# Arduino UNO and GSM Based Real-Time Home Security System Using Self- Generated Password Protection

**Soumyendu Banerjee, Evan Chowdhury, Chaitali Sikder, Debrup Sarkar, Rishab Sarbadhikary**

Department of Electrical Engineering
University of Engineering and Management, Kolkata

DOI: 10.29322/IJSRP.9.04.2019.p8827
http://dx.doi.org/10.29322/IJSRP.9.04.2019.p8827

***Abstract*— In this work, an Arduino Uno based real time home security system using self-generated password protection scheme has been proposed. The main function of this security system is to detect the presence of human being and make the user alert about it whenever it is necessary, by sending text message to user's mobile phone-number, registered previously. In the primary stage, presence of any human being will be sensed by a Pyroelectric (PIR) motion sensor and after that, the person will have to enter the right password through a keypad. The self-generated password protection provides a double-sided benefit to this system viz. any unknown person will have to prove his/her identity by entering the right password to the security system. Every time a password is used, it expires, and a new password gets generated by the system and is sent to the registered mobile number. The real time protection has been performed using a SIM 900 TTL module which sends and receives text messages between user's mobile phone and microcontroller i.e. Arduino. This security system has provided low cost and less complicated home security protection scheme by detecting any unauthorized entry to our home or any other place that needs to be secured.**

***Keywords*— *Home Security, Arduino Uno, Self-Generated Password, GSM Module.***

## I. INTRODUCTION

In this new age, while technology has enriched to a great extent, enhancement of theft and stealing is having a bad impact on society. Although it has been seen that since last few years, the forcible entry of burglar has been reduced but still the burglar entry has not been completely reduced. Therefore, in nowadays to restrict and resist these burglar activities, implementation of various security devices is a vital area of research. The security devices, which can be placed either inside or outside of house, to protect trespassing is generally known as home security devices [1].

At the early stage sound alarms were the only thing which is used as a home security system. But due to the development and advancement of technology as well as the increase in smartness of burglars, sound alarms are not enough for the home security. Hence microcontroller viz. Arduino, Raspberry Pi, PIC microcontroller etc. based home security system have become popular in these days. The components which are used for the home security systems are Arduino, GSM, Smart Vault, etc.

Arduino acts as the brain of the home security system. It is an open-source electronics platform based on easy to use hardware and software. This device senses the environment by receiving inputs from many sensors and affects its surroundings by controlling lights, motors, charger, inverter, and other actuators. Today most of the projects, innovation occur by the help of Arduino [2].

Nowadays the applications of IoT (Internet of Things) [3] are developing vastly. It is a smart system where the home appliances are connected with the internet which is operated by a user-friendly application. For example, if somebody forgets to turn off the light or fan or any other appliances in the house, they can turn it off by the help of the cell phone through wireless communication system. This is the major application of IoT. For this reason, nowadays IoT are also used as in-home security system [4-6].

Camera plays an important role in the home security system. In most of the houses and building, CCTV cameras are used which records every moment happening inside as well as the surroundings [7]. Cyber Security is a system which also helps in security but this system is mostly used in offices, banks, etc. Nowadays ATMs are protected by Cyber Security [8-9].

Global System for Mobile Communication (GSM) is a system which helps to send and receive both call and messages by the help of Arduino and other microcontroller [10-13]. This system is quietly used as a home security system. Another home security system has been developed which is Finger Print

In this project, a GSM based and Arduino Uno controlled home security system has been proposed. A GSM module named as SIM900 TTL modem with active simcard has been used. Also a security keypad has been used to provide better security to this system. Whenever any person enters home or work place or where we want to know the presence of unknown people, the presence of him/her will be detected by sensor. Now if the person is known, then he/she can put a security password on the keypad which will prove that he is a known person who has entered. But if he/she fails to provide right password, then a message will be sent to user's mobile phone to ensure that an unauthorized entry has occurred. The main objective of this project is to prevent and alert user about any unauthorised entry into the desired place. The double-sided protection has provided greater security to this work along with self-generated password scheme, which changes every time an entry occurs.

