IoT Ecosystem- A survey on Classification of IoT

Sivagami. P [1*], Illavarason. P[2] , Dr.Harikrishnan.R[3], Goluguri Venkata Sai Rama Reddy[4]
Research Scholar [1], Assistant Professor[2], Professor[3], UG Scholar[4]
[1,4]Sathyabama Institute of Science and Technology, Chennai, India
[2]Periyar Maniammai Institute of Science and Technology, Thanjavur, India
[3]Symbiosis Institute of Technology,Symbiosis International Deemed University, Pune, India
[1] sivagamitec@gmail.com, [2]illavarason.p@gmail.com,
[3]rhareish@gmail.com,[4]sairamareddy19@gmail.com

Abstract. Digital era transformed the way we use the internet; it is mutated as powerful enabler for it provides personalized solutions to improve the standard of living of the people. A network of devices which can sense, communicate with the help of embedded technology to meet the needs of individual, respond to them, and help in managing their lives in all possible means is Internet of Things (IoT). Availability of infrastructure, availability of resources at the affordable prices, accessibility of IoT devices at any instant are the reasons for the enormous growth of IOT technology in the 21st century. It can be stated that revolution which merges digital and physical world is IoT. COVID-19 pandemic disease caused by the virus called corona. It is serious disease which affected the people and taken lives of people in lakhs in many countries. It spreads from person to person through droplets from nose or mouth from an infectious person. So human to human interaction has to avoided or proper distancing has to be maintained as a precaution from getting infected. Lock downs have been implemented in order to avoid the spread of the disease. The year 2020 has given an opportunity to prove the role played by IoT in the life of people of all sectors. In this pandemic situation any one, anytime, anywhere connected to any part of the thing or people in the world is made possible using IoT. IoT and its classification is discussed in this paper..

Keywords: IoT- Internet of Things, ASIoT- Application Specific Internet of Things.

1 Introduction

IoT connects devices and sensors through wireless mode and make data available to the users. The users can access and have control over the device from anywhere in the world. In simple words IoT performs AAA that is collect data, from any place any time anywhere then analyze, process data and perform actions to support the decision making. IoT interacts in the same way how people interact in physical world. It is done with the help of digital objects. The digital objects provide data as physically provided by the people for processing. IoT replaces human- human communication. According to statistic report from Gartner IoT research, CISCO IoT stability about 25-30 billion of IoT devices will be connected to the Internet. It is estimated that 127 new IoT devices will be connecting every second. The number of IoT devices in home will have a rapid rise and it is expected to be around 12.86 billion. IoT has turned out to be boon not only for a specified sector but for all different sectors.

There are two IoT markets. They are Horizontal and vertical IoT market. IoT market which focuses on the specific services that is in order to meet the demands of specific people is called vertical market and it may be either industry specific or demographic specific.

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2304170

Horizontal IoT market focuses on wide range of customer needs and it has large customer base. In horizontal market consumers and purchasers will be of different sectors of the economy.

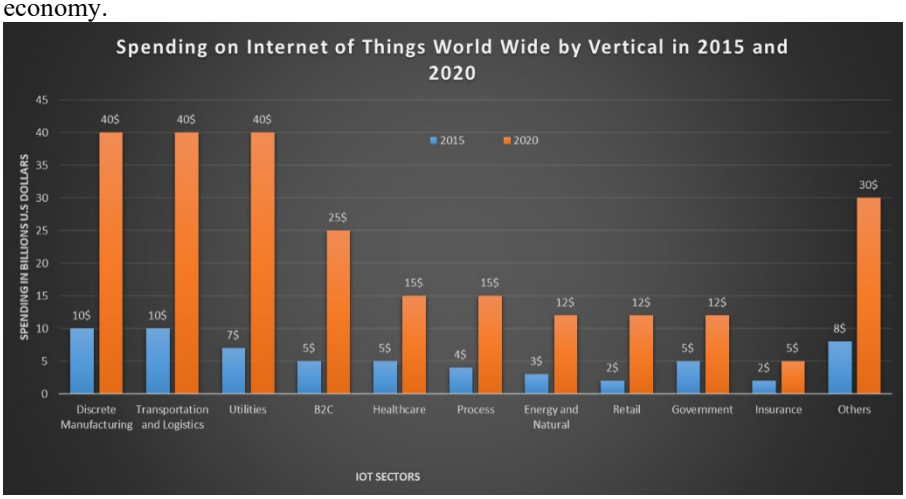

Fig. 1. Investment in billions of U.S dollars in different IoT sectors (source: Forbes)

From the figure 1 it is evident that amount invested on vertical IoT of different sectors has seen rapid growth from 2015-2020. The number of IoT devices connected to the internet is more than that of the mobile devices connected to internet. The estimated increase in market share contributed by different sectors towards IoT application for the year 2015-2025 is shown in the figure 2 and it is found that more investments are made on health care units to transform traditional equipment and appliances into smart products. Because of this pandemic COVID-19 there is possibility to introduce Robots with health monitoring system to avoid human interaction and to provide medicines to infected persons to reduce the virus spread in future. So, percentage of investment in health care IoT applications will have enormous growth when compared to other sectors. COVID-19 impact will cause a tremendous change not only in Medical IoT applications but also in educational sectors as well as industrial sectors where there is possibility of interaction of community of people.

