NATIONAL OPEN UNIVERSITY OF NIGERIA

FACULTY OF SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

COURSE CODE: CIT882

COURSE TITLE: INTERNET OF THINGS

COURSE GUIDE

Introduction

CIT 882 Internets of Things is a Two [2] credit unit course of four modules with eleven units. It is designed to train you for the use of the internet of things in the world of Enterprise. The knowledge gained in this course would lead to proficiency in the usage and application of IoT across different domains. As a computer scientist, savvy in technology, it is advised that you study each unit carefully to ensure you gain the desired skills and knowledge required in the implementation of the Internet of Things. The course material is made up of four modules.

Module 1: This module provides a foundation for the course. In this module, we described the concept of Things and the Internet. The definitions of IoT and the essential Characteristics of IoT provided different applications with diagrammatic representation and provided other details that will help you understand the remaining parts of the course. Also covered in the module are the various design and development considerations, security issues with using IoT, and the evolving extension of the Internet of Everything.

Module 2: The building blocks of IoT are extensively discussed in this module. Four things form the basic building blocks of the IoT system – sensors, processors, gateways, applications. Each of these nodes has to have its characteristics to form a useful IoT system.

Module 3: This module examined the security considerations and challenges in the IoT Network Layer, Support Layer, and application layer. Also, the attack and vulnerabilities with countermeasures of open-source solutions. The security considerations and solution in the IoT Network Layer, Support Layer, and application layer was also discussed. the attack and vulnerabilities with countermeasures of open-source solutions are explained. IoT Use Case in Utility Companies especially the Automatic Smart Metering and Autonomous Vehicle, the IoT Security in Utility challenges and IoT security solutions and IoT security in Manufacturing industry were described.

Module 4: The internet of everything (IoE) is a broad term that refers to devices and consumer products connected to the internet and outfitted with expanded digital

features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices, and items connected to the global internet. The positive impact of the IoT on citizens, businesses, and governments will be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety.

This Course Guide gives you a brief overview of the course content and course materials.

Course Competencies

In this course, you will be exposed to the introductory aspect of IoT and its application across different industries, the use of Data Analytics with business and its efficiency, and other applications such as remote monitoring, smart homes, IoT in Diary Farms e.t.c.

Course Aims

This course aims to equip you with the explicit knowledge of the internet of things and the devotion that brings about digital transformation in the IoT industry. By the end of the course, you should be able to confidently work on IoT architecture and describe the use cases as applicable to different domains

Course Objectives

At the end of this course, you should be able to:

- identify various application areas of IoT
- identify the vulnerabilities and attacks in IoT
- build a countermeasure against the vulnerability
- identify opportunities in IoT

Working Through this Course

To have a thorough understanding of the course units, you will need to read and understand the contents of this course and explore the impact and application of the Internet of Things in today's world. A lot of Use cases example was given in this course, to help understand the concept and the essential security measure to put in place when discussing as well as implementing IoT

Study Units

There are 11 units in this course

Module 1: Introduction to Internet of Things (IoT)
Unit 1: Introduction to Internet of Things (IoT)
Unit 2: IoT Origin and Impact Contents
Unit 3: Overview of IoT-in Digital Transformation

Module 2: Building Blocks of IoT
Unit 1: Building Blocks of IoT
Unit 2: IoT Device Architecture
Unit 3: Platforms Supporting IoT

Module 3: Security Considerations Using IoT
Unit 1: Security Considerations Using IoT
Unit 2: IoT Security Considerations Solutions
Unit 3: IoT Use Cases

Module 4: Internet of Everything (IoE)
Unit 1: Opportunities with IoT
Unit 2: Internet of Everything (IoE)

References and Further Reading

Overview of IoT-in Digital Transformation - Bing

Alavi A., Jiao P., Buttlar W., and Lajnef N., (2018), "Internet of Things-enabled smart cities: State-of-the-art and future trends," Measurement, vol. 129, pp. 589-606

Paraszczak J., (2014), "Maximization of productivity of autonomous equipment in underground mines,", Mining Engineering, vol. 66, no. 6, pp. 24- 34,40-41

Shukla D. (2020), Data Management Systems for The IoT Devices | IoT device management (electronicsforu.com)

Idowu, Park, Ibrahim (2017), A New IoT Architecture for a Sustainable IoT Adoption. International Journal of Computer Science and Information Technology Research Vol. 5, Issue 2, pp: (204-208)

Kumar and Mallick, (2018), The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. International Conference on Computational Intelligence and Data Science (ICCIDS 2018) Procedia Computer Science 109–117

Internet of Things (IoT) - Part 2 (Building Blocks & Architecture) (c-sharpcorner.com)

Knowledge byte: Building Blocks of IoT Architecture | Cloud Credential Council of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Abu-Elkiheir M, Hayajneh M, and Abu N (2013) Data Management for the Internet of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Fuller J. R (2016), The 4 stages of an IoT architecture. How to design an IoT-ready infrastructure: The 4-stage architecture (techbeacon.com)

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127IoTrpt.pdf

7.0 Further Reading

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website:

https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127IoTrpt.pdf

Corser G. et al (2017), Internet of Things (IoT) Security Best Practices. IEEE Internet Technology Policy Community White Paper. internet_of_things_feb2017.pdf (ieee.org)

Strategic

IoE_Economy_FAQ.pdf (cisco.com)

Internet of Everything - GeeksforGeeks

Revolutionized IoT - Internet of Everything - GeeksforGeeks

Banafa A., (2016) The Internet of Everything (IoE)

The Internet of Everything (IoE) | OpenMind (bbvaopenmind.com)

Internet of Everything Market Statistics and Industry Analysis | Forecast (alliedmarketresearch.com)

What is the Internet of Everything (IoE)? - Definition from Techopedia

http://www.cisco.com/web/about/ac79/innov/IoE.html

Internet of Everything Explained - Internet of Things Wiki

Module 1: Introduction to Internet of Things (IoT)

Module Introduction

This module provides a foundation for the course. In this module, we described the concept of Things and the Internet. The definitions of IoT and the essential Characteristics of IoT provided different applications with diagrammatic representation and provided other details that will help you understand the remaining parts of the course. Also covered in the module are the various design and development considerations, security issues with using IoT, and the evolving extension of the Internet of Everything.

Unit 1: Introduction to Internet of Things (IoT)
Unit 2: IoT Origin and Impact Contents
Unit 3: Overview of IoT-in Digital Transformation

Unit 1: Introduction to Internet of Things (IoT)

Contents

1.0 Introduction

In this unit, we shall provide a foundation for this course on the Internet of Things (IoT). To achieve this, some basic concepts of Things and the Internet are discussed. The definitions of IoT and the essential Characteristics of IoT. Specifically, different applications of IoT will be described and diagrammatic representation will be presented to aid the understanding of the remaining part of this course.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Explain the meaning of Things, with respect to the Internet of Things (IoT)
2. Describe the characteristics of IoT
3. Explain some desirable Applications of IoT

3.0 Main Content

3.1 Overview of IoT

A thing, in the respect to the Internet of things (IoT), is a physical object with a unique identifier, an embedded system, and the capability to transfer data over a network and actuators that permit things to act (such as to open or close a door, to switch on or off the light, to increase or decrease engine rotation speed and more). Things are objects of the **physical** world (physical things) or of the **information** world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static or dynamic.

Physical things exist in the physical world and are capable of being sensed, actuated, and connected. Examples of physical things include the surrounding environment, industrial robots, goods, and electrical equipment.

Virtual things exist in the information world and are capable of being stored, processed, and accessed. Examples of virtual things include multimedia content and application software.

3.2 Definitions

The Internet of Things (IoT) is a reference to a collection of devices or objects that are linked together using an Internet connection. The hub for the collection (the "things" part) is what sends and collects data using the Internet, which helps the devices to make decisions and remember particular patterns and routines for action to be carried out without any manual involvement. IoT simply means the connection of multiple devices to the internet.

ITU Definition:

"The IoT can be viewed 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)."

These devices can include multiple appliances that need to be connected for reasons including automation and real-time control of the device. As the IoT has both real-time and historical data stored, it can provide effective decision-making instructions

to devices, and control certain actions and aspects of when and how they function. This technology enables your systems and devices to be automated cost-effectively. This concept includes buildings, vehicles, production machinery, fridges, street lamps, rehabilitation equipment, and everything else imaginable. The sensors are not in all cases physically attached to the things, sensors may necessitate monitoring, for instance, what happens in the closest environment to a thing.

The Internet of Things (IoT) is an emerging paradigm that enables the communication between electronic devices and sensors through the internet to facilitate our lives. IoT uses smart devices and the internet to provide innovative solutions to various challenges and issues related to various business, governmental, and public/private industries across the world. IoT is progressively becoming an important aspect of our life that can be sensed everywhere around us. On whole, IoT is an innovation that puts together an extensive variety of smart systems, frameworks, and intelligent devices and sensors.

3.3 Characteristics of IoT:

- **Interconnectivity**: With respect to IoT make possible the interconnection of anything with the global information and communication infrastructure.
- **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address)
- **Heterogeneity/ Interoperability**: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks. It supports several interoperable communication protocols and can communicate with other devices and also with infrastructure
- **Enormous scale**: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device triggered communication.
- **Dynamic & Self Adapting**: IoT devices and systems may have the capability to dynamically adapt to the changing contexts and take actions based on their operating conditions, users' context, or sensed environment. For instance, the surveillance system is adapting itself based on context and changing conditions. Moreover, the number of devices can change dynamically.
- **Self Configuring:** allowing a large number of devices to work together to provide certain functionality.

3.4 Applications of IoT:

A great transformation can be observed in our daily routine life along with the increasing involvement of IoT devices and technology. For instance, the concept of

i. Smart Home Systems (SHS) and appliances that consist of internet-based devices, automation systems for homes, and reliable energy management systems.

ii. **Smart Health Sensing system (SHSS)**. SHSS incorporates small intelligent equipment and devices to support the health of human beings. These devices can be used both indoors and outdoors to check and monitor the different health issues and fitness levels or the amounts of calories burned in the fitness center etc. Also, it is being used to monitor critical health conditions in hospitals and trauma centers as well. Hence, it has changed the entire scenario of the medical domain by facilitating it with high technology and smart devices. Moreover, IoT developers and researchers are actively involved to uplift the lifestyle of the disabled and senior age group people.

iii. **Smart Transportation**. IoT has brought up some new advancements to make it more efficient, comfortable, and reliable. Intelligent sensors, drone devices are now controlling the traffic at different signalized intersections across major cities. In addition, vehicles are being launched in markets with pre-installed sensing devices that can sense the upcoming heavy traffic congestions on the map and may suggest you another route with low traffic congestion.

iv. **Smart Cities:** Urban cities have now become enormous information gathering centers with IoT sensors collecting data on infrastructure management, home automation, building security, traffic management, and city parking systems every day. All the gathered data is stored and analyzed so that city officials can respond to problems in real-time. Eventually, the data collected from various smart city components are massive. However, the flood of data is a challenge that needs to be considered while planning for a sustainable smart city as it can be very difficult as well as expensive to manage this vast amount of data. To address this issue, smart city initiatives can implement edge analytics, which collects the data and analyzes it.

v. **Financial sector**

Many banking institutions are implementing edge computing together with smartphone apps to provide services to customers in a better manner. Also,

ATMs, banking apps, and kiosks work on similar principles – gathering and processing data, making such utilities more responsive by providing users with a broader suite of abilities. For high-volume trading and finance firms, even a millisecond of delay in a trading algorithm computation can lead to huge losses. The edge computing architecture is placed near the stock exchange data servers to run resource-intensive algorithms which result in reduced latency and localized data traffic. This provides such financial institutes with more accurate as well as up-to-date information to keep their business running. Apart from that, banks and other financial firms use edge analytics to derive insights to understand their customers better and provide a seamless user experience. Banks also use location-based suggestions and customer recommendations to cross-sell products in near real-time.

vi. **Industrial manufacturing:** Manufacturing is one of the industries that has derived maximum value by deploying Industrial IoT. Manufacturers can collect data to enable better predictive maintenance and energy efficiency by incorporating data storage and computing into industrial equipment. Also, IoT sensors can help to reduce costs and energy consumption by maintaining consistency and productive uptime. The continuous data collection and analysis facilitated by a smart manufacturing solution helps to customize production operations to efficiently meet consumer demands. With edge computing for an IoT setup, manufacturers that operate in low bandwidth or no bandwidth can benefit phenomenally. For instance, oil rigs located in remote areas can use edge computing architecture to collect, monitor and process data on various environmental factors without having to rely on a data center infrastructure that is remote.

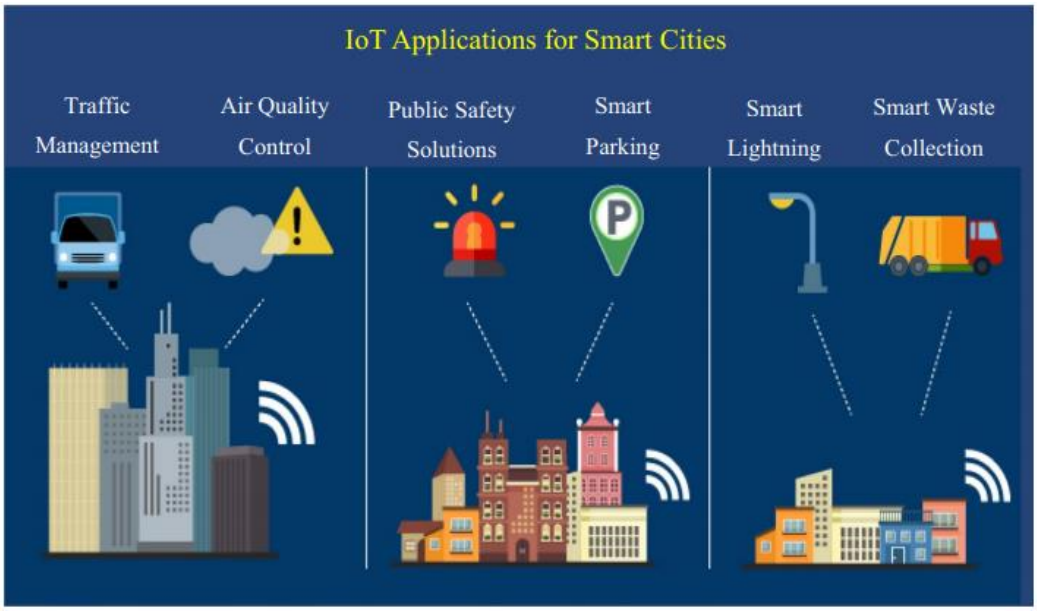


Figure 1: IoT Applications

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. What do you understand by Things in respect to IoT?
2. Define IoT
3. List the characteristics of IoT
4. Explain the applications of IoT

5.0 Conclusion

The IoT can be viewed 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). These devices can include multiple appliances that need to be connected for reasons including automation and real-time control of the device. As the IoT has both real-time and historical data stored, it can provide effective decision-making instructions to devices, and control certain actions and aspects of when and how they function.

6.0 Summary

In this study, we have learned about the meaning of things in the context of IoT, Characteristics of IoT, and Applications of IoT

7.0 Further Reading

Obe O. O. and Abe O. (2018). Development of Wireless Home Automation System for the Disabled People (Deaf, Dumb, and Alzheimer's). International Journal of Scientific & Engineering Research 9(1):1-6.

Folasade Oluwayemisi Akinloye Seminar paper presented at the Faculty of Communication and Information Technology, Igbajo Polytechnic, Igbajo.

www.softwebsolutions.com/resources/edgecomputing-for-IoT-operation.html

Kumar S, Tiwari P and Kumar et al. (2019), Internet of Things is a revolutionary approach for future technology enhancement: a review J Big Data 6:111 https://doi.org/10.1186/s40537-019-0268-2

“Overview of the Internet of Things.” ITU, June 15, 2012. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060

Unit 2: IOT Origin and Impact Contents

1.0 Introduction

With the IoT rapid growth and technology advances, growth in IoT applications deployment has been witnessed. Today's IoT applications include; industrial control and automation, sustainability, resources, waste management, and health and safety. Also, IoT applications, challenges, and opportunities are equally discussed

2.0 Intended Learning Outcomes (ILOs)

The objective of this study is to understand the impact of IoT, its revolution, evolution and Fleet Management in different domains.

3.0 Main Content

3.1 IOT Origin and Impact

The Internet of Things, or IoT, is growing by leaps and bounds, with millions of new sensors and devices going online every month. While it's far from comprehensive, the timeline below should give you a general idea of where IoT has come from and where it's headed in the future.

3.1.1 IoT Origin

The first **telemetry** system was rolled out in Chicago way back in 1912. It is said to have used telephone lines to monitor data from power plants. Telemetry expanded to weather monitoring in the 1930s, when a device known as a **radiosonde** became widely used to monitor weather conditions from balloons. In 1957 the Soviet Union launched Sputnik and with it the Space Race. This has been the entry of **aerospace telemetry** that created the basis of our global satellite communications today. Broad adoption of machine-to-machine (M2M) technology began in the 1980s with wired connections for **SCADA** (supervisory control and data acquisition) on the factory floor and in-home and business security systems.

In the 1990s, **M2M** began moving toward wireless technologies. ADEMCO built its private radio network to address intrusion and smoke detection because budding cellular connectivity was too expensive. In 1995, Siemens introduced the first cellular module built for M2M. The Internet of Things (IoT) has not been around for very long. However, there have been visions of machines communicating with one another since the early 1800s. Machines have been providing direct communications since the telegraph (the first landline) was developed in the 1830s and 1840s. Described as "wireless telegraphy," the first radio voice transmission took place on June 3, 1900, providing another necessary component for developing the Internet of Things. The development of computers began in the 1950s.

The Internet, itself is a significant component of the IoT, started as part of DARPA (Defense Advanced Research Projects Agency) in 1962, and evolved into ARPANET in 1969. In the 1980s, commercial service providers began supporting public use of ARPANET, allowing it to evolve into our modern Internet. Global Positioning Satellites (GPS) became a reality in early 1993, with the Department of Defense providing a stable, highly functional system of 24 satellites. This was quickly followed by privately owned, commercial satellites being placed in orbit. Satellites and landlines provide basic communications for much of the IoT.

One additional and important component in developing a functional IoT was IPV6's remarkably intelligent decision to increase address space. Steve Leibson, of the Computer History Museum, states, "The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough

addresses left to do another 100+ piles of earth." Put another way, we are not going to run out of internet addresses anytime soon.

3.1.1.1 Realizing the Concept

The Internet of Things, as a concept, wasn't officially named until 1999. One of the first examples of an Internet of Things is from the early 1980s and was a Coca-Cola machine, located at the Carnegie Melon University. Local programmers would connect by the Internet to the refrigerated appliance, and check to see if there was a drink available and if it was cold, before making the trip.

By the year 2013, the Internet of Things had evolved into a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems. The traditional fields of automation (including the automation of buildings and homes), wireless sensor networks, GPS, control systems, and others, all support the IoT.

Simply stated, the Internet of Things consists of any device with an on/off switch connected to the Internet. This includes almost anything you can think of, ranging from cellphones to building maintenance to the jet engine of an airplane. Medical devices, such as a heart monitor implant or a biochip transponder in a farm animal, can transfer data over a network and are members of the IoT. If it has an off/on the switch, then it can theoretically be part of the system. The IoT consists of a gigantic network of internet-connected "things" and devices. Ring, a doorbell that links to a smartphone, provides an excellent example of a recent addition to the Internet of Things. Ring signals when the doorbell is pressed and lets the user see who it is and to speak with them.

Kevin Ashton, the Executive Director of Auto-ID Labs at MIT, was the first to describe the Internet of Things while making a presentation for Procter & Gamble. During his 1999 speech, Mr. Ashton stated:

"Today computers, and, therefore, the Internet, is almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture, or scanning a bar code. The problem is, people have limited time, attention, and accuracy. All of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything

and greatly reduce waste, loss, and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best."

Kevin Ashton believed Radio Frequency Identification (RFID) was a prerequisite for the Internet of Things. He concluded if all devices were "tagged," computers could manage, track, and inventory them. To some extent, the tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes. Inventory control is one of the more obvious advantages of the Internet of Things.

3.1.1.2 Connecting Devices in New Ways

When thinking of the IoT, consider the idea, "any device capable, can be interconnected with other devices." The IoT is ripe for new and creative ideas to add to the tasks already in use. Imagine an alarm waking you at 6 AM, and then simultaneously signaling your coffee maker to turn on and start brewing coffee. Imagine your printer knowing when you are running low on paper, and automatically ordering more. Imagine the watch on your wrist telling you "where" you have been the most productive, while at work. The IoT can be used to organize such things as transportation networks. "Smart cities" can use it to reduce waste and maximize the efficient use of energy.

In truth, the IoT provides a nearly endless supply of opportunities to interconnect our devices and equipment. In terms of creativity, this field is wide open, with an infinite number of ways to "interconnect the devices." It can be an exciting time for innovative individuals, in part, because we don't fully understand the impact of these interconnections. The IoT offers both opportunities and potential security problems. At present, the Internet of Things is best viewed with an open mind, for purposes of creativity, and a defensive posture for purposes of privacy and security.

3.1.1.3 Customer Privacy

As sensors and video cameras become more commonplace, especially in public spaces, consumers have less and less knowledge about the information being collected, and no way to avoid it. Many people are uncomfortable with the idea of companies collecting information about them, and even more uncomfortable having that information sold to anyone and everyone. Generally speaking, older people dislike having information about themselves collected more than younger people, but according to one survey, about 45% of "all" respondents did not trust companies to use the data they collected to protect their privacy.

Currently, choices regarding privacy are very black and white, or on/off. The customer is forced to give up all privacy, (often in an agreement so convoluted people don't bother to plow through it) or the customer simply cannot access the service. This has led to continuing discussions about consumer privacy and how to best educate consumers regarding privacy and the accessibility of data.

3.1.1.4 Security

While there are steps to take to help ensure security, it should come as no surprise this issue has become a significant concern with the growth of the IoT. Literally, billions of devices are being interconnected together, making it possible (eventually) for someone to hack into your coffee maker, and then access your entire network. The Internet of Things also makes businesses all around the world more open to security threats. Additionally, data sharing and privacy become issues when using the Internet of Things. Consider how concerns will grow when billions of devices are interconnected. Some businesses will be faced with storing the massive amounts of information these devices will be producing. They will need to find a method of securely storing the data, while still being able to access, track, and analyze the huge amounts of it being generated.

James Lewis, who is a cybersecurity researcher for the Center for Strategic and International Studies, wrote a report describing how the Internet of Things' interconnections will allow computer hackers to wreak havoc through interconnected devices. The threat is so real, even the Federal Trade Commission has gotten involved, wanting to know how to guarantee privacy, and how security safeguards are being installed in new Internet-connected devices. For example, new cars can now be hijacked by way of their Wi-Fi connections. Consider the threat of hackers when automated driving becomes popular. Security and risk management should not be taken lightly when creating new ways to use the Internet of Things.

3.1.2 Impact of IoT

The technology services industry across IT Services, Business Process Management (BPM), and Engineering, Research & Development (ER&D) will witness increased opportunities related to IoT solutions. Impact of IoT on technology services (IT, BPM & ER&D)

IT Services: Focus on the new architecture of IT systems and infrastructure based on IoT expansion of the existing portfolio of services to include components such as data collection and analytics. It also customized solutions for specific IoT use-cases

Engineering, Research & Development (ER&D): Availability of real-time data from devices to get full product transparency. It enhances streamlining of the introduction of new products or upgrade of existing ones, in response to changing consumer needs and market scenarios

Business Process Management (BPM): Accelerated solution deployment, streamlined operations, and continuous process improvements, and higher levels of flexibility, efficiency, and responsiveness for businesses.

Various technological, economic, and behavioral factors are driving the uptake of IoT globally

• Low-cost sensors, declining cost of connectivity as well as reduced cost and time of processing will play a key role in the rise and adoption of IoT

• Use of big data analytics and cloud computing will enable processing and analysis of unstructured data to move from insights to foresight

• Consumer interest in IoT technologies is also rising due to increased reliance on mobile devices

The vast majority of technology enthusiasts are also interested in connecting devices to each other so that they exchange relevant information. For example, a connected car could detect that its owner and their family are traveling, and automatically turn off the home heating system. In the KRC Research, 89% of respondents said they are interested "in having all their household devices communicate constantly and seamlessly with one another to form a completely connected home or lifestyle." There is a clear need to establish standards and interoperability between different connected products or services. As such the GSMA Connected Living programme is facilitating interoperability between solutions from different vendors and service providers, enabling industry collaboration, encouraging appropriate regulation, and helping mobile operators to optimise their networks. The programme is also developing key enablers, such as the GSMA Embedded SIM Specification, which enables the remote provisioning of secure connectivity.

3.2 IoT Revolution in Industries

The world is undergoing constant transformations that somehow change the trajectory and history of humanity. We can illustrate with the first and second industrial revolutions and the information revolution. The introduction of the Internet of Things and Services into the manufacturing environment is ushering in a fourth industrial revolution: Industry 4.0. The industrial revolution has evolved from the 1760s where steam and coal are the major fuel in mechanical production. In the 1860s, the electrification, oil in Mass production, and the late 1900s, IT and Automation which is the third revolution. And now, we are in the 4^{th} revolution of the industry often refer

to as Industry 4.0, the era of the Internet of Things (IoT). The term Industry 4.0 was first coined at Hanover Fair in 2011.

Across the world, forward-thinking manufacturers and industrial product companies have made great strides in connecting their products and appliances to the Industrial Internet of Things (IIoT). But succeeding in the IIoT era demands much more than technology connectivity. The advent of the IIoT is a once-in-a-lifetime business disruption—one that requires new capabilities in managing direct relationships with customers, supported by transformed operating and business models designed specifically for an IIoT-enabled world. And it's a disruption that's coming faster than most companies think. Those manufacturers that move to tackle the necessary transformation today will position themselves as future leaders in their markets. Those that fail to act now risk being left behind—and will face a real struggle to catch up.

IoT (Internet of Things) trends are connecting all business levels and promising transformation. Companies are embracing various technologies and platforms to implement IoT networks such as LTE-M, NB-IoT, LoRaWAN, Sigfox, Zigbee, etc. Generally, IoT networks consist of many controlled intelligent devices, typically deployed to improve the efficiency of the engineering process, enable automation and reduce the wastage of resources. IoT networks are considered suitable candidates for all field operations ranging from exploration to production and refining. This is due to the IoT-enabled qualities, regularly decreased fabrication cost and device size, and low deployment expense. Statistical figures show rapid growth in the number of IoT devices and forecast (within a few years) their numbers to increase to the tune of billions.

IoT applications will help optimize, innovate and transform consumer products as well as business processes

Optimization: IoT helps reduce costs by efficient product usage while increasing efficient use of assets across business processes.

Innovation: IoT applications help create differentiated products/ services and improved operations, eventually leading to better customer service.

Transformation: IoT is blurring industry boundaries by enabling disruptive business models. For example, telematics involves both the automotive and insurance industries. IoT is expected to add value to business processes and take value creation for industrial applications to the next level, specifically in the case of Manufacturing. IoT is perhaps the most crucial element of Industry 4.0, which refers to the digital transformation of the processes and systems in the manufacturing sector.

• Various connected technologies such as high-quality sensors, more reliable and powerful networks, high-performance computing, robotics, artificial intelligence, and cognitive technologies, and augmented reality are changing Manufacturing in

profound ways. IoT market growth will be driven primarily by connected units in the Manufacturing and Automotive industries, with Transportation & Logistics forming the largest share of industry-specific IoT revenue. Among industries, Manufacturing and Automotive are expected to drive the highest volumes in IoT adoption.

India is a rapidly growing hub for IoT solutions with a market value expected to be $9 billion, and an installed unit base of 1.9 billion by 2020

• Although India began its IoT journey much later than developed economies, the installed base of connected units is expected to grow at a rate much faster than theirs. IoT units in India are expected to see a rapid growth of ~32X to reach 1.9 billion units by 2020, from its current base of 60 million. As a result, the India IoT market is expected to grow ~7X to move from $1.3 billion in 2016 to $9 billion by 2020.

• Rise of the tech-savvy consumer along with increasing smartphone and mobile internet penetration is driving consumer IoT applications in the Indian market. However, consumer IoT adoption is expected to be slower than its industrial counterpart due to the cost of IoT devices and security as well as privacy concerns of consumers.

3.2.1 Opportunity of the IIoT

IIoT in Oil, Gas and Mining Application

IoT is rapidly evolving and growing in oil, gas, and mining applications. In the operational field, detecting and reporting catastrophic failures and/or destructive events in real-time reduces production downtime. The information delivery from the end-user to the central processing unit is vital to streamlining production. Organisations are adopting integration approaches to link multiple telecommunications and control systems, such as Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA), Fleet Management System (FMS), Fatigue Detection System (FDS), etc.

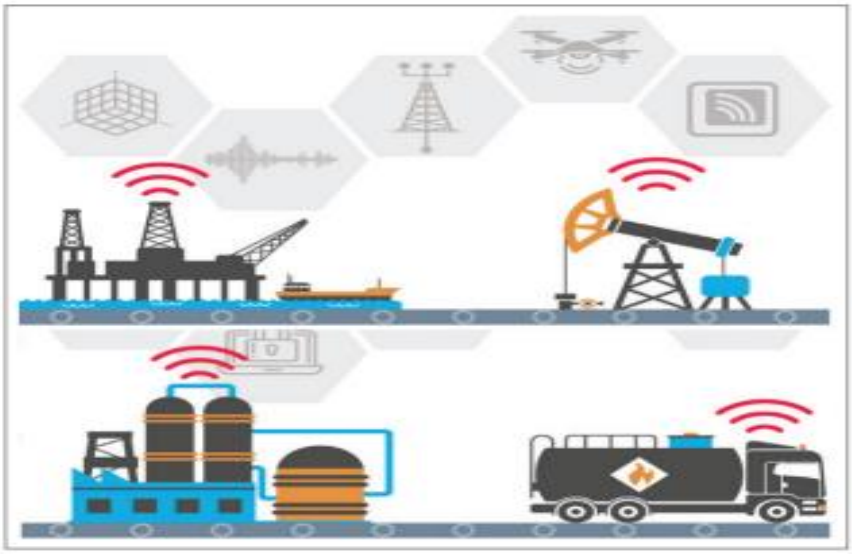


Figure 2: IoT applications in (a) mining (b) oil and gas environment.

