International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

SMART LOCK

Veena A. Patil
Asst. Prof. Dept. of CSE
BLDEA's Dr. P. G. H CET
Vijayapur

Darshana S. Khilari
Dept. of CSE
BLDEA's Dr. P. G. H CET
Vijayapur

Akhilesh S. Sheelavant
Dept. of CSE
BLDEA's Dr. P. G. H CET
Vijayapur

***Abstract*— Smart Lock is a digital door lock which works on the basis of a Microcontroller and provides multilevel security from high-tech technologies being adapted by technically sound thieves. The proposed work is to build a system that provides security which is simple, smart and affordable. The Locking and Unlocking operations on a door are secured and controlled by the system with the help of unique OTPs. The OTPs are sent to the registered mobile number(s). Smart Lock allows a user to remotely lock and unlock the door by using GSM technology. The system is equipped with IR sensor which acts as an Intrusion Detection System (IDS). Sensor monitors the closing and opening of the door and sends alert to the registered user in the event of security breach. The Smart Lock system provides another way to alert the breakdown of security using a burglar alarm system. The major components of the system are Arduino Development Board (ADB), DC Motor, 16x2 Liquid Crystal Display, 4x4 Matrix Keypad, IR Sensors and GSM SIM900A.**

Keywords—**Arduino Development Board (ADB), GSM SIM900A, 16X2 LCD, IR Sensor, OTP, high-tech technologies, 4X4 Matrix Keypad.**

I. INTRODUCTION

BURGLARIES have always been the matter of concern for house owners. Very few owners can afford for installing strict security alarm systems while others have patrolling dogs to guard their individual property. Proposed work is to provide smart security that is simple, affordable and as safe as possible using keyless entry locks. Existing systems have demonstrated the use of NFC based door lock systems that have restrictions on the range between the door lock and the portable device used to operate it. The intellectual motive of the work is to provide remote access to the door lock. The proposed work features an Intrusion Detection System (IDS) by implementing sensor. If the security of the door lock is breached in the absence of house owner(s) then, the information of security breach is sent to the registered number and also alerts the society about the breakdown of security using a burglar alarm system, spontaneously.

Embedded system plays a vital role in the proposed work. An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints.

Properties of typically embedded computers are:

- Low power consumption.
- Small size.
- Rugged operating ranges.
- Low per-unit cost.
- Efficient output.

Modern embedded systems are often based on microcontrollers (CPUs with integrated memory or peripheral interfaces).

A. Percieved usefulness

Microcontroller board designs produced by several vendors forms the basis of Smart Lock system. The microcontroller provides set of digital and analog I/O pins that can interface to various shields (expansion boards) and other circuits. The board features serial communication interfaces, including Universal Serial Bus (USB), for loading programs from personal computers. Arduino IDE is used for programming the microcontrollers which is based on a programming language named Processing, which also supports the languages, C and C++.

The microcontroller of an Arduino is pre-programmed with a boot loader (optiboot) that simplifies uploading of programs to the on-chip flash memory. This makes using an Arduino more straightforward by allowing the use of an ordinary computer as the programmer.

B. Ease of use

In our proposed system, use of the following tools has made it user friendly.

- Arduino Duemilanove
- Arduino IDE
- IR Sensors
- GSM SIM 900A
- 16X2 LCD
- 4X4 Matrix Keypad
- DC Motor

C. Framework

In this paper we develop keyless lock and its corresponding executive. Section II specifies previous work. Section III describes various tools and technology implemented by our

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

system. Section IV introduces OTP and Master Password. Section V illustrates the structure of the system and its operation with detailed explanation of methodology. Finally, Section VI concludes the paper with discussion of the proposed work.

II. PREVIOUS WORK

Since we target to develop a secure key for our proposed system in this paper, we present the relevant work next. In recent years, many smart home security systems have been proposed. For example, in [1] user identity and door security is managed using innovative handwriting recognition technology. Smart phones are used for security system management and control actions. The identity confirmation is performed in two stages. In the first stage, the user name and password verification is done. In the second stage, a pre-recorded text or symbol pattern is used. After successful identification in the second stage, the user is given permission to pass through the door.

In paper [2] the system uses ZigBee network as its backbone. A network of sensor nodes which are deployed at appropriate places at home is used. Also, the power conditions of major home appliances are controlled using ZigBee modules.

The system proposed in the [3] uses the Bluetooth on android mobile devices. Locking, unlocking, or checking the status of the door are performed using commands that are sent from the mobile device via a simple, easy to use GUI. The system then acts on these commands, takes the appropriate action and sends a confirmation back to the mobile device.

The proposed work in [3] offered a very restricted range of operation since it was built using Bluetooth. The system proposed in [4], overcomes this by using Wi-Fi. The system uses Arduino. The lock and unlock operations are performed using Wi-Fi on a mobile device. It surely overcomes the disadvantage of short-range but to a small extent.

