Journal of Engineering Science and Technology
Vol. 13, No. 7 (2018) 2065 - 2083
© School of Engineering, Taylor's University

ENHANCEMENT OF SMARTNESS AND SECURITY IN ATM BY GLOBAL SYSTEM FOR MOBILE COMMUNICATION

S. GANESHKUMARAN, C. R. BALAMURUGAN*

Sri Manakula Vinayagar Engineering College, Coimbatore, India
Karpagam College of Engineering, Coimbatore, India
*Corresponding Author: crbalain2010@gmail.com

Abstract

An automated or Automatic Teller Machine (ATM), also known as the automated banking machine, is a computerized telecommunicating device. Nowadays more people using ATM to withdrawing the money. Therefore, security is more important in ATM centre. This work is to prevent users attacked by strangers during withdraw the money so innovative ideas proposed to improve the security. In this model metal detectors fixed at the doors to detect metals such as a knife, gun, etc. and use of Infrared Ray (IR) sensor to allow one person at a time in ATM centre. If the user is not trained about ATM means at that time security help that person through biometric fingerprint. In this model, the work is also implemented two password systems at the time of user hijacked by a stranger. Finally, the work is implemented, people have to know about ATM working condition without going to the ATM centre. Global System for Mobile communication (GSM) interfaced with an ATM network that provides all information about ATM working condition to users mobile.

Keywords: ATM, GSM, IR, Phone, Real-time.

1. Introduction

The first modern ATMs came into use in December 1972 in the UK; the IBM 2984 was designed at the request of Lloyds Bank. The 2984 CIT (Cash Issuing Terminal) was the first true Cashpoint, similar in function to today's machines; Cashpoint is still a registered trademark of Lloyds TSB in the UK. All were online and issued a variable amount, which was immediately deducted from the account. A small number of 2984s were supplied to a US bank. A couple of well-known historical models of ATMs include the IBM 3624 and 473x series, Diebold 10xx and TABS 9000 series, NCR 1780 and earlier NCR 770 series.

ATM stands for Automatic Teller Machine. It is an electronic banking outlet, which allows customers [1] to complete basic transactions without the aid of a branch representation or tellers. It was invented by John Shepherd-Barron Donald Wetzel.ATM is used for users to withdraw the amount at any time and any place without going to the bank. There are two types of ATM they are basic ATM and complex ATM. Basic ATM only allows the customer to withdraw money and receive a report of the account's balance. Nevertheless, complex ATM will allow deposits credit card payments and report of the account's balance [2]. To access the complex ATM only member of the bank are allowed.

ATM card is a plastic card that contains a unique card number and security information such as expiration date. It has a 4-digit PIN (Personal Identification Number) number for authentication. ATM card is inserted into the ATM machine enter the PIN number, machine identifies the customer and completes the transaction. CPU (Central Processing Unit), magnetic card, crypto-processor, a display device, function key buttons, record printer, and vault these devices used in ATM centre. This work can use ATM for train tickets, movie tickets, shopping mall, hospital, school. Most ATMs are connected to an interbank network enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account. This is a convenience, especially for people who are travelling: it is possible to make withdrawals in places where one's bank has no branches, and even to withdraw local currency in a foreign country, often at a better exchange rate than would be available by changing cash. ATMs rely on Authorization of a Transaction by the card issuer or other authorizing institution via the communications network.

Today, security is very much essential for all kind of activities. Illegal activities are happening in every place today. Therefore, government and corporate sections are concentrating mainly on the security levels with their every invention. This will bring privacy all over the world. Therefore, in a thought of bringing privacy through security level, this model has been developed. This ATM security system mainly uses three divisions, which are IR sensor, metal detector and a biometric sensor. Each unit is having its own major role over the model. IR sensor is used to allow one person at a time. It makes transaction safer. Metal detector fixed at the door to detect the metals such as a knife, gun, etc. If the user is not educated or unaware about ATM means at that time the proposed work have given authority to security person only to help the customers using a biometric fingerprint [3]. People have to know about ATM working condition without going to the ATM centre. Global System for Mobile communication (GSM) interfaced with an ATM network that provides all information about ATM working condition to users' mobile [4].

2. Existing System

The following topics are coming under existing systems and Table 1 gives the existing technologies and drawbacks.

Table 1. Existing technologies and drawbacks.

Existing technologies	
List of Technologies	• Encryption Technology • OTP Technology • Fingerprint Recognition System • Iris Recognition System • Finger Vein Recognition System
Drawbacks	Problems in existing technologies have less security. An unauthorized person accesses the account very easily, avoid that access biometric authentication are used. However, the user after withdrawing the amount, criminals enter the ATM attack the user and take the money. Another problem is not customer satisfied with working in ATM. Because user goes to ATM centre insert ATM card and enter PIN number then only know ATM is working or not. So user waste more time and traffic jam also in front of the ATM centre.

2.1. Encryption technology

ATM transactions are used in DES (Data Encryption Standard) algorithm for more security. Because there are also many "Phantom withdrawals" from ATM'S. Phantom withdrawals mean criminals used fake machines, or fake keypads or card readers to access ATM machines. These fake machines are used to record the customer's PIN numbers and account details. Therefore, Ross Anderson implementing the encryption technology the original information is converted into the coded format. This coded information only understand by the receiver (ATM machine) not by criminals.DES algorithm used a 56-bit key to encrypt the original data. Therefore, it is more secure.

