International Journal of Computer
Science and Engineering (IJCSE)
ISSN(P): 2278–9960; ISSN(E): 2278–9979
Vol. 10, Issue 1, Jan–Jun 2021; 35–44
© IASET

International Academy of Science,
Engineering and Technology
Connecting Researchers; Nurturing Innovations

NEW IOT ECOSYSTEM FRONTIERS - A SURVEY ON CLASSIFICATION IN TERMS OF IOT CHALLENGES AND CONSTRAINTS

***Anjani Yalamanchili*[1]*, D. Venkata Sekhar*[2]*, G. Vijay Kumar*[3]**

[1]Research Scholar, Department of I.T, Annamalai University, Chidambaram, Tamil Nadu, India

[2]Professor, Department of I.T, Annamalai University, Chidambaram, Tamil Nadu, India

[3]Professor, Department of C.S.E., Sri Sunflower College of Engineering and Technology, Challapalli, A.P, India

ABSTRACT

The way using the internet has been changed by the modern era; it is mutated into a strong enabler because it delivers customized ways to boost people's living standards. The Internet of Things (IoT) is a network of machines that can feel, connect with embedded technologies to meet, react to and help control their lives in all possible ways. Infrastructure availability, resource availability at inexpensive prices, IoT system usability at any time are the reasons for the enormous growth of IoT technology in the 21st century. It can be assumed that the IoT is the revolution that fuses the digital and physical world. COVID-19 is a pandemic disease caused by the Corona virus. It is a dangerous disease that in many countries has infected people and taken the lives of people in lakhs. It travels from person to person by the nose or mouth droplets of an infected person. As a protection against being poisoned, person to human contact must be prevented or adequate distancing must be preserved. In order to prevent the transmission of the disease, lock downs have been introduced. The year 2020 has created an opportunity to illustrate the role IoT has played in the lives of individuals from all industries. Anybody anywhere, anywhere linked to any aspect of the thing or part of the thing in this pandemic case. Anyone anywhere, everywhere related to any aspect of the thing or people around the world is made possible using IoT in this pandemic case. IoT and its classification are discussed in this paper

KEYWORDS: *IOT Ecosystem*

Article History

Received: ***21 Jan 2021*** **|** ***Revised:*** ***27 Jan 2021*** **|** ***Accepted:*** ***06 Feb 2021***

INTRODUCTION

IoT interfaces gadgets and sensors through remote mode and make information accessible to the clients. The clients can get to and have control over the gadget from anyplace within the world. In straightforward words IoT performs AAA that's collect information, from any put any time anyplace at that point analyze, prepare information and perform activities to support the choice making. IoT interact within the same way how individuals connected in physical world. It is done with the assistance of computerized objects [1]. The advanced objects give information as physically given by the individuals for preparing. IoT replaces human- human communication. Agreeing to measurement report from Gartner IoT investigate, CISCO IoT solidness approximately 25-30 billion of IoT gadgets will be associated to the Web. It is evaluated that 127 modern IoT gadgets will be interfacing each moment. The number of IoT gadgets in domestic will have a fast rise and it is anticipated to be around 12.86 billion. IoT has turned out to be boon not as it were for an indicated division but for all sectors [2].

There are two IoT markets. They are Even and vertical IoT showcase. IoT showcase which centres on the particular administrations that's in arrange to meet the requests of particular individuals is called vertical showcase and it may be either industry particular or statistic particular [3]. Level IoT showcase centres on wide extend of client needs and it has huge client base. In flat showcase buyers and buyers will be of distinctive divisions of the economy. From the Figure 1 it is obvious that sum contributed on vertical IoT of diverse divisions has seen fast development from 2015-2020. The number of IoT gadgets associated to the web is more than that of the versatile gadgets associated to web [4]. The assessed increment in showcase share contributed by diverse divisions towards IoT application for the year 2015-2025 is appeared within the Figure 2 and it is found that more speculations are made on wellbeing care units to convert conventional hardware and machines into savvy items. Since of this widespread COVID-19 there's plausibility to present Robots with wellbeing checking framework to dodge human interaction and to supply medications to tainted people to diminish the infection spread in future. So, rate of speculation in wellbeing care IoT applications will have colossal development when compared to other divisions. COVID-19 affect will cause a huge alter not as it were in Restorative IoT applications but too in instructive sectors as well as mechanical divisions where there's plausibility of interaction of community of individuals [5].

