Internet of Things (IoT)-Based System for Classroom Access Control and Resource Management

Gleiston Guerrero-Ulloa[1,2] [0000-0001-5990-2357], Jonathan Villafuerte-Solorzano[1] [0000-0002-7801-7369], Michael Yánez[1] [0000-0003-2297-9064], Miguel J. Hornos[2] [0000-0001-5722-9816], Carlos Rodríguez-Domínguez[2] [0000-0001-5626-3115]

[1] State Technical University of Quevedo, Quevedo 120301, Ecuador
[2] University of Granada, Granada 18071, Spain
{gguerrero, jonathan.villafuerte2014, michael.yanez2013}@uteq.edu.ec, gleiston@correo.ugr.es, {mhornos, carlosrodriguez}@ugr.es

Abstract. Internet of Things (IoT) is transforming our society and even the way people interact with their environment. In an IoT-based system (IoTS), the identification, authentication and authorization of people and objects is especially important to be able to avoid privacy and security issues. This paper presents an IoTS to control access to classrooms and to efficiently manage their resources (lights and electric/electronic devices). Since the professor scheduled to teach a lesson at a given moment is the only authorized person to open the classroom door, this IoTS identifies that professor through facial recognition, considering a pre-established classroom schedule. In addition, RFID or fingerprint authentication are used to register the attendance of students to a lesson. To develop this IoTS, TDDM4IoTS (Test-Driven Development Methodology for IoT-based Systems) was used. This methodology encourages user engagement during the IoTS development. In fact, professors were involved from the very beginning, especially to improve the design of the mobile application interfaces, finally achieving 100% acceptance by them.

Keywords: Internet of Things, Development Methodology, Access Control, Facial Recognition, Fingerprint Authentication, Classroom Resource Management.

1 Introduction

Internet of Things (IoT), term coined by Kevin Ashton [1], is one of the paradigms that is in continuous development and is being implemented in a wide range of domains [2]. An IoT-based system (IoTS) integrates multiple devices and technologies, and tries to transform processes, and even change the way people interact with their environment. Although IoT was initially proposed to refer to interoperable and uniquely identifiable connected objects with radio frequency identification (RFID) technology [3, 4], RFID is currently only one of the technologies used.

IoT represents a new paradigm with a holistic environment consisting of many smart devices interconnecting heterogeneous physical objects via the Internet. Many domains, such as logistics, manufacturing, agriculture, home automation, ambient assisted living, smart cities, healthcare, and many other ubiquitous computing applications, are its application fields. By deploying IoTSs, the increased interaction between people and things facilitates the exchange of information and services. However, it also poses new challenges, especially in terms of security and privacy [3].

For the identification of people or things (entities) in an IoTS, one must consider the reliability that the entity is the one it claims to be. RFID is the mechanism for entity identification with which IoT was born. However, the use of this technology facilitates identity theft, as the object that identifies entities (cards, key fobs, tags, etc.) can be easily exchanged. In this context, there are several alternative identity verification methods, especially for individuals, such as biometric fingerprint identification [5, 6], facial recognition [7], iris recognition [8], among other secure methods.

The identification of authorized persons can facilitate the management of resources (e.g., allowing or denying access to certain places, such as buildings, offices, classrooms, etc.) in daily activities and help to reduce wasted time as well as increase people's productivity. Resource management in classroom environments is one of the fields in which IoT has not been widely applied, especially in developing countries. Among the works that have been presented is that of Chan May et al. [9], who proposed an IoTS prototype to control the turning on/off lights and air conditioning according to the schedules established for a cubicle in the building of professors. With this prototype, energy savings were achieved.

In a classroom environment of a higher education institution, it is expected to have, in addition to the lights and air conditioning or heating, the video projector, and of course the entrance control to these environments. In this work, we propose an IoTS that aims not only to manage classroom resources but also to control access to classrooms, deploying the necessary devices in the environment. For this last purpose, and more specifically, to open the classroom door, facial recognition has been used implemented to identify the authorized person (professor) who can open the classroom at a given time, according to the established class schedule. In addition, students are registered by fingerprint.

