Chap 1

Introduction, Characteristics, component, history, difference, architecture, framework, adv & dis challenges,

Automation + Connectivity = IOT

- Automation → general idea of IOT involves direct communication bet" seperate devices, apparatuses & other hardware without human interference.
- Connectivity → Enhanced connections within one network on a worldwide scale provide easy access to various information.

IOT → networking of physical objects that contain electronics embedded within their architecture in order to communicate & sense interactions amongst each other or with respect to the external environment

* Characteristics:
- Connectivity
- Intelligence & Identity
- Scalability
- Dynamic & Self-Adapting (complexity)
- Architecture
- Safety
- Self-configuring
- Interoperability

* IOT enablers:
- RFIDs: uses radio waves in order to electronically track the tags attatched to each physical object.
- Sensors: devices that are able to detect changes in an env (eg: motion detector)
- Nanotechnology: extremely small devices with dimension usually less than a 100 nanometers.
- Smart networks: Mesh topology

* Components:
- Low-power embedded systems
- Cloud computing
- Availability of big data
- Networking connection

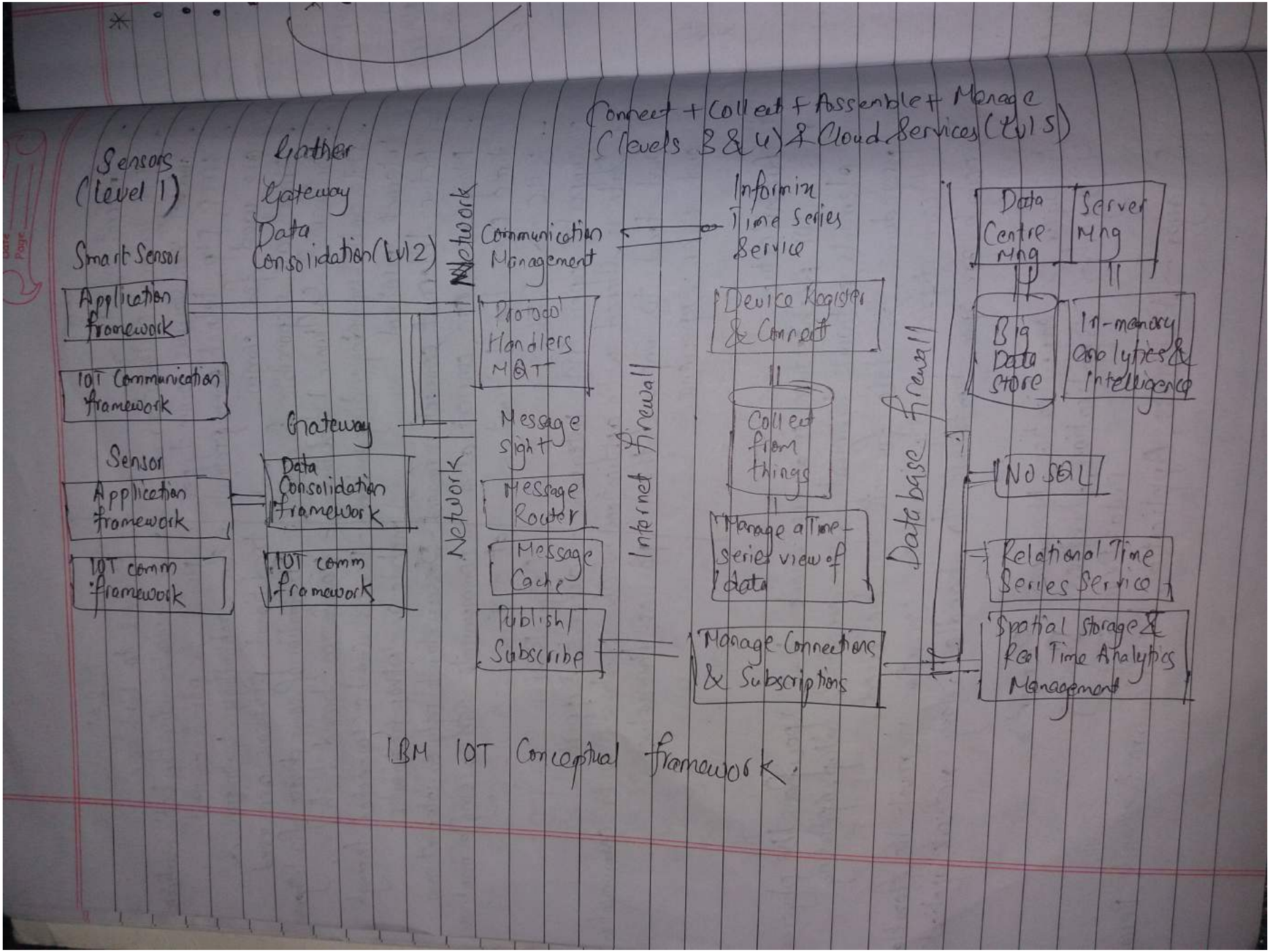
* History
- 1982 → basic concept of network of smart devices was co machine → refrigerator, local programmers controlled the Coca-Cola machine by linking it to the Internet, it could report its if newly loaded drinks were cold or not
- 1985 → the notion of "IOT" as well as term itself first appe
- 1990 → In October 1989, a toaster was designed in INTERO conference which could be turned on/off with Internet, rega as first IOT gadget. TCP/IP was used to link toaster to
- 1991 → the vision of IOT is based on paper on ubiquitous co in 1991: "The Computer of Twenty-first Century"
- 1999 → Kevin Ashton originated the term "IOT" independently the time he saw Radio Frequency Identification (RFID) as to the Internet of Things, which would enable computer manage all individual things.
- 2000 → LG announced plans for 1st Internet refrigera
- 2003-2004 → The phrase "IOT" appears in mainstream m
- 2005 → When the International Telecommunication Union (ITU) of UN published its inaugural report, IOT reached new level.
- 2006-2008: The EU recognizes IOT, the 1st European IOT Conference takes place.
- 2008: Development of the Nest self-learning Wi-Fi enabled thermostat
- 2011-2017: Low-power chipsets with integrated Wi-Fi & 3G/4G connection are smaller, more powerful & less expensive to manufacture. IOT is growing among businesses & homeowners

