

Internet of Things: Current Trends, Architectures and Challenges

Mohamed Osman Elbashir, Awad Haj Ali

Abstract The Internet-of Things (IoT) revolution has gone a long way to reach the current state. This paper addresses the IoT general concepts and discusses the IoT building blocks. Furthermore, the IoT enabling IoT technologies are reviewed such as Radio-Frequency Identification (RFID), Wireless Sensor Networks (WSN), Mobile Communications technology and Wide Area Network (WAN). The paper also reviews and compares the basic most known architectures and also reviews some architectures proposed by researchers. The paper also presents and reviews the possible challenges that face IoT in different aspects such as standards, privacy, identification and authentication, security, trust and ownership, integration, coordination and regulation, spectrum and greening of IoT. Finally, since the IoT is getting increasing popularity for academia, industry as well as government, future research directions are tackled and presented.

Index Terms— Internet of things, IoT, IoT architecture, IoT challenges, IoT enabling technologies, Mobile communication technology, RFID, Wireless sensor networks

1. INTRODUCTION

Nowadays, we can hardly imagine our life without the Internet. As technology becomes more affordable and as more and more devices are connected every day, we might – after a few years – feel it even harder to imagine our life without IoT. The emerging technology breakthrough of the Internet-of-Things (IoT) is expected to offer promising solutions to a wide range of day-to-day problems in our life thus fostering the quality of life in all parts of the globe. IoT revolution has gone a long way to reach the current state. It is a legitimate child of the Internet revolution which emerged for the public in the last decade of the past century.

The research performed by Aldeen, Alsahib [1] state: “One of the buzzwords in the Information Technology is Internet of Things (IoT). The future is Internet of Things, which will transform the real world objects into intelligent virtual objects. The IoT aims to unify everything in our world under a common infrastructure, giving us not only control of things around us, but also keeping us informed of the state of the things.”

The term Internet of Things was first coined by Kevin Ashton in 1999 in the context of supply chain management [2]. However, in the past decade, the definition has been more inclusive covering wide range of applications like healthcare, utilities, transport, etc.

2. DEFINITION

Over the years many different definitions of ‘Internet of Things’ have been proposed. The term heralds a vision of the future Internet where connecting physical things, from shoes to vehicles, through the Internet, will let them exchange information about themselves and their surroundings.

Everyday objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but “things” that we do not do normally think of as electronic at all – such as

food, clothing; and furniture; materials, parts and equipment, merchandise and specialized items; landmarks, monuments and works of art and all the miscellany of commerce, culture and sophistication [3]. The IoT prototype is subject to smart and self-configuring objects that are connected to each other through a global network infrastructure [4].

One of the best definitions of IoT to me is: “An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment” [5].

In a few short years, the Internet of Things (IoT) has gone from a technology – or set of technologies – that were cutting edge, to the situation today where connected household items, or automobiles, are common. However, growth is only really gathering speed now with San Francisco-based Cisco estimating that the "Internet of Everything cisco article" could have as many as 50 billion connected devices by 2020. For IoT, objects are required to be made smart by embedding intelligence into them using technologies such as Wireless Sensor Networks (WSN) and Radio Frequency Identification (RFID)[6].

The IoT is a hot research topic that is getting increasing popularity for academia, industry as well as government. Many European and American organizations and multinational companies are involved in the design and development of IoT to achieve different type of useful and powerful automated service[7].

Being connected is not only through computers, servers and smart phones; in IoT technology connection includes sensors and actuators embedded in physical objects - from jogging shoes to water sprinklers - connected through wired and wireless networks, often using the Internet protocol. These networks produce huge volumes of data that flow to computers for analysis and hence actions.

According to Helsinki, Finland-based F-Secure, a cyber-security company citing research from Gartner, over the next

two years, the number of IoT devices entering households will climb steeply from nine devices per household currently to 500 by 2022, with IoT connectivity being bundled into products whether people want it or not [8].

When talking about “being connected” we immediately think in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. However, when associating this term to IoT, other elements appear like sensors and actuators embedded in physical objects – from temperature regulators to pacemakers – are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks continuously emit data about the working state of the device.

