Hardware based system design using E-authentication approach

Gagan preet Kaur Marwah*, Amandeep Kaur and Mohinder Bassi
Lovely Professional University, Phagwara - 144411, Punjab, India; gaganpreet.marwah@lpu.co.in, Amandeep Kaur eramanlubana87@yahoo.com, mohinderbassi@gmail.com

Abstract
Home Security has been a major issue where crime is increasing and everybody wants to take proper measures to prevent intrusion. To fulfill this requirement, we opted this system named ‘e-Authenticator’. This system possesses wide range of features and made of familiar but vital technologies such as RFID and GSM Communication. The combinations of these technologies interfaced with the microcontrollers are the building blocks of our paper. The main goal of this paper is to design and implement an authentication cum security system based on RFID and GSM technology which can be organized in homes, secured offices and banks. We have implemented an authentication cum security system based on RFID and GSM technology containing door locking system using RFID and GSM which can activate, authenticate and validate the user and unlock the door in real time for secure access. The main advantage of using passive RFID and GSM is because it is more secure than other systems.

Keywords: Radio Frequency Identification (RFID), Global System for Mobile Communications (GSM), Short Message Service (SMS), One Time Password (OTP)

1. Introduction
In this growing business world, care taking and security are the prime requirements of every individual, whether it may regarding oneself or others. And there arises a situation with everybody who needs security or surveillance of their houses belongings especially when they are away. This situation has been regarded as an important issue by us and hence which led to the development of this system, e-Authenticator, with few more features than that cited above.

The main objective of this paper is to develop an Embedded System which is used for Home Care,
Verify and Authenticate the Authorized.

The most of this paper is made possible by the RFID Reader Module and the GSM Module. It is built with 3 AT89S52 microcontrollers, one handling the RFID Reader, other the GSM Communication and the latter controlling and managing the whole system including the earlier two microcontrollers, hence acting as the master.

The key features of the system are enlisted below:
‘If RFID, then Passcode’ kind of authentication.
SMS Alert on authorized door-access.
Access Block/Access Unblock mode remotely through Phone Call.
Auto Suspension mode and Alarm after 3 wrong passcode trials.
Call Alert during Security Breach.
RFID and OTP Verification needed during Passcode Change request.
Solenoid Actuator Locks for doors for improved protection.
SOS Code Facility at times of menace.
Whenever a phone call is being made to the system, it responds to the situation accordingly and responds by hanging the call. At real emergency, a call is being generated by the system to the user where he/she can record the call conversation, if any, which may be useful in legal proceedings.

2. System Architecture
The system internally is segregated into three sub units. One, the microcontroller maintaining the RFID Reader;
Two, the microcontroller controlling GSM Modem activities; Third, managing the earlier microcontroller and few other peripherals like LCD, keypad, solenoid actuator, piezo buzzer, etc.

2.1 Sub unit–1
This is the first sub unit of the paper. The block diagram below depicts the outline of interfacing of this sub unit with other sub unit(s). This sub unit is only the output device which acts as an input for the other two sub units.

2.2 Sub unit-2
This is the second sub unit of the paper. The block diagram below show that it takes the RFID input from the first sub unit which is used to identify the respective tag and accordingly send the respective message at a moment controlled by the third sub unit.

2.3 Sub Unit-3
This is the third sub unit which is having a one way inward communication with the first sub unit and a two way communication with the second sub unit. Also interfaced with the EEPROM (AT24C08), reed switch, relay, LCD, keypad, they perform the respective actions.

The EEPROM here is used to store the updated passcode which is read and compared to the currently entered passcode during the time of authentications.

The relay is activated by 12 V DC which drives the solenoid actuator lock. The reed switch/micro switch is fitted near the door hinge which senses the door events.

3. Detailing of the Circuit (Proteus Design)

The microcontrollers are provided with 5 V DC, RFID Reader and GSM Modem with 12 V DC each, relay and buzzer with 12 V DC and EEPROM, LCD with 5 V DC. The 5 V output step down through 12 V input is obtained through the 7805 voltage regulator IC.

The RFID Reader is connected to the MC1 through MAX232. The 3-bit each output is fed to both MC2 and MC3. The GSM Modem is connected to MC2 again through MAX232. The MC2 take a 2-bit input from MC3 and gives a 1-bit output to MC3. The MC3 is equipped with the LCD on P1 (DB0-DB7), P3.0 (RS), P3.1 (EN); keypad on P0 and P2; relay on P3.2 which further drives the solenoid actuator lock; micro switch on P3.4 and internal door-open switch on P3.5 all as shown in the previous figure.

