UGC Approved Journal

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2017

"Centralized Locking System: A Real Time Fingerprint Authenticated Lab Access System using 2 Wire Communication (CAN)"

Usha H.N.[1], Aishwarya Hariths[2]

Assistant Professor, Department of Telecommunication Engineering, A.P.S College of Engineering, Bangalore, India[1]

BE, Department of Telecommunication Engineering, A.P.S College of Engineering, Bangalore, India[2]

Abstract: In the existing system, we have finger print authenticated locking system but we don't have a system where a room can be accessed remotely. Unlike the use of other forms of authentication, such as passwords or tokens, biometric recognition provides a strong link between an individual and a claimed identity. The CAN based system for Locking/Unlocking of Labs as CAN supports number of nodes. Each Lab can be treated as Individual Locking Unit. The Lab in charge of Finger print is stored as the database in Finger print sensor which acts as the central node present at a central place. When the Central Node reads the Finger print, it checks for authenticity. If it finds it is authenticated then the information will be sent to respective node through CAN bus, to open the respective Lab.

Keywords: Biometrics, Fingerprint authentication, CAN (Controller Area Network).

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics authentication (realistic authentication) is used as a form of identification and access control. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. They are often categorized as physiological versus behavioural characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to, fingerprint, DNA, retina, face recognition, iris recognition. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to, typing rhythm, gait, and voice.
One area where biometrics can provide substantial help is in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. By searching through the stored references, individuals who appear to have previously enrolled using a different identity can be highlighted for further investigation. It is very difficult to perform this type of check without the use of biometrics.

The desirable factors of a good biometric system are:

- **Accurate discrimination between individuals:** Since no two individuals can have the same traits, a biometric system should accurately distinguish between them.
- **Speed of operation:** A good biometric system must also be able to process the individual's traits during enrollment and verification at a good speed, in a matter of seconds.
- **The ability to deal with present and future numbers of individuals:** The system must have a large database to store the data, so that many individuals can be enrolled.
- **Environmental robustness:** If the system can adapt to varying environments, then it is said to be environmentally robust. A good system should have environmental robustness.
- **Ease of use:** The system should be easy to use so that all kinds of people can use it to enhance their security.
- **Capable of coping with as much individual variability as possible:** A biometric system is said to be good if it meets the requirements of many individuals.
- **Social acceptability:** People should be happy to use this system of identification, only then will it be a good biometric system.
- **Secure against potential attackers:** The main purpose of a biometric system is that it should be secure against any external threats, like hackers and frauds.

1.1 OBJECTIVE

This project provides a smart locking system for Lab access in organizations, with high security, using fingerprint authentication along with CAN bus, to enable a connection to any number of labs within the organization. The CAN bus consists of nodes which act as either master node or slave node depending upon the requirement. Using CAN bus

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

mechanism the transmission of the signal can be carried out without any complexity and with high speed as working of CAN is based on broadcast communication technique. The main objective of this project is to design and implement a real-time one point finger-print authenticated locking system of Labs to avoid the following:

- Unnecessary usage of Labs.
- Accessing of Labs by unauthorised persons.
- To make a centralised system to avoid misuse of labs/ resources.
- To have accountability.

An ARM cortex M3 uses serial peripheral interfacing for interfacing with hardware. The fingerprint sensor stores the authorized people's fingerprint template in its database, and allows access only to the individuals whose template is stored in the database. Depending on whether there is a fingerprint match or not, the individual will be allowed access to the lab. The information as to whether the lab can be accessed or not can be viewed using a graphical LCD connected to the system.

1.2 DRAWBACKS OF EXISTING SYSTEMS

In the existing locking systems in organizations, there are certain drawbacks.

- In a lock and key system, there is a possibility of duplication of keys for a single lock.
- RFID cards used as an authentication method is not very secure, since the RFID card can be stolen, replicated or transferred.
- One Time Password (OTP) method of authentication also does not provide high security measures, since this password is susceptible to hacking and can be stolen by unauthorized persons.
- Face recognition does not work well in rooms with poor lighting, or if the individual has long hair, or if the individual has objects like sunglasses covering his face.
- In a non-centralized locking system, it causes an inconvenience to the persons who have to lock/unlock a particular door manually.
- The existing door locking systems in organizations do not have enough security to protect the resources in the labs from theft.

II. CONTROLLER AREA NETWORK (CAN)

2.1 INTRODUCTION

The controller area network was progressed by BOSCH for the purpose of multiple master usage. CAN is serial communication bus defined by International Standardization Organization (ISO) mainly designed for the automotive industry in order to overcome the complexity due to wiring with two-wire bus. The communication of the message in CAN is by broadcast mechanism which specifies a maximum rate of signaling of about 1 megabit per second. Message identifiers, message formatting and bit-wise arbitration are main features of signaling scheme of the CAN.
Adding stations to an existing CAN network is done easily without need of any hardware or software changes to the existing stations as long as the recent stations developed are purely receivers. This allows the receiving of multiple data and the coordination of the processes which are distributed. Thereby transmission of the data does not depend on the presence of the particular type of stations, allows simple servicing and network upgrading.

