IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Architecture, Protocols, Layers and Elements of IoT

[1] P. Ramesh [2] M. Sri Venkat Rami Reddy, [3]Dr. P.Bhaskara Reddy
[1] [2]Assistant Professor of Dept. ECE,. [3] Professor & Director,
Holy Mary Institute of Technology and Science
(An UGC-Autonomous Institution),
Bogaram(V), Keesara(M), Malkajgiri-Medchal (Dt) Telangana, India.

ABSTRACT

The paper provides an overview about IoT, discussing the technologies, protocols and various application issues. IoT is a collection of a number of technologies like smart sensors RF-ID ,communication technologies and Internet Protocols .The basic idea is to have anetwork made up of physical objects with electronics, software, sensors and network connectivity that enables collection and exchange of data between these objects. Year–over– year, the number of IoT devices increased 31% totaling to 8.4 billion in 2017 and by 2020 the count is estimated to go to 30 billion. The current progress in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the starting phase of the IoT. In the future, IoT is expected to combine different technologies and enable new applications by connecting physical objects together supporting intelligent decision making. The paper starts with a general overview of IoT, then an overview of IoT enabled technologies, protocols and applications is given. A detailed summary of the most up to-date protocols is provided, application issues which help researchers and developers understand the protocol suite to deliver desired functionalities is discussed. A brief summary of some of the key IoT challenges and related research is also provided. Moreover, the relation between IoT and other emerging technologies including big data paralytics, cloud computing and fog computing is provided at the end.

Key words: *IoT, machine-to-machine (M2M), IP Address, MAC Address, IPv4 and IPv6, Single Board Computers (SBCs)*

