WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Internet of Things: Introduction, Communication Models, Technologies, Applications and Open Issues

Thanh-Phuoc Nguyen[1], Giao N. Pham[2], Binh A. Nguyen[3], Ngoc T. Le[3], and Trong-Hai Nguyen[4*]

[1]Dept. of Mechatronics, Cao Thang Technical College, Ho Chi Minh City 700000, Vietnam
[2]Dept. of Computing Fundamentals, FPT University, Hanoi, Vietnam
[3]ICT Department, FPT University, Hanoi, Vietnam
[4]HUTECH Institute of Engineering, HUTECH University, Ho Chi Minh City, Vietnam
E-mail: nguyenthanhphuoc@caothang.edu.vn, giaopn@fe.edu.vn, binhnase04865@fpt.edu.vn, ngoclthe131028@fpt.edu.vn, nt.hai75@hutech.edu.vn
(*Corresponding Author)

ABSTRACT

In this paper, we would like to present an overview about Internet of Things (IoT) with aspects: Communication Models, Technologies, Application and Open Issues. For each topic, we will discuss in each section. We hope that this paper will give an overview related issues in IoT.

Keywords: Internet of Things; Deep Learning; Smart City; Digital Twin; and Machine Learning

1.Introduction

The term "Internet of Things" (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) tags [1] used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items. Figure 1 shows visions of IoT and Figure 2 shows the architecture of IoT.

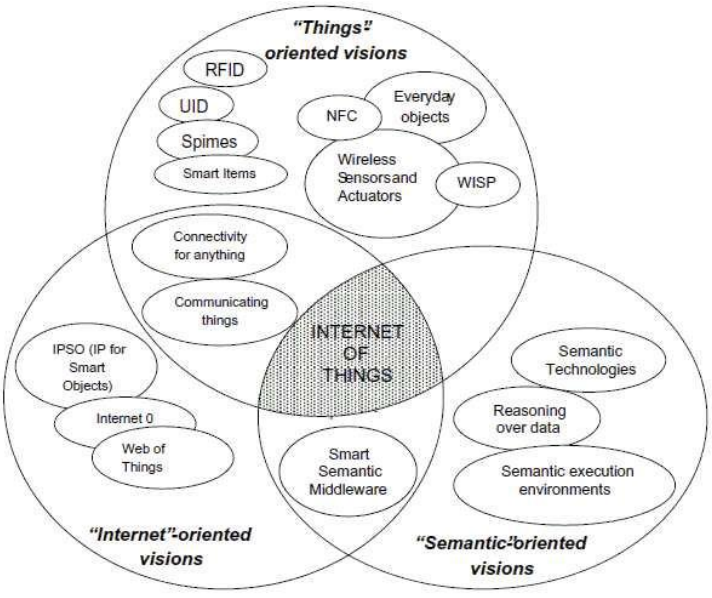

Figure 1. Convergence of different visions of IoT.

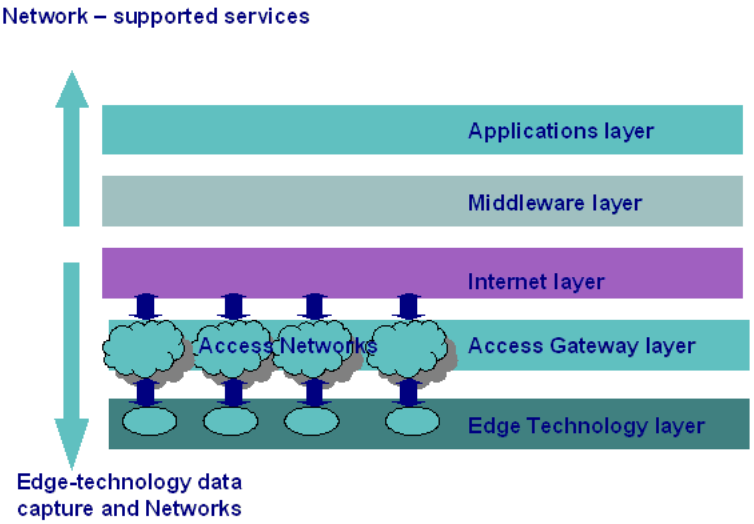

Figure 2. Layered architecture of Internet of Things.

The middleware (a software layer interposed between the technological and application levels) architectures proposed in the last couple of years for IoToften follow the service oriented architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of ecosystem of simpler and well-defined components. The use of common interfaces and standard protocols gives a horizontal view of an enterprise system. Therefore, the development of business process of designing workflows of coordinated services, which eventually are associated with objects actions. An SOA approach also allows for software and hardwarereuse, because it does not impose a specific technology for service implementation. Figure 3 presents a generic SOA-based architecture for the IoT middle-ware.

