IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Physical Access Control Based on Biometrics and GSM

Diptadeep Addy[1], Poulami Bala[2]

Student, Department of ECE, St. Thomas' College of Engineering & Technology, Kolkata, India[1, 2]

Abstract: In this current age of 21st century security and privacy has become a major challenge to all of us. Whether it is in the private sector or government agencies, there remains a constant threat on privacy and security. Bank accounts are being hacked, private information being stolen now and then, lump sum amounts of money and valuable documents are changing hands overnight. Technology is changing and evolving constantly over the years. Hackers have become more ruthless in their methods and have been successful to make their entries into any system in the world and steal things. There are many vaults all across the country where important valuables and secret documents are kept, which are important for safety and security of the nation. So to answer these concerns we have proposed an idea where we are going to integrate some biometric features along with GSM communication and build a multi layered security system-4-layer biometric system. Biometrics has emerged as one of the most convenient, accurate, and cost-effective forms of security. Since Biometric techniques are automated for personal recognition based on physical attributes which include face, fingerprint, hand geometry, handwriting, iris, retina, and voice. Each of the techniques is customized for specific applications. Biometric data are considered to be different and distinct from personal information because it cannot be reverse-engineered to recreate any personal information and cannot be stolen to attempt theft.

Keywords: Security, Facial recognition, Finger print scanning, wireless security systems, GSM verification.

I. INTRODUCTION

Security as we all know in this current juncture of 21st century has become a big question and a cause of concern for everyone because nothing can be said to be totally secured, starting from our bank accounts, to our e-mails, social networking profiles even our private lockers or security systems where highly valuable things are kept. So in this current scenario a big change is needed as most of the security systems use an electronic locking system with predefined passwords and computerized keys or some of the advanced ones uses biometric credentials like finger print, iris recognition, hand geometry, etc. which unfortunately has been proven to be vulnerable. This is because it is easier to penetrate this types of vaults as all they have to do is breach a single layer of security and do their job. Fortunately, this current age has been blessed with all the latest digital technologies available, so we can integrate some of these methods and technologies available to make such a system where the difficulty level for penetration will be much higher.

Although there were many existing studies about biometric bank-vaults systems earlier, the studies had mainly aimed to develop an improved prototype. In this process, a multi-level security system has been designed by us to integrate biometric credentials for increasing the levels of security to prevent any breach of security.

That is why we are proposing an idea of a system where there will be multiple levels of security where each level is co-ordinated with the other one and to reach the final door of the vault you have to pass each and every level of security and a failure in any stage will totally deny access to the vault.

Since our proposal i.e. physical access control is mainly based on biometrics and GSM, we have chosen face and finger prints as the biometric credentials separately for each layer and a random one-time password generation system as the final hurdle or layer of security which is going to operate through GSM communication.

The proposed design has been divided into four stages for better understanding:

1. Account user name and password matching
2. Facial recognition
3. Finger print matching
4. Randomly generated password breaking system through mobile (GSM) communication.

The account holder has to first enter his/her account no. and password to gain access to the security system. This is stage-1 of the verification process. If the account no. matches with the database records, the user is let through. After this, he proceeds to the facial recognition stage, where a snapshot of his/her faces is captured and then verified with his actual credentials. If the stage 2 yields success, door 1 opens. Next the user's fingerprint is enrolled first and then matched with the optical fingerprint scanner. This is stage-3. Once the match is successful, a One Time Password (OTP) is sent to the registered mobile no of the account holder. This verification code sent has to be typed in the keypad to open the final door of the vault, else the siren goes on, closing door 1and alerting the nearest police station for intruder alert. Hence the fourth stage ensures the actual presence of the user at the time of accessing the bank-vault.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

