International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 35 • 2017

Multi-level Authentication and Monitoring System Using IoT

N. Nanda Prakash[a], K. Sreenivasa Ravi[b] and P. Gopi Krishna[c]

[a]*Department of Electronics and Communication Engineering SRKR Engineering College, Bhimavaram. Email: yvijaya456@gmail.com*
[b]*Department of Electronics and Communication Engineering, K.L. University, Guntur, AP, India. Email: siva4580@kluniversity.in*
[c]*Department of Basic Sciences, Shri Vishnu Engineering College for Women, Vishnupur, Bhimavaram. Email: Phaniyedlapalli23@gmail.com;*

Abstract: Spotting attackers is a key tension for associations and public administrations. Now-a-days the largely utilized provisions to avoid them are encroachment detection systems. Biometric knowledge is just the dimension and utilization of exclusive features of living humans to differentiate them from each other which is a lot more helpful since examining passwords and tokens is a simple task which may be missing or even taken. Therefore we certainly have selected the technique of biometric authentication. This paper reviews different identification technologies (fingerprint, speaker recognition and password and face recognition) which will suitable to all the categories of peoples like normal, dumb and blind. The developed system discusses the mode of operation of each of the technologies embedded in a single system.

Keywords: Face Recognition, Fingerprint, Identification, IoT, Security, Verification, Voice Recognition.

1. INTRODUCTION

Biometric knowledge forms a solid connection between an individual and his identification as biometric qualities can never be readily provided, lost, or even reproduced. Therefore biometric knowledge is simply excellent and more immune from public engineering attacks compared to a pair of traditional techniques of acceptance, particularly passwords and tokens. As biometric recognition demands the person to be present during authentication, it also stops individuals from producing fake identifications. In addition, only biometrics can offer destructive identity performance in which the goal is to establish whether a particular person is actually registered in a system although the person may decline it. Because of these features, biometric detection has been extensively hailed as the correct, efficient, and outstanding element of any identification system.

Computer systems are aimed by three types of attacks (1) User-level, each time an actual user makes use of his rights to grab data, (2) System-level, while an intruder makes use of system calls to assault the system, and (3) Network-level, while an assaulter makes use of information stream to implement the assault. In the past few years, large improvements have been manufactured in managing system and network level assaults. However

user-level assaults were handled mainly along with system-level attacks. This type of assault is measured as the most diligent kind of intrusions. A traditional illustration of a user-level assault is masquerade harm; in which scrawled person impersonates a different legible user so as to get access to delicate data is a big problem nowadays because it serves as a precondition for the majority of intrusions. The security features that contradict this danger are identification and authentication. In addition, biometric recognition systems may function in a pair of methods; identification mode, in which the system identifies a user seeking a huge database of registered users for a counterpart and authentication mode in which the system validates a person's stated identification from his previously registered pattern. [5] [9]

The security of an organization depends on the grant of accessing users who are authorized. The developed prototype deals with the biometric identification for allowing the users to access organization which helps in providing the security. It also includes the identification of different users and various security levels designed at each stage. The biometric module system helps in restricting the unauthorized users from entering the organization.

2. LITERATURE SURVEY

Security is the basic concern of today's world. An effective organization will always be established with a high security level. To improve the ease of accessibility for the user there are certain biometric methods.

Douglas A. Reynolds [7] discussed about voice recognition of a user is done in many methods. The most successful methods are through Gaussian Mixture Model and Score Normalization. These methods are used to verify the users tone and process the system for further level. But these methods have a drawback that they can't verify the user in a noisy environment. Some systems use the Viterbi beam search decoder for the recognizing purpose. When a speaker utters the sequence of words this decoder uses the conditional probability involved in the Hidden Markov Model during the training process and compares with the originally stored voice. This is a bit lengthy process so it requires a great amount of time which leads to the degradation of the efficiency of the system.

Iztok Kramberger [1] discussed about the doorway telephone mechanism with collective vice feedback and speech technology is not completely reliable the focus was on components which have more significant impact on efficiency. Utilizing embedded microphone array raises voice detection performance in quite noisy locations. To maximize speech detection functionality, a null syntax with assurance measure assistance was applied. The speaker conformation segment was also maximized for noisy conditions. It offers an individual identification and confirmation process depending on a VoIP doorway telephone embedded system and server-based speaker authentication system. Voice is transported using the widely accepted VoIP technology, which helps to ensure that this system may function in numerous application places with various security stages. There are numerous active doorway telephone devices that assist a variety of networking systems as well as assist to resolve personal mobility issues. This offers an expansion to a VoIP-based doorway telephone system setup with speaker authentication for doorway security [8].

