

# Smart Gateway Based Communication for Cloud of Things

Mohammad Aazam<sup>1</sup>, Pham Phuoc Hung<sup>2</sup>, Eui-Nam Huh<sup>3</sup>  
Innovative Cloud and Security Lab, Department of Computer Engineering  
Kyung Hee University, Suwon, South Korea.  
<sup>1</sup>aazam@ieee.org  
{<sup>2</sup>hungpham, johnhuh<sup>3</sup>}@khu.ac.kr

**Abstract**—Integration of Internet of Things with Cloud Computing is gaining importance, with the way the trend is going on in ubiquitous computing world. Literally, everything is going to be connected to the Internet and its data will be used for various progressive purposes, creating not only information from it, but also, knowledge and even wisdom. Internet of Things (IoT) becoming so pervasive that it is becoming important to integrate it with cloud computing because of the amount of data IoT's could generate and their requirement to have the privilege of virtual resource utilization and storage capacity, but also, to make it possible to create more usefulness from the data generated by IoT's and develop smart applications for the users. Integration of IoT with Cloud Computing, referred here as Cloud of Things, requires smart gateway to perform the rich tasks and preprocessing, which sensors and light IoTs are not capable of doing. This paper focuses on some of the key challenges involved in CoT and the proposal of smart gateway based communication.

**Keywords**—IoT; cloud computing; CoT; smart gateway

## I. INTRODUCTION

Internet of Things (IoT) is no more a buzzword now. Productive work is going on in this area of next generation Internet. IoT's and cloud computing need to be integrated, since IoTs are going to expand and produce a lot of data. With the trend going on, in near future, number of connected devices would be hundreds of times larger than the number of people connected. It is expected that by 2012, 20 households would have been generating more Internet traffic than the whole Internet used to do in year 2008 [1].

### A. Internet of Things

IoT, the term first introduced by Kevin Ashton in 1998, is a future of Internet and ubiquitous computing [2]. This technological revolution represents the future of connectivity and reachability. In IoT, 'things' refer to any object on the

face of the Earth, whether it is a communicating device or a non-communicating dumb object. From a smart device to a leaf of a tree or a bottle of beverage, anything can be part of Internet. The objects become communicating nodes over the Internet, through data communication means, primarily through Radio Frequency Identification (RFID) tags. IoT include smart objects as well. Smart objects are those objects that are not only physical entities, but also digital ones and perform some tasks for humans and the environment. This is why, IoT is not only hardware and software paradigm, but also include interaction and social aspects as well [3]. The architecture of IoT is usually considered to be 3-layer, with Perception layer, Network layer, and Application layer, but some [4][2] add two more layers: Middleware layer and Business layer. This five layer architecture is described in figure 1.

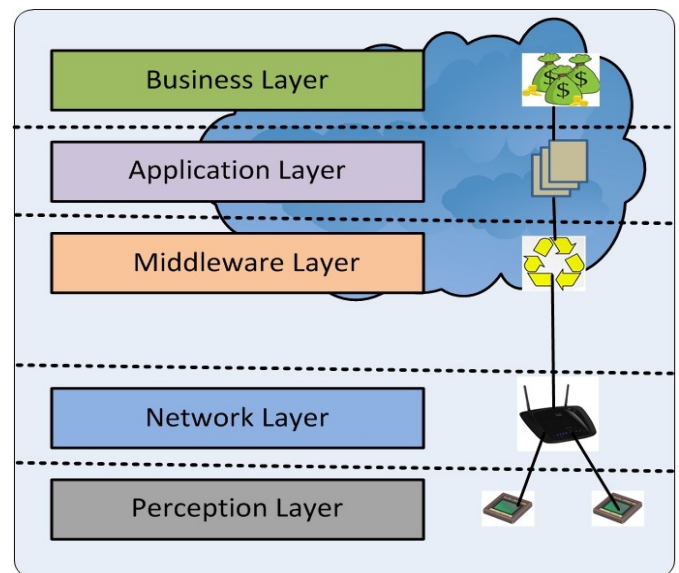


Figure 1. Internet of Things layers

Perception layer is the lowest layer in the IoT architecture. As the name suggests, its purpose is to perceive the data from environment. All the data collection and data sensing part is done on this layer [5]. Sensors, bar code labels, RFID tags, GPS, and camera, lie in this layer. Identifying object/thing and gathering data is the main purpose of this layer.

