A Survey on Home Automation And Smart Security

K. Mohanapriya [1] , Y. Mercy Milcah[2] and K. Moorthi [3]
[1, 2] Dept of Computer Science and Engineering
[3]Assistant Professor, Dept of Computer Science and Engineering
[1, 2, 3] Jansons Institute of Technology, Coimbatore, Tamil Nadu, India.

Abstract- *Internet of things conceptualizes the idea of remotely connecting and monitoring real world objects through the internet. It is an upcoming technology that allows us to control hardware devices through the internet. Home automation aims to bring the control of operating your everyday home electrical appliances to the tip of your finger, thus giving user affordable lighting solutions, better energy conservation with optimum use of energy. Apart from just lighting solutions, the concept also further extends to have overall control over your home security. Which creates an inexpensive security system for homes as well as industrial use.This paper reviews about the use of IOT in order to control home appliances, automating modern homes through the internet.*

Keywords- Arduino, Home automation, Internet of things (IOT), Iot sensors, Smart Security.

I. INTRODUCTION

The Internet of Things refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data. Thanks to cheap processors and wireless networks, it's possible to turn anything, from a pill to an aeroplane to a self-driving car into part of the IoT. This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without a human being involved, effectively merging the digital and physical worlds.

IoT based Home Automation will enable the user to use a Home Automation System based on Internet of Things. The modern homes are automated through the internet and the home appliances are controlled. The user commands over the internet will be obtained by the Wi-Fi modems. The Microcontroller has an interface with this modem. The system status is displayed through the LCD display, along with the system data. This is a typical IoT based Home Automation system, for controlling all your home appliances.

Home automation and wireless Home security are the dual aspects of this paper. The beauty of the Home Automation system lies in the fact that the settings are manageable from your smart phones and other remote-control devices. Smart home IoT devices can help reduce costs and conserve energy. The Home Automation segment includes smart lighting, smart TVs and other appliances. Wearable's (Smart Watch, fitness brands, smart headphones, smart clothing) are also expected to witness the growth in the future. IoT is really the secret that makes this whole system work.

II. LITERATURE SURVEY

Mamathi et al[1], describes about survival on smart home in iot which comprises of Wi-Fi, Ambient intelligence and sensors such as medical sensors, temperature ,sound sensor, biometric. The home applications will have the following functions such as alert, monitor, control, frequency identification, intelligence. They says how the home automation system is working, what are all the management challenges, security and privacy challenges in iot. The main observation of their study is that IoT design can most likely best be delineated by a reference model than one design which there'll be many alternative thus far unknown applications/services which will hook up with the IoT applies additionally to object resolution mechanisms.

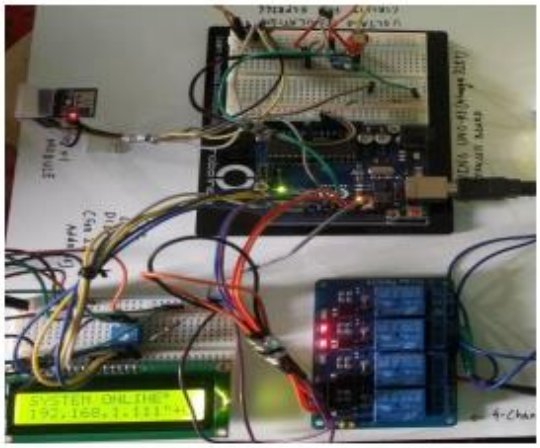
Shweta Singh et al[2] says that, in today's world ,IoT aims to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things.They describes about iot different services ,technologies and architecture which is the backbone of all the activities performed by the electronic devices and what are the different layers that works behind the iot architecture. The applications such as smart home, smart cars, smart tags, smart energy, smart packing etc., The main observation of the paper is that IoT architecture will probably best be described by a reference model than a single architecture and that there will be many different as yet unknown applications/services that will connect to the IoT applies also to object resolution mechanisms.

