Mobile Phone Based Secured Electronic Payment System Using RFID Communication

D. Binu[1], [2]Vijay Anand, [3]R. Gayathri

[1,3]Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India
[2]SNMV College of Arts and Science, Coimbatore, Tamilnadu, India

ABSTRACT

This paper proposed an advanced ATM card security system using GSM. In which the owner controls the ATM transactions done by his assistant. The owner can give the password through SMS rather than sharing the password. This is made possible by adding the GSM technology to the ATM Machines. The ATM Machine is programmed to provide an option by getting Password through SMS. Whenever the user flash the ATM card in RFID, the machine ask the primary password, this password is entered through the keypad, if the password is correct, the card owner will get an SMS asking for the secondary password. The owner sends the secondary password through SMS. This secondary password has dynamic change OTP. The machines checks for the password and processes the further transaction. If any theft finds in this transaction automatically the GSM modem send the SMS to card owner and police. Then ATM CARD automatically blocked and it generates the alarm when theft occurred.

Keywords : MSP430 Microcontroller, RFID Communication, GSM Technique, level controller, RS232 communication, DC Motor, Alarm, LCD Display, Energia tool.

I. INTRODUCTION

In today's world, automation is gaining rapid reputation. As the automation and social computerization has been increased credit card and ATM has been installed to simplify the activity the banking activity has been simplified, however the crime related with financial organization has been increased in proportion to the ratio of spread out of automation and devices [1]. Security and authentication is improved by means of implementing many methods in present environment [2][3][4]. In order to overcome the security issues in bank services several approaches are being implemented[5][6][7].

GSM based secured ATM transaction is proposed in this paper. MSP430 Microcontroller, DC Motor & Relay and driver, RFID reader, Level converter, RS 232 communication, LCD Display, Alarm are used to design the prototype model. The buzzer is used to give signal for corresponding police station and bank .Here DC Motor is used to block the ATM and another DC motor used for transaction intimation. A message is passed to the nearby police stations with the help of

GSM modem. Authentication is provided by the customer entering a personal identification number (PIN). By using GSM module we can send information of balance status by message to user's registered number which solves the problem of paper wastage.

1.1 OTP Verification:

OTP (One Time Password) system is additional feature used in the authentication of ATM card money transactions. After entering the primary pin by the user, the secondary pin is sent with the OTP as text message from the owner's mobile phone. As soon as OTP is verified by the ATM machine, and if the OTP is matched, the transaction is carried out. If the OTP doesn't matches, then transaction is cancelled by the ATM machine.

1.2 ATM Card Theft Process

In case of ATM card is theft or accessed by the unknown user, whenever he insert the ATM card, OTP is received in card holder's mobile phone. So he can identify that the ATM card is missed. At that time

when the card holder sent the message as '@theft', which blocks the ATM card by the bank server and alarm is switched ON at corresponding ATM centre that the card is accessed by the thief.

1.3 GSM (Global System for Mobile communication)

GSM is an open, digital cellular technology used for transmitting and receiving the data. It works in 1.8GHz and 900MHz bands and it also maintains data transfer speeds of up to 9.6kbps. In our proposed project GSM technology is used for sending and receiving the text message for OTP system.

II. RELATED WORKS

In recent days most of them do not carry money for shopping instead they carry an ATM Card. If the customer needs money they can visit to their nearby ATM centre insert their ATM card, and take the required amount needed. ATM (Automatic Teller Machine) is authenticated with the primary PIN (Personal Identification Number), which is not much secure system. PIN number is consisted of 4-digit number, which is easily accessed at any time by the unwanted person. ATM card is encrypted by strong software's so there is no chance to get the PIN number. To keep the PIN number secure, there are a number of ways. Since ATM machines are found almost everywhere, we need not have to carry a huge amount in your hand. Whenever we need money, you can take it from the nearby ATM counter. All we have to do is carry the ATM card wherever we go. Since the ATM card has a unique password, no one can access it even if it is stolen. Because of increased prohibited copies of cards with a magnetic stripe, the European Payments Council established a Card Fraud Prevention Task Force in 2003 that spawned a commitment to transfer all ATMs and POS applications to use a chip-and-PIN solution. The "SEPA for Cards" has completely removed the magnetic stripe requirement from the former Maestro debit cards.

2.1 Design and Implementation of Security Based ATM theft monitoring system

This paper is proposed to avoid ATM theft from robbery and it also reduces the drawbacks that found in our society. Vibration sensor is used to sense vibration produced from ATM machine whenever theft occurs.

