Journal of Information Technology Management
Print ISSN: 2008-5893
Online ISSN: 2423-5059

Quality of Services Parameters for Architectural Patterns of IoT

Anjum Sheikh
Research Scholar, Kalinga University. E-mail: anjnaznus@gmail.com

Asha Ambhaikar
Kalinga University, E-mail: dr.asha.ambhaikar@gmail.com

Abstract

The Internet of things has become an interesting area of research in the last few years due to its ability to make human life simple and easier. Quality of Services (QoS) has gained a lot of importance due to the increasing popularity of the technology. QoS metrics help the IoT users to understand and express their requirements for the selection of services provided by IoT. Researchers in this field have come up with different types of architectures to provide a better view and define all the functions of the technology. In this paper, we have defined a few of the architectures and QoS metrics related to these architectures.

Keywords: The Internet of things, Tiered architecture, Service-oriented, Microservice, Quality of service.

DOI: 10.22059/jitm.2021.80616

Introduction

The Internet of things has enabled a number of the device to be connected through the Internet. It has led to the evolution of smart objects which are able to sense data, transfer data, and also make intelligent decisions. IoT enables the devices to get connected with anyone from any place and at any time (Butzin, B., et al., 2016 and Tandon, A., & Srivastava, P. 2019). The benefits of IoT have eased the lives of people, which had led to an increase in IoT consumers and also the applications. Some of the IoT applications used prominently are smart home, smart health care, intelligent transportation system, smart grid, smart city, etc. To increase the adaptability and trust of the users, it is essential that all the applications succeed in providing quality services to the users. For any of the IoT applications, transmission failures or delays at any of the levels can cause instability, which in turn can cause economic and material losses. Looking at the importance of transfer of data over the IoT platforms by ensuring security and energy efficiency of the energy-constrained IoT devices, Quality of Services (QoS) parameters have started gaining importance.

Quality of Service Parameters determines the degree of satisfaction of the users and is characterized by a combination of factors like integrity, security, accessibility, and operability. The evolution of IoT has led to the evolution of different types of architecture. The basic three-layer architecture first proposed in (Rayes., A, & Salem., S, 2019) consisting of sensing, network, and application layer, which was researched further to have more types of layered architecture with four, five, and six layers to focus on the finer aspects of IoT. To improve the flexibility of IoT applications, more types of architectures came into existence like service-oriented architecture (SOA) and microservice architecture (MSA). All these architectures, though, have a lot of similarities but due to difference in their working variations can be seen in QoS parameters for these architectures.

The rest of the paper is arranged as follows: Section II discusses the different types of tiered architectures, section III lists out the QoS parameters of the tiered architecture, section IV gives a description of the SOA architecture and its QoS, section V includes a description of Microservices, and its QoS and section VI concludes the paper.

Tiered Architecture for Internet of Things

The development of IoT has led to the evolution of different kinds of architecture to ensure better functioning as well as adaptability of technology by people all around the world. In this section, we have tried to mention the characteristics of three, four, five, and six-layer architecture.

A) Three Layer Architecture

The three-layer architecture was proposed by the authors in (Rayes., A, & Salem., S, 2019). to improve the existing architectures adopted by the earlier researchers and to increase the

QoS support for IoT. Many other researchers have extended their research by adopting the three-layer architecture to study the characteristics, technologies, and protocols used in the different layers (Al-Fuqaha, A., et al 2015, Chrysoulas, C., & Fasli, M. 2017, Darwish, D. 2015, Taibi, D. 2018, and Singh, M., & Baranwal, G. 2018). The three layers of IoT are the perception (Rayes., A, & Salem., S, 2019)/sensing (Al-Fuqaha, A., et al 2015) layer, network layer, and application layer.

I. Perception/Sensing Layer

The perception or the sensing layer is the collection of IoT devices or sensors and actuators. The primary function of the sensors is to collect data from the surrounding environment using a physical interface and then convert it into electrical signals so that the information can be used by the communication or computing devices. Sensors commonly used in the IoT environment are pressure sensors, temperature sensors, humidity sensors, imaging sensors, noise sensors, infrared sensors, moisture sensors, etc. The sensors at the perception layer have a crucial role in connecting the objects of things with the Internet. The real-time data collected by the sensors is analyzed and sent to the appropriate system through the gateways. Actuators use the data collected by the sensors for controlling IoT systems like switching off lights and fans when no motion is detected in a room for home automation applications.

II. Network Layer

The network layer consists of network components like routers, switches, and gateways. This layer enables the communication between the perception layer and the upper layers of the IoT through the Internet, mobile networks, and wireless sensor networks of any other private networks. The connection of the devices at the sensing layer with the other layers is enabled by using ZigBee, Bluetooth, or WiFi for short-distance communication and Wide Area Network (WAN) for long-distance communication. This layer decides how the data is sent over a physical network from source to destination by using routing algorithms.

