RFID Based Authentication Security System

Animela Suresh Babu[1], T.Bathina Babu [2]
[1]Dept of ECE
[2]Assistant Professor, Dept of ECE
[1, 2] Seshachala Institute Of Technology,Puttur.

Abstract- *Identification of persons is essential at places like government and corporate organizations, airports, railway stations and banks. Auto-identification means automatic identification of entities. We have various methods for auto-identification. Some of them are barcode systems, optical character recognition, biometrics, smart cards and RFIDs. Out of these RFID technology is widely used.*

Radio Frequency Identification (RFID) Card Readers provide a low-cost solution to read passive RFID transponder tags up to 2 inches away. The RFID Card Readers can be used in a wide variety of hobbyist and commercial applications, including access control, automatic identification, robotics navigation, inventory tracking, payment systems, and car immobilization. The RFID card reader read the RFID tag in range and outputs unique identification code of the tag at baud rate of 9600. The data from RFID reader can be interfaced to be read by microcontroller or PC. In this project, the RFID module reader typically contains a module (transmitter and receiver), a control unit and a coupling element (antenna).This module isinterfaced with the micro controller and when the card is brought near to the RFID module, it reads the data in the card and displays on the LCD. If the data in the card is matched with the data stored in the program memory, then it compares and displays authorized message. If the data is not matched it displays unauthorized. For authorized message, the door will be opened and closes automatically after a small delay. If it is an unauthorized person it alerts the persons through a buzzer. The RFID module alerts the buzzer whenever it reads the data from the RFID card. The door will drive by DC gear motor by l293d driver. The significant advantage of all types of RFID systems is the non contact, non-line-of-sight nature of the technology. Tags can be read through a variety of substances such as snow, fog, ice, paint, crusted grime, and other visually and environmentally challenging conditions, where barcodes or other optically read technologies would be useless. This project can provide security for the industries, companies, etc. In this project 7805 is a regulator and it avoids noise spikes in power supply. RFID modem is connected microcontroller through serial port. These RFID modem works under 9600 or 4800 baud rates. 16X2 LCD connected to microcontroller through digital I/O lines.

I. INTRODUCTION

1.1. Overview

Identification of persons is essential at places like government and corporate organizations, airports, railway stations and banks. Auto-identification means automatic identification of entities. We have various methods for auto-identification. Some of them are barcode systems, optical character recognition, biometrics, smart cards and RFIDs. Out of these RFID technology is widely used. Various applications of RFID are in transportation and logistics, manufacturing and processing, security systems, animal tagging, waste management, time and attendance, postal tracking, airline baggage reconciliation, and road toll management. Access control systems are implemented to deny unauthorized access to important documents or workplaces. Employees are given access cards with a radio frequency identification (RFID) chip in it. This technique uses electromagnetic (EM) fields to exchange data between a token (like a smart card or a tag) and the reader for authentication, identification or tracking purposes.

Radio Frequency Identification (RFID) Card Readers provide a low-cost solution to read passive RFID transponder tags up to 2 inches away. The RFID Card Readers can be used in a wide variety of hobbyist and commercial applications, including access control, automatic identification, robotics navigation, inventory tracking, payment systems, and car immobilization. The RFID card reader read the RFID tag in range and outputs unique identification code of the tag at baud rate of 9600. The data from RFID reader can be interfaced to be read by microcontroller or PC. In this project, the RFID module reader typically contains a module (transmitter and receiver), a control unit and a coupling element (antenna). This module is interfaced with the micro controller and when the card is brought near to the RFID module, it reads the data in the card and displays on the LCD. If the data in the card is matched with the data stored in the program memory, then it compares and displays authorized message. If the data is not matched it displays unauthorized. For authorized message, the door will be opened and closes automatically after a small delay. If it is an unauthorized person it alerts the persons through a buzzer. The RFID module alerts the buzzer whenever it reads the data from the RFID card. The door will drive by DC gear motor by l293d driver. The significant advantage of all types of RFID systems is the non contact, non-line-of-sight nature of the technology. Tags can be read through a variety of substances such as snow, fog, ice, paint, crusted grime, and other visually and environmentally challenging conditions, where barcodes or other optically read technologies would be useless. This project can provide security for the industries, companies, etc. In this project 7805 is a regulator and it avoids noise spikes in power supply. RFID modem is connected microcontroller through serial port. These RFID modem works under 9600 or 4800 baud rates. 16X2 LCD connected to microcontroller through digital I/O lines.

