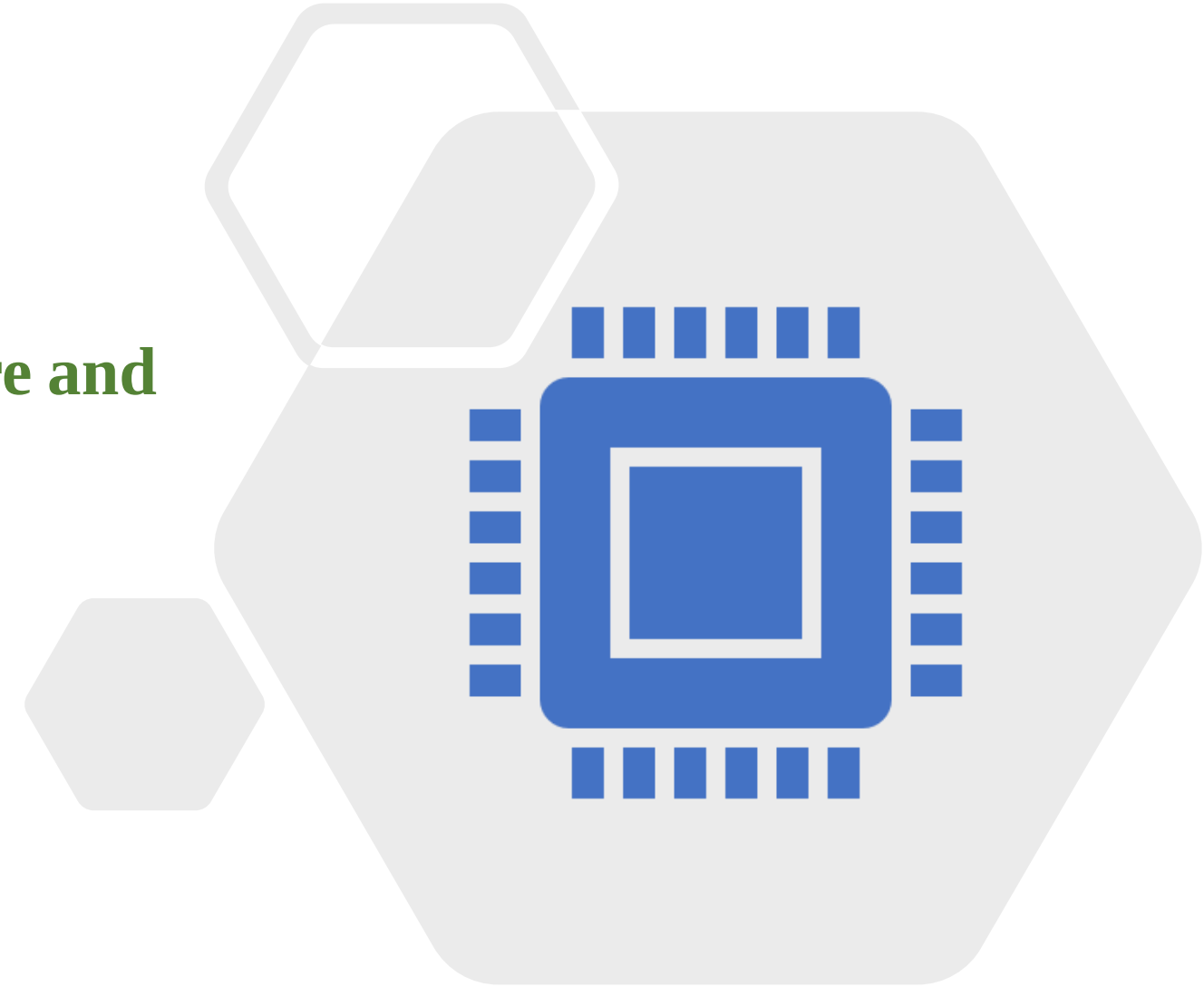
IoT Related ICT Architecture and Design Consideration



Zin May Aye
University of Computer Studies, Yangon, Myanmar

ASEAN IVO FORUM (2020)

Objectives

- To study IoT Architectures and Frameworks
- To observe applications and sensors and communication protocols
- To study protocol related with IoT layers varies and natures of sensors
- To know the technology of securing the IoT Data Network
- To apply the IoT related technology in the ICT applications

Contents

- Introduction to IoT
- IoT components and Impact of IoT
- Types of Technologies in IoT
- Protocol Model Related with IoT Stack and Type of IoT Connectivity
- Design Considerations in an IoT System and Architecture of IoT
- Securing the IoT Data Network
- Communication and Challenges
- LoRaWAN Architecture in Design Consideration
- IoT Environment in Agriculture/Farm
- IoT Security
- Smart Environments
- Conclusion

Introduction to IoT

- Internet of Things (IoT) is the connection of millions of smart devices and sensors connected to the Internet. It is a transformational technology and is converged with operational technologies and information technologies. It is a system of interrelated computing devices and plays a main role in ICT operations with unique identifier and the ability to transfer data over network without requiring human-to-human interaction.
- The smart physical connected products are now improving in processing power and are significant in miniaturization. The IoT network offers the ubiquitous wireless connectivity and the IoT devices apply embedded sensors, actuators, processors, and transceivers for their interconnections.
- IoT can also be described as a large set of technologies and research disciplines oriented to support the IoT related sector, through the deployment of new data-oriented systems comprised of sensors, actuators, network connectivity, Fog-and-Cloud-oriented platforms, and others.

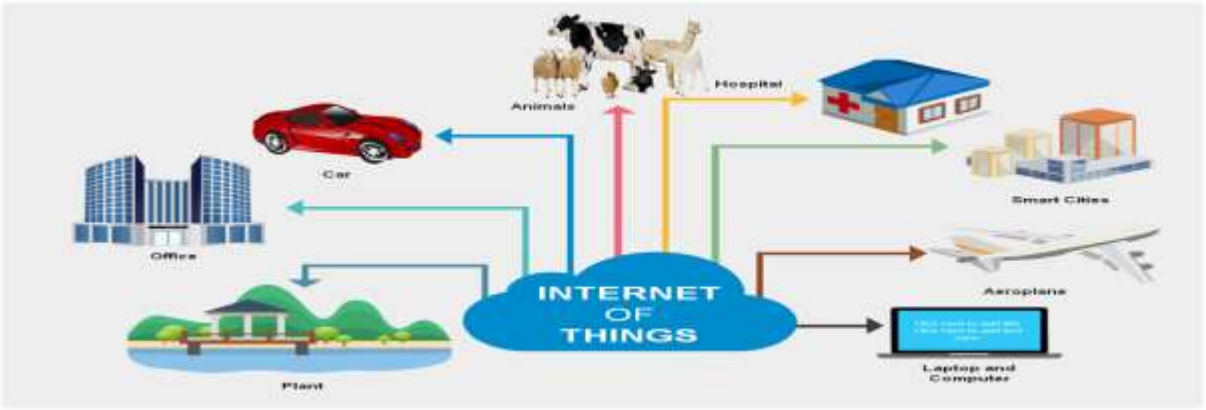


Fig: Internet of Things

Introduction to IoT cont'd

IoT Characteristics

The followings are some of the features of the IoT devices.

