobile presence control information system that utilize the real-time location capabilities of mobile devices was used to demonstrate the effectiveness and reliability of mobile-based geolocation service. A geolocation-based attendance management system which uses geofencing to create a virtual box representing the classroom was proposed in [30] where the user’s exact location is then retrieved using GPS coordinates from their mobile devices. Other location-based attendance monitoring systems that use static QR Code and geolocation were proposed by [31] and [32]. The shortcoming of location-based attendance checking systems is proxy attendance where users can easily log in with their colleagues’ credentials on their devices and register their attendance.

E. International Mobile Equipment Identity (IMEI) based Solutions

The problem of proxy attendance in geolocation-based attendance management system can be addressed via the IMEI number. IMEI is a unique identification number allocated to each mobile device that serves as a base identification for every mobile phone [33]. It is a fifteen-digit number comprised of a type allocation number (TAC), a serial number and a check digit. It enables each device to be uniquely distinguishable from other mobile devices, as no two mobile phones have the same IMEI numbers. In [33], a solution to monitor the attendance of traffic officers was proposed that utilizes geolocation and IMEI number of the user’s mobile phone to monitor their attendance and effectively reduce cases of attendance cheating. A web-based student presence system that utilizes a combination of QR code and IMEI numbers was proposed in [34]. The IMEI number uniquely identified each student’s mobile device, and every attendance registration attempt was validated against it. Attendance fraud was reduced by ensuring that one student could use only one mobile device.

Therefore, this paper presents the design of a robust fraud-resistant attendance monitoring solution that integrates dynamic QR code, geolocation, geofencing, and IMEI checks to reduce attendance fraud. It is worth noting that no previous studies have explored the combination of these technologies and their potential to effectively mitigate fraud in attendance monitoring systems as illustrated in Table I.

III. PROPOSED ATTENDANCE MONITORING SYSTEM WITH FRAUD MITIGATION

A. System Architecture and Techniques

In this investigation, a robust attendance monitoring system that can effectively guard against fraud is achieved by combining dynamic QR code, geofencing, and IMEI technologies. The system primarily consists of two main parts as shown

TABLE I. COMPARISON OF CURRENT ATTENDANCE MONITORING SOLUTIONS WITH PROPOSED SOLUTION

Features / Solutions	[Proposed]	[28]	[29]	[30]	[31]	[32]
Cross Platform	✓	✓	×	×	×	×
QR Code	✓	✓	×	×	✓	✓
Geolocation	✓	✓	✓	✓	✓	✓
Early Exit Detection	✓	×	×	×	✓	×
IMEI	✓	×	✓	×	×	×
Dynamic QR Code	✓	×	×	×	×	×
Geofencing	✓	×	×	✓	×	×
Manual Fallback option	✓	×	×	×	×	✓

in Fig. 1(a): a cross platform mobile application (app) for registering and collecting user information; and a single-page application (SPA) for administration and data analysis. The mobile app is developed to register the unique IMEI

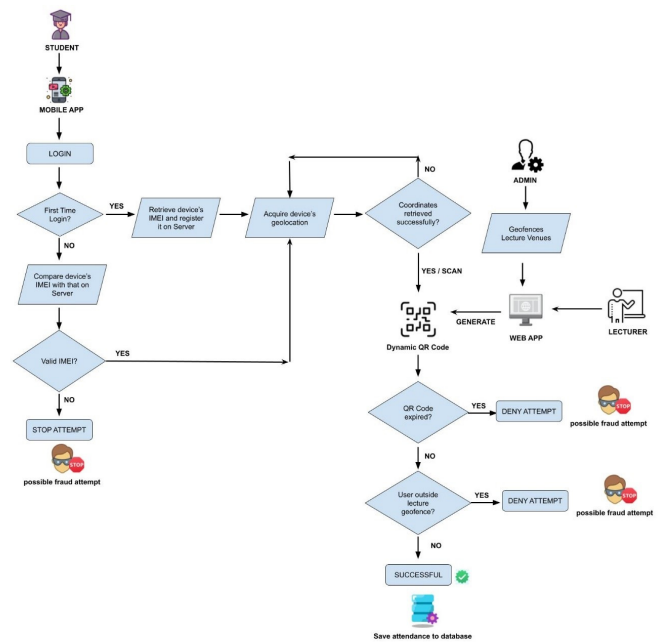


Fig. 1(a). System architecture of the proposed attendance monitoring system with fraud mitigation.

