IOT Applications, Challenges and Emphasis on Energy Efficient System for Smart Home Renovation

Aditya Shukla[1#], Dr. Sanjay Dubey[1]
[1]*Department of Computer Science, SAGE University, Indore, (M.P.) 452001, India*

***Abstract*—The network of physical items, or "things," that are implanted with sensors, software, and other technologies in order to communicate and exchange data with other devices and systems over the internet, is known as the Internet of Things (IoT). A new paradigm known as the Internet of Things (IoT) has transformed traditional living into a high-tech way of existence. These changes brought about by IoT include smart cities, smart homes, pollution reduction, energy conservation, smart transportation, and smart industries. Every device in the Internet of Things (IoT) smart home is controlled by a central hub that is online. Where the central hub is controlled by a mobile app that uses. The capability of controlling and monitoring a variety of systems and devices is one of the main advantages of IoT-enabled home automation. Software, hardware, sensors, protocols, architecture, and platforms are all covered in IoT-based home automation. Home security, air quality monitoring, entertainment delivery, smart locks, smart energy meters, and other features are made possible by utilizing IoT connectivity. This article will discuss the difficulties associated with IoT-based homes, as well as a simulation and a suggested IoT-based smart energy-efficient system for homes of the future.**

Keywords: Home Automation, Smarthomes, energy efficient components, Internet of Things

INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm that enables the communication between electronic devices and sensors through the internet in order to facilitate our lives. IoT use smart devices and internet to provide innovative solutions to various challenges and issues related to various business, governmental and public/private industries across the world. IoT is progressively becoming an important aspect of our life that can be sensed everywhere around us. In whole, IoT is an innovation that puts together extensive variety of smart systems, frameworks and intelligent devices and sensors (Figure 1)[1]

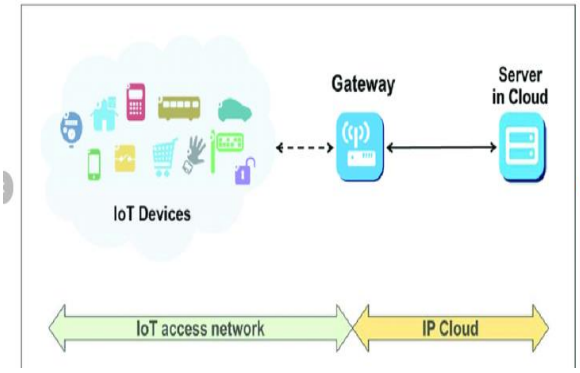

Figure 1: General Architecture of IOT [2]

Furthermore, it leverages the advantages of quantum and nanotechnology to achieve previously unthinkable levels of storage, sensing, and computing speed. To demonstrate the potential efficacy and applicability of IoT changes, much research has been conducted and is available in the form of scholarly articles, news reports, and printed materials on the internet and in print media. Before creating creative, inventive company ideas, it might be used as a preparation task while taking security, assurance, and interoperability into consideration [2]

Our everyday lives are changing significantly as a result of the growing use of IoT devices and technology. The idea of smart home systems (SHS) and appliances, which include internet-based gadgets, home automation systems, and dependable energy management systems, is one example of an IoT development. In addition, the Smart Health Sensing System (SHSS) is another noteworthy IoT accomplishment. Small, intelligent appliances and gadgets are incorporated into SHSS to promote human health. To evaluate and monitor various health conditions, fitness levels, the number of calories expended in the fitness facility, etc., these gadgets can be utilized both indoors and outdoors. Additionally, hospitals and trauma centers utilize it to keep an eye on vital health issues.

As a result, it has completely transformed the medical industry by enabling it with cutting-edge technology and intelligent gadgets [3]. Additionally, IoT researchers and developers are actively working to improve the quality of life for the elderly and disabled. IoT has performed remarkably well in this field and given such people's daily lives a new direction. The majority of people are using these devices and equipment since they are easily accessible and within a regular price range, making them highly cost-effective in terms of development. They are able to lead normal lives because to IoT. Transportation is another essential component of our daily lives. New developments in IoT have made it more dependable, comfortable, and efficient.