ARM controller based embedded system is used to process real time data which is gathered via vibration sensor. Once if the vibration is sensed the beep sound is produced from the buzzer and for closing the door of ATM DC motor is used. The gas leakage occurs inside the ATM to bring the thief into unconscious stage with the help of stepper motor. Camera is always in processing and sending video continuous to the PC and it will be saved in computer. RTC is used to capture the robbery occur time and the information is sent with the message to the neighbouring police station and corresponding bank through GSM. Hear LCD display board using showing the output of the message continuously. This will prevent the robbery and the person involving in robbery can be easily caught. Here, Keil tools are used to implement the idea and results are obtained. For running DC motor and stepper motor Keil tools is used for automatic door lock and also for gas leakage inside the ATM.

2.2 A Smart Security System for Accessing ATM

The basic aim of this paper is to study the system, which is used for ATM access to cash withdrawal with more security. In this mobile number and finger prints from the customer will be collected by the bankers to open the account and then ATM machine can be accessed by the customer. The working of system will start when our customer goes at ATM centre. First there is switch for entry. After getting entry customer has to places his finger on the finger print module. The user identity and validity of finger is checked, if it finds valid then ATM machine will ask for 4-digit ATM pin, which is fixed. If that 4-digit code match with entered pin code then system will automatically generates another different 4-digit code i.e. OTP. The code is send to the customer's mobile number which is registered through GSM. Here customer has to enter this code again. After entering OTP, System will check whether entered code is a valid or not. If it is valid, the customer is allowed for further accessing and the ATM will show various options like cash withdrawal, cash deposit. Also purpose of using Temperature sensor and tilt sensor is to provide security for ATM Terminal.

III. PROPOSED WORK

In our proposed system, we have an advanced ATM card security system using GSM, the owner controls the ATM transactions done by his assistant. The Owner

can give the password through SMS rather than sharing the password. This is made possible by adding the GSM technology to the ATM Machines. The ATM Machine is programmed to provide an option like get Password through SMS. OTP is secondary, random password which is sent through SMS from the corresponding mobile phone.

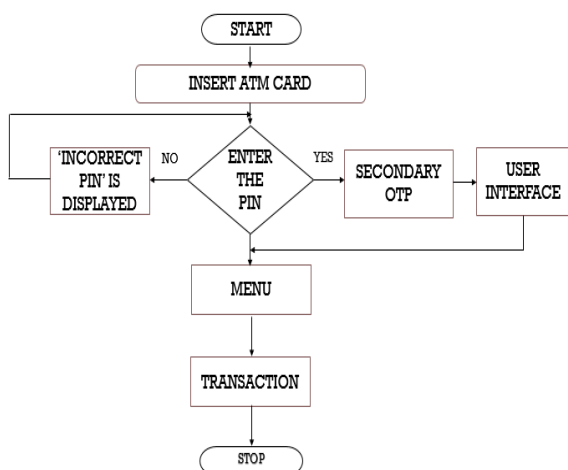The flow of the process is represented in figure 3.1.

Figure 3.1 Flow Chart

If the ATM card is used by the unauthorized person means theft sms is send to the account holder. This flow diagram is shown in figure 3.2.
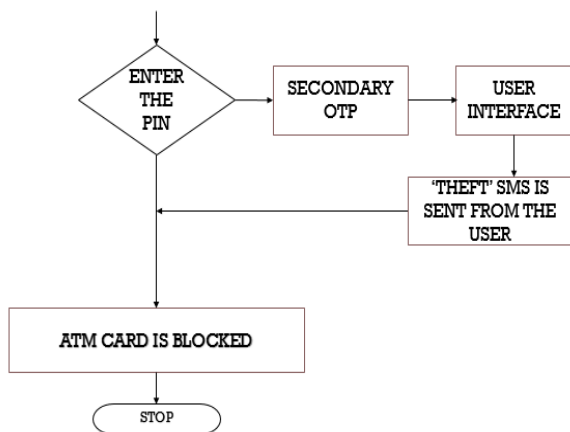

Figure 3.2 Flow Chart for Theft Process

3.1 Block Diagram Description

- The MSP430 can be used for low powered embedded devices. It is a mixed-signal microcontroller family from Texas Instruments.

- The MSP430 is a 16-bit microcontroller that has a number of special features not commonly available with other microcontrollers: Complete system on-a-chip — includes LCD control, ADC, I/O ports, ROM, RAM, basic timer, watchdog timer, UART, etc.., Extremely low power consumption — only 4.2nW per instruction, typical, High speed — 300 ns per instruction @ 3.3 MHz clock, in register and register addressing mode, RISC structure — 27 core instructions.