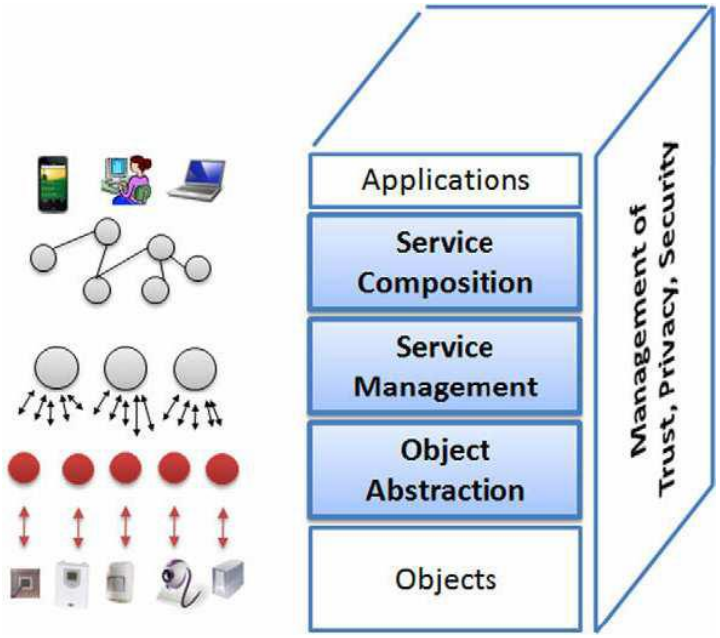

Figure 3. A generic SOA-based architecture for the IoT middle-ware

While the term “Internet of Things” is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use [2]. In the1990s, advances in wireless technology allowed “machinetomachine” (M2M) enterprise and industrialsolutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purposebuilt networks and proprietary or industry specific standards [3] rather than on Internet Protocol (IP)based networks and Internet standards.

Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet “device”an IPenabled toaster that could be turned on and off over the Internet was featured at an Internet conference in 1990 [4]. Over the next several years, other “things” were IPenabled, including a sodamachine [5] at Carnegie Mellon University in the US and a coffee pot [6] in the Trojan Room at the University ofCambridge in the UK (which

remained Internet–connected until 2001). From these whimsical beginnings, arobust field of research and development into "smart object networking" [7] helped create the foundation fortoday's Internet of Things.

From a broad perspective, the confluence of several technology and market trends [8] is making it possible to interconnect more and smaller devices cheaply and easily:

- ✓ *Ubiquitous Connectivity*: Lowcost, highspeed, pervasive network connectivity, especially throughlicensed and unlicensed wireless services and technology, makes almost everything "connectable''.
- ✓ *Widespread adoption of IP–based networking*: IP has become the dominant global standard fornetworking, providing a well–defined and widely implemented platform of software and tools that canbe incorporated into a broad range of devices easily and inexpensively.
- ✓ *Computing Economics*: Driven by industry investment in research, development, andmanufacturing, Moore's law continues to deliver greater computing power at lower price points andlower power consumption
- ✓ *Miniaturization*: Manufacturing advances allow cutting-edge computing and communicationstechnology to be incorporated into very small objects. Coupled with greater computing economics,this has fueled the advancement of small and inexpensive sensor devices, which drive many IoTapplications.
- ✓ *Advances in Data Analytics:* New algorithms and rapid increases in computing power, data storage,and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; theselarge and dynamic datasets provide new opportunities for extracting information and knowledge.
- ✓ *Rise of Cloud Computing:* Cloud computing, which leverages remote, networked computingresources to process, manage, and store data, allows small and distributed devices to interact withpowerful back-end analytic and control capabilities.

From this perspective, the IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectorsincluding automotive, healthcare, manufacturing, home and consumer electronics, and well beyond are considering the potential for incorporating IoT technology into their products, services, and operations.

2.Internet of Things: Communication Models

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452), [9] which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework.

2.1 Device to device communication

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth, Z-Wave or ZigBee to establish direct device to device communications, as shown in Figure 4.