The future of IoT is huge, business intelligence estimate 24 billion IoT devices will be installed by 2020 and IDC predicts that IoT revenue will reach about 375,000,000,000 in 2019 resulting in a lot of opportunities in IT industry. Sources are calling the IoT revolution bigger than the industrial revolution. Some say that by 2020, 43% of IT budget will be dedicated to IoT projects.

2. IOT ELEMENTS AND THEIR PROPERTIES

Understanding the IoT building blocks helps to gain a better insight into the real meaning and functionality of the IoT which is composed of enormous communication networks where devices can interact with each other via the Internet. These devices (things) have specific properties which are analyzed by Al-Fuqaha, Guizani [9] as: Identification, Sensing, Communication, Computation, Services and Semantics. These elements are needed to deliver the functionality of the IoT as illustrated in Fig. 1.

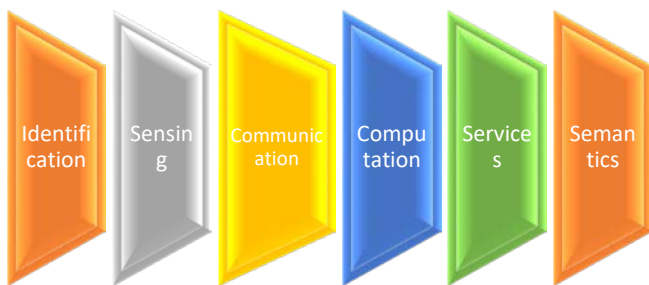


Fig. 1. The IoT Elements [9]

These elements and their characteristics are discussed in the following sections.

- Identification: Each IoT object has to have an identity address in order to distinguish it and make it communicable by other devices.
- Sensing: This is the basic operation of interacting with the physical environment.
- Communication: This refers to the interconnection methods which are used in order to communicate the objects with the users or with other objects.

- Computation: Most of the data communicated need computation methods to process the information which is obtained from the objects.
- Services: Services refer to the functions which are provided by the objects to the users in accordance with the information which they receive from the physical environment.
- Semantics: Semantics implies that the objects in the IoT have the ability to take the right information from an environment and provide this information as services at the appropriate time.

3. MAJOR IOT TECHNOLOGIES

Several enabling technologies have contributed towards the actualization of the IoT concept into the real world. In this section we discuss the most relevant ones. Note that it is not our intension to provide a comprehensive survey of each technology. Our major objective is to provide a picture of the role they will likely play in the IoT.

The major technologies that would dominate IoT applications according to Agrawal and Das [6], are WSN, RFID and Mobile communications along with the existing LAN/WAN. The Fig.2 shows a high-level view of IoT infrastructure as far as major technologies are concerned.

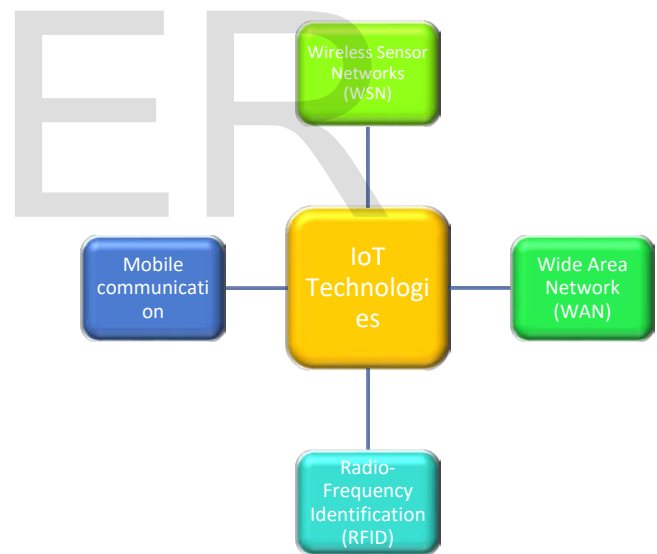


Fig. 2. Major IoT technologies [6]

In the following sections we discuss each of these technologies.

