Enhanced ATM Security System using GSM, GPS and Biometrics

Shivam Mishra, Aakarsh Jain, Shivam Kumar, Ankit Goyal

***Abstract*— There is a drastic increase in the frauds related to the Automated Teller Machine (ATM) and it has actuated the development of advanced authentication mechanisms that can enhance the security of the ATM. As the advancement in the field of technology is taking place, the verification and identification of any person is very easy but a crucial thing. It is requisite for securing the personal information. Nowadays, the lock system, control of the vehicles, safe box and even accessing bank accounts through ATM (Automated Teller Machine) are all dependent on the identification and verification of the person. Earlier, the traditional methods like ID card verification were used but due to advancement in the field of banking, technology has been involved in the identification and verification. The advent of ATM (Automatic Teller Machine) has some positive as well as negative impacts. Due to this, the fraud has also increased which is causing financial losses to the customers. The researchers and engineers are working in this field to make it more reliable and secured. The system which is employed for security purpose must be fast enough as well as robust too. This paper therefore presents a design on enhanced ATM security system using GSM, GPS and finger print scanner. This method adds additional security to the traditional system's security mechanisms. The presented design is unique because of fingerprint scanner, GSM and GPS. It is convenient as it consumes low power and it is portable. The proposed design is realistic as well as cost effective when compared to the other traditional authentication and verification systems of Automated Teller Machine (ATM).**

***Index Terms*— ATM Security, Fingerprint Scanner, GSM Module, GSM Module, ATM, GPS, Authentication.**

I. INTRODUCTION

Earlier, "barter system" was used for the exchange of goods and merchandise due to the lack of monetary instruments [1]. But, the society in the modern days has replaced the barter system by using the different monetary instruments as the unit of exchange. Hence, the money is now used for various denominations as the sole purchasing power. Now, this era has brought "plastic money" in the form of credit cards, debit cards, etc. [2] into the existence which has now replaced the paper and metal based currency. This has introduced the Automated Teller Machine (ATM) and its use is increasing day by day all over the world.

Due to awareness and installation of more and more Automated Teller Machine (ATM) cash points by different banks all around the world, the number of ATM card holders is increasing day by day as it is the most sophisticated way to take out cash from the accounts. But, advancement in technology has also increased the illegal activities like ATM card fraudsters and has given the birth to cyber-crime also. Nowadays, the banks are continuously warning the customers not to disclose their ATM card details to a second party so as to keep the accounts secure. Some of the techniques used by the fraudsters to attack the customer's account are shoulder surfing of users at ATM points, PIN interception via text messages and emails, use of fake PIN Pad overlay and outright card theft.

The problem of ATM frauds affects the banks as well as the customers and even it is the threat to all the parties involved. So, a coordinated and cooperative action is required on the part of the bank, customers and all the law enforcement agencies [3] [4]. These ATM frauds not only cause financial losses to the bank customers but also belittle the confidence of the customers in the ATMs [5]. Greater use of ATM for transactions would be discouraged due to the frauds. Even the ATM service is profitable to the banks also, so the frauds cause losses to the banks also. So, it is necessary for the banks to prevent the ATM frauds. Thus, better technology must be implemented to secure the ATMs. Many banks have employed the second level authentication to ensure the integrity and security of the online payments. Google was the first to use this technology to increase the security of E-mail account holders.

In this paper, a design on Enhanced ATM security system is presented. As the fingerprint of any person is the most unique identity so the fingerprint module is used for the identification purpose. After the verification of fingerprints, the user can proceed for the transaction but if it is not verified for three attempts, the GSM module will send the warning message to the bank customer as well as to the nearest police station. The GPS module will send the location of the ATM (Automated Teller Machine) so that the police can track the perpetrator. This design helps in protecting the user accounts from the unauthorized access. Even if the password is guessed, cracked or stolen, the perpetrator will not be able to access the account without having the verification codes which is obtained by the user only when the fingerprint verification is passed.

