A SURVEY ON IOT ARCHITECTURES, PROTOCOLS, APPLICATIONS, SECURITY, PRIVACY, REAL-WORLD IMPLEMENTATION AND FUTURE TRENDS

***Surapon Kraijak*[1]*, Panwit Tuwanut*[1]**

[1]*King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand*
macro.biggiez@gmail.com, panwit@it.kmitl.ac.th

Keywords: Internet of Things, IoT Architecture, IoT Protocols, IoT Applications, Security, Privacy, Future Trends.

Abstract

The Internet is dramatically evolving and creating various connectivity methodologies. The Internet of Things (IoT) is one of those methodologies which transform current Internet communication to Machine-to-Machine (M2M) basis. Hence, IoT can seamlessly connect the real world and cyberspace via physical objects that embed with various types of intelligent sensors. A large number of Internet-connected machines will generate and exchange an enormous amount of data that make daily life more convenient, help to make a tough decision and provide beneficial services. This paper not only describes about the evolution and how important of IoT in daily life, the generic architecture, its most widely used protocols, numerous possible applications but also concern over security and privacy issues in IoT, real-world implementation of IoT system by using Arduino and its future trends. The IoT probably becomes one of the most popular networking concepts that has the potential to bring out many benefits.

1 Introduction

Though rapidly advancing technologies, society is moving toward an "always connected" model. Wired and wireless networks are everywhere, open standards are defined and allowed for particularly addressing procedure. Concepts associated with the "Future Internet" are being researched [1], developed and continuously adapted in daily life.

One new concept associated with the "Future Internet" is called "Internet of Things" (IoT). The IoT become a vision where real-world objects are part of the internet: every object is uniquely identified, and accessible to the network, its position and status known [1], where numerous services and intelligence are added to effectively expand an Internet, seamlessly combining between the digital and physical world, eventually affecting on personal and social environment.

This paper presents an overview of the Internet of Things, generic architecture and protocols, applications, security and privacy concerns, implementation and its future trends. It is positioned as an introductory paper beneficial to a wide audience ranging such as networks researchers, chief information officers (CIO), information technology specialists, consultants, decision makers in business firm and so on.

The rest of the paper is organized as follows. Section 2 presents the reasoning for and the evolution of Internet of Things. Section 3 describes briefly the generic architecture and protocols of IoT. Section 4 gives real life applications of IoTs and Security and Privacy concerns in IoT are discussed in Section 5. Section 6 presents an implementation and Future trends of IoT. Finally, Section 7 concludes survey study with references at the end.

2 Evolution of Internet of Things

The advancing Internet technologies are expanding the boundaries of the Internet connectivity is becoming cheap and ubiquitous, even in developing countries [1] or rural areas. Device processing power and storage capabilities are significantly increasing while their sizes are becoming smaller which extremely appropriated for equipped with different type of sensors and actuators; the combination between small devices and multi-function sensors producing an extensively across communities where devices are able to connected and communicate over the Internet, has the ability to sense, compute, act and effectively become part of the Internet. Furthermore, physical objects are increasingly equipped with RFID tags (Radio-Frequency Identification (RFID)), NFC tags (Near Field Communications (NFC)) or other electronic bar code [1] that can be scanned by smart devices such as tablet, smart phone and other small device embedded with RFID/NFC readers. This combination connects between the physical world and cyberspace via the smart device, thus enhancing the Internet capabilities toward the next generation of Internet can be called the "Internet of Things".

The terminology of "things" in the IoT aspect is extremely extensive and includes an array of physical stuffs [1]. For instance, personal objects (*i.e.* smart phones, tablets, digital cameras, smart watch, game consoles, etc.), environmental elements and other electronic equipments embed with either RFID or NFC tags which able to connect the Internet via gateway device. According to the word "Things" that mentioned above, the numerous devices and things will be connected to the Internet almost simultaneously and each elements providing gathered data and information, even services.

The Internet of Things (IoT) completely transforms connectivity from "any-time, any-where" for "any-one" into "any-time, any-where" for "any-thing" [1]. The IoT is able to connect real world elements and embeds the intelligent in communication system for smartly process its specific information and autonomous decision. Hence, IoT is a key enabling the different types of beneficial applications and services which can sustain our economies, transportation, environment and health that we never expected before. The generic scenario of IoT is shown in **Figure 1**.

