iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55779

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Inter-Vendor Intra-Operation in Smart Home using Wi-Fi for Capacious Control and Remote Operation

Aayush Neupane[1], Shirshak Neupane[2]
[1]*Dr Ambedkar Institute of Technology, India*
[2]*University of Louisiana Monroe, Louisiana*

Abstract: ***Smart homes have been gaining a lot of momentum lately and people are rushing towards it, because of the ease of control, monitor and security that they offer. Although smart home installation has also become quite easier nowadays, but still pertains to be difficult choice to many, due to the exclusivity of the vendors or the inability of some vendors to support the Zigbee connection. Though Zigbee allows users to assemble their own choice of devices and consumption of low power, as long as the devices support Zigbee interface, but Zigbee still remains sort of unsafe and less capacious (expandable). Inter-vendor Intra-operability using Wi-Fi can provide easier installation and control options to the users and also increase the scalability of the smart homes, allowing the users themselves to choose from the devices that they want to install in their home, and providing them a common platform of control in form of a mobile application, from anywhere wherever the Wi-Fi or mobile internet provided. Also, the data transfer would be more secure and encrypted over Wi-Fi, faster and more expandable, even across the countries. In the project, we explore the interconnection of smart home devices from various vendor together with a Zigbee Bluetooth interface with a mobile application for control, enabling the smart homes more accessible by cost cutting.***
Keywords: Wi-Fi, Zigbee, IEE 802.11.x.x, inter-vendor, intra-operation, Router, Raspberry Pi

I. INTRODUCTION

The escalation in the installation of smart homes has been quite aggressively abrupt in recent times. With the advance in time, and progress in technology, every aspect of our life has seen an evolution. Correspondingly the way we live in our homes have changed. Our homes have become quite smart, being able to control the temperature, light, humidity, surveillance and security, and also take security actions. Therefore, various vendors have grown, providing smart home services. The issue is with the lavished tariff of installation, usually due to the exclusivity of the vendors, not offering the dexterity to the users of opting for the individual devices of their choice or preferred vendors, maybe for cost cutting or extra features, because not every vendor would support the Zigbee Interface.



Fig 1: Smart Home
(Source: https://tridenstechnology.com/what-is-a-smart-home/)

©IJRASET: All Rights are Reserved

Inter-vendor intra-operation using is the probable solution to the problem stated. Inter-vendor intra-operation is the concept wherein smart home devices used are assembled from different vendors, connected via Wi-Fi, instead of Zigbee interface, to a mobile phone app via Wi-Fi. Inter-vendor intra
operation of devices, not only helps users design and create their own blueprint of smart homes, but also allow users to add the custom features, or feasible cost. Wi-Fi today is universal, available easily and in cheap in every urban area. This replaces the use of Zigbee, depleting the risk of security issues and also enhancing the expandability.

