Unit: 4

Internet of Things (IoT) Enabling Technologies

- **IoT(internet of things) enabling technologies are**
1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

1. Wireless Sensor Network(WSN) :

A **WSN** comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.

Example –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

2. Cloud Computing :

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.

With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.

Characteristics –

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service
5. Pay-per-use

Provides different services, such as –

- **IaaS (**Infrastructure as a service**)**
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.
  Ex : Web Hosting, Virtual Machine etc.
- **PaaS (**Platform as a service**)**
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it

provides a platform to develop applications.
Ex : App Cloud, Google app engine

- **SaaS (**Software as a service**)**
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.
  SaaS Applications are sometimes called web-based software on demand software or hosted software.
  SaaS applications run on a SaaS provider's service and they manage security availability and performance.
  Ex : Google Docs, Gmail, office etc.

3. Big Data Analytics :

It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.
Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.
Several steps involved in analyzing big data –

1. Data cleaning
2. Munging
3. Processing
4. Visualization

Examples –

- Bank transactions
- Data generated by IoT systems for location and tracking of vehicles
- E-commerce and in Big-Basket
- Health and fitness data generated by IoT system such as a fitness bands

4. Communications Protocols :

They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network.
Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.
They are used in

1. Data encoding
2. Addressing schemes

5. Embedded Systems :

It is a combination of hardware and software used to perform special tasks.
It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).
It collects the data and sends it to the internet.
Embedded systems used in
Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries.

RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building.

Uses

RFID systems use radio waves at several different frequencies to transfer data. In health care and hospital settings, RFID technologies include the following applications:

- Inventory control
- Equipment tracking
- Out-of-bed detection and fall detection
- Personnel tracking
- Ensuring that patients receive the correct medications and medical devices
- Preventing the distribution of counterfeit drugs and medical devices
- Monitoring patients
- Providing data for electronic medical records systems

The FDA is not aware of any adverse events associated with RFID. However, there is concern about the potential hazard of electromagnetic interference (EMI) to electronic medical devices from radio frequency transmitters like RFID. EMI is a degradation of the performance of equipment or systems (such as medical devices) caused by an electromagnetic disturbance.

Because this technology continues to evolve and is more widely used, it is important to keep in mind its potential for interference with pacemakers, implantable cardioverter defibrillators (ICDs), and other electronic medical devices.

Physicians should stay informed about the use of RFID systems. If a patient experiences a problem with a device, ask questions that will help determine if RFID might have been a factor, such as when and where the episode occurred, what the patient was doing at the time, and whether or not the problem resolved once the patient moved away from that environment. If you suspect that RFID was a factor, device interrogation might be helpful in correlating the episode to the exposure. Report any suspected medical device malfunctions to MedWatch, FDA's voluntary adverse event reporting system.

FDA Actions

The FDA has taken steps to study RFID and its potential effects on medical devices including:

- Working with manufacturers of potentially susceptible medical devices to test their products for any adverse effects from RFID and encouraging them to consider RFID interference when developing new devices.
- Working with the RFID industry to better understand, where RFID can be found, what power levels and frequencies are being used in different locations, and how to best mitigate potential EMI with pacemakers and ICDs.
- Participating in and reviewing the development of RFID standards to better understand RFID's potential to affect medical devices and to mitigate potential EMI.
- Working with the Association for Automatic Identification and Mobility (AIM) to develop a way to test medical devices for their vulnerability to EMI from RFID systems,.
- Collaborating with other government agencies, such as the Federal Communications Commission (FCC), the National Institute for Occupational Safety and Health (NIOSH) and the Occupational Safety and Health Administration (OSHA) to better identify places where RFID readers are in use.

Introduction of ZigBee

- ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the network. As we know that ZigBee is the Personal Area Network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.

  ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. Flow or process control equipment can be place anywhere and still communicate with the rest of the system. It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve.

  IEEE802.15.4 developed the PHY and MAC layer whereas, the ZigBee takes care of upper higher layers.

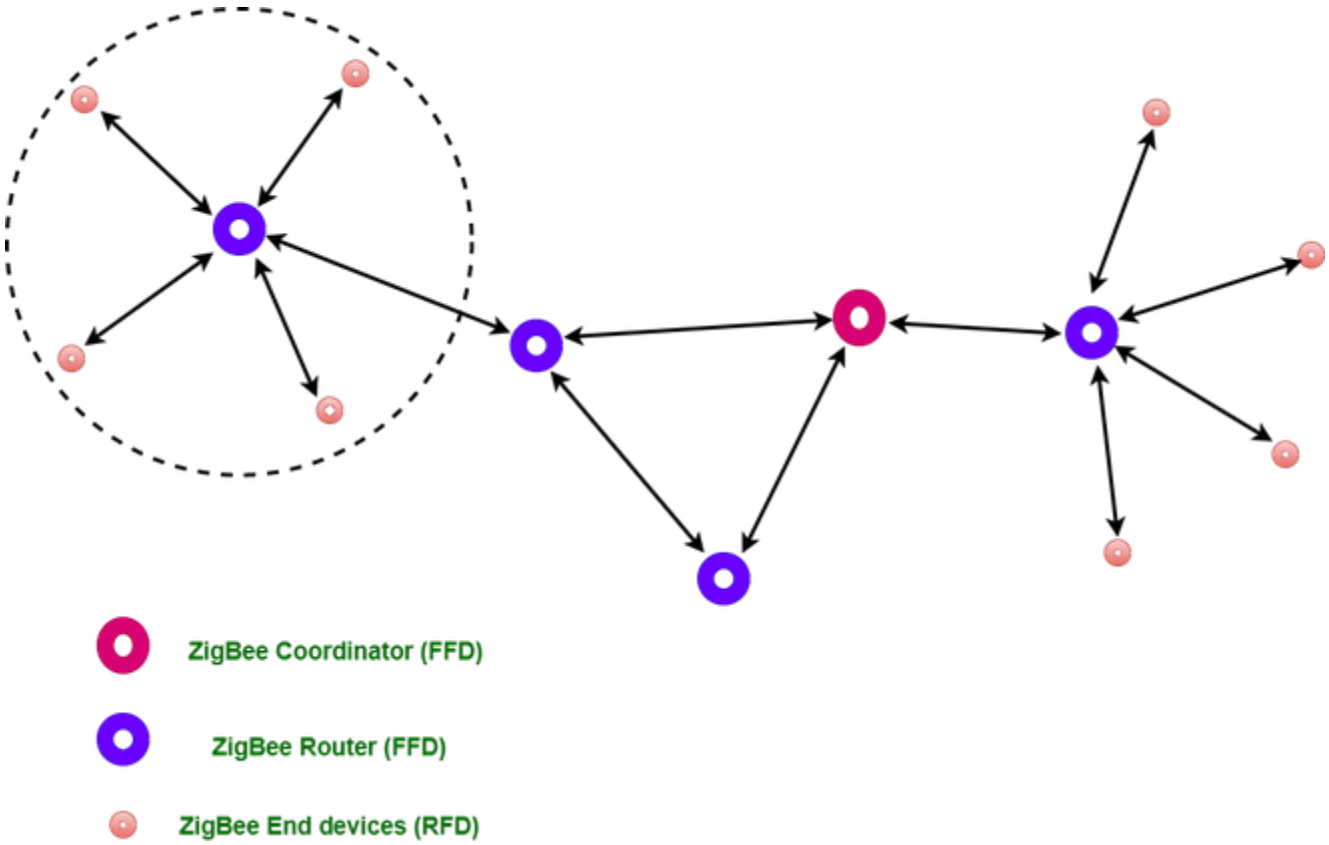
  ZigBee is a standard that addresses the need for very low-cost implementation of Low power devices with Low data rates for short-range wireless communications.

  IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree. ZigBee-compliant devices are sometimes specified as supporting point-to-point and point-to-multipoint topologies.

  Why another short-range communication standard??

Types of ZigBee Devices:

- **Zigbee Coordinator Device:** It communicates with routers. This device is used for connecting the devices.
- **Zigbee Router:** It is used for passing the data between devices.
- **Zigbee End Device:** It is the device that is going to be controlled.



General Characteristics of Zigbee Standard:

- Low Power Consumption
- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)
- Extremely low-duty cycle.
- 3 frequency bands with 27 channels.

Operating Frequency Bands (Only one channel will be selected for use in a network):

1. **Channel 0**: 868 MHz (Europe)
2. **Channel 1-10**: 915 MHz (the US and Australia)
3. **Channel 11-26**: 2.4 GHz (Across the World)

Features of Zigbee:

1. Stochastic addressing: A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents node don't need to maintain assigned address table.
2. Link Management: Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.

3. Frequency Agility: Nodes experience interference report to channel manager, which then selects another channel
4. Asymmetric Link: Each node has different transmit power and sensitivity. Paths may be asymmetric.
5. Power Management: Routers and Coordinators use main power. End Devices use batteries.