- To convert mains AC to low-voltage regulated DC power A power supply unit (PSU). The MSP430 is a 16-bit microcontroller need 3.6V to 5V to run.

- MAX232 converts signals from a RS-232 serial port to signals which is suitable for use in TTL compatible digital logic circuits. MAX232 IC is used as level converter in between the GSM modem and microcontroller.

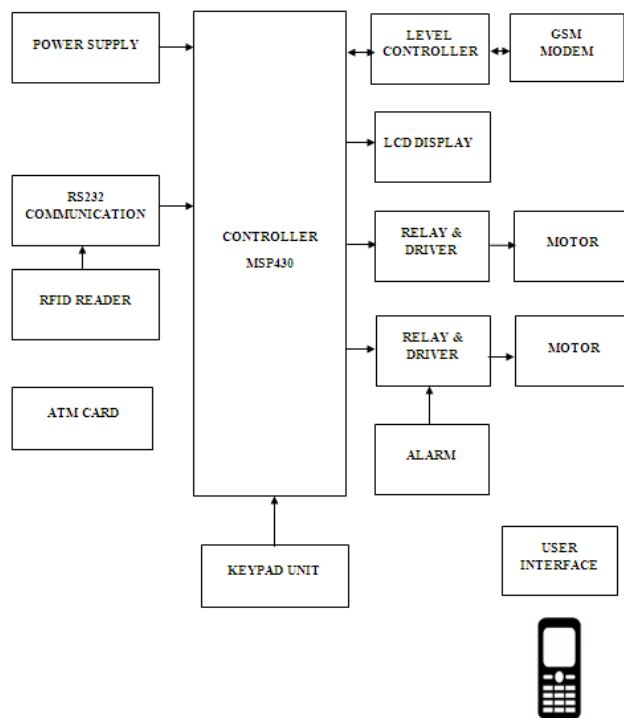The block diagram of the proposed system is shown in figure 3.3.

Figure 3.3. Block diagram

- Just like a mobile GSM modem is used which accepts a SIM cardand operates over a subscription to a mobile operator,. From the mobile operator perspective, a GSM modem looks just like a mobile phone.

- The RFIDreader and tagmust fulfil with the same standard to communicate. If a RFID tag is based on

a proprietary design, a reader must support the same communication protocol to communicate with that RFID tag. In many cases, if proprietary RFID tags are used, only proprietary RFID readers from the same vendor can be used. RS232 cable is used for the communication between the microcontroller and the RFID reader.

- Liquid crystals do not emit light directly. The LCD display, used here is 16x2 segment display.
- A relay is an electrically operated switch. ULN2003A is in driver circuits for relays, lamp and LED displays. A DC motor converts DC electrical power into mechanical power. DC motor is for intimation for money withdrawal in ATM machine.
- Keypad unit is a miniature keyboard or set of buttons for operating a portable electronic device, telephone, or other equipment. Membrane type keypad is used in this project.
- Alarm device or system of alarm devices gives an audible, visual or other form of alarm signal about a problem or condition. Alarm devices are often outfitted with a siren. Here we use a buzzer to intimate the false process in operation.
- A mobile phone is a telephone that can make and receive calls over a radio frequency carrier while the user is moving within a telephone service area. Mobile used here to send secondary password while swiping the ATM card and also to block the card when theft is happened.
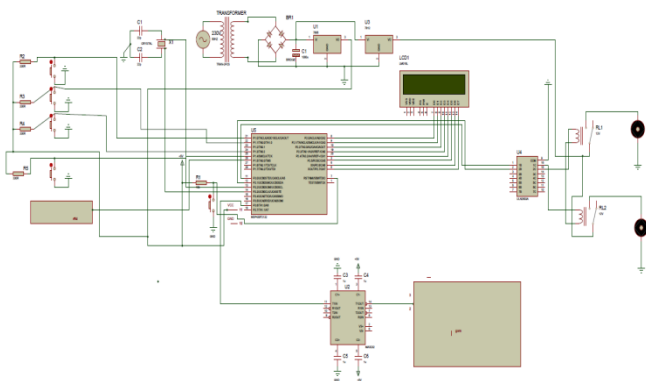
3.2 Circuit Diagram

Figure 3.4 Circuit Diagram of the Proposed System

3.3 GSM System for OTP Text Message

GSM is an open, digital cellular technology used for transmitting and receiving the data. GSM operates in the 900MHz and 1.8GHz bands. GSM supports data transfer speeds of up to 9.6kbps.