The traffic at several signalized crossings in major cities is currently being managed by intelligent sensors and drone gadgets. Furthermore, automobiles are being introduced in markets with sensors built-in. These sensors may identify impending areas of high traffic on a map and recommend an alternate route with less traffic. As a result, IoT is very beneficial in many spheres of technology and life. We can draw the conclusion that IoT has enormous potential to advance technology and benefit humanity [4].

IoT has also demonstrated its significance and promise for a developing region's industrial and economic development. Also, it is regarded as a revolutionary move in the trading and stock exchange markets. Nonetheless, data and information security is a serious problem that requires a lot of work and is something that should be prioritized. Since the internet is the main source of security risks and cyberattacks, hackers have gained access to a variety of resources, making data and information unsafe. IoT is dedicated to provide the greatest solutions available to address data and information security concerns, though. Security is therefore the main issue with IoT in trade and the economy. Therefore, the development of a secure path for collaboration between social networks and privacy concerns is a hot topic in IoT and IoT developers are working hard for this [1-4].

Home automation using IOT:

We refer to the entire set of technologies that make it possible for a device to be online as the "Internet of Things." These systems are dependent on gathering data. The data is then used for data management, monitoring, and transmission to other devices over the internet. This makes it possible for specific actions to be activated automatically in response to specific events. Many different devices are powered by the Internet of Things. It consequently began to show up in a number of sectors, including smart homes. Using IoT in the house is based on the concept of automatically configuring all of the devices, as illustrated in Figure 2. That home is equipped with Internet of Things technology. Rather than having to physically approach the device and complete the required tasks, those actions can be carried out with a simple button push. Nowadays, voice commands or apps are the primary means of controlling most smart Internet of things (IoT) home automation equipment [5, 6].

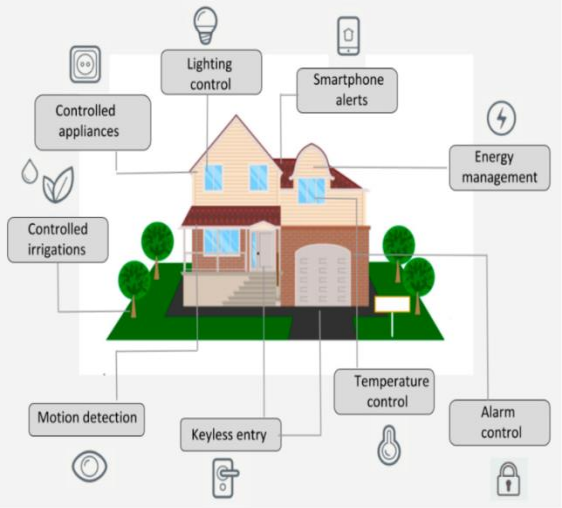

Figure 2 IoT in Smart Home [6]

All connected smart meters, thermostats, security systems, smoke detectors, presence detectors, and other sensors that are linked to gadgets that resemble home automation boxes are together referred to as Internet of Things (IoT). IoT home automation is the process by which a house performs particular functions automatically. The term "Internet of Things" (IoT) in home automation refers to the integration of smart devices and technology to automate and intelligently govern numerous areas of a home. Homeowners may monitor and manage their properties from anywhere with Internet of Things (IoT)-enabled devices that can connect to the network and exchange data with one another via laptops, tablets, and smartphones.

Here are some common examples of how IoT is used in home automation:

Smart Lighting: Users may remotely adjust the brightness, color, and scheduling of their lights with IoT-enabled light switches and bulbs. Moreover, motion sensors can be included to automatically turn on and off lights when someone walks into or out of a room.

Smart Thermostats: thermostats with Internet of Things connectivity let homeowners control their house's temperature from a distance. These gadgets can adjust heating and cooling based on user preferences, conserving energy and improving comfort.

Smart Security Systems: Motion sensors, doorbell cameras, and security cameras powered by the Internet of Things can all be remotely accessed and managed. On their phones, users can get real-time alerts in the event of any questionable activities. Features of a smarthouse include air quality, humidity, water leakage and much more. To make sure everything is in working condition and identify possible problems early on, this data can be accessed remotely.

