IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 10, October 2015.
www.ijiset.com
ISSN 2348 – 7968

Biometric access control system based on Internet of Things and using Free Hardware

Stalin Marcelo Arciniegas-Aguirre[1], Francklin Iván Rivas-Echeverría[2,1], Luis David Narváez-Erazo[1] and Galo Hernán Puetate-Huera[1]

[1] Escuela de Ingeniería, Pontificia Universidad Católica del Ecuador-sede Ibarra,
Ibarra, Imbabura, 100150, Ecuador

[2] Laboratorio de Sistemas Inteligentes, Universidad de Los Andes,
Mérida, Mérida 05101, Venezuela

Abstract

In this work it is presented the design and implementation of a biometric access control system based on Internet of Things (IoT), for optimizing resource's utilization using a free hardware Arduino platform, to improve the access control for personnel entering to different locations in the workplace.

This system is implemented in two Web platforms, the first has been developed on the free Hardware Arduino Mega device, which is configured on a client - server architecture via Ethernet shield, allowing recording the date and time of personnel entry and also gives access to the workplace, and the second is located on a Web server.

Finally, users or human resources managers have access to information anywhere, anytime as long as they have internet access.

Keywords: *Internet of Things, IoT, biometric, Arduino, Free Hardware.*

1. Introduction

People identification systems can recognize persons using cards, passwords or parts of the human body, but often the cards and passwords can be disturbed, whereas, systems using biometrics minimize adulteration, then, it´s considered one of the most reliable systems [11]. Biometric identification systems are divided into three main areas: face recognition, fingerprint recognition and iris recognition, they all have the same operation process, first have a training phase followed by a storage phase and finally the testing phase [7]. Fingerprint recognition focuses on certain characteristics of the ridges of the skin, which may be the amount, elevation and fences between two ridges [7].

Currently we are living in a world where the Internet can be found anywhere, it can be used not only for people to connect to the Internet, but also things. Then the Internet of Things (IoT) or Internet Objects is defined, according to Heredia [9] as "the interconnectivity between people and objects around them, decreasing the barrier between people and machines." Nowadays the internet connection objects grows very fast, mainly in wireless sensor networks and intelligent devices are getting inexpensive [6].

The free hardware Arduino Mega device, consists of an Ethernet module and a biometric sensor; they are designed for easy use by people who have no experience in the software and electronics area [10]; in this case, the Arduino is responsible for receiving the biometric sensor data, process information, make the right decision and send it to a server in the cloud, using Ethernet communication.

2. Biometric access control system design

First, it was made a research on the theoretical foundations of both biometrics and the Internet of Things; this in order to have a vision of the required objectives. In addition, this research can be considered as experimental because it is based on a prototype, where variables have been manipulated and measured, and finally validated, all based on specialized texts, journals, theses, scientific articles and knowledge of the institution.

The methodology used is based on the methodological framework for the development of intelligent and Software Engineering systems [1], [12], which is composed of the following steps:

- Stage 1: Analysis and description of the problem.
- Stage 2: Specification requirements.
- Stage 3: Analysis of costs, time and resources.
- Stage 4: Knowledge Engineering.
- Stage 5: Preliminary design.
- Step 6: Development and Implementation.

ISSN 2348 – 7968

Concerning the materials and equipment used, it can be mentioned the fingerprint scanner as shown in Fig. 1, which is responsible for registering new users, save them into the internal memory and assign a unique number that will be used as internal user identification during the authentication process.

Fig. 1. Biometric Sensor GT511C3
Source: [7]

Next device is the free hardware Arduino Mega shown in Fig. 2, which was selected because the information processing speed and communication pin amount, which allows connection to other devices [10].

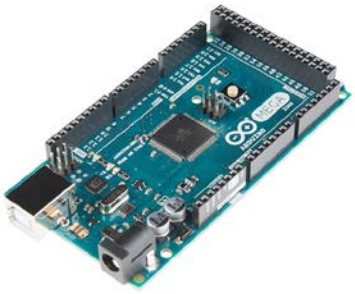

Fig. 2. Arduino Mega 2560
Source: [3]

Concerning the Ethernet shield shown in Fig. 3, allows connecting to the internet through the Arduino Mega RJ45 connector, giving the option of converting the Arduino in a Client or Web server, providing an IP address, default gateway and also one subnetwork. Thus, it is given the feasibility of using TCP and UDP protocols [2].

