Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 8785 - 8789
Received 05 March 2021; Accepted 01 April 2021.

Cyber Security for Atm Terminals

B Poornima[1], Dr. Savadam Balaji[2]

[1]Ph.D. Scholar, CSE Department,
Koneru Lakshmaiah Education Foundation, Hyderabad,
Email: bachupoornima@gmail.com

[2]Professor, CSE Department,
Koneru Lakshmaiah Education Foundation, Hyderabad,
Email :balajis@klh.edu.in

ABSTRACT

In general, customers are identified and checked by their associated passwords and pins at the ATM terminals. However, because of the demonetisation in India, there is a need to improve the protection of these devices, which are easily susceptible to attacks when a card is stolen. Fingerprint biometrics, along with smart card and GSM technologies, will provide the best solution to this issue by increasing the security levels of the user account. It offers a very high level of protection through the use of smart card and technologies of GSM. A smart card reader and a GSM modem are provided for this device. In order to get access to the system, the user should effectively bring with him the same mobile number as specified in the smart card. This prevents the abuse of individual protection systems focused on smart card technology. An improved algorithm for fingerprint recognition is applied which can be used in all ATM terminals across India with quick response time.

Keywords—Biometrics, ATM terminal, security, password, Alarming module.

INTRODUCTION

Reliable user authentication has become an increasingly important task in the present Web-enabled world. The consequences of an insecure identification system may include loss of data confidentiality and data integrity. The reliable user authentication in internet banking became an important issue. Biometric systems (BS) are normally used for individual's recognitions based on the biological characters of individuals such as ears, veins, signatures, voices, typing styles, odours, gaits, and etc [8]. More specifically, this involves the design of conceptualization, development, assessment and innovative application methods to use communication technologies (ICT) and huge information in the rural domain [9].

Now-a-days, the use of ATMs (Auto Teller Machines) by the bank customers has been rapidly increased because of its ease of use. On the other hand, the tampering on ATM cards is also being increased (when the card is stolen). In the traditional ATMs, the user is authenticated by the credit card and password. But this authentication is not sufficient and not up to the mark. And when the card is stolen, the attacker tries to hack the passwords and withdraw money from the user's account. In order to prevent the attacks like this, Biometrics for fingerprints are very helpful in supplying the user's cards with protection since biometric readings vary from many hundreds of bytes to over a megabyte. Normally the information security begins with computer security, which is to provide security physical locations, hardware and software from threats [15]. And they have the advantage that their unique pattern of fingerprint security is normally greater than the password or other one-time passwords.

The benefits of using ATM biometrics are:

- Enhanced security-biometrics will increase the level of security
- Ease of use: no passwords need to be recalled by clients.

As discussed below, the variations between the current system and the proposed system are:

After recognising the smart card, the current system prompts the user to enter the PIN and password. The identity of the user is then authenticated with the assistance of the central authorization system. But the biometric ATM[1] suggested relieves the user to carry the card and to remember the password. The person's fingerprint is acquired by the ATM, and the validation follows like this:

Received 05 March 2021; Accepted 01 April 2021.

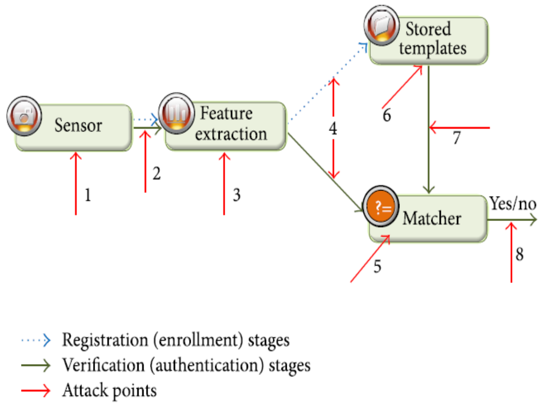


Figure-1. Fingerprint Identification process

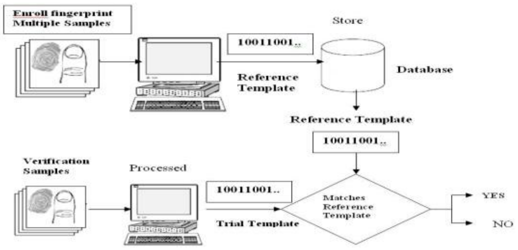


Figure-2. Fingerprint Verification process

The evidence of identity and authentication processes are carried out to validate the client by way of seizing the reside template of the fingerprint.

