Module 2

Architecture and Design Principles for IoT: Internet connectivity, Internet-based communication,IPv4, IPv6,6LoWPAN protocol, IP Addressing in the IoT, Application layer protocols: HTTP, HTTPS,FTP,TELNET and ports.

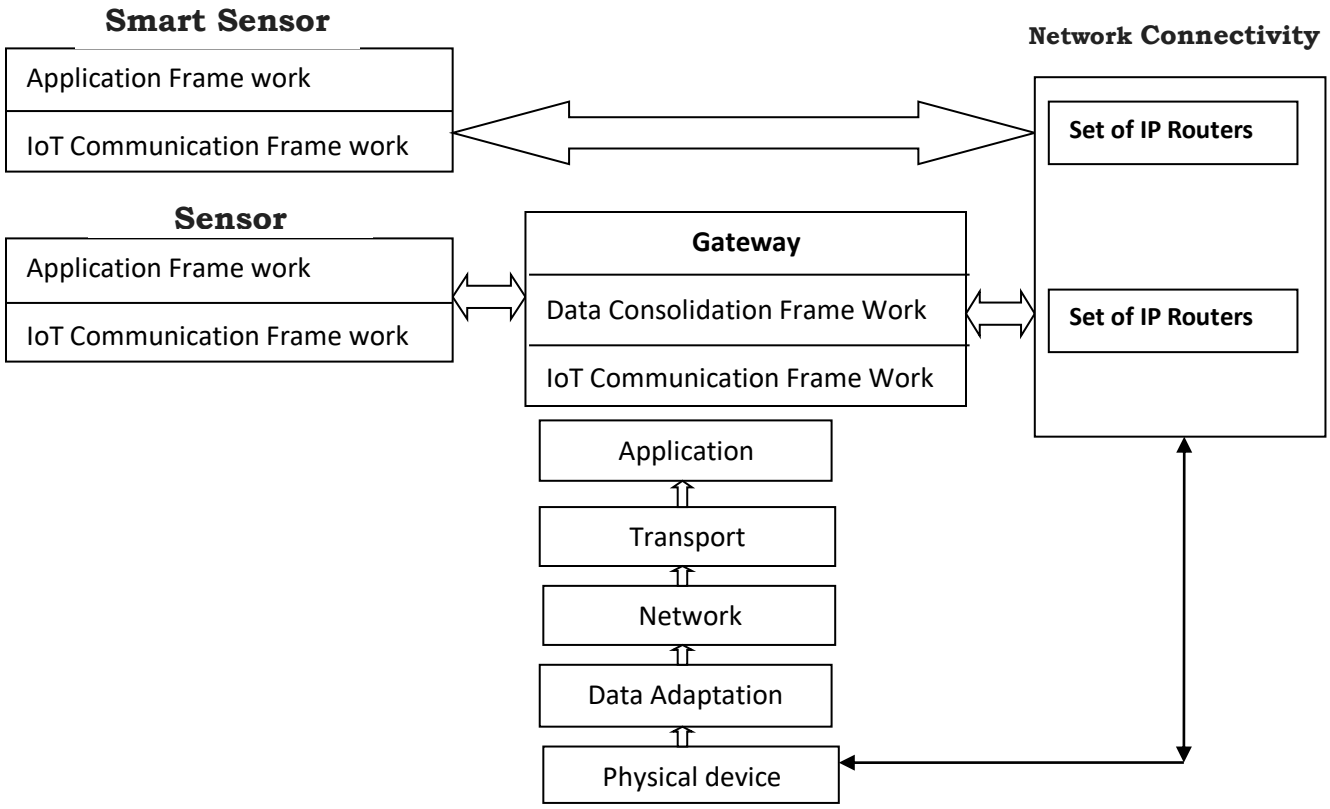
Data Collection, Storage and Computing using a Cloud Platform:
Introduction, Cloud computing paradigm for data collection, storage and computing, Cloud service models, IoT Cloud- based data collection, storage and computing services using Nimbits.

Internet is a global network with a set of connectivity protocols for:

- **Connected devices** gateway for sending the data frames of the devices or to the devices.
- The devices perform the **controlling** and **monitoring functions** using **messages**, **data stacks** and **commands** sent through the internet by the applications, services or business processes.