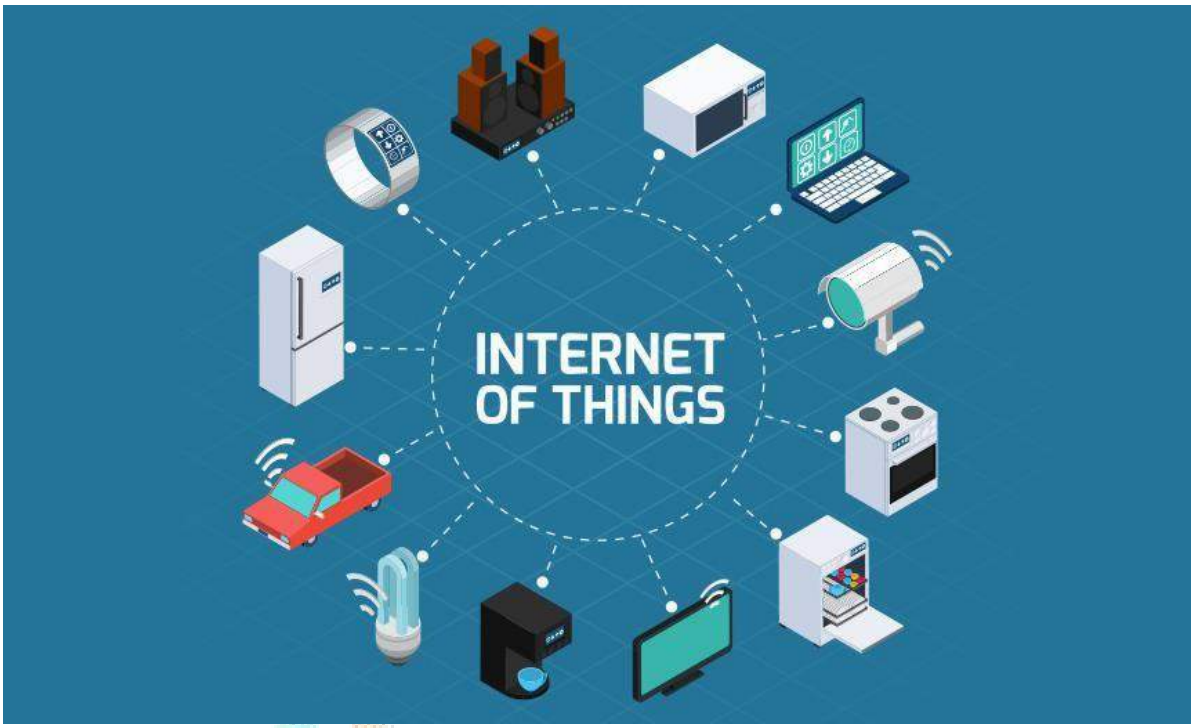


Fig: IoT

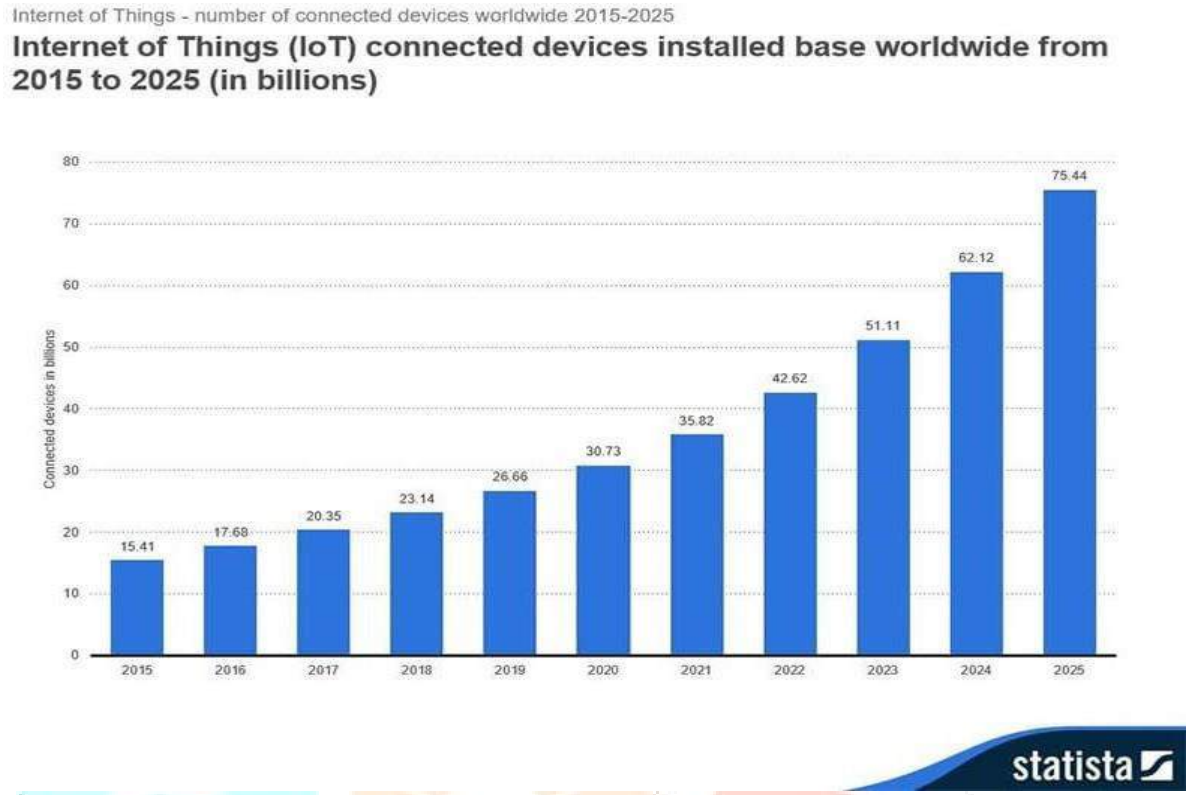
1. INTRODUCTION

Realizing the idea of IoT, a large number of physical objects are being connected to the internet at a faster rate. IoT, with the help of internet, enables objects to share data in between. Examples include HVAC (Heating, Ventilation and Air Conditioning) monitoring and control systems that enable smart homes. Other applications influenced by IOT include transportation, healthcare, industrial automation and emergency response to natural as well as man-made disasters where human decision making is difficult. IoT enabled physical objects share information and coordinate decisions. The devices act as smart objects in an IoT environment. IoT enabled objects are smart due to ubiquitous and pervasive computing, embedded nature of IoT devices, various communication technologies used in IoT devices, sensor networks, various internet applications and protocols

At the Centre of IoT, lies the idea to connect existing and future physical objects to the internet. IoT creates an interconnection between physical world objects with the virtual world of information. With IoT, physical world objects can identify each other, sense each other , have network and computing capabilities that will allow them to share information and accomplish some objectives. Ultimately, with IoT, physical objects can be connected anytime, anywhere, with anything and anyone using any path/ network and any service.