Biometric devices gain incomparable superior individual identification and authentication, performing a huge task in private, national and universal security. Anyway these devices may be baited and apart from the innovative improvements in spoofing detection, latest alternatives frequently depend on domain information, particular biometric reading techniques, and also attack types [2]. We take in account an extremely limited understanding of biometric spoofing at the sensing unit to attain remarkable spoofing detecting devices for iris and fingerprint modalities depending on a pair of strong understandable methods. The initial method includes schooling of perfect convolutional network architectures for every domain, while the subsequent method is

targeted on data of the reliable network by means of back propagation [4]. We analyze nine biometric spoofing conditions consisting of real and imitation examples of a particular biometric modality and assault type and understand strong representations for every benchmark by merging and differing both understanding methods. This layout not just include much better idea of how these methods interplay, but additionally develop devices that go over the widely known results in eight of the nine conditions. The outcomes highly show that spoofing identification devices depending on convolutional networks may be difficult to assaults that are previously noted and likely modified [10][11].

Priyanka Rani [3] detailed about fingerprints are the most commonly used biometric technique yet very powerful. The fingerprint module has certain steps like identification, enhancement and matching. Identification can be done by using Fast Fourier Transform and Gabor Filters which are utilized to improve and rebuild the data of the fingerprint image and to take out a pair of fundamental types of minutiae, ending points and bifurcations. As a final point the extracted features are utilized to carry out the fingerprint detection. Second path for identification is Fusion and Context Switching framework concept which is used in forensic science purpose to equivalent a pair of concealed fingerprints. In this idea nothing like matching latent with live fingerprints, correct study and attention is paid. Third way is Segmentation which is the primary and essential pre-processing methods for any fingerprint verification and it decides the outcome of fingerprint evaluation and recognition. Various segmentation algorithms are utilized for these processes which are Gauss Filtering, Histogram Processing and Histogram Equalization.

3. IMPLEMENTATION METHODOLOGY

The system that is built for the authentication process is a set of different biometric techniques integrated as a single system using the Raspberry Pi processor. It contains a fingerprint module followed by a microphone, keypad, and camera. Other sources like power supply, speakers, monitor and memory card are present. These all components combine to perform the identification and authentication process. The details of the components used in this system and the methods they follow for accessing are discussed in the next sections.