2 Classification of IoT Based on Capability and Performance

Classification of IoT can be carried out in many ways. Based upon the capability and performance IoT devices are classified as Low-end devices, middle-end devices and high-end devices. Low-end devices based on the technical properties such as memory, heterogenous hardware support, network connectivity, efficiency and real time capability it is further classified as Class0, Class1 and Class2. Sensors, actuators, openmote, waspmote, Tmote sky, ATMEL SAM R21 Xplained-pro etc. are low end devices [1].

Class0 has limited resources. It represents the first layer. It includes sensing and actuating functions. Sensors Class1 has more resources compared to low end devices. It

provides more functionality than Class0. The drawback is that it doesn't have computational capability to handle complex requirements. It includes basic microcontrollers. In other words, it enhances the functionality of lower end IoT devices. It has the capabilities like image processing, data filtering etc. Because of more functionalities it is partially secured.

Class2 has CPU, RAM, flash memory and it supports traditional operating system such as LINUX, UNIX. It also supports artificial intelligence, machine learning, deep learning. It can be integrated with almost all communication protocols. Middle end IoT devices have the ability to use more than one communication technology. The clock speed and RAM is the range of hundreds of MHZ. Compared to low end devices it has more constrained resources, but less than that of high-end devices. Table 1 and 2 shows the specification requirement for IoT devices and security requirement for these IoT devices.

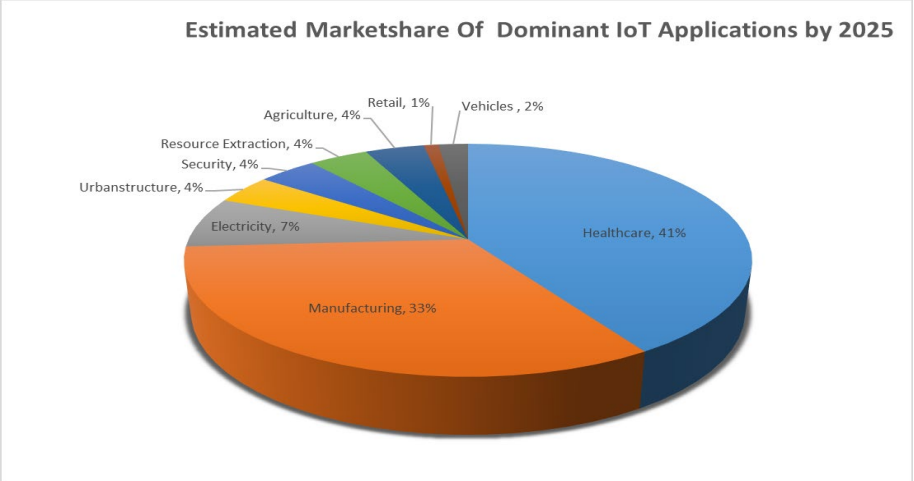

Fig.2. Estimated contribution of dominant IoT sectors

Table1. Specifications for different classes of IoT devices

Low End Devices	**Specifications**				
		RAM	Flash	RTOS Support	Communication Protocols
	Class0	<10 kB	<100 kB	Does not support	Use gateways for communication No protocol stack embedded
	Class1	~10 kB	~100kB	Could be implemented	Use light weight protocols, communicate with other devices without using gateway
	Class2	~50 kB	~250kB	Could be operated	Supports communication protocol such as HTTP

Table2. Based on capability of IoT devices security requirements

Categories	Security Requirements	Class0	Class1	Class2
Confidentiality	Message encryption		Yes	Yes
	Malware response			
	Data encryption		Yes	Yes
	Tamper resistance		Yes	
	Device ID management	Yes	Yes	Yes
Integrity	Data integrity		Yes	Yes
	Platform integrity			Yes
	Secure booting			Yes
Availability	Logging		Yes	Yes
	State Info. Transmission	Yes	Yes	Yes
	Security monitoring			Yes
	Security patch			Yes
	Security policy			Yes
	Software safety		Yes	Yes
Authentication/ Authorization	User authentication		Yes	Yes
	Device authentication		Yes	Yes
	Password management		Yes	Yes
	Access control		Yes	Yes
	Device ID verification			Yes

3 Classification of IoT Based on Entity and Service Life Cycle

Another classification based on the entity's relationship with that of physical devices they are classified as low-level service, resource service, entity service, integrated service. IoT classified based on the service quality as deployable, deployed, operational. The classifications are represented in figure 3 and 4.

4 Classification of IoT Based on Operating System

Bridging the applications or users and devices is a set of programs called operating system. IoT devices has the operating system installed on it in order to execute the programs and manage the devices. Based on operating system (OS) it is further classified as low end and

high end. The schematic representation is shown in figure 5. Some, of the operating system available for low- level and high-level devices are shown in table 3.

