NEW HORIZON
COLLEGE OF ENGINEERING

Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade.

CARD BASED SECURITY SYSTEM

A MINI PROJECT REPORT

SUBMITTED BY

Faizal.F-1NH18EC712

in partial fulfillment for the award of the degree of

BACHELOR

OF

ENGINEERING

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

NEW HORIZON
COLLEGE OF ENGINEERING
Autonomous College Permanently Affiliated to VTU, Approved by AICTE & UGC
Accredited by NAAC with 'A' Grade.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEER

CERTIFICATE

Certified that the mini project work entitled "**Card Based Security System**" carried out by **Faizal (1NH18EC712)**bonafide students of Electronics and Communication Department , New Horizon College of Engineering, Bangalore.

The mini project report has been approved as it satisfies the academic requirements in respect of mini project work prescribed for the said degree.

Project Guide HOD ECE

_____ _____

External Viva Signature with Date

Name of Examiner

1.

2.

ACKNOWLEDGEMENT

The satisfaction that accompany the successful completion of any task would be, but impossible without the mention of the people who made it possible, whose constant guidance and encouragement helped us succeed.

We thank **Dr. Mohan Manghnani**, Chairman of **New Horizon Educational Institution**, providing necessary infrastructure and creating good environment.

We also record here the constant encouragement and facilities extended to us by **Dr.Manjunatha**, Principal, NHCE and **Dr. Sanjeev Sharma**, head of the department of Electronics and Communication Engineering. We extend sincere gratitude to them.

We sincerely acknowledge the encouragement, timely help and guidance to us by our beloved guide Dr.A.B.Gurulakshmi to complete the project within stipulated time successfully.

Finally, a note of thanks to the teaching and non-teaching staff of electronics and communication department for their co-operation extended to us, who helped us directly or indirectly in this successful completion of mini project.

Faizal (1NH18EC712)

LIST OF FIGURES

Abstract: *Over the years, access systems with digital card have become more and more sophisticated and several security measures have been employed to combat the menace of insecurity of lives and property. This is done by preventing unauthorized entrance into buildings through entrance doors using conventional and electronic locks, discrete access code, and biometric methods such as the finger prints, thumb prints, the iris and facial recognition. In this project, a prototyped door security system is designed to allow a privileged user to access a secure keyless door where valid smart card authentication guarantees an entry. The model consists of hardware module and software which provides a functionality to allow the door to be controlled through the authentication of smart card by the microcontroller unit.*

I. Introduction

Access control using door security systems has been in existence in prehistoric times, the systems used then were of different standards ranging from the simple bolt and crossbars to intricate locks which were hand crafted by locksmiths and other practicing professionals. As time went by these systems evolved with improvements on the flaws of the previous generations.

The most recent advancement or trend in door security technology consists mainly of authentication (providing a piece of private information) systems. These systems include Biometrics, Passwords, Bluetooth mobile devices, Memory cards, Smart cards etc.

Despite the high level of security offered by the biometric system it is expensive to implement and the password system is a one factor authentication system as such it is not highly reliable.

This project therefore presents a prototype of a door security system designed to allow a privileged user to access a secure automated door where valid smart card and passcode authentication guarantees an entry.

In the proposed system an automated door is controlled with a card reader and the card reader is controlled by a control program embedded in a microcontroller unit. Implementing the system with a microcontroller will be of great value, cheaper, portable and much benefit to organizations who consistently seek a better means of door access control for their firm

II. LITERATURE SURVEY

Door lock security systems are classified based on technology used as
1) Password based

2) Biometric based

3) GSM based

4) smart card based

5) RFID based

5) Door phone based

6) Bluetooth based

7) Social networking sites based

8) OTP based

9) Motion detector based

10) VB based

11) Combined system.

- **Password Based Systems**

The programmable electronic code lock device [1] 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.

