Research Phase 2 – Internet of Things in General

Smart-Agro

IoT Agricultural Solutions

Digital Labs - Sri Lanka Telecom PLC

Table of Contents

IOT – AN INTRODUCTION

A comprehensive study on IoT, connectivity blocks, communication protocols and standards, Device architecture, security standards and use cases

Introduction

Internet of Things is an expansion to the network based on the internet into the physical world. In an IoT system, physical devices or simply - "Things", are integrated with embedded systems, software, and other technologies to connect and exchange data over the internet. With IoT, the devices that can be connected is not only limited to computers and smart phones but also includes other physical devices such as home appliances, vehicles, industrial machinery or even a simple water valve in a farm plot in one's backyard. IoT is shaping the way that the world functions.

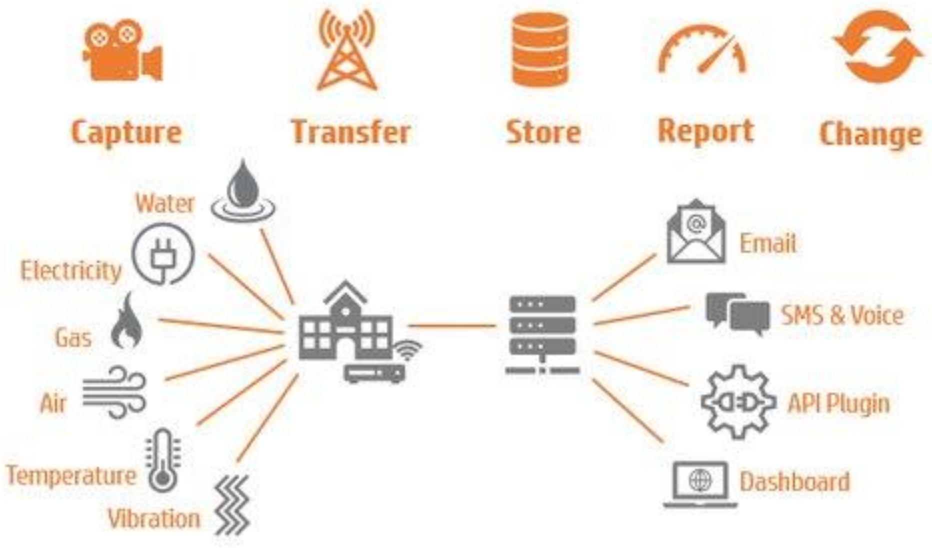
Incorporating IoT to regular operations reduces costs drastically, minimizes waste, improves efficiency and productivity, and creates a variety of opportunities for expansion in every field.

The **growth of IoT** is expected to go through several **stages of development** as:

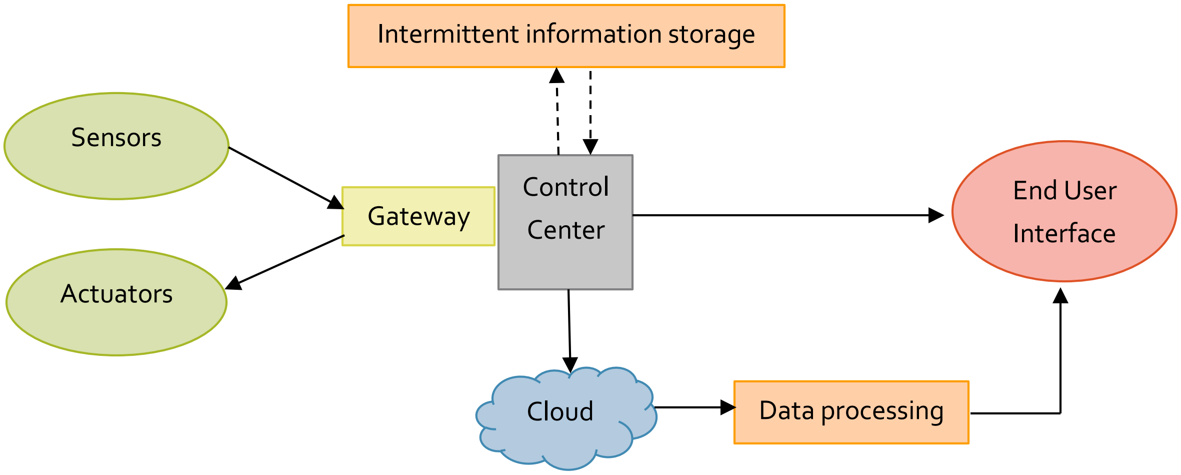
- Passive
- Active
- Aware
- Autonomous

We are currently in a stage between passive and active where sensor data is received from objects and actions are taken either manually or being automated. Aware is a stage where choices could be made based on the received data through analytics. Active involvement of machine learning in IoT is a driving force that could bring the technology to this stage. The autonomous IoT is the era of self-driving cars.

