UNIT I

IOT - What is the IoT and why is it important? Elements of an IoT ecosystem, Technology drivers, Business drivers, Trends and implications, Overview of Governance, Privacy and Security Issues.

What is IoT ?

The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. Oracle has a network of device partners.

IoT intelligent applications

Why is Internet of Things (IoT) so important?

Over the past few years, IoT has become one of the most important technologies of the 21st century. Now that we can connect everyday objects—kitchen appliances, cars, thermostats, baby monitors—to the internet via embedded devices, seamless communication is possible between people, processes, and things.

By means of low-cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. In this hyperconnected world, digital systems can record, monitor, and adjust each interaction between connected things. The physical world meets the digital world—and they cooperate.

What technologies have made IoT possible?

While the idea of IoT has been in existence for a long time, a collection of recent advances in several different technologies has made it practical.

- **Access to low-cost, low-power sensor technology.** Affordable and reliable sensors are making IoT technology possible for more manufacturers.
- **Connectivity.** A host of network protocols for the internet has made it easy to connect sensors to the cloud and to other "things" for efficient data transfer.

- **Cloud computing platforms.** The increase in the availability of cloud platforms enables both businesses and consumers to access the infrastructure they need to scale up without having to manage it all.
- **Machine learning and analytics.** With advances in machine learning and analytics, along with access to varied and vast amounts of data stored in the cloud, businesses can gather insights faster and more easily. The emergence of these allied technologies continues to push the boundaries of IoT and the data produced by IoT also feeds these technologies.
- **Conversational artificial intelligence (AI).** Advances in neural networks have brought natural-language processing (NLP) to IoT devices (such as digital personal assistants Alexa, Cortana, and Siri) and made them appealing, affordable, and viable for home use.

What is industrial IoT?

Industrial IoT (IIoT) refers to the application of IoT technology in industrial settings, especially with respect to instrumentation and control of sensors and devices that engage cloud technologies. Refer to thisTitan use case PDF for a good example of IIoT. Recently, industries have used machine-to-machine communication (M2M) to achieve wireless automation and control. But with the emergence of cloud and allied technologies (such as analytics and machine learning), industries can achieve a new automation layer and with it create new revenue and business models. IIoT is sometimes called the fourth wave of the industrial revolution, or Industry 4.0. The following are some common uses for IIoT:

- Smart manufacturing
- Connected assets and preventive and predictive maintenance
- Smart power grids
- Smart cities
- Connected logistics
- Smart digital supply chains

What are IoT applications?

Business-ready, SaaS IoT Applications

IoT Intelligent Applications are prebuilt software-as-a-service (SaaS) applications that can analyze and present captured IoT sensor data to business users via dashboards. We have a full set of IoT Intelligent Applications.

IoT applications use machine learning algorithms to analyze massive amounts of connected sensor data in the cloud. Using real-time IoT dashboards and alerts, you gain visibility into key performance indicators, statistics for mean time between failures, and other information. Machine learning–based algorithms can identify equipment anomalies and send alerts to users and even trigger automated fixes or proactive counter measures.

With cloud-based IoT applications, business users can quickly enhance existing processes for supply chains, customer service, human resources, and financial services. There's no need to recreate entire business processes.

What are some ways IoT applications are deployed?

The ability of IoT to provide sensor information as well as enable device-to-device communication is driving a broad set of applications. The following are some of the most popular applications and what they do.

Create new efficiencies in manufacturing through machine monitoring and product-quality monitoring.

Machines can be continuously monitored and analyzed to make sure they are performing within required tolerances. Products can also be monitored in real time to identify and address quality defects.

Improve the tracking and "ring-fencing" of physical assets.

Tracking enables businesses to quickly determine asset location. Ring-fencing allows them to make sure that high-value assets are protected from theft and removal.

Use wearables to monitor human health analytics and environmental conditions.

IoT wearables enable people to better understand their own health and allow physicians to remotely monitor patients. This technology also enables companies to track the health and safety of their employees, which is especially useful for workers employed in hazardous conditions.

