ISSN 2581-3463

AJMS
Asian Journal of Mathematical Sciences

CASE STUDY

Hardware/Software Interoperability and Single Point Vulnerability Problems of Internet of Things Multiple Systems: Causes, Solution and Societal Adoption

Rotimi-Williams Bello, Firstman Noah Otobo

Department of Mathematical Sciences, University of Africa, Toru-Orua, Bayelsa State, Nigeria

Received: 10-02-2018; Revised: 20-03-2018; Accepted: 10-04-2018

ABSTRACT

As reiterated by many authors, internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. This is made possible by the communications models with the enabling technologies which make communications possible among IoT connected devices, although, with drawbacks. These drawbacks are the major reasons for adoption problems of IoT services by the society. This paper carried out an investigative study on previous works on the societal applications and adoption problems of IoT, IoT communications models, and pros and cons of IoT. Through the study, it was revealed that for IoT devices and services to be widely adopted with no or minimal problems, future IoT technology will not only address the known drawbacks but also will require hardware and software components that are highly interoperable, dependable, reconfigurable, and, in many applications, certifiable.

Key words: Internet of Things, communications models, Internet of things devices, societal applications, technology

INTRODUCTION

The term IoT generally refers to scenarios where network connectivity and computing capability extend to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human interventions. There is, however, no single, universal definition. The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. IoT can be compared to cyber-physical system; a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to have a networked of physical devices embedded with electronics, software, sensors, actuators, and connectivity which enables the physical devices to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions is a key technological debate. The recent confluence of several technology market trends, however, is bringing the IoT closer to widespread reality. These include ubiquitous connectivity, widespread adoption of IP-based networking, computing economics, miniaturization, advances in data analytics, and the rise of cloud computing. IoT implementations use different technical communications models (device to device (D2D), device to cloud, device to gateway, and back-end data-sharing). These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user, each with its own characteristics. Despite a shared belief in the potential of IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Among the barriers are the desire to have IoT hardware and software components that are highly interoperable, dependable, reconfigurable, and,

Address for correspondence:
Rotimi-Williams Bello,
E-mail: sirbrw@yahoo.com

in many applications, certifiable. It is on this note that an investigative study on previous works on the societal applications and adoption problems of IoT services was carried out in this paper. Not only did this paper address IoT problems but also it proffered a validation and verification need for a better IoT.

RELATED WORKS

IoT definition has worked out due to convergence of artificial intelligence, cyber-physical systems, machine learning, and embedded systems, etc. The concept of a network of smart devices was discussed as early as the 1980s, with a modified coke machine at Carnegie Mellon University becoming the first internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century," as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT.[1,2] In 1994, Reza Raji described the concept in IEEE Spectrum as "moving small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories."[3] Between 1993 and 1996, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned D2D communication as part of his "six webs" framework, presented at the World Economic Forum at Davos in 1999.[4] The term "Internet of Things" (IoT) was likely coined by Kevin Ashton of Procter and Gamble, later MIT's Auto-ID Center, in 1999,[5] though he prefers the phrase "IoT." At that point, he viewed radiofrequency identification (RFID) as essential to the IoT,[6] which would allow computers to manage all individual things.[7-9] A research article mentioning the IoT was submitted to the conference for Nordic Researchers in Logistics, Norway, in June 2002,[10] which was preceded by an article published in Finnish in January 2002.[11] The implementation described that there was developed by Kary Främling and his team at Helsinki University of Technology and more closely matches the modern one, that is, an information system infrastructure for implementing smart, connected objects.[12] Defining the IoT as "simply the point in time when more 'things or objects' were connected to the Internet than people," Cisco Systems estimated that IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.[13] The basic communication models of IoT demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. Moreover, in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems. From a general user perspective, these communication models help illustrate the ability of networked devices to add value to the end user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. Often, however, these devices use protocols such as Bluetooth, Z-Wave, or ZigBee to establish direct D2D communications, as shown in Figure 1. These D2D 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 to communicate between devices with relatively low data rate requirements. Residential IoT devices such as light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other in a home automation scenario. This D2D communication approach illustrates many of the interoperability challenges. These devices often have a direct relationship, they usually have built-in security and trust mechanisms, but they also use device-specific data models that require redundant development efforts by device manufacturers.[14] This means that the device manufacturers need to invest in development

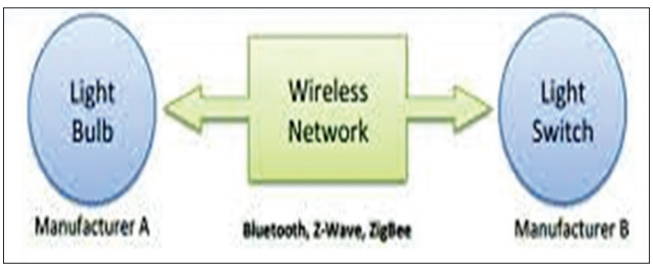

Figure 1: Device-to-device communications model

efforts to implement device-specific data formats rather than open approaches that enable the use of standard data formats.