Smart equipment: Internet of Things-enabled equipment, such as vacuum cleaners, washing machines, refrigerators, and ovens, can be conveniently and effectively controlled from a distance.

Voice Assistants: Apple HomePod, Google Home, and Amazon Echo (Alexa) serve as primary hubs for voice-activated control of a variety of IoT devices.

Automated Window Coverings: To control natural light and privacy, Internet of Things-enabled blinds and curtains can be remotely controlled or programmed to open and close at certain intervals.

Energy Management: By automatically shutting off inactive devices, modifying lighting in response to natural light, and effectively controlling heating and cooling systems, IoT systems can help minimize energy use.

Smart Locks: Internet of Things (IoT)-based smart locks allow homeowners to grant access to guests even while they are not at home. They also provide keyless entry and remote control functionality.

Health and Wellness: Smart scales, fitness trackers, and sleep monitors are examples of IoT devices that may be used in the home to monitor health and wellness. These devices also give consumers access to important health data. To control natural light and privacy, T-enabled blinds and curtains can be remotely controlled or programmed to open and close at certain intervals. The incorporation of IoT technology into home automation has the capacity to augment homeowner convenience, optimize energy efficiency, heighten security, and boost overall quality of life. To guard against potential cyber risks and data breaches, IoT device setup must give privacy and security first priority [6,7].

IOT Components

An Internet of Things solution consists of these five basic components:

- objects (sensors),
- the network (connectivity),
- information,
- data
- programs Operating

Challenges faced By IOT Technlogy

The Internet of Things (IoT) has become a ubiquitous presence in human life, posing a number of difficult challenges and issues due to the diverse technologies used in data transfer between embedded devices. In the sophisticated smart tech society, these problems also provide a difficulty for IoT developers. The problems and need for sophisticated IoT systems are expanding along with technology. As a result, IoT developers must consider potential new problems and offer solutions.

Security and privacy issues

Due to numerous dangers, vulnerabilities, cyberattacks, and threats, security and privacy are among the most significant and difficult IoT challenges. Inadequate permission and authentication, unsafe software, firmware, web interfaces, and inadequate transport layer encryption are the problems that lead to device level privacy. Concerns about security and privacy are crucial factors in building trust in IoT systems in a number of ways. To avert security threats and attacks, security procedures need to be included into every tier of the Internet of Things architecture. Two cryptographic protocols that are used in different Internet of Things systems to provide security solutions between the transport and application layers are Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) [8].

Interoperability/standard issues

The ability to share data between various IoT systems and devices is known as interoperability. The gear and software that have been installed are not necessary for this information exchange. The diverse nature of the many technologies and solutions utilized for Internet of Things development gives rise to the interoperability problem. There are four different layers of interoperability: syntactic, semantic, organizational, and technical. Researchers approved a number of methods known as interoperability handling approaches because they saw interoperability as a critical issue. These solutions could be based on virtual networks or overlays, adapters/gateways, service-oriented architecture, etc. [9].

Ethics, law and regulatory rights

The ethical, legal, and regulatory aspects of IoT development are additional concerns. To uphold moral standards and deter people from transgressing them, there are laws and policies in place. The only real distinction between the terms ethics and law is that the former refers to moral principles, while the latter are constraints set by the state. But rules and ethics are meant to uphold the norm, preserve quality, and keep people from abusing them [10].

Scalability, availability and reliability

If additional services, tools, and devices can be added to a system without causing it to perform worse, then it is scalable. Supporting a vast number of devices with varying memory, processing, storage power, and bandwidth is the primary challenge with IoT. The availability is a crucial element that should not be overlooked. Both availability and scalability ought to be implemented simultaneously in the IoT's tiered architecture. Cloud-based IoT solutions are an excellent illustration of scalability since they offer enough support to grow the IoT network by adding more devices, storage, and computing power as needed.The availability of resources to the legitimate items at the required time and location presents another significant challenge. A number of tiny IoT networks are periodically connected in a dispersed manner to the international IoT platforms in order to make use of their resources and services. As a result, reliability is a crucial issue [11].