IOT	M2M
- Internet of Things	- Machine to Machine
- IOT sensors automation	- communicates directly betⁿ machines
- connectⁿ via various comm types	- point to point connectⁿ
- HTTP, Ftp, telnet ~~comm~~ protocols are used for comm.	- Comm technology techniques & traditional protocols are used
- Objects are responsible for decision making	- Observation of some degree of intelligence
- Hardware & Software based technology	- Hardware based tech
- Data delivery depending on the Internet protocol.	- Devices can be connected through mobile or other networks.
- Active Internet connectⁿ is required	- Devices don't rely on internet conn
- Many users can connect at a time over the Internet	- communicate with a single machine at a time
- B2C & B2B	- Only B2B
- supports open API Integration	- doesn't support
- Data is shared with applications that tend to improve the end user experience.	- Data is shared with communication parties themselves.

* Architecture:

- IOT Architecture is a framework that specifies the physical elements, network technical arrangement & setup, operating procedures & data formats to be used.
- It can differ greatly based on execution; it must be flexible enough for open protocols to handle many network applications.

3 layer → Application, Network, Perception
4 layer → Application, Network, Sensing & Data Processing
5 layer → Business, Application, Middleware, Network, Perceptio



IBM IOT Conceptual framework.

* Advantages:
- Improved productivity of staff & reduced human labour.
- Efficient operation management
- Better use of resources & assets
- Cost-effective operation
- Improved work safety

* Challenges
- Security flaws
- Associated costs
- Power supply dependance
- Network dependance
- High skill requirements

- Thorough Marketing & Business Development
- Improved customer service & retention
- Better business opportunities
- More trustworthy image of the company

* Applications:
1. Health Care.
2. Industrial Use
3. Smart Home
4. Smart City
5. Wearables
6. Traffic Monitoring
7. Agriculture

2) Fundamentals of IOT Mechanisms & Key Technologies

* Identification of IOT objects & Services
There are various types of identifiers with different purposes and practicability.
Identification codes can be classified as
- Object IDs (OIDs)
- Communication IDs
• It is desirable for all
- objects to have a permanent unique identifier, an OID
- end-point network locations and/or intermediary-point network locations to have unique network addresses (NAds)
• Every object then has a tuple (OID, Nodr) which is always unique.
• The 2nd entry of the tuple may change with time, location or situation.

these issues ultimately

* Structural aspect of IOT:
• Environment Characteristics.
- low power (with the requirement that they will run potentially for years on batteries).
- low cost (total device cost in single-digit rupees)
- significantly more devices than in LAN environment
- severely limited code & RAM space
- unobtrusive but very diff user interface for configuration (eg: using gestures physical world)
- requirement for simple wireless communication technology

• Traffic characteristics
- char of IOT/M2M comm is diff from other types of networks of apps
- for eg: cellular mobile networks are designed for human comm
- it involves interactive comm bet^n human (voice, video) or data comm involving humans (web browsing, file downloads & so on).
- cellular mobile networks are optimized for traffic char

- Comm takes place with certain length/ sessions and data volume i.e frequency and patterns (talk-listen, download-reading, etc.).

• Scalability
- some apps (eg: smart grid, home automation) may start covering a small geographic area or a small community of users
- efficiency of a larger system should be better than efficiency of a smaller system
- the goal is to make sure that capabilities such as addressing, comm and service discovery among others, are delivered efficiently in both small & large scale

• Interoperability
- because of access of applications technologies, suppliers & stakeholders, it is desirable to develop and/or re-use a core set of common standards.
- existing standards may prove advantageous to a rapid & cost effective deployment of a tech
- product & service interoperability is of interest

• Security & privacy:
- When IOT relates to electric power distribution, goods distribution, transport and trafficking, e-health and other key app
- It is critical to maintain system-wide confidentiality, identity integrity & trustworthiness.