3.1 RADIO-FREQUENCY IDENTIFICATION (RFID) is the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked. This is why it is preferred to barcodes must be aligned with an optical scanner. RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and

enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this [10]. Put simply, an RFID systems consist of three components: an RFID tag, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader. The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time [10]. RFID tags can be active or passive. Passive: This tag remains dormant since it has no battery. It uses the reader's signal energy to turn on the tag along with reflecting a signal back to the reader that carries the information. Passive tags are cheap and small with short read range. Active RFID tags have a power supply that transmits signals periodically. These tags have a range of up to 100 meters due to the presence of the power supply. Due to this, active tags are useful in location tracking applications.

There are also Semi-Passive/active Tag: Both types of tag contain power supplied on board. The main difference is how the battery is used. Batteries in semi-passive tags are only used to power the internal circuitry. The advantage of semi-passive tags is longer read ranges than passive tags because the energy they absorb from electromagnetic field is fully used to transmit data only. Batteries in semi-active tags are used exactly the same as those in active tags; however, the energy will only be released to power the tags when the tags are being interrogated by RFID readers. The benefit of semi-active tags is that semi-active tags can last longer than active tags since the batteries will only be activated when the tags are being interrogated by RFID readers [11].


RFID system has been widely used for tracking objects, people and animals. One of the crucial factors of IoT infrastructure is identification of trillions of objects. And, RFID provides an important technological support for this requirement.

3.2 WIRELESS SENSOR NETWORKS (WSN) consist of a large number of tiny sensor nodes capable of sensing the objects and environment in physical world and communicate to the digital world of computer systems for making informed decisions [6]. Sensor nodes collect and forward the data to base station to cooperatively monitor the physical objects or environmental conditions such as temperature, vibrations, pressure and motion. In WSN, there are usually one or more base stations and several sensor nodes. The base-station acts as a gateway to connect a WSN to the outside world [12]. WSN technologies are now recognized widely for applications ranging from military services, traffic monitoring and agriculture. However, the present forms of WSN's usage are mostly working in isolation serving a specific application area.

3.3 MOBILE COMMUNICATIONS TECHNOLOGY is the technology used for cellular communication. Mobile code-division multiple access (CDMA) technology has evolved rapidly over the past few years. Since the start of this millennium, a standard mobile device has gone from being no more than a simple two-way pager to being a mobile phone, GPS navigation device, an embedded web browser and instant messaging client, and a handheld gaming console. Many experts believe that the future of computer technology rests in mobile computing with wireless networking.

The mobile communication evolution process started with 1G in the early 1980s. 1G was introduced as voice-only communication. Later in 1991, the development of 2G introduced Short Message Service (SMS) and Multimedia Messaging Service (MMS) capabilities, allowing picture messages to be sent and received between phones [13]. In 1998, 3G was introduced to provide faster data-transmission speeds to support video calling and internet access. 4G was released in 2008 to support more demanding services such as gaming services, HD mobile TV, video conferencing, and 3D TV [13].

5G technology has been planned for the upcoming future. With IoT, even the physical objects (things) used for everyday life such as clothes, food will be connected via network, resulting in lots of information flow. The upload and download speeds on network can restrict our daily life and therefore, with a speed of up to 1 gigabit per second on wireless medium, 3G/4G is inevitably a part of IoT revolution giving easy and fast access, portability and reliability. 5G is the latest generation of cellular mobile communications. It succeeds the 4G (LTE-A, WiMax), 3G (UMTS, LTE) and 2G (GSM) systems. 5G performance targets high data rate, reduced latency, energy saving, cost reduction, higher system capacity, and massive device connectivity [8]. Fig.3 illustrates the cellular standards evolution.



2020	5G	3GPP, IEEE
2015 -	4G	LTE Rel 10, IEEE 802.16m
2001 - 2014	3G	EDGE, CDMA 2000, CDMA, IEEE 802.16e, HSPA+, LTE Rel 8
1991 - 2000	2G	GSM, IS-95A, IS-136, PDC, GPRS, HSCSD, IS-95B
1981	1G	AMPS, CDPO, CNETz, NMT, TACS

Fig 3. Evolution of mobile standards [8]

3.4 WIDE AREA NETWORK (WAN) is any telecommunication network or computer network that extends over a large geographical distance/place. Wide-area networks are often established with leased telecommunication circuits. Business, education and government entities use wide-area networks to relay data to staff, students, clients, buyers, and suppliers from various locations across the world. In essence, this mode of telecommunication allows a business to

effectively carry out its daily function regardless of location. The Internet may be considered a WAN.

