INTRODUCTORY CONCEPTS TO INTERNET OF THINGS (IOT)

Abstract

In this chapter we learn in detail about the History of IOT, Real time and virtual hardware components in IOT, Connectivity and Network considerations for IOT. Also We learn in detail about the logical design model of IOT. Different levels of IOT Models and its configuration and Communication protocols with examples are discussed. Internet of things describes the entity of physical objects which is embedded with sensors, actuators, etc. It is the connectivity between physical entity and virtual entity.

Keywords: hardware components, Internet of things, Communication, virtual entity

Authors

Ms. K. R. Priya Dharshini
Assistant Professor
Department of Electronics and Communication Engineering
Erode Sengunthar Engineering College
Erode, India.

Dr. R. Kalaivani
Professor
Department of Electronics and Communication Engineering
Erode Sengunthar Engineering College
Erode, India.

Ms. E. Sharmila
Assistant Professor
Department of Electronics and Communication Engineering
Erode Sengunthar Engineering College
Erode, India.

Ms. G. Amsaveni
Assistant Professor
Department of Electronics and Communication Engineering
Erode Sengunthar Engineering College
Erode, India.

IoT is the physical objects network which connects hardware, people and cloud services with an internet for building new architectures and business requirements. Improved VLSI Technology for Miniaturization and MEMS Technology for Sensing both leverage IoT. Widespread adoption of intellectual properties is accomplished through it.It is utilized to calculate economics. It serves descriptive, diagnostic, prescriptive, and predictive purposes in data analytics. Its connectivity is faster.The growth of cloud computing gives big data Scalability.

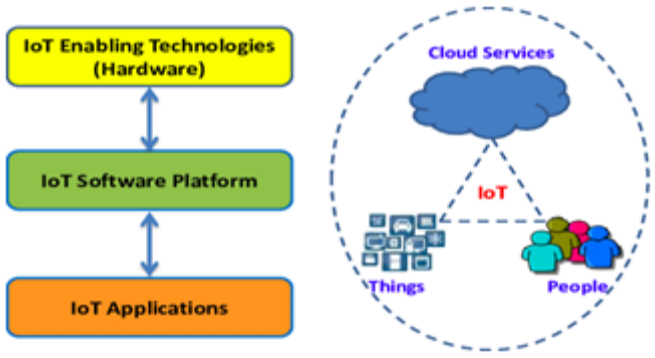

Figure 1: Internet of Things

I. HISTORY OF IOT

- First IoT Device: RFID (1940-1950), Major efforts in development for Tracking and identifying aircrafts in World War II (Friends or Foe)
- 1960: RFID was used for monitoring nuclear and other hazardous materials, RFID companies founded
- 1973: Mario W. Cadullo received the first US Patent for an active RFID tag.
- 1980: RFID research started, and it marks the beginning of transforming RFID into more widespread technology
- 1990: First UHF Reader was invented, RFID usage expanded to shipments, Walmart introduces their RFID program

Figure 2: RFID

- Progression in 1980's: Cloud and Server Space (Data moved to centralized server) Progression in 1990's: Machine to Machine interaction

- 1995: First cellular module built, First GPS network (version 1) complete
- 1998: Generates New IP addresses by adding IoT^ 128 to IPv6
- 1999: Kevin Ashton of MIT coins a new term

- Progression in 2000-2010: Fog oriented architectures (Central Server to Regional Server located closer to Data Server subnetwork)
- 2000: LG announces first smart fridge 2007 : First iPhone released
- 2008: First International Conference on IoT held. 2009 : Google started testing self driving cars.
- Progression in 2010-onwards: High Processing power and Edge computing 2013 : Google glass is released
- 2014: Amazon releases Echo (smart home market opens) 2015 : GM, Uber, Tesla are testing self driving cars
- 2017- : IoT continues to grow

II. REAL TIME AND VIRTUAL HARDWARE COMPONENTS IN IOT

Hardware components widely used in the IoT environment helps in sensing & actuating the real time parameters and also supports for future accessibility by providing cloud services.
Ex: Robots in Industries, Automation

Virtual components supports for storing, processing and accessing the information which is been sensed by the Hardware components. It is very relevant that the hardware and virtual components work in handed with each other and thus supports for building various applications.
Ex: Application software