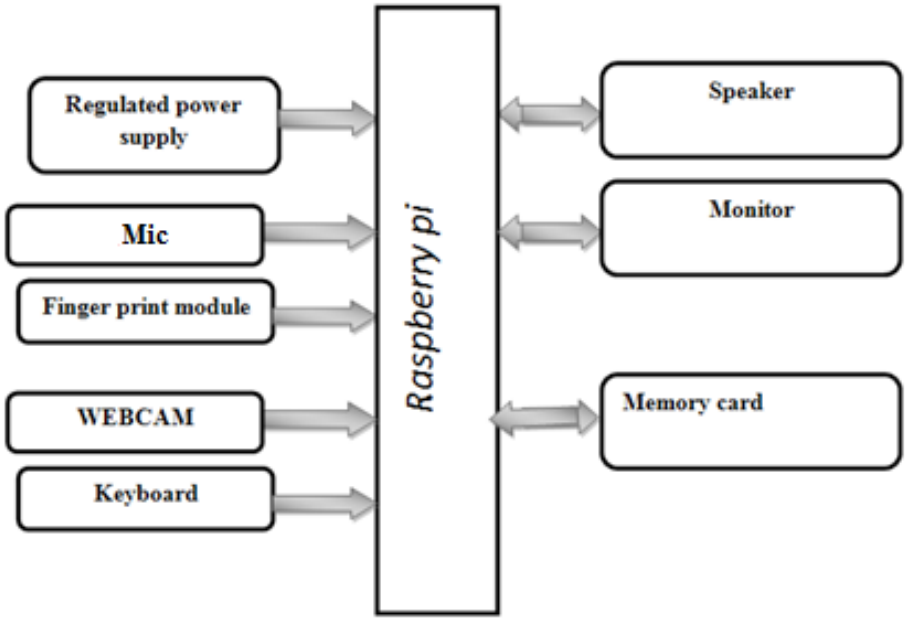

Figure 1: Block diagram of the Multi-level Authentication System

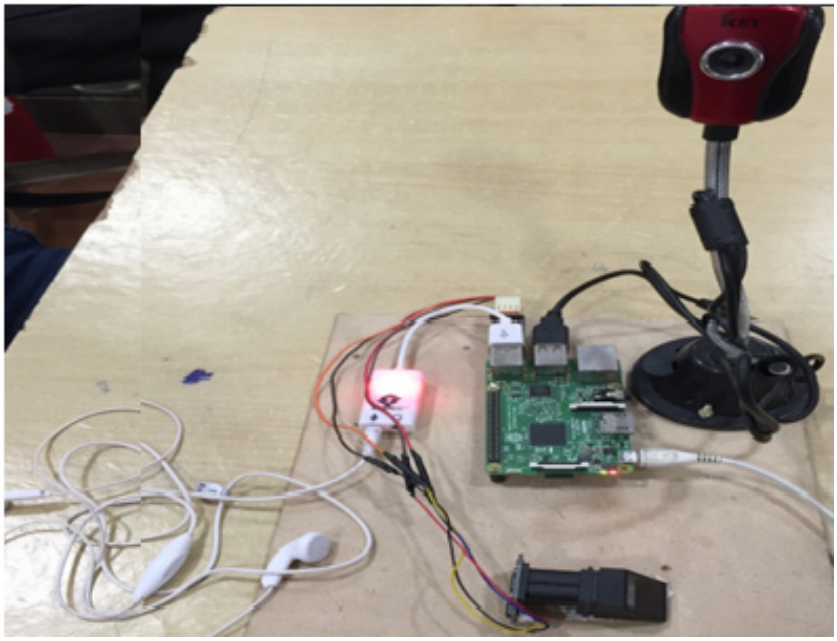

Figure 2: Hardware Implemented System of Multi-level Authentication System

A. Fingerprints

Fingerprints are the graphical flow-like ridges found on a person's fingertips. Finger ridge features will not alter all the way through the existence of a person apart from accidents such as bruises and injuries on the fingertips. This character makes fingerprints an extremely elegant biometric identifier. Fingerprint-based individual identification is being utilized from many years. Operating to their uniqueness and solidity, fingerprints are the preferred biometric options. Most significantly, even the twins don't have similar fingerprints. The conditions in the uterus impact the phenotypic growth of all parts of the twin fetuses. Hence, in spite of the same DNA structure of the two fetuses, fingerprints turn out to be diverse.

Figure 3: (a) Fingerprint of a person

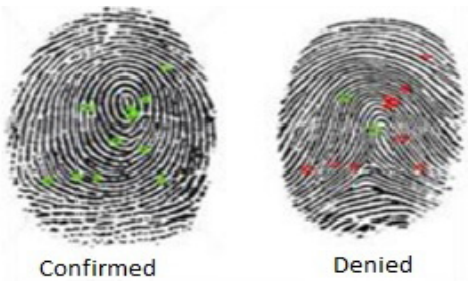

Figure 3: (b) Fingerprint Matching Cases

B. Speaker Recognition

Speaker detection is the determining job of validating a user's stated identity utilizing uniqueness obtained from their voices. Speaker verification is normally used as a "gatekeeper" to be able to give entry to a secure system. These types of devices function with the user's awareness and usually need their co-operation. Speaker detection devices can even be applied covertly without the user's awareness to recognize talkers in a conversation, focused automatic devices of speaker varies, verify in case if a person is already registered in a system. For forensic

purposes, it is frequent to start with a speaker detection technique to produce a bunch of "best matches" after which carry out a number of verification methods to Figure out a precise match. Giving the incorrect voice simply cannot be prevented in voice recognition along with the voice capturing device must be close to the user.

C. Face Detection

Face detection is considered as the work where system detects the persons face, as faces are more usually remembered by humans for distinguishing the person. A system is given the knowledge of the user face which it can differentiate from person to person depending on the previously stored data of the users. This path of the detection in the biometrics helps in tracking and finding the person in a certain situations such as a person robbing under a security cam can be identified and brought to justice. There are different ways in the facial detection process some of them are Feature base approach, Holistic base approach, Hybrid approach. The process contains face detection, feature extraction and classification. Face detection can be done by using methods like Eigenface, Neural Networks, Fisherfaces, Elastic bunch Graph Matching, Template Matching, Geometrical feature Matching.

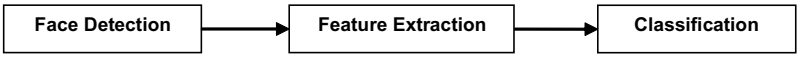

Figure 4: Face Detection System

D. Raspberry Pi

Raspberry Pi is a SoC (System on Chip) with the size of a credit card. Pi has an ARM compatible CPU with a speed range varying from 700 MHz to 1.2 GHz. Pi has a four port USB facility with HDMI slot along with a 3.5 mm audio jack. It supports I^2C and has an 8P8C Ethernet port. Raspberry Pi 3 offers a facility of on board Wi-Fi 802.11n and Bluetooth. Pi 3 has Camera Serial Interface (CSI) and Display Serial Interface (DSI). Raspberry Pi 3 is used because of its unique feasibility for integrating the fingerprint module, camera module, voice recognition module and keypad.

4. MULTI-LEVEL AUTHENTICATION SYSTEM

The Multi-level Authentication System is integrated with fingerprint, voice recognition, and password and face detection on a single board computer called Raspberry Pi 3. The whole module is used to grant access to the authorized person. Every connection to the board is through the USB ports. The first step starts with the fingerprint and depending on the fingerprint the next levels of authentication changes for different user. The module can provide access to disabled persons like blind and dumb depending on the fingerprint.

