Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 7 No. 3, September, 2016 - www.cisdijournal.net

An Overview of Security Issues Relating to the Internet of Things

Akeredolu G.R
Department of Computer Science
Federal Polytechnic, Idah – Nigeria
akmasgbenga3@gmail.com

Elusoji A.A PhD
Department of Computer Technology
Yaba College of Technology, Yaba – Lagos, Nigeria
elusoji872@yahoo.com

Odii J. N. PhD
Computer Science Department,
Federal University of Technology Owerri, Imo-State, Nigeria
jnodii@yahoo.com

Akanji A.W.
computer Science Department
Lagos State Polytechnic
wasak2005@yahoo.com

Aiyegbusi A.E
Department of Computer Science
Micheal Otedola College of Primary Education
Epe-Lagos, Nigeria
aiyegbusied@yahoo.com akmasgbenga3@gmail.com

ABSTRACT

Internet of Things (IoT) is the integration of a variety of technologies which incorporates transparently and impeccably large number of assorted end systems, providing open access to selected data for digital services. IoT is a promising research in commerce, industry, and education applications. The abundance of sensors and actuators motivates sensing and actuate devices in communication scenarios thus enabling sharing of information in IoT. Advances in sensor data collection technology and Radio Frequency Identification technology has led large number of smart devices connected to the Internet, continuously transmitting data over time. In the context of security, due to different communication overloads and standards conventional security services are not applicable on IoT as a result of which the technological loopholes leads to the generation of malicious data, devices are compromised and so on. Hence a flexible mechanism can deal with the security threats in the dynamic environment of IoT and continuous researches and new ideas needs to be regulated periodically for various upcoming challenges. This paper basically elucidates the understanding IoT devices and services, its communications models show how IoT devices connect and communicate in terms of their technical communication models, discusses IoT architecture model and its security challenges.

Keywords : IoT Devices, ICT Systems, Communications Models, Protocol

CISDI Journal Reference Format
Akeredolu, G.R., Elusoji, A.A., Odii, J.N., Akanji, A.W. & Aiyegbusi, A.E. (2016): An Overview of Security Issues Relating to the Internet of Things. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 3. Pp 63-70.
Available online at www.cisdijournal.net

1. INTRODUCTION

The recent rapid development of the IoT and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments. IoT has gradually permeated all aspects of modern human life, such as education, healthcare, and business, involving the storage of sensitive information about individuals and companies, financial data transactions, product development and marketing [2].

The IoT is a vision of connectivity for anything, at anytime and anywhere, It is recognized as an extension of today's Internet to the real world of physical objects. The IoT can be realized in three paradigms—internet-oriented (middleware), things oriented (sensors) and semantic oriented (knowledge) [7]. The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide [5]. Most of these connected devices will be a smaller, cheaper, simpler embedded device which includes smart phones, tablets, TVs, gaming consoles, home appliances, security systems, smart thermostats, smart meters, personal fitness trackers, portable medical devices, smart watches, vending machines and numerous other products.

The IoT combines a heterogeneous disciplines, this multidisciplinary domain covers a large number of topics from technical issues (routing protocols, semantic queries), to a mix of technical, social and business issues (security, privacy, usability) [4]. The IoT has the chance to deliver solutions that improve energy efficiency, security, health, education and many other aspects of daily life for consumers. Also, it can support the solutions that improve decision-making and productivity in manufacturing, retail, agriculture and other sectors for enterprises [6]. Building the IoT needs wide range of technologies. The enhancement of the communications networks infrastructure, through heterogeneous technologies, as well as adoption of IPv6 in order to provide a unique address to each thing connected to the network [8]. Radio Frequency IDentification (RFID) and sensor network technologies will be the backbone of IoT, where information and communication systems are embedded in the environment around us [1].

Security requirements in the IoT environment are not different from any other ICT systems. Therefore, ensuring IoT security requires maintaining the highest intrinsic value of both tangible objects (devices) and intangible ones (services, information and data). The number of threats is also rising daily, and attacks have been on the increase in both number and complexity. Not only is the number of potential attackers along with the size of networks growing, but the tools available to potential attackers are also becoming more sophisticated, efficient and effective [6]. Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities [3].