• Open Architecture
- goal is to support a wide range of apps using a common infrastructure, preferably based on service-oriented architecture (SOA) over an open service platform.

* Key IOT Technologies

• Device Intelligence

- In order for IOT to become a reality objects should be able intelligently sense and interact with the environment
- possibly store some passive or acquired data
- communicate with the world around them
  - Objed-to-gateway device communication or even direct object-to-object comm is desirable
- These intelligent capabilities are necessary to support ubiquitous networking to provide seamless interconnection bet" humans and objects.
  - Some have called this mode of comm "5-Any": Any Services, Any Time, Any Where, Any Devices & Any Networks
- Pervasive computing also called ubiquitous computing is the growing trend of embedding computational capability (generally in the form of microprocessors) into everyday objects to make them effectively communicate and perform useful tasks in a way that adds user's need to interact with computers
- network connected and constantly available

• Communication Capabilities:

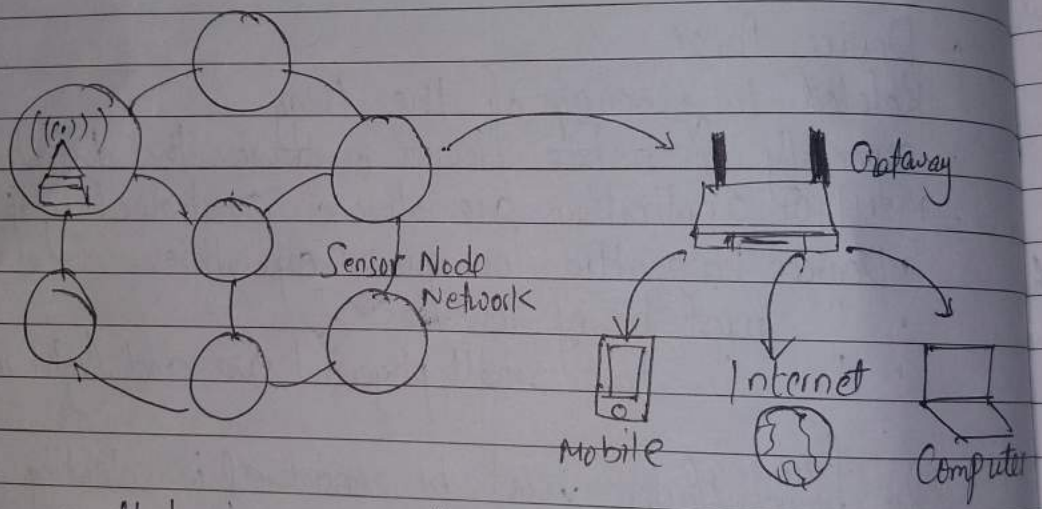
- highly desirable for objects to support ubiquitous end-to-end comm
- to achieve ubiquitous connectivity for human-to-object comm networking capabilities will need to be implemented in the objects ("things")
- IP is considered to be key capabilities for IOT objects
- Self-configuring capabilities, especially how an IOT device can establish its connectivity automatically without human intervention are also of interest
- IPV6 auto-config & multihoming features are useful, particularly scope-based IPV6 addressing features.

- Mobility Support:
  - another consideration related to tracking and mobility support of mobile object
  - mobility-enabled architectures & protocols are required
  - some objects move independently, while others will move as one of group
  - Therefore, according to the moving feature, different tracking methods are required.
  - It is imp to provide ubiquitous & seamless comm among objects while tracking the location of objects
  - Mobile IPV6 (MBIPV6) offers several capabilities that can address this requirement.

- Device Power
  - Related to powering of the thing
  - especially for mobile devices or devices that don't have intrinsic power
  - M2M/IOT applications are always constrained by following factors:
    - Devices have ultra low power capabilities
    - " must be of low cost
    - " " have small physical size and light in weight

  - The following factors must be considered in selecting the most suitable battery for a particular application:
    - Operating voltage level
    - load current and profile
    - Duty cycle - continuous or intermittent
    - Service Life
    - Physical req (Size, shape, weight)
    - Env conditions (Temperature, Pressure, Humidity, Vibration, Shock, pressure)
    - Safety & Reliability
    - Shelf Life
    - Maintenance & Replacement • Cost
    - Environmental impact & recycling capability

- Sensor Technology
- A sensor network is an infrastructure comprising sensing, communication, data collection, monitoring, surveillance & medical telemetry.
- Sensor network tech, specifically with embedded network sensors, ships, aircrafts and buildings can "self-detect" structural faults (eg: fatigue-induced cracks)
- Earthquake oriented sensors in buildings can locate post survivors and can help assess structural damage; tsunami-related sensors can certainly prove useful for nations with excessive coast
- Sensors also find extensive applicability in battlefield for reconnaissance and surveillance.