The study of existing systems disclosed some of the major and common disadvantages as listed below-

- A common password is used to lock/unlock doors.
- Most of the existing systems require physical presence.
- Some systems do not include IDS (Intrusion Detection System).
- Most of the NFC devices can be easily hacked.
- Biometric authentication methods require a large amount of time and financial outlay to collect the biometric data from the intended users.

Along with the above mentioned disadvantages, the study of high-tech systems revealed some more disadvantages:

Card Technologies

Several types of card encoding technologies are now available with the following options and considerations:

- Secured conversion of data into the code.
- Susceptibility of the card reader to environmental damage.
- Resistance of the reader to vandalism.
- Cost – initial and long term.

Disadvantages of using such technologies are as follows:

- Easily lost as they are light weighted, small in size.
- Possible risk of identity theft.
- More expensive to produce and use.
- Replacement of cards is time consuming.

Magnetic Stripe

This used to be the most widely used system. Today, proximity cards have overtaken magnetic stripe units. It is the same application commonly used on ATM cards. Although these systems are relatively inexpensive, they are one of the most insecure cards. Use of this technology is restricted to least secured domains. For high-security areas, this type of card should be used in combination with a biometric device like a PIN pad or hand geometry reader. This type of technology is also subject to wear because of contact between the card and reader and vulnerability to the environment.

A disadvantage of the magnetic stripe cards is that they can easily be cloned or counterfeited by use of magnetic stripe encoders, which are readily available via the Internet.

Bar Code

Like magnetic stripe cards, this technology is not extensively used because converting the data into the code is least secured and there are high chances of getting damaged. This technology can be easily compromised. Bar code readers are encoders that are readily available via the Internet.

Hollerith

This system is golden aged technology which is still in use. Data is fed on to the card by punching holes in the card. End user scans the card by either passing light through the holes or by fine contact brushes that connect with an electrical contact. It is very inexpensive, but its disadvantage is low in security.

Do We Need Fingerprint and Retinal Scanners?

Of all the biometric authentication methods available, fingerprint and retinal scanners have long been considered the pinnacle of such technology, offering a virtually full-proof way of granting permissions to the right individual. After all, without taking drastic steps there is no way to mimic a person's fingerprint and retina. Combine this biometrics with a password and you have a near-perfect way of maintaining appropriate security for authentication or verification of a person.

However there remain issues concerning this type of technology. For instance it is expensive to install and requires

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

a large amount of time and financial outlay to even collect biometric data from the intended users.
After the study of all the systems & technologies discussed so far, we have come up with a technical-idea which aims at developing a new system which would overcome some of the major and considerable disadvantages thrown by the existing systems.
The following section (Section III) introduces various tools and technologies used by the Smart Lock system.

III. TOOLS AND TECHNOLOGY

The selection of tools & technology that the system is going to use is an important task. The tools and type of technology used by the system has significant effect on the system functionality and its performance. In order to build a cost-effective system, the selection of type of tools is important. The selection of the below discussed tools has made the system not only user friendly but also cost effective.

Arduino Duemilanove

The Arduino Duemilanove ("2009") is a development board based on the ATmega328P (datasheet). As shown in the Fig. 1, it has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. It includes Atmel's ATmega328P Microcontroller with 32kb flash memory working at 20MIPS, on-board motor driver for connecting 2 DC motors or 1 stepper motor, PC interface for UART communication through virtual COM port by FT232RL IC.16 MHz external crystal. It has separate power supply option for Motor & Board. Power supply option for microcontroller can be provided through DC source (6V to 16V, 1Amp) or USB. It includes two Rx & Tx surface mounted LEDs for UART receive & transmit indication and two supply indicator LEDs for microcontroller supply & motor supply. On board USB programming provision is through FT232RL USB to Serial converter.

Arduino IDE

The Arduino Integrated Development Environment (IDE) or Arduino Software as shown in the Fig. 2, contains a text toolbar with buttons for common functions and a series of menus. It connects to the ADBs to upload programs and communicate with them. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino the message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom right hand corner of the window displays the configured board and serial port.

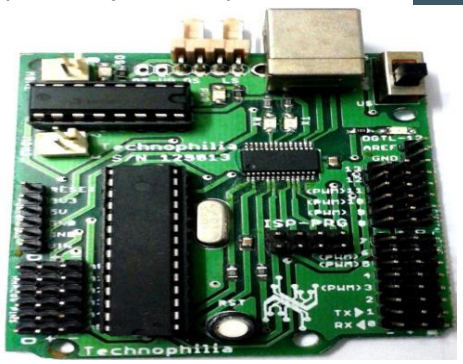

Fig. 1. Arduino Duemilanove

The open-source Arduino Software (IDE) makes it easy to write code and upload it to the board. It runs on Windows, based on processing and other open-source software. This software can be used with any Arduino board.

IR Sensors

The system uses IR sensor to detect the closing and opening of a door. Fig. 3 shows a typical IR sensor used by the proposed system. IR sensor uses LED which produces light at the same wavelength as what the sensor is looking for. When an object is close to the sensor, the light from the LED bounces off the object and into the light sensor. This results in a large jump in the intensity, which we already know can be detected using a threshold. The working of IR sensor is explained below.