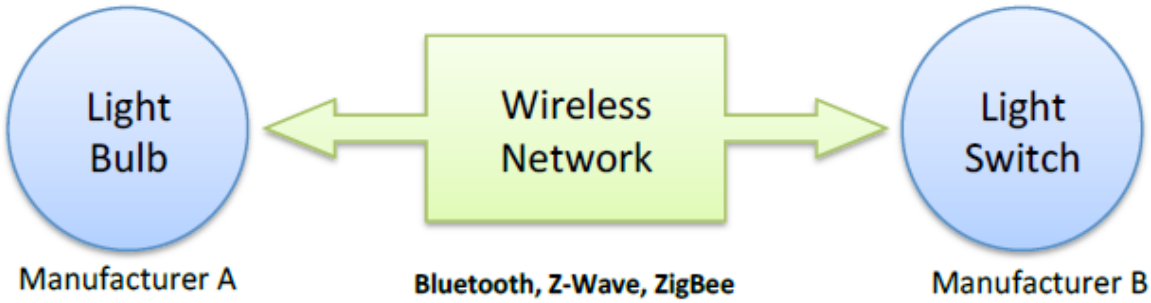

Figure 4. Example of device to device communication model.

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information tocommunicate between devices with relatively low data rate requirements. Residential IoT devices like lightbulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario.

From the user's point of view, this often means that underlying "devicetodevice" communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol. For example, the family of devices using the Z-Wave protocol is not natively compatible with the ZigBee family ofdevices. While these incompatibilities limit user choice to devices within a particular protocol family, the userbenefits from knowing that products within a particular family tend to communicate well.

2.2 Device to cloud communication

In a "device tocloud" communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 5.

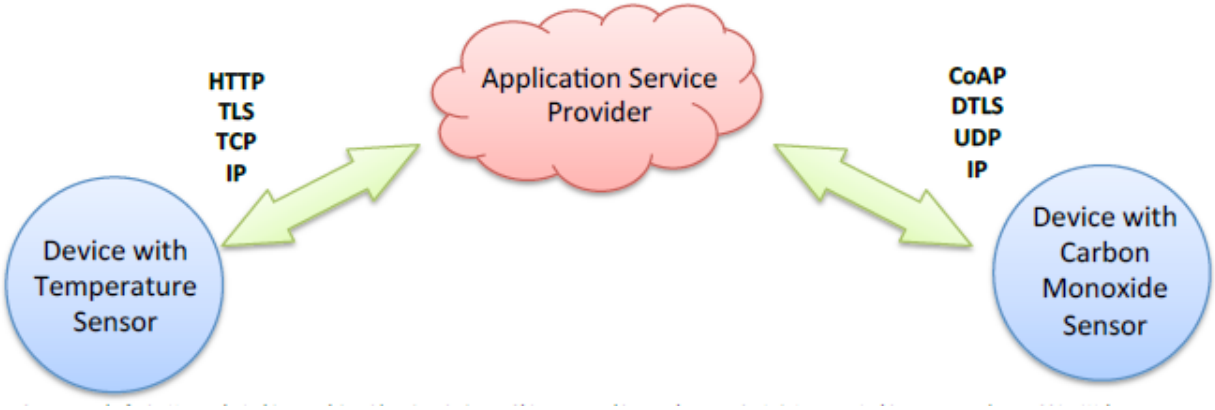

Figure 5. Device to cloud communication model.

This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning, Thermostat and the Samsung Smart TV. In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung SmartTV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV. In these cases, thedevice-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.

However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary dataprotocols are used between the device and the cloud service, the device owner or user may be tied to aspecific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lockin'', a term that encompasses other facets of the relationship with the providersuch as ownership of and access to the data. At the same time, users can generally have confidence thatdevices designed for the specific platform can be integrated.

2.3 Device to gateway communication

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediarybetween the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 6.

Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often themodel employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

The other form of this device-to-gateway model is the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloudservice, but they can also bridge the interoperability gap between devices themselves. For example, theSmartThings hub is a stand-alone gateway device that has Z-Wave and ZigBee transceivers installed tocommunicate with both families of devices. It then connects to the SmartThings cloud service, allowing theuser to gain access to the devices using a smartphone app and an Internet connection.

From a broader technical perspective, the IETF Journal article explains the benefit of the device-to gateway approach: *This [communication model] is used in situations where the smart objects require interoperability with non-IP [Internet protocol] devices. Sometimes this approach is taken for integrating IPv6-only devices, which means a gateway is necessary for legacy IPv4-only devices and services.*

