IOT

“The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Physical object+Controller Sensor and Actuators+Internet = IOT

Works:

1. Sensors
2. Connectivity
3. Data Processing
4. Interface

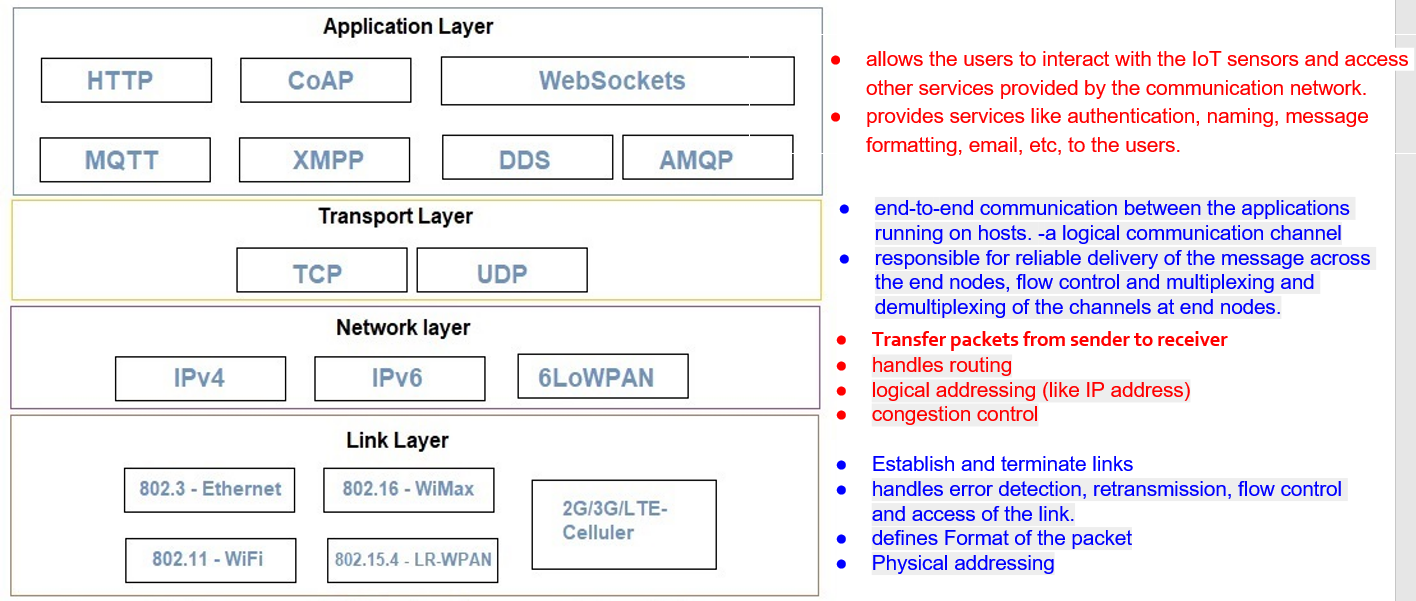
Benefits:

1. IoT platforms can help organizations reduce cost
2. IoT boosts productivity and profitability
3. IoT platforms unearths the new business opportunities
4. IoT promotes optimal asset utilization and tracking
5. IoT improves security levels and minimizes vulnerabilities

Characteristics:

1. Unique Identity
2. Dynamic in Nature and self adapting
3. Self configuring
4. Interoperability
5. Autonomous operation
6. Data Driven
7. Context awareness
8. Ubiquity
9. Scalability

Physical design



Ethernet: Ethernet is a widely used wired networking technology that utilizes twisted-pair or fiber-optic cables to connect devices in local area networks (LANs). It provides high-speed, reliable data transmission, making it a preferred choice for connecting computers, servers, and other networked devices in businesses and homes.

Wi-Fi (Wireless Fidelity): Wi-Fi is a wireless networking technology that enables devices to connect to the internet and local networks without physical cables. It is commonly used in homes, offices, and public spaces, offering convenience and mobility. Wi-Fi operates over radio frequencies and has evolved over the years to provide increasingly faster and more secure wireless connections.

