FOCUS AREA: INDUSTRIAL CONTROL ENGINEERING

TITLE: DESIGN AND SIMULATION OF ENTERPRISE LEVEL TWO FACTOR AUTHENTICATION SECURITY SYSTEM USING FINGER PRINT AND PASSWORD

ADVISOR: AGMUASIE B.

GROUP MEMBERS:

1.FATUMA SEID (0349/06)
2.HAYMANOT MELESE(0436/06)
3.MIFTAH MOHAMMED(0584/06)
4.MISGANA DESTA (0592/06)
5 MINTESINOT MULUGETA (0845/04)

Submission date: April/09 E.C.

Missionstatement

Our mission is to make people, good, institution or other place that needs to be secure like military camps, gunstores, exam centre etc. becomes more secure and safe.

Abstract

In our century the most centered concern of technology and big firms is securing their product and not allowing an individual having access to the information of the company that he is not concerned or does not have the right to see. Because unauthorized access to things might cause harm to the individual person and also can make the company a target to theft and burglary.

In order to tackle this problem there must be most likely an unbreakable level of security which can only be passed by the right person for that purpose.

This kind of security matters cover the following lists

- Big technology research labs
- Army information database servers
- Advanced nanotech laboratories
- Military grade manufacturer
- Highly sensitive chemical labs
- Bio-Hazardous materials…etc.

For these systems to be secured it will normally take high budget, many human resources and consume time to implement it. But what if this all can be done using less and affordable budget and less human resource? What you are about to see in the following pages of this proposal is simply the requirements and implementation methods of the above idea.

Our project is dual authentication institution security control system using GSM- module and biometric sensor. The system is fully controlled by the microcontroller also using GSM module. The password &finger print is stored in the memory so that we can change it at anytime.

The system has a keypad by which the password can be entered through it and also the biometric sensor to detect fingerprint. When the entered password and fingerprint the same with the password and fingerprint stored in the memory then the relay gets on so that the door is opened. If we entered a wrong password or fingerprint more than three times then the alarm will turned on and send SMS to police or the owner. If the password and fingerprint exactly matches with the stored password in the LED turns on and valid is displayed on the LCD. At this time the door is opened.

1. Introduction

1.1. BACKGROUND

Over recent years, security systems have changed from simple control panels and locks into high-tech gadgets. But, todays security systems aren't just the result of the technological developments that have rocketed over the past few years.

When World War I came to an end in1918, an increase in crime followed. As a result, the Americans become eagled to find ways of protecting themselves and their property. In addition to this, many insurance companies began to offer premium discounts to alarm subscribers. These events in turn produced a consumer demand for alarm system. An early model of an advanced video home security system consisted of a large camera that could view the exterior of the home through tiny holes mounted in the front door.

Burglar and safety alarms are found in electronic form nowadays. Sensors are connected to a control unit via either a low-voltage hardwire which in turn connects to a means for announcing the alarm to elicit response. In a new construction systems are predominately hardwired for economy while in retrofits wireless systems may be more economical and certainly quicker to install. Some systems are dedicated to one mission; handle fire, intrusion, and safety alarms simultaneously.

In common security system, the lights are triggered by motion gives the impression to user that someone is at home and able to see the burglar. Infrared motion detectors placed in house security system in crucial areas of the house can detect any burglars and alert the home owner or police. The first security system invented, house alarms were triggered by the release of a pressure button fitted into a door or window frame.

This basic alarm was fundamentally flawed as the entire intruder needed to do to silence. The alarm was to close the door or window. While various systems on the mark ranging from inexpensive house security alarms to highly sophisticated systems requiring professional installation. All modern alarms are based on the same foundation, the electric circuit which is completed either when the door is opened or closed depending on the security system designed.

The alarm is triggered when the circuit is altered and will not be silenced until a code is punched into the control panel.

The most expensive and complicated alarm systems might also involve a combination of motion sensors and pressure pads to ensure even the most cunning intruder doesn't get his hands on treasures.