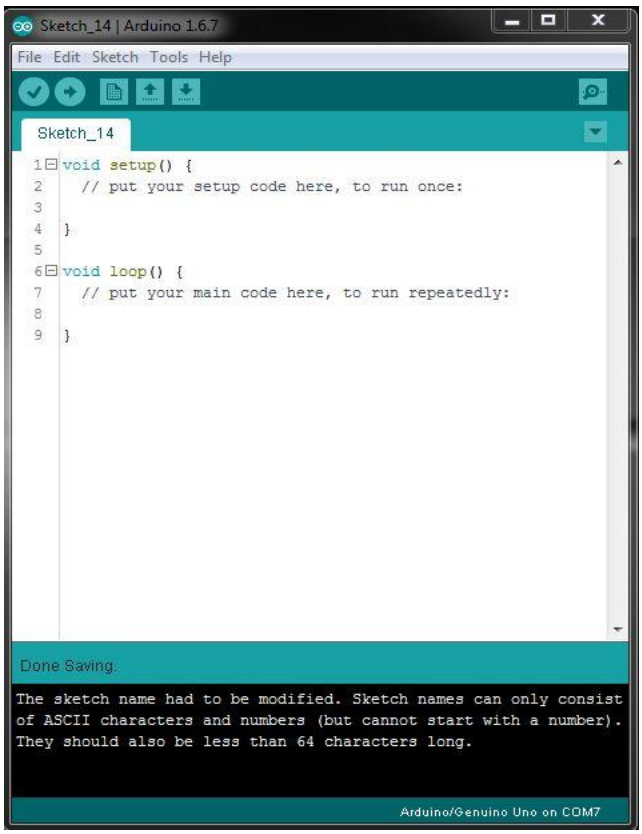

Fig. 2. Arduino IDE

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

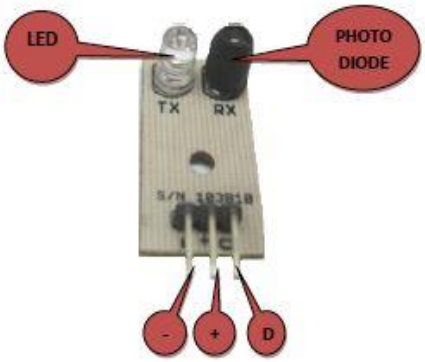

Fig. 3. IR Sensor

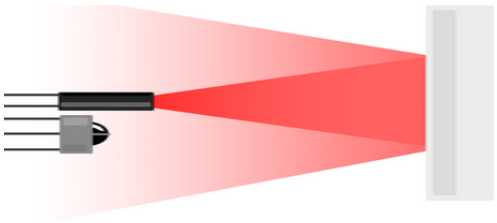

Fig. 4. Bright objects reflect more IR light

The LED emits high intensity red light when current flows through it. If the emitted light of LED falls on any bright surface it is reflected back to the photo diode (see Fig. 4). Photo diode is a device which is able to detect the light intensity and convert it to a corresponding electric current. Other devices present in the board read the electric current generated from the photodiode and convert it to a logic voltage level which is either logic-0 or logic-1. Thus, depending on the presence or absence of the surface, logic data is developed by the light sensor.

GSM SIM 900A

The GSM (Global System for Mobiles) is a world-wide standard for digital cellular telephony, or well-known standard for Digital Mobile Telephones. GSM/GPRS Modem- RS232 (see Fig. 5) is built with Dual Band GSM/GPRS engine-SIM900A, works on frequencies 900/1800MHz. The Modem is tied up with RS232 interface, which provides a way for direct connection to PC as well as microcontroller with RS232 Chip (MAX232). The baud rate is configurable from 9600-115200. The configuration is done through AT command. The GSM/GPRS Modem is having internal TCP/IP stack to enable you to connect with internet via GPRS. It is suitable for SMS, Voice as well as DATA transfer application in M2M interface.

Unlike mobile phones, a GSM modem doesn't have a keypad and display to interact with. It just accepts certain commands through a serial interface (through Rx and Tx pins) and acknowledges for those. These commands are called as AT commands. There is a list of AT commands to instruct the modem to perform its functions. Every command starts with

Fig. 5. GSM SIM900A

"AT". That's why they are called as AT commands. AT stands for attention. The proposed system uses the GSM module to send and receive messages from a user. The below shown table (Table I) lists some of the common AT commands used by our proposed system.

TABLE I
AT COMMAND AND DESCRIPTION

Command	Description
AT+CMGD	DELETE SMS MESSAGE
AT+CMGF	SELECT SMS MESSAGE FORMAT
AT+CMGL	LIST SMS MESSAGES FROM PREDEFINED STORE
AT+CMGR	READ SMS MESSAGE
AT+CMGS	SEND SMS MESSAGE

16X2 LCD

A liquid-crystal display (LCD) is a flat panel display, electronic visual display, or video display that uses the light modulating properties of liquid crystals. The Fig. 6 shows a typical 16X2 LCD. Its low electrical power consumption enables it to be used in battery-powered electronic equipment. The following are some advantages of using LCD:

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

- Very compact and light.
- Very little heat emitted during operation, due to low power consumption.
- No geometric distortion.
- The possible ability to have little or no flicker depending on backlight technology.