The introduction of IoT has come up with challenges to traditional WAN. Digital transformation is exposing the long-standing challenges of the traditional WAN. The cost of MPLS and limited bandwidth, a lack of business agility, escalating complexity and outmoded security – all of these challenges and more mean the traditional WAN is not suited to an IoT-focused age. Software-defined WAN (SD-WAN) capabilities are addressing these challenges, making use of multiple WAN links, policy-based traffic steering and orchestration spanning the entire WAN – from fixed sites to IoT [14].

Atzori, Iera [15], however, tackles the technologies from a somewhat different perspective. [15] divides the enabling technologies into two categories: (a) Identification, sensing and communication technologies, where he discusses RFID systems (RFID), wireless sensor networks (WSN), and RFID Sensor Networks (RSN) and shows the application and advantages of each technology. (b) Middleware, which is “a multipurpose software that provides services to applications outside of what’s offered by the operating system. Any software between the kernel and user apps can be middleware.” [16].

The middleware is gaining more and more importance in the last years due to its major role in simplifying the development of new services and the integration of legacy technologies into new ones. The research performed by [15] shows that the middleware architectures for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex and monolithic systems into applications consisting of an ecosystem of simpler and well-defined components. This facilitates the interaction among the parts of an enterprise and allows for reducing the time necessary to adapt itself to the changes imposed by the market evolution [17].

4. IOT ARCHITECTURES

One of the main problems with the IoT is that it is so vast and such a broad concept that there is no proposed, uniform architecture [5]. Today’s Internet is using TCP/IP protocol stack for communication between network hosts which was proposed long time ago. However, the IoT connects billions of objects which will create much larger traffic, and much more data storage is needed [18]. Also, IoT will face many challenges specially related to privacy and security thus, the new proposed architecture for IoT needs to address many factors like scalability, interoperability, reliability etc. [7]. Since IoT connects everything and everyone to exchange information among themselves, the traffic and storage in the network will also increase in the exponential way. Thus, IoT development depends on the technology progress and design of various new applications and business models.

There are several published survey papers that cover different aspects of the IoT technology. For example, the survey by Atzori, Iera [15] covers the main communication enabling technologies, wired and wireless and the elements of wireless sensor networks (WSNs). Khan, Khan [7] address the IoT architecture and the challenges of developing and deploying IoT applications. Enabling technologies and application services using a centralized cloud vision are presented in [2]. From the pool of proposed models, the basic model suggested by [9] is a 3-layer architecture [19], [7], [20] consisting of the Application, Network, and Perception Layers. Fig. 4 illustrates this.



Fig. 4. The 3-layer architecture [9]

Ray [21] presents various domain specific architectures based on the broad areas, these areas as described by Marrocco, Occhiuzzi [22] are: RFID, service oriented architecture, wireless sensor network, supply chain management, industry, healthcare, smart city, logistics, connected living, big data, cloud computing, social computing, and security. Ray [21] surveys the architectures based on domain. In this context the survey is performed to evaluate a number of segregated sub domains to gain and provide significant knowledge on the following: architectural structure, applicability, associativity, deployability, and incorporation measure.

Khan, Khan [7] suggests a somewhat similar architecture where he proposes five layers of IoT: Perception Layer, Network Layer, Middleware Layer, Application Layer, and Business Layer. This is depicted in Fig. 5. The following sections briefly describe this.

