Iot based Home Security and Automation using Random Number(Password) Generators and Face Detection

Awinash Kaushal, Akhilesh Gaur, E.Sasikala

Abstract: With evolving technology in the field of automation, the implementation of the word "Smart" on the equipments we use in our day to day life has become a sort of a fashion trend among young researchers. Smart Homes and their development are sky-rocketing in reference to controlling daily objects using voice/gesture/apps, paths which are a free flow of development which researchers tend to be inclined to. But intricate care is also given towards using this technology for developing security and safety systems. Safety and security systems are very important in daily life as they tend to be very helpful in stopping crime. Safety and Security will be achieved by a three-layer security system includes a RFID based detection system and Face Detection. This article gives intricate details on a novel Home security system implementing automation and Internet of Things.

Keywords: Arduino, ATmega 256, RFID, GSM Module, Face Detect

I. INTRODUCTION

Safety of homes against theft has become a major concern in today's world. With the increase in digitalization and modernization there has been an overshoot in the demand of smart home protection system for the ease and comfort of the user. Nowadays the use of Internet of Things (IoT) technology has developed that almost all aspects in human's life utilize IoT technology to increase the quality of life.[1] These smart homes are generally equipped with modern actuators and sensors which include the control of lights, fans, automatic pumping systems, temperature monitoring systems and security systems. The main reason behind the conversion of a simple home into a smart home is the enhancement of energy efficiency, comfortable, convenient and improved security.

With the enhancement in smart homes the security system, which is one of the major part of any system, is required to be developed in such a manner that it should be reliable, have proper protocol, have immediate action with the implementation of minimal amount of energy for its own functioning and all these characters must be implemented with lower capital costs .

For meeting these qualities and not to make the system bulky, many electronic components (i.e., different sensors, microcontrollers, supplies) must be configured with care. The choice of the components should be such that the sensing parameters are accurate and the equipment works with higher efficiency and precision.

A three-layer security system includes an RFID based detection system as the initial level of security, password protection as an intermediate level of security which is generated randomly and reached to user at fixed interval of time through GSM module and finally, a camera surveillance for face detection and access authorization. And in case of any abnormality in the process or any kind of breech found in between the process, an alarm will alert the neighborhood followed by a text message which is sent by the GSM module installed on-site.

II. LITERATURE SURVEY

Home Security has been top priority for many reasons. Muhammad Sabirin Hadis , Elyas Palantei , AmilAhmad Ilham ,Akbar Hendra have implemented a way of "Design of smart lock system for doors with special features using Bluetooth technology" [1] . Nowadays the use of Internet of Things (IoT) technology has developed that almost all aspects in human's life utilize IoT technology to increase the quality of life. Lock system is one of those aspects that has been impacted by the massive development of IoT, for example lock system that can be opened or closed by entering the password or by gadget to control it. The main component of smart home concept lays on the door, so the door lock system becomes an interesting topic to discuss

In the same way Yuhn Chin Yun designed a "A practical digital door lock for smart home" [2]. Digital door lock plays an important role on the smart home system, not only for door guardian but also for family member incoming/outgoing awareness. However, most of the current digital door locks still keep the mechanical keyhole with digital interface to fulfill the traditional habit of key usage and consequently results in the doubt of redundant interface design. For this phenomenon, we discuss the design of digital lock and propose a mechanism to keep the traditional key usage with the digital interface.

"A User-Friendly Low-Cost Mobile App Based Home Appliance Control And Circuit Breaker" [3] by Hasan U. Zaman ; Rafiunnisa ; Arafat Muhammad Shams. Along with the constant improvement of different electronic devices, the safety of technicians has also become a matter of great concern, as the lives of technicians are at risk while they work by switching off the circuit breakers,

Manuscript received on April 02, 2020.
Revised Manuscript received on April 15, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author

Awinash Kaushal, B.Tech, Computer Science , Srm Institute Of Science And Technology

Akhilesh Gaur, B.Tech, Computer Science , Srm Institute Of Science And Technology

Dr. E.Sasikala, Associate Professor, Department Of Computer Science,Srm Institute Of Science And Technology

because even after the circuit breaker has been turned off, someone can unknowingly turn it on while the technician is still working. There must be a system for ensuring security for the technicians. Also, people do not like having to walk to switches all the time to turn on/off appliances such as fan/light/air conditioner. It results in wasted energy because of unnecessarily keeping appliance on.