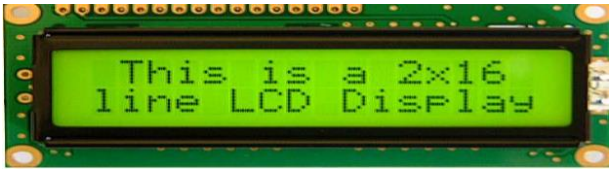

Fig. 6. 16X2 LCD

4X4 Matrix Keypad

Typically one port pin is required to read a digital input into the controller. When there is a lot of digital input that has to be read, it is not feasible to allocate one pin for each of them. This is when a matrix keypad arrangement is used to reduce the pin count. The Fig. 7 shows the 4X4 matrix keypad used by the proposed system.

It consists of 16 keys internally acting as switches, SW0-SW15 (see Fig. 8). When one of the 16 keys is pressed, a pair of pins is connected together. We will use this feature to detect which key was pressed.

DC Motor

The Fig. 9 shows a typical DC Motor. The system uses a 300rpm DC motor for the lock arrangement. It has the following specifications.

- Voltage: 12V Dc
- RPM: 300
- Current: 57.6mA
- Reduction: 1:280
- Shaft length: 7mm double-flat
- Size: 55x48x23 mm
- Weight: 32grams

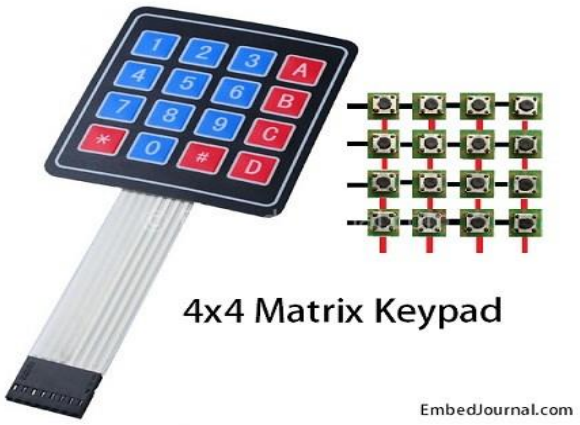

Fig. 7. 4X4 Matrix Keypad

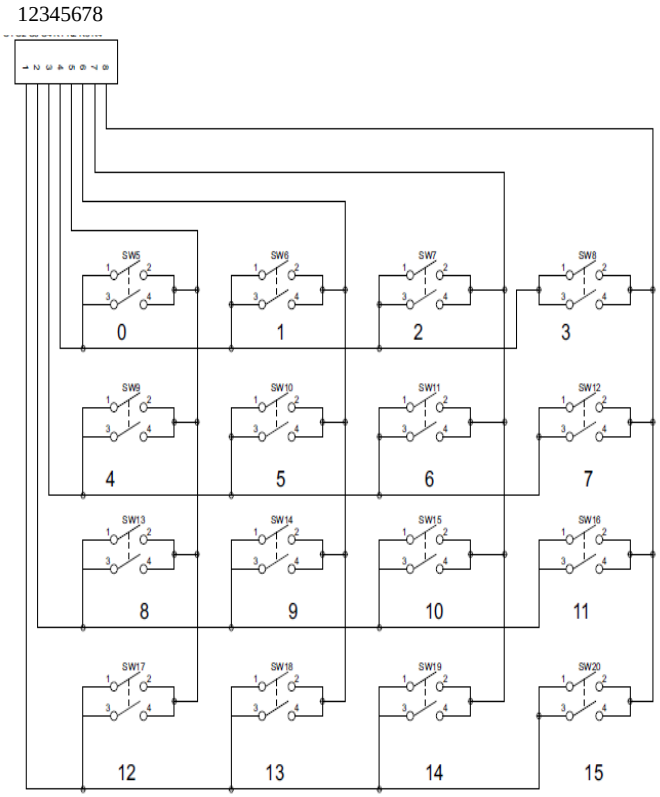

Fig. 8. Keypad Internal Connection

IV. OTP AND MASTER PASSWORD

Our system provides multi-level security. To achieve this, the system implements OTPs. It also allows a user to set a master password which is used in the event when the user loses his/her mobile. The door to which the Smart Lock system is fixed, acts as central base station. In this section we focus mainly on use of master password and OTP.