HARDWARE PROPOSAL:

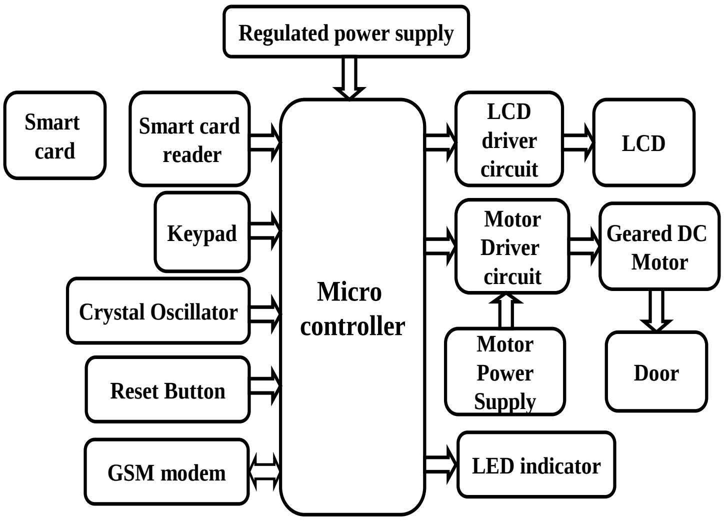
- Alarming module
- SRAM and FLASH
- Fingerprint recognition module
- Ethernet Switch Controller

A Smart card contains extra chip than a magnetic stripe card and it may be programmed for varied applications. Some smart cards can have programming and information to improve more than one programs and a few can also be up to date so as to add novel applications after they are issued. Smart intelligent cards will also be deliberate to be inserted right into a slot and browse through a special reader or to be learn at an hacker point of view. Cards will also be no longer reusable or reloadable.

A trade standard interface between programming and PC hardware in a sensible card has been particular by way of the PC/SC Working Group, on behalf of Microsoft, IBM, Bull, Schlumberger, and different companies. Another standard is called Open Card. There are two main sensible card running systems: Java Card and MULTOS. The proposed device utilises the fingerprint biometric for authentication, cryptography process for confidentiality, and reversible watermarking for the integrity. Basically, the proposed system consists of two stages such as (i) watermark embedding process and (ii) watermark extraction process (SCI) [11].

Received 05 March 2021; Accepted 01 April 2021.

Smart card and GSM based advanced security system



SOFTWARE IMPLEMENTATION

The design of software [3] plays an important role in this type of embedded gadget. The device design consists of three portions. They are:

- Design of main program with function calls
- The initializing ones using oops concepts
- The set of rules of fingerprint recognition

The implementation steps of the instrument in line with the hardware used are as follows:

. Primarily, the Linux kernel and the File gadget user are to be loaded into the principal chip.

. The next step illustrates the system initialization to implement specific process, corresponding to checking ATM gadget, GSM communication module and so forth.

. Thereafter, each and every module is reset to run
instructions

In order to make use of the ATM terminal by the user, the prerequisite is that the user has to get registered with bank so that the user's fingerprint is taken and password is provided to shopper. After all this procedure only, the consumer can get admission to his account.