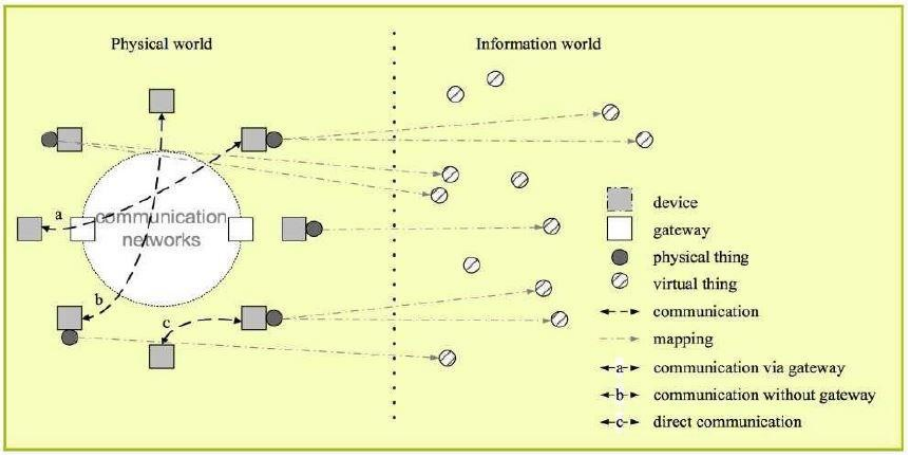

Figure 3: Physical and virtual world

III. CONNECTIVITY CONSIDERATIONS

Network architecture is determined by how IoT devices are connected to the outside world. Hardware specifications and pricing for IoT devices are determined by the communication method chosen. Meeting all the requirements of the consumer is found insufficient with a single paradigm of IoT network as it has increased number of IoT enabled devices. Network complexity includes device interference, network management, network heterogeneity, and internal network protocol standardization.

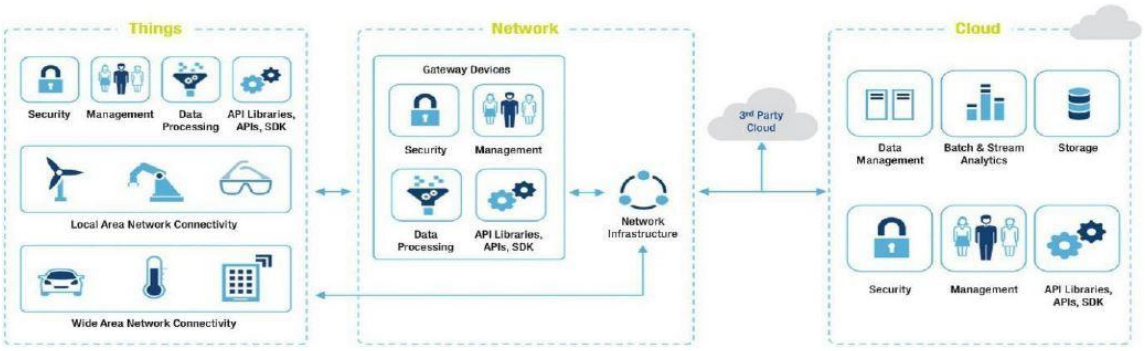

Figure 4: Connectivity Considerations

IV. NETWORK CONSIDERATIONS

1 **LAN:** Very short range communication with or without Internet providence.

2 **WAN:** Especially connected to internet with a combination of different networking segments

3 **Node:** It is a Point, may be hardware at times, has the ability to communicate with other devices in the network and also communicates with other nodal points.

4 **Gateway:** It helps in connecting local and wide area networks to more other local and Wide area networks. Also referred as Routers as it helps the packets by providing the ability to route it along the network.

5 **Proxy:** It builds a virtual application layer among various entities of the network.

V. LOGICAL DESIGN OF IOT BASED SYSTEMS

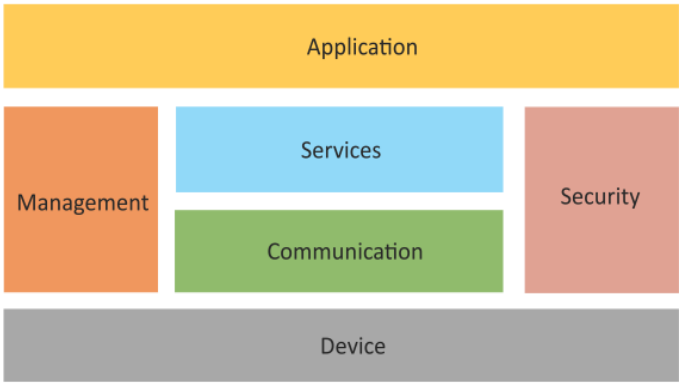

Figure 5: Logical Design of IoT

Without delving into the intricate details of the implementation, core representation of all the hardware components with its process is represented in the IoT logical layer deign. The major functional components for various process inclusive of identification, sensing and other functions are made as a part of IoT system design. Detailed report of all the components used are listed below.

1. **Device:** Identification, remote sensing and monitoring, actuation are all possible with an IoT device.

2. **Resources:** Software part of the IoT device referred as resources are used to access, process, and store sensor data as well as to control actuators.

3. **Controller Service:** It serves between the device and the web service providers. Controller transmits information between devices and gets instructions for managing the device from the application (through web services).

4. **Database:** The data sensed and measured by the IoT device is stored with the databases, which may be local or on the cloud.