number that precisely identifies the user’s mobile device (UE), detect the entry and exit of a UE by collecting geographical location (geo-location) of the UE every minute, scan a dynamic QR code to record attendance, and upload these data for processing. The SPA is developed to undertake administrative functions such as dynamic QR code generation, user and role management, event management, attendance management and analysis. The system is developed using the MERN (MySQL, Express, React, Node) development architecture as shown in Fig. 1(b), consisting of MySql for storing data, ExpressJS for URL routing and HTTP (hypertext transfer protocol) requests and responses handling, ReactJS for building the system’s user interfaces, and NodeJS as the runtime environment [35].

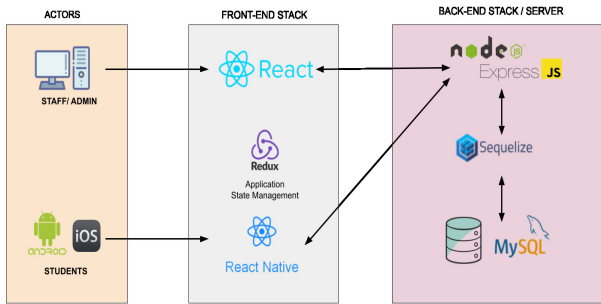


Fig. 1(b). Developmental framework of the proposed attendance monitoring system.

B. System Implementation

The techniques used for fraud mitigation including authentication and authorization, dynamic QR code generation, geofencing and IMEI checking are presented in the following sub-section.

1) *Authentication and authorization:* One of the main components of the proposed system is a robust authentication and authorization mechanism. To enable secure authentication, JavaScript object notation (JSON) web tokens (JWTs) are used, where for a successful login attempt by a user that provides correct credentials, a JWT access token and another JWT refresh tokens is generated and returned to the user agent [36]. To prevent security issues with JWT access tokens, they are stored in the application state managed by the Redux middleware, while the refresh tokens are stored in HTTP-ONLY cookies. This call happens automatically without affecting the user experience. The access tokens are given a short expiration time of 1 hour, while the refresh tokens are given a longer expiration time of 48 hours. The refresh tokens are automatically retrieved and used to generate a new access token whenever the access tokens expire. Fig. 2 presents the JWT authentication design process. The system uses a permission-based architecture [34] to maintain authorization which can be attached to defined roles and assigned to users. This design pattern enables flexible, dynamic, and robust authorization management. Permissions are checked at both the client and server sides to ensure that only authorized users can perform restricted tasks. Unauthorized user attempts at restricted resources are denied.

2) *Geofencing enforcement:* Geofencing is one of the main techniques for fraud mitigation in the proposed system where attendance registration is available only within a defined geofenced area. Users outside of the defined geo-fenced area will not be allowed to register their attendance for a scheduled event. Geofencing is implemented using Google Maps API [37] where each point on the geofence corresponds to a latitude and longitude coordinate as illustrated in Fig. 3. The entire geofence is thus an array of different latitudes and longitudes, forming a polygonal virtual boundary. For a given event, an authorized user must assign a venue in addition to other event information such as delivery method, date and time when creating a timetabled event. The system automatically records latitudes and longitudes to detect when the user enters and

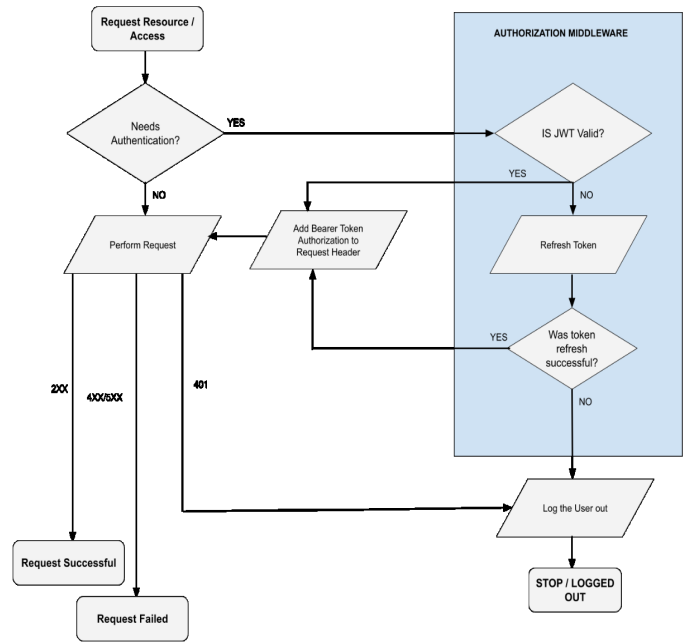


Fig. 2. JWT authentication workflow.

