**Introduction to IoT**

**Define IOT:**

* “Connecting everyday things embedded with electronics, software, and sensors to internet enabling to collect and exchange data without human interaction called as the Internet of Things (IoT).”
* The term "Things" in the Internet of Things refers to anything and everything in day-to-day life which is accessed or connected through the internet
* IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data.

**Features of IOT+ Characteristics:**

1. **Connectivity**: Connectivity refers to establish a proper connection between all the things of IoT-to-IoT platform it may be server or cloud. After connecting the IoT devices, it needs a high speed messaging between the devices and cloud to enable reliable, secure and bi-directional communication.
2. **Analyzing**: After connecting all the relevant things, it comes to real-time analyzing the data collected and use them to build effective business intelligence. If we have a good insight into data gathered from all these things, then we call our system has a smart system.
3. **Self Configuring** – This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.
4. **Intelligence and Identity – The** extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.
5. **Integrating**: IoT integrating the various models to improve the user experience as well.
6. **Sensing**: The sensor devices used in IoT technologies detect and measure any change in the environment and report on their status.
7. **Safety –** There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical
8. **Endpoint Management**: It is important to be the endpoint management of all the IoT system otherwise, it makes the complete failure of the system.

**Challenges in IoT**

The Internet of Things (IoT) has fast grown to be a large part of how human beings live, communicate and do business. All across the world, web-enabled devices are turning our global rights into a greater switched-on area to live in.

*Challenges in IoT:*

* **Smart Sensors**

One the most important component of major IoT system is smart sensors. Industries, food processing, smart farming, retail, storage, healthcare and smart city applications are using smart sensors for data collection. These sensors have to be developed to support specific requirements and reliable real-time operation.

Design, development and successful implementation of wide range of smart sensors are often challenging task.

* **Lack of encryption** –

Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security challenges.

The result is an increase in attacks where hackers can easily manipulate the algorithms that were designed for protection.

* **Privacy Challenges:**

Personal privacy is a significant factor in any system which collect user information. IoT devices collect personal information and transmitted via wired or wireless network.

Personal information of the consumer must be protected by avoiding any chances of unauthorized access and hacking.

* **Connectivity Challenges:**

Majority of the IoT devices would be connected to a wireless network for its specific requirement and convenience. There are many wireless transmission technologies used IoT system like Wi-Fi, Bluetooth, LoRa WAN, SigFox, Zigbee etc… Each of this system has its own advantages and specifications.

* **Brute forcing and the risk of default passwords –**

Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute force.

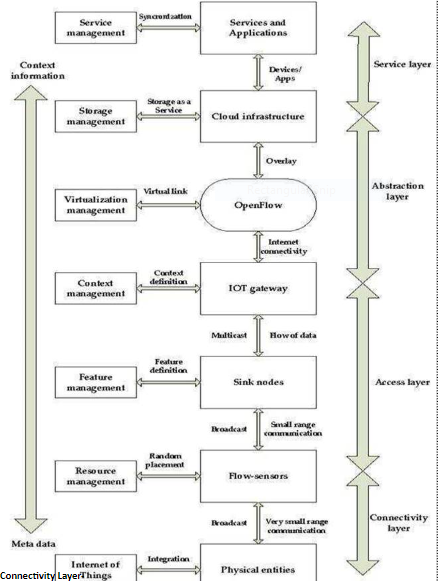
* **Increased cost and time to market** –
* Embedded systems are lightly constrained by cost.
* The need originates to drive better approaches when designing the IoT devices in order to handle the cost modelling or cost optimally with digital electronic components.
* Designers also need to solve the design time problem and bring the embedded device at the right time to the market.

**IOT conceptual view-**

The main tasks of this framework are to analyze and determine the smart activities of these intelligent devices through maintaining a dynamic interconnection among those devices. The proposed framework will help to standardize IoT infrastructure so that it can receive e-services based on context information leaving the current infrastructure unchanged. The active collaboration of these heterogeneous devices and protocols can lead to future ambient computing where the maximum utilization of cloud computing will be ensured.

