Quality of Service Architecture for Internet of Things and Cloud Computing

Daisy Premila Bai T.
Research Scholar
Dept. of Computer Science
St.Joseph's College
Tiruchirappalli,TamilNadu, India

Albert Rabara S.
Associate Professor
Dept. of Computer Science
St.Joseph's College
Tiruchirappalli,TamilNadu, India

Vimal Jerald A.
Research Scholar
Dept. of Computer Science
St.Joseph's College
Tiruchirappalli,TamilNadu, India

ABSTRACT
Internet of Things (IoT) and Cloud Computing paradigm is a next wave in the era of computing and it has been identified as one of the emerging technologies in the field of Computer Science and Information Technology. The complementarity of these two technologies play a major role in accessing any services and applications anywhere, anytime in the smart environment. But from the literature study, it has been understood that the integration of IoT and cloud computing is in its infantile phase and it has not been extended to all application domains due to its inadequate quality of service architecture. Hence, in this paper a novel, quality of service architecture for internet of things and cloud computing is proposed. This architecture facilitates the public to have an easy access over diversified smart applications and services distributed in the cloud with one IoT enabled Intelligent Smart Card (ISC) through mobile devices with assured quality of service. The cloud services are integrated and connected through an Internet Protocol / Multi Protocol Label Switching (IP/MPLS) core System. The QoS requirements are met with differentiated services. The performance of the proposed architecture is tested by establishing a test bed in a simulated environment.

General Terms
Architecture, Performance Analysis.

Keywords
Internet of Things, Cloud Computing, Quality of Service, IP/MPLS, Diffserv.

1. INTRODUCTION
Integrating Internet of Things (IoT) and Cloud Computing, play a vital role in the field of Information Technology [1]. Internet of things is not a single technology, it is a concept in which many of the new things are getting connected and networked. The vision of the IoT is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path or network and any service in heterogeneous environments [2]. IERC states that "Internet of things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interface and are seamlessly integrated into the information network"[3]. In a nutshell, IoT is characterized by the real world of smart objects with limited storage and processing power [4]. In contrast, Cloud Computing is characterized by virtual world with unlimited capability in terms of storage and processing power. According to NIST, "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction" [5]. Cloud computing allows computer users to conveniently rent access to fully featured applications, to software development and deployment environments, and to computing infrastructure assets such as network-accessible data storage and processing with its salient features of on-demand self-service, broad network access, resource pooling, rapid elasticity and measured Service [6].

Though the cloud and IoT have emerged as independent technology, merging these two brings renaissance in the field of future networks. Internet of Things can be enhanced by the unlimited capabilities and resources of cloud to compensate its technological constraints such as storage and processing. On the other hand, cloud can extend its scope to the real world through IoT in a more dynamic and distributed way to deliver new applications and services in a real time scenario at large scale. Consequently, integrating IoT and Cloud, the complementary technologies will enhance the smart world to reach the heights of availing any services and applications anywhere, anytime, any firm and any device irrespective of any underlying technology [7].

Since, the integration of IoT and Cloud in its developmental stage, there are a few significant challenges exist which need to be resolved while taking initiative in creating a smart world. The varied issues are interoperability, security, QoS, load balancing, mobility, IPv6 deployment, data management solution and acceptability of IoT applications by users and citizens [8]. The review of the literature expresses that there is an impelling need to enhance the quality of service which is very much vital and fundamental in IoT and Cloud. Moreover the dynamic nature of the internet of things and cloud computing require QoS attributes that are capable of delivering real time services with assured quality [9]. In this scenario, Qos is considered to be the most important parameters of the network capable of providing better services to the users and the providers where QoS should have a architecture consisting of standards which could be widely used in communication networks to improve overall performance by managing the traffic. Several research efforts have been taken to meet the QoS requirements, yet there is a need for unified, integrated QoS architecture for the internet of things and cloud computing [10].