This IoTS has been implemented at the State Technical University of Quevedo (UTEQ), Ecuador, which has some new buildings dedicated to administrative offices and classrooms, in which post-pandemic on-site activities are carried out, in addition to the previously existing buildings, due to an increase in the number of academic degrees offered. Therefore, staffing needs grown but, due to the economic crisis the country is going through, it is not feasible to increase the number of employees. Consequently, the solution adopted was to automate some tasks, thus avoiding overloading existing staff. Moreover, crime has grown exponentially lately and, although the university has private guards to protect its assets and there have been no robberies yet, these could happen at any time, since there is no control of people walking into the university's facilities. Therefore, a system that allows only authorized persons to enter classrooms and computer labs ensures greater security and protection of the resources in them.

The remaining of the paper is organised as follows: Section 2 is devoted to the related work. Section 3 presents the IoTS proposed and how it has been developed. Finally, Section 4 outlines the conclusions.

2 Related work

Undoubtedly, the identification of people to access information and enable resource use is very important. Mohammad et al. [10] present a system for healthcare management, in which they propose identification using RFID tags and the issuance of digital signatures. The identifier stored on the RFID tag is used to log into a mobile application. Both the physician and the patient are enabled to use the system by the corresponding RFID tag, but not to activate any sensor or get any response from any actuator in the system, since the patient is the one who provides follow-up on their health, and the physician is the one who issues notifications or suggestions to the patient.

Another work where people are identified to control their access to certain spaces (of a house, in this case) is the one presented by Guerrero-Ulloa et al. [11], in which they use RDIF cards and tags. This is an IoTS for the care of people with mild cognitive impairment within the home, which alerts caregivers when patients approach places that are considered dangerous for these people. Being aware of the impersonation problems that RFID tags and cards can cause, Guerrero-Ulloa et al. [12] present a facial recognition system for the identification of people in a multi-patient medication IoTS through a medicine dispenser. Once the system has recognized the patient, it dispenses the medication to be taken at that time.

Moreover, Wang et al. [13] propose a method for worker identification based on their helmet colour identification. The system, which detects moving objects, establishes the head of the people who are among those objects as the region of interest (RoI) of the image. With this RoI, it identifies the worker and the type of work they are doing based on the colour of the helmet they are wearing. In our work, we do something similar. The face of the person in front of the camera is detected with a resolution of 8 bits in grayscale, this being the RoI in our case. This RoI is used to recognize the person and depending on who they are and the moment of recognition grant or deny them access to the classroom in question.

3 Proposed system

The proposed IoTS is a classroom access control and resource management system, called SISGERA (which is the acronym for its name in Spanish: *SIStema de GEstión de Recursos del Aula*). SISGERA aims to achieve two objectives: (1) automating the control of both attendance and access to classrooms, and (2) providing a more efficient use of electrical and electronic devices (lights, air conditioners, and video projectors) installed in classrooms, saving energy whenever possible. In this sense, the mentioned equipment and lights used in each classroom will remain on only if there are people in the classroom and their use is necessary. In addition, the automation of the air conditioning based on the schedule of classroom use and the climatic condition of the moment also aims to save the cost of electrical energy. Nonetheless, the professor who is in the classroom can always make the decisions that s/he deems appropriate regarding the use of electrical and electronic devices installed in it.

A prototype of SISGERA was implemented in classroom FCI-308. This classroom, like any other, has a schedule of use from Monday to Friday, from 07:30 to 20:30. The use of classrooms is per module. Each module consists of 25 to 30 hours of class per week. As an example of a classroom use schedule, we provide below the morning shift schedule of the aforementioned classroom, which is used to teach the nineth module of the Mechanical Engineering degree: Monday, Tuesday and Thursday (07:30-10:30 and 10:30-12:30), Wednesday (09:30-12:30), and Friday (09:30-11:30 and 11:30-12:30). However, lessons are given for the eighth module of the Environmental Engineering degree in the same classroom during afternoon shift, which is as follows: Monday (13:30-15:30 and 15:30-17:30), Tuesday and Wednesday (12:30-14:30 and 14:30-17:30), Thursday (13:30-16:30 and 16:30-17:30), and Friday (12:30-13:30, 13:30-14:30 and 14:30-17:30).