Advantages of Zigbee:

1. Designed for low power consumption.
2. Provides network security and application support services operating on the top of IEEE.
3. Zigbee makes possible completely networks homes where all devices are able to communicate and be
4. Use in smart home
5. Easy implementation
6. Adequate security features.
7. **Low cost**: Zigbee chips and modules are relatively inexpensive, which makes it a cost-effective solution for IoT applications.
8. **Mesh networking:** Zigbee uses a mesh network topology, which allows for devices to communicate with each other without the need for a central hub or router. This makes it ideal for use in smart home applications where devices need to communicate with each other and with a central control hub.
9. **Reliability:** Zigbee protocol is designed to be highly reliable, with robust mechanisms in place to ensure that data is delivered reliably even in adverse conditions.

Disadvantages of Zigbee :

1. **Limited range:** Zigbee has a relatively short range compared to other wireless communications protocols, which can make it less suitable for certain types of applications or for use in large buildings.
2. **Limited data rate:** Zigbee is designed for low-data-rate applications, which can make it less suitable for applications that require high-speed data transfer.
3. **Interoperability:** Zigbee is not as widely adopted as other IoT protocols, which can make it difficult to find devices that are compatible with each other.
4. **Security:** Zigbee's security features are not as robust as other IoT protocols, making it more vulnerable to hacking and other security threats.

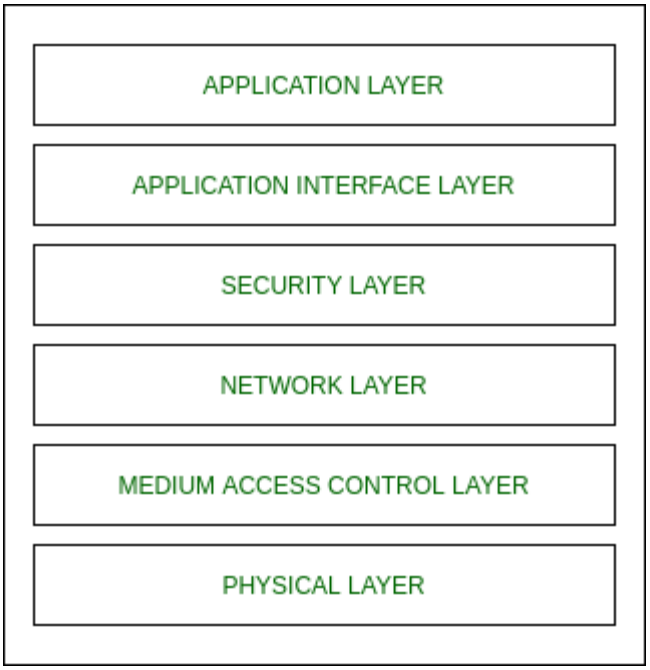
Zigbee Network Topologies:

- **Star Topology** (ZigBee Smart Energy): Consists of a coordinator and several end devices, end devices communicate only with the coordinator.
- **Mesh Topology** (Self Healing Process): Mesh topology consists of one coordinator, several routers, and end devices.
- **Tree Topology**: In this topology, the network consists of a central node which is a coordinator, several routers, and end devices. the function of the router is to extend the network coverage.

Architecture of Zigbee:

Zigbee architecture is a combination of 6 layers.

1. Application Layer
2. Application Interface Layer
3. Security Layer
4. Network Layer
5. Medium Access Control Layer
6. Physical Layer



- **Physical layer:** The lowest two layers i.e the physical and the MAC (Medium Access Control) Layer are defined by the IEEE 802.15.4 specifications. The Physical layer is closest to the hardware and directly controls and communicates with the Zigbee radio. The physical layer translates the data packets in the over-the-air bits for transmission and vice-versa during the reception.
- **Medium Access Control layer (MAC layer):** The layer is responsible for the interface between the physical and network layer. The MAC layer is also responsible for providing PAN ID and also network discovery through beacon requests.
- **Network layer:** This layer acts as an interface between the MAC layer and the application layer. It is responsible for mesh networking.
- **Application layer:** The application layer in the Zigbee stack is the highest protocol layer and it consists of the application support sub-layer and Zigbee device object. It contains manufacturer-defined applications.

Channel Access:

1. **Contention Based Method** (Carrier-Sense Multiple Access With Collision Avoidance Mechanism)
2. **Contention Free Method** (Coordinator dedicates a specific time slot to each device (Guaranteed Time Slot (GTS)))

Zigbee Applications:

1. Home Automation
2. Medical Data Collection
3. Industrial Control Systems
4. meter reading system
5. light control system
6. Commercial
7. Government Markets Worldwide
8. Home Networking

Top Applications of IoT in the World

The most important characteristic of humans is that we can work with each other as a team and gain knowledge from each other. What if this was true for machines as well? What if they could interact with each other and share information and data? That would lead to a truly connected world! And that is the central concept of the **Internet of Things**. This concept just means a connected network of various devices that can collect data and share it with each other to obtain meaningful insights from the data. There are various **applications of IoT** in the world and these are so diverse that you cannot imagine.

Top Applications of IoT in the World

IoT has made our life easier with its applications. You won't believe all the cool stuff IoT can do! Imagine having a home where the lights turn on by themselves, the TV knows your favorite shows, and even the fridge tells you when you're running out of ice cream! Yum!

In big factories, IoT helps machines work together smoothly, like a team of robots! They can even fix themselves when something is not right. Super smart!

And guess what? In hospitals, doctors can use IoT to check on patients from far away. It's like having a superhero doctor with special powers!

All these can be achieved through top IoT applications. So let's see all these **top applications of IoT** in different facets and industries of the world.

1. **Smart Agriculture**

Food is an integral part of life without which we cannot survive. However, it is an unfortunate fact that a lot of food is wasted in developed countries like America while people starve in poorer countries like Chad, Sudan, etc. One way to feed everyone is through better agricultural practices which can be enhanced using IoT applications. This can be done by first collecting data for a farm such as soil quality, sunlight levels, seed type, and rainfall density from various sources like farm sensors, satellites, local weather stations, etc. and then using this data with Machine Learning and IoT to create custom recommendations for each farm that will optimize the planting procedure, irrigation levels required, fertilizer amount, etc. All this will result in better yield or crops with a focus on reducing world hunger in the future. This is done very efficiently by SunCulture, a top IoT application, which is an initiative by Microsoft AI for Earth.

2**. Smart Vehicles**

Smart vehicles or self-driving cars are Iot applications as they can be called are pretty dependent on IoT. These cars have a lot of features that are integrated with each other and need to

communicate such as the sensors that handle navigation, various antennas, controls for speeding or slowing down, etc. Here the Internet of Things technology is critical, especially in the sense that self-driving cars need to be extremely accurate and all the parts need to communicate with each other in milliseconds on the road. Tesla Cars are quite popular and working on their self-driving cars. Tesla Motors' cars use the latest advancements in Artificial Intelligence and the Internet of Things. And they are quite popular as well!!! Tesla Model 3 was the most sold plug-in electric car in the U.S. in 2018 with a total yearly sales of around 140,000 cars. This top IoT application has gained a lot of advancement in recent years

3. **Smart Home**

Maybe one of the most famous applications of IoT is in Smart Homes. After all, who hasn't heard about connecting all the home applications like lighting, air conditioners, locks, thermostat, etc. into a single system that can be controlled from your smartphone? These IoT devices are applications of IoT and becoming more and more popular these days because they allow you complete freedom to personalize your home as you want. In fact, these IoT devices are so popular that every second there are 127 new devices connected to the internet. Some popular ones that you might have heard have, or even have in your home, include Google Home, Amazon Echo Plus, Philips Hue Lighting System, etc. There are also all sorts of other inventions that you can install in your home including Nest Smoke Alarm and Thermostat, Foobot Air Quality Monitor, August Smart Lock, etc. These applications of IoT are getting famous nowadays.

4. **Smart Pollution Control**

Pollution is one of the biggest problems in most of the cities in the world. Sometimes it's not clear if we are inhaling oxygen or smog! In such a situation, IoT applications can be a big help in controlling pollution levels to more breathable standards. This can be done by collecting data related to city pollution like emissions from vehicles, pollen levels, airflow direction, weather, traffic levels, etc using various sensors in combination with IoT. Using this data, Machine Learning algorithms can calculate pollution forecasts in different areas of the city that inform city officials beforehand where the problems are going to occur. Then they can try to control the pollution levels till it's much safer. An example of this is the Green Horizons project created by IBM's China Research Lab.

5**. Smart Healthcare**

There are many applications of IoT in the Healthcare Industry where doctors can monitor patients remotely through a web of interconnected devices and machines without needing to be in direct contact with them. This is very useful if the patients don't have any serious problems or if they have any infectious diseases like COVID-19 these days. One of the most common uses of IoT applications in healthcare is using robots. These include surgical robots that can help doctors in performing surgeries more efficiently with higher precision and control. There are also disinfectant robots that can clean surfaces quickly and thoroughly using high-intensity ultraviolet light (which is pretty useful these days!) Other types of robots also include nursing robots that can handle the monotonous tasks that nurses have to perform for many patients day in and day out where there is little risk to the patients.