exists the defined geo-fenced area. The system enables the authorized administrative user to disable geofencing for events conducted online. As such, events marked as online will skip the geofence enforcement during attendance registration.

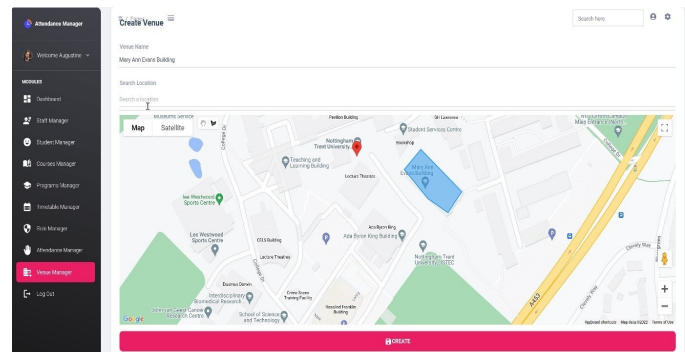


Fig. 3. Geofencing an event venue.

3) *Dynamic QR Code Generation and Scanning:* A critical fraud mitigation component of the proposed attendance monitoring system is dynamic QR code generation. For a given scheduled event, an authorized user such as a tutor can generate and display a two-dimensional QR code for attendance registration. The QR code generated encodes event information such as event title, date, start and end times, and more critically, the geofence polygonal coordinates of the event venue. Given that QR code are not encrypted, the contents of the generated QR code are encoded using base64 encoding format [38]. This makes the encoded content to appear encrypted and serves to prevent fraudulent users who may attempt to scan the QR code using a different QR code scanner. Fig. 4(a) illustrates the encoded data when scanned with a different scanner. A closer examination of the decoded

data shows information separated using slashes, as shown in Fig. 4(b). The individual components of this data are retrieved using JavaScript's split method [36]. The QR code is displayed on a screen where authenticated users can scan it using their UE. The entire process of scanning, decoding and retrieving the QR code encoded data occurs within milliseconds. One of the valuable pieces of information in the decoded data is the geofence polygonal coordinates of the event venue. With this data and the actual geocoordinate of the user, it is possible to determine if the user is within the venue's geofence. The ray casting algorithm [39] is modified and used to solve the problem of identifying whether a point is inside or outside of a polygon, a common geospatial problem in geofencing. Algorithm 1 shows the implementation of this algorithm.

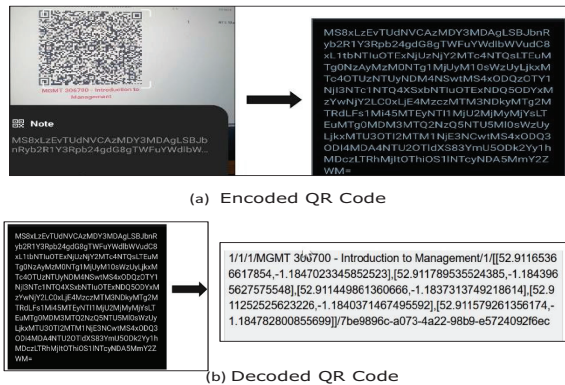


Fig. 4 QR code data.

The QR code generated automatically refreshes every 20s to solve the problem of proxy attendance via QR code sharing. In the unlikely event that geofencing functions are circumvented, the time sensitive QR serves to invalidate any shared QR code. A manual override functionality is implemented to allow an authorized user to manually register the attendance of users who may experience difficulties with the system or have misplaced or forgotten their UE. Once the UE's geo-coordinate is determined to fall within the lecture venue, their information is sent to the server to run final verification checks to determine if the attendance registration request should be approved. The following checks are done before final registration is approved:

- Check if the user is allowed to take the course
- Check if attendance registration is still enabled for the lecture
- Check if the attendance QR code ID has expired
- Check if the student has already marked attendance for the course.

