International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Teledetection System and Management of Intrusions Events, Based on Cloud Infrastructure

José Luis Mela, Edwin Cedeño Herrera, Gloris Batista Mendoza

Abstract*: This document describes the design and development of a low-cost security system to detect unauthorized access of people in an office, using Arduino microcontroller technology. It used a passive infrared sensor (PIR) to detect movements of people, a Wi-Fi interface to send security alerts to the cloud platform and a GSM modem, in the same way, to send the detected security events to the frame of Cloud. The latter will be used if it is not possible to establish a link to the cloud platform, via the Wi-Fi interface. In addition, the security system sends an SMS (Short Message Service) directly to the security agent's mobile every time a security event is detected. A dual communication interface is used to guarantee the sending of alerts to the cloud platform and, on the other hand, to ensure the delivery of notifications of the alerts detected to the security agent, through the channels: Notify my device (NMD), email, Twitter and SMS. As a result, it has been obtained that the fastest interface to send the detected security alerts to the cloud platform is Wi-Fi and the channel with less time to notify the security agent is NMD. Therefore, this proposed security system represents an ideal solution for security problems, both level domestic and commercial, since it has characteristics of being pervasive, that is, it can be used anywhere and agnostic in so far as of the wireless interface Communication.

Keywords: Alert, interface, notifications, cloud platform, security system.

I. INTRODUCTION

Security plays a very important role, in some regions it has decreased, but in others, it has increased [1]. With technological advances and the emergence of new trends in the field of security, has been achieved to some degree, control the rate of thefts. The tendency is to minimize the human resources necessary for security to 60% and to potentiate the technology to 40% [2]. In this sense, this proposed security system aims to develop a low-cost security system, for teledetection of intrusions, based on an event management cloud platform, which allows the user to be notified quickly.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
José Luis Mela, Licenciatura enIngeniería Informática, Universidad de Panamá,
Edwin Cedeño Herrera, Ph.D.*, Profesor, Facultdad de Informática, Electrónica y Comunicación, Universidad de Panamá,
Gloris Batista Mendoza, Profesora, Facultad de Informática, Electrónica y Comunicación, Universidad de Panamá,

The importance of this study lies mainly in the fact that it is tolerant to failures in the links to the cloud platform, integrating dual wireless communication technology (Wi-Fi/GSM), also, it has characteristics of guarantee of delivery of notifications, using four channels to notify the user of the intrusions detected by the security device. This means that it is safe in the delivery of notifications and it does so quickly.

II. LITERATURE REVIEW

In the study by Khirod and Umesh [3] they use a Zigbee to create a wireless sensor network, implementing an ESP8266 microcontroller to send data to a server and a GSM modem to send the alerts detected by the PIR sensor to the user. In the design and implementation of a low-cost Arduino-based smart home system proposed by Souveer, Anshu and Vishwamitra [4], an Arduino Mega 2560 is used to control the system, where it is in charge of monitoring gas leaks, lighting, and smoke detection, among other features. Said system is controlled manually by means of switches or automatically, using a voice recognition system. Instead, in the system proposed by Rajani and Kadar [5], they use a PIR sensor, to detect movements, they control the system from a microcontroller, which acts in the way that, when someone enters the range of the sensor, it is activated and the system sends SMS and call. The internet of things has facilitated wireless control of different electronic devices, providing the ability to implement smart systems for home security [6]. In this sense, Yadav presents a home security system, which will emit a sound when the ultrasonic sensor detects a movement, likewise, this alert is sent to a web server via Wi-Fi and a message is sent via GSM. The proposed security system differs from those presented above and its importance lies it is fault-tolerant in the communication links to the cloud platform, incorporating, as already mentioned, dual wireless communication technology, in addition, the guarantees delivery of the alerts detected by the device of security through four notification channels and all this is offered at a low cost.

III. METHODOLOGY

A. Identification of Non-Functional Requirements

The software and hardware components for the development of this security
system are:
1. NodeMCU ESP32 Wireless Arduino.
2. GSM Module SIM800L.