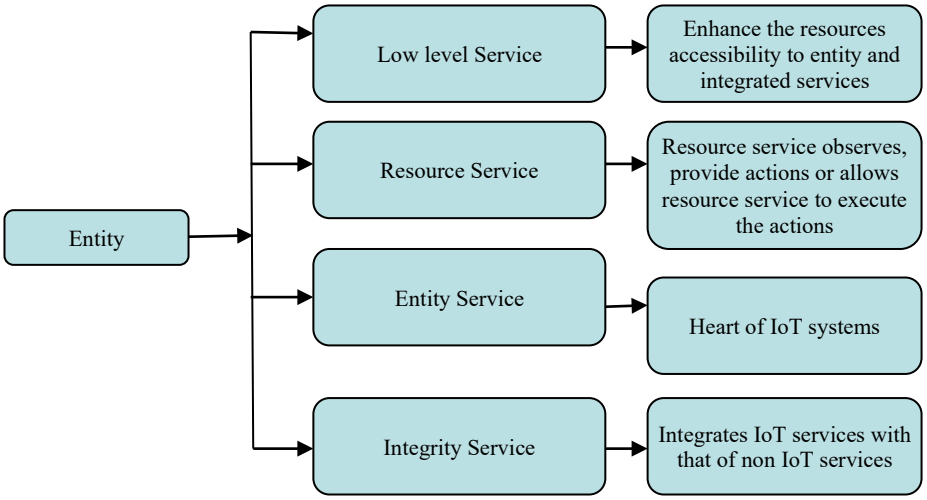

Fig.3. Classification Based on Entity relationship

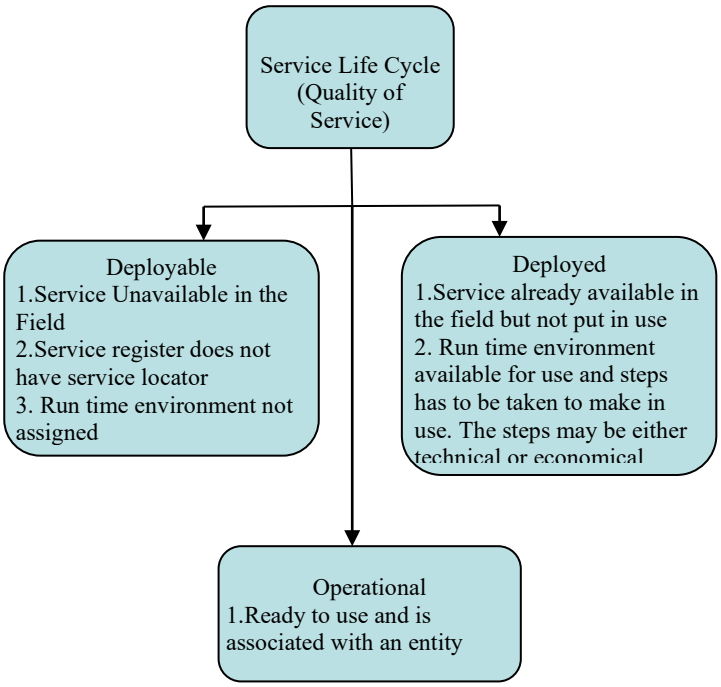

Fig.4. Classification based on Service Life cycle

Table 3.OS for IoT devices

Operating System	Real time support	IoT devices	OS type
TinyOS	No	Low	Non-Linux
Contiki	Yes	Low	Non-Linux
RIOT	Yes	Low	Non-Linux
LiteOS	No	Low	Linux
FreeRTOS	Yes	Low	Non-Linux
Mynewt	Yes	Low	Linux
uClinux	Yes	High	Linux
Raspbian	Yes	High	Linux
Android thing	No	High	Linux

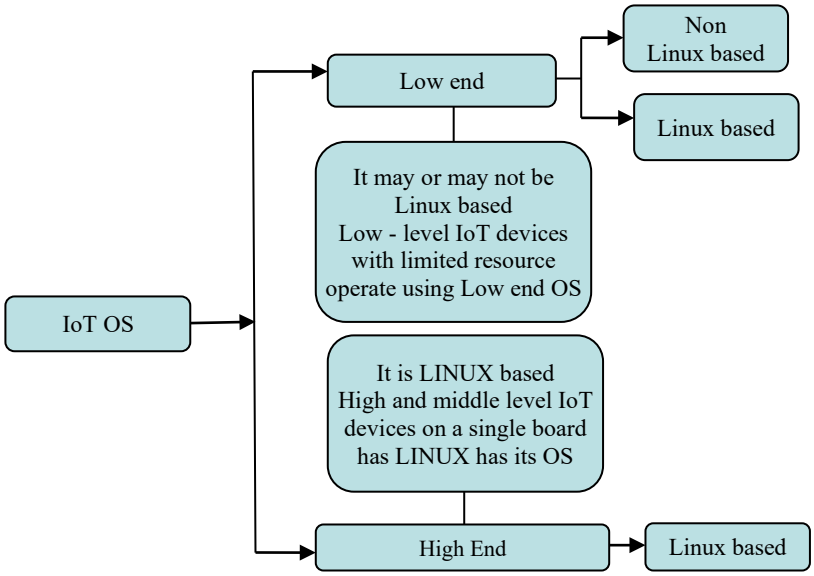

Fig.5. Classification based on type of OS employed

4 Classification of IoT Based on Communication Technologies

IoT requires communication technologies to connect heterogenous objects in order to provide specific smart services. Communication technologies helps in information exchange. Communication can be made locally using Bluetooth, NFC or using internet. The main difference between locally communicated and through internet protocol is based on the factors such as range for communication, power consumption and memory used. Internet protocol

network, though it has high power consumption it has no range limitations that is it not constrained to specific distance. Some of the internet protocols are Near field communication NFC, wireless sensor networks, low power technologies.