In our proposed project GSM technology is used for sending and receiving the text message for OTP system. ATM card holder's mobile number is registered in GSM module so, that he/she has the permission to access on OTP password, whether to send or not. GSM module is main module, used mainly for the OTP password system. Primary PIN is entered and also secondary PIN is used as OTP password for accessing the transactions. Both the PIN can be changed on ATM card holder's knowledge.

3.3 ATM Card Accessed By Unknown User or Thief

Usually the ATM card holder accesses the transactions by entering the PIN after inserting the ATM card in ATM machine. This is present system followed in ATM centres.

In this proposed project, primary PIN is entered and also secondary PIN is used as OTP password for accessing the transactions. Both the PIN can be changed on ATM card holder's knowledge.

When the ATM card holder inserts the card into the card swiping device, the machine asks for primary PIN. After the primary PIN is correct, the OTP text message is sent to the registered mobile number, which is verified with sent OTP password. When both the password is entered correctly, then transactions are allowed to be proceeded.

When the ATM card is accessed by the unwanted person or thief, it is blocked by sending a text message through registered mobile number. When the ATM card is inserted without the card holder's knowledge, a OTP text message is received in the mobile phone, so he can block the card by sending the text message as 'theft' to corresponding number.

IV. RESULTS AND DISCUSSION

In order to provide the secured transaction the prototype model has been developed. That model is represented in figure 4.1.
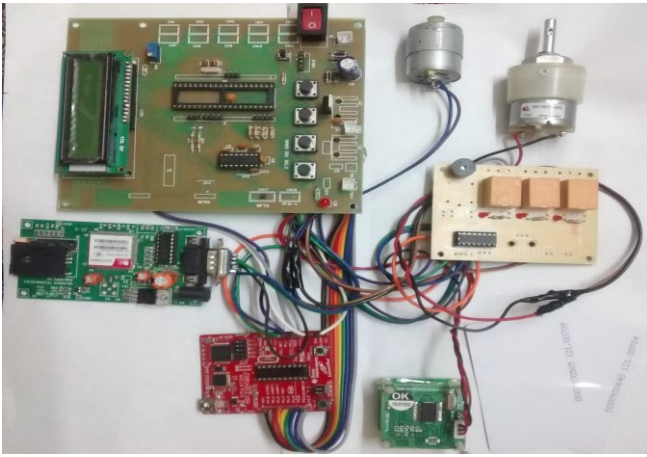
Figure 4.1. Prototype Model

4.1. Transaction Process:

The results for the various transaction processes using Energia software are shown in this section.

STEP-1: While switching on the model welcome message is displayed. This step is shown in figure 4.2

Figure 4.2 Welcome dispaly

STEP- 2: When Invalid card is inserted it is displayed in figure 4.3.

Figure 4.3 Invalid card display

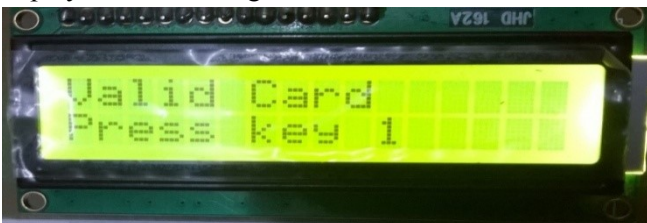**STEP- 3:** When another valid card is inserted the display is shown in figure 4.4.

Figure 4.4. Valid card display

STEP- 4: When the card is valid we should enter the user name and the Password which is also displayed as in figure 4.5. and 4.6.

Figure 4.5.Enter the user Name

Figure 4.6. Enter the Password

STEP -5: After entering the correct password OTP is received in registered mobile number. This step is shown in figure 4.7.
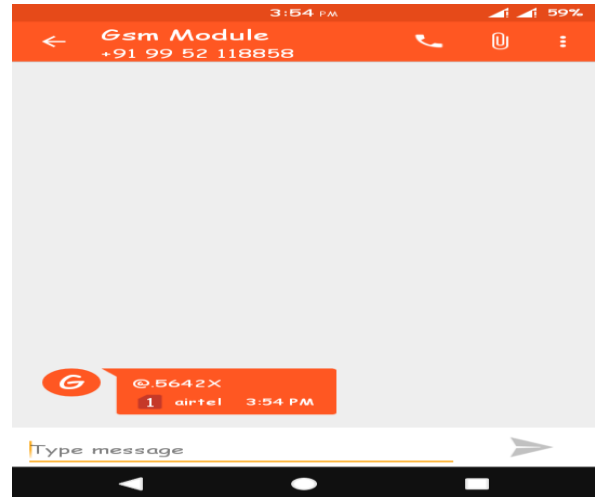

Figure 4.8.Receiving one time password

STEP-6: After receiving the one time password which is send from the registered mobile number which is shown in figure 4.9.

