Multi-location access management system

Eng. Daniel BECHENEA, Prof. Ph.D Eng. Victor CROITORU, Eng. Vasile IORDĂNESCU

Rezumat. *SMAL (Sistem de Management al Accesului în diverse Locații) reprezintă un sistem ce are ca scop centralizarea autentificărilor utilizatorilor din mai multe locații într-o bază de date, într-un anumit interval de timp.*
Cuvinte cheie: *IoT, Sistem de management al accesului*

Abstract*. : MLAMS (Multi-location access management system) is a system aims to centralize user authentications within a certain timeframe from multiple locations into a database.*
Keywords: *IoT, Key Management Systems*

1. INTRODUCTION

Various access management systems implemented in commercial areas, offices and residences are presently described. Such systems are defined both by the complexity of hardware, software, and processed information.

IoT (Internet of Things) is a relatively new concept that envisages a world where different things or objects (home appliances, cars, mobile phones, etc.) can be interconnected by help of computer networks (Internet) [1].

Figure 1. Ecos Systems key management system

2. MLAMS ARHITECTURE

2.1 MLAMS Models - evolution

A system of this kind has been developed by Ecos Systems [2] . Their main purpose was to manage access methods. In addition, this company handled devices like weapons, laptops and phones (Figure 1).

Another example of a company is Morse Watchmans [3], which manages access key control. They have created a system based on access management, adding network functions (Figure 2).

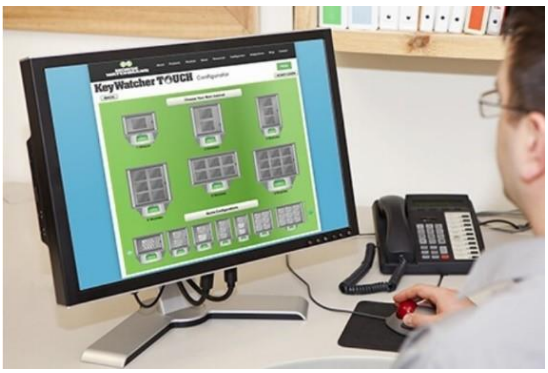

Figure 2. Morse Watchmans online access management system

2.2 Block hardware architecture

Figure 3 presents the block structure of the access management system in various locations. The interconnection of blocks can be unidirectional or bidirectional.

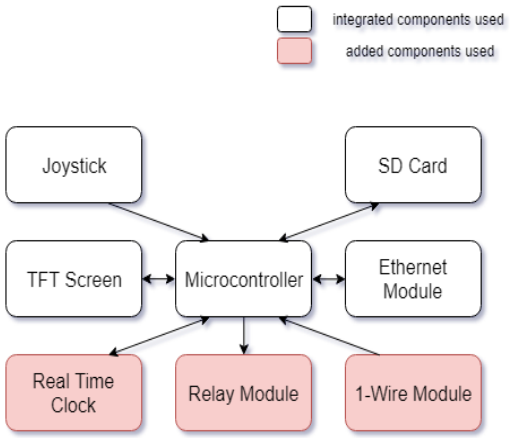

Figure 3. Block structure of MLAMS

2.3 Components

2.3.1 TFT Screen with Touch Screen

It allows the data to be entered and displayed at the same time. The way data is entered and displayed depends on the program loaded on the microcontroller. The Thin Film Transistor (TFT) screen can display the data in 262,000 different colors.

2.3.2 MMC / SD Card Slot

This card slot allows the system to increase its available storage capacity and store a database of users. Communication between the microcontroller and the MMC / SD card (MultiMedia Card / Secure Digital) can be made with the Serial Peripheral Interface (SPI) which is a high-speed standard interface that operates in full duplex mode.

This interface is used for data transmission, where the digital circuits are interconnected based on the master-slave principle.

2.3.3 LED indicators

An LED is an efficient light source. When connecting these LEDs, it is necessary to use a resistor that limits the current. We need 5 such devices: one called POWER to indicate that the system is turned on, one called MMC / SD that shows the activity of the MMC / SD memory card and three general LEDs that can be used for any desired purpose.

2.3.4 Real Time Clock

It helps the microcontroller to keep track of time and date, allowing even an alarm function. Thanks to the battery, this device allows the microcontroller to keep track of the clock even if the development board is not powered.

The real-time clock communicates with the microcontroller via the Inter-Integrated Circuit Interface (I^2C).

I^2C is a multi-master, multi-slave serial interface, characterized by a low transfer speed, but this is not a major drawback for the applications in which it is used. It has an INT (Interrupt) pin that is used to generate an interrupt, a Serial Clock Line (SCL) pin, a Serial Data Line (SDA) pin, a power pin, and a grounding pin.

2.3.5 1-Wire Module

This module is useful because it provides ways to access the user. The digital system operates on a base voltage that works with two contacts, data and ground (mass) for half-duplex bidirectional communication.