Near field communication (NFC) – Radio waves used in identifying the objects is called RFID (Radio Frequency Identification). NFC is a subset of RFID. NFC is a high frequency RFID operating at 13.56 MHZ. RFID consists of reader, tag and antenna and it is a secured form of data exchange. RFID can be either active or passive. Table 4 shows differences between Active and passive RFID.

Table 4. Active and Passive RFID

Active RFID	Passive RFID
It has own power source	Do not have their own power source
It has a read range of up to 100 meters	It has a read range from near contact and up to 50 meters
It finds its application in construction, security, Public works	It finds its applications in paper, textile etc.
Tags are costly and have limited life span	It is small size, light weight and has long life span

Low power technologies- In order to support IoT paradigm low power technologies developed. LPWANS (Low power wide area networks) enhances the provisions for all type of sensors. It has the capability to provide long range communication with small inexpensive batteries lasting for years. It finds its applications in remote monitor, smart meters, building contract etc. It can be operated using licensed versions such as NB-IoT, LTE-M and unlicensed versions such as MYTHINGS, LoRa, Sigfox etc. Cellular technology used in mobile phones offers reliable broad band communication. It requires power for its operation and its operational cost is high. It doesn't support most of the IoT devices because of the factors like frequency, range of communication and security.

Wi-Fi because of high energy requirement it find its applications in smart home appliances, security cameras etc. The factors which make it less prevalent are coverage, scalability, power consumption. In order to over come the data transfer affected by the congested environment Wi-Fi-6 brings about enhanced bandwidth < 9.6Gbps to improve the data transfer. Wi-Fi HaLow has improved power efficiency but lacks security. Blue tooth low energy and blue tooth devices are used along with electronic devices to provide a smart device mainly for medical wearables and fitness. Mesh topology allows Zigbee to communicate to more IoT devices. It supports higher data rates and consumes less power. Because of low power consumption it finds its applications in medium range IoT devices such as energy management, security, HVAC control etc.

The network requirements are not the same for all IoT applications. Each IoT application has its own network requirement. The factors which influence the selection of wireless technology for unique IoT application is range, security, latency of bandwidth, the power consumed by the devices, quality of service, network management. The table 5 shows the wireless technology for various IoT applications.

Table 5. Wireless technology for various IoT verticals

Key IoT verticals	LPWAN (Star)	Cellular (star)	Zigbee (Mostly mesh	BLE (star & Mesh)	Wi-Fi (star and mesh)	RFID (Point-to-point)
Industrial IoT	Highly applicable	Moderately applicable	Moderately applicable			
Smart Meter	Highly applicable					
Smart City						
Smart Building			Moderately applicable	Moderately applicable		
Smart Home			Highly applicable	Highly applicable	Highly applicable	
Wearables	Moderately applicable			Highly applicable		
Connected car					Moderately applicable	
Connected Health		Highly applicable		Highly applicable		
Smart Retail		Moderately applicable		Highly applicable	Moderately applicable	Highly applicable
Logistics & Asset tracking	Moderately applicable	Highly applicable				Highly applicable
Smart Agriculture	Highly applicable					

5 Classification of IoT Based on Middleware

Different domains of application communicating over different domain interfaces is bonded by software platform called IoT Middleware. Middleware also called as software glue as it helps the software developers to develop programs to implement the communication. If complex programming is not designed initially middleware enables to integrate it later with the help of support architecture. The features which influence the middleware are device discovery management, interoperability, context awareness, security, platform portability. The schematic representation of general functions performed by middleware is shown in figure 6. Usability, flexibility, adaptive nature used to classify IoT middleware as service oriented, cloud oriented and actor oriented middle ware. Service oriented middleware- Addition and modification of IoT devices is enabled for the end users, developers. Service oriented may be either standalone or cloud computing services (PaaS). It does not support homogenous system application because it is not cost effective. There is no design provision for security technique to support constrained resources. Cloud oriented middleware- It collects the data, analyze and interpret the data with ease. User unable to configure security and privacy. It has control over sensitive data but it doesn't have design structure to support constrained resources.

Actor oriented middleware – Users are allowed to plug and play IoT devices. Whenever user doesn't require IoT device they can remove that particular IoT device without

disturbing and affecting the other elements of IoT ecosystem. It allows the user to configure security and privacy. Based on the architecture design middleware is further classified as service based, node based, component based, centralized, distributed, client- server. The benefits of this architecture are shown in table 6.

