Delta University Scientific Journal
Journal home page: https://dusj.journals.ekb.eg

Understanding the Internet of Things (IoT) Concepts, Applications and Standards: An Overview

Assoc. Prof. M. S. M. Elksasy,
Dept. of Mechatronics Engineering,
Faculty of Engineering, Delta University for Science& Technology,
International Coastal Road, Gamasa City, Mansoura, Dakhliya, Egypt,
Mohamed.sherif@deltauniv.edu.eg , msmksasy@gmail.com

ABSTRACT

The Internet of things (IoT) is a new revolution of the Internet. It makes objects themselves recognizable, obtain intelligence, communicate information about themselves and they can access information that has been aggregated by other things.

The Internet of Things is a paradigm that involves physical objects with capabilities of sensing, information processing and communication through wireless or wired connection. These physical objects having embedded intelligence and hence decision-making capabilities act as smart things. The paradigm of IoT embraces various domains including sensors, information and communication technology, memory space, data analytics, machine learning and security and privacy mechanisms.

IoT refers to a type of network to connect anything with the Internet based on stipulated protocols through information sensing equipment to conduct information exchange and communications in order to achieve smart recognitions, positioning, tracing, monitoring, and administration. The 'things' are constrained in terms of computing power, memory space and data rate and hence need innovative approaches to address the technical challenges present in the real-life implementation of the concept. The IoT allows people and things to be connected **4As** (i.e. Anytime, Anyplace, with Anything and Anyone).

IoT systems have applications across industries through their unique flexibility and ability to be suitable in any environment. They enhance data collection, automation, operations, and much more through smart devices and powerful enabling technology.

The aim of this paper is to provide a briefly discussion about what IoT is, how IoT enables different technologies, about its architecture, characteristics & applications, IoT functional view and highlights of the technical challenges therein open for research community.

Keywords: *Internet of Things, IoT definitions, IoT technology, IoT applications, Smart Things, IoT challenges.*

1. Introduction

The Internet of Things (IoT) is a new paradigm and probably one of the most important technological revolutions. According to the IEEE IoT initiative [1] IoT is defined as, "A network that connects uniquely identifiable 'things' to the internet." These 'things' have sensing/actuation and programmability capabilities. The word, 'things' in IoT basically refers to smart objects equipped with sensing, storage, data processing , and communication capabilities. The basic concept of IoT is to bring 'anything, anywhere, anytime, anyway, and anyhow' on a common interconnected networking platform as illustrated in Fig. 1.

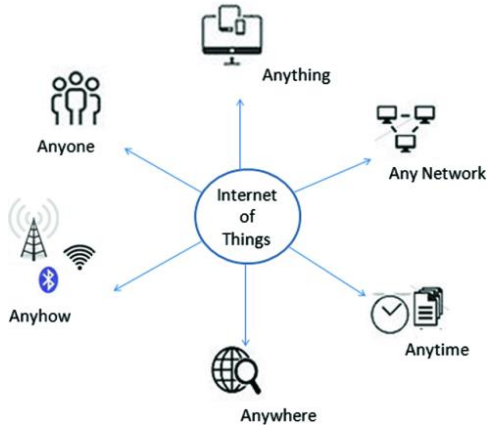

Fig. 1 IoT Concepts

The interesting part of IoT is capability of the objects to directly interact with their surroundings. This technology will make the objects, people, processes, machines, environment and infra structure to interact and communicate with each other. IoT is indeed being evolved as a global network that will embrace almost all walks of our life.

Relative to having less than 1% of the things connected onto the internet today, it is predicted that the advent of IoT will connect more than 24 billion things to the internet by the year 2019 [2]. Projections by Morgan Stanley and Huawei state to have 75 billion by 2020 and 100 billion by 2025 networked devices, respectively [3, 4]. These predictions confirm phenomenal growth and huge impact and influence of IoT on the socio-economic life of the people around the world as depicted in Fig. 2

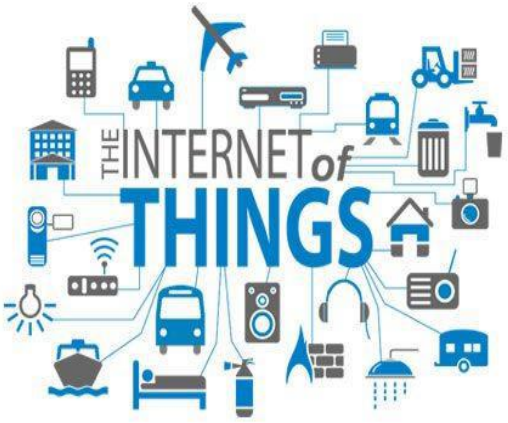

Fig. 2 IoT Applications

IoT enables integration of physical and virtual things through communication technologies, sensors, actuators, Machine-Type Communication (MTC), Device-to-Device Communication (D2D), data analytics and edge computing. Integration of these technologies and supported functionalities results in smart environment, smart transportation, smart home, smart manufacturing, smart health care and so on, which ultimately leads to evolution of the 'Smart World'.