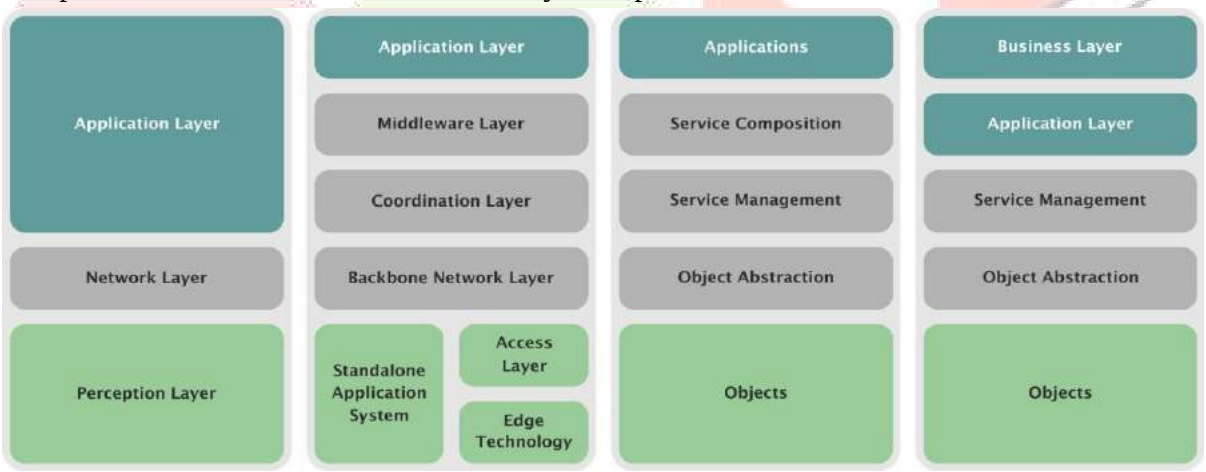
In future, the IoT will -have a prominent impact in home and business applications , to contribute to the quality of life and to boost world's economy. With smart homes, people won't have to get down to open their garages when reaching home, coffee can be prepared automatically, TVs and other appliances can be controlled remotely etc. For achievement of such potential growth, market demands have to be met by emerging technologies and innovations and by the growth of service applications. In addition to this, devices need to be developed to fit customer requirements in terms of availability anywhere and anytime. Also, for compatibility between heterogeneous groups new protocols are required. Moreover, architecture needs to be standardized for the IoT to create a competitive environment for companies to deliver quality products. In addition, to match the IoT challenges ,Internet architecture needs to be revised. For example, the large number of objects connecting to the Internet should be considered in many underlying protocols. In 2010, the number of Internet connected objects surpassed the earth's human population, this means use of a large addressing space (e.g., IPv6) to meet customer demands for smart objects. Due to the inherent heterogeneity of the Internet connected objects and the ability to monitor and control physical objects,

security and privacy become other important requirements for the IoT. For delivering high quality service at an efficient cost, management and monitoring of the IoT should take place



2. IoT ARCHITECTURE

A number of different architectures are proposed in various literature, a 5-layer model isthe most accepted one. A brief discussion of its 5 layers is provided:



1. Objects layer (also called as Perception layer)

This layer comprises of devices that aim to collect and process information. Sensors and actuators are used to perform different functions such as querying location, vibration, temperature, weight motion, humidity, acceleration, etc. In order to configure heterogeneous objects, standardized plug and play mechanisms need to be used by the perception layer. Digitized data is transferred to the Object Abstraction layer through secure channels. Initiation of data created by IoT takes place here.

2. Object Abstraction Layer

Object Abstraction Layer transfers data generated by Objects layer to Service Management layer through secure channels. The various technologies used for data transfer are RF-ID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, infrared, ZigBee, etc. Functions like data management processes and cloud computing are handled here.

3. Service Management Layer

The service management layer's main responsibilities are facilitating information processing, decision-making, and control of pairing requester information processing for relevant tasks. This layer enables the IoT application programmers to deal with heterogeneous objects without taking into consideration a specific hardware platform.

4. Application Layer

The application layer provides the customers with smart high-quality facilities according to the pre-request of the customers. For example, the application layer can provide temperature and air humidity measurements to the customer interested for the relevant data. This layer has the ability to provide high-quality smart services to meet customers' needs. The application layer covers a large base of vertical markets such as smart transportation, smart building, industrial automation and smart healthcare.

5. Business Layer

The Business layer gives a representation of the business model and data that is received from the application layer. This layer manages the overall IoT system activities and services. It also supports decision-making processes based on Big Data analysis. In addition, monitoring and management of the underlying four layers is achieved at this layer.

3. IoT Elements

IoT Elements can be divided into 6-main types:

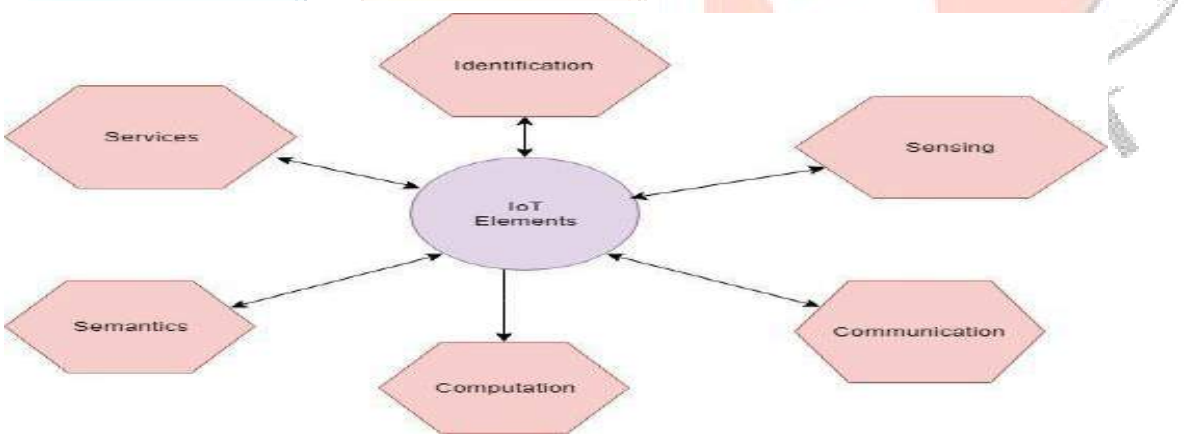


Fig: Elements of IoT

IoT Elements are of 6-types:

1. **Identification:**

The importance of identification is growing in IoT, as more and more devices are getting added day by day and, for the successful communication purpose of the devices. Heterogeneity of platforms in IoT also makes identification an important issue. In order to name and match services with their demand, identification is crucial in IoT. Identification methods such as Electronic Product Codes (EPC) and ubiquitous codes (u Code) are available. Further, addressing the IoT objects is critical to differentiate between object ID and its address. Object ID refers to its name such as "T1" for a particular temperature sensor and object's address refers to its address within a communications network. Addressing methods of IoT objects include IPv6 and IPv4. Making a distinction between object's identification and address is important since identification methods are not globally unique, so addressingAssists to uniquely identify objects. In addition, objects within the network might use public IP's and not private ones. Identification methods are used to provide a clear identity for each object within the network.

2. Sensing:

The gathering of data within the network and sending it to a data warehouse, database or cloud, is called as sensing. The data has to be collected from a wide variety of devices , made up of different platforms and architectures. As the IoT devices usually have limited data storage capabilities, sensing of useful data which is required for processing is very important. The data sensing process in IoT is always related to data storage capabilities of the IoT network. The data is analyzed and based on the requirement, actions are taken. The IoT sensors can be smart sensors, actuators or wearable sensing devices. Single Board Computers (SBCs) integrated with sensors and built-in TCP/IP and security functionalities are typically used to realize IoT products.

3. Communication:

Communication technologies in IoT involve connecting heterogeneous objects together to deliver smart services. The devices in IoT are usually from wide variety of architectures and use different technologies for communication purpose. In IoT, connecting wide variety of devices for smooth communication is a challenging task. IoT nodes are designed to operate using low power in the presence of noisy communication links. The various communication protocols used for the IoT are Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-Advanced.

4. Computation:

The computational ability of the IoT is defined by processing units and software applications. IoT applications are run on various hardware platforms such as Arduino, Friendly ARM, Intel Galileo, Raspberry PI, Beagle Bone,WiSense, Mule etc. Various Os's like RTOS based Contiki have been widely used in IoT. Contiki includes a simulator Cooja which allows researchers and developers to simulate and emulate IoT and wireless sensor network applications. Tiny OS, Lite OS and RIoT OS also offer light weight OS designed for IoT environments. Cloud Platforms form another important computational part of the IoT. These platforms provide facilities for smart objects to send their data to the cloud, for big data to be processed in real-time, and eventually for end-users to benefit from the knowledge extracted from the collected big data. There are a lot of free and commercial cloud platforms and frameworks available to host IoT services.

5. Services:

IoT services can be grouped into 4 classes:

1 . Identity related services, 2. InformationAggregation services, 3. Collaborative-Aware

4. Services and Ubiquitous Services.

Identity related services include applications to map real world objects to the virtual worldfor purpose of identification.

Information Aggregation Services collect and wrap-up sensory measurements that need to beprocessed and send to the IoT application.

On top of Information Aggregation Services lies the Collaborative-Aware Services , theseservices use the obtained data to make decisions and react accordingly.

Ubiquitous Services make sure that Collaborative-Aware Services are available to anyone and at all possible times.

6. **Semantics:**

In semantics, different machines extract knowledge smartly to provide the required services. Knowledge extraction means discovery and usage of resources and information modeling. Also, it means making right decisions by analyzing and recognizing data to provide exact services. This requirement is supported by Semantic Web technologies such as the Resource Description Framework (RDF) and the Web Ontology Language (OWL).

5. Characteristics of IoT

Following are the characteristics of IoT:

1. Inter-connectivity: Inter-connectivity in IoT means bringing together of various objects to share data. Connectivity of objects leads to creation of data in IoT, which forms the basis for analysis purposes. Connectivity between objects is achieved by internet mostly, creating a common communication infrastructure for all the objects connected together. Interconnectivity in IoT enables devices across various platforms to share data using a common communication channel. Devices in IoT can be connected using a number of different topologies such as P2P, Star, Mesh and Hybrid. The common types of protocols used are WiFi, Thread, ZigBee, Bluetooth, RFID and NFC.

2. Heterogeneity: Devices used in IoT are heterogeneous. Different devices with different hardware platforms and different networks are used. Devices with different processing powers and storage capabilities, as well as completely different architecture can be part of IoT. Heterogeneity is one of the essential features of IoT , which lead to its widespread use across different platforms and domains. Heterogeneity in IoT makes possible for a number of devices, based on different technologies, to interact with each other, without any compatibility issues among the devices. Heterogeneity in IoT can be achieved by Cloud Radio Access Network(Cloud-RAN) and Software Defined Radio(SDR) framework that adapt to devices' communication technology.