In a device-to-cloud communication model [Figure 2], 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 such as 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 communication model is employed by some popular consumer IoT devices such as the Nest Labs Learning Thermostat and the Samsung smart television (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.

The device-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 data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in," a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated. 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 intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 3. 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 the model 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 forms of this device-to-gateway model are the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the smart things hub is a stand-alone gateway device that has Z-Wave and ZigBee transceivers installed to communicate with both families of devices. It then connects to the smart things cloud service, allowing the user to gain access to the devices using a smartphone app and an internet connection. This communication model is used in situations where the smart objects require interoperability with non-internet protocol

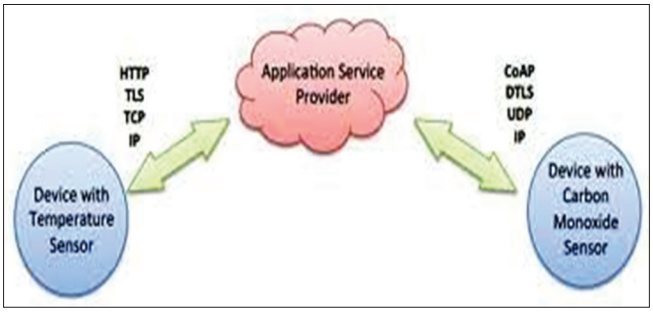

Figure 2: Device-to-cloud communications model

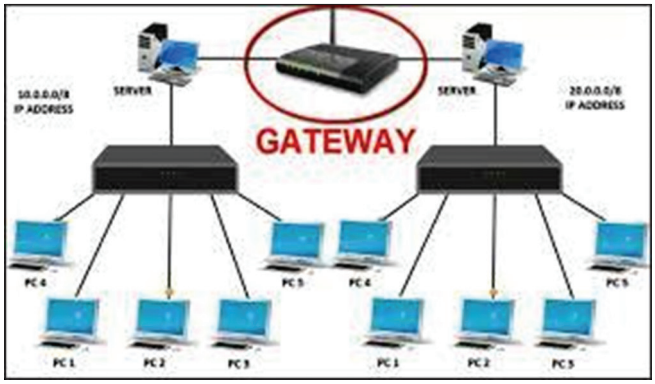

Figure 3: Device-to-gateway communications model

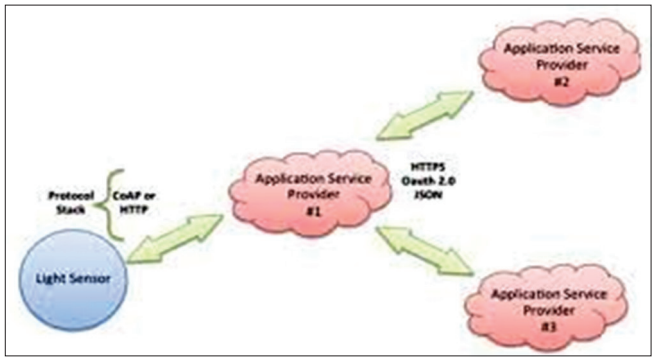

Figure 4: Back-end data-sharing communications model

(IP) devices. Sometimes, this approach is taken for integrating IPv6-only devices, which means a gateway is necessary for legacy IPv4-only devices and services. 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 the necessary development of the application layer gateway software and system adds complexity and cost to the overall system.

The back-end data-sharing model refers to a communication architecture that enables user to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture 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 back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed as shown in Figure 4. Effective back-end data-sharing 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 are needed to achieve interoperability of smart device data hosted in the cloud. This architecture model is an approach to achieve interoperability among these back-end systems. "Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors." In other words, this communication model is only as effective as the underlying IoT system designs. Back-end data-sharing architectures cannot fully overcome closed system designs.