If the above conditions are met, the attendance request is granted, and a successful notification is sent to the mobile app.

4) *IMEI registration and verification:* The proposed system implements IMEI registration and verification technique to solves the issue of proxy attendance which may occur when users log on to the system with their absent colleague's credentials to register attendance for them. When a user lunches

Algorithm 1 : Ray Casting Algorithm for Determining if a Point is Within a Polygon

```

1: Input: p is a simple polygon
2:  $G_i$  is the position of interest
3: Output: true if p contains  $G_i$ , otherwise false
4:  $count = 0$ 
5:  $s$  is an infinite ray in the  $+y$  direction, originating at  $G_i$ 
6: for each edge  $e$  in  $p$  do
7:   if  $G_i$  is within buf of  $e$  then
8:      $e_{x,buf} = e_x - 2 * buf$ 
9:   else
10:     $e_{buf} = e$ 
11:   end if
12:   if  $G_i \prec buf$  of  $e$  or  $e_{buf}$  then
13:     return false
14:   end if
15: end for

```

the mobile app for the first time, they are prompted to confirm whether to register the current UE as the primary device as illustrated in Fig. 5. If confirmed, the IMEI of the UE is requested and stored. This technique prevents fake attendance by ensuring that users can only register their attendance with their verified UE. For subsequent mobile app lunches, the IMEI of the UE is checked and compared against the stored value.

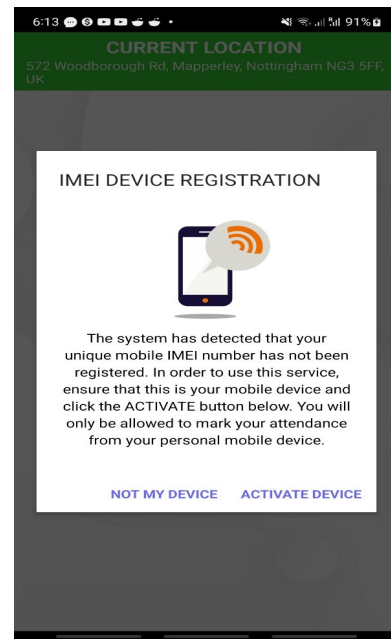


Fig. 5 IMEI registration window.

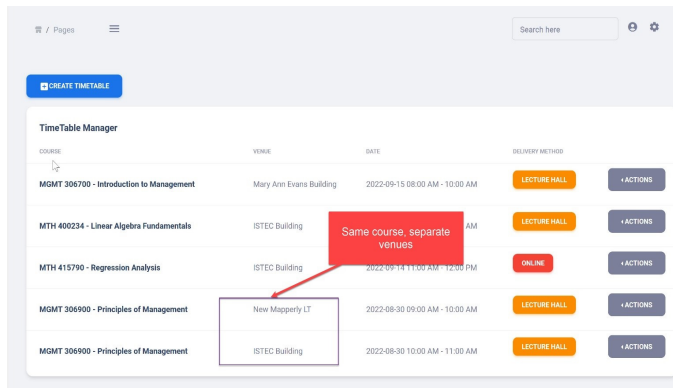
IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the performance of the proposed attendance monitoring system is investigated under three scenarios of attendance restriction fraud attempts. First, the effectiveness of geofencing restriction is tested as an end-user attempts to registering their attendance outside a specified geographic boundary of an event venue. Second, the dynamic QR code restriction is tested in a scenario where a generated QR code is sent to colleagues

in order to commit attendance fraud. Third, the capability of the attendance monitoring system to prevent registering a colleague's attendance from a their own personal UE is tested.

A. Experimental Setup

The web application is deployed on a server equipped with 3 cores and 4GB dedicated memory. The mobile app is deployed on mobile devices equipped with operating systems of Android 10 or later. Event venues named 'New Mapperly LT', 'Mary Ann Evans Building', and 'ISTEC Building' within a university environment, courses of study, event dates and times, are created by an authorized administrative user on the web application and used for testing as illustrated in Fig. 6. Two end-users are asked to register their UEs in order to register their attendance. Geofencing was implemented using the Javascript Google Maps API and location services was enabled on the UEs.