3 Generic Architecture and Protocols of IoT

The TCP/IP protocol stack plays a key role in digital communication which was defined long time ago. Nevertheless, the IoT may connect enormous number of objects which will create a massive traffic and tremendous amount of data capacity is needed. Moreover, IoT will face numerous challenges especially privacy and security issues [2]. Therefore, the new standard architecture and protocols for IoT needs to address many essential factors (*i.e.* sustainability, reliability, Quality of Service, confidentiality, integrity, etc.). Due to the IoT procedures are mainly to connect between everything and everyone to exchange information with each other that not only exponentially increasing the network traffic but also storage capacity as well. Thus, IoT improvement relies on the advances in technology and applies to different types of useful applications and business models. The basic architecture and protocols of IoT proposed in [3] and [4] respectively.

3.1 Generic Architecture

The typical IoT architecture can be divided into five layers as shown in **Figure 2**. Each layer is briefly described below:

Perception Layer: The perception layer is similar to physical layer in OSI model which consists of the different types of sensor (*i.e.* RFID, Zigbee, QR code, Infrared, etc.) devices and environmental elements. This layer generally copes with the overall device management viz; identification and collection of specific information by each type of sensor devices. The gathered information can be location, wind speed, vibration, pH level, humidity, amount of dust in the air, etc. This gathered information transmits through the Network layer for its secure communication toward central information processing system.

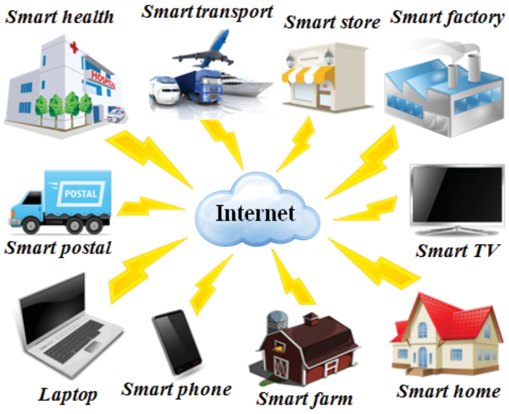

Figure 1. The IoT generic scenarios.

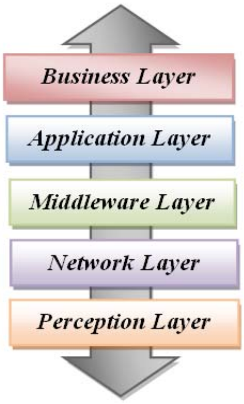

Figure 2. The IoT generic architecture.

Network Layer: The Network layer plays an important role in securely transfers and keeps the sensitive information confidential from sensor devices to the central information processing system through 3G, 4G, UMTS, WiFi, WiMAX, RFID, Infrared, Satellite, etc. dependent upon the type of sensors devices. Hence, this layer is mainly responsible for transfer the information from Perception layer to upper layer.

Middleware Layer: The devices in the IoT system may generate various type of services when they are connected and communicated with others. Middleware layer has two essential functions, including service management and store the lower layer information into the database. Moreover, this layer has capability to retrieve, process, compute information, and then automatically decide based on the computational results.

Application Layer: Application layer is responsible for inclusive applications management based on the processed information in the Middleware layer. The IoT applications can be smart postal, smart heath, smart car, smart glasses, smart home, smart independent living, smart transportation, etc.

Business Layer: This layer functions cover the whole IoT applications and services management. It can create practically graphs, business models, flow chart, executive report, etc. based on the amount of accurate data received from lower layer and effective data analysis process. Based on the good analysis results, it will help the functional managers or executives to make more accurate decisions about the business strategies and roadmaps.

3.2 IoT Protocols

Protocol is the special set of rules and regulations that end point in a telecommunication connection use when they need to communicate to other end point which connected to the same/different network. In this subsection will briefly describe about the most frequently used protocols for Machine-to-Machine (M2M) communication.