2.2. OTP technology

To secure the bank transactions from unauthorized person's this work use two-factor authentications. Two-factor authentications combine the use of PIN and One Time Password (OTP).

In two-factor authentication, the customer enters the card and PIN if the PIN is validated the bank computer generates and sends an OTP to customer's mobile via SMS. The customer enters the received OTP, if it is valid the customer is authenticated and the transaction is permitted. In this method GSM (Global System for Mobile Communication), wireless technology is used [5, 6]. Figure 1 shows the OTP technology.

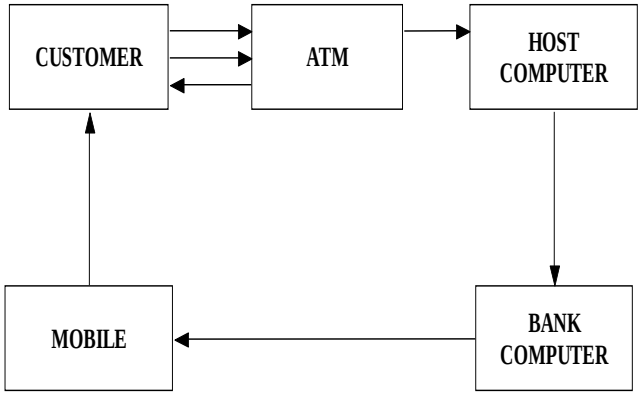

Fig. 1. OTP technology.

2.3. Fingerprint recognition system

Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Figure 2 shows the fingerprint scanning. Among the most remarkable strengths of fingerprint recognition, it can mention the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low- cost small size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC (Personal Computer) logon, etc.
- The use of easy-to-use, ergonomic devices, not requiring complex user-system interaction.
- The customer can save the money if the card is taken by the third party they cannot make the transaction without biometric process.

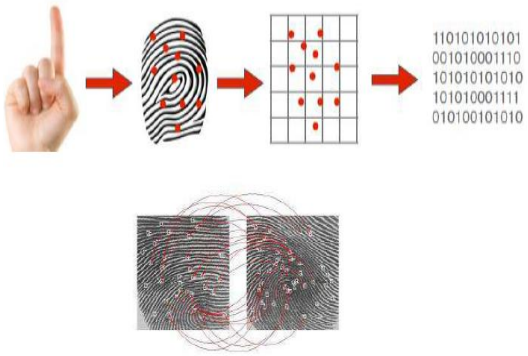

Fig. 2. Finger print scanning.

On the other hand, a number of weaknesses may influence the effectiveness of fingerprint recognition in certain cases its association with forensic or criminal applications.

2.4. IRIS recognition system

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the iris of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. Iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structure of the iris. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single core) CPU, and with infinitesimally small false match rates. This existing system is not perfectly reliable and secure. For example, fingerprint and palm print are usually frayed. Fingerprints, iris and face recognition are susceptible to spoofing attacks i.e., biometric identifiers can be copied and used to create artefacts that can deceive many currently available biometric devices.

2.5. Finger vein recognition system

The finger-vein is a promising biometric pattern for personal identification in terms of its security and convenience. Compared with other biometric traits, the finger vein has the following advantages: (1) the vein is hidden inside the body and is mostly invisible to human eyes, so it is difficult to forge or steal. (2) The non-invasive and contactless capture of finger-veins ensures both convenience and hygiene for the user and is thus more acceptable. The finger-vein pattern can only be taken from a live body. Finger-vein recognition algorithm contains two stages: the enrolment stage and the verification stage. Figure 3 displays the finger vein recognition system. Both stages start with finger-vein image pre-processing, which includes detection of the ROI (region of interest) image segmentation, alignment and enhancement.

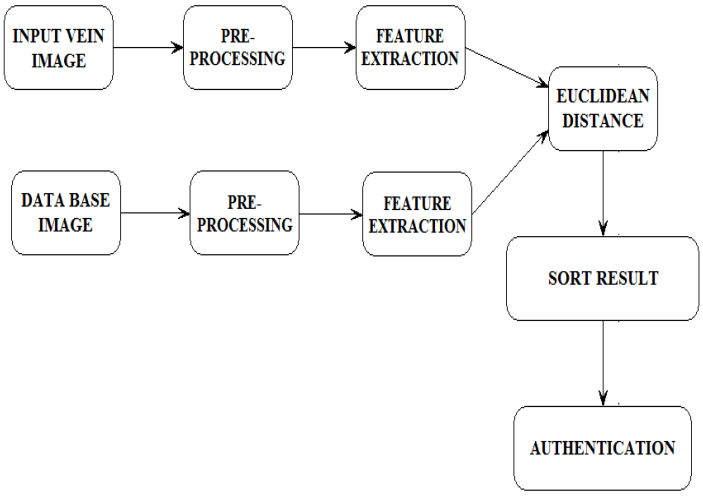

Fig. 3. Finger vein recognition system.