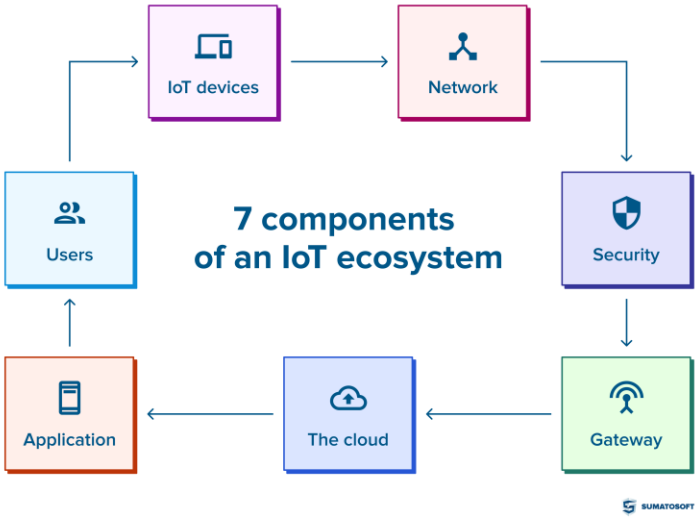
Drive efficiencies and new possibilities in existing processes.

One example of this is the use of IoT to increase efficiency and safety in connected logistics for fleet management. Companies can use IoT fleet monitoring to direct trucks, in real time, to improve efficiency.

Enable business process changes.

An example of this is the use of IoT devices for connected assets to monitor the health of remote machines and trigger service calls for preventive maintenance. The ability to remotely monitor machines is also enabling new product-as-a-service business models, where customers no longer need to buy a product but instead pay for its usage.

Elements of IOT Ecosystems



1. IoT Devices

IoT devices are actually the layer of sensors, actuators and smart objects that collect data about the environment and measure physical parameters.

- So, as we have already mentioned, the basic elements of the Internet of Things ecosystem are sensors and actuators **(or simply "things").**
- Sensors are the perception of the IoT system, whose main function is to extract information from the environment and convert it into data.

In the internet of things ecosystem, it is rare to find only one type of sensor or actuator. Because there are many types of sensors, each type has its subcategories.

So, we want to mention two of the most common and two of the most important sensors for improving the ecological state of the earth:

- **Temperature sensors:** They are one of the most common and popular. A wide range of industries can use these sensors to measure the temperature of industrial machinery to monitor its condition, to monitor the temperature of a patient continuously, or to monitor the condition of a farmer's soil.
- **Subcategories:** Thermocouples, RTDs, Infrared Sensors, etc.
- **Proximity sensors:** They are a popular IoT device because they save light in thousands of homes with these sensors when no one is around.
- **Subcategories:** Inductive sensors, Photoelectric sensors, Ultrasonic sensors.
- **Water quality sensors –** They are particularly important due to ocean pollution. Because these sensors can help monitor water conditions and detect sources of pollution in real time!
- **Sub-categories:** residual chlorine sensor, turbidity sensor, pH sensor.
- **Chemical sensors** – these monitor chemical changes in the air, which is extremely important in large cities where air pollution problems continue to worsen. These sensors are also useful in industrial environmental monitoring, hazardous chemical detection and radioactive detection.
- **Subcategories:** Chemical Field Effect Transistor, Hydrogen Sulfide Sensor, Potentiometric Sensor.

2. Security

It is the part that includes all the other parts, provides security for data transfer and prevents unauthorised connections outside the Internet of Things ecosystem.

In recent years, we also see that the number of IoT-based DDoS attacks has skyrocketed. Therefore, every IoT system needs a strong level of security that at least protects against the most common vulnerabilities.

The security level has a wide range of responsibilities, such as:

- **Access control to the IoT network:** Anyone who connects to the network has access to all its devices, making broken authentication problems particularly acute. Moreover, IoT devices can also trust the local network so that no further authentication is required.

- **Prevention of data loss during data transfer over the network:** The data must be encrypted through the IoT system using protocols such as **AES, DES, DSA** and others.
- **Look for malicious software:** Software bugs can sometimes trick attackers into executing their code on the IoT device. Hence the software versions need to be corrected when a vulnerability is found.