WiMAX (Worldwide Interoperability for Microwave Access): WiMAX is a wireless communication technology that provides broadband wireless access over a broader area, known as a metropolitan area network (MAN). It offers high data transfer rates and is often used to extend internet access to areas where traditional wired infrastructure is less practical.

LRWPAN (Low-Rate Wireless Personal Area Network): LRWPAN is a wireless communication standard designed for low-power, short-range connectivity between devices, such as sensors and actuators. It is commonly used in applications like home automation, industrial control, and environmental monitoring, where energy efficiency and long battery life are crucial.

2G/3G/5G Cellular: These are generations of cellular network technologies used for mobile communication. 2G (2nd Generation) introduced digital voice and text messaging, 3G (3rd Generation) added data services, and 5G (5th Generation) is the latest standard, offering significantly faster data speeds, lower latency, and support for a wide range of IoT devices. Cellular networks like 5G are the backbone of modern mobile communication, supporting smartphones, IoT devices, and more.

—----------------------------------------------------------------------

IPv4 (Internet Protocol version 4): IPv4 is the fourth version of the Internet Protocol and is the most widely used protocol for routing data on the internet. It uses a 32-bit addressing scheme, allowing for approximately 4.3 billion unique IP addresses. However, due to the rapid growth of the internet, IPv4 addresses are becoming exhausted, leading to the adoption of IPv6. IPv4 is still in use and will coexist with IPv6 for the foreseeable future.

IPv6 (Internet Protocol version 6): IPv6 is the successor to IPv4 and was introduced to address the limited number of available IPv4 addresses. It uses a 128-bit addressing scheme, providing a vastly larger number of unique IP addresses, which is essential for the continued growth of the internet and the proliferation of IoT devices. IPv6 offers improved security, network auto-configuration, and better support for mobile devices.

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks): 6LoWPAN is an adaptation layer that allows IPv6 to be used over low-power, low-rate wireless personal area networks. It is designed to enable IPv6 communication for resource-constrained devices such as sensors and embedded systems. 6LoWPAN optimizes the use of IPv6 in these networks, making it suitable for applications like smart homes, industrial automation, and environmental monitoring, where energy efficiency and small data payloads are important.

—------------------------------

TCP (Transmission Control Protocol): TCP is one of the main protocols in the Internet Protocol (IP) suite and is responsible for establishing a reliable, connection-oriented data transfer between devices on a network. It ensures that data is transmitted in a structured and orderly manner, and it provides error checking, flow control, and congestion control. TCP is commonly used for applications that require guaranteed delivery and error correction, such as web browsing, email, file transfers, and remote access protocols like SSH.

UDP (User Datagram Protocol): UDP is another protocol in the Internet Protocol (IP) suite and is an alternative to TCP. Unlike TCP, UDP is a connectionless and unreliable protocol. It does not establish a connection before sending data and does not guarantee delivery, order, or error checking. UDP is favored for applications where real-time data transmission is more critical than reliability, such as video streaming, online gaming, VoIP (Voice over Internet Protocol), and DNS (Domain Name System) queries, as it reduces the communication overhead and latency compared to TCP.

—----------------

HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web, allowing web browsers to request and display web pages. It follows a client-server model, where web clients make requests to web servers for resources.

CoAP (Constrained Application Protocol): CoAP is a lightweight, UDP-based protocol designed for resource-constrained devices in IoT applications. It enables efficient data exchange and is often used for machine-to-machine communication.

Websockets: Websockets is a communication protocol that provides full-duplex, bidirectional communication between a client and a server over a single, long-lived connection. It's commonly used for real-time web applications like chat and online gaming.

XMPP (Extensible Messaging and Presence Protocol): XMPP is an open communication protocol for instant messaging and presence information. It supports real-time messaging, presence updates, and other collaborative features, making it popular for chat applications.

MQTT (Message Queuing Telemetry Transport): MQTT is a lightweight messaging protocol designed for low-bandwidth, high-latency, or unreliable networks. It's often used in IoT and M2M communication to efficiently exchange messages between devices.