Quality of Service (QoS)

An additional crucial component of IoT is quality of service, or QoS. A measure of the effectiveness, efficiency, and performance of IoT systems, architecture, and devices is known as quality of service (QoS) [34]. For Internet of Things applications, dependability, cost, energy consumption, security, availability, and service time are critical and necessary quality of service (QoS) parameters. QoS standards must be met by a more intelligent IoT ecosystem [12].

Applications of Iot

Emerging economy, environmental and health-care

IoT is entirely focused on bringing new public and economic advantages and development to society and its citizens, which in turn promotes industrialization, economic growth, water quality preservation, and well-being, among other things. IoT devices and systems are monitored for potential negative environmental effects in order to promote environmental sustainability [9,13].

Smart city, transport and vehicles

With the concepts of smart homes, smart cities, and smart transportation and vehicles, the Internet of Things is reshaping society's conventional civil structure into a high-tech framework. To create an effective smart city, a variety of technologies, including wireless sensor networks and cloud server technology, must be integrated with IoT servers. The design and development of smart city infrastructure should also take green and energy-efficient technologies into account [14].

Agriculture and industry automation

An essential part of our existence is agriculture. Technology and agriculture must be combined in order to increase production. To feed a vast population, we must improve the current agricultural practices. One technology to improve production is greenhouse technology, which modifies environmental factors. However, this technology cannot be controlled manually, which wastes energy and reduces productivity. It also requires human labor and costs money. The development of the Internet of Things has made it simpler to monitor the process and regulate the chamber's temperature, which saves energy and improves output [15].

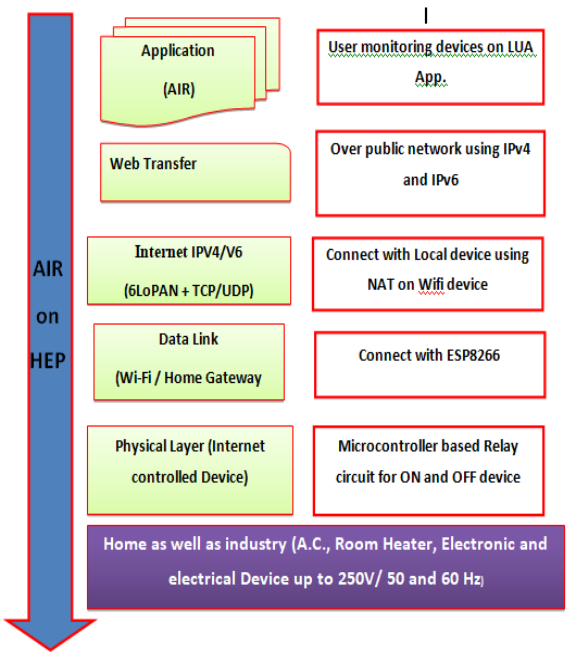

Figure 3. AIRonHEP different layer flow

Proposed Method

The demand of current era in IoT that is security, secure access and controlling of multiple devices, that is the major issue of previous years research work. This problem is rectified in proposed implemented IoT protocol, the proposed method works in two different scenarios. In the first scenario user based controlling shows and the second system is based on Auto controlling system. In the first case user depends on device controlling system for security check for the various device control that is based on home entry point (HEP) shown in figure 6.1 based image processing based identification. In which user perform action immediate response (AIR), direct communication between the user and smart devices via secure protocol (https) layer over IPv6 with server-based security system using home entry point network, So the complete name of the first proposed system is AIRonHEP (Action Immediate Response on Home Entry Point).

Action Immediate Response on Home Entry Point (AIRonHEP)

This proposed system is used to give direct action on HEP. This protocol work starts on IoT application layer and ends on receiver end physical layer device like ON and OFF devices. The action immediate response on home entry point is very important when automatic machine based working is failing and not following the proper instruction, at that time proposed protocol help to control and manage wireless devices and nodes at the far end.