A. OTP (One Time Password)

Travel is among life's greatest pleasures, but it can also become a horror story if the traveller is unprepared. A few simple, preparatory steps before your journey combined with knowledge and vigilance during your trip can make the difference between a pleasant experience and a personal or professional cyber disaster. As preparation is the key, we introduce the strong binding concept of our proposed work the OTP (One Time Password).OTP is the number sequence key which is one login session valid password. It is associated with traditional (static) password-based authentication. OTP is used to overcome the technical shortcomings of static passwords in areas like passive capturing of the data unit and its subsequent retransmission. It's highly impossible for the intruders to

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

record the OTP which is used during first login session and reuse the same to breach through security.
Our system generates 4-digit OTPs which are sent to the registered user's mobile number. The system provides two ways to generate an OTP (discussed in Section V).

Fig. 9. DC Motor

B. Master Password

Smart Lock maintains a 4-digit Master Password which is specially meant for use in the case if user loses his/her mobile. The user can lock the door using OTPs as well as master password. However, when the door is locked with master password, the generation of OTPs is disabled until & unless the user unlocks the door by entering the master password through keypad. The user is provided with an option to change the master password. The use of master password adds one more level of security.

V. STURCTURE AND OPERATION

In this section, we first provide the block diagram followed by the system architecture and its operation.

A. System Overview

Smart Lock is a digital door lock which provides multilevel sucurity. The system requires the user to generate an OTP and use it to pass through the door. The system's operation is controlled by a microcontroller and it acts as the functional core. Fig. 10 shows the block diagram of the system.

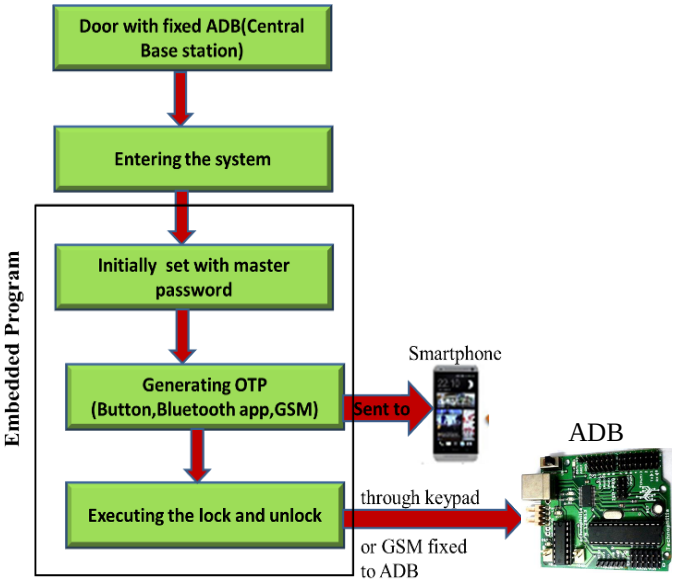

Fig. 10. Block Diagram

When the system is run for the first time, (i.e. at the installation time) it asks the user to set a master password (see Section IV). After the master password confirmation, the system is ready for the first use. Locking and Unlocking of the door can be done either using OTP or Master Password. When the user generates an OTP, it is sent to the registered mobile number. The user can then perform locking/unlocking operations using the received OTP.

B. Architecture

The architectural design process is concerned with establishing a basic structural framework for a system. It involves identifying the major components of the system and communication between these components. In the following sub-section we delve into the design aspects and the scheme is to design and the sub systems involved in this system package. The Fig. 11 shows the overall system architecture. The system includes various modules such as Arduino Development Board (ADB), 16X2 LCD display, 4X4 Matrix keypad, IR sensor, Buzzer, DC motor and GSM SIM900A. The Atmel's ATmega328 microcontroller of ADB controls and manages all the other modules and it acts as the central core of the system. Introduction to all these modules is discussed in Section III.
The chip used here is Atmel's popular AVR Atmega328P microcontroller. Constant voltage supply of 5V is distributed in a coordinated way among ADB and its attached peripherals by a three terminal voltage regulator (5V) IC.
Two separate power supply are used to in order to drive the DC and stepper motor. The input from microcontroller is used by L293D motor driver IC which in turn drives the DC and stepper motors.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

LS (Logic Supply) provide a 2-pin berg strip with one +ve and –ve pin configuration, for either connecting a battery or an AC adaptor to supply the power to ADB. The DC voltage provided to this terminal should lie in between 6 to 16V, 1Amp. To use the supply connected at LS pin the power switch should be toggled towards "LS".

