I Am Here!

Automating Attendance Control

Matilde Paraíso Guerreiro Rosa do Nascimento
matilde.nascimento@tecnico.ulisboa.pt

Advisor:
Daniel Jorge Viegas Gonçalves

Instituto Superior Técnico, Universidade de Lisboa

Abstract. Tracking student's attendance in classrooms has been a problem for the professors for a long time, not only because of the difficulty to guarantee that the student is indeed the room, but also the time it consumes afterwards to manually transcript and validate the data. *I Am Here!* has the goal of being an innovative automated attendance system that aims to fulfill the existing gaps in this area, with a simple, costless, portable and fraud-resistant system using the *Device Fingerprinting* technique. As a case study and form of validation, the system will be deployed in the *Multimedia Content Production* course, where around 100 students will be enrolled, in Técnico Lisboa. Throughout the course, the system's evaluation will take into account its effectiveness, efficiency, error rate, cheating rate, a device fingerprinting analysis and also the attendance tendencies.

Keywords: students attendance system · *I Am Here!* · student · classroom · attendance · automated · professor · device fingerprinting

Table of Contents

1 Introduction

In teaching facilities, such as elementary schools to universities, it is very common to check the student's attendance, to know which students are in the classroom. This action can be done for different purposes: to simply check who is in the class (to get an updated number of students per class, and, if done throughout the year, to check whether students tend to go to class during different moments of the year) or, in some cases, to check if a student has attended a certain percentage of the course, to be able to complete the exam or to get an extra bonus in the final grade.

For different reasons, professors have been trying to implement systems where it is possible to check their student's attendance in a simple and automated manner, without wasting time of the class, nor the students and professor.

1.1 Problem

The most common way used to check if a student is in the class is by roll call or by forcing the students to manually sign an attendance sheet that is passed through the classroom. Both of these systems are vulnerable and not scalable for large numbers of students, being too time consuming (the first one more than the second). The second one can also be easily trespassed - by just one student signing for one colleague (or more).

With increased importance given to attend classes, such as when there is a bonus in the final grade, motivation to cheat the attendance checking increases as well. Because of that, some students will try to trespass the system. Rather than trying to attend the class, students try to manipulate the attendance system, faking their presence, by asking a colleague to sign on their behalf. Also, the professor does not have time or energy to keep track of how many signatures a students is giving, or to count the number of students in the class (that can be constantly entering/leaving the room), given the fact that some classes can have more than 50 students. Also, afterwards, the professor has to manually check all the signatures (that can be easily forged) and possibly transcribe them to a spreadsheet; this can be a very long and tedious process.

1.2 Objectives

The goal of *I Am Here!* is to implement an Automated Attendance System (AAS) to prevent all problems that were mentioned earlier. This system must check the student's attendance in a faculty class, in a way that:

- **does not require extra-hardware** (besides what students and professors usually carry, such as a mobile phone, computer or tablet), which means that:
  - the professor does not have to carry anything between classes
  - the system will **not cost money**
  - it will be **portable**

- if a student **does not have a way to access the internet**, it is also possible to check his/her attendance;
- **is not time consuming** (for the professor and the students);
- is **effective**, as it checks the attendance of the students that are in the class;
- **only students inside the classroom can check their attendance**, i.e., it should be hard to trick the system;
- **does not violate privacy concerns**;
- the student's attendance can be made **available online** (so an updated attendance record is only accessible to the students and professor);
- can **easily be implemented** in any course or faculty;
- **can distinguish between students arriving on time and being late**;
- **students that are not yet enrolled in the course** can still check their attendance.

This system assumes that the classroom has a projector (or a large TV) and that the professor has a computer available. If one of these assumptions does not happen, the system can not be used.

1.3 Document Structure

The remainder of the document is structured as follows. The next two major sections of this document are the ***Related Work*** and the ***Proposed Solution***, in section 2 and section 3, respectively..

In the first one, different types of student's attendance systems that currently exist will be presented, as well as a technique that will be implemented in the proposed system (*Device fingerprinting*). The second and final one details the proposed solution, such as what technology will be used to check the attendance and make it available online, how it is going to be implemented, what type of security and validation will be used, its architecture and how the attendance will be verified. Then, in section 4 and section 5, the system's evaluation and the planned schedule of the following work will be presented.

After these, the section 6 concludes the paper with *Conclusion.*

2 Related Work

For this project, it is useful to research different types of Automated Attendance Systems (AAS). Because the solution aims to eliminate time unnecessarily consumed by the students while having to manually fill an attendance sheet, the research was mostly around systems with the same mindset.

This section is focused on explaining some systems used for attendance tracking in teaching facilities, most of which are universities. It starts with a brief walk-through on *Manual Attendance System (MAS).* Then, a more automated way, it is explained the *Radio-Frequency Identification (RFID)* in subsection 2.2. In subsection 2.3, a different approach is presented, with *Biometrics and Face Recognition* systems. In subsection 2.4, a final and different type of attendance system is analyzed, related with mobile phone features used for attendance systems, and then software only systems in subsection 2.5.

Additionally, a technique that does not require any hardware called *Device fingerprinting* is explored in subsection 2.6, being a possible solution to validate student's authenticity in classrooms.

2.1 Manual Attendance System (MAS)

The most common means of attendance system is the manual one [Kas+12]. This system normally works with an attendance sheet that has the name (and in some cases, the number) of the students (ordered alphabetically by name, for example), the date and time of the class, and the name of the course. This sheet is passed through the class, an it is supposed to be signed only by the students that are actually attending the class.

This approach presents a variety of disadvantages. The most notorious one is that anyone can sign for anyone that is not inside the class. In cases with a lot of students inside the room, is it not possible for the professor to keep track who is signing more than one name in the sheet. Another problem is afterwards, when the professor has to manually check all the signatures. Even if the class does not have a lot of students (for example, a class with 30 students), this process can be very time consuming. Not only because of the repeated action to check the signature and mark it in a virtual spreadsheet, but because the professor usually does not teach a single course and therefore needs to repeat this for other courses, as well. In a scenario where a professor has at least two courses, there are at least four classes at the end of the week to verify. A semester has around 14 weeks, so in the end, there are at least 56 sheets to manually verify. Another problem is the amount of paper that is used for this system - it is expensive and takes a lot of space to store.

This is a very slow process, that could be easily implemented in a more automated manner, without wasting paper and physical space.