MQTT (Message Queue Telemetry Transport): MQTT is a Client Server publishes or subscribes messaging transport protocol. It is light weight, open, simple and designed so as to be easy to implement. The protocol runs over TCP/IP or over other network protocol that provided ordered, lossless, bi-directional connections. The MQTT features include: use of the publish/subscribe message pattern which provides one-to-many message distribution, a messaging transport that is agnostic to the content of the payload, and this protocol also has three qualities of service for message delivery viz; “At most once”, where messages are delivered according to the best efforts of operating environment. The message loss can occur and this level could be used, Secondly, “At least once”, where message are assured to arrive but duplicate massages can occur. Finally, “Exactly once”, where message are assured to arrive exactly once. This level could be used [5]. This that cause to drastically reduce network traffic. Furthermore, the MQTT protocol is not only minimized transport overhead and protocol exchange to reduce network traffic but also has an extraordinary mechanism to notify interested parties when an abnormal disconnection occur as well.

CoAP (Constraint Application Protocol): CoAP is a specialized web transfer protocol for use with constrained nodes and constrained networks (e.g. low-power, lossy). The nodes often have 8-bit microcontroller with small amounts of ROM and RAM, while constrained network often have high packet error rate and typical throughput is 10 kbps [6]. This protocol designed for Machine-to-Machine (M2M) application such as smart city and building automation. CoAP provides a request and response interaction model between application end points, support build-in discovery services and resources, and includes key concepts of the Web [7] such as URIs and Internet media types. CoAP is designed to friendly interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.

4 Applications of Internet of Things

According to survey done by the IoT-I project in 2010 [8] indicated IoT’s circumstance applications could be grouped in 14 domain viz; Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment and Energy. This survey was based on 270 responses from 31 countries demonstrated the most interesting circumstance applications were: smart home, smart city, transportation and healthcare. In this paper, the focus will be briefly on the IoT’s applications in transportation, healthcare, smart city or home, personal and social.

4.1 Assisted Driving

Today’s different type of transportation such as cars, train and buses along with the road and the rails equipped with sensors, actuators and powerful processors may provide beneficial information to the driver and/or passengers (*i.e.* accidents, temporary and/or permanent road closures, traffic congestions) to provide better navigation and safety [9]. The numerous profit and non-profit organizations would benefit from gathered road traffic patterns information such as governmental authorities used for construction/ planning purpose, freight companies used these information to perform more route optimization which allows energy saving, and so on.

4.2 Mobile Ticketing

Electronic posters or billboards providing information in regard to transportation services can be equipped with the NFC tag. The user can get information from the web by either hovering their mobile phone over the NFC tag or pointing the mobile phone to the visual markers [10]. The mobile phone automatically retrieves and combines information from the related web services (stations, number of passengers, costs, available seats, departure and arrival time, and type of services) and provides the suggestion about tickets which suitable for each user.

4.3 Sensing

Sensor device enable multifunction focused on both inpatient and out-patients treatment and especially on diagnosing patient conditions providing real-time information on patient health indicators. Heterogeneous wireless access-based remote patient monitoring system can be deployed to reach the patient everywhere with multiple wireless technologies integrated to support continuous biosignal monitoring in presence of patient mobility [9] [11].

4.4 Identification and Authentication

Identification and authentication are two terms that described the preliminary phases of the security process in computer systems which could apply to healthcare, for instance, patient identification to reduce harmful incidents to patient, current electronic medical record maintenance and infant identification in hospitals to prevent mismatching. An identification and authentication procedure is most frequently used to manage, grant access and improve medical staff morale by addressing patient safely issues [9]. In addition, identification and authentication are essential parts to meet the requirements of security schemes and prevent thefts or losses of precious instruments and products.

4.5 Comfortable Homes and Offices

Sensors and actuators distributed deployment in houses and offices could make our life easier in several aspects: room heating can be adapted as predefined preferences and the weather; the room lighting can automatically change according to the time of day; hazardous incidents can be prevented with appropriate alarm and monitoring system [9] and energy cost could drastically reduced by automatically switching off the electrical equipments such as television, air condition, kettle, fridge, light bulb and so on, when not used.

4.6 Social Networking

Social networking: This application is involved to the automatically update of information and location about our social activities in social networking websites. We probably think of RFIDs which generate events about people and places to assist users real-time updates in their social networks [9]. The mobile/web application user interfaces would display a feed of events that their friends have preliminary defined and the users not only manage their friend lists but also grant permission for each friend who has privileged to reach the information or events.

4.7 Thefts

An application informs the user to know if precious objects are moved from a restricted area, which indicates that the object is being stolen [9]. In this case, the event has to be notified promptly to the owner and/or security guards through SMS, call, e-mail, etc.