6**. Smart Cities**

Cities can be made more efficient so that they require fewer resources and are more energy-efficient. This can be done with a combination of sensors in different capacities all over the city that can be used for various tasks ranging from managing the traffic, controlling handling waste management, creating smart buildings, optimizing streetlights, etc. There are many cities in the world that are working on incorporating IoT applications and becoming smarter such as Singapore, Geneva, Zurich, Oslo, etc. One example of creating smart cities is the Smart Nation Sensor Platform used by Singapore which is believed to be the smartest city in the world. This

platform integrates various facets of transportation, streetlights, public safety, urban planning, etc. using sensors in conjugation with IoT.

7. Smart Retail

There is a way to make shopping even more exciting for customers and that's to use the latest tech like IoT of course! Retail stores can make use of IoT applications in a wide range of operations to make shopping a much smoother experience for customers and also easier for employees. IoT can be used to handle inventory, improve store operations, reduce shoplifting and theft, and prevent long queues at the cashiers. A prime example of this application of IoT is the Amazon Go stores which provide an IoT-enabled shopping experience. These stores monitor all their products using IoT so that customers can pick up any products and just walk out of the store without stopping at the cashier's queue. The total bill amount is automatically deducted from the card associated with the customer's Amazon account after they leave the store.

IoT-based Supply Chains, Smart Grid, and Energy Management

The IoT has revolutionized supply chains, smart grids, and energy management. It helps to improve and fulfill almost all the necessary processes in the aforementioned fields. The benefits are reducing operating costs and improving your company's efficiency. This is also the digital transformation trend of industries. The mass proliferation of IoT devices also brings convenience to users. In particular, this will be a new opportunity for research and development enterprises.

1. IoT-based Supply Chains

IoT devices in the supply chain may be used to track, monitor, authenticate items and shipments using GPS and other technologies. They can also keep track of product and inventory storage conditions, which helps with quality control across the supply chain.

How do IoT-based Supply Chains work?

- **Real-time location-tracking**

Locate goods at any time: IoT devices are attached to products themselves, to raw materials or containers. IoT devices will determine their location through GPS or real-time movement tracking technology.

Solve shipping problems: IoT devices help route planning and goods tracking to determine when and where goods are delayed, possibly due to possible accidents, weather, or other delay-inducing occurrences. This will automatically provide warnings, alternative routes, and contingency planning.

- **Forecast**

Track shipping: make a prediction about the arrival time to help distribution centers, manufacturers and suppliers prepare to receive goods. This ensures the efficient processing of materials and reduces handling times and risks associated with delays.

Handling goods upon receipt: confirm exactly when the goods arrive and can activate the payment service or return the goods.

- **Storage condition monitoring**

Some special products such as chemicals and food need to be stored under the right conditions. IoT devices will monitor factors such as light intensity, humidity, temperature, and other environmental factors. Based on those factors, it will help give warnings if the indicators exceed the threshold.

- **Locate goods in the warehouse**

This is the top warehouse technology trend. Individually label each product on the IoT device, which makes it easy to manage, search and identify the correct products in the warehouse. It also prevents shortages and provides future predictions for the product.

- **Maintenance**

Tracking machine performance metrics gives predictions of breakdowns and any other possible maintenance issues. This helps to provide solutions to prevent problems and prolong the life of the equipment.

Benefits of IoT-based Supply Chains

- **Sustainability**:

is a sustainable technology that helps managers comply with environmental regulations. Thanks to the green IoT sensors, they have a precise picture of the optimal use of energy sources (electricity, water).

- **Transparency**:

real-time location access allows managers to track drivers, ship, and receive goods in the right order.

- **Improved resource management:**

determine possible machine failure, find inefficiencies, predict maintenance and spot detect resource leaks. The IoT camera will monitor and detect defective products and remove them. This helps predict and cut downtime.

- **Automation**:

helps supply chain inventory monitoring, remote control, and warehouse condition monitoring. Automated HR management helps increase resilience, cut costs and increase productivity. IoT devices monitor and issue an alert if the storage condition is unresponsive or there are urgent problems such as a potential fire.

- **Asset management**:

continuous status updates of all assets. By using beacons, RFID tags (active and passive), NFC tags, sensors, internet-connected trackers (using long-range networks or LPWANs) and other technologies that help managers access cargo information,

location, delivery, pickup, user manuals, offer marketing messages, monitor customer traffic, etc) anywhere in the world, even where there is no cellular coverage.

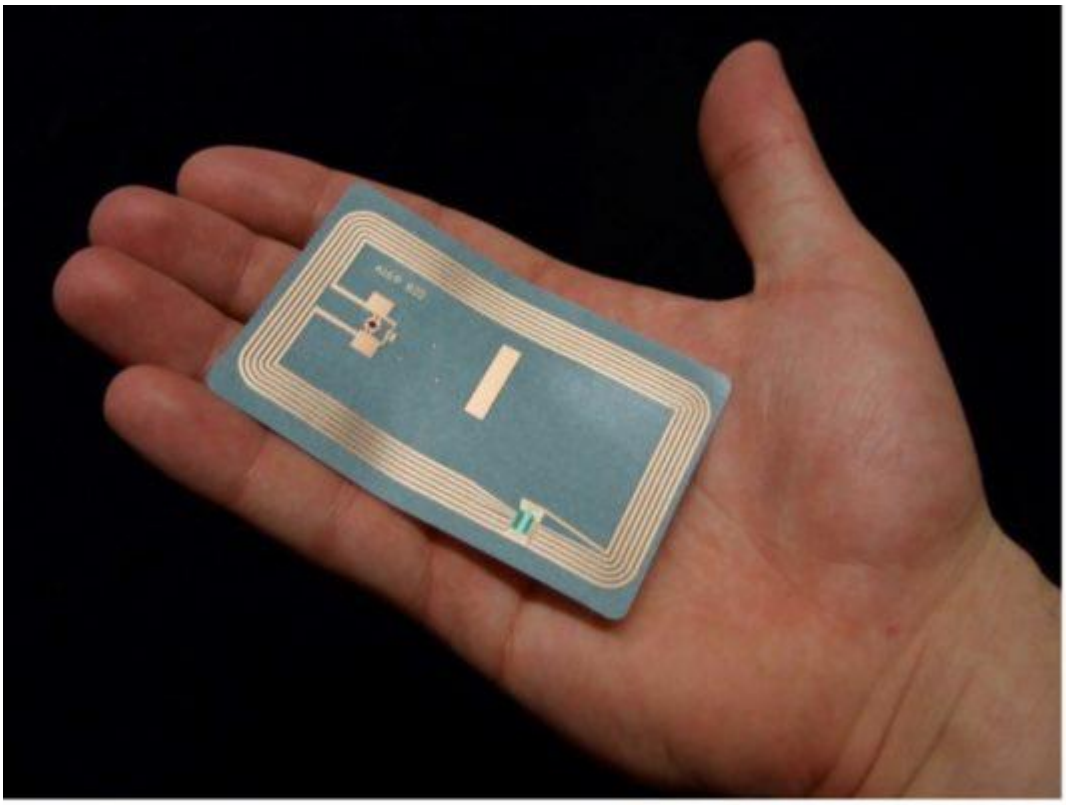


Figure 1: RFID tags *(source: Mọi kích thước | RFID label | Flickr – Chia sẻ ảnh! (flickr.com))*

- **Increased efficiency**:

thanks to green IoT devices will help optimize energy efficiency and savings. As soon as the product is at the source, farmers can use IoT devices to monitor the factors of temperature, humidity, nutrient content in the soil, etc to decide the suitable time to plant and harvest.

- **Better segmentation**:

data about customers, demand, products and the market helps to clearly define the target audience.

- **Improved flexibility:**

the collected data helps to determine the probability that each product can satisfy the market, and how much to enter each supplier's product. Use a backup plan and an alternative if something goes wrong during freight.

- **High accuracy**:

Collected data is stored in the cloud, ensuring it is accessible to all stakeholders, which helps to solve problems quickly and accurately. This data also helps to devise appropriate strategies and anticipate customer needs.

- **High speed**:

IoT tracking technologies and smart route-planning tools help managers accurately locate goods in the warehouse, proactively mitigate delay risks and enable faster decision-making.

Real-life Examples of IoT-based Supply Chains

Amazon uses technology to automatically identify products by scanning QR-codes, and robots for warehouse management.