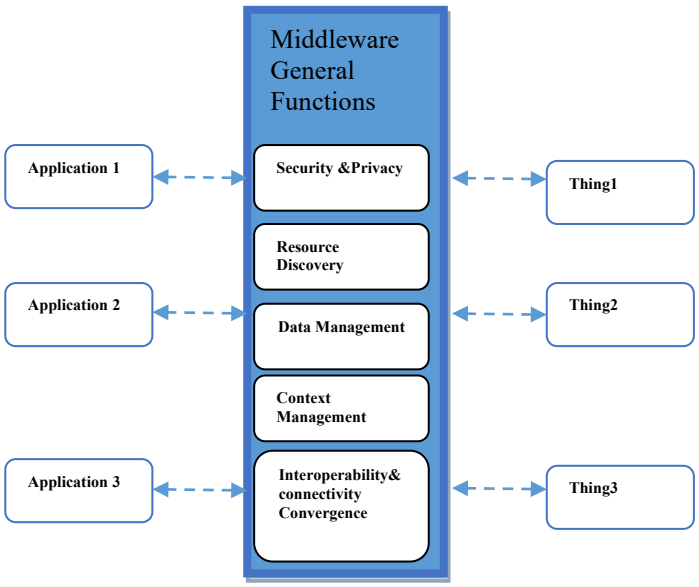

Fig. 6. Middleware functions

Table 6. Benefits of Middleware based on architecture design

Architecture	Benefits
Component based	Reusability, Abstraction support and Independency
Distributed	Resource sharing, Openness, Scalability, Concurrency, Consistency and Fault tolerance
Service-based	Reusability, Scalability, Availability and Platform Independence
Node-based	Availability and Mobility
Centralized	Simplicity, Security and Manageability
Client-server	Servers separation, Resource accessibility, Security, Back-up and Recovery

6 Classification of IoT Based on Architecture

The basic IoT architecture consists of only three layers namely perception layer- performs sensing and actuating, network layer- performs data transmission and processing, application layer – provides the user the requirement. In five-layer architecture in order to provide more abstraction to IoT architecture additional layers are included. It includes perception – where sensor measures the data, transport layer- performs transporting data function, Processing layer- process and analyze the data obtained through transport layer, middleware interconnect heterogenous objects with the heterogenous system is the back bone of IoT ecosystem. Middleware manages the system by having control over the data flow. In middleware-based architecture perception layer along with access layer and edge layer has the sensors and actuators. Coordinate layer along with the application layer gives a final application to the user. In service-oriented architecture objects data are extracted and exposed through interfaces. Application Programming Interface (API) remains the same even though the technology and cloud vary. In fog-based architecture bottom most is the physical layer, the next layer is monitoring- observes and checked the data received from sensors. The pre-processing layer process the data to perform based on processing. Security layer is responsible to provide data security and privacy.

Perception layer–Includes sensors and actuators. Sensors observes the environmental and physical parameters, collect those parameters, removes the unwanted data and passes the data to actuators to perform actions. Transport layer- Carries the preprocessed data for processing to the processing layer using communication protocols like Zigbee, BLE, NFC etc. Processing layer- Filter, format the data received from sensors. It also stores and manages the sensed data received from various devices through communication protocol. Middleware layer- Performs logical and analytical operations on the data available to provide a meaningful information. It uses platforms for processing, cloud for storing. Application layer delivers an application to the user with the help of communication protocols like MQQT, Constrained Application Protocol (CoAp). The figure 7 represents the architecture of IoT.

<table>
<tr><td rowspan="2">Application layer</td><td>Application layer</td><td colspan="2">Application Layer</td><td>Applications</td><td>Transport Layer</td></tr>
<tr><td>Middleware Layer</td><td colspan="2">Coordination Layer</td><td>Service Composition</td><td>Security Layer</td></tr>
<tr><td>Network Layer</td><td>Processing Layer</td><td colspan="2">Middleware Layer</td><td>Service Management</td><td>Storage Layer</td></tr>
<tr><td rowspan="3">Perception Layer</td><td>Transport Layer</td><td colspan="2">Backbone Network Layer</td><td>Object Abstraction</td><td>Pre-processing Layer</td></tr>
<tr><td rowspan="2">Perception Layer</td><td rowspan="2">Perception Layer</td><td>Access Layer</td><td rowspan="2">Objects</td><td>Physical Layer</td></tr>
<tr><td>Edge Layer</td><td>Physical Layer</td></tr>
<tr><td>Three Layer</td><td>Five Layer</td><td colspan="2">Middleware based</td><td>Service oriented Architecture</td><td>Fog based</td></tr>
</table>

Fig. 7. IoT architecture

7 Classification of IoT Platform

IoT platform bridges hardware and software. A part of middleware that interconnects gateways, networks to cloud, server and application is IoT platform. The different layers responsible functioning of IoT platforms are Infra layer- performs intercommunication between devices, messaging function, Communication layer- allows communication between hardware and cloud to transfer data for data analytic process, Core layer- collects data, identifies the device, manage the device, update the system software, Visualization reporting and processing layer- The outcomes can be determined from the generated reports. It frames the rules to process the data. Based on the rules applied reports are generated. This layer bonds the network, gateways with that of cloud or application. The table 7 shows some of the platforms available for IoT.

