Semester-II

18CSP204 INTERNET OF THINGS 4H – 4C

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

COURSE OBJECTIVE

- To Understand the Introduction to IoT and Architectural Overview of IoT
- To Understand the various IoT Protocols (Datalink, Network, Transport, Session, Service)
- To Understand the communication technologies in IoT Know the IoT protocols and web of things
- To Know the various applications of IoT

COURSE OUTCOME

A student who successfully completes this course should at a minimum be able to:

- Understand building blocks of Internet of Things and characteristics.
- Understand IoT protocols, Web of Things and Integrating IOT.
- Understand the application areas of IOT ·
- Realize the revolution of Internet in Mobile Devices, Cloud & Sensor Networks
- Learn about communication technologies used in IoT, Web of Things, Structural models and applications of IoT.

UNIT-I

Introduction : Internet Layers - Protocols - Packets - Services - Performance parameters - Peer-to-peer networks - Sensor networks - Multimedia - IOT Definitions and Functional Requirements –Motivation – Architecture - Web 3.0 View of IoT– Ubiquitous IoT Applications – Four Pillars of IoT – DNA of IoT - The Toolkit Approach for End-user Participation in the Internet of Things. Middleware for IoT: Overview – Communication middleware for IoT –IoT Information Security.

UNIT-II

IoT protocols : Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Issues with IoT Standardization – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – point-to-point protocols - Ethernet protocals - cellular Internet access protocal - Machine-to-machine protocol - Modbus – KNX – Zigbee Architecture – Network layer – APS layer – Security.

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 of Things: Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture.

UNIT-IV

Integrating IOT: 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.

UNIT-V

Applications: 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. Applications - Smart Grid – Electrical Vehicle Charging - Case studies: Sensor body-area-network and Control of a smart home.

SUGGESTED READINGS

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

WEB SITES

1. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot
2. https://www.i-scoop.eu/internet-of-things-guide
3. https://iot-analytics.com

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)

(Established Under Section 3 of UGC Act 1956)

COIMBATORE – 641 021.

LECTURE PLAN
DEPARTMENT OF COMPUTER SCIENCE

STAFF NAME: Dr. T. GENISH
SUBJECT NAME: INTERNET OF THINGS **SUB.CODE: 18CSP204**
SEMESTER: II **CLASS: I M. Sc - CS**

Sl.No	Lecture Duration (Periods)	Topics to be covered	Support Materials
		UNIT- I	
1	1	Introduction : Internet Layers - Protocols - Packets - Services	W1
2	1	Performance parameters - Peer-to-peer networks - Sensor networks - Multimedia	W1
3	1	IOT Definitions and Functional Requirements – Motivation – Architecture - Web 3.0 View of IoT	W1, W2
4	1	Ubiquitous IoT Applications – Four Pillars of IoT – DNA of IoT	T1: 27-90
5	1	The Toolkit Approach for End-user Participation in the Internet of Things.	T2: 65-85
6	1	Middleware for IoT: Overview – Communication middleware for IoT –IoT Information Security.	T1: 137-165
7	1	Recapitulation and Discussion of Possible Questions	
		Total No. Of Hours Planned for unit I	**07**

TEXT BOOK:		T1: The Internet of Things in the Cloud:A Middleware Perspective-Honbo Zhou–CRC Press 2012. T2: Architecting the Internet of Things – Dieter Uckelmann; Mark Harrison; Florian Michahelles- (Eds.) – Springer – 2011	
WEB SITES		W1: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot W2: https://www.i-scoop.eu/internet-of-things-guide	
Sl.No	**Lecture Duration (Periods)**	**Topics to be covered**	**Support Materials**
UNIT- II			
1	1	IoT protocols : Protocol Standardization for IoT – Efforts	W1
2	1	M2M and WSN Protocols – SCADA and RFID Protocols	W3
3	1	Issues with IoT Standardization – Unified Data Standards – Protocols	W1
4	1	IEEE 802.15.4 – BACNet Protocol	T3:3-28
5	1	point-to-point protocols - Ethernet protocols	W1
6	1	cellular Internet access protocal - Machine-to-machine protocol	W3
7	1	Modbus – KNX – Zigbee Architecture	T3: 79-110
8	1	Network layer – APS layer – Security.	W3
9	1	Recapitulation and Discussion of Possible Questions	
		Total No. Of Hours Planned for unit II:	**09**

TEXT BOOK:		T1: Networks, Crowds, and Markets: Reasoning About a Highly Connected World - David Easley and Jon Kleinberg, Cambridge University Press - 2010.	
WEB SITES		W1,W2, W3: https://iot-analytics.com	
Sl.No	**Lecture Duration (Periods)**	**Topics to be covered**	**Support Materials**
UNIT- III			
1	1	Web of Things: Web of Things versus Internet of Things, Two Pillars of the Web	T1:97-105
2	1	Architecture Standardization for WoT– Platform Middleware for WoT	W2
3	1	Unified Multitier WoT Architecture – WoT Portals and Business Intelligence.	W2
4	1	Cloud of Things: Grid/SOA and Cloud Computing –	W2
5	1	Cloud Middleware, Cloud Standards – Cloud Providers and Systems	T1:107-115
6	1	Mobile Cloud Computing – The Cloud of Things Architecture.	W3
7	1	Recapitulation and Discussion of Possible Questions	
		Total No. Of Hours Planned for unit III:	**07**
TEXT BOOK:		**T1**	
WEB SITES		**W2,W3**	

Sl.No	Lecture Duration (Periods)	Topics to be covered	Support Materials
		UNIT- IV	
1	1	Integrating IOT: Integrated Billing Solutions in the Internet of Things Business Models for the Internet of Things	T2:229-275
2	1	Network Dynamics: Population Models	T2:281-297
3	1	Information Cascades	W2
4	1	Network Effects	T2:299-302
5	1	Network Dynamics: Structural Models	W2
6	1	Cascading Behavior in Networks	W3
7	1	The Small-World Phenomenon	W2
8	1	Recapitulation and Discussion of Possible Questions	
		Total No. Of Hours Planned for unit IV:	**08**
TEXT BOOKS:		**T2**	
WEBSITES		**W2, W3**	
Sl.No	**Lecture Duration (Periods)**	**Topics to be covered**	**Support Materials**
		UNIT- V	
1	1	Applications: The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments	T2:195-225
2	1	Resource Management in the Internet of Things: Clustering	T2:159-190
3	1	Synchronization and Software Agents	T2:197-200

4	1	Applications - Smart Grid – Electrical Vehicle Charging	T2:201-203
5	1	Case studies: Sensor body-area-network and Control of a smart home.	W2
6	1	Recapitulation and Discussion of Possible Questions	
7	1	Discussion of Previous ESE Question Paper	
8	1	Discussion of Previous ESE Question Paper	
		Total No. Of Hours Planned for unit V:	**08**
Overall Planned Hours : 40			
TEXT BOOKS:		**T2**	
WEBSITES		**W2**	

SUGGESTED READINGS

1. The Internet of Things in the Cloud:A Middleware Perspective-Honbo Zhou–CRC Press 2012.
2. Architecting the Internet of Things - Dieter Uckelmann; Mark Harrison; Florian Michahelles-(Eds.) – Springer – 2011

WEBSITES

1. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot
2. https://www.i-scoop.eu/internet-of-things-guide
3. https://iot-analytics.com

UNIT I

SYLLABUS

Introduction: Internet Layers - Protocols - Packets - Services - Performance parameters - Peer-to-peer networks - Sensor networks - Multimedia - IOT Definitions and Functional Requirements –Motivation – Architecture - Web 3.0 View of IoT– Ubiquitous IoT Applications – Four Pillars of IoT – DNA of IoT - The Toolkit Approach for End-user Participation in the Internet of Things. Middleware for IoT: Overview – Communication middleware for IoT –IoT Information Security.

Internet Layers:

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the internet protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

IP defines how to address and route each packet to make sure it reaches the right destination. Eachgateway computer on the network checks this IP address to determine where to forward the message.

The history of TCP/IP

The Defense Advanced Research Projects Agency (DARPA), the research branch of the U.S. Department of Defense, created the TCP/IP model in the 1970s for use in ARPANET, a wide area network that preceded the internet. TCP/IP was originally designed for the Unix operating system, and it has been built into all of the operating systems that came after it.

The TCP/IP model and its related protocols are now maintained by the Internet Engineering Task Force.

How TCP/IP works

TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.

The transport layer itself, however, is stateful. It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it, which defines how applications can communicate over a network.

TCP/IP model layers

TCP/IP functionality is divided into four layers, each of which include specific protocols.

- *The application layer* provides applications with standardized data exchange. Its protocols include the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP).
- *The transport layer* is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control,

multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

- *The network layer*, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.
- *The physical layer* consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

Advantages of TCP/IP

TCP/IP is nonproprietary and, as a result, is not controlled by any single company. Therefore, the internet protocol suite can be modified easily. It is compatible with all operating systems, so it can communicate with any other system. The internet protocol suite is also compatible with all types of computer hardware and networks.

TCP/IP is highly scalable and, as a routable protocol, can determine the most efficient path through the network.

Protocol

A **network protocol** defines rules and conventions for communication between **network** devices. **Network protocols** include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.

Types of Protocols

TCP. Transmission control protocol is used for communication over a network. ...

Internet Protocol (IP) IP is also working with TCP. ...

FTP. File transfer protocol is basically used for transferring files to different networks. ...

SMTP. ...

HTTP. ...

Ethernet. ...

Telnet. ...

Gopher.

Common network protocols

1. TCP/IP (Transmission Control Protocol/Internet Protocol) suite.
2. ARP (Address Resolution Protocol)
3. DHCP (Dynamic Host Configuration Protocol)
4. DNS (Domain Name System)
5. FTP (File Transfer Protocol)
6. HTTP (Hyper Text Transfer Protocol)
7. HTTPS (Hypertext Transfer Protocol Secure)

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internetaddress of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

A packet-switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit-switched, is used for networks allocated for voice connections. In circuit-switching, lines in the network are shared among many users as with packet-switching, but each connection requires the dedication of a particular path for the duration of the connection.

"Packet" and "datagram" are similar in meaning.

Services

In computer networking, a **network service** is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with it.

Examples are the Domain Name System (DNS) which translates domain names to Internet protocol (IP) addresses and the Dynamic Host Configuration Protocol (DHCP) to assign networking configuration information to network hosts. Authentication servers identify and authenticate users, provide user account profiles, and may log usage statistics.

Performance parameters

The following measures are often considered:

- **Bandwidth** commonly measured in bits/second is the maximum rate that information can be transferred
- **Throughput** is the actual rate that information is transferred
- **Latency** the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
- **Jitter** variation in packet delay at the receiver of the information
- **Error rate** the number of corrupted bits expressed as a percentage or fraction of the total sent

Latency

- Refers to the amount of time (usually measured in milliseconds) it takes for data to travel from one location to another across a network (or across the Internet, which is a network itself).
- Is sometimes referred to as delay, because your software is often waiting to execute some function while data travels back and forth across the network. For example, Internet Explorer can't display a story from CNN.com until CNN's Web servers respond to your request for that page.
- Is often less than 100 milliseconds on today's high-speed network, which has very little impact on Web surfing.

Bandwidth and throughput

- These two terms are sometimes used interchangeably, and though they are related, they're not quite the same. They both refer to the amount of data transferred between two points on a network in a given period of time. In other words, how many bits per second can you send across your network or over your Internet connection?

Uptime or responsiveness

- Uptime, sometimes referred to as availability or responsiveness, refers to the amount of time that a computer or a network connection is functioning and usable.

Hardware and software

- Your network relies on switches, servers, routers and firewalls, so network monitors can usually track metrics such as CPU utilization, remaining hard drive space and memory use.

Example:

If you're planning to install Voice over IP (VoIP) or any other application that relies on live, real-time transmission of video or audio, you need to ask your service provider about their latency. Real-time voice and video applications are sensitive to network delays. For instance, with VoIP, you'll notice that the audio is choppy, with lots of pauses and dropped syllables. **Jitter** refers to variation in the amount of latency, and it has a similar negative impact on real-time communication.

Peer-to-peer networks

A **peer-to-peer** (**P2P**) **network** is created when two or more PCs are connected and share resources without going through a separate server computer. A **P2P network** can be an ad hoc connection—a couple of computers connected via a Universal Serial Bus to transfer.

A P2P network also can be a permanent infrastructure that links a half-dozen computers in a small office over copper wires.

The initial use of P2P networks in business followed the deployment in the early 1980s of free-standing PCs. In contrast to the minimainframes of the day, such as the VS system from Wang Laboratories Inc., which served up word processing and other applications to dumb terminals from a central computer and stored files on a central hard drive, the then-new PCs had self-contained hard drives and built-in CPUs. The smart boxes also had onboard applications, which meant they could be deployed to desktops and be useful without an umbilical cord linking them to a mainframe.

Characteristics of a Peer Network

Peer-to-peer networking is common on small local area networks (LANs), particularly home networks. Both wired and wireless home networks can be configured as peer-to-peer environments.