5. **Web Service:** It helps in connecting various applications, components and databases with the service providers. Implementation of Web services can be done with WebSocket protocol (WebSocket service) or utilizing HTTP and the REST principles (REST service).

6. **Analysis Component:** This is in charge of processing the IoT data and producing information.

7. **Application:** It provides user boundary which manage and see various functions of the IoT scheme. It helps the user to verify the system status and the data to be processed.

VI. IOT LEVELS AND DEPLOYMENT

1. **IoT Level 1:** IoT Level 1 uses a single node to host applications and carry out the basic IoT functions. At the node, information are stored. The node is where the application runs. They are appropriate for modeling inexpensive solutions where the data is small and the processing demands are modest.

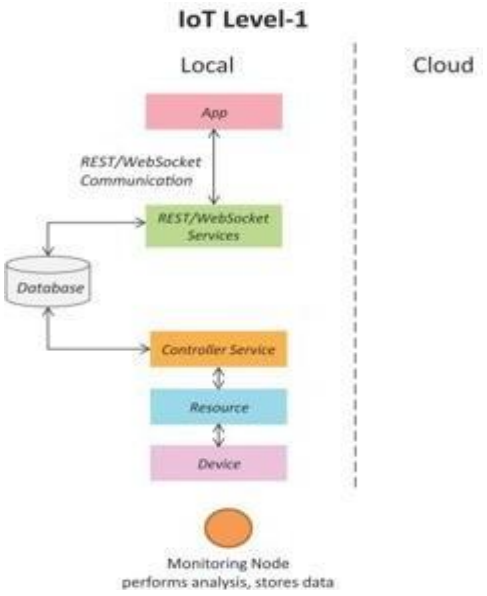

Figure 6: IoT Level 1

Application: Automated remote operated Homes

Figure 7: Smart Home

2. **IoT Level 2:** IoT Level 2 uses a core node for local analysis, sensing, and/or actuation. Cloud based access is provided for all information been collected by the sensors of the IoT system which work well as a complete model.

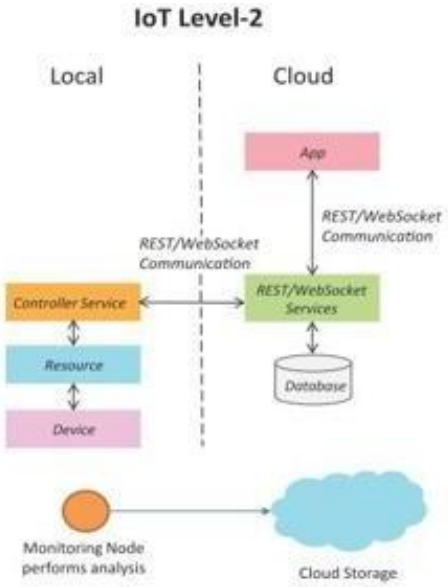

Figure 8: IoT Level 2

Application: Agriculture Automation

Figure 9: Smart Irrigation

3. **IoT Level 3:** IoT Level 3 has the providence for local analysis with sensing the basic real time analogy data with actuation and cloud-based services. They work well for modeling when there is a lot of data. However, analysis requirements require a lot of processing power.

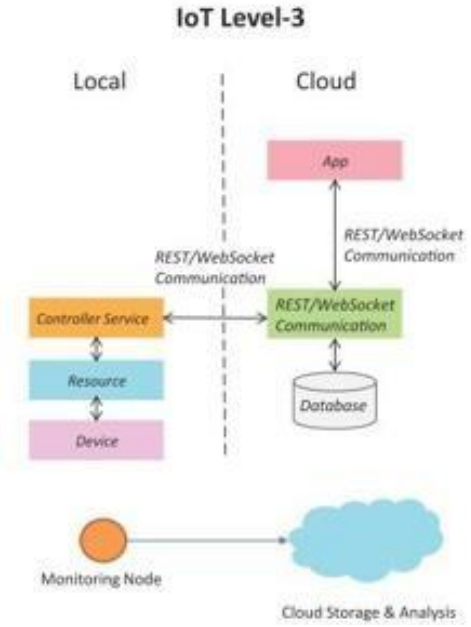

Figure 10: Level 3

Application: Tracking Package Delivery

Figure 11: Package Delivery

4. **IoT Level 4:** Multiple nodes at IoT Level 4 do local analysis with cloud based access. Components in the network with the ability to subscribe to and collect cloud-based data. They are appropriate in situations requiring several nodes, large amounts of data, and computationally demanding analysis needs.