Shivam Mishra, B.Tech, Department of Electronics and Communication, K.I.E.T., Ghaziabad. Phone No. — +91-9582346836

Aakarsh Jain, B.Tech, Department of Electronics and Communication, K.I.E.T., Ghaziabad. Phone No. — +91-7906344351

Shivam Kumar, B.Tech, Department of Electronics and Communication, K.I.E.T., Ghaziabad. Phone No. — +91-7906672850

Ankit Goyal, Department of Electronics and Communication, K.I.E.T., Ghaziabad. Phone No. — +91-9873592529

II. Block Diagram

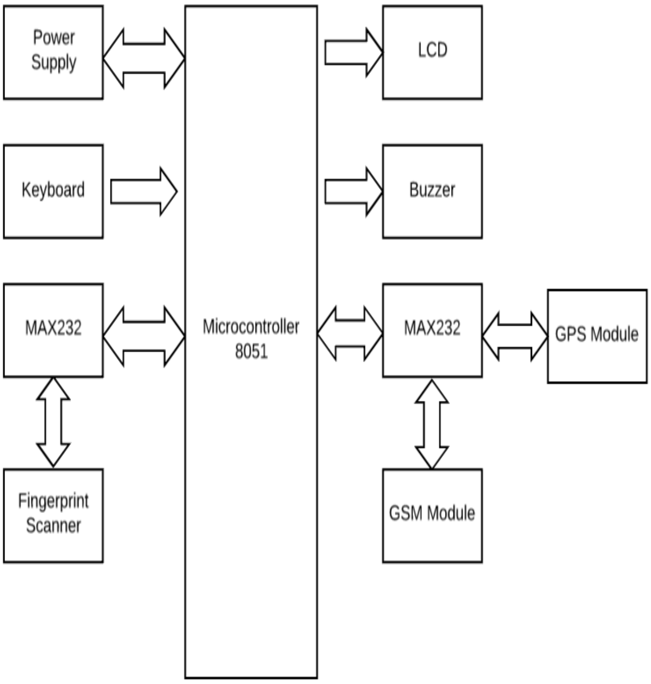

Fig.1. Block Diagram

III. Hardware Design

1. **Micro Controller (8051): -** The micro controller is the most important part of the whole system. It manages all the operations of the designed system. The micro-controller used here is 8051 of the Intel family. The main features include It has 2 external and 3 internal interrupts. It has two 16-bit timers and is also equipped with four 8-bit ports. This includes 32 general purpose registers each of 8-bits and has 16-bit program counter and data pointer. The address bus of 8051 microcontroller is of 16-bit and data bus is of 8-bit. It has 128 user defined software flags and 4 register banks. It also has 64 KB of on-chip memory. The 8051 micro controller is interfaced to different modules using GPIO (General Purpose Input/Output) pins. It receives the fingerprint template coming from the fingerprint scanner. The micro controller will match then coming template with the pre-stored template of the fingerprint. If the stored template matches then the person is allowed to access the processing system. If the mismatch occurs continuously for three times then the microcontroller makes the GSM module to send a prior generated warning message to the bank customer as well as to the nearest police station and will also raise the buzzer i.e. alarm.

2. **GSM Module:-** The GSM module used here is SIM900 which is a complete Quad-band GSM solution which can be used in many applications. This module is interfaced with the 8051 micro controller. When the fingerprint template is not verified continuously for three times then the GSM MODEM is used to send a prior generated warning message to the enrolled user or customer as well as to the nearest police station. It is basically used to communicate with the mobile phone according to the signals provided by the 8051 micro controller.

3. **Keyboard:-** When the fingerprint template matches then the bank sends a six digit OTP (One Time Password) to the mobile phone of the enrolled user. The user types that six digits OTP or code using the keyboard after which the user is allowed to access the further system for the transaction of money.

4. **LCD:-** LCD stands for Liquid Crystal Display. The 2 X 16 LCD display provides user interface and makes the communication possible and easier. It displays the current status of the process running on the system. It also shows the instructions for the users. It is interfaced with the 8051 microcontroller.

5. **Power Supply:-** The power is the most important part of any system and this power supply provides power to all the units. It basically includes a step-down transformer which step down the 230V ac to 18V ac and the bridge rectifier is used to convert ac to dc. This dc is filtered using the capacitor filter. The voltage regulators LM7805 and LM7812 are used so as to provide the positive 12V and 5V respectively to the other units as required.

6. **MAX232:-** The MAX232 includes two receivers that convert from the RS-232 to TTL (Transistor-Transistor Logic) voltage levels and two drivers convert from TTL logic to RS-232 voltage levels. So, only two out of all the RS-232 signals can be converted in each direction. Hence, the first driver or receiver pair of the MAX232 is used for TX (Transmitter) and RX (Receiver) signals, and the second one is used for the CTS (Clear to Send) and RTS (Request to Send) signals.