Table 7. Various platforms available for IoT

Platforms	Device support	Architecture	Protocols	Solution type
AirVantage	✓	Cloud-based	MQTT, CoAP	PaaS
Amazon web services (AWS)	✓	Cloud-based	MQTT, HTTP	IaaS
Carriots	✓	Cloud-based	MQTT	PaaS
Exosite	✓	Cloud-based	CoAP, WebSocket	PaaS
IBM IoT cloud	✓	Centralized	MQTT, HTTPS	Server
Microsoft Azure IoT Suite	✓	Cloud-based	MQTT, HTTP, AMQP	PaaS
Thing Worx	✓	Cloud-based	MQTT, CoAP, WebSocket, AMQP, DDS	PaaS
Xively	✗	Cloud-based	MQTT, HTTP, HTTPS, WebSocket	PaaS
EvryThng	✗	Centralized	MQTT, CoAP, WebSocket	SaaS

8 Classification of IoT Gateway based on operating modes

IoT gateway is middle end device which bridges sensing networks and high end IoT devices. The gateway may communicate to another gateway or low-end device may communicate to gateway or gateway may communicate to controller or gate way communicate to IoT platform. Gateway can operate in any 3 modes namely passive, semiautomated, fully automated. The difference among the operating modes are shown in table 8.

Table 8. Comparison of operating modes of Gateway

Passive	Semiautomated	Fully automated
Devices are added or deleted manually	Devices are plugged according to the network requirement	Ability to do self-configuration
It requires permission	Link available for added devices and gateway for connection	It doesn't require permission
Not flexible in nature	More flexible than passive	Flexible works with heterogenous network

9 Classification based on Storage Techniques used for IoT

The data obtained from physical objects through sensing devices has to be processed, stored. The ways in which it is stored can be of various forms and it is done by middleware. In order to supports storage, the techniques available are Big data, cloud computing and fog computing.

Big data- Huge volume of data are obtained from other devices connected to the internet. The data has to processed and analyzed to determine a correlation and pattern that exist among them. IoT integrated big data helps in improving the decision-making process. Since Big data deals with huge data it should keep track with only the important data. Bigdata performance is limited by storage and number of processors. Cloud computing- It has the ability to share resources, manage servers, networks, services. IoT manages to store huge data using this technique. The congestion, latency, cost of cloud could be reduced by processing the raw data at local nodes. Middleware sends a request directly to cloud if it could not process the request. The cloud then responds to the request. The process of cloud computing is shown in the figure 8. Fog computing- also known as mobile cloud. Bridges smart device layer with that of cloud storage layer. If proper service not provided by middleware then it will opt for either cloud or fog. In case of fog computing middleware sends request to fog. According to the service needs a request can be sent directly to fog. It finds optimal solutions for the specific request. If it is unable to process then it requests the cloud to process [2]. The schematic representation is shown in figure 9.

10 Classification of IoT based on applications

IoT devices can be classified based on the different type of data handled in different type of sectors such as medical, financial, the other sectors available in society are manufacturing, transportation, retail, consumer and home. It can also be classified based upon the domain, communication used and technology constraint driven. Based upon the end users it may be classified as consumer Internet of things CIoT and IIoT that is Industrial Internet of

Things [3]. Consumer IoT is human centered, nodes can be mobile, it handles medium to huge volume of data. New standards for devices are available. IIoT is machine centered. The standards are available for existing devices. It is fixed and has centralized network and it should take into consideration time, reliability, security etc. Data volume it handles is very high. Thus,

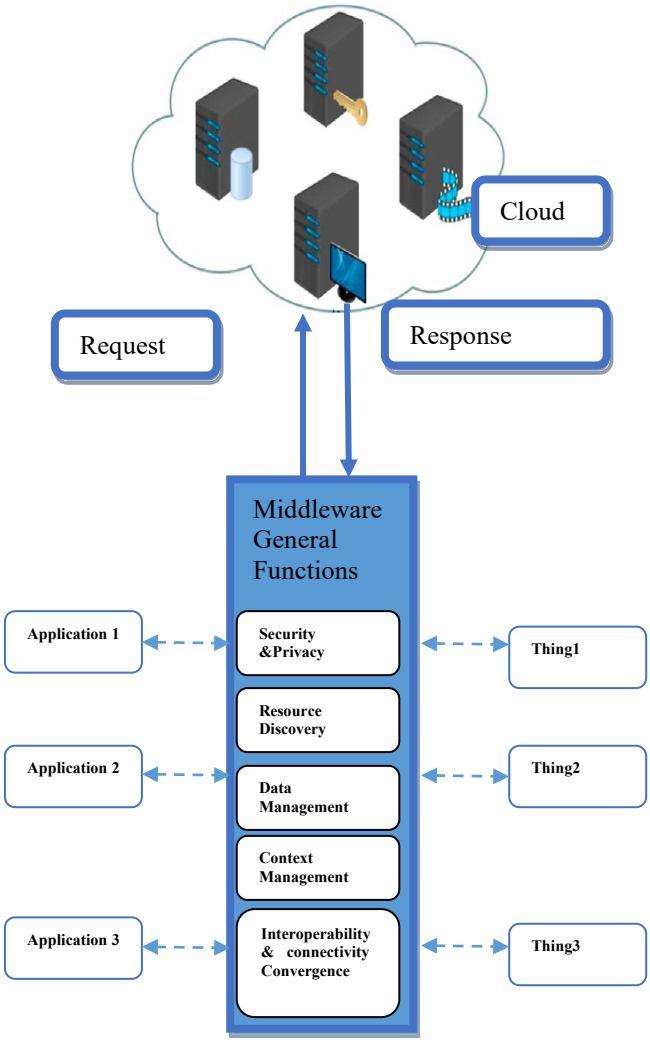

Fig. 8. Function of cloud computing

CIoT is a revolution and IIoT is an evolution. Some of the application specific IoT (ASIoT) under domain based are classified as

Internet of Battle field Things (IoBT) [4-6]- The devices required for performing functions are sensors, weapons, vehicle. It must have fast adaptive network for

communication, must be able to perform real time information processing, must provide high security.