Heating, Ventilation and Air Conditioning (HVAC) units for consumers

Illustration: As the CEO of Heating, Ventilation and Air Conditioning (HVAC) units manufacturing company. You've seen and embraced the emergence of the IIoT, and have invested accordingly in establishing Internet connectivity for the HVAC systems you sell. As a result, you can monitor and maintain your HVAC system's performance remotely in people's homes, detect imminent leaks or failures, and alert your customers of possible problems. But your customers' satisfaction with your offerings seems to be falling rather than rising. Why? The answer lies in the changing expectations and demands of today's connected consumers— but also the pervasive impacts of the IIoT on your operations and business model. Put simply, connecting appliances and devices to the Internet is perhaps the easiest part of the challenge of dealing with the IIoT disruption. Alongside the technology, it's every bit as important to address the behavioural, operational, and business model impacts it brings with it.

On the customer front, there's a growing trend for consumers—and also business customers— to want direct links to the companies that manufacture the products and services they use, cutting out the traditional 'middlemen'. This profound behavioural shift is evident across a host of industries, from energy to telecoms, and from mainstream media to technology. It's one of the key drivers of manufacturers' industry-wide move into services—a change that increasingly involves progressing from product-based to service-based offerings by building platforms, thus simultaneously expanding revenues and building 'stickiness' (see Figure 1). Meanwhile, on the operational front, the fact is that Internet connectivity—for an HVAC system or any other piece of equipment, whether a brake pad or a turbine engine—means much more than just linking it digitally to your business' systems. It also represents a way of getting closer to end-users than ever before, creating a degree of direct customer engagement and interaction that most manufacturing companies have never experienced.

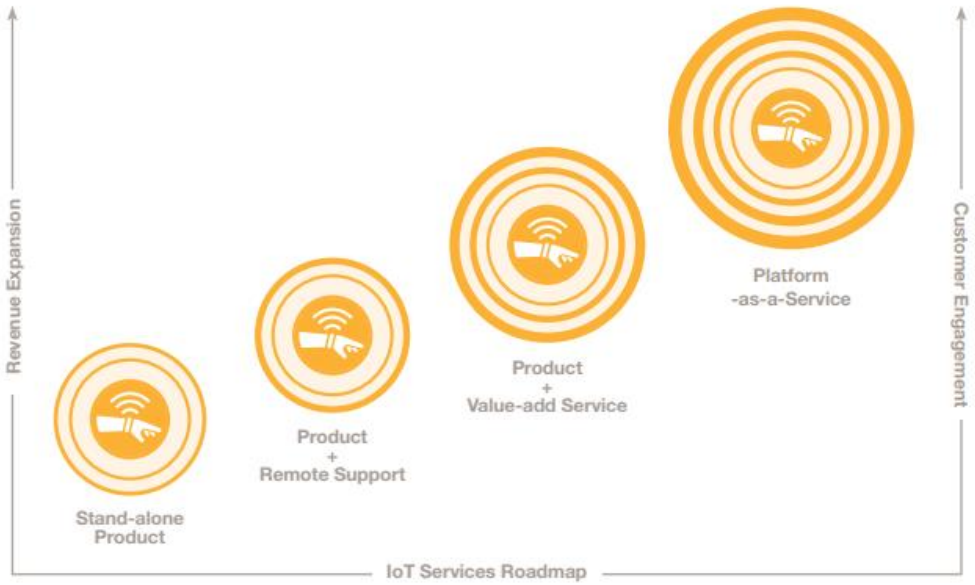


Figure 3 Companies moving from product-based offerings to service-based offerings by building platforms, expanding revenues, and building stickiness (Source: PwC, 2016)

3.3 Use Case: Fleet Management Using IoT

In logistics, the supply chain is made up of various stakeholders including manufacturers, transport companies, and retailers. Information sharing and connectivity are essential for all of them. Therefore, IoT has an important role to play in this industry. Internet of Things in fleet management currently works through 3 main technologies – **RFID, GPS, and OBD II's**. RFID helps control and track products while GPS and OBD II's make it possible to obtain real-time information on routes, vehicle maintenance, and driving conditions.

The automotive industry includes the use of smart things to monitor and report various parameters to monitor surrounding conditions, ranging from tyre pressure to the proximity of other vehicles. In one example, an IoT mesh network is used to support communications between vehicles when cellular service becomes unavailable. IoT assists autonomous vehicles to avoid obstacles by using sensory devices and enables truck-to-truck communications to maintain a safe distance from each other. In 2015, Rio Tinto's Pilbara mines were the first in the world to use fully automated driverless trucks to move iron ore, and other big producers such as BHP and Fortescue are following the vision of automated mining. Automated and self-correcting remote operations will allow to map metrics and deploy machine learning and artificial intelligence-based models to act on events in real-time.

3.4 Benefits of IoT in Fleet Management

Easier and Efficient Operations: Although logistics companies have had connectivity options like mobile phones, GPS sensors, etc, IoT offers many new tools, like in-vehicle streaming cameras, driver mobile apps, etc. making communication easier and prompt. Scheduling, load management, driver and vehicle tracking, and effective routing are some additional benefits offered by the Internet of Things. Besides these GPS and RFID-based tools, IoT also covers advanced applications such as weather APIs, traffic reporting, smart parking, maintenance monitoring, driving behavior monitoring, etc.

Automated Processes: Another major benefit of IoT in fleet management is the ability to automate various processes. As devices are interconnected and work as part of an integrated process, companies can set up an automatic flow of daily logistics processes and trip planning. Internet of Things also allows logistic companies to move daily operations into the cloud and helps remote tracking of fleets at any time from any place. Process automation through IoT is not restricted to the scheduled system. It also helps automate scenarios like broken-down vehicles that send automatic tickets to tow trucks; driver receives weather warning notifications, automatic rerouting, etc.

Better Analytics: The Internet of Things can derive collectivity data from various sensors. This enables fleet management **companies to get useful insights into driver behavior, adherence to laws, vehicle speeding and idling**, etc. These sensors don't just help in tracking data; they also play an important role in improving performance and diagnostics of problems related to processes and equipment.

Competitive Advantage: Early adopters of the Internet of Things in fleet management will enjoy a distinctive technological advantage over the competition. Proper implementation of **IoT reduces overall costs** by optimum utilization of resources and improved performance. Collecting, sharing, and acting on real-time information helps a company make quick decisions and instant improvements. These benefits will get any logistics industry excited about using of Internet of Things in fleet management. But the technology is still evolving, and as companies find more and more use cases, the Internet of Things will become the lifeline of the fleet management industry.

Therefore, integrating information technology improves the performance of your fleet business manifolds. It assures improvement in efficiency and compliance with road security standards. IoT is making the adoption of these changes much easier than ever for companies. They are equipped to strategize better and increase productivity by automating routine tasks.

3.5 Use Case: IoT for Financial Services

The emergence of the Internet of Things (IoT) has created quite a buzz in the business world. The Internet of Things can be best defined as the interconnectivity of computer devices in everyday objects via the internet. It is estimated that by 2025, there will be 64 billion IoT devices worldwide. This figure is a big leap from the 10 billion devices in 2018. Further, according to McKinsey, 127 new devices globally are connected to the internet each second.

3.6 Benefits of IoT for Financial Services

Prompt customer support: Fintech is merging with IoT and AI to challenge banks in offering immediate support to customers. Smartphones can act as beacons by notifying account managers in financial institutions when a customer arrives at their branch. This way, Fintech firms can offer support quickly and save clients time.

Indoor client navigation: By adopting beacons in daily operations, Fintech companies can assist customers in navigating while on the business premises. Instead of clients finding their way manually in the bank, they can state their reason for the visit. Then, they get matched with a suitable expert to resolve their issue. This simple solution improves efficiency, service delivery, and customer experience.

On-site queue management: Queues are common in most banks and other financial institutions. However, they can be managed using the Internet of Things. Added to assisting customers to move around the business premises as well as locate the right rep to talk to, IoT devices can also perform electronic ticketing. In this case, the customer inputs their issue into a smart machine. They are then given a ticket with details about the representative they should see and their number in the queue. The device then notifies them when it's their turn.

Improving customer service: According to a Microsoft report, 96% of customers globally indicate that customer service is an essential factor in their brand choice. Customer service is also crucial in Fintech. IoT applications in financial services can also be used to improve customer care and service. Using smart devices that are context-aware, the financial industry can optimize customer service by sending personalized messages, welcoming customers as they arrive, etc.

Making wireless payments: The Internet of Things in the financial industry is also transforming how people make payments. Wearable smart devices are replacing smartphones and traditional credit cards in making wireless payments and cash withdrawals. Statista predicts that the number of connected wearable gadgets will get to over 1.1 billion by 2022 from 526 million in 2016. Thus, more people will be using these devices for daily activities in the coming years.

Authentication and security: Besides IoT-based bank security systems, IoT wearables have also come into active usage as a way of improving security in the Fintech industry. A good example is the Nymi smart wristband which uses an

individual's heartbeat for biometric authentication. This tech was tested and proved to be secure in making wireless payments.

Increased business efficiency through automation: IoT applications enable companies to boost efficiency using process automation. IoT use cases in financial services will help to improve customer service and streamline daily functions. For example, Citibank adopted beacons that allow customers to use their smartphones to unlock doors at ATMs during off hours rather than using key cards.

Self-checkout services: IoT Fintech startups can use smart devices to offer wireless self-checkout services on various domains. Already, Amazon is implementing such a concept across its self-checkout stores.

3.7 IoT in Dairy Farming

Advances in sensing technology and agricultural software allow farmers to create individual and demographic profiles for the dairy herd. Each cow is equipped with a digital bracelet or pedometer which identifies the Holstein, measures how much milk was produced at each milking, provides data about the cows' activity by recording the number of steps per hour, identifies conductivity levels of the milk which are indicators of the presence of infections or possible ruptured cells in the udder and the duration period for the udder to be drained. The subsequent data is managed by software that allows each cow to be monitored for its overall health and levels of production in ways that previously were impossible. Readings that signal changes in Holstein's normal patterns allow the farmer to accurately predict the needs of each cow. Advances in genetic science and technology have made it possible for dairy farmers to map the genome of a Holstein's calf as early as one day after its birth. A sample of hair or blood can be used to isolate components of the calf's Deoxyribonucleic Acid (DNA). The process allows the farmer to predict with certainty how a heifer will mature to adulthood. Previously a waiting period of two years was necessary before a heifer could be assessed for its milk-producing and breeding capacity. Applications of DNA testing provide firm indicators regarding the cow's future fertility, milk production levels, vulnerability to diseases and indicate the components of its milk such as percentages of buttermilk fat, protein, and lactose levels. The advent of the Internet and applications of smart farming technology allows the herd to be digitally monitored for quality control within the broader context of the dairy industry.

Automation enables dairy farmers to control and manage larger herds, saving time and providing information. This latter aspect is a key factor in managing dairy farms through a -proactive perspective rather than a -reactive one, however depending on the skills of each farmer. Indeed, automation and technology themselves do not solve a problem but rather suggest where the problem is. Only within this perspective, automation can leads to benefits as improved profitability, animal health, lifestyle, and

milk quality. Usually, on a dairy farm, automation concerns three main areas: (i) automation of milking-related tasks; (ii) cow monitoring; (iii) feeding automation.

3.7.1 Automatic Milking System (AMS)

Automatic Milking System (AMS) refers to a system that automates all the aspects of the milking process and cow management usually undertaken in conventional milking (de Koning and Rodenburg, 2004). Automatic milking represents a revolutionary innovation in dairy farming because the adoption of an AMS is not a simple replacement for a milking parlour but rather a new way of managing a dairy farm. AMS does not simply change the way the milking is carried out but also the farmer's schedule, the feeding, and the housing management. With an AMS, milk information from individual cows is measured continuously by using sensors.

3.7.2 Cow Monitoring

Automatic systems to monitor physiological or behavioural parameters, related to the health or the oestrus, of an individual cow and to detect abnormalities of the animals are commonly used in dairy cow farming. Sensors implemented in such systems can be attached or non-attached to the cow. The attached sensors can be placed outside the cow's body (on-cow sensor, e.g. pedometer) or inside (incow sensor, e.g. rumen bolus). Non-attached sensors are off-cow sensors that can be classified as in-line sensors, taking measurements in a continuous flow of milk from a cow (e.g. milk electric conductivity) or online sensors when automatically collecting and analysing milk samples (e.g. somatic cell count sensor). The most widespread attached sensors used in dairy cow farming are pedometers, activity meters, and 3-D accelerometers for automatic detection of oestrus. These devices can either be fastened to the cow's neck or its foot. They are equipped with an internal battery and an electronic device sensitive to the movements of the cow. The internal memory of the device increments a single counter at each step taken by the cow and the final step count is transmitted with the cow's identification code to the control system when the animal is identified by antennas placed in the milking parlour or directly in the barn. The control system records the number of steps taken by the cow since the previous transmission. The step count received is compared with the average step counts of the previous days and all the animals that show an increase in activity level are signaled to the farmer, who can evaluate if the cow is in heat and then proceed with the artificial insemination. The advantages of automatic oestrus detection have been amply demonstrated, even if this technology brings the greatest benefits to farms with large herds (> 100 cows), where the direct observation of animals is particularly difficult and, sometimes, inefficient.

3.7.3 Feeding Automation

Feeding is the largest single cost on a dairy farm (up to 50% of the total running cost) and it is the most time-consuming activity after milking. Feeding automation has long

had a place in dairy farming, even if it has been limited to automatic concentrate distributors or self-feeders for calves. Automatic feeder for concentrates dispense concentrates to supplement nutritional requirements not supplied by the forages according to animals' needs, physiological condition, or productive capacity. Self-feeders for calves are automatic milk dispensers that administer the feed ratio supplementing, if necessary, each animal's diet automatically. The adoption of this technology has a strong impact on farm management, reducing drastically the time for preparing and dispensing feed to the calves and enabling their health status on an individual basis.

3.8 Benefits of IoT in Dairy Farming

i. The data profiles enable the farmer to supervise and monitor the effectiveness of employees.

ii. Dairy production statics support research and quality control and are accessible in both provincial and national databases that are both current and comprehensive.

iii. Workers who operate the milking equipment and oversee the milking process are responsible for the cleaning and stimulation of the udders as preparation for milking. Changes to the readings over time identify potential health risks to the cow such as the presence of udder infections. Analysis of the data supports staff in addressing health risks that potentially threaten the cow's productivity. In some cases, training needs that support staff performance can be identified and managed easily so that the health of the cow is not compromised.

iv. Innovations in smart technology greatly support the quality assurance of milk production and staff effectiveness because decisions are implemented through the interpretation of data based upon input from each cow.

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. Describe the various technological factors driving the uptake of IoT
2. Describe Industry 4.0 Revolution
3. Explain the IIoT in Oil and Gas Application
4. What is Fleet Management?

5.0 Conclusion

The technology services industry across IT Services, Business Process Management (BPM), and Engineering, Research & Development (ER&D) will witness increased opportunities related to IoT solutions. IoT applications will help optimize, innovate and transform consumer products as well as business processes

6.0 Summary

We have been able to overview the constant transformation that changes the trajectory history of humanity with the introduction of the internet of things. Opportunities of IoT in industry 4.0 was discussed and Use Cases such as IoT for Financial Services and Its Benefits examined, also the application of IoT in Dairy Farming and its benefits were explicitly discussed

7.0 Further Reading

PwC, 2016 The Industrial Internet of Things. industrial-internet-of-things.pdf (pwc.com). Please see www. pwc.com/structure for further details

Sabti H. (2018), IoT REVOLUTION IN OIL, GAS AND MINING INDUSTRIES: A REVIEW. A white paper White-Paper-IoT-revolution-in-oil-gas-and-mining-industries.pdf (titanict.com.au)

Hoglund A. et al., (2018), "Overview of 3GPP Release 14 Further Enhanced MTC," IEEE Communications Standards Magazine, vol. 2, no. 2, pp. 84-89

Oh S. and Shin J., (2017), "An Efficient Small Data Transmission Scheme in the 3GPP NB-IoT System," IEEE Communications Letters, vol. 21, no. 3, pp. 660-663

Reynders B., Wang Q., Tuset-Peiro P., Vilajosana X, and Pollin S., (2018), "Improving Reliability and Scalability of LoRaWANs Through Lightweight Scheduling," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1830-1842

Sandoval R., Garcia-Sanchez A., Garcia-Haro J., and Chen T., (2018), "Optimal Policy Derivation for Transmission Duty-Cycle Constrained LPWAN," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3114-3125

https://sumatosoft.com/solutions/internet-of-things-software-development.

Gao M., Wang P., Wang Y., and Yao L., "Self-Powered ZigBee Wireless Sensor Nodes for Railway Condition Monitoring," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 900-909

History of IoT: A Timeline of Development - IoT Tech Trends

Xu L., He W., and Li S., (2014), “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243

Unit 3: Overview of IoT-in Digital Transformation

1.0 Introduction

IoT in digital transformation, many factors are enhancing the utility of IoT and driving its growth. **Data has become extremely valuable to companies and AI has made this possible by making data actionable**.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Explain the evolution of IoT
2. Explain the Digital World Transformation
3. Describe the digital transformation with industry 4.0
4. Discuss the difference between M2M and IoT

3.0 Main Content

3.1 Evolution of IoT

In 1982, a graduate student in Carnegie Mellon University's computer science department, David Nichols, wanted to know if the department's coke vending machine had cold soda bottles. He was tired of going to the machine only to find there was no cold bottle available; the vending machine was quite some distance from his classrooms. So, he wanted to have information beforehand. He was helped in this endeavor by Mike Kazar and Ivor Durham, two fellow students, and John Zsarnay, a research engineer at the university. The code they wrote could check if coke was available in the vending machine, and if yes, whether it was cold or not. Anyone on the university ARPANET could monitor the status of the coke vending machine.

In 1989 Tim Berners Lee proposed the framework of the worldwide web, which laid the foundation of the Internet. In 1990 John Romkey developed a toaster that could be turned on and off over the Internet. It was a toaster wired to the computer as there was no Wi-Fi then!! This toaster is considered to be the first IoT device – the first "thing" that began the Internet of Things. Researchers and scientists seem to have a thing for caffeine – cold or hot. In 1993, the Trojan Room Coffee Pot was built in the computer laboratory of the University of Cambridge by Quentin Stafford-Fraser and Paul Jardetzky 1993. An image of the interior of the pot was uploaded to the building server thrice every minute. Later on, when browsers began displaying images, these images could be viewed online. The next milestone in the development of IoT came in 1999 when Kevin Ashton, current Executive Director of the Auto-ID Labs, coined the term internet of things. It was the title of a presentation he made at Procter and Gamble (where he was working then) about linking RFID in P&G's supply chain to the Internet.

The term IoT began to be used in mainstream publications like The Guardian and Scientific American by 2003-2004. In the same period, RFID was deployed by the US Department of Defence and by Walmart in its stores. The United Nations International Telecommunications Union acknowledged the impact of IoT in its report in 2005. It is predicted that IoT will help create an entirely new dynamic network of networks.
In March 2008, the first IoT conference was held in Zurich. It brought together researchers and practitioners from both academia and industry to facilitate sharing of knowledge. In the same year, the US National Intelligence Council included the internet of things as one of the six disruptive civil technologies. In its 2011 white paper, Cisco Internet Business Solutions Group (CIBSG) said that the internet of things can truly be said to be born between 2008 and 2009 when the number of things connected to the internet exceeded the number of people connected to it. CIBSG calculated that the things to people ratio grew from approximately 0.8 in 2003 to 1.84 in 2010. Together with the white paper, Cisco released many educational materials on the topic and started marketing initiatives to attract clients looking to adopt IoT. IBM and Ericsson joined the race soon after. In 2011 Gartner included IoT in its Hype Cycle for emerging technologies that were on the rise. In 2013 IDC released a report that predicted the IoT market to grow at a CAGR of 7.9% and reach USD 8.9 trillion by 2020.\

By comparison, the Internet has been on a steady path of development and improvement but arguably hasn't changed much. It essentially does the same thing that it was designed to do during the ARPANET era. For example, in the early days, there were several communication protocols, including AppleTalk, Token Ring, and IP. Today, the Internet is largely standardized on IP. In this context, IoT becomes immensely important because it is the first real evolution of the Internet—a leap that

will lead to revolutionary applications that have the potential to dramatically improve the way people live, learn, work, and entertain themselves. Already, IoT has made the Internet sensory (temperature, pressure, vibration, light, moisture, stress), allowing us to become more proactive and less reactive. Internet Business Solutions Group (IBSG). In addition, the Internet is expanding into places that until now have been unreachable. Patients are ingesting Internet devices into their bodies to help doctors diagnose and determine the causes of certain diseases. 10 Extremely small sensors can be placed on plants, animals, and geologic features, and connected to the Internet. 11 At the other end of the spectrum, the Internet is going into space through Cisco's Internet Routing in Space (IRIS) program

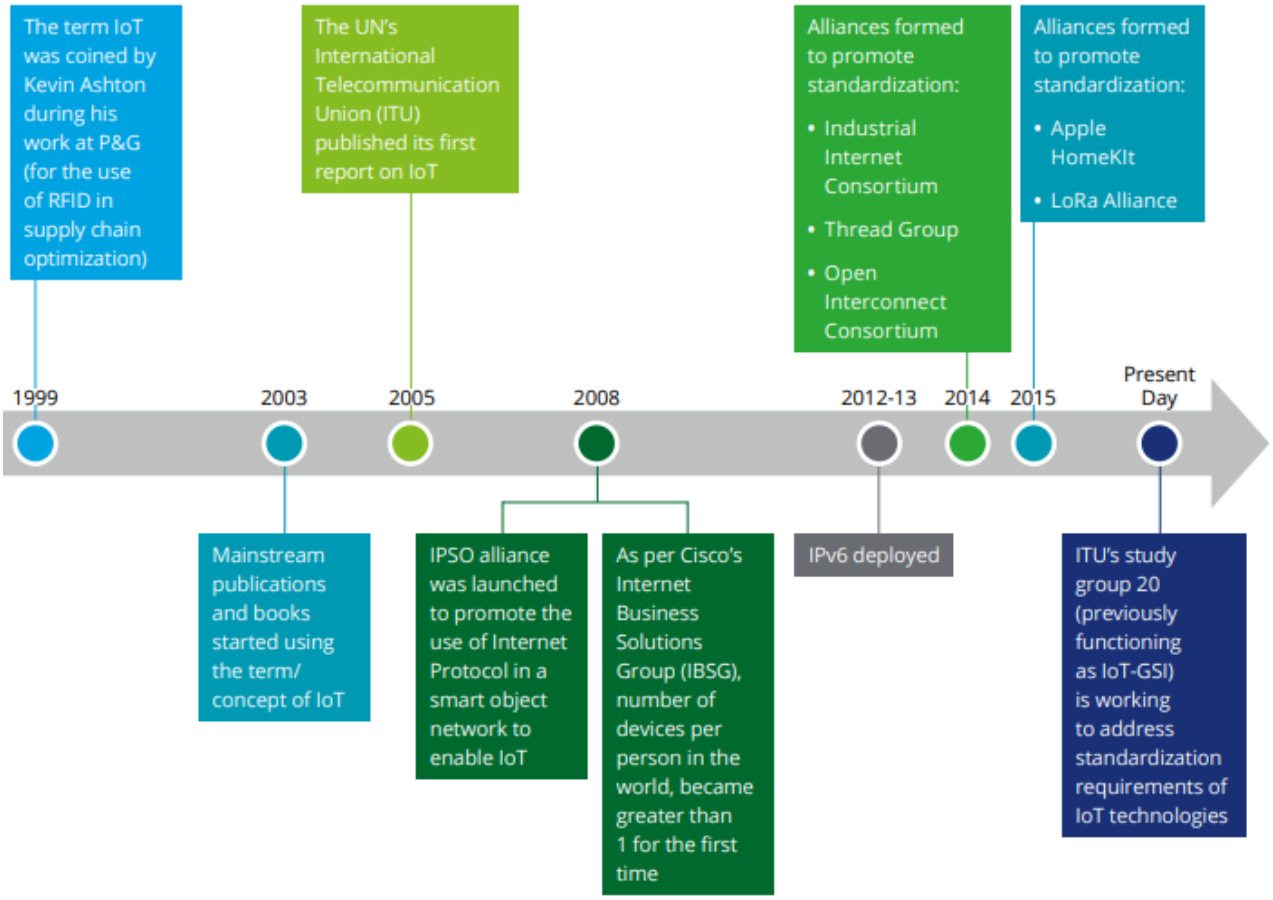


Figure 4: Evolution of IoT

3.2 Transforming Digital World

The Internet of Things or IoT is one of the key digital transformation technologies. It's not just one technology as many keep saying but a series of technological and other components that is vast. The sheer number of devices and connections which are projected to join the Internet of Things is staggering. Yet, it's not that much about the devices of course, although they are an indicator and the larger IoT projects get,

including the number of devices, the more mature digital transformation benefits of IoT become, making it the Internet of Transformation in correlation with other technologies and the transformational goals per use case.

With the addition of sensing and data transmitting devices to networks of connectivity and value comes an avalanche of data on top of our big data universe. With the growth of the Internet of Things, we already have more data in specific industries and applications (e.g. life sciences) than we can humanly handle. While devices and connectivity are of course all important, whether it's in the Industrial Internet of Things or the Consumer Internet of Things where the device has an additional dimension, in the end, the Internet of Things is an umbrella term. It covers many things, and at the same time is part of a bigger ecosystem of technologies and value. Data, why we capture it using IoT, and how we turn it into knowledge (DIKW), matters a lot, especially as the Data Age study shows IoT data volumes grow fastest.

It's how we analyze and use this data to enhance what we do across all areas of society that makes the Internet of Things so powerful and truly the Internet of Transformation. It's the way we combine data and intelligence to power innovative and transformational smart services with data exchange models and business model innovation. Big data analysis, the cloud and other related technologies to enable this move from data to knowledge to outcome are all key digital transformation technologies. While concerns in several areas are tackled and increasingly will, companies across the globe are investing in the Internet of Things and have already achieved considerable benefits. Others move slower, while consumer adoption of the Internet of Things also picks up. Even though connecting devices is not new and that with the Internet of Things we have entered a new dimension in many areas, we are still at the beginning of an era of accelerating Internet of Things adoption. And it will be a key pillar in the digital transformation economy.

Internet of Things 2.0: moving to integration and outcomes on the Internet of Transformation

All components and layers of an Internet of Things project or solution are important. Today most people focus on the devices, the connections, and the volumes. Enter what we could call the Internet of Things 2.0 and where we see all digital transformation technologies meet each other**, depending on the use case, scope, etc. on the road to an Internet of Transformation. The Internet of Things is such a vast reality that it has become an umbrella term for many underlying use cases, technologies, and other aspects.** It's why we started to distinguish between the Consumer Internet of Things and the Industrial Internet of Things. It's also why some prefer terms such as

the Internet of Everything, and in an industrial context, simply the Industrial Internet. Regardless of how we call it, the Internet of Things 2.0 reality is about an Internet of Transformation that is put in the context of related technologies, processes, people, benefits, outcomes, and massive real-life opportunities, rather than just the technology and device aspect. It's about how we move to a hyper-connected world with goals in mind and roadmaps to achieve these goals clearly defined. And in that roadmap will be several digital transformation technologies. The hyper-connected world: leveraging connected knowledge at scale for optimization, innovation, and human purpose.

Internet of Things 2.0 in the end leads to an even more hyper-connected world where eventually the term Internet of Things will disappear or be used like we use the term Internet today: as a given, a new normal, a bit like electricity. That's when it will be the Internet of Transformation although no one will call it like that.

Figure 5: Connected knowledge for optimization and innovation at scale

Internet of Things 2.0 moves from devices and data to actionable intelligence and purposeful action and transformation. The focus will be on the possibilities of hyper-connectivity, less from the connectedness perspective as such but more about how we can improve business, life, and society, using the insights gained, thanks to the hyper-connectedness of which the Internet of Things is a crucial additional component. IoT is not just transforming technologies, industries, and the various digital transformation goals, it is also radically transforming and – yes – disrupting existing channels in IT and IOT with far-reaching consequences in traditional go-to-market approaches. It is also transforming the nature of work, changing the role or even the existence of the middleman, the list is endless.

In order to connect the dots and realize the benefits of this hyper-connected world, it's important to see the Internet of Things puzzle, the various pieces of that puzzle, why we want to complete it to start with, and what is needed to put the puzzle in a safe, valuable and broader perspective. Usually, this requires a high-level understanding, an understanding of how the Internet of Things fits in the scope of digital transformation

and various related digital transformation technologies, insights regarding the Internet of Things beyond the "number of connected devices level" and a holistic view of people, purpose, process, and actionable information.

The Internet of Things is about to change entire industries (look at what's happening with Industry 4.0) and already transforms organizations in the true sense of the word and on all levels, ranging from customer experience to the transformation of business models and real innovation is becoming the state-of-the-art.

