ZKG INTERNATIONAL

ISSN: 2366-1313

SMART ATM SYSTEM USING FINGERPRINT MODULE

[1]Mr.k. Koteswara Chary, [2]A. Pavan Kumar, [3]M. Akshay Reddy, [4]P. Gurva Reddy

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

kkchari530@gmail.com

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

pavanpontu@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

akshayreddy1225@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

padigapatigurvareddy2000@gmail.com

Abstract: *In this project we have survey on biometric authentication system. Biometric authentication system is used for various kinds of authentication system instead of the tension of cards to put with them and to memorize their difficult passwords and pin numbers. Biometric authentication system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like credit card payment system, wireless system and mobile system etc. Biometric authentication system is reliable, economical and it has more advantage as compare with others. In daily life the usage of credit cards, check cards for shopping, bus card, subway card for traveling, student card for library and department, and many kinds of cards for unlimited purpose and so on. So problem is that a person has to take many cards and has to remember their password or secret codes and to keep secure to take with it all time. So, the biometric authentication system will solve this problem. Greater adoption of biometric authentication system will drive down the cost of biometric readers and thus making it more affordable to small business owner.*

Keywords*: Enhancing ATM, Security System for ATM, Biometric Base ATM, and Fingerprint Based ATM.*

I. INTRODUCTION

Biometrics is a technology that helps to make your data extremely secure, unique all the users by way of their personal physical characteristics. Biometric information can be used to perfectly identify people by using their fingerprint,

ISSN: 2366-1313

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. In this paper, we are concentrating on identifying and verifying a user by fingerprint recognition. A modern ATM is typically made up of the devices like CPU to control the user interface and devices related to transaction, Magnetic or Chip card reader to identify the customer, PIN Pad, Secure crypto-processor generally within a secure cover, Display to be used by the customer for performing the transaction, Function key buttons, Record Printer to provide the customer with a record of their transaction, to store the parts of the machinery requiring restricted access -Vault , Housing for aesthetics, Sensors and Indicators. Fingerprint technology is the most widely accepted and mature biometric method

Biometric identify people by measuring some aspects of individual anatomy or physiology (such as your hand geometry or finger print), some deeply Ingrained skill, or other behavioral characteristics (such your handwritten signature), or something that is a of the two (such as your voice). Biometric authentication technologies such as face, finger, hand, and iris and speaker recognition are commercially available today and are already in use. Biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquire data, and comparing this feature set against the template set in the database. Depending on the text, a biometric system may operate either in verification mode or identification mode.

Now a day, in the self-service banking system has wide popularization with the characteristic offering excellent 24 hours' service for customer. Using the ATM (Automatic Teller Machine) which provide customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years, Lot of criminals' tamper with the ATM termina and steals user's credit card and password by illegal means. Once User's bankcard is lost and the password stolen, the criminal withdraws all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the

ISSN: 2366-1313

customer becomes the focus in Current financial circle. Traditional ATM systems authenticate generally by using the credit card and the Password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. In Recent years, the algorithm that the fingerprint recognition continuously updated and sending the four-digit code by the Controller which has offered new verification means for us, the original password authentication method combined with The biometric identification technology verify the clients' identity better and achieve the purpose that use of ATM Machines improve the safety effectively.

In our modern world, all the people used to do truncation in banking like deposit money and withdrawing money. For that, the customers will be standing in queue to withdraw money from bank. All the customers felt like waiting for withdraw cash. Therefore, that bank introduces ATM (Automated teller machine) to help the customer to withdraw money quick. In that ATM system, they introduce CARDS (Credit, Debit, master, Visa) to the customer to withdraw cash by using them. Main advantage is quick cash providing by the ATM system. The customer feels happy and they will not waste time to withdraw cash by standing. but it has the disadvantage like, 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. The banks required a better system to maintain security for the customer to do the transaction in their banks. To overcome these problems, the developed this fingerprint based ATM system

