An integrated access control and lighting configuration system for smart buildings

Hyuri S. Maciel, Isadora Cardoso, Heitor S. Ramos, Joel J. P. C. Rodrigues, and Andre L.L Aquino

Original scientific paper

***Abstract*—This article presents an integrated access control and lighting configuration system for smart buildings. The system uses two-factor authentication, one based on face recognition and other on RFID TAG, and identifies the user inside a room and performs an automatic lighting configuration based on user's behavior. The communication among the devices is performed by Radio Frequency using the low to medium frequency spectrum (LMRF), without providing direct Internet access, and, hence, avoiding known Internet security issues. This system can be easily deployed on meeting rooms or offices in business or government buildings. Through the evaluations we observe an acceptable processing execution time, an acceptable communication time and the robustness of the system.**

***Index Terms*—Access control system, lighting configuration, IoT, smart buildings**

I. Introduction

A smart city is an urban system that uses information technologies and communication to bring more interactivity to the available communication infrastructure and general public services. This interactivity aims at increasing accessibility and efficiency to the citizens. Furthermore, in a smart city, it is expected a commitment to environmental, historical and cultural elements. In this scenario, the infrastructure can be equipped with the most advanced technology solutions to facilitate the interaction of the citizens with the urban elements and the different environments in which they are presented [1].

In a smart city there are several possibilities of using new technologies to improve general urban systems. For instance, the environment monitoring of urban centers (air, rivers and climate conditions) [2]; smart grid solutions in big cities (economy of energy, green energy and remote consumer monitoring) [3]; smart vehicular networks (car interaction, sharing of accident or traffic conditions) [4]; and smart buildings where smart sensors and wireless embedded systems are used for automating restricted areas in business buildings or public offices [5]. In this work, we concentrate in the last scenario.

In this paper we present an embedded integrated system for access control and lighting configuration in restricted areas of smart buildings. The access control task is based on the work of Maciel et.al. [6], which proposes a two-factor authentication, based on facial recognition and RFID authentication (Radio Frequency Identification [7]).

The lighting configuration task, our newest contribution, is made with occupancy and light level sensors combined with magnetic keys (relay) used to configure lights in restricted areas based on user behavior.

The main contributions of this work are:

1) The integration of access control and lighting configuration into the same framework;
2) The conception of lighting configuration based on user behavior; and
3) The evaluation of communication impact of Radio Frequency in a smart building scenario.

Additionally, we present a performance evaluation of face recognition in embedded access control solutions. This study is important because, given a particular scenario, the designer can quickly evaluate and identify the best techniques that can be used. Through the evaluations, we observed an acceptable execution time, an acceptable communication time, and an increase of the robustness of the proposed system.

This article is organized as follow: Section II presents general concepts and related work; Section III shows the proposed system; Section IV presents the main results; and Section V concludes the work.

II. General Concepts

Our proposal is comprised by an access control module with two-factor authentication, based on face recognition and RIFD TAG, and a lighting configuration module based on user behavior. The user information is shared among different devices used in the system that communicate through Radio Frequency. In order to clarify some important aspects of our proposal, this Section presents general concepts about face recognition techniques and Radio Frequency communication, both important concepts to understand and replicate our solution.

A. Facial recognition

There are different access control solutions, such as biometric authentication (face, iris, voice, digital), and magnetic card or RFID tags [8], [9]. Among these, we use a two-factor authentication based on face recognition and RFID.

Manuscript received January 16, 2017; revised May 9, 2017. Date of publication June 1, 2017.

Hyuri S. Maciel, Isadora Cardoso, Heitor S. Ramos, and Andre L.L Aquino are with Computer Institute, Federal University of Alagoas, Maceió - AL, Brazil (E-mails: {smhyuri, isadoracardoso22, heitor.ramos, alla.lins}@gmail.com).

Joel J. P. C. Rodrigues is with National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí - MG, Brazil,Instituto de Telecomunicações, Portugal, and University of Fortaleza (UNIFOR), Fortaleza - CE, Brazil (E-mail: joeljr@ieee.org).

Digital Object Identifier (DOI): 10.24138/jcomss.v13i2.378

Specifically to face recognition, we adopted lightweight techniques of computer vision that can be easily embedded in a microcontroller, in our case a Beaglebone Black board [10].

Eigenface [11] is the most used approach for face recognition. Its basic principle is the use of a probability distribution vector for generating data from faces where it is returned a set of vectors. It typically uses PCA (*Principal Component Analysis*) [12] to project and compute a subspace of facial recognition – the space of face. The visual information is converted into vectors by using a training data set of images. The space of face is defined by eigenfaces vectors consisting of a linear combination of the more relevant points in the original images which are the eigenvectors of the covariance matrix of original facial images.