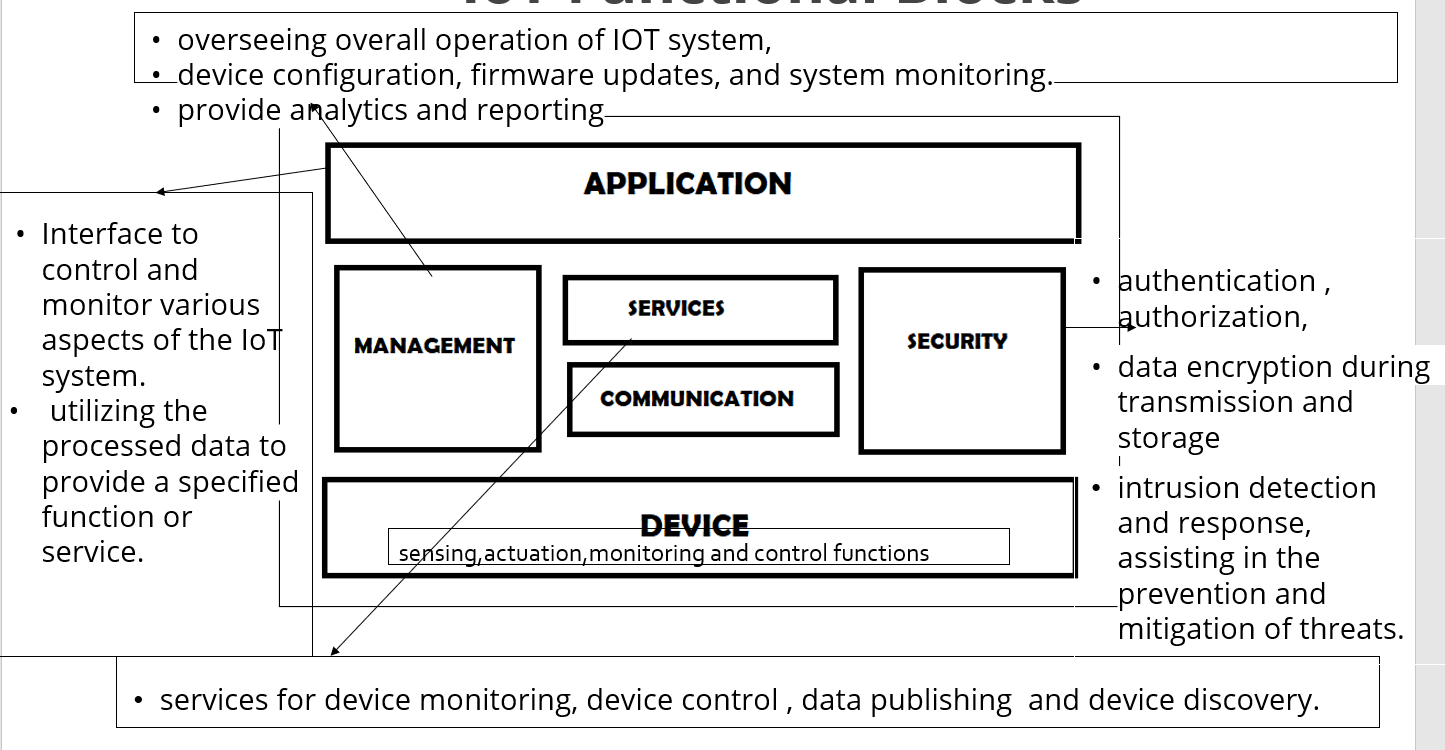
DDS (Data Distribution Service): DDS is a middleware protocol used in real-time and mission-critical systems. It facilitates the efficient and reliable exchange of data between distributed applications, commonly used in industries like aerospace and healthcare.

AMQP (Advanced Message Queuing Protocol): AMQP is a protocol for message-oriented middleware that supports message queuing, routing, and reliability. It's used in various applications, including financial services, healthcare, and enterprise messaging systems.