3. PIR Sensor.
4. Cables Jumper.
5. Protoboard.
6. Open Energy Monitor (Framework Cloud).
7. IDE Arduino.
8. Fritzing.
9. EdrawMax
10. App Geyser.
11. Mobile Apps (Twitter, Notify My Device, E-mail and SMS).
12. Power Bank

B. Security System Device

This Security System is focused on detecting unauthorized access of people in a specific place, for example, an office. The proposed system consists of a physical and logical part. The first part (physical) includes the components that have been used for the development of the safety device. This device is basically formed by a PIR sensor, to detect movements and two communication interfaces to the cloud, to send the alerts detected by the security device. The second part (logic) is comprised of software that has been developed for the security device, the cloud framework, and the mobile application. The security device has been enriched at the software level so that it can commute between one communication interface and the other, that is, when the security device detects an alert, the alert will be sent to the cloud by default via Wi-Fi, but if no Wi-Fi link is established, then the device is capable enough to send the alert to the cloud via the GSM modem. In addition, this system with the GSM modem allows the sending of SMS (short message service) directly to the user's mobile (security personnel) and, on the other hand, the framework in the cloud, is responsible for managing the security events detected by the security device and notify the user through the notification channels: NMD, E-mail, and Twitter. The Safety Device has been designed to use an external power source (Power Bank) for the case when there is a loss in the power supply. Next, you can see the general design of the security device.

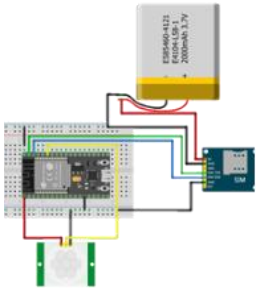

Fig. 1.General design of the security device.

The scenario used to implement the developed Security System is an office (Fig. 2), in such a way that the security device is strategically located so that it has the necessary scope and cone of vision of the PIR sensor [7] [8] [9], therefore, when the security device detects a movement, it sends this alert to the cloud, using the communication interface available at that time (Wi-Fi or GSM), once this event is delivered to the platform cloud, she is responsible for managing and notify the user through NMD, E-mail ,and Twitter. Regardless of which interface is used to send the detected alert to the cloud framework, an SMS will always be sent to the telephone number (s) that are declared at the code level in the software module developed for the security device.

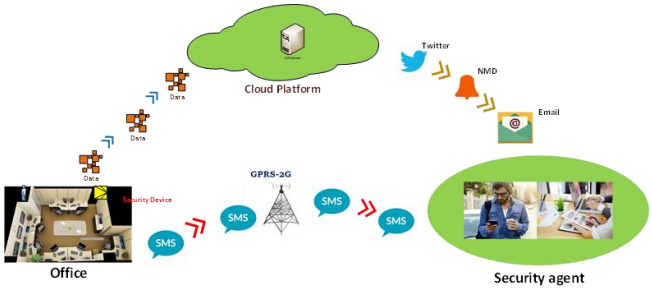

Fig. 2.General scenario of the security system.

The algorithm that is responsible for switching between the two communication interfaces to the cloud is the following (Fig. 3), where it is responsible for making the call of the algorithms, either to connect to Wi-Fi or GSM.