Then our project intends to interface the microcontroller with the LED keypad, biometric sensor and other hardware components like memory, sounder start/stop the stepper motor through sending a right or wrong password. The measure of efficiency is based on how fast the microcontroller can detect the incoming message and act accordingly.

The controlling unit has an application program to allow the microcontroller read the incoming data through the modem and control the engine motor as per the requirement. The performanceof the design is maintained by the controlling unit.

1.2. PROBLEM STATEMENT

- Key lost
- Hacking of password
- Lost of card
- It may be open by similar key
- Dishonest of security guard

2. Literature review

This chapter contains the research and information about the project on several important concepts of home security system technology, tools used in the studies in related work in home security. Various home security system solutions are not available. Most of them are very expensive. We have studied different individual components separately and integrated them together with some more innovative features to make a home security system. Home security system are expected to be the standard in the near future when all aspects of the home can be monitored and controlled remotely by the home owner.

Different methods proposed by researchers around the globe related to the home security system are outlined here:

2.1. Bluetooth-based Home Automation System

The work of N. Sriskanthan *et al.*[1] shows the implementation of a home automation system using Bluetooth. They use a host controller implemented on a PC, which is connected to a microcontroller-based sensor and device controllers. The researchers even built a new protocol on top of the Bluetooth software stack, called Home Automation Protocol (HAP), to make the communication between devices possible. The device controller is connected to electronic devices through the I^2C Bus. The system allows more than one device controller to be connected to the host controller.

The work of H. Kanma*et al.*[2] also proposes a home automation system using Bluetooth that can be accessed remotely through GPRS. The researchers use a cellphone equipped with Bluetooth connectivity as a host controller and a GSM modem that provides Internet connectivity. Home devices are fitted with Bluetooth communication adapters so that they can communicate with the host controller phone via Bluetooth. The paper discusses remotely controlling and updating home devices along with fault diagnostics and detection. The work also talks about providing an electronics user manual on the phone using Bluetooth and Internet.

2.2. GPRS-based Home Automation System

There are a lot of home security systems implemented using GPRS. Most systems use the word security in the traditional sense, and only address the threat put forth by old fashioned intruders in home.

Researchers M. Danaher and D. Nguyen [3] propose a home security system using GPRS. The work uses a webcam to stream video and pictures of the home to its owner’s mobile through GPRS. The webcam detects movement by comparing frames for differences,

including light intensity. Video streaming in the proposed work is done using the home Internet connection, not the GSM modem.

The work describes video camera surveillance using the GPRS facility in mobile phones. The camera is triggered when an intrusion is detected or the door bell is rung. The system identifies intrusions with an infrared sensor. In the case of a doorbell, the system calls the homeowner and establishes voice communication with a live video feed between the visitor and the homeowner. When an intrusion is detected, an email is sent to the user along with a picture, most likely of the intruder. Upon receiving this email the user can start monitoring the video feed on his phone.

2.3. DTMF-based Home Automation System

The work of L. Muhury and A.H.M.A Habib [4]describes the design and implementation of a DTMF-based home automation system. The user calls a SIM number assigned to the home and presses the digits on their phone's keypad to control the home's devices by generating a DTMF tone. The tone is received and decoded by the GSM module at home using a DTMF decoder. The decoded instructions are passed to the microcontroller so that user commands can be implemented at home.

Those projects are their own drawback

Bluetooth-based Home Automation System: it was accessed by every phone that have Bluetooth connection

GPRS-based Home Automation System: it need internet connection.

DTMF-based Home Automation System: Home automation systems using DTMF are not very commonly implemented, maybe because there are other better options for communication available. Like all other systems, DTMF-based home security systems also have their security flaws. They are vulnerable to "fuzzing attacks," as described by R. Sasi [5]. In a fuzzing attack, a user exploits vulnerability in DTMF processing algorithms by giving unusual input data, which results in triggering an exception. This could cause the entire home network to crash.

Our project will solve the above problems by creating strong security system .it have used both finger print and password simultaneously. It was used by only authorized person .and when problem is happen, our system send a message to the owner or police. This make our system more safe and secure than before.