2.2 Radio-Frequency Identification (RFID)

Radio-Frequency Identification, more commonly called RFID, is a technology that was invented around the 1940s as a means for remotely identifying military aircraft [Kas+10][MY09]. It was also used for industrial and commercial purposes by the 1980s, but nowadays, because it is a wireless technique for identifying physical objects remotely, where the wave frequency of their tags stands between 3 KHz and 300 GHz, although the system overall (with all the necessary components) is is still expensive, this technology can replace other concepts that are used in our daily-bases, such as bar code and magnetic cards, because of its various advantages [SGF12][SK12].

RFID systems require two main components: RFID readers and tags, and an application or software package running on a computer [Kas+12].

2.2.1 RFID tag and reader RFID tag and reader are the hardware components of an RFID system. A tag consists of a microchip, that has a unique number, and an antenna and, depending on the use, it can be disguised in a variety of objects (i.e., ID cards, supermarket items, and so on). The microchip can store up to 2KB of information and can be one of three types: active, semi-active and passive. The first two require an internal battery, while the other one does not [Kas+12].

On the other hand, the reader is used to establish the communication between the tags and the software. The reader contains a transmitter and a receiver (some can be equipped with a display interface as well) [Kas+10]. A reader can be active, i.e., it can detect an active RFID tag, and passive, which can only detect a passive RFID tag just a few centimeters away from the reader (the range depends on the device and its cost) [Kas+12].

2.2.2 Software There is always software along with the reader in an RFID system. Because the reader fetches information (from aircraft details to student's name, and time of information exchange), there is normally a Database and a Web Server [Kas+12]. A Database is used to store all the information retrieved from the reader. The Web Server then delivers the information publicly, so it can be accessible on the Internet.

2.2.3 RFID in attendance systems RFID has been used as an student attendance checking system in several teaching facilities. It normally has a passive reader in the entrance of the classroom, and students need to flash their cards to check their attendance [Kas+12]. It is also possible to check online, for example in the university's website, how many classes a student has and has not attended.

Although this type of system does prevent some of the problems of manual attendance checking system (the fact that is automated), this one does not prevent from bringing another student's card and to flash it as well, and does not have a backup solution when a student forgets his/her card. It also requires extra hardware; some faculties do not have RFID readers in every room, and in a case where a class needs to be taken in a different room, it could cost time of the class. Also, not only the maintenance and repair of this type of equipment can be really expensive, but this system, in a class with not just a few students, can create a queue for who is waiting to flash their card (which can delay the beginning of the class).

2.3 Biometrics and Face Recognition

Biometrics and Face Recognition are two types of system that extract key features of human characteristics. Biometric does the identification and verification given physical and behavioral traits, such as fingerprints, irises, retinal patterns, fingerprints, voice, etc [COE17]. Face Recognition analysis key point features of the human's face - nose, mouth, edges, eyes and other characteristics [Luk+16].

In the scope of automated attendance systems, both of these techniques do not require that students bring extra hardware to take the attendance, but it must exist in the faculty, and it also needs to be maintained.

2.3.1 Biometrics in attendance systems Biometrics can be used in many ways for attendance checking system in classrooms.

In Thailand, for a Computer Architecture class in the Faculty of Engineering and Technology, it was implemented the combination between Google Forms and a Speech Recognition system [Tun17]. Upon the beginning of the class, the professor registers the students that arrived on time by marking check boxes in Google Form; for the students that arrive late, because speech recognition can detect numbers more accurately than words, the professor reads the last three digits of the student's number to the (phone's) microphone - students can then check on the screen that their attendance was marked.

Other option is to use fingerprint; G. Talaviya et. al. created a system where, in the first 20 minutes of the class, students can mark their presence by simply putting their finger in a fingerprint sensor, that can be moved dynamically and wirelessly by the students around the classroom [TRS13]. After scanning their fingerprint, students can check their attendance being registered just by looking at the screen projected on the wall. In this system, an updated attendance email is send to the professor and the students, so they can be informed about the student's attendance.

It is also possible to combine biometric and face recognition for an extra layer of authentication. In Covenant University, in Nigeria, it was implemented a bimodal biometric automated attendance system, using the combination of facial recognition and fingerprint from the students [COE17]. The students enter the classroom and have to, one at a time, individually, use the professor's computer to take ten different pictures (with different postures) and capture his/hers fingerprint four times in a fingerprint reader. With this double authentication, it is possible to erase the problems with just one biometric system.

2.3.2 Face Recognition in attendance systems In most scenarios in which attendance systems uses Face Recognition techniques, a camera is installed in the classroom and it viewing angle captures all the sits of the room.

Typically, the systems already has a database with photos of the students who are taking the course, and the picture taken during class is compared with the one that already exists.

In a class with 16 students in Universitas Pelita Harapan in Indonesia, 82% of the results were successful, with 128 out of 148 resulted in a matching face recognition. The other 18% results matched different students or different face expressions [Luk+16].

Other functionalists can be used with this technique. In Slovakia, besides the attendance tracking system, face recognition was used to check if a room was empty or not - this is a good use of this technique, in a case where a class is dismissed earlier, for example [Kai+15].

This system is not time consuming because the students are automatically (and indirectly) monitored during lectures, so it does not take time from the class, the students or the professor to check the attendance [Ash+18]. On the other hand, it requires maintenance of the camera, has a slightly high false-positive rate (around 10%) - which requires the professor to verify those cases and check the students' attendance manually, in every class - and presents privacy concerns for the students. Nowadays, it is required that students allow a picture to be taken of them - in a case where at least one student does not allow this, the system cannot be used.

2.4 Mobile devices and GPS location

It is possible to carry a lot of information and features with a mobile phone - one of them can be to check attendance in a classroom, with passwords or current location, for example.

This type of attendance checking system has the advantage of not requiring the students, faculty and professors to carry extra hardware because nowadays *everyone* carries a smart-phone in their pocket.

2.4.1 Mobile devices in attendance systems For an attendance checking system, a basic implementation can be done with mobile devices. As an example, in Khulna University of Engineering & Technology in Bangladesh it was created a system that uses an Android app where students can register their attendance [Isl+18].

A more complex system was implemented in a Japanese university: an attendance tracking system using a Bluetooth Low Energy (BLE) beacon and Android devices [Nog+15]. In class, the professor turns on the BLE beacon to transmit a magic number to the Android devices inside the room. The students then run the application and scan their cards on a NFC reader. The Android devices receive the magic number and then send it with the scanned ID and name together, to the server. This system not only registers the attendance of students, but it also reduces the time for attendance registration, using multiple devices in parallel; it also eliminates false attempts from students outside the classroom, because of the BLE beacon device - the signal covers the entire classroom (about 30 meters) and it is blocked by the wall, so no one outside can receive the magic number.

