SMART Computing and Internet of Things (IoT)

Presented by
Abdulrazaq Abdulrahman
ICT Infrastructure and Security Consultant (Specialist)
MD, Layer-8 Consulting Ltd.

At a Workshop Organized by the
National Judicial Institute
August 15th -17th 2022

ABSTRACT

Devices can communicate and share information in a smart environment using new generation technology. Smart computing, next-generation computing, and the Internet of Things (IoT) is a combination of hardware, software, and network to provide real-time awareness of real-time systems. It aims to monitor, analyze, and report in a faster and smarter way to make a system, a smart system.

Today's hyper-connectivity involving all things smart, for example, smart cars, smart factories, and so on, are part of the most dynamic, heterogeneous, and distributed infrastructure that software has to run on. As 5G rolls out, the size of this infrastructure will grow exponentially. One of the challenges is to tame the cost of building and operating software in this environment and to maintain human-to-human social interaction, and natural relationship sanity.

.

INTRODUCTION

Today, the world is full of smart technology working in smart environments with smart devices (electronic gadgets and home appliances, vehicles, cameras, etc.) where they can connect, communicate, and transfer information to one another. Computers are performing a more secure and faster computation. Examples of such smart environments consuming smart technologies are smartwatches, smartphones, smart homes, smart cities, smart agriculture, and so on. The IoT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing, and data analytics. Imagine a world where billions of objects can sense, communicate and share information.

SMART COMPUTING

Smart Computing is a combination of two words: Smart and computing, where SMART means Self-**Monitoring, Analyzing, and Reporting Technology**, and Computing means performing critical thinking, and operational/logical (computational) analysis. Therefore, it collects and stores the data, monitors, and detects for what purpose it was designed, analyzes it, and reports (in advance) accordingly to the user.

Computing to perform calculations quickly. Monitoring, analyzing, and reporting in a faster and smarter way to make a system, a smart system. The focus of smart computing is to provide cheaper technology, solve an existing problem, look ahead to future problems and preempt them before happening. It is a sensor-based technology, with the combination of the Internet of things (IoT), machine learning, Big Data, Artificial Intelligence, etc.

The technology through which the hardware and software devices communicate with each other, using the internet to share, store, analyze data/information and produce intelligence information and even act on it, is known as **SMART COMPUTING.** It is the next generation of computing that creates something self-aware, which can sense the activities of its environment, massages the gathered information, perform some analytics, and provides the optimal decisions along with predicting future risks and challenges. In this, the communication process takes place among devices through

- Sensors
- Development boards
- Cloud

Sensors may be hardware or software components that sense the physical world and share the information with the development boards. This development board processes the data with the help of controllers and processors and triggers a task, and the cloud securely stores the shared information with the help of the network and transmits it back when required. To store the information on the cloud and for the communication process, a communication language such as Python, C, or Java and communicating protocols such as HTTP, MQTT, and WebSockets are used. To make the process more secure, only authorized persons to access the data.

Components of smart computing

The components explain how the information travels in this technology and how smart computing functions. These are as follows:

- Sensor devices for sensing the data from hardware and software devices
- Device processors for processing and learning with the previous data
- Cloud for storing the information
- Communicating languages such as Python, C, or Java
- Communicating protocols such as HTTPS, WebSocket, or MQTT

  WebSocket is an event-driven protocol, which means it is good for truly real-time communication. Unlike HTTP, where you have to constantly request updates, with WebSockets, updates are sent immediately when they are available.

  MQTT (Message Queuing Telemetry Transport) is a lightweight open messaging protocol that provides resource-constrained network clients with a simple way to distribute telemetry information in low-bandwidth environments. The protocol, which employs a publish/subscribe communication pattern, is used for machine-to-machine (M2M) communication. Telemetry is the automatic measurement and wireless transmission of data from remote sources. In general, telemetry works in the following way: Sensors at the source measure either electrical data (such as voltage or current) or physical data (such as temperature or pressure)

In smart computing, there is 70% of hardware utilization, which is more use of resources with the smart OS. Smart OS makes computation faster, efficient, and smarter.

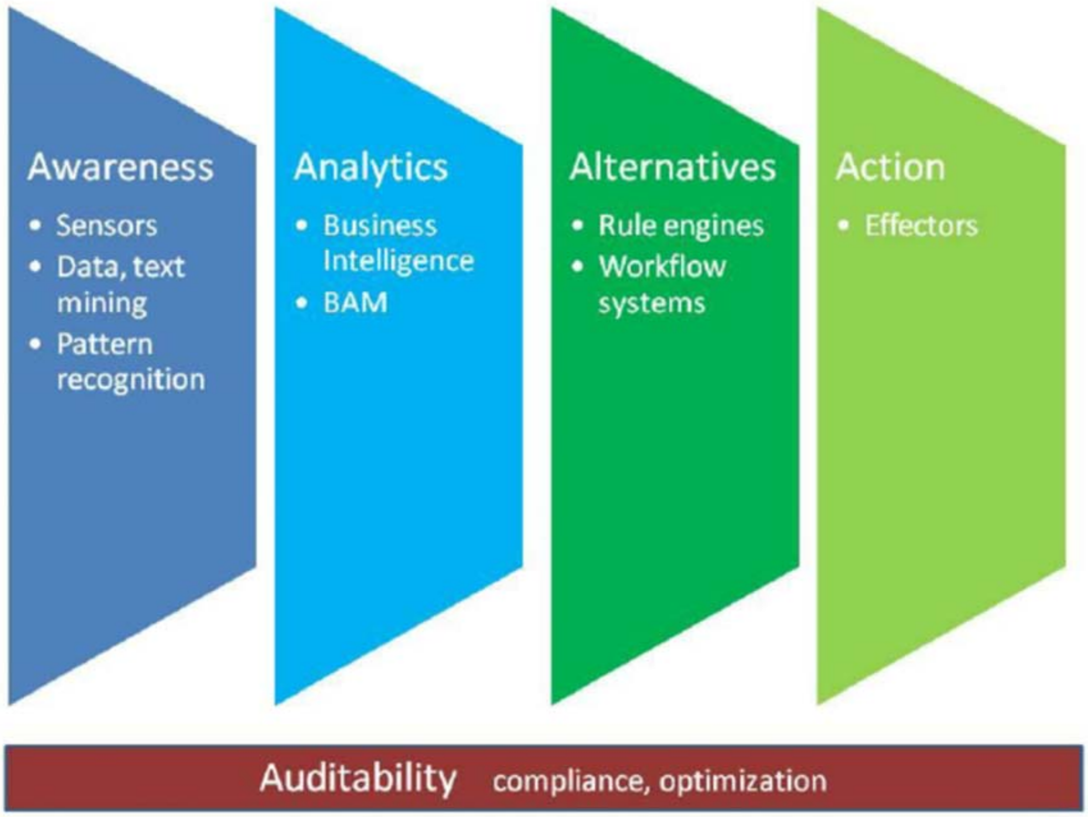
Key functions (5 A's) of smart computing

Smart computing comprises five key functions which are 5 A’s of smart computing:

a. Awareness
b. Analysis
c. Alternative
d. Action
e. Auditability

All the functionality of smart computing evolves around these 5 As and analyzing, reporting and monitoring functions are performed accordingly.