Biometric identification of fingerprint consists of three stages. First one is the Image Generation in which we find the physical devices that catches the energy radiated by the object. This is then sent to the digitizer which will convert the physical device output into digital form. The digital forms are then preprocessed to form the templates. The template creation is done by the processing system and after the template creation it requires a storage address. The address for template storage may be randomly chosen or the programmer may give it as the user id of the particular person. The template containing the digital values of the fingerprint is stored in the specific address. Whenever a user places his finger for identification the module captures the image and preprocesses it and makes a template of digital values which is compared with every template that are stored in the memory.

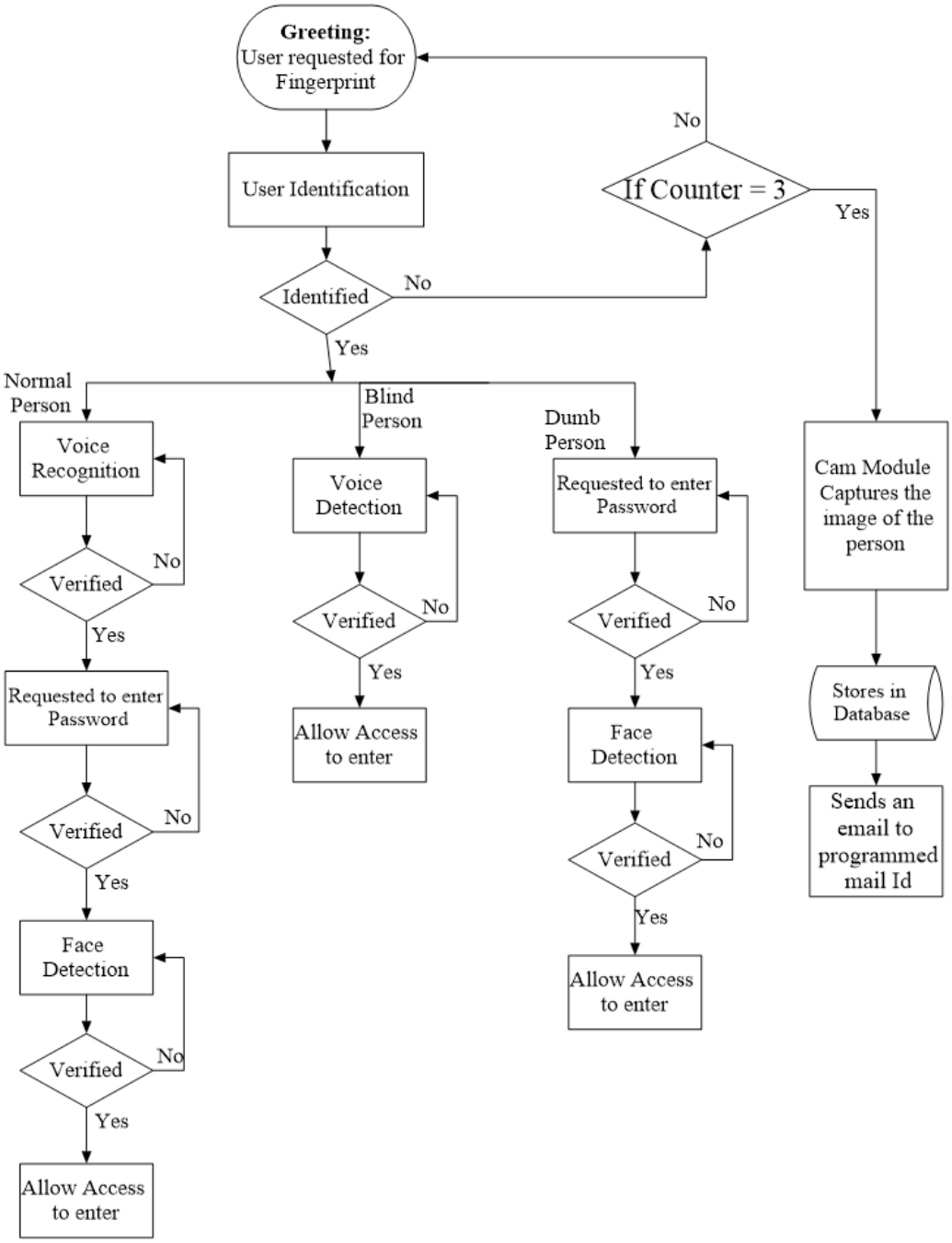

Figure 5: Flowchart of Mechanism of Multi-level Authentication System.

As the fingerprint module identifies the user the system then moves to the second level of authentication depending on the user. Second level for a normal person and a blind will be voice recognition which will be done using the speaker recognition module. In this level the user has to pronounce a certain words which will be captured and compared with the stored information. The speaker recognition module has two major functions namely feature extraction and feature classification. The first function feature extraction is a procedure that captures the specific properties of the speaker. For this purpose Mel-Frequency Cepstral Coefficients is the method applied. MFCC relies upon variety of known frequency for human

hearing views that are over 1 KHz. MFCC bears two kinds of filters that are placed linearly at compact frequency less than 1000 Hz and logarithmic spacing over 1000Hz. A biased pitch is there on Mel Frequency Scale to acquire key feature of phonetic in speech. The primary step will be pre-emphasizing the signal. The signal is passed through a filter that emphasizes higher frequencies. This will boost the energy of signal at higher frequencies, then framing and windowing using Hamming window done. The windowed signal is subjected to Discrete Fourier Transform (DFT). Then DFT output is warped on mel scale. Then logarithm value is taken. And in the final step, Discrete Cosine Transform (DCT) is done for calculating MFCC.

