

# Network Monitoring and IoT based Smart Home Automation

R. Rajesh<sup>1</sup>, Stuti Chauhan<sup>2</sup>, Prashant Kumar Srivastava<sup>3</sup>

<sup>1</sup>Assistant Professor, Department of CSE, SRM Institute of Science and Technology, Ghaziabad

<sup>2</sup>Department of CSE, SRM Institute of Science and Technology, Modinagar, Ghaziabad

<sup>3</sup>Department of CSE, SRM Institute of Science and Technology, Modinagar, Ghaziabad

## ABSTRACT

Router, bandwidth, timer, frequency

Internet of Things or IoT is one of the optimal technologies on which all the appliances work nowadays. The introduction of IoT in home automation is one among the foremost helpful approaches to assist us come face to face with the techno savage world. With this, we will admire the sweetness of commercial IoT implementation in our daily schedule.

With the pandemic of the records and maximum of the population staying at home one thing is for sure that the rate of usage of domestic amenities are going to get off the charts in upcoming years and at same time the work from home culture is sprouting in the IT as well as in government sector in India which leads citizens to be more dependent and hooked to their internet devices. Our Idea is a system where we can actually use a blooming technology to cut-short our day-to-day electricity usage and that too without us participating in this process.

The single sight of this project is to provide the users with a home automation experience that not only gives their home a futuristic appeal but also focuses on the objective of saving electricity. In addition, we plan to create an economically feasible door locking system which will be highly secure and a new introduction in the market. For the switch, it measures the user's internet usage rate between the surfing device and the router or monitors the network and then automatically takes the decision to switch off the lights if no activity is detected. Whereas, the lock is operated by keeping the LAN connectivity as the base. The whole system works on a mobile application linked to the user's fingerprint, hence eliminating the limitations and making it user friendly.

The system provides with security and ease to the user. It also is cost efficient, hence a dream come true in the automation field.

## 1. INTRODUCTION

The IoT or Internet of Things, is an arrangement of interconnected advancements, computerized machines and machines, articles or individuals given one of a kind identifiers (UIDs) and the capacity to send information over the organization with no actual contact with people and machines.

The IoT process starts with the electronic devices such as smartphones, watches, electronic gadgets and appliances like TV, Washing Machine, Fans, lights etc. These are connected to the IoT platform and then their functioning is handled using various other components.

IoT acts as a bridge between the physical environment and the user. The sensors and boards associated with it, helps in the connection (Fig 1). Here, the various hardware components and sensors when linked to internet, make an actual network hence enabling the users to control them without any manual input.

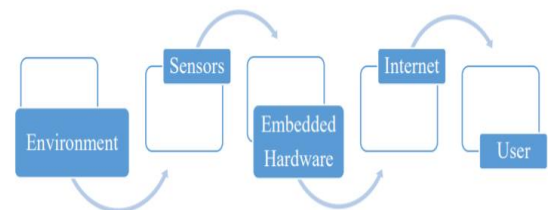


Fig 1 Block representation of home automation

**Keywords-** Home automation, IoT, Arduino, Secure lock, Network Monitoring, Mobile Application, Threshold, Counter, Wi-Fi receiver,

Home automation systems are very popular in today's world. Engineers from all around the world create such, by using different technologies and hardware devices. Nowadays, everything is linked to automation and no manual effort is required.

But, as nothing comes for free, these systems also cost a lot. As a result of which, not everyone is able to afford the setup.

We have tried to make an efficient system using the components and functions in a manner that they give maximum output at minimum cost. This system is affordable and helps in saving electricity too. Hence has an added benefit.

We have used Network Monitoring and LAN connectivity as the base technologies to control the home appliances, hence tried to make a new attempt in this field.