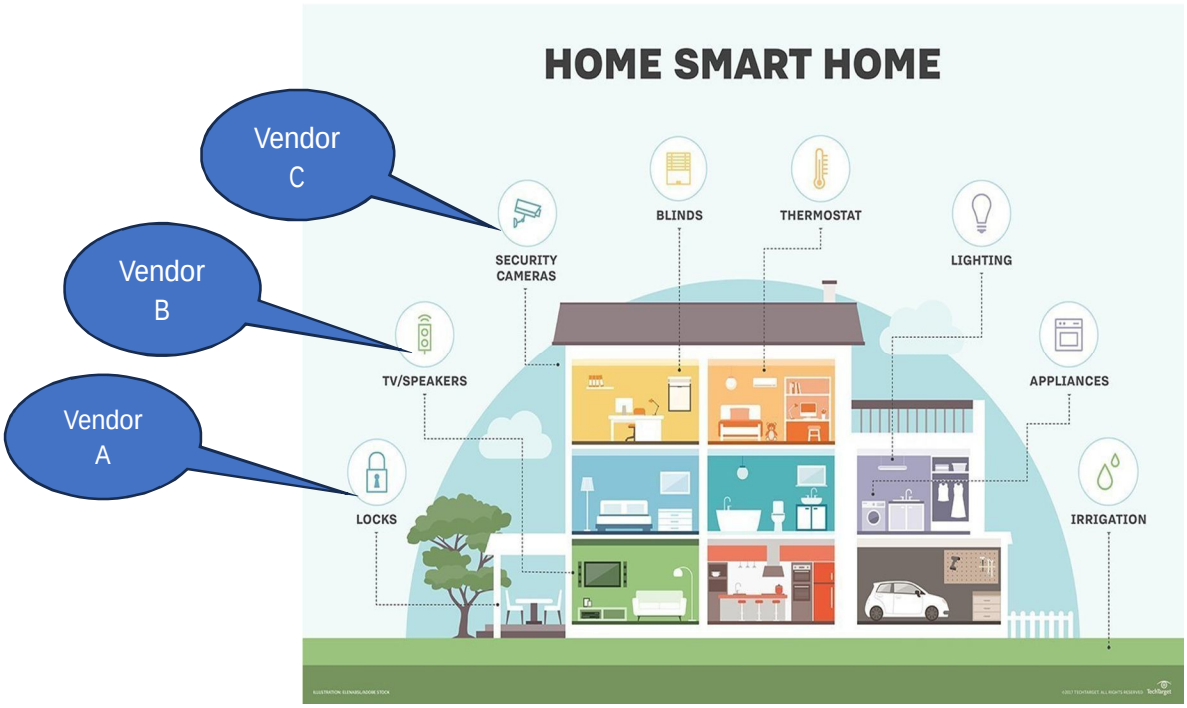


Fig 2: Inter Vendor Smart Home
(Source: https://www.techtarget.com/iotagenda/definition/smart-home-or-building)

II. EXISTING SYSTEM

In the current scenario, the devices from the vendors supporting Zigbee, used in the smart home system, are connected to the Zigbee Router via LAN, in the cluster. The routers are then connected to the central controller. The controller is then connected to the Cloud via the gateway (Zigbee interface). Then the cloud is accessed via the central controller application in mobile phone, allowing users to control the devices like light, fan, thermostat, tv, speakers etc.

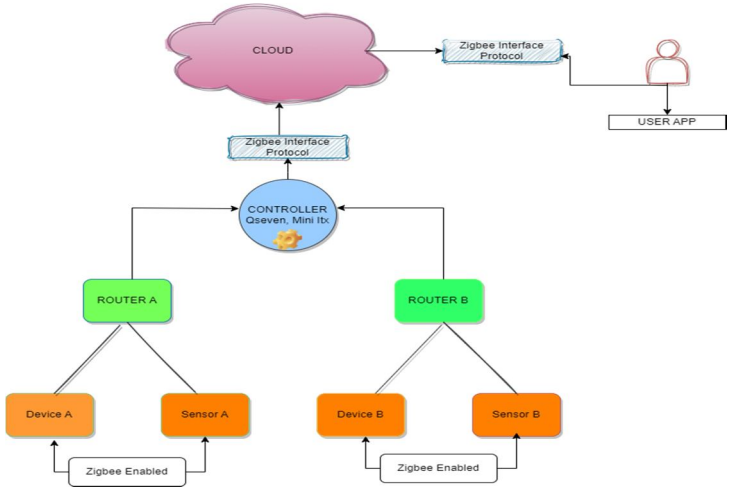


Fig 3: Working of Smart Home Existing Technology

©IJRASET: All Rights are Reserved

Smart homes usually make use of Zigbee interface for the inter connection in smart home automation, and though provide features like less power requirement, but it has some limitations, devices must be able to support Zigbee interface one, and second is the lack of security and third being lack of expandability.

III. PROPOSED SYSTEM

Use of Wi-Fi interface as mesh topology among the smart devices and sensors, removing the Zigbee interface. The devices and the sensors, that support Wi-Fi 802.11.x.x family will be connected to each other via a single Wi-Fi router, which will be transmitting the information to the cloud. Cloud further connects the system to the mobile app or the network to which the phone app is connected. The user will be able to control the automated home and devices via Wi-Fi,

The advantages of the proposed system:

1) More vendors are able to support Wi-Fi nowadays, therefore users being able to congregate varied options of devices according to their needs and budget.
2) Faster rate of Data Transmission
3) Installation cost is decreased as Wi-Fi services are cheaper nowadays.
4) More security offered by Wi-Fi.