II. LITERATURE SURVEY

Most finger print scan technologies are based minutiae. Samir Nanavati states that most finger scan technologies are based on minutiae matching but that pattern matching is a leading alternative. This technology bases its feature extraction and template generation on a series of ridges, as opposed to discrete point. The use of many ridges reduces dependence on minutiae points, which tend to be affected by wear and tear. 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 in byte size. Finger scan technology is proven and capable of high levels of accuracy. This is a long history of fingerprint identification, classification and analysis. This along with distinctive features of fingerprints has set the finger scan apart from other biometric technologies. There are physiological characteristics more distinctive than the

ISSN: 2366-1313

fingerprint such as iris and retina, but automated identification technology capable of leveraging these characteristics have been developed only over the past some years. The technology has grown smaller, more capable and with many solutions available. Devices slightly thicker than a coin and an inch square in size are able to capture and process images. Additionally, some may see the large number of finger scan solutions available today as disadvantages and as advantage by ensuring marketplace completion which has resulted in in a number of robust solutions for desktop, laptop, tablet, physical access and point of sale environments. 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. Current biometric systems are generally inflexible and not optimized for use within an enterprise. Most biometric systems are monolithic, thick-client or standalone applications with very little ability to interface to enterprise management information systems (MISs). Many The word “biometrics” derived from the Greek words “bios” and “metric” which means life and measurement respectively [3]. To implement this concept, we have studied different investigated works and found following data. Most finger-scan technologies 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 fingerprint and then follow certain algorithm for fingerprint matching. This research paper discusses a minutiae detection algorithm to showed 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 other fingerprint representation [4]. Biometric data 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 solving the bugs of traditional identification methods the author of designs a new ATM terminal customer recognition system is used for the core of microprocessor and an upgraded enhancement algorithm of fingerprint

ISSN: 2366-1313

image intensify the security of bank account as well as ATM machine. For image enhancement, the Gabor filter algorithms and direction filter algorithms are used [5]. 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 [6]. If images of fingerprint 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 Authentication Failure then it sends the alert message to the Account holder and Bank [7]. To have good process of operation for fingerprint matching, in 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.

Thus, the biometric market today is continuing a trend towards monopolistic stovepipe systems risking higher prices and less innovation. Small scale, open-source initiatives however demonstrate the opportunity for improving biometric system collaboration and performance through higher quality and modern architectural choices. Our intent with this project is to highlight alternatives for implementing biometric architecture for favourable consideration across an enterprise. This project could become the basis for goals to which an enterprise could subscribe when looking to improve their biometrics-business function capability sets. This could be considered whether an enterprise is updating or upgrading present, existing biometric infrastructure, or is considering a wholesale reconfiguring, re-architecting, or re-implementing of business functions supported by biometric identification capabilities.

III. PROPOSED WORK

The purpose of this project is to document and demonstrate the comparison and trade-off of current systems within their current architecture to like systems supported by a more robust and modern architecture. To enhance the reliability of biometric based ATM systems, we propose that three types of biometrics are used in conjunction for

ISSN: 2366-1313

returning a clear authentication. The user provides at the ATM machine, a fingerprint, eye print and palm print biometrics. These data pass over the network to three different servers and at least two servers must return a clear authentication. This method efficiently fights the hackers and network spyware systems and ensures that the users' resources are safe. Now a day ATM with magnetic strip authenticated only by inserting password on the ATM machine. But according to today's scenario, cases of fraud are another problem. So, they provided fingerprint for more security. Now a days we are directing towards the pile of new powerful, intelligent, auto rated system, which will give us easy to do the work smoothly, thus systems are not dependent on human support, one of these.

The proposal is to use fingerprints in ATMs as passwords involved with the PIN number. Fingerprint recognition will make users relax by preventing unauthorized account access and assuring security. Here, a fingerprint module generates 4-digit code as a message to the customer's assigned mobile number by placing finger on it and on the basis of validation of this code, customers are allowed for further access.

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human hand. A friction ridge is a raised portion of the epidermis on the fingers and toes (digits), the palm of the hand, consisting of one or more connected ridge units of friction ridge skin. Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of user such as pin code and fingerprint matching.