COURSE	VENUE	DATE	DELIVERY METHOD	ACTIONS
MGMT 306700 - Introduction to Management	Mary Ann Evans Building	2022-09-15 08:00 AM - 10:00 AM	LECTURE HALL	+ ACTIONS
MTH 400234 - Linear Algebra Fundamentals	ISTEC Building	2022-09-14 11:00 AM - 12:00 PM	LECTURE HALL	+ ACTIONS
MTH 415790 - Regression Analysis	ISTEC Building	2022-09-14 11:00 AM - 12:00 PM	ONLINE	+ ACTIONS
MGMT 306900 - Principles of Management	New Mapperly LT	2022-08-30 09:00 AM - 10:00 AM	LECTURE HALL	+ ACTIONS
MGMT 306900 - Principles of Management	ISTEC Building	2022-08-30 10:00 AM - 11:00 AM	LECTURE HALL	+ ACTIONS

Fig. 6 Timetable view for courses and event venues.

B. Scenario A: Geofencing Restriction

In order to test the effectiveness of the proposed attendance monitoring system to prevent proxy attendance, two event venues were created and mapped to different geolocations as shown in Fig. 6 to test geofencing restrictions. An end-user located at the New Mapperly LT venue attempts to register their attendance for both events holding at the New Mapperly LT and the ISTEC building venues. It is observed that attendance was successfully registered for the event held at the New Mapperly LT, however, the proxy attendance attempt for event held at the ISTEC building was prevented as shown in Fig. 7.

C. Scenario B: Dynamic QR Code Restriction

In order to assess the effectiveness of the dynamic QR code fraud mitigation mechanism, an end-user captured a generated QR code with their UE and sent it to another user within the same event venue. An attempt was subsequently made to register attendance registration using the shared QR code. It can be seen from the error message shown in Fig. 8 that the system successfully prevents this type of attendance fraud as the QR code generated refreshes every 20s.

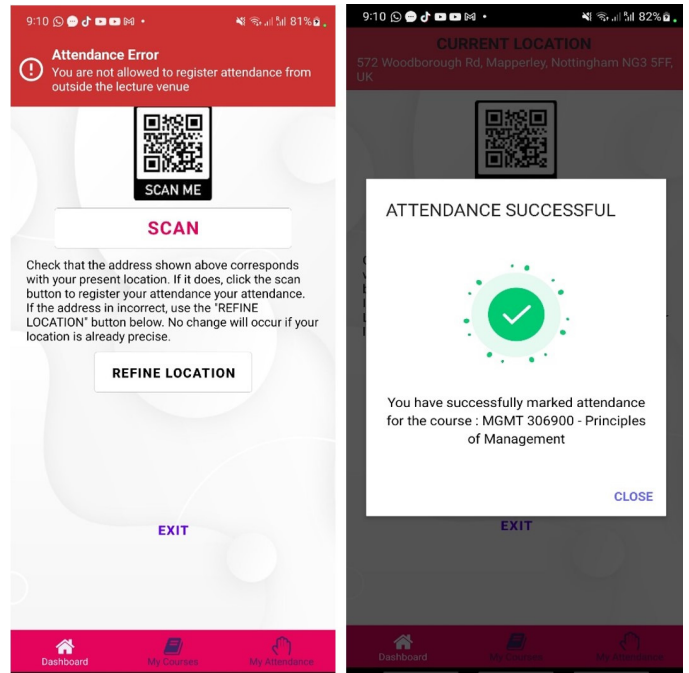


Fig. 7 Effect of geofencing restriction technique.

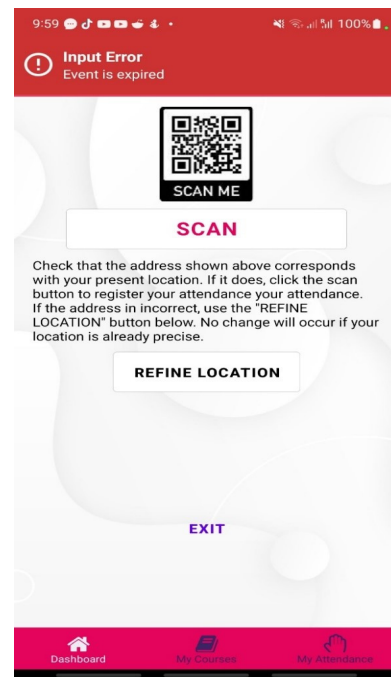


Fig. 8 Effect of dynamic QR code restriction technique.