This model is capable of logical division of physical devices placement, creation of virtual links among different domains, networks and collaborate among multiple application without any central coordination system. IaaS can afford standard functionalities to accommodate and provides access to cloud infrastructure. The service is generally offered by modern data centers maintained by giant companies and organization. It is categorized as virtualization of resources which permits a user to install and run application over virtualization layer and allows the system to be distributed, configurable and scalable.

· Total infrastructure system can be categorized into 4 layers to receive context supported e-services out of raw data from the Internet of Things. These 4 layers establish a generic framework that does not alter the current network infrastructure but create an interfacing among services and entities through network virtualization.

**1.  Connectivity Layer-**

This layer includes all the physical devices involved in the framework and the interconnection among them. Future internet largely depends on the unification of these common objects found everywhere near us and these should be distinctly identifiable and controllable.

This layer also involves assigning of low range networking devices like sensors, actuators, RFID tags etc and resource management checks the availability of physical resources of all the devices and networks involved in the underlying infrastructure. These devices contain very limited resources and resource management ensures the maximum utilization with little overhead. It also allows sharing and distribution of information among multiple networks or single network divided into multiple domains.

**2.  Access Layer-**

·         Context Data will be reached to internet via IoT Gateway as captured by short range devices in form of raw data. Access layer comprises topology definition, network initiation, creation of domains etc. This layer also includes connection setup, intra-inter domain communication, scheduling, packet transmissions between flow-sensors and IoT gateway. The simulation was run later in this paper for different scenario based on this layer. Feature management contains a feature filter which accepts only acceptable context data and redundant data are rejected. Large number of sensor maintains lots of features but only a small subset of features is useful generate a context data.

·         Feature filter helps to reduce irrelevant data transmission, increases the data transfer rate of useful data and reduce energy and CPU consumption too. Number of features can be different based on the application requirements and context data types.

**3.  Abstraction Layer-**

·         One of the most important characteristics of OpenFlow is to add virtual layers with the preset layers, leaving the established infrastructure unchanged. A virtual link can be created among different networks and a common platform can be developed for various communication systems. The system is fully a centralized system from physical layer viewpoint but a distribution of service (flow visor could be utilized) could be maintained. One central system can monitor, control all sorts of traffics. It can help to achieve better band-width, reliability, robust routing, etc. which will lead to a better Quality of Services (QoS).

·         In a multi-hopping scenario packets are transferred via some adjacent nodes. So, nodes near to access points bears too much load in comparison to distant nodes in a downstream scenario and inactivity of these important nodes may cause the network to be collapsed. Virtual presence of sensor nodes can solve the problem where we can create a virtual link between two sensor networks through access point negotiation. So, we can design a three a three layer platform, where common platform and virtualization layer are newly added with established infrastructure. Sensors need not to be worried about reach-ability or their placement even in harsh areas. Packet could be sent to any nodes even if it is sited on different networks.

**4.  Service Layer-**

·         Storage management bears the idea about all sorts of unfamiliar and/or important technologies and information which can turn the system scalable and efficient. It is not only responsible for storing data but also to provide security along with it. It also allows accessing data effectively; integrating data to enhance service intelligence, analysis based on the services required and most importantly increases the storage efficiency. Storage and management layer involves data storage & system supervision, software services and business management & operations. Though they are included in one layer, the business support system resides slightly above of cloud computing service whereas Open-Flow is placed below of it as presented to include virtualizations and monitor management.