III. Application Layer

The application layer consists of the numerous applications of IoT like smart homes, smart cities, smart health care, smart grid, intelligent transportation system, precision agriculture, etc. This layer uses the analyzed and processed data received from the lower layers to provide specific services to the users. One of the key issues of the application layer is to share information with the communities by ensuring safety and security. This layer combines the IoT technologies and sector professional technologies to provide various solutions for improving the quality of life for the people.

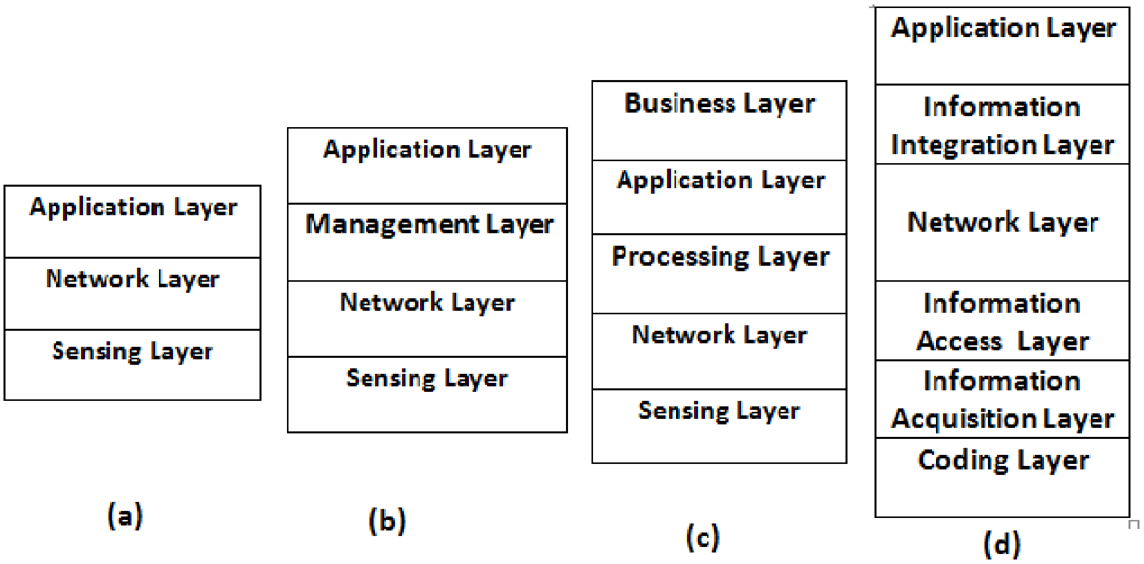

Figure 1. Layered Architecture (a) Three (b) Four (c) Five (d) Six

B) Four-Layer Architecture

The basic three-layered architecture is unable to meet all the requirements of IoT. The development of IoT architecture with four layers was developed, which includes a sensing layer, network layer, management service/ support layer, and an application layer (Nagothu, D., et al 2018, Zhang, M., et al 2012 and Alodib, M. 2016).

Management Service Layer: The management service or the support layer has been introduced in the four-layer architecture. In three-layer architecture, the data is sent from the network to the application layer, which increases the chances of threat attacks. This layer performs the task of service management by using software functions needed for the overall management of the IoT devices. The information received from the network layer is stored in the database. The task of application development is simplified by utilizing services like data management, data normalization, temporary or permanent storage, data analytics, and closed-loop control. The main purpose of this layer is to ensure a good amount of communication. The support layer monitors and controls the IoT elements at the perception and network layer. It enables the researchers to work with heterogeneous devices to improve the accuracy and efficiency of the IoT platforms.

The advantages of the four-level architecture for IoT are (Nagothu, D., et al 2018):

i. It reduces complexity by breaking IoT components into small or simpler components, which in turn facilitates the process of troubleshooting, design, component development, and makes learning easier.

ii. The vendors are able to develop joint solutions or common support models as this model standardizes the specific components at each level and interfaces between various levels.

iii. The problem of interoperability is solved in this model by which the devices belonging to different vendors, working with different kinds of languages are able to communicate with each other.

C) Five Layer Architecture

The researchers working in this field of IoT have proposed some other architecture with five levels. The five-layer architecture consists of the perception layer, transport/network layer, middleware/processing layer, application layer, and business layer (Guinard, D., 2011, Nuaimi, E. A., & Darmaki, N. A. 2017, Al-Masri, E. 2018 and Buyya, R., & Dastjerdi, A. V. (Eds.). 2016). The perception, network, and application layer perform the same tasks as in the earlier architectures. The middleware/ processing layer is similar to the management service/ support layer of the four-level architecture of IoT. The new layer introduced is the business layer.

Business Layer: The decision-making process based on the data analysis obtained is done in the business layer. It collects the data from the application layer to construct business models, flowchart, and graphs. This layer enhances the services and maintains the privacy of the users by comparing the output of each layer with the expected outcomes. On the basis of the outputs, this layer helps to plan future actions and business strategies.