IoT is slowly changing how the world functions. It is transforming many organizations, industries, cities, and societies into a digital age. It is even the basis of the new industrial transformation industry 4.0. It is slowly becoming the global infrastructure for the information age's society. IoT alongside with other game-changing technologies such as AI, cloud computing, big data analytics, block-chain will alter the face of manufacturing, business and infrastructure of the future!



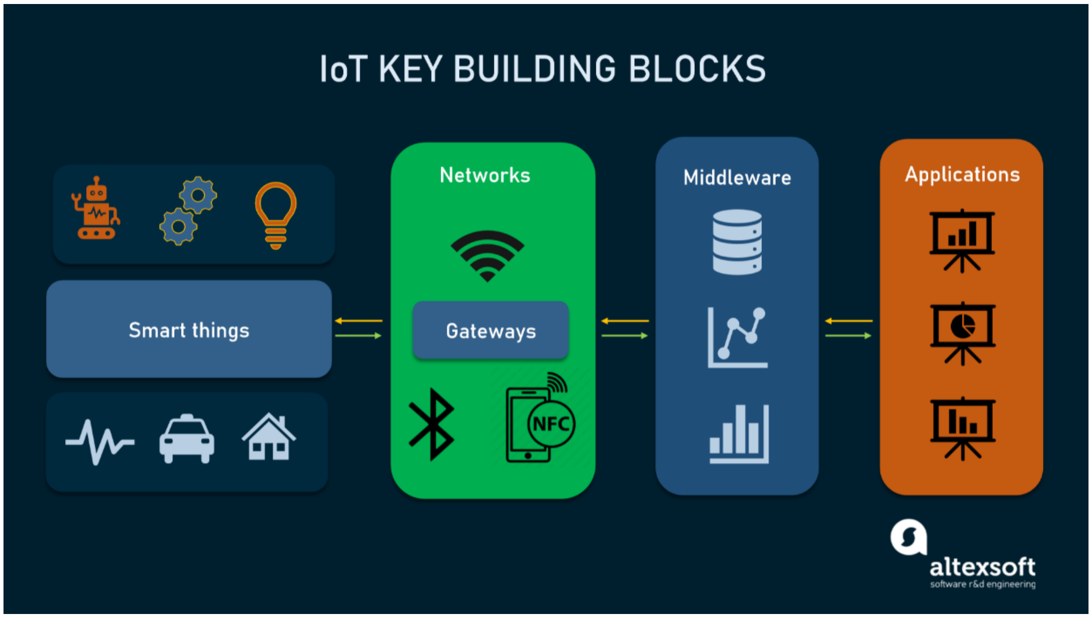
Structure and Components of IoT



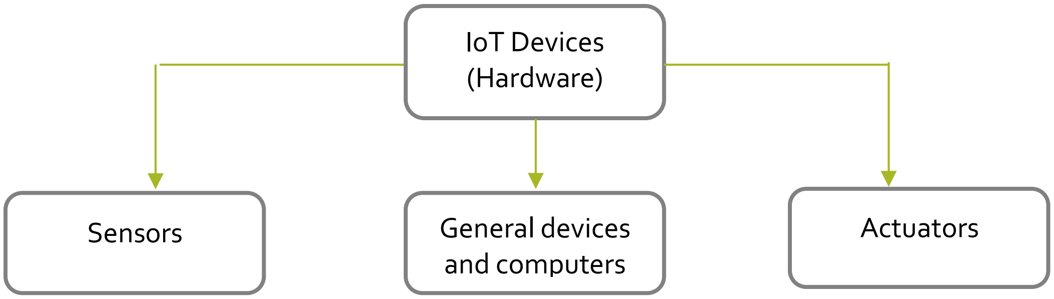
What are the main components of an IoT System?