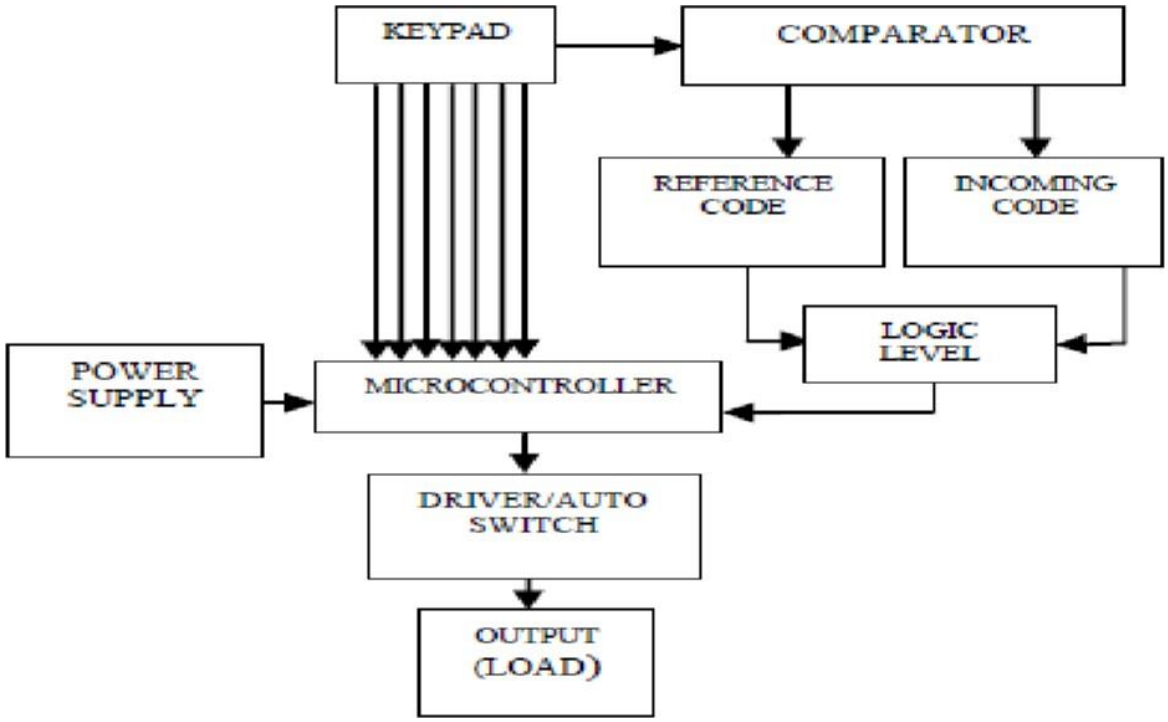

Fig 1: Programmable Electronic Code Lock

- **Biometric Based System**

The palmtop recognition is the next step for fingerprint recognition. It 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. Hence, it reduces the chances of error in other human recognition methods and clarifies the problems which were faced in the fingerprint recognition. The biometric technique is very useful in bank lockers. Except fingerprint recognition the vein detector and iris scanner gives best and accurate result so, in the bank security system, 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. 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

- **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 [12] 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. A recently created model for security of door [13] easily controlled like remote control operations by a GSM hand set acts as the transmitter and the other GSM phone set with the DTMF associated with the motor attached to door with the use of DTMF decoder, a stepper motor and microcontroller unit. Nowadays people want to be secure though they are away from home so, the work proposed by Jayashri Bangali et. al. When the owner is not at his home, security of home and important things is the big issue in front of all. Two frameworks were created which depends on GSM based technology. For detection of the gate-crashes, it takes place by capturing image through web camera. When peoples are not at their homes, the system sends notification in terms of SMS to the crisis number. A novel administrator-based system can login without any stretch to the system and can see guests record and listen their recorded messages and also automatically lock the door using mobile communication technology.

- **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. 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. 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 savvy house innovations that utilizes Bluetooth function available in smart devices [24]. The framework using Bluetooth turns out to be simpler and more 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.

- **Motion Detector Based System**

The Motion Detector System 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 its 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 [33] 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 is as shown in Fig 4 in view of RFID, FINGERPRINT, PASSWORD and GSM technology [34] containing door locking frameworks which can be without much of a stretch, initiated, authenticated and validated by the authorized person. It unlocks the locker door in real time manner.