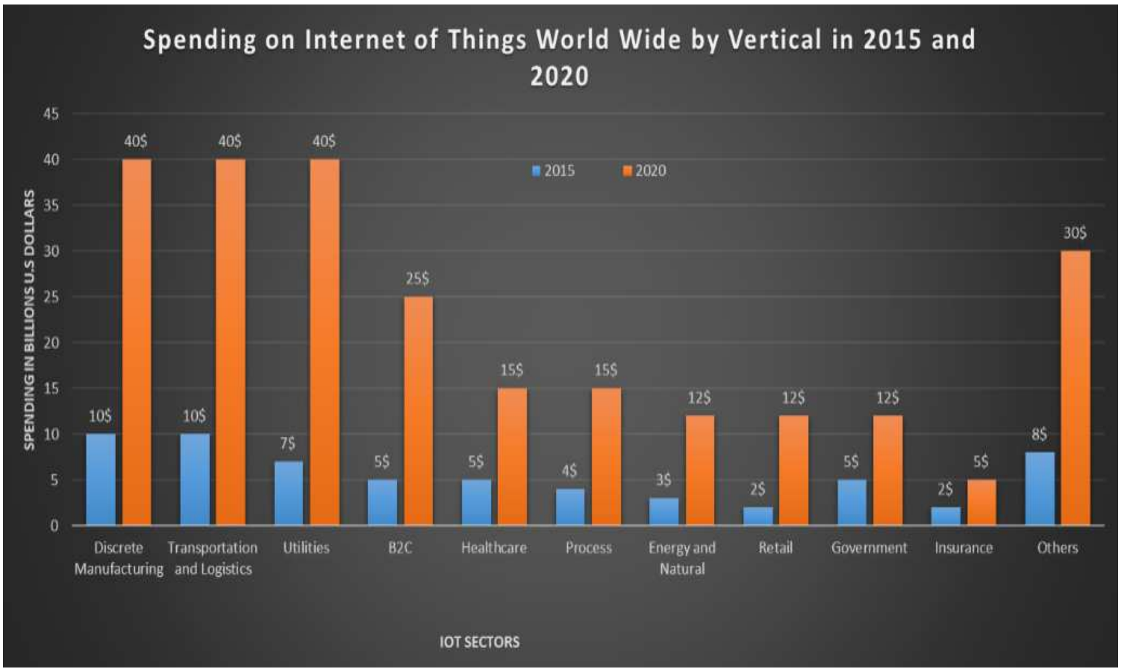

Figure 1: Investment in the Multiple IoT Industries in Billions of US Dollars (Source: Forbes).

IOT CLASSIFICATION BASED ON CAPABILITY AND PERFORMANCE

IoT grouping can be achieved in various ways. IoT gadgets are graded as low, middle and high-ended gadgets on the basis of capability and execution. Low-end gadgets based on advanced features such as memory, backup of heterogeneous devices, network organization, reliability and genuine time capability are categorized as Type0, Type1 and Type2. Cameras, actuators, openmote, waspmote, Tmote sky, ATMEL SAM R21 Xplained-pro, etc. Type0 has resources that are minimal. The first layer reflects it. It contains functions for sensing and actuating. In contrast to low end instruments, Sensors Type1 has more power [6]. It offers more features than Type0.0. The downside is that it has little computational capacity to manage difficult specifications. It requires fundamental microcontrollers. In other words, it increases the functionality of IoT products with lower ends. It has functions such as image recognition, extraction of data, etc. Form 2 requires CPU, RAM, flash memory and supports traditional operating systems such as LINUX, UNIX. It can be combined with nearly all protocols for communication. The ability of middle-end IoT systems to use more than one communication technology. The spectrum of hundreds of MHZ is the clock speed and RAM [7]. It has more limited resources relative to low-end devices, but fewer than those of high-end devices. The design specifications for IoT devices and protection requirements for these IoT devices are outlined in Table 1 and 2.