The aim of this paper is to provide a briefly discussion about what IoT is, how IoT enables different technologies, about its architecture, characteristics & applications, IoT functional view and highlights of the technical challenges therein open for research community. Vulnerabilities of the IoT devices to the security breaches are highlighted and research efforts being invested to address those are also presented.

2. Material and methods

I. Constituent Domains of the IoT System

A. Architecture

Given the projection of the trillions of smart things being connected to the internet, the immediate requirement is to decide on an appropriate architecture to handle this scale of connectivity. Primarily, IoT is a network of sensors and actuator envisaged to manifest as utility network similar to electricity type network. This network consists of multiple systems including home automation with energy management system, health care with possible inclusion of wearable medical devices and so on. The architecture must support proper dependencies among such subsystem of IoT.

Integration of subsystems is a very challenging and complicated task. Each system has its own requirements and objectives to accomplish without giving any consideration to others. For example, in healthcare system, wearable particularly critical ones-pacemakers cannot be turned off to save the energy as we can do for home automation. Developing an interacting and powerful architecture supporting interdependencies is indeed an open and challenging research problem.

The proposed architecture provides support for the coexistence of centralized cloud and mobile edge computing with collaborative computation offloading feature.

B. Communication Technologies for IoT

A number of wireless technologies are being explored for the implementation of IoT systems. Some of the prominent ones are summarized below:

i- **Long-Range (LoRa) WAN** is one of the most common technologies for IoT connectivity [7, 8]. Data rate offered ranges from 0.3 to 50 kbits/s in unlicensed frequency band. It offers communication range of up to 20 km. LoRa WAN is equipped with AES encryption for the provisioning of the security.

ii- **Z-Wave** is a low-power RF communication technology primarily designed for home automation [9]. It operates at 900 MHz frequency band and impervious to interference from Wi-Fi applications. It is optimised for

reliable and low latency communication offering data rate of 100 kbits/s and operates on low energy license exempt band. It is equipped with ECDH for key exchange process.

iii- ***Zig* Bee** is an open standard based on IEEE 802.15.4 protocol for low rate wireless personal area networks. It is an industry standard wireless networking technology providing up to 100 m communication range and supporting data rate up to 31 kbits/s at 868 MHz, which reaches up to 250 kbits/s at 2.4 GHz. This wireless technology is robust, secure and highly scalable and hence found favour for practical implementation in M2 M and IoT applications.

iv- **Bluetooth** is a short-range communication technology consuming significantly reduced power for its operation. Bluetooth Smart also known as Bluetooth Low Energy (BLE) offers a very promising protocol for IoT applications and considered as the highly promising technology particularly for wearable devices [10].

v- **Thread** [11] is based on IPv6 protocol again optimized for home automation. This technology supports a mesh network based on IEEE 802.15.4 standard. It can handle up to 250 nodes. Simple software upgrades enables users to run threads on the existing IEEE 802.15.4-enabled devices.

Low-Power Wide-Area Networks (LPWANs) has been proposed for IoT systems [12]. The typical LPWAN technologies include SigFox, OnRamp, NB-IoT and Lora. SigFox uses ultra-narrowband frequency spectrum primarily designed to handle low data rate

vi- services within 10 to 1000 bits/s. Its power consumption is very low operating with 50 microwatts and hence may have life cycle of 20 years with a 2.5 Ah battery.

vii- **Near-Field Communication** (NFC) is specifically designed for two-way communication between the electronic devices like smartphones within proximity of 4 cm [13]. NFC is based on RFID standards—ISO/IEC14443 and FeliCa.

viii- **NB-IoT** Neul [14] has presented standard for the wireless connectivity of IoT devices. It utilizes TV white space as the spectrum to deliver the services. It is highly scalable with larger coverage, low power and cost-effective wireless networking technology. It is also referred to as the weightless technology available at the price of Bluetooth but offering the range of cellular technology and data rate support from a few bits/s to 100 kbps. It is highly energy efficient, consumes 20–30 mA and hence has extended lifetime of 10–15 years.

C. Scaling of Connectivity

IoT concept invariability leads to immense connectivity scaling up to 200,000 connections/kM2. Currently available communication protocols may not work for this scale of connectivity. Centralized server–client model can handle thousands of devices, but it may not work for billions of connected devices. Maintaining servers to handle such large amount of data is very difficult and challenging task. One possible solution may be decentralizing the IoT networking. Some of the tasks may be transferred to edge-like fog computing model [6]. IoT hubs can handle mission-critical operations and cloud server can handle collection of data and its analysis. Peer to peer communication may also be explored.