Awareness is the most important A among all the 5 A’s of smart computing.



Awareness:

- Identification of tools and devices, use of sensors, GPS,
- Identification of customers (a type of user, identity, location, status)
- Identification of integrated communication technology such as 3G, 4G, etc.

GPS Tracking, Mobile Gyroscope, adaptive brightness, voice detection, face detection, etc are some of the awareness tools we are familiar with.

Analysis:

- Data filtering and categorization
- Stretchy logical processing and computation (AI and ML)
- Big Data Process application (Orchestration and Architecture)

Alternatives:

- Identify rule engines and workflow
- What decision should trigger necessary actions

Action:

- Correct action occurs at the correct time
- On-time notification
- Type of process application (action will execute through integrated links to application)

Auditability:

- Technology needs to capture, track and analyze information
- What actions are taken (right or wrong)
- How to improve analysis
- Identify better alternatives

Internet of Things (IoT)

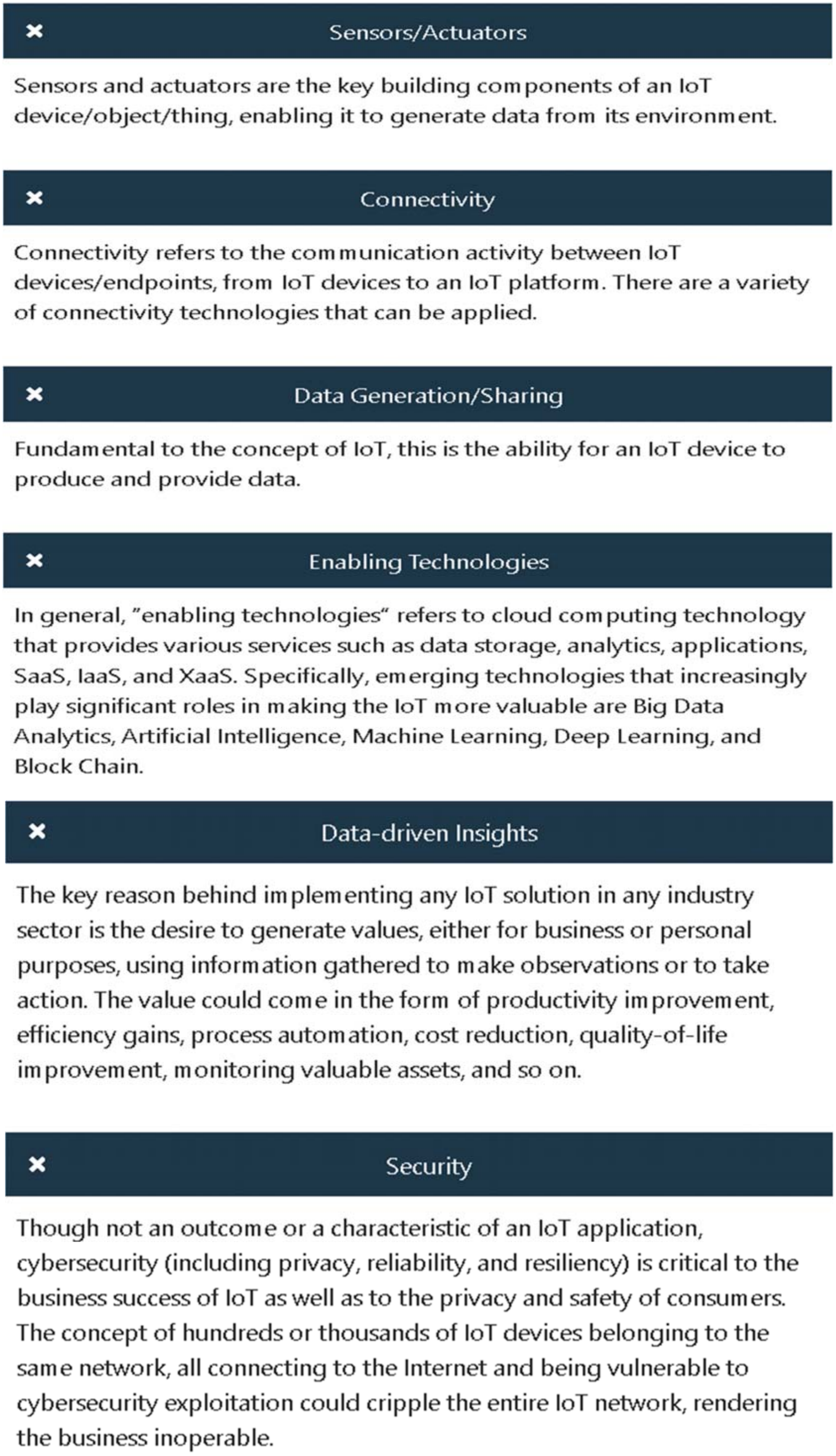
The Internet of Things, IoT, refers to the concept that billions of objects, devices, or things with sensing and/or action capabilities are connected to the internet. These IoT objects are set up to collect data from their environment and to share their data with other systems. The real power of the IoT comes in when the data collected by IoT objects are analyzed, learned, and turned into insights that enable data-driven decisions to be made. Internet-connected devices can be accessed and controlled from anywhere and at any time, and together with insights derived from the collected data, the Internet of Things gives business and social enterprises incredible power to be innovative. While there's no agreed standard definition of what IoT is, the following definitions from selected global bodies illustrate the evolving nature of IoT and our understanding of what IoT can bring.

National Institute of Science and Technology, NIST, defines IoT as a concept based on creating systems that interact with the physical world using networked entities, such as sensors, actuators, information resources, and people. NIST further elaborates the IoT concept by introducing foundation concepts of IoT Component, IoT System and IoT Environment.

The International Telecommunications Union, ITU, on the other hand, defines the IoT as a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies, ICT. According to the U.S. Computer Emergency Response Team, US-CERT, the Internet of Things refers to any object or device that sends and receives data automatically through the internet. This rapidly expanding set of things includes tags, also known as labels or chips that automatically track objects, sensors and devices that interact with people and share information machine to machine. Let's look at one more.

The IETF, the Internet Engineering Taskforce, defines the Internet of Things as the network of physical objects or things embedded with electronics, software, sensors and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices. As you'll see, even though there isn't a singular definition of what IoT is, there are a number of fundamental characteristics that define IoT and what it does.

The Internet of Things is not a technology. IoT involves complex ecosystems comprised of an array of technologies, products, and services, and with the collaboration of many stakeholders. An IoT solution can be realized with a number of technologies, from advances in chipset, modules, hardware, sensors, and actuators, to digital connectivity, cloud computing, AI, blockchain, applications, and smartphones. It is appropriate to say that the Internet of Things is not made up of one enormous network of connected devices. Rather, it is made up of many different networks of devices. Some are private, some are public, and most are connected to the internet in one way or another. This is because IoT is applicable across many industry sectors, from smart cities, consumer and household businesses, automotive, and transportation, to agriculture, healthcare, supply chain, retail, fleet management, and manufacturing. The complexity of IoT presents challenges, but also opportunities for innovations. Regardless of what the definition of IoT is, you'll see throughout that there are several fundamental characteristics that define IoT. These are:



Sensors/Actuators

Sensors and actuators are the key building com ponents of an IoT device/object/thing, enabling it to generate data from its environm ent.

