International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 9 (2018) pp. 6915-6919

Haptic Security System

Anandraj A[1], Aswin Kumar D[2], Dr. Sudhakar T.D[3]

[1-3] St .Joseph's College of Engineering, Chennai, Tamil Nadu 600119, India.

Abstract

Security has been playing a key role in many of our places like offices, institutions, libraries, laboratories etc. In order to keep our data confidentially so that no other unauthorized person could have an access on them. Nowadays, at every point of time, we need security systems for protection of valuable data and even during the access of specific control rooms. This paper presents a hybrid system based on fingerprint and passcode protected door opening system which provides security which can be used for many banks, institutes and various organizations etc.. in excess. Unauthorized access is prohibited by designing a lock that stores the fingerprints of one or more authorized users. Fingerprint is sensed by sensor and is validated for authentication. If the fingerprint matches, the door will be opened automatically otherwise the buzzer connected to an audio amplifier will be activated so that the people near the surroundings will get an alert.

Keywords: Haptic, password, biometric, FPS, hybrid, integrated security

INTRODUCTION

Security represents protection of our life and assets. Ensuring safety of people and their valuable things is very important for the prevention of illegal handling. Hence, mainly focusing on door lock security or gate security is very important to avoid the further problems in the monitored area. Initially, there was mechanical locks, robberies get happened due to the fact that those locks were broken. So followed by that, digital password locks were introduced. This method was outdated when passwords were hacked by thieves. There was then came the biometric based locks. Under significant instances fingerprints were also faked through forensic studies. After this era, emerged the Global System for Mobile(GSM) based system, which used mobile communications for the purpose of unlocking the door each time[1]. Then came the Radio Frequency Identification(RFID) based System. In this system, the authorized users are required to place the card tag in RFID detector[2]. This system was outdated due to frequency issues and manufacture issues.

After this time period, bluetooth based system came into existence. It uses he bluetooth module connected to smart devices to operate the access. This technology was not efficient enough for large companies and were implemented for only domestic low strength people. Then came the social networking sites based Systems. It was hacked easily and was not efficient. One Time Period (OTP) based system used to send a OTP everytime it requires access and the OTP should be entered[3]. This had it own defects viz missing their mobile, more time taken to access etc. Motion detector based system was introduced after this period. It was based on the principle of light falling on the photodiode. Once the motion(key to unlock) was leaked the security no more seemed to be a threat.

Visual Biometric(VB) system which was published after this which used electronic eye representation[4]. It is a module for capturing the door images whenever the door was opened or closed. This security cannot be used in areas where even a one way entry should be restricted. At last came the combined system, which made use of two or more of the above mentioned methods to access the locks[5]. This System remains the latest high end security protocol for banks and other important sectors. This System has the defects of each methods combined which can be done by professional hackers.

The defects of these methods made us realize the need for security issues. The efficiency of the security can be further increased only when there is a combination of several methods.[6] Instead of combining two methods, we integrated two methods of security and made one method hidden and only the other method visible to the people. In detail, this project uses the password based system integrated long with the finger print based system. The later method is kept as a hidden feature so that it becomes impossible for the hosts to break the security. Hence, this system would rise as the best security system available till date.

LITERATURE REVIEW PASSWORD PROTECTED SYSTEM

The programmable electronic code lock device [6] is programmed in such a way that it will operates only with the correct entry of predefined digits. It is also called an integrated combinational type lock. The programmable code lock is shown in Fig 1 as below. Electronics safe is its example. Based on the programmable electronic code lock, the reprogrammable digital door locks [7] were invented in that the password can change any time as it stored in PROM.

GSM Based Systems

In many door lock security systems, GSM is used for

communication purpose. The purpose of a work cultivated by utilization of a circuits like a GSM module which gets activated by a controller [1] for sending SMS in emergency to proprietor and for sending corresponding services of security at the time of break in. For detecting obstacles, the system requires various sensors. It gathers data from the sensors and settles on a choice. With the help of GSM module, sends SMS to a respective number.

OTP Based Systems

The proposed method in latest work does not need administrator's help to access the facility if the user knows OTP technique and has a registered mobile phone [3]. Likewise the OTP is generated and sent to the proprietor's mobile phone whenever user requests to access facility. Then the OTP should enter through keypad on the door [8], the door will open. In case if the mobile is not available or off then the option to open the door is to answer the security question ask by system.