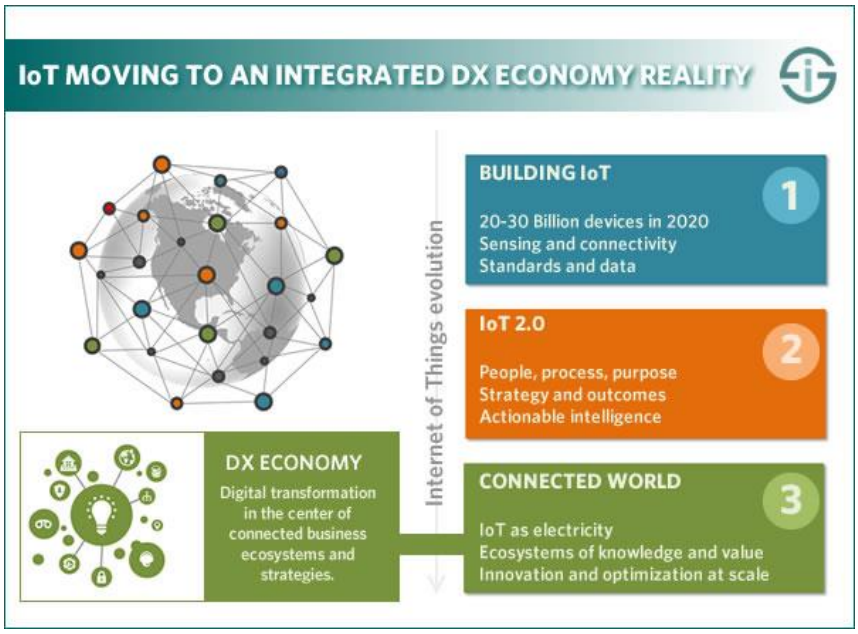


Figure 6: Internet of Things maturity and evolutions in the transformation to a hyper-connected world

3.3 Differences Between M2M and IoT

M2M or Machine to Machine –

M2M concept refers to two or more machines that can communicate with each other and carry out certain functions without human intervention. It is direct communication between devices using wired or wireless communication channels. M2M refers to the interaction of two or more devices/machines that are connected. These devices capture data and share it with other connected devices, creating an intelligent network of things or systems. Devices could be sensors, actuators, embedded systems, or other connected elements. M2M technology could be present in our homes, offices, shopping malls, and other places. Controlling electrical appliances like bulbs and fans using RF or Bluetooth from your smartphone is a simple example of M2M applications at home. Some degree of intelligence can be observed in the M2M model. Some of the key applications which leverage M2M technology to provide services are –

- Warehouse Management Systems (WMS)
- Supply Chain Management (SCM)
- Harvesting energy like oil and gas
- Customer billing like smart meters
- Traffic control
- telemedicine
- Remote monitoring

IoT or Internet of Things –

IoT refers is an ecosystem of connected devices (via the Internet) where the devices have the ability to collect and transfer data over a network automatically without human intervention. It is the network of physical devices embedded with sensors, software, and electronics, enabling these devices to communicate with each other and exchange data over a computer network. The things in the IoT refer to hardware devices uniquely identifiable through a network platform within the Internet infrastructure. Some of the applications and services of IoT Technology are –

- Smart Home
- Connected cars
- Agriculture and Retail
- Smart cities
- Healthcare
- Poultry and Farming

However, there is a lot of confusion between the IoT and M2M, as both refer to communicating and sharing data. M2M is about machines, smartphones, and appliances, whereas the IoT helps objects to interact with internal and/or external environments which in turn control the decision making. IoT is about sensors, cyber-based physical systems, the Internet, and so on.

IoT vs M2M: The Difference

M2M solutions contain a linear communication channel between various machines that enables them to form a work cycle. It's more of a cause and effect relation where one action triggers the other machinery into activity. Conversely, in the case of IoT, multiple devices communicate with each other through sensors and digital connectivity.

While M2M (machine to machine) is commonly associated with isolated solutions like a solution of Wi-Fi thermostats, a vehicle location system, or home automation, IoT (Internet of Things) works by stretching its boundaries and integrating multiple disparate systems into outputs beneficial for Business goals.

Another key differentiator is that M2M's key focus is on direct point-to-point connectivity across mobile networks or fixed-line while IoT communication involves IP networks and will usually employ cloud or middleware platforms.

When we consider the scalability in M2M vs IoT, clearly IOT wins the race since it works on Cloud-based architecture and as we know Cloud can expand substantially. Also, IoT makes use of Open APIs for communication across distinct systems while M2M mostly has limited or no open APIs. Some of the differences between M2M and the IoT are listed in the table below:

Table 1: Difference between M2M and IoT

PARAMETERS	M2M	IoT
Abbreviation for	Machine to Machine	Internet of Things
Philosophy	M2M is a Concept where two or more machines can communicate with each other and carry out certain functions without human intervention. Some degree of intelligence can be observed in M2M model.	IoT is an ecosystem of connected devices (via the Internet) where the devices can collect and transfer data over a network automatically without human intervention. IoT helps objects to interact with the internal and/or external environment which in turn controls the decision-making.
Connection Type	Point to Point	Through IP Network using various Communication types
Communication protocols	Old proprietary protocols and communication techniques	Internet protocols used commonly
Value Chain	Linear	Multi-sided
Focus Area	For monitoring and control of 1 or few infrastructure/assets.	To address the everyday needs of humans.
Sharing of collected data	Data collected is not shared with other applications	Data is shared with other applications (like weather forecasts, social media, etc.) to improve end-user experience
Device dependency	Devices usually don't rely on an Internet connection	Devices usually rely on an Internet connection
Device in scope	Limited devices in scope	A large number of devices in scope

PARAMETERS	M2M	IoT
Scalability	Less scalable than IOT	More scalable due to cloud-based architecture
Example	Remote monitoring, fleet control	Smart Cities, smart agriculture, etc.
Business Type	B2B	B2B and B2C
Technology Integration	Vertical	Vertical and Horizontal
Open APIs	Not supported	Supported
Related terms	Sensors, Data and Information	End users, devices, wearables, Cloud and Big Data

Comparison By: https://ipwithease.com

3.4 Use Cases: IoT in Autonomous Vehicles

Finding out where a vehicle is, taking numerous phone calls to provide location updates to customers, or figuring out which driver is closest to an urgent job is consuming a lot of valuable time that can be spent on processing new orders, invoicing, improving logistics, and delivering better service to your client base.

An IoT-enabled fleet management solution helps businesses gain competitive advantages by automating processes in a cloud-based platform and providing real-time visibility into everything that goes on in the field. Connecting to your fleet vehicles through installed telematics devices, you get their current GPS location and activity status on one web map, together with other reports and analytics that help improve your dispatch, route planning, and business logistics. This real-time visibility is what helps you gain flexibility in your resource allocation, better planning, and quick adaptability to changes in the situation.

With real-time GPS location, businesses can provide customers with the exact times of arrival or instantly update the route for a customer emergency. Using fleet tracking software also helps reduce wait times at destinations and monitor driver behaviour on the road to ensure safety and compliance, as well as minimize the risk of crashes and liability. IoT telematics can collect data on vehicle diagnostics, such as speed, idling time, harsh acceleration or braking, fuel consumption, vehicle faults, tire pressure, and more.

In case of a crash, the hardware, connected to the vehicle's engine module, will send an alert to the head office indicating a collision, so you can dispatch help to your driver without delay. You can also incorporate a better maintenance and vehicle health program for your fleet with better scheduling and routine checkups that will help avoid downtime and breakdown costs on the roadside.

This way, using IoT-enabled fleet management solutions can boost performance through better asset visibility and vehicle utilization, reduced wait times at destinations, and proactive maintenance for cost savings. For autonomous vehicle technology to properly function, it must work in conjunction with other areas. The five most relevant are listed below.

3.4.1 Five Use Cases

5G

An autonomous vehicle is expected to generate 2 Petabytes (2 million GB) of data every year. It would take the best Wi-Fi available months to be able to transfer that amount of information. The nearly real-time speeds of 5G are 10 times faster than 4G. With its infrastructure and dense network, 5G makes the future of autonomous vehicles possible.

Latency

Decreased latency, another characteristic of 5G, can also benefit autonomous vehicles. 4G currently has a latency of 50 milliseconds, which can be seen as a large delay when it comes to passenger safety.

Smart Cities and the Internet of Things (IoT)

For an autonomous vehicle to make smart decisions, it requires information about its environment. Smart cities, which are IoT-ready, allow for that. A city that can report on traffic, signals, etc., can help a self-driving car move smarter and more easily navigate its way around town.

Data Management

Analyzing the amount of data a self-driving car produces takes time. With the potential of nearly 10 million cars hitting the road, edge computing can help streamline this analysis by examining it closer to the source.

V2X

Vehicle-to-everything (V2X) allows the information from autonomous vehicle sensors and other sources to travel through high-bandwidth, high-reliability, and low-latency channels. It creates an ecosystem that enables cars to communicate both with each other and with infrastructures including parking lots and traffic lights.

Not only can this improve vehicle safety, but it also gives drivers or passengers information about road conditions ahead, so that they can appropriately respond. When combined with Artificial Intelligence (AI), a self-driving car will be able to make that decision itself.

Roadblocks

A study from NAMIC found that 42% of surveyed consumers said that no matter how long the technology was available, they would refuse to ride in fully automated vehicles. Similarly, 46% of respondents were skeptical about using fully automated vehicles for ride-sharing services. To gain public trust, the right infrastructure needs to be in place.

Data management challenges, safety concerns, and high manufacturing costs are roadblocks that can prevent widespread autonomous vehicle adoption. However, as large manufacturers and automotive organizations continue to enhance and improve the technology, the potential for an autonomous future continues to grow.

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. Explain the evolution of IoT
2. Explain the Digital World Transformation
3. Describe the digital transformation with industry 4.0
4. Discuss the difference between M2M and IoT

5.0 Conclusion

IoT technologies offer immense value and support the enhancement of a business model in operational fields. Research has shown that mining and gas companies, Diary Farm, Vehicle Automation, and Fleet Managements that have made IoT investments are reporting positive results. IoT technologies are used to enable automation, streamline engineering processes, reduce downtime and provide transparency at every layer of the operation. IoT data enables solution architects to upgrade designs and prevent historical irregularities. In addition to the design and implantation challenges of IoT networks, the overwhelming IoT market increases the difficulty of making a strategic business decision.

6.0 Summary

In this unit, we have considered the evolution of IoT, the Digital World Transformation with respect to industry 4.0 and we have been able to discuss the difference between M2M and IoT. Also, use cases of Autonomous Vehicles were explained.

7.0 Further Reading

Overview of IoT-in Digital Transformation - Bing

Alavi A., Jiao P., Buttlar W., and Lajnef N., (2018), "Internet of Things-enabled smart cities: State-of-the-art and future trends," Measurement, vol. 129, pp. 589-606

Paraszczak J., (2014), "Maximization of productivity of autonomous equipment in underground mines,", Mining Engineering, vol. 66, no. 6, pp. 24- 34,40-41

Oraibi I., Otero C. E., and Olasupo T. O., (2017), "Empirical path loss model for vehicle-to-vehicle IoT device communication in fleet management," Mediterranean Ad Hoc Networking Workshop, pp. 1-4

Leonardi S. (2014), Internet of Things (IoT) and Dairy Farm Automation Università Degli Studi Di Milano Graduate School of Veterinary Sciences for Animal Health and Food Safety

Microsoft Word - IoT_IBSG_0411FINAL.doc (cisco.com)

Evolution of Internet of Things (IoT): Past, present, and future (techaheadcorp.com)

Penna M., Shivashankar, Arjun B., Goutham K., Madhaw L., and Sanjay K., (2017), "Smart fleet monitoring system using Internet of Things (IoT)," IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology, pp. 1232-1236

White-Paper-IoT-revolution-in-oil-gas-and-mining-industries.pdf (titanict.com.au)

Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited, 2017.

Vate-U-Lan, P., Quigley, & Masouras, P. (2016). Smart dairy farming through the Internet of Things (IoT). Asian International Journal of Social Sciences, 17(3), 23 – 36. Retrieved from http://aijss.org/index.php/aijss20170302/

Yeong Y.W., IoT: The 4th Industrial Revolution. Analytics Innovation Forum 2017. Filler slides (sas.com)

IEEE Innovation at work (2021) Use Cases for Autonomous Vehicle Technology

https://innovationatwork.ieee.org/use-cases-for-autonomous-vehicle-technology/

Pareteum (2021), How Can IoT and M2M Connectivity Improve Your Business? https://www.pareteum.com/IoT-use-cases/

i-scoop (2021), Digital transformation technologies: the Internet of Transformation

https://www.i-scoop.eu/digital-transformation/digital-transformation-technologies-IoT/

Krasniqi X., and Hajrizi E. (2016) Use of IoT Technology to Drive the Automotive Industry from Connected to Full. IFAC-PapersOnLine 49-29 (2016) 269–274

Okano M. T., (2017), IoT and Industry 4.0: The Industrial New Revolution. International Conference on Management and Information Systems September 25-26

Foote K. D., (2016), A Brief History of the Internet of Things. A Brief History of the Internet of Things - DATAVERSITY

What are the Differences Between M2M and the IoT (2019) https://www.electronicsforu.com/technology-trends/learn-electronics/difference-between-m2m-and-IoT?

Ipwithease (2021), IoT vs M2M – Difference between M2M and IoT Explained

https://ipwithease.com/internet-of-things-vs-machine-to-machine-IoT-vs-m2m/

Module 2: Building Blocks of IoT

Module Introduction

The building blocks of IoT are extensively discussed in this module. Four things from the basic building blocks of the IoT system –sensors, processors, gateways, applications. Each of these nodes has to have its characteristics to form a useful IoT system.

Unit 1 - Building Blocks of IoT
Unit 2 - IoT Device Architecture
Unit 3 - Platforms Supporting IoT

Unit 1 - Building Blocks of IoT

1.0 Introduction

Things are the concentrated areas where information is sensed with the sensor elements or the actuators. Gateways block is used for connectivity purposes and it is an intermediate block between things and network or cloud infrastructure. Network infrastructure (NI) block helps in providing control over the information provided and allows secure and smooth flow.

2.0 Intended Learning Outcomes (ILOs)

To understand the IoT concept, the insights into the four building blocks of IoT (Things, Gateways, Network infrastructure, and Cloud infrastructure), three main components of IoT (The Things with Networked Sensors and Actuators, Raw Information and Processed Data Stores, and Analytical and Computing Engines) along

with architecture layers. The interaction between three components of IoT is also presented.

3.0 Main Content

3.1 Building Blocks of IoT

IoT implementation includes the four main building blocks, shown in Figure 7. These include the Things, Gateways, Network Infrastructure (NI), and Cloud Infrastructure (CI). Here, things are the concentrated areas where information is sensed with the sensor elements or the actuators. Gateways block is used for connectivity purposes and it is an intermediate block between things and network or cloud infrastructure. Network infrastructure (NI) block helps in providing control over the information provided and allows secure and smooth flow. Cloud infrastructure (CI) is equipped with information storage and computing proficiencies. The four IoT building blocks are:

i. Things: allows to communicate and collect the information from the objects of focused areas without any human interaction through the IoT devices such as Sensors and Actuators.

ii. Gateways: act as an intermediate block and enables strong connectivity between things and cloud infrastructure. It also provides security and manageability abilities during the data flow.

iii. Network Infrastructure (NI): It allows control over the data flow from things to the cloud infrastructure. It also enables security during the information flow. The IoT devices used include Routers, Aggregators, Gateways, and Repeaters.

iv. Cloud infrastructure (CI): It allows analytical, logical, and advanced computing abilities. The IoT devices used include Virtualized Servers (VS) and Data Storage Units (DSU)

3.2 Connectivity Blocks and Communication Protocols

For easy understanding of the IoT implementation and the process flow, the above four building blocks are grouped into three components. The three main components of IoT include Things with Networked Sensors and Actuators (TNSA), Raw Information and Processed Data Stores (RI-PD-S), and Analytical and Computing Engines (ACE).

Things with Networked Sensors and Actuators where they sense the detailed information as per the user requirements. The information sensed can be with respect

to the time duration set by the user. The information is then stored in the second component of IoT i.e. **Raw Information and Processed Data Storage allowing an interaction between the TNSA and RI-PD-S**. The interaction is enabled by sending the report states and the information is stored in various formats such as data, text, videos, and images, etc. The third component of IoT is the **Analytical and Computing Engines (ACE)** where the stored information is analyzed logically with appropriate decisions using numerous models thereby allowing an interaction between the RI-PD-S unit and ACE. This logical analysis is done with multiple iterative procedures until the best results are achieved as required by the user. In this third component human-machine, interactive learning is possible along with cloud and server-based analytics. Based on the human-machine interactive learning, the feedback and control commands or requests were given to the Things with Networked Sensors and Actuators component thereby allowing interaction between TNSA and ACE.

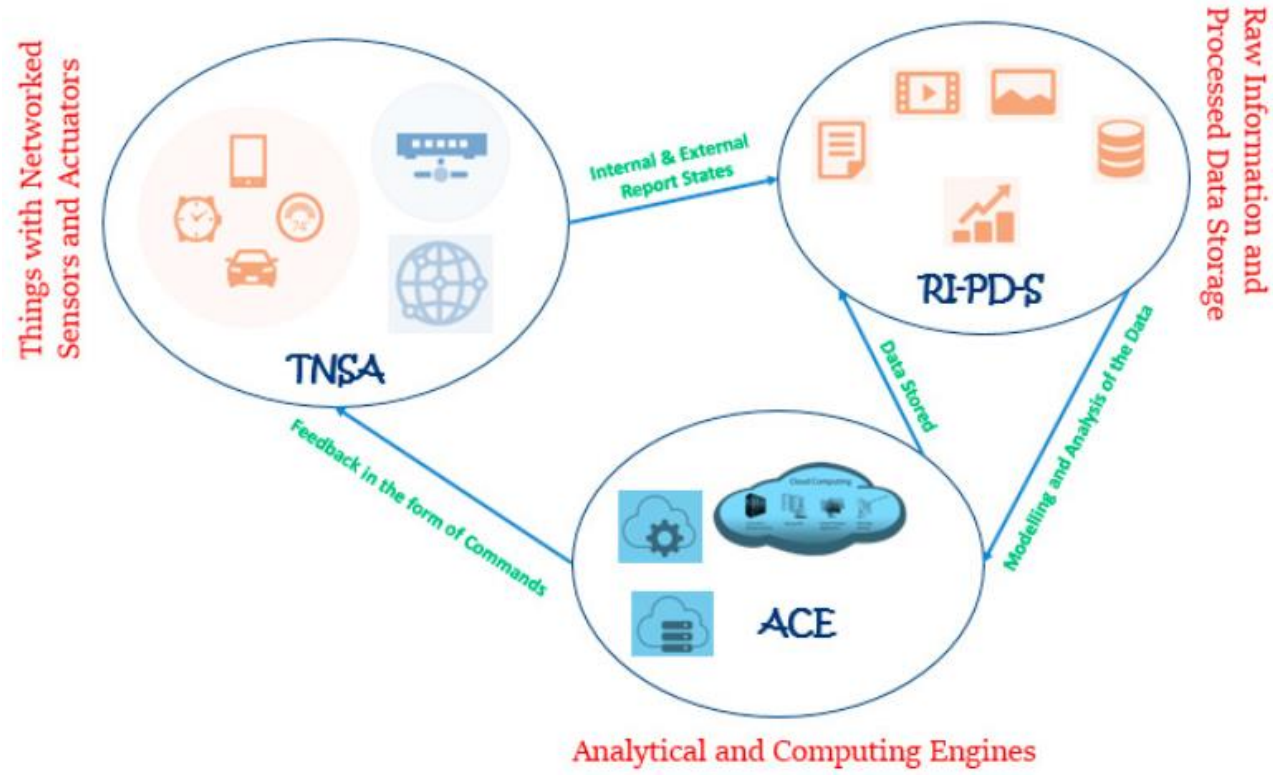


Figure 7: IoT Component Interaction

4.0 Self -Assessment Exercise(s)

Answer the following question:

1. Describe the four building blocks of IoT
2. Explain the three components of IoT in connectivity Blocks and Communication Protocols

5.0 Conclusion

The IoT architecture comprises four basic building blocks: sensors, processors, gateways, and applications. Sensors are responsible for converting a non-electrical input to an electrical signal; processors “handle” the signals; gateways are used to connect a network to another, and, ultimately, an application offers a user interface and effective utilization of the data collected

6.0 Summary

The IoT building blocks include the Things, Gateways, Network Infrastructure (NI), and Cloud Infrastructure (CI) was described. The gateways block used for the connectivity purpose and it is an intermediate block between the things and network or cloud infrastructure was shown in the diagram given in Figure 7.

7.0 Further Reading

Shukla D. (2020), Data Management Systems for The IoT Devices | IoT device management (electronicsforu.com)

Idowu, Park, Ibrahim (2017), A New IoT Architecture for a Sustainable IoT Adoption. International Journal of Computer Science and Information Technology Research Vol. 5, Issue 2, pp: (204-208)

Kumar and Mallick, (2018), The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. International Conference on Computational Intelligence and Data Science (ICCIDS 2018) Procedia Computer Science 109–117

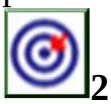
Internet of Things (IoT) - Part 2 (Building Blocks & Architecture) (c-sharpcorner.com)

Knowledge byte: Building Blocks of IoT Architecture | Cloud Credential Council

Unit 2 - IoT Device Architecture

1.0 Introduction

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the network layer, and the perception layer. The technologies of each layer are different, even though the technology used by the device of the same layer may be heterogeneous. The devices and technology in the Internet-of-Things are used to provide a diversity of services, each with its requirements, constraints, and trade-offs



2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Describe the IoT architecture
2. Explain the Network and Cloud as relating to IoT
3. Discuss the standardized and design considerations of IoT

3.0 Main Content

3.1 IoT Architecture

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the network layer, and the perception layer. The technologies of each layer are different, even though the technology used by the device of the same layer may be heterogeneous. The devices and technology in the Internet-of-Things are used to provide a diversity of services, each with its requirements, constraints, and trade-offs. Furthermore, the technologies and devices themselves are highly heterogeneous. This makes their management a difficult and complex enterprise. To address this challenge, a middleware layer is also sometimes added to manage different types of service,

shielding the underlying implementation details. The task of the middleware layer is to collect information from the network layer and store them in the cloud and database. Besides, the middleware layer also provides data processing ability. The four-layer architecture of the IoT constituted by the above factors is used in this paper, and this architecture can be applied to the actual application development.

Figure 8 describes the four-layer architecture of the IoT and the corresponding technologies in each layer. In this section, we discuss the functionality of these layers to motivate their unique security needs.

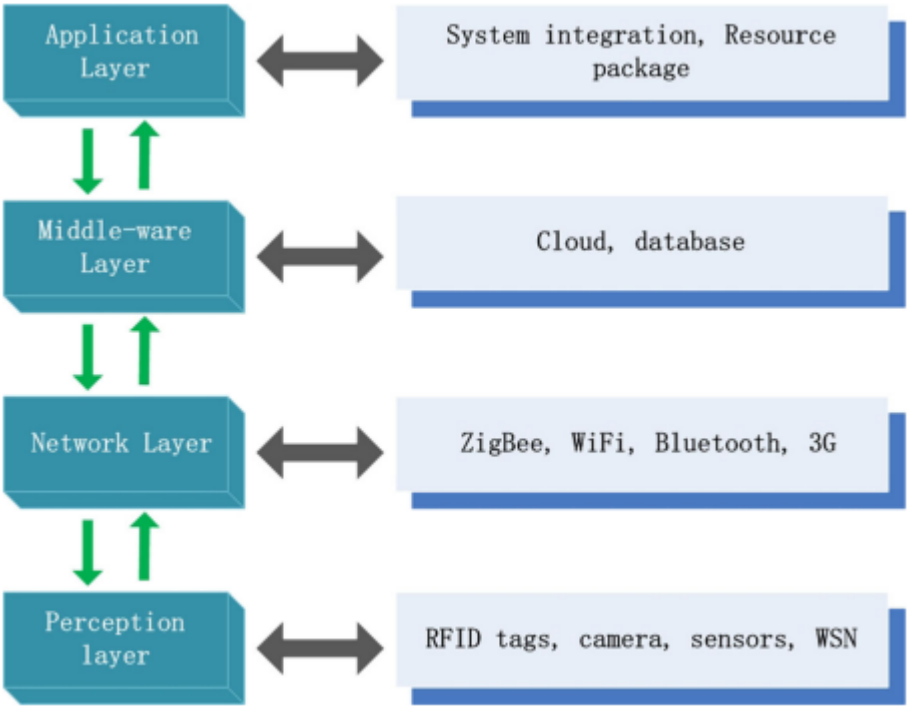


Figure 8: Four-layer architecture of the IoT

Application Layer: The application layer is the social division of the Internet-of-Things, combining with the industry demand and realizing extensive intellectualization. This layer implements different applications for different scenarios. This layer is used to manage and process data from the middleware layer, also providing quality service to the final user. The problem of the application layer mainly occurs in the operation of sensitive data, such as illegal access to data, malicious modification of data, and the lifetime of permission. Attackers can exploit code vulnerabilities to attack systems to gain sensitive data and modify it.

Middleware Layer: The middleware layer obtains data from the network layer, links the system to the cloud and database, and performs data processing and storage. With the continuous development of cloud computing and IoT, the middleware layer can provide more powerful computing and storage capabilities. Meanwhile, this layer

provides APIs to meet the demands of the application layer. Database security and cloud security are the main issues in the middleware layer, which affect the quality of service in the application layer.

Network Layer: This layer is responsible for the connectivity of the IoT infrastructure. It also collects data from the perception layer and transmits it to the upper layer. The transmission medium can be wired or wireless, and the main technologies are ZigBee, WiFi, Bluetooth, 3G, and so on. Attacks on the network layer are diverse, typically affecting coordination of work and information sharing among devices.

Perception Layer: The perception layer aims at identifying objects and collecting target information, and transforms the information into digital signals The key technologies of this layer are RFID tags, cameras, sensors, wireless sensor network (WSN), and so on. The technology of the perception layer is affected by energy and computing power. At the same time, a sensor device may be working in a hostile environment and can be easily destroyed (intentionally and unintentionally). This has a direct effect on the efficiency of the entire system. The main challenge for this layer is the malicious attack on the sensor and identification technology, which interferes with the collection of data

3.1.1 IoT Device Architecture

The internet of things provides fascinating solutions to most problems that the workforce is facing. The approach of attaining a solution is based on how the information technology components were integrated with communication devices with the best hardware and software convergence. Here in IoT, the software and hardware components act and work mutually with the learned outcome-based suggestions or priorities given by the owner who seeks the solution.

The four-stage architecture of an IoT system

Stage 1 of an IoT architecture consists of your networked things, typically wireless sensors and actuators. Stage 2 includes sensor data aggregation systems and analog-to-digital data conversion. In Stage 3, edge IT systems perform preprocessing of the data before it moves on to the data center or cloud. Finally, in Stage 4, the data is analyzed, managed, and stored on traditional back-end data center systems. Clearly, the sensor/actuator state is the province of operations technology (OT) professionals. So is Stage 2. Stages 3 and 4 are typically controlled by IT, although the location of edge IT processing may be at a remote site or nearer to the data center. The dashed vertical line labeled "the edge" is the traditional demarcation between OT and IT responsibilities, although this is blurring. Here's a look at each in detail.

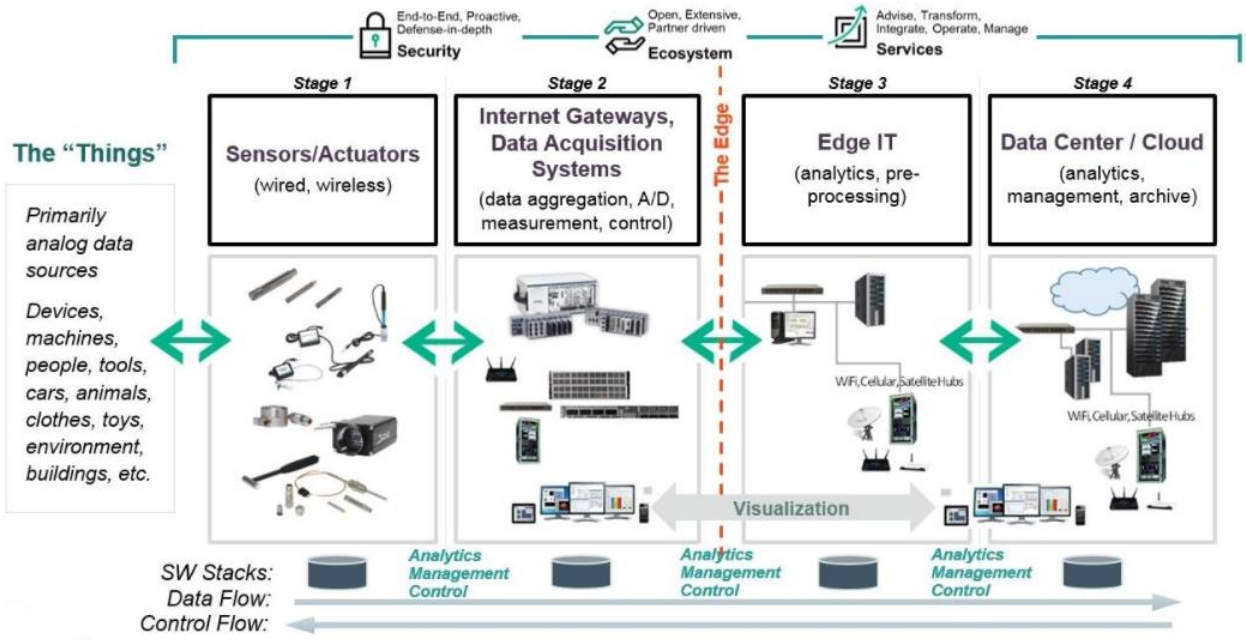


Figure 9: Architecture of an IoT

Stage 1. Sensors/actuators

Sensors collect data from the environment or object under measurement and turn it into useful data. Think of the specialized structures in your cell phone that detect the directional pull of gravity—and the phone's relative position to the "thing" we call the earth—and convert it into data that your phone can use to orient the device. Actuators can also intervene to change the physical conditions that generate the data. An actuator might, for example, shut off a power supply, adjust an airflow valve, or move a robotic gripper in an assembly process.