·         Service management combines the required services with organizational solutions and thus new generation user service becomes simplified. These forthcoming services are necessitated to be co

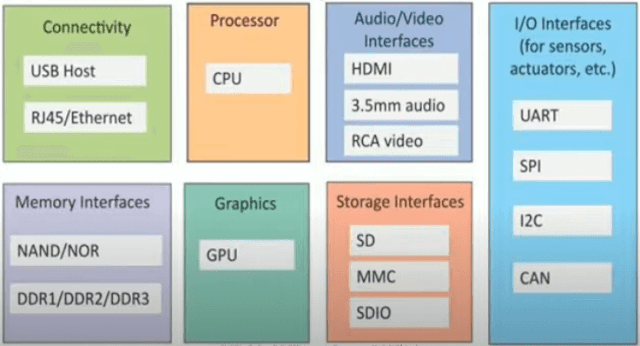
**Physical Design of Internet of Things (IOT):**

The physical design of an IoT system is referred to as the Things/Devices and protocols that are used to build an IoT system. All these things/Devices are called Node Devices and every device has a unique identity that performs remote sensing, actuating, and monitoring work. and the protocols that are used to establish communication between the Node devices and servers over the internet.

**Physical Design of IoT**

**Things/Devices**

Things/Devices are used to build a connection, process data, provide interfaces, provide storage, and provide graphics interfaces in an IoT system. All these generate data in a form that can be analyzed by an analytical system and program to perform operations and used to improve the system.



**Connectivity**: Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

**Processor**: A processor like a CPU and other units are used to process the data. these data are further used to improve the decision quality of an IoT system.

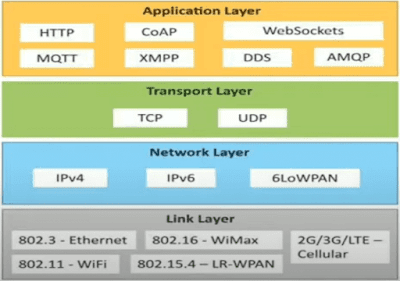
**Audio**/**Video** **Interfaces**: An interface like HDMI and RCA devices is used to record audio and videos in a system.

**Input/Output interface**: To give input and output signals to sensors, and actuators we use things like UART, SPI, CAN, **etc.**

**Storage Interfaces:** Things like SD, MMC, and SDIO are used to store the data generated from an IoT device.

Other things like DDR and GPU are used to control the activity of an IoT system.

**IoT Protocols**: These protocols are used to establish communication between a node device and a server over the internet. it helps to send commands to an IoT device and receive data from an IoT device over the internet. we use different types of protocols that are present on both the server and client side and these protocols are managed by network layers like application, transport, network, and link layer.



**Application Layer protocol** In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface. these protocols include HTTP, WebSocket, XMPP, MQTT, DDS, and AMQP protocols.

**HTTP** Hypertext transfer protocol is a protocol that presents an application layer for transmitting media documents. it is used to communicate between web browsers and servers. it makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between the two requests.

**WebSocket** This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. This protocol is commonly used by web browsers.

**MQTT** It is a machine-to-machine connectivity protocol that was designed as a publish/subscribe messaging transport. and it is used for remote locations where a small code footprint is required.

**Transport Layer** This layer is used to control the flow of data segments and handle error control. also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

**TCP** The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.

**UDP** a user datagram protocol is part of an internet protocol called the connectionless protocol. this protocol is not required to establish the connection to transfer data.

**Network Layer** This layer is used to send datagrams from the source network to the destination network. we use IPv4 and IPv6 protocols as host identification that transfers data in packets.

**IPv4** This is a protocol address that is a unique and numerical label assigned to each device connected to the network. an IP address performs two main functions host and location addressing. IPv4 is an IP address that is 32-bit long.

**IPv6** It is a successor of IPv4 that uses 128 bits for an IP address. it is developed by the IETF task force to deal with long-anticipated problems.

**Link Layer** Link-layer protocols are used to send data over the network’s physical layer. it also determines how the packets are coded and signaled by the devices.

**Ethernet**It is a set of technologies and protocols that are used primarily in LANs. it defines the physical layer and the medium access control for wired ethernet networks.

**WiFi** It is a set of LAN protocols and specifies the set of media access control and physical layer protocols for implementing wireless local area networks.