Figure 4. LUA based device controlling system

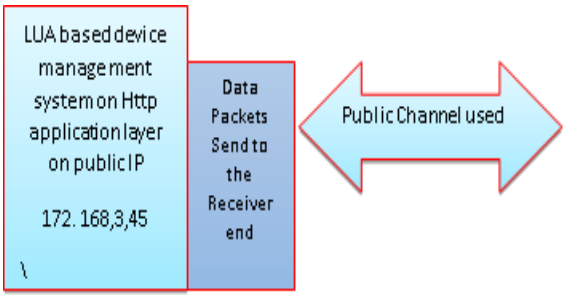

Figure 5. Block Diagram of Transmitter end

In the above Figure 3 shows the work performed on different layers with different devices. This proposed protocol is designed for long-distance device management system. For this use sensor for information, gathering from different location at home and also applicable in different homes in the colony and send data via home entry point (HEP) to sever. It creates data logs on sequel query language (SQL) server. For devices action immediate response(AIR) based quick response device management system using LUA programming script, that is used to send the signal for ON and OFF over public net to wireless fidelity /access point of ESP8266 based home entry point(HEP). As per user instruction ESP8266 sends an instruction to receiver signal check, read instruction and immediately take action using microcontroller – relay based centralized system. Relay applies action down logic and load disconnected with the device. In this way, we can manage the wireless devices from long range. In fact this technique is also useful to control the devices over a country distance. Not only for device management, it is also used for medical operations and another industrial purpose management also used for medical operations and another industrial purpose.

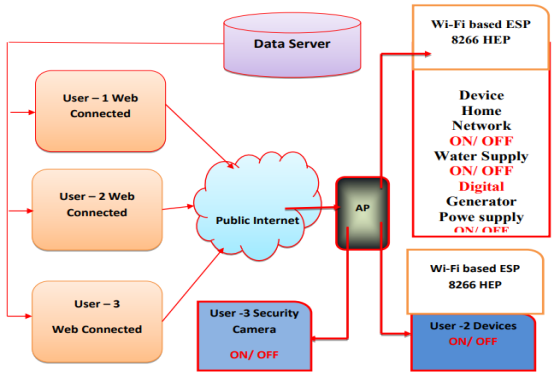

Figure 6. AIRonHEP different layer flow

Transmitter End

On the transmitters end, it sends the input signal over IoT application layer, which is designed for LUA software. LUA software is open source platform used to design IoT architecture. LUA is basically is php+ based. This web page generated a signal and send on public internet to A.P. and Wi-Fi directly. Figure 4 shows the webpage snap and Figure 5 shows the block diagram of transmitters end.

Receiver End

On the previous information that is accessed by data log and checks the work whether it got information from server, devices not working properly then user interrupt the working of devices. At that time user directly connected to the device with locally assigned internet protocol (IP) address by access point (AP), wireless fidelity (Wi-Fi) and directly send command for ON and OFF the particular device

Figure 6 shows that different user how to control the own device by direct – action immediate response on home entry point using ESP8266. In the above information both parts are shown -transmitter as well as receiver part. With the help of access point create personal area network (PAN) that is dedicated to any society or multiple apartments and buildings. This application encompasses a nice flexibility because it is using IoT technology.

In proposal of this method, a lot of research articles have been surveyed. However some research works were too motivational to carryon. These research articles were quite innovative and based on these articles; it was clear what smart home is? How to secure our home, office and personal data? How to help build a smart city? How to contribute in agricultural growth, health and medicine? and much more. The articles are numbered as 16-20].

Simulation and Result

We will now talk about the performance analysis of the suggested method and working in this area of the research activity. Let's now talk about the suggested AIRonHEP (Action Immediate Response on Home Entry Point) scenario and its outcome. The majority of Zigbee-based and Zigbee-based wireless personal area networks developed in earlier work are displayed in a table of comparisons with other approaches. A variety of metrics are available to compare the suggested work to various earlier home automation techniques. Cost, power, energy consumption, and network coverage range are the criteria. These are the real characteristics that are discussed when implementing smart homes and smart cities. due to the fact that both developed and developing nations abound. Fast, effective, affordable, and dependable technology is necessary for both developed and developing nations to raise the standard of life and health of their citizens. Their characteristics were calculated to construct two distinct network-based smart grid-enabled home device control systems. One is based on ZigBee technology, while the other is based on ESP technology. The microcontroller-based relay controlling circuit is depicted in the picture below. It consists of three parts: the relay, the controlling circuit, and the ESP 8266 circuit.