In this module we shall explore the Internet connectivity to the IoT/ M2M devices, Internet Base Communication, Internet Protocol & versions, IP Addressing in the IoT and the Application Layer Protocols.

Internet Connectivity:



- The diagram above shows the source end layer connected to the destination through a set of IP Routers.
- It also shows that a communication frame work uses an IP address and communicates with the IoT/M2M IoT application and services layer using TCP/IP suite of application protocols to a destination IP address.
- Internet connectivity is through a set of routers in a global network of routers that carry the data over the IP address of the host and the destination devices.

Internet Based Communication:

- When the data is transferred from IoT application layer to the Physical/device layer:
  - Each layer processes the data as per the protocols used for communication at that layer.
  - Each layer creates a fresh data stack by adding a new header to the data stack received from the upper layer.
  - Process continues until data communicate is complete over the network.
  - Internet based TCP/IP communications uses application layer, transport, internet and data link layers.
  - The above diagram shows the flow of the data through the modified OSI model when connected to internet.
  - The upper layers use only the header words, while the lower layers provide the trailing bits that can be used as error control bits.
  - Only four OSI layers i.e. 7, 4, 3 and 2 are specified at the TCP/IP suite for internet communication.
- **Physical layer**: The physical layer deals with **bit-level transmission** between different devices and supports electrical or mechanical interfaces connecting to the physical medium for synchronized communication.
- Few protocols that can be used are **Ethernet , Zigbee , Bluetooth**
- **Data link layer** : Data bits are **encoded, decoded** and **organized** in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN.
- **Trailing bits** can be used as error control bits and end of frame indicating bits. Frame sequence check(FRC) bits or cyclic redundancy check(CRC) bits can be part of trailing bits.
- The maximum size **PDU 1518B**.
- Few protocols that can be used are **MAC, PP, ARP,NDP.**

- **Network Layer** : Data is transferred in the form of **packets** via **logical network paths** in an ordered format controlled by the network layer.
- Logical connection **setup, data forwarding, routing** and **delivery error reporting** are the network layer's primary responsibilities.
- The maximum size **PDU 2^{16}B**.
- Few protocols that can be used are **IPV4, IPv6 and RPL.**
- **Transport Layer:** It provides **logical communication** between application processes running on different hosts within a layered architecture of protocols and other network components.
- The transport layer is also responsible for the management of **error correction**, providing **quality and reliability** to the end user.
- This layer enables the host to send and receive error corrected data, packets or messages over a network.
- It transmits segments using **TDP or UDP** protocol
- The maximum size PDU **2^{16}B**.
- **Application layer:** An application layer is an **abstraction layer** that specifies the shared communications protocols and interface methods used by hosts in a communications network
- Few protocols that can be used are **HTTP, FTP, SMTP, DNS and Telnet.**

Addressing in IoT:

- The IoT devices when connected to network/Internet can access resource/object from another device by addressing it.
- Addressing IoT devices is done by using IP addresses provided for every device connected in the network.
- **Static IP Address:** A static IP address is an IP address that was manually configured for a device, versus one that was assigned via a DHCP server.
- It's called *static* because it doesn't change.
- A static IP address is useful if you host a website from home, have a file server in your network, are using networked printers, are forwarding ports to a specific device, are running a print server, or if you use a remote access program.
- **Dynamic IP Address:** A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network.
- A dynamic IP address is an automatically configured IP address assigned by a DHCP server to every new network node.

- **DNS:** The Domain Name System (DNS) is the phonebook of the Internet.
- Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

[Ex: Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1:: c629:d7a2 (in IPv6)**]**

- **DHCP:** Dynamic Host Configuration Protocol (**DHCP**) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

- IP has 2 versions IPV4 and IPV6.

IPV4 Addressing:

- IP uses the packets called datagram A datagram consist of 2 parts:
  1) Payload 2) Header.

1) Payload

• Payload (or Data) is the main reason for creating a datagram.
• Payload is the packet coming from other protocols that use the service of IP.