- There are 4 basic components in a sensor network:
  - (i) an assembly of distributed or localized sensors
  - (ii) an interconnecting network (usually but not always, wireless based)
  - (iii) a central point of info clustering
  - (iv) a set of computing resources at the central point (or beyond) to handle data correlation, event-trending, querying and data mining
- Because the interconnecting network is generally wireless, these systems are known as wireless sensor networks (WSNs).
- WSNs have the potentially large quantity of data collected,

algorithmic methods for data mng play an imp role in sensor networks.
- In-network processing is desirable in sensor networks; furthermore, node power (and/or battery life) is a key design consideration.

- RFID technology:
- RFIDs are electronic devices associated with objects ("things") that transmit their identity (usually a serial no) via radio links.
- RFID tags are devices that typically have a read-only chip that stores a unique no. but has no processing capability
- RFID & barcode facilitate the global supply chain and impact all subsystems within that overall process, including material req planning (MRP), just in time (JIT), electronic data interchange (EDI) & electronic commerce (EC).

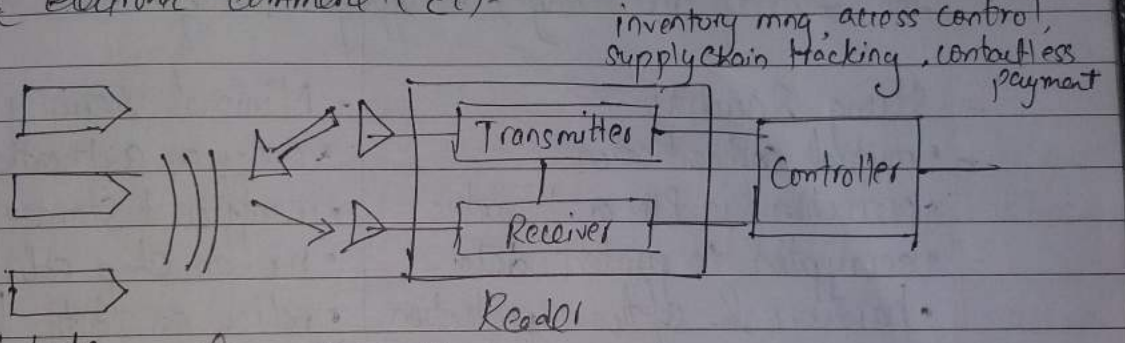


fig: RFID Reader operation

RFID concepts

Air Interface: The complete comm link bet" an interrogator and a tag including the physical layer, collision arbitration algorithm, command and response structure and data-coding methodology

EPCglobal architecture framework: A collection of interrelated standards ("EPC global Standards"), together with services operated by EPCglobal, its delegates and others ("EPC Network Services"), all in service of a common goal of enhancing business flows and computer applications through the use of EPCs.

* Size of sensors
- Nanoscopic (nanoscale) in the order of 1-100nm in diameter
- Mesoscopic scale refers to objects bet^n 100 & 10000 nm in
- The microscopic scale ranges from 10 to 1000 microns.
- The macroscopic scale is at the millimeter to meter-le

* Contactless card	RFID
- contains a microprocessor, a small but real computer computer that make calculations, comm both ways, remembers new info and actively uses these capabilities for security and many other apps	- devices that typically have read-only chip that stores a unique one. but has no process capability. It is more like a radio based bar-code used for identification.
- Strong Security • mutual authentication • protection via PIN or biometric • encryption to protect data • hardware & software protection.	- Minimal security • one-way authentication • insufficient storage for biomet • no-on chip calculation of re • relies on static keys
- Hundreds of security features meaning an individual's details can be safely stored, managed & exchanged!	- Single function used to help machines identify objects to increase efficiency. Eg: inventory control
- Read & Write memory capacity of 512 bytes and more with very large memory storage possible.	- Small memory (96 bytes), often read only
- Short distance data exchange, typically 2 inches.	- Longer distance data exch typically several yards.

* Radio frequency (RF) communication:
1) When a contactless card / RFID tag passes within range, a reader sends out radio frequency electromagnetic waves.
2) The antenna, tuned to receive these waves, wakes up the chip in the smard card or tag.
3) A wireless communications channel is set up between the reader and the smart card or tag

* Standards for RFIDs.
- The ISO 14443
  - operating frequency of 13.56 MHz that embed a CPU; power consumption about 40mW; data throughput about 100 kbps and max working distance (from the reader) around 10 cm.

- The ISO 15693
  - operating at 13.56 MHz freq but it enables working distances as high as 1m, with a data throughput of a few Kbps.

- 18000
  433 MHz
  frequency - 135 KHz, 13.56 MHz, 2.45 GHz, 5.8 GHz, 860-960 MHz, uses the 860-960 MHz range & is the basis for Class 1 Gen 2 UHF RFID, introduced by the EPCglobal Consortium.

* Layers of RFID
- Tag (device) layer: Architecture & EPCglobal Gen 2 tag finite state machine
- Media interface layer: frequency bands, antennas, read range, modulation, encoding data rates.
- Reader layer: Architecture, antenna configurations, Gen2 sessions, Gen2.