3. Dynamic changes: Devices in IoT keep changing on their states, e.g., on and off state. Moreover devices in IoT keep changing their location as well as speed(An IoT enabled vehicle).The total number of devices in an IoT environment keeps on changing also, depending upon the need devices get added up and sometimes devices are also removed. The use of a particular resource in a number of devices also changes dynamically, a device might be using a particular resource (say storage) more at one point of time and at some other point of time, the same device can be using its other resource(say processor) more than other resources.

4. Enormous scale: An enormous number of devices are getting added to IoT at a larger scale, day by day. Devices from different architectures and platforms add to the enormous structure of IoT. The enormity of IoT can be conceptualized by a report. which states that 5.5 million new things will get connected every day and 6.6. billion connected things will be in use worldwide by 2026-30 percent increase from 2015.The report also predicts that the number of devices connected will be 20.8 billion by 2020.The enormous scale feature of IoT makes data management in IoT very critical. With such an enormous data, the interpretation of data for application purposes is a big challenge. To differentiate between useful and vague data, in such a huge database, utmost care and use of sound methodologies have to be implemented.

5. Security: With a large number of things added to IoT, the vulnerabilities of data breach and various security issues are bound to arise. An attack in a single IoT device means breaching the security of a big network. IoT devices are usually resource constrained and don't possess the compute power necessary to implement strong security features. As a result many IoT devices don't afford advanced security features. For instance, sensors for temperature detection can't handle advanced encryption and or other security features. Currently IoT security doesn't have any industry accepted standard. There is no single agreed-upon framework in IoT, organizations usually have their own specific standards.

6. IoT common Standards:

In order to simplify and facilitate programming IoT applications and service providing in IoT, many IoT standards are proposed. Protocols for IoT have been developed by WorldWide Web Consortium(W3C),Internet Engineering Task Force(IETF), EPCglobal, *Institute of Electrical and Electronics Engineers* (IEEE) and the *European Telecommunications Standards Institute* (ETSI). IoT protocols can be broadly classified into four categories: application protocols, service discovery protocols, infrastructure protocols and other influential protocols. We provide an overview of some of the common protocols in these categories and their core functionality.

1. Application Protocols:

Constrained **A**pplication **P**rotocol(CoAP): CoAP is an application layer protocol for IoT applications, created by IETF Constrained RESTful Environments (CoRE) working group. The CoAP defines a web transfer protocol based on Representational *State Transfer* (REST) on top of HTTP functionalities. REST is a cacheable connection protocol that relies on stateless client-server architecture. It represents a simpler way to exchange data between clients and servers over HTTP. It is used within mobile and social network applications and iteliminates ambiguity by using HTTP *get*, *post*, *put*, and *delete* methods. REST enables clientsand servers to expose and consume web-services like the Simple Object Access Protocol(SOAP) in an easier way using Uniform Resource Identifiers (URIs) as nouns and HTTP *get*,*post*, *put*, and *delete* methods as verbs. REST does not require XML for message exchanges. Unlike REST, CoAP is bound to UDP (not TCP) by default which makes it more suitable forthe IoT applications. Furthermore, CoAP modifies some HTTP functionalities to meet theIoT requirements such as low power consumption and operation in the presence of lossy andnoisy links. CoAP can be divided into two sub-layers, namely: the messaging sub-layer andthe request/response sub-layer. The messaging sub-layer detects duplications and providesreliable communication over the UDP transport layer using exponential backoff .Therequest/response sub-layer on the other hand handles REST communications.

1.**Message Queue Telemetry Transport (MQTT):** MQTT is used to connect embedded devices and networks with applications and middleware. The connection operation is based on a routing mechanism (one-to-one, one-to-many, many-to-many) and enablesMQTT as an optimal connection protocol for the IoT and M2M. MQTT is built on top of the TCP protocol and is suitable for devices with low resource availability, unreliable or low bandwidth links. MQTT simply consists of three components, subscriber, publisher,and broker. An interested device would register as a subscriber for specific topics, a broker will inform the registered subscriber once the publisher publishes some topics of interest. Thepublisher acts as a generator of interesting data, the broker acts as an informer to the subscriber. MQTT is used in many applications such as health care, monitoring, energy meter, and Facebook notification. Therefore, the MQTT protocol represents an ideal messaging protocol for the IOT and M2M communications and is able to provide routing for small, cheap, low power and low memory devices in vulnerable and low bandwidth networks.

2. Extensible Messaging and Presence Protocol (XMPP): XMPP is an IETF instant messaging (IM) standard that is used for multi-party chatting, voice and video calling. Users can communicate with each other by sending instant messages on the internet using XMPP. With XMPP, IM applications achieve authentication, access control, privacy measurement, hop-by-hop and end-to-end encryption, and compatibility with other protocols.

1. Advanced Message Queuing Protocol (AMQP): AMQP focuses on message oriented environments and is an open standard application layer protocol. It provides reliable Communication through message delivery guarantee primitives which include at-most-once,at-least-once and exactly once delivery. For exchanging messages AMQP uses a reliabletransport protocol like TCP.