The **main components** of an IoT system includes:

- The things – sensors, actuators, and general devices
- Connectivity over the internet – Networks and Protocols
- IoT Platforms, cloud/server, End user devices, apps and services



The "Things" – Hardware of IoT



The "Things" or simple IoT devices differ from general in terms of power usage and computational power. They are relatively low cost and low power devices which are task specific.

The devices usually require:

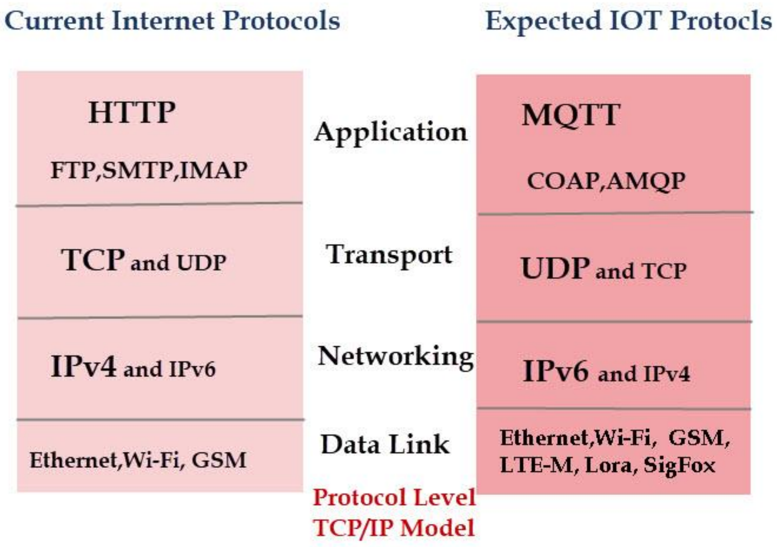
- An embedded processing
- Connectivity either wireless (more popular and convenient) or wired and
- A unique address – Ipv6, IPv4 address

Connectivity – Network and Protocols

IoT is currently being built on the existing network infrastructure and protocols. But major developments in several other network and application protocols have been made to satisfy specific requirements of low power, low energy devices.

General computers rely on Ethernet (wired) or Wi-Fi (Wireless) and mobile phones rely on Wi-Fi or 3G/4G/5G networks. But IoT devices are more varied than this and the characteristics and requirements of these devices are different. They are not only low powered, low cost devices as mentioned above but also have limited processing power and memory. These devices, according to their functionality, operate over a wide variety of ranges.

IoT will mostly run over the existing TCP/IP network and the new IoT protocols replace the existing internet protocols.



Source: http://www.steves-internet-guide.com/

IoT Platforms vs. Custom Dashboards

IoT platforms as opposed to dashboards are third party software while as a dashboard is custom made with its own functionality embedded. Platforms often only contain data visualization, analytics and an administrative center. The user interface cannot be altered or customized.

Amazon Web Services, Azure IoT suite, IBM Watson, Oracle IoT, Google cloud platform are some of the major IoT platforms that can be readily integrated into a project.

Why chose an IoT platform?

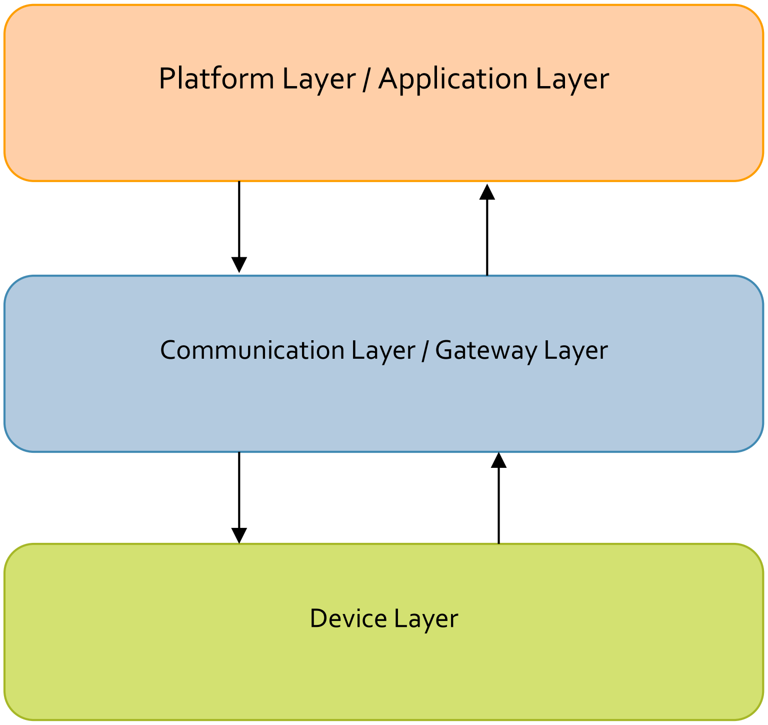
- Instant access
- Less integration time
- Less development cost
- Several Advanced features
- Constant support
- Less inconsistency issues