As the travel time that professors need to go to the corresponding classroom is between 5 and 15 minutes, the time that lights, air conditioners and video projectors will remain on without use will be between 95 and 285 minutes per day, not to mention the days that morning students finish their classes before the afternoon students start theirs. The latter can cause lights and equipment to remain on for hours unnecessarily. In addition, when students have classes in computer labs, applied physics labs or other environments (depending on the degree), they must leave their usual classrooms, which implies the devices (and, in some cases, even the lights) on. Our proposal tries to avoid this waste of energy, also making devices and lights last longer.

3.1 Development of SISGERA

For the development of SISGERA, the Test-Driven Development Methodology for IoT-based Systems (TDDM4IoTS) [14] was used. TDDM4IoTS has been proposed to emphasize the specific activities of IoTSs, such as the analysis of the environment in which the system will be deployed, and the design of the technology layer (hardware and software), among others. In addition, it leverages Test-Driven Development (TDD) to obtain the necessary software.

TDDM4IoTS is a methodology based on the values and principles of the agile manifesto. It defines 4 roles for the project team members. The *user* role and the *project facilitator* role were played by the first author (UTEQ professor), while the *development team* role was played by the second and third authors. The *counsellor* role was not played by either of the two developers, as both had the same level of knowledge and skills in this field. The activities that TDDM4IoTS considers should be carried out in the development of an IoTS are grouped in 11 stages, namely: (1) Preliminary analysis, (2) Technology layer design, (3) Detailed requirement analysis, (4) Model generation and adaptation, (5) Test generation, (6) Software generation, (7) Model refinement, (8) Software refinement, (9) Hardware and software deployment, (10) Deliverable assessment, and (11) Maintenance. Some phases have only been executed once, such as the *preliminary analysis* and the *technology layer design* stages.

3.2 Results of the methodology

This subsection presents the results of the execution of each of the most prominent stages of the TDDM4IoTS methodology, when applied to develop this project.

(1) Preliminary analysis. UTEQ students and professors provided an outline of the needs to be covered by SISGERA. In addition, some interviews with the Dean of the Faculty of Engineering Sciences at the UTEQ provided more detailed requirements. Thus, SISGERA must meet the following *functional requirements*:

- Keep the lights, air conditioning and video projector off when nobody is in the classroom.
- Allow the professors to access the classroom according to the established schedule or upon authorization sent by the Dean.
- Secure authentication of the professor and students entering the classroom, ensuring that the person entering is who s/he claims to be.
- Whenever a professor enters the classroom, the lights, air conditioning and video projector should be turned on (in that order).
- The professor must be able to manually control the equipment (turn it off and/or on).
- Timestamped student attendance must be automatically recorded in the system.

Use case diagrams are one of the tools proposed by TDDM4IoTS to capture the coarse-grained requirements of a system. Fig. 1 shows the use case diagram for SISGERA.

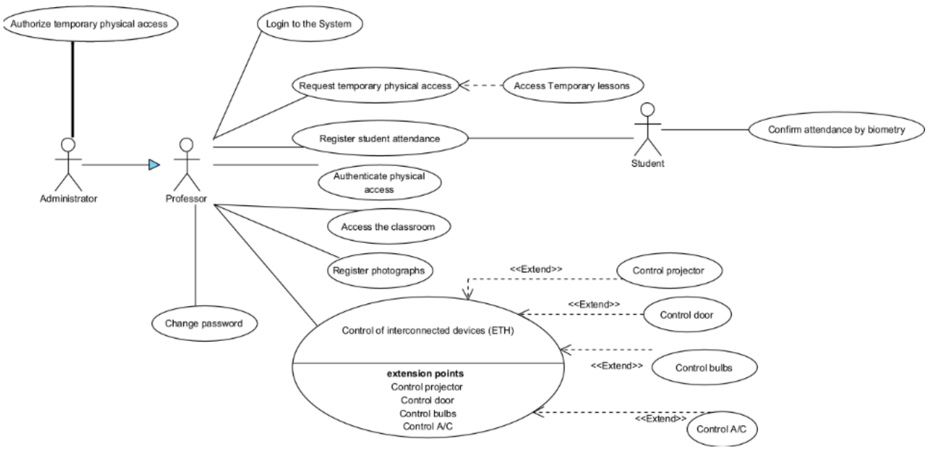


Fig. 1. Use case diagram for SISGERA.