D. Scenario C: IMEI Restriction

In order to demonstrate IMEI checks restriction, an end-user already registered on the application with their primary device attempts to register their attendance from another user's UE. It can be seen from Fig. 9 that system has effectively mitigated this fraudulent attempt as users are only allowed to register their attendance from their own personal UE.

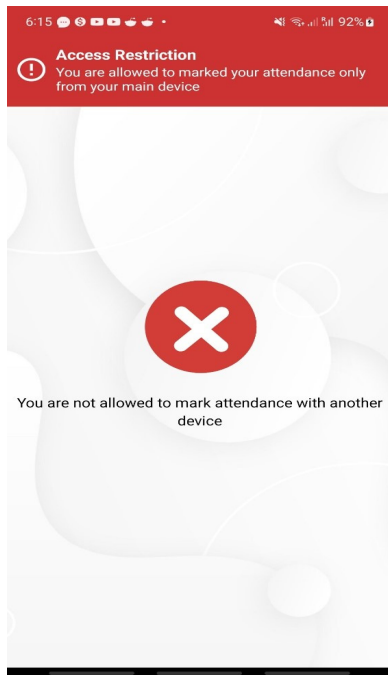


Fig. 9 Effect of IMEI restriction technique.

V. CONCLUSION

This study investigates attendance monitoring systems and proposes a fraud-resistant attendance monitoring system that utilizes a combination of geofencing, dynamic QR code and IMEI checks as preventive techniques to mitigate attendance fraud. A mobile app is developed for registering and collecting user information; and a single-page web app is built for administration and data analysis. Experimental results reveal that the solution effectively mitigates attendance fraud. End-users are effectively and securely authenticated and authorized to use the mobile and web app, and unauthorized user attempts at restricted resources are denied. Geofencing enforcement ensures that attendance registration is only available within a defined geofenced area and solves the proxy attendance problem. The dynamic QR code can only be used within a defined geofenced area, and is used only once within a set time interval to solve the problem of QR code sharing fraud. IMEI restrictions effectively restrict attendance registration to user's own personal UE and effectively eliminates the risk of buddy-punching fraud. This study is of significant importance to institutions and organizations where strict attendance compliance and reliable attendance data are of utmost importance. The efficiency of the application can be fundamentally improved by implementing an in-memory database like Memcached or Redis to cache blacklisted access and refresh tokens. The proposed system can be further enhanced by incorporating machine learning techniques to offer granular visibility into attendance patterns, highlighting those who frequently attempt to commit attendance cheating, as well as those who arrive late and leave scheduled events early. Behaviors like these in attendance data can be duly noted and rectified by the management, upholding engagement, academic achievement and optimal productivity levels in the organization.