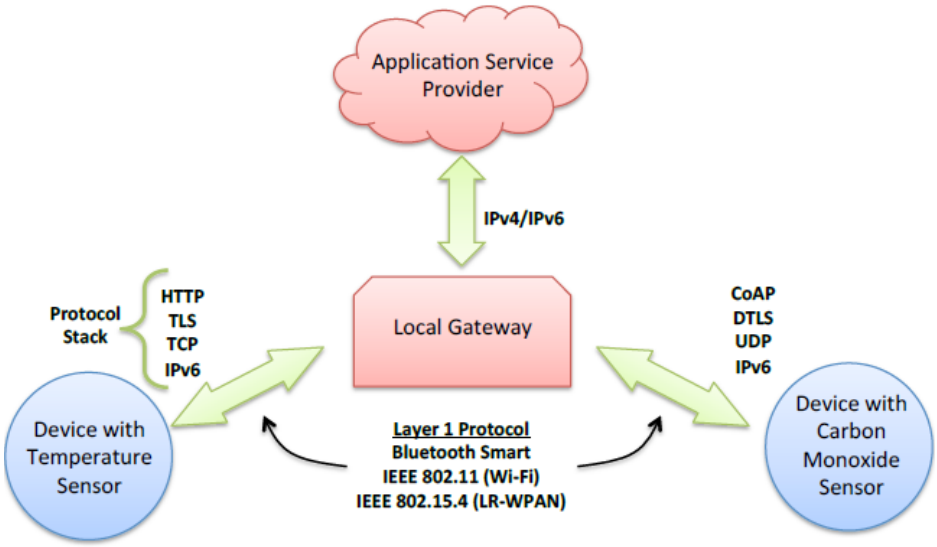

Figure 6. Device to gateway communication model.

In other words, this communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. A downside of this approach is that thenecessary development of the application-layer gateway software and system adds complexity and cost tothe overall system. The IAB's RFC7452 document suggests the outlook for this model*: It is expected that in the future, more generic gateways will be deployed to lower cost and infrastructure complexity for end consumers, enterprises, and industrial environments. Such generic gateways are more likely to exist if IoT device designs make use of generic Internet protocols and not require applicationlayer gateways that translate one application-layer protocol to another one. The use of application-layer gateways will, in general, lead to a more fragile deployment, as has been observed in the past.*

The evolution of systems using the device-to-gateway communication model and its larger role in addressinginteroperability challenges among IoT devices is still unfolding.

2.4 Back end data sharing model

The "*back end datasharing*" model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. Thisarchitecture supports "*the user's desire for granting access to the uploaded sensor data to third parties*". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "*IoT devices upload data only to a single application service provider*''. A "*backend sharing*"architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.

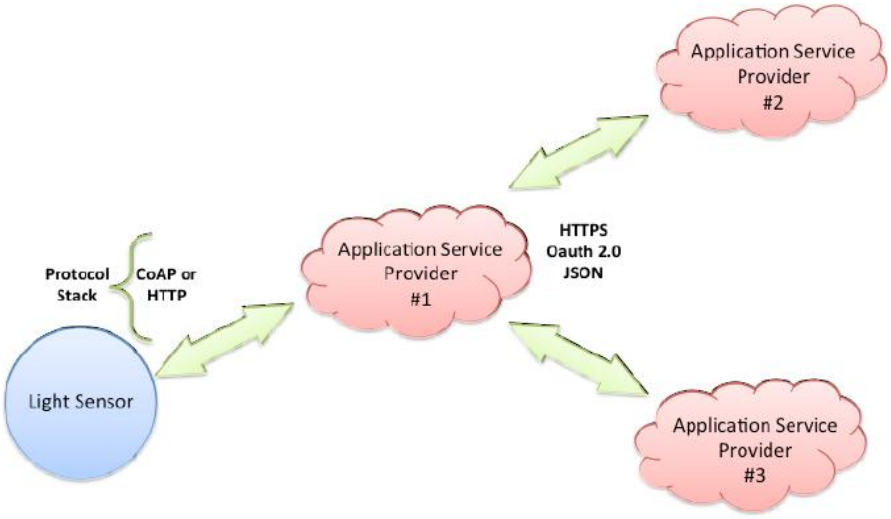

Figure 7. Back-end data sharing model.

For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet enabled utility systems on the premises. Often in the single "*devicetocloud*" model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective "*back end datasharing*"architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud. A graphical representation of this design is shown in Figure 7.

3.Internet of Things: Key Technologies

IoT can only be realized by useful deployment of multiple technologies that covers in the domain of Hardware, Software and extremely robust applications around each domain of industries and operating sectors. Some of the key technology areas that will enable IoT are [10]:

- ✓ Identification technology
- ✓ IoT architecture technology
- ✓ Communication technology
- ✓ Network technology
- ✓ Network discovery technology
- ✓ Software and algorithms
- ✓ Hardware technology
- ✓ Data and signal processing technology
- ✓ Discovery and search engine technology
- ✓ Relationship network management technology
- ✓ Power and energy storage technology
- ✓ Security and privacy technologies
- ✓ Standardization.

Figure 8 shows key technologies used in IoT and Figure 9 shows Key technological developments in the context of IoT.