II. LITERATURE SURVEY

2.1SURVEYOFCONTEMPORARY

In this chapter, we will discuss about the information found by study and research that is critical and have an important value in the contribution of the whole project implementation. It also gives some basic knowledge or theoretical base and is used as a foundation to successfully achieve the main objectives. Most of the literatures are from the related articles, journals, books and previous works of the same fields. These literatures are then compiled and use as a guidance to the work of this project.

The number of Approaches and hardware components I have gathered from previous Articles/journals and other sites are given below. All these are used together and worked according to our requirement.

These seven methods are those most often encountered in a financial services environment, but they would be useful (and adaptable) to just about any area where stronger authentication was needed. Here they are:

Computer recognition software

Using the computer as a second authentication factor is accomplished by installing small authentication software plug-in that places a cryptographic device marker onto the consumer’s computer, which can then be verified as a second factor during the authentication process. The authentication process would then include two factors: password (something you know) and the device marker on the consumer’s computer (something you have). Because the device marker is always on the consumer's computer, the user only has to enter their username and password to log in.

Biometrics

Using biometrics as a second factor is accomplished by verifying physical characteristics such as a fingerprint or eye using a dedicated hardware device. Offering biometric authentication for consumer online banking has significant challenges including distribution of biometric readers and the associated cost per user.

E-mail or SMS one-time password (OTP)

Using e-mail or SMS OTP as a second factor is accomplished by sending a second one-time use password to a registered e-mail address or cell phone. The user must then input that second one-time password in addition to their normal password to authenticate to the online bank. This method is generally considered too cumbersome for everyday logins because there is a time lag before users get the OTP they need to login but is often used for the initial enrolment before providing another form of authentication.

One Time Password (OTP) token

Using an OTP token as a second factor is accomplished by providing users with a hardware device that generates a constantly-changing second password that must be entered into the online banking Web site in addition to the normal password. OTP tokens require the user to carry the token with them to login to the bank Web site. If a customer has multiple banks that require OTP tokens, then the user must carry multiple tokens unless the banks integrate their systems to accept a single token.

Out of band

Using an Out-of-band verification for authentication involves the bank calling a registered phone number and requesting that the user enter their password over the phone prior to allowing the user to login. Similar to e-mail or SMS OTPs, this requirement introduces a time lag and requires that the user be at the location of the registered phone number.

Peripheral device recognition

Using peripheral device recognition as a second factor is accomplished by placing a cryptographic device marker on a user’s existing device such as a USB flash drive, an iPod, Smart Phone memory card and then requiring that device to be plugged into the computer when the user logs into the online banking Web site. This can be good alternative to the OTP token because it provides a hardware based second factor but doesn’t require the user to carry an additional device. In addition, device markers from multiple banks can reside on a single hardware device without requiring the various banks to integrate their systems.

Scratch-off card

Using a Scratch-off card as a second factor is accomplished by issuing the user a card containing several PIN numbers that the user scratches off and then used only one time to log in. This is a lower-cost, one-time password option than tokens.

Note that TriCipher really likes the “Computer recognition software” method - the one I like least, in an online transaction environment, that is. I use many different computer platforms to interact with businesses online, businesses where I have accounts and spend money (or save money, if it’s the bank). I travel a lot but still need to spend money, pay bills, check balances, etc. Any strong authentication method tied to one specific computer actually hampers my access while not really providing a concomitant increase in security. I do like biometrics, but I really like using my cell-phone for out-of-band verification. Either via voice or SMS, it’s the system I wish more folks would adopt. You, of course, are free to choose whichever best serves your purposes.

III. PROBLEM STATEMENT

3.1 PROBLEM STATEMENT

Identity theft is one of the fastest growing types of crime nowadays, since it is more profitable than other types of crime. The aim is to identify the authorized and unauthorized individuals, by using RFID technology consisting of RFID tag and RFID reader, and comparing the details of the tag with the data available in the backend database.