Based on the works of Shraddha Tiwari , Salomi Thakur , Drishti Shetty ,Abhishek Pandey -"Smart Security: Remotely Controllable Doorlock" [4] . Explains the technique of remotely controlling the door using an internet connection and a relay of messages through this connection to communicate between the owner and the system at the door. This door unlocking system aims at creating a more secure and a safe way to provide access to visitors authorized by the owner of the house into their homes. The system at the door can be controlled by any type of small single board computers. IoT is new technology which is growing fast and has many applications.

III. PROPOSED WORK

A three-layer security system with first step as RFID matching, second as password detection and random generation for enhanced security purposes and a face detection model for recognizing the authorized and unauthorized person. System uses temperature, humidity sensors for avoiding any immediate cases of fire alarm, Random password generation with changing passwords for a more secure home security. The security system design uses Arduino as the interfacing microcontroller to which different sensors, electronic components and a GSM-900 module is connected. The sensors collect the data from the surroundings and provide it as an input to the Arduino, the microcontroller the checks for all the conditions which are pre-assigned to the microcontroller and then it provides the other components with an output in accordance with the input provided. The following block diagram shows the flow of signal in between the components connected

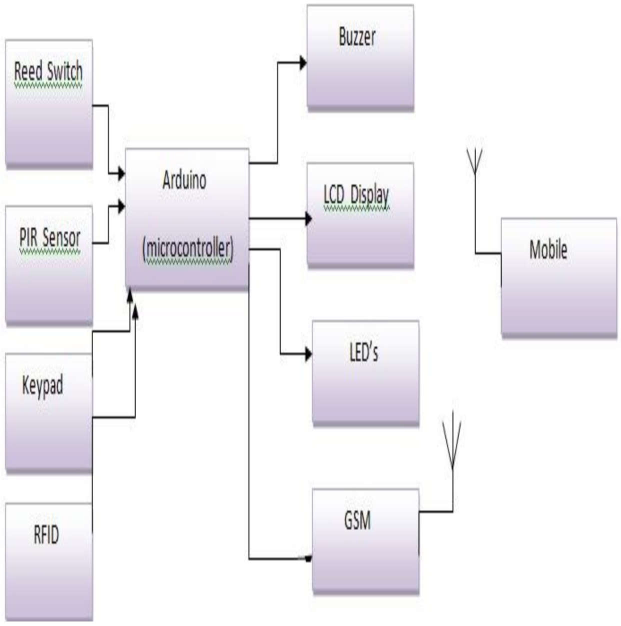


Fig-1 Block Diagram

The system designed for security purposes requires the use of many components and sensors along with Arduino and data transmission module GSM.
For the system mentioned the following components were used

1. Arduino mega 2560
2. 4x4 Keypad
3. 16x2 display
4. Buzzer
5. RFID Sensor
6. GSM Module
7. DC Motor

Aurdino mega 2560: the aurdino mega 2560 is the microcontroller board which uses ATmega 2560 for its processing. Consisting of 54 analog ports, 16Mhz crystal oscillator , incircuit serial programming (ICSP) header, an external USB ,and a power jack. The ATmega 2560 come programmed with a bootloder that permits the user to upload or modify the code using a user frindly IDE. SKT500 protocol is is used by arduino for all knds of communication purpses. Aurdino can either be cowered directly by using the usb port connected to the computer or it could also be powered by connecting an external adoptor giving a 12v output.
Memory: ATmega 2560 is s microcontroller designed to have a flash memoryof 256KB along with 8KB of SRAM and 4KB of EEPROM.
INPUT/OUTPUT: It provides the user with 54 digital pins that can be used as input or output by declearing pinMode() ,digitalRead() and digitalWrite() in the code. All the pins operates at the input voltage of 5volts, but the user could change the upper end of their range using the AREF pin and analogReference() function.
Communication: Arduino Mega 2560 board has been provided with a wide range of facilities for communicating with a computer, other microcontrollers etc. ATmega2560 IC which is used in the Arduino provides four hardware UARTs for TTL (5V) serial communication. The Arduino IDE which acts as interfacing software in between hardware and the code contains a serial monitor which permits simple textual data to be sent to and from the board. When the data is being transmitted via the ATmega8U2/ATmega16U2 chip and the computer is being connected with the USB (but not for serial communication on pins 0 and 1), then the RX and TX LEDs on the board will flash. A Software Serial library allows for serial communication on any of the Mega 2560's digital pins as shown in Fig-2.