Connectivity

Connectivity refers to the com munication activity between IoT devices/endpoints, from IoT devices to an IoT platform. There are a variety of connectivity technologies that can be applied.

Data Generation/Sharing

Fundam ental to the concept of IoT, this is the ability for an IoT device to produce and provide data.

Enabling Technologies

In general, "enabling technologies" refers to cloud com puting technology that provides various services such as data storage, analytics, applications, SaaS, IaaS, and XaaS. Specifically, em erging technologies that increasingly play significant roles in m aking the IoT m ore valuable are Big Data Analytics, Artificial Intelligence, Machine Learning, Deep Learning, and Block Chain.

Data-driven Insights

The key reason behind im plem enting any IoT solution in any industry sector is the desire to generate values, either for business or personal purposes, using inform ation gathered to m ake observations or to take action. The value could com e in the form of productivity im provem ent, efficiency gains, process autom ation, cost reduction, quality-of-life im provem ent, m onitoring valuable assets, and so on.

Security

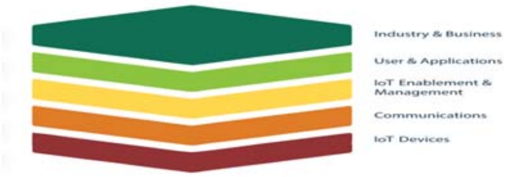
Though not an outcom e or a characteristic of an IoT application, cybersecurity (including privacy, reliability, and resiliency) is critical to the business success of IoT as well as to the privacy and safety of consum ers. The concept of hundreds or thousands of IoT devices belonging to the sam e network, all connecting to the Internet and being vulnerable to cybersecurity exploitation could cripple the entire IoT network, rendering the business inoperable.

Depending on the use case, data collected needs to be managed and most likely combined with other meaningful data such as customer, environmental, and product data. In order to turn data into valuable insights, these sources need to be analyzed through data analytics more sophisticated than a basic statistical model, such as General Artificial Intelligence, Machine Learning, and Deep Learning.

If one were to examine all of the reference architectures from every initiative around the world, one would find, much like the key characteristics of IoT, that there are many commonalities. All architectures offer clear identification of relationships between participants in the IoT ecosystem so accountability can be understood and assigned, implementation of IoT solutions in a timely manner as all necessary components and layers can be identified up front, and assurance of security, privacy, safety, reliability and other aspects to be placed front of mind from solution conception, rather than being added as an afterthought. The essential layers of an IoT reference architecture, shown here, have been developed for this course to represent the complexity of IoT in the most simple of terms, irrespective of the industry sector an IoT solution is deployed in.

IoT Reference Architecture

The IoT Reference Architecture shown here represents the complexity of IoT in simple terms.



Industry & Business

This layer highlights that any IoT solution should be viewed as part of a bigger ecosystem in a particular industry sector. It forces the solution to have linkage and consideration of a number of issues and concerns regarding local laws, regulations, compliance, security, procurement, data privacy, safety, and critical infrastructure.

In addition, as a business, it highlights the relationship and collaboration between the IoT solution owner/operator and the stakeholders that provide services, or products related to the solution.

Users & Applications

Key to any IoT solution, or deployment, is the purpose of why an IoT solution exists: What problems is it trying to solve, and who are the real beneficiaries of the solution?

This layer forces the solution owner to understand and/or define who their real customers are. An IoT solution could have multiple types of users, and each type of user can have different usage or consuming requirements.

For example, an IoT solution can include technical and operations staff, business users such as management, solution sponsors, and those that actually use the solutions to help improve their work/life.

IoT Enablement & Management Platform

This layer can also be viewed as an IoT platform, which is a very common, yet vague term used frequently in the industry. “IoT platform” can mean different things to different people.

This layer provides the following important functionalities:

- Data processing, storage, and analytics
- Networking and security
- Device management, device configuration, rule engine, event log, identity management
- Advanced functions from enabling technologies, such as artificial intelligence, machine learning (A.I.), and block-chain
- User interface management, API gateway, user security, Web portal, apps, visualization
- Communications protocols and management
- IoT Device and endpoints management

These features and functions are realized through different means. Some of these functions could be deployed close to the devices and gateway, which is often referred to as edge processing/computing, or Mobile Edge Computing (MEC). Others are cloud-based, or SaaS such as machine learning, big data, or storage.

Communications

Key to the IoT concept is communication between IoT endpoints and the IoT platform. There are many different technologies and protocols that can be implemented.

Connectivity technologies include:

- Wired – Ethernet
- Wireless short range – WiFi, Bluetooth, RFID
- Wireless long range – known as LPWAN (Low Power Wide Area Networks), which includes LoRaWAN, SigFox, NB-IoT/Cat-M1 (cellular), Weightless, Ingenu, WiSUN
- Cellular – includes NB-IoT/Cat-M1, LTE, Cat-1, 3G, GSM

Some of the most common communication protocols used in IoT deployments today are:

- MQTT (Message Queuing Telemetry Transport)
- CoAP (Constrained Application Protocol)
- HTTP (Hyper Text Transfer Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- SOAP (Simple Object Access Protocol)

IoT Devices or “Things”

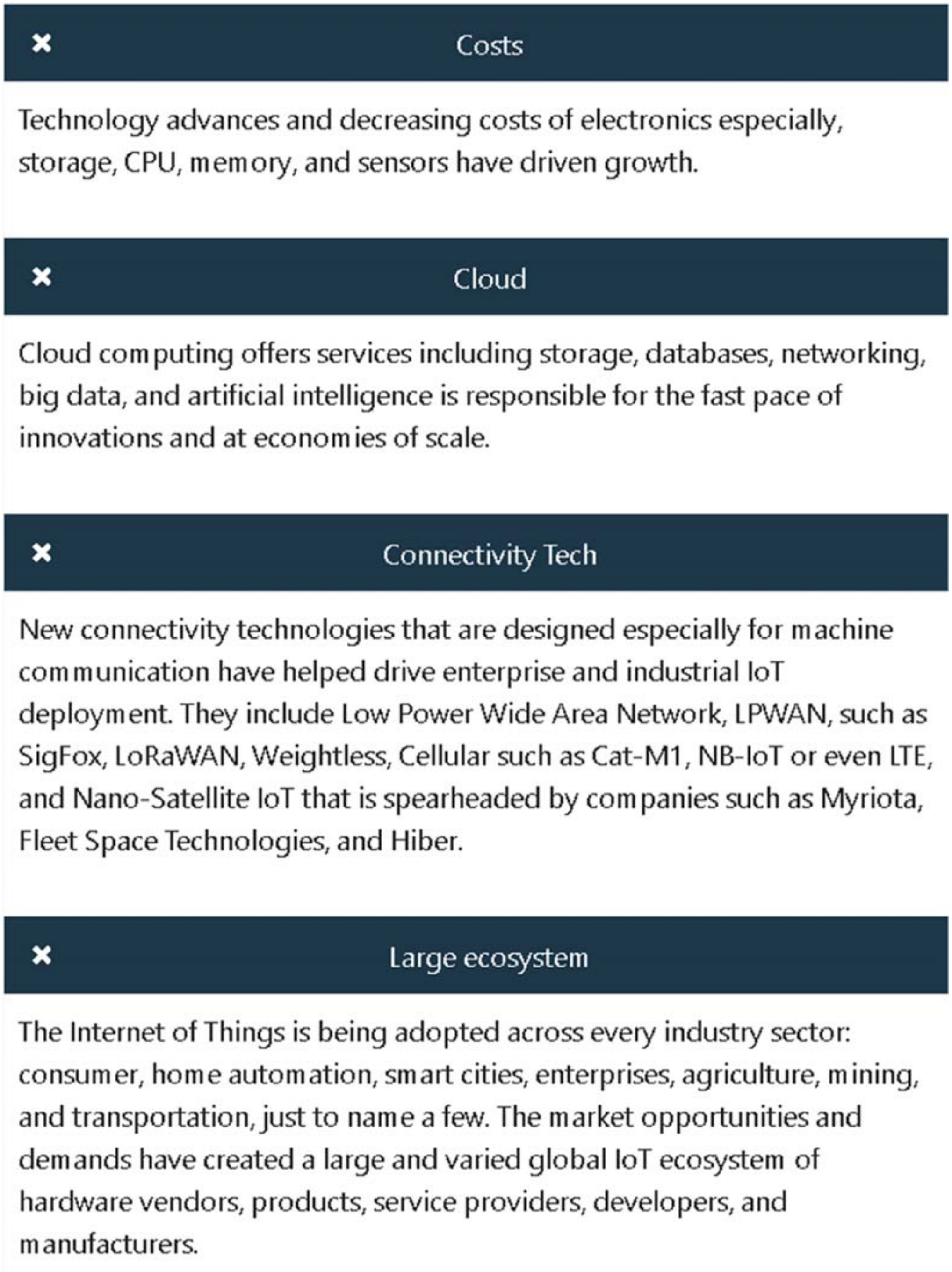
This layer refers to IoT endpoints, devices, or things.
IoT devices can be simple sensors that monitor one particular thing, such as temperature or moisture. Other IoT things can also be a stand-alone product such as a personal tracker, an ODB device, a connected camera, or a toy.
IoT devices or functions can also be embedded within a household item such as a washing machine, a refrigerator, a vehicle, or an air conditioner.

