Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5, May-2018

BioAura Based Continuous Authentication for Bank Locker Security System Using Raspberry Pi

Kuchipudi Pravallika[1], Yellamati Ratna Babu[2]

[1]*M.Tech Student, ECE Dept, Vignan's Lara Institute of Technology & Science, Vadlamudi, Guntur, India*
[2]*Assistant Professor, ECE Dept, Vignan's Lara Institute of Technology & Science, Vadlamudi, Guntur, India*

*Abstract —**Now a day's, banking system is required to incorporate more security features. Banks are one of themost secured places to keep our valuable things the technologies like Biometrics, RFID, GSM and Iris recognition are being used in banking for locker security purpose. Still the problems are arising with an authorized access of lockers. To modify this problem, a method is proposed in this project, by the implementation of Continuous Authentication depend on customer BioAura.Depend upon the BioAuro this system authenticates user and ensemble the biomedical signal streams that are collected continuously and non-invasively using wearable medical devices (WMS). Here each signal is not discriminative of itself but by demonstrate the collection signals with robust machine learning can provide high accuracy levels. This system is very useful for highly secure systems like the bank lockers and other important applications. Here the Heart Rate values are recorded and saved and authentication is provided on the basis of the recorded data and in case the system fails to work due to physical/emotional changes in the BioAura values it additionally has a biometric authentication system.***

Keywords-BiAura; continuous authentication; finger print scanner; machine learning

I. INTRODUCTION

In this present scenario, safety has become an essential issue for most of the people in the society. Increase in anti-social activities is a cause of concern as the banks are considered soft targets by the criminal. The security arrangements have increased a lot by Increasing incidents of crimes against banks and various Guide lines are followed by the banks. The crime scenario demands the compatible, efficient and reliable security and safety measures to overcome this type of frauds, authentication of the person who wants to use the locker is very important. In the ubiquitous network, society the people faced with risk to transform information because the Individuals can easily access their information anytime and anywhere. For personal identification passwords, Personal Identification Numbers and cards are used. But the cards can be stolen, and passwords and numbers can be guessed.

Recently, wearable medical sensors (WMSs) measures biomedical signals like heart rate, blood pressure, and body temperature. All these have drawn a lot of attention from researchers and begun to be adopted in practice [1][2]. In 2015 a recent report by Business Insider [3] claims that 33 million wearable health monitoring devices were sold. It forecasts number will reach 148 million by 2019 then it continues to grow rapidly thereafter. So the biomedical signals that are collected for health monitoring purposes will be used to aid authentication.

In this project a device with high level security for the bank lockers by continuously collecting the ECG values and biometric values of the user and stored in the processor.Basically, there are three reasons for the user verification and identification of continuously collected biomedical data. The three reasons are discussed below. First, the biomedical signals that are collected from WMSs for the purpose of medical uses. But there is no requirement of another device because it is already connected on the body. Second, one is the information is collected transparently from the user. Third, unlike traditional biometrics/ behaviometrics, e.g., the stream of biomedical signals collected by WMSs is always available and the face features andkeystroke patterns,information that may frequently become unavailable. Whenever the user wishes to access his/her locker the data will be compared with the stored data. If the data is matched the locker will be opened else the buzzer will alert the authorities that someone is going to access the locker.

II. EXISTING SYSTEM

In existing system, a system with security for prohibited areas using iris recognition and detection, fingerprint recognition and detection and one time password (OTP) to display recognized person information and this access the control of the person [4]. In this there is a drawback that the Iris recognition systems make use of low-cost cameras that are commonly built into most laptops. They are accurate when the user looks straight at the webcam. However, their performance is affected significantly by illumination pose, expression or changes in the image acquisition method [5] and also the OTP is hacked when the network is not secured.

III. PROPOSED SYSTEM

In proposed system, the hardware architecture consists of Raspberry Pi which is the main part of entire hardware architecture used for storing the heart rate values and the finger prints. We consider sensors such as ECG Shield and Fingerprint sensors. The ECG Shield is connected to the arduino. From the ECG shield heart rate values of 150 samples are collected continuously and non-invasively using the wearable medical devices. Here each signal is not discriminative of itself but by demonstrating the collection of signals with robust machine learning, can provide high accuracy levels. We demonstrate the feasibility of CABA [6] through the analysis of traces form the data sheet. Before allowing the customer to access the allotted locker, first the Finger Print values of the corresponding user are collected and stored in the template number which is provided by the fingerprint module and that template number is taken as the user ID number and then the ECG values are collected and stored in that user ID. When a person wishes to access his/her locker in the bank then he has to use the WMS so that the values are collected from the user and the system will compare the collected values with the stored data in the Raspberry pi processor. If the collected values are matched then the locker is enabled else the buzzer beeps and alert the authorities.