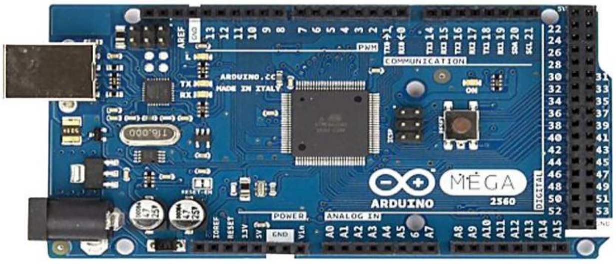


Fig-2 Arduino Mega

A 4x4 keypad: This keypad is also called as the matrix keypad. This keypad follows encoding schemes that manages to give less output pins than the keys present in them. It consists of 16 keys as shown in Fig-3, i.e., 0-9, A-D, *, #. By giving less output pins ,it makes the connections easier to understand and less chance of the error. This makes it as more efficient then other keypad. In the connection the from pin 1-4 it gives for the rows and from pins 5-8 it gives the connection to the columns.

Fig- 3 4*4 Keypad

16x2LCD Display: LCDs (Liquid Crystal Displays) have a parallel interface that supports with Hitachi HD44780 driver as shown in Fig-4. As it is have a parallel interface so it comes with several pins that are used in the microcontroller to use it properly. Some important pins are: RS pin, R/W pin, Enable pin, Data pin. As Hitachi compatibles LCDs are controlled in 2 modes: 4-bit or 8-bit, but for 16x2 LCD uses 4-bit mode.

Fig- 4 Seven segment LCD display

GSM Module: GSM (Global System for Mobile communication), are the protocols for the cellular network as shown in Fig-5. As in Arduino we can use almost as we do in the GSM phone, like give a call, send SMS. The main process is done using GSM Shield which is used to send data from serial port to the GSM Network. The shield uses the radio modem M10 by Quectel. For the working part, it uses digital pins 2 and 3 for software serial communication with M10. Pin 2 is connected with TX Pin and 3 with RX Pin .The GSM Module works on the 5V Supply. Also supply of 12V is given with the DC Adapter to power on the device. When its power on first it finds the proper signal and to setup.

Fig- 5 GSM-900

Buzzer: Piezzo buzzers are basically used to make a beeping noise, which are tethered as alarms or the tones for any system as shown in Fig-6. It is very light weight and very simple in construction. It cannot work under the frequency lower then 31Hz. A specific tone can be created by varying the frequency.

Fig-6 Buzzer

RFID Module: RFID (Radio frequency identification) is an ID system used for the identification of tracking purpose. It is a basically a tagging system that includes tag for read or write purpose and module for data collection, transmission and processing. The main principle behind the working is the use of electromagnetic fields which are transferred back and forth between the tag and the module. It works on the frequency range of 13-56 MHz, which an input voltage of 3.3v as shown in Fig-7.