Drivers for the Internet of Things

The Internet of Things (IoT) has emerged in recent years as a major source of innovation and a growth driver for the global economy.

Advances in technology have meant that the costs of sensors, electronics hardware, CPU, and memory have greatly decreased, and computing power has increased in leaps and bounds. As a result, we have seen technological advancements in the Internet, cloud computing, big data, artificial intelligence, emerging digital technology like Blockchain, and new innovations in networking and Internet connectivity. Cloud-based services such as SaaS, IaaS, and PaaS have become very affordable. This has created a perfect storm for what is known as the Internet of Things, or IoT.

The following technological advancements and trends are driving the IoT market:



✖ **Costs**

Technology advances and decreasing costs of electronics especially, storage, CPU, memory, and sensors have driven growth.

✖ **Cloud**

Cloud computing offers services including storage, databases, networking, big data, and artificial intelligence is responsible for the fast pace of innovations and at economies of scale.

✖ **Connectivity Tech**

New connectivity technologies that are designed especially for machine communication have helped drive enterprise and industrial IoT deployment. They include Low Power Wide Area Network, LPWAN, such as SigFox, LoRaWAN, Weightless, Cellular such as Cat-M1, NB-IoT or even LTE, and Nano-Satellite IoT that is spearheaded by companies such as Myriota, Fleet Space Technologies, and Hiber.

✖ **Large ecosystem**

The Internet of Things is being adopted across every industry sector: consumer, home automation, smart cities, enterprises, agriculture, mining, and transportation, just to name a few. The market opportunities and demands have created a large and varied global IoT ecosystem of hardware vendors, products, service providers, developers, and manufacturers.

Let us look at a simple illustration of how IoT saved a situation

Taking care of John:

A father, John, lives a plane ride away. John is 70 years old, diabetic suffers from arthritis, and lives independently. John is reasonably active and is a creature of habit. He goes about his day in a fairly predictable manner. Every morning without fail, John gets up at 6:30 a.m. He turns off his alarm, goes to the kitchen to put on the kettle, and turns on the TV to watch the morning news. John checks his blood sugar levels and takes his insulin. He never misses his daily news on TV while drinking his favorite cup of coffee and eating a light breakfast. On most days, he goes out to his garden to read the newspaper. His daughter, Maria, lives about 10 minutes away from John by car. She works remotely, so her job allows her to be his primary caretaker. John has had quite a few health scares, given that he lives alone. It was suggested to his son and Maria that they invest in some kind of internet-connected devices that can be accessed by either of them and be controlled from anywhere and at any time to virtually check in on John.

A few weeks later on a Wednesday morning, John wakes up late, never hearing his alarm go off at 6:30. He doesn't feel right. His bedroom seems to be spinning around him. He can't reach the phone for help. He is stuck and feeling helpless. John's house is now equipped with several internet-connected devices. The power plugs for his coffee pot and TV are smart plugs that detect the appliances being used, at what time they are being used, and how many times they are used during the day. His refrigerator door is also equipped with a connected device. Among its features, it counts the number of times the door has opened. All of the doors to the house have smart locks that monitor comings and goings. John's water usage is also recorded. A device monitors when and where water has been used around the house, such as the water in the kitchen, bathroom, and garden hose. On this Wednesday morning, Maria and her brother were notified with SMS messages that there are no activities recorded from John's home within the first 30 minutes of his day. He hadn't checked his blood sugar since the previous afternoon, a very unusual pattern and uncharacteristic of John. The son tried calling John's phone, but he doesn't answer. The son calls Maria, and she tells him that she is already in her car to check on John. Minutes later, Maria uses her smart device to open John's smart lock. Maria finds her father lying on the floor near the garden door, barely responsive. The son can see from the SMS messages on his phone that Maria had entered the house and called for an ambulance, so he was not surprised when she called him seconds later to tell him that help is on the way.

John meets with his doctor at the hospital and is released the next day. Let's take a look at how the Internet of Things saved him from a more serious health concern. John's activities through the day had been non intrusively monitored, recorded, and sent to the cloud for further analysis. And, with a little help from machine-learning technology, John's daily pattern was established, learned, and predicted. Unusual patterns were quickly flagged and given the pre-determined severity of his lack of activity, notifications and alerts were raised and forwarded to John's caregivers. Within minutes of receiving a red alert on their phones, the son and his sister were able to get John the help he needed. There are a number of IoT Solutions that provide living at home assistance. John's solution consists of many devices, but let's follow the path of the smart plugs to illustrate how his IoT Solution worked. John's smart plugs go into power points where his most frequently used household appliances are plugged in. These smart plugs are logged into a wifi network to communicate with a gateway. The IoT gateway is a cellular router which has cellular back haul connectivity to an application

> *server. The gateway provides a dedicated wifi network for all the smart plugs in the household. When an appliance is used such as when John's toaster is put on, the smart plug senses a current being drawn and reports it as an activity to the gateway. John's interaction with his smart devices generates data. Activities recorded from each household appliance with a smart plug are sent to an application server. The collected data is processed by the application. Artificial Intelligence, or rather, machine learning is applied in order to establish John's regular daily pattern. Rules are applied in order to trigger notifications or alarms. When an irregular pattern is established, such as certain activity missing, or not recorded, indicating something might have happened to the person concerned. To close the loop, once the rules are applied and an alert is triggered, the alerts are sent to John's caregivers.*

How did IoT Help?