It is also possible to use a mobile phone as a security token for authentication [HJV07]. Hallsteinsen et. al implemented a One-Time Password (OTP) where, to mark attendance, the students had to complete a challenge that is sent to their mobile phone after logging in. Also using OTP, in American University of Sharjah, exists a system that generates a password with factors that are known by both entities - user and server [AZEH09]. If the password matches, the user in authenticated. If this password expires, an SMS-based mechanism is also implemented so it is possible to retrieve the password to connect to the server.

Also, in Técnico Lisboa, using a small USB powered router wireless access point, IocDev was developed as a means to check the student's attendance

[AB13]. In this system, students need a way to access the internet (via Wifi), and then just need to provide their credentials, the class pin (that the professor writes on the board) and the current shift - besides the first class, where it is required to create an account. The attendance is only valid if it is within the class schedule, and it is restricted to one attendance per device. Also, the attendance is only valid if the student's device can connect to the Wifi access point, that is the student is inside the class (yet, students that are very close to the classroom may be able to connect).

2.4.2 GPS location in attendance system Applying location in an attendance system was implemented in SMARTDOT [AVS18]. This system requires the students to download an Android application and it calculates the distance between the student's and the professor's device. A more complex approach, also using location as an attendance system, was done in Beijing, in School of Software, where it was implemented an automated student attendance tracking system based on location (and voiceprint) [NKA16]. For the location part, because GPS signal is too weak, it is used a service provided by Baidu Inc, which combines results from GPS, cellular network and Wi-Fi signals. In class, after the voiceprint verification, the distance between the student's mobile phone and the professor's computer is verified; if the distance is in range, the attendance is checked, otherwise, it is not.

2.5 Software-only systems

Also related to portable devices, there are some softwares publicly available whose purpose can be to do the attendance checking in classrooms. Usually, these systems are malleable, in a way that, in a students attendance tracking, the professor can manipulate whatever way wanted. From various software-only systems, the more common ones are the *Quick Response (QR) Code* and *Kahoot!*, that are explained in the following two sub-subsections. A not so common solution is *Top Hat*, that is explained in 2.5.3.

As opposed to the attendance systems that were previously described, this software-only systems not only do not require (extra) hardware, but also do not have the solo purpose to do the attendance checking, but can and commonly are used in that sense.

2.5.1 *Quick Response* (QR) *Code* *Quick Response Code*, better known by *QR code*, is a technology that has been widely used by many industries [Tal18]. In the field of student's attendance system, this technology, opposed to the previous ones that required extra hardware, has a cheaper development cost, and it is easier to use.

Instead of using standard attendance systems, an automated application was implemented in Malaysian Institute of Information Technology where students could generate unique (and non-transferable) *QR Code* with their mobile phone, that in class could be scanned by the professor.

2.5.2 ***Kahoot!*** *Kahoot!* is a recent company, born in March 2013, with the purpose of improving the education around the world [1]. Through questions that can be personalized by the professor - for example, inserting pictures - the students only need the code of the game to enter and start playing. As a game-based platform, that can be created by anyone and played by who has the code of the game, its layout engages students in a healthy competitive way. In the end of the quiz, it is possible to check the top 3 players.

In University of Moratuwa, in a class to teach English as a Second Language (ESL), two types of vocabulary quizzes where made for two distinct groups of 15 students each: a pen and paper one, and another using *Kahoot!* [Pre17]. After weeks of testing both quizzes, it was concluded that the group taking quizzes using *Kahoot!* had better results, as well as more attendance. Also, in United Arab Emirates, in an introductory physics class, *Kahoot!* was used not only to challenge and motivate physics students, but also to check their attendance (if the student participates in the *Kahoot!* game has to be in the classroom) [AG18].

2.5.3 **Top Hat** Also using a web browser, Top Hat is a good solution for a costless attendance system [2] . Requires the students to correctly submit a 4-digit code and to be present in the classroom. The presence is checked by the geolocation and proximity to other students that are also submitting the code (it requires access to the device's location to be allowed by the students).

2.6 Device fingerprinting

It is known that Internet of Things is becoming an essential part in the daily life of those who manipulate wireless technologies [Xu+16]. Looking on the bright side, this technologies can be connected anytime and anywhere, at a low cost. Yet, they also come with vulnerabilities, that can compromise confidentiality, integrity and authentication of data communication.

There is a process that can gather signatures and characteristics from a user called Device Fingerprinting. The basic idea is to gather device-specific information (such as mobile phone's brand, screen's dimension or the list of installed fonts) to form a signature - an identification - of a specific user - applying this not to a couple informations, but many, to thousands of people. A experiment made in 2010 showed that half a million users who participated, using Flash or Java, had a unique device fingerprint [Aca+13].

This technique can be used in attendance systems to validate if a student is indeed taking his/her attendance and to catch fraud cases - if a student suddenly changes its way of taking the attendance, or if the fingerprint matches exactly a colleague, this technique can flag the students.

[1] `:https://kahoot.com/` (visited on 10/24/2018)

[2] `https://support.tophat.com/s/article/Student-Secure-Attendance` (visited on 12/05/2018)

2.7 Discussion

After researching different types of student attendance systems, there are advantages and disadvantages that will be taken into account while developing the proposed solution, according with the *Objectives* listed in subsection 1.2. In Table 1, the previous mentioned students attendance system are compared with the features that the proposed system aims to achieve.

	MAS	**RFID**	**Biometrics**	**Face Recognition**	**Mobile**	**Software only**
Uses paper	✓	-	-	-	-	-
(extra) Hardware	-	✓	✓	✓	-	-
Requires Internet-connected device	-	-	-	-	✓	✓
Expensive	✓	✓	✓	✓	-	-
Portable	✓	-	-	-	✓	✓
Efficient	-	✓	✓	✓	✓	✓
Time consuming	✓	✓	✓	-	-	-
Violates privacy concerns	-	-	✓	✓	-	-
Can be cheated	✓	✓	-	-	-	✓
Can be done after class starts	✓	✓	✓	✓	✓	✓
Easily implemented	✓	-	-	-	✓	✓
(afterwards) Available online	✓	✓	✓	✓	✓	✓

Table 1: Comparison between different student's attendance systems.

It is possible to verify that the majority of them does not use paper (only the Manual Attendance System (MAS)), but on the other hand do require extra hardware; more common was hardware that the faculty must have and maintain, such as an RFID reader, or a camera. This is a major disadvantage, because it can be expensive not only because of the material itself, but because it is required to exist in all the classrooms. And because of this, they are also not easily implemented; requires a technician to implement and keep the systems up to date and maintained. In large universities, this can be a problem and can compromise some classes (if the system is not available to be used, or needs to be fixed).