Advantage:

- Provides high level of immunity for electrical disturbances.
- Has capability of self-diagnosing and repairing of the errors occurring in the data.

2.2 CAN NODE

The different parts that constitute a CAN Node can be seen in Fig.1. Central processing unit or host processor decides what the received messages mean and what messages it wants to transmit. Sensors, actuators and control devices can be connected to the host processor.

CAN controller is an integral part of the microcontroller. When receiving, the CAN controller stores the received serial bits from the bus until an entire message is available, this can then be fetched by the host processor. When transmitting, the host processor sends the transmit messages to a CAN controller, which transmits the bits serially onto the bus when the bus is free.
In the transceiver, the receiver converts the data stream from CAN bus levels to levels that the CAN controller uses. And the transmitter converts the data stream from the CAN controller to CAN bus levels. The CAN Bus is used to transfer data from one CAN Node to another.

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

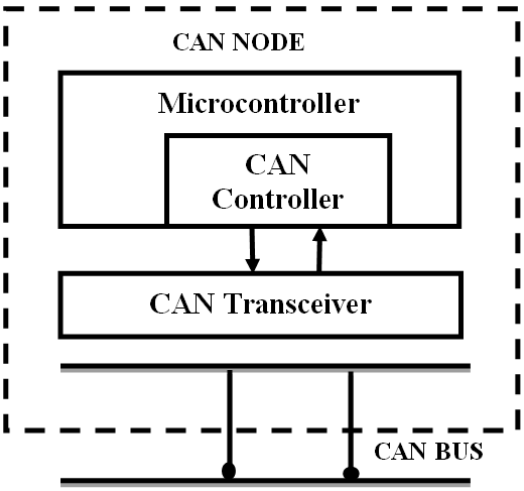

Fig.1: Parts of CAN Node

2.3 DATA TRANSMISSION

CAN data transmission use a lossless bitwise arbitration method of contention resolution. This arbitration method requires all nodes on the CAN network to be synchronized to sample every bit on the CAN network at the same time.
The CAN specifications use the terms "dominant" bits and "recessive" bits where dominant is a logical 0 and recessive is a logical 1. The idle state is represented by the recessive level (Logical 1). If one node transmits a dominant bit and another node transmits a recessive bit then there is a collision and the dominant bit "wins". This means there is no delay to the higher-priority message, and the node transmitting the lower priority message automatically attempts to re-transmit six bit clocks after the end of the dominant message. This makes CAN very suitable as a real time prioritized communications system.
The basic principle of CAN requires that each node listens to the data on the CAN network including the data that the transmitting node is transmitting. If a logical 1 is transmitted by all transmitting nodes at the same time, then a logical 1 is seen by all of the nodes, including both the transmitting node(s) and receiving node(s). If a logical 0 is transmitted by all transmitting node(s) at the same time, then a logical 0 is seen by all nodes. When a node transmits a logical 1 but sees a logical 0, it realizes that there is a contention and it quits transmitting. By using this process, any node that transmits a logical 1 when another node transmits a logical 0 "drops out" or loses the arbitration. A node that loses arbitration re-queues its message for later transmission and the CAN frame bit-stream continues without error until only one node is left transmitting. This means that the node that transmits the first 1 loses arbitration.
The node with the lowest identifier transmits more zeros at the start of the frame, and that is the node that wins the arbitration or has the highest priority. The bit-wise arbitration is as shown in Fig 2.

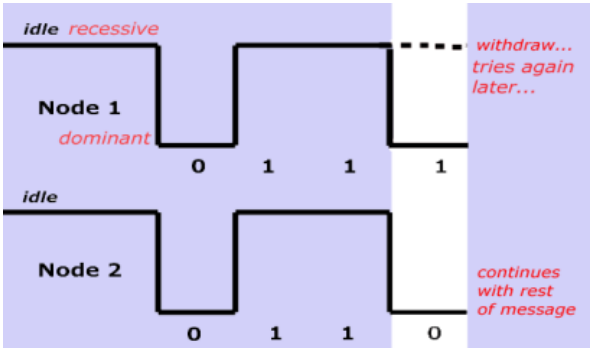

Fig. 2: CAN Bit-wise Arbitration

III. PROPOSED SYSTEM

3.1 SYSTEM OVERVIEW

Fig 3 shows the proposed block diagram. This is a CAN based system for Locking/Unlocking of Labs, as CAN supports number of Nodes. Each Lab can be treated as Individual Locking Unit. The Lab in-charge's finger print is stored as the database in finger print sensor which acts as the central node present at a central place. When the Central

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

Node reads the Finger print, it checks for authenticity and sends the acknowledgement to Microcontroller unit. The MCU checks the acknowledgement to decide whether it is authenticated/not. If it finds it is authenticated, then the information will be sent to respective node through CAN bus. The two wire communication bus makes communication cost effective as same 2 wires can be used for N nodes. The Lab Lock Nodes receives and decides whether to Lock or Unlock the Lab.