IoT is not an industry; it is a concept that can be applied across many industries and sectors. IoT could be viewed as a transformational enabler that brings economic and social benefits to society. For example, the correct application of IoT saved John from potential personal health issues. John's house has been equipped with several types of Internet-connected devices, often referred to as smart home devices. How did each of the devices help monitor John's well-being?

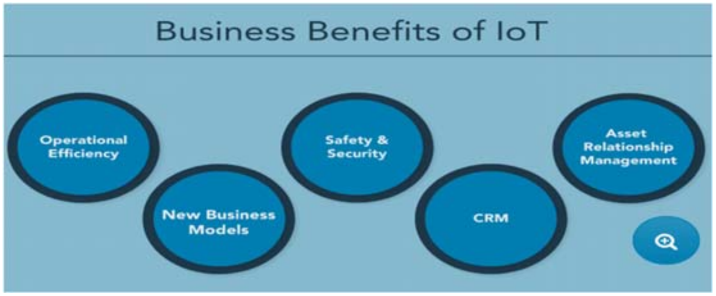
Business Opportunities of IoT

Adoption of IoT

A recent survey conducted by Microsoft in markets across the US, the UK, Europe, China, and Japan, and in five key industries—Manufacturing, Retail/Wholesale, Government, Transportation, and Healthcare—found the following reasons influencing their IoT adoption strategy.

These survey results reflect the main reasons for the adoption of IoT. Business decision makers see these as potential business benefits that could be achieved if IoT is adopted appropriately.

Summary of key business benefits of IoT



Business process optimization – Optimized business processes mean better business operations. Simply put, IoT applications generate valuable data which can enable organizations to fine-tune their business operations through better decision-making. This is referred to as data-driven decision-making.

Predictive maintenance – The use of IoT and AI allows an organization to catch problems before they disrupt business operations, be it a machine in a factory that stopped functioning, or a fleet vehicle that broke down, or a water pump that stopped working in a plant. Here are some benefits of predictive maintenance:

Cost savings - Manufacturers' savings from predictive maintenance could globally total between $240 and $630 billion by 2025 according to a report.

Strengthening workplace safety – Properly maintained plant equipment can have a direct impact on employee safety.

Reduced downtime – Well-maintained equipment minimizes equipment failure.

Increased quality – Improving products, and processes through machine-learning and detecting maintenance issues early increases customer satisfaction.

Greater efficiency and output – Process efficiency, asset utilization, and production output are increased.

Social Impact of IoT

The Internet of Things promises to bring positive impacts to society through applications in various industry sectors such as Smart Cities, Health Care, Smart Homes, and Transport, to name a few.

Environment

There are many ways that IoT applications could directly or indirectly impact our environment, such as reducing vehicle pollution. Intelligent transport is an area where many IoT applications—traffic monitoring, connected vehicles, fleet management, and traffic route optimization—could contribute to reducing carbon emissions. Smart building management systems are another area where IoT applications can optimize HVAC energy consumption and water usage, thus reducing waste and unnecessary energy consumption.

Health Care

Data generated by wearable IoT consumer devices, such as the Apple Watch or Fitbit, allows people to get a much better understanding of their health.

Safety & Security

IoT provides assistive technologies to better support vulnerable people, such as the elderly or people with dementia or autism. Some examples include smart home devices, personal location tracking devices for people with autism and dementia, and personal safety alert devices for lone workers.

In the smart home market, IoT can provide a sense of security through safety monitoring. For example, a Swedish company has created a non-intrusive way to monitor fire (smoke), heat (temperature), noise, and motion in the home which alert the owner or household members if a condition is detected.

Education

IoT devices are being used to provide interactive, cause-and-effect experiences to assist students, especially early learners and those with special needs, with a more engaging way to learn.

Convenience/Automation

In the smart home segment, many time-consuming household chores and activities are being automated.
Garden irrigation systems are already automated. However, IoT gives more flexibility to controlling and changing system settings from anywhere and at any time.
With smart door locks we no longer need to fumble for our keys, we don't have to be home to open the door to let people in, and we can see who's at the door before we allow them in.

IoT applications such as smart parking allow us to find available parking spots quickly.

IoT Supporters and Influencers

Apart from large corporations and businesses, which are already deeply involved in the Internet of Things, governments, regulators, non-profit organizations, standards bodies, and industry representative groups are also preparing for the IoT wave, or the 4th industrial revolution, and the opportunities and challenges that it could bring.

IoT- Advantages

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer:

Improved Customer Engagement – Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.

Technology Optimization – The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

Reduced Waste – IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.

Enhanced Data Collection – Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

IoT – Disadvantages

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues:

Security – IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.

Privacy – The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.

Complexity – Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.

Flexibility – Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.

Compliance – IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

Wearable Electronics

Wearable electronic devices are small devices worn on the head, neck, arms, torso, and feet.

Smartwatches not only help us stay connected, Smart glasses help us enjoy more of the media and services we value, but as a part of an IoT system, they allow access needed for improved productivity.

Current smart wearable devices include:

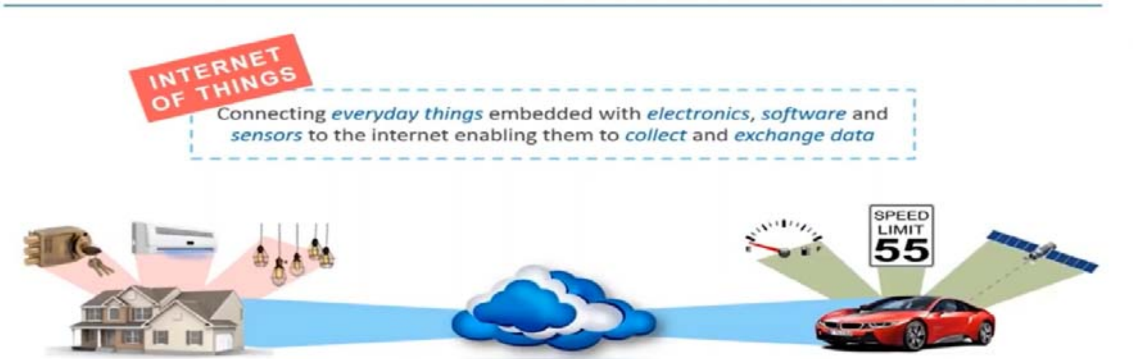
Head – Helmets, glasses

Neck – Jewelry, collars

Arm – Watches, wristbands, rings

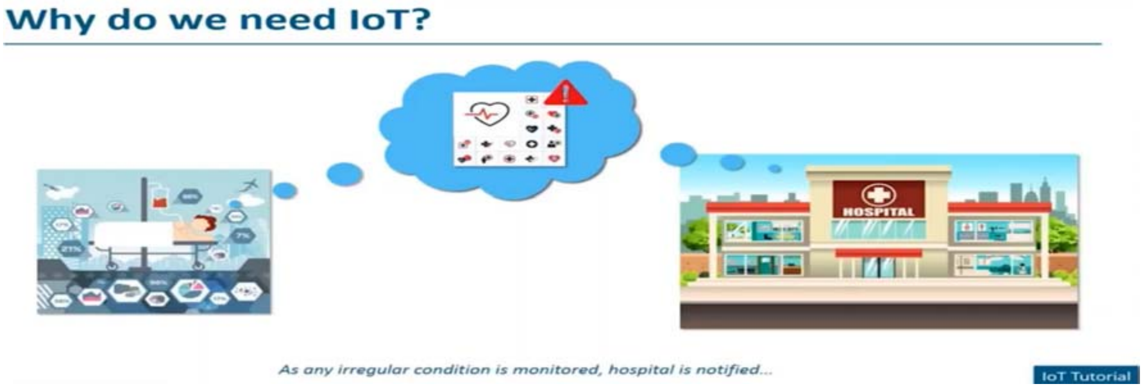
Torso – Clothing, backpacks

Feet – Socks, shoes



Connecting *everyday things* embedded with *electronics*, *software* and *sensors* to the internet enabling them to *collect* and *exchange data*