Smart Card Based System

A model entryway security framework [2] is intended to permit an authorized person for getting a safe (without need of any key) entryway where valid card of smart RFID is necessary for ensuring the pass of the door. Total control activity is performed by the microcontroller.

Door Phone Based System

The earlier system, a specific system in which identification of a visitant is done for the most part by direct communication with the set of the housing estate concerned [9]. A dialling up to the sets over the handsfree telephone is created by the framework at the entryway. Visitors enter inside through the gate by controlling the gate with the help of the telephone set. The latest system is based on video door phone surveillance which is used to identify the visitors, developed by Chau-Huang Wei et. al. [10]. The work utilized a novel powerline communication chip for build up a digital networked video door phone. Moreover, they exchanged audio and visual information and upgraded the passageway guarding capacities.

Bluetooth Based Systems

Bluetooth based system is a bit like sarvy house innovations that utilizes Bluetooth function available in smart devices [11]. The framework using Bluetooth turns out to be more simple and productive for proper utilization. Such systems are generally based on Arduino platform. The hardware of such framework is the combo of android smart phone and Bluetooth module. Arduino microcontroller here is acting as a controller and solenoid can be acting as output of locking system.

Social Networking Sites Based Systems

A specific work [12], the digitalization and safety perspectives were accomplished by utilizing the phone device and web camera. The model can empower a pin to close and open a door from allotted region using SMS from a (social networking site) like Facebook, Whatsapp etc. Recently, a new digital door lock system [13] get designed. At the moment, if wrong password gets detected more than the specified times, the system catches the picture of the unknown visitant and sends it to the owner through smart device. In this manner, increases the strength of the security function.

Biometric protected System

The palmtop recognition is the next step for fingerprint recognition. It [14] operates on the image of palmtop. Firstly system takes an image of the palmtop then it works on that image by partitioning it and process is required. At the end, verify the right person. Except fingerprint recognition the vein detector and iris scanner gives best and accurate result so, in the bank security system [15], microcontroller continuously monitors the Vein Detector and Iris Scanner through keypad authenticated codes. During night the wireless motion detector will be active, if any variation occurs in its output, it will be sensed by the controller and alert sounds will be given by it. Recently, the fast based principal component analysis approach is proposed in which the modification of principal component analysis approach for the face recognition and face detection process is done [16]. The image is captured by the web camera and it gets matched with the image stored in the database. New advanced door lock security systems are available based on the pattern of the human iris for providing a high level of security. And to make the system more efficient n reliable the simulation is done in MATLAB [17]

Motion Detector Based System

he Motion Detector System [18] working is based on the principle of amount of light falling on the photodiode. At the point when the laser light is falling constantly on the photodiode, its reading is 255 in decimals. But when it's hindered by deterrent, the voltage falls less than 50 in decimals. This flames the alarm and gives notification to the owner about the break in. And automatic lock can be activated.

VB Based System

Electronic eye [4] represents the model for capturing the door images with the help of microcontroller to ensure the safety for offices and houses. In this system, the image gets captured when the door is opened and these images are displayed by using VB application on computing system.

Combined System

The locker security system consisting of RFID, FINGERPRINT, PASSWORD and GSM technology [5] containing door locking frameworks which can be used without much of a stretch, initiated, authenticated and validated by the authorized person. It unlocks the locker door in real time manner.

SCOPE AND PROPOSAL OF THE WORK

Among all the security systems established, the password authentication and fingerprint biometric methods are widespread in most parts of the world where security applications are required. Some of the drawbacks associated with these methods are explained as follows.

Drawbacks on password system

Because of high sensitivity with attacks, risk factor is very high in password based authentication process. Broadly the types of attack can be divided into three categories: - technical (brute force), discovery and social engineering. In the brute force attack, two methods can be used, (a) attempting passwords against the system, but this is easily stopped with account lockouts. (b) An offline attack against the password hash file. Password may also be compromised by discovery. Forms of password discovery may vary and include interception of a script file, an exploit on another system, a Trojan program capturing keystrokes, or the discovery of default passwords associated with other system or programs. Social engineering represents an attempt by an intruder to elicit password and account information from a user. This attack is exogenous to the computer system in question, coming via phone, fax, email or causal contact.