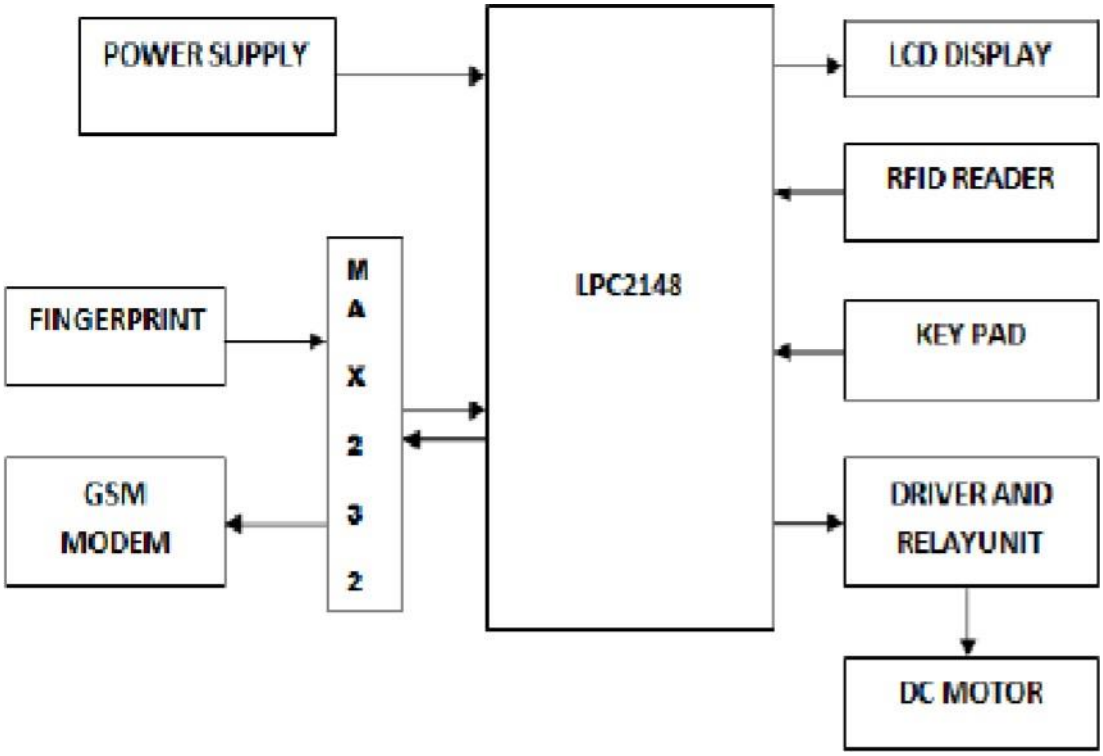

Fig 2: Locker Security System

III. PROPOSED METHODOLOGY

- **Smart Card Based System**

A model entryway security framework 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.

- **RFID Based Systems**

These types of security systems used for digital door lock are utilizing inactive RFID tags (passive). With the help of this, it ensures that only valid person can get entry. Such systems are working in real time basic for opening the door in which user have to place the tag in contact with RFID detector, then the entryway gets opens and in the central server the registration data is stored with necessary data of the users. Attendance and person tracking are possible by using such type of system. RFID Based Gate Access Security System which points out authorized peoples and permits just them was effectively created by K.Srinivasa. This system ought to have the capacity to minimize the trained or specialized human error during secured door access. Latest RFID based door lock security system are based on Arduino platform with audio acknowledgement at the point when card put close to the RFID module, it peruses

IV. System Design

The design and construction of this system consist of a hardware design module, an application program (firmware) for microcontroller unit and a database designed using Microsoft Access 2007 and Visual basic 6.0 for users‟ credentials authentication. The firmware and the database make up the software design module.

Components of the hardware design are shown in Figure 3

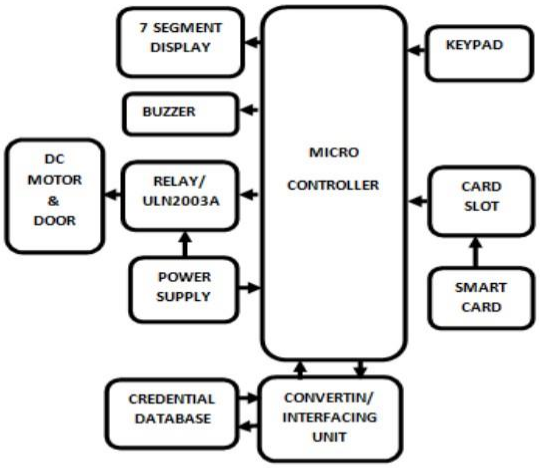

Figure (1): System Block Diagram

Figure 3. System Block Diagram

DC Motor and Door System

The servo motor and door system are attached together; they constitute part of the output unit of the Access control system.