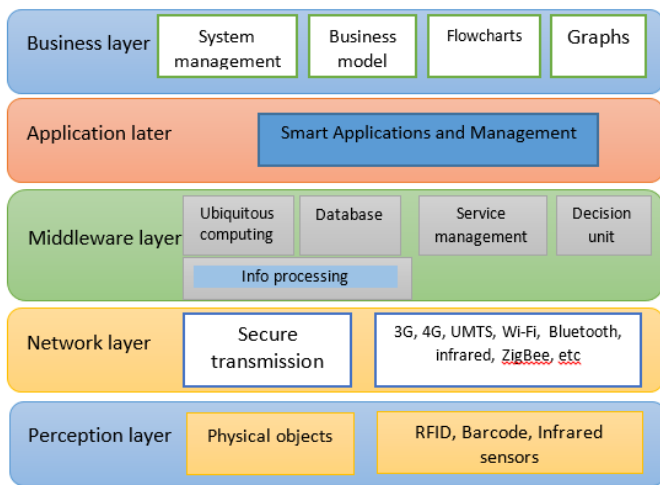


Fig. 5. The IoT Architecture

PERCEPTION LAYER: The Perception layer contains the physical objects and sensor devices. The sensors can be any of RFID, 2D-barcode, or Infrared sensor depending upon objects identification method. This layer is responsible for the identification and collection of information by the sensor devices. Depending on the type of sensors, the information can be about location, temperature, orientation, motion, vibration, acceleration, humidity, chemical changes in the air etc. [7]. The collected information is then passed to Network layer for its secure transmission to the information processing system.

NETWORK LAYER: The Network layer can also be called 'Transmission Layer'. This layer securely transfers the information from sensor devices to the information processing system. The transmission medium can be wired or wireless and technology can be 3G, 4G, UMTS, Wi-Fi, Bluetooth, infrared, ZigBee, etc. depending upon the sensor devices. Thus, the Network layer transfers the information from Perception layer to Middleware layer.

MIDDLEWARE LAYER: The devices over the IoT implement different type of services. This layer is responsible for the service management and has link to the database. It receives the information from Network layer and stores it in the database. It performs information processing and ubiquitous computation and takes automatic decision based on the results.

APPLICATION LAYER: This layer provides global management of the application based on the objects information processed in the Middleware layer. The applications implemented by IoT can be smart health, smart farming, smart home, smart city, intelligent transportation, etc.

BUSINESS LAYER: This layer is responsible for the management of overall IoT system including the applications and services. It builds business models, graphs, flowcharts etc based on the data received from Application layer. The real success of the IoT technology also depends on the good business models. Based on the analysis of results, this layer

will help to determine the future actions and business strategies [7].

Tyagi [23] proposes an architecture composed of five layers: Device layer, Object abstraction layer, Event Processing and Analytics layer, Business Layer and Service Management layer.

DEVICE/OBJECTS/PERCEPTION LAYER: is the bottom layer of the IoT architecture is the where sensors /actuators are present which gather and process information like temperature, location etc. and actuators to perform some actions. This layer digitizes and transfers data to the layer above it through secure channels.

OBJECT ABSTRACTION LAYER: this layer transfers data produced by the perception layer to the Service Management (cloud gateway) layer through secure channels. Indirectly connected devices are connected to cloud via a device gateway. Sensors usually have very limited capabilities in terms of networking connectivity. Sensors majorly utilize Bluetooth Low Energy (BLE) nowadays or are connected in a network using the ZigBee protocol.

SERVICE MANAGEMENT or Middleware layer pairs a service with its requester based on address and name. This layer enables the IoT application developers to work with heterogeneous objects without giving much consideration to a specific hardware platform. Also, this layer processes received data, makes decisions, and delivers the required services over the network wire protocols. The high range of scalability of the IoT requires a resource management mechanism that can register and determine resources and services in a dynamic, self-configured and efficient way. The most predominant service discovery protocols are DNS Service Discovery (DNS-SD) and multicast DNS (mDNS) that can discover services and resources offered by IoT devices.

EVENT PROCESSING AND ANALYTICS: This layer process and act upon the events. This layer first stores the data into a database. Then the data analytics task is carried out using big data analytics. Complex event processing to initiate near real-time activities and actions based on data from the devices and from the rest of the system.

EVENT PROCESSING AND ANALYTICS: This layer processes and acts upon the events by storing the data into a database, then the data analytics task is carried out. Processing complex events is performed to initiate near real-time activities and actions based on data from the devices.

BUSINESS LAYER: The business layer manages the overall IoT system activities and services. Business Layer supports decision-making processes based on Big Data analysis. In addition, monitoring and management of the underlying four layers is achieved at this layer. Moreover, this layer compares the output of each layer with the expected output to enhance services and maintain users' privacy.

