ISSN:0975-9646

Sai Kumar Nadakudhiti et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2885-2888

Analysis and Automation of Security Management System for Remote Terminals Based on Advanced Finger Print Reorganization Algorithm

Sai Kumar Nadakudhiti, A KabirDas
Department of ECE
Sasi Institute of Technology and Science, Tadepalligudem

Abstract: Security Management at the industries or remote terminals like ATM centers is very essential. Security can be provided with man power but in practice this traditional methods are not up to the demand. As increasing number of people needs, number of ATMs increasing and there is no enough man power to monitor each and every terminal with this traditional way. So In this paper we analyzed the present day security policy and need of enhanced security management system for industries and remote terminals. With this analysis we automated the security management system. This system can perform critical task for the security people. Checking for the thefts, power failure, temperature range etc. To improve the security level by implantation of wireless embedded technology will resolve this problem. By dropping the manual power, at the site locations, and by improving the security level with the help of GSM based wireless technology which consist of transmitter (GSM modem) at the site location and receiver is the GSM mobile. Information transmitted by the GSM modem at the home location will be sent to the individual person's mobile as a text message. The security people will take appropriate action according to the problem. For this we are used LPC2148 (ARM7) based microcontroller, which is the current dominant microcontroller in mobile based products.
***Keywords*: ATM; security management; keil;**

1. INTRODUCTION:

With rapid development of the economic requirements every nation is depending on ATMs for basic money transactions. Banks are showing much more interest to provide good service to their customers by arranging many ATMs at distant places. along with the increase with the number of ATMs , money robberies and ATM misuses are also increasing. Banks are failing to provide sufficient security at ATMs, even though in some cases with a proper security thefts are happing because of human power inefficiency. So with this analysis we designed a security management system with ARM Processor which automates security process and helps to restrict the misuse of bank applications.

Banking system intrusion shows the vulnerabilities that exists in financial institution, that have been used by those illegal and unauthorized individuals or groups to intrude an area with secure environment. The violation of system security is all about the money, challenges to intercept data, challenges with acquaintance, data breach, and poor authentication and authorization. With all of the weaknesses occur, well, it is a treat for anybody with high experience and knowledge in information systems to get into the system, using, stealing, modifying and even deleting information in the system.

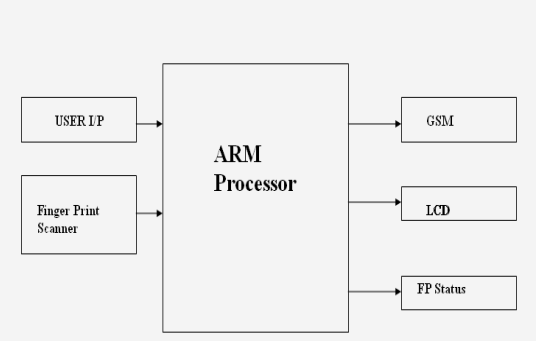
ARM is dominant processor in the mobile industry and more than 80% of embedded devices use ARM as a processor. Since we need communication in this project, this is achieved by using GSM which is interfaced with the ARM processor.

2. HARDWARE DESIGN:

The ARM7 (LPC 2148) is used as the core of entire hardware. Furthermore, the modules of LCD, keyboard, alarm, fingerprint recognition are connected with the main chip (LPC2148).The SRAM and FLASH are also embedded in the

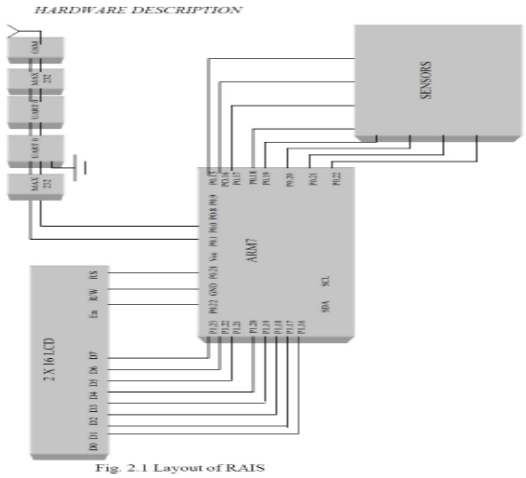
The other major hardware building blocks are

- LCD module: The JDH162A is used in this module as a LCD controller; It displays the information of the system.
- keypad module: It is required to input the user information.
- sms module: sim300 sms module is based on GSM technology used here to send SMS to Bank, Owner or police
- SRAM and FLASH: The 32-bit 512 MB of FLASH chip and the 32-bit 40 kB of SRAM are connected with the main chip. Their functionalities are storing the execution program and the information of fingerprint and the algorithm. There are used as a Data Base for example.
- Fingerprint recognition component: KY-M8I is a sensor dedicatedly designed for the Finger print recognition.