II. LITERATURE SURVEY

There were many works which were previously carried out related to secured access control systems mainly based on biometrics and GSM technology. Some of them are enlisted here. Previous studies mainly focused on a two-step verification process. Several studies using fingerprint biometric recognition were conducted to improve locker systems. One among them was the study of Lay, Yang and Tsai (2011) entitled "Biometric Locker System" wherein fingerprint recognition technique was used to open and close the lock of a storage locker system. The system first captured the fingerprint of the locker renter and matched the fingerprint to reopen the locker door. This was done to reduce troubles about keys and to ensure the security of the renter [1]. Similarly, the study conducted by Gangi and Gollapudi (2013) entitled "Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM," had designed and implemented a locker security system based on the integration of radio frequency identification (RFID), fingerprint, password and global system for mobile (GSM) technologies that can activate, authenticate, and validate the user to unlock the door for secure access. In this system, the RFID reader reads the ID number first and determines if it is valid. If the id number is valid, that is the time that the system gives access to the fingerprint scanner. Then it will scan the fingerprint, and if matched, the microcontroller sends the password to the authenticated person mobile number. The person then has to enter the passwords to the system [2]. Another novel approach to improve the security of such systems came with the inclusion of facial recognition. A new design of ATM's in banks has been proposed in the paper titled 'Secured Banking operations with face-based Automated Teller Machine'[3].In this proposed system, access will be authorized by means of human face picture taken by camera. Secured features of face extracted through facial recognition algorithm would be used as a PIN. Face-based home security systems have been developed too. Zuo et al. [4] proposed Home Face, real-time embedded face recognition system for consumer applications which enables a personalized service by automatic identification of users. This system is embedded into a smart home environment for user identification. I. Yugashini et. al [5] proposed the design and implementation of an automated Door access control system with Facial Recognition. The face recognition and detection process is implemented by modifying principal component analysis (PCA) approach, by which the captured image is detected using a web camera and compared with the image in the database. If the image is an authenticated one the door will be opened automatically else an SMS will be generated using a GSM modem to the user that an unauthorized person has entered home. The PCA approach, first suggested by Turk and Pentland [6] focuses on recognition of person by comparing specific characteristics of the face.

After going through all these papers, we got the idea to design a full-proof, high profile security system by integrating both biometrics and GSM technology. The usage of biometrics is for identification and recognition whereas GSM has been used for valid authentication of the person.

III. SYSTEM DESCRIPTION

A. System Architecture:
This project is built on a multi-level security system. As soon as the account holder enters his/her account no. and password, the database searches for a matching record. The corresponding account details are displayed on screen. Next, the webcam turns on and the snapshot of the person is taken. The system again tries to recognize that person's face; upon success he/she proceeds to the next step of verification process. A user prompt on LCD unit displays, "Scan Your Finger", wherein the fingerprint is enrolled first and then matched with the help of optical finger-print scanner. Upon successful match, a One Time Password (OTP) is sent to the registered mobile of the account holder. Only when this OTP is entered through the keypad attached to the door, the person would be allowed to access the vault.

The entire GUI has been made in MATLAB. The flow of the system is as shown in Fig 1.