4.8 Losses

A search engine for things is an instrument that helps in finding objects that have been lost for a long time. The web-based application is one of the best approaches to finding lost object that provide the latest recorded location for tagged objects or retrieve for a particular object's location [9] [12]. Furthermore, this application allows user-defined events to notify owner when the most recent recorded object location matches predefined conditions.

5 Security and Privacy Concern in IoT

The security and privacy of information and network should be equipped with these basic principles such as confidentiality, integrity, availability, authentication and authorization [9]. Unlike from the Internet, the IoT will be applied to the most significant of global economy. For instance, transportation, healthcare, smart city and home, personal and social. Therefore, the security and privacy issues are the most concerned that need to be addressed in IoT.

5.1 Security Concerns

Internet of Things is seamlessly combined two disparate worlds into one. In the initial stage of IoT, mostly researchers are focused on developing the M2M (Machine to Machine) communication protocol that distinct from general network communication in case of characteristics and deployment environments [13]. Though dramatically improve in IoT it creates a concerning problems which affecting security and privacy of information.

Front-end Sensors and Equipment: Front-end sensors and equipment is responsible for receive data via smart sensors then transmit the data to central processing system by using M2M modules device. Through the typical architecture of IoT some perception sensors or devices are mostly deployed in the absence of monitoring system [13] which create vulnerabilities to attack from the outsiders such as an attacker can readily access and continuously reprogram until these devices could send data not only to registered server but also to many groups of attackers. Thus, the possible threats to front-end sensors and equipment can be categorized into three groups: eavesdropping, unauthorized access to data and denial of service attack.

Network: Network in IoTs is directly responsible for overall M2M communication management as well as reliable quality of service (QoS) [13]. Since the enormous volumes of data sending to high traffic network, large number of devices are currently connected to network may be caused of denial of service attacks.

Back-end: Back-end is the most important part of IoT system which has high security requirements and efficient sensor data analysis and management unit inside to enable real-time data processing. The typical security of IoT system can be classified into seven major domains as follows: privacy protection, access control, user authentication, communication security, data integrity, data confidentiality and availability at any time [13].

5.2 Privacy Concerns

Generally, the IoT standard communication, the distributed environmental sensor devices are connected to the Internet or network then signal the specific information which gathered from sensor devices toward the central server via Mobile or fixed communication.

Privacy issues should be concerned in entire process of wireless communication since in the device, in storage, during communication and even during processing process [13] which helps to conceal the sensitive information. Thus, the privacy of users and personal information are one of the key challenges in IoTs which have to cope with.

Privacy in Device: The unsecure devices always have at least one or more vulnerabilities which probably caused to leak out of confidential information in case of inappropriate hardware and software design. For instance, the attackers can directly remote access to victim's device then change the destination account name and number while doing an online transaction. Hence, reliability and robustness are the essential features for devices that gather sensitive data [13]. Nowadays, there are numerous privacy issues in the device that need to be addressed such as hiding the folder containing personal information (*i.e.* login name and password, registered phone number, citizen ID number, etc.) when the device theft or loss, concealing the current or recorded location information of device holder, encrypting the communication links both wired and wireless in order to prevent unwanted third parties eavesdrop on your conversations.

Privacy during Communication: One of the most useful and effective approaches to maintain data confidentiality during the data transmission process is encryption. However, some encryption algorithms may provide an easier way to attackers for tracing data and analysis of linking packets. Hence, Secure communication protocols should be suitable approach to address this issue.

Privacy in Storage: The common procedures to keep information privacy in storage devices or databases is stored only frequently used data for routine tasks but excluding personal and specific information. To conceal the stored data not only a Pseudonymization and Anonymization technique could be a suitable approach [13] but also hide any specific record and force the database could display only statistical data to ensure the output is not related to particular record.

Privacy at Processing: This problem generally consist of two issues, Firstable, sensitive data must be treated in an appropriate way as desired purpose. Secondly, Mostly data owner are inadequate of information privacy knowledge and cause of their personal data explicitly disclosed or transferred to third party. Thus, the most effective technique that could deal with those crucial problems is Digital Right Management (DRM). The DRM could control and protect against illegally used and re-distribution [13] of commercial media through define a set of privacy policies for each personal data during the data processing procedure. However, for effective and efficient operations of DRM essentially require trusted and powerful devices.