5. CHALLENGES

The IoT has changed the shape of the Internet and offered vast economic and social benefits but it also faces many key challenges. Any new trend in technology in its early stages is faced by a number of challenges; the IoT industry is not an exception. Researchers have recognized many challenges associated with IoT. Agrawal and Das [6] brings eight key challenges that arise in IoT, these are: standards, privacy, identification and authentication, security, trust and ownership, integration, coordination and regulation. However, Khan, Khan [7] agree on the first four challenges and added these other challenges: data confidentiality and encryption, network security, spectrum and greening of IoT.

Data confidentiality and encryption: The sensor devices that perform sensing transfer data to the information processing unit over the transmission system, hence it should have proper encryption mechanism to guarantee the data integrity at the information processing unit. The IoT service determines who can see the data, thus it is necessary to guard the data from intruders.

Security: As in any communication network, the IoT is exposed to various kinds of vulnerabilities and security threats. In particular, security is a critical challenge for the IoT development, as it constitutes an extended version of the conventional unsecured Internet model and combines multiple technologies such as Wireless Sensor Networks (WSNs), optics networks, mobile broadband, and 2G/3G/4G communication networks. Each of the aforementioned technologies is prone to various security risks [24]. For the reasons above, many studies have examined the security issues in the IoT. Some of them determine the security requirements and challenges that the IoT generates. Other studies identify the possible threats, vulnerabilities and countermeasures [24]. Furthermore, many papers examine the security issues of the IoT protocols, while others focus on specific security mechanisms and processes that can mitigate the possible cyber-attacks [25]. Agrawal and Das [6] address this security issue in general, while Khan, Khan [7] divides it to: (a) the safety and security of physical objects dispersed over large geographical areas, and (b) network security: the data from sensor devices is sent over wired or wireless transmission network. The transmission system should be able to handle data from large number of sensor devices without causing any data loss due to network congestion, ensure proper security measures for the transmitted data and prevent it from external interference or monitoring.

Spectrum: The sensor devices will require dedicated spectrum to transmit data over the wireless medium. Due to limited spectrum availability, an efficient dynamic cognitive spectrum allocation mechanism is required to allow billions of sensors to communicate over the wireless medium [7].

Greening of IoT: The network energy consumption is increasing at very high rate due to increase in data rates, increase in the number of Internet-enabled services and rapid growth of Internet connected devices. The future IoT will cause significant increase in the network energy consumption. In order to have a sustainable smart world, the IoT should be depicted by energy efficiency to reduce the greenhouse effects and carbon dioxide (CO₂) emissions of sensors, devices, applications and services [26]. Thus, green technologies need to be adopted to make the network devices as energy efficient as possible.

According to Banafa [27] and Narayanan [28], to thrive and flourish, IoT industry has to overcome three categories of challenges: technology, business and society.

Technology

This part is covering all technologies needed to make IoT systems function smoothly as a standalone solution or part of existing systems. There are many technological challenges, including Security, Connectivity, Compatibility & Longevity, Standards and Intelligent Analysis & Actions, as shown in fig. 6.

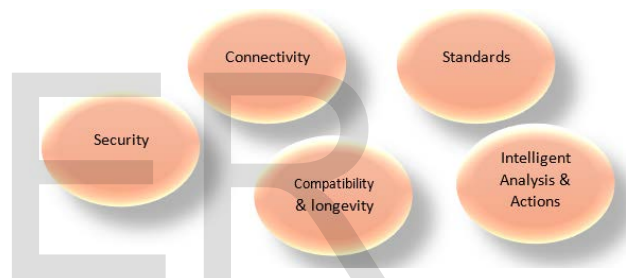


Fig. 6. Technological Challenges [27]

Business

A sound and solid business model for IoT must satisfy all the requirements for all kinds of e-commerce. End-to-end solution providers operating in vertical industries and delivering services using cloud analytics will be the most successful at monetizing a large portion of the value in IoT. In this context IoT can be divided into 3 categories, based on usage and clients base: Consumer IoT, Commercial IoT and Industrial IoT [27]. Each of these categories faces differing types of challenges. Fig. 7 illustrates this.