Massive scaling of IoT raises the pertinent issues of maintenance, protection, access authentication, naming and addressing schemes. Again the identification and developing an architecture to support these functionalities is a huge and complex task.

D. Real-Time Data Processing

IoT deployment will generate immense amount of data. Knowledge creation through interpretation of the data collected from physical world via an array of sensors is a huge and computationally intensive operation. Drawing the inference from the sensed data through data mining techniques may create knowledge but with finite uncertainty. This may be very risky for actuation and hence may result in lack of trust for the adoption of the IoT technology.

E. Security

In this super-connected world, sensitive and private information will flow over wireless channels. As a matter of fact, wireless communication being broadcast in nature lends itself as non-secure medium. It is vulnerable and hence eavesdropper may overhear the confidential messages. Further, the massive scale of connectivity will provide

the attacker huge surface area. An attacker can have easy access to these smart but small devices. The things may be used as botnets by the attacker exploiting their security vulnerabilities. Security mechanisms are required which could provide assurances in terms of integrity of the data flow, confidentiality, authentications and non-repudiation of the information flow. In case of no human intervention, the security risk is increased by order of magnitude.
The things in IoT are resource constrained in processing power, memory and battery life and communication capabilities. Conventionally, security mechanisms are implemented at higher layers and these are based on cryptographic approaches, which are intrinsically computationally intensive and demand large memory space. This makes the security in IoT a major and challenging task.

F. Power Consumption and Energy Efficiency

One of the fundamental requirements of IoT applications is the support for low-power operations. The small devices and sensor nodes are resource-constrained powered by on-board batteries and expected to work for long hours. Particularly in wearable medical devices like pacemakers and in-ear hearing aids, these devices must work without any failure. Standby and sleep mode techniques are used to enhance the battery life. They remain active for brief intervals only to send and receive the data.

II. IoT Architecture

IoT architecture consists of different layers of technologies supporting IoT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IoT deployments in different scenarios. Figure 3 shows detailed architecture of IoT [1][3][4].

A. Smart Device / Sensor Layer:

The lowest layer is made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. In some cases, they may also have a degree of memory, enabling them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telematics sensors, etc. [1].

Most sensors require connectivity to the sensor gateways. This can be in the form of a local area network (LAN) such as Ethernet and Wi-Fi connections or personal area network (PAN) such as ZigBee, Bluetooth and Ultra Wideband (UWB). For sensors that do not require connectivity to sensor aggregators, their connectivity to backend servers/applications can be provided using wide area network (WAN) such as GSM, GPRS and LTE. Sensors that use low power and low data rate connectivity, they typically form networks commonly known as wireless sensor networks (WSNs). WSNs are gaining popularity as they can accommodate far more sensor nodes while retaining adequate battery life and covering large areas [1].

B. Gateways and Networks

Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications. With demand needed to serve a wider range of IOT services and applications such as high speed transactional services, context-aware applications, etc., multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security [1].

C. 3.2 Management Service Layer

The management service renders the processing of information possible through analytics, security controls, process modeling and management of devices [1].

One of the important features of the management service layer is the business and process rule engines. IOT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to post-processing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IOT system [1].

In the area of analytics, various analytics tools are used to extract relevant information from massive amount of raw data and to be processed at a much faster rate. Analytics such as in-memory analytics allows large volumes of data to be cached in random access memory (RAM) rather than stored in physical disks. In-memory analytics reduces data query time and augments the speed of decision making. Streaming analytics is another form of analytics where analysis of data, considered as data-in-motion, is required to be carried out in real time so that decisions can be made in a matter of seconds [1].

Data management is the ability to manage data information flow. With data management in the management service layer, information can be accessed, integrated and controlled. Higher layer applications can be shielded from the need to process unnecessary data and reduce the risk of privacy disclosure of the data source. Data filtering techniques such as data anonymization, data integration and data synchronization, are used to hide the details of the information while providing only essential information that is usable for the relevant applications. With the use of data abstraction, information can be extracted to provide a common business view of data to gain greater agility and reuse across domains. Security must be enforced across the whole dimension of the IOT architecture right from the smart object layer all the way to the application layer. Security of the system prevents system hacking and compromises by unauthorized personnel, thus reducing the possibility of risks [1].