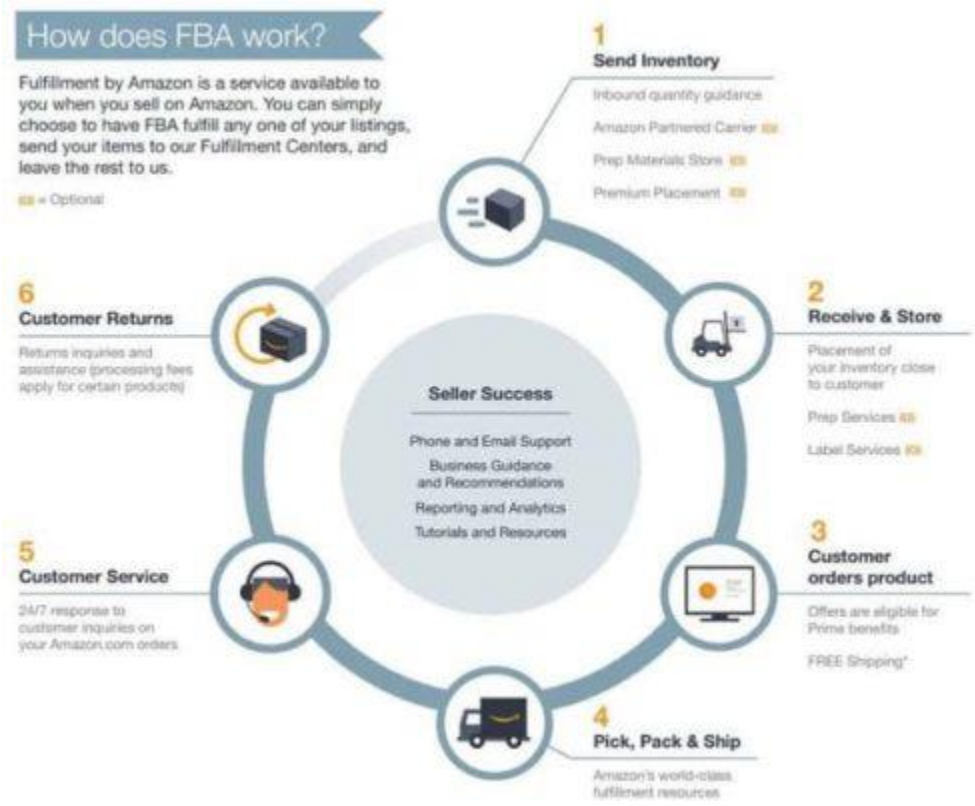


Figure 2: Amazon Supply Chain Strategy Works *(source: How the Amazon Supply Chain Strategy Works (tinuiti.com))*

New Maersk Line: using Remote Container Management System to help monitor humidity and temperature in containers reduces food spoilage. Also, they use real-time tracking and GPS technologies to collect data about the locations of goods.

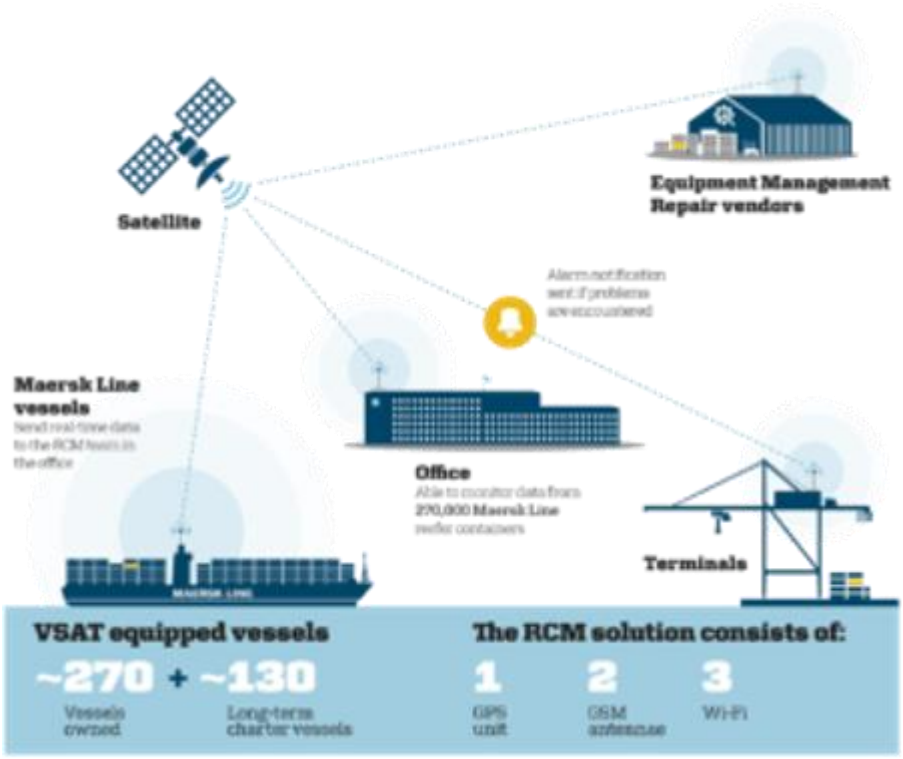


Figure 3: Remote Container Management System *(source: Maersk – reinventing the shipping industry using IoT and blockchain – Technology and Operations Management (hbs.edu))*

Volvo: uses a connected cloud-based system to monitor incoming goods, moving goods, and receiving by distributors.

Farm-to-fork: collect weather data across the UK and analyze soil data to devise a sound strategy for crops and where to place the highest yields.

Figure 4: Farm-to-fork *(source: Farm to Fork Strategy (europa.eu))*

Challenge and Opportunity of IoT-based Supply Chains

- **Connectivity**:

IoT devices need good Bluetooth, Wi-Fi or other connectivity to transmit location to GPS or other IoT devices. It will not work well in an interference environment.

In the future, with the development of 5G, it will be necessary to combine IoT and 5G. This makes the connection better and the bandwidth operates smoothly.

- **Security**:

Bad information security will lead to information leakage to the outside, which will lead to failure and affect the company's image.

Cryptographic hardware monitoring and machine learning limit external network attacks and make access to all data secure.

- **Increased data storage**:

The collected data will be very large. This requires a large power-consuming server to ensure the ability to store and process data.

Data studies are needed to help manage data better, and developing data governance policies are also needed.

- **Skill:**

The process of training employees in-depth skills for using IoT devices and the supply chain is a time-consuming process.

We need experts in the field to come up with a training plan, and at the same time, to analyze and come up with a future development plan because of the rapid development of IoT.

IoT devices serve a specific purpose, so they need to be used correctly. If they are wrong, they will easily be damaged.

2. IoT-based Smart Grid

Existing power networks are being transformed into smart grids in order to satisfy rising power demands. The IoT-based Smart Grid can support transmission, distribution, and consumption of energy, distributed coordination, location awareness, and mobility support.

Overview Smart Grid

A Smart grid refers to a system that combines digital communication with an electricity supply network. It includes the grid, smart homes, and buildings. A Smart Grid helps optimize the electrical needs of buildings and other infrastructures. It allows real-time transmission of electrical data in both directions between the building and the grid. Its benefits are tracking power consumption for enterprises, retail stores, institutions, and industries. In addition, it also detects and prevents leaks and self-repair.

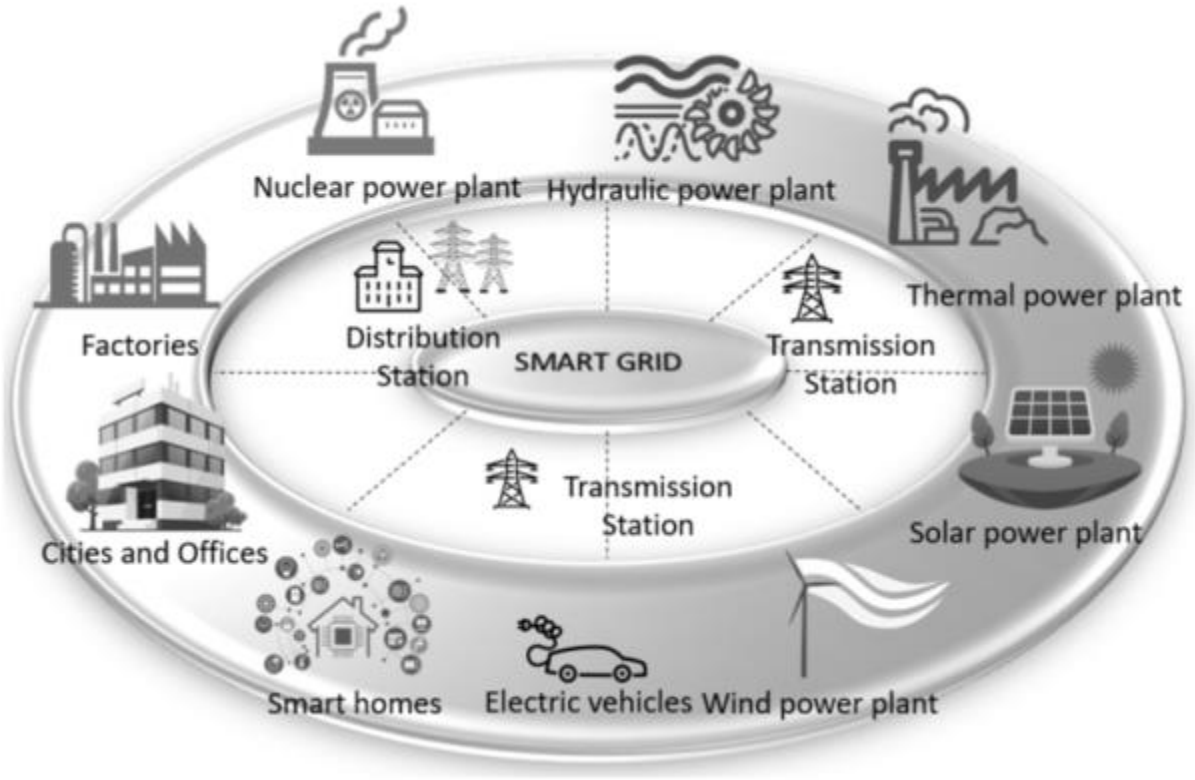


Figure 5: Smart Grid *(source: 02.pdf (irojournals.com))*

What is an IoT-based Smart Grid?

