www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 09, September 2022, pp : 63-67

e-ISSN : 2583-1062

Impact Factor : 2.265

IMPROVING SECURITY OF ELECTRONIC ATM SYSTEM USING FINGERPRINT IDENTIFICATION AND VERIFICATION

Aashish Regmi[1], Prashant Gurung[2], Shulab Pokharel[3], Steven Gurung[4], Hari K.C.[5]

[1,2,3,4,5]Department of Electronics and Computer Engineering, Pashchimanchal Campus, IOE, TU

Corresponding email: **harikc@wrc.edu.np**

(Orcid: 0000-0003-4816-0428)

ABSTRACT

In this modern world, all the people use ATM machines to withdraw and transfer cash. This research is based on implementing the fingerprint mechanism in the ATM system for the purpose of enhancing the security. To increase safety for all customers to make easy to do the transaction. One of the major drawbacks of the existing authentication scheme in ATMs is the usage of only PIN (Personal Identification Number) as password. But PIN numbers are easily stolen and misused. In order to achieve security and to overcome illegal activities, this research project is developed to enhance better security to ATMs. Here PIN numbers are replaced by biometric security. In Biometric ATMs, fingerprints are used to access the transaction of any ATM system. The Fingerprint minutiae patterns are different for each human being. There is no worry of losing ATM card and no need to carry ATM card with you always. By comparing different technologies that are used for ATM security, it observes that fingerprint technology performs better and safer than other technologies. This makes easy and secure transaction also maintaining user-friendly environment with user and ATM machine. This is most promising technology at electronic money transaction.

Keywords: Enhancing ATM, PIN, Security System for ATM, Biometric Based ATM, Fingerprint, python.

1. INTRODUCTION

Automated Teller Machine (ATM) is a specialized computerized device that makes it convenient to manage a bank account holder's funds. It allows the clients of any financial institution to perform financial transactions like with-draw, view balance, mini statement etc. The change in banking activities include the use of ATMs for banking transactions like cash withdrawal, money transfer and so on. In that ATM system, they introduce CARDS (Credit, Debit, Master, Visa, etc.) to the customer to withdraw cash by using them. Main advantage is quick cash provided by the ATM system. In this paper, the main focus is to develop a better security system by using fingerprint-based ATMs. Biometrics is a technology that helps to make your data extremely secure, unique to all the users by way of their personal physical characteristics. Biometric information is used to identify the people perfectly by using their fingerprint, face, speech, iris, handwriting, or hand geometry and so on.

Using biometric identifiers offers several advantages over traditional and current methods. Tokens such as magnetic stripe cards, smart cards and physical keys, can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party. There are two key functions offered by a biometric system. One technique is identification and the other is verification. Fingerprint technology is highly accepted and matured biometric technology and is

the easiest to develop and for an advanced level of security at the fingertips. It is easy to implement and it takes minimum time and effort to obtain one's fingerprint registered with a fingerprint identification device. Thus, fingerprint recognition is considered the least intrusive of all biometric verification methods. Ancient time's officials used thumbprints to seal documents thousands of years back, and law agencies have been using fingerprint identification since the 1800s. We here carry the same technology on a digital platform. Although fingerprint images are initially captured, the images are not kept anywhere in the system. Instead, the fingerprints converted to templates from the original fingerprints [1].

Problem Statement:

Nowadays, the self-service banking system has wide popularization with the characteristics offering excellent 24 hours service for customers. Using the ATM which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years. It has the disadvantage that smart cards and physical keys can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party. In the existing ATM system, the account

holder will be issued with an ATM card and a private PIN as password provided by the bank. The PIN number will always be an important consideration to protect our financial information. But those PIN numbers can easily be hacked and misused by skimming attack, card trapping and ATM malware. The main need of this system is to enhance the security of ATMs and solve all those above problems which are encountered while using PIN. So, a new authentication system which is based on fingerprints. In this system the banking credentials of any customer along with his/her fingerprint are stored in the server

database. Raspberry pi is used as a key component which is connected with a fingerprint sensor. Then, Raspberry pi communicates with the server and if the fingerprint matches with the server, he can withdraw the amount if he has sufficient money in his bank account.

Objectives:

The objectives of this research project are as follows:

- To enhance existing ATMs security using biometric authentication.
- To save ATMs from being misused and provide safe transactions.