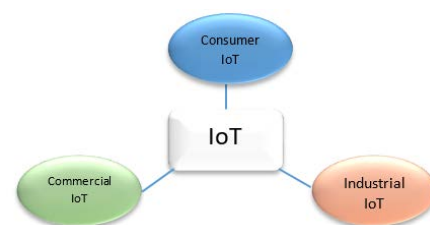


Fig. 7. Categories of IoT [27]

Society

From the customers and regulators prospective, it is not an easy task to understand IoT for the following reasons:

- Customer demands and requirements change constantly.
- New uses for devices — as well as new devices — grow at very high speeds.
- Inventing and reintegrating must-have features and capabilities are expensive and take time and resources.
- The uses for IoT technology are expanding and changing.
- Lack of understanding or education by consumers of best practices for IoT devices security to help in improving privacy, for example change default passwords of IoT devices.

Dickson [29] categorizes the threats and challenges facing IoT into four categories: Security Challenges, Privacy challenges, connectivity challenges and Compatibility challenges. These are described in the next sections.

Security Challenges: There are many reasons behind the state of insecurity in IoT. Some of it has to do with the industry focus on functionality and ignore security issues resulting in products that can easily be exploited remotely. Also many security solutions being used today have been created with generic computing devices in mind. IoT devices often lack the computational power, storage capacity and even proper operating system to be able to deploy such solutions.

Privacy Challenges: Some of the data that IoT devices collect are very sensitive and are protected by legislations, yet the necessary precautions aren't taken when storing the data or sharing it with other service providers. Another consideration to take is that while data generated about a single appliance might not be sensitive per-se, yet when combined with data from other devices, it can reveal information such as the consumer's life pattern, which can become very damaging if they fall into the hands of the wrong people.

Connectivity Challenges: Connecting so many devices will be one of the biggest challenges of the future of IoT. At present we rely on the centralized, server/client paradigm to authenticate, authorize and connect different nodes in a network. This model is sufficient for current IoT ecosystems, where tens, hundreds or even thousands of devices are involved. But when networks grow to join billions and hundreds of billions of devices, centralized brokered systems will turn into a bottleneck. Such systems will require huge investments and spending in maintaining cloud servers that can handle such large amounts of information exchange, and entire systems can go down if the server becomes unavailable.

The future of IoT will very much have to depend on decentralizing IoT networks. Part of it can become possible by moving functionality to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of time-critical operations and cloud servers take on

data gathering and analytical responsibilities. Other solutions involve the use of peer-to-peer communications, where devices identify and authenticate each other directly and exchange information without the involvement of a broker.

Compatibility and Longevity Challenges: As an industry that is going through its baby steps, IoT is growing in many different directions, with many different technologies competing to become the standard. For instance, we currently have ZigBee, Z-Wave, Wi-Fi, Bluetooth and Bluetooth Low Energy (BTLE) all vying to become the dominant transport mechanism between devices and hubs. This will cause difficulties and require the deployment of extra hardware and software when connecting devices. Other compatibility issues stem from non-unified cloud services, lack of standardized M2M protocols and diversities in firmware and operating systems among IoT devices [29].

6. CONCLUSION

The IoT paradigm has gone a long way since its inception by Kevin Ashton in 1999 until the present. Since then a great amount of research has been performed. This paper was an attempt to survey some of the salient research work done with a focus on some definitions on IoT, elements of IoT: Identification, Sensing, Communication, Computation, Services and Semantics. Furthermore, enabling technologies have been reported. This complex IoT path faces a plethora of challenges some of which have been reviewed from various standpoints in this paper. Most reviewed research focus on security, privacy and standardization as top challenges facing IoT. Future efforts are needed to address these challenges and this opens the door for a potential of serious research work to improve the quality of services in the field.

ACKNOWLEDGMENT

The authors wish to thank Dr. Mubarak Himmat of Future University, Sudan for his helpful guidance and useful comments.