The Internet of Things ecosystem is also safeguarded by a number of firmware and security providers, including Azure Sphere, LynxOS, Mocana, Spartan, Forescout, Symantec, etc.

But unfortunately, most Internet of Things vendors and IoT device manufacturers also need to pay more attention to basic security guidelines.

They are:

- The device boot process should be protected from running inappropriate pieces of code.
- Cryptographic keys must be used to execute all commands on devices. This is especially important when managing IoT updates.
- All commands and control information must pass through a gateway to avoid direct access to the device outside the network.
- All IoT devices must install security patches whenever a new security flaw is detected.

3. Network

The network is the logistical heart of the Internet of Things ecosystem. The network is also known as the connectivity layer. It is responsible for all communications within the IoT system: connecting smart objects, transferring data and commands between IoT stages, and connecting to the cloud.

There are two means of communication:

- **The first mode of communication:** Occurs locally in a local area network (LAN) between IoT devices and smart gateways via short-range wireless communication protocols. This communication mode is optional because the sensors can connect directly to the cloud via the Internet using the TCP / IP protocol.

However, connecting via non-IP protocols consumes less power because the devices connect to local smart gateways instead of trying to access the main server in the cloud.

So, the most popular short-distance protocols for IoT architecture are:

1. Wireless internet access (WiFi)
2. Bluetooth and Bluetooth Low Energy (or Bluetooth LE for less powerful devices that generate less data)
3. ZigBee – a universal solution that connects all smart devices
4. Near Field Communication (NFC)
5. Radio Frequency Identification (RFID)
6. Sigfox
7. LoRaWAN

If the system needs to cover long distances in the range of miles, it can use Low Power Wide Area Network (or LPWAN) designed for long-distance wireless data transfer.

- **The second mode of communication:** Occurs when the data of things are transferred to the cloud in cases where there is no smart gateway or in cases of communication between the smart gateways and the cloud. The network layer establishes a connection between the local network and the Internet. The basic protocol here is the IPv6 protocol.

4. Gateways

IoT Gateway is a physical or virtual platform that mediates between IoT devices and the cloud.

There are several main functions of IoT gateways:

- Control the flow of data in the Internet of Things ecosystem. The data flow goes through the gateway from the devices to the cloud and in the opposite direction.
- Ensure the security of the transmission of information in both directions. Also, transmit commands from the cloud to IoT devices.
- Preprocess data before sending it to the cloud. Gateways filter, aggregate, synthesise, and aggregate traffic from different devices.
- Save energy from IoT devices as communication over the internet is energy-intensive, unlike low-energy technologies such as Bluetooth Low Energy (it is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries).
- Reduce response latency to IoT devices. Some devices require a real-time response from the system.

5. The Cloud

The cloud is a computing resource responsible for storing, analysing, and managing data. In other words, it is a group of computers that people access over the Internet to use their computing power for a particular purpose.

The cloud is where a large pile of raw sensor data is converted into neat little piles of valuable information. The cloud can be powered by analytics software, visualisation tools, AI, and machine learning for in-depth data analysis and processing. And the most popular cloud computing providers are **Microsoft Azure** and **AWS** IoT.

Surprisingly one of the main advantages of the cloud solution is that it is easily scalable. It is an essential requirement for building an effective IoT system.

6. Application

When software development companies build software products for the IoT ecosystem, they will cover all seven components. And will create a system that covers all the requirements at every level.

But even still, the IoT application is just the tip of the iceberg in IoT software development. Also, an application is where users can interact with the Internet of Things ecosystem. This interaction is only made possible by the graphical user interface, where the users can consult analyses reports, control the system and manage devices.

The list of technologies used in the development includes:

- **Programming languages:** C/C++, Python, Ruby, JavaScript
- **Development frameworks:** Node.Js (Node-Red for rapid prototyping), OT, IoT.js, Device.js, Eclipse IoT (Kura, SmartHome), AngularJS
- **Third-party APIs:** Google Assistant, Google Home (Actions on Google), Google Vision, Apple HomeKit, MI Light, Cortana, Alexa Voice Service, Philips Hue, Android Things

7. Users

Its users are the most important component among the seven components of the Internet of Things ecosystem.