The door system is made of a dark glass sliding door of about 680mm × 450mm and thickness of 0.3mm. The door is fitted on a door post of 740mm × 495mm × 80mm frame made from aluminium steel where the door slides on. The door system is attached to the motor and placed on a rail on which it slides. The direction of movement depends on the polarity of the voltage supplied by the switching unit.

The dc motor is responsible for the movement of the sliding door; the motor used in this design is a 40W 12V 4000mA dc motor.

The motor is connected to the switching unit (the relay section) and the power supply unit. If the power supply results in a positive voltage the motor rotates clockwise, if it results in a negative voltage the motor rotates anticlockwise (see figure).

Relay Section

The relay and ULN2001A (relay driver) are responsible for all the switching operations of the electronic access door.

The operation of the relay depends on the voltage and current rating. The voltage rating is the voltage

that is applied across the terminals of the electromagnet, while the current rating is the maximum current that it can withstand. The relay rating for this project is 12V dc, 10A.

For a relay to function and be controlled properly, especially in a digital circuit, a relay driver is required for interfacing of TTL signals with high voltage loads. In order to achieve this, ULN2001A chip was used. The ULN2001A is a monolithic high voltage and high current Darlington transistor arrays.

Two relays were used to achieve clockwise and anticlockwise rotation of the dc motor attached to the sliding door. The centre tapped terminals of the relays are connected to both ends of the dc motor. They are then

interlaced with the microcontroller via pin 1 and 2 of ULN2001A (see figure 2).

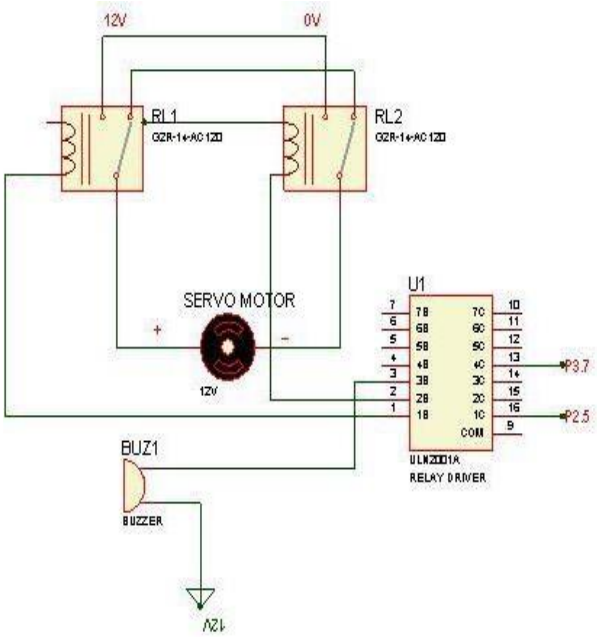

Figure 4: Relay and Relay Driver (Switching) Unit.

Power Supply Unit

The power supply unit is responsible for providing electromotive force (EMF) to power the circuit components that make up the system. The power supplies were designed to convert high voltage AC mains electricity to a suitable low voltage supply for electronic circuits and other devices.

The system requires two power supply system, a 5V/500mA dc supply to power the microcontroller and a 12V/4000mA to drive the relay and the motor (load).

Figure(3) below shows the power supply configuration used to power and drive the dc motor used in this design, it requires a current of 4000mA, in order to achieve this, two centre tap Ac 220/240V, 50Hz. Dc 2 × 12V/1.5A transformers were connected in parallel to double the output current of the dc supply