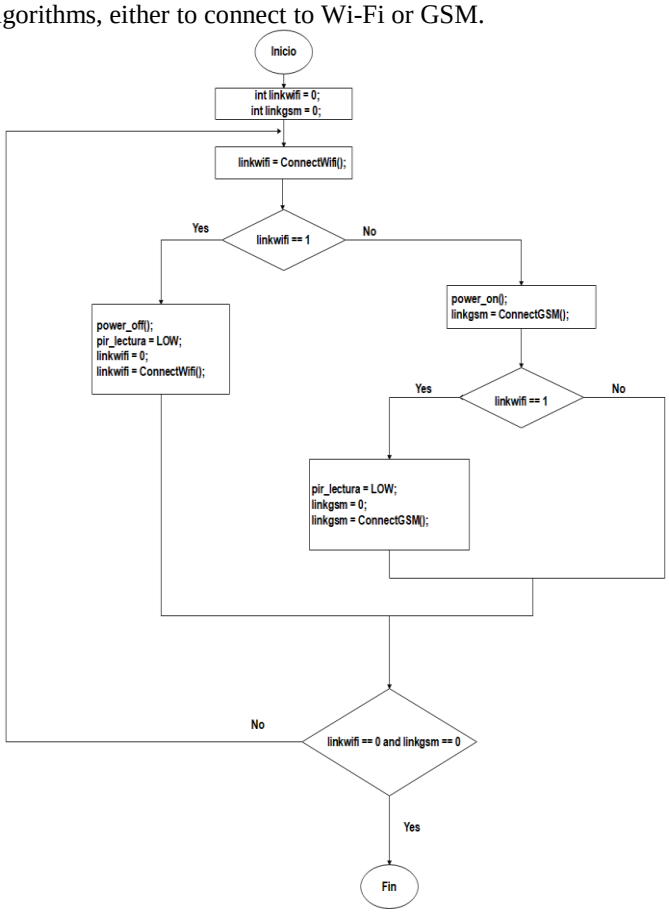

Fig. 3.Connection algorithm Wi-Fi/GSM.

C. Wi-Fi Interface Based Functioning

As mentioned, in the previous section, the Wi-Fi interface is used to send alerts detected by the security device to the cloud platform. It should be noted that this is the interface that has been defined by default for sending alerts to the cloud. Similarly, be takes advantage of the capacity and versatility of the microcontroller Wi-Fi ESP32 to store and execute the code that makes it possible for the security device to act an event against and established link to the cloud platform,

to then management the event and notify the user via the different channels. Next (Fig. 4), presents itself the algorithm that allows connect to an access point, where an attempt number is given (Cycle 1), then asks about the signal strength (Cycle 2) , if it is different from zero, be ask the status of the Wi-Fi network (Cycle 3), if I am connected, I get an IP address, later verify if I am still connected to the Wi-Fi network (Cycle 4), finally connect to the cloud server (Cycle 5) and send the alert to the platform (Cycle 6). If in Cycle 1, a connection to the Wi-Fi network is not achieved in all three attempts, then the call is made of the algorithm that controls the connections (Fig. 3) to execute and carry out the following instruction.