Hence, in this paper a novel QoS architecture for the internet of things and cloud computing has been proposed. Traffic filtering, queue scheduling, congestion management, load balancing, end to end delay management for real time service

and resource allocation across the core for multiple customer types are the inherited unique features of the proposed QoS architecture.This paper is organized as follows. Section 2 briefs the review of the literature with regard to the recent work done in building QoS architecture for the Internet of Things and Cloud Computing. Section 3 describes the proposed architecture. Section 4 explains the experimental setup and the performance analysis. Section 5 concludes the paper.

2. REVIEW OF LITERATURE

A wide range of research results have been found for QoS support in traditional networks, but, only a few research efforts are found with IoT and Cloud although it provides an exciting and promising vision for seamlessly connecting the virtual world of information to the real world.Dores et al. [11] have discussed the state of the art technologies such as Next Generation Networks (NGN), Internet of Things (IoT), Wireless Sensor Networks (WSN), Body Sensor Networks (BSN) and Cloud Computing and have evoked the need for the integration of the technologies in making the future internet a reality. The authors have adopted 'Skynet' a free and open source platform for the development of IoT Cloud integration. Skynet is connected to cloud database and the IoT devices through communication protocols. This platform has the ability to register network devices, to store, update and exchange information. The information is not ciphered and the privacy of the information is not ensured and also the senders and receivers are not authenticated via secure connections. Subsequently, this open communication system is recommended only to the scenario, where the information can be seen and altered by everybody like an air-conditioner thermostat. The authors have also performed a QoS test in terms of delay and jitter and have suggested that more research work is needed to enhance QoS with varied aspects which will assure guaranteed quality of services to users and the providers.

Mohamed et al. [12] have coined the term 'Cloud of Things' (CoT) for IoT and Cloud Computing Integration. The authors have described the necessity of integrating these two paradigms and the various issues involved in this context. They have presented the motive for the CoT as: the ever increasing connected devices share a lot of data which cannot be locally or temporarily stored on the devices and the need foreseen is rental storage space and the efficient utilization of the data and the resources. It demands more processing and computation on rental basis, which is very hard to be realized at the IoT end, while cloud computing makes this achievable. This integration phenomenon creates more business opportunities and equally larger threats from the attackers. Some of the key issues of CoT are protocol support, energy efficiency, resource allocation, identity management, service discovery, quality of service provisioning, IPv6 deployment, data storage location, security and privacy and unnecessary communication of data. The authors have claimed that QoS is one of the major concerns since the amount of data increases at any moment and any type of data can be triggered. The authors have said that the dynamic prioritization of the request is required along with the QoS requirements such as bandwidth, delay, jitter and packet loss.

Giuseppe et al. [13] have proposed a QoS monitoring as a Service architecture (QoSMoNaaS) for cloud services with a substantial study on Internet of Things applications. QoSMoNaaS provide a dependable monitoring facility which is realized as a pilot application in an SRT-15 project (Subscription Racing Application for 2015) a new cloud based platform to connect future internet (FI) applications and services. In this model SLA analyzer collects the information received by Key Performance Indicator (KPI) meter, analyses them and infers the values and gives back to the KPI meter. The Breach Detector (BD) combines the output of the KPI monitor and the SLA analyzer to find the contract violations. The violation certifier enhances the results of the BR with timestamp and digital signature. This model enhances QoS monitoring facility to the realistic FI applications. The authors have insisted that the dynamic nature of cloud computing and internet of things require the QoS attributes which are capable of delivering real time services and applications with guaranteed quality.

Ren et al. [14] have proposed a QoS architecture for IoT as the result of their thorough analysis of the existing QoS mechanism with regard to the characteristics of IoT in a layered basis, such as application layer, network layer and perception layer which insisted the need for the reliable QoS architecture. Enumerating the QoS requirements for each layer, the authors have designed control mechanism for transferring and translation of QoS requirements from top to down. They have also designed cross-layer QoS management facility and brokers residing in the lower layers to support the control-mechanism. The authors have explained that the IoT's QoS problem can be solved by measuring the performance of the service and making clear QoS indicators as well as the interrelationship among them. The application and service layer directly answers the customer's requirement, while the network layer fuses and transmits the information to modules in the upper layer and the perception layer is responsible for perceiving and collecting data. The authors, explaining the functions of each layer of their proposed work they did recommend that the research work is further needed to assure an end to end quality in availing and providing services in smart environment as IoT is integrated with heterogeneous networks.