REFERENCES

- [1] C. Kearney and J. Childs, *Improving school attendance data and defining problematic and chronic school absenteeism: the next stage for educational policies and health-based practices*, *Preventing School Failure: Alternative Education for Children and Youth*, 2022, DOI: 10.1080/1045988X.2022.2124222.
- [2] K. Alice, S. Sharry, A. Arman, P. Celia, and P. Lillian, *Understanding the impact of attendance and participation on academic achievement*, *Scholarship of Teaching and Learning in Psychology*, 6(4), 272–284, 2020, <https://doi.org/10.1037/stl0000151>.
- [3] M. Ferguson, F. Phiri, *Limitations of attendance monitoring as a singular tool for motivating students' academic engagement: The case study of one overseas student*, *International Journal of Teaching and Education*, Vol. IV(1), pp. 16-25. , 2016, DOI: 10.52950/TE.2016.4.1.002.
- [4] D. Sloan, H. Manns, A. Mellor and M. Jeffries, *Factors influencing student non-attendance at formal teaching sessions*, *Studies in Higher Education*, 45:11, 2203-2216, 2020, DOI: 10.1080/03075079.2019.1599849.
- [5] A. Nuhi, A. Memeti, F. Imeri and B. Cico, *Smart Attendance System using QR Code*, 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2020, pp. 1-4, doi: 10.1109/MECO49872.2020.9134225.
- [6] D. Mijić, O. Bjelica, J. Durutović and M. Ljubojević, *An Improved Version of Student Attendance Management System Based on RFID*, 18th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2019, pp. 1-5, doi: 10.1109/INFOTEH.2019.8717750.
- [7] C. Keau, C.K. On, M. Hijazi, and M. Singh, *Smart-Hadir – Mobile Based Attendance Management System*, *International Journal of Interactive Mobile Technologies (IJIM)*, 15(14), pp. 4–16, 2021, <https://doi.org/10.3991/ijim.v15i14.22677>.
- [8] M. Andrejevic and N. Selwyn, *Facial recognition technology in schools: critical questions and concerns*, *Learning, Media and Technology*, 45:2, 115-128, DOI: 10.1080/17439884.2020.1686014
- [9] Z. Gao et al., *A Student Attendance Management Method Based on Crowdsensing in Classroom Environment*, in *IEEE Access*, vol. 9, pp. 31481-31492, 2021, doi: 10.1109/ACCESS.2021.3060256.
- [10] J. Galbally, S. Marcel and J. Fierrez, *Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition*, in *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 710-724, Feb. 2014, doi: 10.1109/TIP.2013.2292332.
- [11] H. U. Zaman, J. S. Hossain, T. T. Anika and D. Choudhury, *RFID based attendance system*, 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 2017, pp. 1-5, doi: 10.1109/ICCCNT.2017.8204180.
- [12] Q. Miao, F. Xiao, H. Huang, L. Sun and R. Wang, *Smart attendance system based on frequency distribution algorithm with passive RFID tags*, in *Tsinghua Science and Technology*, vol. 25, no. 2, pp. 217-226, April 2020, doi: 10.26599/TST.2018.9010141.
- [13] T. Sharma and S. L. Aarthy, *An automatic attendance monitoring system using RFID and IOT using Cloud*, 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/GET.2016.7916851.
- [14] Q. Y. Tan, P. S. Joseph Ng and K. Y. Phan, *JomRFID Attendance Management System*, 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), Kuala Lumpur, Malaysia, 2021, pp. 1-6, doi: 10.1109/i-PACT52855.2021.9696816.
- [15] M. Mohandes, *Class attendance management system using NFC mobile devices*, *Intelligent Automation and Soft Computing*, 23.2 (2017): 251-259.
- [16] S. U. Masruroh, A. Fiade and I. R. Julia, *NFC Based Mobile Attendance System with Facial Authorization on Raspberry Pi and Cloud Server*, 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674293.
- [17] J. Jacob, K. Jha, P. Kotak and S. Puthran, *Mobile attendance using Near Field Communication and One-Time Password*, 2015 International Conference on Green Computing and Internet of Things (ICG-CIoT), Greater Noida, India, 2015, pp. 1298-1303, doi: 10.1109/ICG-CIoT.2015.7380666.