D) Six Layer Architecture

On the basis of the working of the three-layer of IoT, a new extent six-layer architecture has been proposed in (Hasan, M. Z., 2018), which includes six layers: coding, information acquisition, information access, network, information integration, and application service. The function of the information integration layer is similar to the management service layer or support layer, while the application service layer also performs the same task as in previous architectures discussed until now. The sensing and network layer of the previous architectures is divided into sub-layers to deal with the challenge of heterogeneous access, device, and traffic flow in IoT.

i. Coding Layer: This is the first layer that performs the task of assigning a unique identification number or unique address to all the devices that have to be utilized in the IoT system.

ii. Information Acquisition Layer: This layer consists of devices like RFID, sensors, smart objects that will collect data.

iii. Information Access Layer: The function layer is to transmit the data collected from the information acquisition layer to the network layer by using communication technologies like WiFi, WiMAX, GSM, etc.

iv. Network Layer: This layer consists of a large, intelligent network based on IPV6 and IPV4 to utilize all the resources efficiently.

QoS Parameters for Layered Architecture of IoT

Quality of Service (QoS) is one of the basic requirements to ensure satisfactory services to IoT users. The service providers are able to provide clear visibility of their products to the customers by considering the QoS metrics. They can enforce a Service Level Agreement (SLA) and help the IoT users to identify the best IoT service for their applications (Krivic, P., 2017). Implementation of effective resource allocation and scheduling is possible by maintaining QoS at all levels (Rayes., A, & Salem., S, 2019). In this section, we discuss QoS characteristics for the various layers of IoT.

A) Perception/Sensing Layer

The characteristics of the IoT devices like sensors, RFID, and actuators to ensure QoS at the perception layer are:

a. Weight: Sensors used in the device layer should be compact and have low weight because space will be limited for the IoT verticals (Nagothu, D., et al., 2018, and Krivic, P., et al 2017).

b. Accuracy: The maximum uncertainty or error between the actual values and the output values is called accuracy. The sensor nodes are deployed in different environments to accomplish different kind of tasks. Accuracy of sensors includes data accuracy, sensing time accuracy, and spatial accuracy. Data collected from the different IoT nodes is transferred to the upper layers in the form of packets (Al-Fuqaha, A., et al., 2015, Chrysoulas, C., & Fasli, M. 2017., Taibi, D., et al 2018, and Krivic, P., et al 2017).

c. Energy Consumption: IoT devices are very small in size and therefore have small size batteries, which increase the risk of energy constraints. Energy is consumed by the sensors or nodes in sensing and transmitting data. Failure of a single node can disrupt the whole communication path. It is difficult to replace batteries for sensors used in applications like smart grids, smart transportation, etc. as they are deployed in different locations. Network protocol optimization and the adoption of alternative energy sources like solar energy can help to deal with the energy limitations of sensing nodes (Al-Fuqaha, A., et al., 2015, Chrysoulas, C., & Fasli, M. 2017., Taibi, D., et al 2018, and Krivic, P., et al 2017).

d. Coverage: The range of sensors is defined over which the sensors effectively convert the sensed signals into electrical signals. When the range is exceeded, the unsatisfactory accuracy is observed, and in most the cases, the sensors get damaged (Al-Fuqaha, A., et al., 2015, Rayes., A, & Salem., S, 2019 and Nagothu, D., et al., 2018).

e. Smart Detection: The sensors deployed in applications like the smart transportation system keep on moving in the network. Extracting the correct location of the sensors without being in physical contact with it can be done by using efficient positioning and measuring methods. Smart detection of objects can be divided into three types: determining the presence or absence of objects for security applications, determination of accurate speed for traffic monitoring, and accurate or precise position for vehicle collision avoidance (Rayes., A, & Salem., S, 2019 and Nagothu, D., et al., 2018).

f. Interoperability: It is defined as the ability of sensors of different architectures, configurations, and software platforms to interact with each other. A common framework should be established to allow the sensors of different proprietary standards to be able to sense, collect, and share data (Krivic, P., et al 2017).

g. Less Interference: The IoT sensors/devices are subjected to noise and interferences in the frequency spectrum. The noise traffic generated by sensors impacts IoT performance. Sensors should, therefore, be able to filter unwanted noise and produce alerts when the threshold value is reached (Nagothu, D., et al., 2018).

h. Sensitivity: The ratio of change in output electrical signal and the change in physical input parameters is known as sensitivity. The applications use different types of sensors to meet their sensitivity requirements. Generally, sensors with high sensitivity are preferred for IoT applications (Nagothu, D., et al., 2018 and , Krivic, P., et al 2017].