Only the Mobile devices and GPS location and Software-only systems require the students to carry an internet-connect device (such as a mobile phone or computer), offering no option for the students who do not. Also, in underground or indoors classroom, the GPS signal can be weak, which compromises the attendance checking.

Overall, the systems can be available online and are effective, as they get the job done - the attendance is checked for, at least, the students that are in the classroom. But, on the other hand, some can be time consuming. In classes with a lot of students, some systems (namely Manual Attendance System (MAS), Radio-Frequency Identification (RFID) and Biometrics) can create a queue of students, waiting to take their attendance, which can delay the beginning of the class.

All the systems allow the students that do not arrive on time, can also check their attendance. This is an advantage and can also be a disadvantage, because taking the attendance can disturb or, in some situations, stop the class (in a scenario where the professor is involved in the verification).

The Biometrics and Face Recognition systems, although they have a high percentage of recognition/match, present privacy concerns for the students. For instance, if one student does not allow a picture of them to be taken during class, or does not want to scan their fingerprint, systems using this type of verification will not be effective.

With all the systems, only the Manual Attendance System (MAS), Radio-Frequency Identification (RFID) and the Software-only systems can be cheated. The first one, because it is possible to sign for another students without calling the professor's attention; the second one, it is by simply flashing someone else's card (in a class with a lot of students, or when the RFID reader is not close to the professor, it is impossible to keep track of how many cards a student is flashing). The third and final one, in systems where more than one student can take attendance in the same device, without GPS location, it is possible to take the attendance for more than one student.

In conclusion, neither of these systems has the same specification as the one that is proposed. Yet, it is possible to use and improve some ideas from these systems. In the next section the *Proposed Solution* is presented.

3 Proposed Solution

This section presents the work that is proposed, according to the specifications listed in *Objectives*. The subsection 3.1 *Approach* explains the proposed system, regarding the *Security and Validation* (in subsubsection 3.1.1) that will be implemented in the system as well as a more detailed specifications in the subsubsection 3.1.2 - *Architecture*. In *Assessing Code Entry*, a series of tests made are detailed and analyzed. To conclude this section, in subsection 3.3, details the *Prototypes* that were made.

How and what type of evaluation will be done, is explained in the next section 4 - *Evaluation*. To conclude, the plan to be followed during the coming semester is presented in section 5 - *Planning*.

3.1 Approach

The original problem can be summarized as "*How can an attendance be verified in universities in an automated manner without being cheated by the students?*".

To achieve the objectives listed in subsection 1.2 a set of characteristics and boundaries will be implemented.

For a **costless and portable** solution, a website will be developed - so it is not required extra-hardware for the university, students nor the professor. This approach is compatible with the different operative systems that currently exist for portable devices (such as mobile phones and computer, which is what a university student usually carry), and because it will not require students to download any (extra) software. So that **only students inside the classroom can check their attendance**, it will be required, to take the attendance, that students type a series of consecutive random codes with a limited time to type each code. This makes the job to take the attendance for a colleague harder, because students will have just a few seconds to type each code, leaving a shorter time to type the code for another person or even send it.

In a scenario where a student inside the class tries to type the code for a classmate, the system will prevent those attempts using Device Fingerprinting. Each student will have a *unique* fingerprint; if two or more attendances have a very similar fingerprint (which will become more unlikely throughout the testing phase) those students will be flagged and asked by the professor afterwards - to disguise a possible attempt of a student taking attendance for a classmate or if indeed two (or more) students have a very similar fingerprint.

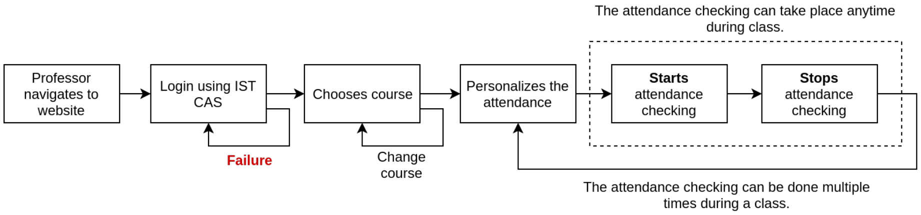
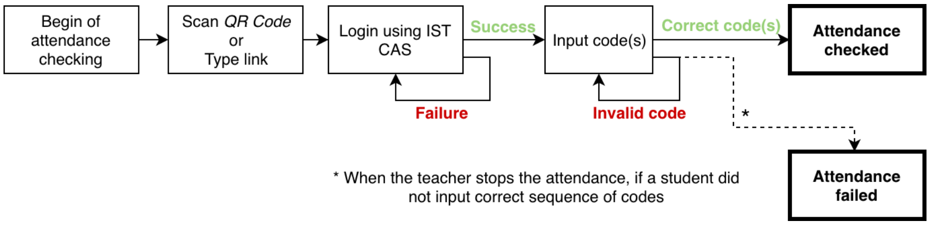

The attendance checking can take place anytime during class.
Professor navigates to website
Login using IST CAS
Chooses course
Personalizes the attendance
Starts attendance checking
Stops attendance checking
Failure
Change course
The attendance checking can be done multiple times during a class.

Fig. 1: Professor's perspective of the attendance checking.

The proposed system will have two distinct sides: the professor's and the student's. For the professor's side, it is only required that the professor (or the classroom) possesses a computer and a projector in the classroom (usually all classrooms in universities have one). The flow of the professor's perspective is visually explained in Figure 1; when intended by the professor - it can be done several times, for example, in the beginning for the students that arrived on time, and/or the end of class, for the students that attended the class but did not arrive on time - the attendance checking can start. Using the computer, that is connected to the projector, the professor navigates to a website, enters the personal credentials and chooses the course that is lecturing. Then, a *QR Code* and a link will appear for the students to scan/type - so the students can access the website to check their attendance. Then, it is possible for the professor to start the attendance (the link to the website will still be available on the screen, so students that did not arrive on time can still type the link). As intended by the professor, it is possible to stop the attendance at any time. In case the students finish the attendance checking (correctly entering the sequence of random codes) the professor can stop the attendance, but because usually the students are running between classes, the time is manipulated by the professor, depending on how many students are in the class or still entering the room. The time to type each code, the number of consecutive correct codes necessary to take the attendance, the length and type of the code (letters, number or letters and numbers) is defined by the professor. This definition can be done until the beginning of the attendance checking, but it can also be done in the beginning of the semester, creating all classes of a course with a specific configuration (that can be adjusted anytime during the semester).