Basically we can explain complete Fingerprint base ATM system in two phases:

1) Enrolment Phase

2) Authentication phase

1. ENROLMENT PHASE:

In the robust fingerprint application, 3-4 fingers should be enrolled. This enables the system to set high security threshold and still be able to cope with everyday real life issue like skewed finger placement dirty, wet dry, cut or worn fingers. Biometric reference data is collected enrolment and stored in database or in portable data carrier such Fig: Enrolment Phase The Enrolment is crucial because the once recorded reference data will normally be used over the active lifetime of user or his/her biometric hardware device. Multiple Finger enrolment: It is

ISSN: 2366-1313

strongly recommended enrolling more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts not affect a robust sized sensor system

AUTHENTICATION PHASE

In these phase user can make transaction by using their fingers. User can place finger on the Biometric scanner and user's finger scan can be matched through database, where all authenticated user ' s fingerprints are stored. If User wants to do transaction, they simply place their finger on biometric scanner and get their money in few seconds. If user's fingerprint cannot be matched by database due to some accidental cuts on their fingers than they can used their other fingers and we will also provide a 4-pin code option, user can also use this option with their convinces. Feature extraction: Feature extraction from a fingerprint image is generally categorized into three levels. Feature can used to categorize into major pattern type such as loop or whorl. The main objective of this system is to develop a system that will increase the ATM security. However, despite the numerous advantages of ATM system, ATM fraud has recently become more widespread. In recent years, biometric authentication has grown in popularity as a means of personal identification in ATM authentication system

ATM SECURITY SYSTEM

which we recent advance in biometric identification techniques, retina scanning, including fingerprinting, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This research investigated the development of a scheme that integrates facial recognition technology into the verification process used in ATMs.

An ATM system that is reliable in providing more security by using facial recognition is proposed. The development of such a scheme would help to protect clients & financial institutions alike from intruders and identity thieves. This paper concentrates on an ATM security system that would combine a physical access card, a Personal Identification Number, & electronic facial recognition that will go as far as withholding the fraudster ' s card. Nevertheless, it's obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts. The combined biometric features approach is to serve the

ISSN: 2366-1313

purpose both the identification and authentication that card and PIN do.

SYSTEM ARCHITECTURE

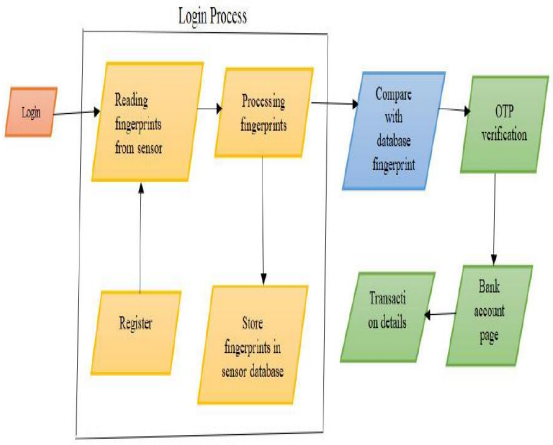

Fig.1 System architecture

5.1 Modules Used in Project :-

1. TKINTER
2. RANDOM MODULE
3. SERIAL MODULE
4. PIL MODULE
5. FINGERPRINT MODULE
6. GSM MODULE

TKINTER:

Tkinter is the inbuilt python module that is used to create GUI applications. It is one of the most commonly used modules for creating GUI applications in Python as it is simple and easy to work with. You don't need to worry about the installation of the Tkinter module separately as it comes with Python already. It gives an object-oriented interface to the Tk GUI toolkit. Some other Python Libraries available for creating our own GUI applications are

- Kivy
- Python Qt
- wxPython

Among all Tkinter is most widely used.

RANDOM MODULE:

Python Random module is an in-built module of Python which is used to generate random numbers. These are pseudo-random numbers means these are not truly random. This module can be used to perform random actions such as generating random numbers, print random a value for a list or string, etc.

