WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Analysis of Enabling Technologies for the Internet of Things

#1Mr. Swapnil N. Naikwadi, #2Mr. Siddharth Lokhande, #3Dr. Bhaskar V. Patil, #4Dr. Pralhad K. Mudalkar

#1, #2Student, MCA, Bharati Vidyapeeth (Deemed to be University), Institute of Management, Kolhapur
#3Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management, Kolhapur
#4*Associate* Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management, Kolhapur

DOI: https://doi.org/10.55248/gengpi.2022.31222

Abstract –

An overview of the Internet of Things (IoT) is given in this paper, with a focus on supporting technology, protocols, and application-specific challenges. The most recent advancements in RFID, smart sensors, communication technologies, and Internet protocols enable the Internet of Things. The fundamental idea is to create a new class of applications by having smart sensors work together directly without human intervention. The present Internet, mobile, and machine-to-machine (M2M) technology boom can be viewed as the beginning of the Internet of Things. The Internet of Things (IoT) is anticipated to connect physical things to enhance intelligent decision-making in the next years, bridging various technologies to open up new applications. This article begins by giving a broad overview of the IoT. Then, we provide a high-level review of a few technical aspects relating to the IoT enabling technologies, protocols, and applications. Our goal is to provide a more thorough summary of the most important protocols and application issues compared to other survey papers in the field so that researchers and application developers can quickly understand how the various protocols work together to deliver desired functionalities without having to read through RFCs and the standards specifications. We also give a brief review of some of the most important IoT challenges that have been discussed recently in the literature and a description of related research. We also investigate the connections between the IoT and other cutting-edge technologies, such as big data analytics, cloud computing, and fog computing. We also discuss how IoT services need to be more horizontally integrated. To show how the various protocols discussed in the paperwork together to deliver desired IoT services, we then present thorough service use-cases.

Keyword: Internet of Things (IoT), CoAP, MQTT, AMQP, XMPP, DDS, mDNS, and IoT gateway are some related terms.

I. Introduction

The concept of the Internet of Things is being realised as an INCREASING number of physical objects are being connected to the Internet at an unprecedented rate (IoT). Thermostats and HVAC (Heating, Ventilation, and Air Conditioning) monitoring and control systems, which enable smart houses, are a simple example of such items. There are further fields and settings where the IoT can make a significant impact and elevate our quality of life. Transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters when human decision-making is challenging are some of these uses. By allowing physical things to "speak" to one another, share information, and coordinate actions, the IoT makes it possible for them to see, hear, think, and carry out tasks. By utilising its underlying technologies, such as ubiquitous and pervasive computing, embedded devices, communication technologies, sensor networks, Internet protocols, and applications, the IoT changes these items from being conventional to intelligent. While ubiquitous computing and analytical services make up application domain agnostic services, smart objects and their purported duties make up domain specific applications (vertical markets) (horizontal markets). depicts the general IoT concept, in which every domain-specific application interacts with services that are independent of any particular domain, but inside each domain sensors and actuators speak directly to one another. It is anticipated that the IoT will eventually have significant uses for homes and businesses, improve quality of life, and expand the global economy. For instance, smart houses will give their occupants the ability to automatically open their garage when they arrive home, make coffee, and operate TVs, air conditioning systems, and other appliances. To realise this potential expansion, new ideas, technology, and services are needed.

The following might be used to summarise the contributions of this study in light of recent publications in the area:

- This survey provides a more thorough summary of the most important IETF, IEEE, and EPC global protocols and standards than other survey papers in the field, allowing researchers to catch up quickly without having to sift through the specifications for the standards and RFCs or the RFCs' detailed descriptions.
- We provide a synopsis of related research projects as well as an outline of some of the major IoT concerns that have been discussed in recent literature. We also investigate the connections between the IoT and other cutting-edge technologies, such as big data analytics, cloud computing, and fog computing.

- We argue that more horizontal integration between IoT services is necessary.
- In order to show how the various protocols discussed in the paperwork together to deliver desired IoT services, we also provide thorough service use-case examples.