- Context Awareness: Adapt changes with respect to changing context
- Embedded and Micro systems: SOC (system on Chips), microchips, microcontroller
- Wireless and Mobile Networks: WiFi, Cellular
- Enormous Scale: Billions of things
- Things-related services: Communicate (physical/virtual) and exchange data with other devices for analysis
- Interconnectivity: Interoperable communication protocols
- Unique Identity: Unique IP address

IoT Components

IoT Components : IoT components comprise of both physical and smart components, connectivity components, communication technology and storage platforms

- Physical components: Comprise the product's mechanical and electrical parts.
- Smart components: Comprise the sensors, microprocessors, data storage, controls, software, and, typically, an embedded operating system and enhanced user interface.
- Connectivity components: Comprise the interfaces, antennae, gateway and protocols enabling wired or wireless connections with the product.
- Forms of Communications: Satellite, WiFi,Radio Frequency (RF),RFID, Bluetooth,NFC
- IoT/cloud Platforms: To support to handle large amounts of data coming into the system via sensors and to provide compute, storage and run applications. As smart things collect huge amount of sensor data, compute and storage resources are required to analyze, store, and process this data. The most common compute and storage resources are cloud based because the cloud offers massive data handling, scalability, and flexibility.

IoT Components cont'd

IoT Components (Sensor, Controller and Actuator in IoT)

- **Sensors:** Things are counted as a sensor as long as it provides inputs about its internal state environmental facts. They are deployed in IoT applications to collect data. They are in small size and low power with less cost. sensors are used to send feedback to the controller of each small system.

- **Actuators:** Act on their immediate environment to enable correct operation of the machines or devices they are embedded into. Interpreting the electrical impulses sent from the control system and converting them into mechanical motion.

- **Controller:** In a typical IoT system, a sensor may collect information and route to a control center. There, previously defined logic dictates the decision. Low-power wireless data communication controller chips enable smart home applications and the Internet of Things (IoT).

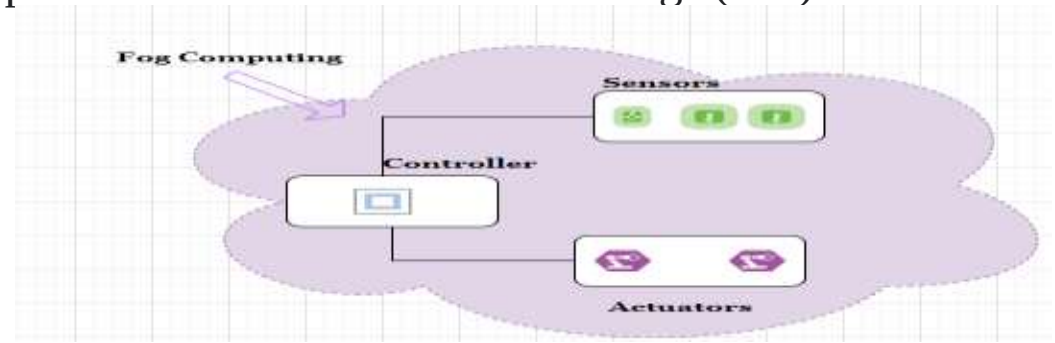


Fig: IoT Components

IoT Components IoT cont'd

Sensors and Power

- Sensors can be either standalone devices or devices embedded in ordinary objects or machines to make them smart, and they can be divided into categories in terms of the physical phenomenon they are intended to measure.
- Environmental sensors are used to sense parameters in the physical environment of temperature, humidity, pressure, water pollution, and air pollution.
- Power : Power consumption is one of the factors in sensors. Many sensors are "out in the field" and are powered by batteries or solar panels, consideration must be given to power consumption. For the extension of sensor life, it is desirable a low power connection in designation.
- Some of the IoT sensors and applications are described in the figure below.

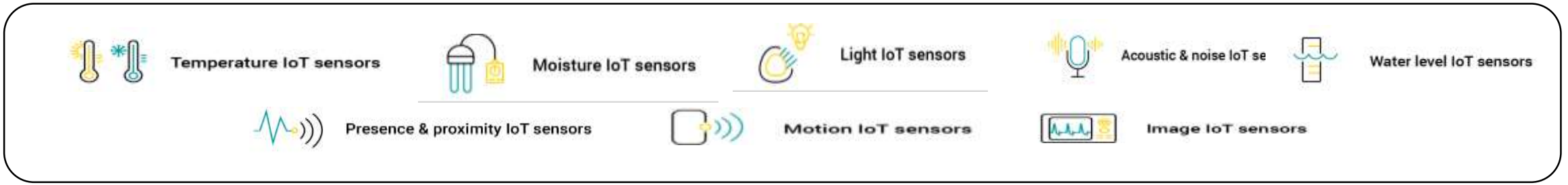


Fig: Type of IoT Sensors

Impact of IoT

IoT promises a way to reduce wastes, costs and inconvenience while increasing efficiency. IOT networks become more pervasive as usage grows, costs of the sensors and such connected devices will drop. Development of low-bandwidth, low-power consuming devices will further drive the costs down. Some of the facts of impact of IoT on Agriculture are as follows:

- **Functional impact**: Real time and remote monitoring of environment, pests, diseases, etc, report conditions, alter its state of connected things.
- **Economic impact**: Increase yield quality/quantity, increase productivity in the field and animal welfare.
- **Environmental impact**: Enhances farming methods and the real-time control of the cultivations. Improving soil quality and reducing use of resources as in water and other natural resources.
- **Social Impact**: Less labour requirement and also improve in trust and satisfaction for the products.
- **Business impact**: Outcome the new business models and cooperation facilities.
- **Technological impact**: Low-power wireless sensor and long range of communication with secure access.