B) Network Layer

The performance metrics to be considered for the selection of network devices like routers, gateways, and switches to obtain QoS in the IoT networks are:

a. End to End Delay: It is one of the most important characteristics for real-time applications and is defined as the time required for the data packets to travel from the source to destination. It is preferred to have less end to end delay (Chrysoulas, C., & Fasli, M.

2017., Rayes., A, & Salem., S, 2019]. The different types of delays in the network are ((Nagothu, D., et al., 2018): Processing delay, which is defined as the time required by the router to process the packet header and determine the destination for the packet, queuing delay is the time spent by the packet in the router queues, the transmission delay is the time needed to push the packet bits onto the link and propagation which is defined as the time required for a bit to propagate from source router to destination router. The total delay is the sum of propagation delay, processing delay, queuing delay, and transmission delay.

b. Jitter: Time difference in the arrival of consecutive packets or variation in delay of the received packet between source and destination is called Jitter. It is caused due to improper queuing, network congestion, and configuration error (Krivic, P., et al 2017).

c. Packet Delivery Ratio: The ratio of the number of packets reaching the destination to the number of packets sent from the source node is called a packet delivery ratio (Gupta, P., et al., 2018). For lossless communication over the networks, the packet delivery ratio should be high. The ratio decreases with the increase in packet loss. If a packet traveling across the network fails to reach the destination, it is called packet loss. Congestion over the networks and an increase in hops over the routing path are some of the factors responsible for the increase in packet loss.

d. Throughput: Throughput can be defined as a successful amount of data that has been transmitted successfully through the network in a unit period of time. The speed of the link or device that processes the information and the time needed to receive a response after the request is sent helps in determining the Throughput of a network (Nagothu, D., et al., 2018). Throughput is, therefore, a measure of how fast a data can be sent over a network.

e. The lifetime of Sensing Networks: The minimum time at which the maximum numbers of nodes are dead or shut down is called network lifetime (Gupta, P., et al., 2018). A dead node is a node that runs out of energy. The lifetime of sensing networks depends on the energy consumption of the nodes. The network lifetime can be increased by using energy-efficient routing protocols so that less amount of energy is needed to transfer data packets on the network.

f. Security and Privacy: As the number of IoT devices is increasing, the amount of data being transferred on the IoT networks has also increased. It has increased the importance of maintaining the security of the IoT networks. The security of networks can be done by securing the data packets and by ensuring the privacy of the nodes. The location privacy can be achieved for the source node, destination node, or both of the nodes as per the requirements. Security is improved for the networks by using privacy algorithms for the source and sink nodes to prevent the adversaries from capturing the nodes.

C) Application Layer

The major requirements for QoS in the application and service layer are as follows:

a. Scalability: Scalability can be defined as the ability to support the increasing number of devices, features, applications, and analytical skills without affecting the quality of performance. Scalability is of immense importance for IoT applications as it enables us to monitor, secure, and manage an increasing number of devices with an increase in the number of devices (Krivic, P., et al 2017). It is related to the Throughput and performance of an application.

b. Service Cost: It is cost given by the service providers for utilizing service, and it is constant for a service round(Al-Fuqaha, et al., 2015 and Rayes., A, & Salem., S, 2019). Service cost is an important criterion for the selection of services because the end-users always prefer the service providers who provide the best QoS at minimum price.

c. Service Time: The time taken between the demand for a service and finishing the task to provide necessary functions ordered by the customers is known as service time (Rayes., A, & Salem., S, (2019). It varies according to the application and the available infrastructure. It can be measured in terms of the arrival rate of the request.

d. Accuracy: Accuracy is the measure of service error rate in a given time interval. It means that the IoT applications should be able to execute the specified instructions from the consumers without any error (Krivic, P., et al 2017).

e. Availability: The percentage of time for a service is able to operate called availability of service. It is the probability of the availability of resources and services to the users.

f. Security: The method adopted to protect data from attacks or hackers determines the security of an application. The IoT applications like smart home, smart transportation, or health care carry a large amount of confidential data. An application without ensuring security can never be accepted by the consumers. Authentication mechanism, confidentiality and data integrity of messages, cryptographic algorithms to protect the data from modification, accountability, and ensuring that the transferred message has been successfully sent or received by the parties are few methods to provide security of data for the applications.

g. Reliability: It is the overall measure of service to ensure quality. Reliability is defined as the ability to perform required functions in given conditions for a specified time period and is related to the number of failures that occur during this time interval. It also assures the successful delivery of transmitted and the received messages between the service providers and consumers.

QoS of Service-Oriented Architecture

The tiered architectures do not provide flexibility to the developers in making changes in the application according to the demand of users. The process of changing any module is time-consuming as it involves the process of rebuilding and testing the whole application. All the features cannot be changed or developed at the same time. The changes have to be made separately. It also lacks scalability. Looking at the disadvantages of the tired architectures, most of the organizations are moving towards advanced software product development architecture like Service Oriented Architecture (SOA).

