International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 8-13
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

INTELLIGENT ACCESS POINT BASED ON A TYPICAL μCONTROLLER'S FUNCTIONALITY

M. Papoutsidakis
Dept. of Automation Engineering, Piraeus University A.S., Athens, Greece

E. Symeonaki
Dept. of Automation Engineering, Piraeus University A.S., Athens, Greece

G.P. Smyrnaiou
Dept. of Automation Engineering, Piraeus University A.S., Athens, Greece

D. Tseles
Dept. of Automation Engineering, Piraeus University A.S., Athens, Greece

***Abstract*— Biometric security systems are automated methods based on people from normal characteristics. Features of biometric security systems consist of facial recognition, fingerprints, the hand geometry, writing, iris, retinal, vein, and voice. The technology of biometric security systems is based on an extensive series of highly secure identification and personal verification solutions. Since the level of security breaches and fraud increases, the need for highly secure identification and personal verification technologies is obvious. Biometric security systems are able to provide the privacy of confidential financial transactions and personal information.**

The aim of this thesis is to design and present an application whereby an Arduino board will be programmed to automatically lock and unlock using fingerprint.

To achieve this objective, the remainder of this study is structured in two chapters. In the next section the general mode of application proposed, with several examples and then show the parts that will be our system, namely the Arduino board, the fingerprint sensor, the Led, relays, the power switch, the buzzer the servomotor and the LCD screen. Then presented on the PCB connections - fritzing and an alternative embodiment similar to the one proposed by this thesis, with fittings necessary for its operation. Then presents the operating scenario, ie programming held to operate all of the application components in the right way. Finally, some proposed future improvements to the application then become more secure and operational

With the passage of time along with the continuous development of technology, homes today could now provide safety, comfort and complete functionality of the site. The needs that were imposed by modern society coupled with the increasing demand for employment, have in effect reduced spare time to such a degree that it had to lead to the creation of automation for daily operations within the home where our physical presence may no longer be required. Therefore, it has become necessary to find a framework of procedures that is able to try and cover as much as possible the needs of people living within a residence. Through this effort developed the concept of the "smart home". The main factors leading to new automation technologies, constantly available on the market is the rise in living standards that generates new needs for comfort, quality and safety conditions in the workplace and residence. In Addition, the increase of the economic and environmental costs (greenhouse effect) of the consumption of natural energy sources that impose rational management and saving of energy of all kinds as well as the requirements (demands) for safety and reliability of electrical installations with potential future expansion and adaptation to rapidly changing needs and requirements (demands). This paper demonstrates the way all the above can be implemented in a modern residence.

Keywords— **Smart home, Sensor Network, Embedded Solutions, Microcontrollers Applications**

I. INTRODUCTION

In certain biometric identification systems there is the category of the double loop which is distinguished by very difficult class ring. In the system of this paper we consider a class of the double loop and ring. Grades stretched arc left and right loop having only a delta point while the class ring has two points of the delta. The arc category has the delta point and the core section which is hardly recognizable from the rest, as in [1], [2], [3] and [4].

Biometric readers are devices that recognize and store the unique fingerprint of each user and allow as access to space. The use of a difference between a biometric reader and a PIN keypad, is that it has a high quality reading sensor and a

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 8-13
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

microprocessor which compares the stored traces of fingerprints, with these scanning. If the fingerprint recognition among the saved, then activates the electronic lock to enter the person in space.
Before analyzing the biometric fingerprint recognition system, the sensor technologies mentioned are used for recording fingerprints extensive description on the sensor used in the present work. The importance of the sensor to the fingerprint system is greater than all other parts of the system. So it is important that the image quality of the fingerprint acquired by the sensor to be great. If the quality is not satisfactory, as perfect and effective the treatment and recognition algorithm entire system will be unreliable, like [5], [6] and [7].
The need for the use of biometric security systems can be found in the federation, state, local governments, the military, and in commercial applications. Operational network security infrastructure, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, health and social services are already benefiting from these technologies. More information about biometric security systems, standards activities, government organizations, industry and research initiatives on biometric technology can be found throughout bibliography like, [8], [9] and [10]. Biometrics is the statistical analysis of biological observations and phenomena. Biometrics is associated with the measurement of biometric technology: measurable, physical characteristics or personal features that are used to recognize the identity or verify the required identity of a person. Dictionary biometrics is "the science that studies with the help of mathematics, statistics, probability and the biological variation within a specified group", which can be found in [11], [12] and [13].
Therefore biometric systems can play an important role in the validation of a user. The Aktronix answers on 'another definition is based on the facts:
A person can be identified by:
- The occupation (ID, passport, driving license, etc ....)
- The knowledge (a password)
- What are (biometrics)
Those facts lead us to a definition:
"Biometrics allows the identification of persons from the natural feature or characteristic behavior that can be automatically detected." The problem with such a determination is that the difference between "biometric science" that has a very different way of implementation and "biometric technology" used in the identification of persons is not really clear. Now, in Europe, there is no legal definition of what is meant by "biometrics". The fingerprint reader is the most important part in an electrical safety lock with fingerprint recognition.
The T5 is an identification system fingerprint and inductive RFID cards. Used as a fingerprint reader as access control and time attendance staff. As an access control system, the use of the SC011 access control panel. As staff time attendance system, the use of access control panel is not required but is suggested to use the professional staff time attendance program for processing the records and on informative reports and the fingerprint reader OA99 to record the fingerprints of users in system.
The recognition of registered users at the terminal T5 is accomplished by fingerprints inductive RFID card or a combination thereof for greater reliability and safety. The reader T5, offers multiple connectivity options with H / Y, access control panel but also used as an auxiliary additional reader with other access control systems and recording clocks loggers. The T5 system is compact device placed even in the casing of the door.