3.1Block Diagram

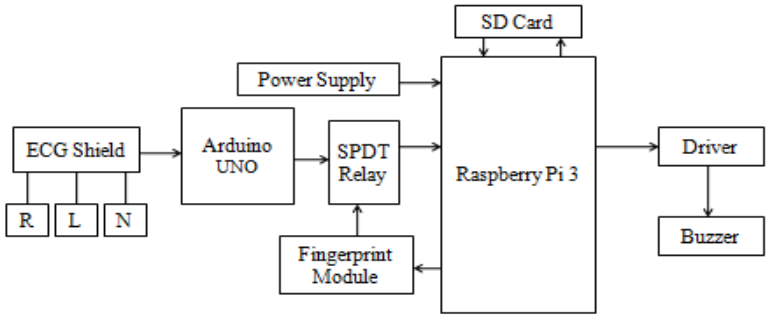

Fig 1.The block diagram of proposed system

In above figure power supply is connected to the processor that is Raspberry pi processor which is the heart of the project. ECG shield collects the values of the customers who are willing to create a locker from the bank. The fingerprint module also captures the image of the customers and create a template to store that captured image. Raspberry pi take those ECG and the fingerprint values and is stored in the memory.

The hardware implementation includes ECG shield for collecting the values of the customer, arduino uno used for converting the ECG values into the digital format, fingerprint module for capturing the image of the fingerprint, SPDT relay for switching the arduino and the fingerprint module and the buzzer-to buzz at set time. The main controller unit is raspberry pi. The software platform used in raspbian(Linux OS), Arduino IDE ,Python programming language and the embedded C language and the SVM library and the pickle library.

3.2 Working Principle

The working procedure starts with First step, the data of the customers fingerprint and the ECG values are stored and maintained a data set. In this step first the finger print value of the customer is captured and generate a image which is in ascii format. The captured image is converted into the template format which is in hexa decimal format using the hexlify library and then it is stored in the ID which is given by the fingerprint module. From the ECG shield 150 samples are collected which is in analog format. The analog data is converted into the digital format by using the arduino uno board for the data base creation by importing the pickle library.

In the second step the data is trained by using Machine Learning technique. In machine learning SVM algorithm is used for loading the data and training by importing the SVM libraries. For ECG data storage we import CSV file. In the third step after data enroll and training we have to search for the stored data which means prediction. At the time of prediction first the ECG values of 450 samples are collected and the finger print is collected. Here in the prediction time we have collected more samples compared to the samples collected at the time of enrollment, so that there will be more accurate chance of matching the ECG values [7]. If the data that is collected is matched to that of the stored ECG values then the locker is enabled, means the locker is opened. If the data that is collected is not matched to that of the stored data then the

buzzer beeps and alert the authority that the unauthorized person is going to access the locker. Once the user is valid then it will show the user ID no and the login time of the user. If the user is not valid then it shows invalid user.