7. **GPS Module:-** GPS stands for Global Positioning System. The GPS module is used for determining the precise location. When the verification of the user continuously fails for three times then the microcontroller using the GPS sends the exact location of the ATM to the nearest police station so that the perpetrator can be tracked very easily by the police or by any other authorized official.

8. **Fingerprint Module:-** The fingerprint scanner is the most important module of the whole security system. Here, we have used FIM3030 by NITGEN. The supply voltage required by the module is 3.3V only. The central processing unit has 8 MB of SDRAM and 1 MB flash ROM, It is ADSP-BF531. The communication between the microcontroller and the fingerprint module is made by using UART (Universal Asynchronous Receiver/Transmitter). A biometric template is created by digitally processing the captured image. This template is stored and it is further used in the process of verification. This fingerprint module has optic sensor OPP03 and the processing board. The fingerprint module is highly efficient and it can provide easy recognition even to wet, dry, small size fingerprint.

IV. Functional Diagram of Operation

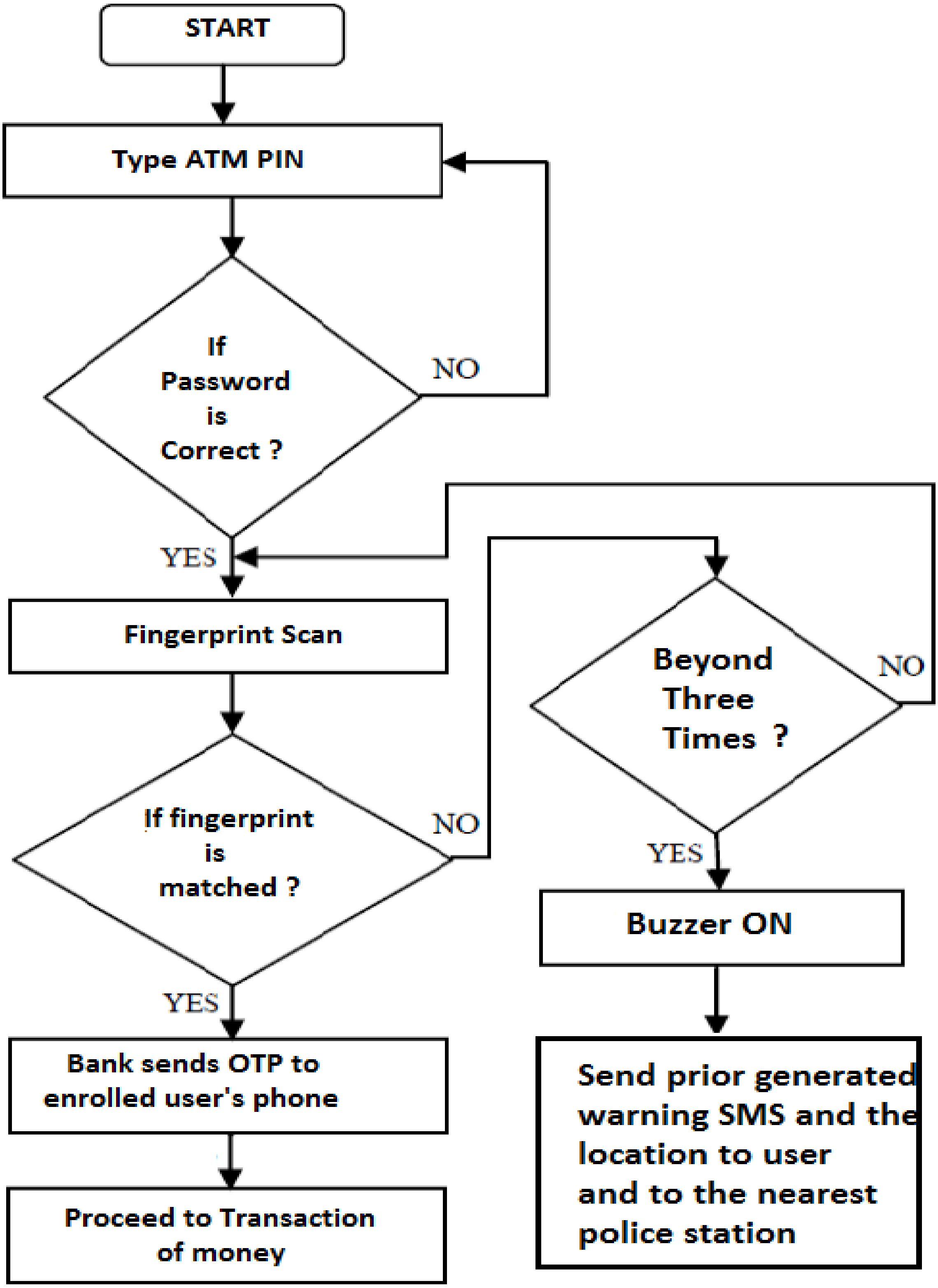
START
Type ATM PIN
If Password is Correct ?
NO
YES
Fingerprint Scan
If fingerprint is matched ?
NO
YES
Beyond Three Times ?
NO
YES
Buzzer ON
Bank sends OTP to enrolled user's phone
Proceed to Transaction of money
Send prior generated warning SMS and the location to user and to the nearest police station