## II. METHODOLOGY

To implement this security system, user should have a mobile phone with active SIM-card. Another SIM-card is also needed

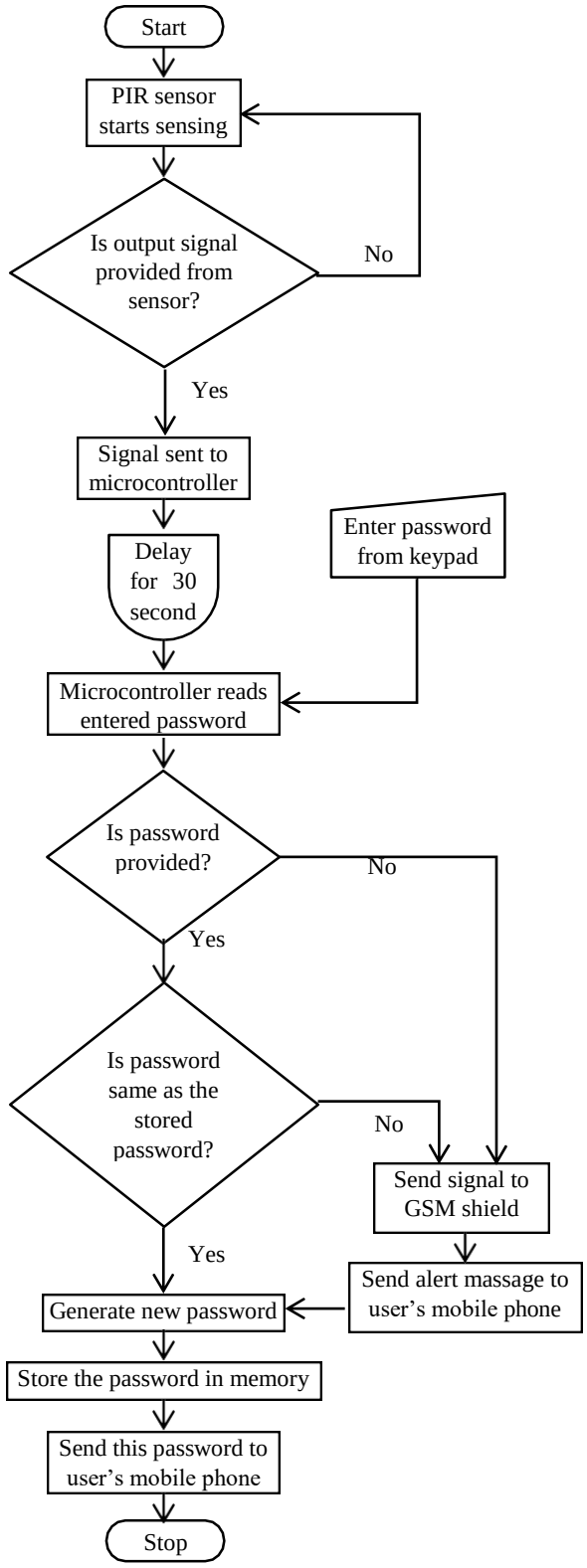


Fig.1 Signal flow diagram

to be placed inside the GSM shield with text message incoming and outgoing facility. The Arduino Uno, GSM shield is to be kept inside home with power supply on and PIR motion sensor is to be kept near door or where human presence is needed to be sensed. Fig.1 represents the signal processing flow diagram of the proposed work. Whenever human presence is sensed by PIR sensor, it sends signal to microcontroller and microcontroller waits for 30 second to receive right password, entered from keypad, failing which microcontroller sends an alert massage, using GSM module, to user's phone regarding presence of any unauthorized person. But if right password is received by microcontroller, then it generates a new password and sends it to user phone which will be treated as new password for the next time operation. The whole procedure is explained in the following five stages; 1. Motion sensing by PIR sensor, 2. Password entry through keypad, 3. GSM shield operation to send alert message, 4. Password generation and updating to user.