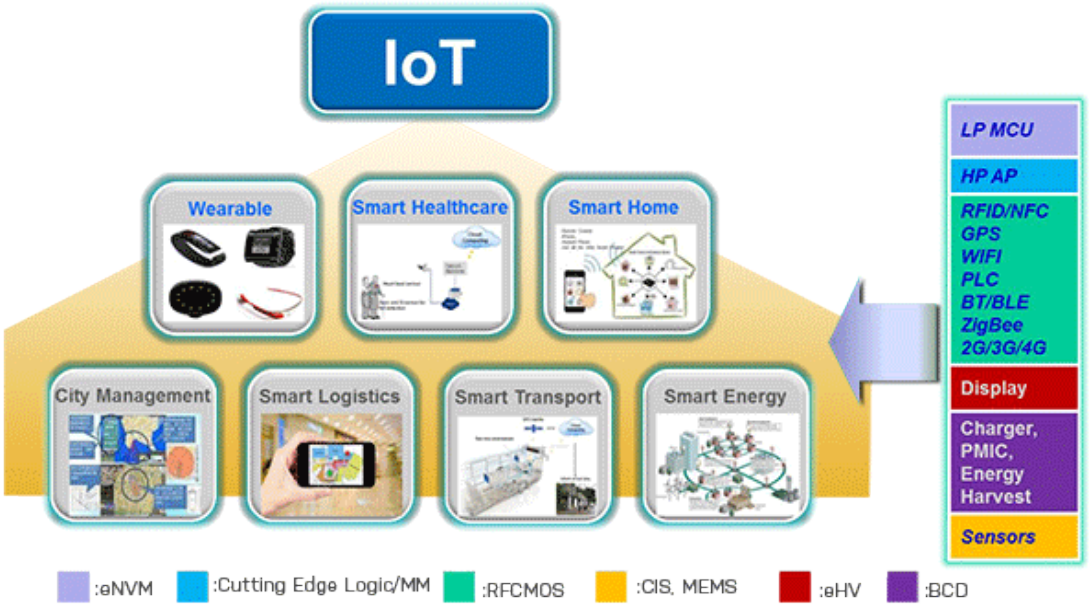

Figure 8. Key technologies used in IoT

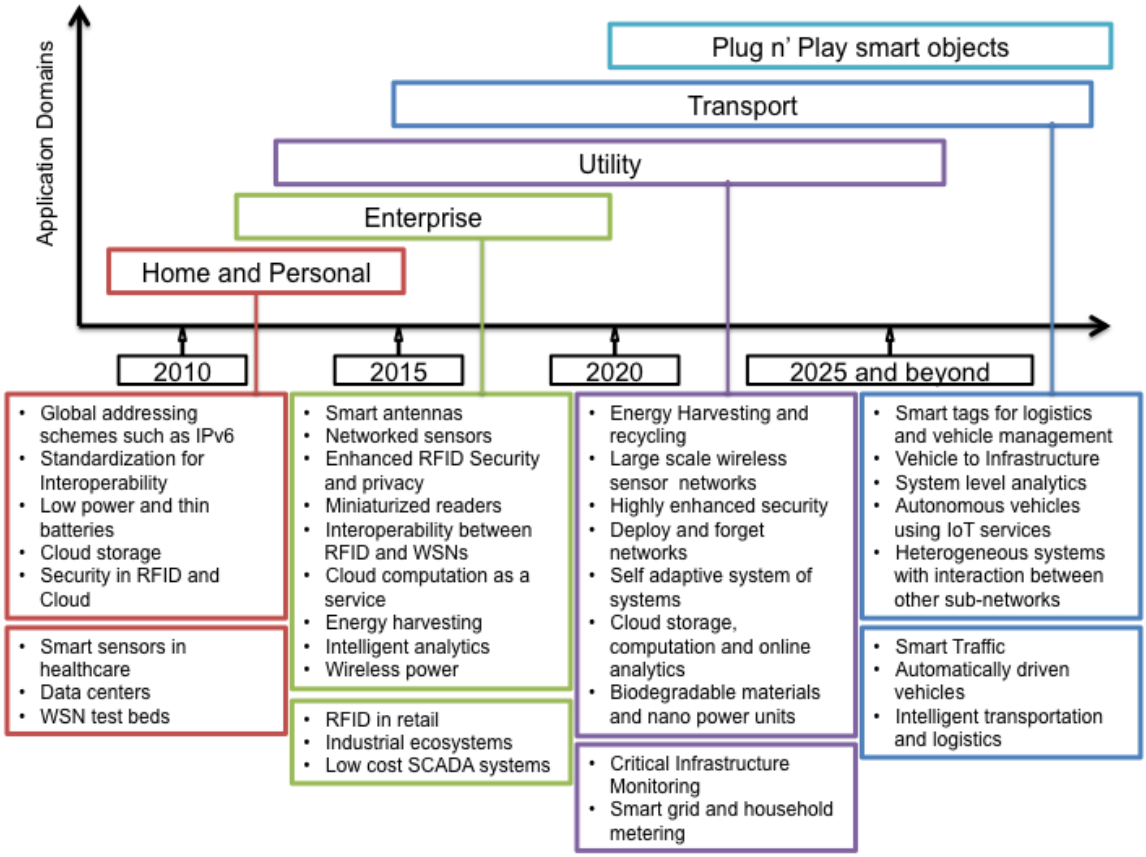

Figure 9. Key technological developments in the context of IoT.