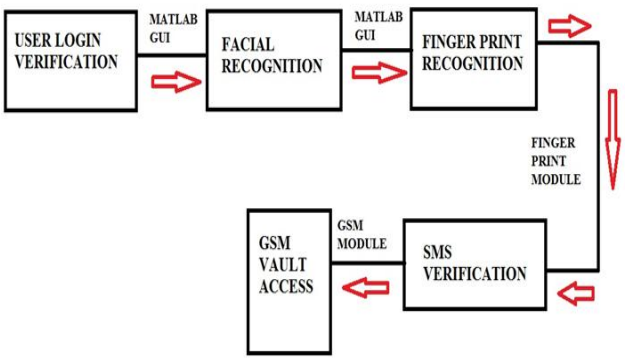


Fig.1.Process flow diagram of the system

B. Hardware Design of the System:
In this system, we have used an Advanced Virtual RISC (AVR) microcontroller unit (MCU). This controls the functions of the entire security system built. As seen from Fig 2, the microcontroller is interfaced with the peripherals like LCD module, servo motors and alarm (buzzer). After the facial recognition stage is complete, the pc sends data serially to the MCU. The MCU then drives the servo motor 1 to close DOOR1.Next, the LCD Module turns on and displays the message to "Scan Your Finger". The adafruit finger print sensor first enrols the person's fingerprints, then performs the verification step. As soon as this step completes, the GSM Module (SIM 900A) is triggered to send a One Time Password (OTP) to the registered mobile number. The person needs to type this OTP in the keypad within 3 chances; only then MCU will send command to drive the second servo motor. And then only the final door to the locker opens, otherwise upon OTP mismatch, door 1 closes and an alarm (buzzer) is turned on for intruder alert.

DOI 10.17148/IJARCCE.2016.55211

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

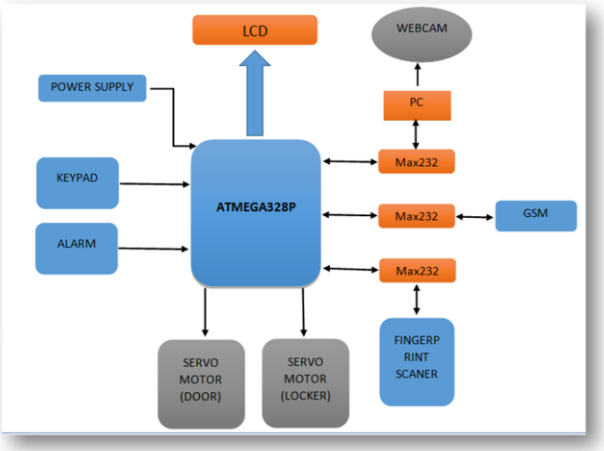


Fig.2.Block diagram of the Hardware architecture of this security system

C. System Implementation:

C. a Account User and Password Matching

Fig3. Snapshot of stage-1 of GUI upon successful match of user-name and password

This is the most primitive step of the total verification process. Previously when the user had opened an account in the bank he had a particular user name and password. This user name and password is unique for each user of the bank. Now when the user needs to access the bank vault, he has to give a prior notification to the bank manager on that particular day. After the manager grants him/her the access, the user is able to log into the GUI. The GUI asks for the user's bank account no. and password. Now after filling the details, the processor machine starts running through its database so that it can exactly verify the user name and password and link with that account only. However, the user is given a chance to enter password three times only, if it does not match a warning bell blows on.

C. b Facial Recognition

After the bank user enters his/her user name and password correctly, then the webcam turns ON and captures the facial image of the user. After it captures the image the processor runs through its database to search for the matched image. This image matching process is carried out by Eigen face algorithm. If after all the calculations the taken image matches with the database image of that particular account user, then only it shows a display message on LCD that the image is matched and DOOR 1 opens.

Fig.4.Snapshot of the GUI showing the face is recognized and the DOOR1 opens.

EIGEN FACE ALGORITHM

The Face-recognition algorithm is based on PCA based on Eigen faces and it is programmed using MATLAB. The PCA algorithm based on Eigen faces is explained in the figure 6. Principal component analysis transforms a set of data obtained from possibly correlated variables into a set of values of uncorrelated variables called principal components. The number of components can be less than or equal to the number of original variables. The first principal component has the highest possible variance, and each of the succeeding components has the highest possible variance under the restriction that it has to be orthogonal to the previous component. We want to find the principal components, in this case eigenvectors of the covariance matrix of facial images. The set of images that are stored in the database are taken as the training set. These set of images are the pictures of the people for whom the access should be granted. From this training set, the mean is calculated and subtracted to get the average vectors from which we can get our covariance matrix and hence the Eigen vectors which are the Eigen faces, E.

The weighted matrix (W) is calculated for the training set using the Eigen faces. When an image a is obtained from the external camera, the weighted matrix (Wa) for the image A is calculated.

