Internet of Things

18 MCA 5 4 E

FACULTY

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,

Associate Professor and Head,

Post Graduate Department of Computer Applications,

Government Arts College (Autonomous),

Coimbatore – 641 018.

UNIT – I

INTRODUCTION

Year	Subject Title	Semester	Subject Code
2018-2019 Onwards	ELECTIVE III: INTERNET OF THINGS	V	18 MCA 5 4 E

Objective: On Successful Completion of the Course the students should have understood IOT Protocols, Web of Things, Network Dynamics applications.

UNIT I:

Introduction: Definitions and Functional Requirements – Motivation – Architecture. The Toolkit Approach for End-user Participation in the Internet of Things. **Web 3.0: View of IOT** – **Ubiquitous IOT Applications** – **Four Pillars of IOT – DNA of IOT – Middleware for IOT:** Overview – Communication Middleware for IOT – IOT Information Security.

(Book 1** | Chapter 1 & 4**; Book 2** | Chapter 1 to 5**)

UNIT II:

IOT Protocol Standardization Efforts: M2M and WSN Protocols – SCADA and RFID Protocols – Issues with IOT Standardization – Unified Data Standards. **Protocols IEEE 802.15.4 – BACnet Protocol – ModBus – KNX – Zigbee Architecture:** Network Layer – APS layer – Security.

(Book 2** | Chapter 6**; Book 3** | Chapter 1, 3, 5, 6, 7**)

UNIT III:

Web of Things: Web of Things versus Internet of Things – Two Pillars of the Web. **Architecture Standardization for WOT:** Platform Middleware for WOT – Unified Multitier WOT Architecture – WOT Portals and Business Intelligence. **Cloud Computing:** Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems. **The Cloud of Things:** Mobile Cloud Computing – The Cloud of Things Architecture.

(Book 2** | Chapter 6.1, 7 to 9**)

UNIT IV:

Integrated Billing Solutions in the Internet of Things – Business Models for the Internet of Things. Network Dynamics: Population Models: Information Cascades – Network Effects. **Network Dynamics: Structural Models:** Cascading Behavior in Networks – The Small-World Phenomenon.

(Book 1** | Chapter 9 & 10**; Book 4** | Chapter 16, 17, 19, 20**)

UNIT V:

The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments – Resource Management in the Internet of Things: Clustering, Synchronization and Software Agents. Smart Grid – **Electrical Vehicle Charging.**

(Book 1** | Chapter 7 & 8**; Book 3** | Chapter 15, 16**)

TEXT BOOKS:

1. Dieter Uckelmann; Mark Harrison; Florian Michahelles, "*Architecting the Internet of Things*", Springer 2011.
2. Honbo Zhou,"*The Internet of Things in the Cloud: A Middleware Perspective*", CRC Press 2012.
3. Olivier Hersent, Omar Elloumi and David Boswarthick, "*The Internet of Things: Applications to the Smart Grid and Building Automation*", Wiley 2012.
4. David Easley and Jon Kleinberg, "*Networks, Crowds, and Markets: Reasoning About a Highly Connected World*", Cambridge University Press, 2010.

INTRODUCTION TO IOT

IoT comprises things that have unique identities and are connected to internet. By 2020 there will be a total of 50 billion devices /things connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data.

DEFINITION:

- The Internet of Things, also called The Internet of Objects, refers to a wireless network between objects, usually the network will be wireless and self-configuring, such as household appliances.

Wikipedia

- By embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves.

WSIS 2005

- The term "Internet of Things" has come to describe a number of technologies and research disciplines that enable the Internet to reach out into the real world of physical objects.

IoT 2008

- "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts".

IoT in 2020

CHARACTERISTICS:

1) **Dynamic & Self Adapting:** IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, users' context or sensed environment. E.g.: the surveillance system is adapting itself based on context and changing conditions.
2) **Self-Configuring:** allowing a large number of devices to work together to provide certain functionality.
3) **Inter Operable Communication Protocols:** support a number of interoperable communication protocols ans can communicate with other devices and also with infrastructure.
4) **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).
5) **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

IOT FUNCTIONAL REQUIREMENTS:

Functional requirements define the products and features that the IoT system must deliver. There are seven categories of requirements to consider when developing any IoT initiative for private or public institutions.