3.1 Internet of Things: Applications

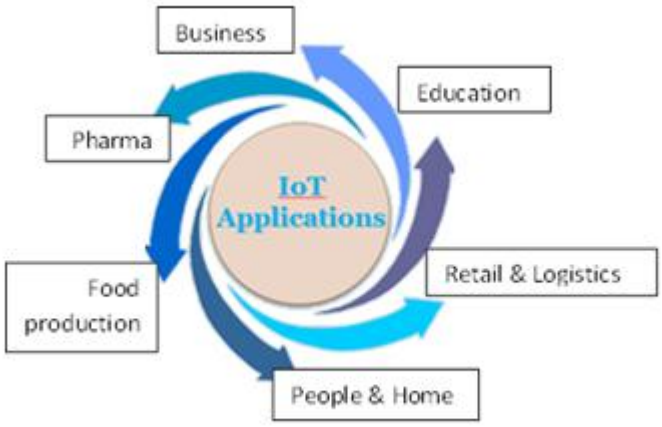

Figure 10. Overview domains of IoT

Internet of Things is applied to many domains as Figure 10. The potentialities offered by the IoT make it possible to develop numerous applications based on it, of which only a few applications are currently deployed. In future, there will be intelligent applications for smarter homes and offices, smarter transportation systems, smarter hospitals, smarter enterprises and factories. In the following this sections, some of the important example applications of IoT are briefly:

- ✓ Telecommunications
- ✓ Medical and healthcare, pharmacy

- ✓ Transportation
- ✓ Home
- ✓ Environment monitoring
- ✓ Transportation industry

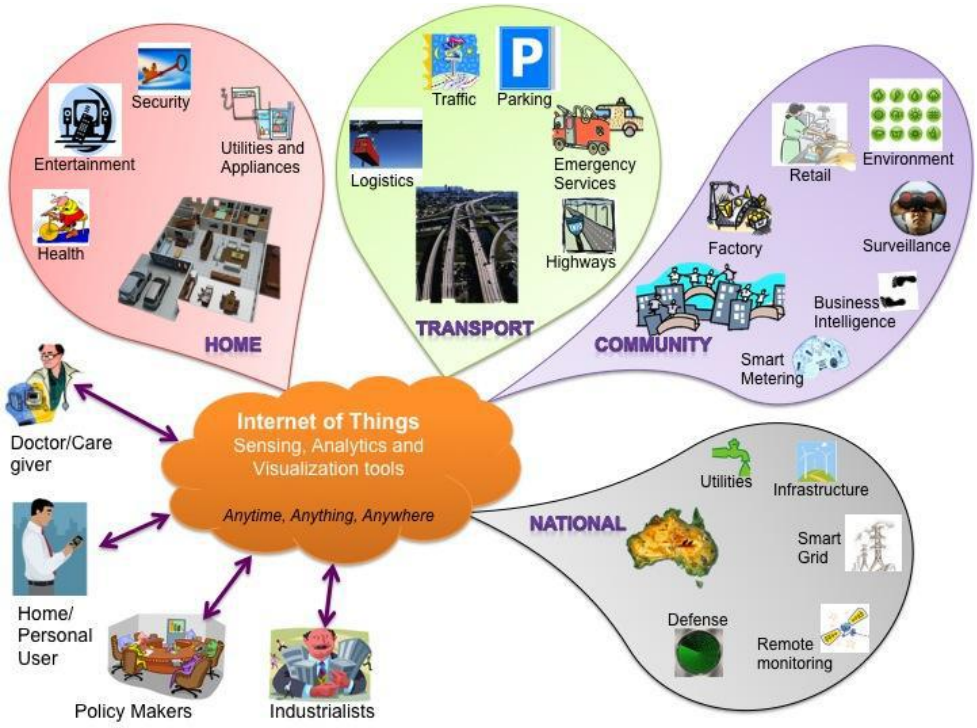

Figure 11. Some applications of IoT.