In the area of microcontroller based research or project works, Arduino Uno has played a vital role as a controlling device. The Arduino Uno is a microcontroller board equipped with Atmega-328P microchip and other peripheral devices and a set of input/output pins. Its working voltage is 5 Volt with operating frequency 16 MHz. Table I Shows the specifications of Arduino Uno. Now in this proposed work, Arduino Uno has been used as a primary controlling device of all other components. The connection scheme of other components with Arduino is explained in each following section.

TABLE I. ARDUINO UNO SPECIFICATION (ATMEGA328))

| | |
|---|---|
| Operating voltage | 5 V |
| Operating current | 50 mA |
| Input voltage limit | 7-20 V |
| Operating frequency | 16 MHz |
| Analog Input/output pin | 6 |
| Digital Input/output pin | 14 |
| Flash memory | 32 Kbyte |
| SRAM | 2 Kbyte |
| EEROM | 1 Kbyte |

### *A. Motion sensing by PIR sensor*

The Pyroelectric (PIR) Motion sensor can detect the change of infrared radiation coming from a hotter body thus ensuring its presence near about itself. In this work this sensor has been used to detect the presence of human being in its vicinity. This sensor needs 5-20 Volt DC supply to operate and if any motion or change in infrared radiation is sensed, it provides a high DC output voltage (almost 3.3-5 Volt), otherwise this output pin goes low ( almost zero voltage). The sensitivity range of this device is almost 6-7 meters with $110^{o}\times70^{o}$ sensation capacity.

The sensing range of PIR sensor varies between 3-7 meter, hence the sensor is to be kept in such a place so that it can sense the presence of human body inside home. The sensing range can also be controlled using sensitivity adjustment knob as shown in Fig.2 In this work, the PIR sensor has been powered from Arduino Uno microcontroller directly from Pin-11 by keeping

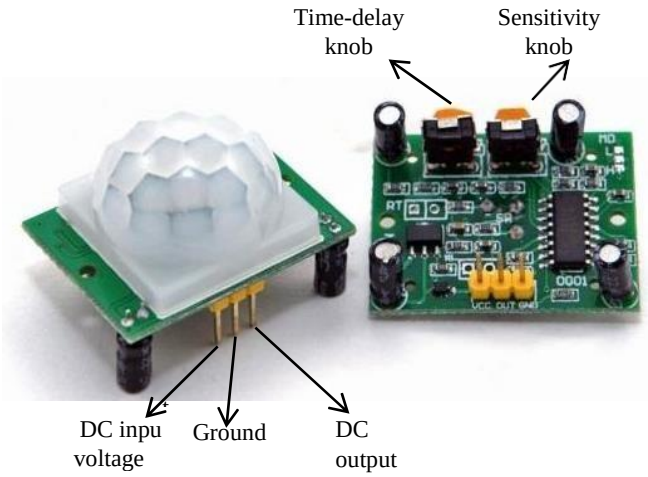


Fig.2 PIR motion sensor

this pin configuration as high output mode and the ground pin is connected to Arduino ground pin (GND). Now the output pin is connected to Arduino Pin-10. In general output signal of PIR sensor is low (viz. 0 volt) but whenever any human presence is sensed by the sensor within its range, it sends a high signal (almost 3 Volt) through its output pin which is connected through Arduino pin.

Now if human presence is sensed, then PIR sends high output signal. Arduino receives this signal and waits for 30 second for the password to be entered through keypad.

Hence, just after entering into room, the person, needs to provide the right password within this 30 second.

### *B. Password entry through keypad*

A 4×4 matrix keypad is used to manually provide 16 character viz. numeric character between '0-9', alphabet between 'A-D' and two special character '*' and '#', by pressing respective keys as shown in Fig.3. This keypad consist of total 8 pins where 4 pins is connected to each row and rest of 4 pins are connected to each column. Now whenever any key is pressed, respective row and column are activated and by detecting the row and column number, microcontroller can read, which key has been pressed.