**logical design of an IoT**

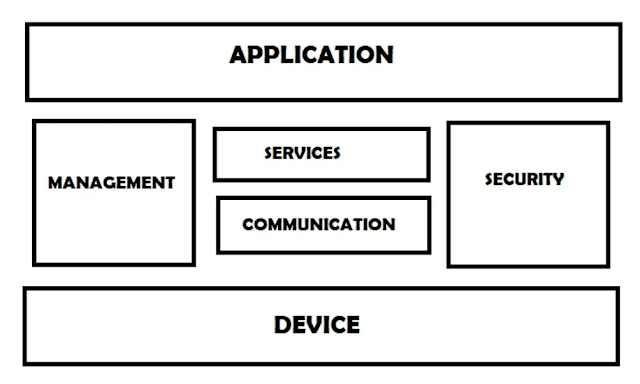
The logical design of an IoT system refers to an abstract representation of entities and processes without going into the low-level specifies of implementation. it uses Functional Blocks, Communication Models, and Communication APIs to implement a system.

Logical Design of the Internet of Things(IoT)

* IoT Functional Blocks
* IoT Communication Models
* IoT Communication APIs.

**IoT Functional blocks**

An IoT system consists of a number of functional blocks like Devices, services, communication, security, and application that provide the capability for sensing, actuation, identification, communication, and management.



These functional blocks consist of devices that provide monitoring control functions, handle communication between host and server, manage the transfer of data, secure the system using authentication and other functions, and interface to control and monitor various terms.

**Application** It is an interface that provides a control system that use by users to view the status and analyze of system.

**Management** This functional block provides various functions that are used to manage an IoT system.

**Services** This functional block provides some services like monitoring and controlling a device and publishing and deleting the data and restoring the system.

**Communication** This block handles the communication between the client and the cloud-based server and sends/receives the data using protocols.

**Security** This block is used to secure an IoT system using some functions like authorization, data security, authentication, 2-step verification, etc.

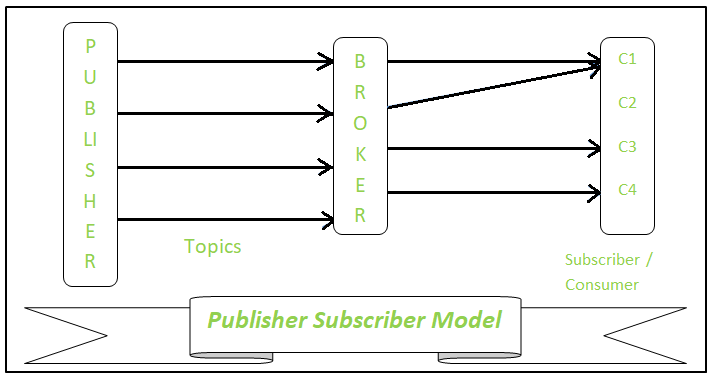
**Device** These devices are used to provide sensing and monitoring control functions that collect data from the outer environment.

**Communication Model:**

Communication model are architectural concepts describing how messages are transported in the network to accomplish certain tasks. Knowledge of these model are important to be able to correctly design and implement applications and scale networks of things accordingly, so that functional and performance requirements are met.

**1 Publisher-Subscriber Model:**

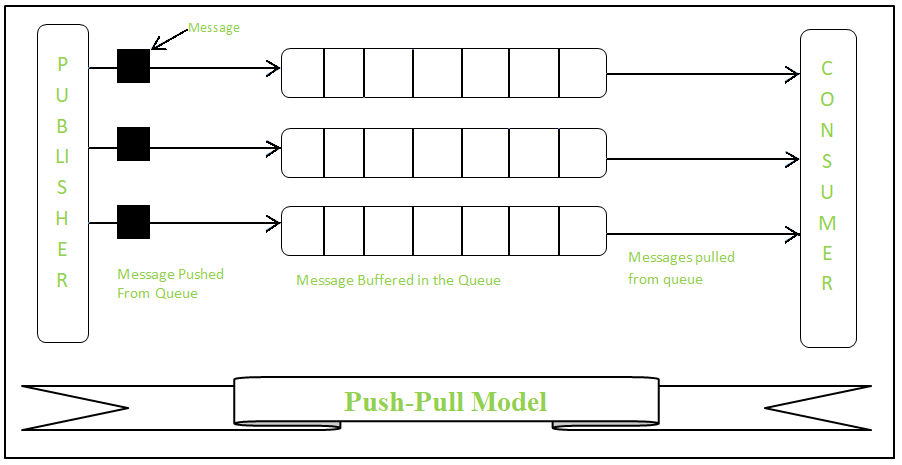
* This model comprises three entities: Publishers, Brokers, and Consumers.
* Publishers are the source of data. It sends the data to the topic which are managed by the broker. They are not aware of consumers.
* Consumers subscribe to the topics which are managed by the broker.
* Hence, Brokers responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.