When to build a custom dashboard?

The main issue with choosing a third-party platform is the lack of control over features and connections. On the other hand a custom dashboard is more customizable, scalable, and secure. Functionality could be changed on demand and they are independent of any company business policies or pricing and payments. But the option of a custom dashboard should only be selected if required capital to invest is available and time could be allocated for development. However development of simple dashboards for small scale companies could be done faster with lesser investment.

IoT Architecture

IoT Architecture Simplified

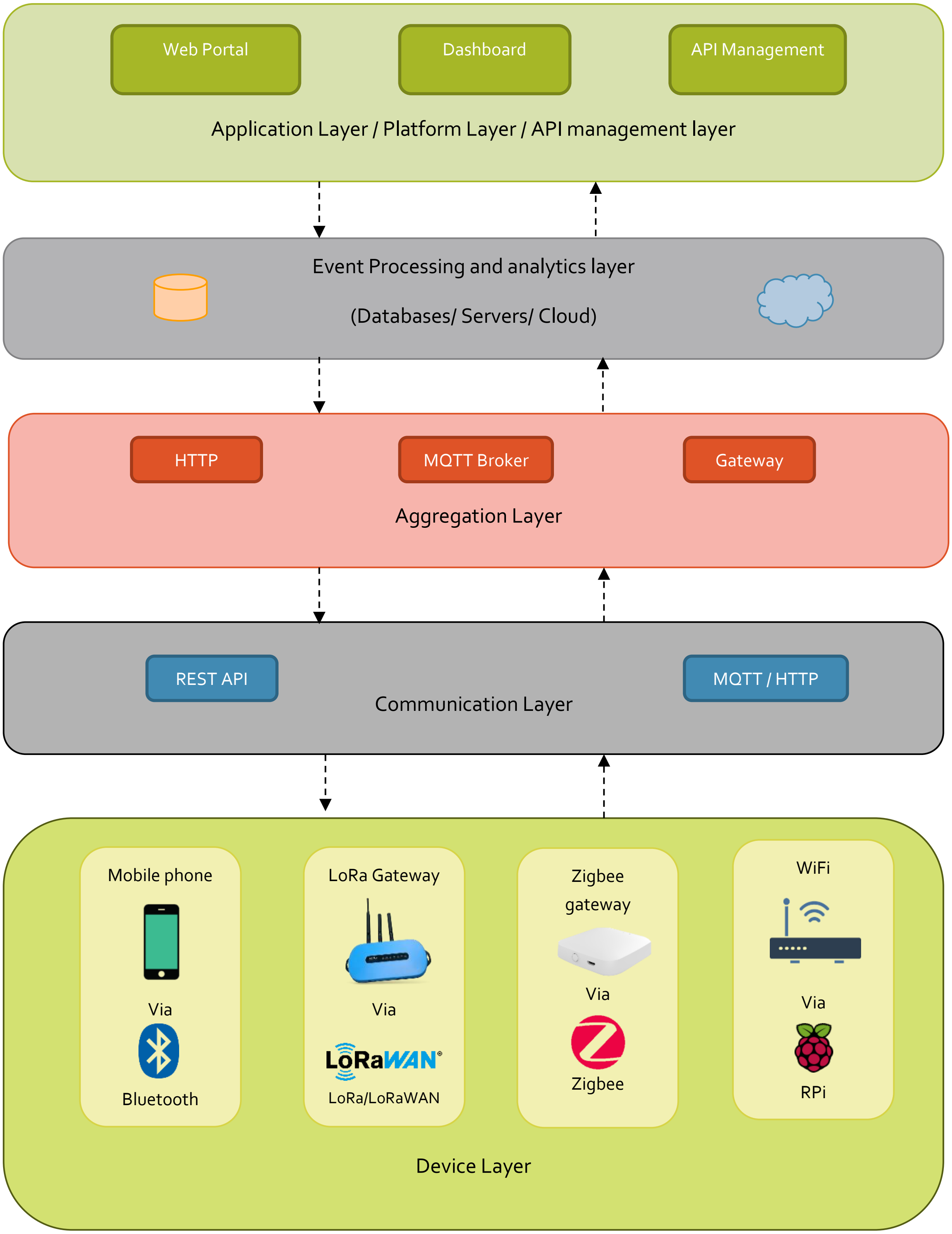


Platform Layer / Application Layer

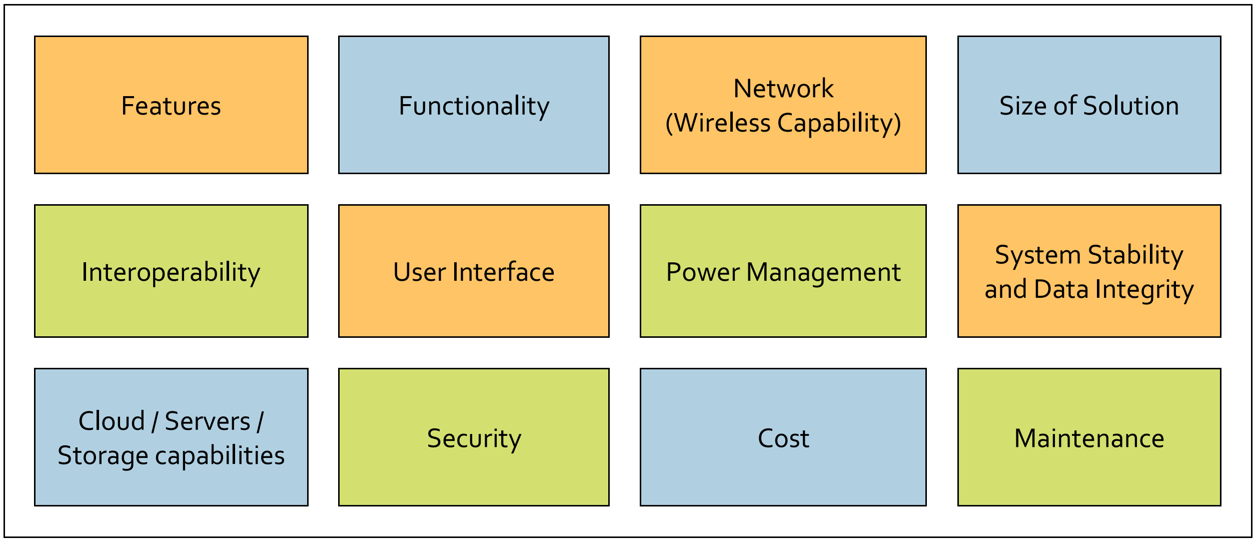
Communication Layer / Gateway Layer

Device Layer

IoT Reference Architecture



IoT Design Considerations



Features	Functionality	Network (Wireless Capability)	Size of Solution
Interoperability	User Interface	Power Management	System Stability and Data Integrity
Cloud / Servers / Storage capabilities	Security	Cost	Maintenance

IoT Security Standards and Best Practices

IoT systems require:

- Necessary authorization and security protocols enabled
- Inbuilt risk assessment systems
- Risk modelling capabilities
- Flexible framework that allows diverse technologies

Best practices for IoT Hardware Security

- Damage Proof, reliable hardware
- Undergone dynamic testing
- Updated on firmware and patches
- Specific data protection algorithms