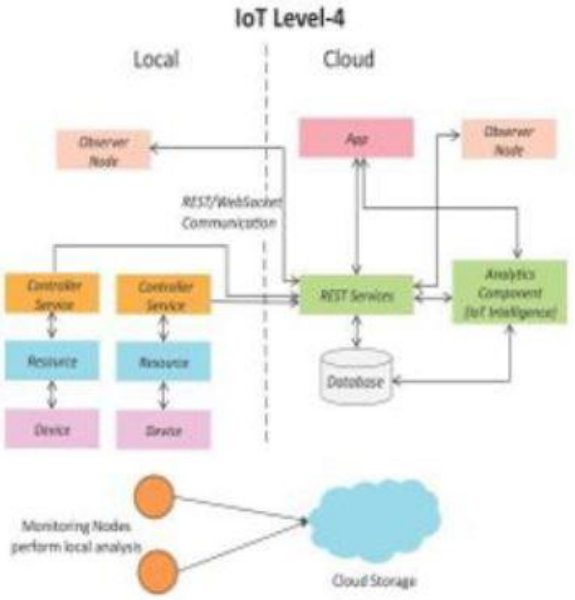

Figure 12: IoT Level 4

Application: Industrial Noise Reduction System

Figure 13: Noise Monitoring System

5. **IoT Level 5:** List of local nodes which is governed by the central coordinator node make up IoT Level 5.The end node performs actuation and sensing. The sensed data from each nodes are consolidated at the collector nodes and stored in the cloud with cloud based access. For wireless sensor network-based solutions with large amounts of data and computationally demanding analysis needs, Level 5 IoT systems are appropriate.

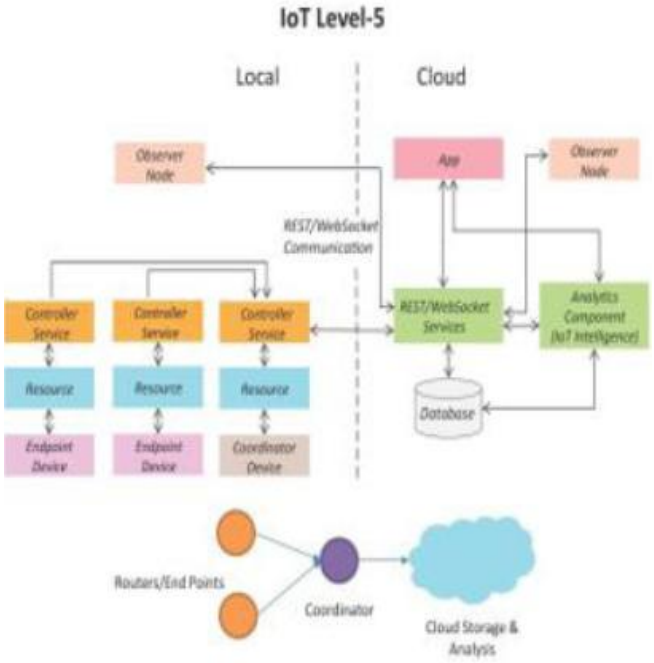

Figure 14: IoT Level 5

Application: Forest Fire Detection System

Figure 15: Forest Fire

6. **IoT Level 6:** Multiple autonomous end nodes at IoT Level 6 senses and store the data in the cloud based services. Data is analysed by the analytics component and stored in a cloud database.

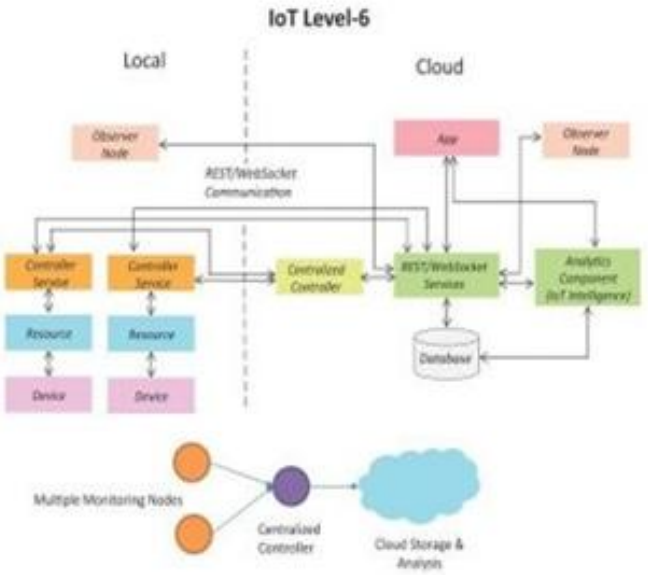

Figure 16: IoT Level 6

Application: Weather Monitoring Station

Figure 17: Weather Monitoring

VII. TRANSMIT AND RECEIVE BASED COMMUNICATION MODELS

In transmit -receive communication model, the nodes makes requests to the server. Response is given to the client when the server selects how to reply, acquires the information, gets the reserve representations, and makes it.