In this work, a password of three digit is to be entered by the user manually through 4×4 keypad. Mainly the password is the proof of that the person who has entered, a known person. Initially, a three digit password was generated by Arduino and saved by itself. This password was also sent to user's mobile phone through GSM shield. Thus this password would be known to user only. Now, when a person enters to room, he/she might be either known or unknown. If the person is known, then before entering, he/she can get information about the right password from user and just after entry, he/she will enter that password through keypad which ensures that he/she is a known person. Now if that person fails to provide any password or provides wrong password within this 30 second, it will be a proof of unauthorized entry. Whenever any unauthorized entry be detected, Arduino sends signal to GSM shield to send an 'alert message' to user to make him/her aware of it. In this way, the PIR sensor along with self-generated password protection scheme provides a better and low cost security system.

To make aware the person about his presence has been detected by microcontroller, two signal Led have also been used. When microcontroller will sense the high output signal from PIR, a Green Led with starts glow. After 20 second it will starts blinking and whenever 30 second completes, the Green light will extinguish and a Red light will glow ensuring that 'alert message' has been sent to user mobile. But if the person provides right password within this interval, both light will extinguish and no message will be sent regarding unauthorized entry.

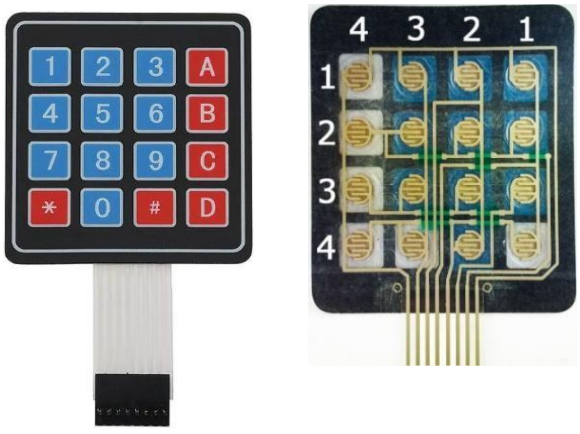


Fig.3 4×4 keypad

### *C. GSM shield operation to send alert message*

The SIM 900 TTL UART modem, shown in Fig.4, is a dual band GSM/GPRS module with operating frequency 900/1800 MHz. This module operates in 5-20 volt DC supply and it is equipped with SMA connector with GSM L Type Antenna. This module can be interfaced with microcontroller unit with AT commands through serial port using TX and RX pin to transmit and receive data, respectively.

In our work we have used a GSM simcard to send message from this module to user's mobile phone. Hence after inserting this simcard, we connected the antenna and provided power supply from Arduino Uno by attaching this module with Arduino Uno. Now there are three status LED, mounted on GSM module, which are 1. PWR LED: it will lit immediately after proving power supply, 2. STS LED: it will lit after 1-2 seconds indicating the module is operating properly, 3. NET LED: it will starts to blink in fast for few seconds (searching for Network) and becomes slow blinking once the Modem registers with the Network. Now, when NET Led will starts blinking slowly, the module starts working properly. A text massage was already been written inside microcontroller to alert users, and it was sent to users mobile phone whenever any unauthorized entry took place. The algorithm is written below,

Alert_MSG='trespassing has been occurred'.*# alert message*

1. if password has been entered goto step 2, else goto step 7
2. if the entered password is right goto step 3, else goto step 7
3. generate new password
4. save new password
5. send new password to users mobile phone
6. go to step 9
7. send Alert_MSG to users mobile phone
8. go to step 3
9. end.

Now to send Alert_MSG, the following commands is used,

1. *mySerial.println("AT+CMGF=1");*
2. *delay(1000);*
3. *mySerial.println("AT+CMGS=\+91xxxxxxxxxx");*
4. *mySerial.println("trespassing has been occurred");*

Where, "xxxxxxxxxx", represents users 10 digit mobile number.