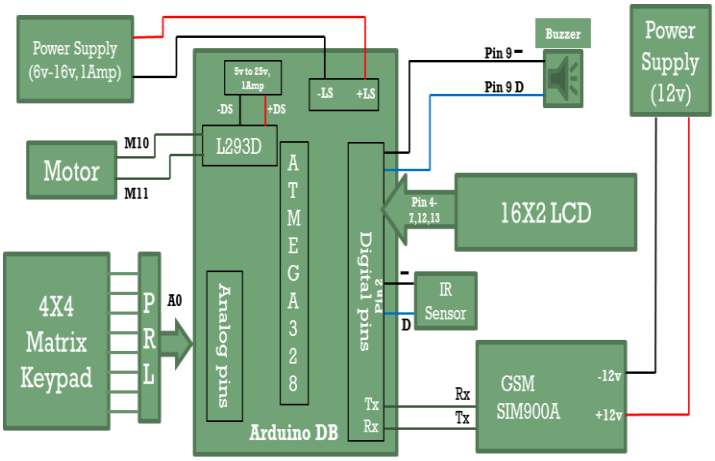

Fig. 11. Hardware Architecture

Like LS, DS (Driving Supply) is a 2-pin berg strip with one +ve and one –ve pin configuration. It provides a constant supply of DC voltage to drive the motors, which is externally supplied through adapter (12V,1Amp). This operating DC voltage should lie in the range 5-25V,1Amp. Unlike LS,DS supplies a high voltage and current to drive the motors connected to its terminal.

GSM is externally connected to pin 0 (Rx), 1 (Tx) for data transfer between the GSM and ADB. Power to the GSM is

IR sensor is connected to digital pins 2 and 3. LCD uses pins 4, 5, 6, 7, 8, 12 and 13.

PRL (Pin Reduction Logic)

The PRL stands for Pin Reduction Logic. It is a technique used to lessen the number of pins to tie up with the Keypad. The 4X4 matrix keypad has 8 pins, and 8 digital pins of the ADB are required in order to connect it to the ADB (without using PRL). Hence for efficient use of pins on the ADB, Smart Lock implements the PRL which reduces 8 pins to 1. Fig. 12 shows the implementation of the PRL.

The logic involves using different registers of values: 10 KΩ, 1KΩ and 220Ω connected to the keypad pins as shown in the Fig. 12. By doing so, the register values calculated for each key is different. To understand this, consider the example shown below.

Key 5 register value is: 1KΩ+1KΩ+220Ω

Key C register value is:
1KΩ+1KΩ+1KΩ+220Ω+220Ω +220Ω

Example for PRL

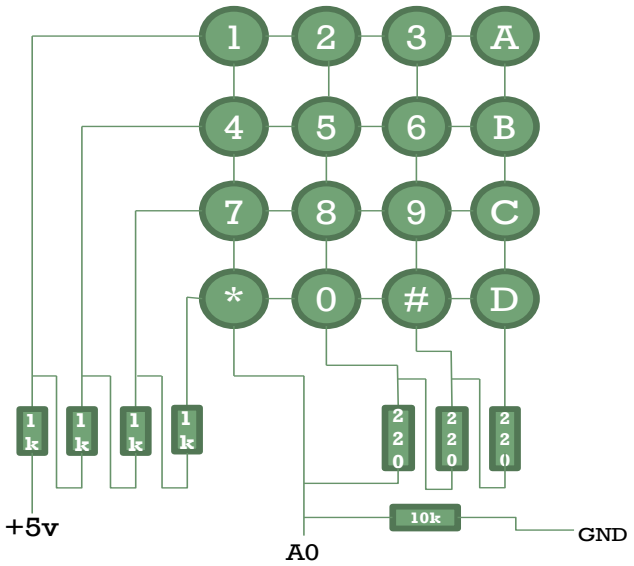

Fig. 12. Pin Reduction Logic

C. **Methodology**

The methodology describes the way in which the system works. It also describes the functionalities that are provided by the system.

As seen in the previous sections, the system includes various modules that are-16x2 LCD, GSM shield, IR sensors, DC motor with lock arrangement and a 4x4 matrix Keypad. The coordination and control of all these modules is handled by the microcontroller. It acts as the core of the system.

Lock/Unlock operations are performed on a door using unique OTPs or master password. The user needs to register his/her mobile number in the system. The OTPs and other alerts are sent to this registered mobile number. There are two different ways that can be used to generate OTPs. They are-

1. Using generate button: The Smart Lock system provides a button (or switch) that would be mounted on the door. The user can use this button to generate OTPs. This is useful in case when the user is close to the door.
2. Using predefined command: The Smart Lock system allows the user to perform locking/unlocking operations on the door from remote place. For this, the system uses GSM Technology. The system provides a set of predefined commands and their formats. These commands are used to generate OTP, lock/unlock door using the received OTP or using the master password. The following are the commands and their formats:
   - Command to generate OTP
     #gen otp/

When the above command is sent to the Smart Lock device via SMS by the registered mobile number, an OTP is generated and sent back to the registered mobile number.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

- Command to lock/unlock using the generated OTP

#otp <received_otp>/

When the Smart Lock device receives the above command via SMS, it validates the command and verifies the mobile number of the sender and performs locking/unlocking operation based on the status of the lock. After performing the operation, it sends alert back to the registered number.

- Command to apply master password

#master <master_pwd>/

This command can be used to apply master password to the "already locked" door. When the master password is applied, the generation of OTP is not allowed and generate button is disabled until the user manually enters the master password through keypad. This is mainly meant for the case when the user loses his/her cell phone. It is worth noting that the above mentioned command can be sent from any mobile number or via internet sites or apps such as Way2Sms, Hike (SMS feature) etc.