For the student's side, the beginning is similar (Figure 2). The students can scan the *QR Code* or type the link that is being projected on the wall. Then, it is required that students login using their student's credentials. After logging in, the students will need to type a series of random codes into their devices to check their attendance successfully.



* When the teacher stops the attendance, if a student did not input correct sequence of codes

Fig. 2: Student's perspective of the attendance checking.

Regarding the students that, usually in the beginning of the course, have not yet enrolled, the professor can also manually mark the attendance in the website (the same happens if a student does not have a way to access the internet). In a scenario where no students show up in class, it is possible, for the professor to mark all students as absent (instead of going to the process of starting the attendance checking).

3.1.1 Security and Validation To assure that the system is secure and does not allow students that are not in the classroom can check their attendance, a set of boundaries and validations will be implemented in the system.

For each class, the link to take the attendance will be different - this is not on the course's website, so only the students in the class are able to scan it; this ensures, to some degree, that the students are in class. Students in class can (and probably will) send a picture or the content of the *QR code* to other students. Some of these attempts can be detected in the following steps of the attendance.

Also, from the very first class, a set of information will be retrieved from the students' browser, as they use the website to check their attendance. A signature will be developed for each students - a *Device Fingerprint* of the device - that can be the device's brand, list of plugins, user agent and so on [3]. When some of this information, in an attendance checking, does not match nix the previous ones, that student will be *flagged* (and can be questioned by the end of the class by the professor). Some students will probably have matching information, but not in every aspect. The same student can try to take two distinct attendances with different browsers in the same device - with Device Fingerprint, it is possible to distinguish, even using different browsers, because it extracts information from the device itself (e.g. operating system, screen resolution, use of local storage, list of fonts, etc). If two (or more) students share the exact same information (and that behavior is not usual), those students are *flagged* and can be questioned by the end of the class (this situation can disguise the students that checked a presence for a classmate that is not in the room).

3.1.2 Architecture The functional architecture of the proposed system is illustrated in Figure 3.

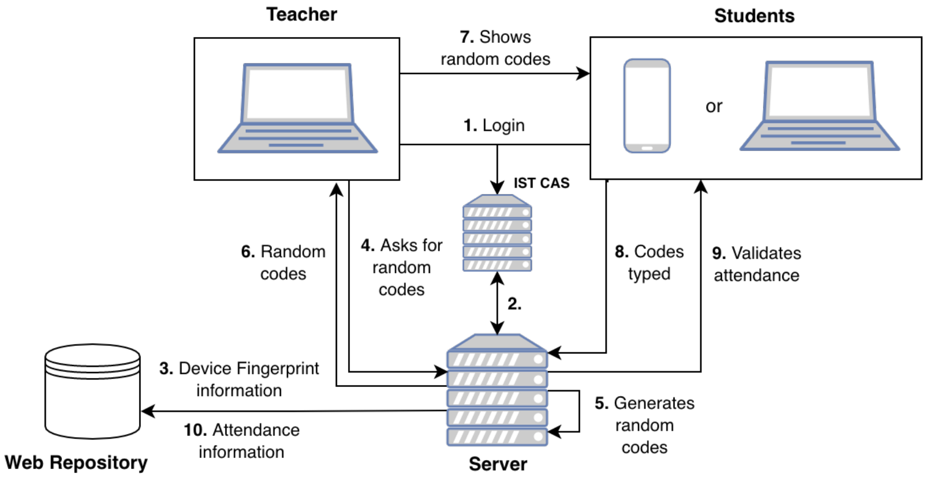


Fig. 3: Overview of the system's architecture.

The student's portable device and the professor's computer will be the clients, and the communication with the server is done via Wi-Fi. The difference between the two clients is that the professor has the ability to show the generated codes (that the server provides) and the student's devices can type the codes and send

[3] https://amiunique.org/ (visited on 12/10/2018)

them to the server (in real time), so that the server can compare with the ones that were generated.

The Web Repository will be used to store the attendance records, the information extracted from each device fingerprint as well as information to do the system's evaluation (it is explained in the following sub-section). In the first implementation, IST *Centralized Authentication System* (CAS), as an authentication system, will serve as an intermediary for the user's authentication [4]. This can be changed during the testing phase with a different authentication system - such as *Google* or *Facebook* - because with these, the students may be more resilient to share their password. Another possible solution can be with no authentication at all, if the device fingerprinting technique shows enough robustness to do the authentication by itself.

3.2 Assessing Code Entry

In order to understand how much time a student needs to type a code, and the perfect length of the code (and if it could be made with capital letters and/or numbers), a series of tests were made. The goal of these tests was to understand, for each type and length of code, how much time a student takes to input the code (without failing) and without giving too much time - so the task does not take too long and does not leave space to send or do for other person.

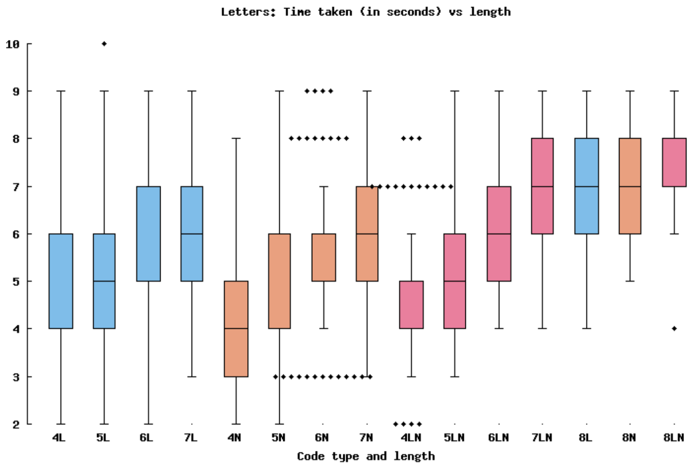


Fig. 4: Overview of the time taken according to the code type and length, in the first tests, where "L" (blue), "N" (orange) and "LN" (pink) stands for "Letters", "Numbers" and "Letters and Numbers", respectively.

[4] `https://si.tecnico.ulisboa.pt/servicos/autenticacao-e-acesso/autenticacao-cas/` (visited on 12/10/2018)

The tests consisted in typing five sequential (and random) codes with five different lengths (from four to eight characters) and three different type of codes (numbers, letters and numbers and letters), with 10 seconds to type each code - giving, in total, 15 combinations. The type of code chosen was to understand, from the three different types of codes, what would suit better in an attendance system, not being too hard but also good enough to not give too much time to send or do for another classmate. The time chosen (10 seconds), given the intended scenario, was the more reasonable that did not take too much time nor too less to do the task in a quick and automated manner. The sequential five codes were chosen as a good length, giving an overall duration of 50 seconds to do the task.