Network layer collects the data perceived by the Perception layer. Network layer is like the Network and Transport layer of OSI model. It collects the data from the lower layer and sends to the Internet. Network layer may only include a gateway, having one interface connected to the sensor network and another to the Internet. In some scenarios, it may include network management center or information processing center.

Middleware layer receives data from Network layer. Its purpose is service management and storage of data. It also performs information processing and takes decisions automatically based on results. It then passes the output to the next layer, the Application layer [4].

Application layer performs the final presentation of data. Application layer receives information from the Middleware layer and provides global management of the application presenting that information, based on the information processed by Middleware layer. Depending upon the type of devices and their purpose in Perception layer and then on the way they have been processed by the Middleware layer, according to the needs of user, Application layer presents the data in the form of: smart city, smart home, smart transportation, vehicle tracking, smart farming, smart health and other many kinds of applications [4].

Business layer is all about making money from the service being provided. Data received at the application layer is molded into a meaningful service and then further services are created from those existing services. Furthermore, information is processed to make it knowledge and further efficient means of usage make it wisdom, which can earn a good amount of money to the service provider.

IoT works on the basis of Machine-to-Machine (M2M) communications, but not limited to it. M2M refers to communication between two machines, without human intervention. In IoT, even non-connected entities can become part of IoT, with a data communicating device, like a bar-code

or an RFID tag, sensed through a device (may even be a smart phone sensing it), which eventually is connected to the Internet. In IoT, non-intelligent objects, known as ‘things’ in IoT terminology, become the communicating nodes.

### B. Cloud Computing

Cloud computing, the recent trend in IT, takes computing from desktop to the whole World Wide Web and yet, the user doesn’t need to worry about maintenance and managing all the resources. User has to bear only the cost of usage of service(s), which is called, pay-as-you-use, in cloud computing terms. With this cloud computing, a smart phone can become an interface to large data center. Cloud computing is extended form of distributed computing, parallel computing, and grid computing [6], [7], [8], and [9]. Cloud computing provides ubiquitous access to the content, without the hassle of keeping large storage and computing devices. Sharing large amount of media content is another feature that cloud computing provides.

## II. CLOUD OF THINGS

We are moving towards web3, the ubiquitous computing web. Since 2011, number of connected devices has already exceeded the number of people on Earth. Already, connected devices have reached 9 billion and are expected to grow more rapidly and reach 24 billion by 2020 [10]. Since, number of connected devices is rapidly increasing, so there is going to be a lot of data as well. Storing that data locally and temporarily will not be possible any more. There is going to be a need of rental storage space. Also, this huge amount of data must also be utilized in the way it deserved. Data must not only be processed to form information and further, to form knowledge, but it should be made a mean of wisdom for the user. This asks for more processing, which is not possible at the IoT end, where devices are low cost and light-weight. Again, processing and computation must also be available there on rental basis. All this is possible with cloud computing. IoT and cloud computing working in integration makes a new paradigm, which we have termed here as Cloud of Things (CoT). Figure 2 presents an overall communication pattern of CoT.