To mathematically understand the *Eigenfaces* algorithm, let $T = (T_1, T_2, \ldots, T_M)$ denote the training set of faces. M is the amount of faces present in the set T, and m the average face (a vector which represents the average face from image facial data set),

$$m = \frac{1}{M} \sum_{i=1}^{M} T_i. \tag{1}$$

Let $\mathbf{\Phi}_i = T_i - m$ denote a subtraction of the average face from each image T_i and the matrix $A = [\mathbf{\Phi}_1\, \mathbf{\Phi}_2\, \ldots\, \mathbf{\Phi}_n]$ where each column represents one image $\mathbf{\Phi}_i$. After that we calculate the covariance matrix $C = A\,A^T$. Computationally, the task of finding eigenvectors and eigenvalues for the matrix C is expensive, so we reduce the matrix dimension using $C' = A^T\,A$. The transformation matrix $U = \mathbf{\Phi}\,C'$ is used to find the eigenvectors and eigenvalues of C'. Then, to project each face in the space of faces, we apply $\Omega = U^T\,\mathbf{\Phi}$. Hereafter, we calculate the subtraction of the test face from the average face (T_1) as $\mathbf{\Phi}_1 = T_1 - m$, thus, we project the test face in the space of faces $\Omega = U^T\,\mathbf{\Phi}_1$. The face in the image data set that has the smallest Euclidean distance from the test face is thus chosen.

Another widely used approach for face recognition is *Haar Cascade* [13]. This approach is defined as a structure which contains levels of classifiers from the most generic to the most specific [14]. It uses features previously extracted from an object for its detection. The function is trained from positives images (images with faces) and negatives images (images without faces). It uses rectangles as features to find faces, in order to have a single value obtained by subtracting the sum of pixels within the rectangular white area from the sum of pixels within the rectangular black area. Different features can represent the same space in image, so, many classifiers considered weak are trained and then combined to generate stronger classifiers. These classifiers can be used in cascade, which performs a search to find negatives, which are discarded whenever found. Whether it passses by all cascade levels, the analyzed area has a face.

Black and white areas in the features represent the difference of the colors intensity among the areas within the images, for instance: darker areas are represented by black sections and lighter areas by white sections. To calculate *Haar Cascade*, we need an integral image, i.e., a matrix with the same dimension of the input image, where (x, y) stores the sum of all pixels of the rectangle between $(0, 0)$ and (x, y). Since that $a(x, y)$ is the input image, the integral image $a'(x, y)$ is calculated by the following recurrence:

$$S(x, y) = S(x, y - 1) + a(x, y)$$

and

$$a'(x, y) = a'(x - 1, y) + S(x, y),$$

where $S(x, y)$ is the line cumulative sum, $S(x, -1) = 0$ e $a'(-1, y) = 0$. After calculating the integral image, the relative value of each rectangle of features can be obtained by four accesses in the memory, i.e., four pixels (x, y). Suppose a rectangular subarea D of feature: left top point (x_1, y_1); right top point (x_2, y_2); left lower point (x_3, y_3) and right lower point (x_4, y_4). We calculate this area as follow:

$$D = a'(x_4, y_4) + a'(x_1, y_1) - (a'(x_2, y_2) + a'(x_3, y_3)).$$

Despite of the above solutions, there are several works [15], [16], [17] related to face recognition. For instance, the study presented by Hu et al. [12], comparing two methods, *Principal Component Analysis* (PCA) and *Two-Dimensional Principal Component Analysis* (2DPCA), using four well-known database of faces in order to find out which showed the best results.

In [18], a face in a single image or a set of faces traced in a video is recognized using two factors: end-to-end learning using a convolutional neural network (CNN), and the availability of very large scale training datasets.

In [19] it is proposed an Independent Component Analysis (ICA) Kernel method, which combines the strong features of the Kernel and the ICA approach. They also compare the performance of the Kernel ICA method with classical algorithms such as PCA and ICA.

Drira et. al. [20] proposes a new geometric structure to analyze 3D images of faces. This technique aims to compare, combine and calculate the mean of faces' shapes. They represent the surface of the faces by radial curves, using analysis of the elastic form of these curves to create a Riemannian structure that analyzes the forms of the full facial surface.

Another interesting work is presented by Kamencay et al. [21], which shows a methodology using an algorithm of *Principal Component Analysis* (PCA) combined with *Canonical Correlation Analysis* (CCA) to learn the mapping between 2D face images and 3D face data. However, these solutions are prohibitive in an embedded environment with limited resources, so we use the combination of *Haar Cascade* and *Eigenface*.

B. Radio Frequency Communication

In our solution, the communication among the devices is performed by Radio Frequency using the low to medium frequency spectrum (LMRF), without providing direct Internet access and, avoiding known Internet security issues. Among the several types of commercial solutions for communication of embedded systems, such as LMRF, Xbee, Bluetooth, and WiFi, we adopted LMRF due to its low cost and ease usage to carry out the communication.

We use a LMRF module that operates in a range known as SubGiga, i.e., it can operate in two frequencies below the 1 GHz band, namely, 433 MHz and 315 MHz. These frequencies are widely used in remote control for automatic gates and car alarms, being one of the cheapest options to build systems that need a wireless communication, or to extend the integration between systems.