SERIAL MODULE:

This module encapsulates the access for the serial port. It provides backends for python running on Windows, OSX, Linux, BSD (possibly any POSIX compliant system) and IronPython. The module named "serial" automatically selects the appropriate backend.

PIL MODULE:

Python Imaging Library (expansion of PIL) is the de facto image processing package for Python language. It incorporates lightweight image processing tools that aids in editing, creating and saving images.

ISSN: 2366-1313

Support for Python Imaging Library got discontinued in 2011, but a project named pillow forked the original PIL project and added Python3.x support to it. Pillow was announced as a replacement for PIL for future usage. Pillow supports a large number of image file formats including BMP, PNG, JPEG, and TIFF. The library encourages adding support for newer formats in the library by creating new file decoders.

FINGERPRINT MODULE:

What is the Fingerprint Sensor?

The fingerprint sensor is one kind of sensor which is used in a fingerprint detection device. These devices are mainly inbuilt in the fingerprint detection module and it is used for computer safety. The main features of this device mainly include accuracy, better performance, robustness based on exclusive fingerprint biometric technology. Both fingerprint scanner otherwise reader are an extremely safe & suitable device for safety instead of a secret word. Because the password is easy to scan and also it is hard to keep in mind.

Fig.2 Fingerprint module

So, better to use USB based fingerprint reader or scanner using biometric software for verification, identification, and authentication, that allow your fingerprints to perform similar to digital passwords. These passwords cannot be forgotten, lost otherwise stolen.

R305 Fingerprint Sensor Module

There are different types of fingerprint modules available in the market like R305, R307. For a better understanding of this sensor, here we are going to discuss an overview of R305 fingerprint sensor module.

ISSN: 2366-1313

Fig.3 R305-fingerprint-sensor-module

The R305 is one kind of fingerprint sensor module used in biometrics for security in fingerprint detection as well as verification. These devices are mainly used in safes where there is a high-powered DSP chip used in the rendering of image, feature-finding, searching and calculation by connecting it to any microcontroller with the help of TTL serial, & send data packets to get photos, notice prints, search and hash. The enrolment of new fingers can be stored directly within the flash memory of on board. Features of Fingerprint Sensor.

Fingerprint Sensor Working Principle

The working principle of the fingerprint sensor mainly depends on the processing. The fingerprint processing mainly includes two elements namely enrollment and matching. In fingerprint enrolling, every user requires to place the finger twice. So that the system will check the finger images to process as well as to generate a pattern of the finger and it will be stored. When matching, a user places the finger using an optical sensor then the system will produce a pattern of the finger & compares it with the finger library templates. For 1:1 fingerprint matching, the system will evaluate the exits finger with a precise pattern which is selected within the module. Similarly, for 1: N matching, the scanning system will look for the complete finger records for the finger matching. In both situations, the scanning system will go back to the corresponding result, success otherwise crash.

IV. RESULTS

Run the program of FINGER SENSOR MODULE by connecting GSM and Fingerprint Sensor

ISSN: 2366-1313

Fig.4 The above screen appears after running the program. Now enter the Admin Credentials like USERNAME and PASSWORD then click on SUBMIT to move to the next screen.

Fig.5 The above screen appears after successful login of admin. Now if you are a new user then need to register and if you are a existing user then you should directly click on login.

Fig.6 If you click on REGISTER the above screen appears ,here you need to add your mobile number and then add your fingerprint by placing your finger on fingerprint sensor.