Computers in a peer-to-peer network run the same networking protocols and software. Peer networks devices are often situated physically near one another, typically in homes, small businesses and schools. Some peer networks, however, utilize the internet and are geographically dispersed worldwide.

Home networks that use broadband routers are hybrid peer-to-peer and client-server environments. The router provides centralized internet connection sharing, but files, printer, and other resource sharing are managed directly between the local computers involved.

In a P2P environment, access rights are governed by setting sharing permissions on individual machines.

For example, if User A's PC is connected to a printer that User B wants to access, User A must set his machine to allow (share) access to the printer. Similarly, if User B wants to have access to a folder or file, or even a complete hard drive, on User A's PC, User A must enable file sharing on his PC. Access to folders and printers on an office P2P network can be further controlled by assigning passwords to those resources.

Benefits of a Peer-To-Peer Network

P2P networks are robust. If one attached device goes down, the network continues. Compare this with client-server networks when the server goes down and takes the entire network with it.

You can configure computers in peer-to-peer workgroups to allow sharing of files, printers and other resources across all the devices. Peer networks allow data to be shared easily in both directions, whether for downloads to your computer or uploads from your computer

On the internet, peer-to-peer networks handle a high volume of file-sharing traffic by distributing the load across many computers. Because they do not rely exclusively on central servers, P2P networks both scale better and are more resilient than client-server networks in case of failures or traffic bottlenecks.

Peer-to-peer networks are relatively easy to expand. As the number of devices in the network increases, the power of the P2P network increases, as each additional computer is available for processing data.

Security Concerns

Like client-server networks, peer-to-peer networks are vulnerable to security attacks.

- Because each device participates in routing traffic through the network, hackers can easily launch denial of service attacks.
- P2P software acts as server and client, which makes peer-to-peer networks more vulnerable to remote attacks than client-server networks.
- Data that is corrupt can be shared on P2P networks by modifying files that are already on the network to introduce malicious code.

Sensor networks

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity.

Building sensors has been made possible by the recent advances in micro-electro mechanical systems (MEMS) technology. Each node of the sensor network consists of three subsystems: the sensor subsystem which senses the environment, the processing subsystem which performs local computations on the sensed data, and the communication subsystem which is responsible for message exchange with neighboring sensor nodes. While individual sensors have limited sensing region, processing power, and energy, networking a large number of sensors gives rise to a robust, reliable, and accurate sensor network covering a wider region. The network is fault-tolerant because many nodes are sensing the same events. Further, the nodes cooperate and collaborate on their data, which leads to accurate sensing of events in the environment. The two most important operations in a sensor network are data dissemination, that is, the propagation of data/queries throughout the network, and data gathering, that is, the collection of observed data from the individual sensor nodes to a sink.

Sensor networks consist of different types of sensors such as seismic, thermal, visual, and infrared, and they monitor a variety of ambient conditions such as temperature, humidity, pressure, and characteristics of objects and their motion.

Sensor nodes can be used in military, health, chemical processing, and disaster relief scenarios. Some of the academic and industry-supported research programs on sensor networks include working on Smart Dust at the University of California, Berkeley (UCB), and wireless integrated network sensor (WINS) at the University of California, Los Angeles (UCLA).

Various protocols for the major operations of data dissemination and gathering are then described, followed by specialized MAC protocols developed or modified to suit sensor networks. Techniques adopted by sensor nodes to discover their location and the measures to assess the quality of coverage of a sensor network are described.

Finally, some sensor-network specific issues such as energy-efficient hardware design, synchronization, transport layer protocols, security, and real-time communication are discussed.

Applications of Sensor Networks

Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events. The military applications of sensor nodes include battlefield surveillance and monitoring, guidance systems of intelligent missiles, and detection of attack by weapons of mass destruction, such as chemical, biological, or nuclear. Sensors are also

used in environmental applications such as forest fire and flood detection, and habitat exploration of animals. Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure. The data collected can be sent regularly over the network to automated monitoring systems which are designed to alert the concerned doctor on detection of an anomaly. Such systems provide patients a greater freedom of movement instead of their being confined to a hospital. Sensor nodes can also be made sophisticated enough to correctly identify allergies and prevent wrong diagnosis.

Sensors will soon find their way into a host of commercial applications at home and in industries. Smart sensor nodes can be built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled. The home can provide a "smart environment" which adapts itself according to the user's tastes. For instance, the lighting, music, and ambiance in the room can be automatically set according to the user's preferences.

Similar control is useful in office buildings too, where the airflow and temperature of different parts of the building can be automatically controlled. Warehouses could improve their inventory control system by installing sensors on the products to track their movement. The applications of sensor networks are endless, limited only by the human imagination.

Multimedia

Multimedia is the field of Computer Science that integrates different forms of information and represents in the form of audio, video, and animation along with the traditional media, i.e., text, graphics/drawings, images, etc.

Multimedia Computer System

Multimedia computer system has high capacity to integrate different media including text, image, graphics, audio, and video.

The multimedia computer system stores, represents, processes, manipulates, and makes available to users.

Significant Features of Multimedia Computer System

Following are the major features multimedia computer system −

Its Central Processing Unit (CPU) is very fast, as it needs to process large amount of data.

It has huge storage capacity.

It has huge memory power that helps in running heavy data programs.

It has high capacity graphic card that helps in displaying graphics, animation, video, etc.

The sound system makes it easy to listen to audio.

With all these features (discussed above), a computer system is known as high end multimedia computer system.

However, all the features listed above are not essentially required for every multimedia computer system, but rather the features of a multimedia computer system are configured as per the need of respective user.

Multimedia Components

Following are the major components of a multimedia computer system −

Text

It contains alphanumeric and some other special characters. Keyboard is usually used for input of text; however, there are some internal (inbuilt) features to include such text.

Graphics

It is technology to generate, represent, process, manipulate, and display pictures. It is one of the most important components of multimedia application. The development of graphics is supported by different software.

Animation

Computer animation is a modern technology, which helps in creating, developing, sequencing, and displaying a set of images (technically known as 'frames'). Animation gives visual effects or motion very similar to that of a video file.

Audio

This technology records, synthesizes, and plays audio (sound). There are many learning courses and different instructions that can be delivered through this medium appropriately.

Video

This technology records, synthesizes, and displays images (known as frames) in such sequences (at a fixed speed) that makes the creation appear as moving; this is how we see a

completely developed video. In order to watch a video without any interruption, video device must display 25 to 30 frames/second.

Multimedia Application

Let us now see the different fields where multimedia is applied. The fields are described in brief below −

Presentation

With the help of multimedia, presentation can be made effective.

E-books

Today, books are digitized and easily available on the Internet.

Digital Library

The need to be physically present at a library is no more necessary. Libraries can be accessed from the Internet also. Digitization has helped libraries to come to this level of development.

E-learning

Today, most of the institutions (public as well as private both) are using such technology to education people.

Movie making

Most of the special effects that we see in any movie, is only because of multimedia technology.

Video games

Video games are one of the most interesting creations of multimedia technology. Video games fascinate not only the children but adults too.

Animated films

Along with video games, animated film is another great source of entertainment for children.

Multimedia conferencing

People can arrange personal as well as business meetings online with the help of multimedia conferencing technology.

E-shopping

Multimedia technology has created a virtual arena for the e-commerce.

IOT Definitions and Functional Requirements

The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.

What is The Internet of Everything ?

The Internet of things refers to the devices like sensors and actuators, but the term The Internet of Everything used by Cisco is broader and encompasses the devices,data, people and processes.

The devices e.g sensors will send data. This data will then be processed and used by people or by machines to control the devices or other devices.

For example: A temperature sensor sends temperature data to a process which determines that the room temperature is too hot and so sends a signal to turn on the air conditioning.

Internet of Things (IOT) Sectors

The IOT will affect many areas of day to day life. Some of the main sectors are:

- Home
- Health medical
- Fitness and wellness
- factory and industry
- Agriculture
- Cars and roads
- Cities
- IOT Development Phases

The growth of the IOT is expected to go through several stages of development.

- Passive – RFID sensors etc –
- Active- Responds to sensor data
- Aware- can make choices based on data.
- Autonomous -e.g. self driving cars

We are currently in the early stages of development (Passive phase) where we are receiving data from objects and manually taking action.

IOT Components

An IOT system comprises three basic Components.

The things -sensors actuators etc
The Network
The Platforms,Apps and services

1. The Things – Sensors and Devices

In contrast to computers and tablets which are the main devices currently connected to the Internet.

Internet of things devices will mainly be:

Low Power- Power usage and computational Power.
Low cost
Wireless
Examples are Simple sensors – temperature, pressure etc

To turn an everyday object like a house or a car into a smart house or car or a "thing" will require that the object has:

A unique address – IPv6 address
A way to connect to a network – Wireless
sensors e.g temperature,light,speed etc

2. IOT Networks

The Internet of things will utilize the existing networking infrastructure, technologies and protocols currently used in homes/offices and on the Internet, and will introduce many more.

Protocols are designed to operate at a particular level in the networking stack. TCP/IP uses a 4 level model and we will discuss IOT networking using this model.

However because of the requirement for low powered end devices there will be major developments in the Wireless connectivity protocols.

Wi-Fi and Bluetooth are being actively developed for low powered applications and there are new connection technologies like LPWAN, ZigBee, 6LoWpan and Thread. See Beginners guide to IOT Wireless Technologies.

At the networking level IPv6 is set to become the standard, but in the intermediate time frame IPv4 will also be used. See IPV6 Basics and IPv4 addressing basics

At the application level there are a host of new protocols. Some have been available for a long time like ,HTTP and MQTT, whereas others have been developed especially for the IOT e.g. COAP.

See IOT Messaging Protocols guide

3. IOT Platforms,Apps and Services

An IOT platform combines several IOT functions in one.

It can collect and distribute data, convert data between protocols, store and analyse data.

They are available as cloud based and standalone platforms and are available from many companies -large and small.

Examples

Amazon Web services (AWS)
IBM Watson Bluemix
Microsoft Azure
ThingWrox
See this article –20 IOT platforms

IOT and The Cloud

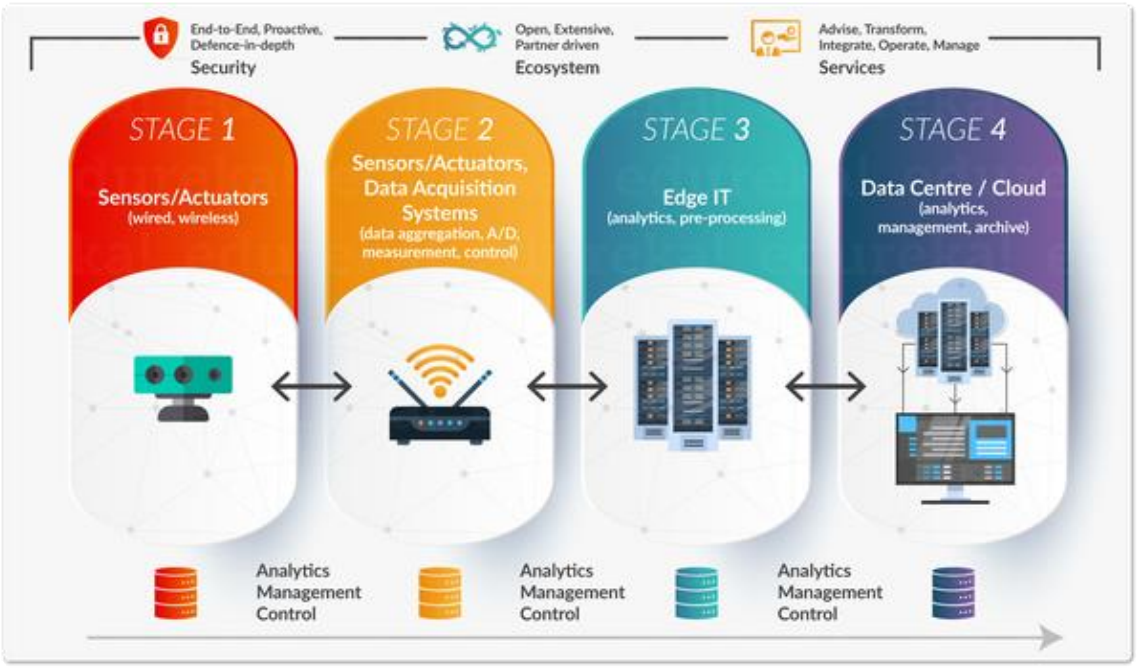
The cloud will have an important role to play in the IOT as it will enable companies to create networks, store data, automate processes without having to build the infrastructure themselves.

This will enable IOT services to be developed much quicker, and at lower cost than using traditional in house systems and services.
Architecture of IoT

IoT Architecture

IoT architecture varies from solution to solution, based on the type of solution which we intend to build. IoT as a technology majorly consists of four main components, over which an architecture is framed.

Sensors
Devices
Gateway
Cloud
The following is the basic 4 Stage Architecture of IoT example:



STAGE 1:

- Sensors: Sensors collect data from the environment or object under measurement and turn it into useful data.