The sensing/actuating stage covers everything from legacy industrial devices to robotic camera systems, water-level detectors, air quality sensors, accelerometers, and heart rate monitors. And the scope of the IoT is expanding rapidly, thanks in part to low-power wireless sensor network technologies and Power over Ethernet, which enable devices on a wired LAN to operate without the need for an A/C power source.

In an IoT architecture, some data processing can occur in each of the four stages. However, while you can process data at the sensor, what you can do is limited by the processing power available on each IoT device. Data is at the heart of an IoT architecture, and you need to choose between immediacy and depth of insight when processing that data. The more immediate the need for information, the closer to the end devices your processing needs to be.

For deeper insights that require more extensive processing, you'll need to move the data into a cloud- or data center-based system that can bring several sources of data together. But some decisions simply can't wait for deep processing. Did the robotic

arm perform the surgery to cut an artery? Will the car crash? Is the aircraft approaching the threat detection system a friend or a foe? You don't have time to send that data to your core IT assets. You must process the data right at the sensor— at the very edge of the edge network—for the fastest response.

Stage 2: The Internet gateway

The data from the sensors start in analog form. That data needs to be aggregated and converted into digital streams for further processing downstream. Data acquisition systems (DAS) perform these data aggregation and conversion functions. The DAS connects to the sensor network, aggregates outputs, and performs the analog-to-digital conversion. The Internet gateway receives the aggregated and digitized data and routes it over Wi-Fi, wired LANs, or the Internet, to Stage 3 systems for further processing.

Stage 2 systems often sit in close proximity to the sensors and actuators. For example, a pump might contain a half-dozen sensors and actuators that feed data into a data aggregation device that also digitizes the data. This device might be physically attached to the pump. An adjacent gateway device or server would then process the data and forward it to the Stage 3 or Stage 4 systems.

Why preprocess the data? The analog data streams that come from sensors create large volumes of data quickly. The measurable qualities of the physical world in which your business may be interested—motion, voltage, vibration, and so on—can create voluminous amounts of constantly changing data. Think how much sensor data a complex machine like an aircraft engine might generate in one day, and there’s no theoretical limit to the number of sensors that could be feeding data into an IoT system. What’s more, an IoT system is always on, providing continuous connectivity and data feeds. IoT data flows can be immense such as 40 TB/second in one case. That's a lot of data to transport into the data center. It's best to preprocess it.

Another reason not to pass the data on to the data center in this form is that analog data has specific timing and structural characteristics that require specialized software to process. It's best to convert the data into digital form first, and that's what happens in Stage 2.

Intelligent gateways can build on additional, basic gateway functionality by adding such capabilities as analytics, malware protection, and data management services. These systems enable the analysis of data streams in real-time. Although delivering business insights from the data is a little less immediate at the gateway than it would be when sent directly from the sensor/actuator zone, the gateway has the compute power to render the information in a form that is more understandable to business stakeholders.

Gateways are still edged devices—they are external to the data center—so geography and location matter. In the pump example, if you have 100 pump units and want to

process data on-premises, you might have instant data at the pump level, aggregate the information to create a plantwide view for the facility, and pass the data on to the data center for companywide view. DAS and gateway devices may end up in a wide variety of environments, from the factory floor to mobile field stations, so these systems are usually designed to be portable, easy to deploy, and rugged enough to withstand variations in temperature, humidity, dust, and vibration.

Stage 3: Edge IT

Once IoT data has been digitized and aggregated, it's ready to cross into the realm of IT. However, the data may require further processing before it enters the data center. This is where edge IT systems, which perform more analysis, come into play. Edge IT processing systems may be located in remote offices or other edge locations, but generally, these sit in the facility or location where the sensors reside closer to the sensors, such as in a wiring closet. Because IoT data can easily eat up network bandwidth and swamp your data center resources, it's best to have systems at the edge capable of performing analytics as a way to lessen the burden on core IT infrastructure. If you just had one large data pipe going to the data center, you'd need enormous capacity. You'd also face security concerns, storage issues, and delays in processing the data. With a staged approach, you can preprocess the data, generate meaningful results, and pass only those on. For example, rather than passing on raw vibration data for the pumps, you could aggregate and convert the data, analyze it, and send only projections as to when each device will fail or need service.

Here's another example: You might use machine learning at the edge to scan for anomalies that identify impending maintenance problems that require immediate attention. Then you could use visualization technology to present that information using easy-to-understand dashboards, maps, or graphs. Highly integrated computer systems, such as hyper-converged infrastructure, are ideally suited to these tasks because they're relatively fast and easy to deploy and manage remotely.

Stage 4: The data center and cloud

Data that needs more in-depth processing, and where feedback doesn't have to be immediate, get forwarded to the physical data center or cloud-based systems, where more powerful IT systems can analyze, manage, and securely store the data. It takes longer to get results when you wait until data reaches Stage 4, but you can execute a more in-depth analysis, as well as combine your sensor data with data from other sources for deeper insights. Stage 4 processing may take place on-premises, in the cloud, or a hybrid cloud system, but the type of processing executed in this stage remains the same, regardless of the platform.

Living on the edge

The 4-stage approach to IoT infrastructure and processing will require new levels of collaboration, particularly as the separations between these stages start to blur. If you're an OT professional, be prepared to work side by side with IT professionals. If you're in IT, get ready to collaborate more closely with OTs. Eventually, the two functions will converge as the IoT pulls domain expertise deeper into data processing. IT professionals can build their IoT skills by starting small and working with domain experts to identify sources of potentially valuable data. Would understand the operating conditions of a machine help operations design more efficient maintenance cycles? Could developing knowledge of air temperature fluctuations in a warehouse help to improve product storage? Investigate the sensors and edge devices you would need to harvest the data. Design the infrastructure. Then experiment to make sure that the project produces results that make for a strong business case.

The IoT continues to reshape commercial, industrial, scientific, and engineering endeavors in profound and unpredictable ways. In the scientific revolution of the 17th century, newly invented instruments extended the reach of human senses far into the microscopic and astronomic realms. The IoT is the instrument that will enable your organization to connect intelligent technologies to the data-emitting universe of objects. The implications for IT infrastructure will be just as far-reaching.

3.2 IoT Reference Architecture

Reference Architecture describes essential building blocks as well as design choices to deal with conflicting requirements regarding functionality, performance, deployment, and security. Interfaces should be standardized, best practices in terms of functionality and information usage need to be provided. The central choice of the IoT-A project was to base its work on the current state of the art, rather than using a clean-slate approach. Due to this choice, common traits are derived to form the baseline of the Architectural Reference Model (ARM). This has the major advantage of ensuring backward compatibility of the model and also the adoption of established, working solutions to various aspects of the IoT. With the help of end-users, organized into a stakeholders group, new requirements for IoT have been collected and introduced in the main model building process. This work was conducted according to established architecture methodology.

A Reference Architecture (RA) can be visualized as the Matrix that eventually gives birth ideally to all concrete architectures. For establishing such a Matrix, based on strong and exhaustive analysis of the State of the Art, we need to envisage the superset of all possible functionalities, mechanisms, and protocols that can be used for building such concrete architecture and to show how interconnections could take place between selected ones (as no concrete system is likely to use all of the functional possibilities). Given such a foundation along with a set of design choices, based on the

characterization of the targeted system with various dimensions (like distribution, security, real-time, semantics) it becomes possible for a system architect to select the protocols, functional components, architectural options, needed to build their IoT systems. As any metaphoric representation, this tree does not claim to be fully consistent in its depiction; it should therefore not be interpreted too strictly. On the one hand, the roots of this tree are spanning across a selected set of communication protocols (6LoWPAN, Zigbee, IPv6,…) and device technologies (sensors, actuators, tags,..) while on the other hand the blossoms/leaves of the tree represent the whole set of IoT applications that can be built from the sap (i.e., data and information) coming from the roots. The trunk of the tree is of utmost importance here, as it represents the Architectural Reference Model (ARM).

The ARM is the combination of the Reference Model and the Reference Architecture, the set of models, guidelines, best practices, views, and perspectives that can be used for building fully interoperable concrete IoT architectures and systems. In this tree, we aim at selecting a minimal set of interoperable technologies (the roots) and proposing the potentially necessary set of enablers or building blocks (the trunk) that enable the creation of a maximal set of interoperable IoT systems (the leaves). The IoT Reference Model provides the highest abstraction level for the definition of the IoT-A Architectural Reference Model. It promotes a common understanding of the IoT domain. The description of the IoT Reference Model includes a general discourse on the IoT domain, and IoT Domain Model as a top-level description, an IoT Information Model explaining how IoT information is going to be modeled, and an IoT Communication Model to understand specifics about communication between many heterogeneous IoT devices and the Internet as a whole. The IoT Reference Architecture is the reference for building compliant IoT architectures. As such, it provides views and perspectives on different architectural aspects that are of concern to stakeholders of the IoT. The terms view and perspectives are used according to the general literature and standards the creation of the IoT Reference Architecture focuses on abstract sets of mechanisms rather than concrete application architectures. To organizations, an important aspect is the compliance of their technologies with standards and best practices, so that interoperability across organizations is ensured.

3.3 IoT Standardization and Design Consideration

1. **Data Integrity**: Data is easily captured and modified and can cause servers to crash in the transmission process. Malicious nodes can inject erroneous information into the network. At the same time, a hostile communication environment can also cause a loss of data. Checksum and cyclic redundancy checks (CRC) are usually used to detect or verify errors that may occur after data transmission or storage. In addition, message authentication code (MAC), digital signature, and version control are also used to ensure the integrity of data.

2. **Data Confidentiality:** There are many ways to ensure data confidentiality. The commonly used methods include access control and data encryption. Data encryption is the process of converting data to ciphertext such that the original content (called plaintext) cannot be accessed until a certain authorization (e.g., decryption key) is obtained. Commonly used encryption algorithms are RSA, DSA, AES, etc. In addition, access control is also a feasible method to control access to system resources by identifying visitors' identities. However, due to the limited resources in IoT devices or embedded devices, sophisticated data encryption and authentication scheme cannot be fully applied, so they cannot provide sufficient protection.

3. **Data Availability:** The availability of information resources is critical to users, and this is an important step in ensuring the quality of service (QoS). The goal of a denial of service (DoS) attack is to make the resources unavailable to users. An effective way to ensure data availability is to provide multiple paths for data transmission, thereby enhancing the ability of attack detection. When a path is not available, other paths can also provide service to ensure the QoS.

4. **Authentication and Authorization:** Authentication and authorization constitute a critical first defense against intrusion. Attackers often exploit the vulnerabilities in authentication and authorization to access the system. For example, in SmartApp, the attacker can violate the privacy of the user because of the lack of effective protection for user input. In addition, in a smart home, attackers can bypass authentication and authorization mechanisms and can execute a malicious operation on intelligent devices in the home. The most common way to solve these problems is to adopt a systematic access control paradigm, such as role-based access control (RBAC). An entity can play multiple roles and each role has different functions. The system manages access and permission according to the role. There are several ways to launch an attack in a specific application scenario. For example, the attacks on the SCADA system can be launched from the software level and the hardware level. An attacker can physically access the system to modify the data, and even if the emergency has occurred, it will not trigger the actual alarm mechanism. Moreover, an attacker can modify the display value to delay human response to an emergency. From the software level, attackers can also exploit program vulnerabilities, such as buffer overflow, SQL injection, and other attack methods to destroy the system. In addition, the attacker can also use the vulnerabilities in the communication protocol. Because SCADA has real-time requirements for information processing, attackers can delay important data in emergencies by using flood attacks, which may lead to an uncertain disaster. Therefore, in the design of security mechanisms and security framework, we must consider not only specific attack methods but also the integration of a variety of attack methods, from a more comprehensive perspective to deal with IoT security issues

3.4 IoT Device Architecture: Network and Cloud

The connectivity between the physical layer and the cloud is achieved in two ways: via gateways — hardware or software modules performing translation between different protocols as well as encryption and decryption of IoT data. Two key models of connectivity between physical and cloud levels in IoT.

3.4.1 IoT Design Considerations for Embedded Connected Devices

IoT networks must be scalable to support the dynamic nature of the IoT (as devices are added and removed from the network). For many applications, resource discovery and service announcements will need to be completed autonomously. Fortunately, zero-configuration networking protocols such as multicast Domain Name System (mDNS) and DNS-based Service Directory (DNS-SD) support these services and can be used to integrate new devices to an IoT network. mDNS provides a channel for devices to broadcast services data without a centralized server. DNS-SD extends mDNS by providing service discovery. Devices can broadcast their services while discovering the services and resources of other devices. To facilitate efficient M2M communication, Representational State Transfer (REST) architectures will also need to be leveraged. The benefits of REST include gains in network scalability, performance, and security. Because the REST architecture features a layered infrastructure designed to maintain separation between the client and server, REST-based systems are easily more scalable and support the seamless addition and removal of IoT devices.

Its also worth noting that as devices and various intermediaries are added to the network, the data paths can be altered which may negatively impact system performance. To correct this, caching data on devices closer to the client, such as proxy servers or gateways, network performance will be enhanced, or least maintained as the data paths change. Additionally, through the use of Uniform Resource Identifiers (URIs), network resources can be addressed by IoT clients. Using HTTP for the transmission, resources can be accessed and/or modified through commonly used protocols such as JSON and XML. For added protection, encryption can be used for safe data transmission HTTP(s).

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. Explain the following:

i. IoT Device architecture
ii. IoT Reference Architecture
iii. Describe Four stages of the IoT architecture

5.0 Conclusion

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the network layer, and the perception layer. The technologies of each layer are different, even though the technology used by the device of the same layer may be heterogeneous. The devices and technology in the Internet-of-Things are used to provide a diversity of services, each with its requirements, constraints, and trade-offs.

6.0 Summary

The functionality of the four layers architecture was described to motivate their unique security needs. The IoT Device Architecture fascinating solutions to most problems that the workforce is facing is also explained in stages and the IoT Reference Architecture describes essential building blocks as well as design choices to deal with conflicting requirements regarding functionality, performance, deployment, and security. Interfaces should be standardized, best practices in terms of functionality and information usage need to be provided. IoT Standardization and Design Consideration and IoT Design Considerations for Embedded Connected Devices were described.

7.0 Further Reading

Abu-Elkiheir M, Hayajneh M, and Abu N (2013) Data Management for the Internet of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Abu-Elkiheir M, Hayajneh M, and Abu N (2013) Data Management for the Internet of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Fuller J. R (2016), The 4 stages of an IoT architecture. How to design an IoT-ready infrastructure: The 4-stage architecture (techbeacon.com)

Abed A. (2017), Internet of Things (IoT): Architecture and Design https://www.researchgate.net/publication/321587819

Unit 3 - Platforms Supporting IoT

1.0 Introduction

Diverse platforms have embraced the advent of the internet of things. With cloud facility, users can have the visualization, machine learning, data analytics options for wider sets of information; taking the overall available data and refining it down to important information is referred to as Data management. Different devices from different applications send large volumes and varieties of information. Managing all this IoT data means developing and executing architectures, policies, practices, and procedures that can meet the full data lifecycle needs. Things are controlled by smart devices to automate tasks, so we can save time.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

1. list the various platforms supporting IoT
2. explain the data processing in cloud and fog based architecture of IoT
3. describes Data management
4. explain IoT Life Cycle

3.0 Main Content

3.1 Platforms Supporting IoT

IoT platforms and tools are considered the most significant component of the IoT ecosystem. Any IoT device permits to connect to other IoT devices and applications to pass on information using standard Internet protocols. IoT platforms fill the gap between the device sensors and data networks. It connects the data to the sensor system and gives insights using back-end applications to create a sense of the plenty of data developed by the many sensors. The Internet of Things (IoT) is the future of technology that helps Artificial intelligence (AI) to regulate and understand things in a considerably stronger way. Below are a mix of best known IoT platforms and tools that help you to develop IoT projects in an organized way.

1. **Zetta**

Zetta is API based IoT platform based on Node.js. It is considered a complete toolkit to make HTTP APIs for devices. Zetta combines REST APIs, WebSockets to make data-intensive and real-time applications. The following are some notable features.

- It can run on the cloud, or a PC, or even modest development boards.
- Easy interface and necessary programming to control sensors, actuators, and controllers.
- Allows developers to assemble smartphone apps, device apps, and cloud apps.
- It is developed for data-intensive and real-time applications.
- Turns any machine into an API.

2. **Arduino**

If you are seeking to make a computer that can perceive and exercise stronger control over the real world when related to your ordinary stand-alone computer, then Arduino can be your wise preference.

Offering an appropriate blend of IoT hardware and software, Arduino is a simple-to-use IoT platform. It operates through an array of hardware specifications that can be given to interactive electronics. The software of Arduino comes in the plan of the Arduino programming language and Integrated Development Environment (IDE).

3. **OpenRemote**

OpenRemote has introduced a new open-source IoT platform to create professional energy management, crowd management, or more generic asset management applications.

Summing up the most important features:

- Generic asset and attribute model with different asset types
- Protocol agents like HTTP REST or MQTT to connect your IoT devices, gateways, or data services or build a missing vendor-specific API.

- Flow editor for data processing, and a WHEN-THEN and a Groovy UI for event-based rules.
- Standard Dashboard for provisioning, automating, controlling, and monitoring your application as well as Web UI components to build project-specific apps.
- Android and iOS consoles allow you to connect to your phone services, e.g., geofences, and push notifications.
- Edge Gateway solution to connect multiple instances with a central management instance.
- Multi-realms multi-tenant solution, combined with account management and identity service.

4. Node-RED

Node-RED is a visual tool for lining the Internet of Things, i.e., wiring together hardware devices, APIs, and online services in new ways. Built on Node.js, Node-RED describes itself as "a visual means for wiring the Internet of Things."

It provides developers to connect devices, services, and APIs using a browser-based flow editor. It can run on Raspberry Pi, and further 60,000 modules are accessible to increase its facilities.

5. Flutter

Flutter is a programmable processor core for electronics projects, designed for students, and engineers. Flutter's take to glory is it's long-range. This Arduino-based board includes a wireless transmitter that can show up to more than a half-mile. Plus, you don't require a router; flutter boards can interact with each other quickly.

It consists of 256-bit AES encryption, and it's simple to use. Some of the other features are below.

- Fast Performance
- Expressive and Flexible UI
- Native Performance
- Visual finish and functionality of existing widgets.

6. M2MLabs Mainspring

M2MLabs Mainspring is an application framework for developing a machine to machines (M2M) applications such as remote control, fleet administration, or smart terminal. Its facilities include flexible design of devices, device structure, connection between machines and applications, validation and normalization of data, long-term data repository, and data retrieval functions.

It's based on Java and the Apache Cassandra NoSQL database. M2M applications can be modeled in hours rather than weeks and subsequently passed on to a high-performance execution environment made on top of a standard J2EE server and the highly-scalable Apache Cassandra database.

7. ThingsBoard

ThingsBoard is for data collection, processing, visualization, and device management. It upholds all standard IoT protocols like CoAP, MQTT, and HTTP as quickly as cloud and on-premise deployments. It builds workflows based on design life cycle events, REST API events, RPC requests.

Let's take a look at the following ThigsBoard features.

- A stable platform that is combining scalability, production, and fault tolerance.
- Easy control of all connected devices in an exceptionally secure system
- Transforms and normalizes device inputs and facilitates alarms for generating alerts on all telemetry events, restores, and inactivity.
- Enables use-state-specific features using customizable rule groups.
- Handles millions of devices at the same time.
- No single moment of failure, as every node in the bundle is exact.
- Multi-tenant installations out-of-the-wrap.
- Thirty highly customized dashboard widgets for successful user access.

8. Kinoma

Kinoma, a Marvell Semiconductor hardware prototyping platform, involves three different open source projects. Kimona Create is a DIY construction kit for prototyping electronic devices. Kimona Studio is the development environment that functions with Set up and the Kinoma Platform Runtime. Kimona Connect is a free iOS and Android app that links smartphones and stands with IoT devices.

9. Kaa IoT Platform

Kaa is a production-ready, flexible, multi-purpose middleware platform for establishing end-to-end IoT solutions, connected applications, and smart devices. It gives a comprehensive way of carrying out effective communication, deals with, and interoperation capabilities in connected and intelligent devices.

It mounts from tiny startups to great enterprises and holds advanced deployment models for multi-cloud IoT solutions. It is primarily based on flexible microservices and readily conforms to virtually any need and application — some other features as below.

- Facilitates cross-device interoperability.
- Performs real-time device control, remote device provisioning, and structure.
- Create cloud services for smart products
- Consists of topic-based warning systems to provide end-users to deliver messages of any predefined format to subscribed endpoints.
- Perform real-time device monitoring
- Manage an infinite quantity of connected devices
- Collect and analyze sensor data

10. SiteWhere

SiteWhere platform offers the ingestion, repository, processing, and assimilation of device inputs. It runs on Apache Tomcat and provides highly tuned MongoDB and HBase implementations. You can deploy SiteWhere to cloud platforms like AWS, Azure, GCP, or on-premises. It also supports Kubernetes cluster provisioning.
The following are some of the other features.

- Run any estimate of IoT applications on a single SiteWhere instance
- Spring brings the root configuration framework.
- Add widgets through self-registration, REST services, or in batches.
- InfluxDB for event data storage
- Connect devices with MQTT, Stomp, AMQP, and other protocols
- Integrates third-party integration frameworks
- Eclipse Californium for CoAP messaging
- HBase for the non-relational datastore
- Grafana to visualize SiteWhere data

11.DSA

Distributed Services Architecture (DSA) is for implementing inter-device communication, logic, and efforts at every turn of the IoT infrastructure. It allows cooperation between devices in a distributed manner and sets up a network engineer to share functionality between discrete computing systems. You can manage node attributes, permission, and links from DSLinks.

12.Thinger

Thinger.io provides a scalable cloud base for connecting devices. You can deal with them quickly by running the admin console or combining them into your project logic using their REST API. It supports all types of hackers' boards such as Raspberry Pi, Intel Edison, ESP8266. Thinger can be integrated with IFTT, and it provides real-time data on a beautiful dashboard.

3.2 Cloud Computing for IoT

Cloud computing is a more flexible and scalable technique that allows various services for IoT systems. These services include information storage options, software tools, and analytics, suitable platform, and core infrastructure for the development. With cloud facilities, users can have the visualization, machine learning, data analytics options for wider sets of information. Cloud-based architecture became popular in IoT systems due to the equivocal nature of the information sensed and produced in the form of data by IoT devices. In most IoT architectures, centralized control over the data is done using cloud-based data processing systems, as shown in Figure 10. This allowed the IoT system to have a cloud-centric architecture making the cloud to be in

between the applications and network of things. Here, the central part is the cloud, applications were placed above to cloud and a network of things were placed just below the cloud

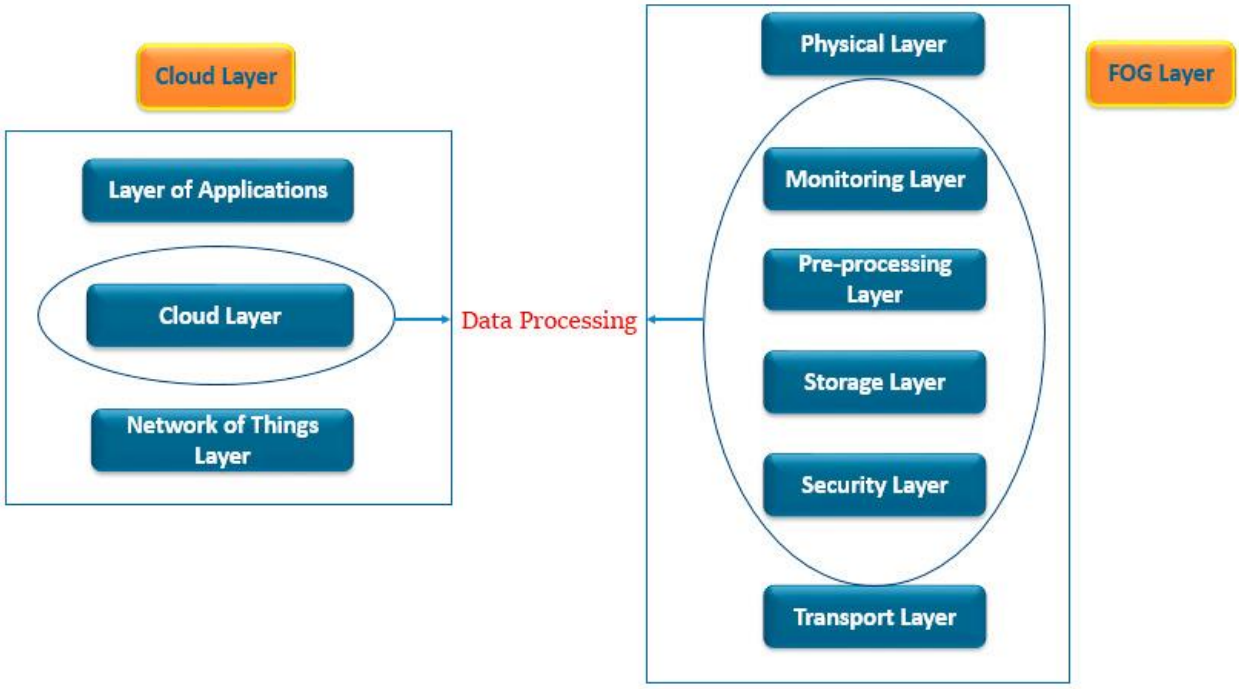


Figure 10: Data processing in the cloud and fog-based architectures of IoT

3.2.1 Cloud Platforms for the Internet of Things

Internet of things is the fastest growing industry today. Here we will look at the most recommended cloud platforms used for IoT development.

1. AWS IoT

There are billions of devices present in the hospital, homes, cars, and N number of places. AWS helps the user to collect, store and analyze the device data even when internet connectivity is down. It provides services like AWS IoT Core, AWS IoT device management, and AWS IoT device defender. AWS IoT analytics services are provided for analyzing their IoT data. It is scalable to use and pay for what you use. It provides security features such as encryption and access control devices, monitor and audit security policies. It is useful for connected homes, industrial and commercial projects and industrial applications like Anel company uses IoT platform for energy management (creating green glass enable gateways for homes, Symantec network uses IoT for the backend.

2. Microsoft Azure IoT Hub

Cloud computing is about accessing computing services like storage, networking over the internet from the service provider Azure. When we store photos online instead of phone gallery is cloud computing. It provides services for deploying applications on a massive global network using preferred tools and frameworks. It is used for meeting business challenges. It is a Microsoft product, less expensive to use, more secure, and reliable. We can scale up and down storage resources when our needs change on azure. It will manage tools and services for hybrid cloud applications. We can build a framework with all the languages and can deploy wherever we want. Help is provided by the expert while using azure.

3. Salesforce IoT

Building an application takes a lot of time but with the help of salesforce, it becomes easy and less time-consuming because it provides the fastest path from thinking of creating an app to building it successfully. No need to worry about infrastructure and tools. It is available in the cloud, anyone can use it from anywhere through the internet. It is scalable to the growth of the company which is seasonally changing it is applications. It supports start-ups and small businesses. It provides software solutions and platforms for users and developers. Infrastructure and up-gradation happen automatically. Sales cloud, service cloud, exact target market cloud, app exchange are services provided to the customers. Organizations can store and process Internet of things data, can utilize services provided by the salesforce IoT cloud. Salesforce handles a massive amount of data generated by devices, websites, sensors, etc, and provides responsive actions to the data provided by customers.

4. Google Cloud IoT

It is used for collecting, processing, and analyzing data and stored at the edge and in the cloud. It is a scalable and fully-managed cloud service. With the help services provided by google cloud IoT data, we can get an insight into the business. Ad hoc analysis is done with the help of Google BigQuery. We discover device performance on the Google Cloud IoT platform. We can make use of Google Maps to visualize the real-time location of the asset and keep track of them. It provides security with less risk. It has intelligent monitoring and control for the assets.

Popular Course in this category

5. IBM Watson IoT Platform

It is a cloud-hosted service that is capable of registration, connectivity, control, rapid visualization, and data storage. We can get real-time analysis of user and machine data such as speech, text video using the smart and scalable platform. This will help us to make better business decisions. It can connect IoT devices, networks, and gateways through ecosystems (it uses standard-based communications like HTTPS). It performs

analysis of structured and unstructured data. We can get history and parse, transform our data. The integration of IoT apps is possible.

6. Oracle Integrated Cloud for IoT
Oracle IoT is a Software as a service (SaaS) solution that is built on highly scalable IoT platforms that runs on Oracle-based cloud infrastructure. It has built-in integrations and extensibility features to extend our business such as ERP. It will provide real-time insight into the data to improve efficiency and derive business values from applications. Security is highly available such as each device has a unique identity and authorization of proof-origin data. Multiple devices are connected to enterprise applications with REST API. It has built-in intelligence and machine learning capabilities to build intelligent IoT solutions.

3.3 Data Management for IoT

Data management is the process of taking the overall available data and refining it down to important information. Different devices from different applications send large volumes and varieties of information. Managing all this IoT data means developing and executing architectures, policies, practices, and procedures that can meet the full data lifecycle needs. Things are controlled by smart devices to automate tasks, so we can save time. Intelligent things can collect, transmit and understand information, but a tool will be required to aggregate data and draw out inferences, trends, and patterns. Developers and manufacturers of embedded systems and devices need to build systems that answer the demands of data management. They need to design a data management framework compatible with all the software and hardware that play a role in collecting, managing, and distributing data. The design needs to be efficient to accelerate the time-to-market of the end-product.

Data from IoT devices are used for analytical purposes. Information that businesses collect and store but remain relatively stagnant because it is not used for analytical purposes, is called dark data. It includes customer demographic information, purchase histories and satisfaction levels, or general product data. To better understand customers, dark data is invaluable to businesses, as it allows them to uncover additional insights more efficiently. Before the release of a product, IoT data management requires field tests. Data from the field tests help improve the design and create a higher-quality product. Collecting field data post-launch helps in continuous product improvement with software updates and by identifying anomalies. This also provides important insights to support the development process of new products.