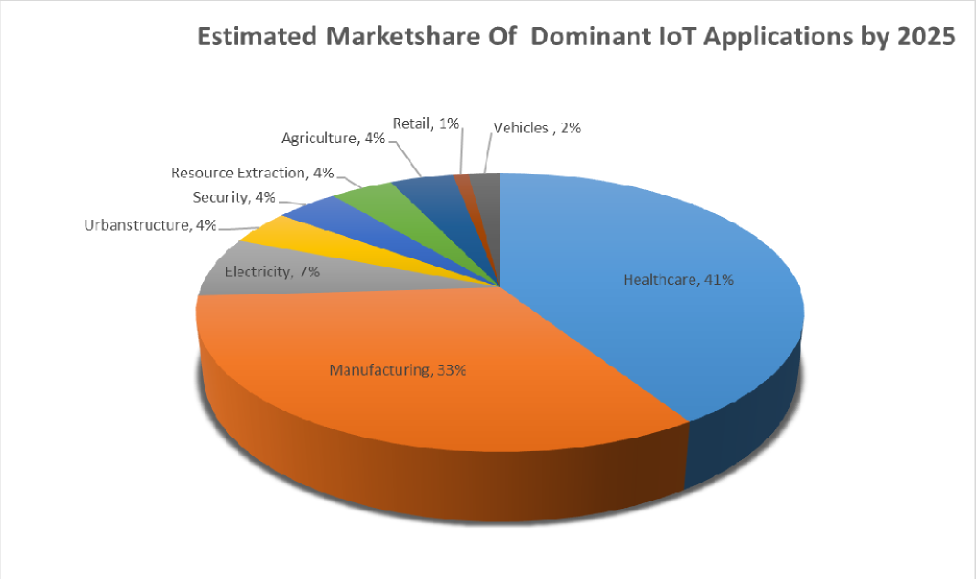

Figure 2: Estimated Contribution of the IoT Industries that Control.

Table 1: Specifications for Various IoT Application Forms

	Specifications				
		RAM	**Flash**	**RTOS Support**	**Communication Protocols**
Low End Devices	Type0	<10kB	<100 kB	Does not support	Use gateways for communication
					No protocol stack embedded
	Type1	~10kB	~100kB	Could be implemented	Use light weight protocols, communicate with other devices without using gateway
	Type2	~50kB	~250kB	Could be operated	Supports communication protocol such as HTTP

Table 2: Security Specifications Focused on the Capability of IoT Devices

Categories	**Security Requirements**	**Type0**	**Type1**	**Type2**
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

Table 2: Contd.,

Authentication/ Authorization	User authentication		Yes	Yes
	Device authentication		Yes	Yes
	Password management		Yes	Yes
	Access control		Yes	Yes
	Device ID verification			Yes

IOT GROUPING BASED ON THE LIFE CYCLE OF ORGANIZATION AND OPERATION

Another grouping, based on the association of the entity with that of physical equipment, is known as low-level operation, assets service, entity service, consolidated service [8]. IoT is defined as deployable, deployed, or operational, depending on the level of service. Figures 3 and 4 reflect the classifications.

IOT GROUPING BASED ON OPERATING SYSTEM

A series of programs called the operating system is a bridge between applications or users and computers. The operating system is built on the IoT computers to run the programs and control the devices. It is further graded as low and high-end depending on the operating system (OS) [9]. In figure 5, the schematic representation is shown. Table 3 displays some of the operating systems required for low-level and high-level computers.