II. Market Potential

For companies that produce equipment, provide Internet services, and create applications, the IoT presents a huge market opportunity. By the end of 2020, there will likely be 212 billion IoT smart object deployments worldwide. M2M traffic flows are anticipated to make up up to 45% of all Internet traffic by 2022. Beyond these forecasts, the McKinsey Global Institute found that there had been 300% more connected equipment (units) over the previous five years. A cellular network in the US that tracks traffic indicated a 250% rise in M2M traffic volume in 2011. IoT-based services have experienced significant economic growth for corporations as well. Applications in healthcare and manufacturing are anticipated to have a significant economic impact. By 2025, it is anticipated that the global economy will grow by $1.1 to $2.5 trillion annually thanks to healthcare applications and related IoT-based services like mobile health (m-Health) and telecare that make it possible to deliver medical wellness, prevention, diagnosis, treatment, and monitoring services effectively through electronic media. By 2025, the IoT is expected to have a total yearly economic impact of between $2.7 trillion and $6.2 trillion. The anticipated market share of the most popular IoT applications. However, Wikibon estimates that by 2020, the value generated by the industrial Internet will be over $1279 billion, with a Return on Investment (ROI) that will have increased to 149% from 13% in 2012. Additionally, according to a recent analysis from Navigant, the market for Building Automation Systems (BAS) is anticipated to grow by 60% between 2013 and 2021, from $58.1 billion to $100.8 billion. However, all of these figures suggest that the IoT and its associated businesses and services will grow in the near future at a potentially considerable and rapid rate. Manufacturers of conventional appliances and equipment have a rare chance thanks to this development to turn their goods into "smart objects." Internet service providers (ISPs) must configure their networks to provide quality of service (QoS) for a variety of M2M, person-to-machine (P2M), and person-to-person (P2P) traffic flows in order to scale the Internet of Things and related services internationally.

III. Architecture for IoT

A flexible layered architecture is essential for the IoT since it should be able to link billions or trillions of diverse things to the Internet. A reference model has not yet been reached among the ever-growing variety of potential architectures. In the meantime, initiatives like IoT-A attempt to provide a standard architecture by analysing the requirements of both researchers and business. The fundamental model is a 3-layer architecture made up of the Application, Network, and Perception Layers, chosen from the pool of possible models. However, additional models that offer more abstraction to the IoT architecture have been suggested in recent research. The 5-layer model, which has been used in but should not be confused with the TCP/IP layers, is one of the popular structures shown in Fig. 3. We then give a brief overview of these five tiers.

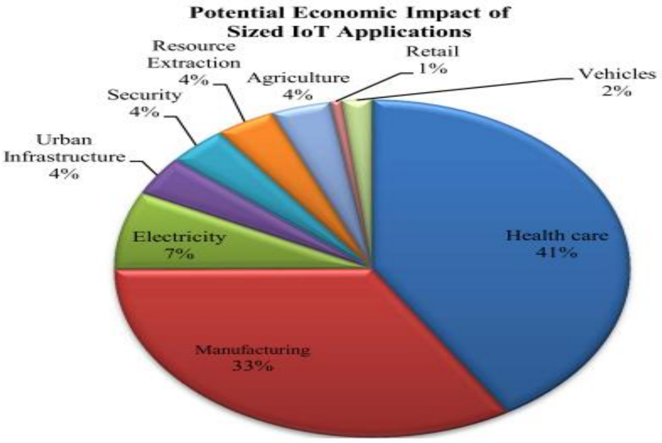
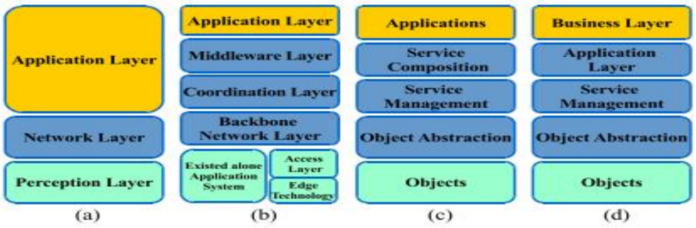


Fig. 2. Projected market share of dominant IoT applications by 2025.