  For example: gyroscope in mobiles
- Actuators: 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 air flow valve, or move a robotic gripper in an assembly process.

- Sensing/Actuating stage covers everything

  Example: Industrial devices to robotic camera systems, water-level detectors, air quality sensors, accelerometers, and heart rate monitors

- Stage 2:

- The 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

Stage 3:

- 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 centre
- 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

Stage 4:

- The data from Stage 3 is forwarded to physical data centre or cloud-based systems, where more powerful IT systems can analyse, 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 in a hybrid cloud system, but the type of processing executed in this stage remains the same, regardless of the platform

Web 3.0 View of IoT

By Vangie Beal The term used to describe the evolution of the Web as an extension of Web 2.0. This definition of Web 3.0 is the popular view held by Tim O'Reilly. In contrast, Nova Spivack defines Web 3.0 as connective intelligence; connecting data, concepts, applications and ultimately people.

Originally thought of as the semantic Web, Web 3.0 is more characteristic of ubiquitous computing (also known as "everyware") in that it marks the era of the arrival of cloud computing, specifically the thin client running against cloud-based data and services.
The internet has become an integrated, seamless, and often invisible part of our everyday lives. Some see this connection as a way to a brighter future, while others have trepidations. The only thing that seems certain is that the Internet is changing rapidly, the laws surrounding the Internet are changing even faster, and it's all we can do to try and keep up.

Changes in style, design, and interactions across the web have big implications for users, but even bigger implications for us as creators. While we often highlight the importance of connecting our design to the big picture goal, it's less often that we consider the much bigger picture: the World Wide Web. Knowing where web technology is now and where it might be going informs the quality of our daily work. How can we create optimal user experiences if we don't at least have a basic knowledge of what the technology is capable of? It's akin to trying to build a house without knowing what houses looked like in the past, or what materials might exist on a future project. So let's explore the web—from the 1990s to today, and onward into the future.

The world of the web

The web was originally a tool used for military, scientific, and academic purposes, but since the early 1990s, it has become a huge part of our everyday lives. As technology has progressed and as more people have begun using the Internet, the web has has gone through (and continues to go through) dominant shifts, specifically Web 2.0, Web 3.0, and the Internet of Things. As the Cretaceous, Jurassic, and Triassic periods delineate the time of the

dinosaurs, so too do the Web 2.0 era, Web 3.0 era, and Internet of Things era identify the shifts in our technologies and how they affect our lives.

Web 3.0

Web 3.0, or the Semantic Web, is the web era we are (arguably) currently in, or perhaps the era we are currently creating. Web 3.0, with its use of semantics and artificial intelligence is meant to be a "smarter web"—one that knows what content you want to see and how you want to see it so that it saves you time and improves your life.

The only problem is that not everyone agrees on whether it exists yet! In his article, What is Web 3.0?, Daniel Nations nicely overviews the various components of what people predict Web 3.0 will be, including a web that is semantic, artificially intelligent, virtual, and ever-present. There is a lot of work being done on all four of these fronts. Content Management Systems (CMSs) and search engines are working hard to make the web more semantic; governments, corporations, and universities are racing to make artificial intelligence and virtual reality a, well, reality; and the ever-present aspect of the web shows in our dependency on smart phones, tablets, and wearables. Let's not forget about the shift in visual design! While there isn't an official Web 3.0 visual design guide, users tend to identify the tenets of Web 2.0 with outdated sites, and designers are opting instead for what has been called "flat design," which champions minimalism and usability.

The Internet of Things

Even as we continue to define what Web 3.0 means, we are simultaneously moving beyond it, and toward the Internet of Things. The Internet of Things (IoT) will likely be the next era, as it takes the notion of an ever-present internet to a new level. Smart devices in the Internet of Things not only use the internet, but speak to each other via machine-to-machine communication (M2M) to accomplish tasks without the need for human input. There are already an abundance of smart devices, as well as automated, internet-connected systems that run without human input, such as automated building climate control. Marco Annunziata gives insight into IoT in his TED talk, Welcome to the age of the industrial internet, where he describes our systems and devices as brilliant, self-aware, predictive, reactive, and social.

Ubiquitous IoT Applications

1. Smart home

Smart Home clearly stands out, ranking as highest Internet of Things application on all measured channels. More than 60,000 people currently search for the term "Smart Home" each month. This is not a surprise. The IoT Analytics company database for Smart Home

includes 256 companies and startups. More companies are active in smart home than any other application in the field of IoT. The total amount of funding for Smart Home startups currently exceeds $2.5bn. This list includes prominent startup names such as Nest or AlertMe as well as a number of multinational corporations like Philips, Haier, or Belkin.

2. Wearables

Wearables remains a hot topic too. As consumers await the release of Apple's new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet. Of all the IoT startups, wearables maker Jawbone is probably the one with the biggest funding to date. It stands at more than half a billion dollars!

3. Smart City

Smart city spans a wide variety of use cases, from traffic management to water distribution, to waste management, urban security and environmental monitoring. Its popularity is fueled by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

4. Smart grids

Smart grids is a special one. A future smart grid promises to use information about the behaviors of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity. 41,000 monthly Google searches highlights the concept's popularity. However, the lack of tweets (Just 100 per month) shows that people don't have much to say about it.

5. Industrial internet

The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearables do. The industrial internet however has a lot going for it. The industrial internet gets the biggest push of people on Twitter (~1,700 tweets per month) compared to other non-consumer-oriented IoT concepts.

6. Connected car

The connected car is coming up slowly. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz around the connected car yet. But it seems we are getting there. Most large auto makers as well as some

brave startups are working on connected car solutions. And if the BMWs and Fords of this world don't present the next generation internet connected car soon, other well-known giants will: Google, Microsoft, and Apple have all announced connected car platforms.

7. Connected Health (Digital health/Telehealth/Telemedicine)

Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential (see our analysis of market segments), not just for companies also for the well-being of people in general. Yet, Connected Health has not reached the masses yet. Prominent use cases and large-scale startup successes are still to be seen. Might 2015 bring the breakthrough?

8. Smart retail

Proximity-based advertising as a subset of smart retail is starting to take off. But the popularity ranking shows that it is still a niche segment. One LinkedIn post per month is nothing compared to 430 for smart home.

9. Smart supply chain

Supply chains have been getting smarter for some years already. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information have been on the market for years. So while it is perfectly logic that the topic will get a new push with the Internet of Things, it seems that so far its popularity remains limited.

10. Smart farming

Smart farming is an often overlooked business-case for the internet of Things because it does not really fit into the well-known categories such as health, mobility, or industrial. However, due to the remoteness of farming operations and the large number of livestock that could be monitored the Internet of Things could revolutionize the way farmers work. But this idea has not yet reached large-scale attention. Nevertheless, one of the Internet of Things applications that should not be underestimated. Smart farming will become the important application field in the predominantly agricultural-product exporting countries.

Four Pillars of IoT

Internet of Things (IoT) is defined as an interconnection of objects embedded with sensing, computing, communication and limited analytical capabilities. The four essential capabilities are the four pillars of Internet of Things technology.

The idea of connecting things is not a new one. In fact, the internet of things (IoT) is a term that has been broadly accepted since the late 1990s. The IoT refers to the network of physical objects accessible through the internet.

Not all of the objects that connect to the IoT will be computing devices, but many will be. So, what is a computing device? While it may be easy to identify a desktop or a laptop computer, the line between what is and is not a computer can become blurred. Is a car a computing device? What about a watch or a television?

The first computing devices (computers) were huge, room-sized machines that took teams of people to build, manage and maintain. Today, they are exponentially faster and only a fraction of the size of their predecessors. For the purposes of this course, a computing device is an electronic machine that performs calculations based on a set of instructions and

comprises three main components: a central processing unit (CPU), memory, and an input/output unit.

Based on the definition above, a digital watch is a computing device, but an analogue watch is not. The digital watch has a CPU to run its program, it has memory to store the program and other information, and it has an I/O device to allow user interaction (screen, display, buttons, sound alerts, etc.). Although the analogue watch has the I/O component, it lacks CPU and memory.

Things:

Currently, the things pillar, highlighted in Figure 2, comprises various types of traditional computers and computing devices, such as desktops, laptops, smartphones, tablets, mainframes, and computer clusters. However, the IoT will include all types of objects, including objects and devices that are not traditionally connected. In fact, Cisco estimates that 99 percent of physical objects will one day be connected.

These objects contain embedded technology to interact with internal servers and the external environment. These objects are network-capable, and can communicate across a secure, reliable and available network platform. However, the IoT refers to a single technology transition; the ability to connect objects that were previously unconnected so those objects can communicate across the network.

The availability of data, when objects can sense and communicate, has the capability of changing how and where decisions are made, who makes the decisions, and the processes that individuals and businesses use to make those decisions. The IoE is built on the connections among people, processes, data, and things. These are the four pillars of the IoE, as shown in the figure. However, the IoE is not about these four dimensions in isolation. Each amplifies the capabilities of the other three. It is in the intersection of all of these elements that the true power of the IoE is realised.

Common devices

The internet connects more computing devices than just desktop and laptop computers. There are devices all around that you may interact with on a daily basis that are also connected to the internet.

For example, people are using mobile devices more every day to communicate and accomplish daily tasks, such as checking the weather or online banking. The table below shows more about mobile devices.

In the future, many of the things in your home could also connect to the internet so that they can be monitored and configured remotely. Table 1 shows more about connected household devices.

There are also many connected devices found in the world outside your home that provide convenience and useful or even vital information. The table below shows more about these commonly found connected devices.

Connecting devices

For the IoE to function, all of the devices that are part of the intended IoE solution must be connected together so that they can communicate. There are two ways to connect devices: wired or wirelessly.

In most cases, connecting devices together using cables is too costly or cumbersome to be practical. For this reason, most devices will need to send and receive data wirelessly.

There are many different types of wireless communication. The most common types of wireless communication are Wi-Fi, Cellular, Bluetooth, and near field communication (NFC). Some devices, such as smartphones and tablets use a combination of wireless communication methods to connect to different devices.

Sensors

Sensors are one way to collect data from non-computers. They convert physical aspects of our environment into electrical signals that can be processed by computers. Some examples are soil moisture sensors, air temperature sensors, radiation sensors, and motion sensors. Sensors of all types will play an important role in connecting what has traditionally been unconnected in the IoE.

Car oxygen sensor

These sensors are very common in cars equipped with electronic fuel injection and are used to monitor the amount of oxygen expelled by the engine after a cycle of fuel burn. Based on that information, the fuel injection computer is able to adjust the air-fuel mixture for optimal engine performance

Data

Data is a key element of all computer systems – from early computing to current systems. A predominant reason for having computer systems, has been to process and transmit data. In this section, you will learn how this is accomplished and what systems are used to convert digital data into human understandable terms.

Data is a value assigned to anything that is around us. Data is everywhere. However, by itself, data can be rather meaningless. As we interpret the data, for example, by correlating or comparing, it becomes more useful. This useful data is now information. As this information is applied or understood it then becomes knowledge.

In electronic communication, data is represented as 1s and 0s. These discrete elements are known as bits (or binary digits). All electronic data is stored in this digital binary format. Whereas humans interpret words and pictures, computers interpret bit patterns.

DNA of IoT

DNA comprised of three building blocks:

D – Digital Transformation

N – Networks

A – Applications

It's an utmost important factor to get the mindset ready with their strategy in adopting Digital Services within the company. We might be talking Digital Economy or Big Data Analytics whatsoever but without a Champion that can break down all the barriers especially in the mindset, that company will be doom within the next 3-4 years when everyone else has increased their productivity multiple folds and create new revenue streams by adopting digital services. Both front-end and back-end systems must be in digital form. Interacting with customers no longer sufficient with a human but must extend the reach using online and mobile services. We have to do away with pen and paper process to be more competitive. Everything MUST be in digital format otherwise your business will be eaten away by your competitor.

Taking control of your assets utilization and understand how your customer use your products are very important. Thus, the assets MUST get connected to allow the companies to monitor their pattern of usage. Find the best connectivity options regardless whether it's inside a building or outside. It can be either a fixed or wireless, short-range or long-range, low-speed or high-speed network – everything depends on the kinds of data that the sensor transmits.

Get ready to transform your new process workflow. It will never be the same again. IoT will break down unnecessary barriers and automate the process flow. You might face some resistance internally when these new processes will obsolete many manual tasks and jobs. However, with the new process, you might need new applications to manage and thus new jobs are created. Thus, you will see many applications are custom built due to the legacy systems that need to be integrated. But it also opens up unlimited possibilities for new applications to be

created for companies who wish to replace their old systems or just wanting to adopt a new business.

IoT is a journey and every journey needs to start with a single step. Along the journey, you might encounter different barriers and probably different options to arrive at the same destination. Choose the path that suits you because every company has its own DNA.

In the long run, the Internet of Things will only be successful if we manage to connect all the different devices in a very uncomplicated manner. Currently, the lack of interoperability is hindering widespread usage. A common language could be a solution and the devices itself have to become more intelligent. A biological organism carries in each cell the complete genotype with individual "working instructions". This could be a paradigm for the Internet of Things.