Internet of Medical Things (IoMT) [7-8]- The devices are medical wearables which measures the parameters such as heartbeat, diabetes, ECG etc. Design has to offer interface to allow interconnection of devices with that of the networks. It must have the ability to manage as well as keep the data secured. From the large volume of data, it must improve us in decision making.

Internet of Animal Things (IoAT) [9-11]- The living creatures are monitored using smart objects and devices. In order to study about the animal life cameras can be placed in the forest and its behaviour can be studied from the information available Smart cattle collars helps in determining the temperature, its activity. The ear tags, sound analysers help in determining the diseases of the animals at the earliest. The energy efficient devices are available for on-animal measurement as well as off body wireless channel for monitoring indoor animal activity using LoRa nodes.

Internet of Waste Things (Iowaste T) [12]- also known as Internet of Bins uses smart devices such as sensors, cameras and actuators to remove the garbage accumulated in a region using wireless mesh networks. From the data provided by the monitoring devices is collected and processed for implementing an action towards clearing it. Internet of Vehicles serves as Mobile Ubiquitous LAN Extensions (MULES).

Based on the medium used for communication it is classified as

Internet of Under Water Things (IoUWT) [13]- It uses underwater sensors, smart buoys etc. The factors affecting the network medium are there is possibility to receive high error bits, long range propagation delay, bandwidth. Under water sensor networks performs better using Medium access control protocol compared to Carrier Sense multiple access or Time division multiple access which is used in terrestrial areas.

Internet of Underground Things (IoUGT) [14]- Under soil sensors, seismometers are some of the smart devices helps in real time monitoring of temperature, moisture content, ph level etc. Similar to IoUWT it also has to face many challenges to overcome the losses occurring due to electromagnetic waves which finds it hard to pass through the soil to allow underground communication, moreover since the devices are buried under the ground it is not physically accessible, replacement becomes difficult.

Based on the technology driven it is classified as

Internet of Nano Things (IoNT) [15]- Information can be transmitted and received by embedding codes in the molecules of nano materials called as molecular communication or by electromagnetic radiations of nanomaterials called as nano electromagnetic communication. The limitation is the availability of nano materials. IoNT interacts with the global environment with the help of smart devices made of nano materials.

Internet of Mobile Things (IoMobT) - Smart personal devices are like mobile phones, tablets etc. vehicles on road can move any here that is it is not fixed that is they are

independent to move and is accessible with in the network. Mobile fog supports (IoMobT). The enhancement is limited by the factors such as mobile data collection and analysis, security and privacy.