Once the user receives an OTP, there are two ways in which he/she can use it to lock/unlock the door. They are-

1. Through keypad: The user can manually enter the OTP using the keypad.
2. Using the command discussed above.

There is another case in which the user may find the master password very helpful. Consider a situation when the user is going to be out of station for some days or weeks. Now, there might occur disturbance if someone presses the generate button (which is provided on the door) unnecessarily. The user would receive unwanted OTPs. To avoid such situations the user can lock the door using master password since it disables the generate button and also it would be a secure way to lock the door when you are away.

OTPs are more secure than common passwords. However, the lifetime of OTP is more valuable. The Smart Lock device allows three attempts for an OTP. If the user enters wrong OTP more than three times, an alert will be sent to the registered number. After three attempts, the OTP will be destroyed and the user has to generate a new OTP. An OTP can be used only once and it is valid till it is used.

Smart Lock system also provides the Intrusion Detection feature. It uses IR sensors for this purpose. IR sensors detect the opening and closing or door. The logic applied is that, when the status of the door is "Locked" but the status of IR sensor indicates that the door is "Open"; it clearly is a security breach. In such accident, the system triggers a burglar alarm and also sends an alert to the user.

In order to turn off the burglar alarm, the user must unlock the door using any of the mechanisms discussed above.

The status of the door is indicated by a red LED. When the LED is on, it indicated that the door is "Locked" otherwise it is "Unlocked".

D. **Data Flow Diagram and Algorithm**

Data Flow Diagrams (DFDs) are an instinctive way of showing the flow of data and the way in which data is processed in a system. The notations used in these models represents functional processing, data stores and data movements between functions. DFDs are used to show data flows through a sequence of processing steps. The data is transferred at each step before moving on to the next stage. These processing steps or transformations are program functions when data flow diagrams are used to explain a system design. The Fig. 13 shows the DFD for the proposed system.

Whereas Algorithm shows step by step instructions that describes how exactly the data is processed within the system. This section also provides description of each step of an algorithm.

The system runs on a loop and continuously checks for inputs if any, received from the modules and change the status of the system accordingly. The Table II shows the type of inputs that are generated by the corresponding modules.

TABLE II
MODULE AND INPUT TYPE

Module	Input Type
Sensor	Digital i/p (HIGH or LOW)
Keypad	Analog input
Button	Digital i/p (HIGH or LOW)
GSM	Serial input

The microcontroller receives the inputs, processes them and performs the associated tasks. The Table III shows the associated tasks for each module's input. Any messages or cautions to the user are displayed on the LCD.

TABLE III
ASSOCIATED TASK OF MODULES

Module's Input	Associated Task
Sensor	Send alert via SMS Switch on the burglar alarm
Keypad	Verify OTP or Master Password Lock/Unlock door
Button	Generate OTP Send OTP to the registered number

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

GSM	Process the message received Lock/Unlock door Generate OTP Send OTP to the registered number Apply Master Password to the lock