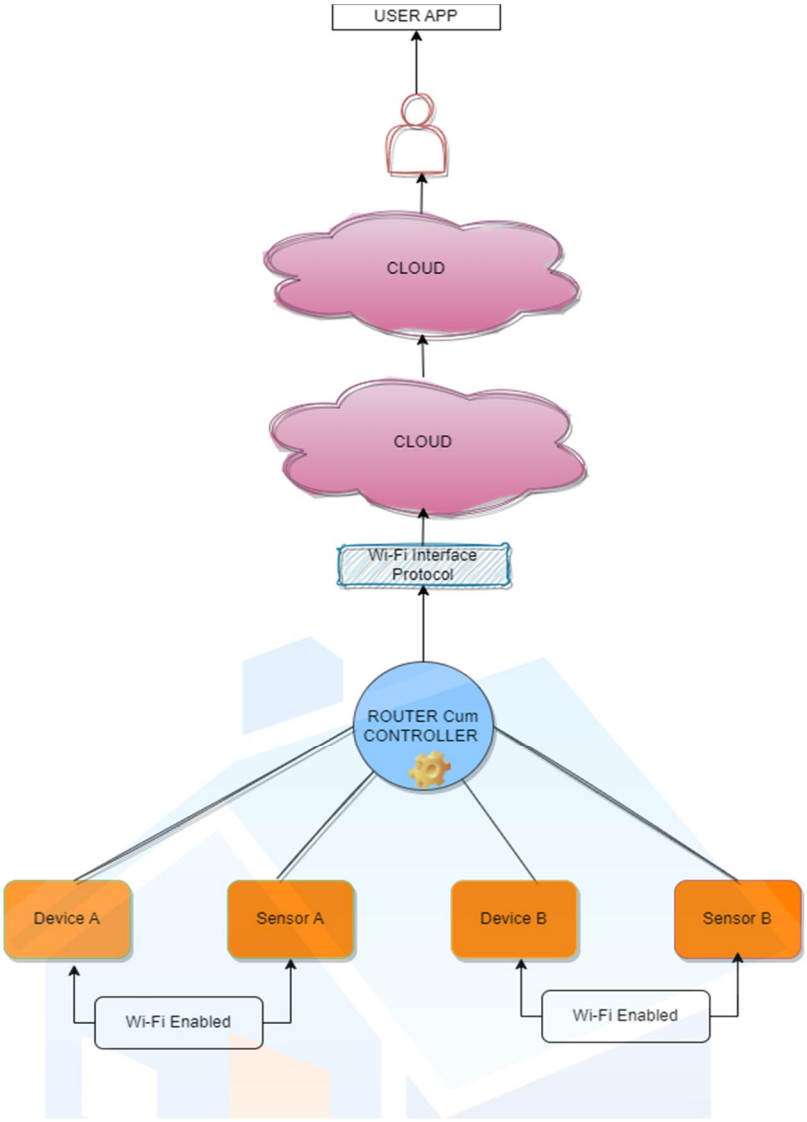


Fig 4: Proposed System of Smart Home Inter vendor Intra operation

IV. LITERATURE SURVEY

"A Research Paper on Internet of Things based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro" by Ahmad Bilal Zia M.Tech(CSE), School of Technology & Sciences,Alakh Prakash Goyal Shimla University, Shimla (HP), Ms. Kshamta Chauhan Assistant Professor, School of Technology & Sciences, Alakh Prakash Goyal Shimla University, Shimla (HP)
Ahmed Bilal Zia and Ms. Kshamta Chauhan [1] have talked about the enhanced security with security risk assessment using OCTAVE Allegro. The octave allegro methodology is intended to create strength in consequences, allowing exhaustive risk evaluation, concentrating totally on information sources. The method investigates how the records are utilized by the clients or frameworks. In addition, it facilitates across the area where the records live and on how it is presented to risks. Octave Allegro gives route, worksheets and surveys for leading the chance appraisal.