1. **Feature requirements**: What are the high-level expectations of the solution? This is the general goal of the initiative.
2. **Business requirements**: This is a description of the new or improved capabilities the user must be able to do as a result of the new system.
3. **Nonfunctional requirements**: This defines the service level expectations of the system such as availability, reliability, scalability, security, backup, and disaster recovery.
4. **Functional requirements**: This is a description of the functions that the user requires from the system. It should contain a process model, data entities, user stories, and use cases.
5. **System design requirements**: This defines the interaction of the IoT system with other systems.

6. **IoT data management requirements**: This describes how the data will be ingested and analyzed. The following four areas need to be defined:
   - **Ingestion**: how the data will be collected and integrated into one data source
   - **Analytics**: defines the predictive analytics models and data analysis requirements
   - **Communications**: who needs to be informed when an alarm is identified
   - **Persistence**: defines how long the data needs to be retained
7. **Reports and dashboards**: This defines the reports and dashboards that users need to rapidly analyze and respond to data collected.

MOTIVATION OF IOT:

IoT systems allow users to achieve deeper automation, analysis, and integration within a system. They improve the reach of these areas and their accuracy. IoT utilizes existing and emerging technology for sensing, networking, and robotics.

IoT exploits recent advances in software, falling hardware prices, and modern attitudes towards technology. Its new and advanced elements bring major changes in the delivery of products, goods, and services; and the social, economic, and political impact of those changes.

IOT – KEY FEATURES

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below;

- AI – IoT essentially makes virtually anything "smart", meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.
- Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.
- Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
- Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.
- Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

IOT ARCHITECTURE:

There is not such a unique or standard consensus on the Internet of Things (IoT) architecture which is universally defined. The IoT architecture differs from their functional area and their solutions. However, the IoT architecture technology mainly consists of four major components:

- Sensors/Devices
- Gateways and Networks
- Cloud/Management Service Layer
- Application Layer