2. Data Distribution Service (DDS): Developed by Object Management Group, DDS is a publish-subscribe protocol for real-time M2M communications. For Quality of Service (QoS) and high reliability to its applications, DDS makes use of broker-less architecture and multi-casting. Its broker-less publish-subscribe architecture suits well to the real-time constraints for IOT and M2M communications. From a developers perspective, DDS addresses a variety of communication criteria like security, urgency, priority, durability, reliability etc. DDS architecture defines two layers: Data-Centric Publish-Subscribe (DCPS) and Data-Local Reconstruction Layer (DLRL). DCPS is responsible for information delivery to the subscribers. DLRL , is an optional layer and serves as the interface to the DCPS functionalities. It facilitates the sharing of distributed data among distributed objects.

6. A Service Discovery Protocols

In order to ensure scalability, IoT requires a resource management mechanism that is able to register and discover resources and services in an efficient and dynamic way. The protocols used are: multicast DNS (mDNS) and DNS Service Discovery (DNS- SD) that can discover resources and services offered by IoT devices.

Multi-cast DNS (mDNS): mDNS acts as a base service, in the form of Name Resolution, for some IoT applications like chatting. mDNS can perform the task of uni-cast DNS server. In mDNS, DNS namespace is used locally without extra expenses or configuration, adding to its flexibility. Some of the advantages which makes mDNS appropriate choice for the internet based embedded devices are:

1. To manage devices, no need of manual reconfiguration or extra administration
2. For its smooth functioning, mDNS doesn't need infrastructure.
3. If a failure of infrastructure occurs, mDNS still works.

DNS Service Discovery (DNS-SD): DNS-based service discovery (DNS-SD) includes pairing of required services by clients using mDNS. Using this protocol, clients can discover a set of desired services in a specific network by employing standard DNS messages. Essentially, DNS-SD utilizes mDNS to send DNS packets to specific multi-cast addresses through UDP. There are two main steps to process Service Discovery: finding host names of required services such as printers and pairing IP addresses with their host names using mDNS.

7. Infrastructure Protocols

Routing Protocol for Low Power and Lossy Networks (RPL): A link-independent routing protocol based on IPV6 for resource constrained nodes, standardized by IETF routing over low-power and lossy links(ROLL) working group. RPL was created to support minimal routing requirements through building a robust topology over lossylinks.

RPL supports simple and complex traffic models like multipoint-to-point, point-to-multipoint and point-to-point.

1. **Low PAN**: IOT communications rely on low power Wireless Personal Area Networks, which have some special characteristics different from former link layer technologies like limited packet size, variable address length, and low bandwidth. A need for an adaptation layer that fits IPV6 packets to the IEEE 802.15.4specifications arised. 6LoWPAN is the specification of mapping services required by the IPv6 over Low power WPANs to maintain an IPv6 network. The standard provides header compression to reduce the transmission overhead, fragmentation to meet the IPv6 Maximum Transmission Unit (MTU) requirement, and forwarding to link-layer to support multi-hop delivery.

2. **IEEE 802.15.4**: This protocol is utilized by IoT due to its low power consumption, low data rate, low cost, and high message throughput. The protocol specifies a sub- layer for MAC and a physical layer for low rate wireless private area networks (LR-WPAN). It provides a reliable communication, Crosshatch operability and can handle a large number of nodes. It also provides a high level of securitystandards, encryption and authentication services.

3. Bluetooth Low Energy: Bluetooth Low-Energy (BLE) or Bluetooth Smart uses a short range radio with a minimal amount of power to operate for a longer time (even for years). Its range coverage (about 100 meter) is ten times that of the classic Bluetooth while its latency is 15 times shorter. BLE can be operated by a transmissionpower between 0.01 mW to 10 mW. With these characteristics, BLE is a good candidate for IoT applications.

4. EPC Global: Electronic Product Code is used in the supply chain management to identify items, as a unique identification number stored on an RFID tag. The underlying architecture uses Internet based RFID technologies along with cheap RFIDtags and readers to share product information. Because of its openness,

scalability, interoperability and reliability, this architecture is recognized as a promising technique for the future of the IoT.

5. LTE-A (Long Term Evolution—Advanced): LTE-A includes a set of cellular communication protocols that fit well for Machine-Type Communications (MTC) and IOT infrastructures especially for smart cities where long term durability of infrastructure is required. In terms of service cost and scalability, it outperforms other cellular solutions.

6. Z-Wave: Z-Wave is used for 30 meters point-to-point communication and is specified for applications that involve small transmissions like light control, household appliance control, smart energy and HVAC, access control, wearable health care control, and fire detection. Z-Wave operates in ISM bands (around 900 MHz) and allows transmission rate of 40 kbps.

8. QOS CRITERIA: IoT CHALLENGES AND FUTURE DIRECTIONS

Key challenges in IoT include availability, reliability, mobility, performance, scalability, interoperability, security, management, and trust. Addressing these challenges will lead to efficiency of service providers and application programmers.

1. Availability: To provide anytime and anywhere services for customers, the availability in IOT must be realized in the hardware as well as software level. Software availability means ability of IoT applications to provide services for everyone at all places, at the same time. Availability of hardware refers to the existence of devices all the time that are compatible with the IoT functionalities and protocols. High availability of IoT services can be achieved by providing redundancy for critical devices and services.