2. UNDERSTANDING IOT DEVICES AND SERVICES

2.1 IoT device

This is a hardware component that allows the entity to be a part of the digital world [12]. It is also referred to as a smart thing, which can be a home appliance, healthcare device, vehicle, building, factory and almost anything networked and fitted with sensors providing information about the physical environment (e.g., temperature, humidity, presence detectors, and pollution), actuators (e.g., light switches, displays, motor-assisted shutters, or any other action that a device can perform) and embedded computers [10]. An IoT device is capable of communicating with other IoT devices and ICT systems. These devices communicate via different means including cellular (3G or LTE), WLAN, wireless or other technologies [8]. IoT device classification depends on size, i.e., small or normal; mobility, i.e., mobile or fixed; external or internal power source; whether they are connected intermittently or always-on; automated or non-automated; logical or physical objects; and lastly, whether they are IP-enabled objects or non IP objects. The characteristics of IoT devices are their ability to actuate and/or sense, the capability of limiting power/energy, connection to the physical world, intermittent connectivity and mobility [13]. Some must be fast and reliable and provide credible security and privacy, while others might not. A number of these devices have physical protection whereas others are unattended [9].

2.2 IoT services

IoT services facilitate the easy integration of IoT entities into the service oriented architecture (SOA) world as well as service science [15]. An IoT service is a transaction between two parties: the service provider and service consumer. It causes a prescribed function, enabling interaction with the physical world by measuring the state of entities or by initiating actions that will initiate a change to the entities. A service provides a well-defined and standardized interface, offering all necessary functionalities for interacting with entities and related processes. The services expose the functionality of a device by accessing its hosted resources [16].

2.3 Security in IoT devices and services

Ensuring the security entails protecting both IoT devices and services from unauthorized access from within the devices and externally. Security should protect the services, hardware resources, information and data, both in transition and storage. In this section, we identified three key problems with IoT devices and services: data confidentiality, privacy and trust. Data confidentiality represents a fundamental problem in IoT devices and services. In IoT context not only user may access to data but also authorized object. This requires addressing two important aspects: first, access control and authorization mechanism and second authentication and identity management (IdM) mechanism. The IoT device needs to be able to verify that the entity (person or other device) is authorized to access the service. Authorization helps determine if upon identification, the person or device is permitted to receive a service. Access control entails controlling access to resources by granting or denying means using a wide array of criteria.

Authorization and access control are important to establishing a secure connection between a number of devices and services. The main issue to be dealt with in this scenario is making access control rules easier to create, understand and manipulate [11]. Privacy is an important issue in IoT devices and service on account of the ubiquitous character of the IoT environment. Entities are connected, and data is communicated and exchanged over the internet, rendering user privacy a sensitive subject in many research works. Privacy in data collection, as well as data sharing and management, and data security matters remain open research issues to be fulfilled.

Trust plays an important role in establishing secure communication when a number of things communicate in an uncertain IoT environment. Two dimensions of trust should be considered in IoT: trust in the interactions between entities, and trust in the system from the users perspective [14]. The trustworthiness of an IoT device depends on the device components including the hardware, such as processor, memory, sensors and actuators, software resources like hardware-based software, operating system, drivers and applications, and the power source. In order to gain user/services trust, there should be an effective mechanism of defining trust in a dynamic and collaborative IoT environment.

3. IoT COMMUNICATIONS MODELS

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models.

3.1 Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-device communications, as shown in Figure 3.1.