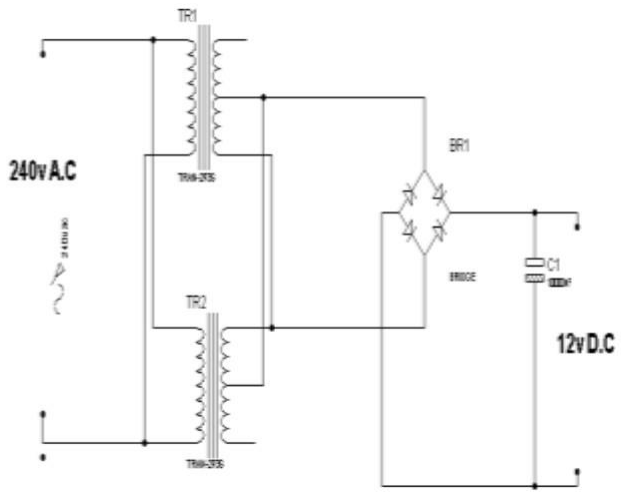

Figure 5: 12V (4000mA) Power Supply Configuration.

Microcontroller Section

The microcontroller section constitutes the control and monitoring unit which is responsible for handling all the system operations. It receives data from the input unit processes it and then transmits the processed information to the appropriate unit where they are to carry out one function or the other.

The microcontroller used in the fabrication of the electronic access control system is the AT89c52 a variant of the 8051 microcontroller architecture, it comes with a wide range of features which makes it accessible to a wide range of applications.

Smart Card Unit

For the smart card unit, a prototype smart card was designed, this was achieved by mounting AT24c64 EEPROM on a Vero board of size 4.5 × 3.5 cm.

A single line data program was stored in the EEPROM to enable the microcontroller read and write data into the device via an 8 bit expansion slot that was gotten from the system board of a computer monitor.

Keypad

The keypad is a part of the input device used in this security system to input authentication digits. A 4×4 matrix keypad was used in this project; at the lowest level, keypads are organized in a matrix of rows and columns. The microcontroller accesses both rows and columns through ports; therefore, with an 8-bit port a 4x4 keypad which has 16 keys requires a single port or 8 I/O lines to be interfaced to a microcontroller. When a key is pressed, a row and a column make a contact; otherwise, there is no connection between rows and columns.

TABLE (1): Keypad Connection to the Microcontroller

PORT 3.2 (D0)	Key 1	Key 2	Key 3	Key 4
PORT 3.3 (D1)	Key 5	Key 6	Key 7	Key 8
PORT 1.2 (D3)	Key 9	Key 10	Key 11	Key 12
PORT 1.3 (D2)	Key 13	Key 14	Key 15	Key 16
	PORT 1.7	**PORT 1.6**	**PORT 1.5**	**PORT 1.4**

Buzzer

The buzzer makes up the alarm system which sounds each time a button is pushed on the keypad, it comprises of a 5V buzzer with a maximum current of 20mA and driven by the ULN2001A IC, when there is a 1 at the out terminal the buzzer will not sound and when there is a 0 the buzzer sound.

Converting and Interfacing Unit

This unit is responsible for the communication between the microcontroller and the computer.

When developing projects that use microcontrollers, it is always helpful to have the microcontroller communicate with a computer for data logging, debugging or boot loading purposes. Serial communication is quite popular because most microprocessors have UART (Universal Serial Asynchronous Receiver Transmitter) hardware already built in. Most microcontrollers operate at logic voltage levels (0 to 5V DC) and uses TTL logic (transistor to transistor logic), whereas the standard computer serial port (RS232) operates at -12v to +12v DC. Connecting a microcontroller directly to the serial port will instantly damage the circuitry inside of it. Most people incorporate voltage level converter chips (such as the MAX 232) and the necessary capacitors into their projects so they can communicate with the computer, this can be expensive and very time consuming.

Communication between the microcontroller and the computer was achieved in this project by using a special universal serial bus (USB) to logic level converter, the CA-45 Connectivity Adapter Cable (PL 2303HX USB to UART RS232 COM CABLE MODULE CONVERTER), with the drivers installed, every time the USB to Logic Level converter is plugged into the computer or hub, a new COM port is automatically created in the computer and assigned to the USB to Logic Level converter cable. The microcontroller can then communicate with the computer software as if it were communicating over a simple serial port.

The CA-45 adapter has four cables. The red cable is connected to a 5V supply (V_{cc}), the black cable is connected to ground (GND), the green cable which is for data transmission (TXD) is connected to P3.0 (RXD) of the microcontroller, while the white cable which is for receiving data (RXD) is connected to P3.1 (TXD) of the microcontroller.