COMMUNICATION MODELS ENABLING TECHNOLOGIES

(1) Addressability: The original idea of the auto-id center is based on RFID-tags and unique identification through the electronic product code; however, this has evolved into objects having an IP address or URI. An alternative view, from the world of the semantic web,[15] focuses instead on making all things addressable by the existing naming protocols such as URI. The objects themselves do not converse, but they may now be referred to by other agents such as powerful centralized servers acting for their human owners. Integration with the internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the IP (IPv6) to scale to the extremely large address space required.,[16-18] IoT devices additionally will benefit from the stateless address autoconfiguration present in IPv6,[19] as it reduces the configuration overhead on the hosts, and the IETF 6lowpersonal area networks header compression. To a large extent, the future of the IoT will not be possible without the support of IPv6, and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future.[18] (2) Short-range wireless: Bluetooth mesh networking specification providing a mesh networking variant to bluetooth low energy with increased number of nodes and standardized application layer (Models). (a) Light Fidelity - wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth. (b) Near-field communication - communication protocols enabling two electronic devices to communicate within a 4 cm range. (c) QR codes and barcodes - machine-readable optical tags that store information about the item to which they are attached. (d) RFID - technology using electromagnetic fields to read data stored in tags embedded in other items. (e) Thread - network protocol based on the IEEE 802.15.4 standard, similar to ZigBee, providing IPv6 addressing. (f) Transport Layer Security - network security protocol. (g) Wi-Fi - technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point or directly between individual devices. (h) Z-Wave - communication protocol providing short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi. This technology is used primarily for home automation. (i) ZigBee - communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low-power consumption, low data rate, low cost, and high throughput. (3) Medium-range wireless: (a) HaLow - variant of

the Wi-Fi standard providing extended range for low-power communication at a lower data rate and (b) LTE-advanced - high-speed communication specification for mobile networks. It provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency. (4) Long-range wireless: (a) Low-power wide-area networking (LPWAN) - wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, and Weightless, (b) very small aperture terminal - satellite communication technology using small dish antennas for narrowband and broadband data, and (c) long-range Wi-Fi connectivity. (5) Wired: (a) Ethernet - general purpose networking standard using twisted pair and fiber-optic links in conjunction with hubs or switches, (b) Multimedia over Coax Alliance - specification enabling whole-home distribution of high definition video and content over existing coaxial cabling, and (c) power line communication (PLC) - communication technology using electrical wiring to carry power and data. Specifications such as HomePlug or G.hn utilize PLC for networking IoT devices.

APPLICATIONS AND ADOPTION PROBLEMS OF IoT

The extensive set of applications for IoT devices [20] is often divided into consumer, enterprise (business), and infrastructure spaces.[21] (1) Consumer applications: A growing portion of IoT devices is created for consumer use, including connected vehicles, home automation/smart home, wearable technology, connected health, and appliances with remote monitoring capabilities.(a) IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media, and security systems.[22] Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off. (2) Enterprise applications: The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that EIoT will account for 9.1 billion devices. (3) Infrastructure applications: Monitoring and controlling operations of sustainable urban and rural infrastructures such as bridges, railway tracks, on- and off-shore wind farms are a key applications of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. IoT can benefit the construction industry by cost saving, time reduction, better quality workday, paperless workflow, and increase in productivity. It can help in taking faster decisions and save money with real-time data analytics. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities.[23] IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, uptimes, and reduce costs of operation in all infrastructure related areas.[24] Even areas such as waste management can benefit [25] from automation and optimization that could be brought in by the IoT. Other areas that make use of IoT devices for infrastructural applications are manufacturing, agriculture, energy management, environmental monitoring, building, and home automation. Other fields of applications are medical and health care, and transportation. As we note in the principles that guide our work, ensuring the security, reliability, resilience, and stability of internet applications and services is critical to promoting trust and use of the internet. As users of the internet, we need to have a high degree of trust that the internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The IoT is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people do not believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector. As we increasingly connect devices to the internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattack by allowing malicious individuals to reprogram a device or cause it to malfunction. Poorly designed

devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and ubiquitous smart devices in the IoT as they are for the computers that have traditionally been the endpoints of internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security, and long-term maintainability vulnerabilities greater than their traditional computer counterparts. Along with potential security design deficiencies, the sheer increase in the number, and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the internet globally, not just locally. To complicate matters, our ability to function in our daily activities without using devices or systems that are internet-enabled is likely to decrease in a hyperconnected world. In fact, it is increasingly difficult to purchase some devices that are not internet connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps, we could unplug our internet-connected TVs if they get compromised in a cyberattack, but we cannot so easily turn off a smart utility power meter or a traffic control system or a person's implanted pacemaker if they fall victim to malicious behavior. This is why security of IoT devices and services are a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact. Innovative approaches to abstraction and architectures that enable seamless integration of control, communication, and computation must be developed for rapid design and deployment of IoT. For example, in communication networks, interfaces have been standardized between different layers. Once these interfaces have been established, the modularity allows specialized developments in each layer. The overall design allows heterogeneous systems to be composed in plug and play fashion, opening opportunities for innovation, and massive proliferation of technology and the development of the internet. However, the existing science and engineering base do not support routine, efficient, robust, modular design, and development of IoT. Standardized abstractions and architectures are urgently needed to fully support integration and interoperability and spur similar innovations in IoT.[26]