The transmission module operates with power between 3.5 and 12 V, which influences the range of the signal. If an antenna is attached to the module, the distance needed between the modules to build a transmission can be increased. With a good quality antenna placed 1.60 m above the ground, a distance of approximately 170 m can be reached in open environments. The module uses an AM modulation (Amplitude Modulation), a modulation type in which the amplitude of sinusoidal signal, the carrier, varies as a function of a signal of interest, the modulating signal. The power required by the module when compared to a 25 W lamp is equivalent to 0.001% of the power, requiring only $2 \cdot 10^{-8}\%$ of the transmitted power to arrive intact at the receiver to achieve a speed of 2000 bps.

The data transmission uses the ASK/OOK encoding. ASK (Amplitude Shift Keying) consists of changing the carrier amplitude level as a function of an input signal with discrete amplitude levels. The transmission is made using just 2 signal levels (1 bit for each signal element). The ASK/OOK modulation allows to transmit a sinusoidal pulse corresponding to a given bit and the value zero in the complementary bit. If the signal level is 1, will be emitted a signal in the frequency 433 /315 MHz. If the signal level is 0, will not be emitted any signal in that frequency. Because of it, the modulation in these modules can suffer with interference. A solution is to insert a second encoding on OOK encoding, in order to increase the reliability [22].

III. Smart Access Control and Lighting Configuration System

Briefly, the system is comprised by: a Beaglebone Board (`BB microcontroller`), for face recognition; an Arduino Board I (`ABI microcontroller`), for RFID authentication; and an Arduino Board II (`ABII microcontroller`) combined with different occupancy and light level sensors, for lighting configuration. The `ABI microcontroller`, additionally, is the device that decides to open or not the magnetic lock. The face data set is located in the `BB microcontroller`, and only the recognized results goes to `ABI`. The users data set is located in the `ABI microcontroller` and shared with `ABII` through Radio Frequency communication.

A. BB microcontroller

The face recognition process initiates when the camera tries to recognize an user. Hereafter, the camera gets the scene image and sends it, trough USB port, to the `BB microcontroller`, which performs the face recognition-based authentication. The `BB microcontroller` is a Beaglebone Black, which has an ARM Cortex A8 1 GHz processor, 512MB of RAM memory, HDMI video output, 2GB of eMMC flash memory, a Debian 7.8 operating system running a Linux Kernel 3.8.

The camera used with `BB microcontroller` is a D-link – HD Wireless N Cube Network Camera – which can capture images in high resolution – HD-720P, ensuring the capture of the details required by the application. It is able to handle video compressing H.264, MPEG-4, and MJPEG. The D-link camera has the following specification: 1/4” 1 Megapixel CMOS progressive sensor, minimum illumination of 1.0 lx, 10× digital zoom, fixed length 3.45 mm, aperture of F2.0, angle of view of H 57.8°, V 37.8°, D 66°.

The results of the face recognition authentication is sent, through serial communication, to the `ABI microcontroller`. However, this communication can be made in other way, for instance, by bluetooth or any other Radio Frequency transmitter. As the `BB microcontroller` has an embedded operating system, we chose to use the serial communication, since the time of sending and receiving information is faster. Moreover, using the `BB microcontroller` with the LMRF module, some functions, such as video output, are disabled. This makes harder its simultaneous use with the face recognition camera.

The face detection uses the *Haar Cascade* approach, previously presented. After detection, the image area containing a face is normalized using the OpenCV [23] library. The face is firstly aligned and imperfections, caused by the environment where the image is acquired, are removed. The *Eigenface* technique is applied to normalized images. The purpose of applying this technique is to extract and encode the relevant features for face recognition. Additionally, with these data, it is possible to register a new user in the system or make the recognition based on stored images.

B. ABI microcontroller

The `ABI microcontroller` is an Arduino UNO board that receives, processes all data, and makes the access decision. This Arduino has a microcontroller based on ATmega328, with 14 pin of input and/or digital output, where 6 can be used as PWM, a 16 MHz oscillator crystal, a USB connection, 6 analog inputs, a power input and a ICSP connection.

To make the `ABI microcontroller` prototype, we have: a RFID reader, a LCD display 2 × 16, a 220 Vac∼12 Vac transformer, a 5 V relay, a LMRF transmitter module, a magnetic lock, a 10 kΩ potenciometer and a LMRF receiver module. The display, relay and RFID reader are connected to the input and output ports of the Arduino. The user uses a medium range RFID TAG which is read even with objects and obstacles, not requiring direct contact. Figure 1 shows the developed `ABI microcontroller` prototype.

C. ABII microcontroller

When the two-factor authentication is validated the door opens. An access log containing the time and confirmation that the user tried or entered the room is stored. A message containing information about the user who has entered the room is sent via LMRF to `ABII microcontroller`, which is responsible for activating the devices in the room.