The Service-Oriented Architecture (SOA) has the ability to expand the opportunities of interoperability and scalability for the IoT devices (Tan, L., & Wang, N. 2010, August). It has the capability to integrate data, organizational knowledge, and business process. The service-oriented IoT is thus able to control, manage, and interact with the real world through the services that facilitate bidirectional information exchange and interaction among devices and users. The four basic layers of SOA are the sensing layer, networking layer, service layer, and interface layer (Li, L., Li, S., & Zhao, S. 2014). The sensing layer consists of the hardware components such as RFID, sensors, and actuators, while the networking layer is responsible for providing networking support and data transfer over the wired or wireless networks among the devices. The service layer performs the task of creating and managing services to satisfy the requirements of the users. The interface layer consists of the interaction methods needed by the users and the different applications.

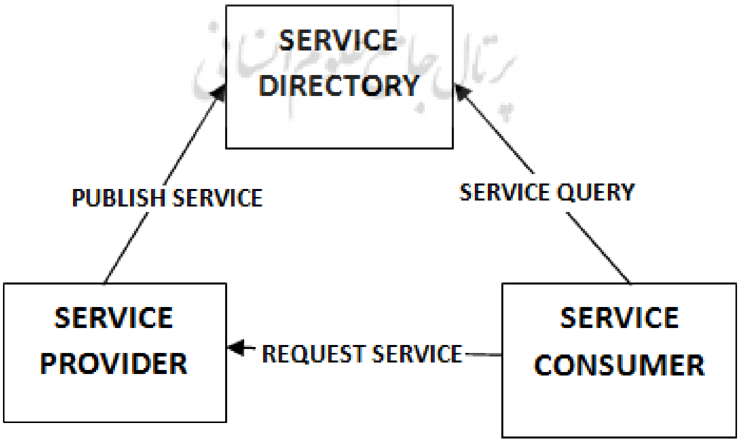

Figure 2. Basic Operation of Service Oriented Architecture (Li, L., et al., 2014)

The basic working of SOA given in Fig 2. shows the three basic elements: service directory, service provider, and service consumer. The task of design and development to service is done by the service provider. The service directory will be updated with the information of the developed services. The service directory is responsible for publishing the service information of the networks. Service consumers will send a request to the service directory for the information of services and contact the service provider for utilizing the available services. The advantage of using SOA is an autonomous operation, modularity, and well-defined interface which enables the services to be described, published, and discovered over the network (Li, L., et al., 2014). These types of architecture possess a modular decomposability feature that divides the complex systems into subsystems. It provides an easy method for the maintenance of the whole system by taking care of the individual components due to which, in case of component failure, the rest of the system operates normally (Avila, K., et al 2017, Panda, I. 2012 and Chaqfeh, M. A., & Mohamed, N. 2012). The SOA offers Infrastructure services that include security, management, and monitoring. Another kind of service offered is Business neutral services, which consist of service brokers and notification, scheduling, and workflow services. It also offers Business neutral services, which consist of service brokers and notification, scheduling, and workflow services Chaqfeh, M. A., & Mohamed, N. (2012, May).

The successful implementation of service-oriented needs to consider new features of IoT to obtain QoS (Al-Fuqaha., et al., 2015). The integration of SOA with the smart objects has to consider QoS and energy efficiency of the composed objects. The IoT devices can join or leave the network; some new devices with better qualities can join the network. This quality of devices leads to the variation of QoS values, which poses a challenge to maintain a balance between QoS and energy consumption (Taherizadeh, S., et al., 2018). QoS of the interactive applications is declared by using contracts called Service Level Agreements (SLA) between the service providers and the users. Another set of parameters that determine QoS of the services include response time, availability, cost, price reliability, sustainability, interoperability, and accuracy (Al-Fuqaha., et al., 2015, and Li, S. et al., 2014). QoS mechanism supports the constraints imposed by the consumers of energy by trying to maintain stable energy flow in the network. Hybrid Execution Service Oriented Architecture (HESOA) in (Yang, Z., et al., 2011) uses multitasking architecture that enables IoT applications to process all possible sensor requests, which is generally not possible for a single SOA unit (Abd Rahim, M. R., et al 2018, Zhang, M., Sun, F., & Cheng, X. (2012, October) and Alodib, M. 2016). The QoS indexes for this architecture include data level and transport-level security, fault tolerance, bandwidth efficiency, latency, high aggregated data volumes, and high individual data rates.

Qos of Microservice Architecture

With the development of IoT technology, the numbers of connected or smart devices have increased rapidly, and therefore the expectations of the users from the cloud-based platforms have also changed. The Microservice approach was developed to cope up with high scalability, maintainability, and fast-changing business models in the cloud. These companies have to store a large number of codes, which is very difficult to maintain. Microservice provides flexibility in changing the codes by allowing modularization of codes. In the monolith system, a small change impacts the whole system, and therefore the whole code has to be revised. This problem is eliminated by using modular codes, which increases the opportunities for using microservice for research and developmental activities. The employees can be easily familiarized with the code as they need to know the code related to their work responsibility eliminating the need to know the whole code(Uviase, O., & Kotonya, G. 2018).