Drawbacks on Fingerprint authentication

Many different fingerprint biometric technologies are available today. A highly secure fingerprint biometrics may be difficult and time-consuming to use. The issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches the expectations in performance and accuracy is of great concern to designers. Above these factors, the digitalized era came up with numerous hacking phenomenons which can hack into the security system and disable or hack the biometric feature of the security system

Proposal to overcome the above drawbacks

The combined System technology was proposed as the finest system [5]. The idea of this project was provoked while calculating the results of integrating two methods instead of its combinations. Thus, the integration of the above two methods can make the security more reliable and efficient than combining the systems. In addition, making one method hidden largely increases the security override defenses.

RELATED WORK

Figure 2: GT511C3 Fingerprint Scanner (FPS)

We will be using the **Arduino Uno board** with **GT-511C3** FPS (fingerprint scanner) which is a small embedded module that consists of an optical sensor mounted on a small circuit board. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC.

System Design Interfacing

The interface of the FPS is very basic consisting of only four pins – power, ground, serial transmit and serial receive. When connecting to arduino uno microcontroller, it uses 5V voltage levels on its pins, a level converter must be used to reduce the 5V output from the microcontroller to the FPS module because the FPS module can only handle 3.3V on its UART pins. A voltage divider consisting of two resistors can be used as a level converter to reduce the 5V incoming signal to 3.3V. The circuit diagram below shows the fingerprint scanner module connected to an Arduino Uno.

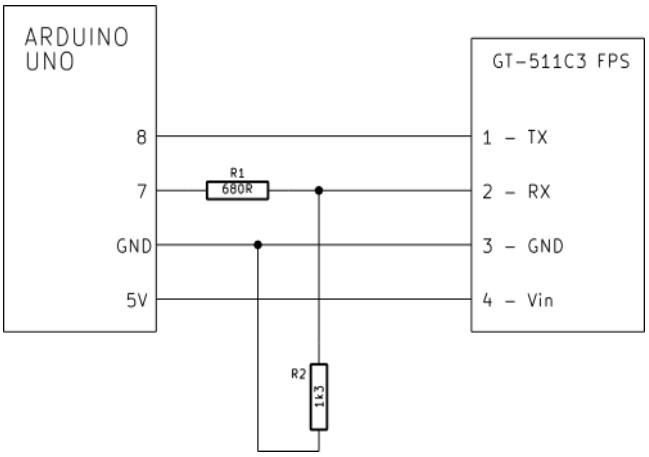

Figure 3: GT-511C3 Interfaced to an Arduino Uno

To get started, just register each fingerprint that you want to store by sending the corresponding command and pressing your finger against the reader three times. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The significant feature of this system is that It makes foreign people (other than the user) unaware of its fingerprint scanning process. Here optical finger print scanner (GT511C3) is used to read the fingerprint of the user. This method requires sensor module equal to the n pass codes. The sensors are numbered from 0 to 9 resembling the numeric digits so that they can be used as the pass codes. The FPS remains on as soon as the supply is turned on and waits for the input. When a specific finger print sensor obtains an input, the FPS (GT511C3) sends the assigned numeric value to the microcontroller. Similarly, the numeric inputs are obtained until the pass code length is satisfied. During this stage the finger print database is not used to verify the user.

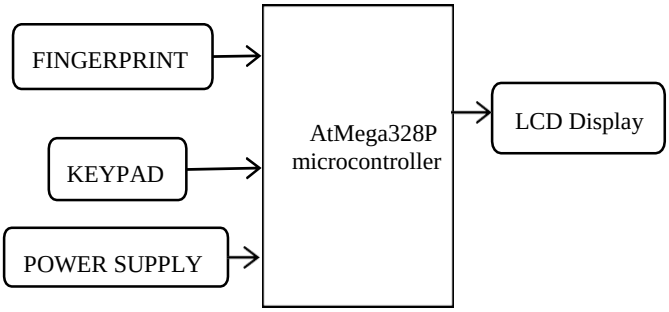

Figure 4: Block Diagram of Haptic Security System

In the above block diagram, Sensors are connected parallelly to the Arduino Uno board. Initially, when the numeric inputs are obtained, the program checks whether the password matches with the preset code. Secondly, the fingerprints obtained in each sensors are now verified with the database provided. When both the inputs(password and fingerprint) are verified, the system is a go. When the figerprint matches with database and password is incorrect, a warning is provided stating "Incorrect password". Where as, when the password stage is verified and fingerprint stage is a mismatch, the system's alarm buzzer is triggered stating "Intruder alert".