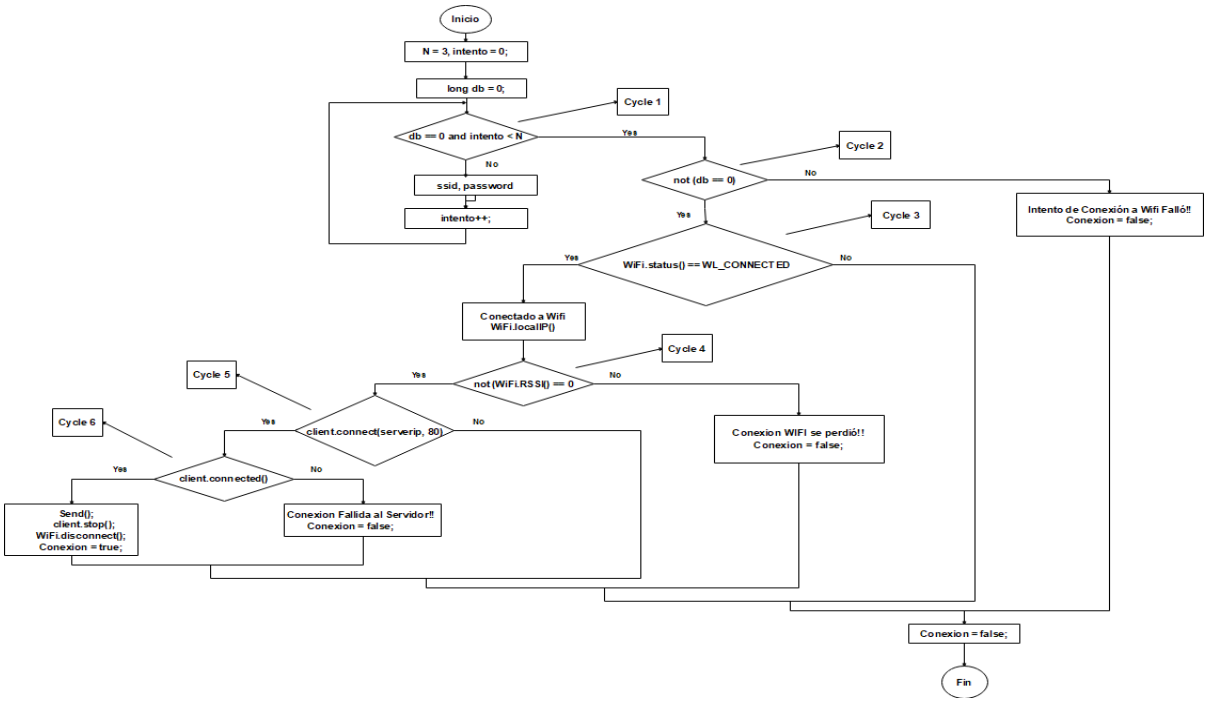

Fig. 4.Connection algorithm Wi-Fi/GSM.

D. Functioning Based on GSM-SIM800L

The GSM SIM800L modem is used to send alerts detected by the security device to the cloud platform. It is important to mention that the use and implementation of this communication interface are made, in the case when it is not possible to establish a link or connection to the Wi-Fi network. Therefore, the proposed security system is fault-tolerant in communication links. Also, this GSM modem is used to send SMS directly to the user's mobile device.

The algorithm that is responsible for making the GSM modem connection and the call of the algorithms to establish and send alerts to the cloud is as follows.

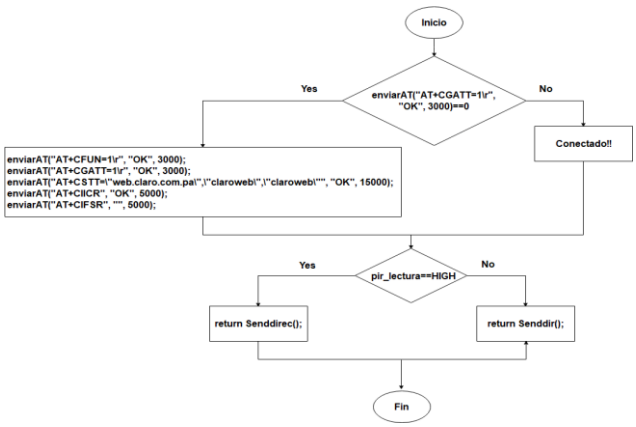

Fig. 5.GSM algorithm connection and sending alert to the cloud.

E. Framework Cloud

The cloud platform that has been used for this security system is Open Energy Monitor (OPM), which once the data sent by the security device is reflected, the feed settings are made and then the dashboard.

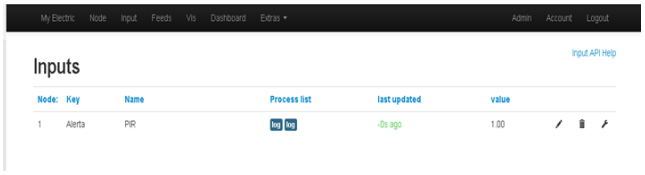

Fig. 6.Event interface on the cloud platform.

This platform, as already mentioned in this document, allows you to manage security events and deliver notifications through different channels or instant messaging applications.

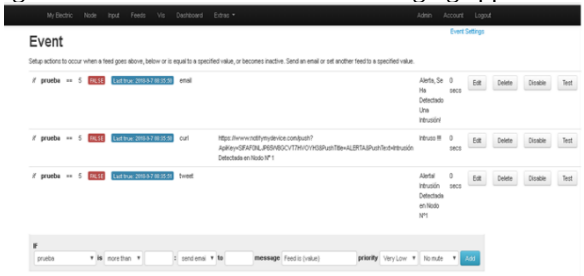

Fig. 7.Configuration of security events on the cloud platform.

F. Mobile Front-End

The web tool that has been used for the development of the mobile application is App Geyser, due to its easy use, deployment rapid and without any cost. To create this application, the cloud platform URL has been used, as follows: http://162.243.87.153/jmela/PIR.