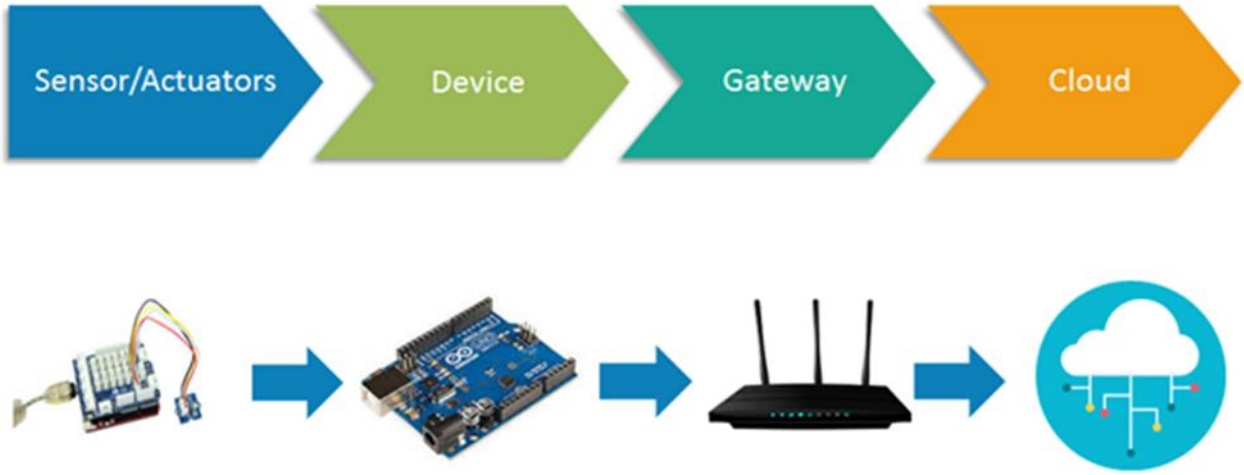


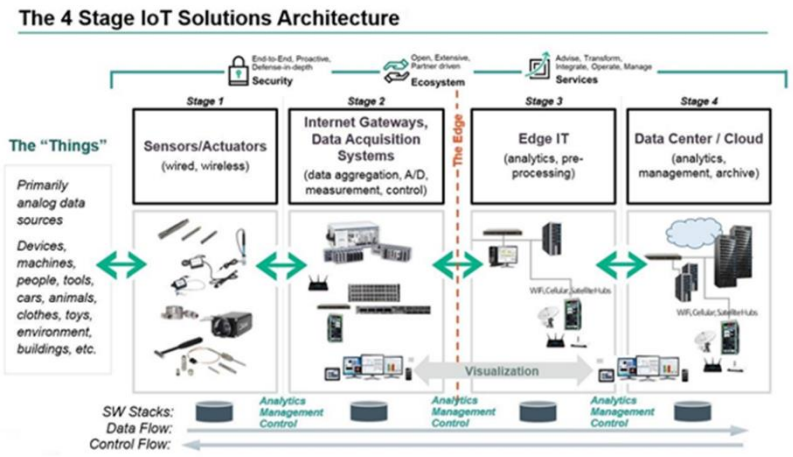
Figure 1: IoT Architecture

STAGES OF IOT SOLUTIONS ARCHITECTURE

There are several layers of IoT built upon the capability and performance of IoT elements that provides the optimal solution to the business enterprises and end-users. The IoT architecture is a fundamental way to design the various elements of IoT, so that it can deliver services over the networks and serve the needs for the future.

Following are the primary stages (layers) of IoT that provides the solution for IoT architecture.

- *Sensors/Actuators*: Sensors or Actuators are the devices that are able to emit, accept and process data over the network. These sensors or actuators may be connected either through wired or wireless. This contains GPS, Electrochemical, Gyroscope, RFID, etc. Most of the sensors need connectivity through sensors gateways. The connection of sensors or actuators can be through a Local Area Network (LAN) or Personal Area Network.
- *Gateways and Data Acquisition*: As the large numbers of data are produced by this sensors and actuators need the high-speed Gateways and Networks to transfer the data. This network can be of type Local Area Network (LAN such as Wi-Fi, Ethernet, etc.), Wide Area Network (WAN such as GSM, 5G, etc.).
- *Edge IT*: Edge in the IoT Architecture is the hardware and software gateways that analyze and pre-process the data before transferring it to the cloud. If the data read from the sensors and gateways are not changed from its previous reading value then it does not transfer over the cloud, this saves the data used.
- *Data center/ Cloud*: The Data Center or Cloud comes under the Management Services which process the information through analytics, management of device and security controls. Beside this security controls and device management the cloud transfers the data to the end user's application such as Retail, Healthcare, Emergency, Environment, and Energy, etc.

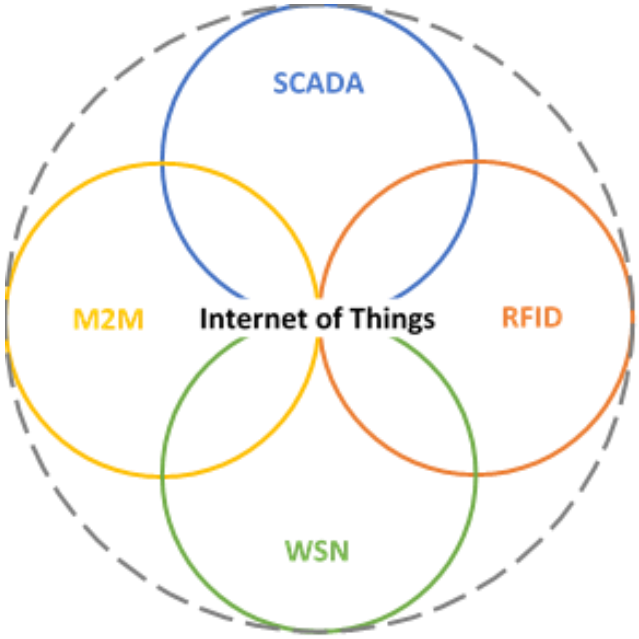


WEB 3.0: VIEW OF IOT:

Web 3.0, at least the concept, will use machines/computers to interpret the data collected from the IoT. This information will then be processed through an A.I. (Artificial Intelligence) that will provide suggestions on how to improve your meeting. These improvements will be based on every single attendees' habits, movements, and interactions with other attendees while attending your event. For example, venues that have grasped IoT technology will be able to track exactly what kind and how much food and beverage is being consumed in real time, allowing them to order food with a just-in-time delivery service to reduce spoilage and increase their margins by becoming more efficient, not by raising prices. This will also help the meeting planner understand what their attendees like and focus future menu items based on this new information.

The adoption of the IoT and Web 3.0 will increase your productivity by working for you. No longer will you need to spend hours processing data or sending out a post event survey and hoping for responses. Web 3.0 will also provide recommendations on venues based on the climate, time of year, number of attendees, and dozens of other factors to streamline your planning process. The data, information, and recommendations provided will arrive to you in real time and even transform your current agenda and meeting flow for next year.

FOUR PILLARS OF IOT:



1. **M2M:**

- Machine to Machine.
- Enables flow of data between machines which monitors data by means of sensors and at other end extracts the information on gathered data and processes it.
- Subset of IoT.
- It uses WAN, GPRS, Cellular and Fixed N/w's

2. **RFID:**

- Radio Frequency Identification
- Uses radio frequency to read and capture information stored on a tag attached to an object.
- A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked.
- Uses NFC (Next Field Communication protocol), IC (Integrated Circuit) Cards, Radio Waves.

3. **SCADA**

- Supervisory means top level.
- Control means controlling things.
- Data Acquisition means acquiring the data / reading the data.
- SCADA is a s/w used to control the hardware i.e., PLC, drives, servers, sensors and also acquire the data which is stored on the personal computer or Human Machine Interface (HMI).

4. **WSN**

- Wireless Sensor Networks.
- It senses and gathers data using sensors which are spatially distributed.
- It collects this data into a centralized location with the help of wired / wireless connection.

DNA OF IOT

DNA Connectivity IoT subscriptions are intended for corporate data transfer between sensors, devices and systems when mobile data transfer is required. We provide this service in 2G, 3G and 4G networks. Subscriptions can be easily and comprehensively managed via the DNA Control Center (a user interface provided by Cisco Jasper).

IoT subscriptions use DNA's nationwide mobile network. Mobile subscriptions are particularly suitable for connecting IoT devices located over a wide area – from large properties or factory buildings to cities – or where devices are in mobile use. IoT subscriptions make use of the mobile network's advanced information security features. The mobile network combines the reliability and continuity of an established technology with predictable development according to mobile technology standards.

SIM cards with various physical characteristics are available to suit the different user cases and devices. Subscriptions can be integrated into secure company-specific APN solutions, and an international roaming feature can also be added if you want to use the connections outside Finland.

THE TOOLKIT APPROACH FOR END-USER PARTICIPATION IN IOT:

PHASE 1: EPLORATION:

The first phase of the toolkit is "exploration". This phase begins with the iteration "understand", and forms the basis for understanding the context, problem, and users. Followed by the second iteration "discover" that is characterized by immersion in the situation, empathizing with the users and observing them, leading to discoveries of new ideas and insights. Having reached a level of understanding, combined with discoveries of ideas and insights, the third iteration "define" consists of framing these insights into well- defined opportunities and needs, pain points and positive experiences of the users. The entire process is iterative, and all these different processes overlap and repeat throughout, and that is especially true for the "think" iteration. Here this toolkit provides you with concrete ideation techniques and brainstorming tools which are helpful throughout the entire journey. Finally, in the "conceptualize" iteration all the insights are gathered and ideas are examined, combined, visualized and framed into a complete concept.