"A secure Bluetooth-ZigBee gateway for IoT" by A.S.Prakash, B.S.S.Tejesh, S.Neeraja, N.Sri Babu
Dept of Electronics and Communication Engineering, SRK Institute of Technology, Enikepadu, Vijayawada
A.S. Prakash, B.S.S. Tejash, S. Neeraja, N. Sri Babu [2], have exchanged a view on secure Bluetooth-Zigbee gateway for IOT. The gateway proposed establishes the short distance transmission of Zigbee and remote data transforming Bluetooth Protocol information or Zigbee Protocol information vice versa and transmitting them to one another. The idea of gateway can be used in our proposed system as well.

"The 10 Research Topics in the Internet of Things" Wei Emma Zhang, Quan Z. Sheng, Adnan Mahmood, Dai Hoang Tran, Munazza Zaib, Salma Abdalla Hamad, Abdulwahab Aljubairy, Ahoud Abdulrahmn F. Alhazmi, Subhash Sagar, and Congbo Ma
School of Computer Science, The University of Adelaide, SA 5005, Australia
Department of Computing, Macquarie University, NSW 2109, Australia
Wei Emma Zhang. Quan z. Sheng, Adnan Mahmood, Dai Hoang Tran, [3] have deliberated various topics on IOT for research in their paper named *"The 10 Research Topics in The Internet Of Things"*. They have talked about Social IOT and Data Security and Privacy in IOT.

"A REVIEW ON ZIGBEE TECHNOLOGY IN INTERNET OF THINGS (IOT) AND ITS APPLICATIONS" by Nazarene Mustoor, Riya Patro, Ankit Mishra, Suniti Purbey, Department of Computer Science, Amity University Chhattisgarh
Nazarene Mustoor, Riya Patro, Ankit Mishra and Suniti Pandey [4] have reviews the Zigbee technology in IOT. The paper describes about the working of Zigbee, and the security provided by it. Zigbee uses the highly secure 128-bit AES based encryption, but due to low cost its security layers are stacked over one another in *'open trust'* model. Also Zigbee's use in Home Automation are backed by Samsung, Bosch, Texas Instruments, Honeywell and Amazon. Zigbee Alliance has more than 400 devices enlisted.

"Smart Home Control" by Syeda Assistant Professor Ayesha Unisa, Final year UG StudentsD Sharath, Adithi Pateriya, Chinmay Chauhan, Sahithi Sri Garimella Department of Computer Science and Engineering, MVJ College of Engineering, Bangalore, India
Syeda Ayesha Unisa, D Sharath, Adithi Pateriya, Chinmay Chauhan, Sahithi Sri Garimella [5], have described on the control system of Smart Homes. They have designed the event of a firmware for smart home control which could successfully be automated minimizing human interaction to preserve the integrity within whole electrical devices within the house. We used *NodeMCU*, a popular open source IOT platform, to execute the tactic of automation. Different components of the system are visiting be conversant in control the appliance supported the user's input through ***NodeMCU.***

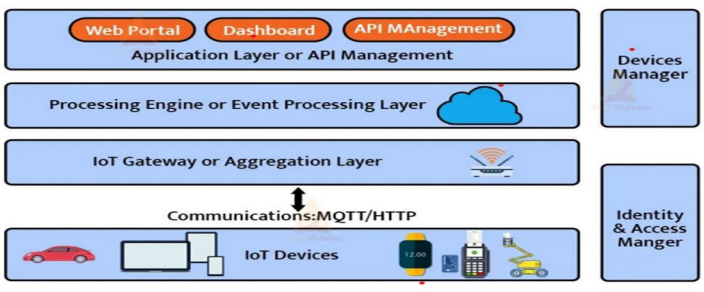


Fig 5: Architecture of Smart home

(Picture Original Credits: Syeda Ayesha Unisa, D Sharath, Adithi Pateriya, Chinmay Chauhan, Sahithi Sri Garimella Assistant Professor, Final year UG Student, Department of Computer Science and Engineering, MVJ College of Engineering, Bangalore, India)