### *D. Password generation*

In this work, a new password generation scheme has been proposed where after completion of each operation, every time a new password is sent to user mobile, thus increasing the security procedure. This password generation procedure can be of three different types, these are 1. if any trespassing occurs, user will aware of it and after that the Arduino Uno has to be restarted and a new password will be sent. 2. if any malfunction has been occurred or any known person has entered and forgot


Fig.4 PIR motion sensor

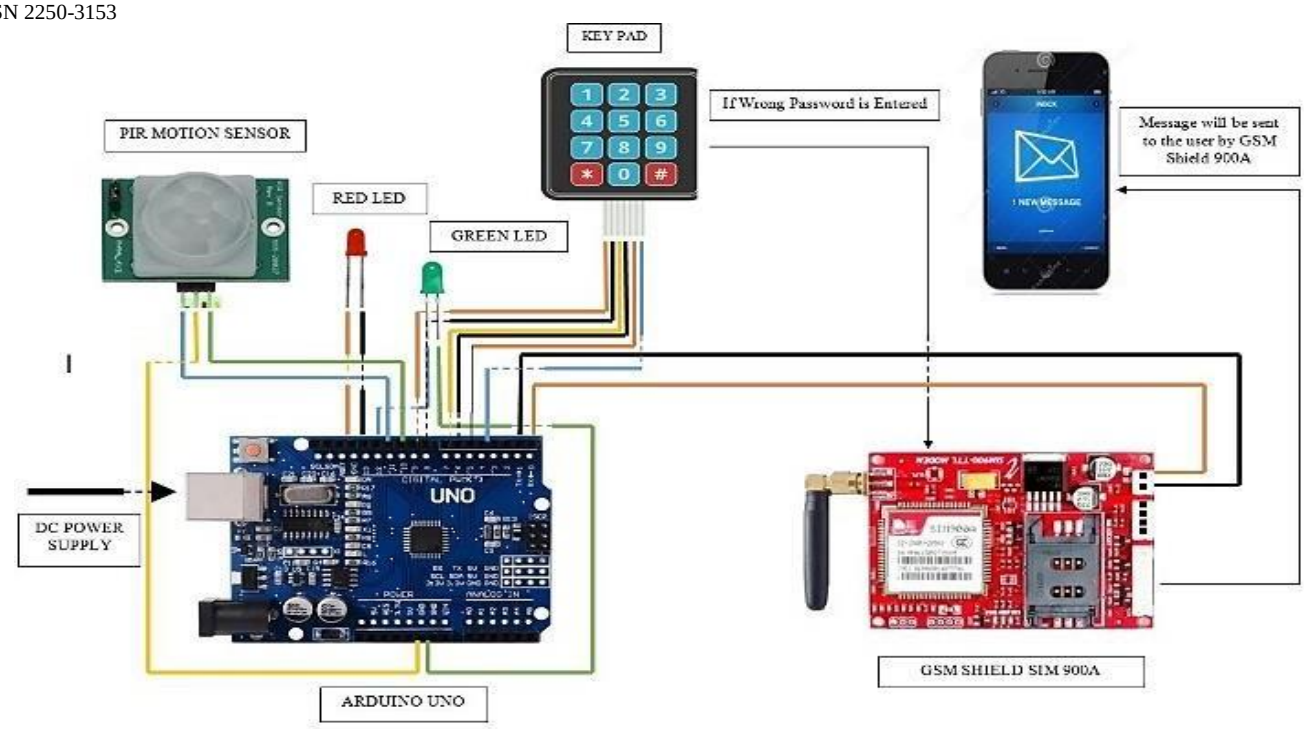


Fig.5 Connection scheme of proposed work

to provide right password, then user will still receive alert message. In that case user can send a missed call to the simcard connected to GSM shield and the device will generate new password and will start working properly. 3. if any known person has entered and provided right password, then the device to just send the new generated password o user and will start working properly.

Now, after password generation and updating of password to user, the microcontroller will treat this password as right one for the next time operation. The connection scheme of this work is explained in Fig.5.

## III. CONCLUSION

In this the main objective was to reduce technical complexity and expenses over the security system along with advancement of security procedure. After detection of human presence, this device needs a password to make user ensure that a known person has entered, failing which an 'alert_ message' will be sent t to user's mobile phone to make him/her aware of that, a trespassing has occurred. After each time operation a new pass word will be generated and treated as right password for the next time operation. Also this new password will only be known to user. In this way the self-generated password protection scheme provided a better security protocol.

## IV. REFERENCES

[1] M. Andriansyah, M. Subali, I. Purwanto, A. Irianto S and R. A. Pramono, "e-KTP as the Basis of Home Security System using Arduino Uno", IEEE 4th Intern. Conf. Comp. Appl. Inform. Proc. Tech., pp. 8-10, August 2017, Kuta Bali, Indonesia.