Every combination was done in a random order. Each time the user submitted a code, the system was registering the code length, type of code, if the code generated was equal to the inserted one and the time left to type that specific code. After each test, two questions were asked: *The number of characters was easy to type?* and *The time to type the code was sufficient?*, giving a 1 to 5 scale to answer, being 1 as *Strongly disagree* and 5 as *Strongly agree*. Given the fact that the tests were done in a random order, the questions were asked to understand how the user felt about the type of code and the time to type it.

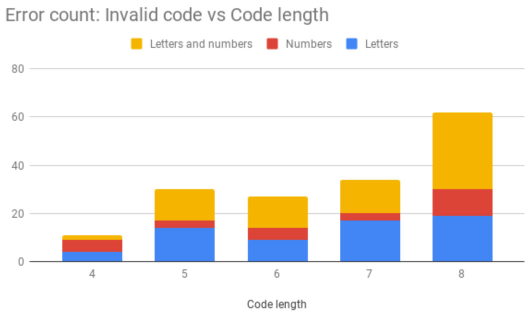


Fig. 5: Overview of the error count, according to the code type and length, in the first tests.

These tests were done with students from Técnico Lisboa; these users were chosen because they are part of the target end-users of the proposed system. Testing with 25 students individually, in a class scenario - where the user used a portable device to type the codes, and the generated random codes were being projected on a wall - 20 of them were done using a (personal) mobile phone, and the rest with a (personal) computer, it is possible to conclude different aspects.

Looking at Figure 4 - a *boxplot* with the time taken by the users to type the different code types and lengths (where blue, orange and pink represents the tests with just letters, numbers and letters and numbers, respectively) - it is possible to conclude that, overall, the users take less time typing codes with just numbers, and take more time typing codes with letters and numbers.

Regarding the errors, i.e., when the users did not type the correct code (may have been because there was no sufficient time, or because some letters seemed numbers and vice-versa), the tests showed that less errors happen when the code is just numbers, and more errors when the code is numbers and letters. In the tests, 162 out of all the input codes (1875 in total) were an error; 63 out of the 162 were codes with just letters, and 72 were letters and numbers, leaving the codes with just numbers with only 27 errors. An overview of the errors, according to the code type and length, can be seen in Figure 5.

Based on the answers from the tests' questions, the results showed that (only) the second question (*The time to type the code was sufficient?*) had a statistically significant difference as determined by *one-way ANOVA* ($F(2, 360) = 7.13, p = 0.001$), and a *Tukey's post hoc* test revealed that the statistically different was in the codes with letters and numbers. Also, taking a look at the answers (Figure 6), codes with just numbers had a significant higher score in both questions - so the students were more comfortable typing just numbers.

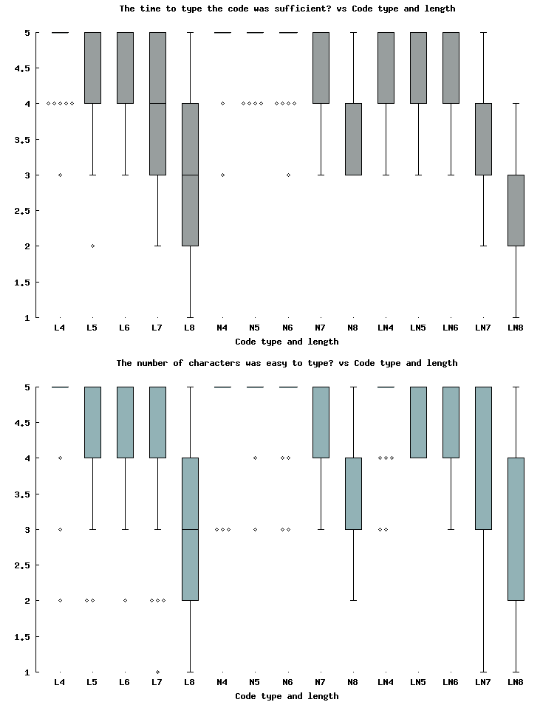


Fig. 6: Answers from the questions *The number of characters was easy to type?* and *The time to type the code was sufficient?*, in a scale of 1 to 5, 1 being *Strongly disagree* and 5 *Strongly agree.*

Then, based on the time taken to input the codes in each test, also using *one-way ANOVA* to analyze the variance, the time taken to input the codes had a significant variance ($F(2, 1811) = 7.59, p = 0.001$), and in *Tukey's post hoc* test, it was concluded that it was in the tests where the code type was numbers and letters and the length higher than five.

Giving into account all the results from the tests, it is possible to conclude that the best combination is letters as a code type and a length of 5 characters, not only because the average students can type with no problem, but also does not give too much time to send or do for a colleague.

3.3 Prototypes

To begin the idea of the system, **Storyboards** were made for an easy, quick and cost-less first prototype. The first ideas were to check the student's attendance in the beginning and end of class, but after re-evaluating the scenario, the end of class could be a problem, because classes tend to finish on a tight schedule, without giving time (during class) for every student to check their attendance. So, it was concluded that the professor is the one that chooses when to take the attendance. It can be done in the beginning for those who arrive on time, and in the only only for those who did not, for example example. After several iterations, the final version of the storyboards were made. The three scenarios of the student's side were designed: students arriving on time and checking their attendance (as presented in Figure 7), students arriving on time and failing to check their attendance, and students arriving late and checking their attendance in the end of class. For the professor's side, a storyboard was also made, showing the professor beginning and ending the attendance checking (as presented in Figure 8).

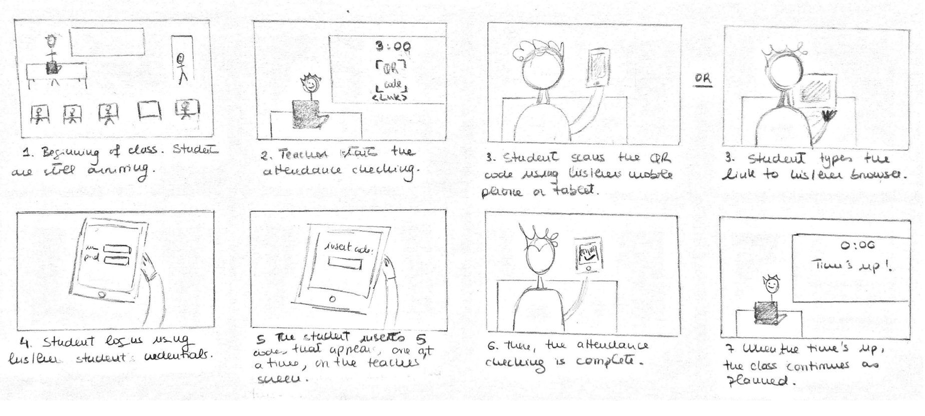

3:00
QR
code
<Link>
1. Beginning of class. Student are still arriving.
2. Teacher starts the attendance checking.
3. Student scans the QR code using his/her mobile phone or tablet.
OR
3. Student types the link to his/her browser.
insert code:
4. Student logs in using his/her student credentials.
5 The student inserts 5 codes that appear, one at a time, on the teacher's screen.
6. Then, the attendance checking is complete.
0:00
Time's up!
7 When the time's up, the class continues as planned.