Then the weighted matrices are compared to get the distance (D). In this case, the Euclidean distance is calculated. The distance D is compared with the threshold value Θ. If the value is lesser than the threshold value, then the image is recognized, else not recognized. The mathematical formulas for calculating the Eigen vectors, weighted matrix, Euclidean distance is explained in the paper (Marijetaat el, 2012) [7].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

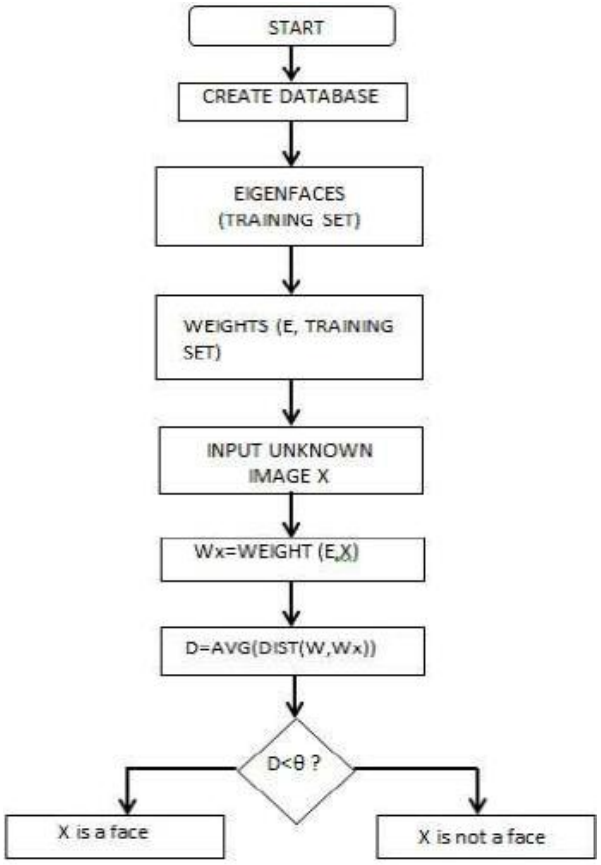


Fig. 5. Flowchart of the Eigen Face approach using PCA

C. c Finger Print Scanning and Verification

As the user approaches DOOR 2, the LCD display flashes the message "scan your finger". An adafruit fingerprint sensor has an optical scanner to scan the user's finger and verify it electronically. There are two separate stages involved in using a system like this. First you have to go through a process called enrollment, where the system learns about all the people it will have to recognize each day. During enrollment, each person's fingerprints are scanned, analyzed, and then stored in a coded form on a secure database. Typically, it takes less than a half second to store a person's prints and the system works for over 99 percent of typical users (the failure rate is higher for manual workers than for office workers).

Fig. 6. Status of the security system when the system scans the finger of the person for finger-print verification.

Once enrollment is complete, the system is ready to use—and this is the second stage, known as **verification**. Anyone who wants to gain access has to put finger on a scanner. The scanner takes in fingerprint, checks it against all the prints in the database stored during enrollment, and decides whether the person is entitled to gain access or not. Sophisticated fingerprint systems can verify and match up to 40,000 prints per second.

C.d GSM Password Verification

This is the last stage of the verification process. Here when the user's finger print has been accepted and verified from the database, then a random keyword is generated from the microcontroller unit. This passkey is send to the registered mobile phone, using GSM Module. After the user gets the key, he types in the keypad attached with DOOR2. If passkey entered is correct DOOR 2 opens and the user is allowed access to his/her locker. If not, the user will be given 2 more chances to put the passkey correctly or else an alarm buzzes and the DOOR 1closes, along with a SMS being sent to the bank manager and that account user for an INTRUDER ALERT.