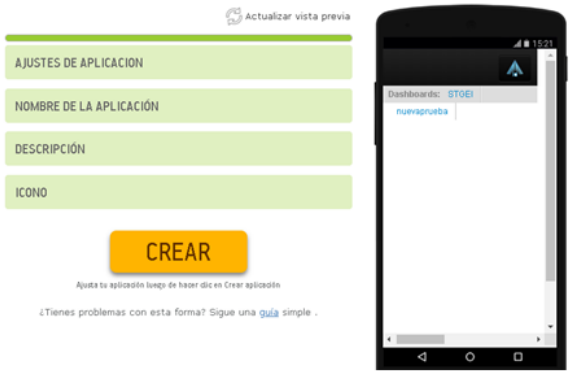

Fig. 8.Mobile application development .

IV. RESULTS AND DISCUSSION

A. General Scenario Validation

The Security System proposed in this study is characterized by being low cost, fault-tolerant in the links to the cloud platform and redundant in the delivery of notifications. This is done using dual wireless communication technology (Wi-Fi / GSM), which is responsible for sending alerts to the cloud framework, a PIR sensor, which has detection characteristics up to seven meters away, with a cone of 95º to 110º vision. As for the delivery of notifications, it is done through four channels (NMD, E-mail, Twitter and SMS), this is done so that the system notifies the user through different routes and thus ensure that its delivery security event notification. The device works so that, when the sensor detects a movement within his detection range, the security device sends the alert to the cloud platform via Wi-Fi, due this interface has been set as the default for sending of alerts to the cloud framework, but, when an event is detected and no link to the cloud is achieved through Wi-Fi, then the GSM SIM800L modem is used to send these alerts to the cloud platform, using the GPRS network (General Packet Service Via Radio). Regardless of the interface used to send alerts to the cloud, an SMS will always be sent directly to the user's mobile, through GSM.

Further, the security device has been designed to continue operating in cases of loss or failure in the power supply. An external rechargeable battery source is used for this (Power Bank). It is important to mention that to establish a communication with the GSM modem, AT commands had to be used because several libraries available for this modem were tested, but they did not work, therefore, they were used at a low level of programming of these modems to use the same.

B. Proof of Concept with Wi-Fi ESP32

The Wi-Fi interface has been defined by default, which is responsible for sending alerts to the cloud platform. The Fig. 10, shows the detection of an event, the attempt to connect to the access point, IP is obtained and the alert is sent to the cloud using the Wi-Fi interface.

```
-> Sin Evento
->
-> Sin Evento
->
-> Sin Evento
->
-> Sin Evento
-> 1
->
-> Evento Detectado
->
-> Intento de Conexión
-> Potencia de señal: -30
-> Intento # : 1
-> Conectado a Wifi
->
-> IP:
-> 192.168.0.104
->
->
->  Enviando ...
-> 1
-> Envio Completo
->
->  Enviando ...
-> 0
-> Envio Completo
-> Desconectado ...
```

Fig. 9.Sending alert to the cloud through the Wi-Fi interface.

C. Proof of Concept with GSM SIM800L

The GSM SIM800L modem is implemented in this security system for the case when no link is established to the cloud platform with the Wi-Fi interface, therefore, the system is smart enough to detect and decide that user interface. In Fig. 10, you can see where an event is detected, no Wi-Fi connection is achieved in three attempts and the GSM modem is turned on.

```
Sin Evento

Sin Evento
1

Evento Detectado

Intento de Conexión
Potencia de señal: 0
Intento # : 1
Intento de Conexión
Potencia de señal: 0
Intento # : 2
Intento de Conexión
Potencia de señal: 0
Intento # : 3
Intento de Conexión a Wifi Falló !!!

Encendiendo Modulo GSM...

AT
OK
Conectando...
```

Fig. 10. Failed attempts to connect to Wi-Fi and turn on GSM modem.