Regarding the *non-functional requirements* of the system, it was determined that, as it is a system to be deployed in a classroom, the power supply is guaranteed by the public utility. As for the Internet connection, a permanent Wi-Fi connection is available.

The results of the *feasibility study* justified the development of SISGERA. The development and implementation costs are low. The project team has the experience and academic background that fits the profile required for the development of this IoTS. The estimated development time is within the expected timeframe. Finally, regarding the operational feasibility, being a system for a university that offers degrees such as Systems Engineering, Software and Telematics, it has trained personnel to keep this system operational.

The *technology* required to implement SISGERA is popular and commercially available. Developers chose the following hardware components: (1) Raspberry Pi, for local processing and sending data via Internet; (2) Arduino Mega, to treat the signals captured by the sensors and send the data to the Raspberry PI through the Bluetooth module; (3) infrared sensors, for turning on and off the controlled equipment; (4) an IP camera, to recognize people through live video; (5) an RFID card reader and RFID cards, to identify students when accessing the classroom; (6) a fingerprint reader, to identify students more securely (when required); (7) a motion sensor, to detect people presence inside the classroom; and (8) relay modules, to switch on and off lights, air conditioner and video projector.

Face recognition has been used to recognize and authorize the professor entering the classroom. The recognition process has been implemented using OpenCV as follows: (1) capture the person face (professor) using an IP camera and send it using Real-Time Control Protocol (RTCP); (2) the live stream is analysed through the Haar cascade classifier to face detection in photograms, which is based on the Viola-Jones framework available in OpenCV; (3) finally, the Local Binary Patterns Histograms (LBPH) algorithm is used to match the captured face with pre-captured photographs of authorized persons, as it provides better results in different lighting conditions, light rays and pose variations. And according to this, it returns the ID of the person with the best similarity.

(2) Technology Layer Design. The two outputs of this stage were: (1) the system architecture (see Fig. 2), and (2) the device or hardware design (see Fig. 3).

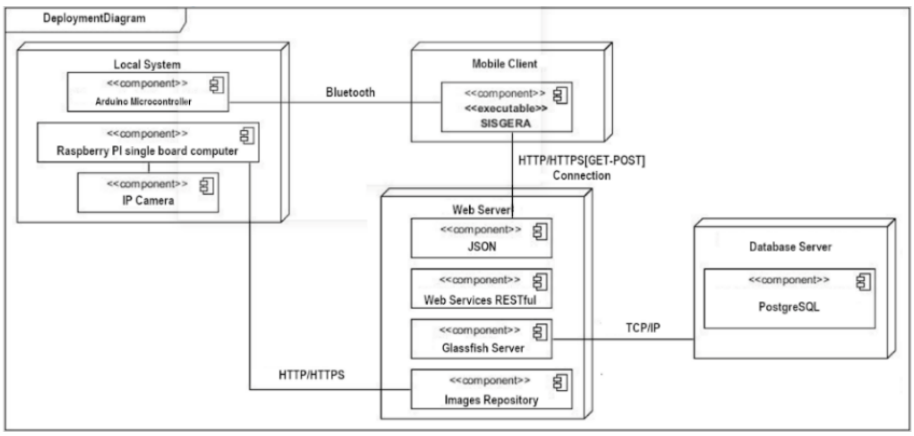


Fig. 2. Architecture of proposed system.

The local system is responsible for processing the information captured in the environment, such as the image sent (using RTCP) to the Raspberry Pi for facial recognition of the professor and fingerprint identification of the students, as well as executing commands to control the equipment, among other tasks. The local system connects via Bluetooth with the mobile app to execute the commands sent by the professor, and with the web server to store and retrieve data to/from the PostgreSQL database. The web server is prepared to serve the app, delivering the requested information through RESTful web services. For this purpose, this server connects via TCP/IP protocol with the PostgreSQL database server.