Security systems play an important role to prevent unknown user entry into a secured place, which may include physical and intellectual property, without being authorized. The security system is basically divided into two types; the use of normal door lock key and the use of electronic automatic identification system. In general, locks are very simple devices that are employed to address a straightforward problem. Basically, lock can be easily hacked by unwanted people thereby allowing unauthorized people into secured premises.

There are several automatic identification technologies including barcode, magnetic stripe and Radio Frequency Identification (RFID) applied in security system. Radio-Frequency Identification (RFID) is an emerging technology and one of the most rapidly growing segments of today’s automatic identification data collection industry.

RFID technology, offers superior performance over other automatic identification systems. Because it is not an optical technology like bar coding, no inherent line of sight is required between the reader and the tagged RFID object

3.2PROPOSED SYSTEM-ARCHITECTURE-WORKING

OBJECTIVE

The goal of this venture is to outline and buildup .This project can be used to provide security for various governmental and corporate organizations, institutes, and in defense applications. This method of security verifies whether the person who is trying to access the secured data is authorized to do so or not.

The user is having an RFID tag assigned to him/her. These tags will be read by the RFID reader when the user logins into the system. Based on the tag number, the RFID reader will send command signals to the ATMEL Microcontroller. Any required changes (such as the change of user ID, their corresponding tag number or the number of authorized users) has to be made by the authorized person handling the backend database.

V. RESULT-ANALYSIS

5.1 RESULT

The result analysis of "Configuration and Execution of a sensor less Enlightenment controlled LED Lighting framework utilizing Neural Network" is done prosperously. The below mentioned figure shows a hardware implementation of the project.

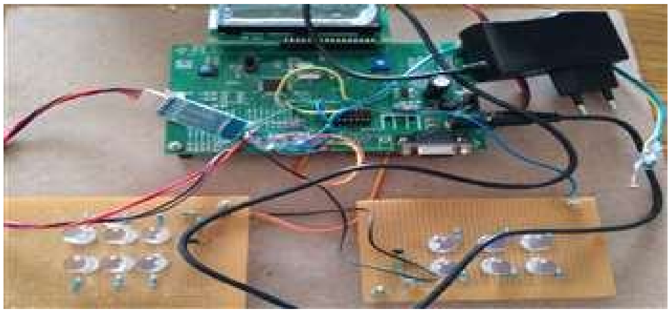


Figure 5.1: Proposed system Hardware

The above figure represents the complete hardware implementation of the proposed system.

Initial Light intensity measurement on LCD and Android versatile:

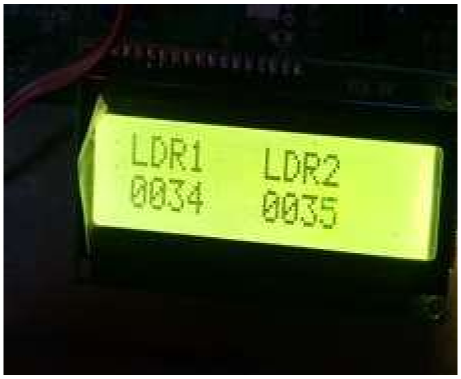
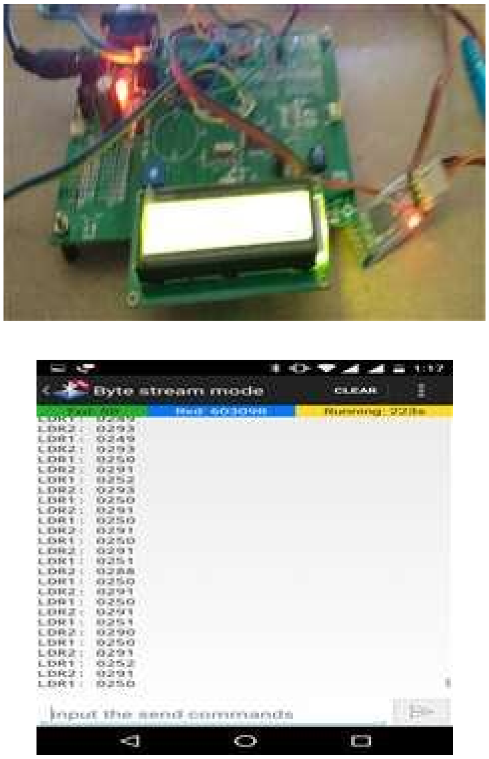


Figure 5.2: Light intensity measurements on Android mobile and LCD

The above figure represents a Light intensity on working places is measured by using LDR measurements on both LCD and Android versatile mobile using wireless data transmission using Bluetooth.