REFERENCES

1. Aldeen, et al., New Trends in Internet of Things, Applications, Challenges, and Solutions. *Telkomnika*, 2018. 16(3): p. 1114-1119.
2. Gubbia, J., et al., Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 2013. 29: p. 1645-1660.
3. Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C., Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. *Advances in Internet of Things: Scientific Research*, 2011: p. 5-12.
4. H. Arasteh, V.H., A.T. V. Loia, O. Troisi, and P.S. M. Shafie-khah, *IoT-based Smart Cities: a Survey*, in

- 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), I.X.d. library, Editor. 2016, IEEE Xplore digital library: Florence, Italy. p. 1-6.
 5. Madakam, S., R. Ramaswamy, and S. Tripathi, Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 2015. Vol.03No.05: p. 10.
 6. Agrawal, S. and M.L. Das, Internet of Things – A Paradigm Shift of Future Internet Applications, N.U.I.C.o. Engineering, Editor. 2011, IEEE Xplore digital library: Ahmedabad, Gujarat, India.
 7. Khan, R., et al., Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. 2012 10th International Conference on Frontiers of Information Technology, Islamabad, 2012: p. 257-260.
 8. Global, T. 5g Technology Introduction. 2018.
 9. Al-Fuqaha, A., et al., Internet of things: A survey on enabling technologies, protocols, and applications. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2015. 17(4): p. 2347 - 2376.
 10. Rathor, K. and V.A. Prakashe, Implementation of RFID in the Libraries of Institutes of National Importance in India, in Proceedings of the International Academic Research Conference on Multiple Academic Disciplines, G.B. Research, Editor. 2018: New York, USA.
 11. Huang, C.-h., An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions. 2009, George Mason University, Electrical and Computer Engineering Department.
 12. Nanda, A., A.K. Rath, and S.K. Rout, Node Sensing & Dynamic Discovering Routes for Wireless Sensor Networks. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010, 2010. 7(3).
 13. secret-bases.co.uk. Mobile Technologies. secret-bases.co.uk; Available from: https://www.secret-bases.co.uk/wiki/Mobile_technologies.
 14. Johnson, D. Using wireless as a primary WAN link to accelerate IoT deployment. The Global Voice of Telecoms IT, 2019.
 15. Atzori, L., A. Iera, and G. Morabito, The Internet of Things: A survey. Computer Networks, 2010. 54(15): p. 2787-2805.
 16. redhat. What is Middleware? 2019 [cited 2019 March. 2019]; Available from: <https://www.redhat.com/en/topics/middleware/what-is-middleware>.
 17. Deugd, S.d., et al., SODA: service oriented device architecture. IEEE Pervasive Computing (Volume: 5 , Issue: 3 , July-Sept. 2006), 2006. 5(3).
 18. Tan, L. and N. Wang, Future Internet: The Internet of Things, in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). 2010, IEEE: Chengdu, China.
 19. Yang, Z., et al., Study and application on the architecture and key technologies for IOT, in 2011 International Conference on Multimedia Technology. 2011: Hangzhou, China. p. 747-751.
 20. Wu, M., et al., Research on the architecture of Internet of Things, in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). 2010, IEEE Xplore Digital Library.
 21. Ray, P.P., A survey on Internet of Things architectures. Journal of King Saud University –Computer and Information Sciences, 2016: p. 291-319.
 22. Marrocco, G., C. Occhiuzzi, and F. Amato, Sensor-oriented passive RFID, in The Internet of Things. Springer, G. D., et al., Editors. 2010, Springer, New York, NY: New York.
 23. Tyagi, N., A REFERENCE ARCHITECTURE For IoT. International Journal of Computer Engineering and Applications. X(I).
 24. Grammatikisa, P.I.R., P.G. Sarigiannidisa, and I.D. Moscholiosb, Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 2019. 5(March 2019): p. 41-70.
 25. Sicaria, S., et al., Security, privacy and trust in internet of things: The road ahead. Computer Networks, 2015.
 26. Albreem, M.A.M., et al., Green internet of things (IoT): An overview, in Conference: 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA 2017). 2017: Putrajaya, Malaysia.
 27. Banafa, A., Three Major Challenges Facing IoT. IEEE Internet of Things, 2017.
 28. Narayanan, K., Addressing The Challenges Facing IoT Adoption. Microwave Journal, 2017.
 29. Dickson, B., 4 Major Technical Challenges Facing IoT Developers. Sitepopint, 2016.
- *Mohamed Osman Elbashir is a lecturer in the computer science faculty in Future University – Sudan, currently pursuing PhD in Information Technology in Neelain University*
 - *Awad Haj Ali is a professor of computer science in Faculty of Computing Science and Information Technology, Neelain University, Khartoum, Sudan*