ISSN: 2366-1313

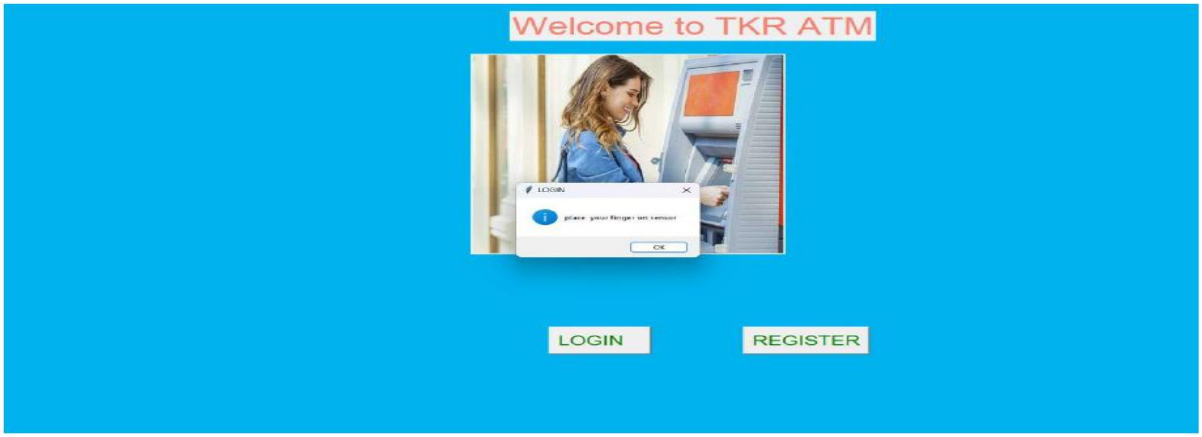

Fig.7 Now if you click on LOGIN icon the above pop-up message appears as please place your finger on sensor

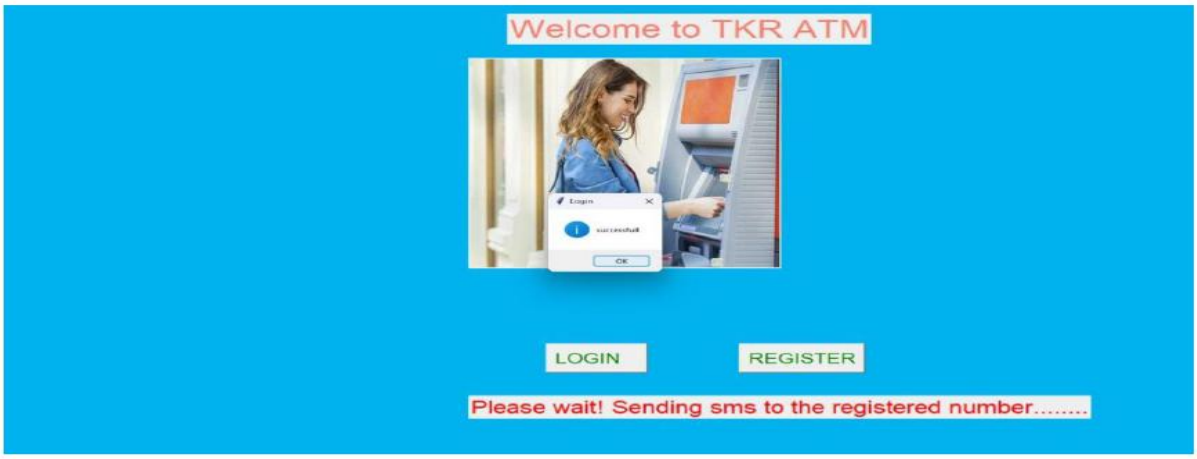

Fig.8 After placing finger on sensor the succesful pop-up message appears on screen and at bottom of screen “Please wait! Sending sms to registered mobile number” appears