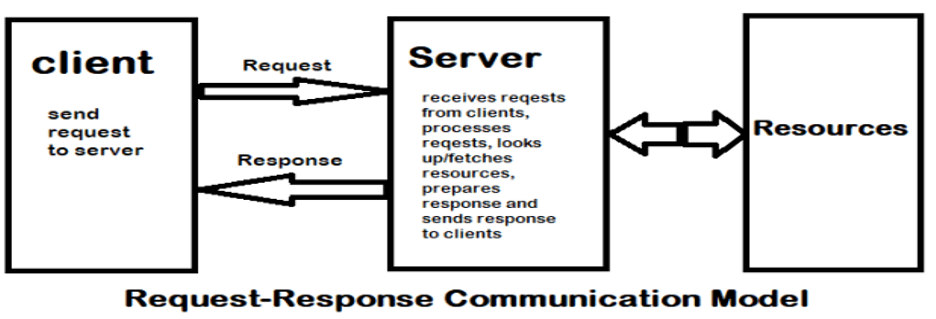
LOGICAL DESIGN

Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation.

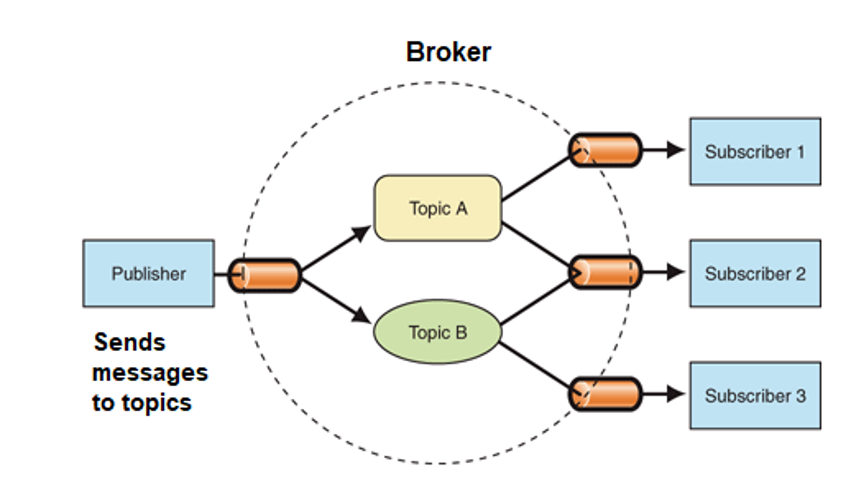
1. Functional Block



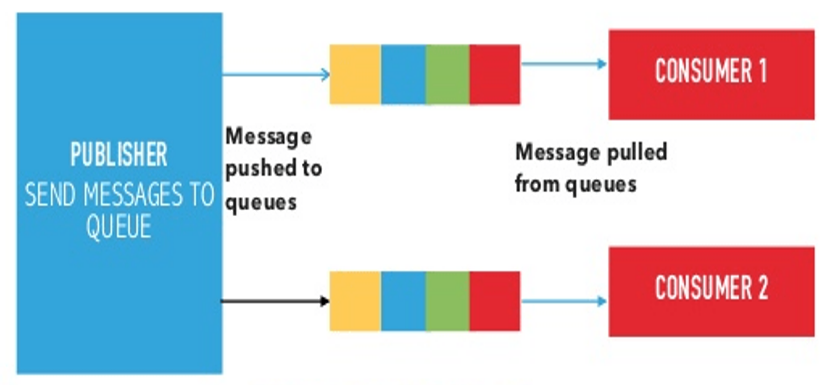
1. Communication block
2. Request-Response Model