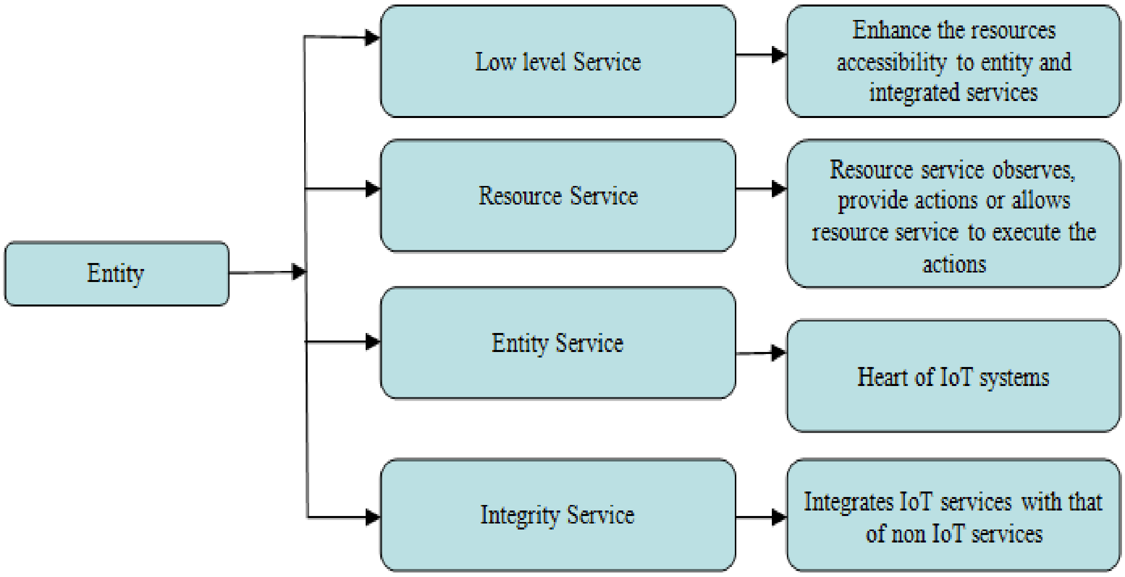
Entity
Low level Service
Enhance the resources accessibility to entity and integrated services
Resource Service
Resource service observes, provide actions or allows resource service to execute the actions
Entity Service
Heart of IoT systems
Integrity Service
Integrates IoT services with that of non IoT services

Figure 3: Entity Partnership Definition Based.

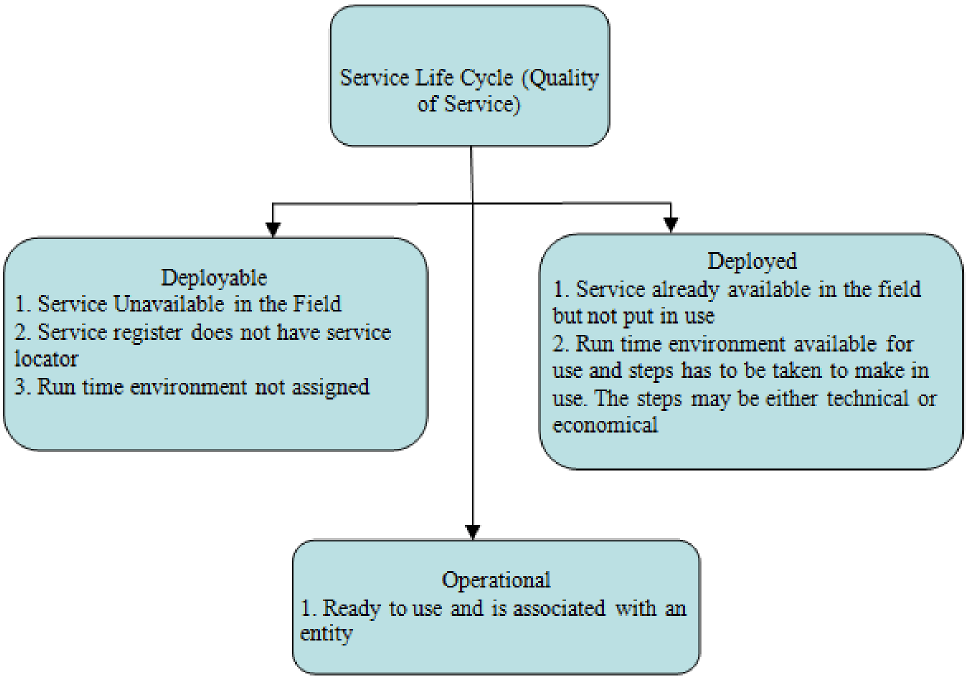
Service Life Cycle (Quality of Service)
Deployable
1. Service Unavailable in the Field
2. Service register does not have service locator
3. Run time environment not assigned
Deployed
1. Service already available in the field but not put in use
2. Run time environment available for use and steps has to be taken to make in use. The steps may be either technical or economical
Operational
1. Ready to use and is associated with an entity