There is a pull-up resistor used at P0 of MC3 so as to eliminate the draining effect. The BC547 transistors are used with the relay, buzzer, LED’s so as to amplify the voltage, also acting as a switch. The pin 1 and pin 2 of the EEPROM are connected to the P2.0 and P2.1 of MC3 respectively; pin 8 to +5 V and rest all pins grounded. The pin 1, pin 16 and pin 2, pin 15 of the LCD are connected to ground and +5 V respectively. The keypad is built by using the push buttons whose one ends are connected to the respective port pins of MC3 while other all are made common and grounded.
Two UART plugs (UART1 for RFID Reader and UART2 for GSM Modem) are taken out from the MAX232 IC in which pin 7, pin 8 are connected to the UART 1’s pin 3, pin 2 respectively and pin 11, pin 12 of MAX232 are connected to the UART2’s pin 2, pin 3 respectively. Pin 5 of both the UART’s are made common and grounded. Pin 5 and pin 6 of MAX232 are connected to Rx and Tx of MC1 while pin 13 and pin 14 are connected to Rx and Tx of MC2 respectively.

The default password being “0000” and when it is keyed-in, the MC3 activates the relay which further drives the solenoid actuator lock and simultaneously changes the state of GSM Modem to send the entry related message to the user. If the scanned RFID tag is not associated with the system, then no action is visible on the LCD.

If the scanned RFID tag is authorized but if the passcode entered is wrong then a “WRONG PASSCODE” message is displayed and if this thing is repeated for three times, immediately the system is put into the suspended state such that there can’t be any action performed on the system externally and immediately there would be an SMS intimation to the user regarding the wrong passcode trials. Until and unless the user responds to the system, the system will remain in its state as it is. To put the system back to the normal state, the user just needs to dial a call to the system and the system automatically hangs up the call telling us that it had received the command and system is back to its state. We name this as ‘Call And Hang’ (CAH) technique.

There is also an “ACCESS BLOCKED” state for the system to be put into by the user when either the entry or the exit is to be restricted. This can be performed by CAH at the first. If CAH is performed for the second time, system would be back to its normal state. During this time, if another CAH is performed within 30 seconds, then the system is designed to enter into a passcode changing catalogue and immediately an OTP is sent to the user’s mobile phone through an SMS. If it is entered, then there is a provision to create new pass code. If OTP is entered wrong, the system gets back to its normal state by displaying a message as “INVALID OTP!” on LCD.

There is also a special feature that the system has two pass codes. One to unlock the door and the other to deceive those strangers present, if any, during the times of menace. No sooner a message as “SORRY! BATTERY LOW! SYSTEM SHUTDOWN!” on the LCD and the system acts as if it is really down but intimates the same through an SMS and a phone call to the user. Now the user can attend to this phone call and record the conversation, if any, which could be helpful in legal proceedings. The user must perform CAH to retrieve the state of the system.

Finally, there is a micro switch at the hinge of the door which senses even small impulsive forces or knock-outs on the door. If any, again there is intimation to the user through both SMS and phone call.

Hence by all the above features, a residence can be secured to the maximum extent possible.
5. Results and Discussion

Initially, this message is displayed and waits for any of the external events to occur.

If the RFID tag is scanned and is a valid access, then this message is displayed. It takes input a 4 digit code.

If the entered code is right, then this message is displayed and the relay is put on to actuate the solenoid.

Now if the door is open, this message is displayed and remains as it until it is closed.

When the door is closed, this message is displayed after de-actuating the solenoid and the system returns to initial state.
Else if the entered passcode is not valid, this message is displayed.

If the user wants to change the passcode, the CAH procedure is to be performed which sends the OTP in a message to enter it here.

If the entered OTP is wrong, this message is displayed and the system returns to initial state without modifications to any of the credentials.

If wrong passcode trial limit exceeds 2 or if there is a security breach, this message is displayed and there is intimation about the same to the user.

If all entries/exits through the house are to be restricted, the user performs CAH to activate the mode and this message is displayed when done.

6. Applications

- Flats/Residential Apartments.
- Locker Safes.
- Bank locker rooms and offices where the access is restricted.
- Industrial equipment controlling.

7. Future Scope

The future scope of this is highly rated because of its simplicity in working and economic in cost for setting up the device. In order to avoid the burglar activities when we go out by locking our home this will be necessary and its activation process is also quite simple, just we need to enable the system and we will receive an SMS if any unauthorized person tries to enter/break through and we can take the necessary steps. Hence according to our view in near future each home should have this security device installed.

The modern wireless communication technology which includes Bluetooth, Wi-Fi, WiMax, ZigBee are offering inspiring appearance and capability that once were not being able in use efficiently on cross-platforms 15 years ago. So by making use of any of these technologies, further developments in the security aspects can be made there by reducing the cost of the product, increasing the accuracy and working of the product. A mobile phone application can be designed which gets connected to the system once if present in range and this can be used as a kind of authentication model either automatically triggering the system peripherals or entering the required credentials in the applications which communicate with the system through any of the above mentioned technologies. Since the mobile phones are being used by millions of people worldwide, this project can be implemented by each and every individual in near future.

8. Conclusion

The sales of the product depend upon the production cost and its accuracy in working. If the sale increases then the revenue of the organization increases, hence the profit yields. So the revenue of the organization increases that meets the business requirements. The draft plan depends upon the annual budget of the organization. As per our view the draft plan we have planned will lead the organization into profits. Capital cost plays a key role in the success of the organization. So planning of a cash flow is very important. If the cash flow fails then it leads to loss of the organization. We recommend using this technique as it uses the latest mobile technology, cost effective and easy to use the device.
9. References