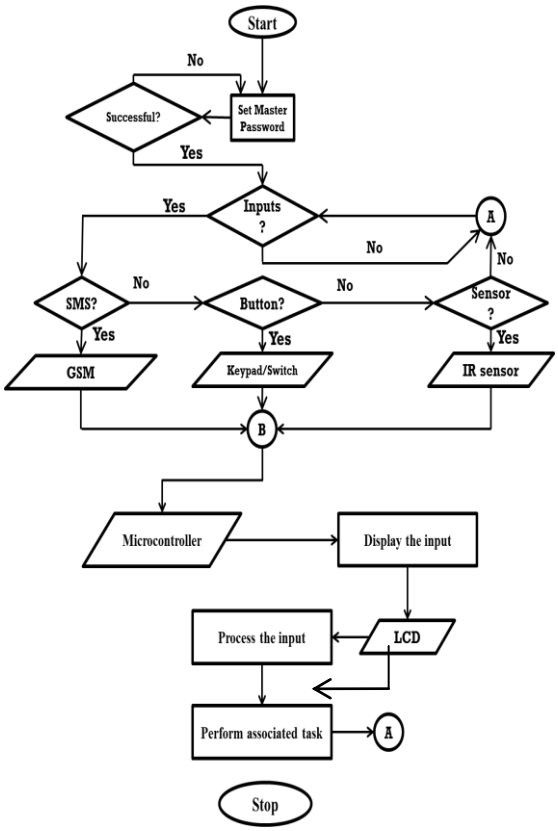

Fig. 13. Data Flow Diagram

The above DFD can be represented in the form of algorithm which includes various steps and at each step some of the system's functionality is implemented. The various steps involved and their description is as follows:

```
Step 1: Start
Step 2: Set master password
Step 3: Confirm master password
        if SUCCESSFUL
                goto Step 4
        else
                goto Step 2
Step 4: Check for inputs
Step 5: if KEYPAD
                goto Step 7
        if SENSOR
                goto Step 8
        if BUTTON
                goto Step 9
        if GSM
                goto Step 10
Step 6: goto Step 4
Step 7: if otp is GENERATED
        {
                read_keys()
                verify_OTP()
                print_appropriate_msg()
                lock_unlock_door()
                send_alert()
        }
        else if '*'
                change_master_password()
        else if '#'
        {
                read_master()
                verify_master()
                print_appropriatemsg()
                lock_unlock_door()
                send_alert()
                disable_button()
        }
        else
                print_appropriate_msg()
        goto Step 4
Step 8: if Door is LOCKED
        {
                send_alert()
                buzzer()
        }
        goto Step 4
Step 9: if generation is ALLOWED
        {
                generate_OTP()
                send_OTP()
        }
        else
                print_appropriate_msg()
        goto Step 4
Step 10: read_message()
         process_message()
         perform_associated_task()
         goto Step 4
Step 11: Stop
```

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 120-129
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

- **Step 1:** This step indicates the start of the program. In this step the following are some tasks that are performed:
  - ✓ Variables declaration and initialization.
  - ✓ Setting the baud rate for serial communication.
  - ✓ Defining the pin mode of the pins used.
- **Step 2:** This step indicates the initial action performed by the system after implementation. The system asks the user to set a master password. The following are the tasks that are performed in this step:
  - ✓ Request master password.
  - ✓ Store master password.
- **Step 3:** In this step, the system asks the user to verify or confirm the stored master password. Tasks performed in this step are:
  - ✓ Confirm master password.
  - ✓ If the master password is verified, the master password is saved and the system is initialized for the first use.
  - ✓ Otherwise, the actions in the previous step are repeated.
- **Step 4:** This describes the working mode of the system. The system runs on a continuous loop and this step indicates the opening brace of the loop.
- **Step 5:** This step indicates the actions performed when the system is working on loop. The list of actions performed is as follows:
  - ✓ Check for inputs from Keypad, Button, GSM and Sensor.
  - ✓ Perform associated task (refer Table III).
- **Step 6:** This step acts as the closing brace of the loop.
- **Step 7:** This step indicates the actions performed when the input is received from Keypad. They are:
  - ✓ Read the entered OTP or master password.
  - ✓ Verify OTP or Master Password
  - ✓ Lock/Unlock door.
  - ✓ Send alert.
  - ✓ Change Master Password.
  - ✓ Track attempts.
  - ✓ Destroy OTP after maximum attempts.
- **Step 8:** The following are the tasks performed when the input is from Sensor:
  - ✓ Check the status of the lock (“LOCKED” or “UNLOCKED”).
  - ✓ If the status is “LOCKED”, send alert to the registered mobile number and switch on the burglar alarm.
- **Step 9:** This indicates the action taken when the Generate Button is pressed.
  - ✓ Check if the Button is enabled.
  - ✓ If enabled, generate OTP and send it to registered number.
- **Step 10:** In this step, the input is received from GSM as serial input. The tasks carried out are:
  - ✓ Read the message.
  - ✓ Validation of the recipient number.
  - ✓ Verification of the message (checking command and its format).
  - ✓ Perform associated task (refer Table III).
  - ✓ Send alert back to the registered number.
- **Step 11:** This represents the stop of the execution. From the algorithm it can be noted that, this step is never reached.

VI. CONCLUSION

By observing a few key precautions, and maintaining vigilance, you will be able to delight in your journey. Our proposed system manoeuvres, a series of tactical exercises usually carried out by GSM for supervising and controlling home security and condition through the smart technology. After reviewing through the whole system it can be observed that Smart Lock system has many advantages. The major advantage here is the usage of GSM technology which allows a user to perform Locking and Unlocking operations from any locations. Also the usage of Arduino Development Board makes the system cost effective. The system delivers multi-level security by implementing OTPs. But for every advantage there exists some disadvantage too; like OTPs may suffer some delay due to network failures. But overall if observed, this greatly helps us, in turn our country to move ahead with the high speed that the world is moving in terms of development and technology.

VII. REFERENCES

[1] Kuang-Yow Lian, Sung-Jung Hsiao, Wen-Tsai Sung, “Home safety handwriting pattern recognition system”, Published in Cognitive Informatics & Cognitive Computing (ICCI*CC), 2012 IEEE 11th International Conference on 22-24 Aug. 2012, Print ISBN 978-1-4673-2794-7, pp. 477 – 483.

[2] Yong Tae Park, Sthapit P., Jae-Young Pyun, “Smart digital door lock for the home automation”, Published in TENCON 2009 - 2009 IEEE Region 10 Conference, 23-26 Jan. 2009, pp. 1 – 6.

[3] Potts J., Sukittanon S. “Exploiting Bluetooth on Android mobile devices for home security application”, Published in Southeastcon, 2012 Proceedings of IEEE, 15-18 March 2012, ISSN 1091-0050, pp. 1 – 4.

[4] Sedhumadhavan. S, Saraladevi. B, “Optimized Locking and Unlocking a System Using Arduino”.