Fig-7 RFID EM-18

DC Motor: The DC motor is a machine that transforms electric energy into mechanical energy in form of rotation. Its movement is produced by the physical behavior of electromagnetism. DC motors have inductors inside, which produce the magnetic field used to generate movement as shown in Fig-8

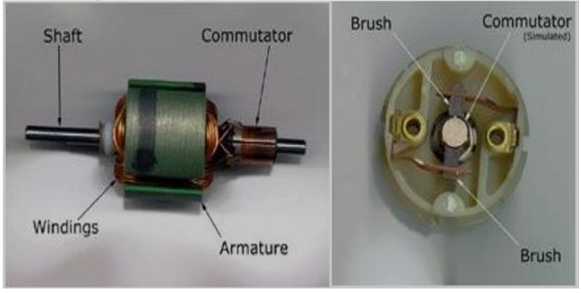


Fig-8 DC Motor

IV. IMPLEMENTATION

The system is equipped with one reed switch, PIR sensor, Keypad and a RFID to serve as input to the Arduino, it will be checking all the pre assigned condition in the code and will provide signals to the other components which involves a buzzer, an LCD display, different LEDs (as indicators), a seven segment display and the GSM module connected in the circuit.

The main structure of the prototype is shown below which contains 3 different rooms, and a garage area involving doors in all the rooms for the passage.

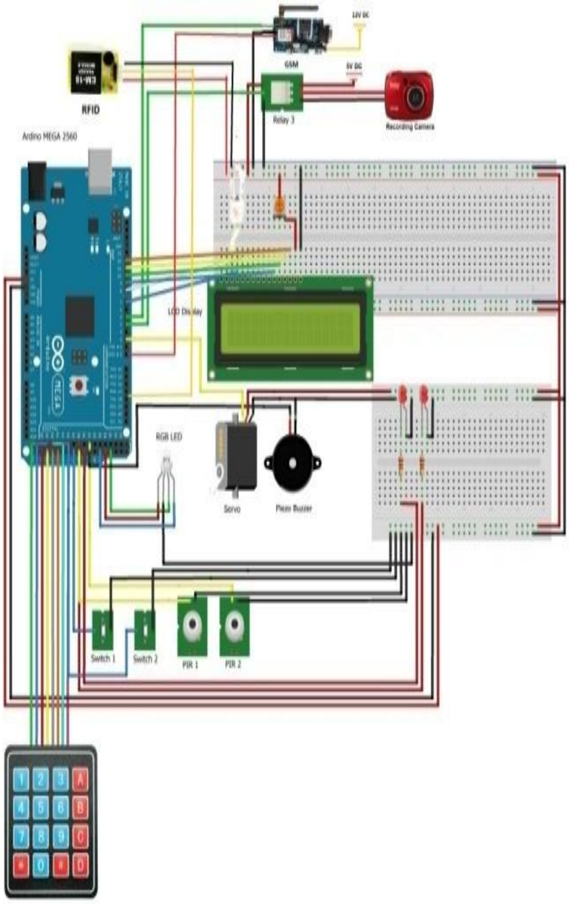
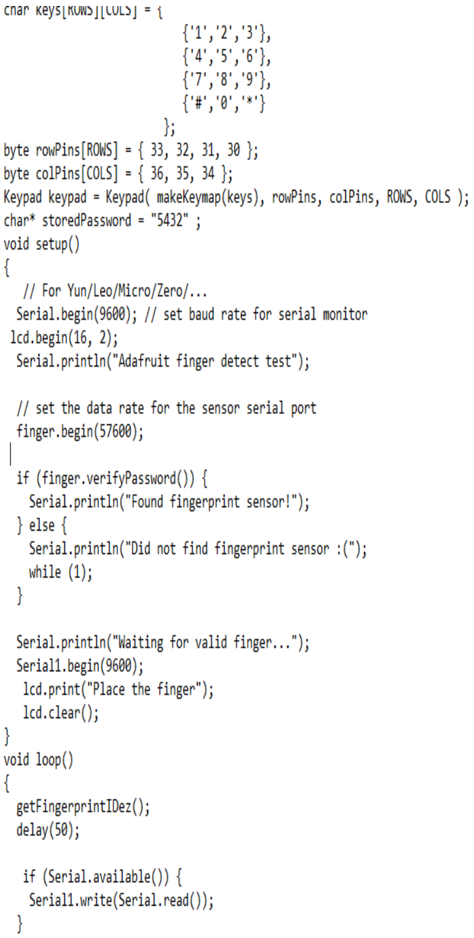