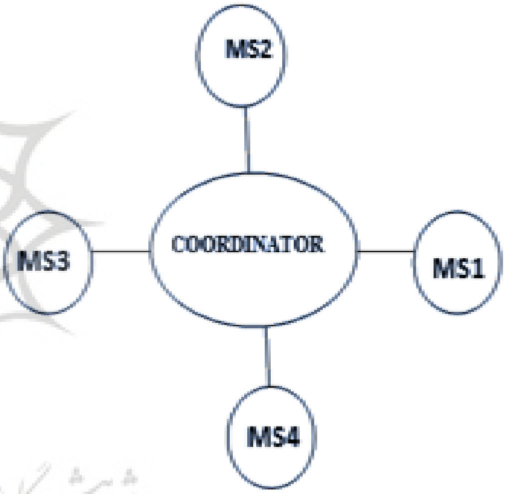

Figure 3. Microservice Orchestration

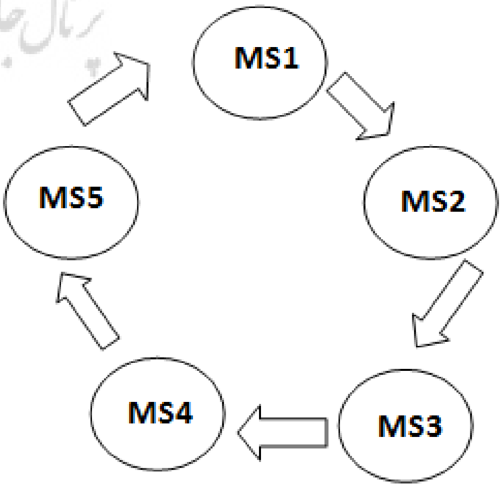

Figure 4. Microservice Choregraphy

Table 1. Differences between SOA and Microservice

SOA	Microservice
A software application is broken down into various features or services	Services are further broken down into task level services due to which there will be multiple tasks and multiple services
Services interact with each other, and they will be delivered as one application.	Services work separately.
Uses many types of messaging protocols	Uses lightweight protocols, HTTP, REST, AMQP
Interoperability is achieved by using Enterprise Service Bus (ESB)	The API layer is used to allow interoperability
Information is stored in a single database	Dedicated database for each service
Better suited for the large and complex business environment	Suitable for small, well-partitioned web systems

Source: Burhan and et al., 2018, Singhal and et al., 2019 and Uviase & Kotonya, 2018

Microservice is basically of two types, functional and non-functional. The functional services are used by external systems or devices and consist of literals such as numbers, letters, etc. This service supports the operational function of a smart system in IoT. On the other hand, the non-functional services are related to non-operational tasks like authentication, monitoring, logging, and auditing, which are required for the reliable use of the system (Singhal, N., et al, 2019).

The process of implementation and testing becomes complex, with an increase in the number of services because each dependent service has to be confirmed to commence testing. The Microservice approach is not suitable for a small number of users. In such cases, the developer can begin with a monolith approach and update it to microservice when growth in users is observed. An increase in the latency period, lack of safety for databases, and complexity in deployment due to multiple independent services are few challenges for microservices that need attention (Sethi, P., & Sarangi, S. R. 2017). As shown in fig.3. (R. C., & Kumar, V. 2015), there are two approaches for collaboration of microservices, i.e., choreography and orchestration. In the microservice choreography approach, the services interact with each other while in the orchestration approach, a centralized controller manages the collaboration process. A combination of microservice choreography and orchestration called a hybrid approach is used in some applications to improve time effectiveness, utilization of power, and memory.

Table 2. Classification of QoS Attributes for Autonomic

Type of QoS Parameters	Static/Dynamic	Attributes
Network Related	Static	Number of Hops
		Network
		Bandwidth
	Dynamic	Packet Loss
		Network
		Throughput
		Network Delay
		Network Jitter
Infrastructure Related	Static	Number of CPUs
		Amount of Memory
		Disk Space Size
	Dynamic	Percentage of CPU
		Percentage of Memory

Orchestration

A single service is unable to fulfill all the requirements of the consumers due to which we need to combine many services, which is according to the demands of the consumers. In such a case, QoS plays an important role in the selection of appropriate services. For containerized microservices, QoS parameters are classified into qualitative and quantitative. The quantitative parameter is expressed in numerical values, which include availability, response time, Throughput, availability, and reliability (Khan, R., 2012 and Bhaddurgatte, R. C., & Kumar, V. 2015) while privacy, reputation, and cost (Khan, R., 2012) are qualitative parameters of Qos. Multiple microservices may offer the same kind of functions, but their degree of performance depends on their QoS values. In most of the applications considering anyone, the QoS attribute is not sufficient. Similarly, considering QoS values at a specific time cannot be considered to be an ideal value. In order to obtain accurate values of QoS, it is required to collect data over a long duration. The autonomic orchestration technique takes a decision for the deployment of services by dividing the whole range of quantitative QoS parameters into two types: (i) network-related and (ii) infrastructure-related (Duan, R., Chen, X., & Xing, T. 2011). The classification of QoS parameters is given in table 2.

