A Review on Internet of Things' Operating Systems, Platforms and Applications

Rebin B. Khoshnaw[1], Dana F. Doghramachi[2], Mazin S. Al-Hakeem[3]

[1] University of Salahaddin,[2]Erbil Polytechnique University,[3]Lebanese French University
Erbil, Kurdistan Region of Iraq
[1] rebin.saleh@su.edu.krd,[2]dana.farhad@epu.edu.krd,[3]dr.mazin@lfu.edu.krd

doi: 10.23918/iec2017.06

ABSTRACT

Internet of Things (IoT) refers to a prospective in which physical objects are used in our daily life are going to be connected to the Internet by appropriate mode of information and communication technologies, but far from traditional desktop environment. The aim of IoT is to create a better world for human beings using a common infrastructure to conjugate everything in our world. This will make us to control of these objects and keep letting us about their state.
Enormous number of devises are participating in this technology, therefore, the security challenges play a vital role while adapting IoT. This paper provides an overview of IoT with emphasis on state of art review on operating systems, platforms and application domains. The IoT architecture and security challenges are presented as well.

Keywords: Internet of Things (IoT), Platforms, Operating System, Application, IoT Security.

1. INTRODUCTION

With the rapidly growing of use Internet - i.e. for sending and receiving email messages, interacting with people via social networking applications, sharing large amount of data, transacting the financial business, playing games, analyzing data and summarizing it and many others -; there are another big area of use Internet begins to emerge as a global platform for allowing the machines, smart devices and electronic objects to communicate, compute and coordinate using Internet as a universal podium.

Nowadays, Internet is available as a non-stitching component of objects on networks. This has led content and services be available around us 24/7. This in turn has provided us a modern style of working and living as well as new ways of amusement. Soon, the concept of having internet as an infrastructure will vanish and will lead to existing a gap in the area of connecting smart objects. These objects form an environment which is called pervasive computing environment [1].

The infrastructure of Internet will be used as universal backbone which plays an important role for sharing information and interconnection of physical objects with communication capacities. To enable this modernization, smart objects have to be made by embedding electronics with everyday physical objects. This will provide a wide range of new services and technologies. This new idea was proposed by Kevin Ashton, the co-founder of AutoID and named it as Internet of Things (IoT) [2, 3].

This term was first used in 1999 by Kevin Ashton [4]. IoT is defined as "the network of physical objects or "things" embedded with electronic devices, software technologies, sensors, and network connectivity, which facilitates these objects to collect and exchange data for availing various services" [5]. The motivation behind IoT is to create

Smart city [6] that aimed "create a better world for human beings" by optimize use of public resources, increase the quality of services offered to people and decrease the operational costs of the services, where objects around us know what we like, what we want and what we need and act accordingly without explicit instructions [7]. It could simply be said that the concept of IoT is essentially connecting physical objects to the internet with the capability of switching it on and off. These objects includes Nano and micro devices such as smart mobile phones, smart homes, washing machines, tea making devices, headphones wearable devices, lamps and anything that will come to minds. Sreekanth et al in [5] says that by 2020, there will over 26 billion objects connected to each other. This will make a huge network of connected objects (things).

The significant ideas behind this paper are to make a comprehensive and analytical review on the Operating Systems domain as well as Platforms and Applications of IoT.

As a matter of fact, the community doing research around IoT focuses on a single aspect of IoT whether it is operating system, platforms or application domain. Authors believe that there are no critical review done which contain all the above mentioned aspects of IoT, hence makes a gap in this research area. Therefore, the scientific contribution of this paper will help filling the gap by critically reviewing most common operating systems and platforms as well as most popular application domains.

For that, this paper presented in the following structure. In the next section, the literature survey will be presented. The IoT ITU architecture will be followed. This is followed by the IoT Operating Systems, IoT Platforms and IoT Applications.The security challenges of IoT will be followed. The paper ends with a conclusions section.