II. HARDWARE EQUIPMENT

The use of access control systems (Access Control), is needed in facilities with increased monitoring requirements and registration of all inputs - outputs. Allowing access both to authorized persons, and to visitors. It can also be used for recording and processing of working hours (loggers) of employees with separate readers, a card or key ring new technology of biometric systems (fingerprint, iris eye, etc.).

A. **The microcontroller**

The Arduino Duemilanove is a small microprocessor device (Figure 1) connected with USB to PC. With the Arduino artists, designers, architects, hobbyists, students and college students learn programming and build entire projects for automation and robotic applications. So especially children start learning programming to flash Led into Wiring language like c / c ++ thanks to Arduino. The Arduino board is composed of a small processor open source where one can program even if it is learner through its own free program (IDE: Integrated Development Environment) that runs on Windows, Linux and MAC OS X. The Arduino connected Led, dimmers, ethernet port to become webserver and communication via bluetooth. Because software and hardware is tied, flexible and tested, with the Arduino made applications which interact between computer-user-environment.

Figure 1: Connecting Servomotor with Arduino

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 8-13
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

B. Fingerprint Sensor AF8600

The need for the quick transfer of fingerprint images (sensor networks), save storage space (use embedded systems to implement processing algorithms and fingerprint identification, with little storage space) and the optimal pretreatment of images for the most reliable feature extraction of them led to the creation of image formats (formats) fingerprints which have been compressed appropriately with simultaneous optimization of the characteristics to be used in recognition. The fingerprint card AFS8600 uses this type optimal images. Specifically optimized image you get from the card uses three coding bits of which yields the following 8 levels of gray tones which have kept the information they need to make optimal feature extraction.

Coding together with pretreatment on the export of eight levels of gray is implemented by a microprocessor incorporated in AFS8600 card. According to the specifications of this image type this pretreatment to enhance (optimize) the edges and the fingerprint valley is such that the image be directly implemented feature extraction algorithms.

Figure 2: Fingerprint Sensor

On the Arduino board is a micro-switch switch and 4 miniature surface mount LED. The operation of the switch (which has its RESET label) and a LED with POWER marking is rather obvious. The two LED with the TX and RX markings are used as indicator of the serial interface, well lit when the Arduino sends or receives (respectively) data via USB. The LED are controlled by the controller Serial-over-USB and therefore does not function if the serial communication is exclusively through digital pin 0 and 1.

For the selected application with 5V DC excitation chosen ready 2 Relay Module as shown in the following Figure 3 and not a simple DC relay for better protection of the Arduino microcontroller.

Figure 3: The Power Handing Board

The Arduino can be powered from the computer through the USB connection or external power supplied via a plug socket of 2.1mm (positive pole in the center) and in the lower-left corner of the Arduino. To prevent problems, the external power supply should be from 7 to 12V, and may be derived from a common transformer of commerce, from batteries or other source of DC. Next to the analog input pin, there is an even array of 6 pin with the POWER marking.

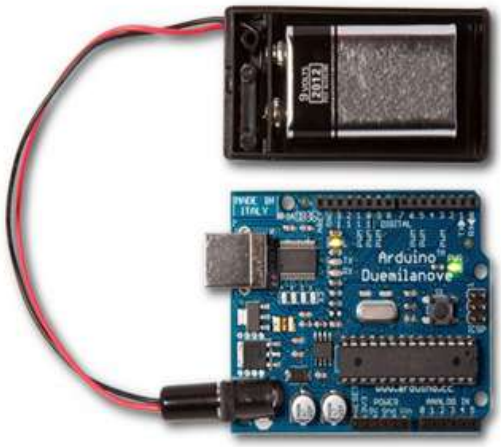

Figure 4: Power Bank for the Microcontroller

Used for the needs of the thesis, a buzzer which is programmed appropriately to start audio on every pass of the finger, whether successful or not accessible. Programming is done through the language and wiring for sound reproduction and highlight the selected appropriate notes to be distinct

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 8-13
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

sound of right or wrong footprint, ie who has access and who does not.
We used a motor of TowerPro Micro Servo sg 5010 mini simulating successful user access with a consequent rotation of the motor and the asserted lock opening giving access to the company. If the user is not successfully recognized, the motor does not rotate and there is no access.