The existing research on IoT and Cloud demands the necessity for dynamic prioritization of the request along with the QoS requirements which are capable of delivering real time services and applications with guaranteed quality. Hence, in this paper a novel Quality of Service architecture for the Internet of Things and Cloud Computing is proposed.

3. PROPOSED GENERAL ARCHITECTURE

The proposed general architecture for the Internet of Things and Cloud Computing is envisaged to offer smart services and applications anywhere, anytime, any firm, any device and any network independent of any underlying technologies with one IoT enabled Intelligent Smart Card (ISC). ISC eases the access of diversified applications and services distributed in a cloud environment with one Unique Identification (UID) number per citizen through the intelligent systems. The intelligent system processes the data at smart gateway and then uploads the necessary data to the cloud through IP/MPLS core network. Figure 1 depicts the proposed general architecture. Intelligent systems are considered to be the customer site and the cloud is considered to be the provider site. Weighted random early detection (WRED) is applied on the egress interface that is intelligent system facing the core network and the network core facing the interfaces of a provider site. The destination router forwards the IP packet based on the bottom label to its correct destination to ensure end to end quality.

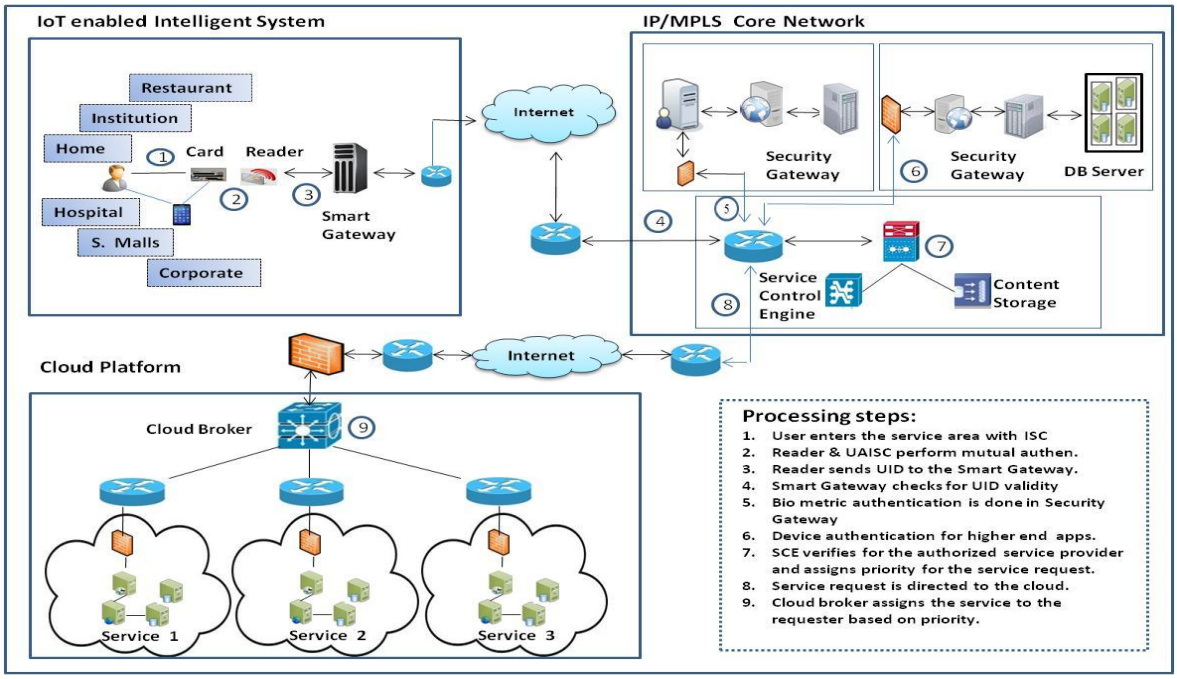

Fig 1: Proposed General Architecture

3.1 QoS Architecture

Quality of Service provides better services to a set of identified users to enhance the experience of service (EoS). Service providers and enterprise use QoS framework for mapping customer traffic to a Class of Service (CoS) queue with a goal of providing end to end QoS to the customer traffic. Though