3.3.1 The IoT data management

In edge computing, data is processed near the data source or at the edge of the network. While in a typical cloud environment, data processing happens in a centralized data

storage location. By processing and using some data locally, the IoT saves storage space for data, processes information faster, and meets security challenges. Edge computing, data governance policies, and metadata management help firms deal with issues of scalability and agility, security, and usability. This further assists them to decide whether to manage data on the edge or only after sending it to the cloud. Sensors produce a large amount of data for edge gateway devices so that they can make decisions by analyzing the data. These high-performance systems not only need to collect data in real-time but also to organize and provide data to other systems.

Sensors and devices can connect indirectly through the cloud, where data is centrally-managed, or send data directly to other devices to locally collect, store and analyze the data, and then share selected findings or information with the cloud. Edge devices for data management help secure the most valuable data and reduce bandwidth costs. These also provide great performance, ownership over data, and lower maintenance cost. Edge devices run a Web-based dashboard that end-users can access to monitor the flow of data, so they can decide how various systems in demonstration and devices are running, and get notified by alarms. A large amount of data can be represented in the form of a graph for any desired range of time, and each point on the graph represents a record that can be found by searching the database, which stores a large quantity of data.

3.3.2 Data Management Challenges

With time, the number of IoT devices will increase, thus increasing the challenges for real-time processing and analysis to reduce the time for storage. Space has to be optimized for metadata like user IDs and passwords to ensure enough space for new information.

Functions such as adaptive maintenance, predictive repair, security monitoring, and process optimization rely on real-time data. Selecting the right tools is a challenge because integration between different sensors should be proven and compatibilities confirmed. When there is no connection, devices must still gain insights, make decisions and prepare for data distribution. There are important factors behind an IoT device data management platform, including interoperability, scalability, security, and standards offered by software technologies to build IoT products. It is important to protect data from unauthorized access and tampering. Organizations need to be compliant with national rules and regulations on securing data.

IoT device data also need to be checked for quality. Having many different devices connected directly to cloud services presents a huge attack surface, which can be mitigated by channeling data through a secure gateway device.

3.3.3 IoT Data Lifecycle

The lifecycle of data within an IoT system—illustrated in Figure 11—proceeds from data production to aggregation, transfer, optional filtering and preprocessing, and finally to storage and archiving. Querying and analysis are the endpoints that initiate (request) and consume data production, but data products can be set to be "pushed" to the IoT consuming services. Production, collection, aggregation, filtering, and some basic querying and preliminary processing functionalities are considered online, communication-intensive operations. Intensive preprocessing, long-term storage, and archival, and in-depth processing/analysis are considered offline storage-intensive operations.

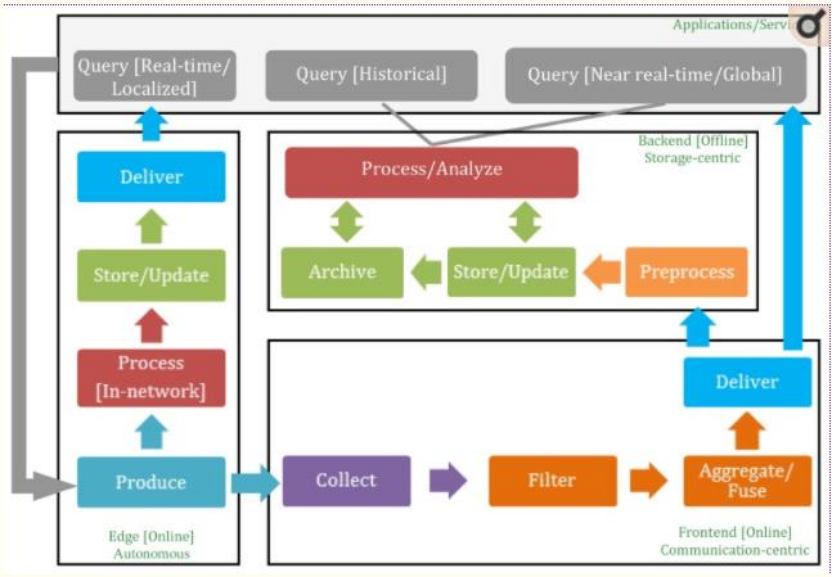


Figure 11: IoT data lifecycle and data management.

Storage operations aim at making data available in the long term for constant access/updates, while archival is concerned with read-only data. Since some IoT systems may generate, process, and store data in-network for real-time and localized services, with no need to propagate this data further up to concentration points in the system, "edges" that combine both processing and storage elements may exist as autonomous units in the cycle. In the following paragraphs, each of the elements in the IoT data lifecycle is explained.

Querying: Data-intensive systems rely on querying as the core process to access and retrieve data. In the context of IoT, a query can be issued either to request real-time data to be collected for temporal monitoring purposes or to retrieve a certain view of the data stored within the system. The first case is typical when a (mostly localized) real-time request for data is needed. The second case represents more globalized views of data and in-depth analysis of trends and patterns.

Production: Data production involves sensing and transfer of data by the "Things" within the IoT framework and reporting this data to interested parties periodically (as in a subscribe/notify model), pushing it up the network to aggregation points and subsequently to database servers, or sending it as a response triggered by queries that request the data from sensors and smart objects. Data is usually time-stamped and possibly geo-stamped and can be in the form of simple key-value pairs, or it may contain rich audio/image/video content, with varying degrees of complexity in-between.

Collection: The sensors and smart objects within the IoT may store the data for a certain time interval or report it to govern components. Data may be collected at concentration points or gateways within the network where it is further filtered and processed, and possibly fused into compact forms for efficient transmission. Wireless communication technologies such as Zigbee, Wi-Fi, and cellular are used by objects to send data to collection points.

Aggregation/Fusion: Transmitting all the raw data out of the network in real-time is often prohibitively expensive given the increasing data streaming rates and the limited bandwidth. Aggregation and fusion techniques deploy summarization and merging operations in real-time to compress the volume of data to be stored and transmitted.

Delivery: As data is filtered, aggregated, and possibly processed either at the concentration points or the autonomous virtual units within the IoT, the results of these processes may need to be sent further up the system, either as final responses or for storage and in-depth analysis. Wired or wireless broadband communications may be used there to transfer data to permanent data stores.

Preprocessing: IoT data will come from different sources with varying formats and structures. Data may need to be preprocessed to handle missing data, remove redundancies and integrate data from different sources into a unified schema before being committed to storage. This preprocessing is a known procedure in data mining called data cleaning. Schema integration does not imply brute-force fitting of all the data into a fixed relational (tables) schema, but rather a more abstract definition of a consistent way to access the data without having to customize access for each source's data format(s). Probabilities at different levels in the schema may be added at this phase to IoT data items to handle the uncertainty that may be present in data or to deal with the lack of trust that may exist in data sources [7].

Storage/Update—Archiving: This phase handles the efficient storage and organization of data as well as the continuous update of data with new information as it becomes available. Archiving refers to the offline long-term storage of data that is not immediately needed for the system's ongoing operations. The core of centralized storage is the deployment of storage structures that adapt to the various data types and the frequency of data capture. Relational database management systems are a popular choice that involves the organization of data into a table schema with predefined interrelationships and metadata for efficient retrieval at later stages. NoSQL key-value

stores are gaining popularity as storage technologies for their support of big data storage with no reliance on a relational schema or strong consistency requirements typical of relational database systems. Storage can also be decentralized for autonomous IoT systems, where data is kept at the objects that generate it and is not sent up the system. However, due to the limited capabilities of such objects, storage capacity remains limited in comparison to the centralized storage model.

Processing/Analysis: This phase involves the ongoing retrieval and analysis operations performed and stored and archived data to gain insights into historical data and predict future trends, or to detect abnormalities in the data that may trigger further investigation or action. Task-specific preprocessing may be needed to filter and clean data before meaningful operations take place. When an IoT subsystem is autonomous and does not require permanent storage of its data, but rather keeps the processing and storage in the network, then in-network processing may be performed in response to real-time or localized queries.

3.4 Mobile Applications for IoT

Mobile IoT technologies are opening up new use cases for the Internet of Things, which enables consumers and companies to remotely monitor, control, and coordinate their assets. Operating in licensed spectrum, Mobile IoT technologies provide low power wide area connectivity using mobile operators' existing infrastructure. Based on global standards, the primary Mobile IoT technologies – LTE-M and NB-IoT – are making it cost-effective to roll out IoT solutions, such as smart metering and asset tracking, that don't require high levels of throughput and low latency connectivity. The operator believes nationwide Mobile IoT connectivity will fuel economic development, improve the daily lives of Thais, support communities, and help to protect the environment. It says the new Mobile IoT technologies are enhancing the capabilities of businesses across multiple industries, as well as enabling IoT innovations that can be used by the public and academic sectors. Early use cases include smart city solutions, such as smart lighting, bike-sharing, and infrastructure monitoring.

There are several platforms for developing smartphone applications such as Windows Mobile, Symbian, iOS, and Android. In the proposed system, the Android platform app is developed as most of the phones and handy devices support Android OS. Java programming language using the Android Software Development Kit (SDK) has been used for the development and implementation of the smart home app. The SDK includes a complete set of development tools such as a debugger, libraries, and a handset emulator with documentation, sample code, and tutorials. Eclipse (running on Windows 7 development platform), which is the officially supported integrated development environment (IDE) has been used in conjunction with the Android Development Tools (ADT) Plug-in to develop the smart home app. The designed app

for the smart home system provides the following functionalities to the user: • Device control and monitoring. • Scheduling tasks and setting automatic control of the smart home environment. • Password change option. • Supports voice activation for switching functions

- **KDDI Mobile IoT Strategy**

KDDI believes low power wide area connectivity is set to change the way people enjoy a wide range of leisure activities beyond mountaineering, such as surfing, music festivals, and other events. Connected sensors, similar to the ones on Mount Fuji, could be used, for example, to measure the size of waves, count the number of people in a supermarket aisle or monitor the number of cars arriving at a festival site or tourist attraction. The information collected by these sensors can enable an event or site manager to monitor congestion levels in real-time, and take action, as necessary. KDDI's Mobile IoT strategy Having first launched its LTE-M commercial network in the northeast of Japan in January 2018, KDDI announced nationwide coverage in June 2018. It says LTE-M will play a key role in enabling IoT services for its customers. KDDI provides IoT customers with SIM management services through a web portal, which can track traffic volumes, billing data, connectivity status, and other information. For large volume deployments, involving over five million LTE-M subscriptions, KDDI charges JPY 40 (US$0.37) per month per SIM, while the cost of a single subscription is JPY 100 per month (US$1) per SIM(in both cases if the monthly usage needs to be 10 KB or less). The operator can also provide data analytics through a joint venture with Accenture, as it seeks to offer a one-stop IoT solution encompassing everything from connected sensors to the analysis and utilisation of data. "We aim to become business partners for our customers, solving their business challenges, rather than following the traditional product-led business model," explains Keigo Harada, General Manager and Head of IoT Business Planning Department at KDDI. KDDI sees potential to use low power wide area connectivity to support a wide range of use cases, spanning telematics, smart meters, remote monitoring of industrial equipment, building facilities and agriculture, the tracking and management of vehicles, delivery, and logistics, and security. The operator believes Mobile IoT technologies could also be used to monitor people's physical condition, flagging signs of heatstroke, for example. In the agricultural sector, for example, KDDI has installed LTE-M-enabled sensors in paddy fields to support fine-grained water level management for the crops. The Toyooka City Smart Agriculture Project is using LTE-M to collect data from water level sensors in the paddy fields, enabling farmers to monitor the growing conditions from a PC and smartphone

3.5 Use Case: Lora Communication Protocol

LoRa is a wireless modulation technique derived from **Chirp Spread Spectrum (CSS)** technology. It encodes information on radio waves using chirp pulses - similar

to the way dolphins and bats communicate! LoRa modulated transmission is robust against disturbances and can be received across great distances.
LoRa modulation and **Chirp Spread Spectrum technology** are simple to understand in practice.

- LoRa is ideal for applications that transmit small chunks of data with low bit rates. Data can be transmitted at a longer range compared to technologies like WiFi, Bluetooth, or ZigBee. These features make LoRa well suited for sensors and actuators that operate in low power mode.
- LoRa can be operated on the license-free **sub-gigahertz** bands, for example, 915 MHz, 868 MHz, and 433 MHz. It also can be operated on **2.4 GHz** to achieve higher data rates compared to sub-gigahertz bands, at the cost of range. These frequencies fall into ISM bands that are reserved internationally for industrial, scientific, and medical purposes

1. **Bandwidth vs. Range**

- LoRaWAN is suitable for transmitting small-size payloads (like sensor data) over long distances. LoRa modulation provides a significantly greater communication range with low bandwidths than other competing wireless data transmission technologies. The following figure shows some access technologies that can be used for wireless data transmission and their expected transmission ranges vs. bandwidth.

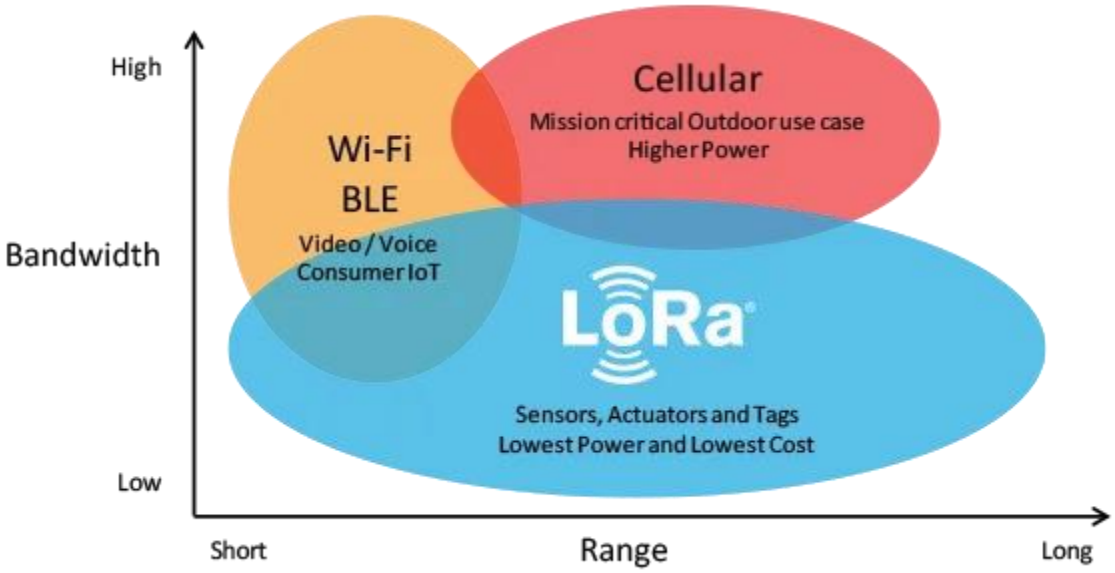


Figure 12: Bandwidth versus Range

2. **Benefits of LoRaWAN**

- **Ultra-low-power** - LoRaWAN end devices are optimized to operate in low power mode and can last up to 10 years on a single coin cell battery.
- **Long-range** - LoRaWAN gateways can transmit and receive signals over a distance of over 10 kilometers in rural areas and up to 3 kilometers in dense urban areas.
- **Deep indoor penetration** - LoRaWAN networks can provide deep indoor coverage, and easily cover multi-floor buildings.
- **License-free spectrum** - You don't have to pay expensive frequency spectrum license fees to deploy a LoRaWAN network.
- **Geolocation**- A LoRaWAN network can determine the location of end devices using triangulation without the need for GPS. A LoRa end device can be located if at least three gateways pick up its signal.
- **High capacity** - LoRaWAN Network Servers handle millions of messages from thousands of gateways.
- **Public and private deployments** - It is easy to deploy public and private LoRaWAN networks using the same hardware (gateways, end devices, antennas) and software (UDP packet forwarders, Basic Station software, LoRaWAN stacks for end devices).
- **End-to-end security**- LoRaWAN ensures secure communication between the end device and the application server using AES-128 encryption.
- **Firmware updates over the air** - You can remotely update firmware (applications and the LoRaWAN stack) for a single end device or group of end devices.
- **Roaming**- LoRaWAN end devices can perform seamless handovers from one network to another.
- **Low cost** - Minimal infrastructure, low-cost end nodes, and open-source software.
- **Certification program**- The LoRa Alliance certification program certifies end devices and provides end-users with confidence that the devices are reliable and compliant with the LoRaWAN specification.
- **Ecosystem**- LoRaWAN has a very large ecosystem of device makers, gateway makers, antenna makers, network service providers, and application developers.

3. **LoRaWAN use cases**

Here are a few great LoRaWAN use cases provided by Semtech, to give you some insight into how LoRaWAN can be applied:

- **Vaccine cold chain monitoring** - LoRaWAN sensors are used to ensure vaccines are kept at appropriate temperatures in transit.

- **Animal conservation** - Tracking sensors manage endangered species such as Black Rhinos and Amur Leopards.
- **Dementia patients** - Wristband sensors provide fall detection and medication tracking.
- **Smart farms**- Real-time insights into crop soil moisture and optimized irrigation schedule reduce water use up to 30%.
- **Water conservation**- Identification and faster repair of leaks in a city's water network.
- **Food safety**- Temperature monitoring ensures food quality maintenance.
- **Smart waste bins** - Waste bin level alerts sent to staff optimize the pickup schedule.
- **Smart bikes**- Bike trackers track bikes in remote areas and dense buildings.
- **Airport tracking** - GPS-free tracking monitors vehicles, personnel, and luggage.
- **Efficient workspaces** - Room occupancy, temperature, energy usage, and parking availability monitoring.
- **Cattle health** - Sensors monitor cattle health, detect diseases, and forecast calves delivery time.
- **LoRa in space** - Satellites to provide LoRaWAN-based coverage worldwide.

4. LoRaWAN is now an ITU standard.

As announced by the LoRa Alliance® on December 7, 2021, LoRaWAN® is officially approved as a standard for Low Power Wide Area Networking (LPWAN) by the International Telecommunication Union (ITU).

3.6 Use Case: Smart Home Using Arduino

The system consists of two parts: First, the Ethernet port, which is responsible for giving the control instruction to home appliances and receiving responses from the sensors. The second part is the Microcontroller unit Arduino Mega board, which is responsible for controlling the devices that connect with relays and sensors. The Microcontroller is the head of the system which controls and operation all information in the system. Figure 13 shows a block diagram of the Structure system.

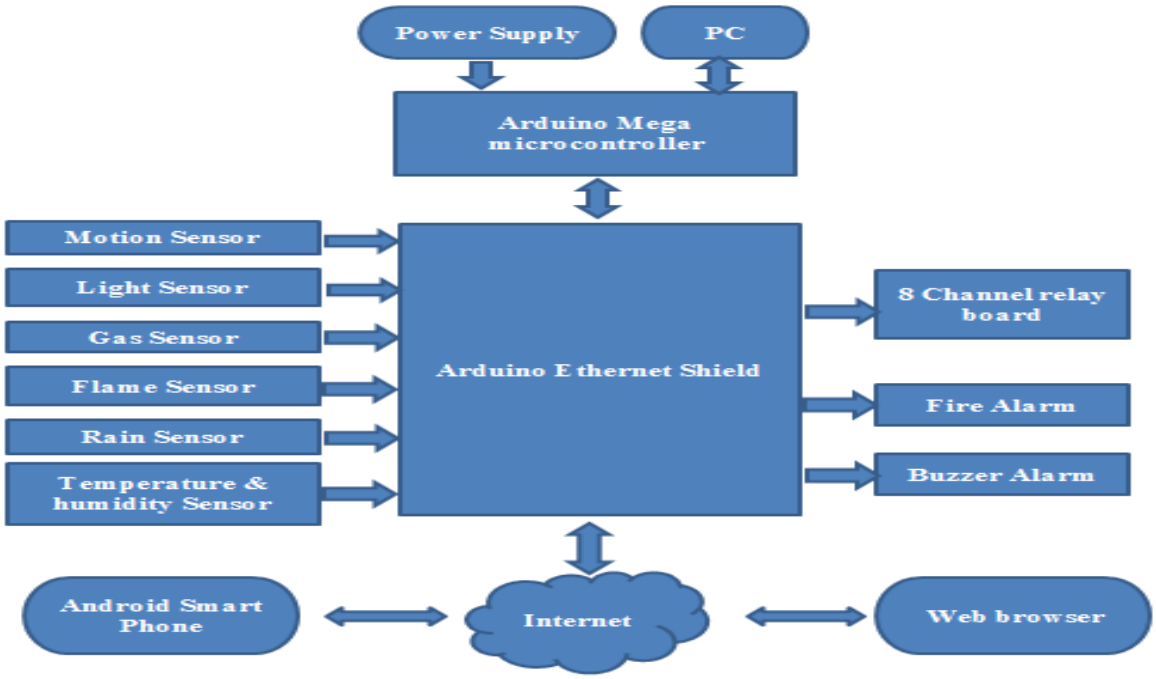


Figure 13: Block diagram of the Structure system.

From this block, there are two main important parts: the Microcontroller Board and the Ethernet Shield Module. The Ethernet shield part is connected with six sensors and an eight-channel relays board, The DHT11 sensor is a temperature & humidity sensor in the system; the motion sensor is a motion detector that uses a passive infrared sensor; the Rain sensor is a YL-83 module; Arduino Electronics DIY Parts Photoresistor is a Light Sensor; the flame sensor is a fire detector, and the MQ5 sensor is a gas detector, also Fire Alarm buzzer and gas buzzer. The data from all these sensors and relay are continually processed by the Microcontroller, and status is given in web browsers and home applications if there is an event in the home by switching ON/OFF the relays. Also, it can see or control every event and status by web browsers or home applications.

These units are responsible for the management and provide smart home automation. The user can control the state of the relay and remotely turn ON/OFF the light and devices in the house. Actually, the Ethernet Shield is the interface between the microcontroller and web browser by using the internet. During this operation, the information is transferred from the Microcontroller to the web browser. The commands sent by the user from a web browser are executed by the Microcontroller. This system works in a smart home automation system providing a guaranty and a remote management system for all devices inside the home.

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. What do you understand by Data management of IoT?
2. Explain Mobile Applications of IoT

5.0 Conclusion

We have learned about IoT cloud computing, how it will help the business to grow in the 20's era where competition is getting tougher for services provided to the users. Types of IoT clouds available to the users. Different IoT cloud provides different features but one common thing is there about different cloud and that is the security and privacy of user data. This will help the company to build users' trust. An internet-based smart home system that can be controlled remotely upon user authentication is proposed and implemented. The Android-based smart home app communicates with the micro web-server via the internet using the REST fully based web service. Any android supported device can be used to install the smart home app and control and monitor the smart home environment. A low-cost smart home system has been developed which does not require a PC as all processing is handled by the microcontroller. The system also uses the Google speech recognition engine thus eliminating the need for an external voice recognition module. Prospective future works include incorporating SMS and call alerts and reducing the wiring changes for installing the proposed system in pre-existing houses by creating a wireless network within the home environment for controlling and monitoring the smart home environment.

6.0 Summary

This module discusses the development process and design considerations that developers must follow to guarantee a successful launch of the Internet of Things (IoT) and wearable products. When developing a new product, there is a set of steps that must be followed to turn an innovative idea into a product available for sale. Some steps can have multiple iterations, which is typical when it comes to developing technically complex products based on hardware and software systems.

7.0 Further Reading

Shukla D. (2020), Data Management Systems for The IoT Devices | IoT device management (electronicsforu.com)

Idowu, Park, Ibrahim (2017), A New IoT Architecture for a Sustainable IoT Adoption. International Journal of Computer Science and Information Technology Research Vol. 5, Issue 2, pp: (204-208)

Kumar and Mallick, (2018), The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. International Conference on Computational Intelligence and Data Science (ICCIDS 2018) Procedia Computer Science 109–117

IoT Cloud Platforms | Top 6 IoT Cloud Platforms for IoT Development (educba.com)

Abu-Elkiheir M, Hayajneh M, and Abu N (2013) Data Management for the Internet of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Abu-Elkiheir M, Hayajneh M, and Abu N (2013) Data Management for the Internet of Things: Design Primitives and Solution Data Management for the Internet of Things: Design Primitives and Solution (nih.gov)

Fuller J. R (2016), The 4 stages of an IoT architecture. How to design an IoT-ready infrastructure: The 4-stage architecture (techbeacon.com)

Abed A. (2017), Internet of Things (IoT): Architecture and Design https://www.researchgate.net/publication/321587819 cussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/308647314

12 Open Source Internet of Things (IoT) Platforms and Tools (geekflare.com)

Fremantle P. (2015), A Reference Architecture for the Internet of Things DOI: 10.13140/RG.2.2.20158.89922

What are LoRa and LoRaWAN? | The Things Network

Almali N, Bahir K. S, Atan O. (2021), Arduino Based Smart Home Automation System. International Journal of Scientific Research in Information Systems and Engineering Volume 2, Issue 2, August – 2016. ISSN 2380-8128

Algoiare T. O., “Design and Implementation of Intelligent Home Using GSM Network” MSc dissertation, Dept. of Computer Engineering, Ankara, Turkey, 2014.

201902_GSMA_APAC_MobileIoT_Case_Study.pdf

Module 3: Security Considerations Using IoT

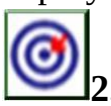
Module Introduction

In its essence, the Internet of Things is comprised of not just humans, but billions of IoT devices talking to each other using the Internet autonomously to fulfill their specific functions. Do you use IoT-powered motion sensor-based lighting solutions or smart locks at home? If so, they need to process the captured motion data within the fraction of a second it takes you to take a step and decide whether to keep the lights on or switch them off. That entire lightning-fast processing of data happens through the Internet. Of course, that's only a very basic example of IoT functionality. True IoT is capable of running entire factory floors, with its evolving complexities, autonomously. Needless to say, IoT represents a degree of autonomy and convenience that's incredibly attractive for consumers (enterprise and public). This is driving widespread adoption much faster than the technology has a chance to mature and before the devices can be properly equipped with required safety standards.

Unit 1 - Security Considerations Using IoT

1.0 Introduction

This unit presents the Internet of Things (IoT) security guidelines and best practices that others can use as a basis for future standards, certifications, laws, policies, and/or product ratings. Most, if not all, of these guidelines, would apply to any Internet-connected device; however, this paper focuses on security and privacy measures either peculiar to the IoT or especially relevant to the IoT. This paper assumes the end-to-end processing model of the Internet, in which application features such as security are handled by end nodes of the network, client, and server hardware. It focuses on security mechanisms, including patching and updating, that should be considered at the manufacturing design phase rather than after devices have already been built or deployed.



2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Explain the security considerations using IoT
2. Explain the standards and the best practices of IoT
3. Explain the challenges of the Architectural Layers of IoT

3.0 Main Content

3.1 Security Considerations Using IoT

Protect sensitive information The basic idea of IoT is to connect everyday objects via the Internet or ad-hoc network. IoT devices provide services that are discoverable by other IoT devices. Most of the protocols leak sensitive personally identifiable information (PII,) like the owner's name or information that may be linkable to an individual, like a device's hostname. This information can be linked to other information sources to target attacks. Service mechanisms and authentication protocols are required so that only authorized clients can discover the device. Encourage ethical hacking, and discourage blanket safe harbor.

Recently a bill was drafted for the Senate of the State of Michigan which would punish automobile hacking with a sentence of life in prison. One of the authors contacted one of the senators proposing the legislation and that senator agreed to modify the bill to allow hacking for beneficial research purposes. Researchers who discover serious vulnerabilities and report them responsibly provide a service to the industry similar to people who discover safety flaws in automobiles and other safety-critical machinery. Legitimate security research may be hindered by excessive legislation. One way to differentiate between research and unethical hacking is to mandate responsible

disclosure of discovered vulnerabilities. Responsible disclosure requires the researcher to first notify the manufacturer or governing authorities and allow reasonable time for the vulnerability to be independently verified and fixed before going public with a system hack.

Another, less desirable, the approach might be to require researchers to first register with a government office or the manufacturer before attempting to break into a device. Certainly, legislation should promote a safe and useful IoT ecosystem for everyone. Legislation should punish offenders. However, legislation should also avoid criminalizing activities that help promote safety and security. Legislation should avoid giving safe harbor to activities that cause harm. This position has been articulately expressed by Terrell McSweeney, Commissioner of the Federal Trade Commission. Manufacturers do not benefit financially from exposing flaws in their products but these flaws must be identified to improve functionality and security. Manufacturer-paid bug bounty systems can enable manufacturers to mitigate bad press while improving product quality at a cost lower than the cost of hiring paid penetration testers. Precautions should be taken by legislators to prevent retaliatory prosecutions of ethical hackers. Explicit provisions should be written into legislation to permit research and ethical hacking. Safe harbor clauses should be avoided for manufacturers who could implement harmful, insecure products for financial gain.

Manufacturers, users/citizens, and especially engineers/researchers should stay aware of pending legislation and make lawmakers aware of their positions. Institute an IoT Security and Privacy Certification Board Because of prevalent problems with security and privacy already caused by IoT devices, engineers must accept responsibility for their creations. IEEE or some international organization should provide a professional certification program for designers, builders, and providers of new IoT technologies who pledge to hold to established best practices for the creation of new devices outlined.

The program board should be empowered to verify whether the provider abides by responsible engineering practices (especially practices that enable security and privacy of the IoT), and would provide endorsement of providers who are bound by them. Negative action would be another dimension of this certification program and should be limited to loss of certification status and potentially reporting to the FTC or other government bodies for further action. The certification body should verify at least the following elements of a provider's products, protocols, and documents:
a) Data are handled, used, protected, and shared responsibly.
b) Protocols used or recommended do not leak information about users beyond the explicit intent of those users.
c) When privacy issues arise, the certified provider responds promptly to concerns.

d) Authentication is suitably strong and follows proven protocols.
e) Devices are not over-powered or under-protected.
f) Devices should have an identifying label that cannot be easily forged and that contains a web link where customers can go to find the certification status of the device along with a device description (model and serial number, etc.). This can be done in cooperation with the FTC or other national bodies.