Today, all the different devices with their individual functions within the Internet of Things communicate via their own, proprietary methods. In fact, there are already many different de facto standards, it's just that these only occur within each individual industry. If you want to connect the different areas and devices with each other, an installation quickly becomes very complex. The expenditure for the necessary hard- and software that consolidates and translates each individual system, creates additional costs in terms of acquisition and maintenance. If just one of the control units fails, the whole system is affected. This can start to present security issues.

Central control unit makes IoT ecosystems vulnerable

The common "connector" to date is via a central point. Sensors collect data and send these to a gateway or cloud server. From there the data is interpreted and actuators controlled accordingly. In the field of building automation, this can often be things like heating controls, light switches, automated gate or shade controls. On their own however, without the central gateway or cloud solution, all of the sensors and actuators are generally helpless. Only thanks to intelligence within that central control unit they are able to fulfill their work and interact with each other.

The Toolkit Approach for End-user Participation in the Internet of Things:

The IoT Toolkit is an open source project to develop a set of tools for building multi-protocol Internet of Things gateways and service gateways that enable horizontal co-operation between multiple different protocols and cloud services. The project consists of the Smart Object API, gateway service, and related tools.

The foundation of the platform is purely bottom up, based on applying best practices and standards in modern web architecture to the problem of interoperability of IoT data models.

The IoT Toolkit is a platform to connect applications and a mixture of devices using various connected protocols. It's real power lies in its broader use, where it can span across all of our connected resources in industry, ranging from commerce, education, transportation, environment, and us. It's a horizontal platform intended to drive Internet of Things more widely as an eventual de facto standard, built for the people who are interested in building out Internet of Things products and services based on broad interoperability.

The Internet of Things interoperability platform stands as an ideal candidate, leveraging the power of the open source community's development process. In turn, community involvement is taken to a new level, across many fields of discipline, and in many directions. Here is where we can get the most benefit of an agile community. Crowdsource the development process based on principles of open communication and free of the need for participants to protect interests toward proprietary intellectual property.

Middleware for IoT: Overview:

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.

Types of Middleware

Message Oriented Middleware.

Object Middleware.

Remote Procedure Call (RPC) Middleware.

Database Middleware.

Transaction Middleware.

Portals.

Embedded Middleware.

Content-Centric Middleware.

Need for middleware

Middleware implies the need for integration, transmission and security. Data from devices will need to be analyzed and then correct actions need to be taken with regards to that data. These actions could generate alerts or invoke corrective processes before routine issues snowball into disaster.

Middleware is needed for integration before data can be analyzed. There should be one tool performing all the actions rather than having different tools from diverse vendors.

Role of middleware

IoT middleware deals with the structure, format and encoding of the information that is being exchanged between different layers, devices and sensors. “It will act as a common standard amongst the diversity of devices, sensors, OS and applications that will make up the IoT ecosystem architecture. Also, it will serve APIs for physical layer communication, without exposing anything to the upper layers,”

Communication middleware for IoT

A communication middleware framework provides an environment that enables two applications to set up a conversation and exchange data. Typically, this exchange of data will involve the triggering of one or more transactions along the way.

In the very early days of distributed computing, the communication between two distributed programs was directly implemented based on the raw physical network protocol. Programmers were involved with acute details of the physical network. They had to create network packets, send and receive them, acknowledge transmissions, and handle errors. Therefore, a lot of effort was spent on these technical issues, and applications were dependent on a specific type of network. Higher-level protocols such as SNA, TCP/IP, and IPX provided APIs that helped reduce the implementation efforts and technology dependencies. They also provided abstraction and a more comfortable application development approach. These protocols enabled programmers to think less in terms of frames at OSI layer 2 or packets at layer 3 and more in terms of communication sessions or data streams. Although this was a significant simplification of the development of distributed applications, it was still a cumbersome and error-prone process. Programming at the protocol layer was still too low-level.

As the next evolutionary step, communication infrastructures encapsulated the technical complexity of such low-level communication mechanisms by insulating the application developer from the details of the technical base of the communication. A communication middleware framework enables you to access a remote application without knowledge of technical details such as operating systems, lower-level information of the network protocol, and the physical network address. A good middleware framework increases the flexibility, interoperability, portability, and maintainability of distributed applications. However, it is the experience of the recent two decades that the developer's awareness of the distribution is still crucial for the efficient implementation of a distributed software architecture. In the remainder of this chapter, we will briefly examine the most important communication middleware frameworks.

RPC

Remote Procedure Calls (RPCs) apply the concept of the local procedure call to distributed applications. A local function or procedure encapsulates a more or less complex piece of code and makes it reusable by enabling application developers to call it from other places in the code. A remote procedure can be called like a normal procedure, with the exception that

the call is routed through the network to another application, where it is executed, and the result is then returned to the caller. The syntax and semantics of a remote call remain the same whether or not the client and server are located on the same system. Most RPC implementations are based on a synchronous, request-reply protocol, which involves blocking the client until the server replies to a request.

The development of the RPC concept was driven by Sun Microsystems in the mid 1980s and is specified as RFC protocols 1050, 1057, and 1831.

Distributed Objects

In the early 1990s, object-oriented programming emerged as a replacement for the traditional modular programming styles based on procedure or function calls. Consequently, the concept of Distributed Objects was invented to make this new programming paradigm available to developers of distributed applications.

Typically, Distributed Objects are supported by an Object Request Broker (ORB), which manages the communication and data exchange with (potentially) remote objects. ORBs are based on the concept of Interoperable Object References, which facilitate the remote creation, location, invocation, and deletion of objects (see Figure 3-5) often involving object factories and other helper objects. By doing so, ORB technology provides an object-oriented distribution platform that promotes object communication across machine, software, and vendor boundaries. ORBs provide location transparency and enable objects to hide their implementation details from clients.

The most common ORB implementations are CORBA, COM/DCOM, and RMI. While RMI is limited to Java and COM/DCOM is restricted to Microsoft platforms, CORBA spans multiple platforms and programming languages.

IoT Information Security:

IoT security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things (**IoT**). To improve **security**, an **IoT** device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted.

The Internet of Things (IoT) – Threats and Countermeasures

- Insecure Web Interface.
- Insufficient Authentication/Authorisation.
- Insecure Network Services.
- Lack of Transport Encryption.
- Privacy Concerns.
- Insecure Cloud Interface.
- Insecure Mobile Interface.
- Insufficient Security Configurability.

IoT security has become the subject of scrutiny after a number of high-profile incidents where a common IoT device was used to infiltrate and attack the larger network. Implementing security measures is critical to ensuring the safety of networks with IoT devices connected to them.

IoT security challenges

A number of challenges prevent the securing of IoT devices and ensuring end-to-end security in an IoT environment. Because the idea of networking appliances and other objects is relatively new, security has not always been considered top priority during a product's design phase. Additionally, because IoT is a nascent market, many product designers and manufacturers are more interested in getting their products to market quickly, rather than taking the necessary steps to build security in from the start.

A major issue cited with IoT security is the use of hardcoded or default passwords, which can lead to security breaches. Even if passwords are changed, they are often not strong enough to prevent infiltration.

Another common issue facing IoT devices is that they are often resource-constrained and do not contain the compute resources necessary to implement strong security. As such, many devices do not or cannot offer advanced security features. For example, sensors that monitor

humidity or temperature cannot handle advanced encryption or other security measures. Plus, as many IoT devices are "set it and forget it" -- placed in the field or on a machine and left until end of life -- they hardly ever receive security updates or patches. From a manufacturer's viewpoint, building security in from the start can be costly, slow down development and cause the device not to function as it should.

Connecting legacy assets not inherently designed for IoT connectivity is another security challenge. Replacing legacy infrastructure with connected technology is cost-prohibitive, so many assets will be retrofitted with smart sensors. However, as legacy assets that likely have not been updated or ever had security against modern threats, the attack surface is expanded.

In terms of updates, many systems only include support for a set timeframe. For legacy and new assets, security can lapse if extra support is not added. And as many IoT devices stay in the network for many years, adding security can be challenging.

IoT security is also plagued by a lack of industry-accepted standards. While many IoT security frameworks exist, there is no single agreed-upon framework. Large companies and industry organizations may have their own specific standards, while certain segments, such as industrial IoT, have proprietary, incompatible standards from industry leaders. The variety of these standards makes it difficult to not only secure systems, but also ensure interoperability between them.

The convergence of IT and operational technology (OT) networks has created a number of challenges for security teams, especially those tasked with protecting systems and ensuring end-to-end security in areas outside their realm of expertise. A learning curve is involved, and IT teams with the proper skill sets should be put in charge of IoT security.

Notable IoT security breaches and IoT hacks

Security experts have long warned of the potential risk of large numbers of unsecured devices connected to the internet since the IoT concept first originated in the late 1990s. A number of attacks subsequently have made headlines, from refrigerators and TVs being used

to send spam to hackers infiltrating baby monitors and talking to children. It is important to note that many of the IoT hacks don't target the devices themselves, but rather use IoT devices as an entry point into the larger network.

In 2010, for example, researchers revealed that the Stuxnet virus was used to physically damage Iranian centrifuges, with attacks starting in 2006 but the primary attack occurring in 2009. Often considered one of the earliest examples of an IoT attack, Stuxnet targets supervisory control and data acquisition (SCADA) systems in industrial control systems (ICS), using malware to infect instructions sent by programmable logic controllers (PLCs).

Karpagam Academy of Higher Education
Dept of CS
Subject: Internet of Things
Class: I M.Sc (CS) **Multiple Choice Questions**
UNIT-1

S.No	Questions	Opt 1	Opt 2	Opt 3	Opt 4	ANSWER
1	TCP/IP Stands for	a)transfer control protocol/intranet protocol	b)transmit control protocol/internet protocol	c)transaction protocol/internet packets	d)transmission control protocol/internet protocol	d)transmission control protocol/internet protocol
2	A set of rules and procedures is commonly referred to	a)TCP	b)IP	c)TCP/IP	d)none of these	d)TCP/IP
3	_____defines how a message is assembled into smaller packets before they are then transmitted	a)TCP	b)IP	c)TCP/IP	d)none of these	a)TCP
4	_____defines how to address and route each packet to make sure it reaches the right destination.	a)TCP	b)IP	c)TCP/IP	d)none of these	b)IP
5	the DARPA created the TCP/IP model in the ____for use in ARPANET.	a)1940	b)1968	c)1970	d)1960	c)1970
6	the TCP/IP model now maintained by the_____	a)intranet engineer task file	b)internet engineering table force	c)Internet Engineering Task Force	d)interactive engineering task force	c)Internet Engineering Task Force
7	TCP/IP uses the	a)master slave model	b)client server model	c)master worker model	d)server client model	b)client server model
8	TCP/IP functionality is divided into _____ layers	a)6	b)5	C)3	d)4	d)4
9	which is transport protocols	a)TCP	b)UDP	C)both a and b	d)only a	C)both a and b
10	which is application layer protocols	a)HTTP	b)FTP	C)SMTP	d)all of these	d)all of these
11	the network layer protocols are	a)IP	b)ICMP	c)both a and b	d)TCP/IP	c)both a and b

12	ICMP stands for	a)Intranet Control Message Protocol	b)Internet Control Medium Protocol	c)Internet Control Message Protocol	d)Interactive Control Messaging Protocol	c)Internet Control Message Protocol
13	HTTPS stands for	a)Hypertext Transfer Protocol Secure	b)Hypertext Transmission Protocol Session	c)Hypertext Transfer Protocol Suite	d)Hypertext Transmission Protocol Secure	a)Hypertext Transfer Protocol Secure
14	DNS stands for	a)Domain Name Service	b)Domain Name System	c)Device Name System	d)Document Name System	b)Domain Name System
15	A _____ is the unit of data that is routed between an origin and a destination on the Internet	a)datagram	b)data	c)packet	d)information	c)packet
16	_____is an application running at the network application layer	a)network service	b) internet service	c)service provider	d)applications	a)network service
17	_____ commonly measured in bits/second is the maximum rate that information can be transferred	a)Bandwidth	b)Jitter	c)Throughput	d)Latency	a)Bandwidth
18	_____ is the actual rate that information is transferred	a)Bandwidth	b)Throughput	c)Jitter	d)Latency	b)Throughput
19	_____ the delay between the sender and the receiver decoding it	a)Bandwidth	b)Latency	c)Throughput	d)Jitter	b)Latency
20	_____ variation in packet delay at the receiver of the information	a)Bandwidth	b)Throughput	c)Latency	d)Jitter	d)Jitter
21	A _____ defines rules and conventions for communication between network devices.	a)protocol	b)router	c)network protocol	d)connection	c)network protocol
22	the _____ to assign networking configuration information to network hosts.	a) Dynamic Host Configuration Protocol	b) Digital Host Configuration Protocol	c) Digital Host Control Protocol	d) Dynamic Hosted Control Protocol	a) Dynamic Host Configuration Protocol