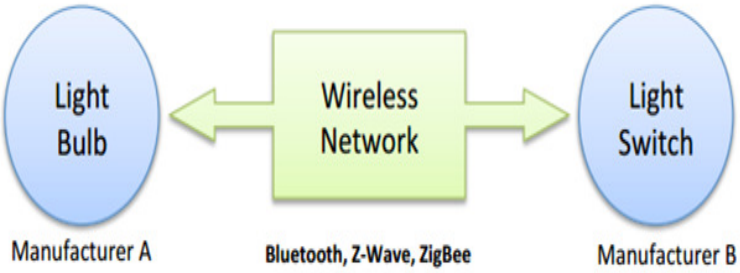

Figure 3.1: Example of device-to-device communication model.

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario [17]. The device manufacturers need to invest in development efforts to implement device-specific data formats rather than open approaches that enable use of standard data formats. From the user's point of view, this often means that underlying device-to-device communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol.

3.2 Device-to-Cloud Communications

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 3.2.

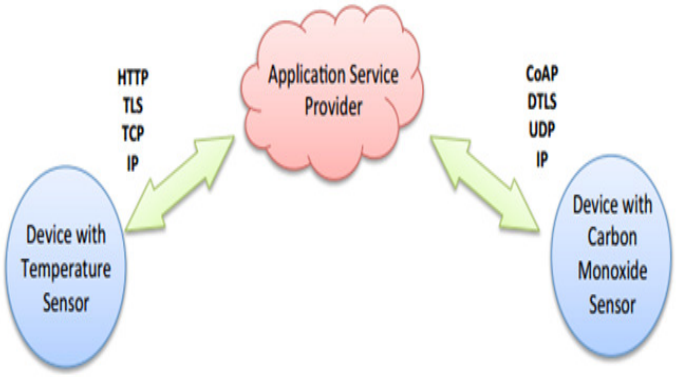

Figure 3.2: Device-to-cloud communication model diagram.

This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat [18] and the Samsung SmartTV. In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyze home energy consumption. Further, this cloud connection enables the user to obtain remote access to their thermostat via a smartphone or Web interface, and it also supports software updates to the thermostat. Similarly with the Samsung SmartTV technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV. In these cases, 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 [19]. 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.

3.3 Device-to-Gateway Model

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 3.3.

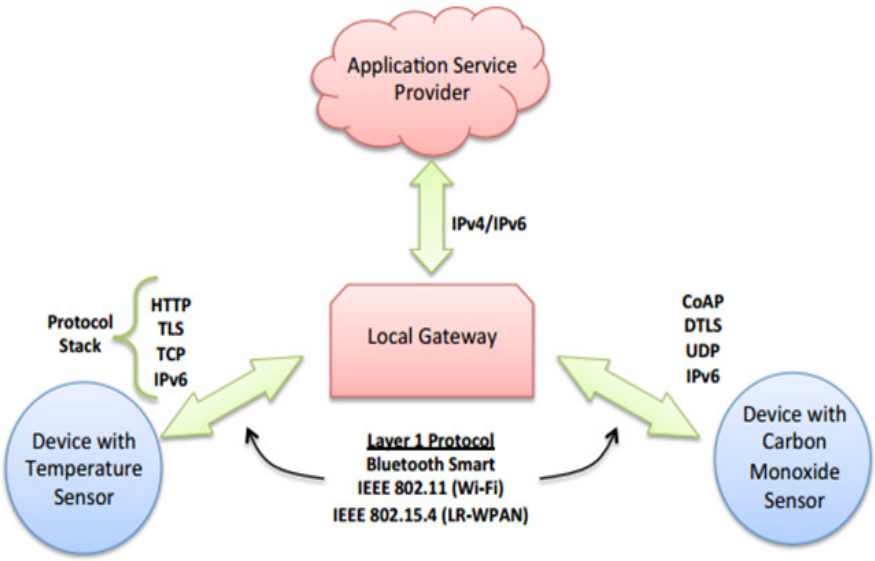

Figure 3.3: Device-to-gateway communication model diagram.

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 [20].
The other form of this device-to-gateway model is the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the SmartThings 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 SmartThings cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection [21]. 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.