Best practices for IoT Network Security

- Division of network
- Network authentication and encryption

Other best practices

- Privacy Protection and user authentication

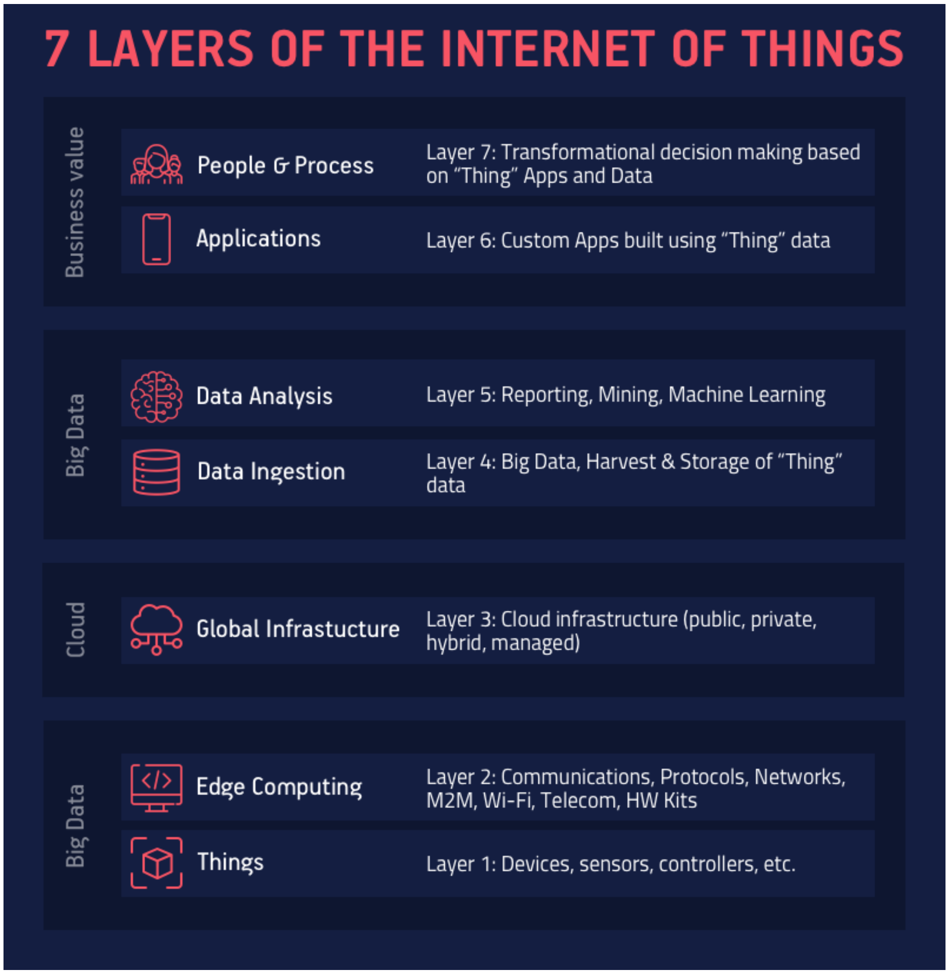
Challenges in IoT

Security is one of the biggest concerns when it comes to IoT. Vulnerability increases when the number of devices increase, due to the lack of standards. IoT is yet to be standardized. Technological inconsistency is the other main challenge. The technology is ever evolving. The industry need to expand among multiple vendors producing different components in IoT that can actually be interconnected with one another, rather than one company producing all components and tech.

Future of IoT

IoT saw a technological boom with the advent of 5G. IoT and 5G are now functioning and being developed as embedded technologies. The following features of 5G paved way for massive leaps in IoT tech.

- Low latency
- Higher bandwidth
- Higher throughput
- Lesser delivery time
- Real time data sharing and predictive analysis



7 LAYERS OF THE INTERNET OF THINGS

Business value	People & Process	Layer 7: Transformational decision making based on "Thing" Apps and Data
	Applications	Layer 6: Custom Apps built using "Thing" data
Big Data	Data Analysis	Layer 5: Reporting, Mining, Machine Learning
	Data Ingestion	Layer 4: Big Data, Harvest & Storage of "Thing" data
Cloud	Global Infrastucture	Layer 3: Cloud infrastructure (public, private, hybrid, managed)
Big Data	Edge Computing	Layer 2: Communications, Protocols, Networks, M2M, Wi-Fi, Telecom, HW Kits
	Things	Layer 1: Devices, sensors, controllers, etc.

Source: https://www.mobindustry.net/