Software programs for the microcontroller

The Arduino hardware has built-in support for serial communication on pins 0 and 1 (which also goes to the computer via the USB connection). The native serial support happens via a piece of hardware (built into the chip) called a UART. This hardware allows the Atmega chip to receive serial communication even while working on other tasks, as long as there room in the 64 byte serial buffer.

The SoftwareSerial library has been developed to allow serial communication on other digital pins of the Arduino, using software to replicate the functionality (hence the name "SoftwareSerial"). It is possible to have multiple software serial ports with speeds up to 115200 bps. A parameter enables inverted signaling for devices which require that protocol.

System flow chart

The above flowchart indicates the sequential control flow programmed in the arduino microcontroller. The program is executed in this manner and the results are obtained as shown in the final step.

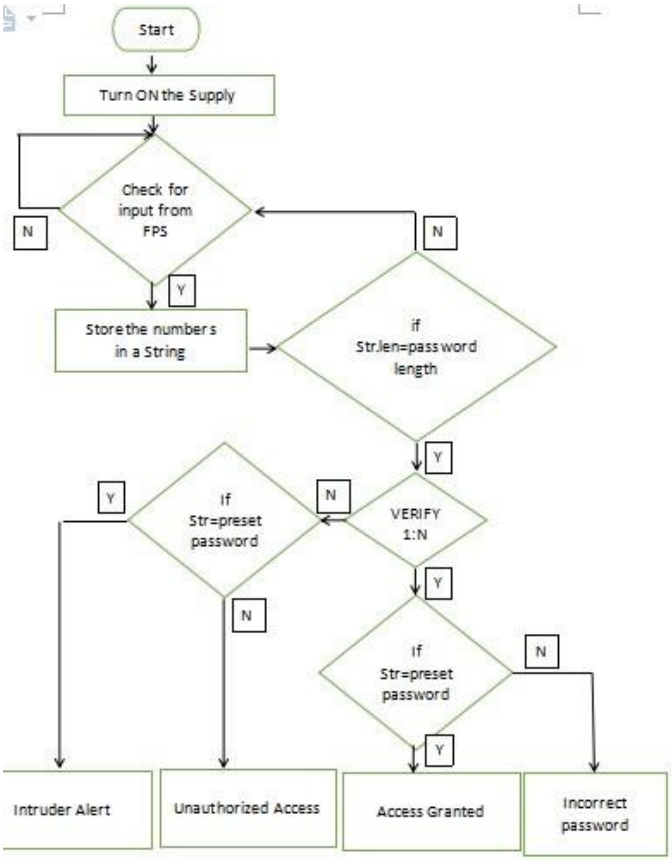

Figure 5: Flowchart of proposed work

FUTURE SCOPE

This security System can be further enhanced by adding extra features to the security module. Features such as using GSM for sending a message to the owner whenever someone enters through the System.

CONCLUSION

In today"s technologically advanced world, autonomous systems are gaining rapid popularity so the advancement in latest technology is continuously and rapidly made on different latest automatic door lock security systems. The need for an advanced door lock security systems using new technologies is increases day by day as security become a very important or serious issue for everybody. This paper

tries to focus on highly confidential door lock security systems in a comprehensive way.

REFERENCES

[1] Sadeque Reza Khan, Ahmed Al Mansur, Alvir Kabir, Shahid Jaman, Nahian Chowdhury "DESIGN AND IMPLEMENTATION OF LOW COST HOME SECURITY SYSTEM USING GSM NETWORK", International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March - 2012.

[2] A.O. Oke, O.M. Olaniyi, O.T. Arulogun, O.M. Olaniyan "DEVELOPMENT OF A MICROCONTROLLER-CONTROLLED SECURITY DOOR SYSTEM." The Pacific Journal of Science and Technology, Volume 10. Number 2. November 2009 (Fall).