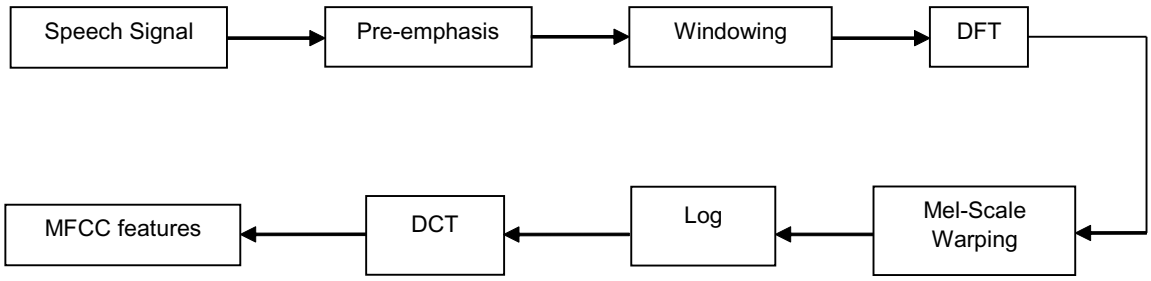

Figure 6: MFCC Block diagram

The classification portion contains two methods: pattern matching and decision. The feature extraction component extracts a bunch of characteristics from the speech signal that indicate certain speaker-specific data. The pattern matching device is in charge for examining the anticipated characteristics to the Speaker models. In this task we are applying MFCC (Mel Frequency Cepstral Coefficients) as features and ANN (Artificial Neural Network) as feature matching technique.

As the voice recognition level verifies and allows access to next level the user has to enter the specific password of his/her to enter the fourth step. The third and fourth levels will not be present for the blind person as the system allows him access to enter. The third step will be a unique code for every user which cannot be shared. If the code matches with the users previous verifications then it allows for the fourth level of verification which is face detection. For face detection a camera module is used to capture the image of the person. This image is then compared with the previously stored images. There are two stages of the comparison of the images. The first one is the Mean Square Error (MSE) value between both the comparing images which should be very low. And the second parameter is the Structural Similarity (SS) of both the comparing images which should be very high. The image captured for comparison is checked for these two parameters with each and every image stored in the database and the image that has lowest MSE and highest SS is chosen. If they both have the highest similarity then the user is allowed access to enter. If not then he has to go through the process once again.

If the fingerprint of the user doesn't match with any of the stored fingerprints in the database the system will not grant access. If the user tries the fingerprint and fails for a particular number of times then the camera module captures the image of the person and sends an email to the authorized person along with the attachment of the image captured. For this task the system is linked with internet. This makes the system an IoT based Multi-level Authentication System which is at ease to the user.

5. RESULTS

The proposed system was fully developed and tested to demonstrate its feasibility and effectiveness. The screenshots of the multi-level authentication system which was developed has been presented below.