Bluetooth commands on L CD:



```
LDR2 : 0293
LDR1 : 0249
LDR2 : 0293
LDR1 : 0250
LDR2 : 0291
LDR1 : 0252
LDR2 : 0293
LDR1 : 0250
LDR2 : 0291
LDR1 : 0250
LDR2 : 0291
LDR1 : 0250
LDR2 : 0291
LDR1 : 0251
LDR2 : 0288
LDR1 : 0250
LDR2 : 0291
LDR1 : 0250
LDR2 : 0291
LDR1 : 0251
LDR2 : 0290
LDR1 : 0250
LDR2 : 0291
LDR1 : 0252
LDR2 : 0291
LDR1 : 0250
```

Input the send commands

Figure: 5.3 Bluetooth commands on LCD, Android versatile

The above figure represents the Bluetooth commands on both LCD, Android versatile like *1,*2,*3,*4,*5 for two set Networked LED lighting system controlled and similarly shows on LCD, Android versatile as Light intensity measurements on both display devices.

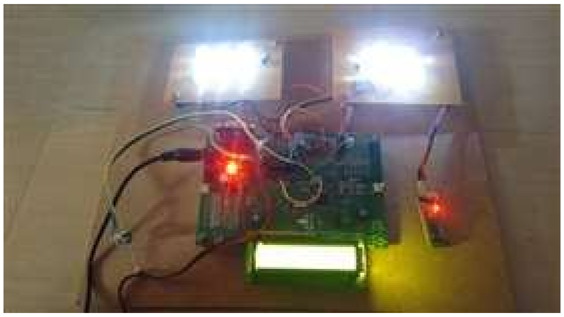


Figure 5.4: working model

The above figure shows a working model of the proposed system.

Figure 5.5: Light intensity Detector (LDR)

The above figure represents the hardware design of the light intensity detector with threshold controlled variable resistor.

5.2 ADVANTAGES

1. Automatic Identification.
2. Without physical contact
3. Wireless detection.
4. Automatic control are comfortable and easy access
5. Low power consumption

DISADVANTAGES

1. Short range controlling preferable not applicable for long distance
2. Need to configure RFID

5.3 APPLICATIONS

1. Home applications
2. Industrial applications
3. Airport checking applications
4. Railway applications
5. Automobile Applications
6. Goods tracking applications
7. Attendance monitoring systems

VI. CONCLUSION

RFID based secure authentication has been implemented and the results have been incorporated in this paper. It is concluded that RFID as a standalone security system provides a basic level of security. To enhance the level of security provided, RFID can be integrated with other stand-alone security systems like OTP and biometric authentication. The backend databases can also be implemented using software languages like SQL, JavaScript for further enhancement of security.

VII. FUTURE SCOPE

The Future scope of this article is to configure multiple nodes to configure and controlled over the distance range using IOT Technology and chip less devices and wireless nodes, to settle. In this soul, it is trusted that the present movement will prompt further improvements. For instance; chip away at future for military imply by the robots.

REFERENCES

[1] D.Surie, O. Laguionie, and T. Pederson, “Wireless sensor networking of everyday objects in a smart home environment, “in Proc. Int.Conf. Intell. Sensors, Sensor Netw. Inf. Process., 2008, pp. 189–194.

[2] S. Son, C. Lim, and N.-N. Kim, “Debugging protocol for remote cross development environment,” in Proc. 7th Int. Conf. Real-Time Computing Systems and Applications, Cheju Island, South Korea, Dec. 12–14, 2000, pp. 394–398.

[3] W. Yiming, X. Qingyuan, W. Guirong, H. Zilian, and W. Lianlian, “The internet-based remote ISP for distant education,” in Proc. 2001Int. Conf. Info-tech and Info-net, Beijing, Oct. 29–Nov. 1, 2001, vol. 6, pp. 54–59.