3. Goal of theproject

1) To minimize man power

2) To minimize the need for a key

3) To keep room security based on microcontroller

4) To use only by the authorized person

5) To know what microcontroller in detail

6) To develop password based door and infrared based window lock security system

4. Objective of the project

4.1 General objective

Design and simulation of enterprise level two factor authentication security system using finger print and password.

4.2 The specific objectives of the project are

- Design hardware.
- Software programming.
- Interfacing this hard ware and software by using coding.

5. Scope of the project

Security should have double meanings; one refers to the life and safety.

We can send this data to remote location within the mobile.

We add finger print sensor so entry will be allowed for authorized person using their finger print.We add a system that if sensor was interrupted by anybody a buzzer turned on automatically

6. Methodology

There are several steps to be applied in designing room security system. The relevant information is gathered through literature review. Data on different hardware materials and security system projects has been collected where the theoretical design is studied based on microcontroller for security concept.

6.1 hardware design

The next is the hardware development according to the circuit designed. This process is just only being preceded if each part of the circuit being improved is valid, else, it will be repeated until it is valid as the theoretical. Once the hardware development circuits have the output as the expected, then, the comparison for both hardware and theoretical analysis will be done. Next is the step where software structure is developed for the security system to be interface with the hardware development. While the final step of this research is on applying the whole project to the real room entrance like doors

•

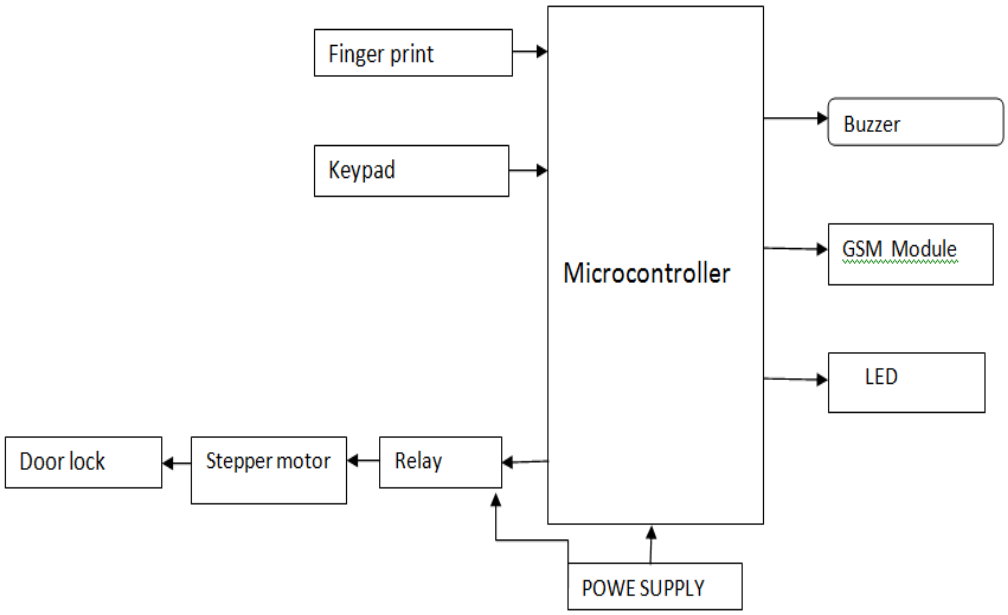


Fig 6.1. Hardware block diagram

6.2. SOFTWARE COMPONENT

Software structure is developed for the security system to be interface with the hardware development.