Certification programs such as these decrease uncertainty and provide device makers, engineers, and authors with best practices to follow. Courts can consider certification as evidence that acceptable practices are generally followed. In the event of litigation, a provider can point to the certification and say that it followed good engineering practice.

3.2 IoT Security Standards and Best Practices

The IoT security best practices include having user and device authorization capabilities, updatable software and firmware, and designing security into the device from the start. The recommended practices from standards organizations are designed to protect users and hardware against the threats commonly seen with IoT devices.

3.2.1 Securing Devices

1. Make hardware tamper-resistant Some IoT devices may operate continuously unattended and not subject to the security implied by this frequent, direct human observation. While it is best to keep devices relatively isolated so that only a few designated persons have physical access, especially for completely unattended devices, making them tamper-proof or tamper-evident may be advantageous. This form of endpoint hardening can help block potential intruders from reaching data. It may also defend against a hacker buying and then weaponizing devices. The physical security of endpoints can include, for example, small simple plastic devices, port locks, and camera covers, which lockout USB and Ethernet ports and cover webcam apertures. Port locks help prevent unwanted malware from coming in. Some tamper-resistive approaches disable the device when it is tampered with. As a best practice, secure endpoint hardening likely implies a layered approach that requires attackers to circumvent a variety of obstacles designed to protect the device and its data from illicit access and use. At the hardware/boot-software level, strong boot-level passwords or requiring the device to boot from local storage only may be sound approaches. Known vulnerabilities should be protected, such as open TCP/UDP ports, open serial ports, open password prompts, places to inject code such as web servers, unencrypted communications, and radio connections. For shipping, tamper-evident packaging will enable the device owner to know if a device has been opened before it arrived. The number and strength of security at each layer depend upon the threat model, acceptable levels of risk, and desired convenience.

2. Provide for firmware updates/patches Inevitably vulnerabilities will be discovered after devices have been deployed. Devices must be patchable or upgradable. Naturally, device firmware should only be modifiable with the proper digital signature. As it stands, device vendors and manufacturers have a little financial incentive in ensuring ongoing IoT patch upgrades since revenue comes from the sale of the device, not the maintenance. The upkeep of IoT devices may detract from revenue. In addition, vendors are not legally held accountable for ongoing maintenance of devices beyond initial sales and competition drives vendors to cut corners, negating on quality for efficiency and speed of release into the market. While these factors may not have been critical previous to IoT, the interconnected nature of IoT devices raises the bar to a new level in terms of functionality and accountability. Detrimental also is the tendency of vendors towards planned obsolescence of devices to maximize profit through continued sales rather than through the upkeep of existing devices. Furthermore, IoT devices are not efficiently designed or configured to respond to OTA (over the air) updates, resulting in, at best costly, and at worst, unmanageable procedures. As it stands, many IoT devices are un-patchable, and as such, cannot be made secure. Researchers have observed that the ubiquitous advancement of IoT and the placement of unsecured and unattended IoT devices throughout homes and businesses will increase exponentially, opening up opportunities for hackers to exploit critical vulnerabilities. Further to planned obsolescence, many IoT devices simply have limited life cycles. Companies must be legally held accountable to monitor and maintain devices through prescribed and agreed-upon lifecycles. For this, there are needs for standards to be established and legislation put in place. In addition, vendors need to remain transparent and forthcoming about the life cycle of devices, especially in terms of service and upkeep policies, including the length of time they plan to support their devices. They need to take an active role in providing details on patches and upgrades as well as security risks and privacy concerns, ensuring that the consumer and/or user is informed about changes in policy, functionality, and security. The full lifecycle of the IoT device must be considered, beginning at manufacturing where security credentials must be “generated, allocated, and securely provisioned into the devices”. Deliberations must also integrate the lifecycle of the original manufacturer. When the original vendor no longer exists, it becomes impossible to trace credentials to patch vulnerabilities and security breaches, and vendors are inevitably replaced and/or go defunct or bankrupt.

3. Perform dynamic testing It is crucial that IoT devices undergo thorough testing, and establish a minimum baseline for security. Static testing is not intended or designed to find vulnerabilities that exist in the off-the-shelf components such as processors and memory into which may be a component of the overall application. Dynamic testing, on the other hand, is capable of exposing both code weaknesses and any underlying defects or vulnerabilities introduced by hardware and which may not be visible to static

analysis. Dynamic testing may discover vulnerabilities that are created when new code is used on old processors. We recommend manufacturers who purchase hardware and software from others do dynamic testing to ensure the items are secure.

4. Specify procedures to protect data on device disposal Eventually devices become obsolete and users may decide to throw them away. Devices should be discarded without exposing private data. This is a security issue because improperly discarded devices may be converted to serve malicious purposes. This is a privacy issue because, if left in operation or if disposed of improperly, obsolete hardware could be used to reveal personal information about the user or other stakeholders in the IoT ecosystem. The same will be true for IoT devices that are sold to second owners or that become standard equipment in homes and are conveyed upon sale of the house. We suggest manufacturers prepare a formal plan for users to sanitize and dispose of obsolete IoT devices. Industry practice in other fields prescribes a "discard, recycle or destroy" (DRD) policy with periodic review of the plan to determine which devices require disposal and how to dispose of them. Some manufacturers encourage users to dispose of products directly through the manufacturer. This may be sensible for laptops and servers, but for IoT devices that may be small and cheap, or that are part of a much larger device (like a refrigerator) special accommodations may be required. Individual users, when purchasing a used IoT product, might attempt to identify what personally identifiable information (PII) or authentication information such as username and password (UNPW) remains stored on the device, or is accessible by the device, or is required to be stored elsewhere to use the device. For example, the Amazon Echo Dot requires users to store their Wi-Fi network router passwords on an Amazon server. The question must be asked whether users should be expected to determine an individual DRD policy or not, which may include deleting information from any Internet-accessible location other than the device itself. As it stands, users are inadequately prepared, not possessing the digital skills needed to navigate this kind of level of security, and being ill-equipped to understand the complexities of password storage in connected devices. Exposure of such complexities often comes too late, as was the case in the recent revelation that modern copiers and fax machines have hard drives that retain copies of documents. Even corporate users with IT departments trained in security were unaware of this fact. The implications for security in the above example are numerous and highlight how easy it is for major security flaws to be left unaccounted for.

3.2.2 Securing Networks

1. Use strong authentication IoT devices should not use easy-to-guess username/password credentials, such as admin/admin. Devices should not use default credentials that are invariant across multiple devices and should not include back doors and debug-mode settings (secret credentials established by the device's programmer)

because once guessed, they can be used to hack many devices. Each device should have a unique default username/password, perhaps printed on its casing, and preferably resettable by the user. Passwords should be sophisticated enough to resist educated guessing and so-called brute force methods. Where possible we recommend two-factor authentication (2FA), which requires a user to employ both a password and another authentication form that does not rely on user knowledge, such as a random code generated via SMS text messaging. For IoT applications, we especially encourage the use of context-aware authentication (CAA), also known as adaptive authentication, in which use contextual information and machine-learning algorithms continuously evaluate the risk of malice without bothering the user in demanding authentication. If the risk is high, then the subscriber (or hacker) would be asked for a multi-factor token to continue having access.

2. Use strong encryption and secure protocols Even if device passwords are secure, communications between devices may be hackable. In the IoT, there are many protocols, including Bluetooth, Zigbee, Z-Wave, 6LoWPAN, Thread, Wi-Fi, cellular, NFC, Sigfox, Neul, and LoRaWAN. Depending on the protocol and available computing resources, a device may be more or less able to use strong encryption. Manufacturers should examine their situation on a case-by-case basis and use the strongest encryption possible, preferably IPsec and/or TLS/SSL. There may be cases where encryption is not desirable, such as in SAE J2735 Basic Safety Messages (BSMs), the wireless communications cars can use to avoid collisions. In those cases, messages can be sent in the open and verified using digital signatures. However, consideration should be given to the implications of omitting encryption. In the SAE J2735 case, BSMs could be used to alert collision-management systems falsely and immobilize an automobile. There is no stock answer that avoids the need for careful thought about the threat models anticipated and the vulnerabilities that will be tolerated. If data are transmitted unencrypted and unsigned, precautions should be made to ensure that false data have little or no chance of causing harm.

3. Minimize device bandwidth Recently DDoS attacks have been conducted in large measure by armies of poorly protected IoT devices that have become zombie systems in massive global campaigns. Most IoT devices are made of commodity components that have vastly overpowered network capabilities for the function they are supposed to perform causing congestion on home networks and potentially contributing to huge costs for the targets of IoT-borne DDoS attacks. If in the future there were 50 billion devices connected to the Internet, and if we assume (based on current conditions) that 1.1% of them are compromised and under coordinated remote control, that is 55 million rogue IoT devices. Suppose each device is capable of generating line-rate attack traffic equivalent to Gigabit Ethernet (81,274 - 1,488,096 frames per second), for example, the ARM9 system-on-a-chip (SoC) has two such connections built-in,

and it costs less than $5 to make per chip. Using this 55-million-device zombie army to generate DDoS events, attackers could generate between 4.47 to 81.8 trillion frames per second or 55 petabits per second. This is well beyond the defensive capabilities of any single service provider. An attack of this magnitude would overwhelm the fastest network interface built to date (300Gbps) by a margin of 183,333 to 1. There is no good way to reduce the malicious traffic produced by these systems apart from squelching it at the source. We recommend device manufacturers should limit the amount of network traffic IoT devices can generate to levels reasonably needed to perform their functions. There is very little need for an Internet-connected refrigerator to spew Internet Control and Management Protocol (ICMP) messages at gigabit-per-second speeds. While some refrigerators are outfitted with video screens, they more than likely do not need to have high-speed upload capabilities. Vendors should use hardware and kernel-level bandwidth limitations to throttle network transmission rates to levels reasonable for the tasks of each device. Such limitations make it much harder for an attacker to use a device in a DDoS attack, even if he has completely compromised it. Additionally, devices should be programmed to self-monitor for unusual behaviors and restore themselves to factory settings when alarming behavior is detected. If resetting devices to factory settings is not feasible, devices should at least reboot to potentially clear code the attacker has running in memory. Now, supposing the aforementioned 55 million malicious IoT devices had hardware/kernel-enforced attenuated bandwidth, say 10 Ethernet frames per second, then their aggregate potential attack profile drops to 550 million frames per second, and not more than 6.6 terabits per second. This is nearly 150,000 times smaller, and while it is still too big for a single defender, that size attack is feasible for a distributed set of defenders to stop. Additional kernel-level controls within devices that notice and attenuate large amounts of uploaded traffic or stop other unexpected behavior could further reduce the destructive capabilities of compromised devices without requiring heroic efforts by network defenders. Thus, we recommend serious consideration of the performance requirements of each device and those modest limitations be emplaced that are difficult to circumvent. This will greatly increase the safety of IoT devices and make it possible to safely field many more of them in the future.

4. Divide networks into segments Separate the network into smaller local networks using VLANs, IP address ranges, or a combination thereof. Network segmentations are utilized in next-generation firewall security policies to identify one or more source and destination interfaces on the platform. Each interface on the firewall must be assigned to a security zone before it can process traffic. This allows organizations to create security zones to represent different segments being connected to and controlled by, the firewall. For example, security administrators can allocate all cardholder or patient data repositories in one network segment identified by a security zone (e.g., Customer Data). Then the administrator can craft security policies that only permit

certain users, groups of users, specific applications, or other security zones to access the Customer Data zone – thereby preventing unauthorized internal or external access to the data stored in that segment. This type of solution is more common in industrial applications but may be useful in broader circumstances. A separate, detached private network for a security system, perhaps with a dedicated channel to a "home base" in the case of a home security system, might suffice. If the system must use the Internet, a virtual private network (VPN) might be implemented.

3.3 IoT Security Challenges in Support Layer

This layer is intended to provide a support platform that is reliable and dependable for the Application layer. In this layer, many different types of intelligent computing are arranged through cloud computing and grids. Bulk data processing and intelligent decision-making about network behavior take place at this level, and there is always the challenge of improving the ability to detect malicious information from healthy data. This layer requires a strong security architecture and the use of strong encryption algorithms and protocols.

Vulnerabilities and Security Threats in IoT Support Layer.

This layer consists of a variety of vulnerabilities and security threats, for example, the management identity and dynamic changes in IoT devices (heterogeneity), which could prevent the information from being sent to a valid node. Other threats to this layer of data access control include system complexity, physical security, encryption, infrastructure security, user identity, management approach to security, and incorrect software settings, privacy threats, and so on

Security in IoT: Threats and Vulnerabilities

The two most common threats and problems of the support layer are:

Denial of service attack and malicious insider attacks Attack: This attack is located in the Support Layer, which is connected to the network layer.

Malicious Insider Attack: This attack is accomplished by a user who is authorized to access the data of other users. It is a very complicated attack that requires different mechanisms to prevent the threat.

3.4 IoT Security Challenges in Application Layer

The application layer is the final layer that could be created in different methods based on the services provided. In this Application layer, end-users are allowed to use information through smart devices, and personalized services are provided according to their needs. The purpose of creating IoT is to use applications to make lifestyle smarter and reduce workload. Applications such as smart grids, smart homes, and cities smart health care systems, and smart transportation protocols are known as

autonomous vehicles that exist in this layer. An application layer protocol is distributed on a few final systems where a protocol is used to exchange packets from a program in one end system with other systems. In addition to the CoAP protocol, there are other protocols in this layer that are mentioned in the CoAP protocol and messages (RFC-7252); it runs on UDP and is, therefore, a lightweight protocol that is recommended for applications that require low bandwidth. DTLS protocol is used as a secured communication protocol that has been authorized by CoAP. The security of MQTT and AMQP protocols is managed using TL/SSL protocols. There is currently no global standard for the IoT application layer; hence security solutions vary for different application environments. For example, some industries use solutions based on 6LoWPAN architecture. Most application security architectures presented their security model using DTLS are based on the CoAP protocol, while some other application security architectures are based on the encryption of HTTP payloads. Moreover, one of the features in the Application layer is data sharing that raises issues related to information disclosure, data privacy, and access control. Every application has many users. Therefore, to prevent the access of unauthorized users, the authentication mechanisms specific to each program should be used. It should also be noted that data protection mechanisms and data processing algorithms are not without flaws, and it could cause the loss of data or information and as well as damaging the catastrophic. Hence, two factors are considered in the Application layer when solving the security problem: First is the authentication conditions and key agreement across the heterogeneous network. The second is the users' privacy protection. Besides that, information security training and management, especially password management, is crucial.

3.4.1 Security Threats and Vulnerabilities in Application Layer of IoT

In this section, some common attacks in the Application layer are mentioned as follows: Firmware Replacement Attack: When an object is running, or in the maintenance phase, its operating system, software, and firmware may be upgraded to take advantage of new features. The attacker may be able to disrupt the object's operational behavior through this upgrade by replacing malicious objects.

SQL injection

XSS Cross-site scripting attacks

Enumeration (CWE / SANS)

Common Weakness

Phishing Attack

Sniffing attack

Buffer overflow

3.5 Challenges of IoT Security

i. Unreliable Communication: Because of the diversity of communication media used in propagating potentially sensitive data, IoT applications can be vulnerability to several security vulnerabilities. Each such vulnerability can be unique, based on the medium involved. The wireless medium is one of the most vulnerable candidates. Note that the nature of this medium is broadcasting. Consequently, the transmission process based on this kind of media is vulnerable to eavesdropping, replay attack, and tampering attacks. The attacker can also inject malicious code into the wireless routing node, thereby affecting the communication of the whole wireless network. Collision is also a problem in wireless networks: even if the channel is available, it cannot guarantee that the communication is reliable. Another critical problem is a delay, particularly for applications that impose real-time constraints. In complex environments, there is large-scale deployment of sensor nodes via several ad hoc technologies, making manageability a non-trivial issue. Finally, the network topology is vulnerable to environment and node failure, which can compromise the reliability of information transmission.

ii. Hostile Environment: In IoT applications, many devices and nodes are deployed in a hostile environment, i.e., within the physical vicinity of the attacker. Attackers can consequently obtain information about devices and nodes through physical access, which can enable attacks such as tag cloning and, even worse, can physically destroy the device directly. At the same time, in a hostile environment, the energy consumption of the device also has certain requirements, making the device is resource-constrained. Attackers can exploit these constraints to launch a series of attacks, such as a sleep deprivation attack. Furthermore, resource constraints often preclude the application of sophisticated security frameworks and security algorithms on such devices.

iii. Inadequate Data and Privilege Protection: The issues of data security and permission have clear correspondence with Internet-of-Things security. Because of the lack of permission protection, the attacker can remotely access and modify the data in the system. The vulnerabilities with authorization, such as the over privilege, can allow attackers to perform unauthorized operations. Users' privacy is often easily violated due to the lack of protection for user input. In addition, by exploiting bugs on the program, attackers can inject malicious code into the system and extract data.

4.0 Self-Assessment Exercise(s)

Answer the following questions:

1. Explain the Security Considerations and challenges in the IoT Network Layer

2. Describe the Security Considerations and challenges in the IoT Support Layer
3. Mention five IoT open-source solutions

5.0 Conclusion

Interconnecting “things” and devices that take the form of wearables, sensors, actuators, mobiles, computers, meters, or even vehicles is a critical requirement for the current era. These inter-networked connections are serving the emerging applications of home and building automation, smart cities and infrastructure, smart industries, and smart everything. However, the security of these connected Internet of things (IoT) plays a centric role with no margin for error. After a review of the relevant, online literature on the topic and after looking at the market trends and developments, one can notice that there are still concerns about security in IoT products and services. This unit highlight the most significant problems related to safety and security in the IoT ecosystems. This unit identifies the general threat and attacks vectors against IoT devices while highlighting the flaws and weak points that can lead to breaching the security.

6.0 Summary

We have examined the security considerations and challenges in the IoT Network Layer, Support Layer, and application layer. We have seen the attack and vulnerabilities with countermeasures of open-source solutions.

7.0 Further Reading

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127IoTrpt.pdf

Corser G. et al (2017), Internet of Things (IoT) Security Best Practices. IEEE Internet Technology Policy Community White Paper. internet_of_things_feb2017.pdf (ieee.org)

Strategic principles for securing the internet of things (IoT) U.S. Department of Homeland Security, 2016. Strategic Principles for Securing the Internet of Things (IoT) (dhs.gov)

Chen K., Zhang S., Li Z., · Zhang Y., Deng Q., Ray S., and Jin Y. (2018), Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. Journal of Hardware and Systems Security (2018) 2:97–110 https://doi.org/10.1007/s41635-017-0029-7

Dhatrak A., and Sarkar A., (2020), Cyber Security Threats and Vulnerabilities in IoT International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 03

Pahlevanzadeh B., Koleini B., and Fadilah S., (2021), Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions M. Anbar et al. (Eds.): ACeS 2020, CCIS 1347, pp. 267–283, 2021.https://doi.org/10.1007/978-981-33-6835-4_18

Security Considerations Using IoT - Bing

Security Considerations for Internet of Things: A Survey | SpringerLink

Unit 2 - IoT Security Considerations Solutions

1.0 Introduction

In this section, we turn to an analysis of IoT security assurance from the point of view of system design. First, we analyze several requirements that must be met and some countermeasures. IoT security requirements Quality attribute IoT security description **Data integrity:** Data integrity ensures data integrity, reliability, and correctness and confirms that data has not been modified and destroyed. **Data confidentiality:** Data confidentiality aims at concealing data from unauthorized individuals, thus protecting users' privacy and sensitive data without being acquired by attackers. Only legitimate users can access the information. **Data availability:** Data availability is used to make sure that resources (e.g., data and service) are available. **Authentication:** Authentication defines verification and differentiation of identities that can access entities. In IoT, authentication protocols play an important role in mutual communication among different entities. **Authorization:** Authorization defines the process of granting, denying, and restricting access to entities. The authorization scheme performs different operations according to different entities.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Explain the Security Considerations and Solutions in IoT Network Layer.
2. Discuss the Security Considerations and Solutions in IoT Support Layer.
3. Describe the vulnerability and challenges of security in IoT

3.0 Main Content

3.1 Security Considerations and Solutions in IoT Network Layer.

Indicative security tips and solutions at the network layer can be focused and discussed in three categories of physical networks, remote connection, wireless networks, which are briefly discussed below:

Key security solutions in physical (wired) networks:

• Apply physical security to the network, for example, using CCTV cameras, entry cards to record people entering, creating safe areas to prevent unauthorized access

• Use of security mechanisms such as firewalls, IPS / IDS, and ACL (Access Control List): on the network

Significant security solutions in remote and mobile connection:

• Apply strong mechanisms (such as Multi-Factor Authentication: MFA) to authenticate authorized users to access the remote network

• Using secure communication channels such as (VPN Site to Site: VPN-S2S) for employees to access the organization's network

Significant security solutions in wireless networks:

• Use secure device and gateway settings when accessing wirelessly

• Use of cryptographic algorithms and authentication

3.2 Security Considerations and Solutions in IoT Support Layer.

Important security considerations and solutions that can be used in this layer are as follows:

• Implement security solutions in virtual machines such as operating system updates, how to access virtual machines (Virtual Machine: VM), and the use of strong control mechanisms in the application

• Secure data in the cloud using appropriate technology and approved encryption algorithms

• Designing solutions for recovery in times of crisis and continuity of service by providing snapshots of VMs, backup, and the existence of standby VMs on the site of cloud suppliers

• Protect the web by detecting and preventing malicious traffic by host-based firewalls and using IPS / IDS
• Log Monitoring, especially for authorized users and management of the event log com-plex from several sources with SIEM (Security Information and Event Management) solutions to analyze security incidents.

3.3 Security Considerations and Solutions in IoT Application Layer.

To secure applications, the following should be considered:

- Create applications (web, mobile applications, cloud applications) with secure standard code to minimize attacks
- Check the accuracy of the input data
- Testing applications (dynamic, static, and dual) to detect their vulnerabilities and take corrective action to eliminate the damage (s) and prevent information disclosure
- Using coded signatures: (Code Signing) to ensure customers the accuracy of the software
- Monitor important files to prevent any unauthorized changes
- Authenticate users
- Pay attention to data storage and retrieval security at each stage of data transfer
- Having a digital signature, certificate signature and certificate chain of a software update package
- Encrypt software images during transfer if the device supports remote softwar e upgrades
- Disable software ports that are not required for normal operation
- Use a single encryption key (different from other software keys) to confirm the final software.
- Separation of sensitive software components such as cryptographic processes from other software components or rating them more

3.4 IoT Open Source Solutions

Open IoT is an open-source IoT platform used to gather information from sensors via the cloud. It is also noted that OpenIoT is simple to use and can connect all your sensors. This helps to provide seamless IoT solutions to your users. OpenIoT also provides smart solutions for developing smart cities.

3.4.1 Encryption Algorithms and Mechanisms in IoT

Encryption and decryption mechanisms are needed to establish an improved IoT model based on its basic infrastructure. Cryptographic mechanisms are needed in all four layers of architecture. The encryption mechanism in the IoT is not a simple process due to limitations in equipment resources such as energy and computing

power. Common encryption algorithms such as MD5, SHA, AES, and RSA have complex computations, so it is necessary to implement lightweight encryption solutions to maintain computations, communications, storage, and ultimately energy efficiency. The problem is that light encryption works based on symmetric keys, which means sharing symmetric keys across different IoT devices, and thus can itself become a security challenge. Many components, strings, and lightweight encoder encryption solutions have been proposed, considering the limitations of hardware and software implementation.

3.4.2 Lightweight Stream Ciphers (LWSC) Algorithms

In this method, Pseudo-random key string that has the same length as plain text is used to encrypt the plain text, such that 'r' bits are encrypted and decrypted at the same time. The cryptographic process contains XORing plain text and a key string. The use of this cryptographic algorithm class is still limited even though it is another way to block cryptography. This limitation is because of the long initialization phase. The disadvantage of this method is that some protocols of communication are unusable. However, their main advantage is the hardware's easiness and simplicity of use when the plain text length is unrecognizable. The standard ciphers algorithms need round iterations with a higher number to access the intended level of security; therefore, other algorithms are invented created to use in IoT devices like WG-8, Fruit, Fruit-v2, Plantlet, Espresso, and Lizard. Algorithms GRAIN v1 (Extensive Analysis, with more flexibility in implementation, has a version with authentication support), Trivium (Extensive Analysis in design and support for 80-bit keys), Mickey v2 (less flexibility in Implementation) are widely used examples in the IoT. A comparison of streaming lightweight cryptographic algorithms.

3.4.3 Lightweight Block Cipher (LWBC) Algorithms

In limited-resource environments, the communication of the intelligent object must be able to handle certain energy limitations, performance, and efficiency. In cryptography, blocks have fixed bit lengths, generated and identified by a symmetric key. Block-based cryptography is the primary component in various cryptographic protocols design, and it is broadly used in the implementation of data encryption. Lightweight switch keys were introduced by the end of the 1990s purposely to ensure the security of communications. The main block cipher algorithms are defined as follows: AES 128 (modified AES), DESL (lightened DES), SIMON and SPECK (for simplification, flexibility and better performance with respect to hardware and software limitations The ISO/IEC 29192–2: 2012 Provides two components of encryption called CLEFIA (block part size with 128-bit length and key size with 128, 192 or 256-bit length and PRESENT (with emphasizing the problem of hardware constraints block part with64-bit length and key size with 80 or 128-bit length)for

using in IoT equipment. The key parameters for a light weight block cipher evaluation consist of block size, the number of rounds, structure type and key size. Light weight block cipher has two major structures, such as Fiestel and SPN (substitution–permutation network), although the other structures could be used, such as GFN. The advantages of lightweight block cipher encryption over conventional are in their sizes. The smaller block size, to save memory, and the smaller key size is used to save energy consumption, simplicity of the round with more repetition (for security access), simpler key scheduling (with the production of subkeys). The full-round of SFN is appropriately secure against major attacks like Man-in-the-Middle, integral and impossible Differential attacks. These results prove that SFN algorithm is more secure than other lightweight block ciphers algorithms. A comparison of the main some other lightweight cryptographic algorithms in the block cipher.

3.4.4 Lightweight Hash Functions (LWHF)

Hash functions can be used to verify message integrity, digital signature and another task such as fingerprint Due to resource constraints, the use of lightweight encryption functions is necessary to lighten the usage of hardware and power. Some of the proposed lightweight cryptographic algorithms using Hash functions are presented as follows. PHOTON, Quark, SPONGENT, SHA3 and Lesamnta-LW, all have lightweight internal structures and functions with less energy consumption. On the other hand, by reducing the size of messages, the computational volume can be maintained by considering the efficiency of the algorithm, which in turn is another advantage of lightweight compatible algorithms in the field of IoT. Studies have shown that the use of block cipher fragment encryption algorithms performs better in the IoT.

3.4.5 Symmetric and Asymmetric Lightweight Cryptographic Algorithms Used in IoT

Several lightweight cryptographic algorithms are currently divided into symmetric and asymmetric algorithms research categories. However, these lightweight algorithms are not providing any guarantee in real-time security, runtime, consumption of power, and the requirements of memory. Symmetric algorithms are lack authentication, while asymmetric algorithms have the issues of larger key size and higher memory consumption. This affects the collection and processing of real-time information and wastes IoT resources. Symmetric algorithms are highly secured and faster than asymmetric algorithms. The important symmetric algorithms are described as follows: The AES algorithm has three versions 128, 192, and 256 bits. This algorithm runs at the IoT application layer under the CoAP protocol. The key of the HEIGHT algorithm is created in the encryption and decryption stages. Lee and his colleagues suggested a parallel run that requires less energy. The TEA algorithm is used for confined environments such as sensor networks or smart objects. It does not

use a complex program but uses simple XOR operations to add and modify. PRESENT is used as a lightweight algorithm for security. Meanwhile, some important asymmetric algorithms are: Due to the RSA algorithm having a key with a large size, it does not own by the lightweight encryption system. As a result of using the first two large numbers and the execution of modular operations, ith as a higher security level and increases the users' privacy. The ECC algorithm requires a smaller key size. In this way, its processing speed is faster and requires less memory, and is suitable for implementation in IoT hardware. ECC algorithm uses a smaller key size in comparison to RSA to provide the exact level of security.

4.0 Self-Assessment Exercise(s)

Answer the following questions:

1. Explain the Security Considerations and solutions in the IoT Network Layer
2. Describe the Security Considerations and solutions in the IoT Support Layer
3. Mention five IoT open-source solutions

5.0 Conclusion

IoT security solutions are the software and embedded tools used to monitor edge devices, proactively detect threats, and facilitate remediation. As such, current IoT security solutions are a mix of standalone and bundle plans that include existing tools like EDR, encryption, IAM, EMM, and more to protect connected devices and networks. The proliferation of IoT devices means securing the next generation of IT environments will require IoT-specific security strategies and solutions. Organizations actively deploying IoT devices should be prudent about the security risks of insecure edge devices and proceed with caution.

Organizations need to visualize IoT assets under management, profile their risk, apply adequate protections, and monitor IoT traffic for unknown threats. Like so much else in cybersecurity, visibility informs action and strategy – making the upfront work of selecting an IoT security solution or assembly a strategy that much more valuable in avoiding unnecessary risk

6.0 Summary

We have examined the security considerations and solutions in the IoT Network Layer, Support Layer, and application layer. We have seen the attack and vulnerabilities with countermeasures of open-source solutions.