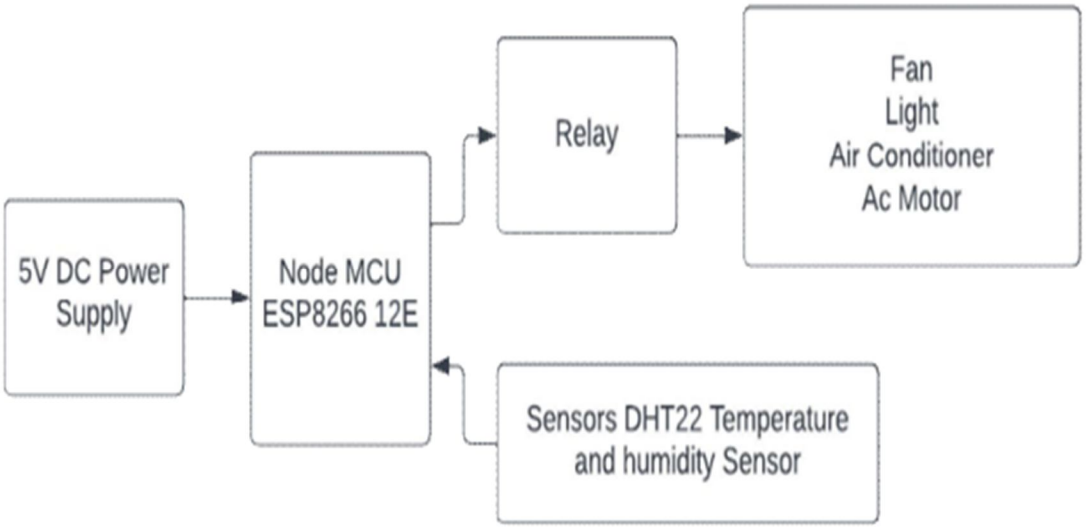


Fig 6: Smart Home Control Using Node MCU ES8266 12E

(Picture Original Credits: Syeda Ayesha Unisa, D Sharath, Adithi Pateriya, Chinmay Chauhan, Sahithi Sri Garimella Assistant Professor, Final year UG Student, Department of Computer Science and Engineering, MVJ College of Engineering, Bangalore, India)

V. METHODOLOGY

The most crucial part of the development of the inter-vendor intra-operation system is to deploy the Wi-Fi enabled devices with Wi-Fi communication protocols communicating it with the server in the cloud. The development of the inter-vendor intra-operation automation system is divided into departments of Essentials, Multimedia, Surveillance, Alarm, Interface and Control.

1) Router: Router is used to connect all the Wi-Fi enabled devices and sensors.
2) Controller: Raspberry Pi is used as a controller.
3) Wi-Fi Dongle: Is used to provide Wi-Fi access to the raspberry pi.
4) Smart Light, Smart Fan, Smart Thermostat, Smart AC, Smart Refrigerator are selected as Essentials.
5) For Multimedia, smart speakers, smart TV, smart sound system selected as Multimedia.
6) Servo Motor: Entryway lock
7) Infrared Sensor (IR): to detect the circumstance of the front entryway.
8) Proximity Sensor: For detection of human and animals.
9) Smoke Detector and Alarm for fire control.
10) CCTV camera for surveillance.
11) Mobile application for control.

All the selected devices are Wi-Fi enabled and connected to Raspberry Pi as controller via Router. The router collects the data from the devices and pushes it to the cloud via controller.
The cloud connects it to the mobile app. The user sends instructions from mobile app, received by router to the controller and controller performs the action. The notification of action completed or not, is again carried by router to the cloud again. Then the user receives the notification from the cloud in their mobile app.