[3] Seung-Soo Shin, Kun-Hee Han, Kwang-Yoon Jin, "DIGITAL DOOR LOCK ON THE ACCESS CONTROL SYSTEM USING OTP-BASED USER International Journal of Computer Applications (0975 – 8887) Volume 153 – No2, November 2016 18 AUTHENTICATION" , International Journal of Digital Content Technology and its Applications(JDCTA), Volume 7, Number 11, July 2013.

[4] Saurabh Vinayak Lawate, M. S. Ali, "ELECTRONIC EYE FOR SECURITY SYSTEM", International Journal of Electronic and Electrical Engineering, Volume 7, Number 9 , 2014.

[5] Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi , "LOCKER OPENING AND CLOSING SYSTEM USING RFID, FINGERPRINT, PASSWORD AND GSM", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) , Volume 2, Issue 2, March – April 2013.

[6] Oke Alice O., Adigun Adebisi A., Falohun Adeleye S., and Alamu F. O. , "DEVELOPMENT OF A PROGRAMMABLE ELECTRONIC DIGITAL CODE LOCK SYSTEM" , International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 02– Issue 01, January 2013 .

[7] Mohammad Amanullah "MICROCONTROLLER BASED REPROGRAMMABLE DIGITAL DOOR LOCK SECURITY SYSTEM BY USING KEYPAD & GSM/CDMA TECHNOLOGY", IOSR Journal of Electrical and Electronics Engineering (IOSR - JEEE), Volume 4, Issue 6 (Mar. - Apr. 2013).

[8] Miss. Pradnya R. Nehete, Kantilal P. Rane "A PAPER ON OTP BASED DOOR LOCK SECURITY SYSTEM" , International Journal For Emerging Trends in Engineering and Management Research (IJETEMR) , Volume II, Issue II -21st June 2016 (ISSN NO: 2455-7773)

[9] K. T. Lau,Y. K. Choo "A MICROPROCESSORBASED GATE SECURITY SYSTEM" IEEE Transactions on Consumer Electronics, Vol. 35, No. 4, NOVEMBER 1989.

[10] Chao-Huang Wei and Shin-An Chen, "VIDEO DOOR PHONE SURVEILLANCE SYSTEM USING POWERLINE COMMUNICATION CHANNEL" , International Journal of Computer and Electrical Engineering, Vol. 5, No. 4, August 2013.

[11] Lia Kamelia, Alfin Noorhassan S.R, Mada Sanjaya and W.S., Edi Mulyana , "DOOR-AUTOMATION SYSTEM USING BLUETOOTH-BASED ANDROID FOR MOBILE PHONE" , ARPN Journal of Engineering and Applied Sciences , VOL. 9, NO. 10, OCTOBER 2014.

[12] M. R. Navya* and Prakash Ramachandran " DEVELOPMENT OF SECURED HOME AUTOMATION USING SOCIAL NETWORKING SITES" , Indian Journal of Science and Technology Vol 8(20), IPL0116, August 2015.

[13] Ilkyu Ha, "SECURITY AND USABILITY IMPROVEMENT ON A DIGITAL DOOR LOCK SYSTEM BASED ON INTERNET OF THINGS" International Journal of Security and Its Applications, Vol.9, No.8 (2015).

[14] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, " AN ADVANCED DOOR LOCK SECURITY SYSTEM USING PALMTOP RECOGNITION SYSTEM", International Journal of Computer Applications (0975 – 8887), Volume 56– No.17, October 2012.

[15] S.Ramesh, Soundarya Hariharan and Shruti Arora "MONITORING AND CONTROLLING OF BANK SECURITY SYSTEM", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[16] 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), Volume-1, Issue12, November 2013.

[17] M.Gowsalya, M.Sangeetha, K. Sri Dhivya Krishnan, N.Divya, T.Devika "A NOVEL APPROACH AUTOMATIC DIGITAL DOOR OPENING AND CLOSING SECURITY SYSTEM", International Journal of Innovative Research in Electrical , Electronics, Instrumentation and Control Engineering , Vol. 2 Issue 2, Feb 2014.

[18] Nikhil Agarwal, G.Subramanya Nayak, "MICROCONTROLLER BASED HOME SECURITY SYSTEM WITH REMOTE MONITORING", International Conference on Electronic Design and Signal Processing (ICEDSP),2012.