Fig: Impact of IoT on Agriculture

Types of Technologies in IoT

Different wireless technologies support different IoT scenarios. Wireless technologies area that can be deployed in IoT applications are as follows:

- Proximity (RFID)
- WPAN (Bluetooth and Bluetooth Low Energy (BLE) and ZigBee)
- WLAN (WiFi)
- WWAN (Cellular/ LPWAN)
  - Cellular (2G/3G/4G/LTE)
  - LPWAN (Sigfox, LoRa)

Types of Technologies cont'd

- Radio frequency identification (RFID) system is an automatic technology and provide computers to identify objects or control target through radio waves. RFID is primarily concerned with the identification of objects and combination of sensors, actuators and upstream internet-based data processing produces an IoT system and can be monitored and controlled IoT items globally in real-time. Its frequency ranges are 120-150kHz (10 cm), 13.5 MHz, an ISM band (1 m), 433MHz and ranges of up to 100m.
- Bluetooth operates in the 2400-2483.5 MHz range within the ISM 2.4 GHz frequency band. Data is split into packets and exchanged through one of 79 designated Bluetooth channels (each of which have 1 MHz in bandwidth).
- Bluetooth Low Energy (BLE) supports 40 channels with 2 MHz channel bandwidth and 1 million symbols/s data rate. BLE supports low duty cycle requirements as its packet size is small and the time taken to transmit is 80 μs. BLE consumes far less energy as compared to Zigbee. The energy efficiency of BLE is 2.5 times better than Zigbee.
- 4G/LTE networks is not optimal for IoT applications, both for cost and nodal power-consumption reasons. 5G IoT is ideal for Smart City for mission-critical and Quality of Service (QoS)-aware applications. Narrowband IoT in cellular is made for a large number of devices that are energy constrained and necessary to reduce the bit rate. The downlink speeds may vary between 40 kbps and 10 Mbps.

Types of Technologies cont'd

Low Power Wide-Area-Networks (LPWAN)

- LPWANs can use licensed or unlicensed frequencies and include proprietary or open standard options. The proprietary, unlicenced Sigfox is widely deployed LPWANs with Ultra Narrowband (UNB) modulation technology. LPWAN technology allows IoT devices to operate reliably for up to 10 years on a single battery charge. For the IoT scenarios, LPWAN is low bit rate communication technologies.

- LPWAN technology comes in many shapes and sizes – ZigBee, SigFox, Nwave, LTE-M, and NB-IoT, are the preferred technologies for IoT applications. This is due to cost efficiency and the ability of these standards to provide longevity, security and mature, wide-reaching networks.

- LPWAN technologies are ideal for Smart meters, Smart city, Track and trace, Smart agriculture, Smart building applications. LPWAN technology (ZigBee, SigFox) supports longevity, security and mature, wide-reaching networks with data transfer rate of 3 Kbps to 375 Kbps for 10 to 1000 bytes packet size. Sigfox uses narrow band communication (10 MHz). It uses free sections of the radio spectrum (ISM band) to transmit its data. Sigfox focuses on using very long waves that can increase to a 1000 kms. SigFox transmits in the 868 MHz ISM band in Europe and the 900 MHz ISM band in North America.

- The ZigBee technology is a low-power, a defined rate of 250 kbit/s, designed to carry small amounts of data over a short and it's a mesh networking standard is connected to each other. The distance is 10–100 meters in line-of-sight. Some products use 802.15–ZigBee and 6LoWPAN secured by 128-bit symmetric encryption keys.

Types of Technologies cont'd

Role of WiFi in IoT

- WiFi provides high bandwidth and low-latency applications. Some IoT applications as in vehicular services, video-based security cameras, will need the broadband network, with low latency .
- WiFi supports broadband and narrowband IoT applications at varying levels of power consumption and signal range. 5G standards will prioritize IoT-focused capabilities with latency below four milliseconds .
- The WiFi standards for IoT, WiFi HaLow (802.11ah), operates at a lower frequency than 802.11ax. It has longer range than 802.11ax and allows clients to operate in 20 MHz-only mode. It is explicitly targeted to IoT applications. 802.11ax could become the de-facto WiFi standard and BLE and ZigBee for home, enterprise and other indoor IoT applications.
- Wi-Fi HaLow operates the low power connectivity necessary for applications including sensor and wearables. It provides a more robust connection and easily penetrate barriers.
- Wi-Fi HaLow is ideally suited for IoT devices as it allows over 8,000 robust connections to a single access point over 1 km range and it can take advantage of new sleep modes that saved power.

Protocol Model Related with IoT Stack

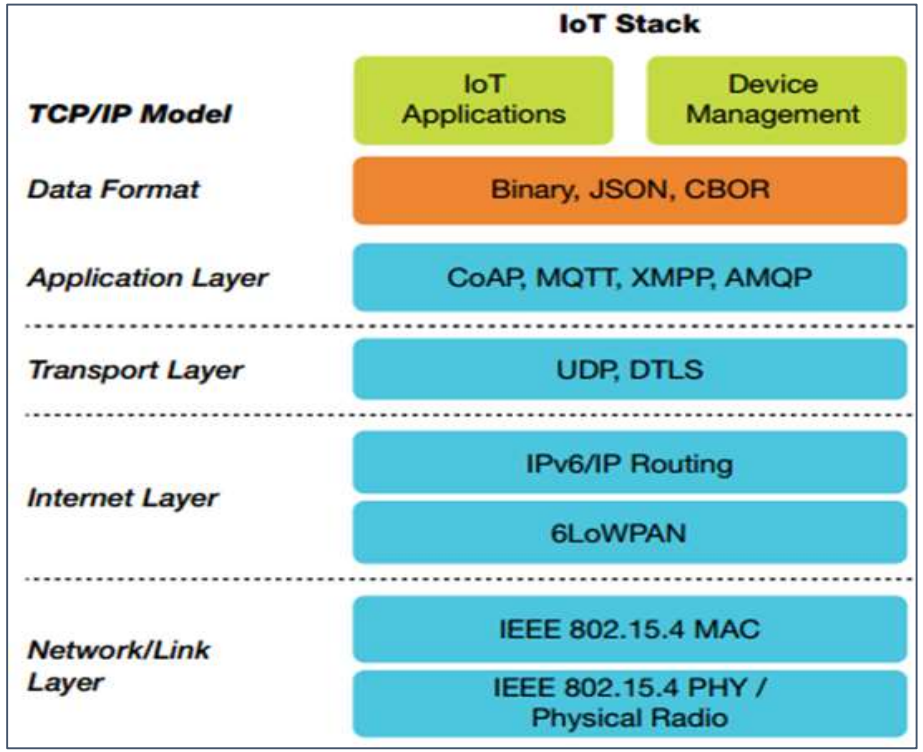


Fig: Protocols in IoT Stack

- Datagram Transport Layer Security (DTLS) provides security for datagram-based applications by allowing them to communicate to prevent eavesdropping, tampering, or message forgery.
- IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) concept is low-power devices with limited processing capabilities should be able to participate on the Internet of Things.