2. LITERATURE REVIEW

The word "biometrics" is derived from the Greek words "bios" and "metric" which means life and measurement respectively [2]. To implement this concept, we have studied different investigated works and found the following data. Most finger scan technologies are based on minutiae. The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger. For fingerprint recognition, a system needs to capture a fingerprint and then follow a certain algorithm for fingerprint matching. This research paper discusses a minutiae detection algorithm to show key parameters of fingerprint image for identification. The maturity of Biometric techniques and generally the dramatic improvement of the captured devices have led to the proposal of fingerprinting in multiple applications but in the last years, minutiae have been the main type of algorithm used. The minutiae are relatively stable and robust to contrast, image resolution and global distortion as compared to another fingerprint representation [3]. Biometric data are separated and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information. They cannot be stolen and used to access personal information to solve the bugs of traditional identification methods. The author designs a new ATM terminal customer recognition system that is used for the core of the microprocessor and an upgraded enhancement algorithm of fingerprint image to intensify the security of bank accounts as well as ATM machines. For image enhancement, the Gabor filter algorithms and direction filter algorithms are used [4]. Miao et al proposed the Gabor filters (GFs) play an important role in the extraction of Gabor features and the enhancement of various types of images. Fingerprint and voice systems have the smallest comparative sizes with eye systems currently the largest [5]. If images of fingerprints are shoddy images, they result in missing features, leading to the degrading performance of the fingerprint system. Hence, it is very important for a fingerprint recognition system to evaluate the quality and validity of the captured fingerprint images. If there is Authentication Failure, then it sends the alert message to the Account holder and Bank [6]. To have a good process of operation for fingerprint matching, depending on the spectral details features two feature reduction algorithms given the Column Principal Component Analysis and the Line Discrete Fourier Transform feature reductions. It can perfectly compress the template size with a reduction rate of 94%. Spectral minutiae fingerprint recognition system shows a matching speed with 125000 comparisons per second on a PC with Intel Pentium D processor 2.80GHz, 1GB of RAM. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information [7]. Fingerprint records usually extend to impressions on the last joint of the fingers and thumb, to the extent that fingerprint cards typically record parts of the lower finger areas of the fingers [8]. Among those new technologies for dealing with payment processing, biometric payment technology has recently attracted more and more attention as a viable solution to decrease identity theft [9].

3. METHODOLOGY

1. System Model

The block diagram of system and flowchart of operation are shown below: -

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 09, September 2022, pp : 63-67