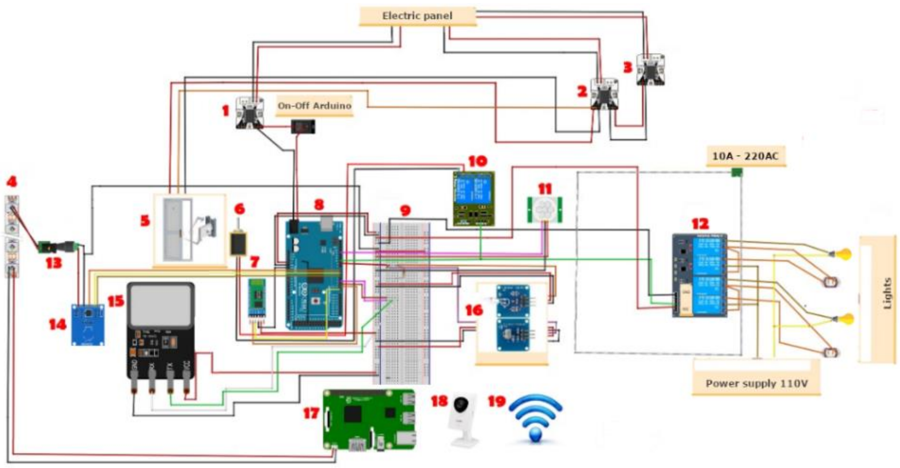
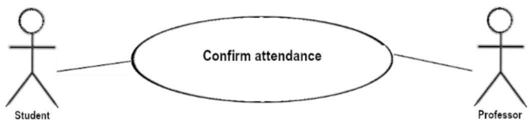


Fig. 3. Design of the proposed system device.

Fig. 3 depicts the interconnection between the sensors, actuators and single board computers that were used in SISGERA: (1) Siemens DC Breaker 220/380V, (2) Merlin Gerin C60hb Multi9 B25 Circuit Breaker, (3) Electric lock transformer 110V-12V, (4) Power strip, (5) Door control, (6) Electric sheet DC motor, (7) Bluetooth HC-5 module, (8) Arduino mega 2560, (9) Protoboard, (10) Relay module 2 channels, (11) HC-SR04 PIR module, (12) 4-channel relay module, (13) Male and female DC Power Jack Socket adapter cable, (14) Wiegand W26 RFID reader, (15) DFRobot fingerprint reader sensor, (16) NE555 IR transceiver module, (17) Raspberry Pi 4, (18) IP camera, and (19) Router (Wi-Fi Service).

(3) Detailed requirement analysis. The development of system was divided into different deliverables. For each one, the requirements were analysed in detail to obtain the tests that the software must pass, thus ensuring that the system meets the requirements demanded by the end users. Semi-structured use cases were used to collect those requirements. As an example, Table 1 shows the confirm attendance use case.

Table 1. Example of use case (Confirm attendance).

Use case:	**Confirm attendance by biometric**
Actor/s:	Student, Professor.
Purpose:	Check a student identity through the registration of his/her fingerprints.
Summary:	The professor, for some reason, needs to corroborate the identity of a given student by registering his/her fingerprints (his/her attendance registration is initially carried out through his/her RFID card).
Type:	Secondary.
Main Section - Normal Flow of Events	
Action of Actors	**System Response**
1. The use case begins when the professor needs to verify the identity of a student.	
2. Ask the student to place his/her thumb on the fingerprint sensor.	
	3. The fingerprint sensor captures the fingerprint and compares it with those registered in the database.
4. The professor observes the changes made after corroboration in the attendance list.	
5. The professor corroborates the student identity and confirm his/her attendance.	
	6. The system confirms the update of the attendance list.
Alternate flows	
Line 3: Fingerprint not recognized, return to line 2.	
Line 5: Rejection of student identity and removal of his/her attendance.	
Use case diagram	
	
List of Methods	
Method Signature	**Purpose of the Method**
public updateAttendanceByBiometric (in_biometric text)	Register the attendance of the student who places his/her thumb on the fingerprint sensor.