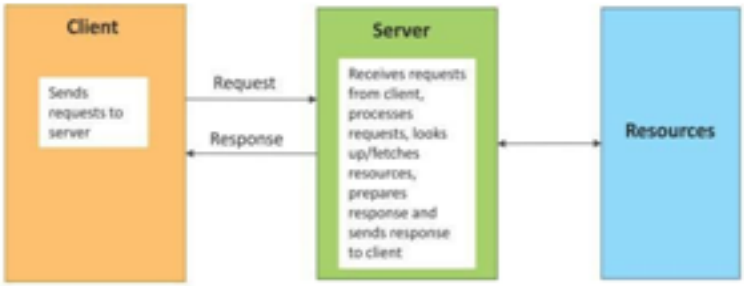

Figure 18: Request- Response Communication models

VIII. PUBLISH & SUBSCRIBE BASED COMMUNICATION MODELS

This communication model includes major publishers and consumers. The statistics are sourced from publishers. Publishers send information to the broker-managed topics. Customers contribute to the topics for the broker manages. Data for a topic is sent to all subscribers by the broker once it has been received from the publisher.

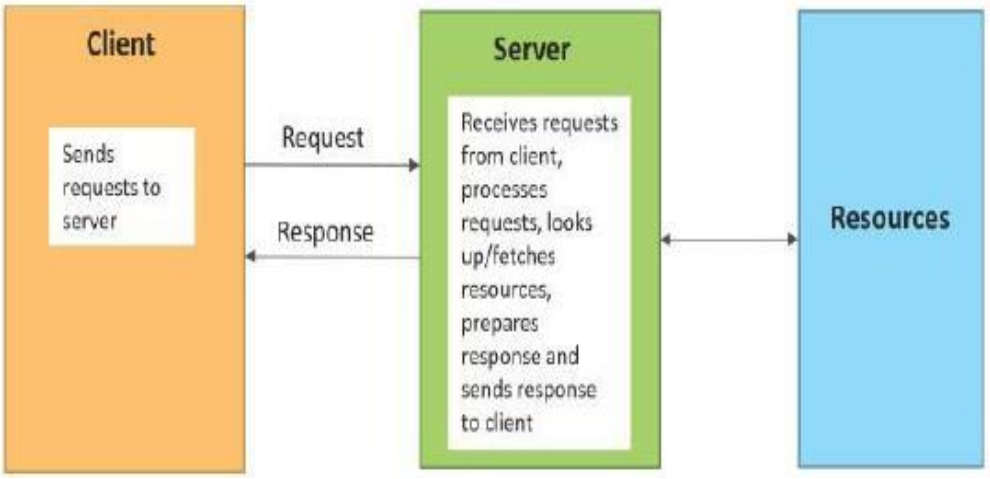

Figure 19: Publish Subscribe communication models

IX. COMMUNICATION MODELS: PUSH – PULL

This model handled the queuing concepts where the data is made to wait and pushed back to the queue based on the demands. The consumers do not need to be known by the producers. The data transfer among the sender and consumers has been differentiated with the help of queues. Additionally, buffer concept is handled in the queue that is beneficial when there is a discrepancy between the rates at which data is produced and consumed.

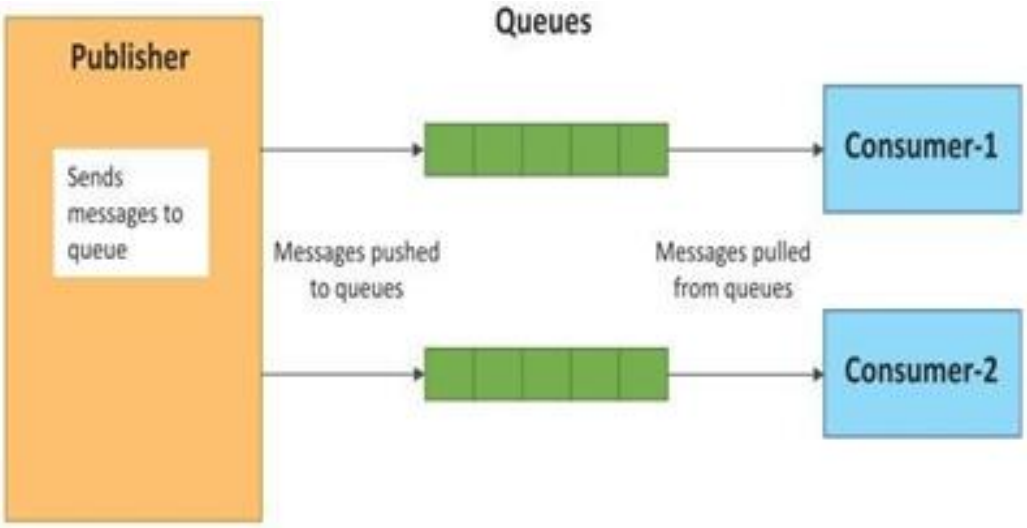

Figure 20: Push-Pull communication models

X. COMMUNICATION MODELS: EXCLUSIVE PAIR

Exclusive Pair is a persistent bidirectional connection between the client and the server. Once established, a connection does not need to be closed unless the client requests it. After establishing a connection, the client and server can communicate by sending messages.