Type of IoT Connectivity Solutions Protocols

- Message Queue Telemetry Transport: MQTT
- Constrained Application Protocol: COAP
- Advanced Message Queuing Protocol (AMQP)
- Extensible Messaging and Presence Protocol (XMPP)

Types of IoT Protocols cont'd

Some of the specialized messaging/data-sharing protocols are often considered for IoT applications

- **MQTT Protocols:** Message Queuing telemetry transport is an ISO/IEC standard, "light weight" messaging protocol and applied as "raw data collectors". It is well-suited to connecting many remote devices to a single server, delivering status at a relatively low rate. It is a broker-reliant publish/subscribe messaging protocol designed to be used with TCP/IP
- **COAP Protocols**: Constrained Application Protocol is a software protocol that was designed to support the connectivity of simple low power electronic devices (wireless sensors) with Internet based systems and also targeted for small low power sensors, switches which are needed to be controlled remotely. The mechanisms for moving data between distributed applications and communicates over the Internet with UDP to work on kilobytes of less microcontroller memory.
- **AMQP Protocols:** Advanced Message Queuing Protocol defines an efficient, binary, peer-to-peer protocol for transporting messages between two network processes (a client and a broker). Features of AMQP are message orientation, queuing, routing, reliability and security.
- **XMPP Protocols:** Extensible Messaging and Presence Protocol (XMPP) is an open community based IoT standard. Software is available in any programming language, Servers, clients, toolkits even browser implementations. XMPP can help build solid, secure and interoperable devices, services and applications for the IoT.

Design Considerations in an IoT System

- Network communication is one of the vital roles in design consideration. The first consideration is the choice of the sensors and the considerations of the specifications in functionalities and capabilities integrated along with the applied sensors and related devices.
- Some IoT application requires low power sensor for a short range. Some sensors use a few hundreds of milliwatt (mW) of power. Data transmission and receiving require a major fraction of the overall power.
- The distance between the sender and receiver is the one of the facts in choosing networking topology. We have to consider on nature of obstacles, interferences, ambient noise, environmental conditions and the regulations.
- For wireless communication, Zigbee, Xbee can be applied in low power IoT design applications and implementations.
- For the citywide applications, we need to choose Sigfox or LoraWAN,etc. Frequency and the power limitations are considerable facts in the design consideration.
- Device protocols and compatibility is another fact to be taken into account in design consideration.
- Creating dashboards of data in application level is required to setup and to provide visualization and monitoring with IoT network frameworks.

Architecture of IoT

The five-layer architecture is applied for the finer aspects integrating various technologies and wide parametric IoT application. It is described in the following figure.

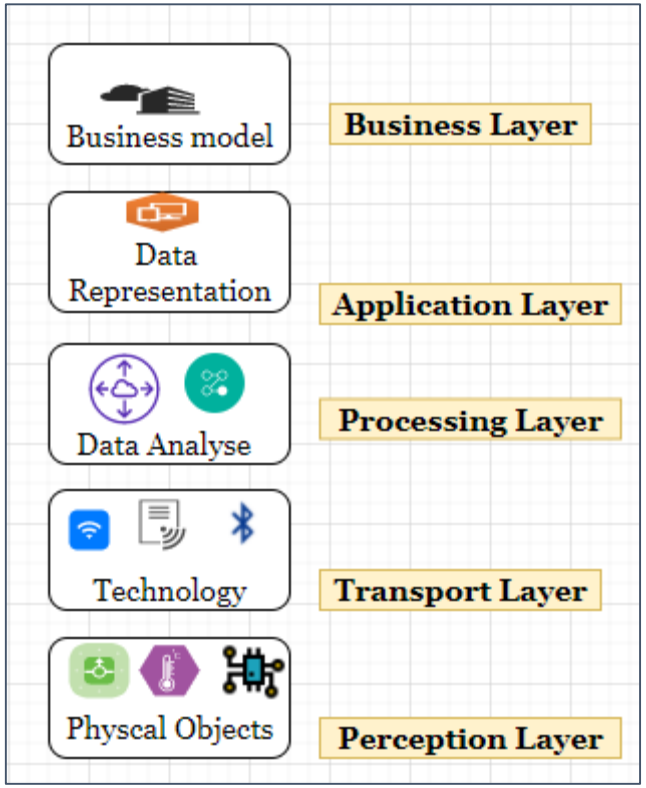


Fig:5-Layer Architecture of IoT

Architecture of IoT cont'd

5-Layer IoT Architecture

The five-layer are perception, transport, processing, application, and business layers . The role of the perception and application layers is the same as three layers architecture.

- **Perception layer** : The first layer of IoT architecture and apply to gather information with the provision of sensors and actuators The main function is to get data from region of interest and to pass data to another layer.
- **Transport layer**: It transfers the sensor data between the perception layer to the processing layer through communication networks .
- **Processing layer** : Middleware layer. It stores, analyzes, and processes data from the transport layer. It can manage and provide services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.
- **Application layer** : It manages all application processes (sending emails, activating alarm, security system,etc.) based on information obtained from middleware layer.
- **Business layer**: It manages the whole IoT system, including applications, business and profit models, and users' privacy.

Securing the IoT Data Network

Most of the IoT applications applied wireless communications in implementation of the ICT infrastructure. The security of wireless environment becomes one of the considerable facts in design consideration of IoT application and environment.

Wireless Network

- They are easy to set up and convenient to use.
- If a wireless network is not properly secured, hacktivist or script kiddies within range can access it and infiltrate the network.
- Many businesses require virtual Private Network (VPN) access into their internal networks if employees are working remotely or are mobile. The employee will be provided with the VPN client, as well as user ID and password information.

Factors that Impact Network Security in the IoT

Some factors that can impact IoT Network security are as follows:

- Non-traditional Location of Devices
- Increasing number of devices
- Lack of Upgradeability

For the protecting devices for malicious traffic we need to do at least the security options of keeping on status for Firewall. It is also a must to update and upgrade the applied OS software, firmware and browser in system.

Securing the IoT Data Network

Exploits and Incidents

❖ **Hardware Exploits**

- Cheap, generic and mass production IoT device implies common vulnerability and will sacrifice security.
- Lightweight HW architecture, less powered device with very limited OS programming couldn't afford complex security measures. Theoretically will be very vulnerable and easy to target.
  Wireless communication devices is ubiquitious, easy to deploy malicious "in the middle" Trojan equipment.

