IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Analysis of IoT Enabled Architecture in Various Sectors and their Challenges

Kottilingam Kottursamy

Associate Professor, Department of CSE, SRM Institute of Science and Technology, Kattankaluthur, Chennai, India.

E-mail: k.kottilingam@gmail.com

Abstract

Internet of Things (IoT) aims at being the quickest developing technology, with a huge effect on global life and manufacturing environment. The current mode of communication is either between humans or human and device; however, the concept IoT promises a bright future for the online platform where the mode of communication is machine-machine (M2M). Everything will be automated and smart, with a single tap. An effort has been made in this study to explore the key technologies, new innovative applications of IoT, as well as a comprehensive comparative literature survey. The survey helps in getting better knowledge on various real time applications and its impacts on the daily routine of human lives. The IoT tends to take numerous considerations from the commercial world and research community as a key advancement in the upcoming age of the Internet.

Keywords: Internet of Things, M2M, RFID, WSN, IoT applications

1. Introduction

Internet of Things (IoT) steps the concept that has the potential to drastically alter our future world. The Internet of Things has expanded into multiple functions and contexts, showcasing that everything can be identified, connected, and used for exchanging data and decision-making [1]. IoT is rapidly developing and is a popular research area with endless opportunities. The Internet of Things focuses on improving people's lifestyle.Retail Site Intellectual ability, a Krogan-based online marketplace, is an extensive commerce platform for computer vision, wireless things, computerised devices, portable sensors, IP cameras, and video handling events designed to assist customers in improving their shopping experience[2]. According to the study, the overall number of internet-connected objects is expected to be 75.44 billion [3]. IoT seems to be a computer processing trend in the

DOI: https://doi.org/10.36548/jsws.2022.1.004
Received: 13.04.2022, received in revised form: 07.05.2022, accepted: 20.05.2022, published: 30.05.2022

development of daily physical objects being connected to the web and able to recognise other devices.

2. Architecture of IoT

The architecture can be defined as a framework, the physical components, the network's functional entity and design, work requirements, and data structures which will be used. IoT architecture can differ significantly depending on integration; it must be accessible with open protocols to support multicast applications. Any IoT based services the below four are the important layer that is mainly implement for the best of its application-oriented supports. The following is the used four layers of IoT:

- Layer 1-Perception-sensors and accumulators
- Layer2-Network layer-Routers and Gateway
- Layer3-application layer-Severs and cloud

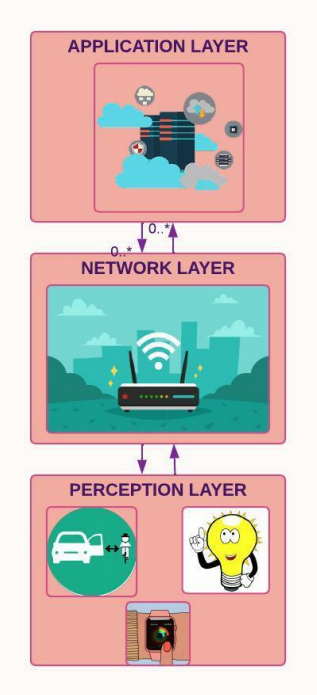

Figure 1. Three important layer in architecture of IoT

2.1 Sensors and accumulators

This is the architecture's physical layer. It is recognised by the wide range of digital devices which gathers and seek information for the process. This layer contains sensors accumulators and edge devices. IoT devices collect massive amounts of data regarding their

surroundings—weather, traffic conditions, human nature, and other factors—all of which make a significant contribution to the exactness of this technology's analysis capabilities. The mainly used sensors in IoT are temperature, solar, humidity, pressure, chemical, biomedical, proximity, gyroscope, cameras and optical sensor, gas and air sensor and Accelerometers.

Sensors detect physical parameters and repurpose them into usable information. A three-axis accelerometer is one of the mostly used sensor in smart watches used to count the moves. For more accurate results, some phone/watch models include motion sensors (gyroscopes) in relation to an accelerometer.