2.6. Problems with the existing system

ATM networks are vulnerable to many kinds of attacks and very often, the possibilities are underestimated. Nowadays the problem of using ATM centre is being drastically increased due to the strangers. Due to the modernization of the Indian culture, the number of persons using the ATM for the withdrawal of money and exchange of cash is being increased. Most of the companies pay salaries to the employees through the banking. Therefore, the security level of the ATM centres is to be improved. The problem in older ATM centre has less security. An unauthorized person accesses the account very easily, avoid that access biometric authentication are used. However, the user after withdrawing the amount, criminals enter the ATM attack the user and take the money. Now-a day's most of the companies, colleges, industries pay salary to the employee through ATM. Therefore, the security level of the ATM centre is to be improved. Another problem is not customer satisfied with working in ATM. Because user goes to ATM centre insert ATM card and enter PIN number then only know ATM is working or not [7, 8]. Therefore, the user waste more time and traffic jam also in front of the ATM centre.

3. Proposed system

The proposed system improves the security when strangers enter into the ATM [9, 10]. It has four methods, which are shown below in Table 2.

Table 2. Proposed idea for implementation for different condition.

Sl.no	Conditions	Actions to be followed	Advantages
1	More than one person or no person in ATM (if N>1 and N= 0) N- No. of Persons inside the ATM	ATM monitor and keyboard will be inactive	If more than one person allowed the keyboard and monitor are inactive. To improve the security to users.
2	Metal Detector	To scan the weapons (knife, gun, etc.) carried by the strangers if found ATM monitor and keyboard will be inactive	The metal detector detects metals. This work prevent the criminal's damage ATM machine and prevent users attacked by strangers
3	If the person not having knowledge about ATM	Proposed work gave authority to the security personnel only. He can access the ATM by using biometric system	Security person helps uneducated peoples using a biometric fingerprint [11]. Suppose any theft happens it's easy to find out through security person.
4	If user hijacked by the strangers, use of two password option.	1. One for transaction purpose only 2. Another for creating an abnormal account to withdraw a minimum amount from the ATM to avoid the attention of the stranger	When user hijacked by criminals they use two password system to save money and confuse the criminals.
5	GSM	Enquiries about ATM with the help of GSM [12]	About ATM condition

3.1. Metal detector

The stranger is carrying the weapon to attack the person using the ATM to get money from him/her when need help. However, it is not possible to get help instantly. So this work fixes metal detector at the door to detect harmful weapons such as a knife, gun, etc. The metal detector detects the only adequate size of metals. When the metal detector detects metals, the keyboard and monitor of the ATM are inactive. If any persons enter ATM centre with metals this metal detector detects that metals and makes the keyboard and monitor inactive. The interfacing process is carried out with the circuit shown below. It consists of the metal detector fixed with the door, which is being interfaced, with the computer monitor and the keyboard.

3.2. IR sensor

A sensor is attached to the door to count the number of persons entering the ATM at a time. If the number of persons, entering the ATM is more than one the monitor and keyboard become inactive and lights will be off. When card inserted into the ATM machine the door will be automatically closed and finishing all his transaction the door automatically opens. The uneducated person will get help from the security. Security enters into the ATM by using biometric fingerprint that time only two persons allowed. Otherwise, only one person allowed in ATM centre that time the keyboard, monitor, and one light will be on. It is also for the power saving purpose and security. The transaction completes the door automatically opens. The uneducated person will get help from the security. Security enters into the ATM by using biometric fingerprint that time only two persons allowed. Otherwise, only one person allowed in ATM centre that time the keyboard, monitor, and one light will be on. It is also for the power saving purpose and security.

3.3. Biometric system

In addition to all these securities, it is possible to use the biometric sensor in addition to the metal detector circuit to increase the safety level in the ATM. If the user is not well educated or not aware of ATM means at that time, proposed work has given authority to the security person only to help the customer. His biometric is fed by a bank authority [13, 14].

3.4. Two password system

Until now our government providing a single password for the transaction, the proposed work had an alternate idea, by issuing two passwords for two different purposes. One for transaction purpose only and another password is used in emergency time. For example, the user is hijacked by the stranger and asked to take money from the ATM, here in this situation user as to use the second password, after entering the password money 5000 in original account transferred to a second abnormal account in M>5000 conditions (M-Money in user account). In this second up to 24 hours, this account should be accessed for security. After 24 hours, using the abnormal (second) password again transferred 5000 to abnormal account only emergency time. Suppose a user has less than 5000 that time access original account in M<5000 conditions. Otherwise, the proposed work use the first password for normal transaction. .

3.5. GSM

In this busy world, people enter the ATM centre then only they can be able to know about ATM working condition. To avoid this situation a novel idea is proposed, the ATM is interfaced with GSM [15]. Steps to improve the idea first all ATM servers should connect in one centralized server. Figure 4 displays the flow chart for GSM. Assign GSM number to the server and it collects all ATM working condition and distance information. When a user calls that GSM number that sends first own bank ATM information, suppose it is not working then the server sends nearest ATM information [16].