❖ **IoT related Incidents**

Some of the IoT related exploits of incidents are described as follows:

- STUXNET- The original **Stuxnet** malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes.
- Smart Grid- US CRS report:150 attack since 2010-2014
- Health Care- US FDA report:4.5 million record leaks
- Oil rigs- Malware shutdown floating rig vessel computer control system for 19 days.
- Hacker exposed- taking over home appliance devices

Securing the IoT Data Network cont'd

Security Best Practices

- ❖Educate and share ICT as well as IoT knowledge to users
- ❖Use antimalware and software for the devices
- ❖Use advanced router with crypto and security appliances and security monitoring solutions
- ❖Encrypt all sensitive data
- ❖Employ incident response team and test emergency response scenarios
- ❖Configure user role and privilege levels and user authentication
- ❖Periodic update devices with IOS, patches and programs
- ❖Backups data and analysis data recovery from backups

Communication and Challenges

IoT communication is the basis for remote monitoring, data exchange and analytics. IoT is increasingly prevalent at all scales and in all application domains. When goods, machinery, and processes are integrated with the IoT, significant new business opportunities are enabled.

A unique challenge of IoT communication includes security, reliability, and efficiency. Other IoT challenges are privacy, scalability, precision, interoperability, compatibility, mobility, and investment. Challenge in IoT also includes the addressing and identifications, low power communication, apply routing protocol, and high speed and lossless communication. Some of the facts need to be addressed and to check the in pre-processing of the IoT implementations in fog computing are as follows:

- Low Latency: Less time required to access computing or storage resources
- Distributed Nodes: Fog nodes are distributed which provides in the proximity
- Mobility: The smart device can communicate to smart Gateway in the proximity
- Real-time response: Applications with high latency requirements receive real-time response from Fog-nodes
- Interaction with cloud: The data which need high processing is sent to cloud.

LoRaWAN Architecture in Design Consideration

- The LoRaWAN protocols are defined by the LoRa Alliance. For the smart applications LoRaWAN can be designed in the implementation. Data coming from perception-level nodes are collected by LoRaWAN-oriented End Nodes (ENs) and forwarded to a Network Server (NS) by a LoRaWAN Gateway (GW). Collected data are retrieved from the NS in order to feed high-layer modules (the Application Server) and visualize to end users.
- The modulation in LoRa is based on Chirp Spread Spectrum (CSS) deploy with, long range, low power, low bandwidth (250bit/s and 11kbit/s). Gateway is connected to a NS, and finally connected to high-layer applications. In LoRaWAN operations, a LoRa-compliant node must be registered and activated through the NS.
- Gateway is based on a Raspberry Pi, and functionality is running on it. It is designed to allow low-powered devices to communicate with Internet-connected applications over long-range wireless connections. LoRaWAN consists of Processing Unit , Networking Unit, Cooling Unit.

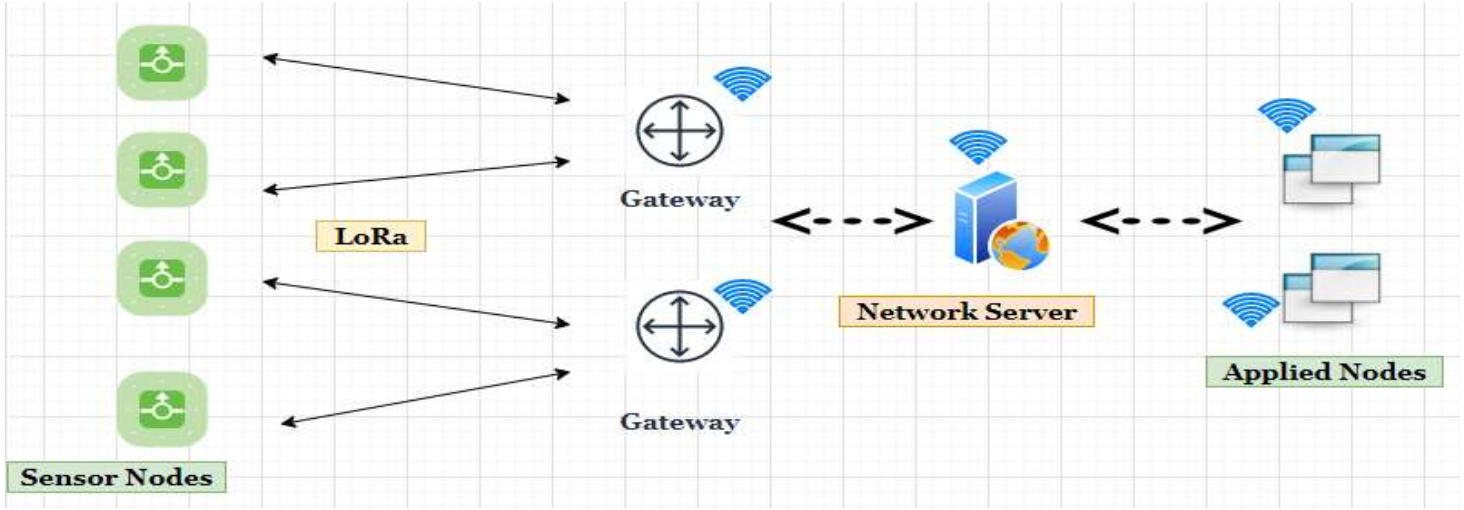


Fig: LoRaWAN Design

LoRaWAN Architecture in Design Consideration

IoT Gateways

- IoT gateways have mainly been used to connect legacy devices that do not have a network interface to connect to a bus system such as Modbus or TCP / IP, to convert signals and media or to carry out simple logic operations. IoT gateway is acting as an intermediate block and enables the strong connectivity between the things and cloud infrastructure or with servers.
- The IoT gateways have modern processors, sufficient capacity of memory RAM, and enough mass storage for a Linux or Microsoft operating system and multiple applications. Connectivity options for wired and wireless networks are included, as are firewalls and other security mechanisms.
- All data from sensors and actuators is securely encrypted from the exit of the IoT gateway. The result is the user who can avoid restrictions in the hardware and software configuration of IoT devices, does not require manufacturer approval for software changes. Users are using IoT gateways as a VPN client to solve insufficient computing power. Some several manufacturers offer a VPN component that can be installed on an IoT gateway with a Linux operating system.