Figure 4: Operation Life Cycle-Based Grouping.

Table 3: OS for Device with IoT

Operating System	Supporting Device	IoT-Enabled Devices	OS Supporting
Tiny OS	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

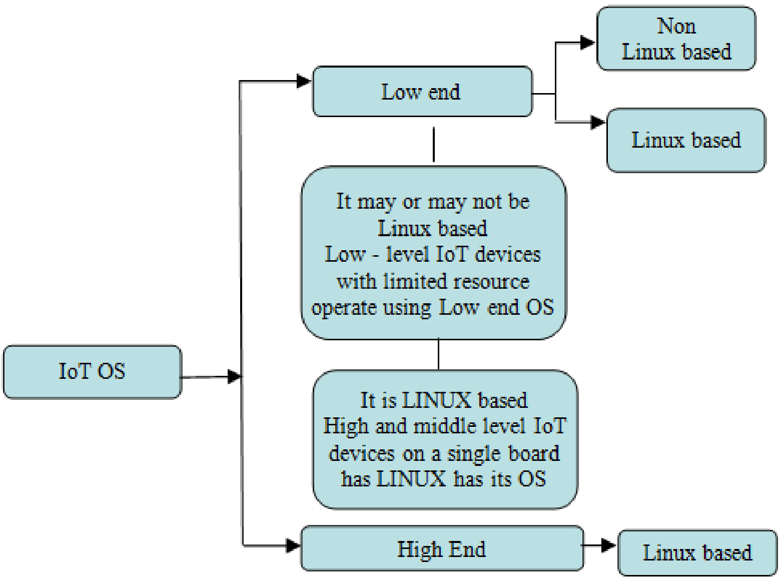
Non Linux based
Low end
Linux based
It may or may not be Linux based Low - level IoT devices with limited resource operate using Low end OS
IoT OS
It is LINUX based High and middle level IoT devices on a single board has LINUX has its OS
High End
Linux based

Figure 5: Classification by Type of OS Used.

IOT GROUPING BASED ON NETWORKING TECHNOLOGY

To provide basic smart services, IoT requires connectivity technologies to connect heterogeneous objects. In the sharing of information, communication technology support. It is possible to connect locally using Bluetooth, NFC or the Internet [10]. The key distinction between local and internet protocol communications is focused on variables such as transmission range, power usage, and memory used. IoT includes networking technologies to connect heterogeneous objects in order to provide simple smart services. Communication infrastructure assists in the exchange of knowledge. Bluetooth, NFC or the Internet may be used to connect locally. Variables such as propagation range, power consumption, and memory used reflect on the main difference between local and internet protocol communications. A subclass of RFID is NFC. NFC is a 13.56 MHZ high frequency RFID. RFID is a protected method of data sharing, consisting of a reader, tag and antenna. RFID may either be passive or aggressive. There are variations between Active and Passive RFID in Table 4.