Mithun Prasad et al[3], describes about low value and versatile home management and monitoring system using an embedded based web server, with ip connectivity for accessing and controlling the devices and appliances remotely through android plat formed smart phone. They proposed an

architecture which consists of three layers: Home Environment, Home Gateway and Remote Environment . Remote Environment represents authorized users who can access the system on their Smart phone app using the Internet via Wi-Fi or 2G/3G/4G networks. Home Environment consists of Home Gateway and a hardware interface module. The primary function of the Home Gateway for the proposed architecture is to provide data translation services between the Internets. Android plat formed smart phone with inbuilt Wi-Fi are often used to access and manage the devices at home. Once a Wi-Fi connection isn't available, mobile cellular networks like 2G or 3G or 4G are often used to access the devices. They have a tendency to conjointly offer notification to the user regarding any error happens within the devices and send mail or SMS to the service supplier regarding the issues.

Ravi Kishore Kodali et al[4], focuses on building a smart wireless home security system which sends alerts to the owner by using Internet in case of any trespass and raises an alarm optionally. Embedded micro-controller and an onboard Wi-Fi shield making use of which all the elctrical appliances inside the home can be controlled and managed.The home automation system implementation setup consists of TI CC3200 LaunchPad, AccessibleWifi, Pir motion detector Sensor, Alarm, Relays for connecting home appliances, electromechanically controlled doors or windows, Mobile phone to recieve Voice Call, Energia (Software). If the system is dependent on the user's discretion and judgeability of the situation (whether it is a guest or an intruder entering his house) the use of a camera connected to the microcontroller might help the user in taking decisions whether to activate the security system or welcome the guest.

Lalit Mohan Satapathy et al[5], they takes a review about three different technologies such as Bluetooth, Zigbee, Esp8266-01 and finally design the system. It gives an idea about the operation of home automation system. The four different appliances such as fan, light, room heater and TV are operated remotely using Wi-Fi and through an application installed on android or iPhone. These appliances are connected through Arduino Uno with its digital input/output pins. These devices are connected with local Wi-Fi using a communicating module called esp8266-01.To implements their home automation system we have design a experimental setup.TheyusedArduino Uno as a main controlling unit. And a four channel relay board to control electrical home appliance. And they have included a Wi-Fi module in their system to connect android and local Wi-fi present in the home of user. The below diagram (figure-1) represents the experimental setup,



Figure(1)

Gaurav Panwar et al[6], in this paper they use IOT based home automation system which goal is to develop a home automation system that gives the user complete control over all remotely controllable aspects of his or her home. The experimental setup comprises of micro-controller module,ESP8266 is a system-on-a-chip (Soc), Analog-to-digital conversion (10bit ADC),serial peripheral interface(SPI) and different relays. They have embedded the ESP8266 Wi-Fi module with sugar cube relays to control devices wirelessly or from particular distance. Here they use hotspot configurations, that to achieve their project goal, it create a hotspot channel to connect other devices and so ESP8266.

Rahul Godha et al[7], they introduce access control for home automation devices for Internet of Things. which offers capabilities to identify and connect many physical sensors into a unified secure system. They proposed a solution that concentrates on controlling the access for the devices or objects that are connecting in home network. Irrespective of the authentication mechanism used, it focus on how much access should a device must get. Some home sensors can have access to a particular Server 1 while other sensor can have access to server 2 but not to server 1 [From Fig 2]. This access control can vary from sensor to sensor. There can also be sensors that cannot get any Internet access. The implementation setup consists of Centralized server that maintains the Access level codes to each connected sensor. The below diagram represents how two different servers connected to the home appliances.

Figure(2)

Awadalla Taifour Ali et al[8], describes about voice recognition based smart home control system which comprises of Smart Home, Wireless Technology and RF. Their paper aims to describe the method of testing the implementation of voice control over operating and technical functions of smart home. They use two different RF chips for transmitting and receiving signals. One of them is connected to the firstATmega328 working as the transmitter to transmit the signal and the other one is connected to the second ATmega16 working as the receiver. They captures human voice and compares with the recorded voice if it matches commands are send to the corresponding relays through RF , if it will not matches no commands are send and no appliances are activated. Based on these comparison they design their voice recognition system.