Discussions on QoS Management

The growing popularity of IoT has led to the extensive utilization of the technology for applications like home automation, health care, intelligent transportation, industrial management, etc. The tremendous increase in the number of end-users for IoT has generated the necessity to maintain QoS for satisfying the customers. In this paper, we have discussed QoS parameters at different levels of IoT architecture. Few requirements for the management of QoS in IoT are discussed below:

i. The QoS requirements of an application differ from other kinds of applications used by the people. Therefore while an application has to be developed, we need to consider all the available QoS parameters, evaluate it, and then consider the factors that are more important. This method will help in increasing the efficiency of the application.

ii. ii. For developing a QoS application or service, we need to consider QoS at all levels of the architecture. A study of QoS only at one level is not sufficient. The network layer communicates with the device and application layer to execute a service requested by the users. The vendors and service providers can improve quality by considering the demands of customers. Firstly the QoS of devices should be decided, and the devices should be selected to provide accuracy, stability, and minimize error. Similarly, at the network level, the vendors should select the communication medium according to the range of communication to decide whether a wired or wireless medium can be used. At the application level, energy consumption, security, privacy are some of the factors to be considered for ensuring QoS.

iii. There some QoS attributes that overlap between different layers and impact each other. For example, the service time in the application layer is dependent on the end-to-end delay or transmission at the network layer. A delay in the transmission or reception of messages at the network layer will increase the service time in the application layer. More time required for an application may affect the satisfaction level of the customer, which in turn may affect the adaptability of an IoT service or application. Though a lot of work is being done to improve QoS, research in the field of cross-layer attributes needs more attention.

iv. Maintaining a balance between QoS, scalability, interoperability, energy consumption, and security is difficult. For ex., paying more attention to security can ensure QoS, but energy consumption is increased. Similarly, there are many routing algorithms that try to minimize energy consumption, but it directly affects the throughput and packet delivery ratio. Poor results of these parameters affect the performance of an application.

Looking at the above requirements, we can say that for the management of QoS, we should try to pay attention to computing methods like machine learning that utilizes the past information for better execution of the future programs. Machine learning can provide improved solutions for obtaining enhanced QoS by the efficient utilization of resources for the IoT platform.

Conclusion and Suggestion

In this paper, we have studied the different types of tiered architecture, service oriented architecture, and microservice architecture and also listed the QoS metrics for them. This work will help the users to define their requirements and, at the same time, will enable the researchers as well as the service providers to develop a model to face challenges in fulfilling the demands of the end-users. A lot of research still needs to be done in the area of technologies and applications of IoT. Though a lot of technological advancements have taken place in this field, issues like security, privacy, energy consumption, scalability, interoperability need more attention.

References

Abd Rahim, M. R., Rashid, R. A., Rateb, A. M., Sarijari, M. A., Abdullah, A. S., Hamid, A. H. F. A., ... & Fisal, N. (2018). Service-oriented architecture for IoT home area networking in 5G. *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management*, 577-602.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

Al-Masri, E. (2018, December). Enhancing the microservices architecture for the internet of things. In *2018 IEEE International Conference on Big Data (Big Data)* (pp. 5119-5125). IEEE.

Alodib, M. (2016). QoS-Aware approach to monitor violations of SLAs in the IoT. *Journal of Innovation in Digital Ecosystems*, *3*(2), 197-207.

Amar Rayes, Samer Salem, Internet of Things from hype to Reality: The Road to digitization, 2019, Springer

Avila, K., Sanmartin, P., Jabba, D., & Jimeno, M. (2017). Applications based on service-oriented architecture (SOA) in the field of home healthcare. *Sensors*, *17*(8), 1703.

Bhaddurgatte, R. C., & Kumar, V. (2015). A review: QoS architecture and implementations in IoT environment. *Research & Reviews: Journal of Engineering and Technology*, 6-12.

Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, *18*(9), 2796.

Buyya, R., & Dastjerdi, A. V. (Eds.). (2016). *Internet of Things: Principles and paradigms*. Elsevier.

Butzin, B., Golatowski, F., & Timmermann, D. (2016, September). Microservices approach for the internet of things. In *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1-6). IEEE.

Chaqfeh, M. A., & Mohamed, N. (2012, May). Challenges in middleware solutions for the internet of things. In *2012 international conference on collaboration technologies and systems (CTS)* (pp. 21-26). IEEE.