When a person comes to the ATM terminal to accomplish the transactions, the ATM terminal asks the consumer to enter his password. If the password authentication is sure, then it asks the consumer to enter his fingerprint. After entering the fingerprint, the gadget does the authentication process. The person has to go into his fingerprint within a maximum of 3 times. After exceeding 3 times, if the fingerprint does no longer fits with the original fingerprint, then it mechanically calls the police and it additionally alarms the bank manager as well. In image steganography techniques, the images are used for covert communication [14]. The techniques
like cryptography and steganography can provide security to the transmitted data [12].

The AT77CI04B is the fingerprint tool which is composed of linear sensors during which it captures the fingerprint. The results temporarily saved in the SRAM. Later it uploads to the remote fingerprint data server. The major chip (S3C2440) is used to regulate these types of resulting processes.

In the initialization process, the instrument and hardware units exist. Then a couple of interface modules get began. According to precedence assigned, each module will start executing programs. Primarily the system clock will synchronise, and executes the open interrupt codes and open interrupt calls. Then the system commences in order that every module process is executed properly. At last, the multiple tasks are being attempted by means of the device.

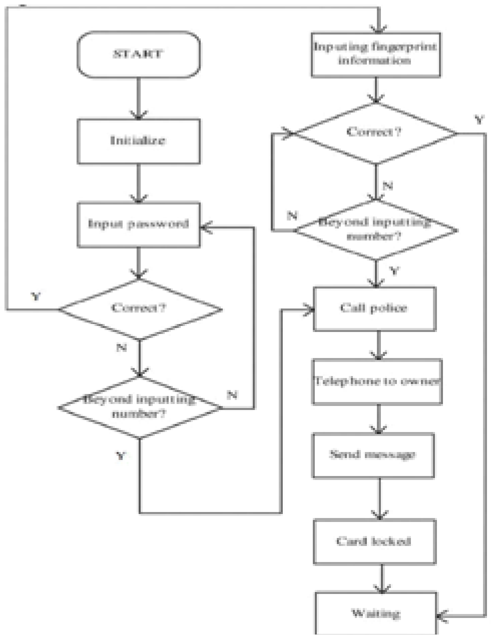


Figure-4. The Flow Chart of the Software

PROS AND CONS OF BIOMETRICAL ATM

There are enormous benefits to the banks and in addition to the purchasers via using card free fingerprint security in ATM. They are:

- The customers need not carry the card for transactions and no necessity to remember in mind passwords.
- Banks can provide environment friendly and well-timed provider for all of its ATM customers and clients.
- Pension recipients can easily obtain their money in a well securable means.
- Some further taxes like gst on the shoppers will probably be lowered.
- Apart of those advantages, there are some disadvantages additionally. They are:
- Sometimes, user's fingers might move dry or wet, tough so that matching process might get failed.
- Image compression techniques are required because fingerprint symbol occupies greater capture area.

CONCLUSIONS

This paper proposed a new technique for amendment of the existing machine of ATM by using fingerprint authentication. Passive and active attacks can be minimized. By imposing this approach of ATM, the fraudulent activities on the user's account can be diminished to a maximum extent so that simplest authenticated user can gain access to his checking account. In future liveness detection techniques can be included so that the authentication is done effectively and get right of entry. Even though the authentication is done and cloud access is granted to the user the data needed to be decrypted in order to get original data [7]. It is essential to build security solutions by adopting a Security Framework for any organization to find solutions for majority of vulnerabilities and flaws [10].

ACKNOWLEDGEMENTS

The author would like to thank everybody, KL University management for providing important amenities to carry out this work.

REFERENCES

[1] Dr.S.R.Suresh —*A Socio-Technical Business Model Using Automatic Teller Machines And Biometrics*‖ IJREISS Volume2,Issue 1, ISSN: 2250-0588.

[2] Pennam Krishnamurthy , M. Maddhusudhan Reddy, *implementation of ATM Security by Using Fingerprint recognition and GSM*‖ IJECCE,Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X ,2012.

[3] Yun Yang, JiaMi, "*ATM terminal design is based on fingerprint recognition*‖,[Volume 1] 2nd International Conference on Computer Engineering and Technology,2010.