2. Reliability: Reliability plays an important role for increasing the success rate of IoT service delivery it becomes critical and has more stringent requirements when it comes to the field of emergency response applications. Reliability must be implemented in software and hardware throughout all the IoT layers. For an efficient IoT, the communication must be reliable.

3. Mobility: As most of the IoT services are expected to be delivered to mobile users, mobility becomes a challenge for the IoT implementations. An important premise of the IoT is connecting users with their desired services continuously while on the move. Service interruption for mobile devices can occur when these devices transfer from one gateway to another. A resource mobility scheme has been proposed which proposes two modes: caching and tunneling to support service continuity. Using these methods, applications can access IoT data even in the case of the temporary unavailability of resources.

4. Performance: Performance of IoT services depends on the performance of many components as well as the performance of the underlying technologies. Many metrics can be used to assess the performance of the IoT including the processing speed, communication speed, device form factor, and cost.

5. Management: Management in IoT includes managing Fault, Configuration, Accounting, Performance, and Security (FCAPS) aspects of billions and trillions of smart devices. Fault management in IoT includes fault detection, fault diagnosis and isolation, restoration of service, event correlation and aggregation, and problem resolution. Fault management in IoT means ensuring that an IoT network won't go down if there is malfunctioning of any device in the network. Fault management makes sure that an IoT network is up all the time. Any problems associated with any of the IoT devices should be handled properly without any performance affect on the whole IoT network. Configuration in IoT deals with maintaining consistency of a device in terms of its performance throughout its lifetime. This calls for the development of new light-weight management protocols.

6. Scalability: Scalability in IoT refers to adding more devices, services and functions for customers without any affects on the QoS. The number of devices added, depending upon the need, to an IoT network shouldn't lead to challenges. A proper IoT network should be able to adjust the number of devices according to the need and with time. An IoT network should be able to meet future demands and should be able to accept any system changes. With the presence of diverse hardware platforms and communication protocols, scalability remains an issue in IoT. Scalability in IoT can be either Vertical or Horizontal. In

vertical scaling, also known as scaling-up, capacity of a single software or a hardware unit is increased by adding more resourcesto it. In horizontal scaling, also known as scaling-out , multiple hardware or software units are added to form a single unit.

7. Inter-operability: IoT includes a number of heterogeneous devices that belong to different platforms. A number of devices form multiple platforms become part of IoT,the devices should be able to inter-operate without any changes made to the basic device configuration. An IoT network should ensure that all devices are communicating properly and with efficiency, without any conflict in the interoperability of devices. An IoT network which fails to ensure smooth communication among a wide variety of devices wouldn't stand for a long as an independent IoT network. Interoperability should be taken into consideration by both application developers and IoT device manufacturer's to ensure the best delivery of services for all customers regardless of the architecture of the hardware platform that they use.

8. Security and Privacy: Security poses an important challenge for the IoT implementations due to the absence of common standard and architecture for the IoT security. It is not easy to guarantee the security and privacy of users, in heterogeneousnetworks like IoT. Many IoT providers rely on default or hard coded passwords that can create room for security breaches. The distribution of keys among the devices is an open challenge in IoT security, IETF's Smart Object Life cycle Architecture for Constrained Environments (SOLACE) started some work to overcome this problem. The problems associated with IoT security can be drastically reduced with security analytics, Data from multiple sources is collected and analyzed, to identify potential threats.

9. ABOUT AUTHORS

Mr. P. Ramesh, Working as Assistant Professor of E. C. E. Dept. in Holy Mary institute of Technology & Science, Hyderabad. He Graduated B. Tech. in Electronics & Communications Engineering from J. N. T. Univesity, Hyderabad, in the year 2005. He Post-Graduated M. Tech. In Embeded Systems from J. N. T. Univesity, Hyderabad. His Research interests are Embeded Systems, IoT and Image Processing.

Mr. M.Sri Venkat Rami Reddy, Working as Assistant Professor of E. C. E. Dept. in Holy Mary institute of Technology & Science, Hyderabad. He Graduated B. Tech. in Electronics & Communications Engineering from J. N. T. Univesity, Hyderabad, in the year 2004. He Post-Graduated M. Tech. In V. L. S. I. System Design from J. N. T. Univesity, Hyderabad, in the year 2012.

His Research interests are V. L. S. I. System Design, Image Processing, Cyber Security and Artificial Intelligence & Machine Learning (AI& ML). He is a Life Member of Indian Socity for Technical Education(LM-ISTE), New Delhi, India.