2) Header

• Header contains information essential to routing and delivery.
• IP header contains following fields:

1) Version Number (VER)

- This field indicates version number used by the packet. Current version=4

2) Header Length (HLEN)

- This field specifies length of header.
- When a device receives a datagram, the device needs to know
  → when the header stops and
  → when the data starts.

3) Service Type

- This field specifies priority of packet based on delay, throughput, reliability & cost requirements.

4) Total Length

- This field specifies the total length of the datagram (header plus data).

- Maximum length=65535 bytes.

5) Identification, Flags, and Fragmentation Offset

- These 3 fields are used for fragmentation and reassembly of the datagram.
- Fragmentation occurs when the size of the datagram is larger than the MTU of the network.

6) Time-to-Live (TTL)

- This field is indicates amount of time, the packet is allowed to remain in the network.
- If TTL becomes 0 before packet reaches destination, the router
  → discards packet and
  → sends an error-message back to the source.

7) Protocol

- This field specifies upper-layer protocol that is to receive the packet at the destination-host.
- For example (Figure 19.3):
  For TCP, protocol = 6 For UDP, protocol = 17

8) Header Checksum

- This field is used to verify integrity of header only.
- If the verification process fails, packet is discarded.

9) Source and Destination Addresses

- These 2 fields contain the IP addresses of source and destination hosts.

10) Options

- This field allows the packet to request special features such as
  → Security level
  → Route to be taken by packet and
  → Timestamp at each router.
- This field can also be used for network testing and debugging.

11) Padding

- This field is used to make the header a multiple of 32-bit words.

IPV6 Addressing:

- An **IPv6 address** is a 128-bit alphanumeric string that identifies an endpoint device in the Internet Protocol Version 6 (**IPv6**) **addressing** scheme.
- In more precise terms, an **IPv6 address** is 128 bits long and is arranged in eight groups, each of which is 16 bits.

Sl. No.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Address format:

- Each block is then converted into Hexadecimal and separated by ':' symbol: 2001:0000:3238:DFE1:0063:0000:0000:FEFB
- IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

- IPV6 addresses are classified into three classes: **Unicast address, Anycast address, Multicast Address.**
- **Unicast Address:** In unicast mode of addressing, an IPv6 interface host is uniquely identified in a network segment.
- The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.
- When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.
- **Multicast:** The IPv6 multicast mode is same as that of IPv4.
- The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first.
- All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.
- **Anycast:**IPv6 has introduced a new type of addressing, which is called Anycast addressing.
- In this addressing mode, multiple interfaces hosts are assigned same Anycast IP address.

- When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message.
- With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

6LoWPAN

- In the Internet a packet passes through many different interconnected networks on its way from source to destination.
- Thus, considering the link layer technology of each traversed network, there is need of an ``IP-over-X'' specification (i.e., of an adaptation layer) to define how to transport IP packets.
- Following this need, in the process of shaping the IoT world, the IETF IPv6 over Low power WPAN (6LoWPAN) working group [6LoWPAN WG] started in 2007 to work on specifications for transmitting IPv6 over IEEE 802.15.4 networks [IEEE802.15.4].
- Typically, Low power WPANs are characterized by: small packet sizes, support for addresses with different lengths, low bandwidth, star and mesh topologies, battery supplied devices, low cost, large number of devices, unknown node positions, high unreliability, and long idle periods during when communications interfaces are turned off to save energy.
- Given the above features, it is clear that the adoption of IPv6 on top of a Low power WPAN is not straightforward, but poses strong requirements for the optimization of this adaptation layer.
- For instance, due to the IPv6 default minimum MTU size (i.e., 1280 bytes), a no-fragmented IPv6 packet would be too large to fit in an IEEE 802.15.4 frame.
- Moreover, the overhead due to the 40 bytes long IPv6 header would waste the scarce bandwidth available at the PHY layer.
- For these reasons, the 6LoWPAN working group has devoted huge efforts for defining an effective adaptation layer in [rfc4944,6lowpanhc].
- Further issues in the auto-configuration of IPv6 addresses, the compliance with the recommendation on supporting link-layer subnet broadcast in shared networks, the reduction of routing and management overhead, the adoption of lightweight application protocols (or novel data encoding techniques), and the support for security mechanisms (i.e., confidentiality and integrity protection, device bootstrapping, key establishment and management).