23	A _____ network is created when two or more PCs are connected and share resources without going through a separate server computer	a)machine to machine	b) peer-to-peer	c)client server	d)none of these	b) peer-to-peer
24	You can configure computers in peer-to-peer workgroups to allow _____	a)sharing of devices	b)sharing of networks	c)sharing of files	d)sharing of security	c)sharing of files
25	_____ networks are vulnerable to security attacks.	a)client -server	b)peer-to-peer	c)machine to machine	d)machine to human	b)peer-to-peer
26	_____ networks are highly distributed networks of small, lightweight wireless nodes.	a)Parellel	b)Sensor	c)client server	d)connection less	b)Sensor
27	_____deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity.	a)Electronics	b)Parallel network	c)Digital network	d)Sensor Network	d)Sensor Network
28	_____ is the field of Computer Science that integrates different forms of information	a)Digital Electronics	b)Multimedia	c)Micro processor	d)Operating System	b)Multimedia
29	_____ is very fast, as it needs to process large amount of data.	a)kernel	b)Calculator	c)ALU	d)CPU	d)CPU
30	Computer _____ is a modern technology, which helps in creating, developing, sequencing, and displaying a set of images(frames).	a)graphics	b)animation	c)video	d)audio	b)animation
31	most of the institutions are using this technology to education people.	a)E-Library	b)Digital Library	c)E-Learning	d)Video games	c)E-Learning
32	Multimedia technology has created a virtual arena for the e-commerce	a)E-Learning	b)E-library	c)E-banking	d)E-shopping	d)E-shopping

33	The _____ is the network of physical devices, vehicles, buildings and other items.	a)internet of things	b)sensor	c)cloud computing	d)artificial intelligence	a)internet of things
34	An IOT system comprises _____ basic Components.	a)5	b)8	c)2	d)3	d)3
35	Internet of things devices will mainly be	a)Low cost	b)Wireless	c)Low Power	d)all the above	d)all the above
36	IoT as a technology majorly consists of _____ main components, over which an architecture is framed	a)Five	b)Three	c)Four	d)Seven	c)Four
37	which collect data from the environment or object under measurement and turn it into useful data.	a)Electronics	b)Wireless	c)Sensor	d)Actuator	c)Sensor
38	The definition of_____ is the popular view held by Tim O'Reilly.	a) Web 1.0	b) Web 2.0	c) Web 5.0	d) Web 3.0	d) Web 3.0
39	which of these are four pillers of IOT	a)things,data,sensors and devices	b)devices,information,data and sensor	c)people,process, data and things	d) none of the above	c)people,process,data and things
40	What is DNA of IOT?	a)Digital Networks Applications	b)Deoxyribonucleic Acid	c)Digital Transformation Networks Applications	d)Digitized Neural Analysis	c)Digital Transformation Networks Applications
41	_____connects different, often complex and already existing programs that were not originally designed to be connected.	a)Interface	b)Gateway	c)Middleware	d)Transmitter	c)Middleware

42	_____ is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things (IoT)	a)IoT security	b)IoT control	c)IoT privacy	d)IoT Services	a)IoT security
43	_____ are supported by an Object Request Broker (ORB) which manages the communication and data exchange with remote objects	a)Distributed Objects	b)Static Objects	c)Dynamic Objects	d)Remote Objects	a)Distributed Objects
44	sensors has been made possible by the recent advances in _____ technology	a)mechanical-electrical micro system	b)micro-electronics mechanical syndrome	c)macro-elements mechanical systems	d)micro-electro mechanical systems	d)micro-electro mechanical systems
45	the_____ to assign networking configuration information to network hosts.	a)Domain Name System (DNS)	b)Dynamic Host Configuration Protocol (DHCP)	c) Address Resolution Protocol(ARP)	d)Gopher	b)Dynamic Host Configuration Protocol (DHCP)
46	which are not the application of MultiMedia	a)movie making	b)video games	c)presentation	d)sensors	d)sensors
47	_____ can also intervene to change the physical conditions that generate the data.	a)Interpreter	b)Actuators	c)Sensor	d)Transmitter	b)Actuators
48	The ____ was originally a tool used for military, scientific, and academic purposes, but since the early 1990.	a)IOT	b)MILNET	c)ARPANET	d)Web	c)ARPANET
49	What is web 3.0?	a)Dynamic Web	b)Static Web	c)Semantic Web	d)World Wide Web	c)Semantic Web

UNIT II

SYLLABUS

IoT protocols: Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Issues with IoT Standardization – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – point-to-point protocols - Ethernet protocals - cellular Internet access protocol - Machine-to-machine protocol - Modbus – KNX – Zigbee Architecture – Network layer – APS layer – Security.

Protocol Standardization for IoT

The Internet of Things covers a huge range of industries and use cases that scale from a single constrained device up to massive cross-platform deployments of embedded technologies and cloud systems connecting in real-time.

Tying it all together are numerous legacy and emerging communication protocols that allow devices and servers to talk to each other in new, more interconnected ways.

At the same time, dozens of alliances and coalitions are forming in hopes of unifying the fractured and organic IoT landscape.

The following Channel Guide:

- Provides overview list of popular protocols and standards helping power IoT devices, apps and applications
- Drill down on specific layers or industry specific protocols
- List head-to-head comparisons of popular protocols (ie: mqtt vs xmpp)

Protocols

Rather than trying to fit all of the IoT Protocols on top of existing architecture models like OSI Model, we have broken the protocols into the following layers to provide some level of organization:

1. **Infrastructure** (ex: 6LowPAN, IPv4/IPv6, RPL)
2. **Identification** (ex: EPC, uCode, IPv6, URIs)
3. **Comms / Transport** (ex: Wifi, Bluetooth, LPWAN)
4. **Discovery** (ex: Physical Web, mDNS, DNS-SD)
5. **Data Protocols** (ex: MQTT, CoAP, AMQP, Websocket, Node)

6. **Device Management** (ex: TR-069, OMA-DM)
7. **Semantic** (ex: JSON-LD, Web Thing Model)
8. **Multi-layer Frameworks** (ex: Alljoyn, IoTivity, Weave, Homekit)

Security
Industry Vertical (Connected Home, Industrial, etc)

Infrastructure

IPv6 - "IPv6, is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks.

6LoWPAN - "6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. It is an adaption layer for IPv6 over IEEE802.15.4 links. This protocol operates only in the 2.4 GHz frequency range with 250 kbps transfer rate."

UDP (User Datagram Protocol) - A simple OSI transport layer protocol for client/server network applications based on Internet Protocol (IP). UDP is the main alternative to TCP and one of the oldest network protocols in existence, introduced in 1980. UDP is often used in applications specially tuned for real-time performance.

- QUIC (Quick UDP Internet Connections, pronounced quick) supports a set of multiplexed connections between two endpoints over User Datagram Protocol (UDP), and was designed to provide security protection equivalent to TLS/SSL, along with reduced connection and transport latency, and bandwidth estimation in each direction to avoid congestion.

- Aeron - Efficient reliable UDP unicast, UDP multicast, and IPC message transport.

uIP - The uIP is an open source TCP/IP stack capable of being used with tiny 8- and 16-bit microcontrollers. It was initially developed by Adam Dunkels of the "Networked Embedded Systems" group at the Swedish Institute of Computer Science, licensed under a BSD style license, and further developed by a wide group of developers.

DTLS (Datagram Transport Layer) - "The DTLS protocol provides communications privacy for datagram protocols. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees."

ROLL / RPL (IPv6 routing for low power/lossy networks)

NanoIP
"NanoIP, which stands for the nano Internet Protocol, is a concept that was created to bring Internet-like networking services to embedded and sensor devices, without the overhead of TCP/IP. NanoIP was designed with minimal overheads, wireless networking, and local addressing in mind."

Content-Centric Networking (CCN) - Technical Overview
"Next-gen network architecture to solve challenges in content distribution scalability, mobility, and security.
CCN directly routes and delivers named pieces of content at the packet level of the network, enabling automatic and application-neutral caching in memory wherever it's located in the

network. The result? Efficient and effective delivery of content wherever and whenever it is needed. Since the architecture enables these caching effects as an automatic side effect of packet delivery, memory can be used without building expensive application-level caching services."

Time Synchronized Mesh Protocol (TSMP)
A communications protocol for self-organizing networks of wireless devices called motes. TSMP devices stay synchronized to each other and communicate in timeslots, similar to other TDM (time-division multiplexing) systems.

Discovery

mDNS (multicast Domain Name System) - Resolves host names to IP addresses within small networks that do not include a local name server.

Physical Web - The Physical Web enables you to see a list of URLs being broadcast by objects in the environment around you with a Bluetooth Low Energy (BLE) beacon.

HyperCat - An open, lightweight JSON-based hypermedia catalogue format for exposing collections of URIs.

UPnP (Universal Plug and Play) - Now managed by the Open Connectivity Foundation is a set of networking protocols that permits networked devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Data Protocols

MQTT (Message Queuing Telemetry Transport)
"The MQTT protocol enables a publish/subscribe messaging model in an extremely lightweight way. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium."
-Additional resources

MQTT-SN (MQTT For Sensor Networks) - An open and lightweight publish/subscribe protocol designed specifically for machine-to-machine and mobile applications

-Mosquitto: An Open Source MQTT v3.1 Broker
- IBM MessageSight

CoAP (Constrained Application Protocol)

"CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity. The CoRE group has proposed the following features for CoAP: RESTful protocol design minimizing the complexity of mapping with HTTP, Low header overhead and parsing complexity, URI and content-type support, Support for the discovery of resources provided by known CoAP services. Simple subscription for a resource, and resulting push notifications, Simple caching based on max-age."

-Additional resources

- SMCP — A C-based CoAP stack which is suitable for embedded environments. Features include: Support draft-ietf-core-coap-13, Fully asynchronous I/O, Supports both BSD sockets and UIP.

STOMP - The Simple Text Oriented Messaging Protocol

XMPP (Extensible Messaging and Presence Protocol)
"An open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data."
-Additional resources

- XMPP-IoT
"In the same manor as XMPP silently has created people to people communication interoperable. We are aiming to make communication machine to people and machine to machine interoperable."

Mihini/M3DA
"The Mihini agent is a software component that acts as a mediator between an M2M server and the applications running on an embedded gateway. M3DA is a protocol optimized for the transport of binary M2M data. It is made available in the Mihini project both for means of Device Management, by easing the manipulation and synchronization of a device's data model, and for means of Asset Management, by allowing user applications to exchange typed data/commands back and forth with an M2M server, in a way that optimizes the use of bandwidth"

AMQP (Advanced Message Queuing Protocol)
"An open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security."
- Additional Resources

DDS (Data-Distribution Service for Real-Time Systems)
"The first open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems."

JMS (Java Message Service) - A Java Message Oriented Middleware (MOM) API for sending messages between two or more clients.

LLAP (lightweight local automation protocol)

"LLAP is a simple short message that is sent between inteligent objects using normal text, it's not like TCP/IP, bluetooth, zigbee, 6lowpan, WiFi etc which achieve at a low level "how" to move data around. This means LLAP can run over any communication medium. The three strengths of LLAP are, it'll run on anything now, anything in the future and it's easily understandable by humans."

LWM2M (Lightweight M2M)

"Lightweight M2M (LWM2M) is a system standard in the Open Mobile Alliance. It includes DTLS, CoAP, Block, Observe, SenML and Resource Directory and weaves them into a device-server interface along with an Object structure."

SSI (Simple Sensor Interface)
"a simple communications protocol designed for data transfer between computers or user terminals and smart sensors"

Reactive Streams
"A standard for asynchronous stream processing with non-blocking back pressure on the JVM."

ONS 2.0

REST (Representational state transfer) - RESTful HTTP
-Additional Resources in context of IoT

HTTP/2 - Enables a more efficient use of network resources and a reduced perception of latency by introducing header field compression and allowing multiple concurrent exchanges on the same connection.

SOAP (Simple Object Access Protocol), JSON/XML, WebHooks, Jelastic, MongoDB

Websocket

The WebSocket specification—developed as part of the HTML5 initiative—introduced the WebSocket JavaScript interface, which defines a full-duplex single socket connection over which messages can be sent between client and server. The WebSocket standard simplifies much of the complexity around bi-directional web communication and connection management.

Multi-layer Frameworks

Alljoyn - An open source software framework that makes it easy for devices and apps to discover and communicate with each other.

IoTivity is an open source project hosted by the Linux Foundation, and sponsored by the OIC.

IEEE P2413 - Standard for an Architectural Framework for the Internet of Things (IoT)

Thread - Built on open standards and IPv6 technology with 6LoWPAN as its foundation.

IPSO Application Framework (PDF)
"This design defines sets of REST interfaces that may be used by a smart object to represent its available resources, interact with other smart objects and backend services. This framework is designed to be complementary to existing Web profiles including SEP2 and oBIX."

OMA LightweightM2M v1.0
"The motivation of LightweightM2M is to develop a fast deployable client-server

specification to provide machine to machine service. LightweightM2M is principly a device management protocol, but it should be designed to be able to extend to meet the requirements of applications. LightweightM2M is not restricted to device management, it should be able transfer service / application data."