2. LITERATURE SURVEY

One of the IoT's capability is making homes and life smarter. IoT provides us a convenience security, comfort, activities of the everyday life. Sick and elderly people can also get benefit from IoT either by having smart home which increases quality of life[8]. Most of the research attention is on how to embed intelligence into the environment using technologies such as RFID, Wi-Fi, cellular networks and Bluetooth. Researchers approached to controlling home appliances and devices using remote access and network interoperability using gateways of homes. This was the introduction of using web servers based on PCs using Wi-Fi based systems[9].

IoT referred to a general term that cover the entire scope to which the Internet and web has spread through the physical realm, in which devices placed are spread and embedded into objects. In order to identify them, enhanced sensing capabilities are used[1]. Tan and Wang in [10] mention that in near future, every physical object will have a unique identification used to interconnect and form IoT. As a result, communications will take a new way from human to human to human and things. Identification of physical objects will be based on RFID and other sensing devices (IoT Enabling Technologies) in IoT environment.

Research studies regarding technology development have advanced qualitatively, specifically in understanding how technologies advanced from public domain to private space of homes. Authors Gaglio and Lo in [11] argue that IoT is the transformation process from cold products to eligible home applications. Based on the architecture and frameworks desirable in IoT environment, for most of IoT technologies, it is required to have governmental, commercial, and individual cooperation and agreements.

The retrieved data from objects could be used to understand both individual and home appliance behavior. One of the most common use of IoT is monitoring and awareness

of objects and individuals. Although this is a bright side of IoT for work place managers and parents, Gubbi et al in [12] monitoring and surveillance will increase the tension between parents and their children as well as between employer and employee.
Gubbi et al reached this conclusion after monitoring blood glucose level in children when monitored by parents.

IoT is also used in the field of caring elderly individuals in remote monitoring and direct assistance. It is difficult for care givers to monitor for long periods in order to make sure the elder person is safe and the elder person prefers area without surveillance technology. Atzori et al in [13] reviews several aspects of IoT. He reports different paradigm of IoT and several enabling technologies. Zanella et al in [14] focus on urban IoT system. Enabling technologies required in urban IoT system are also discussed in their paper. Al Fuqaha et al in their review paper discusses the latest technologies protocols and applications around IoT era [15]. They found that IoT can automate almost everything in world. They have also reported challenges and issues which pertain to the design and deployment of IoT implementations which they have presented in their review paper. Al –Fuqaha et al used use-cases to show typical protocol integration scenarios for service delivery of IoT. Bhumi and Tushar in [16]studied various IoT platforms. In their study, Bhmui and Tushar found that for IoT solution development, Microsoft Azure and ThingWorxs compared to others are the most favorable platforms and ThingSpeak is mainly used to provide analytics of data and its visualization. Kang et al studied various IoT applications [17]. Debasis et al in [18] reviewed state-of-art IoT applications, challenges and showed the future research area in the application domains of IoT.

3. IOT ARCHITECTURE

There have been several architectures for IoT systems. Standards regarding architecture have been issued by International Telecommunication Union (ITU), European FP7, Qian Xiaocong, IoT forum, Kun Han, Shurong Liu, Dacheng Zhang, Ying Han and Zhang Jidong's architecture[19]. Based on several review papers which is mentioned in [20, 21], it is generally divided into six layers which are Collaboration and Processes, Application, Data Abstraction, Data accumulation, Esge Computing, Connectivity and Physical devices and controllers. The architecture mentioned has become a standard for developing IoT architecture and is illustrated in figure 1. Study around IoT architecture is growing and new models are presented each day with the growth of Internet. There are several development efforts regarding models of IoT architecture such as ITU-IT model, smart grid's NIST model, ARM from EU IoT- A and Machine to Machine from ETSI[21].