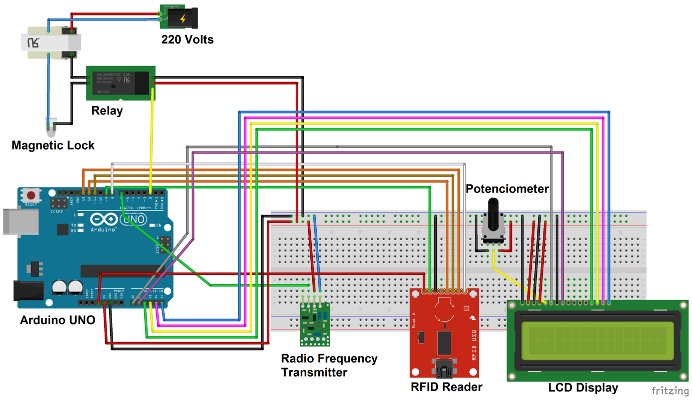


Fig. 1. Access control prototype - ABI microcontroller

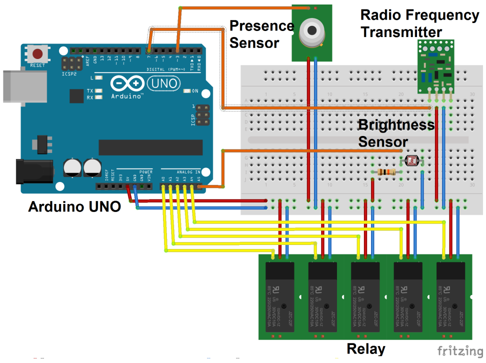


Fig. 2. Lighting configuration prototype - ABII microcontroller

The ABII microcontroller is equal to Arduino UNO board used on ABI one. To make the lighting configuration prototype, we used: an Arduino UNO, five relays, a PIR occupancy sensor, a LDR brightness sensor, a LMRF transmitter module, and a 440 Ω resistor. Figure 2 shows the developed ABII microcontroller prototype.

The ABII microcontroller (2) uses 5 relays to activate 5 lamps. The data are read and interpreted by an Arduino UNO and depending on the environment lighting condition, the system decides how many lamps will be activated.

The ABII microcontroller decides to activate or not the lights based on where the user is located and the lighting conditions in the area. This information could be used to regulate the light intensity based on user behavior history, this task is subject of future work. To detect the user location is used a motion sensor which detects movements in an area up to 7 meters. So, if movements are detected in that area, a signal is sent to the ABII microcontroller. This detection could be improved by another camera to track the user and calibrate the lighting in a personalized way, this task is also subject of future work.

To verify the lighting intensity in the environment, it is used a sensor LDR (Light Dependent Resistor), which its resistance varies according with the light intensity. The more light reaches it, lower is its resistance. The sensor is attached to an analog input of the ABII microcontroller, which should have a range from 0 to 1024. So the light intensity in the environment determines which lights must be triggered, if it is necessary.

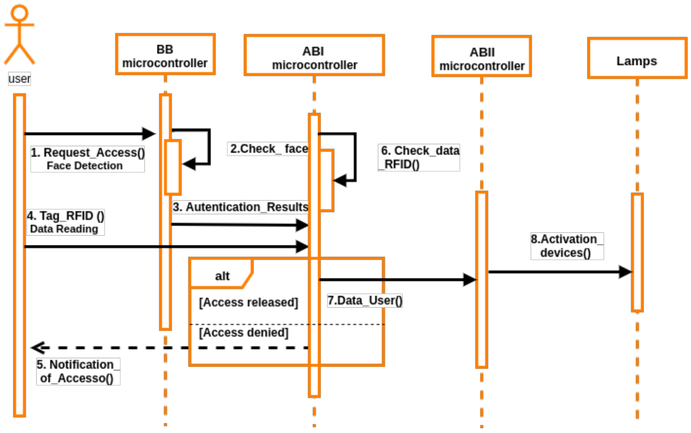


Fig. 3. Sequence diagrams

D. System execution summary

Figure 3 shows the components of the sequence diagram of our system. The actors presented in the sequence diagram are: user, it is the real user using the system; BB microcontroller, responsible to perform the face recognition; ABI microcontroller, responsible to read and verify the RFID data; ABII microcontroller, responsible to analyze the data of sensors (occupancy and light level); and Lamps, the real lamps that will be controlled.

The diagram sequence is described as follow:

1) The user requests access to BB microcontroller: the face is detected by the camera;
2) BB microcontroller checks the face: it is verified if the face detected belongs to someone registered in the database;
3) BB microcontroller sends authentication results to ABI microcontroller: if the face is registered on the system, a positive message is sent to ABI microcontroller.
4) The user uses the tag RFID() on ABI microcontroller: the user shows the RFID tag on the reader;
5) ABI microcontroller checks the RFID data: it is verified if the data in the tag belongs to the user who had the face detected, and it is verified if this user can access the room;
6) ABI microcontroller notifies the access: the user is notified through a message in the display if the access was allowed or denied;
7) ABI microcontroller shares the data user to ABII microcontroller: if the user had the access allowed, it sends, through LMRF, to the ABII microcontroller that someone has entered the room and who is this user;
8) ABII microcontroller configures the lights: some commands are sent to configure the lamps.