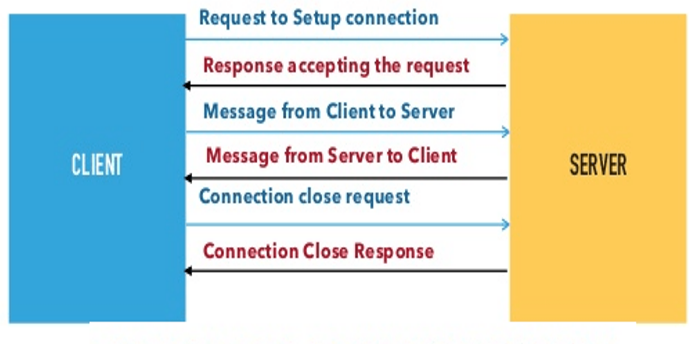
1. Publish-Subscribe Model



1. Push-Pull Model



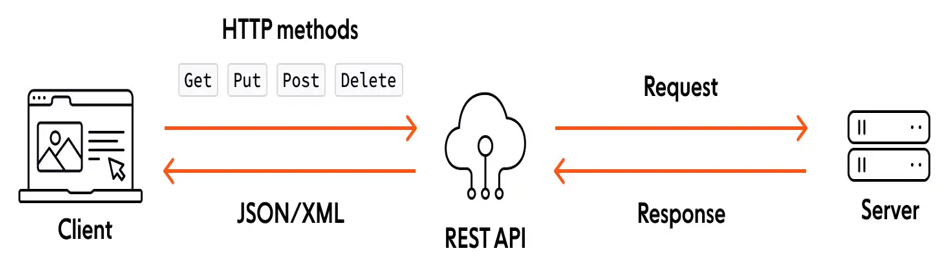
1. Exclusive Pair Model