Fig. 3. Ethernet Module
Source: [8]

It also has a real time clock, which works regardless of whether or not there is energy in the Arduino because it contains a battery, and in this way it can be determined the exact time and date. In addition, a relay for opening the door and allowing access as detailed in the general circuit of Fig. 4 is implemented.

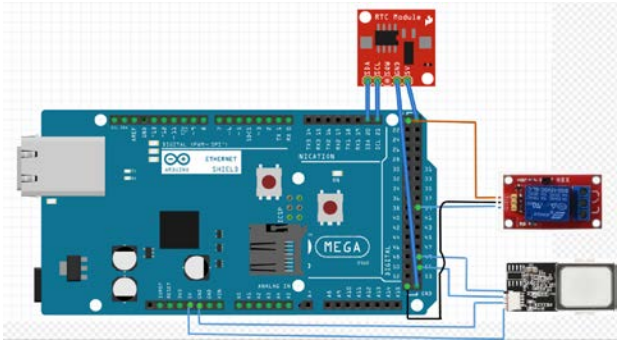

Fig. 4. Complete circuit
Source: Own preparation

3. Biometric access control system implementation

The system begins with the users' registration, this is done in the presence of the system's Manager, which is responsible for assigning a unique number to each user, which only is valid for internal system, this is stored in the memory of the biometric sensor, and whenever a user is authenticated, it will be identified with this number.
The connections of biometric access control based on Internet of Things are detailed in Fig. 5.

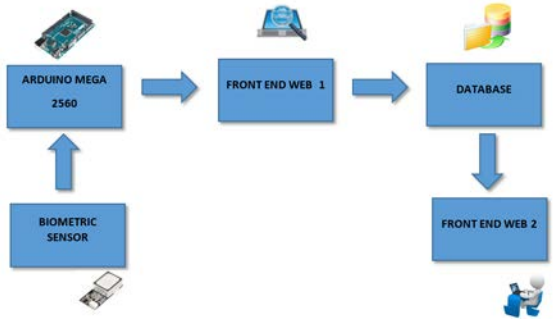

Fig. 5. General System Schematic
Source: Own preparation

The system begins scanning the fingerprint, which authenticates and sends the user number to Arduino, which is responsible for registering the time and date from the real time clock, then the Arduino verifies if there is any impediment to allow access. It then sends a typical HTTP header and is expected a standard response. If there is received the appropriate response, it's proceeded to send for data authentication, which travels through a Http object to front end website 1, once the data is published,

ISSN 2348 – 7968

these are copied by a proprietary server, which stores information in a database, with information available for both the administrator and users through the front end website 2.

The selected configuration is Client - Server, where the Arduino is set as Client with its own media access control (MAC) and Internet protocol (IP), the gateway (Gateway), and its subnet (Subnet). Language that enables Web page design for the Arduino is based on HTML codes.

The administrator can access the data through an access page, as shown in Fig. 6.

Fig. 6. Access page
Source: [4]

It also has the ability to generate reports, review history and even deny access to a particular user in real time as shown in Fig. 7.

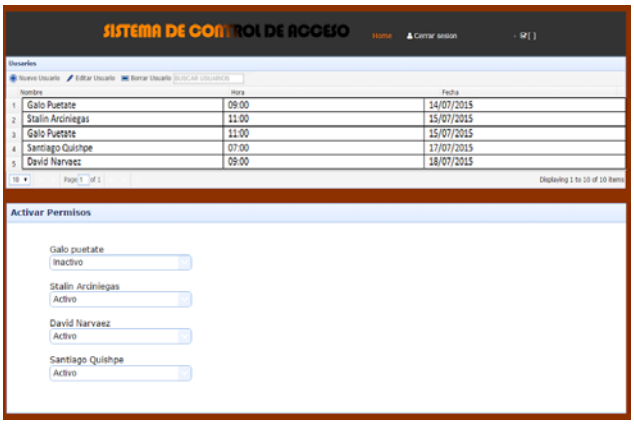

Fig. 7. Reports
Source: [4]

After this, all users can access the system to check the hours of authentication as shown in Fig.8.