- Satellite Technology
  - Ability to support mobility in all geographical environments (including Antartica)
  - Global reach
  - Offers interesting commercial possibilities
  - Can play critical role in many broadly distributed M2M

3) IOT Protocols

* Protocol Standardization for IOT:
  - IOT-Architecture one of the few efforts targeting a holistic architecture for all IOT sectors
  - This consortium consists of 17 European organizations from 9 countries
  - Summarized current status of IOT standardization as:
    - fragmented architectures
    - No holistic approach to implement IOT has yet been proposed
    - many islands sol's do exist (RFID, sensor nets, etc)
    - little cross-sector re-use of technology and exchange of knowledge

* M2M & WSN Protocols:
  - Most M2M apps are developed today in a highly customized fashion.
  - high level M2M architecture from M2M Standardization Task force (MSTF) does include fixed & other non cellular wireless networks.
  - means it's generic, holistic IOT architecture even though it is M2M architecture.
  - M2M & IOT sometimes are used interchangeably in the OS
  - Other M2M standard activities include:
    - Data transport protocol standards - M2M XML, JSON, BiTXML, etc

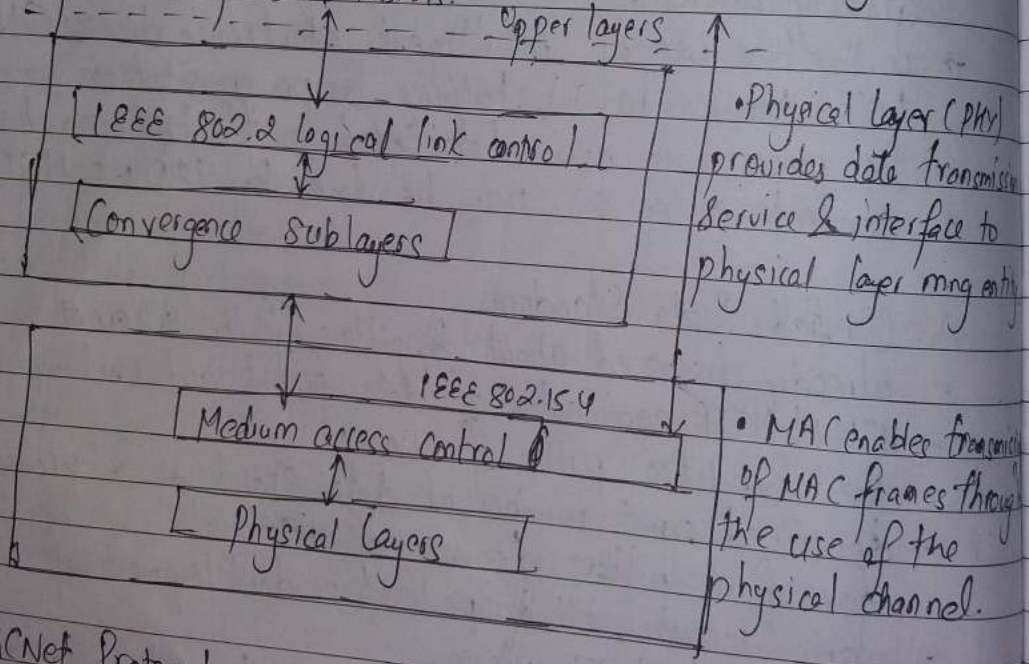
- Remote mng of device behind firewall
- M2M security & fraud detection

* SCADA & RFID protocols.
- Supervisory Control & Data Acquisition
- Out of the IOT pillars to represent the whole industrial automation arena.
- IEEE created standard specification called std C37.1™, for SCADA automation systems in 2007
- In recent years, network-based industrial automation has greatly evolved
- with the use of intelligent electronic devices (IEDs) or IOT devices in substations & power stations
- The process is now distributed so it's that can be done at control center can now be done by IED i.e M2M bet" devices

* Unified Data Standards
- already discussed about 2 pillars of the internet
- HTML/HTTP combination of data format and exchange protocol is the foundation pillar of WWW
- described great number of data standards & protocols proposed for four pillars domains of IOT
- many issues still impede the development of IOT and especially WOT vision.
- many standardization efforts have been trying to define unified data representation, protocol for IOT
- Before IOT, internet was actually an Internet of documents or multimedia docs
- two pillars of Internet including HTML/HTTP turned the Internet to WWW
- There are different lvls of protocols but the ones that most directly relate to business & social issues are the ones closest to the top so called apps protocols such as HTML/HTTP for the web

- Web has always been visual medium but restricted cuz recently HTML devs were limited to CSS and JS in order to produce animations or they would have to rely on plug-in

* IEEE 802.15.4 (LR-WPANs)
- Defines operation of low-rate wireless personal area networks
- Specifies physical layer and media access control for LR-WPAN
- maintained by IEEE 802.15 working group, which defined the standard in 2003
- Basic framework conceives a 10m communications range with a transfer rate of 250 kbit/s.