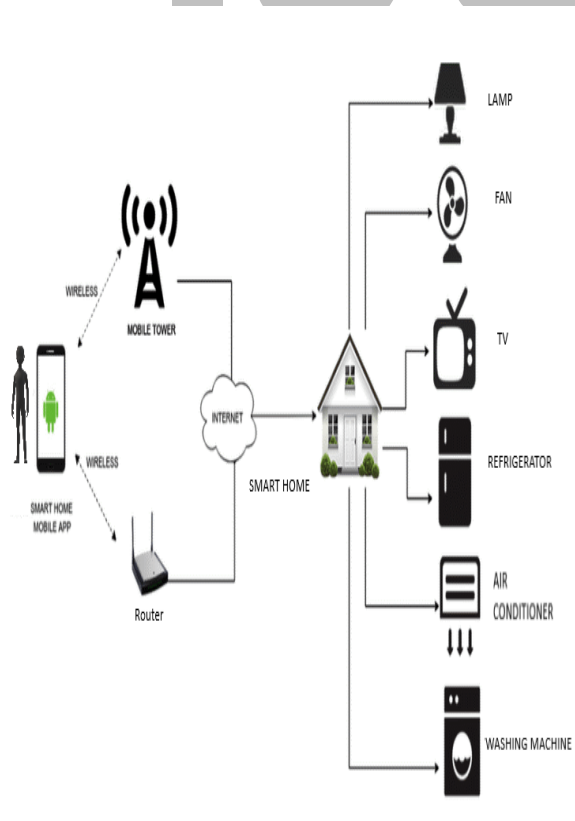


Fig 3 Home automation connectivity

## 2.LITERATURE SURVEY

In mid-nineties, Jim Sutherland invented the first ever home automation system. The system was used to store recipes, control the house temperature etc. and was the beginning of the technical era.

Furthermore, the work of Yong Tae and Parnesh Sthapit dealt with a system that used Zigbee administered smart lock system that was controlled by automatic wi-fi network detection which was protected by a password.

The project put up by Sandhya Patil, Muhammad Tabish Quadri, Riya John, Sanket Said, Ranjita Gaonkar brought up an android based home automation where an android application could control the various appliances of the home. The project that was put up used Remote XY component assembler and an Arduino uno board with a wi-fi data adapter and led relays.

Research work by Rizwan Ma-jeed, Nurul Azma Abdullah, Imran Ashraf, Yousaf Bin Zikria, Muhammad Faheem Mushtaq and Muhammad Umer proposed a research paper offering multiple operations home automation system which monitored the devices, temperature etc. securely by using temperature sensors used to monitor the temperature and an android application to operate it.

The study by Brahmjit Singh, Anand Pratap Singh, Arghya Biswas made the IoT Based Smart Home Automation Enabled with Manual Mode Switch Control to control appliances through internet and by manual switches too. Certain modifications were done to add new features, retaining the older ones

Paper by Mohammad Hasnain R, Swapnil G , Mayank P and Rishabh S proposed Automatic detection of surrounding through AI and functioning of home appliances through IoT. Computer Vision and Segmented Image Processing Controls home appliances with the help of artificial intelligence and IR blasters.

Waseem Akram, Dr. Prahalada Raod developed a smart IoT switch using internet to connect and control all electrical home appliances. It was both a study and a project about an analysis of how IoT when combined with networks, plays role in

home automation, saving money and time. It indicated the role of internet in controlling multiple devices.

Amirita Deswani, Sania Bhatti, Pirah Memon, Veena Kumari, Anum Arain and Ayaz Jiskani proposed Keyless Smart Home: An Application of Home Security and Automation in which Bluetooth controlled the lock system, operated by a mobile application.

The mobile application let the person lock and unlock the door lock by a single click. Limitations were reported as being controlled by Bluetooth, it could not function at large distances.

Marko Pavelić, Zvonimir Lončarić, Marin Vuković, Mario Kursk came up with an IoT assembly that was Bluetooth controlled, hardware equipped digital lock with pin monitor. Card or pin was required to unlock the door. They lacked in the fact that the user still needed to manually insert the pin to unlock the door and hence was a contrary.

Research made by Tanishq Sehgal and Shubham More in 2017, proposed a system where an android based home utility communicated with the micro internet-server through internet and the use of the REST API. Any android supported tool could be used to install the smart app, and control or monitor the domestic surroundings.

Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar, Mayur Shingate, proposed a project based on Android and Arduino platform. The user could interact with the android phone and send control signal to the Arduino ADK which in turn would control the other embedded devices/sensors.

Baris Kurt, Engin Zeydan, Utku Yabas, Ilyas Alper Karatepe, Gunes Karabulut, and Ali Taylan Cemgil are the network engineers that found out the way to a Network Monitoring System for High Speed Network Traffic.

They used PTR algorithm which would monitor the network and note their statistics. As per the statistics the microcontroller set the pins high and low which would tell the network traffic in real time.

### 3. PROPOSED ARCHITECTURE

The proposed system will consist of basically three parts  
 Networking Monitoring for controlling the lights, LAN connectivity for the smart lock and a mobile application for accessing the automation system.

The user will use only the mobile application to operate and control the devices.

Mobile application helps the user to access all the IoT devices, entering the credentials to login and putting the fingerprint to access the appliance which he wants to operate, hence providing a double secure system.

Fig 4 depicts the architecture system of the proposed system

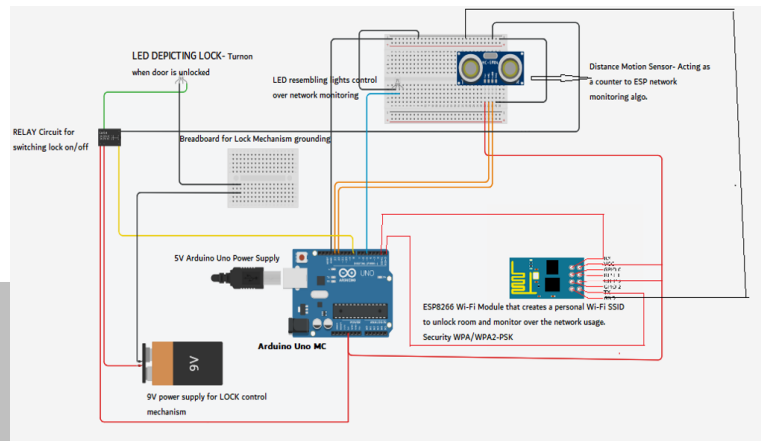


Fig 4 Architecture diagram of the proposed system

After logging in to the application, two options will be displayed, one for the lights and another for the door. As the user selects the option targeting the devices, that particular device starts functioning, hence giving user the freedom to operate it.

The door lock can be controlled by a single tap to lock and unlock it.

And the lights will automatically turn off if the network usage is zero, once the user starts the system from the app.

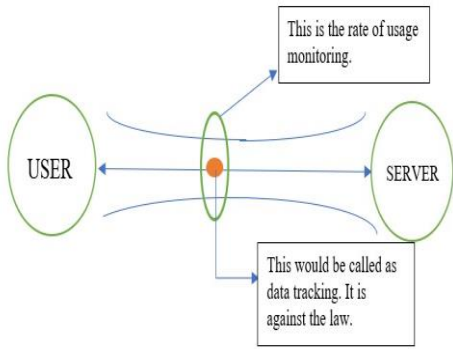
The user can also turn off the network monitoring system if he does not want it to function at some time.

The architecture is drawn keeping in mind the working and functioning of the hardware components when connected together to perform both the tasks in the automation system.

### 3.1 TECHNOLOGIES USED

#### 3.1.1 NETWORK MONITORING

When we use the term network monitoring, that doesn't mean that the system can track what the user is surfing or in any way causes hindrance to the user's privacy. There is no active or passive sniffing of the data packets that are transmitted over the network protocols. Instead, in clear words monitoring is done only on the rate of internet usage of the user. Fig 5 shows the difference between tracking and monitoring



As with the orange area it is clearly depicted that the program is coming in between the transfer of the packets, whereas monitoring is occurring over the network but not coming anyway in between hence there will be a no chance of information leakage, hence is completely secure.

### 3.1.1.2 PTR ALGORITHM

Packet Transmission Rate Algorithm works on the principle of counting the acknowledgement. Whenever sender sends an information to the receiver, the receiver generates an acknowledgement which is sent back to the sender in response. PTR Algorithm measures the weight of these packets and multiplies it by the number of packets transmitted over one loop of the connected topology. As the packets which are carrying the information have a size of one bit, the band transmission is also measured by the name unit. And the rate of transmission is measured in bps, kbps or mbps depending upon the strength of the band spectrum allotted by the service provider. Fig 6 shows the PTR model used in the automation model

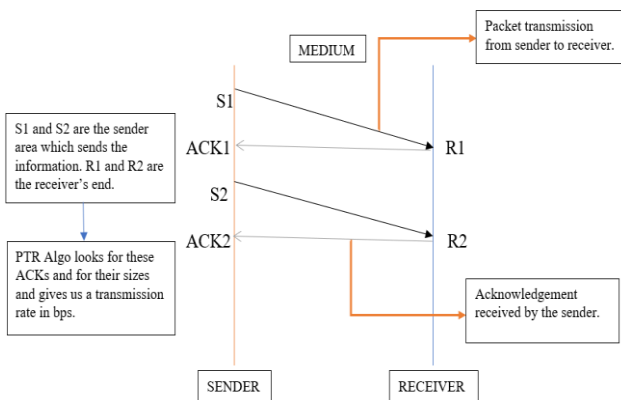


Fig 6 PTR model used in the automation model

### 3.1.2 INTERNET OF THINGS

IoT or Internet of Things, is an arrangement of interrelated technologies, digital machines and gears, creatures, natures or objects and the capacity to send information over the organization without any physical contact with humans and machines.

IoT makes truly the whole thing smart by improving components of our existence with the power of networks, statistics collection and algorithms. IoT has become a very famous technology used for human advancement. IoT when combined with hardware components come out to be a very effective and easy to use technique. When home automation comes in the mind, IoT comes as the addition.

IoT plays a crucial role in the automation world and more advancements are done when more technologies are implemented.

### 3.1.3 ANDROID

Android is an operating framework for mobiles based on open-source softwares and their updates. It is designed primarily for smart devices such as mobile phones, tablets, televisions etc.

Android is the base platform for accessing or performing tasks when devices are connected using IoT. Here, IoT connects and prepare the devices to perform tasks. But, Android acts as the bridge between the user and the devices. A user accesses the devices through a mobile application or through web. We, here, in our model have used Android as the medium.

### 3.2 COMPONENTS USED

1.	<b>Arduino Uno</b>	It is a micro-controller board which is based on Microchip ATmega328P microcontroller and is produced by Arduino.cc. The board consists of sets of digital anchors and analogous (I/O) that can be intermittent on various shields or boards or other circuits.
2.	<b>ESP8266</b>	The ESP8266 is a minimal expense Wi-Fi computer chip, with a full TCP/IP stack and microcontroller ability, delivered by Espressif Systems in Shanghai, China. The chip initially went to the consideration of Western

		creators in August 2014 with the ESP-01 module, made by an outsider maker Ai-Thinker
3.	<b>Bread board</b>	A breadboard is a solderless gadget for impermanent model with hardware and test circuit plans. Most electronic segments in electronic circuits can be interlinked by embedding their leads or terminals into the openings and afterward making associations through wires where proper.
4.	<b>Jumper wires</b>	They are wires that have plain connector pins at each edge, letting them to be connected to each other without any mechanical soldering. They are mechanically used with breadboards and other tools and hence letting it to form circuits as desired.
5.	<b>5V relay</b>	It is often utilized in an automatic manipulate circuit. To place it truly, it is an automated transfer to manipulate an already famous circuit type with a low-modern sign. 5V relay sign enter voltage variety, 0-5V. VCC electricity to the system. JD-VCC relay in the strength supply.
6.	<b>Distance/Motion sensor</b>	Distance sensors usually process via outputting a signal of a few kind, (like IR LED, laser, ultrasonic waves) and then noting the way it has changed on returning. That change may be in the depth of the lower back signal, the time it took for the sign to go back, and many others.

### 3.METHODOLOGY FOR SECURE LOCK

We created this home automation system keeping Network Monitoring as the base technology for the lights

and LAN connectivity for the door lock. A mobile application summed this system in a small area.

For the network monitoring switch, ESP8266 is used as Wi-Fi Receiver Adapter and 3.3V through Arduino is used as the power source. A Remote -XY package and Arduino are also used to measure the network usage.

A distance motion sensing is also used as a counter. When device is pinged, the algorithm generates an approximated integer value which is then compared to a standard constant coded within the program itself to get the threshold between active and passive internet usage. When the usage goes below 95kbps, there is a timer triggered for 15 minutes.

If during that time, the usage doesn't go above 95, the flag is marked as TRUE. Parallely to that distance motion sensor looks for any activity within the room at the specified points which when not detected any sensing within the room turns the flag TRUE. Only when both the flags are marked as TRUE, the Digital Pin 5 is triggered to be LOW, which the turns off the lights of the room. The flowchart implementation is shown in (Fig 7).

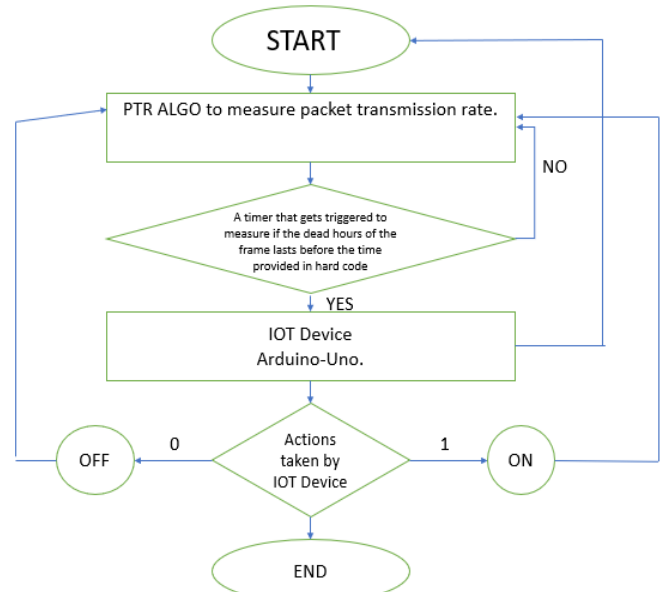
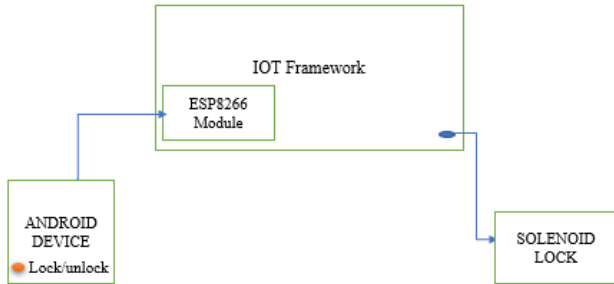


Fig 7 Flowchart implementation of the network switch

For the smart lock, ESP8266 is used as the Wi-fi module and a 5V Single Channel relay to switch the circuit between ON/OFF. It uses WPA/WPA2-PSK Wi-fi security protocol and operates with the help of Remote-XY package. The Remote XY handler function checks for the command from the app that marks the switch on or off. After this, a Boolean value is passed through the Wi-fi module to the Arduino which triggers the pin 8 of



the micro controller to LOW the relay to go in shifted ON state. As the default state of the lock is OFF i.e. locked. When the relay circuit switches on the current through the 12 V solenoid the door gets unlocked. The block implementation is shown in (Fig 8).

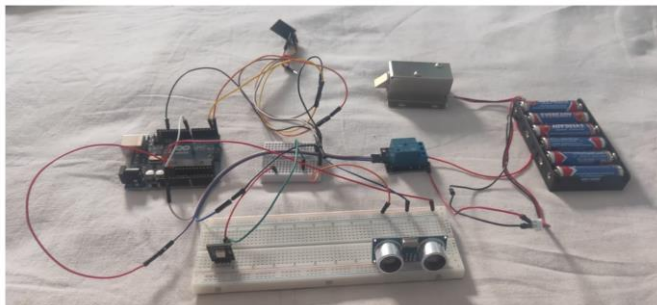


**Fig 8** Block implementation of door lock

#### 4. EXPERIMENTAL RESULTS

Home automation has been a very widely used concept in today's market. Nowadays, the use of technology is increasing, and so its implementation. Multiple technologies such as AI, Bluetooth, Cloud etc. have been used to act as a base for the automation system. Usage of such technologies is complicated as well as costly. We in our model have used Network Monitoring as the base for controlling the lights, which is a completely new concept and has not been implemented in this field earlier. To support this system, we have also included a digitalsmart locksystem which is linked to the Wi-fi module and is an extremely secure setup. This system works on a mobile application throughout. The system works on the various weak points of the other systems imposed too. It is a cheap, completely safe and user-friendly system. It does not require constant servicing; hence money is saved. Electricity is also saved in this system.