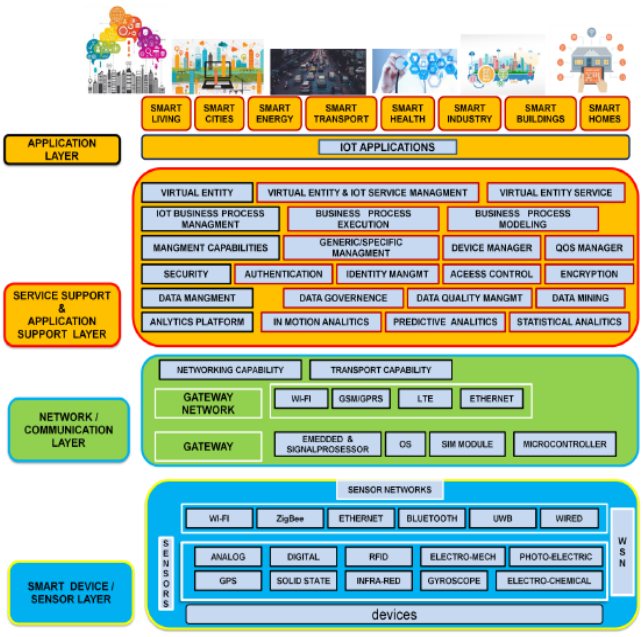

Fig. 3 IoT Architecture.

D. 3.3 Application Layer

IoT application covers "smart" environments/spaces in domains such as: transportation, building, city, lifestyle, retail, agriculture, factory, supply chain, emergency, healthcare, user interaction, culture, tourism, environment and energy [1].

Conclusion

IoT may be characterized by ubiquitous connectivity and data collection along with very high level of security risks. Its implementation has myriad of problems and an array of technical challenges. These need to be resolved to realize the vision of smart world through IoT paradigm. Given all the risks and challenges, it is going to become a reality unleashing plethora of opportunities in all walks of life defence, agriculture, industry, retail, environmental monitoring and automotive industry, urbanization, health care and business. IoT is evolving as the third in top ten strategic technologies which is expected to grow to $14 trillion business opportunities. The world is indeed transforming into its smart version through a network of connected intelligent things.

References

[1] Minerva, R., Biru, A., Rotondi, D.: Towards a definition of the internet of things (IoT), In: IEEE Internet of Things Initiative (2015).
[2] Cloud and mobile network traffic forecasting – visual networking Index (VNI) Cisco- (2015).
[3] Tony, D., Stanely, M.: 75 Billion devices will be connected to the internet by things by 2020, Business insider (2013).
[4] Global Connectivity Index Huawei Technologies Co. Ltd 2015 Wen 06 Sept 2015.
[5] Suganuma. T., Oide, T., Kitagami, S., Sugawara, K., Shiratori, N.: Multiagent based flexible edge computing architecture for IoT. IEEE Netw. 16–23 (2018).
[6] Guo, H., Liu, J., Qin, H.: Collaborative mobile edge computation offloading for IoT over fibre-wireless networks. IEEE Netw. 66–77 (2018).
[7] Sornin, N., Luis, M., Eirich, T., Cramp, T., Hersent, O.: LoRaWAN specifications (2015).
[8] Centenaro, M., Vangelista, L., Zanella, A., Zorzi, M.: Long-Range Communications in Unlicensed Bands: the Rising Star in the IoT and Smart City Scenarios. IEEE Wirel. Commun. **23**(5), 60–67 (2016).
[9] Marksteiner, S., Jimenez, V.J.E., Vallant, H., Zeiner, H.: An overview of wireless IoT protocol security in the smart home domain. In: IEEE Conference on Internet of Things Business Models, Users, and Networks, pp. 1–8 (2017).
[10] Hussain, S.R., Mehnaz, S., Nirjon, S., Bertino, E.: Secure seamless bluetooth low energy connection migration for unmodified IoT devices. IEEE Trans. Mobile Comput. (99), 1–17 (2017).
[11] Sujin Issa Samuel, S.: A review of connectivity challenges in IoT smart home. In: 3rd MEC International Conference on Big Data and Smart City (2016).
[12] Krupka, L., Vojtech, L., Neruda, M.: The issue of LPWAN technology coexistence in IoT environment. In: 17th International Conference on Mechatronics-Mechatronika (2016).
[13] Choi, Y., Choi, Y., Kim, D., Park, J.: Scheme to guarantee IP continuity for NFC based IoT networking. In: 19th International Conference On Advanced Communication Technology, pp 695–698 (2017).
[14] Miller, F., Vandome, A., McBrewster, J.: Advanced encryption standard (2009).
[15] Yap, H., Khoo, K., Poschmann, A., Henricksen, M.: EPCBC- A block cipher suitable for electronic product code encryption. www1.spms.ntu.edu.sg/~kkhoongm/epcbc
[16] Indesteege S, Dunkelman NKO, Biham E, Preneel B. A practicalattack on KeeL oq. http://www.cosic.esat.kuleuven.be / publications/article-1045.pdf
[17] Granjal, Jorge, Silva, Edmundo Monteiro Jorge Sa: Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Trans. Surv. Tutorials **17**(3), 1294–1311 (2015)