AN EFFICIENT MULTISTAGE SECURITY SYSTEM FOR USER AUTHENTICATION

PRERNA MEDHI
Dept. of Electronics & Communication Engineering
Amity University, Noida
E-mail: medhiprerna@gmail.com

Abstract—This paper proposes a multilayer security system which can be used in Home, Bank Lockers etc. to prevent thefts. Multilayer security provided by the combination of three securities which is based on the sequence of (I) RFID, (II) password and (III) Biometric consecutively. All the three modules are controlled through a microcontroller. The Proposed system is more efficient and reliable due to multistage security and may not be breached with the combination of all three stages.

Index Terms—GSM, Microcontroller, RFID, Security system

I. INTRODUCTION

Now day’s security of assets is the main concern for any person. This paper aims at providing a reliable security system. It provides a way for identifying authorized and unauthorized persons, by using RFID, keypad password and fingerprint technology. The main contribution of this paper is to provide a multistage security so that unknown person will not be able to breach the security.

In Conventional security system, there is either an RFID system or a password based system or a biometric based system (which could either be a fingerprint based system, retina scanner or voice recognition system), there is a greater chance to break such one stage security system. To improve such systems, a multistage security system consisting of microcontroller based matrix keypad & GSM network in addition to RFID technology and fingerprint module can be used. In this, verification will also be involved without which the system doesn’t provide access and a notification is sent to the authorized person.

Related works include development of a digital security system containing door lock system using passive RFID [8], RFID based security systems and microcontroller based reprogrammable digital door lock security system by using keypad & GSM/CDMA technology [10].

The microcontroller based digital door lock security system is an access controlled system in which only authorized persons can access restricted areas. The proposed security system consists of the following three stages-

Stage 1: RFID module consists of RFID tag and RFID reader. When the user punches his card (containing the tag), the 12 byte serial number of the tag is read by the RFID reader and is sent to the microcontroller. The microcontroller then compares the data with the existing data stored in the EEPROM memory(internal memory of the microcontroller). If the data matches with the existing data in the memory, it means the person is authorized and the user enters the second stage of the security system. If the data is not matched then the user will not be permitted to enter the premises. The buzzer starts ringing to provide an alarm indicating the presence of an unauthorized person and a message is sent to the authorized person via GSM module.

Stage 2: The second stage includes the entering of password via the keypad by the user. If the password is correct then he will reach the third stage of the security system. But, if the password is wrong then access is denied and the authorized person is notified through the GSM module.

Stage 3: The user reaches the third stage if his RFID tag and password is correct. In the third stage he has to punch onto the fingerprint module. If the fingerprint of the person matches with the existing finger prints stored in the memory of the fingerprint module, then, the lock opens and the user gets access else it is denied.

Fig (a) : Block Diagram

II. WORKING

Figure (c) shows the complete schematic diagram of the circuit. An RFID system consists of a reader device and a transponder (tag). A transponder or tag has a unique serial number which is identified by the reader
and is sent to microcontroller for checking. If an unauthorized person tries to enter then a notification will be sent to the authorized person by the GSM module which is connected with the system. The user then has to enter his password via the keypad.

The password is stored in EEPROM so that only registered user can reset it when desired. A keypad is used for inputting the password manually, which is a matrix of 4*4 elements. When one enters the code in the matrix keypad, microcontroller verifies the code. The code can be a combination of digits 0-9, four letters a,b,c,d and special characters * and #. If the user enters the wrong code, the buzzer connected will give an alarm and he will not be able to move on to the third stage.

The third stage is the fingerprint verification stage. This is done in two steps, the first step is fingerprint enrolment and the second is fingerprint matching. During enrolment, the user has to place his finger twice. The module will process the fingerprint images and will create a template and store it in a memory slot. In the second stage of matching, 1:N matching is done in which the user enters the fingerprint onto the optical sensor, a template is generated and is compared with all the templates stored in the memory slots. After matching the result is displayed on the 16*2 LCD screen as success or error. If the result is success, the person gets entry.

GSM module can be used as a receiver, which sends messages to the authorized person to notify him that the an entry is being made. AT commands have been used for GSM module[3]. For this a desired mobile number is used in the system. In this, without verification it doesn’t allow the door to be opened and a notification is sent to the authorized person.

III. RESULTS

Figure (d) shows complete system design of the circuit. The proteus simulation of the circuit for showing the virtual hardware prototype working has been shown in figure 5 and figure 6 shows the actual hardware model of the designed system.

After verification of RFID tag and password, the microcontroller proceeds to the next step i.e to store the fingerprint. In this step, LCD displays “Place Finger”. We have to place finger on the fingerprint module so that the module can verify the input fingerprint with the stored one. Figure 5 figure illustrates the model. We have used a DVD driver to show the door movement. When the RFID tag is matched, password entered is correct and fingerprint is matched, the door opens and access is granted.

Comparison of the existing security systems and our proposed security system is shown in Table 1. Table 2 shows the comparison of the time required to hack the system with different combinations of the security provided and the probability of breaching them.
CONCLUSION

This paper provides a solution for highly secured and reliable door lock system. The security system based on RFID tag, matrix keypad, finger print and GSM technology has been successfully designed and implemented. This system can be used in places where high security is required. This security system can be further economized.
An Efficient Multistage Security System For User Authentication

Table 1: Comparison of existing and proposed security system.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>RFID Based</th>
<th>Digital Password Based</th>
<th>RFID + Digital Password Based</th>
<th>Biometric Based</th>
<th>RFID + Password + Biometric Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Breaching Time Comparison

<table>
<thead>
<tr>
<th>Security System</th>
<th>Approx Time Required to Hack the System</th>
<th>Security Breaching</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID</td>
<td>Few minutes[1][1]</td>
<td>Could be breached</td>
</tr>
<tr>
<td>Password containing digits 0-9</td>
<td>5sec</td>
<td>Could be breached</td>
</tr>
<tr>
<td>Password containing letters a-d</td>
<td>20sec</td>
<td>Could be breached</td>
</tr>
<tr>
<td>Password containing digits 0-9</td>
<td>Within 1 minute</td>
<td>Could be breached</td>
</tr>
<tr>
<td>Password containing letters a-d</td>
<td>More than 1 minute</td>
<td>Could be breached</td>
</tr>
<tr>
<td>Biometric</td>
<td>Probability of hacking is very very</td>
<td>Can be breached using high resolution (2400 dpi)</td>
</tr>
<tr>
<td></td>
<td>less[2][2]</td>
<td>photographs of finger print. Chances of breaching this is very slim.</td>
</tr>
</tbody>
</table>

REFERENCES