* BACNet Protocol
- Comm protocols for Building Automation & Control (BAC) networks
- provides mechanisms for computerized building automation devices to exchange info
- designed to allow comm of building automation & control system for application like
  - HVAC
  - Lighting Control, Access Control
  - fire Detection Systems & their associated Equipments

- defines a no. of services that are used to comm bet^n building devices
- protocol services include Who-Is, I-Am, Who-has, I-have which are used for device & Object discovery
- services such as read property and write-property are used for data sharing
- defines no. of data link/physical layers including
  - ARCNET, Ethernet, BACnet/IP, BACnet/IPv6, Master-Slave, ZigBee
- defines 60 object types that are acted upon by services

* Modbus

- Serial communications protocol originally published by Modicon in 1979
- commonly available for connecting industrial electronic devices
- Reasons for the use of Modbus in industrial env:
  - Developed with industrial apps in mind
  - openly published & royalty-free
  - easy to deploy & maintain
- enables comm among many devices connected to the same network

Object types

Object Type	Access	Size
Coil	Read-write	1-bit
Discrete Input	Read-only	1 bit
Input register	"	16 bits
Holding	Read-write	16 bits

* ZigBee

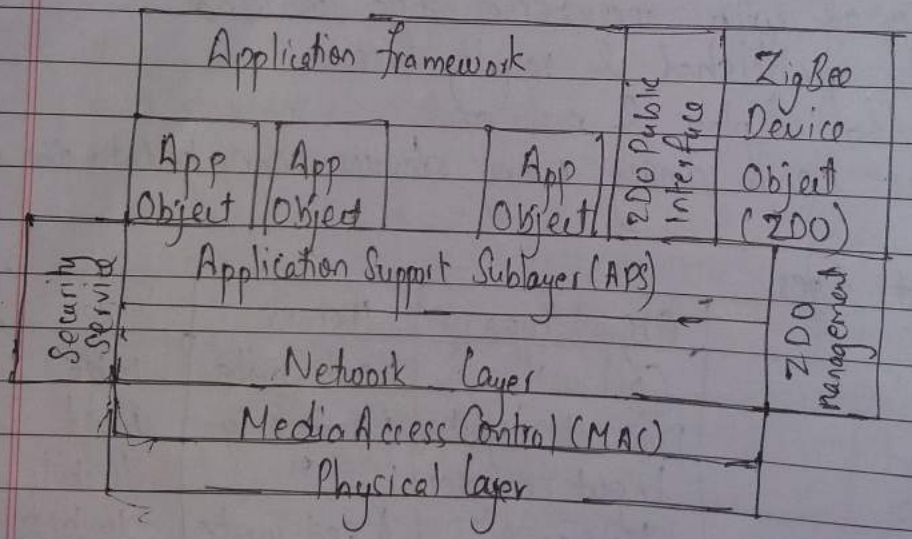
- protocol which provides comm for wireless PAN of resource constrained device
- developed by Zigbee alliance & IEEE jointly.
- aims to provide the upper layers of the protocol stack (network to application layer).
- reside on top of PHY & MAC sub layers.

- with its sleepy, battery-powered end devices, is a perfect fit for wireless sensors.
- less expensive & simpler comm system.

Features: Multi-hop routing, Link Mng, frequency Agility, fragmentation and Reassembly, Power Mng, Security

Applications: Building Automation, Personal Health Care, Industrial Control, Commercial Control, PC & Peripherals, Consumer Electronics.

Network topologies: Star, Mesh, Cluster



- Network layer
  - located between MAC & APS
  - Provides following f's:
    - → Starting a network
    - → managing end devices joining or leaving a network
    - → route discovery
    - → Neighbour discovery

- APS layer
  - provides services necessary for application objects (end points) & the ZigBee device object (ZDO)
  - some services provided by APS to the application objects for data transfer are request, confirm, response

- Application Object (end point)
  - defines input & output for to the APS
  - for eg, a switch that controls a light is the input from the app object & the output is the light bulb cond^n.
  - each node can have 240 seperate app objects

- ZigBee Device Object (ZDO)
  - Control & Mng of app objects
  - Performs overall device mng tasks:
    - → Determines the type of device in a network (end device, router, etc)
    - → Initializes APS, Network layer & Security Service provider.
    - → performs device & service discovery
    - → initializes coordinator for establishing a network.
    - → Security mng
    - → Network mng

- End Node
  - each end node or end device can have multiple EPs
  - Each EP contains an app profile, such as home automation
  - can be used to control multiple devices or single device

- ZigBee Addressing Mode : uses direct, group & broadcast addressing for transmission of information

* IOT Security
- fundamental idea: IOT will connect all objects around us to provide smooth comm
- Economic of scale in IOT presents new security challenges global devices in terms of
  - Authentication
  - Addressing
  - Embedded Security
- Devices like RFID & sensor nodes have no access control facility
- Can freely obtain or enchange info from each other so authen & authorization scheme must be established between these devices to achieve the security goals for IOT
- privacy of things & security of data is one of the key chall

* CoAP: Constrained Application Protocol
- application layer protocol for M2M apps, meant for constrained environments with cons devices & cons networks.
- Like HTTP, COAP is a web transfer protocol & uses a client-server architecture where clients communicate with servers using connectionless datagrams.
- Request-response model, however it runs on UDP instead of TCP
- designed to easily interface with HTTP and supports methods such as GET, PUT, POST & DELETE