V. Software Design

Microcontrollers are just silicon wafers until they are programmed on what to do according to requirement.

Microcontroller programming is a term used to describe a set of instructions which is provided by the manufacturer to aid the development of user (application) programs.

The source code for the microcontroller used in this design was written in an assembly language, and converted to Hex code with the aid of MIDE 6.0 and the Hex code was burned into the microcontroller via an electronic device known as Machine code loader/programmer.

The users‟ database which is used to assign password and monitor access to the security door was developed using Microsoft Access. Visual Basic was used to develop the administrator interface and house the users‟ database because of its ability to communicate to the serial port of the computer using an in-built communication protocol known as MSComm control.

V. System Circuit Diagram

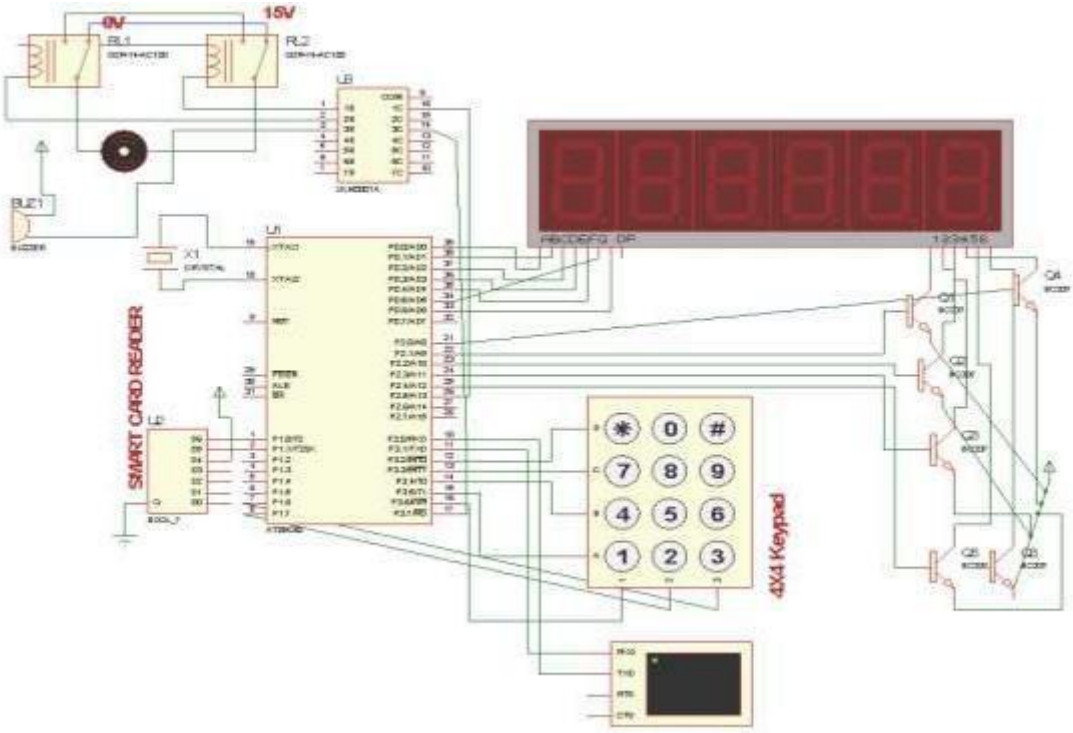

Figure 6. System Circuit Diagram

VII. Circuit Operation/Process Description

The circuit is powered up by connecting its power supply terminal to a 240/220V ac source, the seven-segment display immediately lights up. The AT89s52 microcontroller checks for the

presence or absence of an access card (in this case an EEPROM mounted on a 4.5 × 3.5 Vero board), if no card is detected it sends appropriate signals to the display unit, these signals are in the form of voltage pulses which are recognized by the LED seven segment display. This unit then displays „ENTER CARD“. The verification process continues to loop until a valid card is inserted into the card reader.

When the card is inserted into a smart card reader, it makes contact with an electrical connector for „reads and writes to“ from the chip, it is via these physical contact points, that transmission of commands, data, and card status would take place.

When a credential (smart card) is presented to the reader with the card corresponding passcode, the reader sends the credential“s information, usually a number, to the control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to the database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel through a microcontroller operates a relay which completes the circuit of a servo motor that in turn unlocks the door.