Here, users have two roles:

- They use an IoT ecosystem for their needs. Here, the possibilities offered by the Internet of Things ecosystem are becoming a valuable database for all types of users. For example, sensors and IoT applications can become professional healthcare assistant that measures the patient's biometry. This will help to make a more accurate diagnosis.
- Secondly, the Internet of Things ecosystems should serve people. And meet their needs, and provide information that assists them in achieving their goals. Moreover, focusing on people's needs, the IoT ecosystem was built by and for people. So, the users determine what the IoT ecosystem will do and won't.

Technologies Drivers in IoT (internet of things) enabling are

- Wireless Sensor Network.
- Cloud Computing.
- Big Data Analytics.
- Communications Protocols.
- 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 –

8. Broad network access
9. On demand self-services
10. Rapid scalability
11. Measured service
12. 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 –

13. Data cleaning
14. Munging
15. Processing
16. 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

17. Data encoding
18. Addressing schemes

5. Embedded Systems :

It is a combination of hardware and software used to perform special tasks.

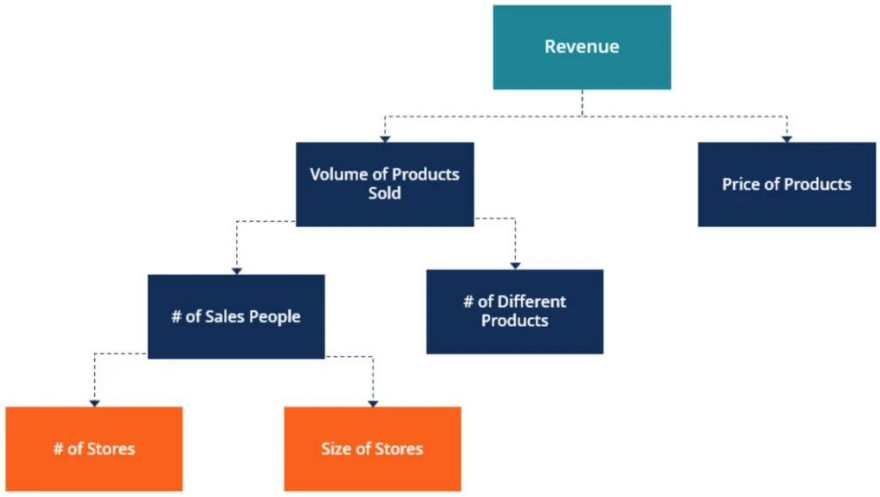
It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).

It collects the data and sends it to the internet. Embedded systems used in Examples –

- Digital camera
- DVD player, music player
- Industrial robots
- Wireless Routers etc.

What is a business driver?

Business drivers are the key inputs and activities that drive the operational and financial results of a business. Common examples of business drivers are salespeople, number of stores, website traffic, number and price of products sold, units of production, etc.



Examples of business drivers

Drivers vary significantly by industry, but they can all be determined using the same type of root cause analysis.

Here is a list of common business drivers:

- Number of stores or locations
- Average size (i.e., square feet) per location
- Number of products sold (volume)
- Prices of products/services sold

- Number of salespeople
- Effectiveness of salespeople
- Traffic volume to a website
- Conversion rate of traffic to a website
- Production rate for manufacturing
- Efficiency rates and downtime
- Energy and electricity costs
- Rent and office space
- Salaries and wages per employee
- Commissions, fees, and other selling expenses
- Foreign exchange rates
- Commodity prices (e.g., oil, copper, pulp, rubber, etc.