3.3 Flow Chart

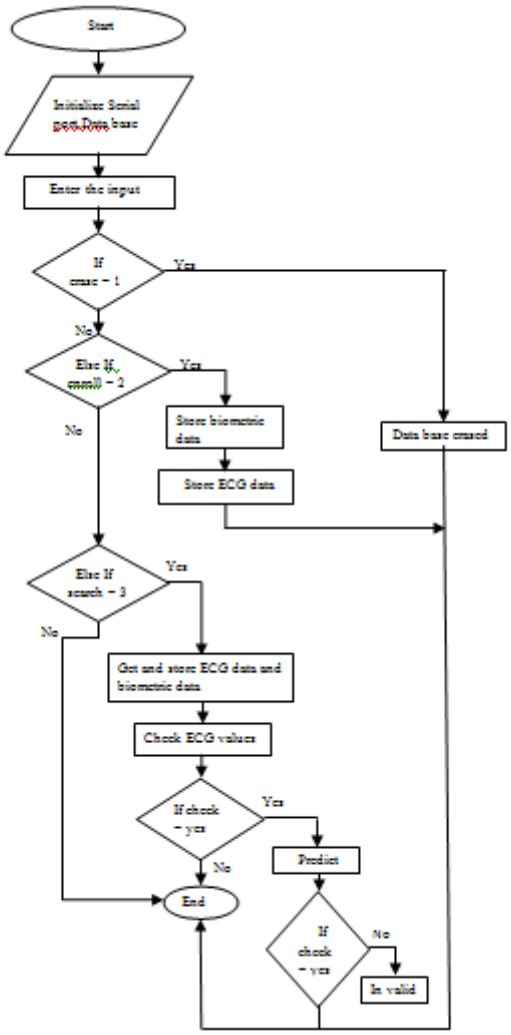

Fig. 2. Flow chart

IV. RESULTS

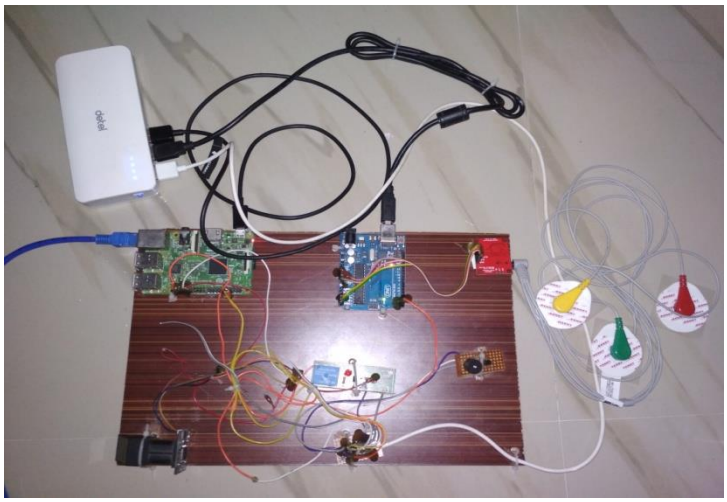

Fig .3. Hardware Implementation

The above Fig.2 shows the Hardware Implementation for the BioAura based Continuous Authentication for bank lockers