When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked. The reader would provide a feedback through a seven-segment display to show when access is granted or denied. (See system flow chart below).

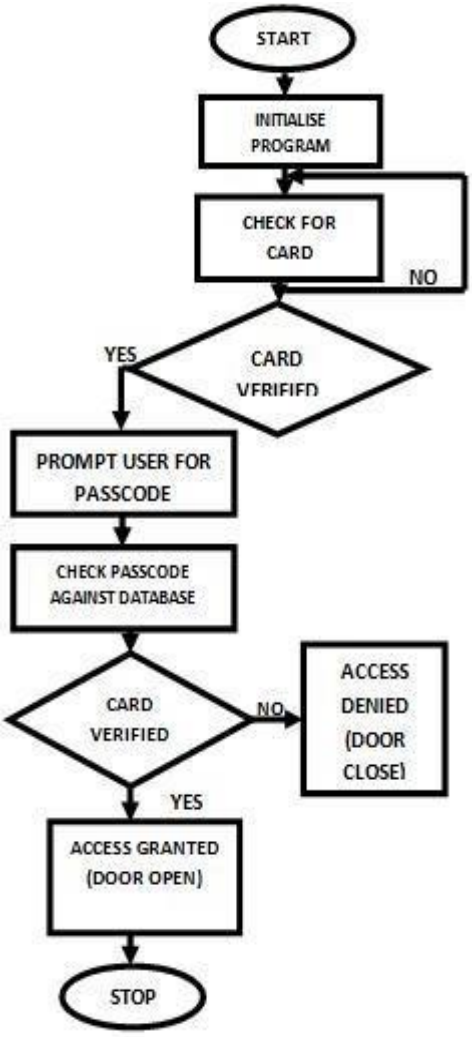

FIGURE 7: SYSTEM FLOW CHART

VIII. Result

FIGURE 8: OVERALL SYSTEM/DESIRED OUTPUT

The system has a controller PC which contains the record of the check-in and check-out of the user. User must have RFID tag which contains the personal information of that particular user. A door along with locking system is driven by stepper motor. Stepper motor acts as actuator, which is able to open and close the door in real-time. The RFID Reader detects tag in real-time and

open door automatically and closes it again after a specific time interval. In this application, user authentication information is searched on the database first. If the user does not have any previous record registered to the database, the door will not be open thus unauthorized entries will be avoided.

In this work we have successfully implemented security system which can be apply to record attendance in class room of institute or can deploy in secured zone so that only authentic person can enter in secure space. Once the user information matched with information stored in central database system, then user only can enter within the confined place as the door will open only when the tag information match with the database. The system can be deploy in various secure places within a building. The system is also able to maintain the record of a user such as how many time and what time user check-in and which area. All the databases are stored in database server as well as local server. Administrator can access database server remotely through internet or intranet and can see all the records.

IX. Conclusion and Future Scope

Conclusion

The outcome of this study will represent the major achievements and promising avenues for future enhancements in the iris segmentation stage of the iris based biometric authentication system, which are likely to yield useful results. Biometrics can be used in verification and in identification mode. In identification mode, biometric sample is taken for further recognition purpose and in verification mode; the biometric system is used to authenticate the user's individuality.

Sometime it becomes difficult to recognize a user directly as noise may be present in iris images. Iris is a reflective mirror and is located behind the cornea. The iris images or templates are disturbed by most common noise factors that result of non-cooperative image capturing processes. There are nine causes that are considered for noise: the iris obstruction by eyelids (NEO), eyelashes (NLO), specular (NSR), lighting reflections (NLR), poor focused images (NPF), partial (NPI), out-of iris images (NOI), off-angle iris (NOA) and motion blurred irises (NMB). During feature extraction phase, the uniqueness and discriminative level of the characteristics will determine the reliability of the recognition system. Therefore, unnecessary information must be discarded. A quantifiable set of features may be assigned to each of iris pattern obtained in this step,

which will allow the computation of similarity measure between two iris patterns. The matching performance of a recognition system may also be affected by intra-class and inter-class variation and improper user interaction.