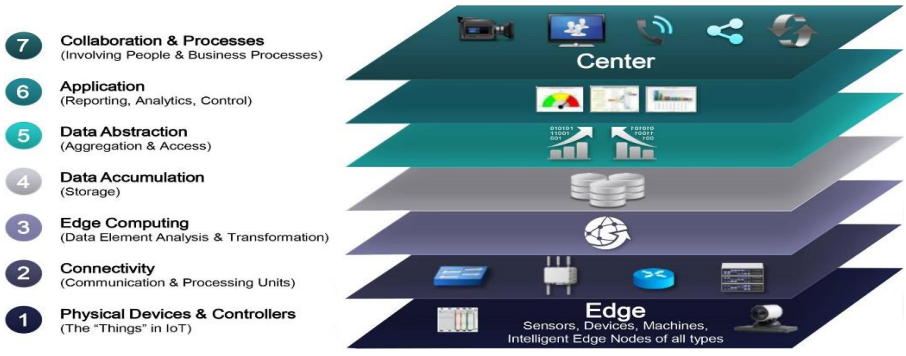

FIGURE 1. IoT ITU Architecture Model [22]

4. IOT OPERATING SYSTEMS

Using internet infrastructure, several IoT devices have been integrated with various objects through interaction between wireless sensor network and Radio Frequency Identifications (RFID) technology with software. This interaction has been available by having an operating system running behind. Each IoT device will be a useless and a non-functioning device without operating system. Hahm et al in [23] have studied several IoT operating systems for low-end devices. In a survey conducted by Eclipse IoT working group, IEEE IoT and Agile IoT, it was found that 73.1% of people who has devices on IoT use Linux Operating system and second most popular OS was freeRTOS [24]. Several different operating system have been listed in Table 1. Both RIOT and Linux support C and C++ language and fully support multi-threading. Android OS different from others support Java language. Minimum RAM and Min ROM criteria also been used in listing below IoT operating systems.

TABLE 1.
IoT Operating Systems [10, 13, 23]

Operating System	Min RAM	Min ROM	Multi-Threading	Support language
FreeRTOS	< 10 KB	< 12 KB	Full support	C
Contiki	< 2 KB	< 30 KB	Partial support	C
RIOT	~ 1.5 KB	~ 5 KB	Full support	C, C++
Tiny OS	< 1 KB	< 4 KB	Partial support	C
nuttX	32KB	-	Full support	C
Open WSN	-	-	Partial support	C
Nut/OS	-	20 KB	Full support	C
Linux	~1MB	~1MB	Full support	C, C++
Android	-	-	Full support	Java
LiteOS	4 KB	-	Full support	C

5. IOT PLATFORMS

IoT applications can be built using IoT platforms which support general information system functionalities. These functionalities are application independent. Castro et al in [25] analyze several machine to machine (M2M) platforms using inaugural approach. Several different platforms are listed in Table 2 according to several criteria such as scalability, availability, security and privacy provisioning and number of device supported. Axeda and IBM, Azure, and ThingWorx can be seen that they are most popular platforms based on the criteria mentioned. Nimbits and ThingSpeak do not have the ability to support more than a million devices.

TABLE 2.
Platforms for Internet of Things [16, 20, 25]

Platform	Scalability	Availability 24 * 7	Security and privacy provisioning	Support for millions of devices
Axeda Oracle java Embedded	Yes	Yes	Yes	Yes
IBM Blue Mix	Yes	Yes	Yes	Yes
Nimbits	Yes	Yes	No	No
Thing Worx	Yes	Yes	Yes	Yes
Microsoft Azure	Yes	Yes	Yes	Yes
Thing Speak	Yes	Yes	No	No
Sensor cloud--	Yes	Yes	Yes	--
Digital Service Cloud	Yes	Yes	Yes	Yes
Yaler	Yes	Yes	No	No
Xively	Yes	Yes	Yes	Yes
Amazon web service	Yes	Yes	Yes	Yes
Google Cloud Compute	Yes	Yes	Yes	Yes
Zetta	No	Yes	No	No

TABLE 3.
IoT Applications [8, 14, 15, 18]