The home and the appliances (AC, refrigerator, Cooker, light, etc.) in it are connected to the mobile devices of the owner, allowing for remote control and automation.

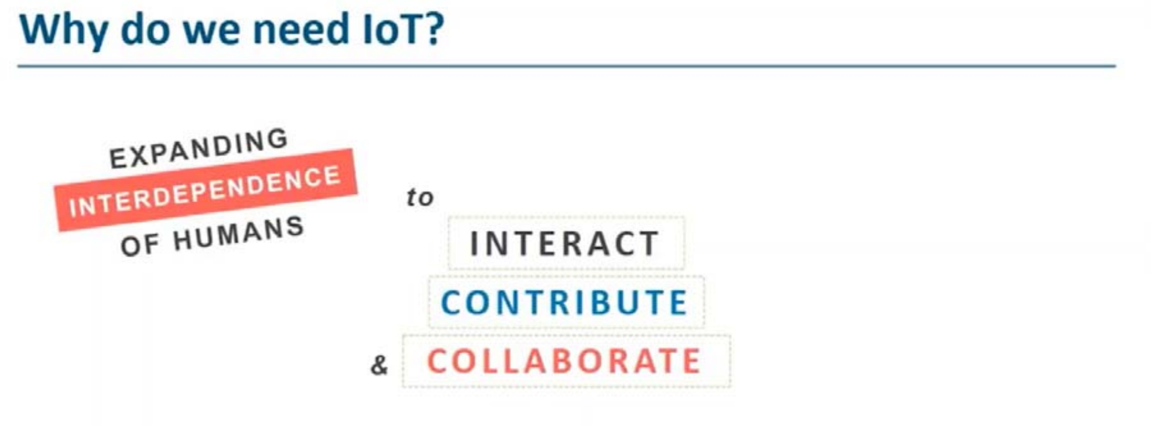


Why do we need IoT?

As any irregular condition is monitored, hospital is notified...

IoT Tutorial

The vital signs of the patient at home are monitored via IoT. If any measurement goes beyond normal, it can be seen from the hospital or the hospital will be alerted and an ambulance is rushed to the home. Before the ambulance arrives back at the hospital, all the facilities are ready for the patient based on his report.



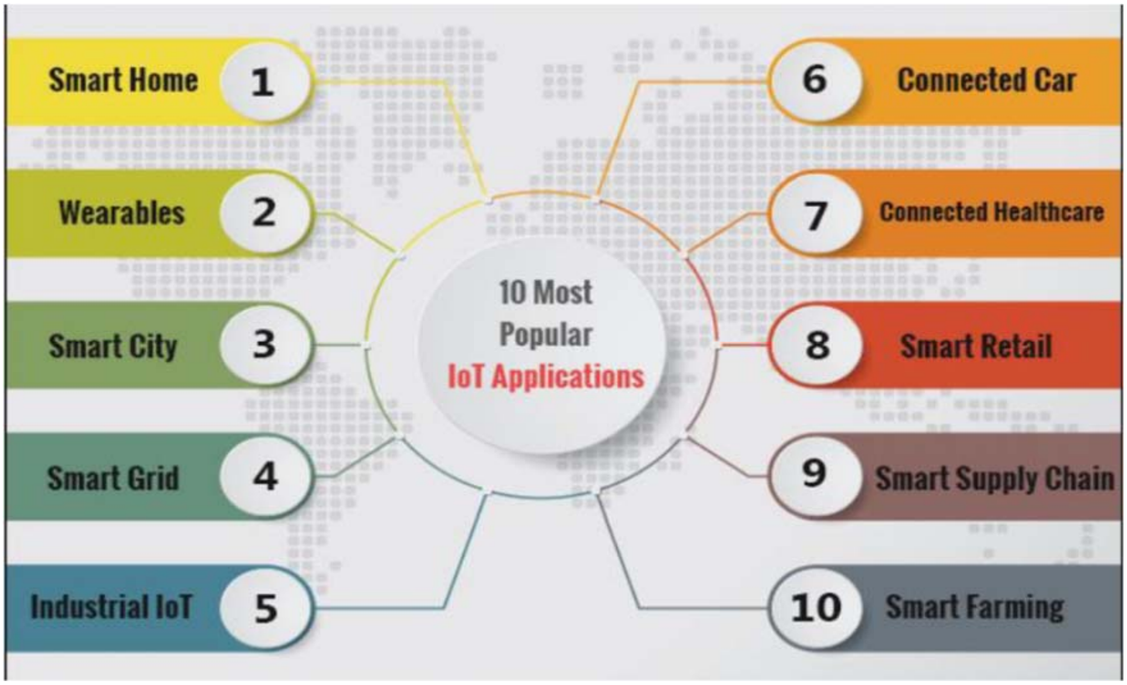
Why do we need IoT?

EXPANDING INTERDEPENDENCE OF HUMANS to INTERACT CONTRIBUTE & COLLABORATE

Iot brings about:

- Efficient utilization of resources
- Minimizing human effort
    - Smart home, hospital, office, etc.
- Saves time
- Development of AI through IoT
- Improved security

Popular applications of IoT:



Smart City

A smart city is an intelligent city that integrates digital technologies into its networks, services, and infrastructure. It means smart urban transportation networks, upgraded water supply, waste disposal facilities, efficient ways to light and heat buildings

The main objective of a smart city is to promote cities that provide core infrastructure, a clean and sustainable environment, and give a decent quality of life to citizens through the application of 'smart solutions.' These cities make the most out of the information and communication technologies to improve the level of services, their citizen's well-being, sustainability, and overall economic growth.

Advantages of Smart City

There are several advantages of Smart City, and learning about these can help you to weigh the benefit.

- **Better transportation services**: A smart city has the potential to drastically improve the current level of transportation throughout a city. It will have better traffic management, the ability to track public transportations and serve its citizens better with constant information and low prices.
- **Safer Communication:** A smart city will have the most technological advances and partnerships with the private sector will benefit society since there will be lesser criminal activity. Example of such technology is license plate recognition, connected crime centers, shooting detectors, better emergency services, and body cameras.
- **Efficient public services:** Since there is a limited amount of natural resources left to meet the demand of the people, smart cities will have technologies and the necessary tools to cut down on our usage of natural resources and decrease the waste of water, electricity, etc. without having to cut down on any factors.
- **Reduced environmental footprint:** A smart city has thousands of energy-efficient buildings that can improve the air quality, use renewable energy sources, and decrease the dependence on non-renewable energy sources. These will help to decrease the ecological impact we have on the environment.
- **More digital equity:** People must have access to high-speed internet services at affordable prices and devices. If they have access to public Wi-fi in local areas in the city, all residents will have equal opportunities.
- **Economic development opportunities:** Investing in smart cities will lead to improving their regional and global competitiveness and attract new residents and improve business. Since the entire city will have access to an open data platform, information, etc. companies will flourish.