e-ISSN : 2583-1062

Impact Factor : 2.265

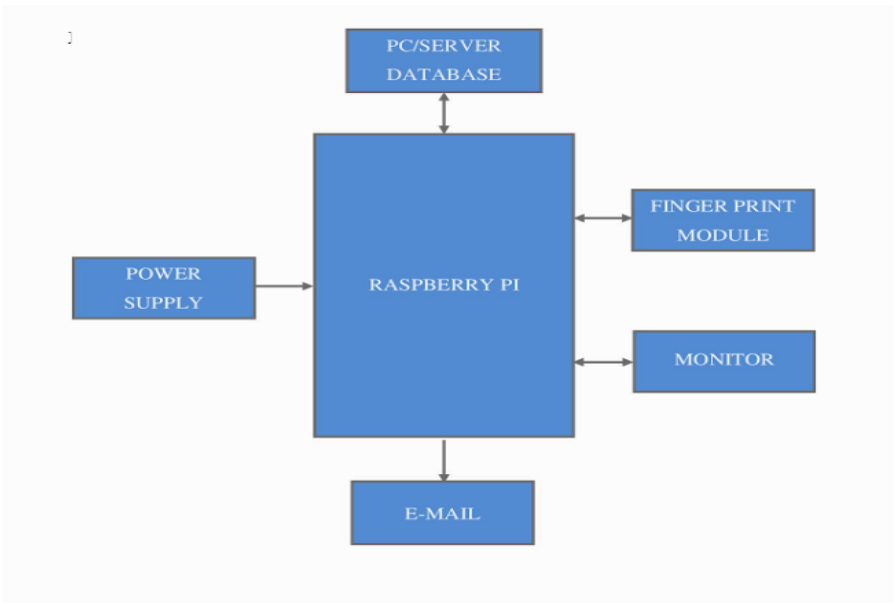

Figure: Block diagram of electronics ATM system

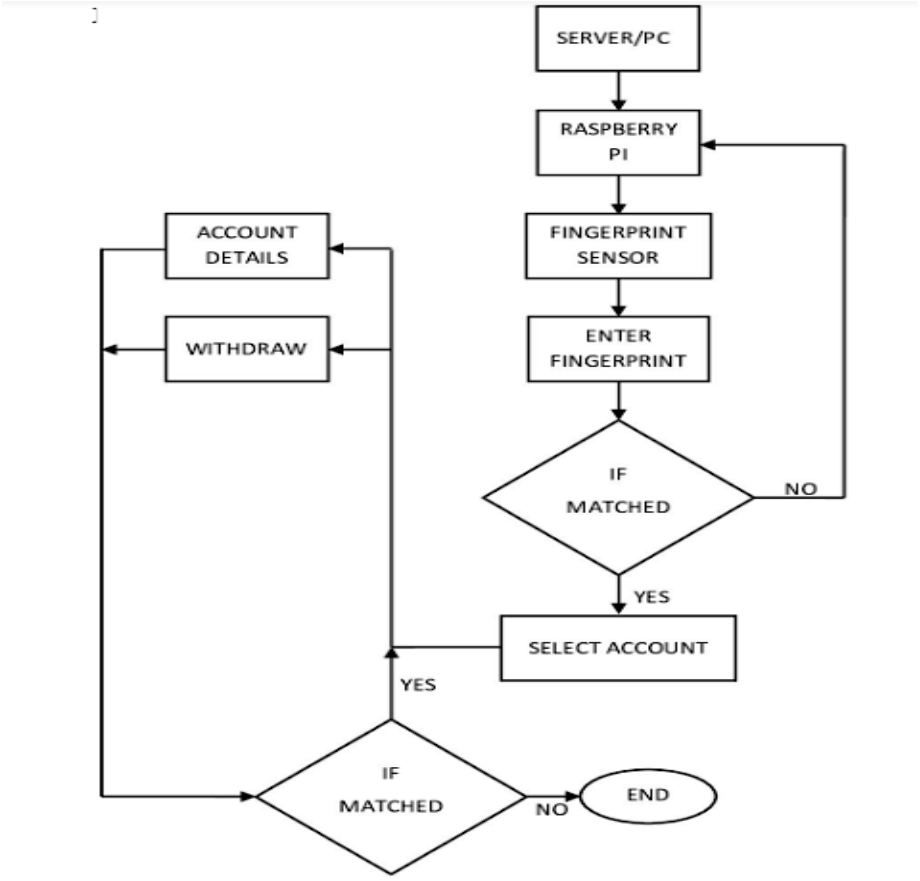

Figure: Flow chart of working of biometric ATM

Hardware's like Raspberry pi, fingerprint sensor, monitor, USB TTL are used whereas in software, Python, Django, SQLite and Tkinter. Sufficient amount of power is supplied to Raspberry pi. Raspberry pi connected with the server database which communicates with the server database using python.

Databases are stored using SQLite. Raspberry pi is then connected with a fingerprint sensor which recognizes the fingerprint of the customer and sends it to the server. After sending to the server, the given fingerprint is checked. Here all this information is displayed on the monitor. If fingerprint authorization is successful then the person can perform his banking transaction according to the information displayed on the monitor.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 02, Issue 09, September 2022, pp : 63-67

e-ISSN : 2583-1062

Impact Factor : 2.265

Transactions performed like checking the remaining amount, withdrawal of deposited money and our savings are sent to email using raspberry pi. For this Django is used. The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. A fingerprint sensor is a type of technology that identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility. It is a type of biometric security technology that utilizes the combination of hardware and software techniques to identify the fingerprint scans of an individual. A fingerprint scanner typically works by first recording fingerprint scans of all

authorized individuals for a particular system or facility. These scans are saved within a database. The user requiring access puts their finger on a hardware scanner, which scans and copies the input from the individual and looks for any similarity within the already-stored scans. If there is a positive match, the individual is granted access. Fingerprint scanners most commonly use an individual thumbprint as identification.

Firstly, need to register his information in server database. Name, contact number, email, account number and fingerprint id will be registered. Then when a person deposits the money, account will be updated. After that the person must keep his finger on the fingerprint sensor. Then the fingerprint sensor scans the fingerprint pattern of te person and sends the scanned fingerprint to Raspberry pi which is connected using USB to TTL. Then the Raspberry pi communicates with the server database and checks if the fingerprint id is matched or not. If it matches then the screen will appear which will allow to perform operations like balance checking, withdrawal, etc. If chooses to show savings then balance amount will be shown and if chooses to withdraw money then a user interface will appear which will allow to take the cash out. After that money will be deducted from the server and mail will be sent to email address.