[4] Amtul Fatima —*E-Banking Security Issues – Is There A Solution in Biometrics?*‖ Journal of Internet Banking and

Commerce, vol. 16, no.2. August 2011.

[5] Anil K. Jain, Karthik Nandakumar, and Abhishek Naga

[5]—*Biometric Template Security"*EURASIP Journal on Advances in Signal Processing , Article ID 579416, volume 2008.

[6] Manvjeet Kaur,Dr. Sanjeev Sofat, Deepak Saraswat,

—*Template and Database Security in Biometrics Systems: A Challenging Task* ‖IJCA (0975 – 8887)Volume 4 – No.5, July 2010,

[7] Sahithi, S., Anirudh, A., Swaroop, B., Ruth Ramya, K. Biometric security for cloud data using fingerprint and palm print 2019 International Journal of Innovative Technology and Exploring Engineering863383432https://www.scopus.com/inward/record.url?eid=2s2.085069451595&partnerID=40&md5=6a4102e306106fd16731338b23028bd9

[8] Tarannum, A., Rahman, M.D. Multi-modal biometric system using Iris, Face and fingerprint images for high-security application 2019 International Journal of Recent Technology and Engineering 76314320 https://www.scopus.com/inward/record.url?eid=2-s2.085067962719&partnerID=40&md5=b1b1c2acd0ee967c767d7a35cad52cbc

[9] Puvvada, N., Prasad Babu, M.S.Semantic web based banana expert system 2018 International Journal of Mechanical and Production Engineering Research and Development833643713 https://www.scopus.com/inward/record.url?eid=2-s2.085062992172&partnerID=40&md5=3579f6c1ea568fcc5ab66dc77cdd7dd1

[10] Veerapanenic, S.S., Raja Sekhar, K. A systematic study of asset management using hybrid cyber security maturity model 2019 International Journal of Recent Technology and Engineering 76678683https://www.scopus.com/inward/record.url?eid=2s2.085065160274&partnerID=40&md5=ab47677f05cff6ca9f2834f94c41ac1e

[11] Aparna, Puvvadi; Kishore, Polurie Venkata Vijay Biometric-based efficient medical image watermarking in E-healthcare application IET IMAGE PROCESSING FEB 28 2019 13 3 421 428 10.1049/iet-ipr.2018.52886

[12] Sahu, Aditya Kumar; Swain, Gandharba Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis INTERNATIONAL JOURNAL OF ELECTRONIC SECURITY AND DIGITAL FORENSICS 2019 114458476 10.1504/IJESDF.2019.102567

[13] Biometric-based efficient medical image watermarking in E-healthcare application Aparna, P; Kishore, PVV IET IMAGE PROCESSING FEB 28 2019 10.1049/iet-ipr.2018.528864

[14] Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks Pradhan, A; Sekhar, KR; Swain, G SECURITY AND COMMUNICATION NETWORKS 2017 10.1155/2017/19246184

[15] A Dependency analysis for Information Security and Risk Management Krishna, BC; Subrahmanyam, K; Kim, THE INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS AUG 2015 10.14257/ijsia.2015.9.8.17

[16] Bangare, Sunil L.; Pradeepini, G.; Patil, Shrishailappa: a new computational technique for precise medical imaging INTERNATIONAL JOURNAL OF BIOMEDICAL ENGINEERING AND TECHNOLOGY 2018 27 1-2 76 85

AUTHORS PROFILE

Mrs B. Poornima, B.Tech(CSIT), M.Tech(CSE), pursuing her Ph.D. in Koneru Lakshmaiah Education Foundation(KLH Deemed to be University) at Hyderabad. She has teaching experience of 16 years. Presently working as Asst Professor in Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Hyderabad. She has various research papers published in the International Journals of repute. Her research area consists of Image processing, Cyber Security, Digital Forensics, Machine Learning, IoT, AI etc.