Figure 4.9.OTP send from registered mobile number

STEP -7: In order to send the OTP text message we should press Key 2 which is shown in figure 4.10.

Figure.4.10. OTP sends after pressing number key 2.

STEP -8: After sending the OTP, which is verified which is shown in figure 4.11.
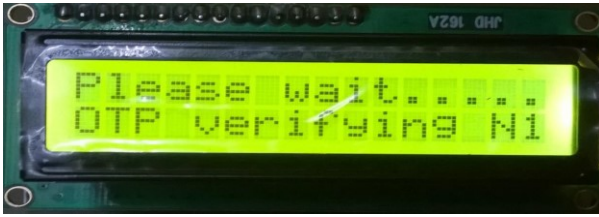

Figure 4.11 Verification of OTP

STEP-9: After the verification of the OTP the cash is collected by the user which is displayed in figure 4.12.

Figure 4.12. Cash Collection message

STEP-10: When the transaction is completed that information is also displayed as in figure no 4.13.

Figure 4.13. Transaction completed message

4.2.THEFT PROCESS:

If some unauthorized person used the ATM card means which is also shown in the following results.

STEP- 1 to 6: same as in the normal transaction process.

STEP- 7: The OTP is sent to the owner's mobile phone only. Hence the unauthorized person does not know the OTP.Hence the '@theft' SMS is sent from the owner's mobile phone to the server system of the bank.This step is shown in figure 4.14.
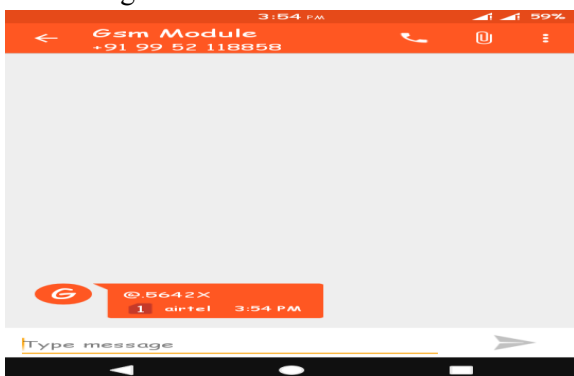

Figure 4.14. '@theft' SMS is sent from the owner's mobile phone

STEP- 8: When the theft message is received from the ATM card owner's registered mobile number to the server system of the bank then the card is blocked by the ATM machine and the same is sent to the ATM card owner also.This step is shown in figure 4.15.

Figure 4.15.Card blocked message from ATM

V. CONCLUSION

Thus, this project has the advanced electronic payment system in the Automated Teller Machine as it consisted with the secondary randomised password system as One Time Password(OTP) system. When the ATM card is a theft or accessed without the knowledge of card owner, then ATM card is been blocked by sending a single text message as 'theft' in the place of One Password Time and the card is also blocked from further transactions. This provides more secured transaction compared with the current ATM scenario.

VI. REFERENCES

[1]. H. C. Yu, K.-H. His , and P.-J. Kuo , "Electronic Payment Systems: An Analysis and Comparison of Types". Technology in Society, vol. 24, no. 3, 2002, pp. 331-347.

[2]. Binu,D, Malathi, P, 'Multi Model based Biometric Image Retrieval for Enhancing Security',Indian Journal of Science and Technology, vol. 8, no. 35, 2015, pp. 1-10.

[3]. S.T.Bhosale, Dr.B.S.Sawant, "Security in E-Banking via Card Less Biometric ATMs", International Journal of Advanced Technology & Engineering Research, Vol.2, pp.9-12,2012.

[4]. Binu,D,Malathi, P,'Two modal Biometric based Content Based Image Retrieval Approach(TMB-CBIR) for Biometric Authentication',Asian Journal of Information Technology, vol. 15, no.13, 2016, pp. 2154-2161.

[5]. Kim, Bo-Ra, "Domestic ATM status and meanings", Payment and Settlement, and IT, Vol. 44, pp. 76, 2011.

[6]. D.Binu,M.Arun Athithyan, G.K.Felins, A.Mohammed Anish, D.Sathish Kumar,"Secure Bank Locker System with Biometric" in International Journal Innovative Research and scientific Technology ,March 2017,pp.85-89, (IJIRST/Conf/NCNICS/2017/017).

[7]. M.R.Dineshkumar, M.S.Geethanjali, R.Karthika, M.Nagaraj, N.Vijayanandam,"Protected Cash Withdrawal in ATM Using Mobile Phone", International Journal Of Engineering And Computer Science, Vol.2, pp.1346-1350, 2013.