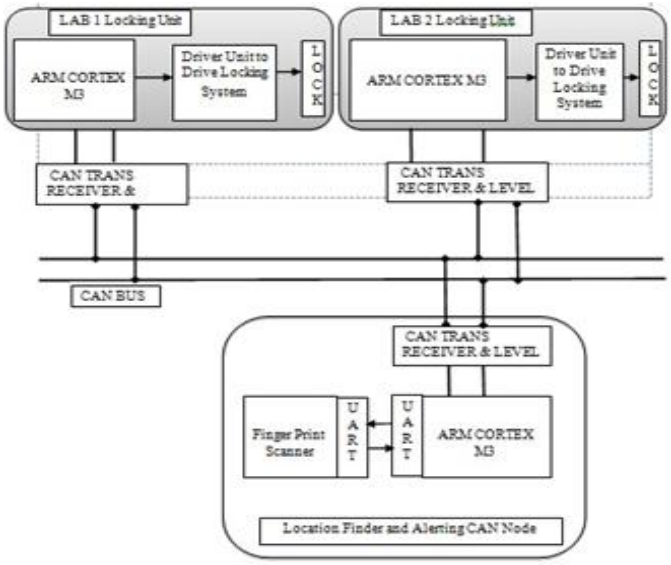

Fig.3: Block Diagram

3.2 HARDWARE REQUIREMENTS

3.2.1 ARM CORTEX M3

ARM is a family of instruction set architectures for computer processors, based on RISC architecture. ARM processors require significantly fewer transistors than CISC processors. This approach reduces costs, heat and power use. Such reductions are desirable traits for light, portable, battery-powered devices.

Some desirable features of ARM CORTEX M3 (LPC1768) are:

- General purpose 32-bit microprocessor.
- Operating frequencies of up to 100 MHz on high speed.
- Built-in Nested Vectored Interrupt Controller
- (NVIC).
- Up to 512 kB on-chip flash program memory with In-System Programming (ISP) and
- In-Application Programming (IAP) capabilities.
- Eight channel General Purpose DMA controller (GPDMA) on the AHB multilayer matrix
- Synchronous Serial Port (SSP)
- Inter Integrated Sound (I2S) – Audio/video
- UART, ADC (12), DAC (10), Timer, GPIO, and M to M transfer.

Peripherals:

- ADC -12 bit, DAC -10 bits.
- Timer/ Counter.
- PWM.
- GPIO -70 programmable pins
- RTC, Watchdog Timer.

Serial Protocols:

- Synchronous Serial Port (SSP).
- Serial Peripheral Interface (SPI).
- Inter Integrated Circuit (I2C)
- Inter Integrated Sound (I2S)
- Ethernet, CAN, UART, USB.

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

3.2.2 GRAPHIC LCD

LCD is the short form of liquid crystal display is the method employed in displays for notebook and other smaller computers. An LCD is composed of passive matrix or an active matrix grid for display. The active matrix has at intersection of pixel a transistor which consumes low power for controlling pixel luminance.

The passive matrix consist of grid of conductors with pixels positioned at each intersection of the grid. The graphical liquid crystal display is utilized for exhibiting customized characters and pictures. The graphical LCDs can be utilized as display units in various applications like video games, mobile phones, lifts. The 128x64 GLCD is interfaced with the LPC1768 Microcontroller to display certain messages, as seen in Fig.4.

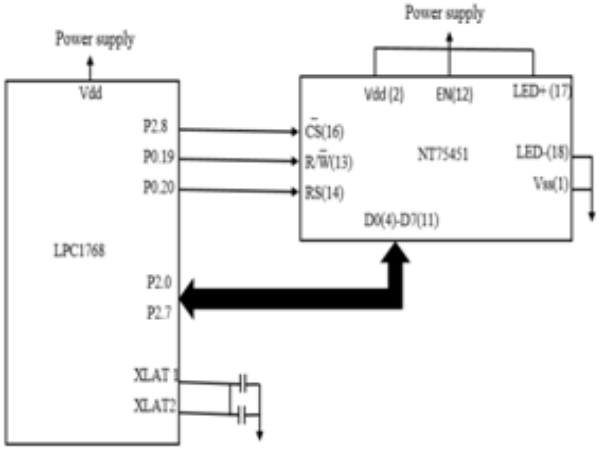

Fig.4: Interfacing of GLCD with LPC1768

3.1.3 FINGERPRINT SENSOR

The fingerprint sensor that has been used is shown in Fig 5. Fingerprint processing includes 2 parts: Fingerprint Enrollment and Fingerprint Matching/Verification.