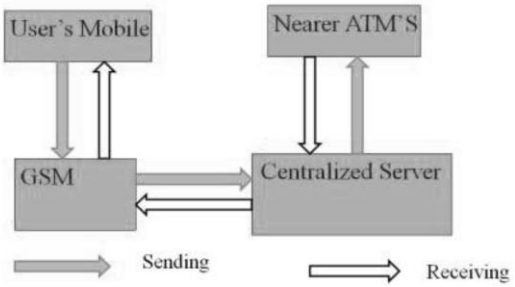

Fig. 4. Flow chart for GSM.

4. Hardware description

4.1. Hardware specifications

Table 3 shows the hardware specifications of the proposed setup. The various components used for the development of hardware are listed in Table 3. The hardware setup consists of Metal detector, IR sensor, Biometric system, GSM module, RF transmitter, RF receiver, DC motor, Relay driver, step down transformer, Bridge circuit for conversion of AC supply to DC supply, Filter circuit to eliminate harmonics, voltage regulator to give a constant voltage, encoder, decoder for exchange of information, keyboard, liquid crystal display, buzzer and subscriber identity module.

Table 3. Hardware specifications of the proposed setup.

Sl. No.	Hardware Components	Specifications
1.	Metal detector	-
2.	IR sensor	LM358 IC
3.	Biometric system	
4.	GSM module	
5.	RF transmitter pic1650	Max232 (434 MHz)
6.	RF receiver pic1650	Max232 (434 MHz)
7.	DC motor	12 V
8.	Relay driver	
9.	Step-down transformer	230 V/ 5 V/12 V- 50 Hz
10.	Bridge rectifier unit	4*IN4007
11.	Filter	-
12.	Voltage regulator	IC7805
13.	Encoder	HT12E
14.	Decoder	HT12D
15.	Keyboard	-
16.	Liquid crystal display	14 Pin
17.	Buzzer	-
18.	Subscriber identity module	-

4.2. Hardware block diagram for the transmitter

PIC act as ATM. IR sensor is used to allow one person at a time [17]. When it allows more than one person, the keypad and monitor are inactive. RFID reader reads the tag card (ATM card) the door is automatically closed.

For this purpose, the DC motor rotates forward direction. When the transaction is completed, the door is automatically open. For this purpose, the DC motor rotates reverse direction. DC motor operates at 12 V but PIC operates 5 V, so it is interfaced through relay driver. Relay driver provides external power supply. Max 232 is used for communication, it transmits and receives information. It converts voltage into TTL level voltage. Switch act as a biometric device, when the switch is pressed IR sensor allows two persons to help uneducated persons. When the metal sensor detects metals on the keypad and monitor are inactive. The encoder encodes the information and sends to the RF transmitter. Figure 5 shows the block diagram for a security system for ATM using a PIC controller. Fig. A-1 (*Appendix A*) displays the block diagram of PIC 16F877A controller.

4.3. Hardware block diagram for the receiver

PIC acts as a centralized server. More ATM servers connected to that server. GSM interfaced with PIC controller through max232 and assign a number to that. RF receiver receives the ATM working condition information from the transmitter circuit [18, 19]. The decoder decodes that information and stores that information to the PIC. Figure 6 displays the block diagram for GSM interfaced ATM. User calls that GSM number and receives ATM working condition information with also distance information [20].

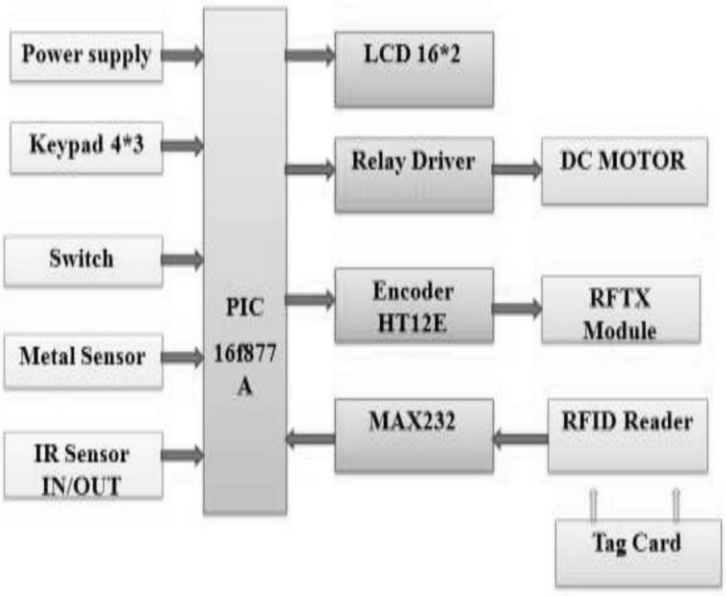

Fig. 5. Block diagram for security system for ATM.

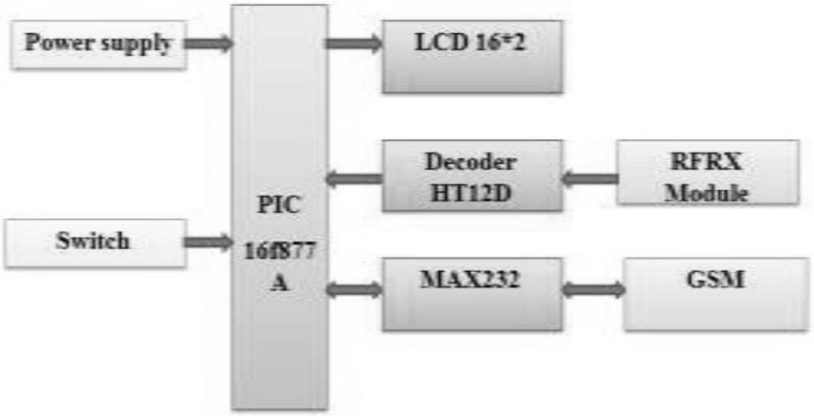

Fig. 6. Block diagram for GSM interfaced ATM.