2.2 Network layer-Routers and Gateway

The sensors help in providing data in analogue format. They must be transferred to a computer format before they can be further processed. Data Acquisition Systems (DAS) handles these conversions and aggregation of data for you. It plays the the role of the network layer. It links these smart objects to other intelligent devices, cloud services, and network equipment. It is also in responsible of data transfer.

Information from the sensors is in the form of digital data do the needful pre-processing and the transfers the pre-processed data to the data centres.

IoT Gateways are crucial intermediaries that act as messengers and translators between both the cloud and agglomerations of smart devices. They are physical components or computer programs that usually run from the field, near the edge sensing devices. To serve a large number of edge nodes, large IoT systems may utilise a plethora of gateways. They can provide a variety of services, but their primary function is to normalise, connect, and transmit files between the physical hardware level and the cloud. In fact, all data that travels in between cloud and the hardware layer passes through a gateway. Intelligent gateways or control tiers are other names for IoT gateways[4].

2.3 Application layer-Severs and cloud

Data Computation and storage with user-specific services and functionality are carried out in this layer. In IoT architecture data systems is a key phase because the data must be saved for further depth analysis. It also facilitates in follow-up revision for feedback. In IoT implementations, cloud computing is the desired storage method. The data gathered could be physically located or in the cloud platform [4]. This stage involves more powerful data analysis and storage. In these cloud services, data that requires further processing is

thoroughly analysed. Because there is a serious study taking place, it takes more time than the analysis that occurred earlier stages.

3. Key Concepts of IoT

The key concepts related to IoT are shown in the figure 2.where the digital devices and sensor analyse and interpreted the extract information to allow intelligent services. In this section, the two major technologies that lay their impact on the IoT services and applications have been summarised [5-7].

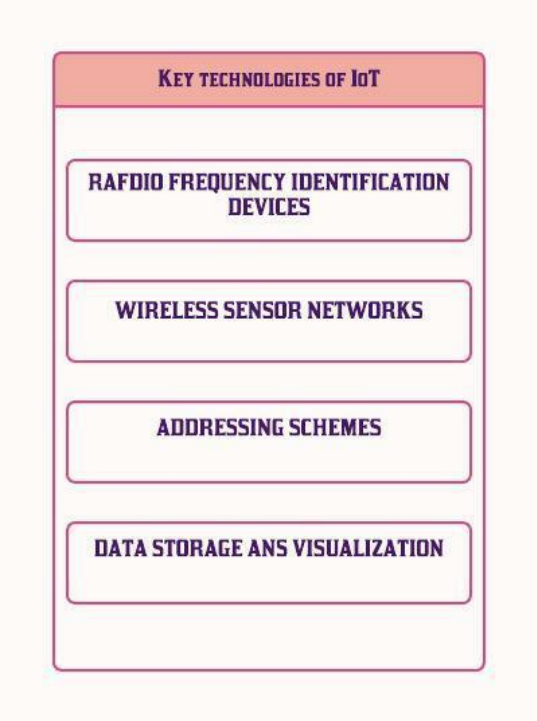

Figure 2. Key Technologies of IoT

3.1 RFID (Radio Frequency Identification Devices)

RFID technology, is one of the most promising technologies of the IoT, plays a critical role in its innovation. Because of its small size and low cost, it can be embedded with any object [5]. It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application [6] There are several other international standards, the most influential of which are the EPC Global standards, the ISO / IEC standards, which support every super group, and the UID standard, which is supported by SONY, NEC, and other domestic companies of 992 Japanese [7]. Furthermore, an RFID can be used as an actuator to trigger multiple events, and it has modification functionalities that bar codes do not.

3.2 Wireless Sensor Network (WSN)

Actuators and sensors play critical roles in IoT. Sensors and actuators allow IoT devices to communicate with the material world. Smart agriculture, smart home, smart cities and many other IoT applications are technically intelligent systems that help to connect in an automated way of reducing human effort. The overall goal of such system applications is to foster the concept of IoT, which is accomplished through the use of intelligent sensors. The entire Sensor Node is tightly coupled, either directly or indirectly, with the communication network (Internet), where tracking, governance, and data processing smart can be accomplished by utilising interconnected cloud computing devices.