Weave - A communications platform for IoT devices that enables device setup, phone-to-device-to-cloud communication, and user interaction from mobile devices and the web.

Telehash - JSON+UDP+DHT=Freedom
A secure wire protocol powering a decentralized overlay network for apps and devices

Security

Open Trust Protocol (OTrP) - A protocol to install, update, and delete applications and to manage security configuration in a Trusted Execution Environment (TEE).

X.509 - Standard for public key infrastructure (PKI) to manage digital certificates and public-key encryption. A key part of the Transport Layer Security protocol used to secure web and email communication.

M2M and WSN Protocols:

With critical industries turning increasingly toward automated solutions, data transmission in the Industrial Internet of Things (IIoT) is taking center stage as the most important piece of the puzzle. Sensor technology is helping industries of all types navigate the continuous flow of data to make better decisions and improve operational efficiency, all while increasing productivity.

As wireless sensor networks continue to proliferate, the needs of the real-time enterprise network seamlessly coexisting within the industrial sectors are driving digitalized business models. This creates a wider emphasis on proactive IT departments and next-generation networking technologies.

As the automation of manual processes continues to grow in both popularity and necessity, decision makers have an opportunity to select from a plethora of available communication technologies. Enabling data collection via wireless sensor networks, while important, still depends on the quality, breadth and reliability of the wireless machine-to-machine (M2M) communications solutions implemented by an organization.

Wireless M2M communication

Wireless M2M communication technologies offer a wide variety of potential benefits. This underscores why an increasing number of industries are anticipating deploying M2M in the future to automate extensive sensor networks. The specific benefits gained vary based on the application served, but in general, the overall benefits from these solutions include:

- Optimizing resource utilization
- Better visibility into potential failures and key operational success factors through real-time visibility.

- Reducing costs and environmental impact through monitoring/control across large geographic regions
- Automating safety and security measures reduces critical event response time via specialized sensor networks.
- Centralizing policy management creates greater adherence and more uniform enforcement of regulatory and compliance factors
- Flexibility, Scalability and Mobility of deployment increase agility to adapt to changing market demands
- Improving product quality

For industries that require many geographically dispersed assets and an increasingly mobile workforce, M2M networking technology ultimately is the glue connecting everything and, therefore the backbone of the Industrial Internet of Things (IIoT) ecosystem – and the connected sensor networks within the IIoT.

When we talk about the IIoT ecosystem, most people think of data and devices, and how the two are inextricably linked together, essentially, the concept behind M2M. This ecosystem, however, does not, and cannot, exist without highly reliable and secure wireless communications technology.

In today's fast paced, get-it-done-yesterday environment, we don't have time to hardwire, or worry about interfaces, and protocols. Connecting the unconnected to automate processes, sensor networks, and access data plus control is what it's all about. This cannot be done with wires, unless our oil and gas producers, public utilities, municipalities and energy companies are willing to invest heavily in the time and resources to develop an expansive and retrenched network infrastructure across long distances one wire at a time (see fig. 1). Time-to-market and time-to-evenue drive business decisions and technology choices.

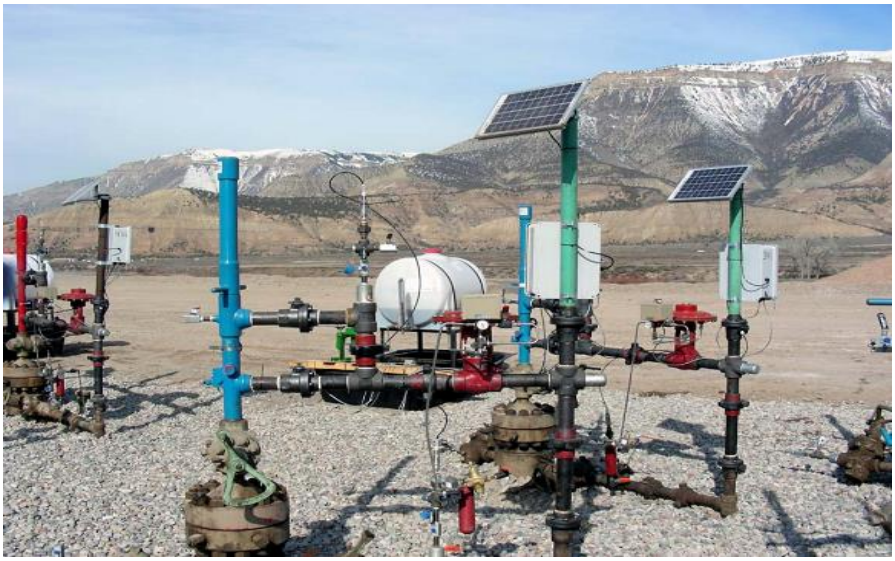


Fig. 1: Sensor networks in remote locations, such as an oil and gas setting, are enabled by M2M wireless communications.

Enabling wireless sensor networks with M2M applications within our nation's critical infrastructure is a top objective today, but how can operators and IT departments leverage the best possible solution(s) for their assets and facilities? Before decision-makers purchase any wireless M2M communication technologies available today, it is imperative to review two important success factors that need to be addressed with these solutions: security and reliability.

Proprietary wireless communication technologies and devices, particularly when they offer many knobs and configuration options to create private, user-defined networks, actually offer a higher degree of security. But even those technologies are subject to security and reliability threats. Therefore, network access control is one of the most important security features for M2M communication and sensor networking technology for preventing unauthorized access and intrusion.

A proven communication network security strategy should go even further and protect data that's in-transit as well. Even if an unauthorized device manages to gain access to the M2M communication network, it isn't necessarily gaining access to the actual data without passing yet another layer of security. Also, a communication network security strategy needs to address and implement policies that serve as safeguards, which make it difficult to circumvent security measures and limit the potential impact of a security breach.

Finally, in order to complete the M2M security approach to wireless sensor networks, it takes vigilance. Vigilance is the action or state of keeping careful watch for possible danger or difficulties. Today's M2M networks are not heuristic, self-healing, adaptive, self-optimizing automatons. They require an educated observer who is looking for anomalies, aberrations, outliers, exceptions, and flat-out failures. Cutting-edge M2M requires standards-based protocols for determining the health of the network, integrity of the links, and performance of the overlying applications.

SCADA and RFID Protocols

SCADA

SCADA is an acronym for supervisory control and data acquisition, a computer system for gathering and analyzing real time data. **SCADA** systems are **used to** monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

Supervisory control and data acquisition (**SCADA**) is a system of **software** and hardware elements that allows industrial organizations to: ... Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) **software**.

A supervisory system gathers data on the process and sends the commands control to the process. The **SCADA** is a remote terminal unit which is also known as RTU. Most control actions are automatically performed by RTUs or PLCs. ... The **SCADA** system controls can **run** completely all kinds of industrial process.

How SCADA Systems Work

A SCADA system gathers information, such as where a leak on a pipeline has occurred, transfers the information back to a central site, alerting the home station that the leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion. SCADA systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or incredibly complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system.

SCADA systems were first used in the 1960s.

Supervisory control and data acquisition (**SCADA**) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-levelprocess supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery. The operator interfaces that enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA computer system. However, the real-time control logic or controller calculations are performed by networked modules that connect to the field sensors and actuators.

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers allowing access through standard automation protocols. In practice, large SCADA systems have grown to become very similar todistributed control systems in function, but using multiple means of interfacing with the plant. They can control large-scale processes that can include multiple sites, and work over large distances as well as small distance.[1] It is one of the most commonly-used types of industrial control systems, however there are concerns about SCADA systems being vulnerable to cyberwarfare/cyberterrorism attacks.

The SCADA concept in control operations

The key attribute of a SCADA system is its ability to perform a supervisory operation over a variety of other proprietary devices.

The accompanying diagram is a general model which shows functional manufacturing levels using computerised control.

Referring to the diagram,

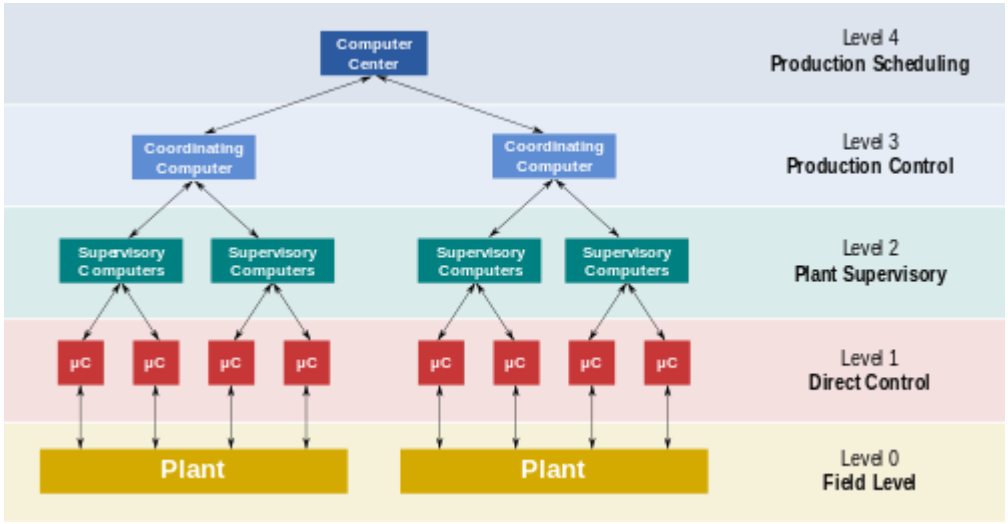
- Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
- Level 1 contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors.
- Level 2 contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.

- Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
- Level 4 is the production scheduling level.

Level 1 contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

Level 2 contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow. The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

Levels 3 and 4 are not strictly process control in the traditional sense, but are where production control and scheduling takes place.



Examples of use

Both large and small systems can be built using the SCADA concept. These systems can range from just tens to thousands of control loops, depending on the application. Example processes include industrial, infrastructure, and facility-based processes, as described below:

- Industrial processes include manufacturing, Process control, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electric power transmission anddistribution, and wind farms.

- Facility processes, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption.

RFID Protocols

Radio-frequency identification (**RFID**) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically-stored information. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Unlike a barcode, the tag need not be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows for positive identification of animals.

Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns.[2] These concerns resulted in standard specifications development addressing privacy and security issues. ISO/IEC 18000 and ISO/IEC 29167 use on-chip cryptography methods for untraceability, tag and reader authentication, and over-the-air privacy. ISO/IEC 20248 specifies a digital signature data structure for RFID and barcodes providing data, source and read method authenticity. This work is done within ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques. Tags can also be used in shops to expedite checkout, and to prevent theft by customers and employees.

Design

A radio-frequency identification system uses *tags*, or *labels* attached to the objects to be identified. Two-way radio transmitter-receivers called *interrogators* or *readers* send a signal to the tag and read its response.

RFID tags can be either passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.

Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.

RFID tags contain at least three parts: an integrated circuit that stores and processes information and that modulates and demodulatesradio-frequency (RF) signals; a means of collecting DC power from the incident reader signal; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

An RFID reader transmits an encoded radio signal to interrogate the tag. The RFID tag receives the message and then responds with its identification and other information. This may be only a unique tag serial number, or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Since tags have individual serial numbers, the RFID system design can discriminate among several tags that might be within the range of the RFID reader and read them simultaneously.

Uses

The RFID tag can be affixed to an object and used to track and manage inventory, assets, people, etc. For example, it can be affixed to cars, computer equipment, books, mobile phones, etc.

RFID offers advantages over manual systems or use of bar codes. The tag can be read if passed near a reader, even if it is covered by the object or not visible. The tag can be read inside a case, carton, box or other container, and unlike barcodes, RFID tags can be read hundreds at a time. Bar codes can only be read one at a time using current devices.

- Access management
- Tracking of goods
- Tracking of persons and animals[23]
- Toll collection and contactless payment
- Machine readable travel documents
- Smartdust (for massively distributed sensor networks)
- Airport baggage tracking logistics[24]
- Timing sporting events
- Tracking and billing processes

Issues with IoT Standardization

The rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions. Additionally, large amounts of funding are being deployed at IoT startups. Consequently, the focus of the industry has been on manufacturing and producing the right types of hardware to enable those solutions. In current model, most IoT solution providers have been building all components of the stack, from the hardware devices to the relevant cloud services or as they would like to name it as "IoT solutions", as a result, there is a lack of consistency and standards across the cloud services used by the different IoT solutions.

As the industry evolves, the need for a standard model to perform common IoT backend tasks, such as processing, storage, and firmware updates, is becoming more relevant. In that new model, we are likely to see different IoT solutions work with common backend services, which will guarantee levels of interoperability, portability and manageability that are almost impossible to achieve with the current generation of IoT solutions.

Creating that model will never be an easy task by any level of imagination, there are hurdles and challenges facing the standardization and implementation of IoT solutions and that model needs to overcome all of them.