Table 1 Cost of different parts of project

Devices	Quaintly	Prize	Source
ESP 8266	01	4.3USD	www.amazon.in
Relay	02	1.1USD	www.electroncomponents.com
Other small components	R, C, Tri etc.	2USD	www.electroncomponents.com
Total		7.5USD	

Table 2 Cost analysis of ZigBee based wireless sensor

Devices	Quantity	Prize(USD)	Source
ESP 8266	03	4.3	www.amazon.in
DS18B20 T sensor	01	3.9	www.amazon.in
Fire Sensor	01	3.5	www.amazon.in
LPG gas sensor	01	3.0	www.amazon.in
Other	R, C etc	2.0	www.electroncomponents.com
Total		23.3	For temperature sensing in-house

In Figure 7, the circuit is displayed. In the AIRonHEP system. Comparable to it, Table 1 below illustrates the cost of creating a sensing network based on an ESP8266. For this, we need one ESP device, several sensors (CO_2, CO, Smog, microcontroller, register I, capacitor I, and transistors (T) for each sensing node. The temperature (T), fire and LPG gas detecting microcontroller, register I, capacitor I, and transistors (T) are all connected to the WiFi module, which is already included in the ESP module in this personal area network (PAN) based sensing network The PAN-based sensing network's approximate cost is displayed in Table 2. Thus, information can be delivered straight to the server via this method and end up on the Wi-Fi. PAN-based WSN is expected to cost roughly $23.3 USD.

The three sensor parameters—temperature (T), liquid petroleum gas (LPG), and fire—have an overall cost of about $25 USD. The transmitter end of the AIAR, which transmits the sensor data to the server, uses all of these circuits. Let's talk about the price of a ZigBee-based sensing network, which is built on a PAN or WSN network and comprises a sensor, ZigBee, and another little device. An additional ZigBee-based network component that raises the price is the Wi-Fi module. The overall cost study of an ESP-based WSN/PAN and a ZigBee-based wireless sensor network is presented in Tables 2 and 3.

Table 3. ZigBee based WSN network

Devices	Quantity	Prize (USD)	Source
ZigBee	03	54.54	www.amazon.in
DS18B20 T sensor	01	3.9	www.amazon.in
Fire Sensor	01	3.5	www.amazon.in
LPG gas sensor	01	3.0	www.amazon.in
Other	R,C etc	2	www.electroncomponents .com
Total		66.94	For temperature sensing in-house

Subsequently, we will address additional characteristics and analyses that are critical to the successful implementation of any smart sensing network. Following the comparison, Table 4 above displays the final proposal for AIRonHEP (Action Immediate Response on Home Entry Point) using an alternative technique. The open-source ULA software

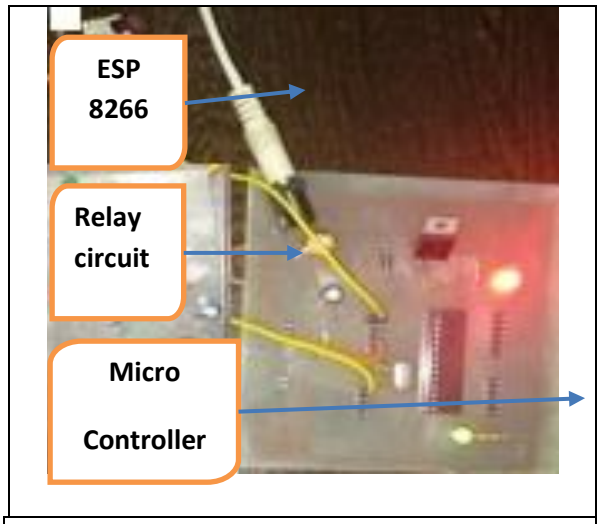

Figure 7 Shows that hardware implementation of proposed system

is used to develop and simulate the suggested design, while Arduino software is used for embedded work. Finally, compare the graphical form outcome for the various parameters displayed in this graph.