Once connected to the GSM network, the connection to the host of the OPM cloud platform is established and the detected alert is sent, using the GPRS network (General Packet Service Via Radio), Fig. 11.

```
-> Intento de conexion al Servidor ....
->
-> AT+CIPSTART="TCP","162.243.87.153","80"
-> OK
->
-> CONNECT OK
-> AT+CIPSEND=155
-> >
-> GET http://162.243.87.153/input/post.json?node=1&json={Alerta:5}
-> HTTP/1.1
-> Host:emoncms.org
-> Connection: close
->
->
->
-> SEND OK
-> AT+CIPCLOSE
-> CLOSE OK
->
-> Conectando...
-> AT+CGATT=1
-> OK
-> Conectado !!!
-> Intento de conexion al Servidor ....
->
-> AT+CIPSTART="TCP","162.243.87.153","80"
-> OK
->
-> CONNECT OK
-> AT+CIPSEND=155
-> >
-> GET http://162.243.87.153/input/post.json?node=1&json={Alerta:0}
-> HTTP/1.1
-> Host:emoncms.org
-> Connection: close
```

Fig. 11. Link to the cloud framework and send of alert via GSM.

As mentioned, this security system allows the sending of SMS directly to the user's mobile through the GSM modem. This option has been established to be the first notification to be sent because it is a bit slow due to the same infrastructure of cell cells. The process of turning on the GSM modem, connecting to the network and sending SMS is presented below (Fig. 12).

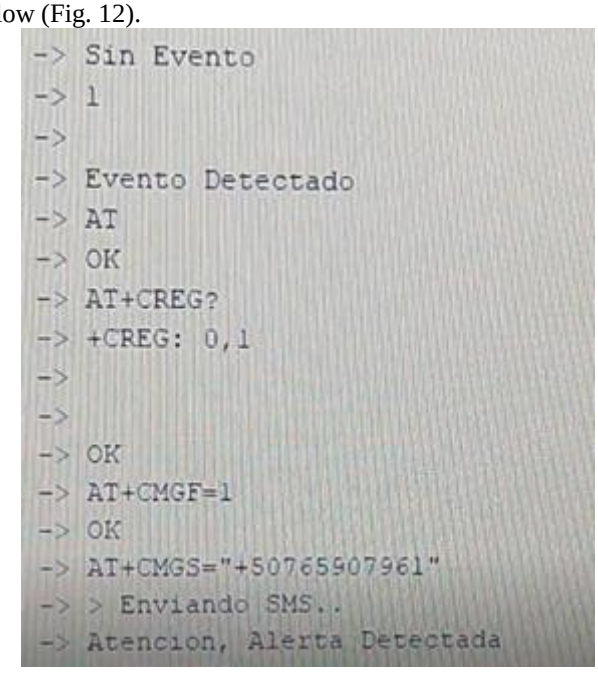

Fig. 12. Send SMS.

D. Framework Cloud Functioning

Open Energy Monitor, allows you to access notifications from anywhere with internet access, where we find an interface, such as the one shown in the Fig. 13.

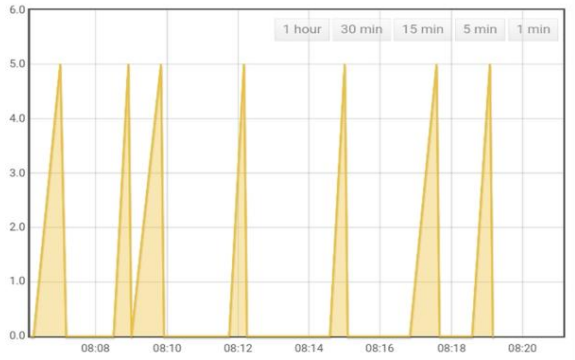

Fig. 13. Event interface on the cloud platform.

It should be mentioned that the graph of the previous figure every time the security device detects an event, it will go up to five (5), because at the software level this value has been defined, otherwise, if it does not generate any event the graph will remain at zero (0).

E. Mobile App

The application that has been developed allows real-time monitoring of the security system from an application for devices with limited resources.