Table 4: Active and Passive RFID

Active RFID	Passive RFID
It has own power source	Do not have their own power source
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- Developed Low Power Technologies to support the IoT model. The arrangements for all forms of sensors are improved by LPWANS (Low Power Large Area Networks). With thin, cheap batteries lasting for years, it has the potential to provide long-range communication. It finds its applications in remote controls, smart meters, construction contracts, etc. Registered versions such as NB-IoT, LTE-M and unlicensed versions such as MYTHINGS, LoRa, Sigfox and so on can be used. Reliable broad band connectivity is provided through wireless technologies used in mobile phones [11]. For its service, it needs power and its operating cost is high. Due to factors like frequency, contact range and security, it does not support most IoT products. Due to high energy demand, Wi-Fi finds its applications in intelligent home appliances, surveillance cameras, etc. Coverage, scalability and power usage are the considerations that make it less widespread. Wi-Fi-6 offers increased bandwidth < 9.6Gbps to improve data transmission in order to address the data transfer caused by the congested environment. Wi-Fi HaLow has enhanced energy output but lacks security. Along with electronic sensors, blue tooth low energy and blue tooth devices are used to provide a smart interface specifically for medical wearables and exercise. The topology of Mesh helps Zigbee to connect with more IoT computers. Higher data rates are enabled and less electricity is used. It finds its applications in medium-range IoT devices such as energy management, protection, HVAC control and so on due to low power consumption. For all IoT programs, the network specifications are not the same [12]. Each IoT application has a prerequisite for its own network. Availability, security, bandwidth latency, power consumed by devices, service quality, network management are the factors that affect the selection of wireless technology for specific IoT applications. The wireless technology for different IoT implementations is seen in Table 5.

Table 5: For Separate IoT Verticals, Wireless Technology

Key IoT Verticals	LPWAN	Cellular	Zigbee	BLE (Star & Mesh)	Wi-Fi (Star and Mesh)	RFID
	(Star)	(Star)	(Mostly Mesh)			(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			Very High	Very High	Very High	
Wearables	Moderate			Very High		
Connected car					Moderate	
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					

IOT GROUPING BASED ON MIDDLEWARE

The computing layer called IoT Middleware connects various application domains to interact over different domain interfaces. Middleware is often referred to as software glue because it allows software engineers to build contact implementation programs. If complex programming is not designed initially middleware enables to integrate it later with the help of support architecture. Schematic representation of the general functions that middleware executes [13]. In order to identify IoT middleware as service-oriented, cloud-oriented and actor-oriented middleware, accessibility, versatility and adaptive design are used. Service-oriented middleware- For end users, developers, extension and modification of IoT devices is allowed. Standalone or cloud storage systems can be service-oriented. Since it is not cost-effective, it does not support homogenous framework deployment. To support constrained services, there is no architecture provision for security techniques. Cloud-oriented middleware, which conveniently captures data, analyzes and interprets data. Security and privacy cannot be configured by the user. It has autonomy over critical details, but to support limited capital, it has no architecture framework. Users are permitted to plug and play IoT devices with actor-oriented middleware. They will uninstall the specific IoT device without disrupting and impacting the other elements of the IoT environment whenever the consumer does not need an IoT device. It enables protection and privacy to be configured by the user. Middleware is also defined as service-oriented, node-based, component-based, clustered, distributed, client-server, based on architecture nature.

IOT GROUPING BASED ON DESIGN

The simple IoT architecture consists of only three layers, namely perception layer-performing sensing and actuating, network layer-performing data transmitting and processing, device layer-providing the necessity to the user. Additional layers are used in the five-layer architecture to provide additional abstraction to the IoT architecture. Middleware interconnects heterogeneous objects with the heterogeneous device is the back bone of the IoT ecosystem, involving perception-where sensor tests the data, transport layer-performs transporting data function, processing layer-process and evaluating the data collected through transport layer. Through having control over the data flow, Middleware controls the system. The sensors and actuators have the vision layer in the middleware-based architecture along with the access layer and edge layer. The Coordinate layer provides the customer with a final application along with the application layer. Data objects in service-oriented architectures are extracted and exposed through interfaces. While the technologies and the cloud differ, the Application Programming Interface (API) stays the same. The physical layer is often the bottom in fog-based architecture, the next layer is monitoring-observing and testing the data obtained from sensors. The pre-processing layer processes the data for processing-based results. In order to provide data protection and privacy, the security layer is liable. Perception layer-Includes actuators and sensors. Sensors track the physical and environmental parameters, gather certain parameters, erase the undesirable data and transfer the data to the actuators in order to execute actions. Transport layer-Utilizing communication protocols like Zigbee, BLE, NFC etc., brings the preprocessed data for processing to the processing layer. Processing layer- Filter, formatting information gathered from sensors. It also stores and handles, via communication protocol, the sensed data received from different devices. Middleware layer- To provide useful information, it conducts conceptual and analytical operations on the data available. It uses computing platforms and cloud storage. The application layer provides the user with an application using communication protocols such as MQQT, Restricted Application Protocol, and (CoAp). IoT architecture is shown in Figure 6.