They can make informed decisions with the available technologies and lead to economic development.

- **Improvement of infrastructure:** Old roads, buildings, highways, bridges require massive investments to maintain their state and increase their useful life. But, with the help of smart technologies, cities will have the ability to analytically predict and identify the areas that can cause infrastructure failures before it occurs.
- **Job opportunities:** A smart city will have many businesses and job opportunities since the people will get equal access to basic resources such as transportation, internet connection, and job offers.
- **Decrease of crime:** Since the authorities can monitor the dealings of people closely with the help of technology, there will be a reduced amount of crime. Besides, crime increases when there are fewer jobs and more unemployed people. However, if job opportunities increase, it will simultaneously lead to a decrease in crime.

Disadvantages of Smart City

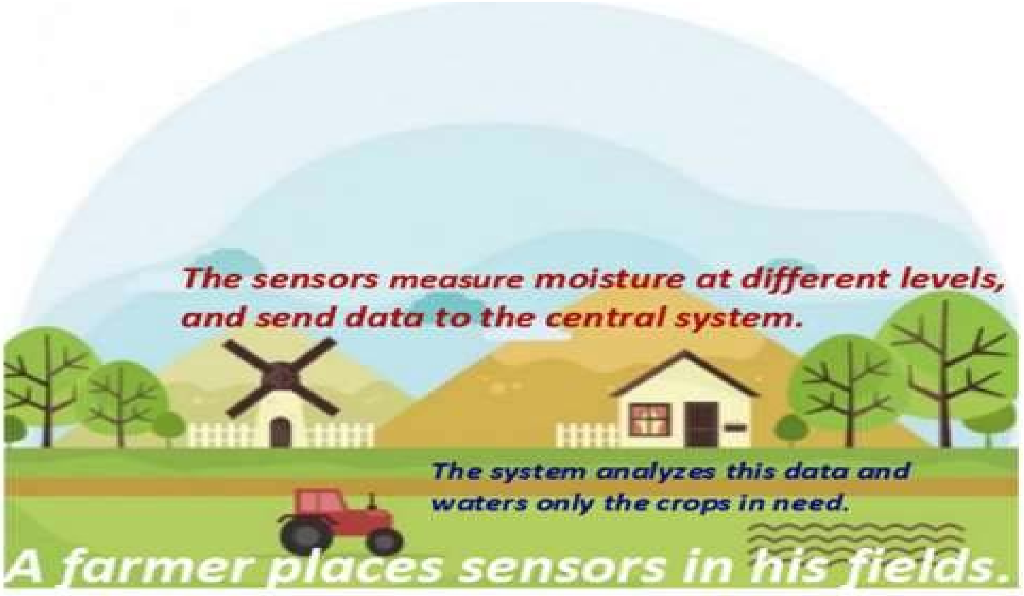
Though Smart City has many advantages, there are some disadvantages. Knowing these can help one to understand the other side of the coin.

- **Limited privacy:** Since the authorities or the government will have access to security cameras and intelligent systems connected through many different spaces, the citizens will have difficulty in maintaining their anonymity. Facial recognition and such things will drastically change the concept of privacy or personal space.
- **Social control:** The people who can track and centralize the data they gather with security cameras will have greater power. It can be a government, a private agency, or other authorities. They will have the power to control a citizen’s data and can easily manipulate public opinions.
- **Excess network trust:** Since the citizen of these smart cities will rely almost entirely on electronics and networks, they will lose autonomy in their decision-making and could become incompetent. They would not be able to react appropriately in a scenario where these tools are not usable.

Smart Farming (Agriculture)

The Internet of Things has made smart farming possible. Now, you may wonder what exactly is smart farming. Smart farming is a capital-intensive and hi-tech method of **growing food cleanly and sustainably**. We can also call it the application of **ICT (Information and Communication Technology)** in Agriculture. IoT in agriculture uses robots, drones, remote sensors, and computer imaging combined with continuously progressing machine learning and analytical tools for **monitoring crops, surveying, and mapping the fields, and providing data to farmers for rational farm management plans to save both time and money**

When we talk about IoT-based smart farming, we are looking at a system built to monitor the crop field with the help of sensors. These sensors track every essential for crop production like soil moisture, humidity, light, temperature, etc., and automate the irrigation system. This system allows farmers to monitor the field conditions from anywhere. IoT-based farming is way too efficient when compared to conventional farming.


The sensors measure moisture at different levels, and send data to the central system.
The system analyzes this data and waters only the crops in need.
A farmer places sensors in his fields.

Precision Farming

Precision farming, also known as precision agriculture, is anything that makes the whole process of farming accurate and controlled when it comes to raising livestock and growing crops

Agricultural Drones

Technology has progressed significantly and at a higher rate in the past few years. Agricultural drones are a prime example of this development. Drones are being used in the agricultural sector to enhance many farming practices.

The two types of drones- ground-based and aerial-based drones are being used in agriculture for crop health assessment, crop monitoring, spraying pesticides, irrigation, planting, and analyzing the field. These drones capture multispectral, thermal, and visual imagery during their flight.

Since IoT is about sensors, data collection, and analysis, the more data collected in offices and crime scenes, with the right tools, the time stamp on the recorded data, and events can surely be of help in resolving court cases.

IoT is already been used in solving difficult crimes where the prime suspects (eventual real criminals) are been investigated using data from smart devices (mostly without them knowing), this is done by checking some devices (things) directly, or data transmitted to cloud storage, connected to IoT directly or in a forensic lab.

Some of these IoT devices that give away hard criminals who thought that they have left no trail to their crimes are:

Smartphones and apps, Fitbit wristbands, Smartwatches, Debit/credit payment cards, Email accounts, Internet sites visited, Things bought online, etc.

Handling Internet of Things Data in Litigations

As the reach of the Internet of Things (IoT) expands, counsel must learn to harness the increasing explosion of data to effectively extract relevant information in litigation while balancing the operational and privacy challenges that these new sources of digital evidence raise.

Preserving Iot Data

At the outset of a dispute, counsel should analyze whether IoT devices and data may be relevant to any party's claims or defences. While not every case will implicate IoT data, where IoT data may be relevant, counsel should determine early on the potential need to specifically address IoT devices and data with:

- The parties' counsels represent.
- Adverse parties or non-parties.

As with other forms of ESI (Electronically Stored Information), a data's source or location is a consideration when determining whether and how to ensure the preservation of IoT data. Counsel should keep in mind that IoT data is likely to exist in multiple locations that are controlled by various parties and non-parties, including service providers, device manufacturers, and owners of tangible IoT devices.

Collecting And Requesting Iot Data

Where IoT data is relevant in litigation, counsel must carefully consider:

- Defensible methods to collect IoT data.
- The appropriate parties or non-parties from whom to request the relevant IoT data.
- The potential need for protective orders, given the privacy and confidentiality issues that the disclosure of IoT data is likely to raise.