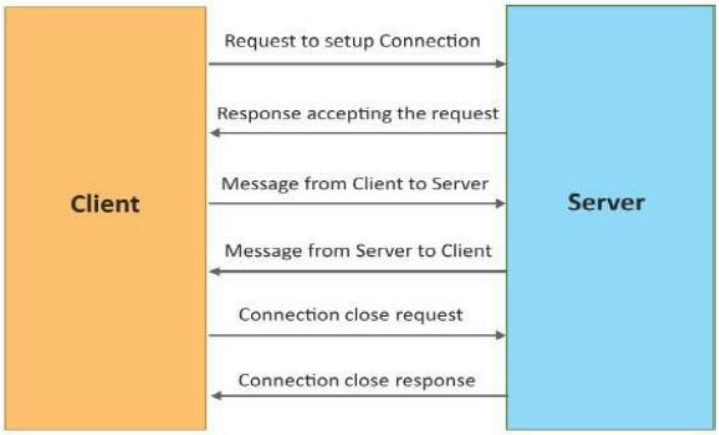

Figure 21: Exclusive pair

XI. REST BASED APIS

Representational State Transfer (REST) helps in building the system resources with a clear vision of addressing and communicating with them. REST architectural constraints apply to the components, connectors and data elements within a distributed hypermedia system.

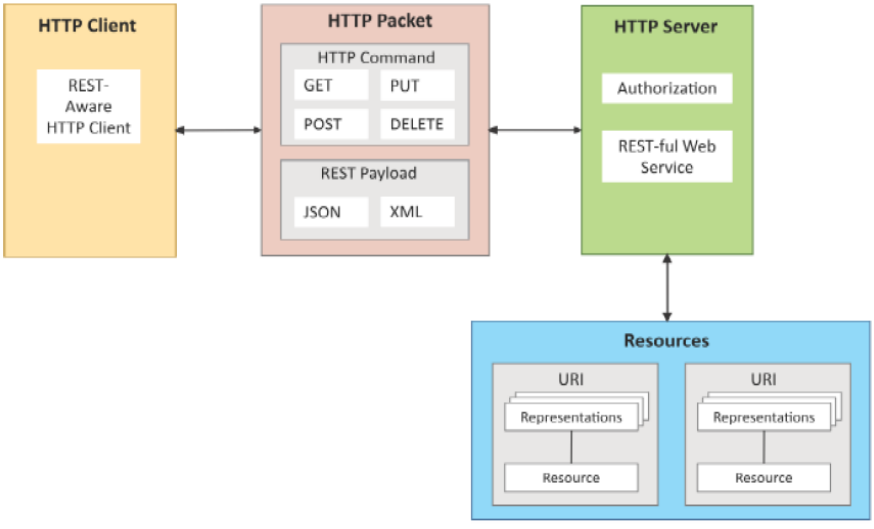

Figure 22: REST based API

XII. M2M FACILITIES

M2M refers to the networking of equipment for the exchange of data as well as remote monitoring and control. M2M services are solutions that concentrate on remote data

gathering and transfer from hardware components installed on fixed or mobile assets. Using M2M technology, smart mobile devices are utilized to communicate with and manage numerous equipment (devices).

Machines (or M2M nodes) that contain rooted hardware modules for various IoT functions make up an M2M area network. Zigbee, Bluetooth, 6LoWPAN, and IEEE.802.15.4 are employed as communication technologies in M2M. They employ non-IP or proprietary protocols. Access to the M2M area network is provided by the communication network. IP-based connectivity protocols are used in communication networks.

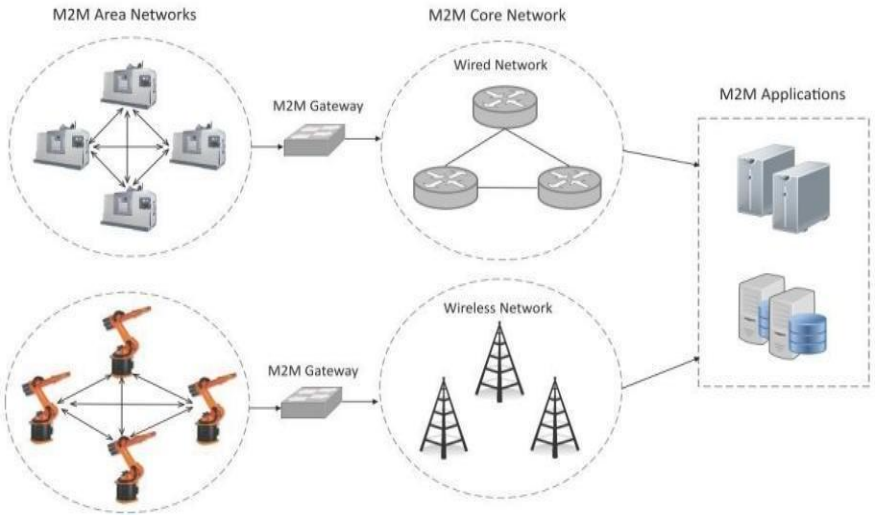

Figure 23: M2M

XIII. MACHINE TO MACHINE (M2M) GATEWAY

The M2M nodes within one network are unable to connect with nodes in an external network because of non-IP based protocols in M2M. M2M gateways are used to allow communication between distant M2M area networks.