IoT Environment in Agriculture/Farm

- The agriculture/farm industry is looking for new ways to monitor and manage the fields, and optimize resources (money, time and fertilizers). Connected sensors are the ideal solution for this industry.
- Smart agriculture/farm includes all sorts of solutions and devices that can help better manage the environment or that can be used by farmers. Smart farming-oriented domains are improving with IoT technologies using sensors, microcontroller and communication and Cloud platforms. Physical sensors are deployed the agriculture field to get real-time data.
- In the agriculture/farm sector, the impact of temperature, soil condition, humidity, pesticide residues, weather conditions are important parameters. To get the real-time data for those parameters are crucial for analysis data in server and that further helps in improving the quality of the products. In the system, the automated irrigation according to weather conditions can be deployed in the internal cultivation (Green house).
- Wireless Sensor Networks (WSNs) composed of spatially spread sensing nodes can be deployed in distributed in smart farm fields. These nodes can be used to monitor and record environmental conditions. The data are collected by a tens to hundreds or even thousands number of sensor nodes and are gathered by a hop or multi hop connectivity with respect to gateway locations.
- With the one LoRaWAN Gateway which can cover the whole fields and can connect to hundred of sensors as in ambient temperature and humidity sensor, soil electrical conductivity, temperature and moisture sensor, light sensor.

IoT Environment in Agriculture/Farm cont'd

IoT Application Design Consideration

The system manages the considering the facts may include the followings in design.

- Irrigation Pattern changes due to irregular drought
- Moisture content/ minimum moisture requirements.
- Time-domain reflectometry (TDR) soil-water sensors
- Fertigation pattern due to soil change
- Change of Pest pattern due to abnormal biodiversity
- Smart Irrigation system
- Easy Fertigation System
- Pest Monitoring system

IoT Security

- Internet of Things devices are prone to targeted attacks . IoT devices are often developed with very low computing power as a complex system is not necessary to perform most IoT tasks. Many IoT devices consist of a microcontroller, sensors and a GSM module, making it difficult to implement robust device encryption. When an IoT device communicates over the public internet, the unencrypted data it transfers is easily susceptible to attackers. Firewall gateway can provide for secure the internal network access form outsiders.
- Some facts need for security designs are:
  - Hardware security (e.g., device security, embedded SIM options)
  - Traffic path and medium
  - Software (Antivirus, secure cloud storage)
  - Computing Power

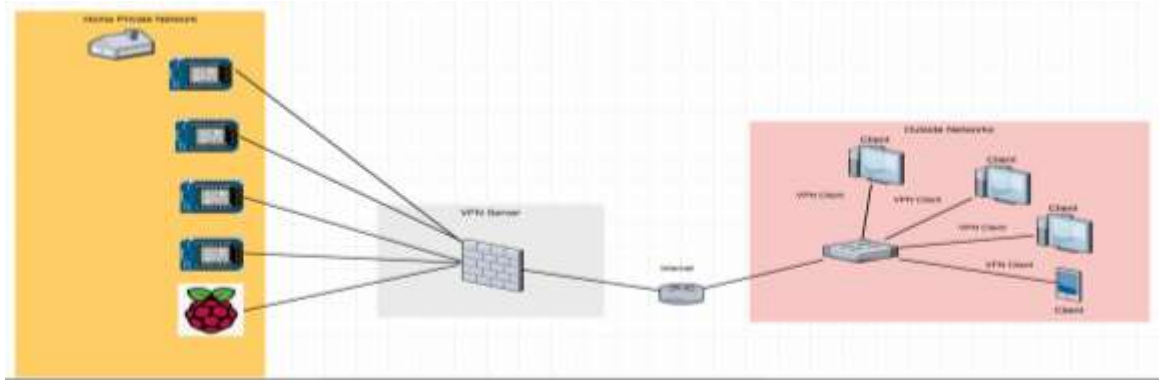


Fig: Security Design in Sample

IoT Security cont'd

Enhance IoT Security and Optimize Data with a VPN

Virtual Private Network is a technology that creates a secure network within the internet to which users and M2M/IoT devices are connected.

- A VPN technology can deploy to mitigate the various risks associated with IoT networks. When a device is connected to a VPN, all of the traffic running to and from it is encrypted. Even if someone were to intercept network traffic, they would be virtually unable to interpret the cipher texts. The drawback of using a VPN is that the encryption is likely to slow overall internet speed, but it overcomes the threat vectors that penetrate the vulnerability of the system, with the connection with a VPN-enabled router.

- A VPN provides a secure connection between a user and an IoT device. Even when data being transferred between you and a device is "sniffed" by a third party, encrypted VPN data only appears as incomprehensible characters. A robust security system is not complete with a VPN alone. Other security measures you should consider as part of a comprehensive solution include:

- By implementing a VPN between the IoT application server, all traffic is fitted with strong encryption before it is sent over the public internet. Additionally, this process is completely transparent for the mobile device and does not require special hardware or any additional configuration on the IoT device itself.

IoT Security cont'd

IPSec and OpenVPN

It is important to secure all remote connections and the monitoring of IoT devices with proven VPN technology.

- IPSec is the highest security VPN, closely followed by OpenVPN.
- IPSec sets up a tunnel from a remote device to a central business server. It is designed specifically for internet traffic and ensures private, secure communication over the public internet by cryptographic security services. IPSec is recommended for large, global enterprises, especially when multiple peers and security layers are in utilized. IPSec requires a static IP address, and technical resources to implement. Larger enterprises are often those with the needs and resources to meet these barriers.
- OpenVPN is an open-source software that utilizes the security protocol SSL/TLS. It has strong feature and is know for ease of implementation. It allows customers to authenticate each other using a pre-shared key. OpenVPN works in a client-server mode, and OpenVPN users connect to the OpenVPN server and from there have full access to the internet. It

IoT Security cont'd

Connect Internet Client to Local IoT Server with Public IP

- For private internal network remote from IoT server, want to access IoT server which stores critical the IoT data stored in IoT , NAT and port forwarding technology can be applied. Information are all stored in private IoT network.
- A Virtual Private Network (VPN) like the OpenVPN can be utilized to prevent attacks that seek to alter or collect your IoT data. While ensuring that only authorized IoT devices can become part of your private network, this VPN employs public networks to provide you private network connectivity away from threats.
- Without a VPN, data is transferred openly through the public internet, and is susceptible to security violations such as eavesdropping, information leakage and hacking. By using a VPN, data are contributing greatly to the safe and reliable operation of M2M and IoT connected devices.