Fig-9 Circuit Diagram

Initially the code starts with checking whether the reed switch attached at the main door of the house is in the close position which as an indicator weather the door is open or closed if the switch is closed the compiler moves down to the rest of the code but in case of abnormality (the switch found open) then the microcontroller triggers the buzzer to ring an alarm, simultaneously instructing GSM to send a text message to the owner and the camera which is mounted at the top will move towards the breeched area and start recording. During the initial compiling if the switch is found close then the code is such that it allows the guest to scan the RFID tag which will be attached to the wall and then the display will be showing the initial welcome message to the guest and asks to enter the password only if the scanned tag is incorrect. The next step for the security check becomes password which is to be entered manually using the keypad provided, the password should be same as administrative password ending with #. At each interval of time, the password is generated randomly (using random number generator algorithm as shown in Fig-10) and via GSM module it reaches to user. The algorithm is such that using random library we are generating the number and it send to user using GSM.[4] If the guest enters the correct password then a green led glows along with a Access Granted message on the display on the screen and then the door gets open, in case the entered password is incorrect the it will display a invalid message on the screen and the red led glows providing three chances to the user to enter the correct password before the alarm rings and the message is sent.[2] The same procedure for which occurred for a wrong procedure or wrong password repeats if any motion is detected even the main door being closed (breech).

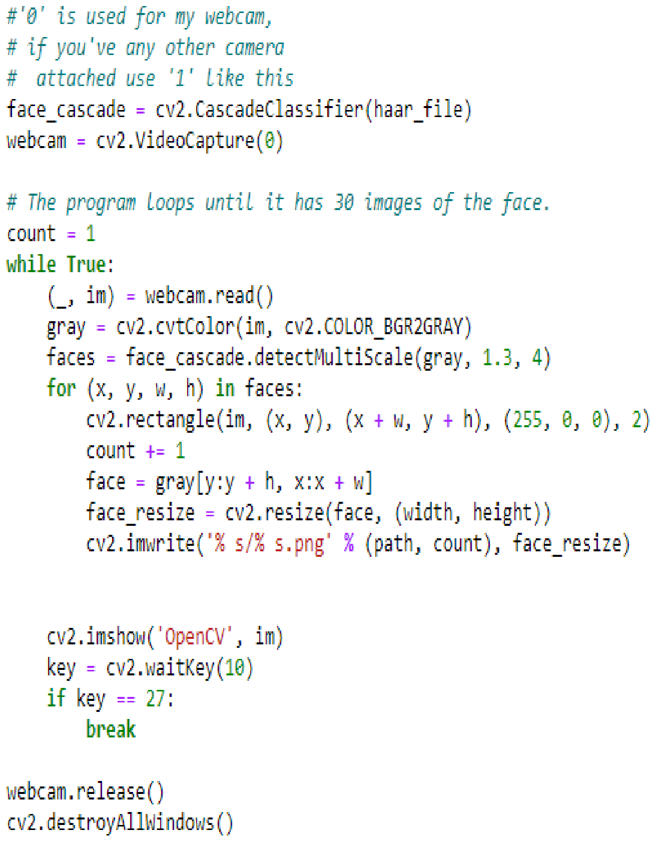


```
char keys[ROWS][COLS] = {
                            {'1','2','3'},
                            {'4','5','6'},
                            {'7','8','9'},
                            {'#','0','*'}
                         };
byte rowPins[ROWS] = { 33, 32, 31, 30 };
byte colPins[COLS] = { 36, 35, 34 };
Keypad keypad = Keypad( makeKeymap(keys), rowPins, colPins, ROWS, COLS );
char* storedPassword = "5432" ;
void setup()
{
   // For Yun/Leo/Micro/Zero/...
  Serial.begin(9600); // set baud rate for serial monitor
 lcd.begin(16, 2);
  Serial.println("Adafruit finger detect test");

  // set the data rate for the sensor serial port
  finger.begin(57600);
 |
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1);
  }

  Serial.println("Waiting for valid finger...");
  Serial1.begin(9600);
   lcd.print("Place the finger");
   lcd.clear();
}
void loop()
{
  getFingerprintIDez();
  delay(50);

   if (Serial.available()) {
    Serial1.write(Serial.read());
  }
```