A WSN is made up of several Sensor Nodes that monitor their surroundings using various tiny sensors and provide output results in the form of electromagnetic waves that are sent to the control system for further processing. When the sensor nodes are on same network, they communicate together via radio signals[6]. When sensor networks want to send data to the cloud or interact with sensor nodes on different networks, a Gateway is required because these devices lack a TCP/IP stack. The Gateway functions as a bridge, converting protocols and transmitting data to the system or to various devices.

4. IoT applications

Real - world applications seen nowadays are already smart, that they're unable to share information with one another. Facilitating them to converse with one another and share useful information will lead to a wide variety of innovative applications. This approach is based refers to a network of multiple devices that can gather data in order to derive meaningful knowledge from big data. In the modern world, there are numerous IoT applications that are as varied as you can't imagine.

IoT puts its hand on a wide range of applications, from agriculture in managing the devices, results increases the productivity of food products creates a smart farm, connecting all of your home's devices to design a perfect home to connecting all of a city's govt and civic services to develop smart city and the elevation of IoT goes on .It move and operates the universe in a single click, right from the home to the rocket space station.

There are a wide variety of IoT application that makes it a smart and intelligent system as seen in figure 3.

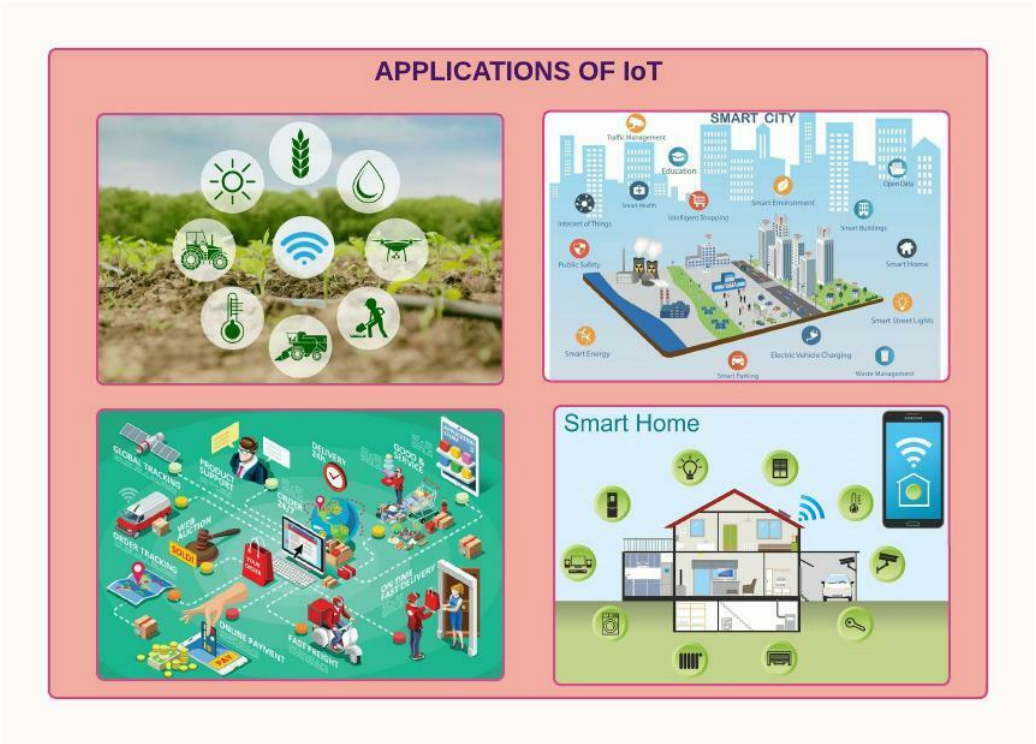

Figure 4. Applications of IoT

In this section, few major applications of IoT are discussed:

4.1 Smart Agriculture

The use of IoT in agriculture entails providing farmers with decision-making tools and autonomous systems that incorporate products, knowledge, and services for productivity improvements, reliability, and revenue. Recent surveys on IoT in agriculture also highlight the challenges and restrictions for large-scale pilots across the entire agri - food supply chain [8].