3.4 Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports "the [user's] desire for granting access to the uploaded sensor data to third parties" [22]. 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. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building [23]. Also, this kind of architecture facilitates data portability needs. 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 (APIs) are needed to achieve interoperability of smart device data hosted in the cloud. A graphical representation of this design is shown in Figure 3.4.

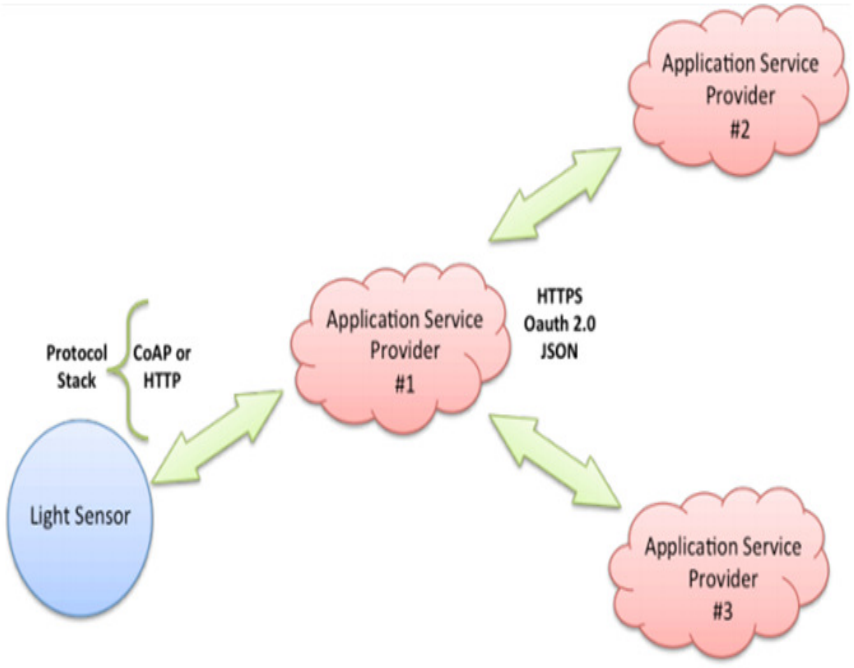

Figure 3.4: Back-end data sharing model diagram.

4. IOT ARCHITECTURE

IoT Architecture can be divided into three layers Perception, Network and Application. As shown in Figure 4.1 Perception layer (also called as recognition layer) gathers data or information and identifies the physical world. Network layer is the middle one (also called as wireless sensor networks), which accountable for the initial processing of data, broadcasting of data, assortment and polymerization. The topmost application layer offers these overhauls for all industries. Among these layers, the middle one network layer is also a "Central Nervous System" that takes care of global services in the IoT, since it acts the part of aggregating with upward application layer and makes the link downward of perceptual layer. Various basic networks including, mobile/private network, wireless and wired network offers and affirms the underlying connection. IoT are set up in this new network which is composed Business applications of networks [3].