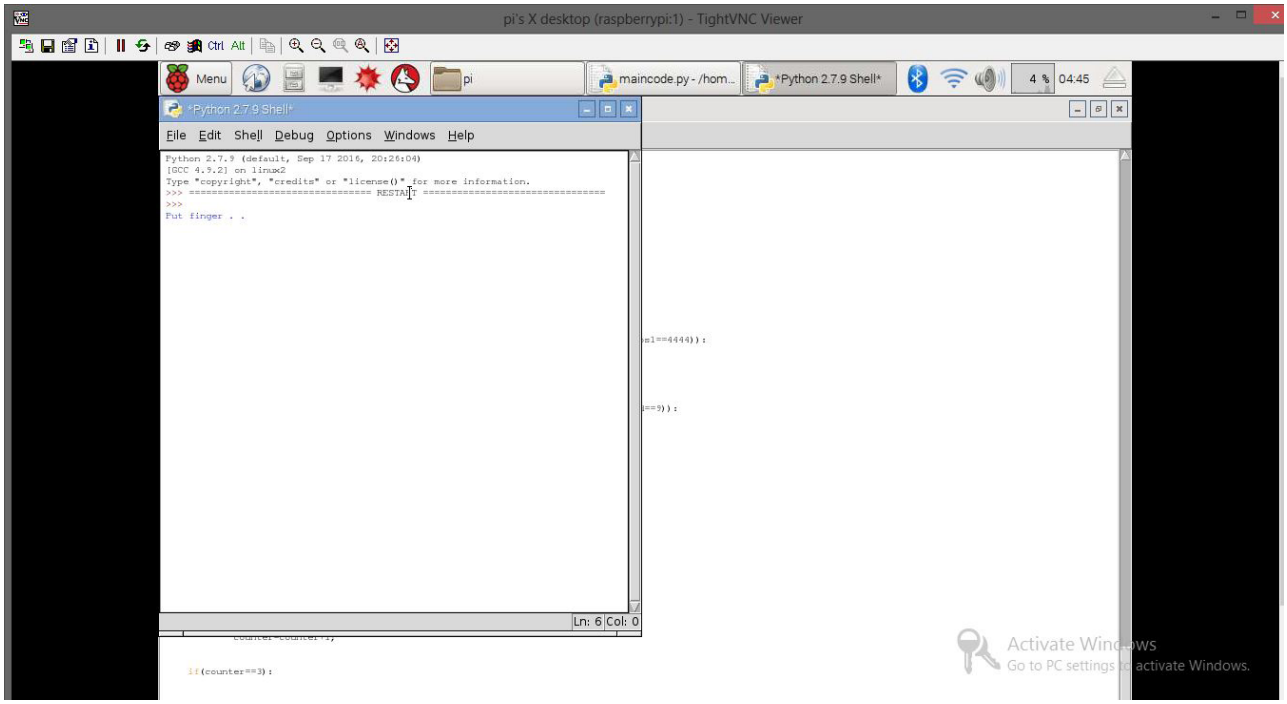

Figure 7: First level (Finger Print) Authentication

As the first level is finger print we need to place the finger on the biometric module for verification which is shown in Figure 7. Once the first level gets verified it will be moved to second level.

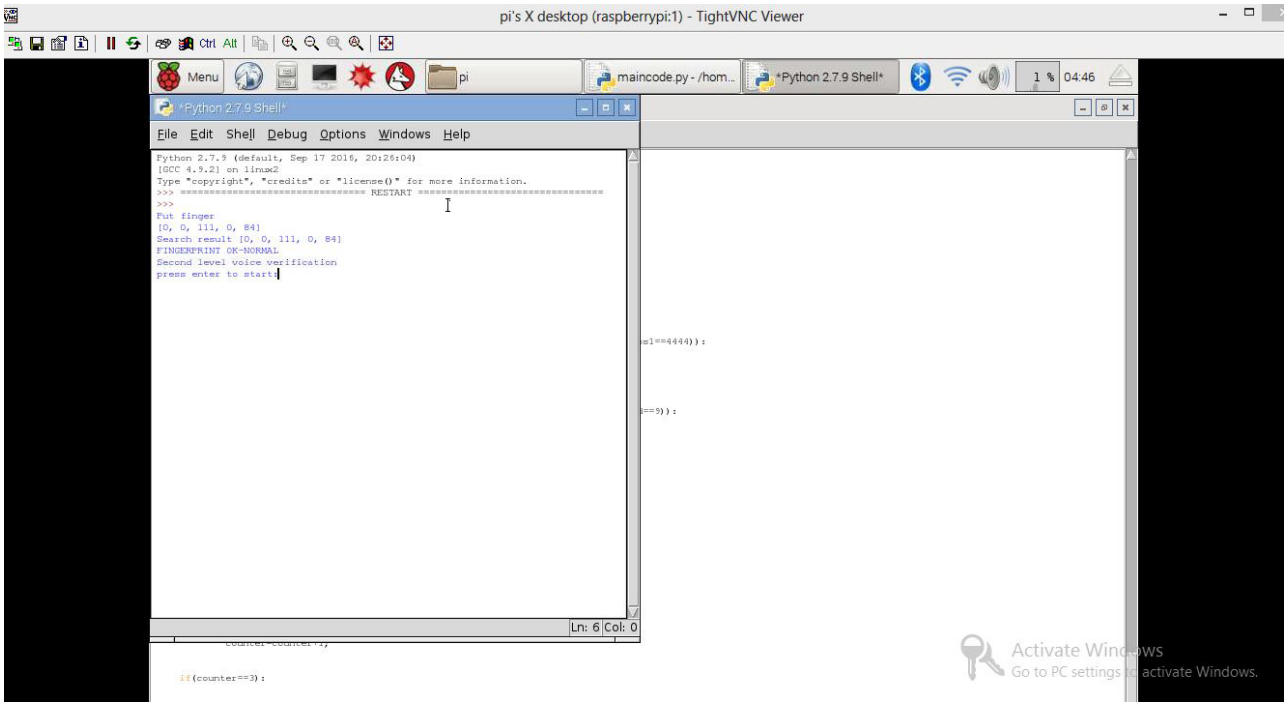

Figure 8: Second level (Voice Recognition) Authentication

The second level consists of voice recognition in which a user has to speak in the microphone provided for authentication shown in Figure 8. If the second level gets authorized then it will be moved to third level.