The IoT-based Smart Grid allows sharing of information between all components in the grid and smart energy management over any kind of network, wireless or wired.

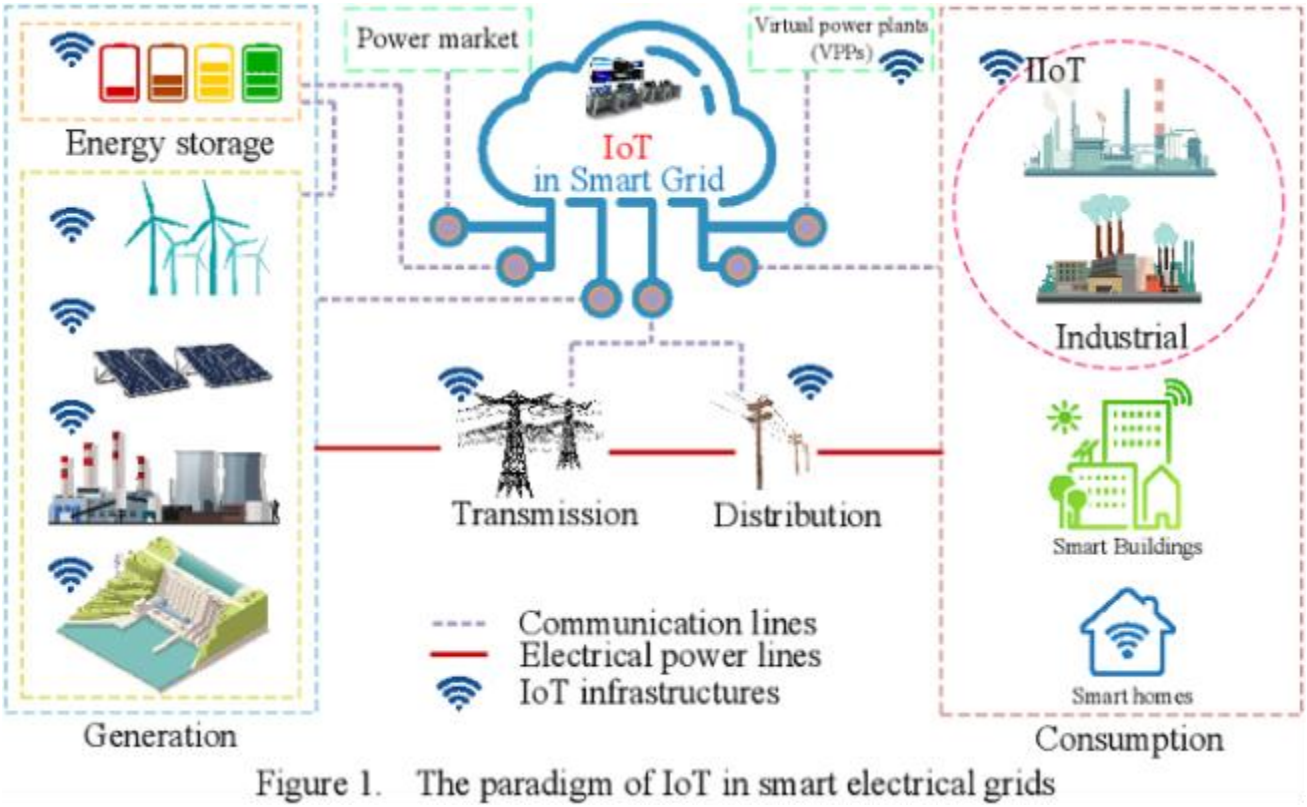


Figure 6: IoT-based Smart Grid *(source: Figure 1 from IoT Architecture for Smart Grids | Semantic Scholar (semanticscholar.org))*

IoT in the generation level

All generations and fluctuations on both the demand and supply sides can be accurately and automatically monitored in IoT-based smart grids, allowing the operator to have more elaborate grid supervision.

In order to improve the performance of the generation sector and maintain the static and dynamic security of the power system, IoT technologies at the generation level deal with the integration of a few energy resources (hydro, nuclear, coal, oil, gas) and renewable energy sources (wind, geothermal, solar, and marine-based energy).

Due to a higher degree of controllability and observability, the deployment of IoT at this level can lead to a higher level of efficiency and performance, which has enormous benefits for power systems.

IoT in transmission level

The transmission level connects the two levels of generating and distribution. This level is an important component of power systems because it guarantees that demand is met reliably. In two ways, IoT integration at the transmission level is critical.

- The first is the role of the IoT in improving congestion management.

- The second point to consider is the influence of the IoT on system security.

IoT in the distribution level

All key locations of the distribution network must be outfitted with IoT technologies as a requirement of a smart distribution grid.

This provides benefits such as remote monitoring and control during unplanned disasters, power loss management, the ability to implement self-healing schemes, the capability to implement emergency demand response programs, detection of problems in low-voltage transmission lines, intelligent control of generation and consumption of energy, and online supervision of the consumption patterns of consumers, etc.

IoT in consumption level

A smart city is an urban region that uses various types of IoT sensors and ICT infrastructures to communicate information that is used to manage assets efficiently and manage resources. The data must be analyzed to control and monitor water supply networks and waste management, electricity generation micro sources, traffic, and affairs corresponding to different energy consumption in a city.

Smart buildings are a crucial part of smart grids. In terms of quantity, residential and commercial customers account for a significant portion of the loads. Many new IoT devices have been developed to aid in boosting efficiency and lowering electricity consumption while maintaining the needed energy of a building. This will change traditional structures, resulting in more efficient, safe, sustainable, and comfortable.

Industrial internet of things (IIoT): industries are classed as sensitive loads, which need a more reliable electricity supply. In this area, power management is quite important. IIoT is described as the use of the internet in industries. IIoT corresponds with the IoT, cognitive computing, cyber-physical systems, and cloud computing. The key principles of IIoT are decentralized decisions, technical assistance, information transparency, and interconnection.

The function of IoT-based Smart Grid

In smart grids, the system response reallocates surplus power to areas where there is a power deficit locally.

Automation: Smart grid software enables consumer-level control and monitoring of energy consumption, helping save energy and money. In the event of an accident on the line or maintenance, a residence might temporarily go off the grid. They may dynamically distribute loads in the house to meet their energy demands, or they can completely rely on the energy they create and therefore be completely self-sufficient.

Reduce emissions and carbon-heavy electricity: It enables green energy. Firstly, it reduces emissions and wasted energy. Secondly, the architecture of a smart grid allows for the integration of renewables into the network, making clean energy sources more

accessible to consumers. The adoption of renewable energy, such as energy from solar panels or windmills, will create a decentralized energy source. Any incident such as terrorism or natural disaster will not lead to widespread power outages and energy shortages.

Cut costs and risks: smart grid technology allows for real-time monitoring and management of energy usage, as well as cost-cutting optimization. Improved visibility of each grid piece enables early detection of any problem, cutting risk and potentially harmful issues such as downtime due to untimely maintenance and outages.

Charging stations and smart storage: this helps to provide power anytime, anywhere. Devices will be fully charged to ensure any long-distance travel, such as travel or long-distance travel.

Real-life Examples of IoT-based Smart Grid

Schneider Electric: provides energy storage and solar systems that can deliver power even in the most extreme weather. The devices enable real-time monitoring and control. In addition, it also allows the use of independent energy sources, combining efficient use with other energy sources. The result is guaranteed energy in the event of a power failure and cost savings.

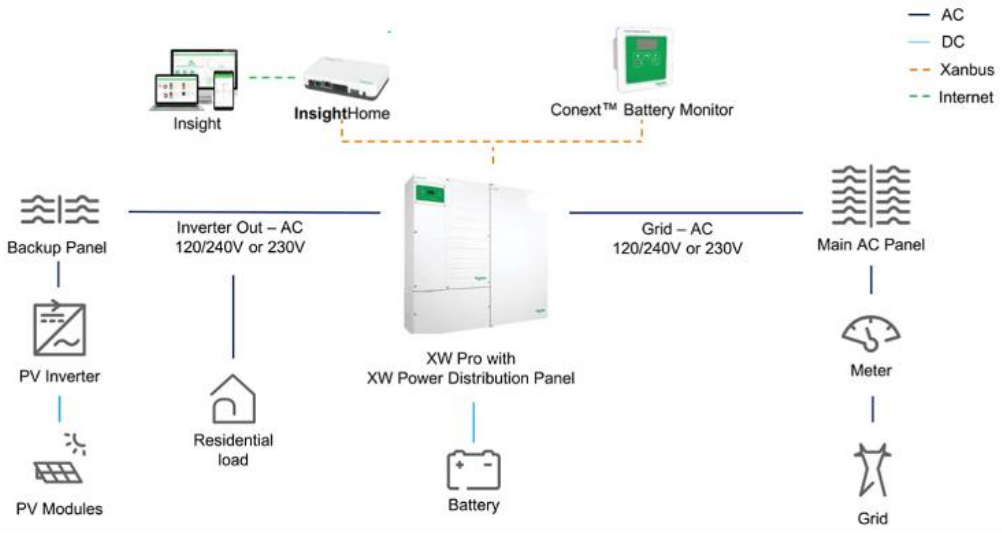


Figure 7: Solution model of Schneider Electric *(source: Residential Grid-Tied Solar with Battery Backup | Schneider Electric Solar (schneider-electric.com))*

Lumin Smart: With data collection tools, the analysis will be provided from which there are reasonable plans to manage and optimize the use of electrical energy.