2.3.6 Relay module with one channel

This module has been added to provide physical access to a desired location. This device is ideal for this IoT project because it is small in size.

2.3.7 Ethernet Module

Thanks to this module, the system can access the local network to establish connections with devices outside the local network. The Ethernet module works with IEEE 802.3 / 802.3u and ISO 802-3 / IEEE 8021.3 (10BASE-T) standards. The development board connects to the local area network (LAN) using an RJ45 Ethernet connector.

2.3.8 Joystick

This device allows users to send commands to the microcontroller. Although it is used in the vast majority of gaming cases, it can be used to send an order to restore the system to its original state. It can have five commands: one when pressed and four for the four coordinates (top, bottom, left, right).

2.4 A new MLAMS - proposal

2.4.1 Software organization chart

Software architecture is based on hardware architecture. The description of all the states presented in Figure 4 is described in the Operation subchapter.

2.4.2 Operation

Once all the necessary elements (booklets, stacks, variables, static parameters, etc.) have been initialized, the system encounters the user with a start-up animation and enters a queue where he is waiting for the user's initiative (touching the TFT Touch Screen). If the TFT Touch Screen has been pressed, the system will display the main application screen where the user can communicate with the system. If the user has received a 1-Wire authentication device from the administrator, they can log in with the device. Once the user has successfully logged in, the system will act on the relay and generate a successful authentication screen, where it will be greeted with a "Welcome" message, its name being extracted from a file where all users are on SD card and also the time it was logged in, in accordance with the real time clock. An intruder is supposed to get into a location. He will not be allowed access if he does not know the user's password. If the user enters the wrong user code, the code box will be colored red and an unsuccessful user ID will be stored in the log file along with the date and time that this test was performed. If the intruder knows the code, but does not know the password and inputs the wrong password, the password box will be colored red and an unsuccessful user password authentication will be stored in the authentication file, along with the date and time that this attempt was made.

At the same time, all the authentication data, i.e. the log in date and time, authenticated user information, and type of authentication (1-Wire or code entry and password on the TFT Touchscreen) are saved in a variable named bufferWeb. Viewing this variable is made by the administrator only, on a login page with a name and password. If you enter the correct code and password, you will be able to view the latest logins in the system as an administrator.

A minimalist database is presented in Table 1:

Table 1

User:1234. Password:[2004] Andrei Mariș;
User:5678. Password [1357] Daniel Bechenea; 0114D2B418000097
User:5223. Password [2468] Ana Maria Enache; 0109D6B418000099
User:1623. Password [2423] Tiberiu Vlăsceanu;
User:1111. Password [1111] Teo Colda;

The ID’s of these users, Daniel Bechenea and Ana Maria Enache, 0114D2B418000097 and 0109D6B418000099 respectively, are the unique codes on 1-Wire slave devices. If a user has forgotten or lost the 1-Wire device,

he or she will be able to authenticate to the system using a code and a password on the Touch Screen, received from the system administrator. If he entered the correct user ID, he will need to enter the password again. If both information has been entered correctly, it will be successfully logged into the system.