RPL – Routing Protocol for Lossy and Low Power Networks (LLNs)

- LLN: Low-Power and Lossy Network " LLN: Low-Power and Lossy Network.
- Typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4 or low-power Wi-Fi.
- There is a wide scope of application areas for LLNs, including industrial monitoring, building automation (heating, ventilation, and air conditioning (HVAC), lighting, access control, fire), connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking, and refrigeration." RFC 7228.
- RPL is typically a **Distance Vector (DV) protocol** and **Source Routing Protocol**.
- Routing issues are very challenging for 6LoWPAN, given the low-power and lossy radio-links, the battery supplied nodes, the multi-hop mesh topologies, and the frequent topology changes due to mobility.
- Successful solutions should take into account the specific application requirements, along with IPv6 behaviour and 6LoWPAN mechanisms.
- An effective solution was developed by the IETF "Routing over Low power and Lossy (ROLL) networks" working group [ROLL WG].
- For each of them, a Destination Oriented Directed Acyclic Graph (DODAG) is created by accounting for link costs, node attributes/status information, and an Objective Function, which maps the optimization requirements of the target scenario.
- Optimal routes between sink and all other nodes for both the collect and distribute data traffics. Redundant equivalent routes are kept for reliability in case of link or node failure.

RPL Instance and DODAGs

- An RPL Instance consists of multiple Destination Oriented Directed Acyclic Graphs (DODAGs). Traffic moves either up towards the DODAG root or down towards the DODAG leafs.
- **DODAG and RPL Instance Properties**

DODAG Properties

- Many-to-one communication: upwards
- One-to-many communication: downwards
- Point-to-point communication: upwards-downwards

RPL Instance Properties

- Instance Properties DODAGS are disjoint (no shared nodes)
- Link properties: (reliability, latency, . . .)
- Node properties: (powered or not, . . .)
- RPL Instance has an optimization objective
- Multiple RPL Instances with different optimization objectives can coexist

Route Construction and Forwarding Rules

Route Construction

- Up routes towards nodes of decreasing rank (parents)
- Down routes towards nodes of increasing rank Nodes inform parents of their presence and reach ability to descendants
- Source route for nodes that cannot maintain down routes
- All routes go upwards and/or downwards along a DODAG When going up, always forward to lower rank when possible, may forward to sibling if no lower rank exists When going down, forward based on down routes

RPL Control Messages

- DAG Information Object (DIO)
- A DIO carries information that allows a node to discover an RPL Instance, learn its configuration parameters and select DODAG parents
- DAG Information Solicitation (DIS)
- A DIS solicits a DODAG Information Object from an RPL node Destination Ad
- Destination Advertisement Object (DAO)
- A DAO propagates destination information upwards along the DODAG

DODAG Construction

- Construction Nodes periodically send link-local multicast DIO messages
- Stability or detection of routing inconsistencies influences the rate of DIO messages.
- Nodes listen for DIOs and use their information to join a new DODAG, or to maintain an existing DODAG Nodes may use a DIS message to solicit a DIO
- Based on information in the DIOs the node chooses parents that minimize path cost to the DODAG root

- RPL can serve different kinds of traffic and signalling information exchanged among nodes depends on the requirements of the considered data flows. In details, it supports: Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP), and Point-to-Point (P2P) traffic.

Application layer protocol HTTP,HTTPS and others

HTTP - Hyper Text Transfer Protocol

- The protocol primarily defines two different types of messages, the request from the client and the response from the server to the client.
- Each of these messages consists of two parts, the HTTP header and the HTTP body.
- The header contains metadata about the message body such as the character set used (encoding) and content type (for example, HTML document). The HTTP body contains the data that is to be displayed later at the client.
- The protocol primarily defines two different types of messages, the request from the client and the response from the server to the client.
- Each of these messages consists of two parts, the HTTP header and the HTTP body.
- The header contains metadata about the message body such as the character set used (encoding) and content type (for example, HTML document).
- The HTTP body contains the data that is to be displayed later at the client.
- The key functions of the HTTP protocol are the **request procedures**.
- They regulate the transmission of the actual data.
- Using HTTP GET, the most commonly used method, files can be downloaded from the server, for example.
- By sending a URI **(Uniform Resource Identifier)**,which is a single identifier, to the server, it will be able to identify what resource it has to return.
- From the user's perspective this is done by accessing a link or URL.
- The server or host will then return the requested document along with a status code to the web client.