(a) (b) (c) (d)

A. Objects Layer, first The IoT's physical sensors that seek to gather and interpret data are represented by the first layer, the Objects (devices) or Perception layer. This layer consists of sensors and actuators that can be used for a variety of functions, including asking about position, temperature, weight, motion, vibration, acceleration, and humidity, among others. The perception layer has to configure heterogeneous objects using standardised plug-and-play procedures. Through secure channels, the perception layer digitises and sends data to the object abstraction layer. At this layer, the IoT starts to generate large data.

B. Object Abstraction Layer: Using secure channels, Object Abstraction sends data generated by the Objects layer to the Service Management layer. Different technologies, including RFID, 3G, GSM, UMTS, WiFi, Bluetooth Low Energy, infrared, ZigBee, etc., can be used to convey data. Additionally, this layer handles other tasks including cloud computing and data management procedures.

C. Service Management Layer - Based on addresses and names, the Service Management or Middleware (pairing) layer matches a service with its requester. This layer makes it possible for IoT application developers to operate with a variety of objects without considering a particular hardware platform. Additionally, this layer manages data received, makes choices, and provides the necessary services via network wire protocols.

D. Application Layer - This layer offers the services that clients have requested. For instance, if a consumer requests information on temperature and air humidity, the application layer can supply such information. The capacity to offer top-notch smart services to satisfy customers' expectations makes this layer crucial for the IoT. Numerous vertical markets, including smart homes, smart buildings, transportation, industrial automation, and smart healthcare, are covered by the application layer.

E. Business Layer - The business (management) layer oversees all operations and services provided by an IoT system. This layer's duties include creating business models, graphs, flowcharts, etc. using data obtained from the Application layer. Additionally, it is expected to design, analyse, implement, assess, monitor, and create components connected to IoT systems. Big Data analysis-based decision-making processes can be supported thanks to the Business Layer. At this layer, it is also possible to monitor and manage the four lower layers. Additionally, in order to improve services and protect users' privacy, this layer contrasts each layer's output with what was anticipated.

IV. The Current Issues And Their Challenges

The IoT comprises of a variety of additional components that can either be referred to as "specific difficulties" or as an extension of the IoT's general challenges. The section aims to provide a concise explanation of some of these components.

4.1 Identification through radio frequency (RFID)

RFID is a breakthrough in embedded communication and WSN; in WSN, RFID is utilised to produce an object's unique ID. It is composed of two components: access control and passive RFID, which uses the reader's interrogation signal to transmit the ID to the RFID. application as well, International Journal of Computer Applications (0975 - 8887) Volume 128 - No. 1, October 2015 43 RFID readers that are active have their own power sources and initiate communication. In a particular IoT application field, RFID leverages Ultrawide Bandwidth (UWB) technology to improve RFID performance. With the use of UWB technology, the next generation of RFID will be able to overcome many of its current limitations, including its low security, small coverage area, and sensitivity to interferences. The three main components of RFID are the object-carrying RFID tag or transponder, the reader or transceivers that read and write tags, and the back-end database.

4.2 Wireless Sensor Networks (WSN)

WSN is a crucial component of the Internet of Things and is regarded as the building block of the IoT. It is made up of a collection of specialised sensors that share data about events or states of items like temperature, sound, and pressure among themselves and with communication infrastructure. These sensor nodes operate independently and can be connected to one another through self-organization. It should be noted that WSN support the idea of distribution between sensor nodes, and each sensor network includes a few components like a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interacting with the sensors, and an energy source.

The section aims to demonstrate the elements of WSN in the following ways:

- The sensor interface, processor units, transceiver units, and power supply make up the WSN hardware. For most applications, the nodes in a WSN communication stack are deployed ad hoc. WSN middleware provides a way to link cyber infrastructure with service-oriented design (SOA). With the aid of loosely linked and interoperable services, applications can be composed utilising the SOA architectural design.
- Secure data aggregation is crucial for ensuring accurate sensor data collection.
- Protocols for communication and addressing
- It is thought that one of the key goals of the addressing procedure is to locate the numerous objects on the Internet in order to carry out the communication process effectively. The Internet Protocol (IP), which has two different versions, is typically used to identify items over the Internet.