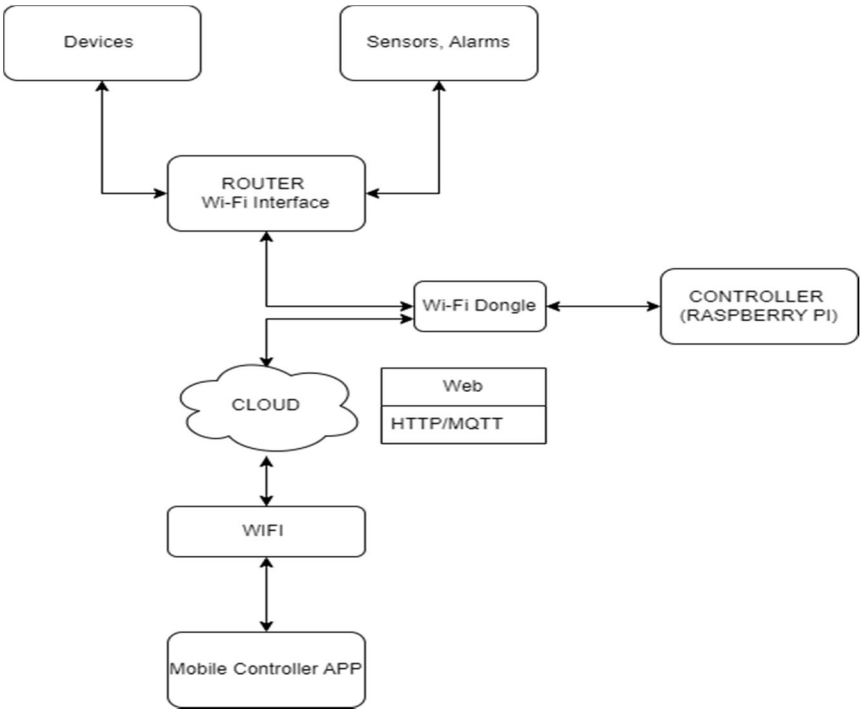


Fig 7: Flowchart of working of Proposed System

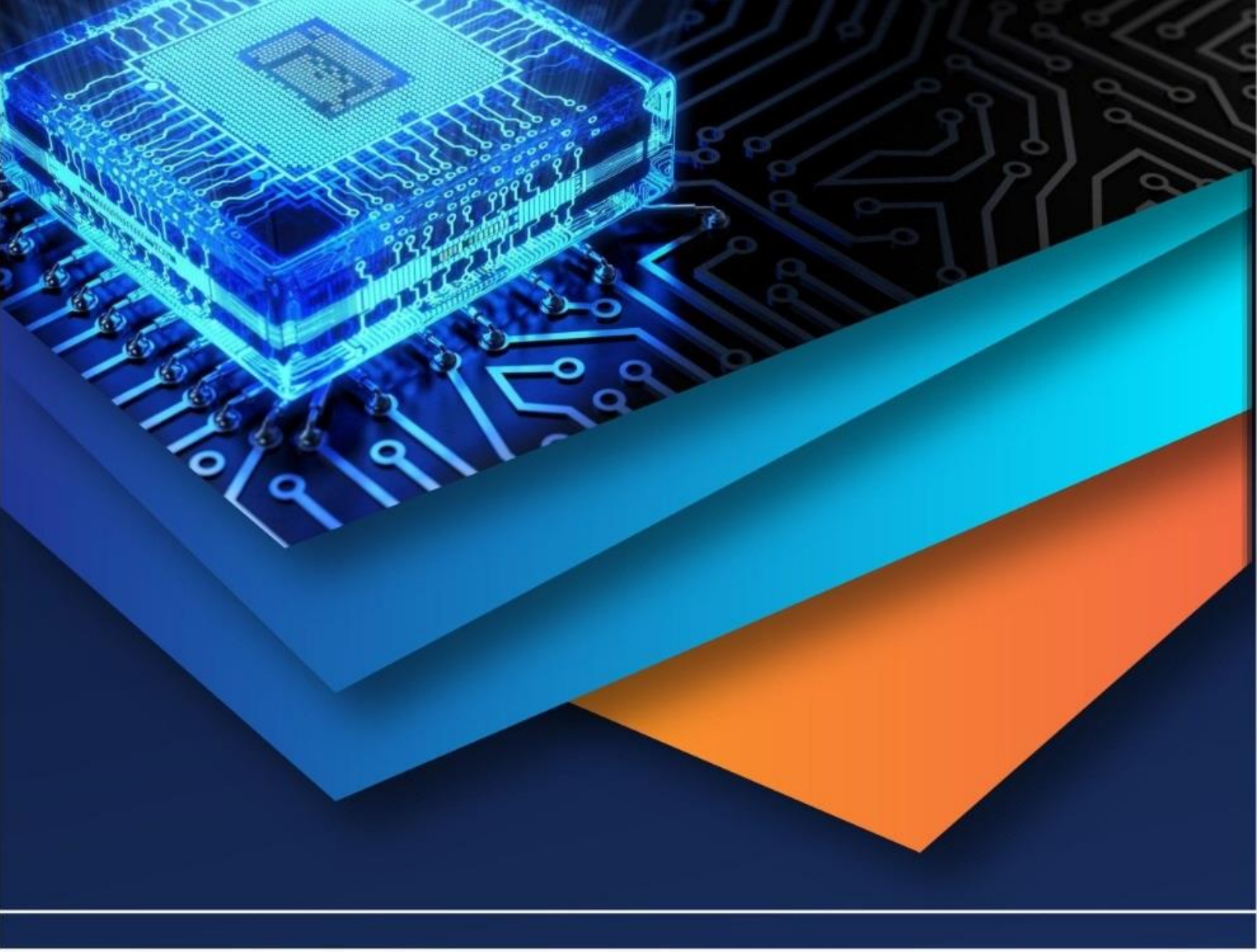
VI. CONCLUSION

"Everything is connected" in this world nowadays, due to the advancement of IOT. And our way of living and housing does not remain unaffected. Smart home automations have been in an ascension. Multiples vendors have come up and vendors like Samsung, Amazon have their devices Zigbee enabled in order to be stockpiled in smart home automation. Though Zigbee provide multi vendors to communicate to each other and is also low powered option, but controlling and monitoring automated home only from inside of home is not enough. People want to control and Monitor home from distance maybe from office. For this extent of expandability, Wi-Fi provides the ability. Therefore, the inter-vendor intra-operation is more effective, also in a sense that Wi-Fi is omnipresent, faster, secure and can provide a real good option when it comes to devices selection to the users.

REFERENCES

[1] "A Research Paper on Internet of Things based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro" by Ahmad Bilal Zia M.Tech(CSE), School of Technology & Sciences,Alakh Prakash Goyal Shimla University, Shimla (HP), Ms. Kshamta Chauhan Assistant Professor, School of Technology & Sciences, Alakh Prakash Goyal Shimla University, Shimla (HP)
[2] "A secure Bluetooth-ZigBee gateway for IoT" by A.S.Prakash, B.S.S.Tejesh, S.Neeraja, N.Sri Babu Dept of Electronics and Communication Engineering, SRK Institute of Technology, Enikepadu, Vijayawada