PHASE 2: EXPERIMENTATION:

Having formed a concept in the previous phase, it's now time to put it to the test. First, the "plan & engage" activities are considered important at the beginning of experimentation, to ensure sustainable end-user involvement. With careful planning the piloting or experimentation activities can be carried out in an engaging manner, keeping the stakeholders involved and informed throughout the process. The following "prototype" iteration consists of building and creating a prototype. Prototypes can take on many forms, from tangible MVPs (Minimum Viable Products) to intangible service or experience design prototypes, but the main goal of the

prototype is always the same: to "test" it in the third iteration. The purpose of building a prototype is to find answers, discover new insights and ideas, and to filter and measure the assumptions made. Therefore, these two iterations are often repeated numerous times, bringing you back to the first phase of exploration for new insights, ideas and concepts – by debunking your assumptions or validating insights. Once a well-defined, tested and validated prototype has come out from the many iterations throughout the processes, the process of "pre-launch" has to do with analyzing, validating, distilling and orchestrating the upcoming launch of the prototype. The "develop" iteration continues to develop, deploy and generate the prototype into a product or service.

PHASE 3: EVALUATION:

Many of the toolkits available across the various sources have focused on the previous two phases, but the third phase of evaluation is equally important. Beginning with the first iteration "launch", the final prototypes, products and services are realized and delivered. Very similarly, the second iteration "implement" refers to delivering to the stakeholders, but further so, focuses on the process of fully implementing the product/service and explaining its importance and impact for the context. The third iteration "Identify" finally identifies the outcome of the process and ensures the ongoing sustainability of the product/service in the future. LSPs looking for tools that serve in answering to their current needs can use the filters below to display the specific tools relating to each of the tracks: 1. use cases, 2. co-creation, 3. prototyping & testing, 4. user research. A selection can also be made according to the skill level, effort needed and overall level of difficulty in using the tool: beginner, intermediate, advanced.

IOT MIDDLEWARE:

Internet of Things middleware is software that serves as an interface between components of the IoT, making communication possible among elements that would not otherwise be capable.

Middleware connects different, often complex and already existing programs that were not originally designed to be connected. The essence of the Internet of Things is making it possible for just about anything (any Thing) to be connected and to communicate data over a network. Middleware is part of the architecture enabling connectivity for huge numbers of diverse Things by providing a connectivity layer for sensors and also for the application layers that provide services that ensure effective communications among software.

MuleSoft, Oracle, RedHat and WSO2 are among the companies that offer IoT middleware. These products provide API management as well as basic messaging, routing and message transformation. More comprehensive IoT platforms include middleware along with sensors and networking components.

IOT INFORMATION SECURITY:

The sheer volume of Internet of Things devices makes their security a high priority and is crucial for the future wellbeing of the internet ecosystem.

For device users, this means abiding by basic security best practices, such as changing default security passwords and blocking unnecessary remote access (e.g., when not required for a device’s functionality).

Vendors and device manufacturers, on the other hand, should take a broader approach and invest heavily in securing IoT management tools. Steps that should be taken include:

- Proactively notifying users about devices running outdated software/OS versions.
- Enforcing smart password management (e.g., mandatory default password changes).
- Disabling remote access to a device, unless it’s necessary for core functions.
- Introducing a strict access control policy for APIs.
- Protecting C&C centers from compromise attempts and DDoS attacks.

Imperva cloud WAF helps IoT manufacturers protect their C&C centers by providing on-edge traffic filtering services that ensure only authorized and authenticated client requests are allowed to reach their APIs.

Combining industry-leading WAF services and DDoS mitigation solutions, Imperva cloud WAF is able to secure its users against all online threats and efficiently handle multi-versioning from different devices.

For added reliability, the service is also equipped with load balancing and failover features that help operators handle organic traffic spikes, such as the kind that can occur upon the release of a new firmware patch.

THANK YOU

Study material for this course is taken from the Text Books and Reference Books, mentioned in the Syllabus.