Protocols

① Universal Plug and Play (UPnP)

- a networking protocol that enables devices like personal computer, WiFi, printers, etc to discover each other and establish connections for sharing services and data
- intended for residential purpose
- considered as an extension of Plug and Play
- uses established standard protocols like TCP/IP

Working

- UPnP assumes that a device is compatible with IP addressing.
- uses these protocols to adeverstise the devices presence and for data transfer

Key Comp (Phases)

- Discovery
  - how your device is visible to other device and vice versa
  - SSDP (Simple Service Discovery Protocol)
    (i) when a device is added to a network, it allows the device to adverrise its services to other connected devices by sending SSDP alive message
    (ii) SSDP also allows a device to passivly listen to the SSDP alive messages from other devices on network
    (iii) When 2 devices discover each other, a discovery message is exicharged containing essential information like the device type & it's services.

- Description
  - when device discover each other, they exchange information in XML format to learn more about each other. These messages contain information like manufacture name, model name, services provided, etc

- Control
  - After getting the information, the control point can call for the service to the URL by function calling.
  - This is done by protocol known as Simple Object Access Protocol (SOAP) that parses XML message

- Event Notification
  - General Event Notification Architecture or GENA is used to notify about event in UPnP.
  - These messages are also sent in XML

- Presentation
  - A device contains a manufacture ~~device for~~ website URL for presentation which is used by control point to retrieve information.

Advantages

(i) It allows real Plug n Play
(ii) An Ideal architecture for home devices and protocol
(iii) can be used ~~by~~ for NAT Traversal or Firewall Punching

Disadvantages

(i) Control point don't require any authentication, hence any program on pc can ask to forward UPnP port
(ii) Any malicious program on your network can use UPnP in the same way a legitimate program uses it.

② Constrained Application Protocol (CoAP)

- CoAP is a session layer protocol that provides the RESTful (HTPP) interface between HTTP client and server.
- It is designed to use devices on same constrained network between devices and general nodes of internet
- CoAP enables low-power sensors to use RESTful services while meeting their low-power consumptions
- This protocol is specially built for IoT systems primary based on HTTP protocol.
- The whole architecture of CoAP consists of CoAP client, CoAP server, REST CoAP proxy, and REST internet
- The data is sent from CoAP client to CoAP server and the same message is routed to REST CoAP Proxy.
- The REST CoAP proxy interacts outside CoAP enviroment and uploads the data over REST internet

③ MQTT Protocol

- MQTT stands for Machine Queuing Telemetry Transport, and is a machine to machine IoT ~~protocol~~ connectivity protocol
- This protocol is useful for the connection with a remote location where ~~for~~ bandwidth is premium.
- It is a publish and subscribe system where we can publish and recieve message as a client.
- Makes easy for communication between multiple devices.
- Some Characteristics are:
  (i) machine to machine protocol, i.e. provides communication between the device
  (ii) does not require for the client and server to establish connection at same time.

(4) XMPP

- stands for Extensible Messaging Presence Protocol.
- protocol for streaming XML elements over network in order to exchange messages and information.
- mainly used by instant messaging applications like WhatsApp.
- XMPP means:
  - X : X for Extensible. XMPP is open source project which can be changed or extended acc to the req.
  - M : XMPP is designed for sending messages in real time. It has very effecient push mechanism composed to other protocol.
  - P : determines whether you are online or offline. It indicates the state.
  - P : XMPP is a protocol, that is, set of standards that allow systems to communicate with each other.
- Advantages
  - (i) free & decentralized, i.e., anyone can set up XMPP server
  - (ii) based on open standard
  - (iii) Security is supported via SASL & TLS
  - (iv) & Flexible, XML based & can be extended.

IoT Service as a Platform

① Clayster

- Console Applications outlines process to create a simple console application. When we create a service for a service platform, the exe file already exists.
- ∴ we have to create a library project instead & make sure that the target framework corresponds to version of Clayster platform.
- Libraries available in Clayster distribution

(i) Clayster.AppServer.Infrastructure
- This library contains the application engine available in platform
- Apart from managing applications, it also provides report tools, cluster ~~tools~~ support, management support, etc

(ii) Clayster.Library.Abstract
- This library contains a data abstraction layer, and is crucial tool for efficient management of objects in the system.

(iii) Clayster.Library.Installation
- This library defines the concept of packages

(iv) Clayster.Library.Meters
- contains an abstraction model for things like sensors, actuators, controllers, meter and so on.

~~(v)~~

② Thingor.io

- It is a platform that allows connecting things to internet.
- It is an open source so you can take the code an build your own cloud if you want
- It provides thing API discovery right out of the box, so you can ~~acti~~ code your things & interact easily with web.
- Extremely scalable & efficient infrastructure

③ SenseIoT

- It is a platform for storing & procesing sensor data safely and securly on cloud.
- comes with tools for visualizing data, setting triggers, and remotely managing data
- It enables developers to integrate the platform & its function with any devices or sensors.
- In the API, HTTP request that are supported are : GET, PUT, POST, DELETE and Options.

④ Carriots

- It is an application hosting & development platform specialy designed for projects related to the IoT and M2M.
- Enables data collection from connected objects, store it, build powerful applications with few lines of code & integration with external IT System.
- Carriots provide a development enviroment & hosting for IoT projects development.

Risks

(i) Security Vulnerabilities
- Weak authentication, encryption, and insecure communication protocols can expose device to hacking, data breaches, and unauthorized acces.

(ii) Data Privacy Concern
- IoT devices collect vast amount of data from sensor and user interaction raising privacy concern about collection, storage and usage of this personal data. Unauthorized access can lead to privacy vidation, and surveillance issues.

(iii) Data Integrity and Trustworthiness
- Ensuring the integrity and trustworthiness of IoT data is essential. Data tampering and manipulation can lead to lack of trust

(iv) Lack of Interoperability
- Interoperability challenges can arise when IoT devices and system from different vendor can not ~~work~~ work together.

(v) Operational Risk
- IoT deployed systems may face operational risk such as system failure, network outrage, and performance issues

(vi) Supply Chain Risk
- IoT devices rely on complex supply chain involving multiple supplies and manufactures compromising integrity

(vii) Regulatory and Complience Challenges
- Complience with regulations and standards, such as data protection law can poses challenge for IoT deployment

Modes of attack

(i) Denial of Service (DoS) and Destributed Denial of Service (DDoS)
- Attackers can overwhelm IoT networks or devices, causing them to become unresponsive

(ii) Man-in-the-middle (MitM)
- Attackers can intercept communication between Iot devices or servers and can steal or manipulate the data.

(iii) Physical Attacks
- Direct access to IoT devices can allow attackers ~~bypassers~~ to bypass security measure, steal data.

(iv) Software Exploits
- Vulnerabilities in IoT device firmware can be exploited to gain access or control.

(v) Ransomeware Attacks
- IoT devices can be hacked by ransomware locking the users out unless a ransome is paid.

(vi) Eavesdropping
- By capturing data ~~fa~~ packets in transits, attackers can gain access to sensitive data

(vii) Supply Chain Attack
- Supply chain attacks vulnerabilities in manufacturing, distribution or procurement process of IoT devices.