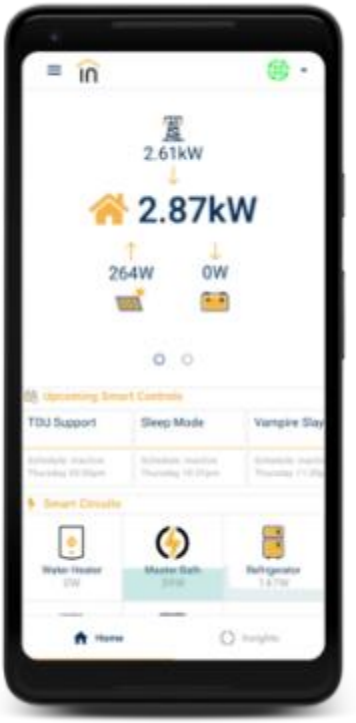


Figure 8: Dashboard of Lumin Smart *(source: Load Management Platform + Hardware | Lumin (luminsmart.com))*

)

Future of IoT-based Smart Grid

Information Security: information management tools and deep packet inspection are solutions to specific information security problems. The use of a wired network is prone to interruptions and failures. Meanwhile, wireless networks are more vulnerable to attacks. This requires improving the security of both networks.

Improve equipment: it is always necessary to avoid electromagnetic interference, temperature changes, dustproof, waterproof and to improve equipment life. A large number of devices are monitored by the grid operator. This needs the employment of big data analytical techniques and improving the smartness of grids.

Connection Stability and Communication: It is critical that systems communicate with one another. This requires a fast internet connection, quick response, and small latency. An effective support technology to solve this problem is cloud storage.

- Power outages are unacceptably inconvenient, so they need an immediate self-healing mechanism. Setting up a wireless network is much simpler than the process of providing connectivity.
- Real-time data analytics and visualization: helps manage data in real-time from the moment the energy is produced to the point it’s consumed by an end-user.

Machine learning and big data: make the system work well with massive datum sets, identifying trends, making predictions.

IoT-based Energy Management

Introduction IoT-based Energy Management

IoT devices help manage energy efficiently and economically. There are many ways to IoT-based Energy Management, such as device automation, M2M, cloud-server.

IoT-based Energy Management is the control and management of IoT devices to help save energy, optimize resource usage, control device usage accordingly, improve process automation, management, prediction, notify and automatically correct potential hazards by deploying networks of smart, connected assets and devices that are connected, continuously collecting, sharing, and analyzing data.

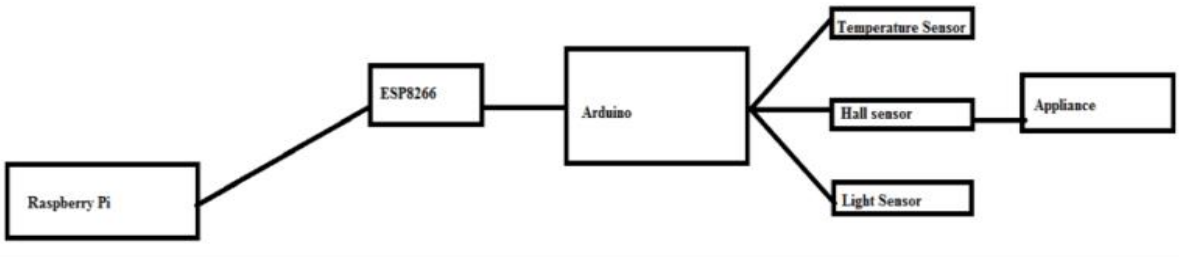


Figure 10*: A solution model of IoT-based Energy Management*(source: Preparation_Instruction (ripublication.com))

Advantage of IoT-based Energy Management

Anticipate and solve problems: by collecting data, the system will analyze it to make predictions about the possibility of incidents, give warnings, and make plans to solve problems. This helps balance demand and balance overload, solving problems before they happen. If due to sudden impact factors such as natural disasters or terrorism, the system helps to determine the correct location of the incident, the severity, from which it can automatically repair and minimize damage to the lowest level.

Reasonable energy distribution: predicting future energy demand from which to have an appropriate energy distribution plan, for production, industry, or daily activities. This meets the needs of users, sharing data with suppliers to adjust prices accordingly.

Cost reduction: the combination of automation, effective asset maintenance, and streamlined human effort results in a considerable reduction in operational costs. It helps to identify when the load is too high to minimize energy usage.

Automation: improving operational processes to maximize automation, thereby optimizing human potential and reducing labor costs.

Optimize asset maintenance: monitor the condition and performance of machines. It helps reduce wear and tear, increasing the working life of machines.

Green energy: Using more renewable energy sources such as wind and solar energy will help reduce environmental pollution emissions and minimize carbon emissions. It helps to comply well with environmental policies.

Reduce energy spending: Efficient use of energy resources will give energy time to recover.

Real-life Examples of IoT-based Energy Management

Wait time: a non-profit platform that helps users reduce emissions into the environment. Switch to using renewable energy.

Sense: is a smart metering system. It connects to a user-friendly control panel, displaying full information on energy usage status. Users can participate in energy usage management.

Figure 11: Sense Energy Monitor *(source: Sense Energy Monitor – Track Electricity Usage in Real Time and Save Money – Meets Rigorous ETL/Intertek Safety Standards – – Amazon.com)*

WebNMS: Using data from a network of sensors and meters on-site, the system proposes energy-saving methods to improve efficiency and productivity.

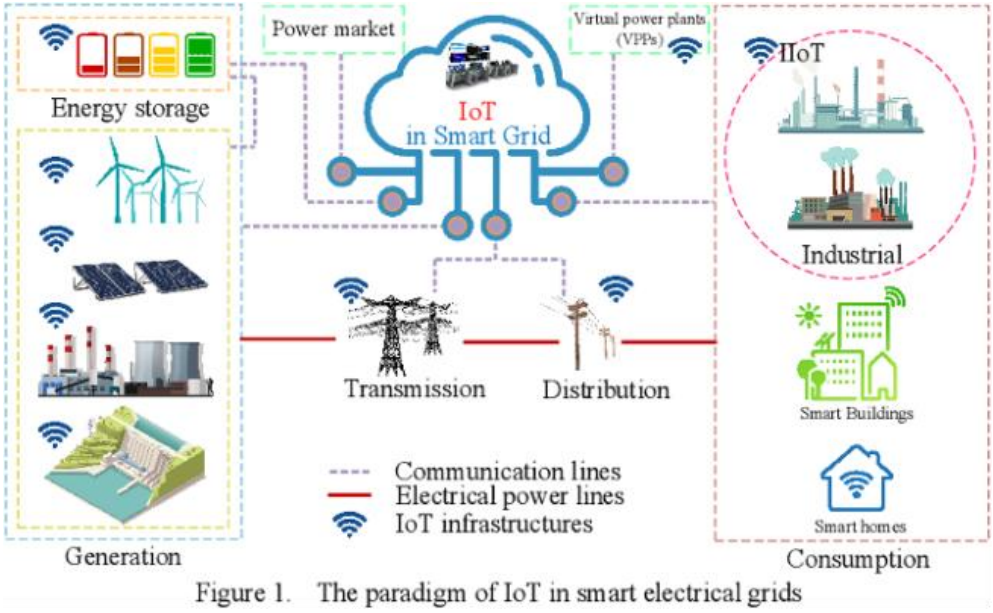


Figure 12: Smart metering solution of WebNMS *(source: Smart metering solution|WebNMS|IoT (webnms.com))*

Future of IoT-based Energy Management

The latest generation of smart lighting, learning thermostats, and sensor-based HVAC systems are meant to automatically maintain ideal conditions in rooms while reducing energy consumption.

In the future, there will be a need for an overall system that connects many devices (analytics tools, applications, controls, meters and sensors, prediction, maintenance) to help individual users, businesses, and communities connect connections to control processes, assets, resources and optimize performance.

Using natural, renewable energy sources to bring green IoT devices to serve a green life significantly reduces costs. Realization of smart farms, green hydrogen

The issue that needs the most attention and development is energy storage. Energy storage ensures that power is always available to the user no matter what happens. This also helps control the surplus, better manage the renewable energy they create and guarantee that their power network performs at its best.

Data analysis: collect, manage, and analyze data based on the development trends of IoT, AI, edge, and cloud technology. Build a big data map of energy use.