(4) Model Generation and Adaptation. IoTS are heterogeneous in nature, so a platform-independent model was obtained before generating a platform-specific model. Fig. 4 shows a part of the class diagram representing the system model.

(5) Test generation. Below are the tests for the functional requirements related to SISGERA must keep both the classroom lights and the equipment off when nobody is in the classroom.

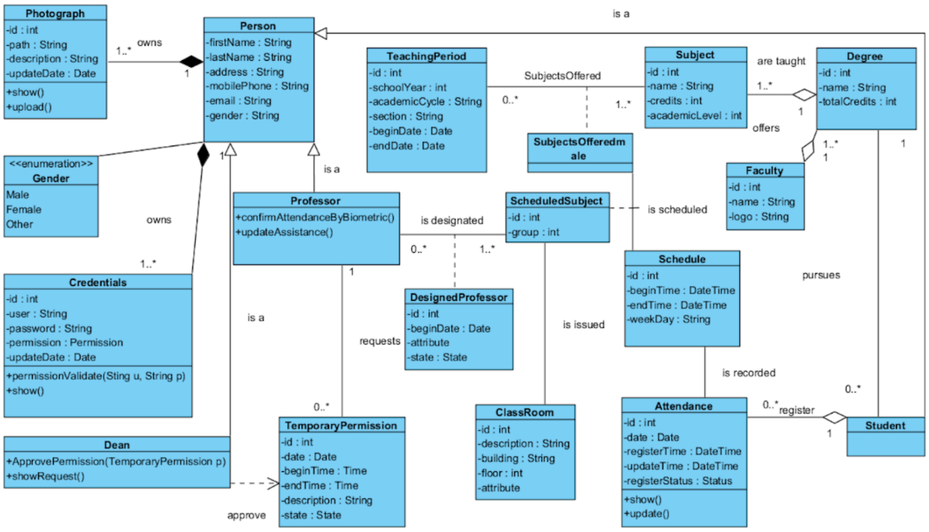


Fig. 4. Class diagram for SISGERA.

- A professor, who is scheduled to teach a lesson in classroom FCI-008 on Mondays at 10:30, arrives on the correct day but at 10:00. The system informs her/him that it is not time for her/his class and keeps everything turned off.
- A person who does not teach in classroom FCI-008, goes to this classroom. The system informs her/him that s/he has no classes scheduled in classroom FCI-008.
- A professor leaves the classroom:
  - When leaving the classroom, both equipment and lights are turned on. The system turns off the lights and equipment.
  - When leaving the classroom, only the lights are on. The system turns off the lights, and the equipment remains off.
  - Before leaving the classroom, lights and equipment are manually turned off. Lights and equipment remain off.
  - When leaving the classroom, only the air conditioning is on. The system turns off the air conditioning, and the lights and video projector remain off.
  - When leaving the classroom, only the video projector is on. The system turns off the video projector and the lights and air conditioning remain off.
  - When leaving the classroom, only the lights are off. The system turns off the air conditioning and the video projector, and the lights remain off.

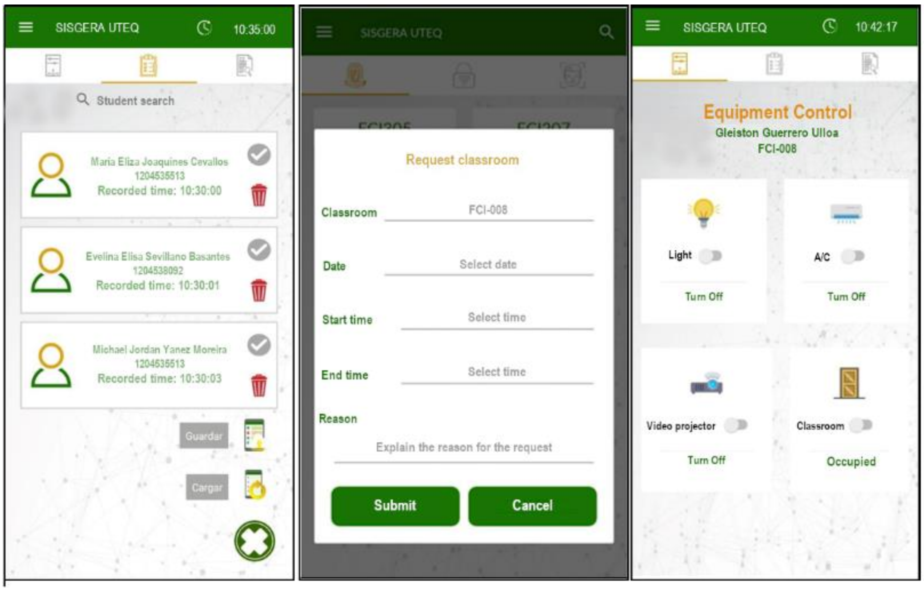
The tests of the mobile app encompass the direct manipulation of the air conditioner, video projector and lights. In addition, it is verified that the data captured by the sensors and those generated by other operations (e.g., user creation, password modification, and student attendance confirmation, among others), are correctly stored in the database.