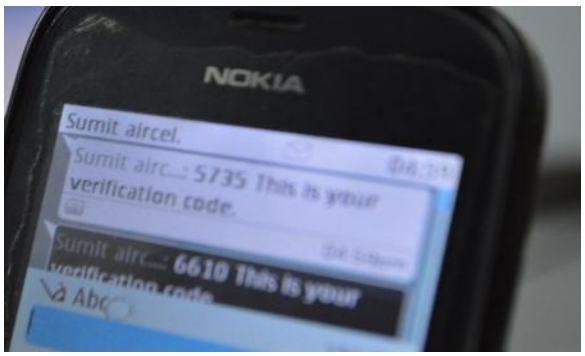
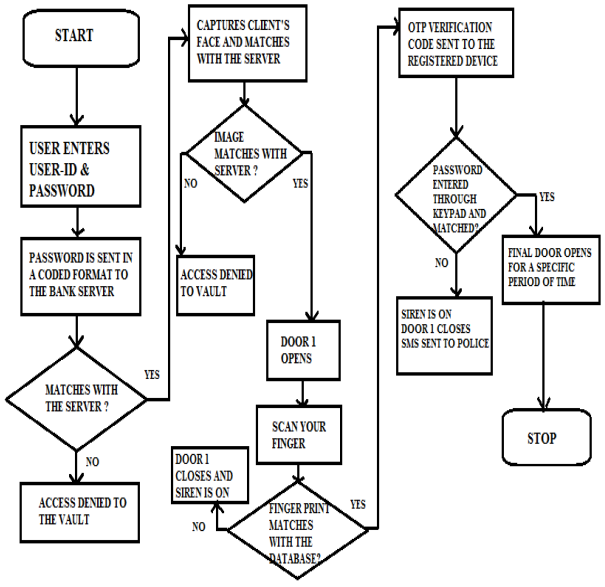


Fig. 7. Status of the security system when OTP verification is done using GSM

D. Detection and processing algorithm

The algorithm of the entire security system is provided using a flowchart as given in Fig. 7.



DOI 10.17148/IJARCCE.2016.55211

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

IV. RESULTS AND DISCUSSIONS

The results obtained for various stages of verification of the security system are explained in a chronological manner as follows.

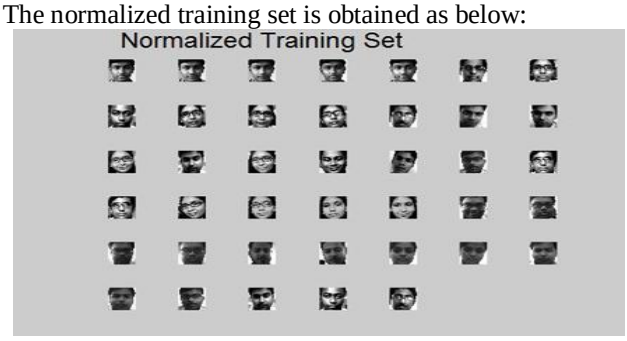
A. Analysis of Stage-1: Identification of the authentic account user

The figure below shows the account details of a person whose account no:1278. These details will be fetched from the banks database only upon successful match of user name and password entered in the MATLAB GUI. There is no false mismatch recorded at this stage.

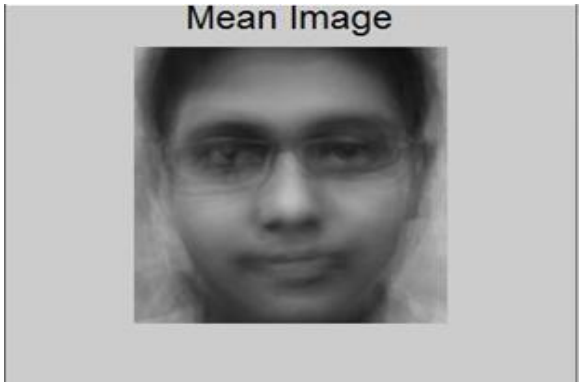
B. Performance Analysis of Stage-2: Facial Recognition Module

Here we have collected pre-processed facial images of each person we want to recognize. The database consists of 40 training images.