* 6LowPAN: This protocol is used at Adaptation layer before a data stack transmits to IPV6 Internet layer.
- Internet layer receives & transmits to/from adaptation layer. The data stack uses 6LowPAN (IPv6 Over Low Power Wireless Personal Area Network) at adaption layer before the data stack transmits to IPv6 Internet layer.
- IEEE 802.15.4 WPAN device has a 6LowPAN interface serial port for

- An adaptation - layer protocol for the IEEE 802.15.4 network devices. (low speed & low power devices).
- features: header compression, fragmentation & reassembly.
- specifies the IETF recommended methods for reassembly of fragments, & IPv6 and UDP (or ICMP) headers compression, neighbour discovery (6LoWPAN-hc, 2nd adaptation layer)
- supports mesh routing
- can be implemented using Berklay IP implementation with O.S TinyOS or 3BSD or other implementation for IOT nodes from Sensinode or Hitachi.

5) IOT, Privacy, Security & Governance

* Vulnerabilities of IOT

- Unauthorized access
- one of the main threats is tampering of resources by u.a
- Identity-based verification should be done before granting the access rights

- Information Corruption
- device credential must be protected from tampering
- secure design of access rights, credential and exchange is required to avoid corruption

- Theft of resources
- access of shared resources over insecure channel causes theft of
- results into man-in-the-middle attack

- Info disclosure
- data is stored at diff places in diff forms
- distributed data must be protected from disclosure
- content-aware access control must be enforced to regular access to system resources.

- Denial of Service (DoS) attack,
  - makes an attempt to prevent authentic user from accessing services which they are eligible for
  - eg: unauthorized user sends to many requests to server
  - that flood the network & deny other authentic users from access to the ~~intern~~ network

- Distributed DOS (DDOS) attack
  - type of DOS attack where multiple compromised systems are used to target single system causing DoS
  - compromised systems - usually infected with trojan
  - victims of DDOS atk consist of both
    - end targeted systems
    - all systems maliciously used and controlled by the hacker in the distributed attack

* Security Requirements
- Access Control
  - provides authorized access to network resources
  - IoT is ad-hoc & dynamic in nature
  - efficient & robust mechanism of secure access to resources must be deployed with distributed nature.

- Authentication
  - identity establishment btw communicating devices
  - due to diversity of devices & end users, an attack resistant lightweight sol for authentication

- Data Confidentiality
  - protecting data from unauthorized disclosure
  - secure, lightweight, and efficient key exchange mechanism is.

- Availability
  - ensuring no denial of authorized access to network resources
- Trust Mng: decision rules needs to be evolved for trust mng in IOT
- Secure Software Execution: Secure, managed-code, runtime env designed to protect against diff apps
- Secure storage: involves confidentiality & integrity of sensitive info stored in the system
- Tamper resistance:
  - desire to maintain security req even when device falls in hands of malicious parties
  - can be physically or logically probed
- Scalability
  - IOT consist of var types of devices with diff capabilities from intelligent sensors & actuators to home applications
  - Comm (wireless/wire) & protocols (Bluetooth, ZigBee, RFID, Wi-Fi, etc.)
- Flexibility & Adaptability
  - IOT will consist of mobile comm devices
  - can roam around freely from one type of env to others with diff types of risks and security threats
  - users are likely to have diff privacy profile depending on env

* Threat Modeling
  - presented by first defining misuse case
  - means ive scenario describing the ways the system should not work
  - and then standard use case assets to be protected in IOT will vary with respect to every scenario case

* Threat Analysis
  - Assets needs to be identified to drive threat analysis process
  - Smart home is localized in space, provide services in a household

- devices in smart homes are combined with n/w to provide means for entertainment, monitoring of appliances, controlling of house components & other services
- uncovering the security design flaws after specifying the stride category, dfd, elements bet" that the interactions occuring during the stride & processes which are activated for analysis.

* Use Case & Misuse cases

- actor in use case & misuse case in the scenario of smart home includes
  - infrastructure owner(smart home)
  - IoT entity(Smartphone device / software agent)
  - attacker (misuser)
  - intruder (exploiter)
- access rights granted to unauthorized entity
- Corruption of access credentials
- Unauthorized data transmission
- DOS attack
- Man-in-the-middle attack