**2. Push-Pull Model –**

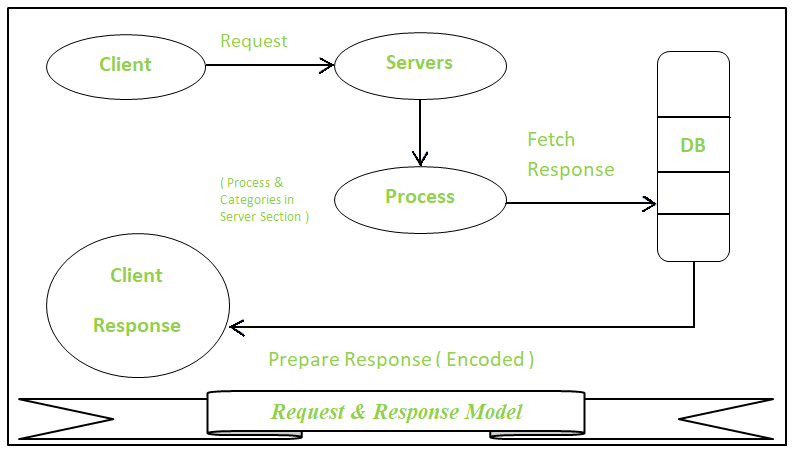
The push-pull model constitutes data publishers, data consumers, and data queues.

* Publishers and Consumers are not aware of each other.
* Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer.
* Queues help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.



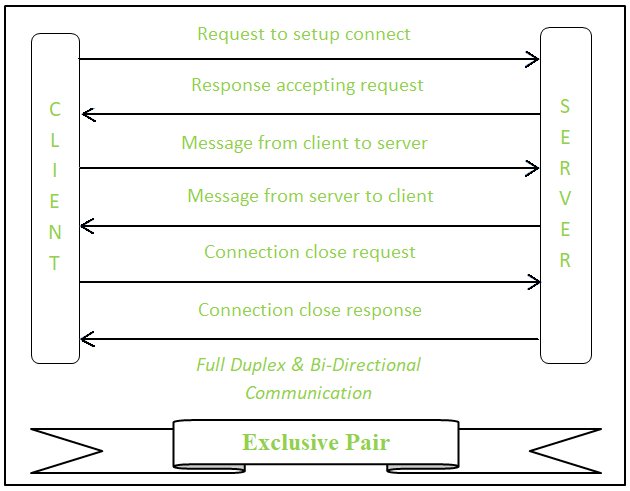
**3 Request & Response Model –**

* This model follows a client-server architecture.
* The client, when required, requests the information from the server. This request is usually in the encoded format.
* This model is stateless since the data between the requests is not retained and each request is independently handled.
* The server Categories the request, and fetches the data from the database and its resource representation. This data is converted to response and is transferred in an encoded format to the client. The client, in turn, receives the response.
* On the other hand — In Request-Response communication model client sends a request to the server and the server responds to the request. When the server receives the request it decides how to respond, fetches the data retrieves resources, and prepares the response, and sends it to the client.