Distributed energy: blockchain-based development for connection, sharing, and data transparency

How the Cloud Will Change Operating Systems

Cloud with Operating System : Operating systems allow users to run programs, store and retrieve data from one user session to next. Through virtualization, most server operating systems now support and will continue to support hypervisors that allow multiple (and possibly different) operating systems to run simultaneously. Virtualized servers will continue to play huge role in driving operations of cloud. Many organizations are opting for on-demand model operating systems, in which servers download user's operating system applications and environment settings to any computer user logs in to. With the advent of more programs that run within browser, there may be much less need for powerful desktop operating systems, such as Windows and Mac Os.
Cloud with Internet of Thing :

1. Cloud-based location-tracking applications – A location-tracking application utilizes data from Global Positioning System (GPS) capabilities built into mobile devices to integrate individuals' location into processing it performs. As GPS capabilities are built into more devices, applications will begin to deliver more location – tracking solutions. Using cloud and location-tracking solutions, you will be able to track not only packages you ship, but also stolen cars, lost luggage, misplaced cell phones, missing pets, and more. **2. Cloud-based smart fabrics and paints –** Ability to connect devices to cloud from any place, at any time will open door to wide range of cutting-edge applications. Devices that once had to be read by utility or city employees, such as electric meters and parking meters, will connect to web and create report. Intelligence will be built into fabrics of our clothes, bedding, and furniture. These intelligent fabrics will provide wide range of services including following :

- Automatically adjust room temperature when body temperature becomes too warm or too cold.
- Notify rooms when we enter or leave so that lights, music, and other devices are automatically controlled.
- Monitor body functions such as blood pressure, blood sugar levels, stress, and more, and notify person and adjust environment to affect those functions.
- Notify others when elderly person has fallen.
- Provide deterrence against mosquitoes and other insects.

Similarly, new paints being developed change form based on environmental conditions. Currently, paints can change color on roads to indicate presence of ice. In the future, intelligent paint may report driving conditions back to cloud.

3. **Cloud TV –** Few companies are changing way consumers watch TV. With greater bandwidth available everywhere, DVD's have fallen by wayside. TV viewers will not just watch shows on-demand in their homes, in their cars, and on airplanes but also new breed of projection devices will make any flat surface TV screen.

4. **4. Cloud-based smart devices –** Cloud's ability to provide internet access and at any time makes such processing reality. Some devices may initially be intelligent with reference to their ability to regulate power consumption, possibly avoiding power use during peak times and costs. Using the cloud for communication, devices can coordinate activities. For example, your car may notify your home automation system that you are down blocking and instruct it to

light house, turn on your favorite music and prompt refrigerator for list of ready to cook meals.

5. **Home based Cloud Computing :** Today most households have wireless network capabilities that allow family members to connect to Web and access sites and contents they desire. With arrival of smart devices, intelligent fabrics, and greater use of frequency identification devices (RFID), relations will expect on-demand personalized technology solutions. Families will use cloud devices to customize their environments and experiences. Within such environment, families will want to restrict processing to within home, meaning that they will not want neighbors to receive signals generated by their devices and clothing. That implies ability to encrypt wide range of signals within home. To that end, you should expect to see cloud-based in-home devices that store family files, maintain appliance settings. download and store movies and TV shows, and more.

6. Modular Software : With cloud computing, companies no longer have to raise capital required to fund large data center. Instead, they can leverage PaaS solution. Furthermore, companies no longer have to pay expensive licensing fees for various software tools such as database management systems. Instead, they can leverage pay-on-demand solutions. Hence developers will release software solutions at faster rate, bringing solutions to market that expects high functionality and demands lower cost. 85% Software developed since 2012 is cloud-enabled and increase in future data requirements will enable more services through Cloud. All-State and Center will have its own Cloud Platform for providing basic services in health, agriculture and social, etc. Aadhaar Card is major example of Cloud Computing projects and all banking platforms are moving towards serving 7 billion people in world. All Stock exchanges have to move towards cloud computing to provide efficient and real-time stock details

What is Home Based Cloud Computing?

Home cloud computing is the process of using a remote server to store, manage and access data and applications from home. It allows users to access their files, applications, and other digital content from any device with an internet connection, whether it be a computer, phone, or tablet. Private cloud storage services can also be utilized to store data securely, backing up and safeguarding information in case of emergencies.

A lot of individuals and small businesses use home/private cloud computing to browse, search through files and even work on projects from any device. It’s a great alternative to setting up a server in your house because it eliminates the need for physical storage devices that contain data.

What is Autonomic Computing?

Need Of Autonomic Computing

With the increase in the demand for computers, computer-related problems are also increasing. They are becoming more and more complex. The complexity has become so much that there is a spike in demand for skilled workers. This has fostered the need for autonomic computers that would do computing operations without the need for manual intervention.

Areas Of Autonomic Computing

There are four areas of Autonomic Computing as defined by IBM. These are as follows:

1. **Self-Configuration:** The system must be able to configure itself automatically according to the changes in its environment.
2. **Self-Healing:** IBM mentions that an autonomic system must have property by which it must be able to repair itself from errors and also route the functions away from trouble whenever they are encountered.
3. **Self-Optimization:** According to IBM an autonomic system must be able to perform in an optimized manner and ensure that it follows an efficient algorithm for all computing operations.
4. **Self-Protection:** the IBM States that an autonomic system must be able to perform detection, identification, and protection from the security and system attacks so that systems' security and integrity remain intact.

Characteristics

1. The Autonomic system knows itself. This means that it knows its components, specifications capacity, and the real-time status. It also has knowledge about its own, borrowed, and shared resources.
2. It can configure itself again and again and run its setup automatically as and when required.
3. It has the capability of optimizing itself by fine-tuning workflows.
4. It can heal itself. This is a way of mentioning that it can recover from failures.
5. It can protect itself by detecting and identifying various attacks on it.
6. It can open itself. This means that it must not be a proprietary solution and must implement open standards.
7. It can hide. This means that it has the ability to allow resource optimization, by hiding its complexity.
8. An autonomic system according to IBM must be able to know or expect what kind of demand is going to arise for its resources to make it a transparent process for the users to see this information.

Autonomic Computing (AC) Architecture

The autonomic computing is needed so that it overcomes the problem of the increased complexity of the computing systems that acts to prevent further growth of the systems. There are several predictions with suggesting growth of 38% devices per annum with increased complexity. There is a need for autonomic computing in distributed computing because of the management of the computer networks complexes and a limiting factor in the future development of distributes computing systems.

Mobile computing has brought with it an increased complexity for employee management systems as employees need to access their company's data even when they are not in the office. All such cases of complexity arise a need for autonomic computing as it's better than manual computing that is erroneous and time-consuming. Autonomic computing is a system that deploys high-level policies to make decisions. It is based on the architecture that is called MAPE that stands for monitor, analyze plan, and execution. The architecture revolves around the idea of a reduction in management costs. The AC architecture comprises attributes that allow self-management, according to various vendors by involving control loops.

- **Control loops:** A resource provider provides control loops. It is embedded in the runtime environment.
  It is configured using a manageability interface that is provided for every resource e.g. hard drive.
- **Managed Elements:** The managed element is a component of the controlled system. It can be hardware as well as a software resource. Sensors and effectors are used to control the managed element.
- **Sensors:** This contains information about the state and any changes in the state of elements of the autonomic system.
- **Effectors:** These are commands or application programming interfaces (API) that are used to change the states of an element.
- **Autonomic Manager:** This is used to make sure that the control loops are implemented. This divides the loop into 4 parts for its functioning. These parts are monitor, analyze, plan, and execute.

The Autonomic Computing must involve the following 3 properties :

1. **Automatic:** It must be able to execute its operations without human intervention.
2. **Adaptive:** Autonomic computers must be able to make changes according to their environment and other unforeseen conditions such as security attacks and system breakdowns.
3. **Aware:** it must also have awareness of the processes and internal states that would allow the previous two features to be executed.

Advantages

1. It is an open-source.
2. It is an evolutionary technology that adapts itself to new changes.
3. It is optimized hence gives better efficiency and performance thereby taking lesser time in execution.

4. It is very secure and can counter system and security attacks automatically.
5. It has backup mechanisms that allow recovery from system failures and crashes.
6. It reduces the cost of owning (Total Cost of Ownership) such a mechanism as it is less prone to failure and can maintain itself.
7. It can set up itself thereby reducing the time taken in manual setup.

Disadvantages

1. There will always be a possibility of the system crashing or malfunctioning.
2. This would result in an increase in unemployment due to the lesser needs of people after it is implemented.
3. The affordability would be an issue because it would be expensive.
4. It would need people who are very skilled to manage or develop such systems, thereby increasing the cost to the company that employs them.
5. It is dependent on internet speed. Its performance decreases with a decrease in internet speed.
6. It would not be available in rural areas where there are lesser provisions of stable internet connection.

Jungle Computing

Jungle Computing is a distributed computing paradigm. It simply emerged out of the plethora of distributed resources available. A Jungle Computing System consists of all compute resources available to end-users, which includes clusters, clouds, grids, desktop grids, supercomputers, as well as stand-alone machines and even mobile devices.

There are several reasons for using Jungle Computing Systems. Firstly, an application may require more compute power than available in any one system a user has access to. Secondly, different parts of an application may have different computational requirements, with no single system that meets all requirements.