Fig. 7: Storyboard of the attendance checking in the beginning of class from the student's point of view.

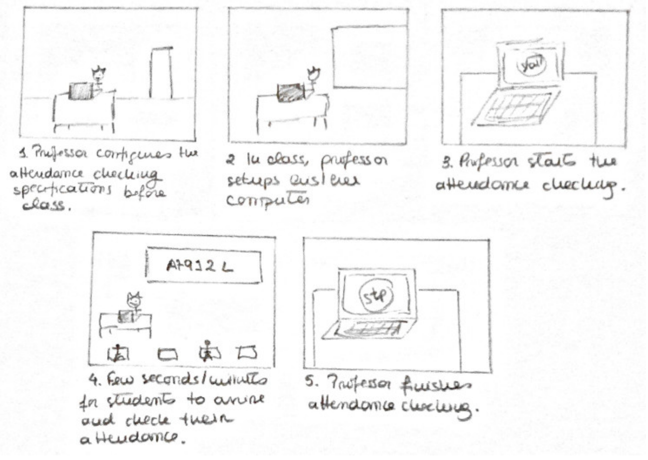

1. Professor configures the attendance checking specifications before class.
2 In class, professor setups his/her computer
3. Professor starts the attendance checking.
4. Few seconds/minutes for students to arrive and check their attendance.
5. Professor finishes attendance checking.
you
A7912L
stp

Fig. 8: Storyboard of the attendance checking from the professor's point of view.

4 Evaluation

For the evaluation of this system, the participants will be students from *Técnico Lisboa* who are taking the masters in Information and Software Engineering, taking the *Multimedia Content Production* course, that takes place annually in the second semester, and, in this case, in the second semester of 2018/19. The evaluation will be done in classes during this semester, in the Alameda campus (with approximately 80 students enrolled). Because in this faculty there are 10 minutes given in each class for the students to arrive *on time*, the attendance checking will be made in between of those 10, in the beginning of the class; in the end, it will be during the last minutes of the class. The first checking will validate the students that arrive on time; the last one, will check who could not make it in the beginning of the class, but arrived sometime during. The rest of the evaluation will be based on the following data:

1. Effectiveness;
2. Efficiency;
3. Error rate;
4. Cheating rate;
5. Device fingerprinting analysis:
   - False negative rate;
   - Threshold;
6. Attendance tendencies.

To evaluate the first metric, the intended data that must be retrieved if a student did check his/her attendance in the right time. For this, during each class, the number of students inside the classroom will be counted. Then, the effectiveness will be calculated accordingly with the respective formula:

$$\frac{N_{present}}{N_{registered}} * 100 \tag{1}$$

where *N_registered* is the number of attendance registered by the system, and *N_present* the number of students in class, which will be counted by the author. The multiplication by 100 is done to get the result in percentage.

The second metric is to evaluate the time and number of clicks the students take to check their attendances. The efficiency will be subdivided in two categories/formulas: the number of clicks and the duration of the attendance. The average efficiency formula will be calculated based on the efficiency calculated for both data, based on the following formula:

$$\frac{real}{expected} * 100 \tag{2}$$

where *expected* is the time or number of clicks expected, and *real* the time or clicks the students take to check their attendance. The results of this should show that, in the first classes, the students take some time (to learn and get used to the systems) and do more clicks; throughout the weeks, the action will gradually take less time, and, proportionally, less clicks. A graphical representation of the learning curve, giving the learning throughout the experience, will be made.

The third metric will register the number of failed attempts per students. This evaluation will take into account the number of students that attend the class, resulting in a line graph representation. In the beginning of the classes, the students should not have a high error rate and, by the end of the semester, this result should be close to zero.

Then, given that the number of students in each class will be counted, it is possible to compare with the number of students that check their attendance, to evaluate the *Cheating rate* - the fourth metric. This metric will also help with the following one, the *Device fingerprinting analysis*, to analyze the False negative rate (i.e., when the system failed to identify the same device used to check two, or more, attendances) and also to evaluate the Threshold - to improve the attendance checking, it is possible that this value change through testing. For the *Device fingerprinting analysis*, each extracted attribute will have a different weight - to distinguish the attributes, according to its uniqueness - so it possible to have two distinct thresholds: one for the cases where a student is suspected to be tricking the system, and another one that confirms that the student indeed tricked the system.

The sixth and final evaluation is to check the *Attendance tendencies* throughout the semester. It is expected that students attend more classes in the beginning of the semester and more close to evaluation dates.

5 Planning

Next, the plan to be followed, while developing and testing this project during the coming academic year, is visually present in Figure 9.

The system is ready to be tested upon the beginning of the classes, in the second semester, starting in February 18th, 2019. It will be used until May 31th, 2019 (the end of the semester). The evaluation will be done along with the go live system, until the end of the semester.

Upon the beginning of the semester and the first contact between the students and professors with the system, improvements and bug fixes will happen according to the needs of the users, with the possibility of new features being added to the system. During the semester, (major) updates will be made in the system, and will go live in the second week of each month, until the end of the semester. The second week of the month was chosen due to the fact that the semester begins in the middle of February, and comes to an end in the end of May, so in this scenario it is possible to have three major updates that can be tested correctly, with enough time and without leaving a major gap in the last month of class.

As of March, the writing of the dissertation begins, as the system evolves along the semester. The dissertation will be delivered by the end of June.

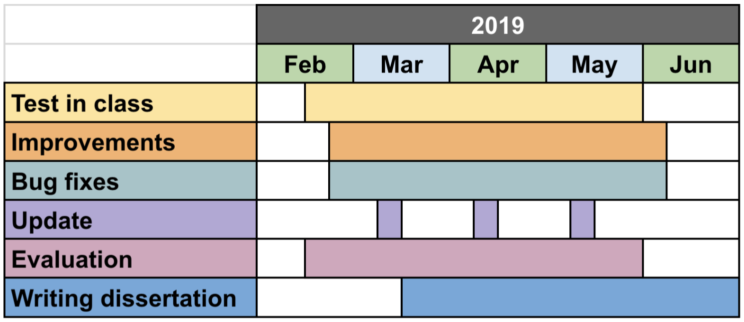


Fig. 9: Planed schedule for the coming semester.