7.0 Further Reading

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127IoTrpt.pdf

Corser G. et al (2017), Internet of Things (IoT) Security Best Practices. IEEE Internet Technology Policy Community White Paper. internet_of_things_feb2017.pdf (ieee.org)

Strategic principles for securing the internet of things (IoT) U.S. Department of Homeland Security, 2016. Strategic Principles for Securing the Internet of Things (IoT) (dhs.gov)

Chen K., Zhang S., Li Z., · Zhang Y., Deng Q., Ray S., and Jin Y. (2018), Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. Journal of Hardware and Systems Security (2018) 2:97–110 https://doi.org/10.1007/s41635-017-0029-7

Dhatrak A., and Sarkar A., (2020), Cyber Security Threats and Vulnerabilities in IoT International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 03

Pahlevanzadeh B., Koleini B., and Fadilah S., (2021), Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges, and Solutions M. Anbar et al. (Eds.): ACeS 2020, CCIS 1347, pp. 267–283, 2021.https://doi.org/10.1007/978-981-33-6835-4_18

Unit 3 - IoT Use Cases

1.0 Introduction

Internet of Things (IoT) applications are becoming more widespread. According to Mckinsey, the percentage of businesses that use IoT technology has increased from 13% to 25% between 2014 and 2019. IoT enables a myriad of different business applications. Knowing those IoT examples and use cases can help businesses integrate IoT technologies into their future investment decisions. That is why we set out to create the most comprehensive list of IoT use cases in industries.

2.0 Intended Learning Outcomes (ILOs)

At the end of the unit, you should be able to:

1. Explain the IoT Use Cases in Utility companies
2. Discuss use case in Autonomous Vehicle

3. Describe IoT Security in Utilities Challenges
4. Explain IoT Security Solutions
5. Elucidate Use Case: IoT Security in Manufacturing Industry

3.0 Main Content

3.1 IoT Use Case: Utility Companies

Internet of Things (IoT) has transformed the energy industry. IoT-enabled products such as smart meters, automation control systems, home IoT sensors, power monitoring, and control equipment, and electric grid automation and protection relays help energy and utility companies drive efficiency and sustainability. These technologies maximize visibility and control over daily operations, allowing businesses to monitor asset performance, investigate accidents remotely, identify performance issues, plan for predictive maintenance strategies, and greatly improve operating efficiency. With energy and utility infrastructure spread across multiple generation assets, thousands of miles, and billions of devices (and growing fast), it is easily one of the most complex technology ecosystems to manage and run.

3.1.1 Automatic Smart Metering

The most common use case for utilities IoT is **Advanced Metering Infrastructure** (AMI) via smart meters. Smart meters provide utilities a direct channel to offer consumer value-adding services, such as direct usage feedback, flexible tariffs, and smart home applications. Realizing the full potential of IoT will be key in addressing challenges and opportunities utilities are facing today and in the overall digitalization of their business. Customer expectations, market regulations, increasing energy and power demand, electrification of transport, and the climate challenge are some of the things where digitalization will play a key role.

3.1.2 Trends in the utility industry

Short term

- IoT investment focused on regulatory compliance, operational efficiency, and sustainability
- The popularity of LPWA for a meter reading
- Climate change focus will speed up investments in the Smart Grid
- Direct communication link to consumers enables new services and more engaged consumers

Long term

- The breakthrough of electric vehicles will increase demand on grids
- Near real-time data will lead to intelligent energy distribution planning
- IoT facilitates the growth of the localized green energy production

3.1.3 Regulatory compliance and operational efficiency

Increasingly, regulations require the recording of accurate meter data at regular intervals, and that the data collected be made available to all actors in the grid being producers, consumers, or both. AMI is a cost-efficient way to collect accurate readings based on actual consumption from millions of meters. Smart meters also give utilities the ability to operate and upgrade every node remotely.

3.1.4 Electrical vehicle (EV) charging and smart home offerings

As more people buy electric cars, the demand for smart, connected charging stations installed at businesses and residences will increase. Intelligent charging stations have the potential to play a vital role in the grid as it can help balance the load. Energy suppliers can further influence demand by offering consumers incentives to use energy at non-peak times. For the end-customer, transparent pricing leads to lower bills, while the grid operator can reduce the cost of building greater capacity.

3.1.5 Mobile network connectivity for utilities

Mobile networks are well-tested and are not going away anytime soon. Our mobile IoT connectivity solution gives you access to well-established global networks which use licensed radio spectrum, free of disturbances and congestion from competing networks. Mobile technology offers a range of services from LPWA to 5G, meeting various use cases and requirements on speed and latency. Managed Connectivity allows you to conquer the complexity of IoT, we can help you simplify the development, rollout, and management of your connected solutions. With our solution, your solutions use the best available mobile networks to securely connect to your network or the internet.

3.1.6 IoT is redefining the power grid

With increasingly rapid mobile connectivity speeds, smart meters provide near real-time information on energy consumption and transmission. This data allows for more efficient, demand-based electricity generation and distribution. Smart meters are also facilitating the growth of the local, micro-production of energy such as solar panels and wind turbines. This creates potentially new revenue streams, as well as further efficiencies in production and distribution. It also creates interaction with other market players in – or outside the “traditional” ecosystem.

3.1.7 Collect consumption data effortlessly

Put an end to time and money spent on manual on-site meter readings and data processing of water, gas, and electricity consumption. Once activated, connected meters immediately start transmitting data over the Sigfox public network with no pairing or configuration required, and run for years without replacing the battery. You can now monitor and optimize your infrastructure in real-time to detect leaks and

breakdowns, and service providers can automate billing and remotely activate and deactivate services

3.1.8 On-site visits required only for maintenance and repair

Keeping an eye on operations at any kind of wind or solar energy installation is now easy and extremely cost-effective. Remotely monitored, real-time sensors can detect any failure or abnormal decrease in energy efficiency. These findings can be accessed instantly from any Internet-connected device and users can be alerted to abnormalities by SMS message or email

3.1.9 Monitor your backup power facilities

A reliable battery backup supply is crucial. It's usually on hand to pick up the strain if the main power source fails, but what happens if the backup battery has failed too? The result is a complete service breakdown. With the help of IoT monitoring solutions, companies can now monitor backup power supplies like never before. Maintenance crews can work far more efficiently with instant visibility of the status of all backup power sources, carry out remote diagnoses and obtain immediate alerts to any important event

3.1.10 Maintain stocks at optimum levels

Storage facilities are only useful if companies can accurately monitor stock levels. For most companies, the only solution currently available is manual checks, which are time consuming, costly and inefficient. The IoT provides a cost-effective solution for remote and accurate monitoring of tanks.

3.1.11 Electricity pole surveillance

Tilting of electricity poles as a result of strong wind, traffic accidents, earth movements, etc. can cause mechanical tension and cable breakage. To prevent the pole falling completely, it is essential to locate the problem quickly and carry out remedial action. Periodic measurements performed remotely by IoT devices enable preventive maintenance, and alerts are sent if major tilting occurs. Maintenance crews can now act before the pole falls and identify where urgent repairs are needed.

3.1.12 Monitor water facilities simply and remotely

IoT sensors provide crucial data on important water infrastructure conditions, which helps prevent malfunctions and flooding as well as improve maintenance crew efficiency. It's never been so easy to remotely measure water levels, pressure, turbidity, Ph, salinity, ORP, flow, etc. to prevent overflows, track drinking water supply and monitor the waste water network and treatment operations.

3.2 IoT Security in Utilities Challenges

Protection and testing mechanisms are critical in the implementation of any IoT program. We've highlighted the top security issues you can consider to help you build more stable and attack-proof internet of things connected devices and applications.

A. IoT Security-Data encryption

The Internet of Things (IoT) apps accumulates a large amount of data. Data storage and processing are essential components of the IoT ecosystem. Most of this information is personal and must be encrypted. Wherever the data is present online, one can use Secure Sockets Layer protocol, or SSL, to fix this IoT security problem. SSL certification is now used for websites to encrypt and secure consumer data on the internet. This is just half of the equation; the other half involves safeguarding the wireless protocol. Encryption is often needed when data is transmitted wirelessly. Sensitive information, such as locations, can only be accessible to the person in question. As a result, be sure to use a wireless protocol that includes encryption.

B. IoT Security Data Authentication

Also after good data encryption, there is always a risk that the system will be compromised. Protection is jeopardized if there is no way to verify the accuracy of data sent to and from an IoT computer. Assume one built a temperature sensor for smart homes. Even if the data is encrypted, if there is no way to verify the source of the data, someone can make up false data and send it to the sensor, telling it to cool the room even though it is cold, or vice versa. Authentication problems may not be obvious at first, but they do pose a security risk.

C. IoT Security Side-Channel Attack

Even with encryption and authentication in place, side-channel attacks are still possible. Such attacks are more concerned about how it is delivered than with the information itself. For example, if anyone has access to data such as timing, power consumption, or electromagnetic leak, any of this data will be used in side-channel attacks.

D. Hijacking of IoT Devices and Ransom-ware

Ransom-ware, a virus that encrypts and prevents access to users' confidential data, can attack IoT devices with poor measures of security. The real trouble starts when a hacker who compromised the computer with ransom-ware requests ransom money for the victim's files to be opened. It might sound dystopian, but it is a fact - although an uncommon one at the moment. However, in the underground hacker world, this is becoming more common. It's a frightening idea to see a house that's been locked up or a smart car that won't operate until the ransom is paid. Attacks like Ransom-ware have the potential to lock users out of IoT computers and associated platforms, as well as

uninstall devices and steal data. Because of the rapid growth in the number of IoT devices around the world, this particular IoT protection problem would be volatile in terms of potential permutations. However, since most IoT data is saved in the cloud, this ransom-ware does not have any sensitive data to lock.

E. Lack of updates and insufficient testing

One of the reliability problems with IoT systems is that manufacturers are often too sloppy when it comes to rigorous monitoring and timely app upgrades. Resultantly, the Internet of Things computer running obsolete applications may be vulnerable to a variety of ransom-ware and hacker attacks, as well as other security flaws. Another frightening probability is that when a computer transfers its data to the cloud after an upgrade, there can be downtime. If the link is not encrypted at this time, the upgrade files can be left vulnerable, allowing hackers access. For preventing IoT security problems, regular automatic updates are important. It is the responsibility of the vendor to their software that will help to discover the bugs and some ransom-ware type common attacks.

F. Home Intrusion

Home intrusions or home invasions IoT security problem. The idea of "smart houses" was born as the Internet of Things technologies became a feature of an increasing number of homes. This home automation poses a significant risk because rogue devices with weak protection mechanisms can broadcast IP addresses. Hackers could be able to find the address of the computer owner using so-called Shodan searches. The potential for misuse is obvious, and it may also lead to the user's address hitting criminal circles. Connecting with VPNs and protecting login credentials are two ways to avoid this IoT security violation, which we'll go through later in the post.

G. IoT driven Financial Crime

Financial crime and synthetic identity theft may increase for e-payment organizations that use the IoT. Several of these businesses are experimenting with IA and deep learning, but others quickly realize the value of combining data across many business layers. This is to ensure that deep learning is used to identify fraud patterns and complicated signals on time. Because of regulatory and technical challenges, all financial firms will face difficulties in launching these new versions. If they develop their model lifecycle and risk management plans to account for the growing danger of IoT security breaches.

H. Remotely access of Smart Vehicle

The hijacking of smart vehicles is an IoT security problem that is similar to a home invasion. Vulnerable IoT devices will open the door to serious dangers, such as remote access to the smart car. This deliberate intrusion poses a significant risk to public safety

because it can result in injuries. This vehicle control may also be vulnerable to attack because an attacker can demand payment in exchange for accessing the vehicle or for engine activation. Fortunately, since these attacks often occurred before the mainstream use of wireless networks, the developers had plenty of time to react accordingly.

I. Counterfeit and rogue

IoT devices Perimeter closing and controlling all single gadgets of user's even single user is a major IoT security problem. The rapid growth in popularity and manufacturing volume of Internet of Things products has created a problem with home networks.

J. Lack of Knowledge in IoT area

Users are also getting used to the Internet of Things' quirks and characteristics because it is such a modern application. Malware, viruses, and attacks are all areas where people have effectively perfected their security. Consumer illiteracy, perhaps the most serious IoT issue as puts anyone at risk, even consumers and others who are attached to their own IoT devices in any way. Through attacking people with the Internet of Things, social engineering attacks take advantage of the easiest to avoid by human aspects. The disastrous 2010 attack on an Iranian nuclear facility was an especially serious case of such misuse of the unprepared human element.

K. IoT Security Hardware Issue.

The hardware for the internet of things has been a challenge from the beginning. of the excitement and unexpected interest in IoT applications, chipmakers such as ARM and Intel are strengthening their processors for increased security with each new generation, but the practical scenario does not seem to ever close the security gap. The issue is that, due to the new architecture of chips designed especially for IoT applications, their costs will rise, making them costlier. Furthermore, the complicated architecture would necessitate more battery capacity, which would be a difficulty for IoT applications. Such chips cannot be used in low-cost portable IoT systems, necessitating a new strategy.

3.3 IoT Security Solutions

Having a rigorous research process in place is the only way to mitigate the hardware security risks of the internet of things. Some of the security solutions as

A. Device Range

The IoT device's range coverage network is critical. one must be very precise when it comes to the range metrics for the app or tablet. For example, if you're using Zigbee technology to control the device's network, one will need to figure out how many

repeaters one will need inside a building to give the computer enough connectivity range. However, one cannot simply add any number of repeaters because the power of the machine reduces as the number of repeaters increases. As a result, system range testing would allow one to discover the sweet spot where one can optimize range without exceeding the limit.

B. Capacity and Latency

Capacity refers to the network's bps (bits per second) handling speed, while latency refers to the total time it takes for data to migrate between application endpoints. To boost performance, developers are still looking for ways to increase ability and latency in their IoT applications. The problem is that these two variables are inversely proportional, which means that improving one degrades the other. Latency and power balancing should be carefully checked in data-intensive systems and applications.

C. Test for Manufacturability

It is rare that to build your own IoT system from the ground up. In most cases, you will be using third-party components and modules in the program. It is important to test these modules for proper operation. Manufacturers do assembly line checking on their own, so one can double-check. Additionally, after all of the components are assembled on a board, checking is necessary to ensure that no defects have been introduced due to soldering and wiring. Manufacturability testing is needed to ensure that the application functions as expected.

D. Make Strong Passwords and Change

Them Often Changing passwords on internet accounts, laptops, and handheld devices daily has become the standard in recent years. It should be standard for Internet of Things devices by now. For security reasons, each IoT system has its password, which one can update at least once a year, stop using standard or generic passwords, and make it complicated to crack. Password managers can help one recall them all because they can be cracked as well.

E. Do not Count the Cloud Computing

Cloud technology is certainly easy, but it is still a highly insecure and attack-prone new technology. Per product one purchase from an IoT manufacturer typically comes with cloud storage space. Although it may be tempting to choose something free, keep in mind that accessing the saved data in the cloud requires an active link, which can be hacked while one is accessing the cloud accounts. Often, ensure that the data is encrypted or, better still, that you store the files and data locally, away from the grasp of fraudsters. Stay away from universal plug-and-play features. 1) A majority of IoT units have a Universal Plug & Play feature that allows several devices to link to each other. This ensures one won't have to customize each computer separately.

2) While this gives a clear benefit to the Internet of Things environment in the home or office, be cautious.
3) Local networks are used to link Universal Plug & Play protocols.
4) As we have learned, these networks are vulnerable to outside threats and can be readily hacked.
5) If the attack were effective, it may affect a large number of IoT devices by allowing attackers to control from a remote location.

F. Make use of a backup network

Wi-Fi users also build several networks and define their access as limited for them or their friends. This method of creating a second network can be used for IoT devices because it aids in data collection.
1) Protect the confidential files from unauthorized entry.
2) Put an end to all efforts to take control of IoT devices and install malware.
3) Fully isolate the IoT system from the outside world, protecting protected info.
4) Make sure the IoT device is up to date regularly.
Automatic upgrades must be to search for official updates from the system vendor, as mentioned regarding the lack of updates as one of the IoT protection concerns. This applies security patches to the computing or digital devices which will prevent attackers from infiltrating them. Daily IoT product updates have the following benefits:
1) Peace of mind in ensuring that the devices are up to date with the most up-to-date security protocols, allowing one to avoid the most recent types of threats.
2) It provides a high level of protection to our offices, home and areas in which we need a high level of security like banks, etc.

3.4 Use Case: IoT Security in Manufacturing Industry

The IoT has had a large impact on manufacturing, and this is merely the beginning. The below discussed how the manufacturing industry is making headways through IoT.

1. Remote Monitoring

Remote monitoring is a great use case for leaders with industrial assets out in the field, such as machine builders. With IoT-connected assets, you can monitor equipment usage and health to assess performance and deploy service should there be any problems. Furthermore, with equipment data in hand, you can better understand the performance of your equipment to improve product design and ensure customer satisfaction. Not to mention, this could open an entirely new business model of Equipment-as-a-Service. Learn more about remote monitoring for machine builders and OEMs.

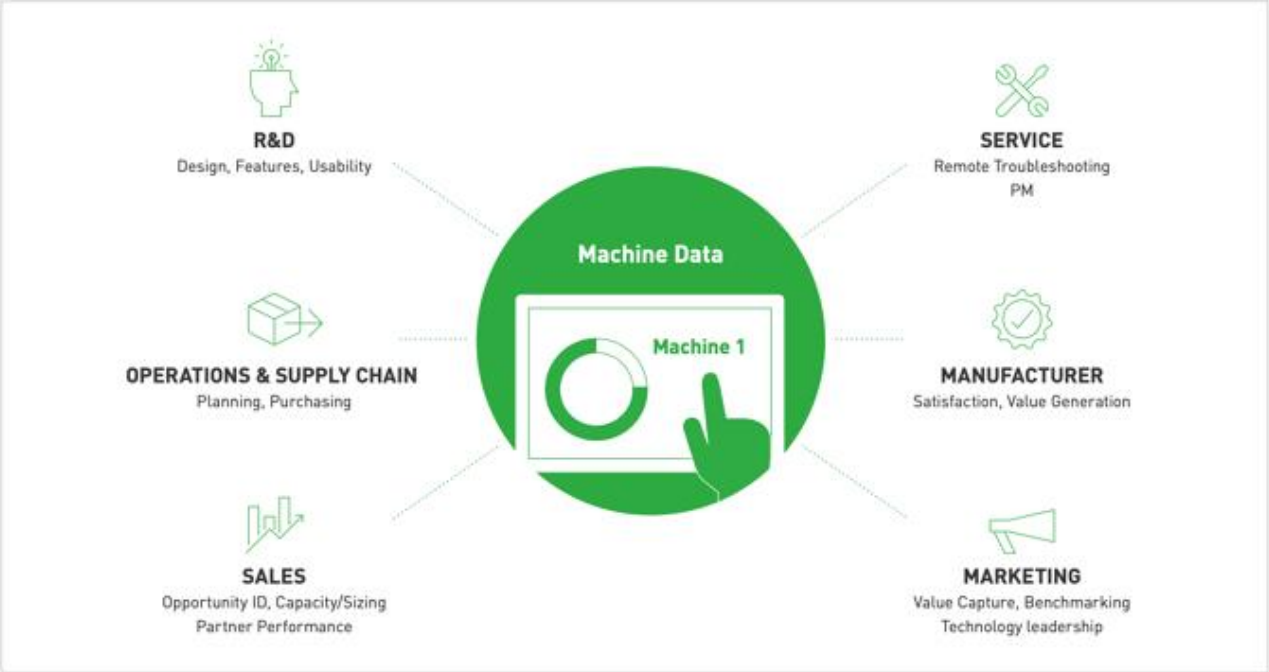


Figure 14: IoT Remote Monitoring

3. Supply Chain Management and Optimization

Imagine if the entire supply chain was connected? Imagine how each component of the supply chain was able to access and use data to ensure the highest rate of productivity? With the Internet of Things, there are several major benefits that the supply chain will experience, summed up well by SupplyChain:

- Real-time tracking of assets and products
- Automating warehouse tasks
- Paperwork management can be digitized
- Forecasting accuracy improves dramatically
- Operations have far greater control of inventory

4. Digital Twins

A virtual, or simulated real-world object, concept, or area within a digital space, digital twins are an interesting and powerful use case of IoT. They can even include a 3D representation of all of the physical assets, operational systems, and structures within an entire facility. This can help manufacturers test changes and simulate the impact without actually rolling out any physical changes.

5. Real-Time Machine Monitoring

Imagine giving operators and managers a gauge of how well machines are performing in real-time? They would have access to all the data they need to fix problems fast and ensure production schedules are met.

Real-time machine monitoring makes this possible, providing a stream of data straight from the machine control to provide accurate data analytics that can be used for in-the-moment decision-making or in-depth analysis.

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. Explain the IoT Security in Utilities
2. Describe the IoT Security Solutions

5.0 Conclusion

In conclusion, there are many different types of security issues and infrastructural challenges in every IoT architecture layer that should be considered for IoT creation and development. Meanwhile, each IoT security approach is required to have a new design of security classification. It could be used more easily and accurately to classify those IoT security threats and vulnerabilities. a four-layered IoT framework for security architecture is presented. Furthermore, the characteristics and performance of each layer were identified based on various threats and vulnerabilities, and security solutions and considerations that could improve security services at each IoT layer were stated. To have a secure system, it is essential to enhance the basic security principles in network implementation, including creating a safe and secure network environment, creating scaled protection, and data protection. As a final point, considering the future IoT security, standardization of global security mechanisms, and finding effective and efficient lightweight encryption techniques are described. In future researches, attention to the important intelligence, active defense systems, and resource conservation capabilities, comprehensive prevention and information security improvement, enhanced technology management, ongoing technological research, and ensuring IoT control capability is needed.

6.0 Summary

We have described the IoT Use Case in Utility Companies especially the Automatic Smart Metering and Autonomous Vehicle. We also discussed IoT Security in Utility challenges and IoT security solutions. IoT security in the Manufacturing industry was also described.

7.0 Further Reading

Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127IoTrpt.pdf

Corser G. et al (2017), Internet of Things (IoT) Security Best Practices. IEEE Internet Technology Policy Community White Paper. internet_of_things_feb2017.pdf (ieee.org)

Strategic principles for securing the internet of things (IoT) U.S. Department of Homeland Security, 2016. Strategic Principles for Securing the Internet of Things (IoT) (dhs.gov)

Chen K., Zhang S., Li Z., · Zhang Y., Deng Q., Ray S., and Jin Y. (2018), Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. Journal of Hardware and Systems Security (2018) 2:97–110 https://doi.org/10.1007/s41635-017-0029-7

30+ IoT Applications/Use Cases of 2021: In-Depth Guide (aimultiple.com)

Dhatrak A., and Sarkar A., (2020), Cyber Security Threats and Vulnerabilities in IoT International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 07 Issue: 03

Pahlevanzadeh B., Koleini B., and Fadilah S., (2021), Security in IoT: Threats and Vulnerabilities, Layered Architecture, Encryption Mechanisms, Challenges and Solutions M. Anbar et al. (Eds.): ACeS 2020, CCIS 1347, pp. 267–283, 2021.https://doi.org/10.1007/978-981-33-6835-4_18

Intertrust: How energy and utility companies can create a secure IoT device ecosystem, 2021

IoT trends in the utilities industry | Telenor Connexion

IoT use cases for utilities & energy. CBSigfox_UseCase_for_Utilities.pdf (connectedbaltics.com), 2021

managing-IoT-risks-in-power-and-utilities.pdf (assets.kpmg)

Afzal S, Faisal A., Siddique I., Afzal M. (2021), Internet of Things (IoT) Security: Issues, Challenges and Solutions. For all IJSER International Journal of Scientific & Engineering Research Volume 12, Issue 6

IoT in Manufacturing: Top Use Cases and Case Studies (machinemetrics.com), 2021

NXP EdgeLock™ SE050 Use Case: Securing the Industrial IoT, 2021

Module 4: Internet of Everything (IoE)

Module Introduction

The internet of everything (IoE) is a broad term that refers to devices and consumer products connected to the internet and outfitted with expanded digital features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices, and items connected to the global internet. The positive impact of the IoT on citizens, businesses, and governments will be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety.

Unit 1 - Opportunities with IoT
Unit 2 - Internet of Everything (IoE)

Unit 1 - Opportunities with IoT

1.0 Introduction

After years of hype, anticipation, and steady uptake, the Internet of Things (IoT) seems poised to cross over into mainstream business use. The number of businesses that use IoT technologies has increased from 13 percent in 2014 to about 25 percent today. And the worldwide number of IoT-connected devices is projected to increase to 43 billion by 2023, an almost threefold increase from 2018

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. describe the Opportunities with IoT in Business
2. discuss the Data Analytics with IoT
3. explain the Preventive and Predictive maintenance

3.0 Main Content

3.1 Opportunities with IoT

IoT is currently considered one of the most profound transitions in technology. Current IoT provides several data analytics opportunities for big data analytics.
shows examples of use cases and opportunities.
E-commerce
Smart Cities Retail & Logistics
Healthcare

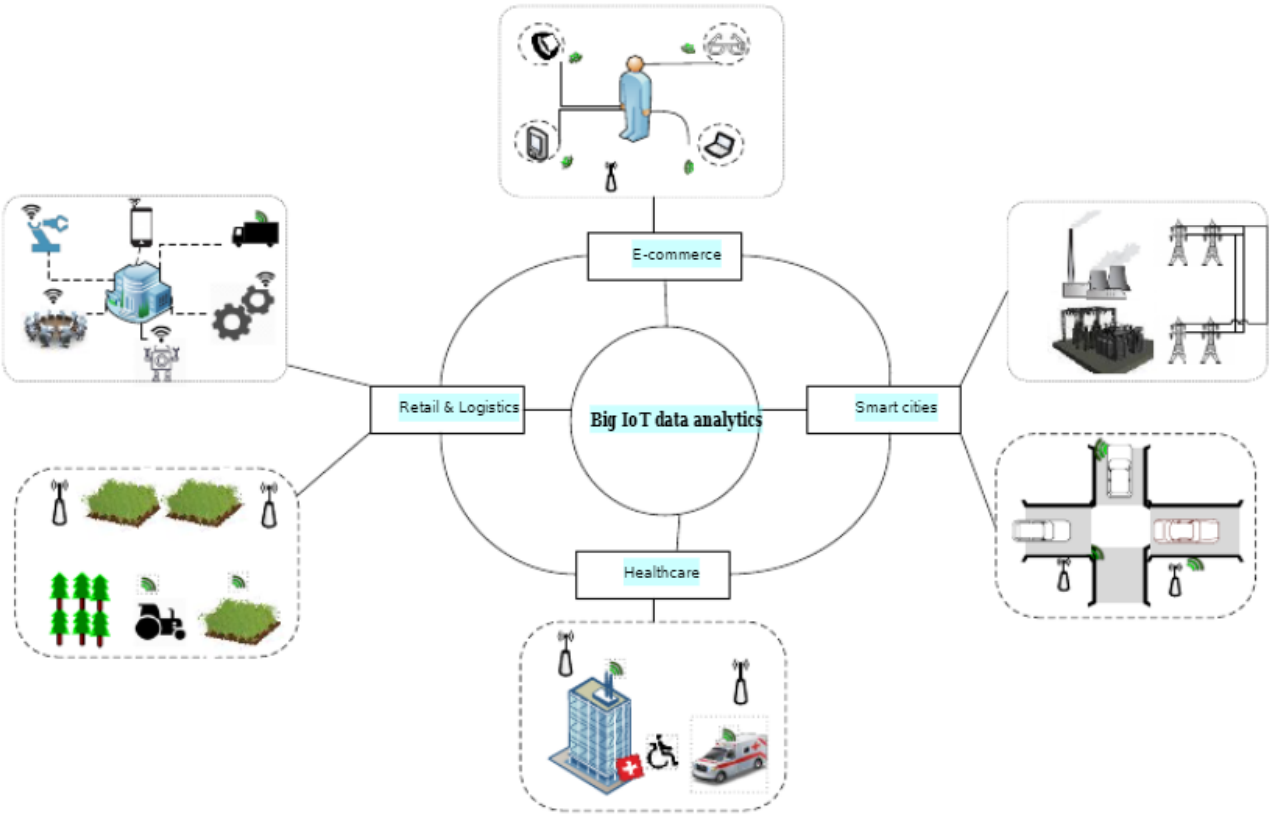


Figure 15: Example of use cases and opportunities for big IoT data analytics architecture

A. E-commerce

Big IoT data analytics offers well-designed tools to process real-time big data, which produce timely results for decision making. Big IoT data exhibit heterogeneity, increasing volume, and real-time data processing features. The convergence of big data with IoT brings new challenges and opportunities to build a smart environment. Big IoT data analytics has widespread applications in nearly every industry. However, the main success areas of analytics are in e-commerce, revenue growth, increased customer size, the accuracy of sale forecast results, product optimization, risk management, and improved customer segmentation.

B. Smart cities

Big data collected from smart cities offer new opportunities in which efficiency gains can be achieved through an appropriate analytics platform/infrastructure to analyze big IoT data. Various devices connect to the Internet in a smart environment and share information. Moreover, the cost of storing data has been reduced dramatically after the invention of cloud computing technology. Analysis capabilities have made huge leaps. Thus, the role of big data in a smart city can potentially transform every sector of the economy of a nation. Hadoop with the YARN resource manager has offered recent advancements in big data technology to support and handle numerous workloads, real-time processing, and streaming data ingestion.

C. Retail and logistics

IoT is expected to play a key role as an emerging technology in the area of retail and logistics. In logistics, RFID keeps track of containers, pallets, and crates. In addition, considerable advancements in IoT technologies can facilitate retailers by providing several benefits. However, IoT devices generate large amounts of data daily. Thus, powerful data analytics enables enterprises to gain insights from the voluminous amounts of data produced through IoT technologies. Applying data analytics to logistic data sets can improve the shipment experience of customers. Moreover, retail companies can earn additional profit by analyzing customer data, which can predict the trends and demands of goods. By looking into customer data, optimizing pricing plans and seasonal promotions can be planned efficiently to maximize profit.

D. Healthcare

Recent years have witnessed tremendous growth in smart health monitoring devices. These devices generate enormous amounts of data. Thus, applying data analytics to data collected from fetal monitors, electrocardiograms, temperature monitors, or blood glucose level monitors can help healthcare specialists efficiently assess the physical conditions of patients. Moreover, data analytics enables healthcare professionals to diagnose serious diseases in their early stages to help save lives. Furthermore, data analytics improves the clinical quality of care and ensures the safety of patients. In addition, physician profiles can be reviewed by looking into the history of the

treatment of patients, which can improve customer satisfaction, acquisition, and retention.