It is worth mentioning that the lighting configuration can be extended to control another devices in the environment, such as air conditioning, curtains, projector and so on. The control system can be changed to add or delete a user from using the room, as well as the lighting configuration can also be modified, changing the amount of light needed for a lamp, which environment can be more or less illuminated, etc. It is also possible to use some inference technique to make the environment context sensitive, so the environment will be prepared for the users by the time they arrive, for instance, activating the air conditioning or activating the computer, thereby bringing more convenience for the users and saving resources for the environment as well.

Data integrity assures the receiver was not changed during a transmission. Ensuring the integrity of the data transmitted between the modules is important as these nodes can be deployed in a variety of environments and susceptible to various types of attacks.

To ensure data integrity and control we can use control layer protocols such as Media Access Control (MAC), specific tailored to WSN. We adopted the IEEE.802.15.4 standard, which includes the features: short-range connection with low baud rate, latency and low power consumption, and integrated support for secure communications. Being classified as a WPAN (Wireless Personal Area Networks) and operating in POS (Personal Operating Space) of 10 m and its transmission rate varies between 20 and 250 Kb/s. The MAC uses the CSMA/CA (Carrier sense multiple access with collision avoidance). It is an effective way to manage and order packet traffic in a computer network used to reduce collisions.

IV. Results and Experiments

In order to evaluate the performance of our system we chose four important aspects to verify: precision of the face recognition process; face recognition authentication performance; LMRF communication performance; and test of the complete system, the two-factor authentication and lighting configuration. Our system has a satisfactory answer for all performed tests.

A. Precision of face recognition process

These experiments were performed because we use lightweight strategies for face recognition capable of executing on limited hardware. We execute different experiments with 10 faces, of which 5 were registered in the image data set and 5 were not. The data set contained 12 different registered faces: 100 photos were captured of each face when signing up, resulting in a total of 1200 images.

The tests were performed in real time using the D-Link camera with resolution of 352×288. We test three faces poses, namely, front, over and side. The front position refers to the camera positioned in front of the face; in the over position the camera is positioned in a place above the face, but the user must look at the camera (to simulate a camera on the wall in a higher level compared to the user); and the side position is similar to the over position, but it makes a different angle of 90°to the face. For each position were performed 30 image shots and the method was repeated for 3 different confidence levels: 0.975, 0.980 and 0.985, resulting 300 analyses for each level, a total of 900 analyses.

TABLE I
Result of face recognition with user present in the image data set.

Confidence level	0.975	0.980	0.985	
Front	0.940	0.794	0.173	Right
	0.060	0.180	0.053	Wrong
	0	0.026	0.774	Unknown
Over	0.740	0.507	0	Right
	0.253	0	0	Wrong
	0.007	0.493	1	Unknown
Side	0.467	0.300	0	Right
	0.380	0.100	0	Wrong
	0	0.520	0.967	Unknown

TABLE II
Result of face recognition with user not present in the image data set.

Confidence level	0.975	0.980	0.985	
Front	0	0.613	1	Right
	1	0.387	0	Wrong
	0	0	0	Unknown
Over	0.060	0.947	0.987	Right
	0.840	0, 007	0	Wrong
	0	0	0	Unknown
Side	0.007	0.920	0.980	Right
	0.867	0	0	Wrong
	0	0	0	Unknown

Table I shows the results with existing faces in the data set. Setting the confidence level to 0.975, we obtained satisfactory results for the front and over positions, which can be seen in the accuracy rate, 94% and 74%, respectively. In the side position the correct recognition was below 50% and closer to the wrong results, and 15.3% of the images did not achieved success at face detection.

Increasing the confidence level to 0.980, the results remained consistent. In the over position, even with the correct recognition a little above of 50%, the wrong results were eliminated, improving the algorithm efficiency. With the confidence level 0.985, there was only correct recognition for the front position; however, with a low success rate and often getting as output “unknown face”.

Table II shows the results of tests made with unregistered faces. For the confidence level 0.975, the face recognition output were in most of them wrong; however, increasing the confidence level, the algorithm output was generally correct.

In the two aforementioned tables were observed that a good result in the first reflected in a bad result in the second one. For this reason, Table III was created to unify the results of the previous tables. The values for confidence level 0.980 for the front and over positions in general were satisfactory, achieving a good success rates and low error rates. The result for the side position was with a good percentage of success, the reason is that high success rate of faces not registered, although the success rate for registered faces is low.

TABLE III
RESULT OF FACE RECOGNITION WITH USER PRESENT AND NOT PRESENT IN THE IMAGE DATA SET.