there are common applications and protocols exist in the heterogeneous network within the smart environment, each network has its own unique traffic types in addition to the common ones. To implement QoS it is a prerequisite to study and identify the traffic types and to define the QoS requirements for each identified traffic type. The proposed Qos architecture incorporates RFC – 4594 guidelines for QoS marking and provisioning which enables end to end QoS in a smart environment. In the proposed QoS architecture, IP/MPLS core which integrates both Internet of things and cloud computing has the ability to differentiate traffic types per port, MAC address, IP address and TCP/UDP port that are essential for prioritization of real time and business critical services in order to provide services with assured quality. Figure 2 depicts the functioning of the QoS model.

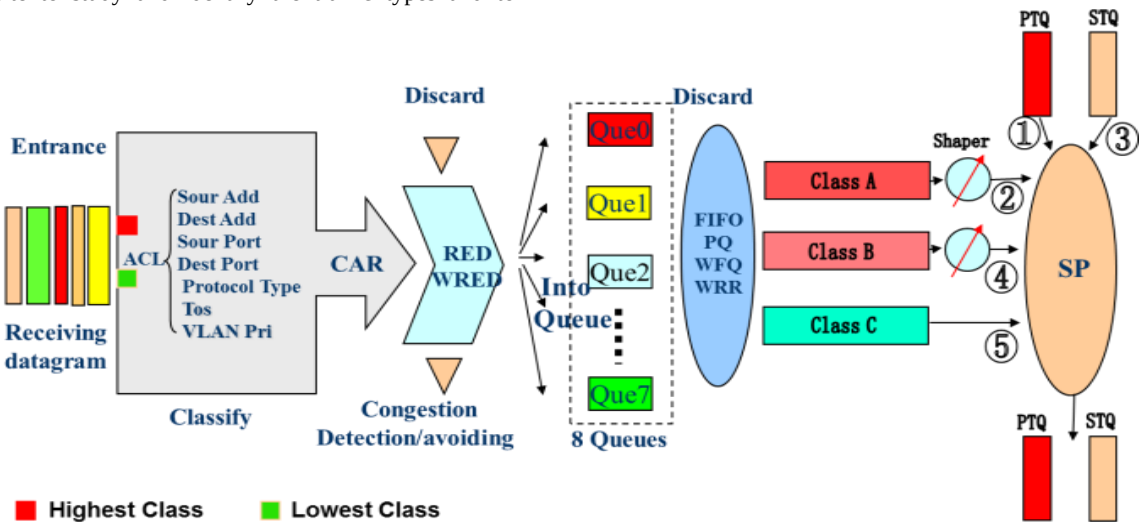

Fig 2: Functioning of the QoS Model

When service is requested by the customer, service control engine in the IP/MPLS core receives IP traffic and performs packet classification and applies the MPLS label and appropriate experimental bits pertaining to the service requested. Experimental bits are used as the classifier for mapping traffic into the various QoS classes. Class of Service (CoS) values are used to classify traffic at the network edge. The proposed architecture supports multiple protocols that serve different customers, services and applications. This support for multiple protocols and technologies have unique approaches to provide guaranteed QoS. Customers and service providers are in different Diffserv domains. The service provider's Diffserv begins at the ingress provider's Edge (PE's) ingress interface and terminates on the egress of the PE's ingress interface. The service provider could enforce its own Diffserv policy and