3.2 Data Analytics with IoT in Business

Advanced analytics on IoT data would help in analyzing the data collected over a large period, and in turn, gain a better insight into systems and their behavior. To create models to forecast future outcomes and to optimize the same. Collect information to estimate factors that would not be directly measured by sensors, by determining the relationship between different system parameters, and their impact on each other. To create real business value from the Internet of Things by leveraging IoT data and Analytics, companies need to set up their business objectives across the organization and identify and prioritize specific IoT use cases that support each of the organizational functions. Companies that have invested in IoT with a long-term view and business focus are well-positioned to succeed in this fast-evolving area.

Figure 16: Use cases of IoT data analytics

MARKETING / SALES / CUSTOMER SERVICES

Goals: To identify and meet customer needs, improve customer experience, differentiate product and service offerings, identify sales leads, develop long-term customer relationships, identify and generate new revenue streams, create new business models (e.g., pay per usage), and others.

Identification of Customer Insights and Opportunities: Companies use IoT analytics to analyse usage data of IoT-enabled products, device condition, and customer data to foresee customer needs, device usage, and purchasing behaviour to drive sales optimisations. They can automatically trigger alerts for cross-selling and up-sell opportunities, predict future purchases, and create new models for multiple purchases. On the consumer products and services side, for example, it is easy for Oil and Gas retailers to integrate vehicle-related services into cars with connected fueling, targeting drivers with tailored offerings based on their proximity to locations. Similarly, manufacturers of smart refrigerators with IoT-enabled technology, would be able to foresee when a customer's water filter is about to expire and automatically add them into a sales pipeline that market to that specific filter. Companies can create new dynamics in sales departments by providing upsell and cross-sell opportunities and

enabling sales staff to focus on selling, by reducing the time and effort required for data collection and account management tasks. In addition, companies can integrate.

3.3 Data Analytics with IoT: Business Efficiency

Data though collected by the devices need to be filtered to make it relevant and useful. The redundancy in the data being collected is predominant due to the sheer nature of the framework of IoT. The data is continuous hence the extraction of valuable information is not simple. This requires a good mechanism of protocols and software to ensure that the data is secured and also significant. Data is generally collected by the sensor devices in which these devices collect and transmit data to a centralized server. Similarly, the data is distributed back to the devices also. These activities require the performance efficiency of the network to be optimum. IoT involves several heterogeneous networks like wireless Sensor Networks (WSN), Wireless mesh networks, Wireless LAN. These networks would help in the transmission of data and also involve various types of quality issues ranging from performance to energy efficiency.

Big Data and IoT are complementary to each other and are two dimensions of perception. Managing the data and extracting information from it is a very vital task associated with IoT. An appropriate analytical platform is required to enable the derivation of knowledge from IoT data. IoT devices generate continuous streams of data in a scalable way. It is essential to handle the high volume of stream data and exploit the data. In a normal scenario of Big Data, the data might not be stream data, but the actions are. While in IoT data, it is a continuous flow. Applying real-time analytics is the need in the IoT environment. The advantages of IoT can be seen only when real-time analytics is applied to the data stored.

3.4 Industry and IoT

IOT DATA ANALYTICS APPLICATIONS/USE CASES BY INDUSTRY VERTICALS The IoT landscape is large and heterogeneous and many industry-specific data analytics applications have emerged around IoT-generated data. In industry verticals, insights generated from data analytics have to be matched with a deep understanding of industry dynamics and functional best practices. The following section of the Report illustrates some of the key examples of IoT data analytics use cases in various industry sectors including Agriculture, Energy, Utilities, Environment, and Public Safety, Healthcare/Medical and Lifestyle, Wearables, Insurance, Manufacturing, Military/Defence and Cyber Security, Oil and Gas, Retail, Public Sector (e.g., Smart Cities), Smart Homes/Smart Buildings, Supply Chain, Telecommunication and Transportation.

3.5 Use Case: Industry -Predictive Maintenance

AGRICULTURE

- USE CASES: Real-time crop monitoring and management, soil moisture monitoring for controlled irrigation, smart usage of fertilizers and pesticides to manage and reduce environmental impact, equipment scheduling and maintenance, animal health monitoring, and energy and greenhouse gas emissions management.
- Benefits: Reduction of environmental impact, reduced water, fertilizer, and pesticide consumption, resource optimization, livestock tracking, augmented crop productivity as well as numerous operational controls such as tracking water consumption to enable tariffing and detection of unauthorized water consumption

MANUFACTURING INDUSTRY

Case Study: Fastenal Uses Real-Time Machine Monitoring to run faster, gain production hours, take on more jobs, and produce more parts than ever before.

Predictive Maintenance

- There are many types of maintenance that manufacturers can employ at their facilities. As they advance in maturity, they can deploy more advanced forms of maintenance that are based on data. This data provides insight into the performance and health of equipment, giving maintenance teams a better understanding of when equipment needs to be serviced.
- With IoT-connected equipment, manufacturers can move from a calendar-based plan to a condition-based strategy. If manufacturers collect enough data on equipment performance and health, they can closely monitor variables to establish a threshold that can predict impending machine failure.
- This advanced form of maintenance, predictive maintenance, enables manufacturers to get the absolute most out of their maintenance spending while reducing downtime as much as possible.

Case Study: Predicting and Preventing Tool Failure

Production Visibility

- The only way for most manufacturers to know what is happening on the shop floor is to walk out onto the shop floor. Even then it may take some time to observe the operators and machines to truly understand where performance stands. They may have to engage with managers, analyze a whiteboard of part counts, etc.

- With connected equipment via a machine monitoring solution, manufacturing leaders, plant managers, and operators have insight into all their machines with visual dashboards tracking the performance against production goals.
- This opens many use cases for optimizing the performance of equipment, including process optimization, maintenance, and quality.

4.0 Self -Assessment Exercise(s)

Answer the following question:

1. Discuss the Opportunity in IoT use Cases
2. Describe Data Analytics with IoT in Business
3. Explain the Industry and IoT
4. What do you understand by Preventive maintenance?

5.0 Conclusion

The positive impact of the IoT on citizens, businesses, and governments will be significant, ranging from helping governments reduce healthcare costs and improving quality of life, to reducing carbon footprints, increasing access to education in remote underserved communities, and improving transportation safety.

6.0 Summary

Opportunity in IoT Use Cases has discussed and Data Analytics with IoT in Business. We also explain the Industry and IoT with preventive and predictive maintenances.

7.0 Further Reading

Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017, Gartner, December 2017, gartner.com.

Tulasi B, Girish J Vemulkar (2016), Blending IoT and Big Data Analytics International Journal of Engineering Sciences & Research Technology, 5(4)

Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Jayavardhana Gubbi, a Rajkumar Buyya,b, Slaven Marusic,aMarimuthu Palaniswami, Future Generation Computer Systems 29 (2013) 1645–1660

IoT Data Analytics Report, (2016) Ideya Ltd. /Camrosh Ltd. IOT Analytics Excerpts Final.pdf (ideya.eu.com)

Marjani M., Nasaruddin F.H., Gani A., Karim A., (2017), Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges (PDF) Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges (researchgate.net)

Unit 2 - Internet of Everything (IoE)

1.0 Introduction

The emergence of the Internet of Everything (IoE) technology addressed the rise in needs for better lifestyles and energy optimization. The growth of portable devices, such as smartphones and tablets, supports the new technology evolution. The global Internet of Everything (IoE) market is segmented into hardware, software, and services based on component type.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

1. Explain the basic concepts of the Internet of Everything
2. Describe the Economy effect of IoE
3. Describe the Use Cases of IoE

3.0 Main Content

3.1 Internet of Everything: Overview

The Internet of Everything (IoE) brings together people, processes, data, and things to make networked connections more relevant and valuable than ever before - turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries.

3.1.1 Internet of Everything (IoE) Market Overview:

Internet of Everything (IoE) refers to the network of embedded computing devices that are interrelated distinctively in the existing internet infrastructure. It is a networked connection of people, processes, data, and things. The emergence of the Internet of Everything (IoE) technology has addressed the rise in needs for better lifestyles and energy optimization. The growth of portable devices, such as smartphones and tablets, supports the new technology evolution. The global Internet of Everything (IoE) market is segmented into hardware, software, and services based on component type. In addition, the market includes several industry verticals, such as government, retail, Banking, Financial Services, and Insurance (BFSI), healthcare, IT & telecom, manufacturing, energy & utilities, transportation & logistics, and others (automotive, education, consumer electronics, and media & entertainment).

Top Investment Pockets

The following graph signifies the growth potential of the global Internet of Everything (IoE) market by industry. It was observed that the market is driven by the manufacturing and government sector, which occupied the maximum market share in 2014. The major factors that drive the growth in these segments include rise in penetration of smartphone devices; increase in online transactions; innovation of technology; growth in inclination of industries, such as manufacturing & mining toward process automation; surge in government initiatives to adopt Internet of Everything (IoE) technologies; rise in adoption of cloud-based Internet of Everything (IoE) solutions; and evolution of business models across various industries that include manufacturing.

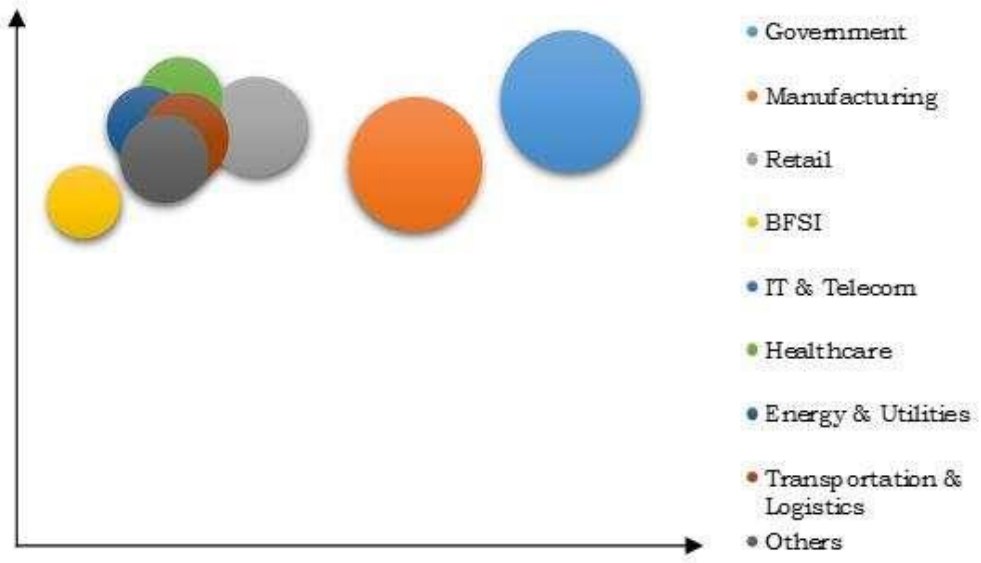


Figure 17: Top Investment Pockets

Drivers, Restraints, and Opportunities

Increase in Government Initiatives to Adopt Internet of Everything (IoE) Technologies

Government organizations in developed and developing nations, such as Germany, Russia, India, Mexico, and Brazil, focus on introducing various IT projects to encourage the end-users to increase expenditures on innovative technologies to enhance customer experience. For instance, the Malaysian Ministry of Science, Technology, and Innovation (MIMOS) launched the National Internet of Things (IoT) Strategic Roadmap in July 2015 to drive the adoption of the Internet of Everything (IoE), which is expected to contribute $2.49 billion to the country's gross national income by 2020.

Introduction of Smart Sensors and Devices

The growth in automation of manufacturing and operational processes across the industrial sector has encouraged the demand for smart sensors and devices. In addition, enhancing Internet of Everything (IoE) component providers to come up with advanced sensors, systems, and solutions to meet customer expectations. For instance, in 2016, ABB Ltd. in collaboration with EM Microelectronic developed smart sensor hardware that is used to transform traditional motors into an intelligent machines. It allows operators to get regular updates regarding operating conditions of the motor and scheduled repair & maintenance.

Storage Technology

In the component segment, the software segment is expected to grow at a considerable growth rate during the forecast period. Software used in the Internet of Everything (IoE) is applied for network connectivity, data analytics, management & automation, security, and connectivity management, thus offering security, data management, analytics, and communication. Expenditure on Internet of Everything (IoE) software has increased by both large- and medium-sized enterprises, globally. In addition, connectivity and network security software are in high demand to enhance customer experience and ensure protection against cyber-attacks.

Storage System

Automation of processes has significantly improved the operational competency of the manufacturing industry with reduced turnaround time and high productivity. The potential for cyber-physical systems to improve productivity in the manufacturing process and supply chain is enormous. The demand for smart devices that can make acceptable decisions in the process is expected to increase during the analysis period. Software, sensors, and wireless connectivity are vital parts of the manufacturing industry that offer an adequate foundation for the Internet of Everything (IoE). Manufacturers are investing in Internet of Everything (IoE) technology and solutions to simplify the processes, produce the maximum outcome, and meet the customers increasing requirements.

The Healthcare Internet of Everything (IoE) market size is expected to grow at the highest CAGR during the forecast period. Healthcare Internet of Everything (IoE) devices include mobile medical applications or wearables that allow patients or medical experts to capture health data. Hospitals use the Internet of Everything (IoE) to keep track of the location of medical devices, patients, and personnel. Advancements in medical technology and the high adoption of healthcare-connected devices are expected to increase the Internet of Everything (IoE) market share in the healthcare sector. However, a few factors that negatively impact the market growth include privacy & security of data, and reliability of devices.

3.2 Internet of Everything: Introduction

The Internet of Everything (IoE) is a broad term that refers to devices and consumer products connected to the Internet and outfitted with expanded digital features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices, and items connected to the global Internet. Cisco estimates that 99.4 percent of physical objects that may one day be part of the Internet of Everything are still unconnected. With only about 10 billion out of 1.5 trillion things currently connected globally, there is vast potential to “connect the unconnected.” Cisco predicts

that $14.4 trillion of value will be “at stake” over the next decade, driven by “connecting the unconnected” (people-to-people, people-to-machines, machines-to-machines, etc.) via the Internet of Everything. What do you mean by “Value at Stake” in the “Internet of Everything Economy”? Value at Stake is the potential bottom-line value that can be created, or that will migrate among private-sector companies and industries, based on their ability to harness the Internet of Everything over the next decade. Cisco predicts that this Value at Stake will be $14.4 trillion for companies and industries worldwide over the next 10 years. More specifically, over the next 10 years, the Value at Stake represents an opportunity to increase global aggregate corporate profits by about 21 percent. In other words, from 2013 through 2022, $14.4 trillion of value (net profit) will be “up for grabs” for private-sector businesses globally — driven by the Internet of Everything (IoE). IoE will both create new value and redistribute (migrate) value, based on how well companies take advantage of the opportunities that IoE presents. Those that harness IoE best will reap this value in either of two ways

The “Internet of Everything” terminology has been used frequently by technology analysts and research firms over the past couple of years. IoE is generally viewed as the next phase of the “Internet of Things,” another common term among technology analysts and research firms. Cisco did not coin the “Internet of Everything,” although our definition of IoE — combining people, process, data, and things — does differ somewhat from those of other technology companies and research/analyst firms.

IoE is a major market transition that, by its very definition, will attract the participation of many companies. However, Cisco is pursuing its research on IoE independently. Of course, Cisco and its partners will be working with customers to bring IoE to life. How does Cisco’s concept of the “Internet of Everything” differ from Qualcomm’s? Qualcomm uses the expression “Internet of Everything” as an umbrella term to define both the market opportunity associated with increasingly pervasive connectivity and new sources of information, especially machine-to-machine (M2M) and next-generation connected consumer devices, as well as the company’s wide-ranging solutions in this area. With an ecosystem of M2M technology partners, Qualcomm offers wireless technologies and chipsets for numerous industry-focused IoE applications, spanning passenger-car telematics, smart energy and security, industrial and enterprise automation, consumer M2M devices, and others. Cisco’s work on the Internet of Everything Economy explores the economic and strategic implications of IoE innovations for companies and looks at many of the same kinds of applications, such as smart buildings and factories, smart energy grids, intelligent vehicles, and connected healthcare and patient monitoring.

Internet Of Everything (IoE) has been one of the trendiest topics lately and it’s here, IoE is the upcoming most innovative and Ubiquitous technology advancement which

is going to make networked connections more relevant and valuable than ever before. Turning information into action creates new capabilities, richer experiences, and unprecedented economic opportunities for businesses, individuals, and countries.
Technically IoE refers to billions of devices and consumer products connected to the internet in an intelligent networked environment with expanded digital features.
It is a philosophy in which our technology future is compromised of different types of appliances, devices, and things connected to the global internet.
As of now, the internet connection is only restricted to Phone's/Tablet's, PC's and a handful of other devices but the idea behind IoE is that in the future, Machines will become more intelligent and cognitive by having more access to data and expanded network opportunities.

In simpler terms, IoE is the intelligent connection of people, processes, data, and things that will be transforming our world in such a way that there will be billions of connected devices having sensors to detect, measure and access their status all of which will be connected over a public or private network built over standard protocols like TCP/IP.

So how is the; **Internet of Everything** any different from the **Internet of Things**?
The difference is the **intelligent connection**. IoT is mostly about physical devices and objects communicating with each other but IoE brings with it the network intelligence to bind all these concepts together into a cohesive system. IoT has been limited to only machines thus achieving Machine to Machine Communication but IoE brings together people, processes, data, and things and adds them into the network therefore not just Phone/tablets and PCs but People. Health Fitness bands, Coffee pots, Marine containers all become a Node in an intelligent network communicating with each other. The more expansive IoE concepts include, besides M2M communication, M2P, and technology-assisted P2P communication. The IoE Economy will profoundly affect four major Aspects of our lives:

1. **People** –
   People will be connected to the internet in more relevant ways and will be generating data and interacting with devices not only through Mobile's/Tablet's, PC's and Social networks but also through Sensors placed on human skins or sewn into clothing which will provide a person's vital signs. In this way, people will themselves becomes Nodes on the internet.

A good example is Nike's wearable fitness band's which read a person's vital signs and sports apparel and gears embedded with chips that track the performance of Athletes.

2. **Things** –
   Things and physical items such as sensors, industry devices, consumer products, enterprise assets will be connected to the internet or each other, also fetching information from its surroundings, will be more context-aware, more cognitive, more intelligent, often so-called the internet of things.

As of 1984, only 1000 devices were connected to the internet which increased to about 1 million in 1992 and shot across 10 Billion in 2010, and as Cisco predicts there will be around 50 billion devices connected to the internet by 2020. These devices will be fetching data from their environment internally or externally and sending it back to the server for analyzing and making much more intelligent decisions.

3. **Data** –
   Rather than simply collecting Raw data, these connected devices will be sending higher level, more processed data back to respective servers for faster evaluation or more intelligent decision making.

Here the data is more about insightful information and action plan than just a random chunk. Figuring out a way to decipher the right flow of information is the key to making the best use of Big Data and as the types of data and sources increase, to draw useful insight's there will be a need to classify information and analyze it.

4. **Process** –
   With the equivalent to the IOE process, the right information will be delivered to the right person at the right time in an appropriate way. Technology-based Businesses will be relying on data to make further decisions and advance their workflow processes and strategies and will be therefore competing to leverage the data faster than their competitors for agile and faster decision making.

General Electrics predicts that IoE can add 15 trillion dollars to the Global Domestic Product while Cisco estimates 19 trillion in savings and profits for companies that can leverage IoE. But as the number of devices connected to the internet increase and therefore collect more data, privacy is put at risk which increases security concerns but as these devices grow more intelligent, hopes is that the device and network will grow knowledgeable enough to detect, stop and prevent any harmful threats. IoE is here and is inevitable, we should embrace ourselves to adapt our lives to the changes that it brings with it.

3.3 Internet of Everything: Use Cases

IoE is an intersection where all the roads like people, machines, and technology meet. To make things simpler, IoE is a world of sensors and detectors used to supervise and assess every move of either technology or human and keep in check their status.

Applications:

1. **Saving Lives by Connecting Roads and Hospitals:** Traffic crashes influenced the deaths of around 857 bicyclists in 2018 in the US, according to the US Department of Transportation some analysts had suggested that these lives could have been saved by leveraging the IoE. Connecting the helmet of a rider to necessary services like traffic signals, hospitals, and nearby police stations through sensors, medical treatment can be provided which can save innumerable lives. This way information about the patient's criticality can be directly received by the doctor by tracking a hospital around the vicinity right away so that the ambulance reaches the spot on time, enabling the ambulance to interact with the streetlights thus, showing green lights all the way, to take the victim to the hospital without any obstacles blocking the way, and allows the doctor to be ready with the essentials by the time patient arrives.

2. **Supply Chain Management:** Supply chain management has become a crucial sector after globalization and there has been immense competition in this sector. If there is a mechanism to alert the trucks about the early harvest, the time of delivery can be arranged with the supermarkets earlier, they can keep in check the available stock so that overstocking sales don't take place. This way the markets can escape from financial losses and the consumers can avail fresh produce every time. Even the harvesters can directly connect with retailers through a common platform and sell their products with profit without having to incur losses bypassing the intermediaries. To further boost customer gratification, customers can interact with the stores through their smartphones and can check notifications on the stock arrivals and the stores can even give early bird offers. It's a win-win game for all the stakeholders involved. Ever wondered why do you get all the advertisements about items that you just looked for on some app? It's all IoE! It is possible to collect data about the various searches that you look for all-day and IoE helps you by giving all the other available options that may be better.

3. **Elderly Care:** A significant amount of the population is now senior citizenry, and the needs of this section of people are completely different. There have been numerous attempts by various academicians and developers to fulfill these needs and to alleviate their day-to-day hardships. The role of IoE can serve as a solution to these everyday problems by helping the senior citizens stay active, and keeping them in touch with their loved ones. There are many robots in the market to nurse the elderly, take care of their health, give them timely medication and even by conversing with them these robots can alleviate their mental health issues if any. From assisting them on how to use smartphones to interact with their loved ones to offering companionship to those who are struggling with a disturbed mind, these robots provide emotional simulation.

4. **Connecting Homes for a Comfortable Life:** By establishing connections between different devices and equipment to automate the life processes IoE has innumerable opportunities to explore. Imagine how you would feel waking up to serene music with hot coffee beside your bed, imagine a robot feeding and watching your pets timely when you are not home, imagine a robot that knows your mood, taste, and health status and cooks accordingly. Imagine a home that adjusts to the outside temperature automatically. Doesn't it look like a wonderful and comfortable life? Imagine your home and life becoming like that one from the Sci-Fi movies you see, like, and desire to have. No, don't imagine it is possible with IoE now!

5. **Agriculture is No More a Hectic Human Task:** Demand for food supply is ever-increasing with increasing population but the supply even though increasing has always remained far below the demand. Governments across the world are bringing in new policies, giving incentives to farmers to equip new technologies, and increasing their spending in the R&D department to find ways to increase food production. Smart farming has always been in news but despite limited trials, it has never been employed on a full scale. To yield better results on investment for farmers, to eradicate hunger, and to reduce the demand-supply gaps smart farming is the way to go. From assisting the farmers in sensing the soil moisture, nutrient content, and controlling the water usage to connecting the farmers directly to the markets IoE has the potential to become an enabling factor in transforming the agriculture sector.

6. **Smart city technology as a solution to urban mobility:** According to an estimate of the UN, the population living in cities is expected to increase to 68% in 2050 from 55%. With increased growth comes increased challenges. WHO in a report said that approximately a 1.35million people die every year in road accidents. Overcrowding and congestion are two of the major reasons at the heart of this issue. Santa Clara, a city in California uses cloud-based data to optimize traffic. Highway cameras are centralized in the cloud-based operations center to analyze the videos. More dynamic traffic estimates are provided hence reducing the congestion on roads and providing the commuters the less congested routes thereby minimizing the traffic accidents.

San Jose, yet another city from northern California, has piloted a traffic optimization project to understand the peak hour traffics and reduce the accidents thereby caused. These are some cases where IoE has been tried and tested but there is more to this transformational technology that can serve as examples in the history of technology evolution.

IoE in Business

The business process has been in existence since the beginning of time and has been growing endlessly. What has caused the growth? The first thing that shaped an impressive business model was the feedback mechanism thus, bringing "target

marketing" in the game, consumer satisfaction being a major factor affecting the entire business. IoE has majorly influenced this department by bringing into the market various technologies that identify the needs of its customers. Micromarketing is majorly associated with numerous websites that allow the requirements of the customers to reach the business owners.

Not only that but IoE has also been implemented in the building of ERP software platforms like SAP Cloud Platform. This is used as an extension and integration platform for the running of various applications. SAP Fiori applications support the consumer goods system and enhance the sales process. It is all about reconnecting and re-engaging various service lines to remodel the business.

Pros: In this section, let us have a look at some benefits of the Internet of everything.

1. Information access- Information accessibility will now become a hassle-free task despite your location. The network of devices makes it easy for you to access information from any corner of the earth.
2. Communication- Better communication with interconnected devices with reduced inefficiencies.
3. Affordability- The same data that once took hours to transfer will now be done within no time hence negligibly reducing the delay and hence reducing the costs involved.
4. Automation- Automation has become the buzzword and has been intriguing humankind for quite a long time. This helps reduce human intervention and boosts the quality of services.

Cons: In this section, let us have a look at all the cons of the Internet of everything:

1. Privacy and security- There are a lot of "what ifs" and "buts" in the case of security and privacy. The leakage of data has always been a matter of concern. The privilege of technology comes at the cost of security. This is a major drawback but can be overcome with adequate measures and safety protocols. Data breaches and issues in law enforcement regarding the "deep web" have blown out in the world Recently, testimony has been held against Facebook accused of leakage of data.
2. Dependability- Technology has made us depend on it even for small tasks, making humans lazy and killing creativity in humans. The impact of technology is paramount in our everyday life processes

There are other obstacles like the availability of finance for the purpose and availability of power the entire time.

3.4 The Future Work:

The opportunities available for the future of IoE are endless. The capacity to automate, deploy and secure devices can change the face of industrial processes. The potential is

not just in connecting devices and hence in simplifying the life processes but to leverage data that can diversify the business processes and to overcome these challenges, new service providers come up in the markets opening new streams of revenue. High stakes have been put by scientists and academicians into IoE believing it will meet the high-end requirements of the market in the coming future. A human-machine interacting ecosystem is going to provide new experiences to the technology-driven world, new opportunities within remote learning. Developments in wireless networking like Li-Fi, 5G provide further impetus to IoE.

The Internet of Everything will re-invent industries at three levels: business process, business model, and business moment.
"At the first level, digital technology is improving our products, services and processes, our customer and constituent experiences, and the way we work in our organizations and within our partnerships," said Hung Le Hong, research vice president, and Gartner Fellow. "We do what we normally do, but digitalization allows us to do it better or develop better products within our industry."

As companies digitalize products and processes, completely new ways of doing business in industries emerge. Gartner analysts expect more transformational changes as digitalization re-invents industries at the business model level. Mr. Le Hong gave the examples of Nike, playing on the edge of the healthcare industry with its connected sporting clothes and gear, and Google having a visible presence in autonomous vehicles. "These organizations had no business in your industry, and are now re-inventing them," said Mr. Le Hong. The third level of digital re-invention is created by the need to compete with unprecedented business velocity and agility. Gartner calls this the "business moment." But as devices get more connected and collect more data, privacy and security concerns will increase too. How companies decide to balance customer privacy with this wealth of IoE data will be critical.

4.0 Self -Assessment Exercise(s)

Answer the following questions:

1. What do you understand by the Internet of Everything (IoE)
2. Explain the major areas where the IoE economy will affect our lives

5.0 Conclusion

The fusion of IoT and Big Data and the role of real-time analytics in IoT is an emerging technology that can drive a new wave of application of analytics into the regular

routines of humans. The scalability of IoT would lead to smarter applications in various domains ranging from health care to smart and secure homes. The actionable intelligence obtained by the application of real-time analytics on the data or "Big Data" of IoT is one of the main benefits of IoT. To tap into the advantages of IoT, Big Data analytics is needed. Even though it may feel like IoE has covered as much ground as it can, IoE has been mapping new territories enhancing its implementations, and expanding unexpectedly. Signaling more connectivity from cars, electronic gadgets, and toys to traffic lights and home security systems IoE facilitates connectivity between a range of internet-supported physical devices and non-internet supportive devices. With this emerging involvement of IoE in almost every field, many other technologies can be expected to naturally wane out of the process. Beyond just pure technological concepts for academicians, IoE is capable of transforming the socio-cultural fabric of the world by connecting people and processes.

6.0 Summary

At the end of this unit, we have described the overview of the Internet of Everything and its uses cases. The future work was also described.

7.0 Further Reading

IoE_Economy_FAQ.pdf (cisco.com)

Internet of Everything - GeeksforGeeks

Revolutionized IoT - Internet of Everything - GeeksforGeeks

Banafa A., (2016) The Internet of Everything (IoE)

The Internet of Everything (IoE) | OpenMind (bbvaopenmind.com)

Internet of Everything Market Statistics and Industry Analysis | Forecast (alliedmarketresearch.com)

What is the Internet of Everything (IoE)? - Definition from Techopedia

http://www.cisco.com/web/about/ac79/innov/IoE.html

Internet of Everything Explained - Internet of Things Wiki

http://internetofeverything.cisco.com/

http://www.cisco.com/web/solutions/trends/IoT/overview.html

http://time.com/#539/the-next-big-thing-for-tech-the-internet-of-everything/

http://www.gartner.com/newsroom/id/2621015

http://www.livemint.com/Specials/34DC3bDLSCItBaTfRvMBQO/Internet-of-Everything-gains-momentum.html

http://www.tibco.com/blog/2013/10/07/gartners-internet-of-everything/

http://www.eweek.com/small-business/internet-of-everything-personal-worlds-creating-new-markets-gartner.html