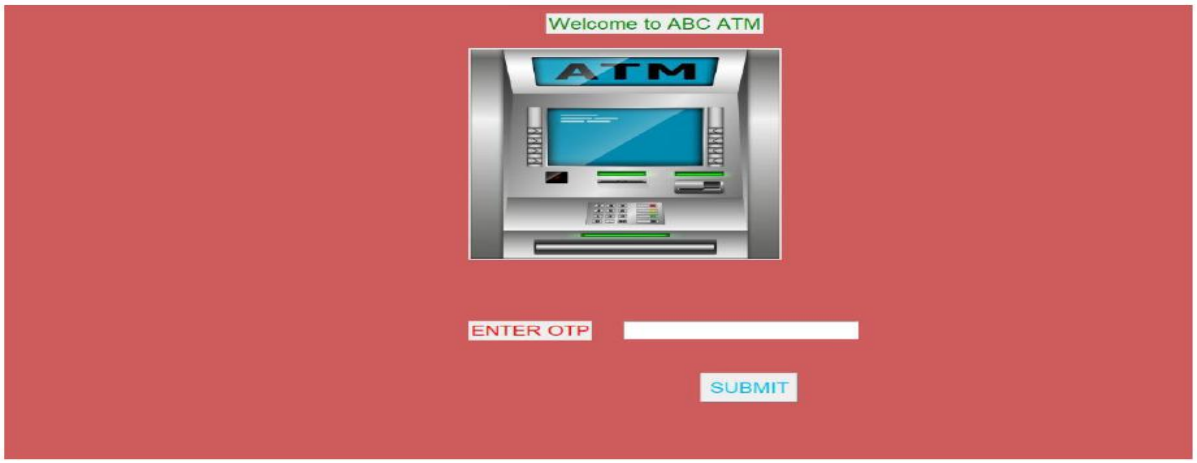

Fig.9 After Successful sent of OTP the above screen appears so as to validate your OTP and then click on SUBMIT button.

ISSN: 2366-1313

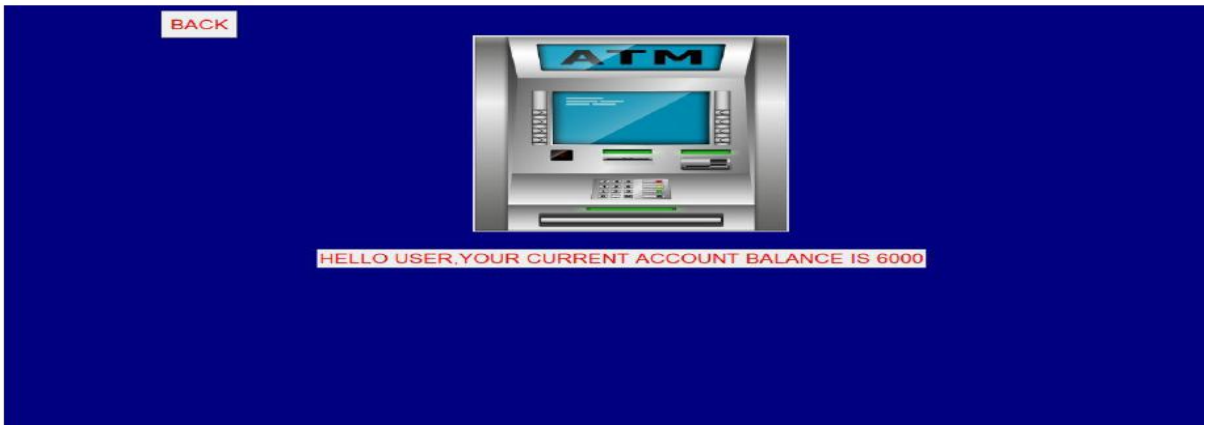

Fig.10 By clicking on "balance enquiry" tab the above screen appears to show the user his/her current account balance

Fig.11 By clicking on "Debit amount" tab the above page opens , and here user need to enter amount he/she willing to debit and then click on "Submit" button