CONCLUSION

This paper through literature review studied IoT, communications models, communications models enabling technologies, and the applicability of IoT in the society. The societal adoption problems of IoT were also reviewed in the course of the study. Since one of the key drivers of the IoT is data, this means that the success of the idea of connecting devices to make them more efficient is dependent on access to and storage and processing of data. For this purpose, companies working on IoT collect data from multiple sources and store it in their cloud network for further processing just the way automobile manufacturers collect components from multiple vendors. This leaves the door wide open for interoperability problem, privacy and security dangers, and single point vulnerability of multiple systems. After considering IoT in detail and subject to analysis, it was discovered that the hardware and software components, middleware, and operating systems of IoT devices need to be developed that go beyond existing technologies. The hardware and software must be highly dependable, reconfigurable, and, where required, certifiable, from components to fully integrated systems. Such complex systems must possess a trustworthiness that is lacking in many of today's IoT infrastructures.

REFERENCES

1. Friedemann M, Christian F. From the internet of computer to the internet of things. Inform Spektrum 2010;33:107-21.
2. Mark W. The computer for the 21st century. Sci Am 1991;265:94-104.
3. Raji RS. Smart Networks for Control. IEEE Spectrum Magazine; 1994.
4. Jason P. ETC: Bill Joy's Six Webs. MIT Technology Review Magazine; 2013.
5. Ashton K. That 'internet of things' thing. RFID J

2009;22:97-144.
6. Magrassi P. Why a Universal RFID Infrastructure Would Be a Good Thing. Gartner Research Report G00106518; 2002.
7. Magrassi P, Berg T. A World of Smart Objects. Gartner Research Report R-17-2243; 2002.
8. Commission of the European Communities. Internet of Things-an action plan for Europe. COM, 278 Final. Brussels: European Union; 2009.
9. Alex W. The Internet of Things is Revolutionizing Our Lives, But Standards are a Must. The Guardian; 2015.
10. Eero H, John G, Kary F. In: Olav S, editor. Tracking and Tracing Parcels Using a Distributed Computing Approach. Trondheim, Norway: Proceedings of the 14th Annual Conference for Nordic Researchers in Logistics (NOFOMA'2002); 2002. p. 12-4, 29-43.
11. Kary F. Tracking of Material Flow by an Internet-Based Product Data Management System (in Finnish: Tavaravirran Seuranta Osana Internet-Pohjaista Tuotetiedon Hallintaa). Tieke EDISTY Magazine, No. 1, 2002. Finland: Publication of Tieke (Finnish Information Society Development Centre); 2002. p. 24-5.
12. Kary F, Jan H, Timo A, Mikko K. Product Agents for Handling Information about Physical Objects. Report of Laboratory of Information Processing Science Series B, TKO-B 153/03, Helsinki University of Technology; 2003. p. 20.
13. Evans D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. San Jose, CA, USA: CISCO White Paper; 2011.
14. Carolyn DM. IAB releases guidelines for internet-of-things developers. IETF J 2015;11:6-8.
15. Hassan QF. Internet of Things A to Z: Technologies and Applications. Hoboken, New Jersey, USA: John Wiley and Sons; 2018. p. 27-8.
16. Sheng M, Qun Y, Yao L, Benatallah B. Managing the Web of Things: Linking the Real World to the Web. Elsevier, Cambridge: Morgan Kaufmann; 2017. p. 256-8.
17. Jean-Baptiste W. Nano Computers and Swarm Intelligence. London: ISTE; 2008. p. 227-31.
18. Kushalnagar N, Montenegro G, Schumacher C. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. IETF, RFC 4919; 2007. DOI: 10.17487/RFC 4919.
19. Charles CS. Stop using Internet Protocol Version 4! Computerworld Magazine; 2014.
20. Vongsingthong S, Smanchat S. Internet of things: A review of applications and technologies. Suranaree J Sci Technol 2014;21:359-74.
21. Perera C, Liu CH, Jayawardena S. The emerging internet of things marketplace from an industrial perspective: A survey. IEEE Trans Emerg Top Comput 2015;3:585-98.
22. Min KW, Yeon MS, Hyuk PJ. An enhanced security framework for home appliances in smart home. Hum Centric Comput Inf Sci 2017;7:6.
23. Jayavardhana G, Rajkumar B, Slaven M, Marimuthu P. Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener Comput Syst 2013;29:1645-60.
24. Ersue M, Romascanu D, Schoenwaelder J, Sehgal A. Management of Networks with Constrained Devices: Use Cases. IETF Internet Draft; 2014. DOI: 10.17487/RFC 7548.
25. Michael C, Markus L, Roger R. The Internet of Things. McKinsey Quarterly. New York: McKinsey and Company; 2014.
26. Graham S, Baliga G, Kumar PR. Abstractions, architecture, mechanism, and middleware for networked control. IEEE Trans Automat Contr 2009;54:1490-503.