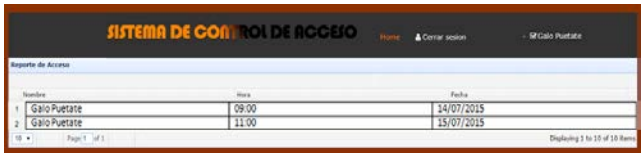

Fig. 8. User display.
Source: [4]

4. Conclusions

The development of a biometric access control system based on Internet of Things using Free Hardware, aims to have greater accessibility to microelectronic devices through a widely disseminated tool as is the internet, in order to have greater control regardless of place and time.

The use of biometric access system based on Internet of Things allows any user with Internet access to enter and supervise date and hours of admission, through history.

This biometric access system based on Internet of Things can be implemented for academic staff and students in order to control their entry into the classroom and laboratories, as well as a record of attendance for students. In addition it can be improved the interfaces and cloud database in order to give better presentation to users and provide statistic information.

As a free software and hardware system it has the advantage of having a great number of companies where can be obtained the required materials at moderate cost, also there are many information, bookstores, and case studies concerning the use and implementation.

Acknowledgments

Authors want to thanks the support given to this project by the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación of Ecuador and Prometeo Program.

References

[1] Aguilar, J., & Rivas, F. Introducción a las técnicas de computación inteligente. Mérida: Meritec. 2001.
[2] Arduino. Arduinoshield. 2013. http://www.arduinoshield.wordpress.com
[3] Arduino Mega 2560. 2015. https://www.sparkfun.com/products/11061
[4] Biometric access control system based on Internet of Things and using Free Hardware. 2015. https://iot.pucesi.edu.ec
[5] Biometric Sensor GT511C3. 2015. https://www.sparkfun.com/products/11792
[6] Cama, A., De la Oz, E. & Cama, D. Las redes de sensores inalámbricos. INGE CUC. 2012.
[7] Espinosa Duró, V. Evaluación de Sistemas de Reconocimiento. JCEE. 2001.
[8] Ethernet Module. 2015. https://www.sparkfun.com/products/11229
[9] Heredia, C. INTERNET DE LAS COSAS. 2014. https://estefan345.wordpress.com/2014/03/
[10] Margolis. Arduino Cookbook. United State of America: Teresa Elsey. 2011.

ISSN 2348 – 7968

[11] Motato Toro, Ó. F., & Loaiza Correa, H. “Biometric identification using infrared dorsum hand vein images”. Revista Ingeniería e Investigación Vol. 29 No. 1, 2009, pp. 90-100.
[12] Rivas F., Colina E., Rivas C. Expert Systems methodology for Management Processes. Proceeding of IASTED International Conference on Software Engineering. Las Vegas, USA. 1998.

Stalin Marcelo Arciniegas-Aguirre. Mechatronic Engineer (2011), Magister in Technologies for the Management and Teaching Practices (2015). Full time professor at Universidad Católica del Ecuador-sede Ibarra (PUCE-SI), Ecuador. Author of the patent Eco-colector Automático de Apitoxina, IEPI-2015-36251.

Francklin Iván Rivas-Echeverría. Systems Engineer (1993), Magister Scientiae in Control Engineering (1996), Doctor in Applied Sciences (2000). Full time professor at Universidad de Los Andes (ULA), Venezuela, Invited Research at Pontificia Universidad Católica del Ecuador-sede Ibarra with Prometeo Program, Ecuador. President of the Board of Directors of diverse national and international consortiums. Founding member and Coordinator for the ULA’s Intelligent Systems Laboratory. More than 230 scientific articles in journals, books, and international conference proceedings. Author of four books. Awarded by Halliburton for “contributions and dedication to the development of petroleum technology”. Recognition awarded by “Revista Gerente” as one of the 100 most successful Managers in Venezuela.

Luis David Narváez-Erazo. Electronic and field netwoks engineer. (2012), Magister in Technologies for the Management and Teaching Practices (2015). Full time professor at Universidad Católica del Ecuador-sede Ibarra (PUCE-SI), Ecuador. Research coordinator on Systems Engineering School, Author of the patent Eco-colector Automático de Apitoxina, IEPI-2015-36251. Electronic and mathematics project developer.

Galo Hernán Puetate-Huera. Systems Engineer (2009), Magister in Technologies for the Management and Teaching Practices (2015), telecommunications, servers and technical support in Emergency center (911). Full time professor at Universidad Católica del Ecuador-sede Ibarra (PUCE-SI), Ecuador. Geographic information system consultant.