Confidence level	0.975	0.980	0.985	
Front	0.470	0.703	0.587	Right
	0.530	0.283	0.027	Wrong
	0	0.013	0.386	Unknown
Over	0.400	0.727	0.494	Right
	0.547	0.003	0	Wrong
	0.003	0.247	0.500	Unknown
Side	0.237	0.610	0.490	Right
	0.623	0.050	0	Wrong
	0	0.260	0.483	Unknown

B. Face recognition authentication performance

For the sake of comparison of the response time of the BB microcontroller, we executed in real time the face recognition module also in a desktop computer. The desktop computer used has a Linux Ubuntu 14.04 LTS operating system, 8 GB of RAM memory, an Intel Core i7-3770 CPU@3.40 GHz x 8 processors, an AMD Radeon HD 6450 graphic board and 1 TB of HD.

Figure 4 illustrates the average of sixty execution for both cases, i.e., for the desktop and the microcontroller. It is noteworthy that, in order to improve the view, the scales on the y axis are not the same. It can be seen that only when the system is running without any face in front of the camera is when the processing is higher, these scenarios occurs when some object passes in front of the camera. However, in the other scenarios the processing times, when using the BB microcontroller, are similar to a server. An important fact is that we are considering the isolated execution of a single request. In case of several parallel requests, certainly a greater computational burden will be required for the server processing. It is worth noting that in our proposal the system is disconnected from the Internet, so, by using a PC, we should have a machine dedicated for this task.

C. Radio Frequency communication performance

Finally, this section evaluates the LMRF communication performance in order to identify the communication impact of our system. We verify two different tests: one to verify the packets loss rate in different time intervals during the packets transmission; and another to verify the influence of distance between the devices during the transmission.

The first test were performed at a distance of 80 cm without barrier between the modules, with a rate of 5.000 bit. A message containing an integer value was sent for 3 min. Nine different time intervals in milliseconds were used to send the messages: 200, 300, 400, 500, 1.000, 1.000, 1.500, 2.000, 2.500 and 3.000. The packet loss rate was evaluated in each test. These results are shown in the Table IV.

TABLE IV
PACKET LOST EVALUATION

Time (ms)	Packets sent	Packets lost
200	853	11
300	548	7
400	423	1
500	340	2
1,000	177	0
1,500	120	0
2,000	90	1
2,500	72	0
3,000	60	0

TABLE V
DATA TRANSMISSION DISTANCE

Distance (cm)	Packets sent	Packets lost
80	340	2
100	322	1
200	354	4
300	352	3
400	322	1
500	324	2
600	322	2

To evaluate the distance in which the data can be transmitted, seven tests were performed, using different distances in centimeters: 80, 100, 200, 300, 400, 500 and 600. No barrier was put between the modules. The messages containing an integer value was sent at a fixed interval of 500 ms, with a rate of 5.000 bit. The results are shown in the Table V.

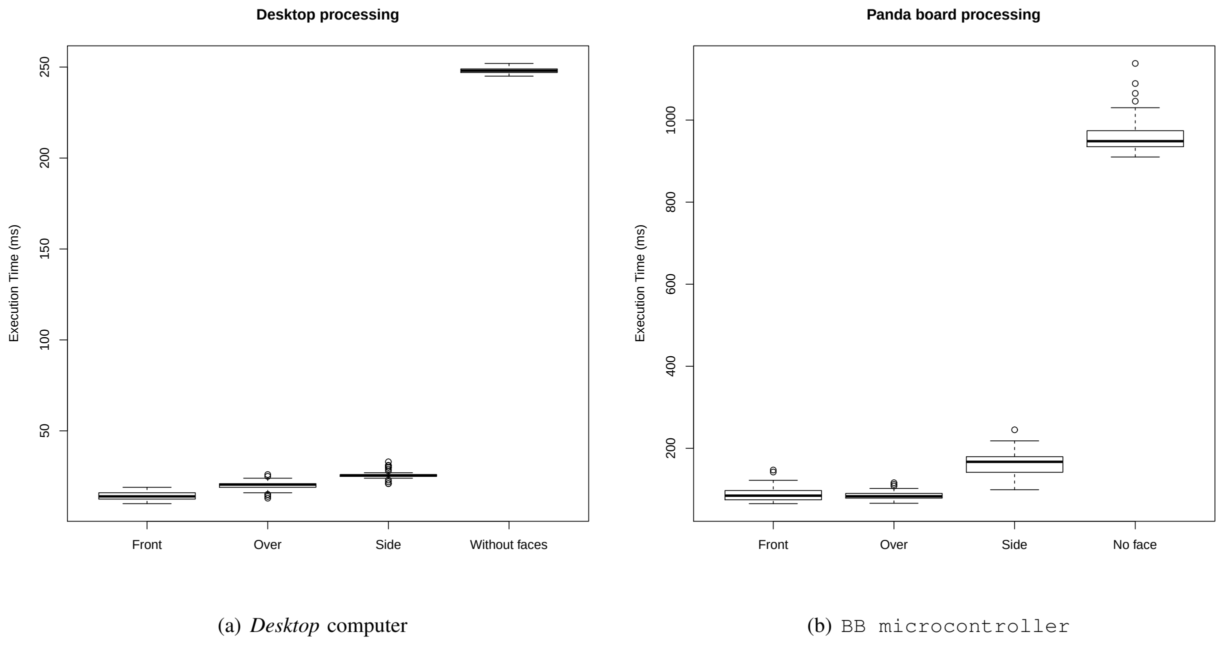
We observe that both results are considered good with a low packet loss. It costs more than 500 ms for the system to allow the access, time enough to the information arrive to the receptor. Packet loss may have occurred due to some interference or external noise. Even if there are missing packets, the system also analyzes the data in the occupancy sensor to take the decision of activating or not the lights, so if there is some communication failure, the lighting configuration would work anyway.