6 IoT Implementation and Future Trends

The IoT can entirely change the current communication of Internet and also provide numerous beneficial opportunities for research and development in real-world. The following section will briefly describe about an implementation IoT with MQTT protocol and its future trends.

6.1 IoT Implementation

The MQTT is a lightweight, fast communication protocol designed for IoT. It is well known that things will communicate to the others by using publish/subscribe model and thing will get information from the others by push protocol from a broker. Hence, the key point of implementation IoT is a broker. There are various types of MQTT brokers available such as IBM Message Sight, HiveMQ, Mosquitto and etc. They vary in their feature set and some of them implement additional features on top of the standard MQTT functionality and provide commercial broker's service. In this proposed paper, Mosquitto is applied to implement IoT because it is free license, eases to install and can install in several operating system for example: Ubuntu, Redhat, CentOS, Fedora, FreeBSD, Windows, Mac and openSUSE. Next, Ponte is used to install via NPM, since Ponte is built on a top of Node.JS framework. The most significant feature of Ponte is a permit to publish and receive the data using any protocol such as HTTP, MQTT and CoAP. The architecture of Ponte is shown in **Figure 3**.

The next important part of IoT is a device which can communicate with each other, access data on the Internet, store and retrieve data, and interact with users. Some popular board and development platform for IoT such as Arduino uno with Ethernet shield, Arduino Yun and Raspberry Pi. The main point of implementation is a *PubSubClient* library which provides a client for publish/ subscribe messaging with a broker. In Arduino Sketch, *Ethernet* library and *PubSubClient* library must be included in the top of the program and IP Address, Subnet mask and Gateway must be assigned in a setup part. Next, create a topic for publish/subscribe. Hence, a device can communicate with others. The weak point that we met in the experiment is a problem with broadcast model, for example, a master station publish a traffic jam message to a broker with/*traffic* topic. The others subscribe/*traffic* topic will get information from a master station and display on a board. If anybody know publish/subscribe topic, they can publish any message to a broker and then the others will display wrong information. The security and permission policy will discuss in protocol development.

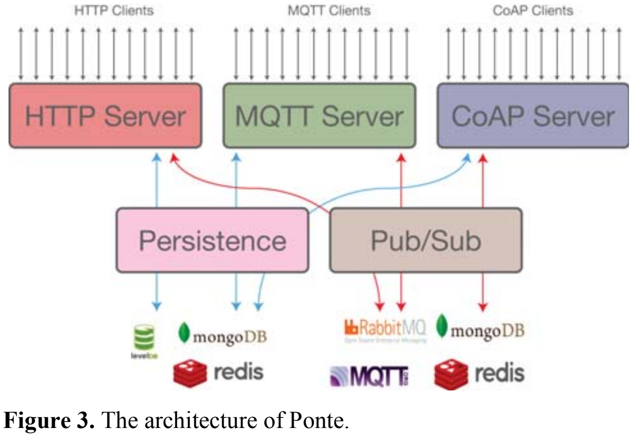

Figure 3. The architecture of Ponte.

6.2 Future Trends

The innovation of IoT will drive the future of technology, various innovative and creative products will design. However, some challenge problems need to address, the following subsection show three examples of the IoT trends will matter.

Low-power Sensing unit: The low-power consumption is one of the most interesting issues in IoTs which focused on energy-efficient designs. The low-power sensing unit can operate over the lifetime without the need for battery replacement. However, high performance processing units or intelligent sensor modules may consume a huge amount of power and become a major design problem that needs to address. There are two common alternatives that widely used to design low-power sensors viz; Firstly, create a group of low-accuracy modules to reduce sensor power consumption then apply the fusion technique to recover high-accuracy information. Secondly, based on circuit researches found that digital circuits consume the power less than analog circuits in wireless communication aspect [14]. Hence, the types of transmitters are one of concerning factors that should examine for designing an energy-efficient sensor. One of the common and appropriate techniques is replacing the analog transmitters with digital transmitters in wireless communication.

High efficiency in connectivity: Through rapid growth and popularity in Internet technologies. Many wired/ wireless standards and protocols are defined. However, currently used standards and protocols may not handle a large amount of traffic from intelligent or mobile devices which connect to the Internet at the same time. Furthermore, the number of sensor devices is dramatically increased that differ from the increasing rate of available wireless spectrum. Fortunately, the IoT communication has various particular characteristic such as low data rate, correlation of information even from the different sensors and do not require real-time monitoring [14]. Hence, the most suitable technique to cope with the problems that mentioned above is clustering. This technique has several benefit viz; reduce network traffic through send a massive amount of gathered information to cluster head which is nearest to the particular node and then transmit to base station, increase rate of spectrum reusability and prevent malicious groups to directly connect in order to reprogramme at the base station.