The hardware circuit diagram designed using proteus software. It is used to design and implement the circuit. Some hardware devices and IC chips are available in proteus software. Output also checked using this software. PIC has 40 pins each pin provides some functions. Metal and IR sensor o/p pin connected to the PIC. Row and column pins of the keyboard are connected to port B pins. RS(Register Select, R/W(Read/Write) pins connected to connected to corresponding RD and WR pins. Enable pin is the data read from and write to PIC memory. RFID RX and TX pins are connected to PIC through max232. Encoder 4 data pins connected to PIC and o/p pin is connected to RF TX pin. Figures 7 and 8 show the transmitter and receiver circuits using proteus software.

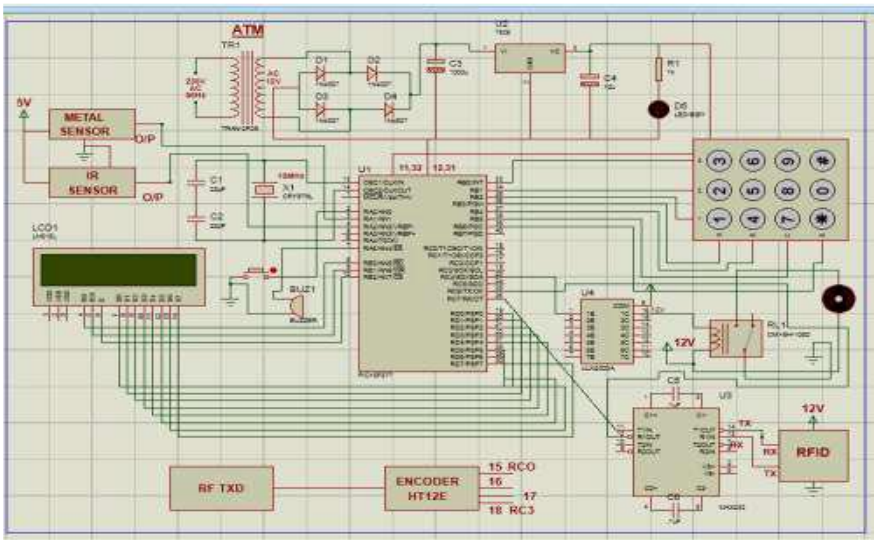

Fig. 7. Transmitter circuit using proteus.

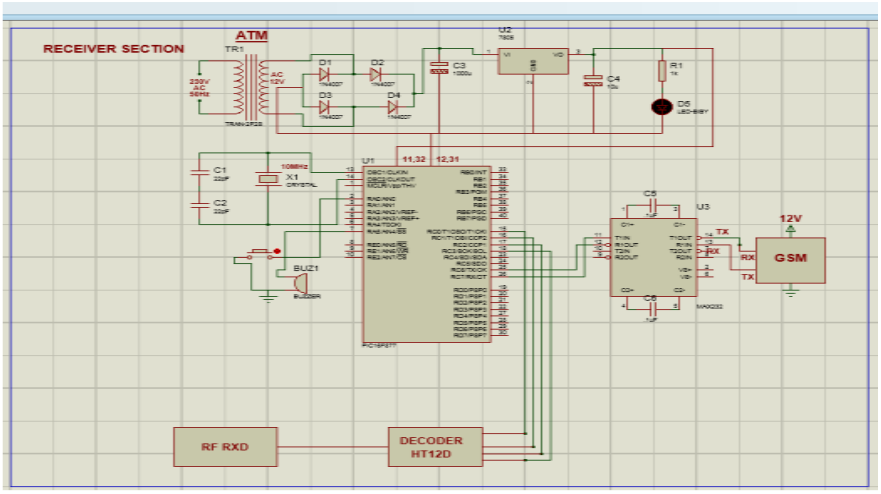

Fig. 8. Receiver circuit using proteus.

Decoder 4 data pins connected to PIC and o/p pin of RF RX connected to the decoder. GSM RX and TX pins are connected ted to PIC through max23the 2 [21, 22]. The switch output pin is connected to the PIC. LCD data pins are connected to a PIC controller.

Figures 9 to 12 display the hardware output for ATM working and not working condition for GSM and Phone. Figures 13 and 14 show the hardware prototype for transmitter and receiver side. Figure 15 displays the entire hardware setup.

Fig. 9. ATM working condition using GSM.

Fig. 10. ATM not working condition using GSM.