Figure 5: The Servomotor for Lock Operation

The is an LCD screen attached to the system which is used to display the message such as the name of what enters and signs such as welcome or forbid the entrance and the other for the most realistic representation of the system used a 16x2 screen.
The connections are quite easy, using the following schematic to breadboard:

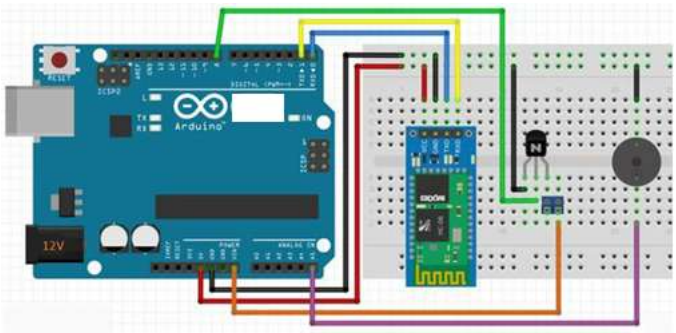

Figure 6: The System Wiring Diagram

The board on which the microcontroller is hosted includes also an Ethernet Shield. If the Arduino must be installed at a location away from the router (and do not want to pull ethernet cable) then use an A / P which is adjusted to Client Mode. Other things that we used: breadboard, jumper wires, photocells, resistors, insulating, multimeter, screwdrivers, etc.

Some details of the electronic connections of the system are listed below:
BT HC-06:

- Vcc - 5V
- GNG - GND
- RX -TX
- TX -RX

NPN Transistor:

- The pin B Base on pin 9 of Arduino
- The pin C Collector 1st pin terminal
- The transmitter E to GND

The second pin of the connector will connect to the Arduino pin "Vin" and give power to the electric opening our door (9V to 12V).

III. Operation Scenario and Code

In order for the proposed operational scenario to be functional, C code language was compiled and downloaded to the microcontroller. At this point it must be stated that a large number of experiments were designed and executed prior to these results outline. The system has already proven its reliability throughout these testing process and some parts of the programming code along with the relative comments are presented below for demonstration reasons.

```
# Micro-processor: Arduino UNO
# Language: Wiring / C ++ / Edit / Fritzing / Arduino IDE
# Purpose: Arduino RFID - System Security and Access Control
# Operation: Using RFID RC - 522, access control of individuals.
// Define the RFID
RFID rfid (10,5);
byte USER1 [5] = {0x04,0xCF, 0xE8,0x04,0x27};
// Byte USER2 [5] = {0xD5, 0x75, 0x6A, 0xD5, 0x1F};
// Here we can give access to other cards
// Declare the LCD, the address and the type of
LiquidCrystal_I2C lcd (0x27,16,2);
byte serNum [5];
byte data [5];
// Specifies the tune access and rejection / error melody
int access_melody [] = {NOTE_G4,0, NOTE_A4,0,
// Set LEDs, Buzzer and Servo-motor
int LED_access = 2;
int LED_intruder = 3;
int speaker_pin = 8;
int servoPin = 9;
// Set the servomotor
Servo doorLock;
void setup () {
 doorLock.attach (servoPin); // Preparation servomotor
 Serial.begin (9600); // Initialize serial communication
 lcd.init (); // Prepare the LCD
SPI.begin (); // Preparing the SPI communication for RFID
```

International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 8-13
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

```
rfid.init (); // Start RFID
lcd.setCursor (0,0);
lcd.print ( "Arduino-RFID");
// Here we create a variable for each user
// Onoma_finger or kleidi_finger
boolean USER1_finger = true; // Footprint
// Boolean USER2_finger = true;
if (rfid.isfinger ()) {// If the valid fingerprint found
if (rfid.readfinger ()) {// read the fingerprint
delay (1000);
data [0] = rfid.serNum [0]; // Store the serial number
Serial.print (data [4], HEX);
for (int i = 0; i <5; i ++) {
if (data [i]! = USER1[i]) USER1_finger = false;
// If (data [i]! = USER2 [i]) USER2_finger = false;
// If there is one of the active prints, remove "false impression"
// Here we can not control the other prints allowed, simple need to put what there like energy above
}
Serial.println ();
if (USER1_finger) {// If found an active footprint
lcd.setCursor (0,0);
lcd.print ( "USER1");
Serial.println ( "HELLO USER1!"); // Print message
for (int i = 0; i <12; i ++) {// playing welcome music
else {// If the fingerprint is not recognized
lcd.setCursor (0,0);
lcd.print ( "WRONG ID!");
lcd.setCursor (0,1);
lcd.print ( "ACCESS IS DENIED");
Serial.println ("CARD NOT RECOGNISED CONTACT THE ADMINISTRATOR!"); // Print message
DigitalWrite (LED_intruder, HIGH); // The LED glows orange in color
for (int i = 0; i <6; i ++) {// plays the sound rejection of the user
```