Chrysoulas, C., & Fasli, M. (2017). Towards an adaptive SOA-based QoS & Demand-Response Provisioning Architecture for the Smart Grid. *Journal of Communications Software and Systems*, *13*(2), 77-86.

Darwish, D. (2015). Improved layered architecture for Internet of Things. *Int. J. Comput. Acad. Res.(IJCAR)*, *4*, 214-223.

Duan, R., Chen, X., & Xing, T. (2011, October). A QoS architecture for IOT. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 717-720). IEEE.

Guinard, D., Trifa, V., Mattern, F., & Wilde, E. (2011). From the internet of things to the web of things: Resource-oriented architecture and best practices. In *Architecting the Internet of things* (pp. 97-129). Springer, Berlin, Heidelberg.

Gupta, P., Satyanarayan, K. V. V., & Shah, D. D. (2018). Iot Multitasking: Development Of Hybrid Execution Service Oriented Architecture (Hesoa) To Reduce Response Time For Iot Application. *Journal of Theoretical & Applied Information Technology*, *96*(5).

Hasan, M. Z., Al-Turjman, F., & Al-Rizzo, H. (2018). Analysis of cross-layer design of quality-of-service forward geographic wireless sensor network routing strategies in green internet of things. *IEEE Access*, *6*, 20371-20389.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology* (pp. 257-260). IEEE.

Krivic, P., Skocir, P., Kusek, M., & Jezic, G. (2017, June). Microservices as agents in IoT systems. In *KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications* (pp. 22-31). Springer, Cham.

Li, S., Oikonomou, G., Tryfonas, T., Chen, T. M., & Da Xu, L. (2014). A distributed consensus algorithm for decision making in service-oriented internet of things. *IEEE Transactions on Industrial Informatics*, *10*(2), 1461-1468.

Li, L., Li, S., & Zhao, S. (2014). QoS-aware scheduling of services-oriented internet of things. *IEEE Transactions on Industrial Informatics*, *10*(2), 1497-1505.

Li, L., Rong, M., & Zhang, G. (2014, August). An Internet of things QoS estimate approach based on multi-dimension QoS. In *2014 9th International Conference on Computer Science & Education* (pp. 998-1002). IEEE.

Nagothu, D., Xu, R., Nikouei, S. Y., & Chen, Y. (2018, September). A microservice-enabled architecture for smart surveillance using blockchain technology. In *2018 IEEE international smart cities conference (ISC2)* (pp. 1-4). IEEE.

Nuaimi, E. A., & Darmaki, N. A. (2017, March). Managing QoS in IoTs: a survey. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing* (pp. 1-7).

Panda, I. (2012). QoS Parameters Analysis to Improve QoS in MANETs Routing Protocol. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, *1*(7), 43-49.

Singh, M., & Baranwal, G. (2018, February). Quality of service (qos) in internet of things. In *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-6). IEEE.

Singhal, N., Sakthivel, U., & Raj P., Efficient Hybrid Research for QoS-Aware Mcroservice Compostion, *International Journal of Recent Technology and Engineering*, ISSN: 2277-3878, volume 8, Issue 2, 2019

Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.

Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-376). IEEE.

Taibi, D., Lenarduzzi, V., & Pahl, C. (2018, March). Architectural Patterns for Microservices: A Systematic Mapping Study. In *CLOSER* (pp. 221-232).

Tandon, A., & Srivastava, P. (2019). Location Based Secure Energy Efficient Cross Layer Routing Protocols for IoT Enabling Technologies. *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN*, 2278-3075.

Taherizadeh, S., Stankovski, V., & Grobelnik, M. (2018). A capillary computing architecture for dynamic internet of things: Orchestration of microservices from edge devices to fog and cloud providers. *Sensors*, *18*(9), 2938.

Tein-Yaw Chung, A Fast IoT Service Composition Scheme of Energy Efficient QoS Services, ICCCM 2019, ACM, ISBN 978-1-4503-7195-7/19/07

Uviase, O., & Kotonya, G. (2018). IoT architectural framework: connection and integration framework for IoT systems. *arXiv preprint arXiv:1803.04780*.Osam a Alsaryarh, Ibrahim Mashal,

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011, July). Study and application on the architecture and key technologies for IOT. In *2011 International Conference on Multimedia Technology* (pp. 747-751). IEEE.

Zhang, M., Sun, F., & Cheng, X. (2012, October). Architecture of internet of things and its key technology integration based-on RFID. In *2012 Fifth International Symposium on Computational Intelligence and Design* (Vol. 1, pp. 294-297). IEEE.

Bibliographic information of this paper for citing:

Sheikh, Anjum & Ambhaikar, Asha (2021). Quality of Services Parameters for Architectural Patterns of IoT. *Journal of Information Technology Management*, Special Issue, 36-53.