IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 8, Issue 5, October - November 2020
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Internet on Things Based VBS

V.SWATHI[1], P.KAVITHA[2], P.RANI[3]
[1]Research Scholar, CMR Engineering College,
[2] Assistant Professor, CMR Engineering College,

ABSTRACT:
A wide variety of system needs reliable personal recognition system to either authorize or determine the identity of an individual demanding their services. The goal of such systems is to warrant that the rendered services are accessed only by a genuine user and no one else. In this project, we proposed a multifactor (OTP and fingerprint) based authentication security arrangements to enhance the security and safety of virtual banking and its users. For example, Automated Teller Machine (ATM)'s now a day are extensively used all over the world for the withdrawal of cash. But there is a number of disadvantages to these machines. Frauds attacking the automated teller machine has increased over the decade which has motivated us to use the biometrics for personal identification to procure high level of security and accuracy. This project describes a system that replaces the ATM cards and PINs by the physiological biometric fingerprint scanner. Moreover, the feature of the one-time password (OTP) imparts privacy to the users and emancipates him/her from recalling PINs. One Time Password (OTP) is sent to the user registration mobile number through GSM Module system. After that, the user will be able to complete the transaction securely.
Key words:GSM,ATM.

INTRODUCTION:
This project aims at designing and developing biometric finger print technology[3] based money transaction system for shopping. As more global financial activity becomes digitally- based, banks are utilizing new technologies to develop next-generation identification controls to combat fraud, make transactions more secure, and enhance the customer experience.

The sensor is a solid-state fingerprint sensor that reliably captures fingerprint information. It is designed to integrate into devices for improved security and convenience. The sensor provides a reliable, quick and user-friendly alternative to passwords, PIN's and other forms of user authentication. User need not carry any physical cards (credit, debit etc.) or mobile phones for money transaction. User just need to keep finger print enter transaction amount using keypad. This transaction information is sent to server over secure IoT (WiFi) and further processing done there. If the transaction is successful then user gets SMS confirmation message to his registered phone number.This onboard computer consists of number of input and output ports. The onboard computer is commonly termed as micro controller. The input and output port of the micro controller are interfaced with different input and output modules depending on the requirements. In other words micro controller acts as a communication medium for all the modules involved in the project.The device also consists of GSM modem, WiFi modules, Keypad, LCD which displays the information about transactions.

EXISTING SYSTEM

RFID based transaction
In this system, we provide inbuild programmed unique pin for every user. When the user RFid is scanned by the machine, the system will verify the respective user on bases of the unique code. The unique code has to be typed by the user. If the code entered by the user is matched with the pre-programmed code, the system will allow transaction.

RFID &GSM based transaction

In this system, we provide GSM [6] based security. when ATM user Insert the ATM in ATM machine [1], he can type the password and second, then message goes through card holder via GSM then card holder can send the security code or OTP using GSM through main system and start the transaction via card holder. When we lost the ATM card then in second case card holder cannot send the security code and stop the transaction and he directly block the card using GSM system.

PROPOSEDSYSTEM:

The main objective of this system is to propose a system, which is used for ATM[1] security applications. Here Bankers will collect the customer finger prints and mobile number while opening the accounts then customer can access the ATM machine. The finger prints of respective user along with his mobile number is stored in the data base. When the customer enters ATM, he must place finger on the finger print module then he get automatically generated 4-digit code every time as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the touch screen, after only that he will be able for further transaction. This proposal will go a long way to solve the problem of account safety.

BLOCK DIAGRAM

In this chapter the block diagram of the project and design aspect of independent modules are considered. Block diagram is shown in fig.

FIG 1 :Block diagram of Virtual banking system using IOT

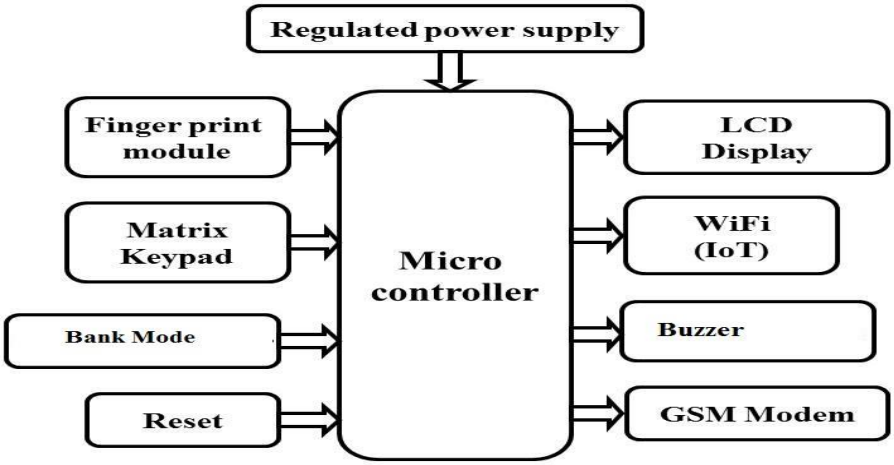
METHODOLOGY OF THE PROJECT

Data storage

In this step, the main operation performed is to obtain finger prints of the respective users along with their mobile number. The obtained data i.e. finger prints and mobile number is stored in the system for future matching operation. In general, vast number of users will be registered in particular bank. So, the data is mostly stored in the data base, so that the memory requirement can be efficiently utilized.