From a high-level view, all resources in a Jungle Computing System are in some way equal, all consisting of some amount of processing power, memory and possibly storage. End-users perceive these resources as just that: a compute resource to run their application on. Whether this resource is located in a remote cloud or located down the hall in a cluster, is of no interest to an end-user, as long as his or her application runs effectively. Despite this similarity of resources, a Jungle Computing System is highly heterogeneous. Resources differ in basic properties such as processor architecture, amount of memory and performance. As there is no central administration of these unrelated systems, installed software such as compilers and libraries will also differ.

For example, where a stand-alone machine is usually permanently available, a grid resource will have to be reserved, while a cloud requires a credit card to gain access. Also,

the middleware used to access a resource differs greatly because of using different interfaces.

The heterogeneity of Jungle Computing Systems makes it hard to run applications on multiple resources. For each used resource, the application may have to be re-compiled or even partially re-written, to handle the changes in software and hardware available. Moreover, for each resource, a different middleware interface may be available, requiring different middleware client software. Once an application has been successfully started in a Jungle, another aspect that hinders usage of Jungle Computing Systems is the lack of connectivity between resources.

Jungle Computing Systems

When grid computing was introduced over a decade ago, its foremost visionary aim was to provide efficient and transparent (i.e. easy-to-use) wall-socket computing over a distributed set of resources. Since then, many other distributed computing paradigms have been introduced, including peer-to-peer computing, volunteer computing and more recently cloud computing. These paradigms all share many of the goals of grid computing, eventually aiming to provide end-users with access to distributed resources (ultimately even at a world-wide scale) with as little effort as possible.

These new distributed computing paradigms have led to a diverse collection of resources available to research scientists, which include stand-alone machines, cluster systems, grids, clouds, desktop grids, etc.

With clusters, grids and clouds thus being equipped with multi-core processors and many-core 'add-ons', systems available to scientists are becoming increasingly hard to program and use. Despite the fact that the programming and efficient use of many-cores is known to be hard, this is not the only problem. With the increasing heterogeneity of the underlying hardware, the efficient mapping of computational problems onto the 'bare metal' has become vastly more complex. Now more than ever, programmers must be aware of the potential for parallelism at all levels of granularity.

What is Docker?

- Docker is a set of platforms as a service (PaaS) products that use Operating system-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries, and configuration files; they can communicate with each other through well-defined channels. All containers are run by a single operating system kernel and therefore use fewer resources than a virtual machine.
  What is Docker?
  Docker is an open-source containerization platform by which you can pack your application and all its dependencies into a standardized unit called a container. Containers are light in weight which makes them portable and they are isolated from the underlying

infrastructure and from each other container. You can run the docker image as a docker container in any machine where docker is installed without depending on the operating system.

Docker is popular because of the following:

1. Portability.
2. Reproducibility.
3. Efficiency.
4. Scalability.

What is Dockerfile?

The Dockerfile uses DSL (Domain Specific Language) and contains instructions for generating a Docker image. Dockerfile will define the processes to quickly produce an image. While creating your application, you should create a Dockerfile in order since the Docker daemon runs all of the instructions from top to bottom.

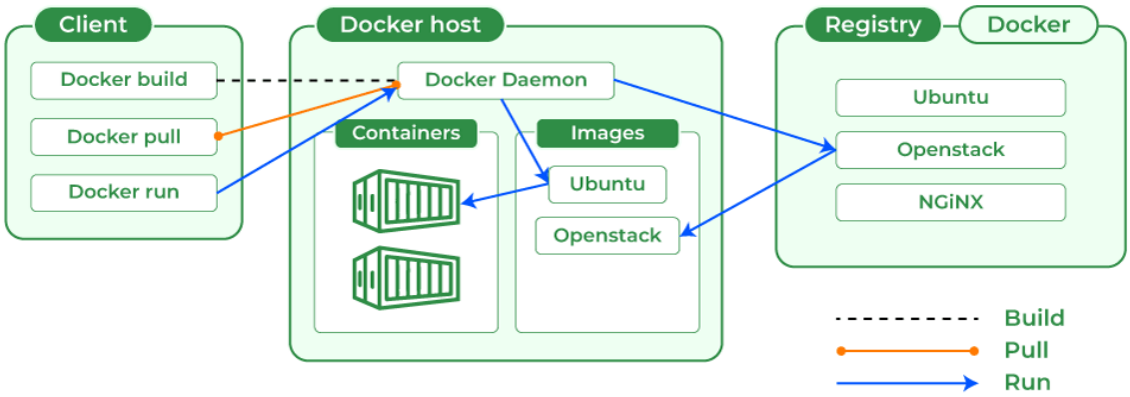
- It is a text document that contains necessary commands which on execution help assemble a Docker Image.
- Docker image is created using a Docker file.

Dockerfile is the source code of the image

To Know more about the Dockerfile refer to the Docker – Concept of Dockerfile.

How Docker Works

Docker makes use of a client-server architecture. The Docker client talks with the docker daemon which helps in building, running, and distributing the docker containers. The Docker client runs with the daemon on the same system or we can connect the Docker client with the Docker daemon remotely. With the help of REST API over a UNIX socket or a network, the docker client and daemon interact with each other. To know more about working of docker refer to the Architecture of Docker.



What is Docker Image?

It is a file, comprised of multiple layers, used to execute code in a Docker container. They are a set of instructions used to create docker containers. Docker Image is an executable package of software that includes everything needed to run an application. This image informs how a container should instantiate, determining which software components will run and how. Docker Container is a virtual environment that bundles application code with all the dependencies required to run the application. The application runs quickly and reliably from one computing environment to another.

What is Docker Container?

Docker container is a runtime instance of an image. Allows developers to package applications with all parts needed such as libraries and other dependencies. Docker Containers are runtime instances of Docker images. Containers contain the whole kit required for an application, so the application can be run in an isolated way. For eg.- Suppose there is an image of Ubuntu OS with NGINX SERVER when this image is run with the docker run command, then a container will be created and NGINX SERVER will be running on Ubuntu OS.

What is Docker Hub?

Docker Hub is a repository service and it is a cloud-based service where people push their Docker Container Images and also pull the Docker Container Images from the Docker Hub anytime or anywhere via the internet. Generally it makes it easy to find and reuse images. It provides features such as you can push your images as private or public registry where you can store and share Docker images

Mainly DevOps team uses the Docker Hub. It is an open-source tool and freely available for all operating systems. It is like storage where we store the images and pull the images when it is required. When a person wants to push/pull images from the Docker Hub they must have a basic knowledge of Docker. Let us discuss the requirements of the Docker tool.

What is Docker Compose?

Docker Compose will execute a YAML-based multi-container application. The YAML file consists of all configurations needed to deploy containers Docker Compose, which is integrated with Docker Swarm, and provides directions for building and deploying containers. With Docker Compose, each container is constructed to run on a single host.

How to Download Docker Desktop?

Docker Desktop provides GUI to work on docker containers, docker images and docker networks. Docker desktop provides and separate environment which contains Docker Engine, Docker CLI, Docker Compose, Kubernetes, and other tools whcih are needed to build,ship and run the applications in the form of containerization which make it more user friendly. To know more how to install docker desktop refer to Docker Desktop Sample Image.

Docker Commands

There are “n” no.of commands in docker following are some of the commands mostly used.

1. Docker Run
2. Docker Pull
3. Docker PS
4. Docker Stop
5. Docker Start
6. Docker rm
7. Docker RMI
8. Docker Images
9. Docker exec
10. Docker Login

To Know more about the docker commands refer tot the Docker – Instruction Commands.

Docker Engine

The software that hosts the containers is named Docker Engine. Docker Engine is a client-server based application. The docker engine has 3 main components:

1. **Server:** It is responsible for creating and managing Docker images, containers, networks, and volumes on the Docker. It is referred to as a daemon process.
2. **REST API:** It specifies how the applications can interact with the Server and instructs it what to do.
3. **Client:** The Client is a docker command-line interface (CLI), that allows us to interact with Docker using the docker commands.

Why use Docker

Docker can be used to pack the application and its dependencies which makes it lightweight and easy to ship the code faster with more reliability. Docker make every simple to run the application in the production environment docker container can be platform independent if the docker engine is installed in the machine.

What is Docker For AWS?

Docker is the most powerful tool to run the application in the form of containers. Docker container are light in weight and can be run on any operating system.

AWS provides the Amazon Elastic Container Service (Amazon ECS) it is an fully managed container service by which you can deploy, scale and manage the docker containers. Amazon ECS is the most reliable platform according to the performance and also it can be integrated with the other AWS Service like load balancing, service discovery, and container health monitoring. To know more about Amazon Elastic Container Service (Amazon ECS).

Difference Between Docker Containers and Virtual Machines

Docker Containers	Virtual Machines
Docker Containers contain binaries, libraries, and configuration files along with the application itself.	Virtual Machines (VMs) run on Hypervisors, which allow multiple Virtual Machines to run on a single machine along with its own operating system.
They don’t contain a guest OS for each container and rely on the underlying OS kernel, which makes the containers lightweight.	Each VM has its own copy of an operating system along with the application and necessary binaries, which makes it significantly larger and it requires more resources.
Containers share resources with other containers in the same host OS and provide OS-level process isolation.	They provide Hardware-level process isolation and are slow to boot.