Fig(i) Conceptual Diagram

The conceptual diagram is shown in the below figure(i). It consists of all hardware modules connected with the core processor. The individual connections to the core processor is explained below. When user inputs some data through keyboard, It accepts and this data is compared to the DB provided. Hence for this purpose we used internal memory as the database. A finger print scanner is connected as input divide to the processor to get user finger print data. The comparison of the finger print data with the data base is done according to the user input pin number. If user fails to enter the input password correctly there will be no more checking of the fingerprints. Once user enters the correct password then only system goes forward to check the finger prints. This comparison of the finger prints done by specific algorithm to get more accuracy. A model of authenticating based on the finger print technology is described in the fig(iii) below. It compares the finger print according to the light intensities.



Fig(ii) Hardware Model Implementation diagram

32-bit ARM processor is the contemporary general purpose microprocessor in the embedded market used in industrial level applications. GSM, as we know, is the most widely used mobile technology. Using a simple Subscriber Identity Module (SIM), it has taken the world of mobile communication to new heights. It is based on a simple architecture. Even with the introduction of new technologies like CDMA, GSM has stood its strength due to its efficiency and simplicity.

We have used ARM7TDMI processor in our model due to its advanced features described below. ARM7 consists of a number of peripherals interfaced to it. We use only the keypad matrix, LCD display, UARTS, GPIO and I2C protocol. ARM7 processor is a link between GPS and GSM modules for communication. The description of ARM7 is discussed in further sections. 3.1 software snippets

- 16/32-bit ARM7TDMI-S microcontroller is a 64 or 144 pin package.
- 16 kB on-chip Static RAM.
- 128/256 kB on-chip Flash Program Memory. 128-bit wide interface/accelerator enables high speed 60 MHz operation.
- In-System Programming (ISP) and In-Application
- Programming (IAP) via on-chip boot-loader software. Flash programming takes 1 ms per 512 byte line. Single sector or full chip erase takes 400 ms.
- B Two 32-bit timers (with 4 capture and 4 compare channels), PWM unit (6 outputs), Real Time Clock and Watchdog.
- Multiple serial interfaces including two UARTs (16C550), Fast I2C (400 kbits/s) and two SPIs
- 60 MHz maximum CPU clock available from programmable on-chip Phase-Locked Loop.
- On-chip crystal oscillator with an operating range of 1MHz to 30 MHz.
- Two low power modes, Idle and Power-down.
- Processor wake-up from Power-down mode via external interrupt.

3. SOFTWARE SECTION:

The design of software includes the implementation of algorithm,. This process consists of understanding of the present situation and automating the security management system. We divided this design into three modules as Main flow, Fingerprint part and SMS part. He combined algorithm is shown bin the below fig(iii).This system of software is implemented by the steps as follows: first of all, the OS and the File system are loaded into the main chip. The next, the system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. first entering into the ATM terminal fingerprint is required If fingerprint is correct, we will enter into the ATM terminal Before using ATM terminal, the password and fingerprint is required. First need to enter owner's password, if password is successful then the system is required the owner's fingerprint. If all the recognition is right, the system would enter into the waiting status. In addition, the number of times that recognition of fingerprint and password are restricted to 3. If more than 3 times, the system will send message to the police through police network, send message to the owner and send message to relevant staff. Then locked the owner's credit card. The overall flow chart of software is shown in figure 2.

In the process of inputting fingerprint, the KY-M8I which is a linear sensor that captures fingerprint images by sweeping the finger over the sensing area, will used for acquiring the image of fingerprint. This product embeds true hardware based 8-way navigation and click functions. The fingerprint information will be temporarily stored in SRAM and upload to the remote finger data to compare

through bank network. The result of process will be controlled by main chip(LPC2148). The initializing process means that set the hardware and software and then start the multiple mission module, each module will be started according to the priority processes. At first, initialize the system clock, and execute the codes of open interrupt and the open interrupt task.