The basic approach of this study is to design a secure and effective technique for personal authentication on noisy iris recognition. The proposed iris segmentation technique to handle Noisy Iris Images consist six modules, namely determine the expected region of the iris using K-means image clustering algorithm; Apply the Canny Edge Detection algorithm; Apply the Circular Hough Transform on the binary edge image and find the Cartesian parameters; Localization of Upper eyelid; Localization of Lower eyelid; Isolate the specular reflections and remove the pupil region to make the IRIS recognition accurate.

For experimentation and implementation, a dataset of UBIRIS v1, UBIRIS v2 and CASIA-IrisV4 iris image database has been used and the evaluation results clearly demonstrate that the proposed iris segmentation technique provides better accuracy in iris recognition rather than existing techniques for noisy iris images. This proposed technique can be used to improve an iris recognition system performance with non-cooperative images capturing in non-ideal conditions.

The performance of the proposed iris segmentation framework is compared with existing techniques for noisy iris images with the help of parameter like Accuracy, Execution Time and Equal Error Rate (EER). The results clearly demonstrate that the proposed iris segmentation technique provides better accuracy and execution time rather than existing techniques.

To secure iris template, a hybrid protection mechanism is proposed. The proposed hybrid protection mechanism is comprised with proposed iris segmentation technique followed by non-invertible feature transformation and key-binding biometric cryptosystem. During the whole process, a random key will be generated by using Pseudo Random Key Generator; encode the key by applying Error Correction Encoder and store the resultant value into codeword. Resultant codeword and iris

template will be integrated applying Key-binding biometric cryptosystem using fuzzy commitment scheme.

Establishing the individuality of a person with assurance is becoming precarious in a number of applications in an interconnected society. Biometrics is being gradually integrated in variety of applications categorized into three main sections 1) Commercial applications such as Internet access control, e-commerce, e-banking, ATMor credit card, Login on Computer, mobile phone. 2) Government applications such as registration of birth, death, voter etc. driver licence, passport, national unique identity card as AADHAAR etc. in India for social welfare distribution. 3) Forensic science applications such as criminal enquiry, corpse identification, missing children etc.

The proposed iris segmentation technique for noisy iris images as well as the proposed hybrid protection mechanism to secure iris template are the extension of existing traditional exploration process.

Future Scope

To make the study more useful and effective the following suggestion have been proposed for further improvements in this area

I. To develop improved algorithms and data capturing sensors to reduce the level of failure to enrol and failure to acquire rate.

9. To concern segmenting noisy irises when the lower or upper eyelids and eyelashes cover the pupil of the iris, which is currently not handled?

K. To work on optimization of the code, so that the segmentation software can run-in real-time applications.

Λ. To study additional type of noises like off-angle iris images may be more useful. A low quality and degraded eye images have been considered here.

M. To concern to security analysis of the proposed hybrid mechanism on noisy irises when the lower or upper eyelids and eyelashes cover the pupil of the iris.

X. REFERENCES

[1] 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 .

[2] 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).

[3] Ashish Jadhav, Mahesh Kumbhar, Mahesh Walunjkar, *"FEASIBILITY STUDY OF IMPLEMENTATION OF CELL PHONE CONTROLLED, PASSWORD PROTECTED DOOR LOCKING SYSTEM"* , International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 6, August 2013.

III. P. K. Gaikwad, *"DEVELOPMENT OF FPGA AND GSM BASED ADVANCED DIGITAL LOCKER SYSTEM"*, International Journal of Computer Science and Mobile Applications, Vol.1 Issue. 3, September-2013.

JJJ. Annie P. Oommen, Rahul A P, Pranav V, Ponni S, RenjithNadeshan, *"DESIGNAND IMPLEMENTATION OF A DIGITAL CODE LOCK"*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014.

KKK. Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K.Dubey, *"PASSWORD BASED SECURITY LOCK SYSTEM"*, International Journal of Advanced Technology in Engineering and Science, Volume No.02, Issue No. 05, May 2014.

LLL. E.Supraja, K.V.Goutham, N.Subramanyam, A.Dasthagiraiah, Dr.H.K.P.Prasad, *"ENHANCED WIRELESS SECURITY SYSTEM WITH DIGITAL CODE LOCK USING RF &GSM TECHNOLOGY*", International Journal of Computational Engineering Research, Vol 04, Issue 7, July – 2014.

MMM. 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