When identifying hosts or other Internet-connected objects using IPv4, which employs 32-bit addresses (addresses), this technique is thought to be somewhat constrained; and

The most recent IPv6 protocol, which employs 128-bit (addresses), has a larger coverage area than IPv4. In order to identify items in WSN and IoT, RFID technology generates unique IDs that can be used to identify smart objects. "IPv6 over Low-power Wireless Personal Area Network (6LoWPAN)" is another option. The IEFT group wants to make IPv6 work with low-capacity hardware.

V. Applications

IoT technology has recently emerged as one of the fundamentals in our lives because it touches many key areas like healthcare, smart water, transportation, surveillance, and so on. Additionally, a wide variety of apps have developed to support this idea. According to the four categories into which IoT applications can be grouped are as follows:

Wi-Fi serves as the backbone for personal and domestic networks, enabling higher bandwidth data transfer and sample rates. The healthcare industry is the most well-known example of this category.

Enterprise, the data in this category may be gathered from networks; the first popular example of this category is environment monitoring, such as video surveillance; this is followed by smart homes and the smart environment in general.

When using a mobile device, a large-scale WSN can be used to acquire sensor data for online travel time tracking; transportation is a common example of this category.

Networks can provide utilities with information to optimise services and power use. The primary goals of businesses employing this kind of apps are typically profit maximisation and cost reduction. The smart grid, smart metres, smart water, and drinking water quality are the best examples of this type. The most well-known examples of each of the aforementioned categories will be discussed in this section. Table 5 also provides a summary of the different types of IoT applications.

VI. Conclusions and Future Directions

IoT is one of the primary methods for expressing the concept of ubiquitous computing, but it is still not as well-known as cloud computing. Through its three sections, this essay aimed to highlight the Internet of Things (IoT) concept in general. Section I provided an overview of the IoT concept by highlighting its history and introduction in 1999 by Kevin Ashton, who is regarded as one of the IoT's early pioneers and currently works for Cisco. The primary concept for designing the IoT structure that depends on the fusion of three dimensions—information items, independent networks, and intelligent applications—was then examined. As a result, integration between the actual or physical world, the digital world, and the social world is essential for the IoT structure's future. Last but not least, this section highlights the distinctions between the traditional network and the Internet of Things.

Acknowledgement

The authors, writers, and editors of the books and articles that were cited in order to create the study paper that is being presented are all thanked by the researchers. Researchers have a responsibility to keep in mind their parents, whose blessings are always with them.

VII. References

[1InternetofThings,2014 Publications.aspx?parent=SPOLIR.IT2005&me dia=paper at http://www.itu.int/en/publications/gs/pages/publications.aspx

[2] Internet of Things, 2015, available at http://www.rfidjournal.com/article s/view?4986.

[3] Mohammad M. R. Chowdhury, Josef Noll, and Sarfraz Alam, "2010 SenaaS:An Event-driven Sensor Virtualization Approach for Internet of Things Cloud," Networked Embedded Systems for Enterprise Applications (NESEA), 2010 IEEE International Conference on, 1-6.

[4] Context-aware Addressing in the Internet of Things Using Bloom Filters by Andras Kalmar, Rolland Vida, and MarkoszMaliosz, Cog l nfoCom, 2013. (Dec. 2013) 487–492; 4th IEEE International Conference on Cognitive I noncommon Cations.

[5] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and MarimuthuPalaniswami, 2013. Computer Systems of the Future, 1645–1660.

[6] Yingyi Chen and Daoliang Li, Computer and Computing Technologies in Agriculture, October 2010. 24-31 in Springer.

[7] The Internet of Things: Survey. Computer networks, 2787–2805. L. Atzori, A. lera, and G. Morabito. 2014 Internet of Things http://postscapes.com/internetof-things-history.