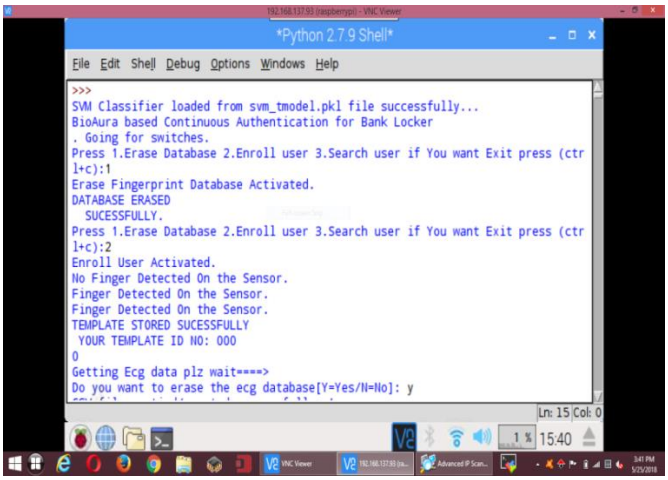

Fig .4. Data Enrollment

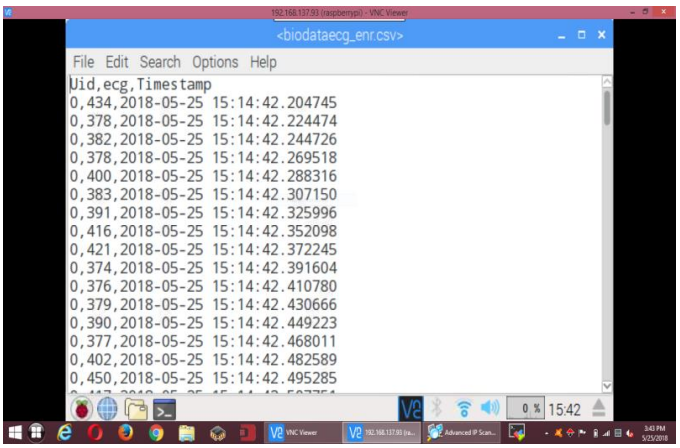

Fig .5. Data base created

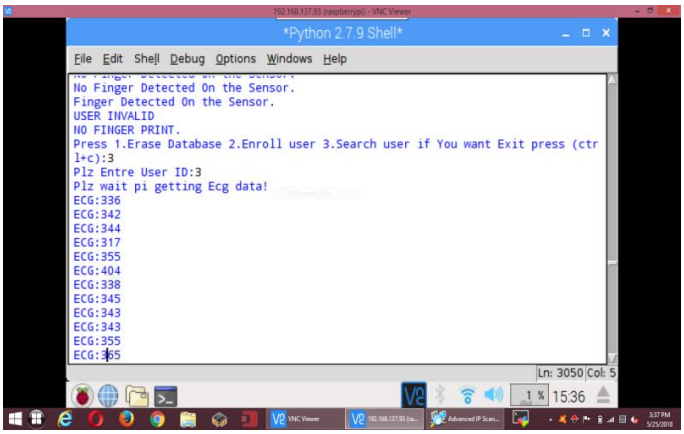

Fig .6. Data Prediction

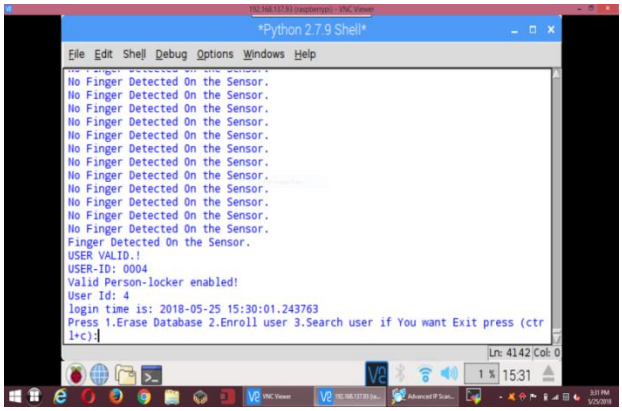

Fig .7. Final output

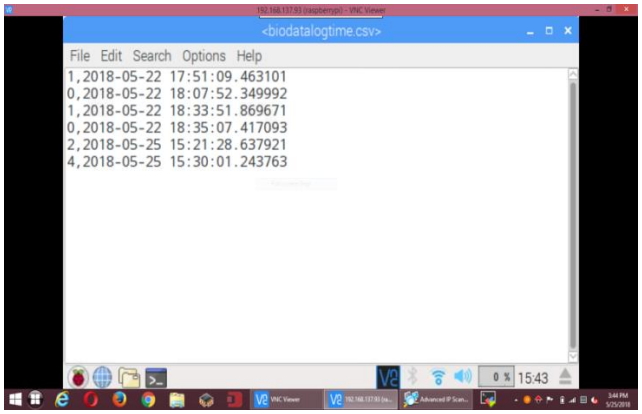

Fig .8. Valid User ID and Login time details

V. CONCLUSION

A prototype of wearable sensors based system is implemented in order to provide authentication to banking systems. Our study tells that the use of ECG Shield and other biomoetric sensors used along with machine learning algorithms is very useful for securing the systems which need high security. For users, the unit is easy to operate. They need neither prior training nor do they need to remember passwords and user ids. It provides more security than the previous methods present as it is difficult to decode the system. Our future endeavor would be making the system compact, inexpensive and energy-efficient.

REFERENCES

[1] *A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensorbased systems for health monitoring and prognosis," IEEE Trans. Systems, Man, and Cybernetics, vol. 40, no. 1*, pp. 1–12, 2010.

[2]*R. Gravina, P. Alinia, H. Ghasemzadeh, and G. Fortino, "Multi-sensor fusion in body sensor networks: State-of-the art and research challenges," Information Fusion, vol. 35*, pp. 68–80, 2017.

[3] *"Growth trends, consumer attitudes, and why smartwatches will dominate," http://www.businessinsider.com/the-wearable-computing-marketreport*-2014-10, accessed: 08-1-2015.
[4] *Prof.K.D.Mahajan, SharvariTatwawadi, Ayesha Shaikh, RashmiShewatkar " Biometrics Based Security System For Bank Lockers With OTP Support" International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 6, Issue 4*, April 2017.
[5*] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," Proc. SPIE Defense Secur. Sensing, vol. 7667*,2010, Art. no. 76670L.
[6] *Arsalan Mosenia, Student Member, IEEE, Susmita Sur-Kolay, Senior Member, IEEE, Anand Raghunathan, Fellow, IEEE, and Niraj K. Jha, Fellow, IEEE "CABA: Continuous Authentication Based on BioAura" IEEE TRANSACTIONS ON COMPUTERS, VOL. 66, NO. 5*, MAY 2017
[7] S. S. Mehta, and N. S. Lingayat "Support Vector Machine for Cardiac Beat Detection in Single Lead Electrocardiogram" IAENG International Journal of Applied Mathematics, 36:2, IJAM_36_2_4.