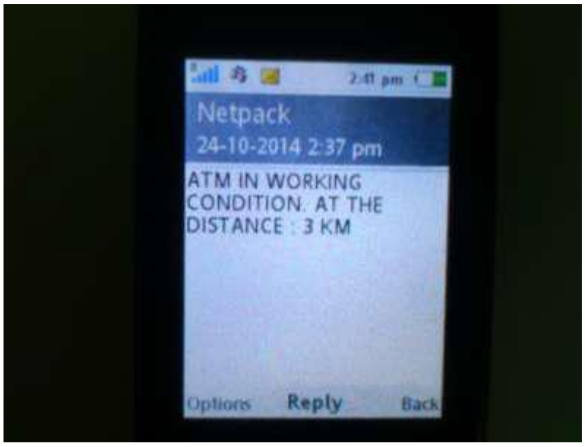

Fig. 11. ATM working condition using phone.

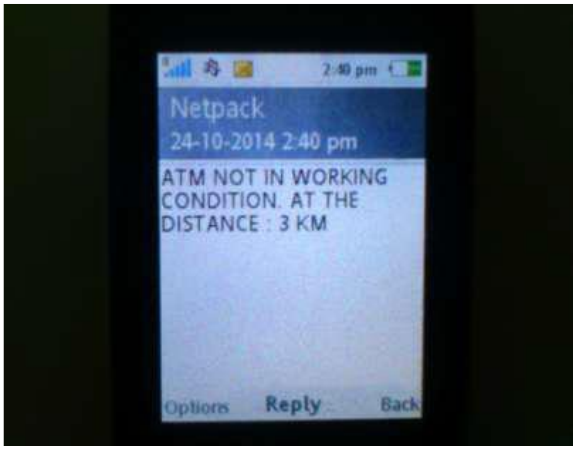

Fig. 12. ATM not working condition using phone.

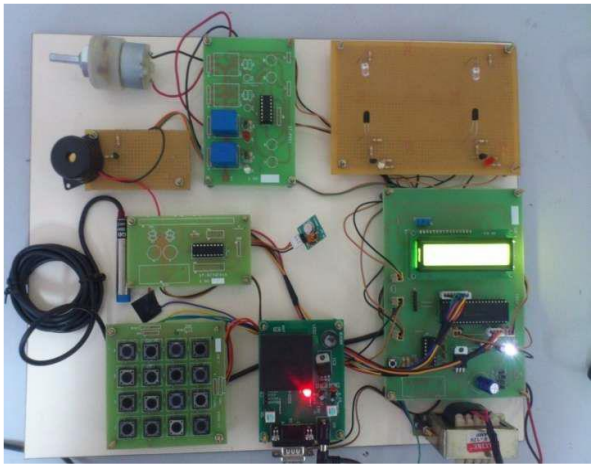

Fig. 13. Hardware prototype of transmitter kit.

Fig. 14. Hardware prototype of receiver kit.

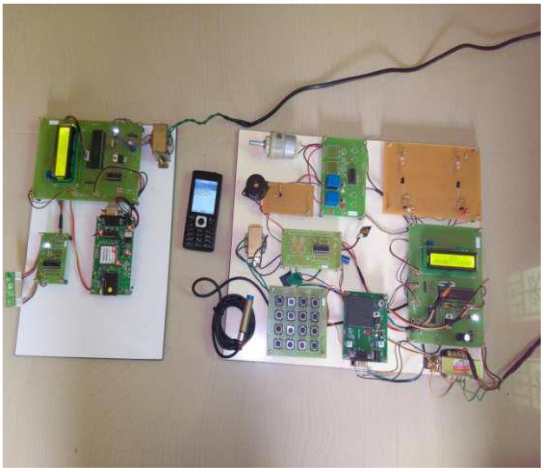

Fig. 15. Entire hardware kit.

5. Conclusions

The advantages of this model are more secure and protect the privacy and confidential information when compared to recent researches. It is power and time saving, user-friendly. It can be easily interfaced with any ATM machine and can be upgraded for future progress. Helps people to avoid strangers attack and forced to take money. It makes the use of the ATM in the safe and secure way. It provides more security during hijacked by a stranger. People avoid a traffic jam in front of the ATM centre at the time of the busy schedule. Reduced traffic jam in front of the ATM centre at the time of peak hours. Customers will be more satisfied to use ATM by implementing this idea. Future scope of this model has overviewed the process of notifying the process and service of the ATM machine in advance to solve the present fundamental problems. This model satisfies the customers in the ATM centre during the transaction. The user-friendly environment of the wireless display unit using RF Transmitter and the PIC microcontroller can also be updated for futuristic development. The security level in the ATM centres can be increased by means of implementing this idea.