3.2 Internet of Things: Trends, Challenges and Open Issues

Internet of Things has been identified as one of the emerging technologies in IT. The popularity of different paradigms varies with time. The web search popularity, as measured by the Google search trends during the last 10 years for the terms Internet of Things, Wireless Sensor Networks and Ubiquitous Computing are shown in Figure 11. As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for Wireless Sensor Networks. This trend is likely to continue for the next decade as other enabling technologies converge to form a genuine Internet of Things.

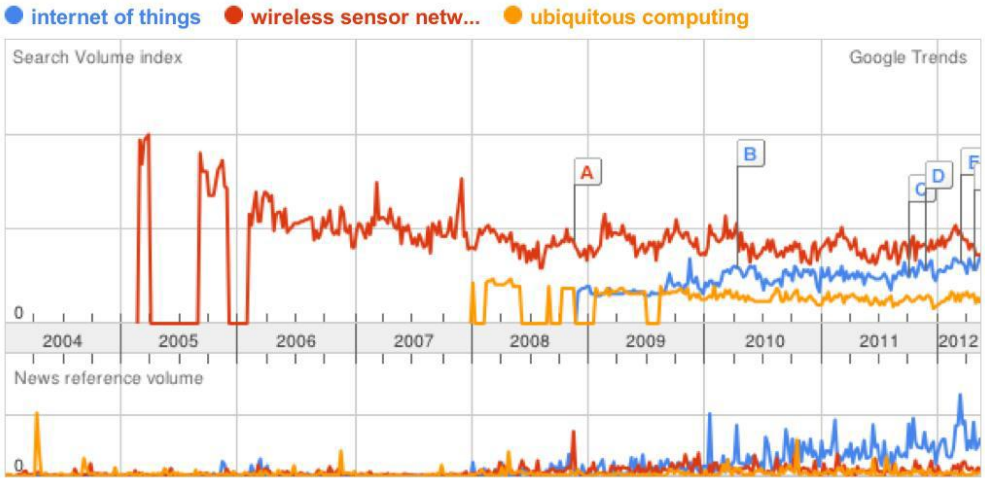

Figure 12. Trend of IoT.

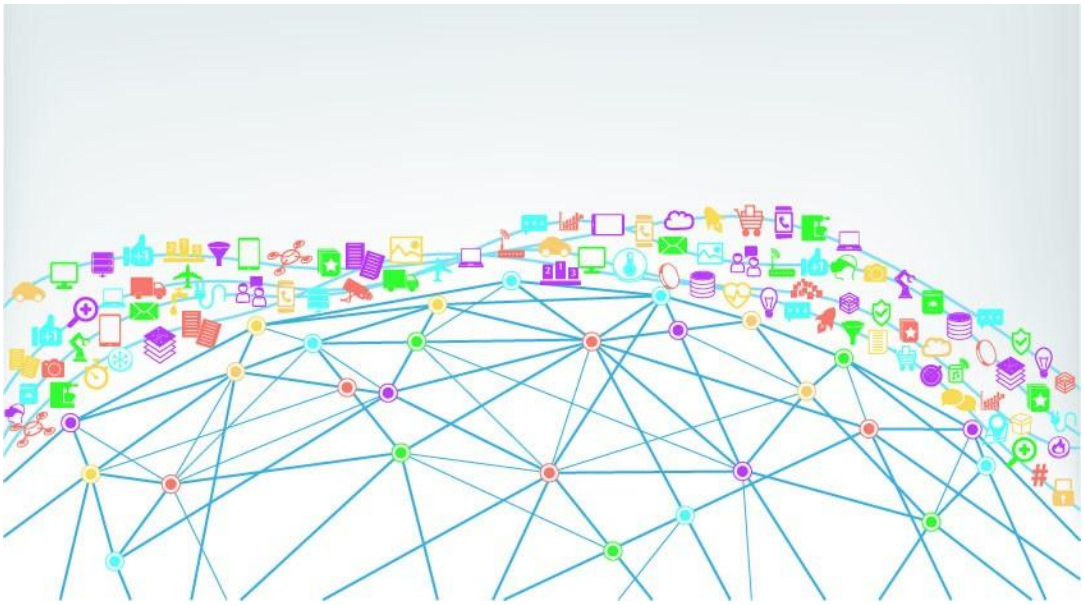

Figure 13. Challenges of IoT

The workflows in analyzed enterprise environment, home, office and othersmart spaces in the future will be characterized by cross organization interaction, requiring the operation of highly dynamic and ad-ho relationships. Atpresent, only a very limited ICT support is available, and the following key challenges exist [11].