Fig-10: Random Number Generator Algorithm

A camera mounted on a servo mounted is installed in the system. This camera essentially rotates in all directions covering the whole house at definite intervals. This camera can be further used to be connected to the user's mobile (generally via an app) which can be used to monitor the household wherever necessary.

Another level of security using Face detection and recognition. Face detection and recognition of the authorized person is done using the OpenCV Harr Cascade Algorithm as shown in Fig-11. The dataset of the authorized person is feed to the system and then if any person tries to open the door lock then his face detection is done if the face of person matched with authorized person then the door motor starts running otherwise if it is some intruder then security persists and person is not allowed to enter.



```
#'0' is used for my webcam,
# if you've any other camera
#  attached use '1' like this
face_cascade = cv2.CascadeClassifier(haar_file)
webcam = cv2.VideoCapture(0)

# The program loops until it has 30 images of the face.
count = 1
while True:
    (_, im) = webcam.read()
    gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
    faces = face_cascade.detectMultiScale(gray, 1.3, 4)
    for (x, y, w, h) in faces:
        cv2.rectangle(im, (x, y), (x + w, y + h), (255, 0, 0), 2)
        count += 1
        face = gray[y:y + h, x:x + w]
        face_resize = cv2.resize(face, (width, height))
        cv2.imwrite('% s/% s.png' % (path, count), face_resize)


    cv2.imshow('OpenCV', im)
    key = cv2.waitKey(10)
    if key == 27:
        break

webcam.release()
cv2.destroyAllWindows()
```

Fig-11: Harr Cascades Algorithm

Harr Cascade is a machine learning object detection algorithm used to identify objects in an image or video. Hardware and software interact to run the door motor when a person face is detected.

V. RESULT

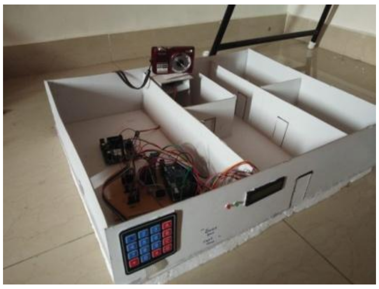


Fig-12 Side View

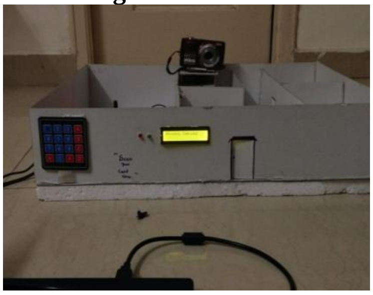


Fig -13 Front View

All three possible conditions were tested for the proper working of the hardware and the code. One using RFID tag able to access the door. Second is to enter password after RFID as 2-step verification and password is generated random by which security has incresed . Third is know whether person is known or not using Face deection. Desired results were seen and condemned.

VI. CONCLUSION

The article discusses in intricate detail about a smart home protection system which not only is useful for a small scale integrated system, but can be scaled to a larger proportionate. A cheap and effective home security system is the need of the hour in the current scenario. Most the home security systems involve the use of very expensive, heavy scale and overly emphasized components and supplements. Sometimes, some of these components are not required to be implemented for the scale of implementation but are added just to jack up the prices for eternal profit. This article has shown solutions that tackle these basic problems and the problems listed in the preceding sections. The use of Arduino, which is the cheapest and most viable micro-controller as the brain of the system is an emphasis we want to stress on. The use of very cheap components such as the GSM module, a camera (the main element of any security system) and keypad protect just work to be effective enough towards a low range security system which is capable of protecting a small area, such as a medium scale house. In-short, the system is designed to be implemented in the houses of the common man (a classic middle class house in India) where the threat of theft from daily commotions such as visitors (maids, repairmen, etc.,) is a matter of concern. Sometimes, small children are left unattended at home which also proves as a risk. Implementing the proposed model will not only ensure the child's safety, but at a reasonable cost. Hence, in conclusion, the article gives the design of a smart home security system which is scaled in such a manner that, by implementing minor changes and touches, can be implemented to any house from any sector of the population, making home security system, not just something practiced by the "Higher ups" of the society, but the vast majority of the population which is the middle class population. This paper has been written in inspiration, coming from such a background experiencing this threat on equal basis of life. Hence, we present the Smart home security system.