Application Domain	Technology / Technique	Strengths/ Benefits	Weaknesses
Smart Aerospace and aviation	RFID tags	Safety and operational reliability of aircrafts can be significantly improved	Suspected unapproved parts
Smart Transportation	DSRC, RFID, accelerometer, smart phone, GPS	Reduces cost by using smart phone as a connector device.	Ease of security attack
Smart Tele-communications	GSM, NFC, low power Bluetooth, WLAN, multi-hop networks, GPS and sensor networks together with SIM-card	High Security	/
Smart Medical and healthcare	• Basic data of patient will be stored in server for comparison. •RFID, Internet, mobile network, camera, microphones and other equipment.	• Provides options for both Internet and mobile network. • Convenient to users.	High computation cost for patient parameter comparison Time consuming and threshold dependable.
Smart City	RFID,NFC and Sensor network	•Control over light, water and other resources in a city •Traffic light control	Network failure due to security attack
Smart House	Smart phone Sensors (Heat, Light), NFC, Bluetooth	•Household appliance controlling, •Distance learning, •Energy saving	/
Smart Agriculture	WLAN, Sensors and RFID	•Real time detection of animals, •Delivering crops directly to consumers •Managing quality	/

6. IOT APPLICATIONS

According to a survey conducted by Internet of Things European Research Cluster (IERC) [26], the IoT applications can be categorized into twelve different application domains such as Transportation, smart city, smart home, agriculture, communication, health, supply chain and logistics, environment and energy, utilities, wearables, smart industry and manufacturing, and smart grids. Table 3 lists some of the application domains including their technology and strength points/benefits as well as their weaknesses if applicable. Most of the application's technology is Radio Frequency Identifier RFID plus sensors. Using these two technologies data are sensed, collected and transmitted to the control center.

7. SECURITY CHALLENGES OF IOT

There have been different challenges and vulnerabilities around IoT environment and this is due to the connectivity with the Internet and as it is obvious the main issue of Internet is its security.

One of the challenges facing IoT is Denial of Service (DoS) attacks. When devices get IP addresses and contribute in a pool of things, they may recruit to a platform as Network bots, hence can be used for sending massive amount of traffic which is known as distributed attacks. Yan in [27] reports that attackers use DoS to hijack sensors, cameras, printers and routers which are not secured and using them to attack third parties. Identifying and controlling botnets are difficult and challenging.

Another challenge which makes a great concern in IoT, is Eavesdropping which passively attacking networks and retrieving data from the information flow though communication channels such as wired and wireless networks. Data is shared among devices in IoT environment hence the shared information could take a slippery slope. It is more important to focus on caution than data ownership in IoT environment, says Tan and Wang in [10].

Securing Sensors physically is another issue in IoT devices [28]. Physical attacks can make sensors permanently inoperable or physically destroyed. An attacker could penetrate into a house installed with sensors. The attacker will use signal detection device to find place of sensors and then steal, disable or destroy it.

Al-Hamami and Al-Hakeem in [29] have addressed seven issues that related to increase the level of IoT security, these are End-to-End Security Mechanisms, End-to-End Data Encryption, Access and Authorization Control, Activity Auditing, Hardened Cloud Infrastructure, Equal Protection across Multiple protocols and users security and privacy education.

8. CONCLUSION

The followings are some points derived from the comprehensive and analytical review on IoT's Operating Systems, Platforms and Applications:

a. Although the studies around IoT architecture is growing and new models are presented each day with the growth of Internet. But the ITU-IT model that issued by International Telecommunication Union (ITU) still is the standard.
b. There should be aware towards the suitable programming language that use to developing IoT operating system. Nowadays, most of IoT Operating Systems are fully supporting multi-threading, and most of people who have devices on IoT use Linux Operating System and most second popular OS was freeRTOS then

Android, both RTOS and Linux support C and C++ languages while Android OS support Java language.

c. The scalability, availability, security and privacy provisioning and number of devices supported are the main criteria that should take into consideration when developing a new IoT platform or when enhancing any existing one.
d. Set of supporting technologies such as RFIDs, sensor/ actuators, etc. are the main technologies which are used to develop applications.
e. The traditional security services are not directly applied on IoT due to the devices running on different platforms and uses different protocols to communicate, especially when the wireless or wire system need to communicate with other devices without human. There is a need for a new framework to apply the security services on IoT environment.
f. Biometric sensors can be used instead of RFID sensors to add a level of personality-authentication for Certification Authority. Also the cryptographic techniques can be used to add a level of confidentiality for the implemented security services.
g. The comprehensive and analytical review in this paper opens the door for researchers as a future works to implement or improving many Operating Systems, Frameworks or Applications which deals with security threats in IoT environment.