IoT standardization

The hurdles facing IoT standardization can be divided into **4** categories; Platform, Connectivity, Business Model and Killer Applications:

- **Platform:** This part includes the form and design of the products (UI/UX-User Interface/User Experience), analytics tools used to deal with the massive data streaming from all products in a secure way, and scalability which means wide adoption of protocols like IPv6 in all vertical and horizontal markets is needed.
- **Connectivity:** This phase includes all parts of the consumer's day and night routine, from using wearables, smart cars, smart homes, and in the big scheme, smart cities. From the business prospective we have connectivity using IIoT (Industrial Internet of Things) where M2M communications dominating the field.
- **Business Model:** The bottom line is a big motivation for starting, investing in, and operating any business, without a sound and solid business models for IoT we will have another bubble, this model must satisfy all the requirements for all kinds of e-commerce; vertical markets, horizontal markets and consumer markets. But this category is always a victim of regulatory and legal scrutiny.
- **Killer Applications**: In this category there are three functions needed to have killer applications: control "things", collect "data", and analyze "data". IoT needs killer applications to drive the business model using a unified platform.

All four categories are inter-related, you need all them to make all them work. Missing one will break that model and stall the standardization process. A lot of work needed in this

process, and many companies are involved in each of one of the categories, bringing them to the table to agree on a unifying model will be daunting task.

IoT implementation
The second part of the model is IoT implementations; implementing IoT is not an easy process by any measure for many reasons including the complex nature of the different components of the ecosystem of IoT. To understand the gravity of this process, we will explore all the **five** components of IoT Implementation: Sensors, Networks, Standards, Intelligent Analysis, and Intelligent Actions.

Sensors
There two types of sensors: active sensors & passive sensors. *The driving forces for using sensors in IoT* today are new trends in technology that made sensors **cheaper, smarter** and **smaller**. But the c*hallenges facing IoT sensors are:* power consumption, security, and interoperability.

Networks
The second component of IoT implantation is to transmit the signals collected by sensors over networks with all the different components of a typical network including routers, bridges in different topologies. Connecting the different parts of networks to the sensors can be done by different technologies including Wi-Fi, Bluetooth, Low Power Wi-Fi , Wi-Max, regular Ethernet , Long Term Evolution (LTE) and the recent promising technology of Li-Fi (using light as a medium of communication between the different parts of a typical network including sensors).

*The driving forces for wide spread network adoption in IoT are h*igh data rate, low prices of data usage, virtualization (X - Defined Network trends), XaaS concept (SaaS, PaaS, and IaaS), and IPv6 deployment. But the c*hallenges facing network implementation in IoT are t*he enormous growth in number of connected devices, availability of networks coverage, security, and power consumption.

Anything as a service (**XaaS**) is a term that describes a broad category of services related to cloud computing and remote access. With cloud computing technologies, vendors offer companies different kinds of services over the web or similar networks.

Software as a Service (SaaS)- represent the largest cloud market and are still growing quickly. SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a web browser without any downloads or installations required, although some require plugins.

Cloud platform services, or Platform as a Service (PaaS), are used for applications, and other development, while providing cloud components to software. What developers gain with PaaS is a framework they can build upon to develop or customize applications. PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective.

Infrastructure as a Service (IaaS), are self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute (virtualized or bare metal),

storage, networking, and networking services (e.g. firewalls).

Standards

The third stage in the implementation process includes the sum of all activities of handling, processing and storing the data collected from the sensors. This aggregation increases the value of data by increasing, *the scale, scope, and frequency* of data available for analysis but aggregation only achieved through the use of various standards depending on the IoT application in used.

There are two types of standards relevant for the aggregation process; *technology standards*(including network protocols, communication protocols, and data-aggregation standards) and *regulatory standards* (related to security and privacy of data, among other issues). *Challenges facing the adoptions of standards within IoT are:* **standard for handling unstructured data, security and privacy issues** in addition to **regulatory standards for data markets**.

Intelligent Analysis

The fourth stage in IoT implementation is extracting insight from data for analysis. IoT analysis is driven by *cognitive technologies (natural language processing, data mining and pattern recognition)* and the accompanying models that facilitate the use of cognitive technologies. With advances in cognitive technologies' the ability to process varied forms of information, vision and voice have also become usable, and open the doors for in-depth understanding of the none-stop streams of real-time data. *Factors driving adoption intelligent analytics within the IoT;* **artificial intelligence models, growth in crowdsourcing and open- source analytics software, real-time data processing and analysis**. *Challenges facing the adoption of analytics within IoT* **; Inaccurate analysis due to flaws in the data and/or model, legacy systems' ability to analyze** *unstructured data, and l***egacy systems' ability to manage real- time data**

Intelligent Actions

Intelligent actions can be expressed as #M2M (Machine to Machine) and M2H (Machine to Human) interfaces for example with all the advancement in UI and UX technologies. *Factors driving adoption of intelligent actions within the IoT;*lower machine prices, improved machine functionality, machines "influencing" human actions through behavioral-science rationale, and deep Learning tools. *Challenges facing the adoption of intelligent actions within IoT* **: m**achines' actions in unpredictable situations, information security and privacy, machine interoperability, mean-reverting human behaviors, and slow adoption of new technologies

Unified Data Standards

The emerging concepts of the Internet of Things (IoT) and Software-Defined Architecture promise breakthroughs in achieving interoperability, portability, and configurability of connected machines, systems, and applications.

A unifying interoperability standard is critical to minimize the cost and time to manufacture and implement these machines within automation systems, and to accelerate global adoption.

This standard needs to be simple, universally adopted, and sustainable, just as the Simple Mail Transport Protocol (SMTP) has been universally adopted for sending email for over three decades.

Creating, sending, and receiving email messages involves human-to-machine-to-machine communications within a client/server network (Figure 1).

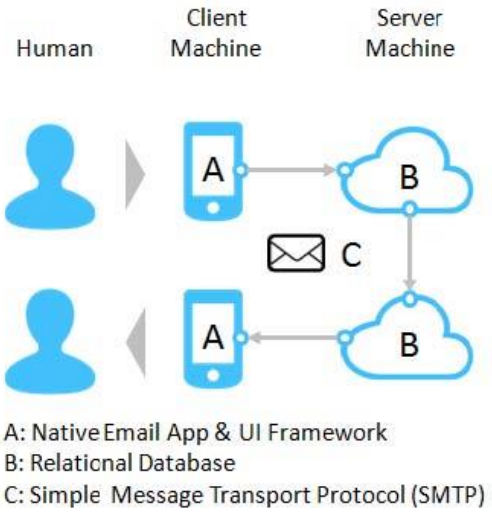


Figure 1 – Human-to-Machine-to-Machine Communications

A person interacts with a purpose-built, natively-installed email app (e.g. Outlook) on a mobile device (the client machine) to create, read, update, and delete (CRUD) email messages and contact records that are typically maintained within a relational database and synchronized between the client and a server machine.

The app is compatible with the client machine's operating system framework (e.g. Windows), which renders the user interface (UI) supporting these CRUD operations. Email apps and UI frameworks are typically developed using human-readable programming languages that generate human-readable commands to update a relational database with human-readable table and field names.

When an email message is sent, its status is updated by the email app, and it is transported via a communication protocol (SMTP) that is understandable from machine-to-machine. Email messages are sent and received via purpose-built data services (or APIs) linking machine to framework to app.

information fragmentation is a pervasive problem in personal information management (PIM). This information is fragmented by the very tools that have been designed to help us manage it.[6] Applications often store their data in their own particular locations and representations (i.e. data protocols) that are inaccessible to other applications (Figure 2). Consumers must launch multiple applications and perform numerous repetitive searches for relevant information, to say nothing of deciding which applications to look in.

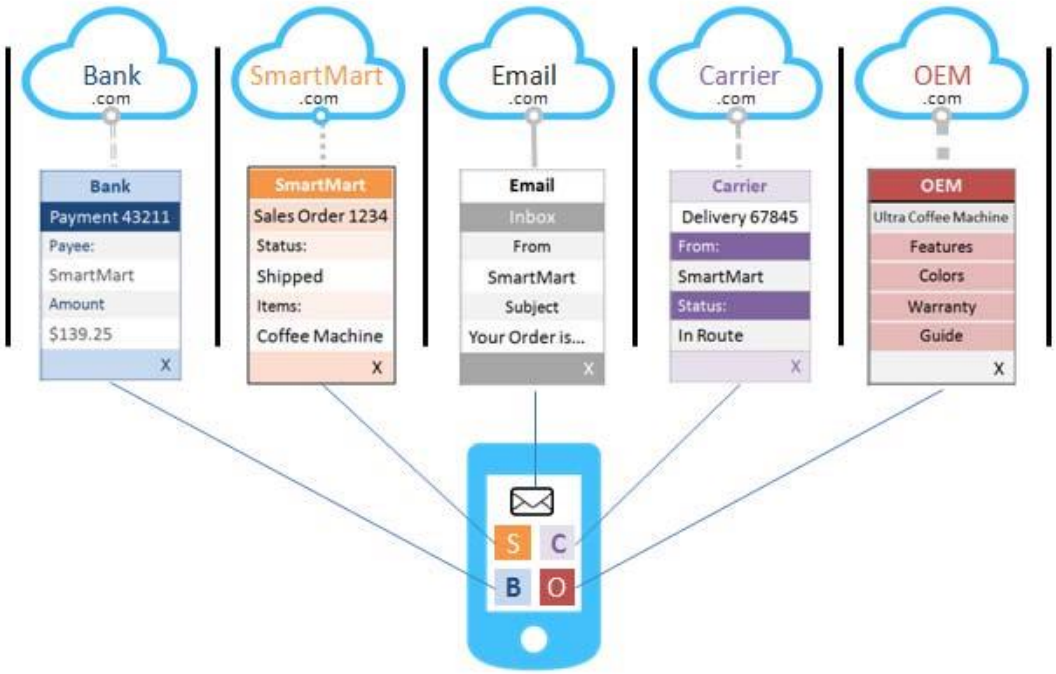


Figure 3 – Example of Related Information Object Silos with varying Data Protocols

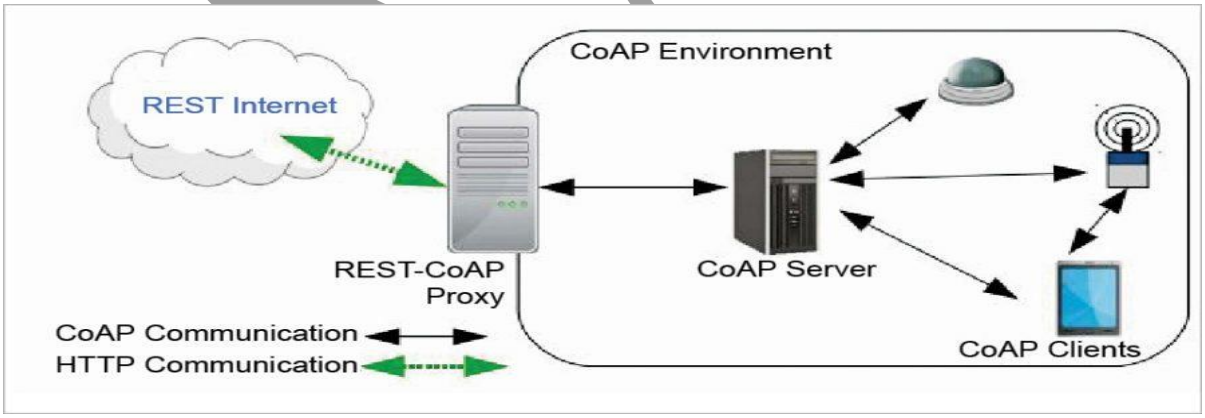
Data unification and application interoperability can offer many benefits to consumers needing context-based access to their information and to work simultaneously with several information objects in order to complete a given task.

IoT protocols

IEEE (Institute of Electrical and Electronics Engineers) and ETSI (European Telecommunications Standards Institute) have defined some of the most important IoT protocols, as listed below;

This was created by the IETF Constrained RESTful Environments (CoRE) working group. CoAP is an Internet application protocol for constrained devices. It is designed to be used between devices on the same constrained network, between devices and general nodes on the Internet, and between devices on different constrained networks—both joined on the Internet. This protocol is especially designed for IoT systems based on HTTP protocols.

CoAP makes use of the UDP protocol for lightweight implementation. It also makes use of RESTful architecture, which is very similar to the HTTP protocol. It is used within mobiles and social network based applications and eliminates ambiguity by using the HTTP *get*, *post*, *put* and *delete* methods. Apart from communicating IoT data, CoAP has been developed along with DTLS for the secure exchange of messages. It uses DTLS for the secure transfer of data in the transport layer.



MQTT Protocol

MQTT (Message Queue Telemetry Transport), a messaging protocol, was developed by Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999. It is mostly used for remote monitoring in I oT. Its primary task is to acquire data from many devices and transport it to the IT infrastructure. MQTT connects devices and networks with applications and middleware. A hub-and-spoke architecture is natural for MQTT. All the devices connect to data concentrator servers like IBM's new MessageSight appliance. MQTT protocols work on top of TCP to provide simple and reliable streams of data.

MQTT Protocol consists of three main components: subscriber, publisher and broker. The publisher generates the data and transmits the information to subscribers through the broker. The broker ensures security by cross-checking the authorisation of publishers and subscribers.