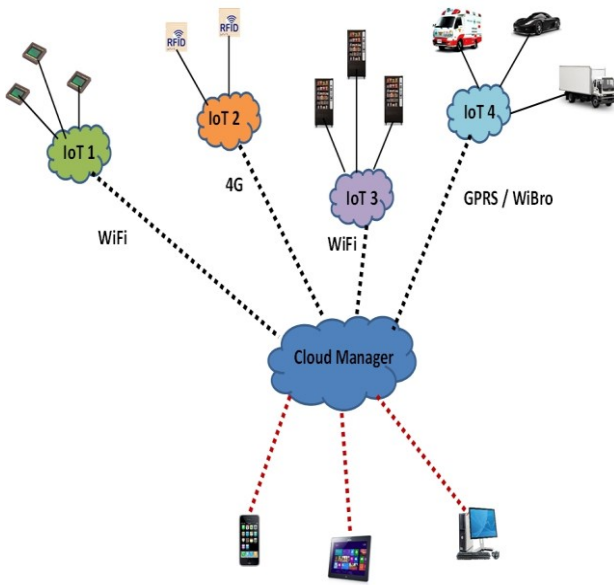


Figure 2. IoT's and cloud – data communication

### III. ISSUES IN CLOUD OF THINGS

It is not going to be that simple to allow everything become part of IoT and then having all the resources available through cloud computing. There lies some issues that have to be taken care of to allow CoT prevail, for the betterment of the world in general and humanity in specific. Other than data and resources, cloud has to deal with the business point of view as well. CoT will create more business opportunities, making it bigger threat from the attackers. Security, privacy, and specially, identity protection becomes very important in hybrid clouds, where there is an essence of private and public clouds, used by businesses [10]. In CoT, heterogeneous networks will be involved, which support different types of data and services. The network must have the flexibility to support all types of data, according to their requirements, with QoS support [10]. Some of the key issues are discussed below.

#### 1) Protocol support

For different things to be connected to the Internet, different protocols will be there in use. Even if there are homogenous entities, for example a sensor IoT, then there is a possibility that sensors may be working on different protocols, like: WirelessHART, ZigBee, IEEE 1451, and 6LOWPAN. As shown in figure 3, some of the protocols will be supported by the gateway device, while some protocols might not have a support.

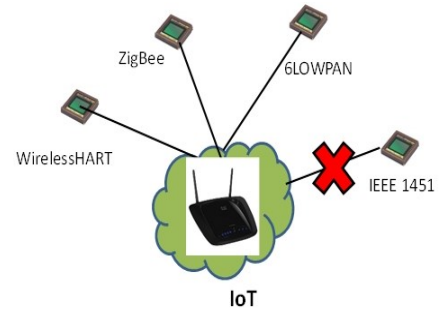


Figure 3. Protocol support, an example

It all depends upon the gateway as well as the sensor being used. In user's perspective, cheaper or easily available sensor would be a preference. So, it cannot be guaranteed whether a newly added sensor will be successfully configured or not. Solution to this kind of problem may be mapping of standardized protocols in the gateway.

#### 2) Energy efficiency

With sensor networks everywhere and connectivity with the cloud will lead to a lot of data communication, which consumes a lot of power. A typical wireless is composed of four components: sensing unit, processing unit, transceiver, and power unit. In case of video sensing, video encoding and decoding, power plays a vital role. Normally, video encoding is more complex, as compared to decoding. The reason behind this is that for efficient compression, the encoder has to analyze the redundancy in the video [1]. It is not going to be suitable to have a temporary power supply, like batteries and have to replace them every now and then. With billions of sensors and low power devices, it is beyond possibility. Having efficient usage of energy and rather permanent power supply would be required. There should be means for sensors to generate power from the environment, like, solar energy, vibration, and air [11]. Also, effective sleep mode can be very handy in this regard as well.

#### 3) Resource allocation

When IoT's of entirely different and unexpected things would be asking for resources on a cloud, resource allocation would be a challenge. Because it would be very difficult to decide how much a particular resource may be required by an entity or a particular IoT. Depending upon the sensor and the purpose for which sensor is being used, the type, amount, and frequency of data generation, resource allocation has to be

mapped. Sending a sample packet from the newly added node can also be useful.

#### 4) Identity management

Communicating nodes over the Internet are identified uniquely. When objects are becoming part of Internet (IoT), they also need a unique identification. Also, in case of mobile devices, like mobile sensor nodes on vehicles and other objects, need to have identity mapping in the new network they have just entered. Since IPv6 address space is believed to be enough to support even this kind of ubiquitous networking, assigning IPv6 addresses can be more than a reasonable way in this regard.

#### 5) IPv6 deployment

If IPv6 is to be used for the identification of communicating objects, then formal deployment of IPv6 would also be an issue. Unless a proper, standardized, and efficient mechanism of IPv4-IPv6 coexistence is adopted, objects being assigned IPv6 would be of no great benefit. We present more work on it in [13].

#### 6) Service discovery

With Cloud of Things, the cloud manager or broker has the responsibility to discover new services for the users. In IoT, any object can become part of it at any moment and can leave the IoT at any moment. Some of the IoT nodes may also be mobile. It would be an issue to discover new services and their status and update the service advertisement accordingly. For complex and bigger IoT's, there may be a need of IoT manager as well, which can perform the responsibility of managing the status of IoT nodes, track mobile nodes and keep the updated status of existing nodes and newly added nodes of its IoT. A uniform way of service discovery would be required for this purpose.