When enrolling, the user needs to enter the fingerprint two times. The system will process the two finger images, generate a template of the finger based on the processing results and store the template. When matching/verifying, the user enters the finger through an optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live image with a specific template designated in the module. For 1:N matching, the system will search the whole finger library for the matching template. In both circumstances the system will return a verification message (success or failure).

Fig.5: R303A Fingerprint Sensor

IV. RESULT ANALYSIS

The ARM Cortex M3 is interfaced with the Graphic LCD to display the “WELCOME TO APS” message, which is displayed when the system is turned on as in Fig 6.

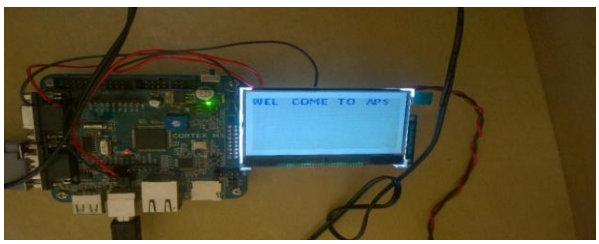

Fig.6: Welcome message displayed

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

The user then enters his fingerprint for authentication, to access a specific Lab. Each room is assigned a different fingerprint, to make the system secure. If the fingerprint is authenticated for Lab 1, then the door of lab 1 is opened and the system displays a message informing that the room is open, as shown in Fig 7.

Fig.7: Message displaying that Room 1 is open.

Similarly, if the fingerprint is authenticated for the opening of Lab 2, then the door of Lab 2 will open and the appropriate message is displayed, as seen in Fig 8.

Fig 8: Message displaying that Room 2 is open

If the fingerprint entered is not authenticated, then the doors remain locked and the system displays a message informing the user that door cannot be opened as in Fig 9.

Fig 9: Message displaying that room cannot be opened

V. CONCLUSION

The system uses CAN which already exists in the vehicle for controlling the electronic device unit. CAN uses two wire communication bus that makes communication cost effective, as same two wires can be used for N nodes. CAN is used for off-board communication which provides high level security. The system uses CAN protocol implementation using Finger print authentication for the security purpose so as to avoid fraudulent identity.

The system uses ARM-Cortex LPC1768 microcontroller, which consumes less power and is also cost effective. The fingerprint Recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database in the form of stored samples. Biometric method requires the physical presence of the person to be identified. Thus, biometric recognition systems offer greater security and convenience than traditional methods of personal recognition.

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

VI. FUTURE SCOPE

In the future, alarm can be introduced. When an intruder tries to break the door, the vibration is sensed by sensor which triggers an alarm. This will inform the neighbors about intruders and will help to take further action to prevent the intruder from entering. A buzzer can be interfaced with the controller and if the scanned finger print is mismatched, the indication can be given by the buzzer.
Infrared lasers can be attached to the doors so that if the intruder enters the room without turning off the lasers, which is done by the finger print authentication, the alarm goes off.

By using cloud technologies and GSM, security can be provided for a larger distance. The user will receive an SMS via the GSM, which will inform the user if there is a burglar or imposter trying to enter the room. This can be further extended by adding OTP for more security reasons, where the OTP will be send to the registered mobile number.

REFERENCES

[1] Rakesh Verma, "WAVELET BASED FINGERPRINT AUTHENTICATION SYSTEM:A REVIEW", Electrical and Electronics Engineering: An International Journal (ELELIJ) Vol 5, No 1, February 2016, Page No. 61-72
[2] Seung-Soo Shin, Kun-Hee Han, Kwang-Yoon Jin, Digital Door Lock on the Access Control System using OTP-based User Authentication, International Journal of Digital Content Technology and its Applications(JDCTA) Volume 7, Number 11, July 2013, Page No.436-442
[3] Aditya Shankar, P.R.K.Sastry, A. L.Vishnu Ram, A.Vamsidhar, Finger Print Based Door Locking System, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 3 March 2015, Page No. 10810-10814
[4] I.Yugashini, S.Vidhyasri, K.Gayathri Devi, Design And Implementation Of Automated Door Accessing System With Face Recognition, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386,Volume- 1, Issue-12, November 2013, Page No. 10-13
[5] Dr.Boyina.S.Rao, Deepa.k, Abarna.I, Arthika.S, Hemavathi.G, Mohanapriya.D, CONTROLLER AREA NETWORK FOR MONITORING AND CONTROLLING THE ENVIRONMENTAL PARAMETERS USING ZIGBEE COMMUNICATION, International Journal of Advanced Engineering Technology(IJAET) Volume 3 Issue 2 April-June 2012, Page No. 34-36