International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

Enhanced ATM Security System using GSM, GPS and Biometrics

Ketan D. Lokhande[1], Harshda M. Bodhe[2], Vishal G. Hushange[3], Pavan R. Shiraskar[4], Kirti B. Nagne[5]

[1-4]*Student, Dept. of Electrical Engineering, DES'S COET, Dhamangaon Rly*
[5]*Professor, Dept. of Electrical Engineering, DES'S COET, Dhamangaon Rly*

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 seminar 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.*

Key Words: **Authentication Protocol, Biometrics, Fingerprint, GSM, Multi-server.**

1. INTRODUCTION

An ATM card or debit card authenticates person after verification of card number, Expiry date, card holders name and the PIN. Security has always been a major concern and goal of all organization. For this we require a higher level of security which coined up an idea of adding Biometric to the current technology. On one hand where it has freed us from standing in long queues to carry out cash withdrawal, depositing money, transferring money and many more on the other it has also increased the risks of theft [1]. When talking about ATM machines or EDC we are mainly concerned with Physical security which aims at ensuring Access control, Identification and Authentication. But what in case your card is stolen, or PIN is known to an unknown entity. Biometric has emerged as a measure for highly. Security is not only confined to network but also includes Physical security. Access control is another consideration of Information System security to confirm the identity of individual so that only authorized entity is accessible to the system. ATM (Automatic Teller Machine) has proved to be an easy and convenient way to carry out all our banking tasks in just few minutes [2]. With the development of banking technology the way of banking has changed. There is no such object which can be considered as completely secure especially if it is about money.

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 cardholders 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.

In this seminar, 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.

2. RELATED WORK

As a result of rapid enhancement in Information and Communication Technology security challenges have popped up as the security breachers always aims at finding a loophole in the system. In ATM Security Using Fingerprint Biometric Identifier: An Investigative Study by M.O. Onyesolu has described how biometric procedure has enhanced security to ATM machines by solving the drawback of additional system. A.T. Siddiqui has explained how biometric has emerged to control ATM spam as it only allows

genuine entry to the system. A.K. Jain et al. have explained the complete procedure of conduction biometric verification in ATM devices. K. Archana and A. Gowardhan have explained how biometric performance and security can be increased by adding concept of Multimodal Biometrics in place of Unimode Biometric scheme. In a guide describes in detail the collection and matching procedure of biometric sample. Jain et al. describes the detailed concept of miniature extraction in fingerprint verification scheme. Authors of has explained and defines a complete analysis of performance by making comparison with various schemes. R.S Germain et al. has defined parameter clustering mechanism to speed up matching technique of biometric procedure. U. Jayaraman et al. has defined how fingerprint verification scheme could be improved reducing time of verification.

In our proposed system, Fingerprint verification scheme is used in the machine (ATM or EDC) preserving the advantages of existing technology added with the proposed concept solving the sensor efficiency issues. While using the ATM equipped with biometric system, the person first enters the PIN, which is first verified and if matched is asked for option of cash withdrawal or balance statement. Once cash withdrawal is selected min_trans is incremented to 1(min_trans=0 initially updated at very 00:00 hour).

According to the selected option the system responds i.e. if only enquiry is to be done, system does not require any biometric verification but for withdrawal, amount is to be entered. After the amount is entered, a check is conducted to determine if the amount exceeds the defined cash-limit OR min_trans> 3. If satisfied then the individual has to undergo biometric verification else if amount is below the cash-limit withdrawal AND the min_trans< 3 is allowed without undergoing biometric procedure. In case of biometric verification the individual has to present the fingerprint to the sensor. This collected characteristics sample is sent to the server to match with the stored template. If matched then the individual is authorized personnel and is permitted to dispense cash from ATM else access is denied. The min_trans counter is set to 0 at every 24 hrs to record the number of transactions made per day. The procedure is represented as under:

3. METHODOLOGY

3.1: Block diagram

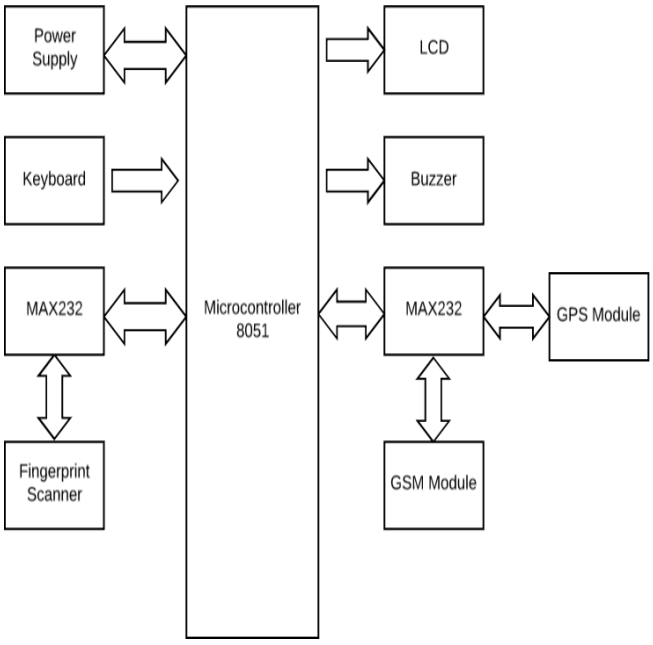

Fig.3.1: Block Diagram of Proposed System

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.1.7 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.