- ✓ *Network Foundation*: Limitations of the current Internet architecturein terms of mobility, availability, manageability and scalability are some of the major barriers to IoT.
- ✓ *Security, Privacy and Trust*: In the domain of security the challenges are: (a) securing the architecture of IOT - security to be ensured atdesign time and execution time, (b) proactive identification and protection ofIOT from arbitrary attacks (e.g. DoS and DDoS attacks), and (c)proactive identification and protection of IOT from malicious software. In thedomain of user privacy, the specific challenges are: (a) control over personalinformation (data privacy) and control over individual's physical location andmovement (location privacy), (b) need for privacy enhancement technologiesand relevant protection laws, and (c) standards, methodologies and tools foridentity management of users and objects. In the domain of trust, some ofthe specific challenges are: (a) Need for easy and natural exchange of critical,protected and sensitive data - e.g. smart objects will communicate on behalfof users / organizations with services they can trust, and (b) trust has to bea part of the design of IoT and must be built in.
- ✓ *Managing heterogeneity*:Managing heterogeneous applications,environments and devices constitute a major challenge.
- ✓ *In addition to the above major challenges, some of the other challenges are*: (i) managing large amount of information and mining large volume of data to provide useful services, (ii) designing an efficient architecture for sensor networking and storage, (iii) designing mechanisms for sensor data discovery, (iv) designing sensor data communication protocols senor data query, publish/subscribe mechanisms, (v) developing sensor data stream processingmechanisms, and (vi) sensor data mining correlation, aggregation filteringtechniques design. Finally, standardizing heterogeneous technologies, devices,application interfaces etc. will also be a major challenge.

4.Conclusion

There are several areas in which further research is needed for making deployment of the concept of IoTreliable, robust and efficient. Some of the areas are identified in the following. In identification technology domain, further research is needed in development of new technologies that address the global ID schemes, identity management, identity encoding/ encryption, revocable anonymity, authentication of parties, repository management using identification, authentication and addressing schemes and the creation of global directory lookup services and discovery services for IoT applications with various identifier schemes. In architecture design domain, some of the issues that need attention are: design of distributed open architecture with end-to-end characteristics, interoperability of heterogeneous systems, neutral access, clear layering andresilience to physical network disruption, decentralized autonomic architectures based on peering of nodes etc.

In communication protocol domain, the issues that need to be addressed are: design of energy efficient communication by multi frequency protocol, communication spectrum and frequency allocation, software defined radios to remove the needs for hardware upgrades for new protocols, and design of high performance, scalable algorithms and protocols. In network technology domain further research is needed on network on chip technology considering on chip communication architectures for dynamic configurations design time parameterized architecture with a dynamic routing scheme and a variable number of allowed virtual connections at each output.

In addition, power-aware network design that turns on and off the links in response to burst and dips of traffic on demand, scalable

communication infrastructures design on chip to dynamically support the communication among circuit modules based on varying workloads and /or changing constraints are some of the important research issues.

Acknowledgement

This research is supported by FPT University, Hanoi, Vietnam; Cao Thang Technical College, Ho Chi Minh City, Viet Nam; and HUTECH Institute of Engineering, HUTECH University, Ho Chi Minh City, Vietnam.

References

[1] "Radio-Frequency Identification,"https://en.wikipedia.org/wiki/Radiofrequency_identification, accessed on 21, Dec., 2021.
[2] "Machine to Machine," https://en.wikipedia.org/wiki/Machine_to_machine, accessed on 21, Dec., 2021.
[3] Polsonetti and Chantal, "Know the Difference Between IoT and M2M," Automation World, July 15, 2014.
[4] "The Internet Toaster," http://www.livinginternet.com/i/ia_myths_toast.htm, accessed on 21, Dec., 2021.
[5] "The Only Coke Machine on the Internet," Carnegie Mellon University Computer Science Department.
[6] Stafford-Fraser and Quentin, "The Trojan Room Coffee Pot," May, 1995.
[7] RFC 7452, "Architectural Considerations in Smart Object Networking," March 2015.
[8] Corporation's statement to U.S. House of Representatives hearing on IoT, available at: http://docs.house.gov/meetings/IF/IF17/20150324/103226/HHRG-114-IF17-Wstate-SchoolerR-20150324.pdf, accessed on 21, Dec., 2021.
[9] Tschofenig, "Architectural Considerations in Smart Object Networking." Tech. No. RFC 7452, Internet Architecture Board, Mar. 2015.
[10] Debasis and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," Innovation Labs, Tata Consultancy Services Ltd. Kolkata - 700091, INDIA.
[11]J. Gubbi, R. Buyya, S. Marusic and M.Palaniswamia, "Internet of Things: A Vision, Architectural Elements, and Future Directions," Dept. of Electrical & Electronic Engineering, University of Melbourne, Australia.