Fig.2. Flow Chart of Operation

The functional flow diagram shows the working of the whole security system. Firstly, the user will enter the ATM pin; if it matches then only the user can proceed further for fingerprint scanning. If the fingerprint template do not matches with the stored template consecutively for three times then the buzzer will sound and a prior generated warning SMS along with the exact location of the ATM will be sent to the enrolled user's mobile phone as well as to the nearest police station. If the fingerprint template matches then the bank will send a six digit OTP (One Time Password) to the enrolled user's mobile phone and after entering that six digit OTP, the user can proceed for further transaction of the money.

V. Circuit Diagram

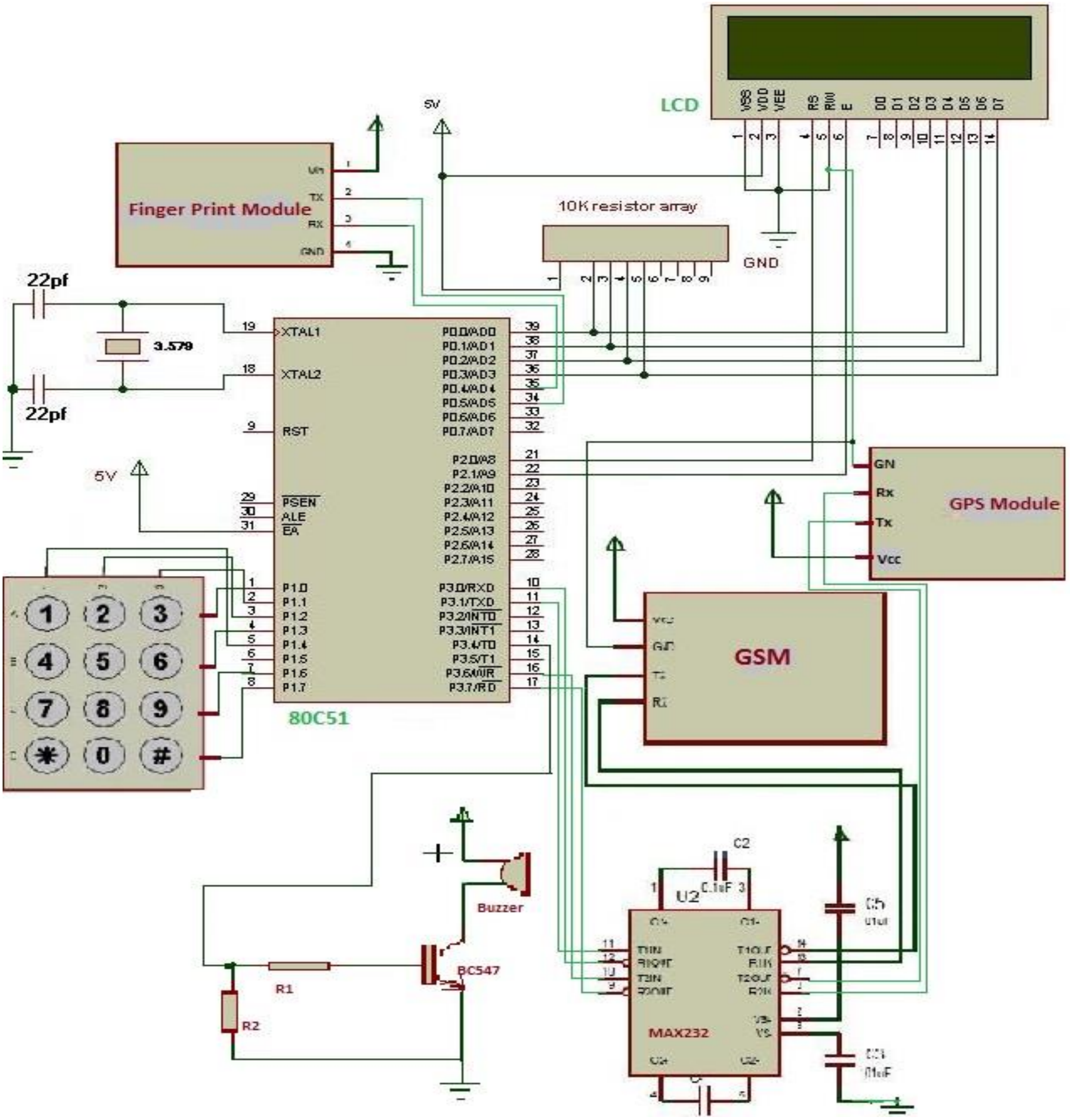

Fig.3. Circuit Diagram

In the circuit, the software RX and TX is created so that the GSM, GPS and Fingerprint module can be connected to the single microcontroller.

VI. Future Development

In future, this security system can be brought to the higher levels by incorporating face recognition methodology. Also, a lot of improvements can be done so as to enhance the speed of the security system. The robustness can also be increased by improving the modules which are used in this security system. This security system will definitely reduce the frauds related to the ATM (Automated Teller Machine).

VII. Conclusion

These days a lot of criminals tries to steal the ATM passwords or tries to tamper with the ATM bank accounts. As only one level of security is provided by the bank i.e. the ATM password only so it gets easy for the criminals to attack on the bank accounts. In this paper, a design is presented so as to enhance the security system of the ATM (Automated Teller Machine). A second level of security is provided using the fingerprint module which matches the fingerprint template with the stored template then only allows the user to proceed for the transaction and if it does not matches then after three attempts a prior generated warning SMS along with the location is sent to the enrolled user's mobile phone as well as to the nearest police station. In this way a second level of security is provided and this will reduce the number of ATM frauds.

ACKNOWLEDGMENT