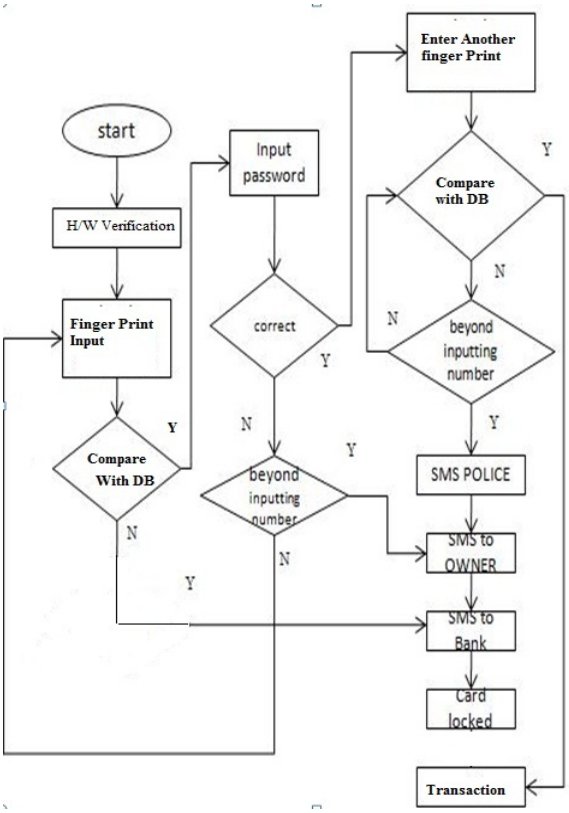
The below code snippet shows the serial interfacing of the different blocks to the ARM processor.

3.1 Serial data reading

```
unsigned char recvmsg()// serial reading
{  unsigned char x;
 while((U1LSR&0X01)!=0X01); //checking for character form com1
   x=U1RBR; //store the character to variable x
 return x;}
```

So this program enabled the data sending through the serial communication. Before sending the data serial port we need to enable serial port. For this a communication protocol must be defined . this is shown as below.

```
//enable serialport1(serialport1,open())
        buf(0) = "!"//declare as char
      SerialPort1.Write(buf, 0, buf.Length)
      tx = TextBox1.Text//where we enter the text
      buf = tx.ToCharArray()
      SerialPort1.Write(buf, 0, buf.Length)
```



Fig(iii) Algorithm for Automation of Security management.

With this technique without human interception security monitoring is done and when any misuse of remote terminals done, immediately security alert created automatically. The LCD display connected here is to display the information reg. the current operation. And is useful to display the password which has to entered by the user for authentication in first step.

The interfacing of LCD with the ARM processor is explained through the below code snippet.

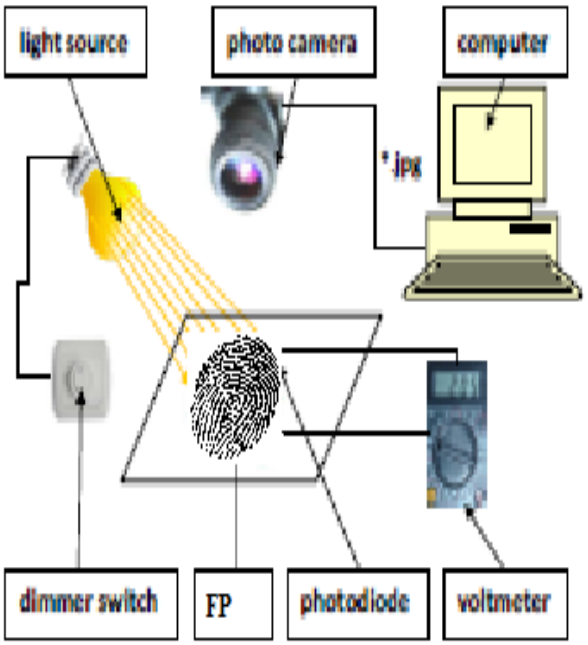
3.2 LCDs interfacing:

```
void lcdinit1(unsigned int x)// to send commands
{                IOCLR0=0x00FFFFFF;   IOSET0=x;
//IOSET0=IOSET0<<16;
  IOCLR0=0x00004000;  //RS  // IOSET0=x;
  IOSET0=0x00008000;  //EN
  delay();   IOCLR0=0x00008000;}  //EN
 void lcddata1(unsigned char y)// to send data
{       IOCLR0=0x00FFFFFF;       IOSET0=y;       //
IOSET0=IOSET0<<16;
  IOSET0=0x00004000;  //IOSET0=y;
  IOSET0=0x00008000;   delay();
  IOCLR0=0x00008000;}
```

Here we have use 2x16 LCD to interface with the ARM processor. This technique involves the initialization of LCD and sending the data by using 8 data lines.