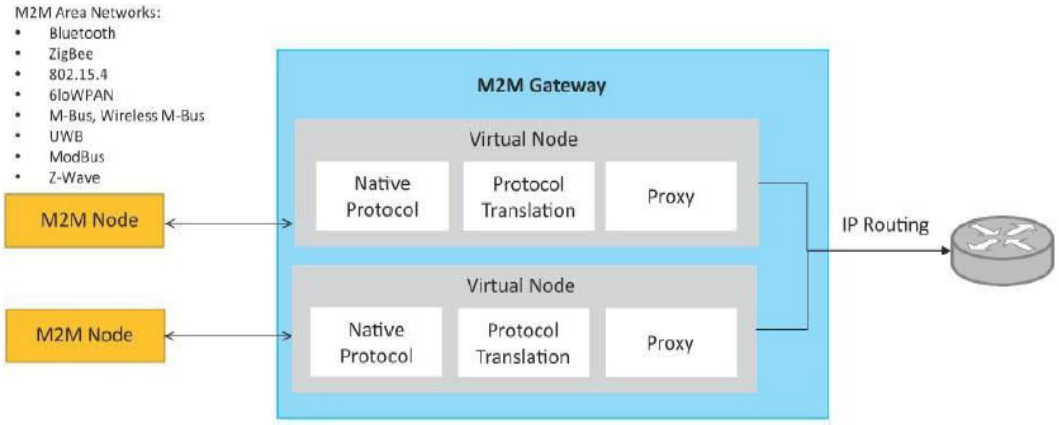

Figure 24: M2M Gateway

XIV. SOFTWARE DEFINED NETWORKING

SDN centralizes the network controller (which has data contained in it) and divides the control plane (network control) and data plane (network devices). Separation of control makes it possible to separate network services from the underlying parts and aids in treating the network as a logical entity. SDN controllers simplify configuration, maintenance, and provisioning while maintaining a uniform view of the network. Instead of specialized hardware, underlying infrastructure makes use of packet forwarding devices in traditional networks.

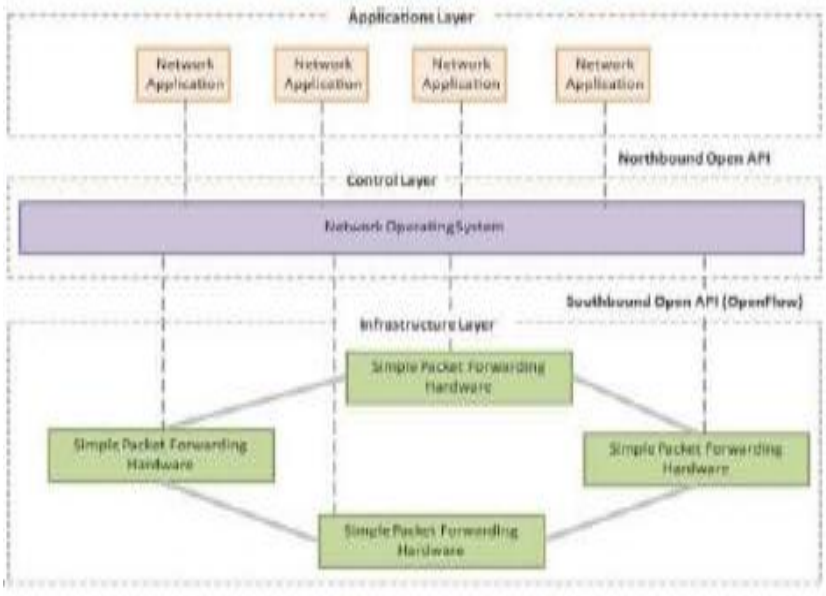

Figure 25: Software Defined Networking

For a specific process to occur, an abstract conception is building with a plane. Control plane helps to structure the forwarding pattern of packets and the Data plane defines the way by which the packet must be forwarded. For collecting, measuring and configuring the equipment's, management plane is used.

XV. SDN CONTROLLER

An application for enabling intelligent networking by managing flow control. They are built upon protocols like Open flow, which let servers instruct switches on where to send packets.