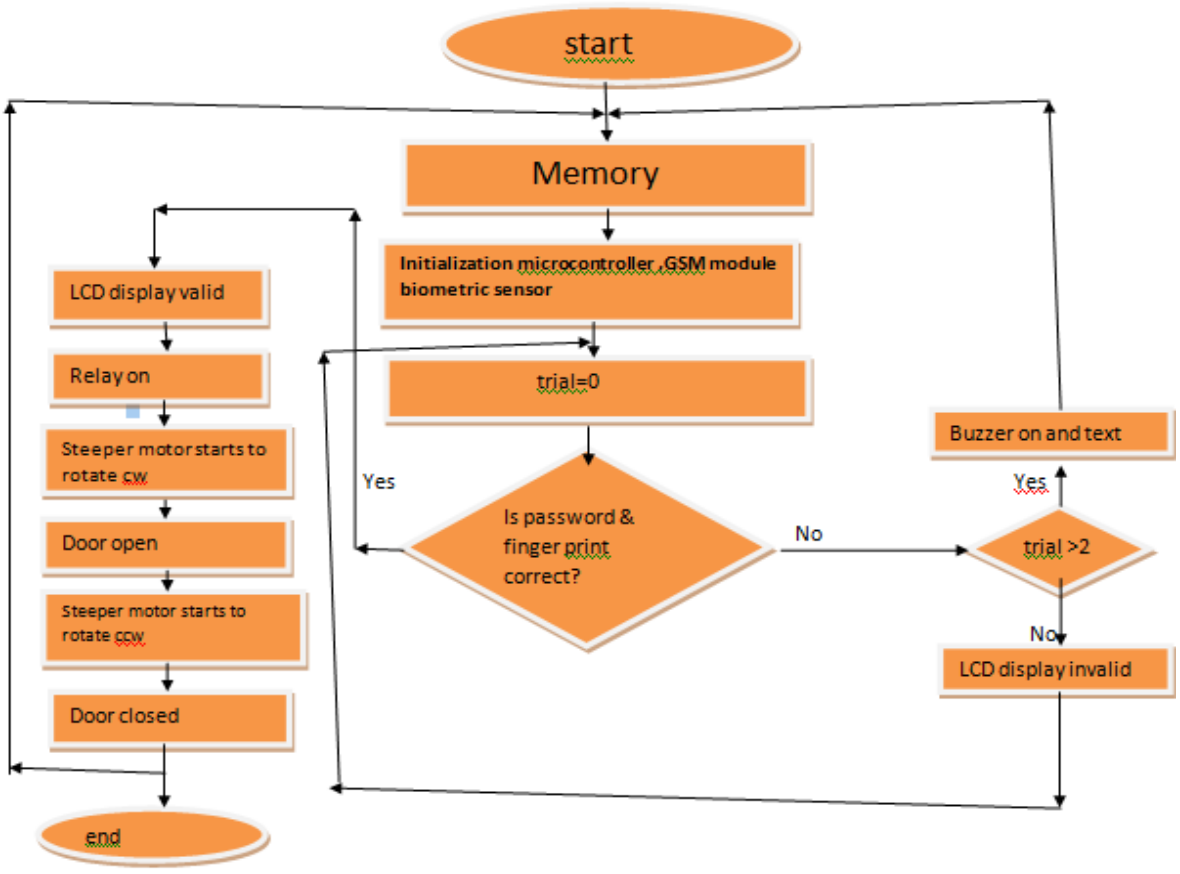


Fig 6.2.Software flowchart

7. WORK PLAN

Activity	Year 2009		
	April	May	June
1. .Literature review 2. Proposal writing &presentation			
3. design& simulate the project 4. Testing the system.			
5. Final presentation			

11. References

[1]N. Sriskanthan, "Bluetooth based home automation system," *Microprocessors and Microsystems, Elsevier,* vol. vol. 26, pp. 281-289, 2002. 44

[2]H. Kanma, "Home Appliance Control System over Bluetooth with a Cellular Phone," *IEEE Transactions on Consumer Electronics,* vol. 49 , pp. 1049-1053, Nov. 2003.

[3] D. N. M. Danaher, "Mobile Home Security with GPRS," *in proceedings of the 8 International Symposium for Information Science,* Oct. 2002.

[4] A. H. L. Muhury, "Device Control by Using GSM Network," *15th International Conference on Computer and Information Technology (ICCIT),* pp. 271-274, Dec. 2012..

[5] R. Sasi, "How I DOS'ed My Bank," in *Hack in the Box Security Conference (HITBSecConf2013),*, OCT 20