(6) Software generation. As mentioned in TDDM4IoTS, this process can be manual or automatic. For the automatic generation of the software, Visual Paradigm [15] was used. Visual Paradigm generated a file for each class with its definition, including its attributes and methods, to be used in the mobile application. 100% of the Arduino code, and the rest of the business logic code was written by the development team.

(7) Software Refinement. This stage of TDDM4IoTS was executed only once, after obtaining the mobile application software for SISGERA. It was not necessary to refactor the device configuration software, as it was written by only one of the development team members, considering from the beginning the guidelines to obtain a clean code.

(8) Hardware and software deployment. The hardware deployment took considerable time compared to the rest of the activities. Locksmith work was required to embed a secure electric lock into the classroom entrance door. The infrared emitters were installed at a safe distance from the air conditioner and video projector so that the signal from the emitters would not be obstructed. In addition, the IP camera was secured in the hallway, so that malicious persons would not remove it from its location.

The deployment of the app consisted of being installed on an Android smartphone and the database installed on a PostgreSQL server in the cloud. Fig. 5 shows the screenshots of the SISGERA app. More specifically, Fig. 5 (a) shows the students who have registered their entry to the classroom. Fig. 5 (b) shows the screen used by the professor to request a classroom outside his assigned schedule. Fig. 5 (c) shows the interface to control the classroom equipment.



(a) Registered students (b) Request classroom (c) Equipment control options

Fig. 5. Screenshots of the SISGERA mobile app.

(9) Deliverable assessment. The usability evaluation of SISGERA was done along 5 weeks. At the initial stage, there were some negative comments and a rating of 3 out of 10 for the system. Following these results, more professors were involved in the design of the mobile application interfaces, to implement improvements. Those improvements resulted in 100% acceptance by professors. Fig. 6 shows the results of the usability evaluation of the proposed IoTS.

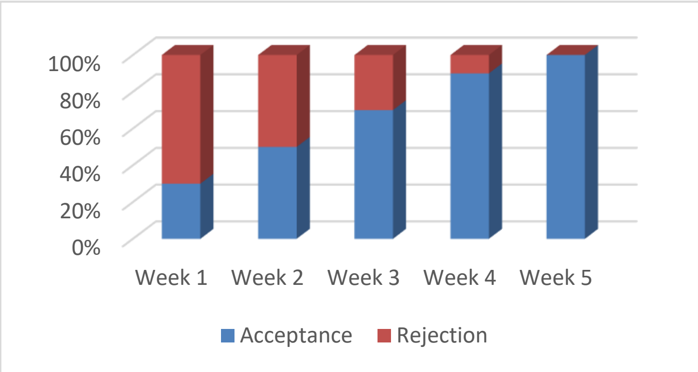


Fig. 6. Results of usability evaluation of SISGERA at five moments

4 Conclusions

We have presented an IoTS for classroom access control and managing their resources. It uses facial and fingerprint recognition as well as RFID as user authentication methods and a schedule of the subject to be taught at each time and the people (professor and students) related to it. Facial and fingerprint recognition are more secure authentication methods than traditional methods, such as password authentication, although their response time are slightly longer, especially in facial recognition. As the number of students to authenticate is considerable (each group ranges from 15 to 45 students), we also use RFID authentication, because it is a faster method. Moreover, each professor knows her/his students, and in case s/he doubts about their identity, s/he can use the mobile application to ask the student to confirm his attendance using the fingerprint authentication method.