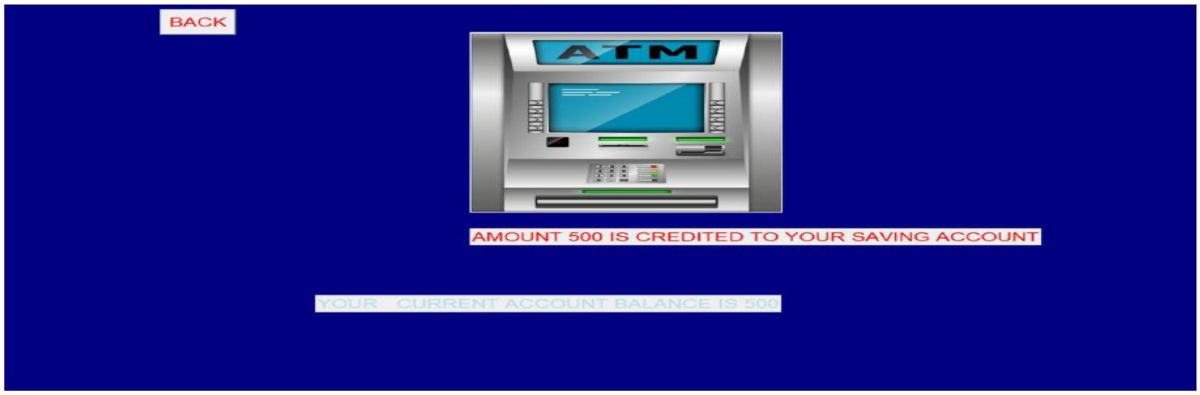

Fig.12 After Successful Credit of amount in user account the above page appears as how much amount is credited and the current balance of the account will be displayed.

ISSN: 2366-1313

V. CONCLUSION

ATM machine increase the reliability of the bank organization by providing the easy access to the cash transaction. We can withdraw the cash anywhere and anytime without waiting in queue. Hence, ATM card is used wildly but we have to face the fraud related to the ATM transaction. To make ATM transaction more secure we are using biometric scanning machine to identify the account holder. Finger is unique identity of each person so the use of Biometric Fingerprint scanner we can avoid ATM related fraud. The Security feature enhanced stability and reliability of owner recognition. The whole system designed by using technology of embedded system which makes the system more secure, reliable and easy to use. The Implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additionally, the system also contains the original verifying methods which was inputting owner's password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on technology. In the present days it is being used for computer network access and entry devices for building door locks. Fingerprint readers are being used by banks for ATM authorization and are becoming more common at grocery stores where they are utilized to automatically recognize a registered customer and bill their credit card or debit account. Finger-scanning technology is being used in a novel way at some places where cafeteria purchases are supported by a federal subsidized meal program. The system can be extended using a GSM module. The GSM module sends alert messages to the respective authorities when unauthorized person " s finger print is detected.

REFERENCES

1. Pranali Ravikant Hatwar and Ravikant B Hatwar, BioSignal based Biometric Practices, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

2. Edmund Spinella, Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, on/biometric scanning technologies- finger-facial-retinal-sca nning-1177.

3. Gu J, Zhou J, Zhang D.A combination model for orientation field of fingerprints. Pattern Recognition, 2004, 37:543-553.

4. Selvaraj and G. Sekar, A Method to enhance the Safety Level of the ATM banking industry using AES Algorithm,

ISSN: 2366-1313

International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010

5. Haldorai and A. Ramu, Security and channel noise management in cognitive radio networks, Computers & Electrical Engineering, vol. 87, p. 106784, Oct. 2020. doi:10.1016/j.compeleceng.2020.106784.

6. A. Haldorai and A. Ramu, Canonical Correlation Analysis Based Hyper Basis Feedforward Neural Network Classification for Urban Sustainability, Neural Processing Letters, Aug. 2020. doi:10.1007/s11063-020-10327-3.

7. Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation [J]. . IEEE Transactions on Pattern Analysis and Machine intelligence. 1998,20(8):777-789.

8. ESaatci, V Tavsanogh. Fingerprint image enhancement using CNN gabor-Cpe filter[C].Proceedings of the 7th IEEE International Workshop on Cellular Neural Networks and their Applications 2002: 377-382.

9. Cheng J, Tian J. Fingerprint enhancement with dyadic scale-space. Pattern Recognition Letters,2004, 25(11): 1273-1284.

10. Salil Prabhakar, Anil Jain: "Fingerprint Identification" Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

11. Prasadu Peddi (2019), "Data Pull out and facts unearthing in biological Databases", International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.