Initially the finger prints of the respective user is stored. This is done by obtaining two images from the finger print module. This phase of the process is called "Fingerprint Enrollment." When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. This templet is used in future operation for matching. The mobile number which is taken from the user will be stored as a number or string in the program which is pre-programmed in the micro-controller.

Data authentication



In this stage of authentication, the operation performed to identify the individual user and process the transaction if the authentication of the user is successfully completed. Initially the user have to place his finger on the optical sensor of the finger print module. The module will generate a templet from the user finger print image. So, the obtained templet is then compared with already stored finger print templet of the user. In general this process is called matching process. The finger print module performs matching operation for 1:1 templets if there is only one identification templet is given. This type of matching is used for very high secured systems where only one user has access to the system. However, in banking systems mass number of users are found. In this case, the module performs matching operation for 1:N templets. Here N is the total number of templets available in the fingerprint library. In both circumstances, system will return the matching result, success or failure.After matching, the mobile number which is associated with the matched fingerprint templet will be used to send an One Time Password(OTP) through GSM module. The generated OTP is stored in the system and is valid for few seconds which is programmed in the micro-controller. The user have to enter the OTP which is received using the 4x4 matrix keypad of the system. The input taken from the keypad is then compared with the OTP which is stored in the system. If they match, then the system will display the amount available in the user's account on LCD display. Now, the user have to enter the amount he would like to withdraw. If the funds available are less than or equal to the amount user entered then the transaction is processed accordingly. The account ummary of the user's account will be displayed on the LCD display followed by a SMS stating the transaction information of the user's account to the registered mobile number through GSM module.

In case of unavailability of the input fingerprint templet or entering the wrong OTP or entering withdrawal amount greater than the available funds in the account will lead to termination of the process and will automatically restart the process.

UPDATING THROUGH IOT:

Initially the micro-controller is connected to the internet through Wi-Fi module. In the system, after the transaction is completed by the user, the controller will update the account summary of the respective user's account in the webpage. So that the user can monitor or get knowledge about the transactions made through his account anytime by connect to the web.

RESULTS:

Fig 2: Output of the project

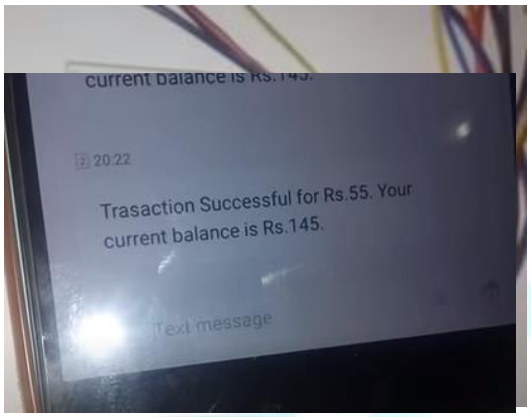


Fig:3 Virtual banking

CONCLUSION:

Integrating features of all the hardware components used have been developed in it. Presence of every module has been reasoned out and placed carefully, thus contributing to the best working of the unit. Secondly, using highly advanced IC's with the help of growing technology, the project has been successfully implemented. Thus the project has been successfully designed and tested.

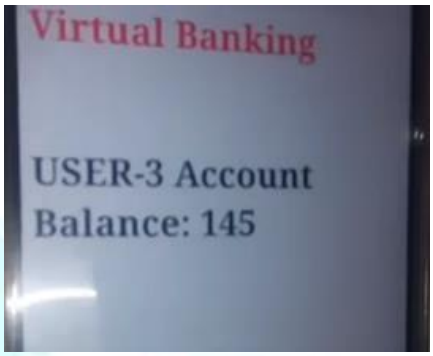
REFERENCES

1. P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

2. N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

3. Ms. Archana S. Shinde and Prof. Varsha Bendre, "An Embedded Fingerprint Authentication System", 2015 International Conference on Computing Communication Control and Automation, 978-1-4799-6892-3/15 $31.00 © 2015 IEEE DOI 10.1109/ICCUBEA.2015.45

4. RishigeshMurugesh, "ADVANCED BIOMETRIC ATM MACHINE WITH AES 256 AND STEGANOGRAPHY IMPLEMENTATION", IEEE-Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012, 978-1-4673-5584-1/12/$31.00©2012 IEEE.



5. R. Priya, V. Tamilselvi, G.P.Rameshkumar, "A Novel algorithm for Secure Internet Banking with finger print recognition", International Conference on Embedded Systems - (ICES 2014).

6. T.N.S.Pallavadhar and V.Srinivas, "ATM Security using GSM and Fingerprint with Authorized Permission for Transaction", International Journal of Emerging Engineering Research and Technology Vol. 3, Issue 11, November 2015, pp. 86-91.

7. Moses OkechukwuOnyesolu and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, pp. 68-72.

8. Chaitali Bhosale, Pooja Dere, Chaitali Jadhav, "ATM security using face and fingerprint

9. recognition", International Journal of Research in Engineering, Technology and Science, Vol. VII, Special Issue, Feb 2017.