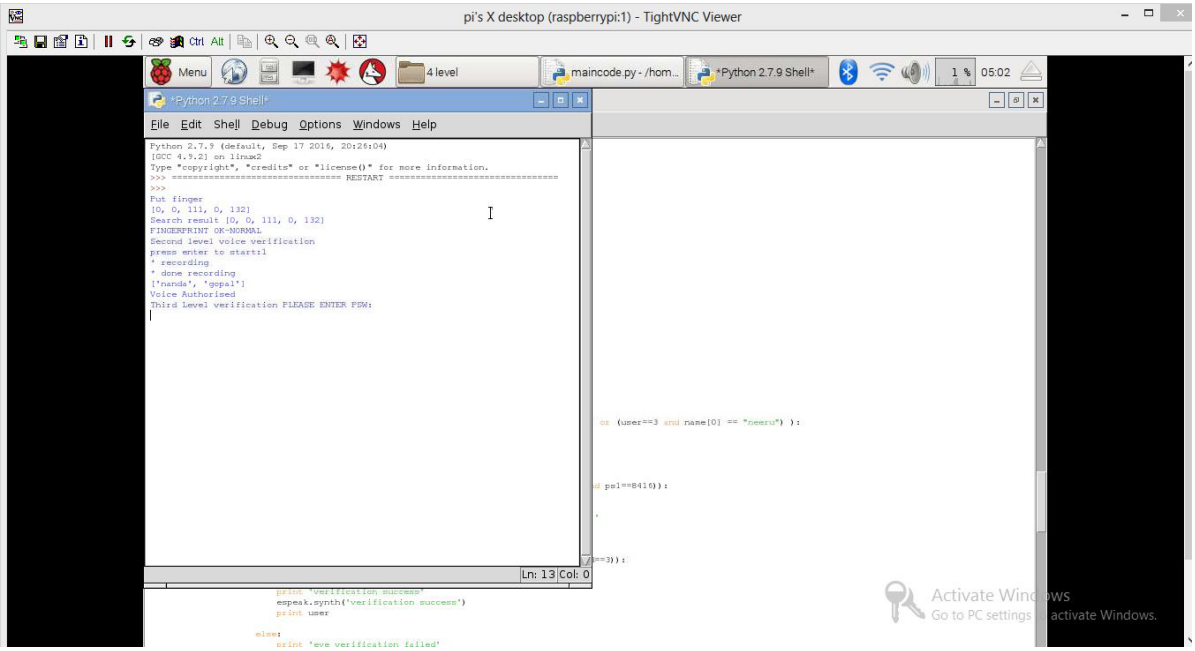

Figure 9: Third level (Password) Authentication

The third level is Password authentication which is manual for getting access to fourth level.

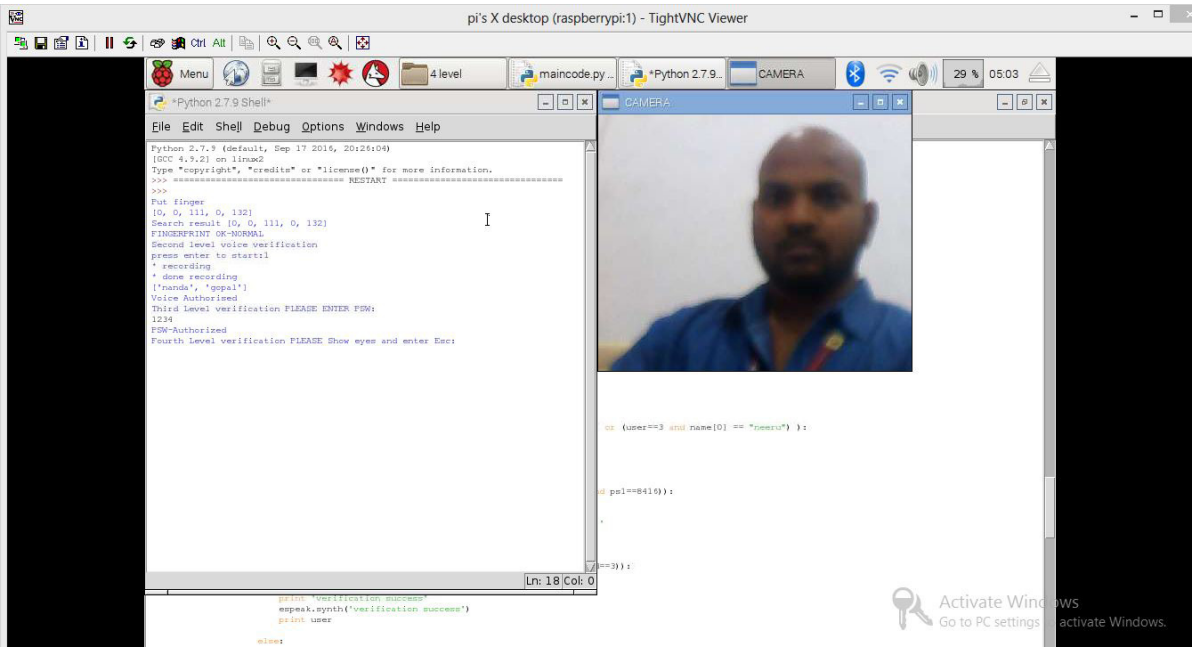

Figure 10: Fourth level (Face Recognition) Authentication

Fourth level which is final authentication is face recognition which is done by capturing image using a cam module. If the image is verified then it allows access to the user which is shown in Figure 10.