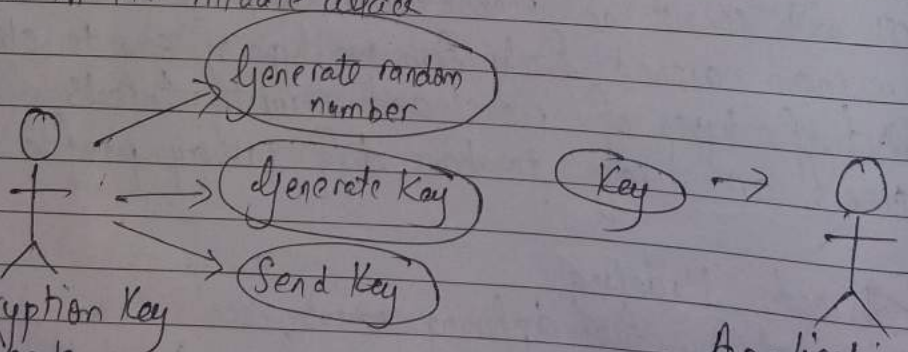


fig: Simple use case diagram for generating & communicating key

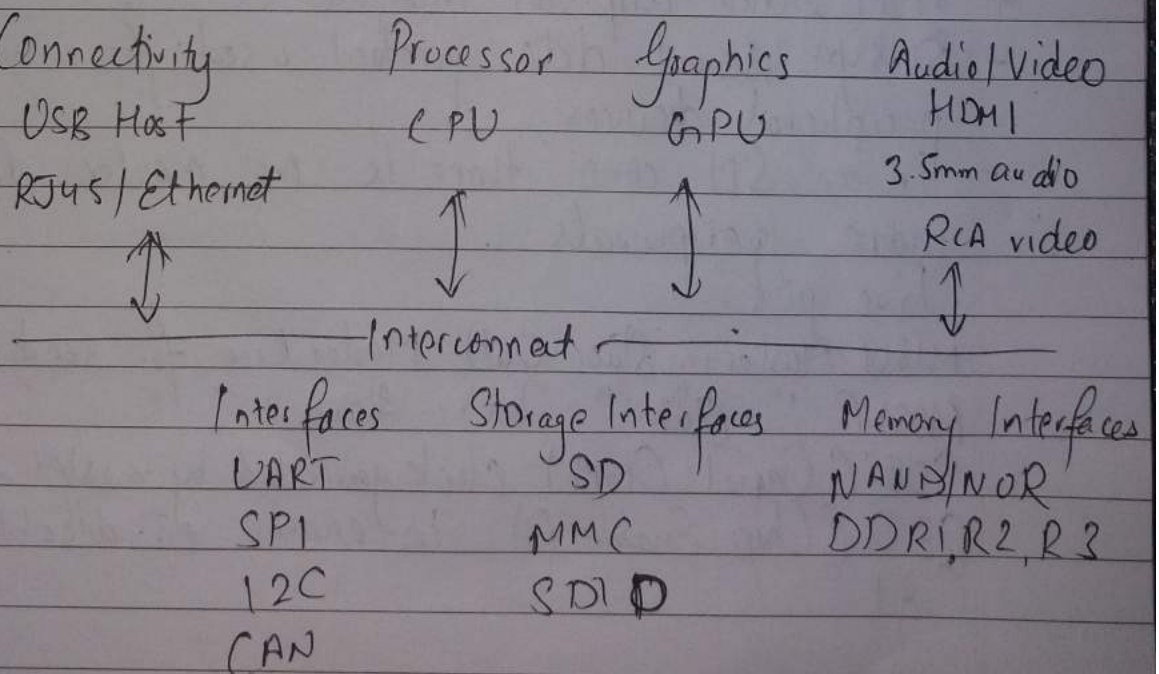
Firstly, the actors & collaborating actors are identified. Then, misuse cases are developed for each of them. Purpose of this is creating specifications for communicating the potential risks and rationale for security-relevant decisions to the device platform, app or servio.

- Web Service that provides computing capacity in the form of virtual machines.
- EC2 can be use for several purposes for IOT systems

4) * Basic building block of IOT device
- Sensing
- Actuation
- Communication
- Analysis & Processing

* Raspberry Pi
- low-cost mini-computer with the physical size of credit card
- runs various flavors of Linux & can perform almost all tasks a normal computer can do.
- allows interfacing sensors & actuators through the general purpose I/O pins.
- runs on Linux OS, supports Python "out of box".

* Block Diagram :



* R-Pi Interfaces

SYNC	SYNC	ASYNC
Serial	Serial	Serial
↕	↕	↕
I2C	SPI	UART

* Serial

The serial interface on R-pi has receive (Rx) & transmit (Tx) pins for comm with serial peripherals.

- GPIO 14 - UART Tx
  15 - Rx

* Serial Interface UART

- Universal Asychronous Receiver/Transmitter is a serial comm protocol in which data is transferred serially bit by bit.
- Asy serial comm is widely used for byte oriented transmission
- In " " " , a byte of data is transferred at a time.

* SPI (Serial Peripheral Interface)

- Synchronous serial data protocol used for comm with 1 or more peripheral devices.
- In an SPI conn, there is one master device & one or more peripherals.

Five pins:

MISO (Master in Slave Out): Master Line for sending data to peripherals

MOSI (" Out " In): Slave " " " " " master

SCK (Serial Clock): clock generated by master for data sync

CE0 (Chip Enable 0): To enable or disable devices

CE1

I2C (Inter Integrated Circuit)

- Syn serial protocol that comm data betn 2 devices
- master slave protocol which may have 1 or many masters and many slaves where as SPI has only 1 master
- generally used for comm over short distance