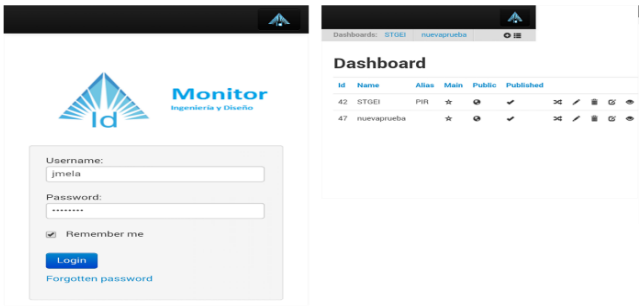

Fig. 14. Mobile application interface.

Once the application is installed on the mobile, the user is authenticated (Fig.14) and then we go to the dashboard new test, where we will find an interface like the Fig. 15.

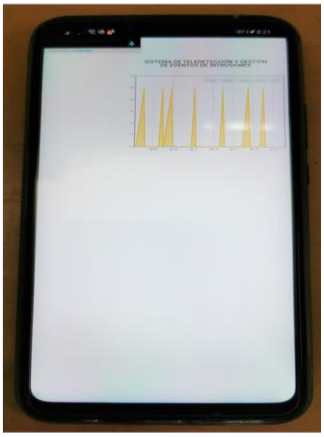

Fig. 15. Mobile application for security system monitoring.

F. Safety System Performance Test

Performance tests performed on the security system include timing the time from which the sensor is activated until the notification is delivered to the user's mobile. It is important to take into account for these tests the bandwidth of the access point to which it is anchored and the delays between the communication architectures and the cloud platform. It has taken several of tests, which has obtained the following times in seconds.

Table- I: Security System Performance Test

Tiempos Medios por Canal de Notificaciones			
Canal	**Proof Nº1**	**Proof Nº2**	**Proof Nº3**
Wi-Fi NMD	4.98 s	4.60 s	5.09 s
Wi-Fi EMAIL	9.05 s	7.78 s	10.02 s
Wi-Fi TWITTER	12.52 s	10.53 s	8.03 s
GSM NMD	27.99 s	13.36 s	9.02 s
GSM EMAIL	20.03 s	22.01 s	19.43 s
GSM TWITTER	38.08 s	40.23 s	41.32 s
SMS	32.32 s	30.12 s	33.45 s

As we can see in the previous table, the tests were performed for each notification channel and communication interface, where these times can be represented graphically, the following form.

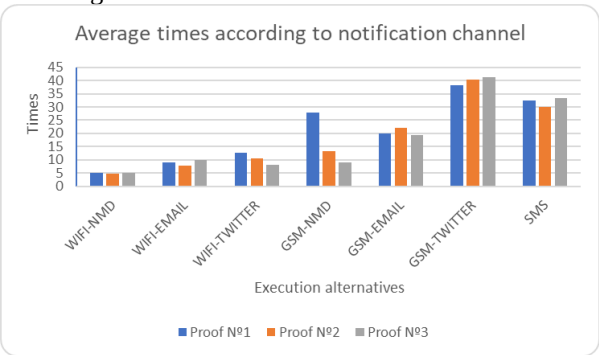

Fig. 16. Average times per communication interface and notification channel.

We can see that the fastest interface to send alerts to the cloud platform is Wi-Fi and with GSM it takes a little longer to send notifications. Therefore, when making a comparison to determine the interface and the notification channel with less time, we select the following graph.

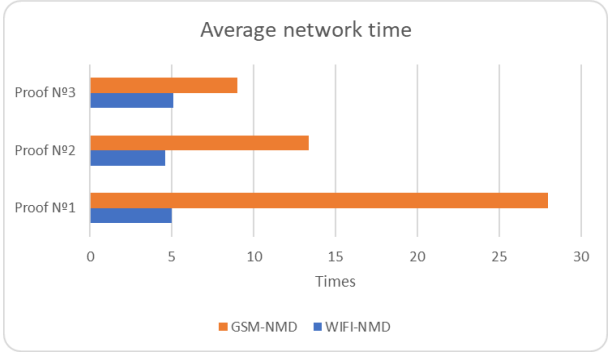

Fig. 17. Interfaces faster communication and notification channel.

Where the NMD notification channel and the Wi-Fi and GSM interface are obtained, resulting then fastest interface for sending alerts to the cloud framework, Wi-Fi and the channel to notify with less time, It's Notify My Device.