Table 7.4. Response time comparison of the proposed system and previously proposed systems

Ref. No.	Technology Used	Used device	Range of W/L device	Response Time
Prop-osed.	AIRonHEP	ESP 8266	Up to 200 m and P2P 5km	Below 10 ms
[21]	Node JS	NodeMCU ESP8266 micro-controller	Up to 200 meter in P2P 2km	Below 13.36 ms
[22]	NodeMCU	NodeMCU	Up to 200m in P2P 2km	11 ms
[23]	Message Queuing Telemetry Transport (MQTT)	ESP 8266 + Wi-Fi	Up to 200m in P2P 2km	Below 15.36 ms
[24]	ESP8266 with ZigBee based WSN	ESP 8266 + Xbee	Up to 100m	Below 15.36 ms
[25]	XMPP with cloud based UHG	Zig Bee	Up to 100 m	Below 15.36 ms
[26]	ZigBee based (SAS) construct for sensible homes.	Zig Bee	Up to 100 m	Below 15.36 ms
[27]	SHEMS based on an IEEE802.15. 4 and ZigBee.	Zig Bee	Up to 100 m	Below 15.36 m.s.

Data rate, cost, band memory count, and other factors are examples of parameters. The response times of the suggested system and earlier suggested systems are contrasted in Table 4. The cost comparison between the previous ZigBee-based architecture shown in Figure 8 below and the proposed works EPS8266-based design is depicted graphically. To carry out this work, the innovative research articles are reports elsewhere [21-27].

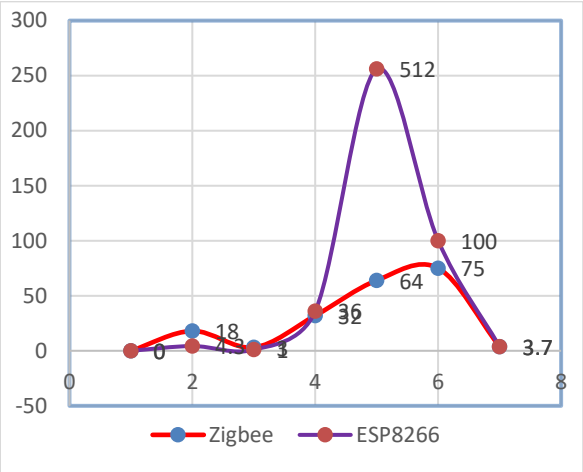

Figure 8: Graphical comparison of ESP and ZigBee

CONCLUSIONS

This article gives the two new proposed gateways, "Action Immediate Response on Home Entry Point (AIRonHEP) Access point" based on multi-user. Both systems discusses on layer architecture level with devices specification. Both method comparisons are Re provided. Also, we have discussed cost-efficient structure of the smart cities and smart industry, all these processes are implemented on the hardware that is shown in simulation and result part. There are different benefits of this robust method. The important part of this proposed method is security and device control – management is not totally dependent on the machine or totally automated. If the system takes any action so first send information to do self if user does not operate after that it will do it on auto mode. In the auto mode threshold values decide by the user self. The major and critical work of any automation cover a large distance, in this proposed work use access point that covers wide area for point to point connectivity up to 20 km and local up to 2 km. In the series ZigBee and other devices were dominating in the last era but a new era is started with proposed system, because of its low cost, long distance, high security. In case of ZigBee based network, most of the Wi-Fi modules extra cost is added plus ZigBee self-high contain highly cost with low memory. The proposed system is designed for higher data storage capacity with sound speed of transmission and receiving for quick response to ON and OFF device, which prevents the accident. The main motive is to fulfill the proposed system that is Security of User Hand, Long range cover, Fast response, easy to move, Reliable and the important things is operating from anywhere in the world.

In future, implementation must be on a single chip using very large scale integration (VLSI). In large scale, very large scale integration (VLSI) reduces the cost, size and power consumption of the system. Also, try to improve the security enhancement of the proposed model using different machine learning approach. This proposed model shows the connectivity worldwide similarly different attacks are also possible like Wormhole, black hole, intrusion detection system (IDS), and others. Try to implement the security in the proposed model.