REFERENCES

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, pp. 1497-1516, 2012.
[2] S. Santhi, P. Rajendra, and Y. Vijayalakshmi, "A review on the state of art of Internet of Things " International Journal of Advanced Research in Computer and Communication Engineering(IJARCEE), vol. 5, July 2016.
[3] D. V. Dimitrov, "Medical Internet of Things and Big Data in Healthcare," Healthcare Informatics Research, vol. 22, pp. 156-163, 2016.
[4] O. Vermesan and P. Friess. (2014). Internet of Things- From Research and Innovation to Market Deployment.
[5] K. Sreekanth and K. Nitha, "A Study on Health Care in Internet of Things," International Journal on Recent and Innovation Trends in Computing and Communication(IJRTCC), vol. 4, February 2016.
[6] C. Perera and C. Zaslavsky, "Improve the Sustainability of Internet of Things Through Trading-based Value Creation," in Proceedings of the IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 2014, pp. 135-140.
[7] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things(IoT)," presented at the IEEE Internet Initiative, 2015.
[8] H. Ning and S. Hu, "Technology classification, industry, and education for Future Internet of Things," Int. J. Commun. Syst., vol. 25, pp. 1230-1241, 2012.
[9] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the internet of things," IEEE Internet Computing, vol. 14, pp. 46-53, 2010.
[10] T. Lu and W. Neng, "Future internet: The Internet of Things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V5-376-V5-380.
[11] S. Gaglio and G. Lo Re. (2014). Advances onto the Internet of Things : how ontologies make the Internet of Things meaningful. 260.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, pp. 1645-1660, 2013.
[13] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, pp. 2787-2805, 2010.
[14] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, pp. 22-32, 2014.
[15] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.
[16] B. Nakhuva, STUDY OF VARIOUS INTERNET OF THINGS PLATFORMS: Academy & Industry Research Collaboration Center (AIRCC), 2015.
[17] M.-R. H. K.-S. H. J.-B. K. Young-Mo Kang, "A Study on the Internet of Things (IoT) Applications," International Journal of Software Engineering and Its Applications, vol. 9, pp. 117-126, 2015.
[18] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," Wireless Personal Communications, vol. 58, pp. 49-69, 2011.
[19] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," Journal of Computer and Communications, vol. 3, pp. 164-173, 2015.
[20] L. Afifa and T. Priyambodo, "Review on Internet of Things " International Journal of Research and Applications, vol. 113, 2016.
[21] M. Zhang, F. Sun , and X. Cheng, "Architecture of Internet of Things and Its Key Technology Integration Based-On RFID," presented at the Fifth International Symposium Computer Intelligence Design, 2012.
[22] P. Biggs, J. Garrity , and C. LaSalle, "Harnessing the Internet of Things for Global Development," 2015.
[23] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating Systems for Low-End Devices in the Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 3, pp. 720-734, 2016.
[24] Eclipse, IEEEIoT, and AgileIoT, "IoT Developer Survey," 2016.
[25] M. Castro, A. J. Jara, and A. F. Skarmeta, "An Analysis of M2M Platforms: Challenges and Opportunities for the Internet of Things," in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp. 757-762.
[26] I. o. T. IERC and E. R. Cluster, The Internet of Things 2012 - New Horizons, 3rd ed. Halifax, UK, 2012.
[27] L. Yan, The Internet of things: From RFID to the next-generation pervasive networked systems. New York: Auerbach Publications, 2012.
[28] S. Das, K. Kant, and N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure: Morgan Kaufmann, 2012.
[29] M. S. Al-Hakeem and A. Al-Hamami, Everything about Internet of Things and Smart Cities Applications. Jordan: Dar al Raya for Publication and Distribution, 2016.