IV. CONCLUSIONS AND FURTHER RESEARCH

In this project it was outlined that the designed system is suitable for applications where we want electronically and wirelessly access to a place to with the assistance of fingerprint technology. This technique offers greater reliability and security in places where access requires control of individuals who have authority to prevent theft, vandalism and other similar events. Naturally the system can be developed more or even be modified, as needed. It could also be applied to a security system where there are real conditions in the authorization control for people who have or not access to some space.

After completion of the work we are able to note some improvements. A future development of the system, it could be the creation of a suitable software on the computer, which will communicate with the microcontroller and keeps input file of people who have requested access to a memory card to a hard disk. Also the input file (database) can keep statistics and provide us full control for people who got access to the system (Time, Day, Month).

Also with the addition of another fingerprint sensor can be achieved and output control in order to know the time and date of entry and exit of authorized persons. Thereby completely cover the entrance and exit of those who have access to our system.

A growing nowadays also technology that is worth noting is communication near-field (near field communication, NFC), which is an innovative connectivity technology that spreads and progresses rapidly with the primary purpose of solution of several problems of modern times and future. The operation is based on contact or approach, a 4 or 5 cm of the device that contains the NFC chip. This technology combines older wireless technologies like Bluetooth and RFID, which are harmonized to provide services to users in the following indicative cases:

- Security entrance check
- Online transactions
- Exchange and gather information
- Legality
- Payments
- Transportation / Transfers
- Certifications

V. ACKNOWLEDGEMENTS

All authors would like to express their gratitude to the Piraeus University of Applied Sciences for providing the required data and funding in order to undertake and complete this research project as part of “Automation of Production and Services” Postgraduate Program of Studies.

VI. REFERENCE

[1] Kim, J., Brewer, P., & Bernhard, B. (2008). Hotel customer perceptions of biometric door locks: Convenience and security factors. Journal of Hospitality & Leisure Marketing, 17(1-2), 162-183.

[2] Smith, A. D. (2005). Exploring the acceptability of biometrics and fingerprint technologies. International Journal of Services and Standards, 1(4), 453-481.

[3] Zhang, S., Janakiraman, R., Sim, T., & Kumar, S. (2006, January). Continuous verification using multimodal biometrics. In International Conference on Biometrics (pp. 562-570). Springer Berlin Heidelberg.

[4] Jo, J. G., Seo, J. W., & Lee, H. W. (2007, August). Biometric digital signature key generation and cryptography communication based on fingerprint. In International Workshop on Frontiers in Algorithmics (pp. 38-49). Springer Berlin Heidelberg.

[5] You, L., Zhang, G., & Zhang, F. (2011). A cryptographic key binding method based on fingerprint features and the

threshold scheme. International Journal of Advancements in Computing Technology, 3(4), 21-31.

[6] Thian Song, O., Teoh Beng Jin, A., & Connie, T. (2007). Personalized biometric key using fingerprint biometrics. Information Management & Computer Security, 15(4), 313-328.

[7] Chen, H., Sun, H., & Lam, K. Y. (2007, November). Key management using biometrics. In Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on (pp. 321-326). IEEE.

[8] Feng, Q., Su, F., & Cai, A. (2008). Fingerprint-based key binding/recovering scheme based on fuzzy vault. Journal of Electronics (China), 25(3), 415-421.

[9] Gangi, R. R., & Gollapudi, S. S. (2013). Locker opening and closing system using RFID fingerprint password and GSM. International Journal of Emerging Trends & Technology in Computer Science, 2(2).

[10] Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015, December). Fingerprint Biometric based Access Control and Classroom Attendance Management System. In India Conference (INDICON), 2015 Annual IEEE (pp. 1-6). IEEE.

[11] Liu, Y. (2008). Identifying legal concerns in the biometric context. J. Int'l Com. L. & Tech., 3, 45.

[12] Hemalatha, A. (2011). A Secured Biometric Attendance System (Thumsec System) With Access Lock Control.

[13] Yaakob, M. K. B., Jamia'an, M. B., Ramli, N. I. B. N., Elias, M. R. B., & Zulkifli, A. B. (2013). Embedded Door Lock System Using Biometric Technology (EDLS).