[2] S. Monk, "Programming Arduino", ISBN: 978-0-07-178423-8, The McGraw-Hill Companies, 2012.

[3] O. Vermesan and P. Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystem", ISBN: 978-87-92982-73-5, River Publishers, Denmark, 2013.

[4] J. Han, Y. Jeon and J. Kim, "Security Considerations for Secure and trustworthy smart home system in the IoT environment", IEEE Intern. Conf. Inform. Comm. Tech. Conv., pp. 28-30, October 2015, Jeju, South-Korea.

[5] L. Salman, S. Salman, S. Jahangirian, M. Abraham, F. Germah, C. Blair and P. Krenz, "Energy efficient IoT-based smart home", IEEE 3rd Wor. For. Intern. Thin., pp. 12-14 December 2016, Reston, USA.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things: A vision, architectural element, and future directions", ELSEVIER, Future Gener. Computet. Syst., vol. 29, issue 7, pp. 1645-1660, 2013.

[7] J. Chhabra and P. Gupta, "IoT based Smart Home design using power and security management", IEEE Intern. Conf. Inn. and Chall. Cyb., pp. 3-5, February 2016, Noida, India.

[8] M. Chen and Y. Chuang, "Supporting Home Security System in OSGi Platform", IEEE 24th Intern. Conf. Adv. Inform. Net. Appl. Workshops, pp. 20-23, April 2010, Perth, WA, Australia.

[9] S. Rehman, V. Gruhn, "An Approach to Secure Smart Homes in Cyber-Physical Systems/ Internet of Things" 5th Intern. Conf. Soft. Def. Sys., pp. 23-26, April 2018, Barcelona, Spain.

[10] A. Ibrahim, A. Paravath, P. K. Aswin, S. M. Iqbal, S. U. Abdulla, "GSM based digital door lock security system", IEEE Intern. Conf. Pow. Instr. Control Comp., pp. 1-6, Thrissur, India.

[11] H. Huang, S. Xiao, X. Meng, Y. Xiong, "A Remote Home Security System Based on Wireless Sensor Network and GSM Technology", IEEE 2nd Intern. Conf. Net. Sec. Wir. Comm. Trus. Comp., pp. 535-538, 2010, Guntur, India.

[12] J. Nicklas, M. Mamrot, P. Winzer, D. Lichte, S. Marchlewitz and K. Wolf, "Use Case based Approach for an Integrated Consideration of Safety and Security Aspects for Smart Home Applications", 11th Sys. Sys. Eng. Conf., pp. 12-16, June 2016, Kongsberg, Norway.

[13] G. M. S. M. Rana, A. Khan, M. N. Hoque and A. F. Mitul, "Design and Implementation of a GSM Based remote home security and appliance control system", IEEE 2nd Intern. Conf. Adv. Elec. Eng., pp. 19-21, December 2013, Dhaka, Bangladesh.

[14] R. Priya, V. Tamilselvi and G.P. Rameshkumar, "A novel algorithm for secure Internet Banking with finger print recognition", IEEE Intern. Conf. Emb. Sys., pp. 3-5, July 2014, Coimbatore, India.

[15] R. Liu, M. Zhang and S. Ma, "Design of face detection and tracking system", IEEE 3rd Intern. Cong. Imag. Sig. Proc., pp. 16-18, October 2010, Yantai, China.

[16] Authors

**Soumyendu Banerjee**, Assistant Professor, University of Engineering and Management, Kolkata,
banerjeesoumyendu@gmail.com

**Evan Chowdhury**, student, University of Engineering and Management, Kolkata,
evanchowdhury357@gmail.com

**Chaitali Sikder**, student, University of Engineering and Management, Kolkata, 2014chaitalis@gmail.com

**Debrup Sarkar**, student, University of Engineering and Management, Kolkata s.debrup10@gmail.com

**Rishab Sarbadhikary**, student, University of Engineering and Management, Kolkata
sarbadhikaryrishab97@gmail.com