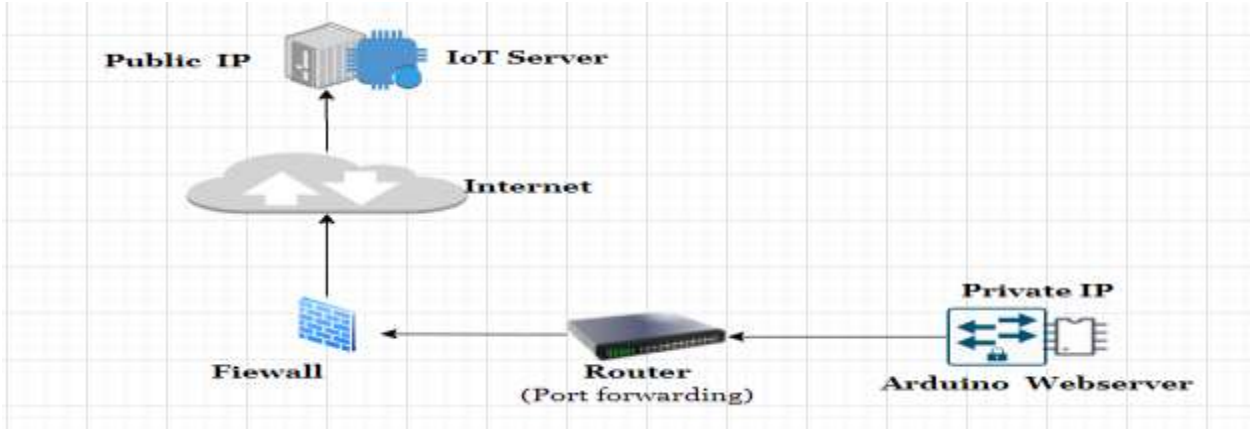


Fig: Port forwarding with NAT Router

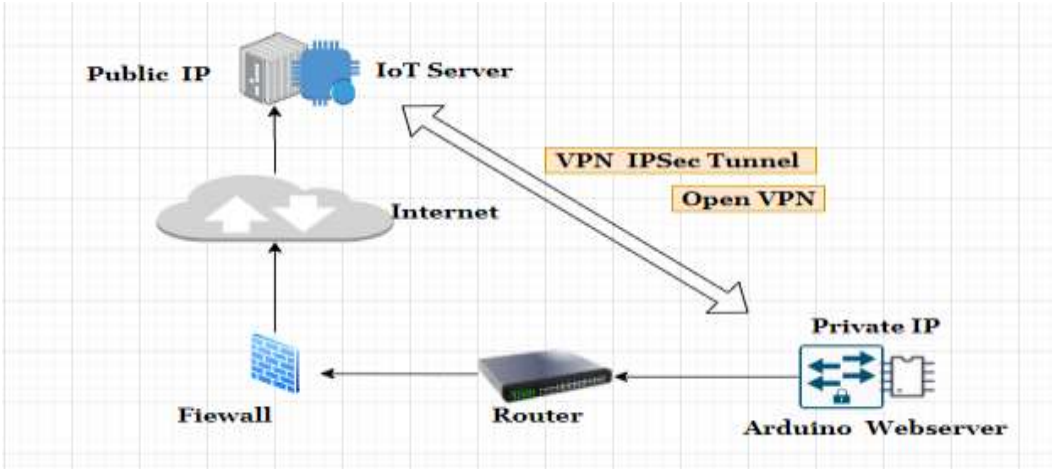


Fig: VPN Tunnel

Smart Environments

Figure depicts the environments that deployed IoT with ICT infrastructures with development of IoT technologies.

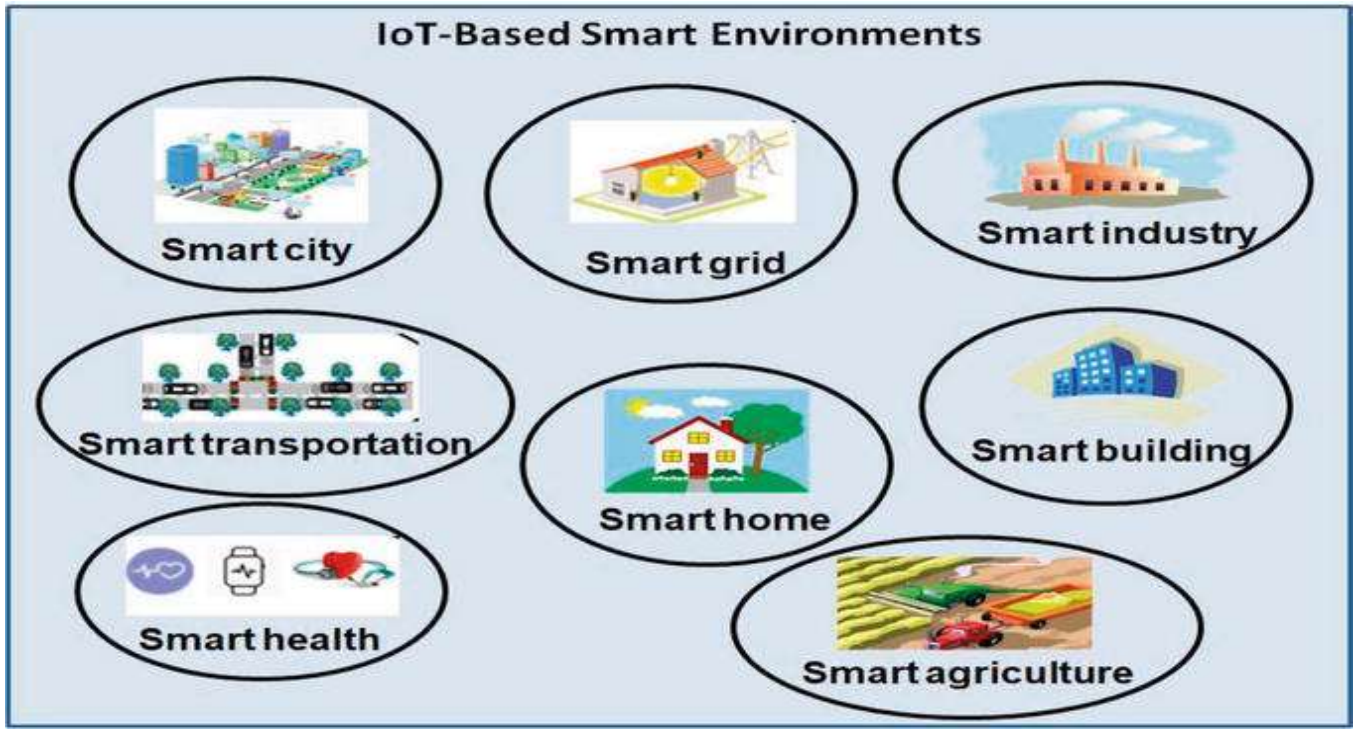


Fig: Some IoT Smart Environments

Smart Environments cont'd

Smart Home Environment

- Many IoT devices including an air conditioner, ceiling fan, coffee maker, and CO detector.
- These devices can be connected to network wirelessly or with a physical cable.
- To connect the devices need a home gateway or registration server.

Two options to connect

- Interact directly with a device or connect remotely over the network using a remote PC, phone, a web browser to the home gateway or registration server. Home Gateway device acts as a local connection to IoT smart devices with Internet and wireless connectivity and provides IoT registration service.