6 Conclusion

Tracking student's attendance in classrooms has been a problem for professors for a long time, not only because of the difficulty to guarantee that the student is indeed the room, but also because of the time it sometimes consumes afterwards.

Thereby, to fill the existing gap in this field, an automated attendance system is proposed. Combining the perks of the existing attendance systems, and also having in mind the flaws, ***I Am Here!*** is a promising solution for this problem.

References

[Kas+12] Murizah Kassim et al. "Web-based student attendance system using RFID technology". In: *Proceedings - 2012 IEEE Control and System Graduate Research Colloquium, ICSGRC 2012*. Icsgrc. 2012, pp. 213–218. DOI: `10.1109/ICSGRC.2012.6287164`.

[Kas+10] A. Kassem et al. "An RFID attendance and monitoring system for university applications". In: *2010 IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2010 - Proceedings* (2010), pp. 851–854. DOI: `10.1109/ICECS.2010.5724646`.

[MY09] Mohd Ikhsan Moksin and Norizan Mohd Yasin. "The implementation of wireless student attendance system in an examination procedure". In: *2009 International Association of Computer Science and Information Technology - Spring Conference, IACSIT-SC 2009* (2009), pp. 174–177. DOI: `10.1109/IACSIT-SC.2009.130`.

[SGF12] Nurbek Saparkhojayev, Selim Guvercin, and Engineering Faculty. "Attendance Control System based on RFID-technology". In: *IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012* 9.3 (2012), pp. 227–230.

[SK12] Zatin Singhal and Rajneesh Kumar Gujral. "Any Time Any Where-Remote Monitoring of Attendance System based on RFID using GSM Network". In: *International Journal of Computer Applications* 39.3 (2012), pp. 37–41. DOI: `10.5120/4803-7031`.

[COE17] Atuegwu Charity, Kennedy Okokpujie, and Noma-osaghae Etinosa. "A Bimodal Biometric Student Attendance System". In: *IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)* (2017), pp. 464–471.

[Luk+16] Samuel Lukas et al. "Student attendance system in classroom using face recognition technique". In: *2016 International Conference on Information and Communication Technology Convergence (ICTC)* (2016), pp. 1032–1035. DOI: `10.1109/ICTC.2016.7763360`.

[Tun17] Vasutan Tunbunheng. "Automatic attendance system for late student using speech recognition corresponding with google forms and sheets". In: *Ubi-Media 2017 - Proceedings of the 10th International Conference on Ubi-Media Computing and Workshops with the 4th International Workshop on Advanced E-Learning and the 1st International Workshop on Multimedia and IoT: Networks, Systems and Applications* (2017), pp. 4–7. DOI: `10.1109/UMEDIA.2017.8074119`.

[TRS13] Gunjan Talaviya, Rahul Ramteke, and A K Shete. "Wireless Fingerprint Based College Attendance System Using Zigbee Technology". In: *International Journal of Engineering and Advanced Technology* 2.3 (2013), pp. 201–203.

[Kai+15] O. Kainz et al. "Visual system for student attendance monitoring with non-standard situation detection". In: *ICETA 2014 - 12th IEEE International Conference on Emerging eLearning Technolo-

gies and Applications, Proceedings (2015), pp. 221–226. DOI: 10.1109/ICETA.2014.7107589.

[Ash+18] C Ashwini et al. “An Efficient Attendance System Using Local Binary Pattern and Local Directional Pattern”. In: 8.4 (2018), pp. 43–46.

[Isl+18] Md Milon Islam et al. “Development of smartphone-based student attendance system”. In: *5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017* 2018-Janua (2018), pp. 230–233. DOI: 10.1109/R10-HTC.2017.8288945.

[Nog+15] Shota Noguchi et al. “Student attendance management system with bluetooth low energy beacon and android devices”. In: *Proceedings - 2015 18th International Conference on Network-Based Information Systems, NBiS 2015* (2015), pp. 710–713. DOI: 10.1109/NBiS.2015.109.

[HJV07] Steffen Hallsteinsen, Ivar Jørstad, and Do Van Thanh. “Using the mobile phone as a security token for unified authentication”. In: *Second International Conference on Systems and Networks Communications, ICSNC 2007* Icsnc (2007). DOI: 10.1109/ICSNC.2007.82.

[AZEH09] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. “Two factor authentication using mobile phones”. In: *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* February 2016 (2009), pp. 641–644. DOI: 10.1109/AICCSA.2009.5069395.

[AB13] João Amaral and Rodrigo Bruno. “locDev Client Presence Detection”. In: *Mobile Computing, IST(Instituto Superior Técnico)* 67014 (2013).

[AVS18] Ms Aria, Ms Urvi Verma, and Ms Simran Swamy. “SmartDot – Location Based Attendance”. In: 13.10 (2018), pp. 8507–8510.

[NKA16] Sudheer Kumar Nagothu, Om Prakash Kumar, and G. Anitha. “GPS Aided Autonomous Monitoring and Attendance System”. In: *Procedia Computer Science* 87 (2016), pp. 99–104. DOI: 10.1016/j.procs.2016.05.133.

[Tal18] Bazilah A Talip. “MOBILE ATTENDANCE SYSTEM USING QR CODES TECHNOLOGY”. In: 3.1 (2018), pp. 1–3.

[Pre17] P. B.T.K. Premarathne. “A study on incorporating gamification into ESL classroom via Kahoot!” In: *International Conference on the Humanities (ICH), 2017 Faculty of Humanities, University of Kelaniya, Sri Lanka* (2017), p. 54.

[AG18] Randa Asa’D and Cindy Gunn. “Improving problem solving skills in introductory physics using Kahoot!” In: *Physics Education* 53.5 (2018). DOI: 10.1088/1361-6552/aacade.

[Xu+16] Qiang Xu et al. “Device fingerprinting in wireless networks: Challenges and opportunities”. In: *IEEE Communications Surveys and Tutorials* 18.1 (2016), pp. 94–104. DOI: 10.1109/COMST.2015.2476338. arXiv: 1501.01367.

[Aca+13] Gunes Acar et al. “FPDetective : Dusting the Web for Fingerprinters Categories and Subject Descriptors”. In: *Ccs* (2013), p. 12. DOI: `http://dx.doi.org/10.1145/2508859.2516674`.