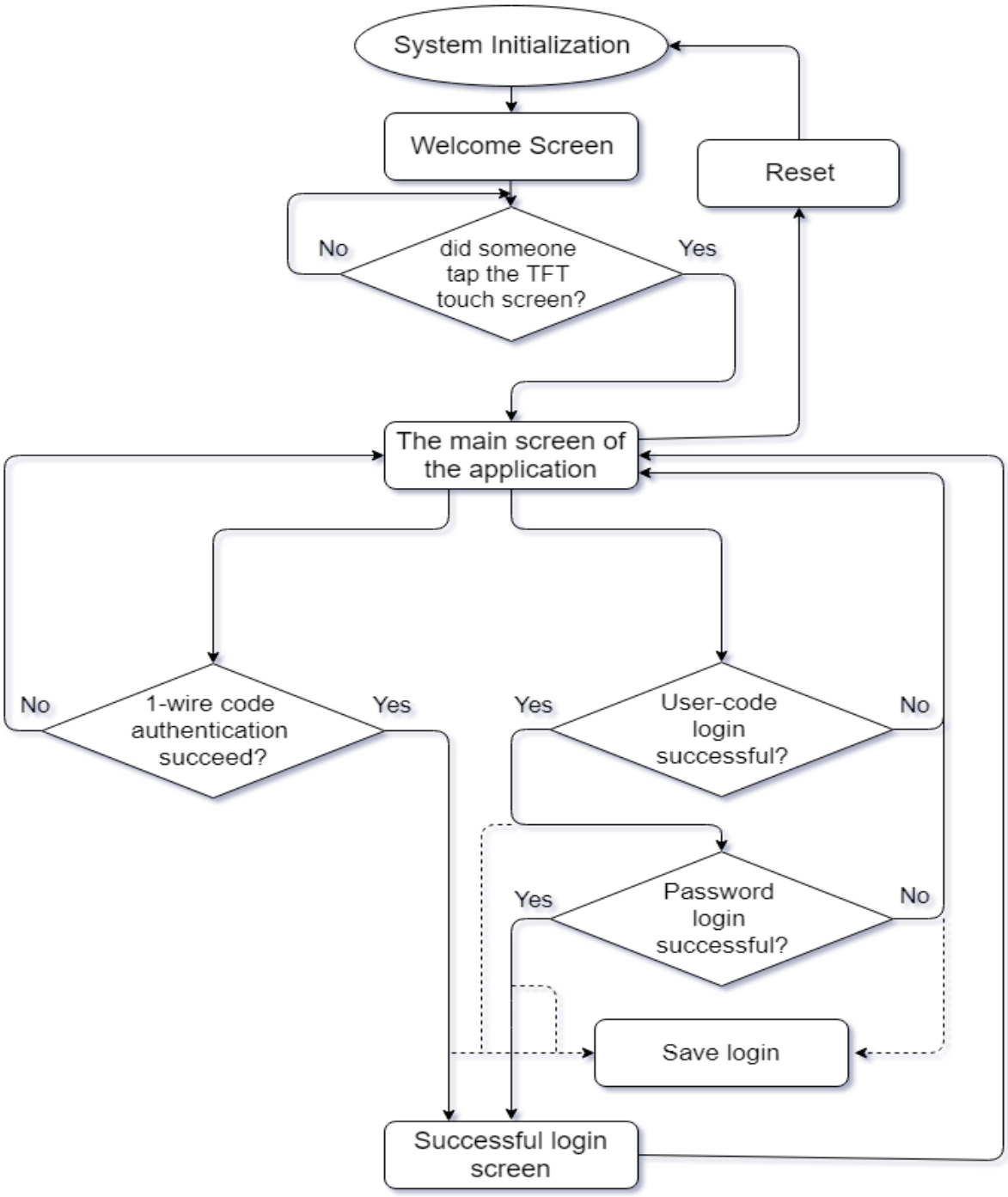

Figure 4. Software organization chart

3. MLAMS - IOT - PROPOSAL ARHITECTURE

An administrator will handle the management of multiple locations, verifying at any time a database of users [4].

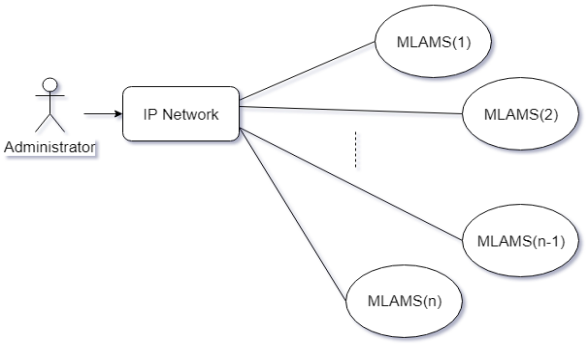

Figure 5. MLAMS-IoT Network

The Internet of Things can thus be used in the new access management system because the administrator can access the management system via an IP network and within each MLAMS we have different sensors for and modules that allow the development of a complex system (Figure 5).

4. CONCLUSIONS

As the number of devices connected to the Internet grows continuously, exponentially, the IoT model is much more present in society. These devices are essential in some cases, both for individuals and for multinational companies. As compared to the MLAMS systems presented in paragraph 2.1, Ecos Systems and Morse Watchmans, we tried to create a reliable, inexpensive system that includes the main features of an access management system such as: developing modern authentication methods (code / password and slave device 1-Wire iButton); creating a simple database that stores information about each user who has the right to authentication; updating the date and time using the real time clock that stores this data and remains saved even if the microcontroller power is turned off; saving to an SD card authentication file and a buffer that is used as a dynamic variable for the Web site, satisfying the need to authenticate the administrator with password and code only.

Acronyms

IEEE - Institute of Electrical and Electronics Engineers

I²C - Inter-Integrated Circuit Interface

IoT – Internet Of Things

ISO - International Organization for Standardization

LAN - Local area network

LED - Light-emitting diode

MLAMS - Multi-location access management system

MMC / SD - MultiMedia Card / Secure Digital)

SCL - Serial Clock Line

SDA - Serial Data Line

SPI - Serial Peripheral Interface

TFT - Thin Film Transistor

Bibliography

[1] A. McEwen și H. Cassimally, “Designing the Internet of Things“, Wiley, 2014.

[2] Ecos Systems, [Interactiv]. Available: http://www.ecos-systems.com. [Accesat 26 Aprile 2017].

[3] Morse Watchmans, [Interactiv]. Available: http://www.info.morsewatchmans.com. [Accesat 26 Aprilie 2017].

[4] D. Bechenea, V. Croitoru, V. Iordănescu, "Sistem de management al accesului multilocație, bazat pe modelul IoT", lucrările CNEE 2017, pag.156-159, Sinaia, 25-27 Oct. 2017, România.