We are very grateful to all those who were beside us during the course of making this project. We would like to thank our family and our friends who were always there with us with their constant support and encouragement. We would also like to thank Mr. Vibhav Kumar Sachan who helped us a lot in making this project. This project is sponsored by Department of Electronics and Communication Engineering, Krishna Institute of Engineering and Technology, Ghaziabad.

REFERENCES

[1] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17

[2] Adepoju, A.S & Alhassan, M.E. (2010). Challenges of automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis. Journal of Internet Banking and Commerce. Vol 15, No. 2. pp. 1-10. [Online]. Available: http://www.arraydev.com/commerce/JIBC/2010-08/Solomon.pdf

[3] Siddique, M.I & Rehman, S. (2011). Impact of Electronic crime in Indian banking sector – An Overview Int. International Journal of Business & Information Technology. Vol-1 No. 2 September 2011 pp.159-164.

[4] Leow, H.B. (1999). New Distribution Channels in banking Services. Banker"s Journal Malaysia, No.110, June 1999, pp.48-56. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

[5] Aliyu, A.A. & Tasmin, R.B. (2012) Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions. In proceedings of 3rd International Conference in Business and Economic Research (3rd ICBER 2012) MARCH 2012. pp. 150-164 C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

Shivam Mishra is a student in B.Tech, in Krishna Institute of Engineering and Technology, Ghaziabad. He has done a lot of project in embedded systems and is also leading a team of enthusiastic engineering students in the college's robotics team. He is a dedicated and compassionate student committed to the field of research. He is the author of this Research Paper.

Aakarsh Jain is a student in B.Tech, in Krishna Institute of Engineering and Technology, Ghaziabad. He is working on several projects based on embedded systems.

Shivam Kumar is a student in B.Tech, in Krishna Institute of Engineering and Technology, Ghaziabad. He is working on several projects based on embedded systems.

Ankit Goyal is an Asst. Professor in Krishna Institute of Engineering and Technology, Ghaziabad. He is working in the field of embedded systems