Finger Print Recognition Technique:

Here is the model for recognition of finger print based on the fixed light source technique. When user enters his finger print, we can expect different atmospheric conditions. The comparison of the finger print is done with the already stored image. Suppose when user enters his finger print during night time, the light intensity may differs. This may lead to incorrect comparison and a correct user authentication may fail. So to avoid these types of situations we need to have a advanced developed design for this finger print reorganization system. So with deification of this problem, we can find that source of light is the cause of the intensity. So by providing a fixed source of light and taking inputs from the source will reduce the problems to a great extend. So here we have used a common bulb as a reference light source. When finger print scanned with this specific light source, it will be comported with the already available user's finger print with the system database. The reference finger print is also taken with the same light source to avoid the intensity variations. To extend this technique we have used a Database (PC in the figure(iv)) which consists of all users essential references. When specific source of light falls on the finger print then it reflects, and this reflection of the light is converted into voltage using photo diode, and this voltage is compared with the Voltmeter. The system database having the reference values for each fingerprints, this voltage level compared with the reference voltages. So based on this comparison results, we will get the accurate (+5% tolerance) results. So this process eases the authentication.



Fig(iv) FP reorganization using fixed light source

4. ADVANTAGES:

1) System Robustness due to strong security authentication procedure.
2) A new level of Finger print recognition technique
3) Easy to implement at remote terminals
4) Effective management of database.
5) Automation Security management causes reduction in manpower and avoids human inefficiency.

5. APPLICATIONS:

1) At Industry to monitor different areas in sites.
2) Remote monitoring of fields.
3) Useful to implement the authentication at "face reorganization" applications.
4) Easy maintaining of all remote terminals which connected through a network.
5) Adaptable to estimate " Adharcards " genuinely, which were introduced by Govt. Of India recently.

CONCLUSION:

In this project we have automated the security management system from ground to elevated level, which meets the industry needs. In this we have also proposed a procedure for better finger print recognition technique for dual security purpose. The further work of this project includes implementation of authentication system with the face reorganization which is very demanding application in emerging economical country like India.

ACKNOWLEDGMENTS

We are very much thankful to Mr. T J V SubrahamanyeswaraRao, Associate Professor, Department of ECE, Sasai Institute of Technology Tadepalligudem for his continuous encouragement and support

REFERENCES

[1] ATM terminal design is based on fingerprint recognition Yun Yang, Jia Mi ,Shaanxi University of Science & Technology Xi' an, China
[2] ESaatci, V Tavsanogh. Fingerprint image enhancement using CNN gabor-Cpe filter[C]. Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications 2002: 377-382.
[3] Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37: 543-553.
[4]Individual Plant Recognition Using theRGB Color Model Mihaela Tilneac, Valer Dolga *Mechatronics Departament, Mechanical Engineering Faculty, Politehnica University of Timisoara Blv.Mihai Viteazu 1, Timisoara, Romania*
[5] Illinois Department of Financial & Professional Regulation
[6] Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation[J]. IEEE Transactions on Pattern Analysis and Machine intelligence. 1998,20(8): 777-789.
[7]Real-Time Automization Of Agricultural Environment for Social Modernization of Indian Agricultural System by Mahesh M. Galgalikar Dept of Electronics and Telecommunication Jawaharlal Darda Institute Of Engineering & technology, Yavatmal , India
[8]Research on Compund display connections to ARM based Processors by Deepak Chamarthi and T J V S subrahamaneswaraRao, International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 pp [3194-3201]
[9] Smits G FJordaan E M.Improved SVMRegression using Mixtures of Kernels[A]. Proceedings of the 2002 International Joint ConferenceonNeural Networks[C]. Hawaii: IEEE. 2002. 2785-2.
[10] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. Image enhancement and minutiae matching in fingerprint verification. Pattern Recognition Letters 24 (2003)1349-1360.