[3] "The 10 Research Topics in the Internet of Things" Wei Emma Zhang, Quan Z. Sheng, Adnan Mahmood, Dai Hoang Tran, Munazza Zaib, Salma Abdalla Hamad, Abdulwahab Aljubairy, Ahoud Abdulrahmn F. Alhazmi, Subhash Sagar, and Congbo Ma School of Computer Science, The University of Adelaide, SA 5005, Australia Department of Computing, Macquarie University, NSW 2109, Australia
[4] "A REVIEW ON ZIGBEE TECHNOLOGY IN INTERNET OF THINGS (IOT) AND ITS APPLICATIONS" by Nazarene Mustoor, Riya Patro, Ankit Mishra, Suniti Purbey, Department of Computer Science, Amity University Chhattisgarh
[5] "Smart Home Control" by Syeda Assistant Professor Ayesha Unisa, Final year UG StudentsD Sharath, Adithi Pateriya, Chinmay Chauhan, Sahithi Sri Garimella Department of Computer Science and Engineering, MVJ College of Engineering, Bangalore, India
[6] https://homey.app/en-au/wiki/what-is-zigbee/
[7] https://www.pocket-lint.com/smart-home/news/129857-what-is-zigbee-and-why-is-it-important-for-your-smart-home
[8] https://en.wikipedia.org/wiki/Zigbee
[9] https://zigbeealliance.org/about/
[10] https://en.wikipedia.org/wiki/IEEE_802.15.4
[11] https://web.archive.org/web/20120319184855/http://sensor-networks.org/index.php?page=0823123150
[12] https://www.electronicshub.org/zigbee-technology-architecture applications/#:~:text=Although%20Zigbee%20Technolog

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)