The deployment of sensor nodes deep within the soil can help farmers plan the period and time of year when to plant the seeds, hold the increasing seedlings healthy by keeping it independent of diseases by using the right quality of pesticides, and adequate timely delivery of groundwater that increases the productivity of crops and farmers can gain high profit from the production.

4.2 Smart Home

Smart homes are an evolving field that will provide remote connection for controlling home appliances via IoT [9].

Smart Homes have become the innovative success in the interior homes, and it is estimated that Smart Homes will be as popular as smart phones. Discussing on Iot applications, the most efficient and useful that comes to mind is Smart Home, which ranks as the highest IOT application across all channels. It puts its part in saving power from unwanted wastage of current that in return helps the house owner in electricity saving. It manages the devices in the home right from the lights ,air conditioners ,bathrooms heaters and pipes, kitchen equipment's, Televisions, Home automation and security system and so on using the sensors and cameras. Furthermore, members can influence household appliances via an Android platform on their mobile phone, reducing individual effort.

4.3 Smart Cites

Throughout its variety of applications in sectors such as engineering, medical services, commercial, agribusiness, transportation, and home automation, IoT is involved in the development of the entire city. Aside from that, smart cities employ IoT technology to manage major city pollution problems, crime, traffic congestion, effluents, parking, and environmental concerns. [10]Data from embedded sensors, metres, and other measuring devices are collected, surveyed, analysed, and networked via the central cloud platform. The primary benefit of smart cities is to conserve energy optimise mineral wealth, make cities safe and secure, and achieve a healthy environment.

5. Related Study

Table 1. Work related to the wide range of IoT applications

Reference	Applications	IoT challenges and inferences
[11]	Healthcare, Industrial IoT, Home Automation, Smart Cities, Emergency Care, Smart Agriculture	Architectures, Reliability, Interoperability, Self-Diagnosis & Adaptability
[12]	Smart meter, smart retails ,smart city	Access of data, connectivity, time saving, Expenditure effect.
[13]	Intelligent Transportation System, Public Safety, Smart Grids, Industry 4.0, Smart Homes	Security, Fog Computing

[14]	Smart home,IoT on agriculture-healthcare, Physically Challenged Persons, E-HealthCare /E-Medical Care	Routing of the messages using the MQTT(Message Queuing Telemetry Transport) and COAP(Constrained Application Protocol)
[15]	Health care, smart city, smart home, connected cars, smart retails, smart farming	Security challenges like data integrity, encryption capabilities, privacy issues
[16]	Monitoring health conditions, E-Health care	Microsoft Kinect sensors
[17]	Home automation system	Reduce power consumption
[18]	Industry, Environment and society	Power efficiency and time synchronisation
[19]	Smart kitchen	Access the kitchen equipment's through mobile
[20]	Smart Homes, Smart Health, Smart Transportation, Retail, Industry 4.0, Smart Agriculture	Security

6. Challenges and future work

Data Integrity: Gadgets are part of an interconnected ecosystem that is linked by IoT. Modification of even an individual data point results in deception of the original dataset that is exchanged and shared between the sensor and the main server. To ensure integrity, a decentralised record and digital signatures should be implemented.

Connectivity: To ensure the survival of connected devices, the current centralised Server-Client model will be replaced by a decentralised Peer-to-Peer model. Furthermore, mobile network fog computing models would bring their functionalities to the edge.

Sensor-Nodes Security Breach: By interfering with the frequencies of sensor nodes, interference obstructs the entire network. Tampering is a type of attack where the attacker extracts or modifies the node data in order to create a controllable node. The Sybil attack

makes the claim multiple completely anonymous identities for anode, giving it significant clout. Flooding is a type of DOS attack resulting from excessive traffic that causes memory exhaustion.

Energy resource: Every device on the planet requires energy to function and craves it. Faced with the truth, IoT systems must perform a variety of tasks that require a significant amount of energy. They are fallible enough that current technology cannot support a lifetimes that meets our expectations.