REFERENCE

[1] Dae-Young Kim 1, Young-Sik Jeong 2 and Seokhoon Kim, Symmetry 2017, 9, 16; doi:10.3390/sym9010016

[2] Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. International conference on smart, monitored and controlled cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017.

[3]Boban Davidović, Aleksandra Labus, FACTA UNIVERSITATIS Series: Electronics and Energetics Vol. 29 (2016), 451 - 460 DOI: 10.2298/FUEE1603451D

[4] Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities. IEEE IoT-J. 2014;1(1):22–32

[5] S. Kumar, P. Tiwari, M. Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, Journal of Big Data, 6 (2019 111).

[6] C. Stolojescu-Crisan, C. Crisan and B. P. Butunoi, An IoT-Based Smart Home Automation System, *Sensors* *21*(11) (2021) 3784

[7] R. K. Kodali, V. Jain, S. Bose, L. Boppana, IoT based smart security and home automation system. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, (2016) 1286–1289

[8] Babovic ZB, Protic V, Milutinovic V. Web performance evaluation for internet of things applications. IEEE Access. 2016;4:6974–92.

[9] Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Comput Netw. 2018;144:17–39

[10] Tzafestad SG. Ethics and law in the internet of things world. Smart Cities. 2018;1(1):98–120

[11] Pereira C, Aguiar A. Towards efcient mobile M2M communications: survey and open challenges. Sensors. 2014;14(10):19582–608.

[12] Temglit N, Chibani A, Djouani K, Nacer MA. A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Syst J. 2018;12(2):1655–66.

[13] Fafoutis X, et al. A residential maintenance-free long-term activity monitoring system for healthcare applications. EURASIP J Wireless Commun Netw. 2016.

[14] Park E, Pobil AP, Kwon SJ. The role of internet of things (IoT) in smart cities: technology roadmap-oriented approaches. Sustainability. 2018;10:1388

[15] Source:https:// www.iotsworldcongress.com/iot-transforming-the-future-of-agriculture/

[16] I. Ali, S. Sabir, Z. Ullah, International Journal of Computer Science and Information Security (IJCSIS), 14 (2016)456-465

[17] S. A. Chaudhry, K. Yahya, F. Al-Turjman and M. -H. Yang, in *IEEE Access*, vol. 8, pp. 139244-139254, 2020,

[18] Source: https:// www.redhat.com/en/topics/security/security-for-iot-devices#overview

[19] A. Garg, T. Lee, Internet of Things, 11 (2020) 100249

[20] M. U. Aftab, A. Oluwasanmi, A. Alharbi, O. Suhaib, Secure and Dynamic Access Control for the Internet of Things (IoT) Based Traffic System, 7(5):e471 (2021)

[21] N.Satheeskanth, S. D. Marasinghe, R. M. L. M. P. Rathnayaka, A. Kunaraj, and J. Joy Mathavan. "IoT-Based Integrated Smart Home Automation System." In Ubiquitous Intelligent Systems, pp. 341-355. Springer, Singapore, 2022.

[22] R. Kishore, U. R. Vigneshwari, N. Prabagarane, K. Savarimuthu, and S. Radha. "IoT Based Intelligent Control System for Smart Building." In 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), pp. 1-6. IEEE, 2020.

[23] L. Xing, C. Qian, W. G. Hatcher, H. Xu, Weixian Liao, and W. Yu. "Secure internet of things (iot)-based smart-world critical infrastructures: Survey, case study and research opportunities." IEEE Access 7 (2019): 79523-79544.

[24] Y. Aimin, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu. "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms." IEEE Internet of Things Journal 7, no. 4 (2019): 2521-2530.

[25] A. Eirini, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap. "A supervised intrusion detection system for smart home IoT devices." IEEE Internet of Things Journal 6, no. 5 (2019): 9042-9053.

[26] L. Weixian, et al. "A novel smart energy theft system (SETS) for IoT-based smart home." IEEE Internet of Things Journal 6.3 (2019): 5531-5539.

[27] S. Radosveta, M. A. Akkaş, and E. Demir. "IoT supported smart home for the elderly." Internet of Things 11 (2020): 100239