preserve the customers' Diffserv information through the MPLS VPN cloud in order to provide end to end QoS.The service control engine receives the IP traffic, performs packet classification and applies the MPLS label and EXP bits. The value for the MPLS EXP is set explicitly on the ingress PE's ingress interface, according to the service provider's administrative policies. In the case of any re-marking occurrence within the service provider's MPLS VPN cloud, changes are done only in MPLS EXP re-marking which are not propagated down to the underlying IP packet's Type of Service (ToS) byte. This helps in implementation of CE to CE quality of service by using six class Diffserve (Differentiated Services) model in the core and 3 class model in the customer edge for mapping. MPLS DiffServ tunneling is used to end-to-end Differentiated Services. Since the end to end is more granular and more extensible, Differentiated Service Code Point (DSCP) markings are used. Figure 3 depicts the proposed QoS architecture which includes QoS for Customer Edge and Provider Edge QoS and QoS at the Core.

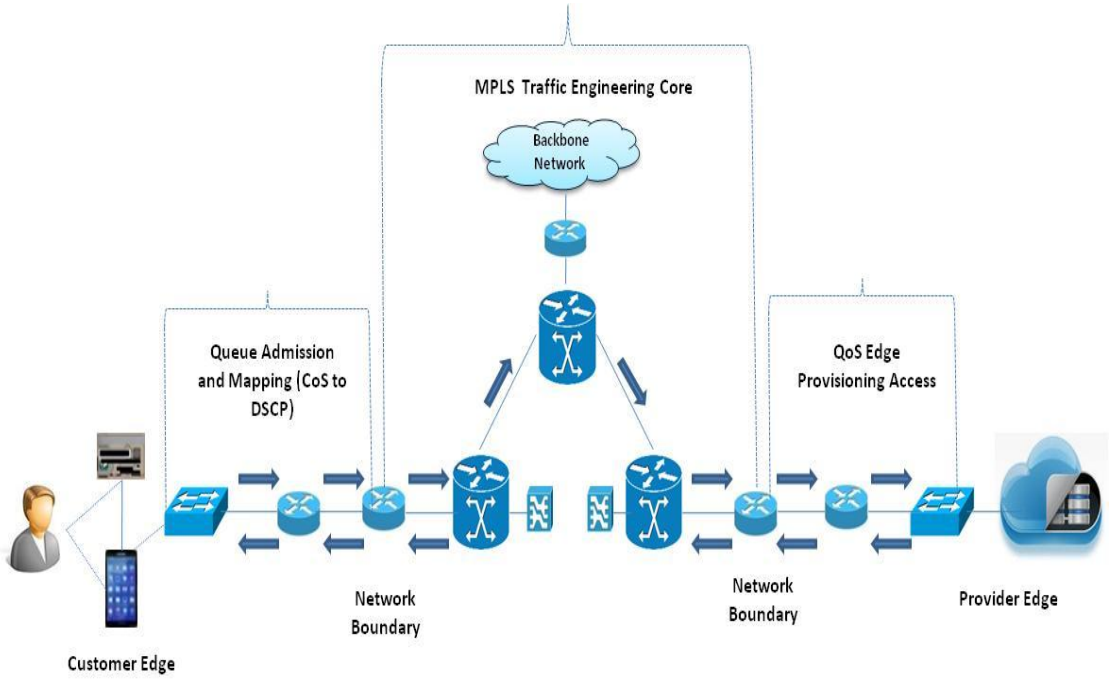

Fig 3. Proposed QoS Architecture

In policing and marking, the unwanted traffic drops at a subsequent node, especially when the unwanted traffic is the result of Denial of Service (DoS) or worm attacks. Queuing and dropping marks the critical applications such as health care which requires service guarantees regardless of network conditions and provides service guarantees even at the time of congestion.This model is generated end to end not only to Campus-to-WAN/VPN edges, but also to campus Access-to-Distribution or Distribution-to-Core links, where over subscription ratios create the potential for congestion. This guarantees end to end QoS.