Fig: IoT Sensors Applications in Smart Home

Smart Environments cont'd

Smart Agriculture Field Design

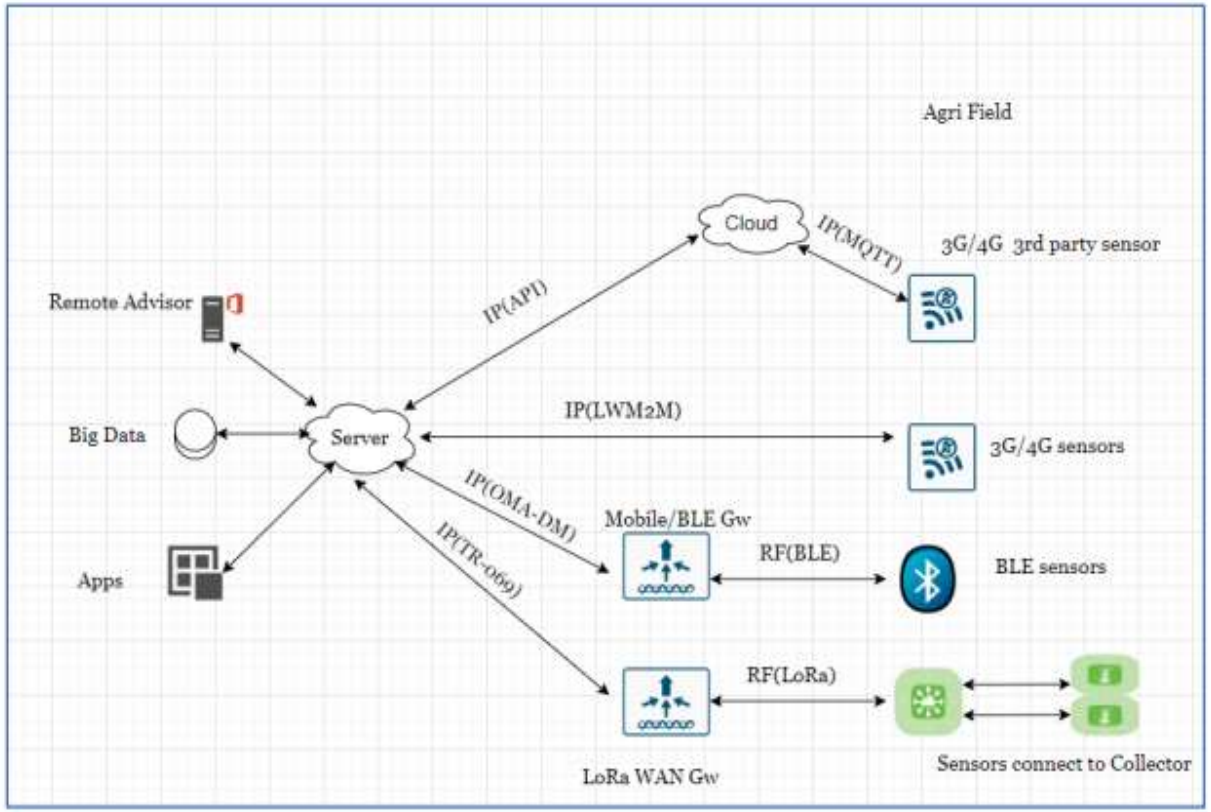


Fig: Smart Farm Design

- For designing IoT system, it is started to find the basic architecture as Perception layer ,Transport layer, and the Application layer.

- **Data Collector can include four modules:**
  - Sensors
  - Servers
  - Tasks
  - Settings
- Arduino, ZigBee, Raspberry Pi 3 and open-source software can apply for framework design.
- This architecture will process real-time data and maximize the delivery of raw data to the cloud for post processing.
- By collecting, forwarding, processing and analyzing relevant data coming from farm processes, IoT-oriented systems allow proper monitoring and management of farm and agricultural production.

Conclusions

- IoT is a region where digital world converges with physical world. The applications of IoT in the agriculture industry has helped the farmers to monitor the water tank levels, soil humidity level and other facts in real-time which makes the irrigation process more efficient.

- With the everchanging landscape of the digitized world, we must stay current in order to realize the full potential of what the IoT has to offer. Internet of Things is envisioned as multitude of heterogeneous devices densely interconnected and communicating with the objective of accomplishing a diverse range of objectives, often collaboratively.

- Information Communication Technology promises a wide range of applications and devices for learning environments, whereas Internet of things is all about connecting devices, making them smart and self-controllable.

- The concern of secure communication is a must in IoT Design considerations as the data and information are private for the organizations. Selecting a robust IoT platform is the first step in the communication.

- The layers architecture is a basic concept and reference for the design considerations of IoT in ICT applications. The technology and the respective protocols are also the main factors in IoT applications. The sensors are deployed with the connection to cloud via IoT network technologies and support decision making for the supervisor to get the real-time data from the sensing devices. It will make the system more effective in analyzing and troubleshooting processes.

Conclusion

- IoT-related technology and their impact on new ICT and enterprise systems. Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices.

- For the IoT design considerations, it is needed to have to determine the number of devices deployed for the facilitation of transmission. The range of communication is also an important facts with indoor or urban area for the signal to propagate with nearest server or gateway. The requirements for these remote IoT devices can include being as power efficient as possible either to extend battery life or to meet green energy goals. The transmitting power and the power source feeding to IoT components is crucial for electrical devices.

- We regard on the environmental considerations for potential hazard and interferences in wireless and wired network for a Network design. The compatibility of the device technology standard and protocols is need to addressed to interoperate with other physical products. With concerning with the main advantages for the users and the organization security or privacy considerations have to be included in design architecture.

References

1. Bilal Javed, Waseem Iqbal, National University of Sciences and Technology"Internet of things (IoT) design considerations for developers and manufacturers", IEEE International Conference on Communications Workshops (ICC Workshops), 2017
2. "Top considerations before starting your IoT design project, Embedded Staff ," https://www.embedded.com/top-considerations-before-starting-your-iot-design-project/, July 10, 2015.
3. ANDREW CAPLES , Manager, Nucleus "Internet of Things (IoT) Design Considerations for embedded connected devices",2014
4. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications",, Volume 2017 , Article ID 9324035, 26 Jan 2017.
5. "Requirements for Testing and Validating the Industrial Internet of Things", Liliana Antão, University of Porto, 11th IEEE Conference, , April 2018.
6. "5 Applications of IoT in Agriculture - Making Agriculture Smarter",. Biz4intellia Inc.019. All Rights Reserved Biz4intellia Inc, 2019.