Collection Methods

The collection of IoT data may take multiple forms. As with other forms of ESI, a vendor may be retained to forensically collect the data. Alternatively, data that is readily accessible from an IoT device or a related application or website may be collected by counsel or the client. However, if counsel intend to collect the data, or have the client collect the data, counsel should consider discussing collection methods with opposing counsel to eliminate objections later.

Some cases busted using data/information from smart devices

iPhone health app data used to uncover a murder plot in the UK

Date: 5th December 2018

Location: United Kingdom

On 14 May 2018, the husband of the victim, a pharmacist living in Linthorpe in Middlesbrough, subdued his wife with an insulin injection before strangling her. He then ransacked the house to make it appear like a burglary. The data recorded by the health app on the murderer's phone, showed him racing around the house as he staged the burglary, running up and down the stairs. The victim's app showed that she remained (still) after her death apart from a movement of 14 paces when her husband moved her body outside to make it look as though the burglar left it there. Prosecutors said his motivation had been to flee to Australia to be with his lover and start a new family. He also stood to inherit a £2m life insurance policy.

Source: https://www.theguardian.com/uk-news/2018/dec/05/uk-pharmacist-mitesh-patel-jailed-for-30-years-wife-jessica-murder-premeditated?CMP=Share_iOSApp_Other

Police Use Fitbit Data to Charge 90-Year-Old Man with murder

Date: 3rd October 2018

Location: United States of America

The 90-year old suspect when to his stepdaughter's house at San Jose, California for a brief visit. Five days later, his stepdaugter's body, Karen was discovered by a co-worker in her house with fatal lacerations on her head and neck. The police used the data recorded by the victim's Fitbit fitness tracker to determine the time of the murder. It was been reported that the Fitbit data showed that her heart rate had spiked significantly around 3:20 p.m. on September 8, when her stepfather was there.Then it allegedly recorded her heart rate slowing rapidly, and stopping at 3:28 p.m., about five minutes before he left the house.

Source: https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

Witness "Alexa" is called to give evidence in ongoing murder investigation in Florida

Date: 1st November 2019

Location: United States of America

A woman was killed by a spear to the chest at her home in Hallandale Beach, Florida, north of Miami, in July. Witness "Alexa" has been called yet another time to give evidence and solve the mystery. The police are hoping that the smart assistance Amazon Echo, known as Alexa, was accidentally activated and recorded key moments of the murder. "It is believed that evidence of crimes, audio recordings capturing the attack on victim Silvia Crespo that occurred in the main bedroom … may be found on the server maintained by or for Amazon," police argued and managed to obtain the recordings. The victim's husband, who is the primary suspect at the moment, denies the offence.

Source: https://www.theguardian.com/us-news/2019/nov/01/alexa-florida-death-witness-amazon-echo

Apple Watch data assist in a murder investigation

Date: 3rd April 2018

Location: Australia

The body of a 57-year-old was found in the laundry room of her home in Valley View, Adelaide, in September 2016. Her daughter-in-law who was in the house at the time of the murder claimed that she was tied up by a group of men who entered the house and managed to escape when they left. However, the data from the victim's smartwatch did not corroborate her story.The prosecution alleged that the watch had recorded data consistent with a person going into shock and losing consciousness. "The evidence from the Apple Watch is a foundational piece of evidence for demonstrating the falsity of the defendant's account to police," said the prosecutor.

Source: https://www.bbc.co.uk/news/technology-43629255

Apple health data used in a rape and murder investigation

Date 11th January 2018

Location Germany

A 19-year-old medical student was raped and drowned in the River Dresiam in October 2016. The police identified the accused by a hair found at the scene of the crime. The data recorded by the health app on his phone helped identify his location and recorded his activities throughout the day. A portion of his activity was recorded as “climbing stairs”, which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up. Aparently, an investigator of similar build to the suspect went to the area where the body was found and recreated how the police believe he disposed of the body. "For the first time, we correlated health and geo-data," chief of police reportedly told the court.

Sources: https://www.vice.com/en_us/article/43q7qq/apple-health-data-is-being-used-as-evidence-in-a-rape-and-murder-investigation-germany and https://www.bbc.co.uk/news/technology-42663297

Fitbit data tests murder suspect's alibi

Date: 27th April 2017

Connecticut police have used the data collected by a murder victim's Fitbit to question her husband's alibi. Richard Dabate, accused of killing his wife in 2015, claimed a masked assailant came into the couple's home and used pressure points to subdue him before shooting his wife, Connie. However, her Fitbit's data acts as a "digital footprint", showing she continued to move around for more than an hour after the shooting took place. A 2015 report from the National Institute of Justice predicted that the data derived from digital devices will form an increasingly important part of criminal investigations.

External Link to Story

https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate

New Hampshire double murder case in another Amazon Echo case

Date: 14th November 2018

Location: United States of America

In yet another murder case, a New Hampshire judge ordered Amazon to turn over two days of Amazon Echo recordings in a double murder case in November 2018.

Prosecutors believe that recordings from an Amazon Echo in the Farmington home where two women were murdered in January 2017 may yield further clues as to who their killer might be. Though the Echo was seized when police secured the crime scene, the recordings are stored on Amazon servers.

Timothy Verrill, of Dover, New Hampshire, was charged with two counts of first-degree murder but pleaded not guilty and awaits trial. The order granting the search warrant, said that there is “probable cause to believe" that the Echo picked up "audio recordings capturing the attack" and "any events that preceded or succeeded the attack." Amazon has also been directed to hand over any "information identifying any cellular devices that were linked to the smart speaker during that time period." Amazon told the Associated Press that it wouldn't release any information "without a valid and binding legal demand properly served on us."

Is it forensic in Nigeria? (Evidence Act)

Data from smart devices, smart computing and IoT may not be forensic or easy to use as evidence to prove a case, but the security agencies (investigators) surely have something to probe a suspect and get confession.

Other ways that SMART Computing and IoT can be of great service to the courts and the judiciary:
Is virtual proceedings possible?
Can a witness appear virtually?
Can the public follow proceedings online? Especially law students.

Conclusion

With the current state of computer technology, smart computing, IoT and the adoption and usage by all, it is imperative that our security agencies will use greatly the trillions of Gigabytes of (Big) Data that contain in it some information that can be used to crack, especially criminal cases. These data may not be accepted as evidence in our courts for now but can be used to make a suspect confess.

THANK YOU FOR LISTENING

References:

- Khushboo Roy & Neelendra Badal (2020): An Intelligent Approach for Improving the Effectiveness of Smart Computing. *International Journal of Computer Applications (0975 – 8887) Volume 175 – No. 28, October 2020*: Kamla Nehru Institute of Technology https://doi.org/10.5120/ijca2020920807
- Samantha v. Ettari, e-discovery counsel, Kramer Levin Naftalis & Frankel LLP. Handling Internet of Things Data in Litigation E-Discovery Bulletin. https://www.kramerlevin.com The Journal, Litigation, January 2019
- Understanding Security in The IoT Ecosystem, International Information Systems Security Certification Consortium (ICS^2)

- https://privacyinternational.org/timelineiotincourt
- http://us.practicallaw.com