4. EXPERIMENTAL STUDY

The objective of the experimental study is to test the performance of the proposed system with respect to response time in general and service based response time. The proposed architecture is tested in a simulated environment. Ixia generator is used for traffic generation and to analyze the overall performance under different priority service with different load type. System throughput of the proposed system is tested with Jmeter tool, the open source.The test lab is equipped with smart gateway, IP/MPLS core switch, security gateway and the required servers. Service control engine in the IP/MPLS core processes the requests according to the priority assigned with Class of Service and the response time is recorded for the sample data. System throughput of the proposed system is tested with Jmeter tool, the open source.

4.1 Performance Analysis on Ping Response Time

To analyse the response time for the proposed system, the sample data set for the requesters ranges from 50 to 400 with the increase of 50 requesters is taken, assuming each requester's data is about 3 kbps. Traffic is generated with IXIA generator for about 24 Mbps, providing the bandwidth for about 12 mbps. Table 1 presents the data and Figure 4 depicts the response time taken by the proposed system for 4000 requesters.

Table 1. Ping Response Time

No. of Users	Bandwidth (Mbps)	Round Trip Delay (Ms)	Drops %
50	1.464844	8	0%
100	2.929688	8	0%
150	4.394531	9	0%
200	5.859375	10	0%
250	7.324219	10	0%
300	8.789063	10	0%
350	10.25391	10	0%
400	11.71875	10	0%

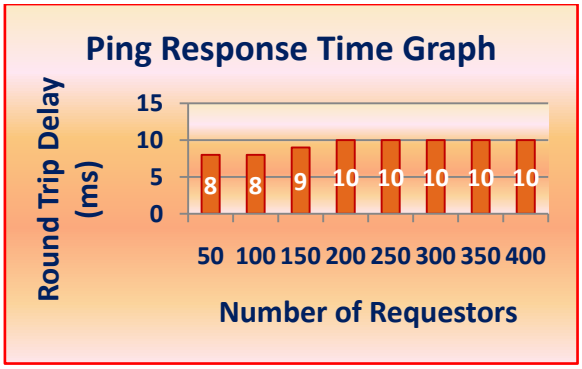

Fig 4: Ping Response Time Graph

The results show that there is only minimal delay which is just 10 milliseconds, even for the 4000 requests. It proves the efficiency of the proposed system in processing the requests faster with no drops of the packets.

4.2 Performance Analysis on Priority based Response Time

There are 500 requesters requesting for various services such as 100 for health care, 100 for transportation, 100 for corporates, 100 for restaurant booking and 100 for banking. Assuming each requester's data is about 3 kbps, the total bandwidth allocated is 1 Megabit. When the request reaches the control engine, it classifies the services and process the data according to the priority. Table 2 presents the results obtained for the priority based response time for various requests. Higher priority services are served without any delay. Low priority services are queued and will be processed accordingly. According to the graph, requests for the health care service has no delay, banking has processed 97% of the request leaving only 3% to be in queue, transportation has processed 92% of the requests leaving the 8 % to be in queue, Restaurant has processed 90% request and leaving the 10% to be in queue and corporates have processed 85% leaving only 15% to be in queue.

Table 2. Priority based Response Time

Services	No. of Users	Packet Drops (%)	Bandwidth (Mbps)
Health Care	100	0	0.292968750
Banking	100	3	0.284179688
Transportation	100	8	0.205078125
Restaurant	100	10	0.146484375
Corporates	100	15	0.958007813

The results show that the system intelligently prioritizes the services and processes the requests accordingly.

4.3 Performance Analysis on System Throughput

The performance test is carried out to measure the system throughput. It represents the amount of the work, the proposed system does at a given time. To analyze the system throughput, Jmeter, an open source tool is used. Sample tests have been done with 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110 and 120 service requesters, requesting for the service through the proposed system. The system throughput increases gradually up to 10 requests and keeps rapidly increasing till 120. At one point, the system has reached the saturation point due to various factors and the throughput declines. However, the proposed system provides responses to the service requests with a reasonable response time. The overall system throughput is depicted in Figure 5.