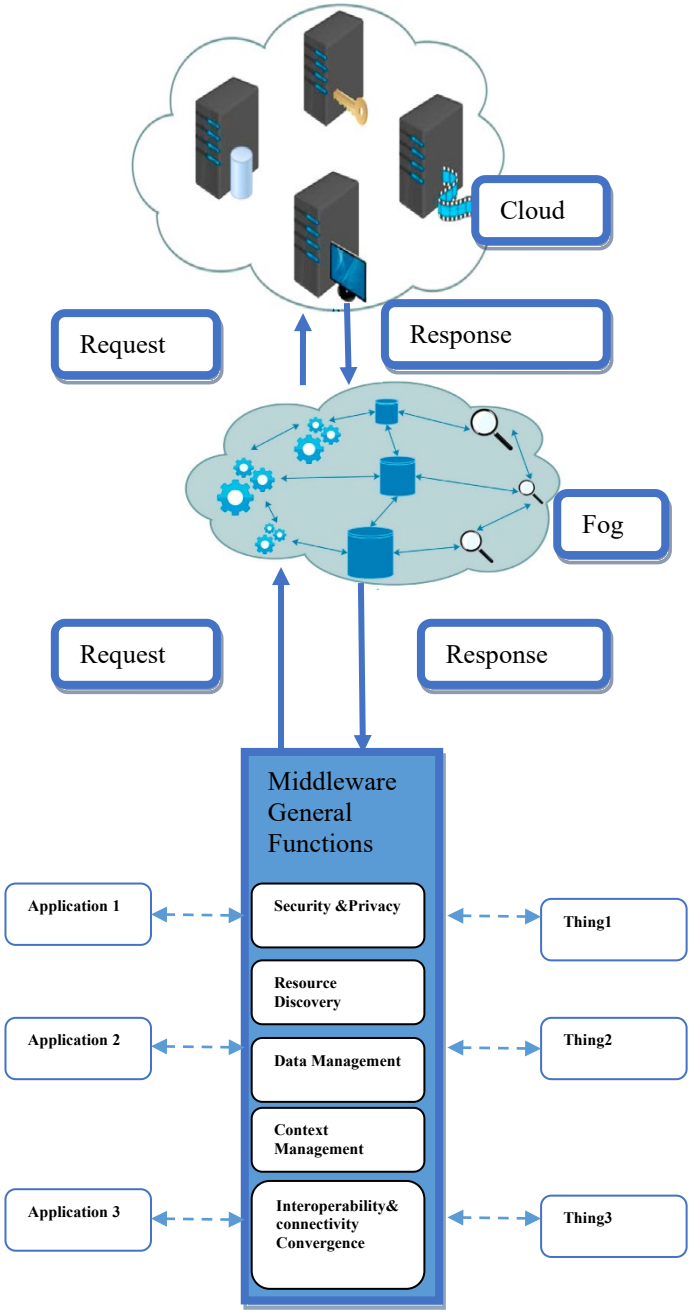

Fig. 9. Function of Fog computing

11 Conclusion

World has changed the way we live, travel and do business because of the Internet and the applications developed based on the internet. The Internet is largely focused on a totally useful creation. Interactions in all situation turns out to be impossible without IoT. IoT's going to change everything and it is the basis of a new industrial transformation, known as Industry 4.0. It is the key to the digital transformation of organizations, cities and society as a whole. IoT incorporates a number of devices. IoT has a power to expand its visibility by allowing connectivity between the smart devices. These devices are equipped with the capabilities such as sensing, processing, communicating, networking and actuating. Ubiquitous use of sensors and actuators are because of their compact size, less weight and inexpensive. This paper offers an outline of the evolving IoT based on capability and performance, entity, service-based life cycle, operating system, architecture, middleware storage, gateway, platform, communication technologies, applications. A variety of innovations are involved to improve the comfort and standard of living of people. Researches need to resolve critical issues such as security, privacy, scalability, interoperability, mobility and availability in order to face the challenges which arise when large volume of data is handled by IoT.

References

[1] Seungyong Yoon, Jeongnyeo Kim, Yongsung Jeon, “Security Considerations Based on Classification of IoT Device Capabilities”, The Ninth International Conferences on Advanced Service Computing Service Computation 2017.

[2] Amirhossein Farahzadi, Pooyan Shams, Javad Rezazadeh, Reza FarahbakhshMiddleware technologies for cloud of things: a surveyDigital Communications and Networks 4 (2018) 176–188E.

[3] Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724-4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[4] A. Kott, A. Swami, and B. J. West, “The Internet of battle things," Computer, vol. 49, no. 12, pp. 7075, Dec. 2016.

[5] Abuzainab and W. Saad, ``Dynamic connectivity game for adversarial Internet of battle_eld things systems," IEEE Internet Things J., vol. 5, no. 1, pp. 378_390, Feb. 2018.

[6] M. J. Farooq and Q. Zhu, ``Secure and recon_gurable network design for critical information dissemination in the Internet of battle_eld things (IoBT)," in Proc. 15th Int. Symp. Modeling Optim. Mobile, Ad Hoc,Wireless Netw., May 2017, pp. 1_8.

[7] Sivagami, P., Pushpavalli, M., et al., “Implementation of PV Powered Wireless Healthcare Monitoring Using IOT”, 2018 IEEE 4th International Symposium in Robotics and Manufacturing Automation, ROMA 2018

[8] P Illavarason, JA Renjit, PM Kumar, “Medical diagnosis of cerebral palsy rehabilitation using eye images in machine learning techniques”,Journal of medical systems 43 (8), 278

[9] S. Benaissa et al., ``Internet of animals: Characterisation of LoRa sub-GHz off-body wireless channel in dairy barns," Electron. Lett., vol. 53, no. 18, pp. 1281_1283, Aug. 2017.

[10] S. Neethirajan, ``Recent advances in wearable sensors for animal health management," Sens. Bio-Sens. Res., vol. 12, pp. 15_29, Feb. 2017.

[11] J. Vandermeulen et al., ``Discerning pig screams in production environments," PLoS ONE, vol. 10, no. 4, 2015, Art. no. e0123111

[12] B. Keerthana, S. M. Raghavendran, S. Kalyani, P. Suja, and V. K. G. Kalaiselvi, ``Internet of bins: Trash management in India," in Proc. 2nd Int. Conf. Comput. Commun. Technol., Feb. 2017, pp. 248_251.

[13] C.-C. Kao, Y.-S. Lin, G.-D.Wu, and C.-J. Huang, ``A comprehensive study on the Internet of underwater things: Applications, challenges, and channel models," Sensors, vol. 17, no. 7, p. 1477, 2017.

[14] M. C. Vuran, A. Salam, R. Wong, and S. Irmak, ``Internet of undergroundthings in precision agriculture: Architecture and technology aspects," Ad Hoc Netw., vol. 81, pp. 160_173, Dec. 2018

[15] I. F. Akyildiz and E. P. Stuntebeck, ``Wireless underground sensor networks: Research challenges," Ad Hoc Netw., vol. 4, no. 6, pp. 669_686, Nov. 2006