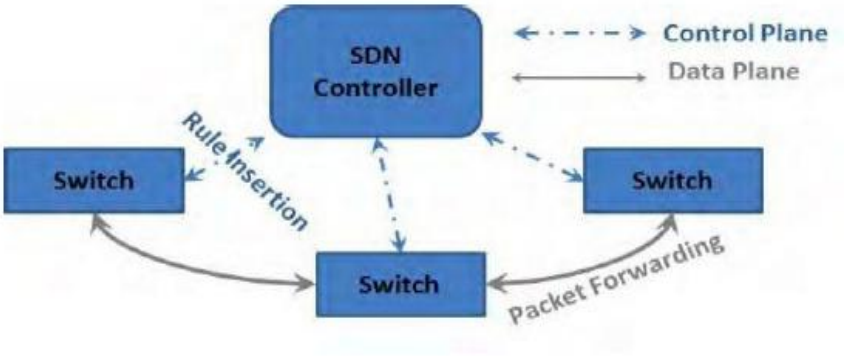

Figure 26: SDN Controller

XVI. NETWORK FUNCTION VIRTUALIZATION (NFV)

NFV aims at achieving the high volume standards of industrial based networks devices by promoting the heterogeneous network devices. It also supports with an infrastructure for SDN to run.

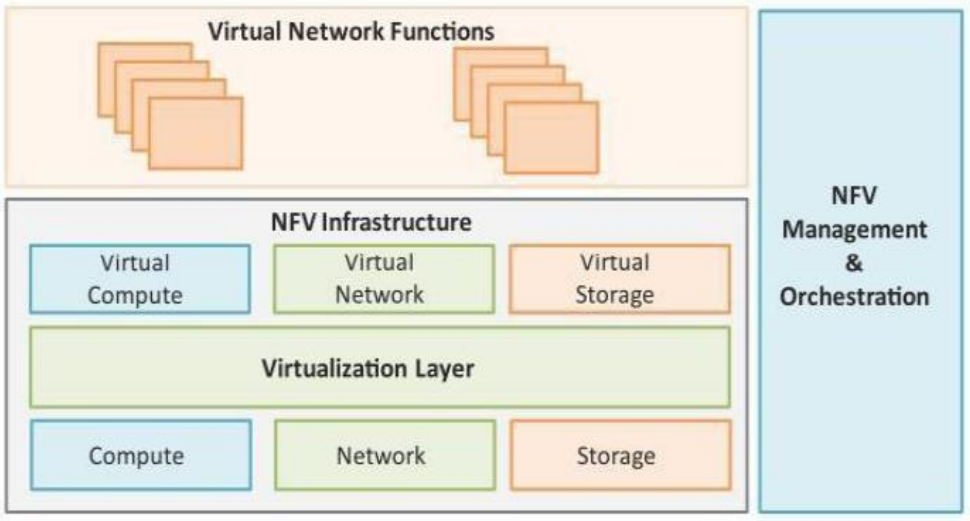

Figure 27: Network Function Virtualization

Virtualized compute, network, and storage resources has been encompassed with the NFV Infrastructure (NFVI). NFV Management and Orchestration focuses on all virtualization- specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs.

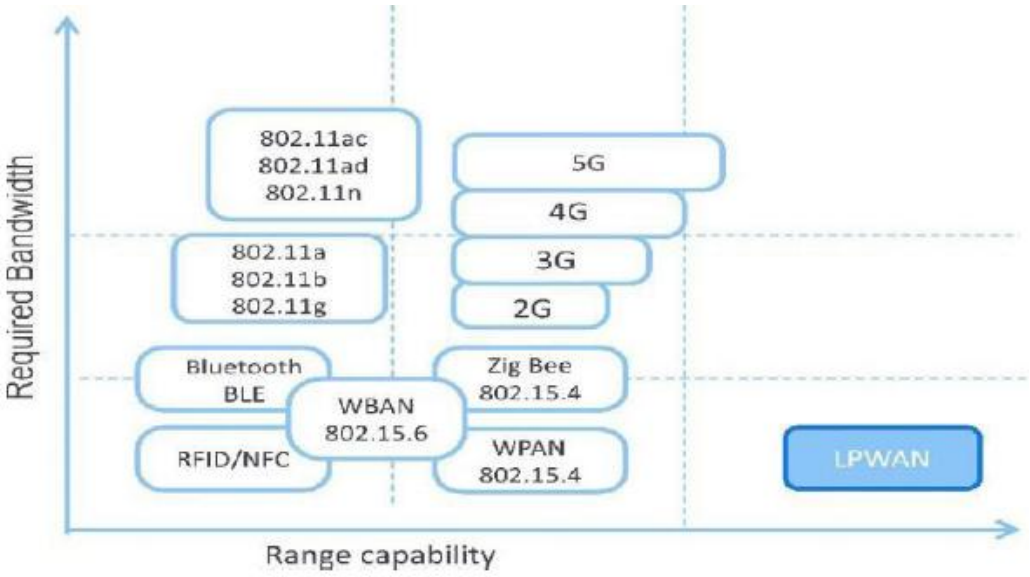

Figure 28: Bandwidth Requirements