#### 7) Quality of Service provisioning

As the amount of data increases and the type and unpredictability also comes into play, QoS becomes an issue. At any moment, any type and amount of data can be triggered. It may also be an emergency data as well. Dynamic prioritization of the requests would be required on cloud side [10]. QoS would mostly be measured in terms of bandwidth, delay, jitter, and packet loss ratio [14]. Depending upon the type of data and its urgency to be sent to the sync node, QoS must be supported. We have extended our work in [14].

#### 8) Location of data storage

Location also matters for critical and latency or jitter sensitive data. Time sensitive data, like video, should be stored in the closest possible physical location to the user, so that minimum possible time should be involved in accessing big data. For multimedia data, nearest possible virtual storage server must be allocated.

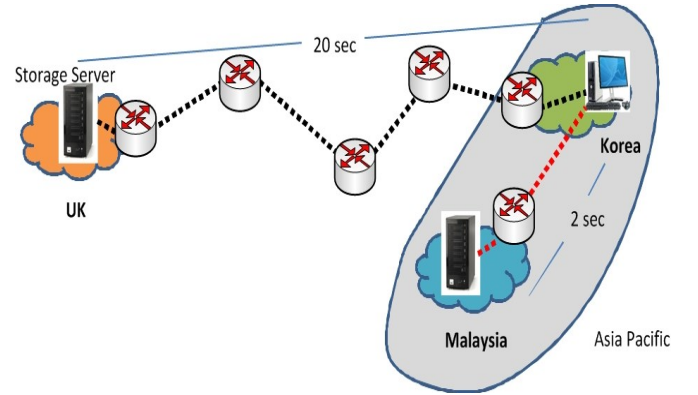


Figure 4. Location of data storage on the cloud

#### 9) Security and privacy

Security and privacy will become more of an issue with the kind of ubiquitous computing we are going to have in future. Data security would be an issue on IoT side as well as on cloud side. Similarly, in terms of privacy, more concern would be there. On Feb 01, 2013, it was read on The Independent [12], stating, "British internet users' personal information on major 'cloud' storage services can be spied upon routinely by US authorities". So, sensitive or private data must also be stored in a virtual storage server located inside the user's country or trusted geographical domain, which can be a friendly country as well.

### IV. SMART GATEWAY BASED COMMUNICATION

Extending our study in [16], we present smart CoT communication in this section.

When anything would be able to connect to the Internet and generate data, there is a possibility that at some stage it is no longer necessary to upload the data to the cloud or sync device. Momentarily, the data may not be required. In that scenario, either the device must be stopped from generating data or gateway device must decide when it is required to stop uploading the data and not to consume resources of the network and cloud, for that while. It will also help in efficient



utilization of power. For this purpose, the gateway device, connecting IoT to the cloud, should be having extra functionality to do a little processing before sending it to the Internet and eventually to the cloud. Based on the feedback from application, gateway must decide the timings and type of data to be sent. This kind of a gateway, we refer it here as ‘smart gateway’ would help in better utilization of network and cloud resources. The data collected from wireless sensor networks and IoTs will be transmitted through gateways to cloud. The received data is then stored in the cloud and from there it is provided as a service to the users. The generic communication of smart gateway with cloud and IoTs is presented in figure 5.

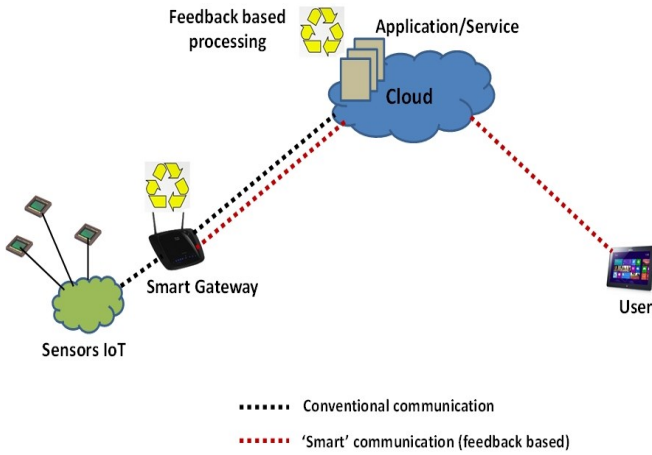


Figure 5. Smart gateway, communicating data only when it is needed

#### A. Fog computing and Smart Gateway architecture

Smart gateway has to manage various aspects of underlying IoTs. Smart gateway performs a number of tasks, like, collecting the data and performing preprocessing, filtering the data and reconstructing it into more useful form, uploading only necessary data to the cloud, keeping check on IoT objects and sensors’ activities, keeping check on energy consumption of power constrained nodes of IoTs, security and privacy of the data, and overall service monitoring and management.