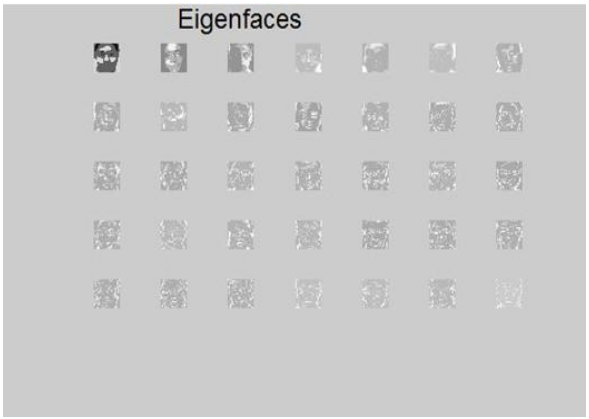
The normalized training set is obtained as below:



Using “Principal Component Analysis" we convert all our 40 training images into a set of "Eigen faces" that represent the mean differences between the training images. First finds the "average face image" of our images by getting the mean value of each pixel.



Then the eigen faces are calculated in comparison to this average face, where the first eigenface is the most dominant face differences, and the second eigenface is the second most dominant face differences, and so on, until we have about 40 eigen faces that represent most of the differences in all the training set images.



The experiment is performed under varying conditions and the success rate also depends on that. The parameters we have considered are summarized in the Table 1.

TABLE I. PERFORMANCE ANALYSIS TABLE FOR FACIAL RECOGNITION

PARAMETERS	RESULTS
NO. OF SUBJECTS	40
SUBJECT’S AGE	22-24 years
GENDER	MALE, FEMALE
LIGHTING	HIGH-100% MEDIUM-80% LOW-60%
FACIAL HAIR, GLASSES	SUCCESSFUL

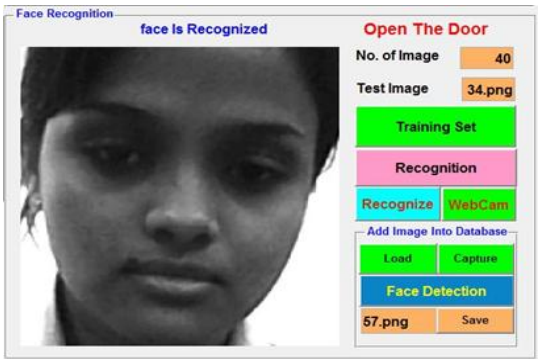
The results obtained under various conditions are subdivided under 4 distinct cases for better understanding of the working of the system.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

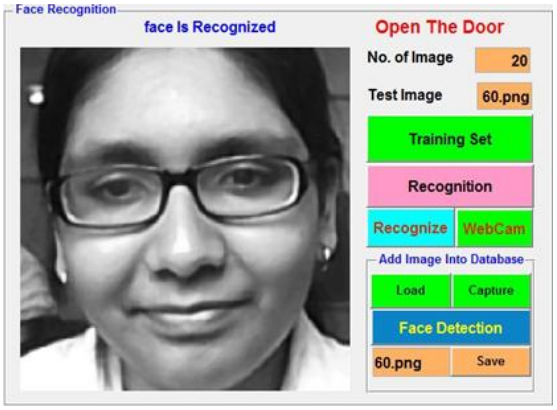
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