Abhay Kumar et al[9], proposed an energy efficient smart home automation system. They aim for the planning of a system which will minimize energy waste in home environments with efficiency managing devices operation modes. Materials and methodology based on VBB and optimization of smart home. Their model represents the automatic fan and its working.Firstly they have to provide the 220v supply to the model project, after that step down transformer is used to step down the power from 220V to 5V to the circuit. It works smartly if anyone enters through the door than IR sensors which are placed in door to count the person, if person enter in the room then the starts working, it means it won't work if there is no person inside the home then automatically the loads of the home is turns off. The main objective of their paper is to save the electrical energy that is wasted by many people in regular span of time.

Dhakad Kunal et al[10], designed an smart home system where the electrical appliances are controlled by the website. Their main objective is to help handicapped and aged people that will enable them to control home appliances and alert them in critical situations. They are developing a website, the application consist functions like light, fan, humidity and temperature control. When website opens, user is authenticated. Moved to main screen which displays home appliances. User has to select one to access it. Then he can check and change its status if he wishes. This system can be accessed from the web browser from any PC in the same LAN using server IP, or it can be accessed remotely through real IP or mobile handheld device connected to the internet with appropriate web browser .Wi-Fi technology connects server and the sensors. Wi-Fi is chosen to improve system security and to increase system mobility and scalability.

Jhonattan et al[11] , describes about security over smart home systems which comprises of Iot, Security, SHAS, Smart Home, Mechanisms. Their paper surveys several previous works from the security perspective with the purpose of providing the most important approaches in this field. They discussed about four different approaches used for home automation system such as Privacy approaches, Security approaches, Authentication approaches, Risk analysis approaches. Then explain the working procedure of those approaches. Finally they concluded that, iot is a new challenge for security; therefore, manufacturers need to improve their building processes and start considering security and privacy as part of the product rather than out-of-the-box solution or patch.

Daniel Schwarz et al[12], describes the current state of security in smart home systems. It examines what a smart home system is, how it is constructed and which protocols are used to communicate between the components themselves and their users. What are all the common threats to different sub-areas of smart home systems are discussed and the most popular communication protocols as well as their current state of security are presented. Their paper shows the current state of security of the five most common smart home local area communication protocols such as Z-Wave, ZigBee, BidCos, EnOcean, KNX. They introduce many new communication protocols and combine them with all the traditional web technologies. Therefore, one has to face all the well-known web vulnerabilities, as well as new, sophisticated low-level communication protocol flaws.

Andreas Jacobsson et al[13], describes the risk analysis of a smart home automation system . They says that, understanding the risks related to the use and potential misuse of information about homes, partners, and end-users, as well as, forming methods for integrating security-enhancing measures in the design is not straightforward and thus requires substantial investigation. In the risk scenarios of smart homes, it has been shown that connected devices may cause undesirable consequences to user privacy with respect to, e.g., access to potentially sensitive meta-information, and the misuse of user-intense mobile devices, and the risk of concept drift as novel devices, such as, surveillance cameras and personal wearables, which are often unplanned for, are dynamically attached to the smart home automation system.

The most sensitive part of smart home automation systems concerns information registry, in this case about the users' energy consumption, from which conclusions about a family's daily routines, life situations, etc., can be drawn, which may form decision support for criminal activities, such as, burglary, stalking, and identity theft.

Hanan Aldowah et al[14], discussed about the security in Internet of things such as Issues, Challenges and Solutions. Their paper reviews the research progress of IoT, and found that several security issues and challenges need to be considered and briefly outlines them. The aim of this study was to provide a review of the most critical aspects of IoT with specific focus on the security issues and challenges involved with IoT devices. Several problems and challenges related to the security of the IoT are still being faced. Research focuses are much needed in this area to address these security issues and challenges in IoT heterogeneous environments so that users can confidently use IoT devices to communicate and share information globally with safety assurance. In addition, their paper recommended some solutions from academic, technical, and industrial aspects. These solutions came in the form of architecture, new approaches and models, and mechanisms through which they aim to increase the quality of security in IoT environment.

Huichen Lin et al[15], presents the IoT Privacy and Security Challenges for Smart Home Environments. Their research is investigating two enhancements that are needed for a gateway-based Smart Home architecture to make it sufficiently secure for widespread adoption. Work is still in the early stages, so they present the problems, and overall system architectures, as a first step towards solutions. Auto-Configuration Support and IoT Software and Firmware Updates. A particular issue is that the security of the network depends on installation and configuration by largely untrained staff. This makes effective security policies and mechanisms much more difficult to develop, implement, enforce and maintain, unless this can be done automatically. A Smart Home gateway architecture supported by web-services for automatic device and network configuration and automatic system updates is their preferred approach for solving these problems.