If the fingerprint fails for three times consequently then the cam module captures the image of the person and sends an email to the programmed mail ID. This is done by linking the system to internet which makes it a IoT based system. The mail that is generated by the system is shown in Figure 11.

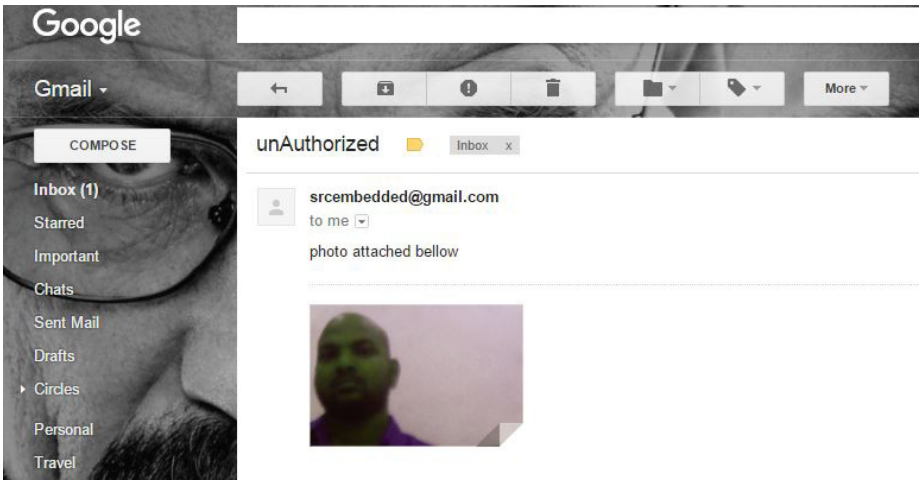

Figure 11: Email to Authorized mail ID

6. CONCLUSSION AND FUTURE SCOPE

There are many assaults that attempt to obtain a computer device using a number of techniques similar to unauthorized access. These assaults might be decreased if a verification device is employed to match previously placed intrusion detection system. The leading identification devices are based on biometrics. So, a number of biometrics methods begin to come up with host-based Intrusion detection devices. So far, behavioral biometric was the solely method that had been used because they do not require any unique systems. In comparison, some researchers verified that these methods are not so efficient; this inspired to layout a verification device depending on fingerprint method.

Acknowledgements

Authors are greatly thankful to K L University authorities for providing necessary infrastructure facilities to carry out this project work.

REFERENCES

[1] Iztok Kramberger. "Door Phone Embedded System for Voice Based User Identification and Verification Platform". IEEE Transactions on Consumer Electronics, Vol. 57, No. 3, August 2011.

[2] David Menotti. "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection". IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, April 2015.

[3] Priyanka Rani and Pinki Sharma. "A Review Paper on Fingerprint Identification System". International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) Vol. 2, Issue 3 (July - Sept. 2014).

[4] Riddhi Patel and Shruti B. Yagnik. "A Literature Survey on Face Recognition Techniques". International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 4 –Nov 2013.

[5] A. Ahmed and I. Traore. "Anomaly intrusion detection based on biometrics". In 6th IEEE Information Assurance Workshop, 2005.

[6] Khalil Challita. "Biometric Authentication for Intrusion Detection Systems". 2010 First International Conference on Integrated Intelligent Computing, 08/2010

[7] Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. "Speaker Verification Using Adapted Gaussian Mixture Models". Digital Signal Processing 10, 19–41 (2000). doi:10.1006/dspr.1999.0361.

[8] Y. J. Oh, E. H. Paik, and K. R. Park, "Design of a SIP-based real-time visitor communication and door control architecture using a home gateway", IEEE Trans. Consumer Electron., Vol. 52, No. 4, pp. 1256-1260, Nov. 2006.

[9] Smita S. Mudholkar, Pradnya M. Shende, Milind V. Sarode. "Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition". International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012.

[10] Ravi Subban and Dattatreya P. Mankame. "A Study of Biometric Approach Using Fingerprint Recognition". Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

[11] Arun Ross and Anil Jain. "Biometric Sensor Interoperability: A Case Study In Fingerprints". International ECCV Workshop on Biometric Authentication (BioAW), (Prague, Czech Republic), LNCS Vol. 3087, pp. 134-145, Springer Publishers, May 2004.