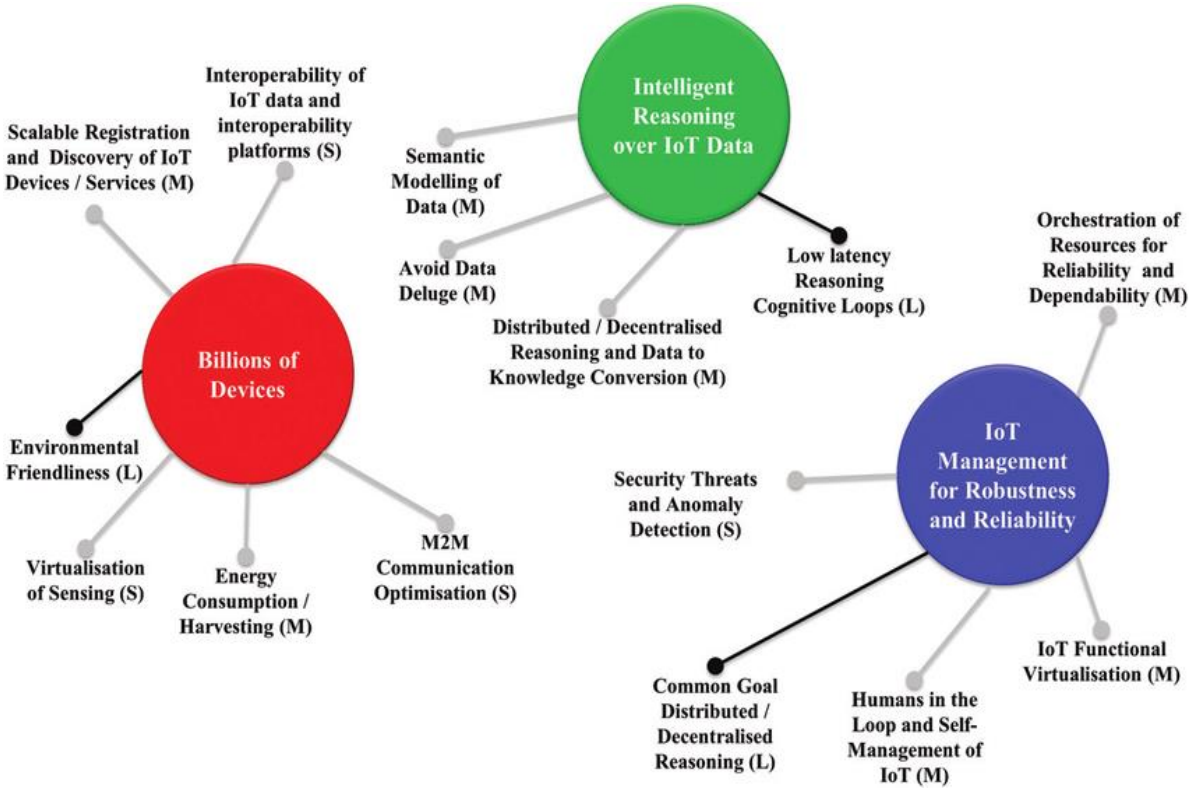
How to determine what the business drivers are

Drivers impact all financial aspects of a business: revenues, expenses, and capital costs. In identifying what the main drivers are, it's important to do a root cause type of analysis.

Trends and Implication in IOT

1. IoT supply chain issues

Some civic IoT investments were delayed during the pandemic, and chip shortages due to factory shutdowns and supply chain problems made IoT technology unavailable in many industries, such as the automotive sector. Although there are significant investments in building new semiconductor fabrication plants to meet increasing demand, these new fabs can take more than two years to come on line. Thus, the shortages that appeared in 2021 may not be fully resolved until sometime in 2024. An interesting trend to relieve some supply chain issues is the building of new semiconductor fabs closer to demand.



2. More AI support for IoT data analytics

In 2022, major advances were made in AI software algorithms and hardware to train these models on. Many companies are working to accelerate the rate that IoT-derived data can be analyzed and turned into useful insights in data centers and at the edge. Also, with more IoT devices collecting data, there is more data for analysis and training. Once these models have been created in data centers, they can be implemented as an inference engine at the network edge or in IoT endpoint devices to enable new and better-performing applications. Some of these models can also learn locally, adjusting their capabilities as they gain experience with data in the field.

THIS ARTICLE IS PART OF

Ultimate IoT implementation guide for businesses

- Which also includes:
- **9 IoT trends to keep an eye on in 2023 and beyond**
- **AI and IoT: How do the internet of things and AI work together?**
- **Top 12 most commonly used IoT protocols and standards**

DOWNLOAD1

Download this entire guide for FREE now!