- [18] O. Nodirbek, M. Faxriddin, A. Gulzira, and U. Ra'no, *Biometrics authentication: A study*, *ACADEMICIA: An International Multi-disciplinary Research Journal*, vol. 10, (5), 2020. DOI: 10.5958/2249-7137.2020.00374.2
- [19] D. Feng, P. Wang and L. Zu, *Design of Attendance Checking Management System for College Classroom Students Based on Fingerprint Recognition*, *2020 Chinese Control And Decision Conference (CCDC), Hefei, China*, 2020, pp. 555-559, doi: 10.1109/CCDC49329.2020.9164638.
- [20] M. Chandra, F. Feisal, M. Gunawan, F. Gaol and T. Oktavia, *Application of "face recognition" technology for attendance management system*, *Journal of Advances in Information Technology*, vol. 12, (3), pp. 260-266, 2021. DOI: 10.12720/jait.12.3.260-266
- [21] A. K. M Zamin et al, *Design and Implementation of an IRIS Recognition Attendance Management System*, *International Journal of Computer Science Issues*, vol. 15, (4), pp. 64-67, 2018. . DOI: 10.5281/zenodo.1346059.
- [22] S. M. Anzar, N. P. Subheesh, A. Panthakkan, S. Malayil and H. A. Ahmad, *Random Interval Attendance Management System (RIAMS): A Novel Multimodal Approach for Post-COVID Virtual Learning*, in *IEEE Access*, vol. 9, pp. 91001-91016, 2021, doi: 10.1109/ACCESS.2021.3092260.
- [23] A. Chowanda, J. Moniaga, J. C. Bahagiono and J. Sentosa Chandra, *Machine Learning Face Recognition Model for Employee Tracking and Attendance System*, *2022 International Conference on Information Management and Technology (ICIMTech), Semarang, Indonesia*, 2022, pp. 297-301, doi: 10.1109/ICIMTech55957.2022.9915078.
- [24] S. M. Bah and F. Ming, *An improved face recognition algorithm and its application in attendance management system*, *Array*, vol. 5, pp. 100014, 2020.
- [25] T. -C. Li, H. -W. Wu and T. -S. Wu, *The Study of Biometrics Technology Applied in Attendance Management System*, *2012 Third International Conference on Digital Manufacturing and Automation, Guilin, China*, 2012, pp. 943-947, doi: 10.1109/ICDMA.2012.223.
- [26] A. Nuhi, A. Memeti, F. Imeri and B. Cico, *Smart Attendance System using QR Code*, *2020 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro*, 2020, pp. 1-4, doi: 10.1109/MECO49872.2020.9134225.
- [27] R. Focardi, F. L. Luccio and H. A. M. Wahsheh, *Usable cryptographic QR codes*, *2018 IEEE International Conference on Industrial Technology (ICIT), Lyon, France*, 2018, pp. 1664-1669, doi: 10.1109/ICIT.2018.8352431.
- [28] G. W. Wiriasto, R. W. S. Aji and D. F. Budiman, *Design and development of attendance system application using android-based flutter*, in *2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE)*, Surabaya, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICVEE50212.2020.9243190.
- [29] S. Ríos-Aguilar and F. Lloréns-Montes, *A Mobile Business Information System for the Control of Local and Remote Workforce through Reactive and Behavior-based Monitoring*, *Expert Systems with Applications*, vol. 42, (7), pp. 3462-3469, 2015, ISSN 0957-4174, doi: https://doi.org/10.1016/j.eswa.2014.12.030.
- [30] A. Morankar, R. Baviskar, R. Vishwakarma, S. Patil, and N. Ujgare, *Geolocation Based College Attendance System*, *International Research Journal of Modernization in Engineering Technology and Science*, Vol 03, Issue 04, April-2021, e-ISSN: 2582-5208.
- [31] Z. Ayop, C. Lin, S. Anawar, E. Hamid, and M. Azhar *Location-aware event attendance system using QR code and GPS technology*, *International Journal of Advanced Computer Science and Applications*, vol. 9(9), pp. 466-473, 2018, doi: https://10.14569/IJACSA.2018.090959.
- [32] H. Elbehery, *Enhancement of QR code Student's Attendance Management System using GPS*, *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 21(4), pp. 18-30, 2019.
- [33] A. B. Nasution, *Traffic Officers Attendance System Design Using GPS and IMEI Smartphone*, *Infokum*, vol. 10, (1), pp. 206-214, 2021.
- [34] N. Hermanto and W. M. Baihaqi, *Implementation of QR code and imei on android and web-based student presence systems*, in *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, Yogyakarta, Indonesia, 2018, pp. 276-280, doi: 10.1109/ICITISEE.2018.8721009.
- [35] N. Kozma and D. Krstić, *Design of Information System for Bookstore support Student paper*, *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 2022, pp. 1-6, doi: 10.1109/INFOTEH53737.2022.9751271.
- [36] I. Darmawan, A. P. A. Karim, A. Rahmatulloh, R. Gunawan and D. Pramesti, *JSON Web Token Penetration Testing on Cookie Storage with CSRF Techniques*, *2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, Bali, Indonesia, 2021, pp. 1-5, doi: 10.1109/ICADEISS2521.2021.9701965.
- [37] R. Shinde, A. Nilose and P. Chandankhede, *Design and Development of Geofencing Based Attendance System for Mobile Application*, *2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22)*, Nagpur, India, 2022, pp. 1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791781.
- [38] A. Azizi, Y. Yusof, and F. Ahmad, *Expanding the data capacity of QR codes using multiple compression algorithms and base64 encode/decode*, *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 9.2-2 (2017): 41-47.
- [39] Y. Ye, F. Guangrui and O. Shiqi, *An Algorithm for Judging Points Inside or Outside a Polygon*, *2013 Seventh International Conference on Image and Graphics, Qingdao, China*, 2013, pp. 690-693, doi: 10.1109/ICIG.2013.140.