This IoTS has been developed using a specific methodology for this type of systems, called TDDM4IoTS, which helps to obtain a system that meets the functional requirements specified by the customers, and also considers its non-functional requirements. TDDM4IoTS is an effective guide for IoTS developers, especially for those who do not have sufficient experience in IoTS development.

Moreover, for an IoTS to be successful, users must be involved in its design, especially in the design of its user interfaces. The more users participate in this process, the greater their acceptance of the system. TDDM4IoTS encourages user participation from the earliest stages of IoTS development.

References

1. Ashton, K.: That ‘Internet of Things’ Thing. RFID journal 22, 97–114 (2009).
2. Pan, J., Jain, R., Paul, S., Vu, T.: An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments. IEEE Internet of Things Journal 22, xix–xxvi (2012).
3. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey. Computer Networks 54, 2787–2805 (2010).
4. Tragos, E.Z., Foti, M., Surligas, M., Lambropoulos, G., Pournaras, S., Papadakis, S., Angelakis, V.: An IoT Based Intelligent Building Management System for Ambient Assisted Living. In 2015 IEEE International Conference on Communication Workshop 2015, ICCW, pp. 246–252, IEEE (2015).
5. Golec, M., Gill, S., Bahsoon, R., Rana, O.: BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0. IEEE Consumer Electronics Magazine 11, 51–56 (2022).
6. Bedari, A., Wang, S., Yang, J.: A Two-Stage Feature Transformation-Based Fingerprint Authentication System for Privacy Protection in IoT. IEEE Transactions on Industrial Informatics 18, 2745–2752 (2022).
7. Sadiq, M., Shi, D., Liang, J.: A Robust Occlusion-Adaptive Attention-Based Deep Network for Facial Landmark Detection. Applied Intelligence 52 9320–9333 (2022).
8. Francese, R., Frasca, M., Risi, M.: Are IoBT Services Accessible to Everyone? Pattern Recognition Letters 147, 71–77 (2021).
9. Chan May, O.A., Sandoval Gio, J., Peña Koo, J.J.: Internet of Things to Control the On/Off Switching of Air Conditioners and Light Fixtures. Pistas Educativas 38, 100–119 (2016).
10. Mohammad, G.B., Shitharth, S., Syed, S.A., Dugyala, R., Rao, K.S., Alenezi, F., Althubiti, S.A., Polat, K.: Mechanism of Internet of Things (IoT) Integrated with Radio Frequency Identification (RFID) Technology for Healthcare System. Mathematical Problems in Engineering 2022, (2022).
11. Guerrero-Ulloa, G., Rodríguez-Domínguez, C., Hornos, M.J.: IoT-Based System to Help Care for Dependent Elderly. Communications in Computer and Information Science 895, 41–55 (2018).
12. Guerrero-Ulloa, G., Hornos, M.J., Rodríguez-Domínguez, C., Fernández-Coello, M.M.: IoT-Based Smart Medicine Dispenser to Control and Supervise Medication Intake. In: Iglesias, C.A., Moreno Novella, J.I., Ricci, A., Rivera Pinto, D., and Roman, D. (eds.) Ambient Intelligence and Smart Environments. pp. 39–48. IOS Press, Madrid, España (2020).
13. Wang, S., Li, X., Chen, W., Fan, W., Tian, Z.: An Intelligent Vision-Based Method of Worker Identification for Industrial Internet of Things (IoT). Wireless Communications and Mobile Computing 2022 (2022).
14. Guerrero-Ulloa, G., Hornos, M.J., Rodríguez-Domínguez, C.: TDDM4IoTS: A Test-Driven Development Methodology for Internet of Things (IoT)-Based Systems. Communications in Computer and Information Science. 1193 CCIS, 41–55 (2020).
15. Ideal Modeling & Diagramming Tool for Agile Team Collaboration, https://www.visual-paradigm.com/, last accessed 2022/07/28.