Reliable communication: The IoT connects billion of perception objects that spread over the specific area to exchange a large amount of gathered information and provide numerous convenient services over wireless networks. Unfortunately, most wireless networks often create insecure connections that allow the intruders or anybody can easily access to the particular objects and sensitive information. Hence, the IoT essential needs at least an appropriate mechanism to prevent unauthorized access, eavesdropping and external interference. One of the most commonly and widely used techniques to address these problems is encryption, to ensure data integrity, maintain confidentiality of information and prevent unwanted third parties eavesdropping on private conversations. Another efficiency approach is defined security policies and regulations during transmission or reception data across the wireless network.

7 Conclusion

The Internet of Things, things which can communicate with each other via Internet, access data on the Internet, store and retrieve data, and interact with users. This paper describes the evolution and how important of IoT in daily life, the generic architecture, its most widely used protocols, numerous possible applications, future trends and how to implementation IoT by using MQTT Protocol with Arduino platform. Based on a lightweight and fast communication protocol designed for IoT, there is trade off with the security and permission policy that should be discussed in protocol development in a future.

References

[1] Coetzee, L. and Eksteen, J. (2011) The Internet of Things—Promise for the Future? An Introduction. *IST—Africa* 2011 *Conference Proceedings* (*CSIR*), Pretoria, May 2011.

[2] Khan, R., Khan, S.U., Zaheer, R. and Khan, S. (2012) Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. 10*th International Conference on Frontiers of Information Technology*, December 2012, 257-260. http://dx.doi.org/10.1109/fit.2012.53

[3] Tan, N. and Wang, N. (2010) Future Internet: The Internet of Things. 3*rd International Conference on Advanced Computer Theory and Engineering*, August 2010.

[4] Wu, M., Lu, T., Ling, F., Sun, J. and Du, H. (2010) Research on the Architecture of Internet of Things. 3*rd International Conference on Advanced Computer Theory and Engineering* (*ICACTE*), August 2010.

[5] http://www.mqtt.org/documentation

[6] Palattell, M., Accettura, N., Vilajonasa, X., Watteyne, T., Grieco, L., Boggia, G. and Dolher M. (2013) Standardized Protocol Stack for the Internet of (Important) Things. *IEEE Communication Surveys & Tutorials*, 1389-1430.

[7] Birmann, C., Castellani, A.P. and Shelby, Z. (2012) CoAP: An Application Protocol for Billions of Tiny Internet Nodes. *IEEE Internet Computing*. http://dx.doi.org/10.1109/MIC.2012.29

[8] Vermesan, O., Friess, P. and Furness, A. (2012) The Internet of Things 2012. By New Horizons.

[9] Atzori, L., Iera, A. and Morabito, G. (2010) The Internet of Things: A Survey. *Computer Networks Journal*, June 2010, 2787-2805. http://dx.doi.org/10.1016/j.comnet.2010.05.010

[10] Bing, K., Fu, L., Zhao, Y. and Yanlei, L. (2011) Design of an Internet of Things-Based Smart Home System. 2*nd International Conference on Intelligent Control and Information Processing*, 2011, 921-924. http://dx.doi.org/10.1109/icicip.2011.6008384

[11] Niyato, D., Hossain, E. and Camorlinga, S. (2009) Remote Patient Monitoring Service Using Heterogeneous Wireless Access Networks: Architecture and Optimization. *IEEE Journal on Selected Area in Communications*, 412-423.

[12] Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymar, S., Balazinska, M. and Borriello, G. (2009) Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *IEEE Internet Computing*, 48-55. http://dx.doi.org/10.1109/MIC.2009.52

[13] Kumar, J.S. and Patel, D.R. (2014) A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, March 2014, 20-25.

[14] Chen, Y.K. (2012) Challenges and Opportunities of Internet of Things. 17*th Asia and South Pacific Design Automation Conference*, February 2012, 383-388. http://dx.doi.org/10.1109/ASPDAC.2012.6164978