HTTPS Objectives

- The purpose of an HTTPS connection is to protect the data being transmitted.
- An HTTP connection can be easily intercepted, allowing specific attacks on individuals.
- Data entered by a user in their browser window is often personal (account information, e-mail, credit card information, etc.) and must be protected from such access.

Use and relevance

- HTTPS is used for all websites where a user enters data.
- A major field of application is online banking.

- Anywhere where a password-secured account is used, an HTTPS connection would be sensible.
- This includes social network access, or e-mail and shopping accounts, where otherwise great personal harm could be inflicted with the illegal acquisition of personal data.
- Personal information could also be submitted without an account. If, for example, a flight or an entire vacation gets booked online, then applicable data must be communicated to the providers in a secure way.
- In their own interest, any internet user should pay attention to a secure connection at the right place and thus protect their privacy.
- Whether an HTTPS connection exists can be easily seen in the address bar. It will show "https" at the beginning and is even highlighted in many cases.
- A small lock icon is also displayed.

Disadvantages

- HTTPS has some disadvantages compared to HTTP connections. However, these are very few and should be accepted as a compromise for the security it provides.
- There are additional fees for certificates and increasing costs with increasing traffic. These can be particularly high.
- Especially for new and small websites these fees can become relatively high.
- With HTTPS connections, content cannot be cached. But the trend towards higher bandwidth counteracts this disadvantage.
- A weakness is also the poorer performance resulting from the use of SSL encryption. The server must perform a lot more computations, thus increasing the response time.
- Virtual hosts do not work with HTTPS.

Advantages

- Besides the obvious advantage of online privacy, there is also another big plus. Use of HTTPS does not require any additional software installation.
- This means it can be used without restrictions by anyone.
- The authentication with a certificate also inspires confidence in potential clients.

Differences between HTTP and HTTPS:

Data collection, storage and computing using a cloud platform

- All the data collected from the IoT/ M2M device can be stored in many ways like: 1) On SD Card 2) Local Disk Storage 3)In distributed DBMS 4)on the Web Server like Google Drive.
- Cloud is a new generation method of Saving remote data called through the IoT/M2M device.
- It also facilitates computing and analysis of data collected and stored.

Definition:

Cloud Computing is a shared pool of configurable computer system resources and higher level services that can be rapidly provisioned with minimal management effort, often over the Internet.

Cloud Computing Model/ Paradigm:

- Usually consists of:
  1) Data collection at the device web server
  2) Local Files
  3) Dedicated Data store center
  4) Internet Connected Data center
  5) Internet Connected server
  6) Cloud Infrastructure and Services

Why Cloud?

When you Host a website:

a) You need to buy a stack of servers- costly
b) Traffic requirement- data traffic on a website which is not constant throughout the day.
c) Monitoring and maintaining the server.
d) Amount of data generated is huge.
e) Usage of Internet has increased.
f) Storage of data from Internet is huge.

We need a space to store the data taken online.

Cloud – a Huge space to store the data/ access data online.

Cloud computing: is storing the data/ application on remote server
Processing data/ application from servers
Accessing data/ application online

Cloud computing-Service models:

- Anybody accessing the storage data online acquires the same as per the requirement/ application.

- Depending on the requirement there are 3 basic service models:
    1) IAAS- Infrastructure as a service
    2) PAAS- Platform as a service
    3) SAAS- Software as a service.