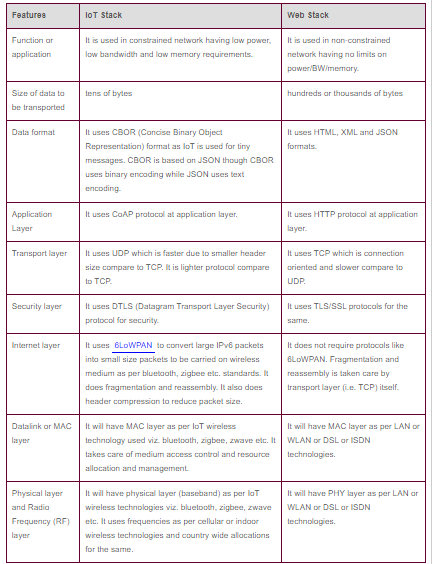
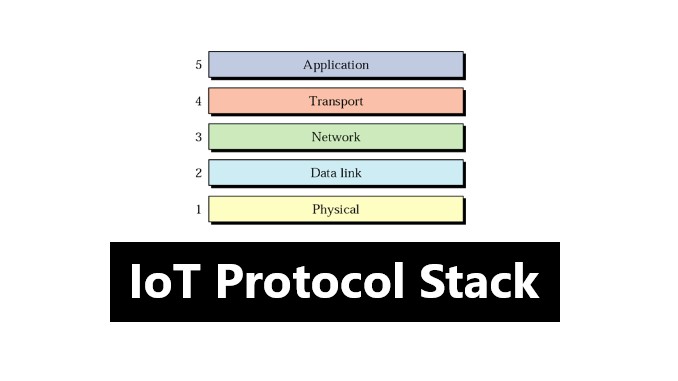


**4. Exclusive Pair –**

* Exclusive Pair is the bi-directional model, including full-duplex communication among client and server. The connection is constant and remains open till the client sends a request to close the connection.
* The Server has the record of all the connections which has been opened.
* This is a state-full connection model and the server is aware of all open connections.
* WebSocket based communication API is fully based on this model.



| **S.No.** | **IT Network** | **OT Network** |
| --- | --- | --- |
| 0. | Inforamation tecnology | Opratinal tec |
| 1. | IT network is business-oriented, which mainly deals with information rather machines. | OT network is industrial-oriented, which mainly interacts with machines. |
| 2. | Different types of data in IT networks include: Transactional, voice, video and bulky data. | Different types of data in OT networks include: monitoring, control and supervisory data. |
| 3. | IT network is limited to people which have certain privileges. | OT network is connected with the outside world whose access is not limited. |
| 4. | IT network works on transactional processing of data. | OT network works on real-time processing of data. |
| 5. | IT network may have automation risk. | OT network may have risk regarding the information. |
| 6. | IT network failure can result in loss of data. | OT network failure can result in end-of life. |
| 7. | IT has frequently changing environment. | OT has less changing environment as the requirements are not frequently changing. |
| 8. | IT network often requires network upgrades. | OT network requires network upgrades only during operational maintenance windows. |
| 9. | IT network failure can be business impacting, and it depends on industry. | If there is any disturbance in OT network, it will directly impact the overall business. |
| 10. | IT network ensures security by authenticating the devices and users to the network. | OT network controls physical access to any device. |



**Advantages of IoT**

Internet of things facilitates the several advantages in day-to-day life in the business sector. Some of its benefits are given below:

1. **Efficient resource utilization**: If we know the functionality and the way that how each device work we definitely increase the efficient resource utilization as well as monitor natural resources.
2. **Minimize human effort**: As the devices of IoT interact and communicate with each other and do lot of task for us, then they minimize the human effort.
3. **Save time**: As it reduces the human effort then it definitely saves out time. Time is the primary factor which can save through IoT platform.
4. **Enhance Data Collection:**
5. **Improve security**: Now, if we have a system that all these things are interconnected then we can make the system more secure and efficient.

**Disadvantages of IoT**

As the Internet of things facilitates a set of benefits, it also creates a significant set of challenges. Some of the IoT challenges are given below:

1. **Security**: As the IoT systems are interconnected and communicate over networks. The system offers little control despite any security measures, and it can be lead the various kinds of network attacks.
2. **Privacy**: Even without the active participation on the user, the IoT system provides substantial personal data in maximum detail.
3. **Complexity**: The designing, developing, and maintaining and enabling the large technology to IoT system is quite complicated.