Abbreviations

ATM	Automatic Teller Machine
CPU	Central Processing Unit
CIT	Cash Issuing Terminal
DC	Direct Current
DES	Data Encryption Standard
GSM	Global System for Mobile Communication
IBM	International Business Machine
IC	Integrated Circuit
IR	Infra Red
IRIS	Infra Red Identification System
LCD	Liquid Crystal Display
OTP	One Time Password
PC	Personal Computer
PIC	Programmable Interface Controller
PIN	Personal Identification Number
RF	Radio Frequency
RFID	Radio Frequency Identification
SMS	Short Message System
TTL	Transistor-Transistor Logic

References

1. Hashimoto, K.; Morinako, K.; Yoshiike, N.; Kawaguchi, C.; and Matsueda, S. (1997). People count system using multisensing application. *Proceedings of the IEEE Conference on Solid State Sensors And Actuators.* Chicago, United States of America, 1291-1294.
2. Leitold, H.; Payer, U.; and Posch, R. (1998). A hardware independent encryption model for ATM devices. *Proceedings of the IEEE Conference of 14th Annual Computer Security Applications*. Phoenix, United States of America, 205-211.
3. Sako, H.; and Miyatake, T. (2004). Image recognition technologies towards advanced automated teller machine. *Proceedings of the 17th International IEEE Conference on Pattern Recognition.* Cambridge, United Kingdom, 282-285.
4. Hamad, M.; Kassem, A.; Jabr, R.A.; Bechara, C.; and Khattar, M. (2006). PIC based microcontroller design laboratory. *Proceedings of the IEEE Workshop on System and Chip for Real Time Applications.* Cairo, Eqypt, 66-69.
5. Ng, R.Y.F.; Tay, Y.H.; and Mok, K.M. (2008). A review of iris recognition algorithms. *Proceedings of the IEEE Symposium on Information Technology*. Kuala Lumpur, Malaysia, 1-7.
6. Islam, S.; and Ajmal, F. (2009). Developing and implementing encryption algorithm for addressing GSM security issues. *Proceedings of the IEEE Conference on Emerging Technologies.* Islamabad, Pakistan, 358-361.
7. Wang, Y.; Zhang, Y.; Sheu, P.C.-Y.; Li, X.; and Guo, H. (2010). The formal design model of an automatic teller machine. *International Journal of Software Science and Computational Intelligence*, 2(1), 102-131.

8. Kim, C.S. and Lee, M.-K. (2010). Secure and user friendly PIN entry method. *Proceedings of the International Conference on Consumer Electronics Digest of Technical Papers. Las Vegas, United States of America*, 203-204.
9. Onwudebelu, U.; Longe, O.; Fasola, S.; Obi, N.C.; and Alaba, O.B. (2010). Real time SMS based hashing scheme for securing financial transactions on ATM systems. *Proceedings of the IEEE Conference on Adaptive Science and Technology. Abuja, Nigeria*, 1-6.
10. Das, S.S.; and Debbarma, S.J. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian E-banking system. *International Journal of Information and Communication Technology Research*, 1(5), 197-203.
11. Mohammed, L.A. (2011). Use of biometrics to tackle ATM fraud. *International Conference on Business and Economics Research*. Langkawi, Malaysia, 331-335.
12. Oancea, C.D. (2011). GSM infrastructure used for data transmission. *Proceedings of the IEEE Symposium On Advanced Topics In Electrical Engineering*. Bucharest, Romania, 1-4.
13. Soni, N.; and Jyoti (2012). ATM security by using fingerprint recognition. *International Journal on Applied Engineering Research*, 7(11), 1827-1830.
14. Lasisi, H.; and Ajisafe, A.A. (2012). Development of stripe biometric based fingerprint authentications systems in automated teller machine. *Proceedings of the IEEE Conference on Advances in Computational Tools for Engineering Applications.* Beirut, Labenon,172-175.
15. Skomersic, M.; Gojevic, T.; and Zuvanic, M. (2012). Impact of non-service related signalling in GSM mobile networks. Proceedings of the *IEEE 35th International Convention MIPRO. Opatija, Croatia*, 589-592.
16. Kazemi, R.; Mosayebi, R.; Etemadi, S.M.; Boloursaz, M.; and Behnia, F. (2012). A lower capacity bound of secure end to end transmission via GSM Network. *Proceedings of the International Symposium on Telecommunications.* Tehran, Iran, 1015-1020.
17. Xiao, Y.; Li, C.-C.; Lei, M.; and Vrbsky, S.V. (2014). Differential virtual passwords, secret little functions, and codebooks for protecting users from password theft. *IEEE System Journal*, 8(2), 406-416.
18. Kumar, M.S.; and Balamurugan, C.R. (2016). Self propelled safety system using CAN protocol. *Proceedings of the World Conference on Futuristic Trends in Research and Innovation for Social Welfare* (Startup Conclave). Coimbatore, India, 1-4.
19. Namrata; and Singh, S. (2015). Review paper on enhance the ATM security using fingerprint recognition. *International Journal of Computer Science and Mobile Applications*, 3(10), 38-47.
20. Syed, A,K.R.; and Wadhankar, V.R. (2015). Theft identification and remote information of ATM card by a unique system. *International Journal of Science and Research*, 4(7), 1377-1380.
21. Dutta, M.; Psyche, K.K.; and Yasmin, S. (2017). ATM transaction security using fingerprint recognition. *American Journal of Engineering Research* (*AJER*), 6(8), 41-45.
22. Kaiwartya, O.; Prasad, M.; Prakash, S.; Samadhiya, D.; Abdullah, A.H.; and Abd Rahman, S.O. An investigation on biometric internet security. *International Journal of Network Security*, 19(2), 167-176.

