ENHANCED SECURITY IN ATM TRANSACTIONS USING GSM

S. Sudharani, K. Suriya, R. Swapna, M. Varshini¹ and Shaik Thasleem Banu²

Department of ECE, Rajalakshmi Engineering College, Chennai
¹varshvidhya@gmail.com, ²thasleem.red09@gmail.com

ABSTRACT

Now-a-days the usage of ATM Cards has been increased globally for providing various Banking Services. As its usage increases, fraudulent activities using ATM cards also have been increased. This paper mainly concentrates on improving the security of the ATM Transactions by generating an OTP-One Time Password using GSM. Once the ATM card is inserted a message containing the required Pin number to access the account is sent to the customer’s mobile. The Proposed system consists of a Transmitter & a Receiver Module, where the Transmitter module includes the ATM Machine which is represented here by an ARM Microcontroller along with a GSM module for sending the generated OTP to the customers. The Receiver was the mobile phone of the customer. The main outcome of the paper is to provide an easy access & to detect the fraudulent transactions and avoids the fraud before it happens.

Keywords – GSM, ATmega32, OTP, AVR Studio, GLCD.

I. INTRODUCTION

ATM- Automated Teller Machines are the most commonly accepted Payment modes for providing banking services all over the world. With the Help of ATM, customer can perform various banking operations like cash withdrawal & deposit, paying bills, money transfer, etc. beyond working hours and also without any physical contact with the banking officials which also updates the accounts and records of the banking system automatically. In ATM, the general Process Involves

- Identifying the customer by the ATM card,
- Customer is authenticated by entering the required PIN-Personal Identification Number.
- Access is granted for performing banking activities.

However, many challenges are faced to provide a highly secured services to the customers by avoiding fraudulent activities. As the use of ATM cards have been increased, the fraudulent activities¹ using the card has also increased which includes in the case of missing/theft of ATM cards, duplicate ATM cards, misuse of ATM Cards by unauthorized persons, etc.

The existing Fraud Detection Systems includes

- Finger Print Recognition⁶,
- Image/Video Processing⁷,etc.

Here, Crime plays an important role here for investigation i.e. the fraud is detected after the fraudulent transaction is processed. Hence, the customer has to face a lot of problems before he could recover his accounts. It seems to be time consuming as it need a long investigation process.

In the case of image/video processing, once the recording devices like cameras are damaged, further processing could not be proceeded. Even in finger print recognition fake ones can be easily used to access.

In recent times, even the PIN numbers that we are entering can be easily found out using a thermal detecting cameras –infrared cameras. Thus, to avoid these fraudulent activities & to overcome the disadvantages of the existing systems, security features of the ATM should be enhanced.

II. SYSTEM

Fig. 1 - Flow Chart
DESIGN
With reference to the paper on online banking\[^3\],
We are proposing a 2 Module system for ATM which includes

- **Module 1 – Transaction by generating OTP(One Time Password) using GSM**
  - First, by inserting the ATM card, the details of the customer are found.
  - Then, a message containing a pin number is sent to the mobile phone of the particular user.
  - This number is entered in the ATM machine.
  - In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal.
  - Scenario like, the password is found to be defective, passage out will be locked.

- **Module 2 – Image authentication in the case of non-availability of cell phones – no signal, power off, etc. by selecting an image set by the customer correctly from a number of images with a less no. of attempts.

Additional Features like Alarm & Door lock in the case of breaking of ATM Machines are also included.

III. HARDWARE SYSTEM DESIGN

i) **Microcontroller ATMEGA32**
A low-power CMOS 8-bit microcontroller based on the AVR enhanced RISC (Reduced Instruction Set Computer) architecture. It consists of a 32 Kbytes of In-System Self-programmable Flash program memory. It Possess a clock cycle of 1 MHz, so a throughput of 1 MIPS per MHZ is achieved. They have a total of 131 Powerful Instructions of which most are Single-clock Cycle Execution .It has 4 Times faster & Simpler Instruction Set compared to PIC controller as it follows CISC(Complex Instruction Set Computer) architecture. It also has a Inbuilt Serial USART Communication & Analog to Digital Converters.
These AVR chips are only used for developing latest Arduino platform.

ii) **GSM – Global System for Mobile Communication**
GSM Module is used for sending the OTP to the customers via SMS. GSM - A globally accepted Standard for Digital Cellular Communication. It is designed as a second generation (2G) cellular phone technology providing Call, SMS & data services (up to a speed of 1Mbps) It uses a TDMA – Time Division Multiple Access Approach. It makes use of a band of 900MHz.