Dr.P.Bhaskara Reddy, the Director HITS is dynamic Professor of ECE, has 32-years of Industry, Teaching, Research and Administrative experience in Various Reputed Engineering Colleges & Industry. In 32-years of experience served various positions from Asst. Professor to Principal/Director
Research & Guidance: Published 2 Books 1. "Information Technology in Technical Education – Economic Development by "LAMBERT Academic Publishing" 2. Innovative Methods of Teaching Electronic Devices and Circuits by "Hi Tech Publisher" Published 9-Laboratory Manuals, 136-Research papers at National and

International Level journals/Conferences on Education, Electronics & Communications, I.T, Computer Networks, E-Commerce etc. Guided 8-Research Scholars for their Doctorates, about 50-M.Tech., M.C.A. and B.Tech projects and completed 4-DST Projects an amount of Rs.2.71 Crores.

Symposiums Conducted: 18-National Level Technical Symposiums on various topics in Electronics, Communications, and Computers etc.

Awards Received: 1). Bharath Jyothi Award in the year 2003 from IIFS, New Delhi, 2). Rastraprathiba Award in the year 2004 from ICSEP, New Delhi, 3). Knowledge Award from Alumni of SVHCE for the year 2001, 4). World Book of Records, London Certificate of Commitment into validate dedicated and relent-less commitment for promoting safety against the Covid-19:2021

10. REFERENCES

[1] S. U.-J. Lee, "An Effective Methodology with Automated Product Configuration for Software Product Line Development," Mathematical Problems in Engineering, vol. 2015, 2015.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[3] A. Abbas, I. F. Siddiqui, and S. U.-J. Lee, "Contextual Variability Management of IoT Application with XML-Based Feature Modelling," Journal of Theoretical & Applied Information Technology, vol. 95, 2017.

[4] A. Abbas, I. F. Siddiqui, S. U.-J. Lee, and A. K. Bashir, "Binary Pattern for Nested Cardinality Constraints for Software Product Line of IoT-Based Feature Models," IEEE Access, vol. 5, pp. 3971-3980, 2017.

[5] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 40, pp. 1-12, 2010.

[6] W.-Y. Chung, Y.-D. Lee, and S.-J. Jung, "A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO 2," in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE, 2008, pp. 1529-1532.

[7] R. Rákay, M. Višňovský, A. Galajdová, and D. Šimšík, "Testing properties of e-health system based on arduino," Journal of Automation and Control, vol. 3, pp. 122-126, 2015.S. U.-J. Lee, "An Effective Methodology with Automated Product Configuration for Software Product Line Development," Mathematical Problems in Engineering, vol. 2015, 2015.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[9] Gurram Dheeraj Reddy, Shashank Chutke, M.Sri Venkat Rami Reddy, Dr. D. Nageswara Rao Wireless Sensor Network Application for IoT basedHealthCare System

[10] A. Abbas, I. F. Siddiqui, and S. U.-J. Lee, "Contextual Variability Management of IoT Application with XML-Based Feature Modelling," Journal of Theoretical & Applied Information Technology, vol. 95, 2017.

[11] A. Abbas, I. F. Siddiqui, S. U.-J. Lee, and A. K. Bashir, "Binary Pattern for Nested Cardinality Constraints for Software Product Line of IoT-Based Feature Models," IEEE Access, vol. 5, pp. 3971-3980, 2017.

[12] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 40, pp. 1-12, 2010.

[13] W.-Y. Chung, Y.-D. Lee, and S.-J. Jung, "A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO 2," in Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE, 2008, pp. 1529-1532.

[14] R. Rákay, M. Višňovský, A. Galajdová, and D. Šimšík, "Testing properties of e-health system based on arduino," Journal of Automation and Control, vol. 3, pp. 122-126, 2015.

[15] D. Evans, "The Internet of things: How the next evolution of the Internet is changing everything,"CISCO, San Jose, CA, USA, White Paper, 2011.

[16] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[17] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. FIT*, 2012, pp. 257–260.

[18] J. Gubbi, R. Buyya, S.Marusic, and M. Palaniswami, "Internet of Things(IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[18]P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, "Survey of Internet of Things technologies for clinical environments," in *Proc. 27th Int. Conf. WAINA*, 2013, pp. 1349–1354.

[19] D. Yang, F. Liu, and Y. Liang, "A survey of the Internet of Things," in *Proc. 1st ICEBI*, 2010, pp. 358–366.

[20]A. Gluhak *et al.*, "A survey on facilities for experimental Internet ofThings research," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 58–67, Nov.2011.

[21] Z. Sheng *et al.*, "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," *IEEE Wireless Commun.*, vol. 20, no. 6, pp. 91–98, Dec. 2013.

[22] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, biggerdigital shadows, and biggest growth in the far east," *IDC iView: IDC Anal. Future*, vol. 2007, pp. 1–16, Dec. 2012.

[23] S. Taylor, "The next generation of the Internet revolutionizing the way we work, live, play, and learn," CISCO, San Francisco, CA, USA, CISCO Point of View, 2013.

[24] J. Manyika *et al.*, *Disruptive Technologies: Advances thatWill Transform Life, Business, and the Global Economy*. San Francisco, CA, USA: McKinsey Global Instit., 2013.

[25] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: Large scale measurement and characterization,"in *Proc. ACM SIGMETRICS Perform. Eval. Rev.*, 2012,pp. 65–76.