D. Test of complete system

Once it was possible to identify the low impact of using face recognition in embedded way, we perform tests to identify the robustness of our two-factor authentication, i.e., considering the face recognition and the RFID authentication at the same time. We conduct tests with four users, in which three of them had their faces registered in the face recognition system and one had not. Two different RFIDs key chains were used, one with allowed access and another without it.

We perform four scenarios of tests, with the following results:

1) **Registered faces and valid RFID keychain**: in this test the system worked correctly for all attempts of face recognition and RFID keychain validation, hence allowing the user access to the ambient;
2) **Registered faces and not valid RFID keychain**: in this case the system recognized the faces but not allowed the access, since the keychain was not valid;
3) **Not registered faces and valid RFID keychain**: in this test the system recognized the face few times, generating a false positive and allowing the access;



(a) *Desktop* computer

(b) `BB microcontroller`

Fig. 4. Response time for face recognition.

4) **Not registered face and not valid RFID keychain**: in this case, even generating some false positive, the access was denied due to the keychain, which was not valid to access the ambient.

These scenarios were executed in both, PC and `BB microcontroller`, and the same results were observed. It was observed a larger time to make the face recognition in the `BB microcontroller`, since the processing time and memory access are superior of that observed in the desktop computer.

Additionally, in order to test the lighting configuration, different tests were performed in different scenarios. When the occupancy sensor detected someone in a specific area in the environment, the lighting sensor value was analyzed to decide how many lamps should be activated.

The following values were used in LDR sensor:

1) Between 700 and 799, a lamp was activated;
2) Between 800 and 899, two lamps were activated;
3) Between 900 and 999, three lamps were activated; and
4) Equal or greater than $1,000$, five lamps were activated.

In these scenarios, when detected no movement within a three-minute period, all the lamps were deactivated. It was possible to test all the different scenarios just covering the surface of the LDR sensor, which change its values, in order to simulate the different light in the ambient. The system worked as expected in all the scenarios, activating the right amount of lamps according to LDR sensor value when detected a movement.

V. Conclusion and Future Work

This work presented a proposal of an embedded system for access control considering two-factor authentication (face recognition and RFID) and a lighting configuration. The face recognition and RFID authentication happen in a parallel fashion, both verifying if the user is registered in the database and if the data about this two parts of system match. After that, the lighting configuration uses the information received by the occupancy sensor, which alerts when the user has entered in the room, to activate or not the lights.

The experiment that conducted herein shows the viability of the proposed embedded system, without needing a server to process the requests. Since the face recognition is executed in the camera itself, without Internet access and needing two-factor authentication, facial recognition and RFID authentication, to allow the access, the system security is improved. Even with a small detection delay, when compared with an execution in a desktop computer, the system worked as expected, allowing access only for authorized users.

Although there is a low packet loss in some cases when sending data between the systems, this loss does not affect the final goal of allowing the access and activate the lights, since the tests were made in an atypical scenario with a much greater demand of data transmission than in a real world scenario. The experiment about communication between the modules using different distances also worked satisfactorily, with a low packet loss, not interfering in the system work.

For future work, we intend to track users inside the building. We plan to insert other sensors elements in the system, such as temperature sensors and controller of air conditioning, so we could control not only the access and lights but also make a full monitoring of any desired room. Also, it is desirable a context sensitive environment using inference techniques, which would make possible to prepare the environment before the user arrives, bringing more convenience for them as well as saving resources for the environment.

Acknowledgments

This work has been partially supported by National Funding from the FCT - Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project, and by Finep, with resources from Funttel, grant no. 01.14.0231.00, under the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações CRR) project of the National Institute of Telecommunications - Inatel, Brazil.

References

[1] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, "A global perspective of smart cities: A survey," in *7th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2013.

[2] G. Han, L. Shu, A. S. K. Pathan, J. J. P. C. Rodrigues, and A. Mellouk, "Wireless sensor networks based on environmental energy harvesting," *The International Journal of Distributed Sensor Networks*, vol. 2013, no. 816063, p. 2, 2013.

[3] M. Weixiao, R. Ma, and H. H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Network*, vol. 28, no. 1, pp. 24 – 32, 2014.

[4] J. A. F. F. Dias, J. J. P. C. Rodrigues, and L. Zhou, "Cooperation advances on vehicular communications: A survey," *Vehicular Communications*, vol. 1, no. 1, pp. 22 – 32, 2014.

[5] F. Sadri, "Ambient intelligence: A survey," *ACM Computing Surveys*, vol. 43, no. 4, pp. 36:1 – 36:66, 2011.