Fog Computing refers to bringing networking resources near the underlying networks. It is a network between the underlying networks and the clouds. Fog Computing extends the traditional Cloud Computing paradigm to the edge of the network, enabling creation of refined and better applications and services. Fog Computing is a highly virtualized platform,

which provides computation, storage, and networking services between the end nodes in an IoT and traditional Clouds [15]. Fogs are not exclusively located at the edge of network. For smart communication, Fogs are going to play an important role. For many of the tasks a gateway has to perform, it is not possible for a gateway to do effectively being standalone. The underlying nodes and networks are not always physical. Virtual sensor nodes and virtual sensor networks are also requirements for various services. Similarly, temporary storage, preprocessing, data security and privacy, and other such tasks can be done easily and more efficiently in the presence of a smart network or Fog, co-located with the smart gateway. Fog computing allows real-time delivery of data, specially for delay sensitive and healthcare related services. It can perform the preprocessing smart tasks and notify the cloud, before cloud could further adapt that data into enhanced services.

Keeping in view all these things, the smart gateway is presented in layered architecture in figure 6. In the Physical and Virtualization layer, physical nodes, wireless sensor networks, virtual nodes, and virtual sensor networks are managed and maintained according to the needs. Monitoring layer monitors the activities of the underlying nodes and networks. Which node is performing what task, at what time and what is required from it next is monitored here. Other than this, the power constrained devices or nodes are monitored on their energy consumption basis as well, so that effective measures can be taken in time. Preprocessing layer performs data management related tasks. It analyzes the collected data, performs data filtering, trimming, and in the end, more meaningful and necessary data is generated. Data is then temporarily stored on the Fog resources. Once the data is uploaded on the cloud and it is no more required to be stored locally, that data is then removed from the storage media. IoTs and WSNs may generate some private data as well. Ubiquitous healthcare and smart healthcare services generate private data of the patients. Similarly, location aware data may also be sensitive in some cases, which should be made secure. This is where Security layer comes into play. In the end, the ready-to-send data is then uploaded to the cloud, burdening the core only to the extent it had to be burdened and allowing cloud create more useful services. Transport layer handles this task.

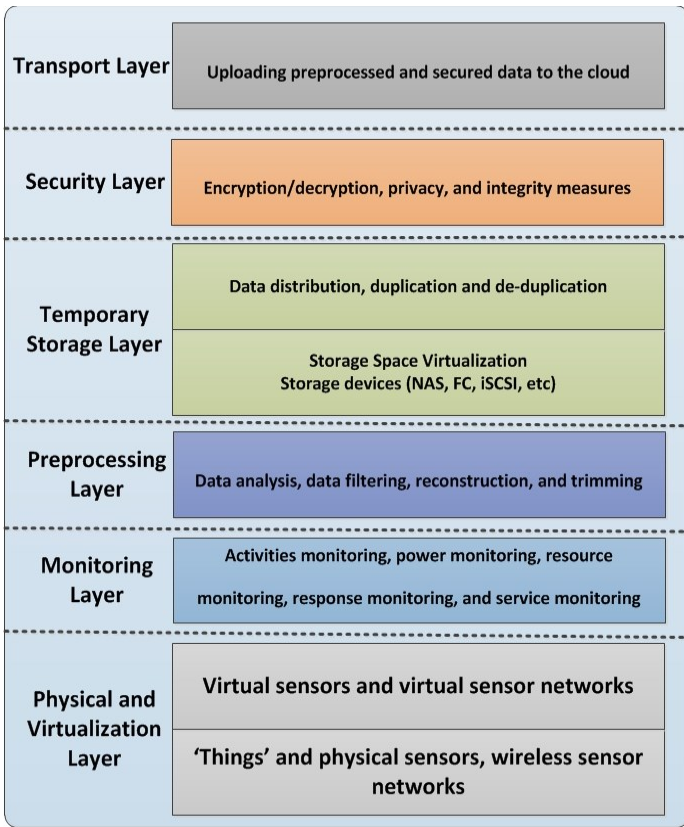


Figure 6. Smart gateway layered architecture.