3.1.8 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.

Biometric data and Biometric Identification combine to form Biometric System. It involves two phase. First is the Enrollment Phase which is defined as the interval when the individual encounters the biometric system initially, here the subject gets their biometric information stored in the database. Since it is a single-time work it is conducted slowly and multiple times to make an accurate entry in the system. Second is the Verification Phase which involves several steps Data Collection. The very first, time consuming step where the user presents its characteristics to sensing device. In case of fingerprint or palm geometry scan requires a physical contact each time with the sensor. In schemes such as retina scan requires no physical contact. Transmission: It is only carried out in open system where the sensor is located at one location and processor at the other. It involves compression of data. Signal Processing or Pre-Processing: Having acquired the biometric characteristics need to prepare it for matching. It involves removal of noise and distortion. Feature Extraction: The pre-processed data is re-processed to obtain more précised feature with reduced size.

Having undergone the concept and working of Biometric, we came across its limitations with respect to input of the system i.e. the sensor .While providing the biometric sample the subject has to physically contact with the sensor of the Biometric system. This touching of sensor each time could degrade the working capability and accuracy of the system. As each time a new individual have to enter and provide his biometrics irrespective of the cleanliness of their hands. It affects the sensitivity of input device being used again and again even in case of small amount. In other schemes too, comes an issue of time consumption as for data capturing the system requires the subject to continuously look at the sensor for a fixed duration. Any movement could blur the image e.g. Retina scans or Face recognition. Here we apply our concept on ATM and EDC (Electronic Data Capture) machines which is also called swipe card machine which facilitates payment through debit cards.

3.2: Advantages

i. Fast

ii. Reliable

iii. Higher security

iv. No card problems

v. Accurate

3.3: Disadvantages

i. Failure of sensor result in the failure of whole security system.

ii. Electricity is always necessary as power failure leads to failure of whole system.

3.4: Application

i. Banking

ii. Self-service ATM

iii. Transaction/ Check deposit ATM

4. CONCLUSION

The sudden growth in electronic transaction and banking technology has demanded for higher level of security. Traditional methods of PIN or I-Cards can be forged or stolen and many times are too easy to be cracked as mostly these PIN are birth dates, security number, contact number or as such which can be easily guessed, but Biometric measures provide a hard-core security which neither can be stolen or forged. It provides a high level security by authentication and access permission to only genuine card holder. The proposed scheme aims at solving the sensor performance issues by limiting the users going through biometric verification and screening the customers who just want to know their balance. If the card user needs to withdraw an (amount>cash limit) but the (mantras< 3) or (amount3) need to present biometric else if (amount< 3) biometric procedure can be compromised. It also saves time together with solving sensitivity issue of input system.

REFERENCES

[1] O. Onyesolu and I. M. Ezeani, "ATM security using fingerprint biometric identifer: An investigative study," International Journal of Advanced Compuer 176 International Journal for Modern Trends in Science and Technology S.Naga Gowri, R.Durga Devi and P.Gowshalya : A Biometric based ATM Security System using RFID & GSM Technology Science and Applications, vol. 3, no. 4, pp. 68–72, 2012.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, vol. 14, no. 1, pp. 4–20, January 2004.

[3] C. Archana and A.Govardhan, "Enhance the security in the ATM system with multimodal biometrics and two-tier security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 261–266, October 2013.

[4] H. T. Siddiqui, "Biometrics to control ATM scams: A study," International Conference on Circuit Power and Computing Technology ICCECT, pp. 1598–1602, 2014.

[5] K. S. Hossian, A. Nawaz, and K. Grihan, "Biometric authentication scheme for ATM banking system using energy efficient AES processor," International Journal of Information and Computer Science, vol. 2, pp. 57–63, 2013.

[6] P. Singh, S. Singh, and R. Kumar, "Secure swipe machine with help of biometric security," unpublished.

[7] Prost & Sullivan "a – best – practices – guide – to – fingerprint - biometrics.pdf." (White Paper)

[8] R. O. Gorman, "Fingerprint verification," Springer, vol. 3, no. 1, pp. 43-64, 1998.

[9] S. K. Jain, H. Faulds, F. Galton, and E. Henry, "Fingerprint matching," IEEE Computer Society, pp. 36-44, 2010. [10]A. A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multibiometrics," Springer, 2006.

[10] S. Barman, S. Chattopadhyay, D. Samantha, S. Bag, and G. Show, "An efficient fingerprint matching approach based on minutiae to minutiae distance using indexing with effectively lower time complexity," International Conference of Information Technology IEEE, pp. 179– 183, 2014.