III. PROPOSED SOLUTION

This solution concentrates on controlling the access for the devices or objects that are connecting in home network. The next phase for the home automation market will occur based on a few key improvements in the technology available in automation, such as improvements in wireless automation solutions as well as lowering of price points as the market begins to accept home automaton usage in larger volumes. our main objective of this paper is to provide safe and secured home automation system with minimum cost and how to overcome the challenges in iot.

IV. CONCLUSION

IoT technology has great impact in everyone's everyday life. This survey describes various methodologies used in home automation system to control and access the home appliances remotely through Internet services anywhere anytime. Several unlock issues related to privacy and security needs to be focused for future Internet of Things. Securing data, data management and privacy of every user plays a key role in the challenges of Internet of Things.

REFERENCES

[1] P. Mamathi , Dr. Venkatesh Kumar .S ,"A Survival on Smart Home in IOT", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Volume: 4 , Issue: 10 , September- October-2018.
[2] Shweta Singh, Kishore Kumar Ray, " Home automation system using internet of things", International Journal of Computer Engineering and Applications (IJCEA), Issn: 2321-3469.
[3] Mithun Prasad .R , Kesavamoorthy .M , Gunasekaran .S and Prof. B.M.Prabhu, " Internet of Things (IoT) – Ubiquitous Home Control and Monitoring System Using Android based Smart Phone", International Journal of Trend in Research and Development (IJTRD), Volume: 3(2), Mar - Apr 2016.
[4] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, " IoT Based Smart Security and Home Automation System", International Conference on Computing, Communication and Automation (ICCCA2016).
[5] Lalit Mohan Satapathy, Samir Kumar Bastia Nihar Mohanty," Arduino based home automation using Internet of things (IoT)", International Journal of Pure and Applied Mathematics (IJPAM), Issn: 1311-8080 (printed version); Issn: 1314-3395 (on-line version), 2018.
[6] Gaurav Panwar , Rajat Maurya , Rajesh Rawat, Rohit Kanswal4 and Praful Ranjan," Home automation using IOT application", International Journal of Smart Home (IJSH), Vol. 11, No. 9 (2017), pp. 1-8.
[7] Rahul Godha , Sneh Prateek , Nikhita Kataria," Home Automation: Access Control for IoT Devices", International Journal of Scientific and Research Publications (IJSRP), Volume: 4, Issue: 10, October 2014.
[8] Awadalla Taifour Ali, Eisa B. M. Eltayeb , Esra Altigani Ahmed Abusail," Voice Recognition Based Smart Home Control System", International Journal of Engineering Inventions, Volume: 6, Issue:4, April -2017.
[9] Abhay Kumar, Neha Tiwari," Energy Efficient Smart

Home Automation System", International Journal of Scientific Engineering and Research (IJSER), Volume: 3, Issue: 1, January- 2015.
[10] Dhakad Kunal , Dhake Tushar, Undegaonkar Pooja, Zope Vaibhav , Vinay Lodha," Smart Home Automation using IOT", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol: 5, Issue: 2, February- 2016.
[11] Jhonattan . J, Barriga. A, Sang Guun Yoo," Security over Smart Home Automation Systems: A Survey", Conference Paper (Research Gate) , April -2018.
[12] Daniel Schwarz," The Current State of Security in Smart Home Systems", SEC Consult Vulnerability Lab - Vienna, Version: V1.0 , Date: 2016-01-25.
[13] Andreas Jacobsson, Martin Boldt , and Bengt Carlsson," A Risk Analysis of a Smart Home Automation System".
[14] Hanan Aldowah , Shafiq Ul Rehman , Irfan Umar," Security in Internet of Things: Issues, Challenges and Solutions", Conference Paper (Research Gate), August - 2019.
[15] Huichen Lin , Neil W. Bergmann ," IoT Privacy and Security Challenges for Smart Home Environments", Article in Information (Research Gate), July - 2016.