## V. CONCLUSION AND FUTURE WORK

This paper discusses about the expanding IoT's and their integration with cloud computing, for enhanced and more useful service provisioning to the user and efficient utilization of resources. This integration or working in coordination, termed here as Cloud of Things (CoT), involves some key challenges as well, which have been discussed in this paper. More study on the impact of these issues, specially, keeping in view the type of IoT and type of service being provided, can be done in the future. Some of the data being generated by a specific IoT may require special type of storage and development of application on it. This can as well be a potential future work in this regard.

## ACKNOWLEDGEMENT

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2013- H0301-13-4006) supervised by the NIPA (National IT Industry Promotion Agency). The corresponding author is Prof. Eui-Nam Huh.

## REFERENCES

- [1] Yen-Kuang Chen, "Challenges and Opportunities of Internet of Things", in the proceedings of 17<sup>th</sup> Asia and South Pacific Design Automation Conference, 30 Jan. – 02 Feb., 2012, Santa Clara, CA, USA.
- [2] Miao Wu et. al., "Research on the architecture of Internet of things", in the proceedings of 3<sup>rd</sup> International Conference on Advanced Computer Theory and Engineering, 20-22 August, 2012, Beijing, China,
- [3] Gerd Kortuem, Fahim Kawsar, Daniel Fitton, and Vasughi Sundramoorthi, "Smart Objects and Building Blocks of Internet of Things", IEEE Internet Computing Journal, volume 14, issue 1, pp. 44-51, Jan.-Feb., 2010
- [4] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", in the proceedings of 10<sup>th</sup> International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17-19 December, 2012.
- [5] Dieter Uckelmann, Mark Harrison, and Floria Michahelles, "Architecting the Internet of Things," Springer-Verlag Berlin Heidelberg, 2011.
- [6] Shuai Zhang et. al., "Cloud Computing Research and Development Trend", in the proceedings of International Conference on Future Networks, 22-24 Jan., 2010, Sanya, China.
- [7] W Ma et. al., "The Survey and Research on Application of Cloud Computing", in the proceedings of 7th International Conference on Computer Science and Education, 02-04 November, 2012, Wuyishan Mountain, China.
- [8] Y. Jadeja, et. al., "Cloud Computing - Concepts, Architecture and Challenges", in the proceedings of International Conference on Computing Electronics and Electrical Technologies, 21-22 March, 2012, Nagercoil, India.
- [9] Minqi Zhou et. al., "Services in the Cloud Computing Era: A Survey", in the proceedings of 4th International Universal Communications Symposium, 18-19 October, 2010, Beijing, China.
- [10] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", Technical Report CLOUDS-TR-2012-2, July 2012.
- [11] Dave Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", Whitepaper, Cisco Internet Business Solutions Group (IBSG), April 2011.
- [12] "British internet users' personal information on major 'cloud' storage services can be spied upon routinely by US authorities", The Independent, 30 January, 2013, available at: <http://www.independent.co.uk/life-style/gadgets-and-tech/news/british-internet-users-personal-information-on-major-cloud-storage-services-can-be-spied-upon-routinely-by-us-authorities-8471819.html>.
- [13] Mohammad Aazam and Eui-Nam Huh, "Impact of IPv4-IPv6 Coexistence in Cloud Virtualization Environment", Annals of Telecommunications, vol. 68, DOI: <http://dx.doi.org/10.1007/s12243-013-0391-6>, August 2013.
- [14] Mohammad Aazam, Adeel M. Syed, Eui-Nam Huh, "Redefining Flow Label in IPv6 and MPLS Headers for End to End QoS in Virtual Networking for Thin Client", in the proceedings of 19<sup>th</sup> IEEE APCC, Bali, Indonesia, 29-31 August, 2013
- [15] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, "Fog Computing and Its Role in the Internet of Things", in the proceedings of ACM SIGCOMM, August 17, 2012, Helsinki, Finland.
- [16] Mohammad Aazam, Pham Phuoc Hung, Eui-Nam Huh, "Cloud of Things: Integrating Internet of Things with Cloud Computing and the Issues Involved", in the proceedings of 11<sup>th</sup> IEEE IBCAST, 14-18 January, 2014, Islamabad, Pakistan.