3. Increased industrial IoT use cases

IoT in industrial settings also increased in 2022, and according to a recent survey from IEEE, industrial IoT will be one the most important areas of technology in 2023. This year's increase was partly in response to worker shortages and infection concerns during the pandemic. IoT-capable factories can combine greater monitoring and local intelligence with robotics and automation to take over some operations that would otherwise require people to work in proximity to each other. With the intelligence of IoT-based systems, humans are increasingly filling roles where their unique capabilities to make decisions using both objective and subjective criteria can be combined with machine intelligence to create safer and more efficient factories.

4. More widespread connectivity for IoT devices

IoT Analytics projected that 2023 will see a growth of IoT devices by 18% to 14.4 billion, and by 2025, this could increase to 27 billion connected IoT devices. One of the trends in 2023 that will enable this growth is the increased replacement of 2G/3G wireless networks with 4G/5G networks. This will particularly increase connectivity in urban communities, but many rural areas will still depend on lower-performing networks. That will widen the digital divide between wealthy urban areas and poorer rural areas.

5. Lower costs for IoT product components

Another enabler of IoT growth in 2023 will be the gradual relief of many chip shortages as new production goes on line but perhaps also due to lessening demand. Although chip shortages are projected into 2024, declining demand due to financial uncertainty has caused prices on many chips, including dynamic RAM (DRAM) and NAND flash, to decline. Lower prices on components will result in lower costs for the end IoT products, which could accelerate further adoption and perhaps limit any potential financial downturn.

6. New technological developments

Because it is a growing market, IoT is attracting many new technological developments that will drive growth in 2023 and beyond. These developments include changes in computer architectures -- driven in part by changes in storage and memory approaches -- that will affect the way data is stored and processed in data centers and at the network edge. This will result in less data movement and lower power data processing. Also, new chiplet packaging technology will enable denser and

more specialized chip-based systems, including at the network edge and in endpoint IoT devices. Further in the future, fundamental changes in computer processing could impact IoT applications.

7. System disaggregation enabling more efficient data processing

Disaggregation of traditional data center servers and composing virtual computing systems enable more efficient data processing, as well as lower power consumption. Much of the data processed in data centers is from IoT applications, and as IoT grows, this processing will grow. Non-volatile memory express, Compute Express Link and the changes in computer architecture they enable will reduce the costs of many IoT applications.