CASE I. When the user's image is in the database and it matches

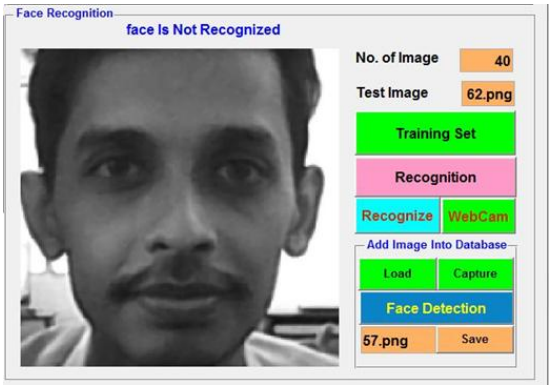


CASE II. When the user's image is in the database and it does not match

CASE III. When the user's image is not in the database and it matches



CASE IV. When the user's image is not in the database and it doesn't match



C. Analysis of Stage 3: Fingerprint Enrollment and Verification

Fingerprint enrolment and recognitions were conducted to ensure that the biometric sensor was properly interfaced to the microcontroller unit. For security purposes, enrolment of fingerprints was done using a third party software. We liked this particular sensor because not only is it easy to use, it also comes with fairly straightforward Windows software that makes testing the module simple - you can even enroll using the software and see an image of the fingerprint on our computer screen.

D. Analysis of Stage 4: Generation of OTP

After successful matching of the fingerprints, an OTP is sent to the registered mobile no. of the account holder using GSM Module.

The LCD Unit prompts the user to "Enter the OTP".

If this entered passcode matches with the system generated random passcode sent to the mobile number, then only the final door to the vault opens.If the last stage fails, siren blows on.

IV.CONCLUSION

So here we have finally designed a system where there will be 4 tiers of security measures to finally access the vault and each tier has to be verified and passed to reach

the next tier. Since our main topic was physical access control which actually means physically accessing and controlling a particular system based on some parameters, we have designed the whole system according to it by taking 2 biometric credentials (face & finger print) and random OTP verification through GSM as the basic parameters. As we have developed the system we have realized a few shortcomings of this model i.e the place where the system will be kept has to be properly illuminated or else it can give false errors, the system is very complex in nature so it can only be used in places where that much security is necessary like bank vaults, government vaults where highly valuable documents are kept. But the system can obviously be modified so that it can be implemented for home security or for places where less level of security is needed.

The system we have designed here is the basic prototype and can be modified. Like the facial recognition algorithm can be changed and a more accurate algorithm be implemented where all other facial characteristics like physiological, behavioral, ambient conditions (e.g., temperature and humidity) can be taken into consideration. The finger print scanning can be modified by taking into consideration the user's interaction with the sensor. It has been seen that due to lack of connectivity or weak mobile signals the random OTP can't be properly sent at the right time, so this also has to be taken into consideration while implementing in such a place where mobile signal is strong enough to send proper data. This system has given some false errors at times so a more robust and accurate system should be made to eliminate this type of errors.

REFERENCES

[1] Y. L. Lay, H. J. Yang, and C. H. Tsai, "Biometric locker system," in Proc. the World Congress on Engineering and Computer Science, vol.1, San Francisco, USA, October 2011.

[2] R. R. Gangi and S. S. Gollapudi, "Locker opening and closing system using RFID, fingerprint, password and GSM," International Journal of Emerging Trends & Technology in Computer Science, vol. 2, issue 2, March-April 2013.

[3] Olutola Fagbolu, Olumide Adewale, Boniface Alese and Osuolale Festus," Secured Banking operations with face-based Automated Teller Machine", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.

[4] F. Zuo, and P. H. N. de With, "Real-time embedded face recognition for smart home", IEEE Trans. Consumer Electron., vol. 51, no. 1, pp.183-190, Feb. 2005.

[5] I.Yugashini, S.Vidhyasri, K.Gayathri Devi," Design And Implementation Of Automated Door Accessing System With Face Recognition", International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-12, November 2013.

[6] M. Turk, A. Pentland: Face Recognition using Eigenfaces, Conference on Computer Vision and Pattern Recognition, 3 – 6 June 1991, Maui, HI , USA, pp. 586 – 591.

[7] Marijeta Slavković1, Dubravka Jevtić1 'Face Recognition Using Eigenface Approach' Serbian Journal Of Electrical Engineering Vol. 9, No. 1, February 2012, 121-130.