Appendix A

Sample Coding

```
#include<htc.h>
__CONFIG(PWRTE_OFF & BOREN_OFF &CPD_ON & DEBUG_ON &
WRT_OFF
& CP_ON & FOSC_HS & WDTE_OFF & LVP_OFF );
#define _XTAL_FREQ 10000000
#define rs RE0
#define rw RE1
#define en RE2
#define rf_bit1 RB0
#define rf_bit2 RB1
#define rf_bit3 RB2
#define rf_bit4 RB3
#define button RB5
void lcd_con(unsigned int);
void lcd_display(unsigned int);
void lcd_command(unsigned int);
void lcd_data(unsigned int);
void delay(unsigned int);
void lcd_str(unsigned char *,unsigned int);
void transmit_data(unsigned char);
void gsm_init();
void main()
{
unsigned char value,portB_pin,i,working_condition=0,not_working_condition=0;
ADCON1=0x07;
TRISE=0;
TRISD=0;
TRISB=1;
TRISA=1;
SPBRG=15;
TXSTA=0x20;
RCSTA=0x90;
lcd_command(0x01);
lcd_command(0x0E);
lcd_command(0x38);
lcd_command(0x80);
lcd_str(" ATM ",0);
lcd_command(0xc0);
lcd_str(" SECURITY SYSTEM ",0);
lcd_command(0x80);
while(1)
{
portB_pin = PORTB & 0x0F;
if(portB_pin == 0 && working_condition == 0)
{
working_condition=1;
lcd_command(0x80);
```

```
lcd_str("ATM IN WORKING ",0);
lcd_command(0xC0);
lcd_str(" CONDITION.",0);
not_working_condition=0;
}
else if(portB_pin > 0 && not_working_condition == 0)
{
not_working_condition=1;
lcd_command(0x80);
lcd_str("ATM IN NOT WORKING",0);
lcd_command(0xC0);
lcd_str(" CONDITION.",0);
lcd_command(0x80);
working_condition=0;
}
if(RCIF == 1)
{
RCIF=0;
if(RCREG == 'R' || RCREG == 'I' || RCREG == 'N' || RCREG == 'G')
{
RCREG=0;
delay(10);
transmit_data('A');
transmit_data('T');
transmit_data('H');
transmit_data(0x0D);
lcd_command(0x80);
lcd_str("message ",0);
lcd_command(0xC0);
lcd_str("sending.....",0);
portB_pin = PORTB & 0x0F;
if(PORTB & 0X20)
portB_pin = 9;
if(portB_pin == 0)
{
gsm_init();
lcd_str("AATM IN WORKING CONDITION. AT THE DISTANCE : 3
KM",1);
transmit_data(0x1A);
}
else
{
gsm_init();
lcd_str("AATM NOT IN WORKING CONDITION. AT THE
DISTANCE : 3 KM",1);
transmit_data(0x1A);
}
lcd_command(0x80);
lcd_str("message ",0);
lcd_command(0xC0);
```

```
lcd_str("send....send ......",0);
working_condition=not_working_condition=0;
}
RCIF=0;RCREG=0;
}
}
}
void gsm_init()
{
lcd_str("AT",1);
transmit_data(0x0D);
lcd_str("AT+CMGF=1",1);
transmit_data(0x0D);
lcd_str("AT+CMGS=",1);
transmit_data(0x22);
lcd_str("9894742081",1);
transmit_data(0x22);
transmit_data(0x0D);
}
void lcd_command(unsigned int val )
{
unsigned char t;
PORTD=val;
rs=0;
rw=0;
en=1;
delay(1);
en=0;
}
void lcd_data(unsigned int lcd_val)
{
unsigned char t;
PORTD=lcd_val;
rs=1;
rw=0;
en=1;
delay(1);
en=0;
}
void lcd_str(unsigned char *disp, unsigned int n)
{
int x;
if(n == 0)
{
for(x=0;disp[x]!='\0';x++)
{
lcd_data(disp[x]);
}
```

```
}
else if(n == 1)
{
for(x=0;disp[x]!='\0';x++)
{
transmit_data(disp[x]);
delay(3);
}
}
}
void delay(unsigned int n)
{
unsigned int e,a;
for(e=0;e<n;e++)
{
for(a=0;a<10000;a++);
}
}
void transmit_data(unsigned char A)
{
TXREG=A;
while(TXIF==0);
TXIF=0;
}
```

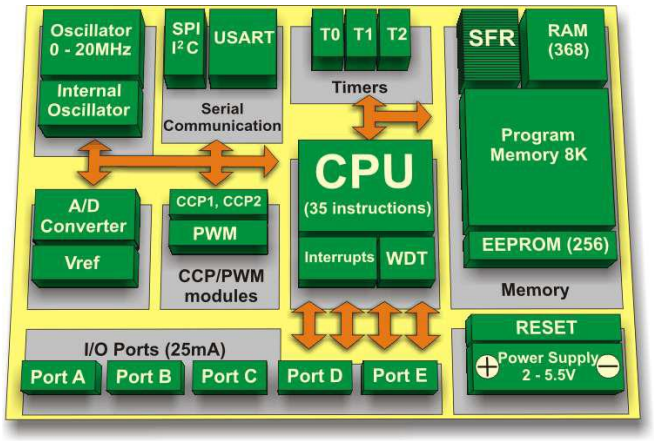

Fig. A-1. Block diagram of PIC16F877A.