- **UPLINK - 890 to 915 MHz**
- **DOWNLINK - 933 to 960 MHz**

Communication of the MCU to the GSM is performed through a Serial USART.

![Block Diagram](image)

**Fig. 2 – Block Diagram**

```c
USART_putstring("AT+CMGS="$919751337841"""); //phone number to which you want to send sms
_delay_ms(1000);
USART_putstring("OTP for your transaction is :"); //SMS body
UART_Put_int(otp);
_delay_ms(1000);
UWriteData(0x1A); // sends ctrl+z end of message
```

**Fig. 3 Code for Generating OTP**

iii) **RFID Tag & Reader**
RFID Tags are used in the case as an alternative to the ATM cards. RFID – Radio Frequency Identification Device - used to track or identify an object. A Reader is used to gather digital information from an RFID tag. Radio waves are used to transfer data from tag to reader.

Two types of tag
- **ACTIVE TAG** – self powered RFID tags with a use of Battery(high range)
- **PASSIVE TAG** – powered by electromagnetic energy transmitted from an RFID reader

Frequency Range
- Low Frequency Systems - 125 or 134 KHz
- High Frequency Systems - 850 to 950 MHz

Reader must be in the range of 3 to 300 feet

iv) **A 4*4 Matrix Keypad – Input Device**
It is used for Entering the obtained OTP received through SMS.A matrix keypad is used as it reduces the no. of ports pins required to read a lot of digital Input.
v) GLCD – Graphics liquid Crystal Display (128*64) - Output Device
Helps in displaying the graphical images for required authentication & security.

vi) Motors & Relays
Two motors are used
- Motor 1 - Withdrawing Money
- Motor 2 - Door Lock
Simple DC Motor is used - converts Electrical power into Mechanical Energy. Relays are Electromagnetic switch operated by a relatively small electric current which are used for providing the required voltage to the motor from the low powered microcontroller.

vii) Vibration Sensor & Buzzer
Vibration sensor are used in the case of breaking of ATM by the people involved in burglar activities. The output from the sensor is sent to the controller which Activates the buzzer alarm & send an alert message to the nearby police station and also to the required bank officials.

IV. SOFTWARE SYSTEM DESIGN
1. Win AVR
   Compiler – converts C file into .hex file
   WinAVR is a suite of executable, open source software development tool for the Atmel AVR series of RISC microprocessor hosted on windows platform.

2. AVR Studio 4.1
   AVR Studio is an Integrated Development Environment (IDE) by Atmel for developing applications based on 8 bit AVR microcontrollers. Prior to installation of AVR Studio, you have to install the compiler WinAVR. This will allow the AVR Studio to detect the compiler.

3. Extreme Burner - A GUI interface used to burn the .HEX file to the MCU.

V. OBSERVATIONS & RESULTS

Fig. 4 explains the interfacing of various components like GSM, RFID Reader, GLCD, etc. First we have to place the ATM card i.e. the RFID Tag over the reader. Once the card is placed it will ask for the ATM Pin and then the menu is displayed as shown Fig. 5 & 6.

Fig. 5 - ATM card – RFID tag to be Placed

Fig. 6 - Card Detected & Options Displayed

Fig. 7 - OTP & Transaction Details Received Via SMS

In the case of selecting the OTP Generation option, the required OTP will be sent to the registered phone of the customer. By Entering the correct OTP received, it will move to further options for providing banking services, which is shown in Fig. 7.

If wrong OTP pin is Entered, it will display as ‘wrong password’ as shown in Fig. 8.

If Image authentication option is selected, as in Fig. 9 several images will get displayed. By selecting the registered image we can move to the next step of banking as shown in Fig. 10.
In the case of entering the password wrongly for more than a no. of attempts, door will be locked alerting with an alarm and an alert message is sent to the required Banking authorities and also to the Police Officials.

As this systems involves Generation of OTP by GSM, it has a major disadvantage of the absence of signals in the mobiles. This can be rectified by improving the signals of the cell phones using a signal booster or by undergoing an ATM transaction using the image authentication method.

VI. CONCLUSION
As the Generation of OTP is now presently used only in the case of Internet banking, money transactions, etc., this can be implemented in ATM Machines for improving the security of the ATM transactions as it overcomes several disadvantages of the previous systems. This can also be implemented in future by using the network services of the banks by integrating the details of the customer.

VII. REFERENCES