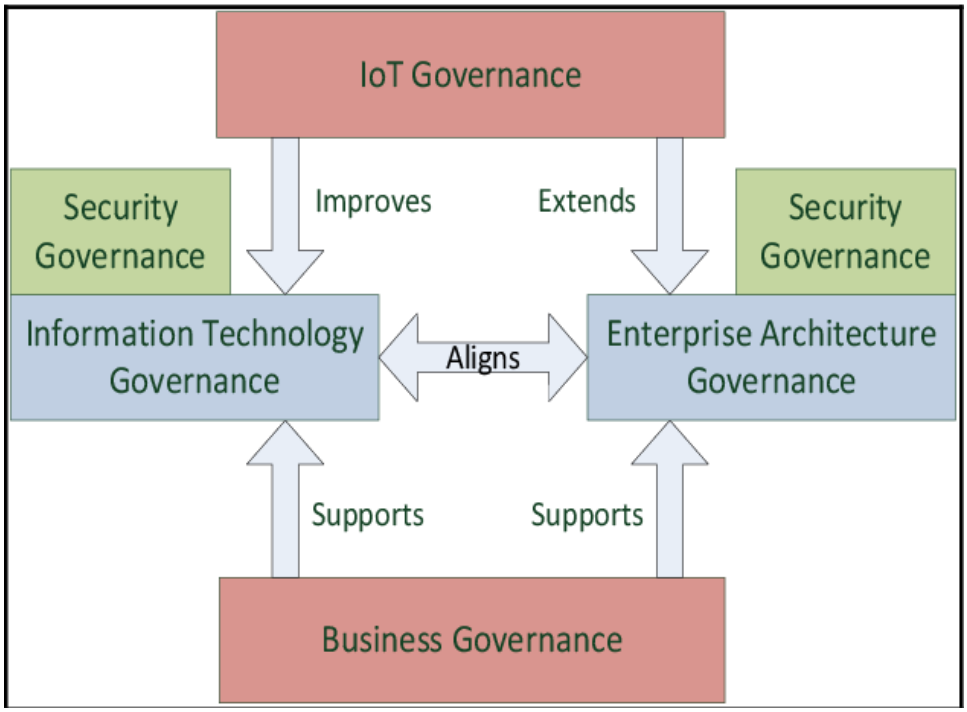
8. New chip design and standards

In addition to this system disaggregation, traditional semiconductor device design is undergoing its own disaggregation with the introduction of chiplets. Chiplets separate many of the traditional CPU functions into separate smaller chips that are connected to each other with high-speed interconnects on a small package. In 2022, a new standard, called Universal Chiplet Interconnect Express (UCIe), was introduced that will enable specialized chips from many manufacturers to be combined together in a compact package. This enables the creation of more specialized semiconductor chiplet packages for special applications and creates the need for a new type of foundry for assembling chiplets into a UCIe package. UCIe will enable more efficient semiconductor devices for data centers, the network edge and IoT endpoint devices.

9. Emerging non-volatile or persistent memory technologies for IoT

Lower prices on DRAM, NAND flash and other important semiconductors for IoT devices and the increasing density of these memory devices will lower the costs and increase the capability of these devices. In addition to these traditional memory technologies, there are emerging non-volatile or persistent memory technologies that are starting to show up in IoT devices. In particular, magnetic RAM (MRAM) and resistive RAM are used in some consumer IoT devices, such as wearables. Replacing static RAM with a non-volatile memory, such as MRAM, enables more lower-power states when the IoT device is not being actively used. For energy-constrained applications, such as those that run on batteries, this increases the usefulness and life on a charge for the IoT device.

Overview of IoT Governance, Privacy and Security Issues



Governance, security and privacy are probably the most challenging issues in the Internet of Things(IoT) and they have been extensively discussed in many forums. While most of the organisation work on *Internet* governance, a logical step can extend these concepts to *IoT* governance. But the difficulty of IoT is that the high number and heterogeneity of technologies and devices, which require even more specific Governance solutions and approaches that are more complex in nature. Size and heterogeneity in fact, are the two main components that affect the governance of IoT. The governance is considered as a double-edged sword, because it can offer stability and support for decisions but it can also become excessive and result in an over-controlled environment.

Nevertheless, since there are no legal frameworks for IoT governance, even if the differences between the IoT and the Internet have been overestimated at the beginning, an analysis of the major IoT governance issues (legitimacy, transparency, accountability, anti-competitive behaviour) seems to be worthwhile to design and develop.

Heterogeneity requires security to overcome the impossibility of implementing efficient protocols and algorithms on all the devices involved across the many IoT application areas. Without guarantees in security, stakeholders of governance ecosystem are unlikely to adopt IoT solutions on a large scale. For this reason, the development of enforcement techniques to

support scalability and heterogeneity, to anonymise users' data and to allow context aware data protection are key factors.

In the IoT context, it is difficult to separate the concepts of Governance, Security and Privacy, because addressing privacy and security aspects to achieve trust in IoT would probably need governance mechanisms as well. As mention before, at the higher level of the interaction of IoT with users, ethical aspects cannot be disjointed from the governance, security and privacy aspects as well.

In addition to that the proliferation of wireless devices with ubiquitous presence is expected to worsen the issue of privacy due to the current design of the link-layer and lower layer protocols, which usually expose information like implicit names and identifiers that can reveal users identity. To eliminate these issues, these layers should be redesigned in order to minimize the collection of such data, conceal important information from the un-trusted parties and, to reveal proper information to the authorized or trusted parties. The management of heterogeneous devices, applications and protocols can be also addressed using the principles of service-oriented computing, which going to achieve a significant flexibility in different levels of the IoT architecture