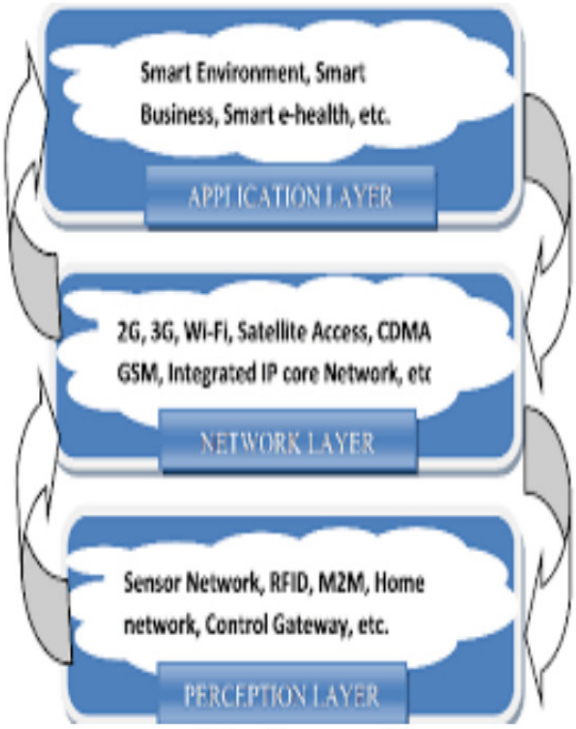

Figure 4.1: IoT architecture model

5. SECURITY CHALLENGES IN IoT

Majority of the devices in IoT are not reachable as most of the time devices remain disconnected or loses connection. They could be lost or stolen thus making security very difficult. Expectation of strong security is difficult without processing power. As most of the devices are sensors and depends on battery life, devices maintain a finite lifetime. Devices are transportable and mostly mobile and should be recognised by readers based on Radio Frequency Identification addresses or tags along with proper authentication and device identification. Security works on IoT must include assurance of risk analysis, device analysis, crypto capability and export analysis and must fulfil certain security objectives such as privacy protection, identity protection and traffic analysis protection [24].

Security in IoT is mainly depended on the capability of the users to have faith in their environment. It is the top priority of the sector. Poorly secured IoT devices could serve as ingress points for cyber attack by allowing malicious programmers to re-program a device or cause it to perform a malfunction intentionally. Poorly designed devices can expose user data to theft by leaving data streams and objects unattended. Competitive cost and technical constraints on IoT devices challenge manufacturers to reasonably design security characteristics into these devices, potentially creating safety measures and enduring maintainability vulnerabilities greater than their traditional computer counterparts. The sheer increase in the number and nature of IoT devices could increase the attacks. When united with the extremely interconnected character of IoT devices, every poorly secured device linked online affects the security and flexibility of the Internet [1].

The increasing level of dependence on IoT devices and the Internet services they interact with also enhances the pathways for wrongdoers to have access to devices and get compromised as their behavior has a global reach and impact. Turning off the devices is not an ideal solution at the same time for such issues. Thus security of IoT devices and services is a critical issue. The security of such devices is not absolute. The overall security and resilience of the IoT is a utility of assessing and managing security risks. It is very important to understand the interrelatedness of IoT in a wide manner [11]. It is important to know that :-

- Existing tools, methods, and strategies associated with IoT security needs new consideration in comparison to the conventional system and strategies.
- Deployment of homogenous IoT may compromise its simplicity. Hopefully, a heterogeneous implementation strategy might work out properly.
- Problems might arise in backgrounds like reconfiguration, evolution of the devices.
- Long-term support and management of these devices
- Improper knowledge regarding the device functionalities from the end users' part
- Attackers may have direct physical access to IoT devices. Anti-tamper features needs to be considered to ensure security in such cases
- Security breach persists for long periods without detection
- Future devices might be the products of various self manufacturers who find themselves to be highly fascinated towards the technology in a similar manner today people are fascinated towards the development of enormous number of Android projects and devices of their own.
- Shielding Programmable Logic Devices from human interference
- Maintenance of control systems for nuclear reactors receiving software updates periodically without impairing functional safety.

The effective and appropriate security solutions can be achieved only if the users involved with IoT emerge with mutual security. The collaborative model emerges as an effective approach in industry, governments and public authorities to help secure the Internet, cyberspace and IoT. This model includes a range of practices and tools including bidirectional voluntary information sharing, valuable enforcement equipments, cyber exercises, awareness raising and training, agreement on international norms of behaviour, and development and recognition of international standards and practices. However, collaborative and shared risk management-based approaches needs to keep on evolving such that it suits the scale and complexity of IoT device security challenges of the future. Besides secure booting, access control, firewalls, IP address, device authentication, updates and patches, end-to-end security are also some of the solution to the security of IoT [25].

6. CONCLUSION

This paper has tried to cover the entire concept of IoT on security issues as far as possible based on various surveys and research works carried out so far and has tried to accomplish completeness -firstly with the introduction, its communication model, IoT issues, IoT architecture, key components and elements, challenges, issues, security issues and threats, IoT devices, security management, Quality of Services etc. The IoT aims to effortlessly merge the real and implicit worlds such that tomorrow's globe will be a synthesis of human life and information. The current security services are inadequate for IoT. The future research directions mainly consist of dealing with the development and challenges related to various issues on IoT.