FURTHER WORKS

The system involves the use of Internet of Things and implements use of smart sensors and technology. In regards to this, the advancement and scalability of the system is a hit-on-the-go which means it can be easily improved and scaled to be made into an advanced system. The implementation of finger-print scanners, UV protection equipment and other large scale sophisticated systems which give highly accurate results. The system can also be improvised by the implementation of a communication network between the GSM module and the nearest local police station. All this advancement proves for a sustainable and safe future.

REFRENCES

1. Design of smart lock system for doors with special features using Bluetooth technology byMuhammad Sabirin Hadis , Elyas Palantei , AmilAhmad Ilham ,Akbar Hendra,2018
2. A practical digital door lock for smart home by Yuan Chih Yun,2018

3. A User-Friendly Low-Cost Mobile App BasedHome Appliance Control and Circuit Breaker byHasan U. Zaman , Rafiunnisa , Arafat Muhammad Shams ,2018
4. Smart Security: Remotely Controllable Doorlockby Shraddha Tiwari , Salomi Thakur , Dhristi Shetty, Abhishek Pandey,2018
5. Design and Implementation Security System for Smart Homes by M Akhil Raj, G Rakesh Reddy, Mrs.Ajitha,2019
6. Design and Implementation Low-Cost Arduino-Based Smart Security System by Souveer Gupta, Anshu Prakash, Vishwamitra in 9th IEEE Conference on communication software and network 2017.
7. Design of Small Smart Home Security Based on Arduino by Andi, Akhmad Dani in EECCIS 2014.
8. Design and Implementation GSM based Remote Home Security System by Mahumad Rana, Abdualla Ali Manu Khan in 2nd International Conference Advances in Electrical Engineering.
9. Advance low-cost Security system Using Arduino, Sensors by Vaivabhav Sharma, Chiranj Fatnani, Pranjal in IEEE TechSym 2014.
10. Intelligent Home Security System using Agent-Based IOT Devices by Takumi Kato, Hinduyeki in IEEE 4TH Global Conference on Consumer Electronics, 2015.
11. Smart GSM Based Home Automation System by R. Ozita in IEEE Conference, 2013.

AUTHORS PROFILE

Awinash Kaushal:B.Tech. in Computer Science SRM Institute of Science and Technology

Akhilesh Gaur:B.Tech. in Computer Science SRM Institute of Science and Technology

Dr.E.Sasikala:
Associate Professor
Area: Network Security, Wireless Sensor Networks, Intelligent Techniques
Department of Computer Science and Engineering, Kattankulathur Campus, SRM Institute of Science and Technology (formerly known as SRM University).

Publication work:

- Sasikala E “Device Power Consumption Avoidance Using Image Processing”, Pak. J. Biotechnol., Vol. 14 (4), pp. 607-613, 2017. (Indexed by SCOPUS)
- Sasikala E “Artificial Neural Networks with Vertical Handoff Prediction Based On User Behaviour ”, Pak. J. Biotechnol.,Vol. 15, No.1, pp. 89-93, 2018. (Indexed by SCOPUS)
- Sasikala E “ A Study on Biometric Authentication using Visual Cryptography Techniques and its application”, Journal of Advanced Research in Dynamical and Control Systems, 18 Special Issue, pp. 415-422, 2017. (Indexed by SCOPUS)

Retrieval Number: A2020059120/2020©BEIESP
DOI:10.35940/ijrte.A2020.059120
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication