HOME AUTOMATION THROUGH SMART LIGHTING, SMART SECURITY AND OTHER APPLIANCES

Rajarajeswari S [1*] *, Shola Usha Rani* [1]*, Alpanshu Kataria* [1]*, Soumitro Dutta* [1]

[1]*School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India*

Abstract: The smart home automation system is designed to conveniently manage and monitor household appliances and lighting fixtures remotely, to save time and to use resources effectively. It is a control system for allowing access to home automation devices. The automation devices include lights, fan, camera and doors. It even enhances the main features of the project to control the home appliances from anywhere as remotely. With the camera module, continuous surveillance and protection of the home is accomplished. A significant improvement is achieved in utility costs by an optimal use of energy. Using inexpensive electronic and interactive tools, this initiative can be applied, making it economically, physically and operationally feasible. Basically it involves controlling everything remotely via a visual interface and mobile application. The automation system employs the use of MQTT protocol in order to secure the transmitted device based information to and from in the network. The defense against Man in the Middle attack (MITM) is the main focus of our automation system. The routed messages are checked at the intermediate hub to check for the occurrence of MITM based DoS attacks through manual reset points. .

1. Introduction

There is a huge energy shortage in our world. People are not using the electricity available appropriately. People sometimes fail to turn off their home appliances, such as light fixtures, etc., before leaving home. In these sorts of situations, home automation makes it easy to regulate them conveniently from our mobile from a distant location. People keep running from place to place, working on their never-ending "to-do" list to complete everything. Because of the home automation system, we've never got to think about unlocking the door, shutting off the equipment, and so on. In short, we will save valuable time and maximize everyday efficiency and security.

The convenience, energy management, security are main components initiates the importance for implementing smart home systems. This is new area of research for integrating various components in Smart Home systems, but all the components are not integrated yet. This requires many domains need to communicate through the common interface layer to make the system to work smoother. The further cost will add if other components are connected together to the system. This makes large barrier while doing development to the smart home system as the technical components are getting cheaper the expense cost of smart home system will become cheaper even though it is incorporated with many other components.

*Corresponding author:rajarajeswari.s@vit.ac.in

Smart homes are evolving and becoming more sophisticated, but the goal of giving peace of mind is still there. We believe that the future of home automation will be focused on the continued integration of home devices, and even appliances, to increase personalization, control, comfort, and convenience in the home.

One of the newer fields of science that has not been completely implemented into our everyday lives is Smart Home solutions. This is because research involves the development of a proper smart home in many other research and engineering disciplines. The cost of a smart home is still a major impediment to the advent of smart home solutions on the market. The added cost of the installation is because, while most homes have been installed in the recent past, technology has evolved exponentially. This suggests that before this technology was available, most homes were constructed, and this becomes a hindrance to smart home systems production and sales. However, technology is getting stronger and cheaper, and as new homes are constructed, this will continue to make smart home solutions an investment worth making.

Smart homes are changing and becoming more complicated, but there is still the purpose of ensuring peace of mind. In order to improve personalization, security, and usability in the home, the future of home automation will concentrate on combining home electronics, and even appliances.

Home automation isn't a modern technology at all. Home Automation history goes back further. Since the advent of science fiction, science fiction has centered on smart home technologies, but it is not just that. The best minds in the world have been working for decades on

technology that can almost think for itself. There are a lot of highlights in it. 1966: Although never marketed commercially, ECHO IV was the world's first home automation system. The "Electronic Computing Home Operator" (ECHO) was invented by Jim Sutherland to store recipes, relay messages, regulate the temperature of a home and switch appliances on or off. 1969: DARPA launched ARPAnet, the first network in the world, the predecessor to the digital Internet and all our smart technology for the Internet of Things (IoT).

1981: A predecessor is invented to the cellular (802.11) technology of today. In the 1980s, in the form of garage doors, home surveillance systems, motion-sensing lighting, thermostat controls, and other innovations, home automation became prevalent.

1991: Ad van Berlo pioneers the gerontechnology-technology sector to better the lives of elderly people. These early innovations formed a solid foundation for the intelligent, life-enhancing characteristics that we enjoy about the smart systems of today.

1998-2000s: Smart homes have been prevalent. Smart technology evolved in the late 1990s and early 2000s, with gadgets and

computers becoming more and more available.

Thales is bringing some of the latest home protection IOT solutions, as well as an IOP publication dated 2017, to the industry. The Thales Approach offers an application that is compliant with multiple security systems and sensors, as well as offering a protected network and unique ID for each newly attached device to keep international devices at bay, eliminating many kinds of cyberattacks. The "Home security system using the internet of things" approach in the IOP Publication (2017) talks about using Reed Sensors to track room doorway operation, this is combined with Arduino and Wifi modules, further linked to Blynk Software that the user can connect and receive warning about and unusual behavior tracked by the doorway activity.

2. Existing System

Day by day, energy usage is growing. Remote access to home appliances using IoT is really important to have. That's why the next study field is Smart Home [7][10]. Applications based on IoT have also been very effective for elderly people and persons with any kind of disability [6][11]. This allows the user to monitor equipment such as lamps, fans, etc. without having any physical touches. Some of the Existing Home Security IOT solutions are the ones currently introduced to the market by Thales, and also an IOP Publication dated 2017. The Solution by Thales offers an application that is compatible with various Security devices and Sensors, it also provides a secured network and unique ID for every device that get's newly connected, so as to keep foreign/unlisted devices at bay, preventing many sorts of cyber attacks.

The Solution in the IOP Publication (2017) "Home security system using internet of things", talks about usage of Reed Sensors to track Doorway activity of rooms, this is paired up with Arduino and Wifi modules, further connected to Blynk App that the user can access and be notified about and unusual activity that is monitored by the doorway activity.

The research carried out is recorded in the following sections: [7][9][10][12][14]. The bulk of earlier devices based on these approaches are either Bluetooth-based or DTMF-based [6][7][12][13][15][17]. The fundamental problem is that separate PSTN channels for communication between controlling devices and main supply units are necessary for DTMF-based home automation. In addition, Bluetooth demands that the running appliance be in its range. It is only helpful for short-range engagement.

Home automation in [14] uses MQTT for the sending and receiving of sensor data. Raspberry Pi is used to access sensor information that is used to monitor the room's humidity and temperature as a gateway. Another Raspberry Pi-based home automation system is seen in[9] and the user uses a web-based GUI to monitor the home appliances. The [12] Mobile home automation demonstrates which device is built using ZigBee. We can transform non-smart devices into smart devices with the aid of IOT, which enables us to connect these via the internet. It turns a typical home into a smart home and offers a more efficient way for home appliances to be operated. Protection can also be improved by installing cameras in the home that can be tracked through the internet. Users can also track their home from anywhere and can turn their ON/OFF appliances. This will conserve energy as well as electricity costs as shown in Fig 1

System	Primary Communication	Remote access	Number of Devices	Cost	Speed	Real Time
GSM	SMS messages	Access from anywhere in the world	Unlimited	High cost due to SMS charges	Slow due to delivery issues	No
Bluetooth	Bluetooth and AT commands	Restricted to Bluetooth range- 10 metres	Unlimited	Fast due to proximity	Fast due to proximity	Yes
Phone Based	Phone lines	Anywhere with a phone line	12 due to 12 frequencies of DTMF	Fast	Fast	No
Zigbee	Zigbee and AT commands	Around 10 metres	Unlimited	Fast	Fast	Yes
Wireless	Radio, infrared or other waves	Depending on range and spectrum of waves used	Unlimited	High cost due to licensing and other spectrum issues	Slow due to interferences	Yes

Fig.1. Comparison of energy cost, speed for Phone based and system

3. Proposed System

The proposed system combines the features that an energy saving IOT system can provide with the features of a Secure Home Solution. The solution can even have high cost, high resolution, huge data producing Cameras and Sensors. The system is based on the detection of motion of a human body that is performed by PIR sensors. These PIR Sensors have the ability to work at very low electricity consumption. These PIR's to not only control simple appliances such as lights or fans, but also other security related sensors. Without the presence of objects like Human being the PIR sensor will not sense anything and, the devices will remain in off state and did not produce any data, this will keep the overall database light as well as lower electricity consumption.

The system also consider the situations of MiTM or DoS attacks that can occur at the MQTT broker, hence it'll be secured by TLS. Other than that, QoS is set to 0 as PIR's release data at short intervals of time, and all the messages are not so important to need a guaranteed delivery. QoS 0 makes the part of the MQTT broker easier and faster, also reduces load.

The data created by any security sensors or devices will transmit independent of the system, hence in cases of server malfunction or any malfunction at the microcontroller end can be easily solved by resetting the system and restarting it, this would not cause any loss to precious security data captured by the security sensors or devices.

The microcontroller will also be programmed to get data from MQTT Broker and take actions. Since at this stage too it might be vulnerable to attack, checkpoints that strip the topic of MQTT at which it is subscribing, are present. Abnormal messages getting through to the microcontroller will be filtered out and discarded at the early stages itself (Shown in Fig. 2).

A "Lockdown Mode" is introduced in the system, the same PIR will detects an unusual activity in various rooms, then the sophisticated devices such has high resolution cameras and other sensors will be turned on. This will confuse the burglar because while scoping the house from outside he'll notice the devices in off state, and hence not care about their working at a later stage, and be caught off by the guard. The system connects to mobile devices through LAN. This connection too might be vulnerable to sniffing, so encryption of alerts is supposed to be performed at the microcontroller, and decryption will be done at the end user through APP. This will ensure that alerts is passed to the end user, the one who are using the application. The architecture diagram representing the above proposed system can be seen in the Fig 2.

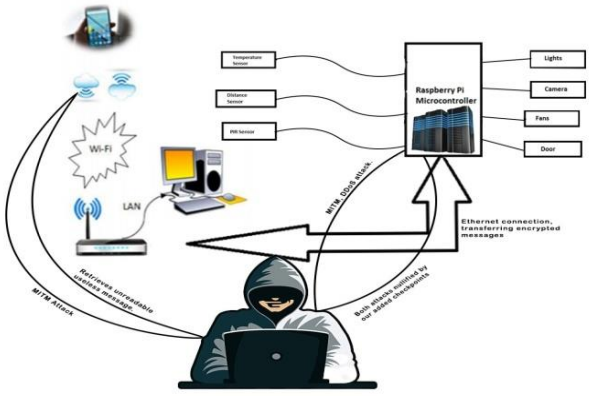

Fig.2. Architecture diagram of the proposed system

In some applications only simple notification through alarm is sufficient. But some solutions requires more secure and safer applications. To incorporate with simple security system need to be added with more security measures. with the consumption of video surveillance, the user can see who is at their opposite door, even can be alerted is any abnormal even happened at their door steps. And even the system can added an emergency system to add a call to nearby police or sending an SMS to the registered mobile numbers. To add this security feature video cameras are installed in all the rooms inside and outside to improve the security. the sever connected with this cameras will receive the upgraded storage of video and audio streaming. The data related from these cameras is updated into the server based on the infrared sensor data or motion sensor connected to the rooms. This sensor will detect the objects and send the abnormality to the server if find anything. . Light sensors could be included to monitor the light strength during the day and alter the lights in the room accordingly.

The system here it is designed with feature of cameras to note down the entrance and to maintain the log related to the entry. The log includes entrance of object, exit of an object, timestamp and presence of people inside house.

This will automate the feature of alerting the user when some abnormal event occurs. And notified or indicates to the user through the registered mobile number... All the cameras can be set to only activate upon another sensor being tripped in order to keep cameras in a "sleep mode". To control the energy and to increase the efficiency of the system the secure system is incorporated with the feature of central control location. Where this system will invoke the cameras system if it needs otherwise it automatically closes the camera feature. So lockdown mode feature is added, so if the home in lock mode then only the PIR sensor will initiate a signal to camera. Then the camera will start observing the data from the surroundings of the house. If the system make these features to generate an environment that

can exchange the common alarm system most households have. With creating an away mode or lockdown mode, it would even be able to be configured to have the household message owner if the away mode is not deactivated within a certain threshold of time when someone enters then house, and alert all household residents via cell phone when someone enters the house.

4. Implementation

The implementation is started with a very simple two-state sensor that could be externally controlled using MQTT. The sensor can be used to simulate real-world objects such as lighting, doors, etc. that have two ON or OFF/Open or close states, etc. The agreed commands are on and off, which, whether acting as a door sensor, switch the lights on and off or open and closed. All other commands are neglected and, using a function node, commands are rendered case-insensitive. As per the instruction, the sensor changes its state and publishes the current state. In node red workspace, a PIR sensor simulating nodes is added. Then the MQTT protocol send the sensor data to the microcontroller and then to the actuators. The model simulates the device such as light bulbs, doors and camera on the dashboard. The system is added different function nodes with the purpose of preventing any type of unauthorized access to the appliances. All the nodes implementation in Node Red can be seen in Fig 3. The system is also configured to send a notification to the user about the bad weather conditions, to alert the user while going out. The notification alert will be sent h by mail or by text message on phone(Fig 4 and Fig 8) Also, manual override switch in the dashboard that will ensure system reset and removal of any private data, in case of malfunction or attack.

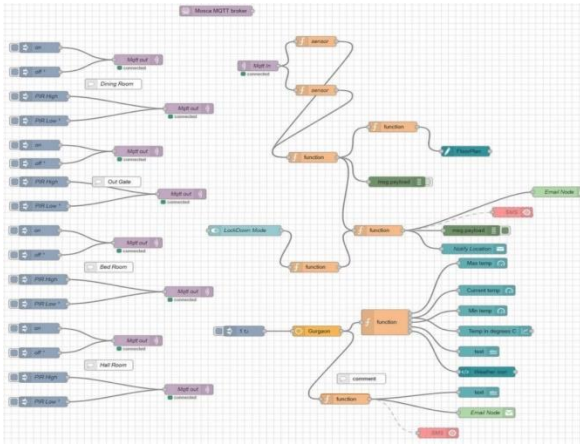

Fig.3. Node red workspace showing all nodes

5. Results and Discussion

Wastage of energy will happen when the usage of is rising. The following pie chart (Fig 5) tells us how much energy is used by various appliances. From the figure 4 it is noticed that the lights and fans absorb full energy. It also observed that means that lamps and fans work excessively; much of the loss of energy arises. The proposed work would aid in the savings of a lot of electricity and thus reducing the electricity bills as well as reducing the harmful impact on environment.

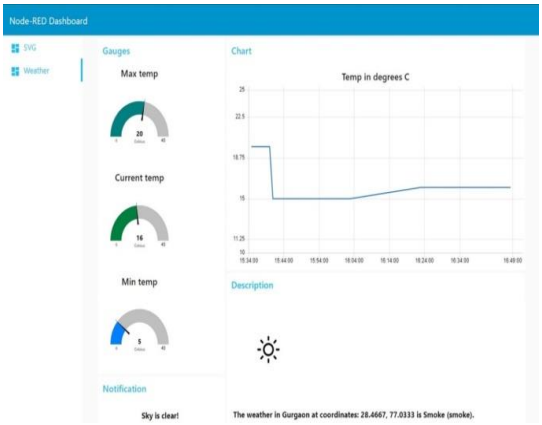

Fig.4. Weather Info on Dashboard

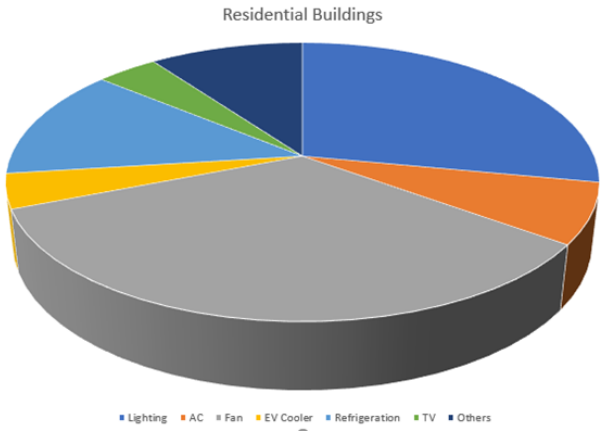

Fig.5. Electricity consumption in India

A basic sound alert system is appropriate for others, while for some, they are not happy until their house is cleaner and safer than anyone else. The device offers protections for those who are interested in a basic security configuration, and may have stronger security measures for those who are looking for more than that. The customer would be able to see who is at their main door by the use of video monitoring, as well as be alerted if anyone stands outside the door. The system can also be programmed to warn the user via text message, in addition to sending notifications to the user from any configuration unit, if the user wishes to. When the device is in away mode and an intrusion gets into the building, the user will set the system to warn 100, and he has been encountered.

In addition, video cameras in all the rooms in the house and outside will be placed on the wall to provide additional protection to the device. However, when they want privacy, users can still quickly switch off the camera. To allow for mass storage and streaming of audio and video, the server will then require an update. The probability of detecting subjects will be obtained by infrared motion sensors on walls. To track the light intensity during the day and change the lighting in the room accordingly, light sensors may be mounted.

A surveillance camera to track the main entrance is included with the current function which can be updated to retain a record on whether someone has entered and left the home, what time, and whether or not someone is present in the house at the moment. A major piece of security is the installation of surveillance cameras around the residence in numerous locations around the home. They can be automated with these cameras to warn the user when anyone is detected in an area, and to inform the user by text message or some other way. Only when another sensor is activated will all cameras be programmed to activate in order to hold cameras in "sleep mode" in order to save electricity and prevent the cameras from wasting extraneous quantities of power in order to observe nothing of significance. For these cameras, another security feature we should introduce is to be able to wake them up and monitor them from a central control spot. In order to create an ecosystem that can replace the common alarm system that many households have the group would like to create these features. Additional Lockdown mode is configured, which notifies the user about any unknown activity in the house.(Fig 6 and Fig 7). A switch kind of function is built to activate the lockdown mode. Finally the burglar alerts and weather notifications are intimated to the user through mail of the registered user as shown in Fig 8.

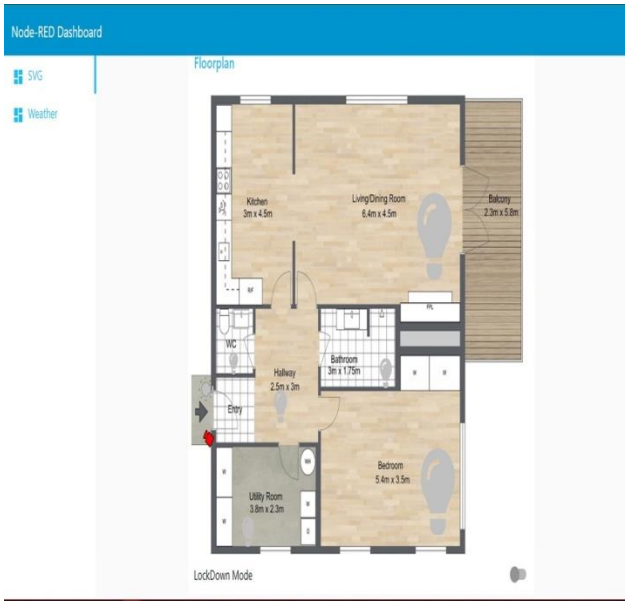

Fig.6. House Plan Showing all devices when Lockdown Mode OFF

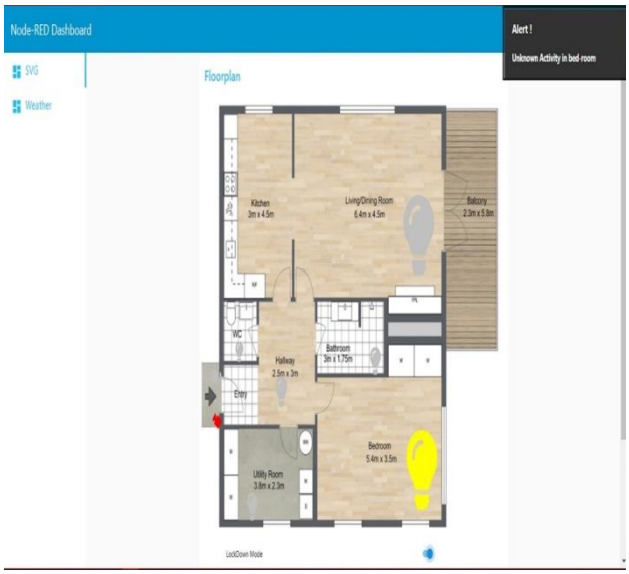

Fig.7. House Plan Showing all devices when Lockdown Mode ON

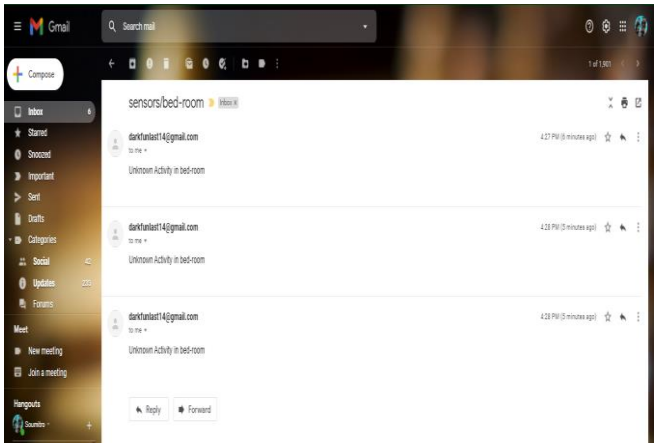

Fig.8. E-Mail Notification

6. Conclusion and Future work

For this project, there are several potential future iterations, incorporating new functionality to boost the user's performance and easier methods of interfacing the device, its individual components and the user. Increased protection capabilities, phone apps, audio/video features, touch screen control, wireless connectivity, speech recognition, faster on-screen navigation, and easy user download are some of these potential implementations. Users will customize the device, whether they want it to be armed in a remote mode, in a standard mode or in a low security mode. In addition to all this, users can watch their home, a record of comings and goings, and a live camera feed at the front door. This can be achieved by broadcasting the video via Wi-Fi over the internet. A sensor will watch when the sun shines through a

window and when it is, close the drapes. This would minimize the incoming heat and hence the air conditioner's power demand would be minimized. When the exterior lights that are used hit the stage where the electrical lights produce the same amount of energy, the electrical lights may be switched off. The machine should take advantage of the natural energy provided by the atmosphere. Using the cold air from the outside to cool the house when the weather is cooler rather than depending on the AC when it is not required, the device can operate according to outside temperatures. In addition, it will help to use natural capital in the most productive manner around the building. A graphics-based UI panel in the house is another addition which could be made.

Although the device addresses much of the needs of the customer as being able to use the system without a computer, the system need to support for the mobile phone devices from remote access.

References

1. 1.N. Sriskanthan and Tan Karand. Bluetooth Based Home Automation System. Journal of Microprocessors and Microsystems
2. 2.Muhammad Izhar Ramli, Mohd Helmy Abd Wahab, Nabihah, Towards Smart Home: Control Electrical Devices Online, Nornabihah Ahmad International Conference on Science and Technology: Application in Industry and Education.
3. 3.E. Yavuz, B. Hasan, I. Serkan and K. Duygu. Safe and Secure PIC Based Remote Control Application for Intelligent Home. International Journal of Computer Science and Network Security.
4. Amul Jadhav, S. Anand, Nilesh Dhangare, K.S. Wagh Universal Mobile Application Development (UMAD) On Home Automation Marathwada Mitra Mandal's Institute of Technology, University of Pune, India Network and Complex Systems (2012)
5. 5.Pratik Gadtaula, Home Automation, Telemark University College, Faculty of Technology, Master's Thesis
6. 6.A. J. Jara, Wearable Internet: Powering Personal Devices with the Internet of Things Capabilities 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, Beijing,, pp. 7-7(2014)
7. Y. Kung, S. Liou, G. Qiu, B. Zu, Z. Wang and G. Jong, Home monitoring system based internet of things 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, pp. 325-327(2018)
8. Y. Sun, Y. Xia, H. Song and R. Bie, Internet of Things Services for Small Town 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, Beijing, , pp. 92-95(2014).
9. D. Pavithra and R. Balakrishnan, IoT based monitoring and control system for home automation, Global Conference on Communication Technologies (GCCT), Thuckalay, , pp. 169-173.(2015)
10. H. V. Bhatnagar, P. Kumar, S. Rawat and T. Choudhury, Implementation model of Wi-Fi based Smart Home System, International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, pp. 23-28(2018).
11. M. C. Domingo, An overview of the Internet of Things for people with disabilities, Journal of Network and Computer Applications, vol. 35, Issue 2, pp. 584-596, (2012).
12. A. Olteanu, G. Oprina, N. Tapus and S. Zeisberg, Enabling Mobile Devices for Home Automation Using ZigBee,19th International Conference on Control Systems and Computer Science, Bucharest, pp. 189-195(2018)
13. R. Piyare and M. Tazil, Bluetooth based home automation system using cell phone, 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, pp. 192-195(2011)
14. Y. Upadhyay, A. Borole and D. Dileepan, MQTT based secured home automation system Symposium on Colossal Data Analysis and Networking (CDAN), Indore, pp. 1-4 (2016)
15. T. Wang, Y. Li and H. Gao, The smart home system based on TCP/IP and DTMF technology 2008 7th World Congress on Intelligent Control and Automation, Chongqing, pp. 7686-7691(2008).
16. T. M. Ladwa, S. M. Ladwa, R. S. Kaarthik, A. R. Dhara and N. Dalei, Control of remote domestic system using DTMF, International Conference on Instrumentation, Communication, Information Technology, and Biomedical Engineering 2009, Bandung, pp. 1-6 (2009)
17. N. M. Morshed, G. M. Muid-Ur-Rahman, M. R. Karim and H. U. Zaman, Microcontroller based home automation system using Bluetooth, GSM, Wi-Fi and DTMF, 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka,pp. 101-104(2015)
18. H. Brooke Stauffer Smart Enabling System for Home automation, IEEE Transactions on Consumer Electronics, Vol. 37(2) , pp. 29-35.(1991)

19. Faisal Baig, Saira Beg and Muhammad Fahad Khan, ZigBee Based Home Appliances Controlling Through Spoken Commands Using Handheld Devices International Journal of Smart Home, Vol. 7(1), pp 19 -26. (2013)
20. Pooja S Chinchansure, Charudatta V Kulkarni, Home Automation System based on FPGA and GSM, International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1 - 5 (2014)
21. A. Alheraish, Design and Implementation of Home Automation System, IEEE Transactions on Consumer Electronics ,Vol. 50(4) , pp. 1087-1092(2004).
22. Manoj Kumar Singh, Sadhan Mahapatra, Atreya Kumar Sudhir Green Building Design: A step towards sustainable habitat Conference Paper • (2012),
23. Home Automation Systems - A Study. Article in International Journal of Computer Applications • DOI: 10.5120/20379-2601(2015)