Figure: Fingerprint ATM homepage.

Figure: Menu of Fingerprint ATM

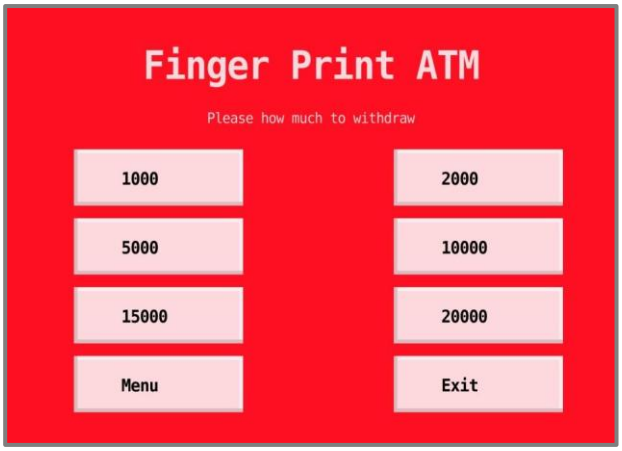

Figure: Option selection for withdraw

Figure: Balance Check

To access the account , one must click on the start and place our finger on the fingerprint sensor. After the fingerprint is read and if it is matched to the stored fingerprint, the screen shows the menu page where the user can choose whether to withdraw money or check balance. The user can select multiple options to withdraw cash. He can withdraw ranging from Rs 1000 to Rs 20000 at a time. For the balance checking one needs to select the option “Check Balance” .

4. RESULT AND ANALYSIS

It has been able to prove that the Biometric ATM is practicable and could be implemented in a real production. Anyone is able to withdraw money by fingerprint. After the money is withdrawn, individual will get notified about the recent transaction via Email on phone. One can also check their savings and see the remaining balance in account from the ATM. On the other hand, in the database, the administrator can insert the customer's name, account number, contact number, E-mail address, Bank balance etc. The administrator can also change the respective information of the customer. To insert new customer's information, they are also asked to insert their fingerprint. Their fingerprints are read by the sensor and stored in the database. If the fingerprint doesn't match then, the user is asked to try again. The advantages of enhancing ATM security using fingerprints are low educated people can access them easily. When ATM card is misplaced then no one uses or can access, it automatically blocks, no one can hack the pin code.

5. CONCLUSION

The main reason for introducing biometric systems is to increase overall security. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. In others it is the only viable approach. Decision-makers need to understand the level of security guaranteed through the use of biometric systems and the difference that can exist between the perception and the reality of the sense provided. The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness.

6. REFERENCES

[1] A.K. Ojha, "ATM Security using Fingerprint Recognition", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, No. 6, pp. 170-175, 2015.

[2] G. Eason, B. Noble and I.N. Sneddon, "On Certain Integrals of Lipschitz-Hankel Type Involving Products of Bessel Functions", Philosophical Transactions of the Royal Society A, Vol. A247, pp. 529-551, 1955.

[3] M.R. Girgis, A.A. Sewisy and R. F. Mansour, "Employing Generic Algorithms for Precise Fingerprint Matching based on Line Extraction'', Graphics, Vision and Image Processing Journal, Vol. 7, No. 1, pp. 51-59, 2007.

[4] Duresuoquian Miao, Qingshi Tang and Wenjie Fu, "Fingerprint Minutiae Extraction Based on Principal Curves", Pattern Recognition Letters, Vol. 28, pp. 2184-2189, 2007

[5] Pranali Ravikant Hatwar and Ravikant B Hatwar, "Bio-Signal based Biometrics Practices", International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

[6] Edmund Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", Available at: https://www.sans.org/reading-room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scannin-1177.

[7] J. Swann, "Teaching Ethics: It's the Right Thing to Do", Available at: https://www.informs.org/ORMS-Today/Archived-Issues/2004/orms-604/Teaching-Ethics-It-s-the-Right-Thing-to-Do.

[8] O.W. Fatai, J.B. Awotunde and O.E. Matluko, "A Novel System of Fingerprint Recognition Approach for Immigration Control", IOSR Journal of Computer Engineering, Vol. 16, No. 3, pp. 39-42, 2014.