(Fig 9) shows the assembled hardware components of the model.

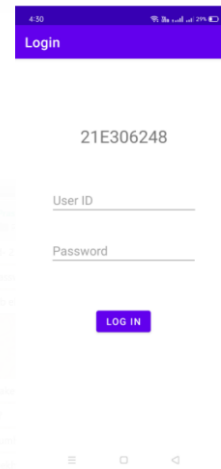


**Fig 9** Assembled hardware components used in the model

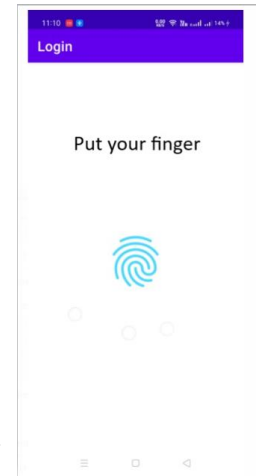
The assembling resulted in connecting the lights and locks to the Wi-Fi router. The coding helped in linking the IoT devices to the mobile application.

The application requires login credentials to log in to the application (Fig 10) and gets locked if wrong credentials are entered more than three times.

It then requires fingerprint of the user and then enables him to access or use the devices (Fig 11).



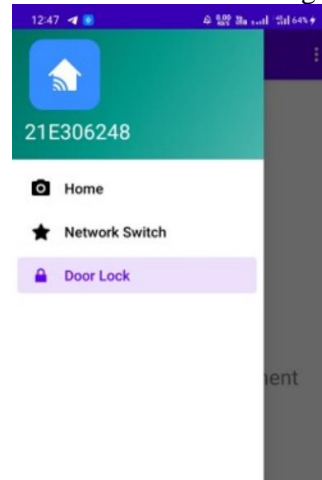
**Fig 10** Login Page



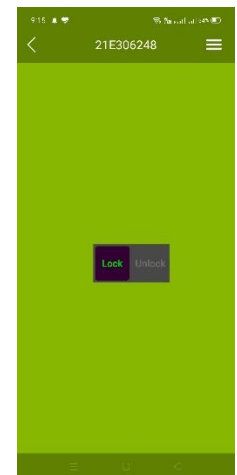
**Fig 11** Fingerprint page

After the fingerprint verification, the user gets the access to the devices and freedom to select between the lights or doors (Fig 12). If the user chooses to operate the lights, the network monitoring system will come into play and PTR algorithm will function. And if he selects the doors, two buttons will be shown, and he'll be able to lock and unlock the doors by simply clicking on them. (Fig 13)

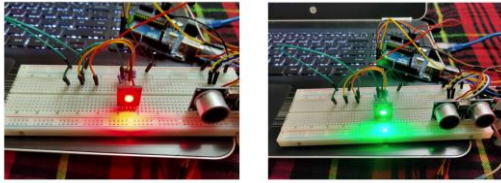
Also, the LED in the IoT board will glow red to indicate that the door is locked and green if it is unlocked (Fig 14).



**Fig 12** Inside the app



**Fig 13** Buttons for the lock



**Fig 14** LED indicating the condition of lock

## 5. CONCLUSIONS

Home automation systems have been popular for more than seventy years now. Many different automation systems have been launched for the professional as well as domestic usage. Multiple technologies like IoT, cloud, artificial intelligence, Bluetooth etc. have been used. This system is basically an economically feasible automation technique. The network monitoring technique has not been used for home automation till date. Use of network monitoring as the base technique increases security and admin involvement in the system, hence eliminating errors. The system has scope for future enhancements too. For this, we plan to use better R&D and smart electricity saving domestic modules. Further, more functionality could be added by using AI to switch between day and night mode. The system might come up with a better GUI in future. Methods to create a self-installable IoT kit can also be considered. Many more automation techniques can be implemented to make the system a better one. Multiple updates can carry it forward.