REFERENCES

[1] D. Jiang and C. ShiWei, "A study of information security for m2m of Internet of Things," in Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, vol. 3. IEEE, 2010, pp. V3–576.
[2] Feng Wang, Liang Hu, Jin Zhou, and Kuo Zhao, "A Survey from the Perspective of Evolutionary Process in the IoT", International Journal of Distributed Sensor Networks, February 2015, Hindawi Publishing Corporation.
[3] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista and Michele Zorzi , "IoT for Smart Cities" , IEEE IoT Journal, Vol. 1, No. 1, February 2014.
[4] Omar Said and Mehedi Masud, "Towards IoT: Survey and Future Vision", International Journal of Computer Networks (IJCN), Volume (5) , Issue (1), 2013.
[5] Ashvini Balte, Asmita Kashid and Balaji Patil, " Security Issues in IoT: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 4, 2015.
[6] M. Blackstock and R. Lea, "Toward interoperability in a web of things," in Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication, 2013, pp. 1565-1574.
[7] M. Welsh and G. Mainland, "Programming Sensor Networks Using Abstract Regions," in NSDI, 2004, pp. 3-3.
[8] Y.-K. Chen, "Challenges and opportunities of internet of things," in 2012 17th Asia and South Pacific Design Automation Conference (ASP-DAC), 2012, pp. 383-388.
[9] C. C. Aggarwal, N. Ashish, and A. Sheth, "The internet of things: A survey from the data-centric perspective," in Managing and mining sensor data, ed: Springer, 2013, pp. 383-428.
[10] N. A. Ali and M. Abu-Elkheir, "Data management for the internet of things: Green directions," in Globecom Workshops (GC Wkshps), 2012, pp. 386-390.
[11] Isam Ishaq , David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester , "IETF Standardization in the Field of the IoT:A Survey", Journal of Sensor and Actuator Networks, ISSN 2224-2708, April 2013.
[12] Min-Woo Ryu, Jaeho Kim, Sang-Shin Lee and MinHwan Song. Survey on IoT: Toward Case Study. Smart Computing Review. Korea Electronics Technology Institute, vol.2, no. 3, June 2012.
[13] Prajakta Pande and Anand R. Padwalkar, "IoT–A Future of Internet: A Survey", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 2, February 2014.
[14] Chen Qiang , Guang-ri Quan , Bai Yu and Liu Yang, "Research on Security Issues of the IoT", International Journal of Future Generation Communication and Networking, Vol.6, No.6 , pp.1-10, 2013.
[15] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "Iot gateway: Bridging wireless sensor networks into internet of things," in 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), 2010, pp. 347-352.
[16] C. H. Liu, B. Yang, and T. Liu, "Efficient naming, addressing and profile services in Internet-of Things sensory environments," Ad Hoc Networks, vol. 18, pp. 85-101, 7 2014.
[17] M. Chui, M. Löffler, and R. Roberts, "The internet of things," McKinsey Quarterly, vol. 2, pp. 1-9, 2010.
[18] L. Yang, S. Yang, and L. Plotnick, "How the internet of things technology enhances emergency response operations," Technological Forecasting and Social Change, vol. 80, pp. 1854-1867, 2013.
[19] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.
[20] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.
[21] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash ―Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications‖ ieee communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.
[22] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal ―A Review on Internet of Things (IoT)‖ International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.
[23] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of Things-based Smart Home System," 2nd International Conference on Intelligent Control and Information Processing, 2011, pp. 921-924.
[24] J. Liu, and L. Yang, "Application of Internet of Things in the Community Security Management," Computational Intelligence, Communication Systems and Networks,Third International Conference on IEEE, 2011, pp. 314-318.
[25] D. Jiang, and C. ShiWei, "A Study of Information Security for M2M of IoT," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 576-579.