- **SAAS- Software as a Service:**
    - Use the service available- Consuming Service
      Ex: gmail.com
    - Cloud provider leases application or software which are owned by them to the client.
    - A method for delivering **software applications** over the Internet, on demand and typically on a subscription basis.
    - With this, cloud providers host and manage the software application and handle any maintenance, like software upgrades and security patching.
- **PAAS-Platform as a Service:**
    - A platform is provided where an application for a specific need can be created. Ex: Google App Engine.
    - The control of the underlying architecture including OS, Storage, Servers etc are still under the control of cloud provider.
    - It supply an **on-demand environment** for developing, testing, delivering and managing software applications.
    - Used to make developer's life easier to quickly create web or mobile apps, without worrying about setting up infrastructure.
- **IAAS- Infrastructure as a service:**
    - The basic category of cloud computing services.
    - It's like rent the **IT infrastructure** (servers & virtual machines, storage, networks, operating systems).
    - Create a system with all necessary services in just a few minutes, is never been so easy.

Cloud Deployment Models:

- Cloud computing is defined with several deployment models, each of which has specific trade-offs for agencies that are migrating services and operations to cloud-based environments.
- cloud computing outlines four cloud deployment models: private, community, public, and hybrid.
- **Private cloud:** A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- It may be owned, managed, and operated by the organization, a third party,

or some combination of them, and it may exist on or off premises.

- In general, federal agencies and departments opt for private clouds when sensitive or mission-critical information are involved.
- The private cloud allows for increased security, reliability, performance, and service. Yet, like other types of clouds, it maintains the ability to scale Quickly and only pay for what is used when provided by a third party, making it economical as well.
- **Community Cloud:** The Community Cloud is a type of cloud hosting in which the setup is mutually shared between many organizations that belong to a particular community, i.e. banks and trading firms.
- It is a multi-tenant setup that is shared among several organizations that belong to a specific group which has similar computing apprehensions.
- The community members generally share similar privacy, performance and security concerns.
- The main intention of these communities is to achieve their business-related objectives.
- A community cloud may be internally managed or it can be managed by a third-party provider.
- It can be hosted externally or internally. The cost is shared by the specific organizations within the community, hence, community cloud has cost saving capacity. A community cloud is appropriate for organizations and businesses that work on joint ventures, tenders or research that needs a centralized cloud computing ability for managing, building and implementing similar projects.
- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
- The community cloud deployment model is ideal and optimized for agencies or independent organizations that have shared concerns, and therefore need access to shared and mutual records and other types of stored information.
- Examples might include a community dedicated to compliance considerations or a community focused on security requirements policy.
- **Public Cloud:** The general public provisions the cloud infrastructure for open use.
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.
- It exists on the premises of the cloud provider.
- The public cloud deployment model have the unique advantage of being significantly more secure than accessing information via the Internet and tend to cost less than private clouds because services are more commoditized.

- One example of a public cloud deployment model based solution is the Treasury Department, which has moved its website Treasury.gov to a public cloud using Amazon's EC2 cloud service to host the site and its applications.
- The site includes social media attributes, including Facebook, YouTube and Twitter which allows for rapid and effective communication with constituents.
- **Hybrid Cloud:** The cloud infrastructure is a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
- Large portions of agencies that have already switched some processes over to cloud based computing solutions have utilized hybrid cloud options.
- NASA is one example of a federal agency who is utilizing the Hybrid Cloud Computing deployment model. Its Nebula open-source cloud computing project uses a private cloud for research and development as well as a public cloud to shared datasets with external partners and the public.

IoT Cloud Based Data Collection, Storage and Computing Services Using Nimbits:

- Nimbits is an open source IoT distributed cloud.
- It supports PAAS, deploys an instance of Nimbits server out the device nodes.
- It functions as an M2M data stores, data collector and logger with access to historical data.
- Its architecture is based on Google App Engine.
- Nimbits is an open source process data historian for Google App Engine.
- It provides data logging, calculations and M2M communication for sensors and devices such as Arduino.
- It can be used to record and share data points on the cloud and lets users record their changing numeric, text based, GPS, JSON or xml values into them.
- The API lets users access the public server to push and pull their data from.
- The API also provides access to a chart image service, which can generate PNG format images of user data.
- The API uses HTTP calls and responses are formatted in JSON or TXT.

Advanced Features:

- It is not pure Java and have provisions for in memory or encrypted databases.
- Uses security tokens.
- Breakthrough performance and data integrity.
- Alerts- uses Jabbar IDs for a single points, XMPP.