## 6. REFERENCES

- [1] Sandnya Patil, Muhammad Tabish Quadri, Riya John, Sanket Said, Ranjita Gaonkar, "Android based Secure and Smart Home Application using IoT", in International Research Journal of Engineering and Technology (IRJET), 2020, Volume: 07 Issue: 03 | Mar 2020
- [2] Rizwan Majeed, Nurul Azma Abdullah, Imran Ashraf, Yousaf Bin Zikria, Muhammad Faheem Mushtaq and Muhammad Umer,"An Intelligent, Secure, and Smart Home Automation System", in Hindawi Scientific Programming,2020, Volume 2020, Article ID 4579291
- [3] Anand Pratap Singh , Arghya Biswas , Brahmjit Singh, "IoT Based Smart Home Automation Enabled with Manual Mode Switch Control" in 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), 2019, DOI:10.1109/ICCT46177.2019.8969062
- [4] Marko Paveli'c, Zvonimir Lon'cari'c, Marin Vukovi'c, Mario Ku'sek,"Internet of Things Cyber Security: Smart Door Lock System", in International Conference on Smart Systems and Technologies (SST), 2018, DOI:10.1109/SST.2018.8564647
- [5] Mohammad Hasnain R, Rishabh S, Mayank P, Swapnil G, "Smart Home Automation using Computer Vision and Segmented Image Processing", in International Conference on Communication and Signal Processing (ICCSP), IEEE, 2019, DOI: 10.1109/ICCSP.2019.8697997
- [6] Amirita Dewani, Sania Bhatti, Pirah Memon, Veena Kumari, Anum Arain and Ayaz Jiskani, "Keyless Smart Home: An Application of Home Security and Automation", in ISSN, 2018, ISSN: 0974-6471, Vol. 11, No. (2) 2018, Pg. 107-114
- [7] G S MD Waseem Akram, Dr. Prahalada Rao, "A smart switch to connect and disconnect electrical devices at home by using internet", in International Research Journal of Engineering and Technology (IRJET), 2018, Volume: 05 Issue: 01| Jan-2018
- [8] Gartner homepage, available, <https://www.gartner.com/technology/home.jsp>
- [9] The institute blog [online], available <http://theinstitute.ieee.org/ieee-roundup/blogs/blog/is-it-smart-to-have-a-smart-home>
- [10] Collotta, Mario, et al., "Bluetooth 5: a concrete step forward towards the IoT." arXiv preprint arXiv:1711.00257 (2017).
- [11] ChangTing-Yee, Min-Shang Huwang, and Chow-Chinn Yang. "Password Authenticated Key Exchange and Protected Password Change Protocols." Symmetry 9.8 (2017): 134.
- [12] Jain, Ankit, Anita Shukla, and Ritu Rajan. "Password Protected Home Automation System with Automatic Door Lock.", MIT International Journal of Electrical and Instrumentation Engineering, Vol.6, No. 1, January 2016, pp. 28-31.
- [13] Shankar, A. Aditya, et al. "Finger Print Based Door Locking System." International Journal of Engineering and Computer Science 4.3 (2015): 10810-10814.
- [14] Kartika Wong, Felix Hoi Chak Satya, Uriel Jethro "Smartphone-Controlled Fingerprint- Enabled Door Lock System.", Department of Electronic and Computer Engineering The Hong Kong University of Science and Technology, Final Year Project Report, April 15, 2015.
- [15] Sadeque Reza Khan, Farzana Sultana Dristy, "Android based security and home automation system", International Journal of Ambient Systems and

Applications (IJASA), Vol. 3, No. 1, pp. 15-24, March 2015.

- [16] Anu, and Dinesh Bhatia. "A smart door access system using finger print biometric system." International Journal of Medical Engineering and Informatics 2 6.3 (2014): 274-280.
- [17] Kamelia, Lia, et al., "DoorAutomation System Using Bluetooth-BasedAndroid For Mobile Phone." ARPN Journal of Engineering and Applied Sciences 9.10 (2014): 1759-1762.
- [18] Inderpreet Kaur, "Microcontroller based home automation system with security", in International Journal of Advanced Computer Science and Applications, Vol. 1, No. 6, December 2010
- [19] Verma, Gyanendra K., and Pawan Tripathi. "A digital security system with door lock system using RFID technology." International Journal of Computer Applications (IJCA)(0975–8887) 5.11 (2010).
- [20] K. Atukorala, D. Wijekoon, M. Tharugasini, I.Perera, and C. Silva, "Smart eye - Integrated solution to home automation, security and monitoring through mobile phone", NGMAST '09: Proceedings of the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, September 2009