V. CONCLUSIONS

The security system incorporates fault tolerance in the communication links to the cloud platform.

Guarantee is offered in sending the alerts detected by the security device to the cloud framework.

The cloud platform allows access to security alerts detected from anywhere with an internet connection (Fig. 13).

The security system offers guarantee in the delivery of notifications through the channels established in the system (NMD, email, Twitter and SMS).

The security system can be monitored with a real-time mobile application.

The interface faster and with less time to send alerts to the cloud platform is Wi-Fi.

The notification channel with less time and faster to alert the security agent about an intrusion is Notify my Device.

REFERENCES

1. A. Coriat, "La estrella de Panamá," 3 March 2018. [Online]. Available: https://www.laestrella.com.pa/nacional/180328/16-situa-nivel-indice-victimizacion.
2. D. Cerrud, "La estrella de Panamá," 10 December 15. [Online]. Available: https://www.laestrella.com.pa/nacional/151210/servicios-seguridad-tecnifican.
3. S. Khirod and P. Umesh C. “IoT based intrusion detection system using PIR sensor”. 2017 9th IEEE International Conference on Communication Software and Networks. DOI: 1641-1645. 10.1109/RTEICT.2017.8256877.
4. G. Souveer, M. Anshu and O. Vishwamitra. “Design and implementation of a low-cost Arduino-based smart home system”. 2017 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT). DOI: 1491-1495. 10.1109/ICCSN.2017.8230356.
5. U. S. Rajani and A. A. Kadar. “GSM Based Home Security System Using PIR Sensor”. International Journal of Electronics & Communication Technology (IJECT). ISSN: 2230-7109. Vol. 8, Issue 2, 2017.
6. Y. Girish. “Arduino based Security System – An Application of IOT”. International Journal of Engineering Trends and Technology (IJETT). ISSN: 2231-5381, Special Issue, 2017.
7. I. Galiulina and P. Karlstén, 2018. [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1232494/FULLTEXT01.pdf
8. C. Platt and F. Jansson, Encyclopedia of Electronic Components, San Francisco: Maker Media, Inc., 2016.
9. L. Gonzalez, "Scribd Inc., 26 Agoust 2017. [Online]. Available: https://es.scribd.com/document/357270269/Manual-Del-Usuario-Sensor-de-Movimiento-Pir-Hc-Sr501

AUTHORS PROFILE

José Luis Mela, Degree in computer engineering from the Universidad de Panamá. I have participated as an exhibitor in the national scientific congress of the Universidad de Panamá and attended conferences and workshops on methods, guidelines and methodologies for the elaboration of project proposals. In addition, I have worked on several investigations for publications. The areas of research interest focus on wireless networks, operating systems, computer architecture, robotics, internet of things, Smart city, vertical agriculture, cloud computing, quantum computing, blockchain, software engineering and artificial intelligence.

Edwin Cedeño Herrera received his Master degree in Computer Science (2009), Master degree in Network and Communications (2009), and Master degree in Distributed Systems Engineering and Communication (2011), from the Metropolitan University of Science and Technology of Panama, Technological University of Panama and Technical University of Madrid respectively. Received his Ph.D. degree in Telematics Engineering from the Technical University of Madrid in 2017. Participates in several national and international research projects. His research interests are Service Architectures, Wireless Sensor and Actuator Networks, IoT, Delay and Disruption Tolerant Network, Distributed Systems Engineering. Since 2001 he is a professor on Informatics Engineering at the Universidad de Panamá. Currently, he is a Full-time professor, senior category II.

Gloris Batista Mendoza currently is an Assistant Professor at the Faculty Informatics, Electronics, and Communication at the Universidad de Panamá. She received her Bachelor's degree in 1998 from the Technological University of Panama and her Master's degree in Business Administration (2006), and International Relations and Foreign Trade (2013), from Latin University of Panama and Training and Employment Institute (Madrid, Spain), respectively. She has participated in several innovation and development projects sponsored by the Secretariat National of Science, Technology, and Innovation of the Republic of Panama. Since 2017 she has to work in areas related information systems and software engineering.