[6] H. S. Maciel, I. Cardoso, D. F. Silva, C. G. M. do Nascimento, H. S. Ramos, J. J. P. C. Rodrigues, and A. L. L. Aquino, "An embedded access control system for restricted areas in smart buildings," in *International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, 2016.

[7] S. A. Weis, "Rfid (radio frequency identification): Principles and applications," 2016.

[8] K. Delac and M. Grgic, "A survey of biometric recognition methods," in *46th International Symposium Electronics in Marine*, 2004.

[9] V. Suhendra, *Communications in Computer and Information Science*. Springer Berlin Heidelberg, 2011, ch. A Survey on Access Control Deployment, pp. 11–20.

[10] *BeagleBone Black System Reference Manual*, Beagleboard.org, April 2013, rev. A5.2.

[11] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of cognitive neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[12] J. jun Hu, G. zheng Tan, F. 0gang Luan, and A. S. M. L. Libda, "2DPCA versus PCA for face recognition," *Journal of Central South University*, vol. 22, no. 5, pp. 1809–1816, 2015.

[13] P. Viola and M. J. Jones, "Robust real-time face detection," *International journal of computer vision*, vol. 57, no. 2, pp. 137–154, 2004.

[14] W. A. R. dos Reis, "Detecção de sinais de trânsito através do método de classificação adaboost," *UNOPAR Científica Ciências Exatas e Tecnológicas*, vol. 12, no. 1, 2014.

[15] L. M. D. C. Carcagn P, Del Coco M, "Facial expression recognition and histograms of oriented gradients: a comprehensive study," *SpringerPlus*, 2015.

[16] D. K. chroff, Florian and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015.

[17] A. V. Parkhi, Omkar M. and A. Zisserman, "Deep face recognition," *Proceedings of the British Machine*, 2015.

[18] A. Z. Omkar M. Parkhi, Andrea Vedaldi, "Deep face recognition," 2015.

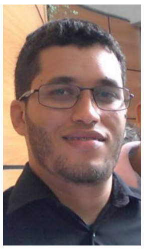
[19] P. T. D. T. Martiriggiano, M. Leo, "Facial feature extraction by kernel independent component analysis," 2005.

[20] A. S. M. D. Hassen Drira, Boulbaba Ben Amor and R. Slama, "3d face recognition under expressions, occlusions, and pose variations," *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 2013.

[21] P. Kamencay, R. Hudec, M. Benco, and M. Zachariasova, "2D-3D face recognition method based on a modified ccapca algorithm," *Int J Adv Robot Syst*, vol. 11, p. 36, 2014.

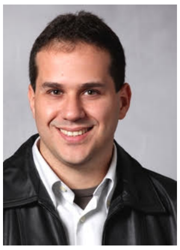
[22] S. Arnon, J. Barry, G. Karagiannidis, R. Schober, and M. Uysal, Eds., *Advanced Optical Wireless Communication Systems*. Cambridge University Press, 2012, ch. Wireless optical CDMA communication systems, pp. 54–86.

[23] G. Bradski, "The opencv library," Dr. Dobb's The World of Software Development, 2000.



Hyuri S. Maciel is a Undergraduate Student in Computer Science at Federal University of Alagoas, Macei, Brazil. His research interest in Sensor Networks, Internet of Things, and Ubiquitous Computing.

Isadora Cardoso is a Undergraduate Student in Computer Engineering at Federal University of Alagoas, Macei, Brazil. Her research interests include Data Science, Artificial Intelligence, and Internet of Things.



Heitor S. Ramos is graduated in Electrical Engineering from the Federal University of Campina Grande, Brazil, his master in Computing Modeling from the Federal University of Alagoas, Brazil, and his PhD in Computer Science from the Federal University of Minas Gerais. His research interests rely on wireless networks, sensors networks, mobile and ad hoc networks, and urban computing. He is currently a Professor at the Institute of Computing of the Federal University of Alagoas, Macei, Brazil.

Joel J. P. C. Rodrigues [S'01, M'06, SM'06] is professor at the National Institute of Telecommunications (Inatel), Brazil and senior researcher at IT, Portugal. He is the leader of NetGNA Research Group, the President of the scientific and technical council at ParkUrbis - Covilhã Science and Technology Park, the Past-Chair of the IEEE ComSoc TCs on eHealth and on Communications Software, Steering Committee member of the IEEE Life Sciences Technical Community. He is the editor-in-chief of three international journals and editorial board member of several journals. He has authored or coauthored over 500 papers in refereed international journals and conferences, 3 books, and 2 patents.

Andre L. L. Aquino is a Professor at the Institute of Computing of the Federal University of Alagoas, Brazil. He received his Ph.D. in Computer Science from the Federal University of Minas Gerais, Brazil, in 2008. His research interests include data reduction, distributed algorithms, wireless ad hoc and sensor networks, mobile and pervasive computing. In addition, he has published several papers in the area of wireless sensor networks.