Table 6: Design of IoT

Application Layer	Application Layer	Application Layer		Applications	Transport Layer
	Middleware Layer	Coordination Layer		Service	Security Layer
				Composition	
Network Layer	Processing Layer	Middleware Layer		Service	Storage Layer
				Management	
Perception	Transport Layer	Backbone Network Layer		Object	Pre-processing
Layer				Abstraction	Layer
	Perception Layer	Perception	Access Layer	Objects	Physical Layer
		Layer	Edge Layer		Physical Layer
Three Layer	Five Layer	Middleware based		Service oriented Architecture	Fog based

IOT PLATFORM GROUPING

The IoT interface bridges hardware and technology. The IoT platform is a feature of middleware that links gateways, cloud, server and device networks. Infra layer-performs intercommunication between devices, messaging feature, connection layer-enables communication between hardware and cloud to transfer data for data analytic processes, core layer-collects data, identifies the device, manages the device, updates the software framework. From the produced reports, the results can be calculated. To process the data, it frames the rules. Reports are created based on the rules applied. This layer connects the network, the gateways, to the cloud or device layer.

CONCLUSIONS

Because of the Internet and the apps generated on the internet, the environment has changed the way we work, move and do business. The Internet is predominantly based on a totally beneficial growth. Without IoT, contact turned out to be unlikely in all cases. IoT will change everything and is the cornerstone of a modern technological transformation, referred to as Business 4.0. It is the secret to organizations, cities and culture as a whole being digitally changed. A variety of sensors are built into the IoT. By having communication between smart devices, the IoT has the ability to extend its visibility. These systems are fitted with features such as identification, sorting, interaction, networking and service. Due to their small nature, less weight and cheap use of sensors and actuators is omnipresent. This paper provides an overview of the emerging IoT based on power and performance, organization, life cycle based on operation, operating system, infrastructure, storage of middleware, portal, network, technologies of communication, applications. In order to improve people's convenience and quality of life, a series of technologies are involved. In order to face the difficulties that occur as vast quantities of data are managed by the IoT, research needs to tackle key problems such as stability, anonymity, scalability, interoperability, mobility and availability.

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 Farahbakhsh Middleware technologies for cloud of things: a survey Digital 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 battlefield things systems," IEEE Internet Things J., Vol. 5, No. 1, pp. 378_390, Feb. 2018.*
6. *M. J. Farooq and Q. Zhu, ``Secure and reconfigurable network design for critical information dissemination in the Internet of battle field things (IoBT)," in Proc. 15th Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw., May 2017, pp. 1_8.*
7. *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.*
8. *S. Neethirajan, ``Recent advances in wearable sensors for animal health management," Sens. Bio-Sens. Res., Vol. 12, pp. 15_29, Feb. 2017.*
9. *J. Vandermeulen et al., ``Discerning pig screams in production environments," PLoS ONE, Vol. 10, No. 4, 2015, Art. no. e0123111*
10. *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.*
11. *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.*
12. *M. C. Vuran, A. Salam, R. Wong, and S. Irmak, ``Internet of underground things in precision agriculture: Architecture and technology aspects," Ad Hoc Netw., Vol. 81, pp. 160_173, Dec. 2018*
13. *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.*