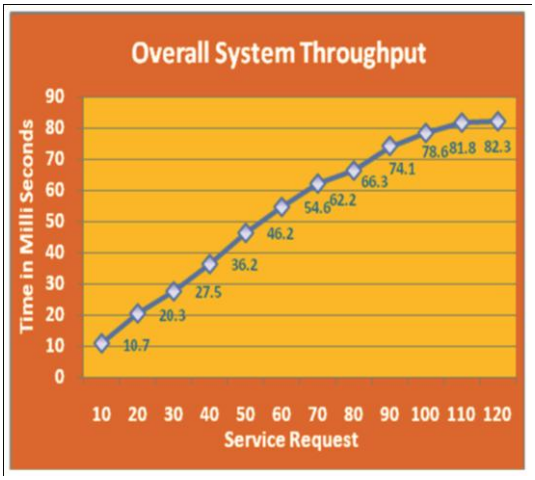

Fig 5: System Throughput

The performance results prove that the proposed system is very efficient in processing the request with guaranteed end to end quality of service and the time taken to process the request is relatively less.

5. CONCLUSION

The proposed quality of service architecture for Internet of Things and Cloud Computing uses differentiated services to meet the QoS requirements. The performance analysis proves that the proposed architecture is efficient and capable of delivering real time services with assured quality of service. The future work is to establish the security architecture for IoT and Cloud and to implement the same in real time scenario.

6. REFERENCES

[1] Gubbi,J., Buyya,R., Marusic,S., and Palaniswami,M. 2013. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Future Generation Computer Systems.

[2] Vermesan, O., and Friess,P. 2014. Internet of Things from Research and Innovation to Market Deployment, River Publishers Series in Communications.

[3] Vermesan, O., and Friess, P. 2013 Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers Series in Communications.

[4] Roman, R.,Najera, P., and Lopez,J. 2011. Securing the Internet of Things, IEEE Computer.

[5] Badger, L., Grance, T., Corner, R.P. and Voas, J. 2011, DRAFT Cloud Computing Synopsis and Recommendations, National Institute of Standards and Technology.

[6] Buyya,R., Broberg, J., and Goscinski,A. 2011. Cloud Computing Principles and Paradigms, WILEY.

[7] Atkins, C., Koanagi,K., Tsuchiya,T., Miyosawa,T., Hirose, H., and Sawano, H. 2013. A Cloud Service for End-User Participation Concerning the Internet of Things, Proceeding of IEEE Conference on Signal-Image Technology and Internet-Based Systems (SITIS), IEEE.

[8] Pereira, P.P., Eliasson, J., Kyusakov, R., Delsing, J., Raayatinezhad, A., and Johansson, M., 2013. Enabling Cloud Connectivity for Mobile Internet of Things Applications" Proceedings of IEEE Symposium on Service Oriented System Engineering (SOSE), IEEE.

[9] Aguzzi, S., Bradshaw, D., Canning, M., Cansfield, M., Carter, P., Cattaneo, G., Gusmeroli, S., Micheletti, G., Rotondi, D., and Stevens, R.. 2013. Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Final Report, European Commission, SMART.

[10] Sekhar, M., Kumar, R., Venugopal, R.K., Rao, N.S. 2013. Guaranteed Quality of Service in Cloud Ready Application. IEEE.

[11] Dores, C., Reis, L.P., Lopes, N.V. 2014. Internet of Things and Cloud Computing.

[12] Mohammad, A., Khan, I., Abdullah, A.A., Huh, E.N. 2014. Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved. Proceedings of the 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST). IEEE.

[13] Giuseppe, C., Coppolino, L., Cristaldi, R. G., Salvatore D.A., and Romano,L. QoS Monitoring in a Cloud Services Environment: the SRT-15 Approach.

[14] Ren, D., Chen, X., and Xing, T. 2011. A QoS Architecture for IoT, International Conferences on Internet of Things, and Cyber, Physical and Social Computing, IEEE.