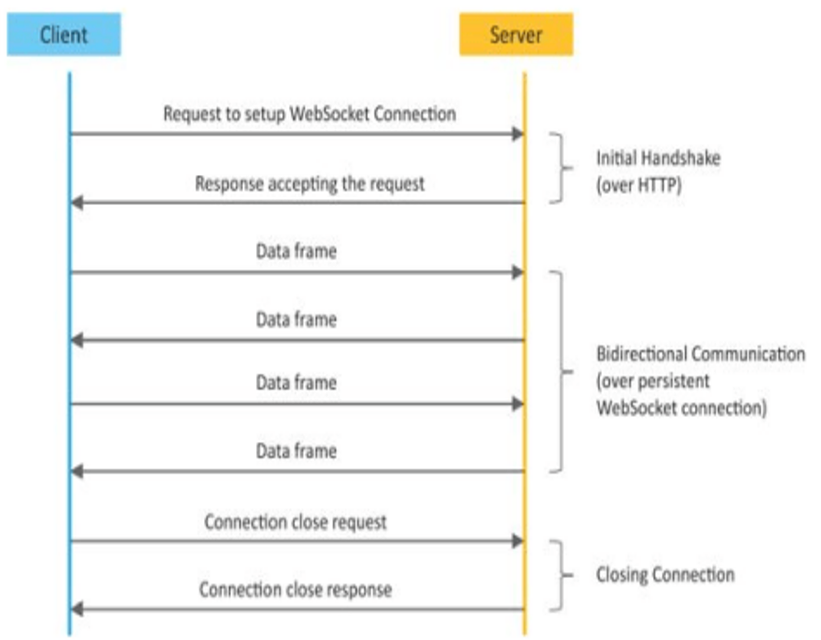
1. IOT Communication APIs
2. REST based

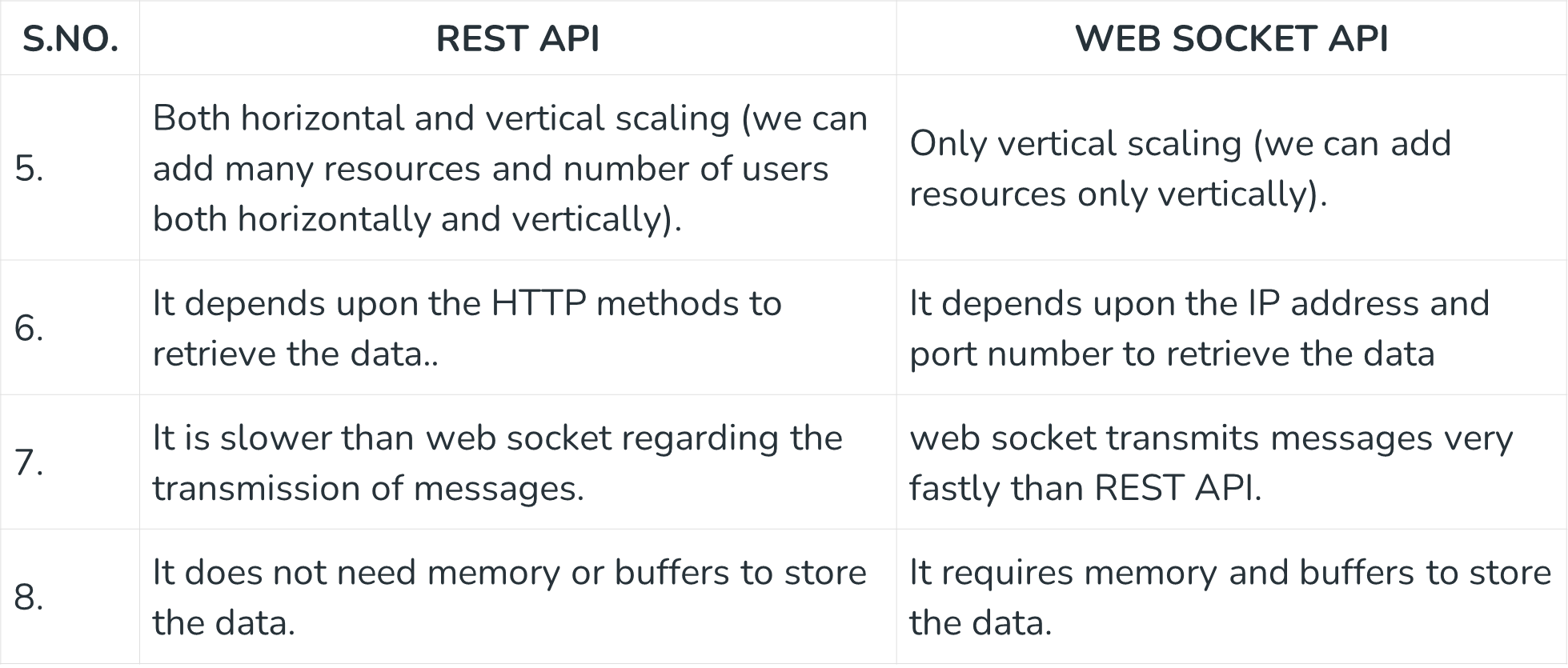
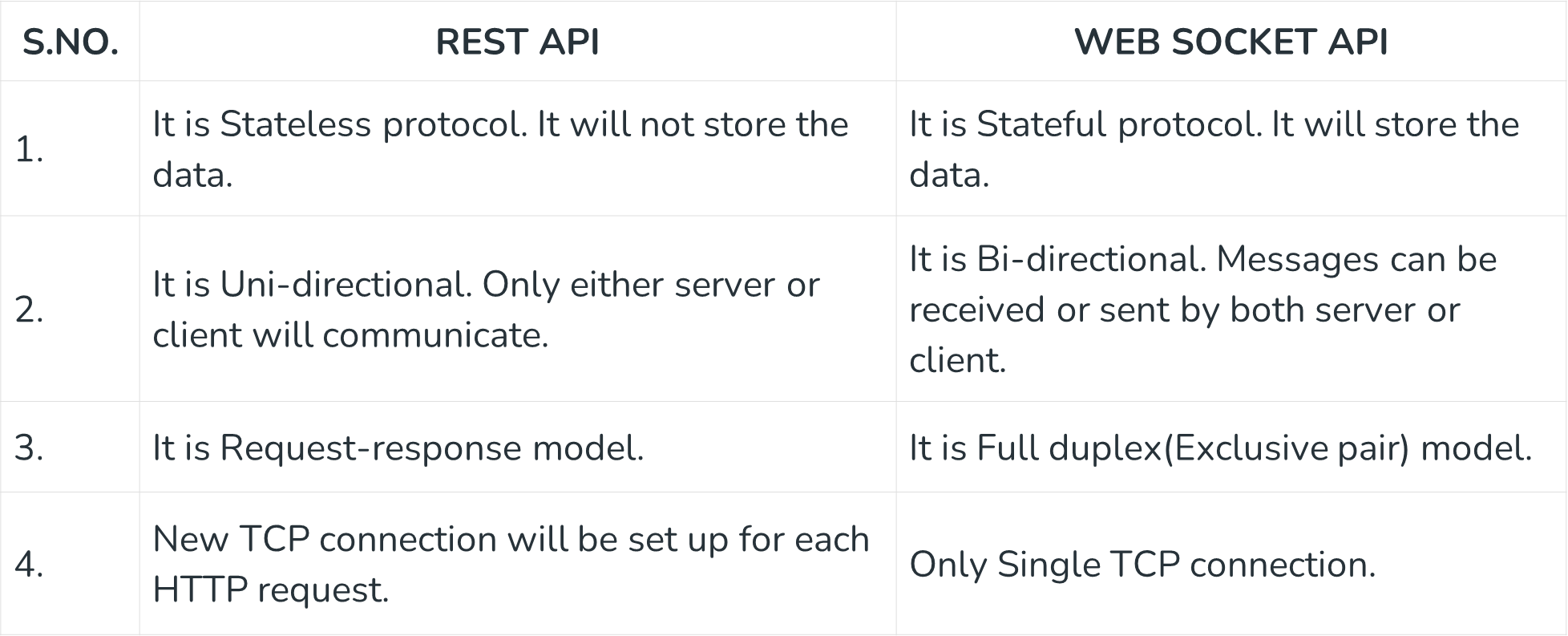
Constraints:

* Client server model
* Stateless
* Cacheable
* Uniform interface
* Layered
* Code on Demand

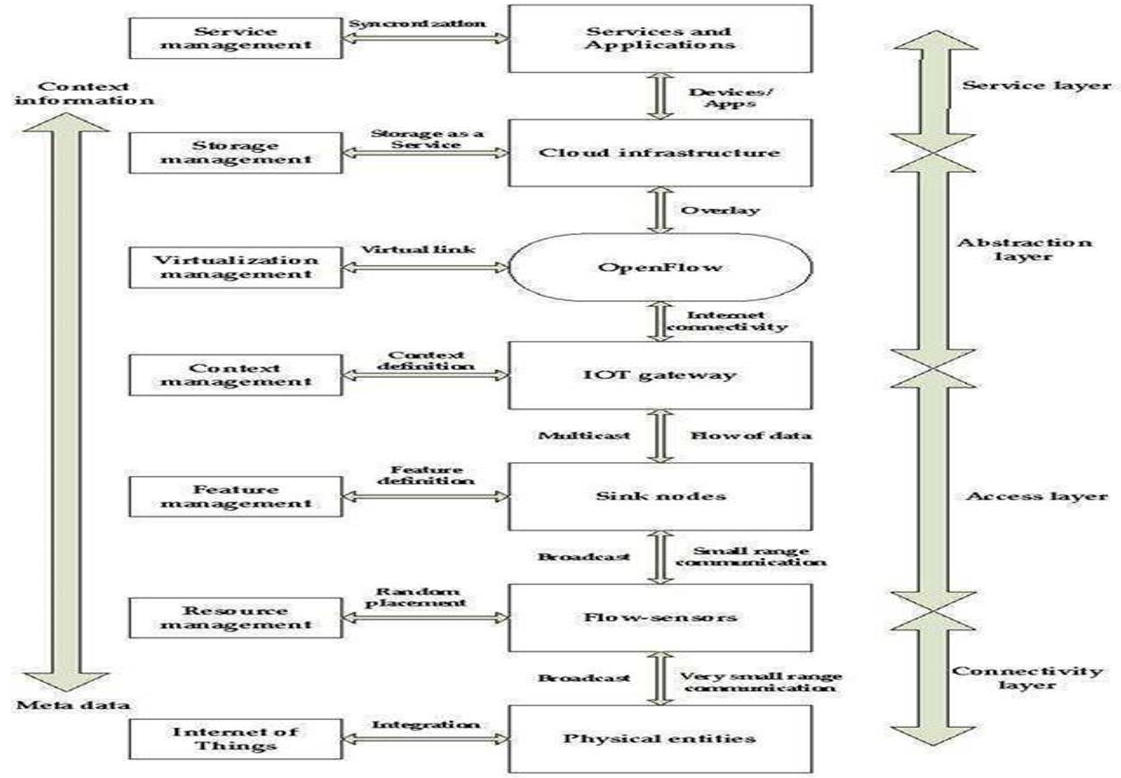


1. Websocket based





Conceptual view:



Challenges of IOT

1. Insufficient testing and updating
2. Concern regarding data security and privacy
3. Software complexity
4. Data volumes and interpretation
5. Integration with AI and automation
6. Devices require a constant power supply which is difficult
7. Interaction and short-range communication

Design challenges

1. Interoperability
2. Security
3. Scalability
4. Reliability
5. Power consumption
6. Privacy

IOT LEVELS 1-6