At each layer, the IoT gateway is susceptible to attack. As a result there are various security attacks and requirements that must be addressed. The current state of IoT research is primarily focused on authentication and authorization working program, but with the rapid advancement of technology the main challenge is going to maintain the security and connectivity issues related to the IoT oriented real time applications.

7. Conclusion

IoT is a technique that keeps on simplifying lifestyle. Having said that, many new technologies also have been disastrous; however, in the current situation, it is necessary to live a classic style of life equipped with various modern technologies. Many connected devices become easy targets due to inadequate security mechanisms, as well as the negligence of the victim that they have been infected. This survey paper deals with the terminologies related to IoT, its applications, its related security attacks and challenges. The future scope is to design and build a resource i.e., coherent, and protect reprogrammable edge base station for IoT applications, and improve the smart lifestyle.

References

[1] L. Tan, N. Wang. “Future Internet: The Internet of Things”, 3 rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE Xplore, vol 5, Sept 2010, DOI: 10.1109/ICACTE.2010.5579543.

[2] K.Bonsor-and-C.Keener,-“HowStuffWorks "How RFID Works"” 2010,

[3] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The effect of IoT New Neatures on Security and Privacy: New Threats, Existing Solutions, and Challenges yet to be Solved,” IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, 2019.

[4] What is an IoT Gateway? - Definition from TechTarget.com

[5] Wang Chen, ”AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS,” in Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1046, 1049

[6] L.Atzori, A.Iera, G. Morabito,”The Internet of Things: A survey,” in Computer Networks - Science Di

[7] Complete RFID Analysis and Forecasts, 2008-2018, www.idtechex.com/researchreports/

[8] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, “IoT in agriculture: Designing a Europe-wide large-scale pilot,” IEEE Communications Magazine, vol. 55, no. 9, pp. 26–33, 201

[9] 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, 2018, pp. 325-327.

[10] Introduction To IoT in Smart City - Qmansys Infosolutions

[11] Mostafa Haghi Kashani a , Mona Madanipour b , Mohammad Nikravan a , Parvaneh Asghari c , Ebrahim Mahdipour b, “A systematic review of IoT in healthcare: Applications, techniques, and trends”, 2021, Journal of Network and Computer Applications, Volume 192, 15 October 2021, 103164.

[12] Abhishek Malik, Amrit Thapa Magar, Harsh Verma, Meeta Singh, Pinki Sagar ,” A Detailed Study Of An Internet Of Things (Iot)” INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 12, DECEMBER 2019

[13] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A Survey of Internet of Things (IoT) Authentication Schemes,” Sensors, vol. 19, no. 5, p. 1141, Mar. 2019

[14] Mohit Kumar Saini, Rakesh Kumar Saini,” Internet of Things (IoT) Applications and Security Challenges: A Review” International Journal of Engineering Research & Technology (IJERT), NCRIETS – 2019 Conference Proceedings, Special Issue – 2019

[15] Luma Carolina Gradim, Marcelo Archanjo José, Daniel Marinho Cezar da Cruz and Roseli de Deus Lopes” IoT services and applications in rehabilitation: an interdisciplinary and meta-analysis review” DOI 10.1109/TNSRE.2020.3005616, IEEE.

[16] 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, 2015, pp. 101-104

[17] Antar Shaddad Abdul-Qawy*, Pramod P. J**, E. Magesh**, T. Srinivasulu*" The Internet of Things (IoT): An Overview", Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 5, Issue 12, (Part - 2) December 2015, pp.71-82

[18] Rajeev Piyare and Seong Ro Lee "Smart Home Control and monitoring System using Smart phones" Department of Information Electronics Engineering, Mokpo National University Mokpo 534-729, South Korea

[19] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," Comput. Networks, vol. 151, pp. 147–157, Mar. 2019.

Author's biography

Kottilingam Kottursamy is currently working as an associate professor in the Department of CSE, SRM Institute of Science and Technology, Kattankaluthur, Chennai, India. His area of research includes bio statistics, machine learning algorithms, database tuning, high speed networks, information sciences & analytics.