MQTT Protocol is the preferred option for IoT based devices, and is able to provide efficient information-routing functions to small, cheap, low-memory and power-consuming devices in vulnerable and low bandwidth based networks.

Extensible Messaging and Presence Protocol (XMPP)

This is a communication IoT protocol for message-oriented middleware based on the XML language. It enables the real-time exchange of structured yet extensible data between any two or more network entities. The protocol was developed by the Jabber open source community in 1999, basically for real-time messaging, presence information, and the maintenance of contact lists.

XMPP enables messaging applications to attain authentication, access control, hop-by-hop and end-to-end encryption. Being a secure protocol, it sits on top of core IoT protocols and connects the client to the server via a stream of XML stanzas. The XML stanza has three main components: message, presence and IQ.

Advanced Message Queuing Protocol (AMQP)

This was developed by John O'Hara at JPMorgan Chase in London. AMQP is an application layer protocol for message-oriented middleware environments. It supports reliable communication via message delivery assurance primitives like at-most once, atleast once and exactly once delivery.

The AMQP protocol consists of a set of components that route and store messages within a broker service, with a set of rules for wiring the components together. The AMQP protocol enables client applications to talk to the broker and interact with the AMQP model. This model has the following three components, which are connected into processing chains in the server to create the desired functionality.

- **Exchange:** Receives messages from publisher based applications and routes them to 'message queues'.
- **Message queue:** Stores messages until they can be safely processed by the consuming client application.
- **Binding:** States the relationship between the message queue and the exchange.

- ## Data Distribution Service (DDS)

- This IoT protocol for real-time machine-to-machine communication was developed by the Object Management Group (OMG). It enables scalable, real-time, dependable, high-performance and interoperable data exchange via the publish-subscribe methodology. As compared to MQTT and CoAP IoT

protocols, DDS makes use of brokerless architecture and of multicasting to bring high quality QoS to applications.

- DDS can be deployed in platforms ranging from low-footprint devices to the cloud, and supports efficient bandwidth usage as well as the agile orchestration of system components.

- The DDS protocol has two main layers: Data Centric Publish-Subscribe (DCPS) and Data-Local Reconstruction Layer (DLRL). DCPS performs the task of delivering the information to subscribers, and the DLRL layer provides an interface to DCPS functionalities, enabling the sharing of distributed data among IoT enabled objects.

- Simple Text Oriented Messaging Protocol (STOMP)

- This text based protocol was developed to work with message-oriented middleware. It provides an interoperable wire format that enables STOMP clients to communicate with any STOMP message broker to enable easy and widespread messaging interoperability among many languages, platforms and brokers. Like AMQP, STOMP provides the message header with properties and a frame body.

- STOMP does not, however, deal in queues and topics—it uses a SEND semantic with a 'destination' string. The broker must map it onto something that it understands internally, such as a topic, queue, or exchange. Consumers then SUBSCRIBE to those destinations. Since those destinations are not mandated in the specifications, different brokers may support different flavours

of the destination. So, it's not always straightforward to port code between brokers.

- However, STOMP is simple and lightweight (although somewhat verbose on the wire), with a wide range of language bindings. It also provides some transactional semantics. One of the most interesting examples is with RabbitMQ Web Stomp, which allows you to expose messaging in a browser through Web-sockets.

• Very Simple Control Protocol (VSCP)

- This is more a framework than a protocol. VSCP is highly scalable, has a low footprint and is a free-cum-open source solution for device discovery and identification, device configuration, autonomous device functionality and secure firmware updates. VSCP makes things interact at the application layer. It makes use of CAN, RS-232, Ethernet, TCP/IP, MQTT and 6LowPan.

- VSCP uses an event format and supports global unique identifiers for nodes, thus making a node identifiable no matter where it is installed in the world. Besides, it includes a register model in order to provide a flexible common interface for node configuration and a model for controlling the functionality of each node. VSCP does not make any assumptions regarding the lower level system used to realise the physical interconnection with the node; therefore, it works with different transport mechanisms such as Ethernet, TCP/IP, wireless, Zigbee, Bluetooth, CAN, GPRS, RS-232 and USB.

IEEE 802.15.4

IEEE 802.15.4 is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). It specifies the physical layer and media access control for LR-WPANs, and is maintained by the IEEE 802.15 working group, which defined the standard in 2003.

It is the basis for the Zigbee, ISA100.11a, WirelessHART, MiWi, 6LoWPAN, Thread and SNAP specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4. In particular, 6LoWPAN defines a binding for the IPv6 version of the Internet Protocol (IP) over WPANs, and is itself used by upper layers like Thread.

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

The physical layer.

The physical layer is the initial layer in the OSI reference model used worldwide. The physical layer (PHY) ultimately provides the data transmission service, as well as the interface to the physical layer management entity, which offers access to every layer management function and maintains a database of information on related personal area networks.

The MAC layer

The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

BACNet Protocol

BACnet is "a data communication protocol for building automation and control networks." A data communication protocol is a set of rules governing the exchange of data over a computer network that covers everything from what kind of cable to use to how to form a particular request or command in a standard way. What makes BACnet special is that the rules relate specifically to the needs of building automation and control (BAC) equipment, i.e., they cover things like how to ask for the value of a temperature, define a fan operating schedule, or send a pump status alarm.

BACnet testing

BACnet Testing Laboratories ("BTL") was established by BACnet International to test products as per BACnet standard and support compliance testing and interoperability testing activities and consists of BTL Manager and the BTL working group ("BTL-WG"). The general activities of the BTL are:

Publish the BTL Implementation Guidelines document
Certifying the products as per BACnet testing and BTL guidelines
Support the activities of the BTL-WG
Maintain the BTL test packages
Approves Testing Laboratories for BTL Testing

History

The development of the BACnet protocol began in June, 1987, in Nashville, Tennessee, at the inaugural meeting of the ASHRAE BACnet committee, known at that time as SPC 135P, "EMCS Message Protocol". The committee worked at reaching consensus using working groups to divide up the task of creating a standard. The working groups focused on specific areas and provided information and recommendations to the main committee. The first three working groups were the Data Type and Attribute Working Group, Primitive Data Format Working Group, and the Application Services Working Group.

BACnet objects

ANSI/ASHRAE 135-2016 specifies 60 standard object types:

Some of them are:

Access Credential
Access Door
Access Point
Access Rights
Access User
Access Zone
Accumulator
Alert Enrollment
Analog Input
Analog Output
Analog Value

Point-to-Point protocols

Point-to-point protocol (PPP) is a computer network protocol used to transfer a datagram between two directly connected (point-to-point) computers. This protocol is used for a very basic level of connectivity providing data linkage between the computers.

Point-to-point protocol is widely used for the heavier and faster connections necessary for broadband communications. Point-to-point protocol is also known as RFC 1661.

There are many physical mediums for point-to-point connectivity, such as simple serial cables, mobile phones and telephone lines.

For Ethernet networks, TCP and IP were introduced for data communication purposes. Both of these protocols have specifications for Ethernet networks only. Thus, TCP and IP do not support point-to-point connections. Therefore, PPP was introduced for point-to-point connectivity without Ethernet.

When two computers are being connected directly, both ends send a request for configuration. Once the computers are connected, PPP handles link control, data control and protocol encapsulation.

In terms of the OSI model, PPP provides Layer 2, or data-link, service. PPP is a full-duplex protocol that can be used on a variety of physical media, includingtwisted pair copper wire, fiber optic lines or satellite links. PPP can provide services over everything, from a dial-up modem connection to a Secure Sockets Layer (SSL) encrypted virtual private network (VPN) connection. PPP uses a variation of High-level Data Link Control (HDLC) for packet encapsulation.

For example, a high-security application on a company network connects to the network via the VPN and establishes an SSL link. The client for the application can then establish a PPP tunnel on top of that, which will carry IP packets to the application's server.

Point-to-Point Protocols are sometimes considered a member of the TCP/IP suite of protocols. Variations of PPP exist for running over Ethernet using the PPPoE specification and for asynchronous transfer mode (ATM) using the PPPoA specification.

PPP is sometimes hidden from view -- for example, it has been used to connect Digital Subscriber Line (DSL) and cable modems to their back-end services. Its visible use has been declining steadily over time, along with dial-up modem services.

Ethernet Protocols

Ethernet Industrial Protocol (Ethernet/IP) is a communication standard in networks used for transferring large amounts of data with a speed ranging from 10 Mbps to 100 Mbps and at a rate of 1500 bytes per data packet. The network specification makes use of an open protocol at the application layer. Open DeviceNet Vendor Association and the Industrial Ethernet Association support the specification. Ethernet Industrial Protocol is one of the most proven, developed and complete industrial solutions for manufacturing automation and also helps users to benefit from the advantages of both Internet and open technologies.

Ethernet Industrial Protocol provides a range of functionalities by layering the Common Industrial Protocol over the protocols such as User Datagram Protocol and Transmission Control Protocol/Internet Protocol. With such a combination of accepted standards, Ethernet Industrial Protocol ensures it can support control applications and information data exchange. In order to provide a cost-effective plant floor solution by means of understood and accepted infrastructure, Ethernet standard protocol makes use of physical media and commercial, off-the-shelf Ethernet components as well.

One of the biggest advantages of Ethernet Industrial Protocol is that it is easy to configure, operate, maintain and scale up. Again, it is compatible with many Ethernet switches. The protocol is one of the preferred protocols for network connectivity in enterprise systems. It also remains one of the best options when multi-device connectivity is required, and it serves as an economical solution for connecting multiple computers.

The protocol is used in a wide range of appliances such as robots, personal computers, programmable logic controllers, mainframes, input/output adapters and other similar devices.

Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol

As a data-link layer protocol in the TCP/IP stack, Ethernet describes how network devices can format and transmit data packets so other devices on the same local or campus area network segment can recognize, receive and process them. An Ethernet cable is the physical, encased wiring over which the data travels.

Any device accessing a geographically localized network using a cable -- i.e., with a wired rather than wireless connection -- likely uses Ethernet -- whether in a home, school or office setting. From businesses to gamers, diverse end users depend on the benefits of Ethernet connectivity, including reliability and security.

Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions -- whether from radio wave interference, physical barriers or bandwidth hogs. It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling -- making it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

Cellular Internet access protocol

In computing, the **Internet** Message **Access Protocol** (IMAP) is an **Internet** standard**protocol** used by email clients to retrieve email messages from a mail server over a TCP/IP **connection**. IMAP is defined by RFC 3501.

Internet Message Access Protocol (IMAP) is a standard protocol for accessing email on a remote server from a local client. IMAP is an application layer Internet Protocol using the underlying transport layer protocols to establish host-to-host communication services for

applications. This allows the use of a remote mail server. The well-known port address for IMAP is 143.

The IMAP architecture enables users to send and receive emails through a remote server, without support from a particular device. This type of email access is ideal for travelers receiving or answering emails from their home desktop or office computer.

This term is also known as interactive mail access protocol, Internet mail access protocol, and interim mail access protocol

IMAP was originally designed as a remote mailbox protocol in 1986 by Mark Crispin. This was during the popular use of Post Office Protocol (POP). IMAP and POP are still both supported by the majority of modern email servers and clients. However, IMAP is a remote file server, while POP istores and forwards. In other words, with IMAP, all emails remain on the server until the client deletes them. IMAP also permits multiple clients to access and control the same mailbox.

When a user requests an email, it is routed through a central server. This keeps a storage document for the email files. Some of IMAP benefits include the ability to delete messages, search for keywords in the body of emails, create and manage multiple mailboxes or folders, and view the headings for easy visual scans of emails.

IMAP is still used extensively, but is less important now that so much email is sent via web-based interfaces such as gMail, Hotmail, Yahoo Mail, etc.

Machine-to-Machine protocol

M2M technology was first adopted in manufacturing and industrial settings, and later found applications in healthcare, business, insurance and more. It is also the foundation for the internet of things (IoT).

History of machine-to-machine technology

The roots of M2M are planted firmly in the manufacturing industry, where other technologies, such as SCADA and remote monitoring, helped remotely manage and control data from equipment.

In 2003, *M2M Magazine* launched. The publication has since defined the six pillars of M2M as remote monitoring, RFID, sensor networking, smart services, telematics and telemetry.

How M2M works

The main purpose of machine-to-machine technology is to tap into sensor data and transmit it to a network. Unlike SCADA or other remote monitoring tools, M2M systems often use public networks and access methods -- for example, cellular or Ethernet -- to make it more cost-effective.

The main components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link, and autonomic computing software programmed to help a network device interpret data and make decisions. These M2M applications translate the data, which can trigger preprogrammed, automated actions.

One of the most well-known types of machine-to-machine communication is telemetry, which has been used since the early part of the last century to transmit operational data. Pioneers in telemetrics first used telephone lines, and later, radio waves, to transmit performance measurements gathered from monitoring instruments in remote locations.

The internet and improved standards for wireless technology have expanded the role of telemetry from pure science, engineering and manufacturing to everyday use in products such as heating units, electric meters and internet-connected devices, such as appliances.

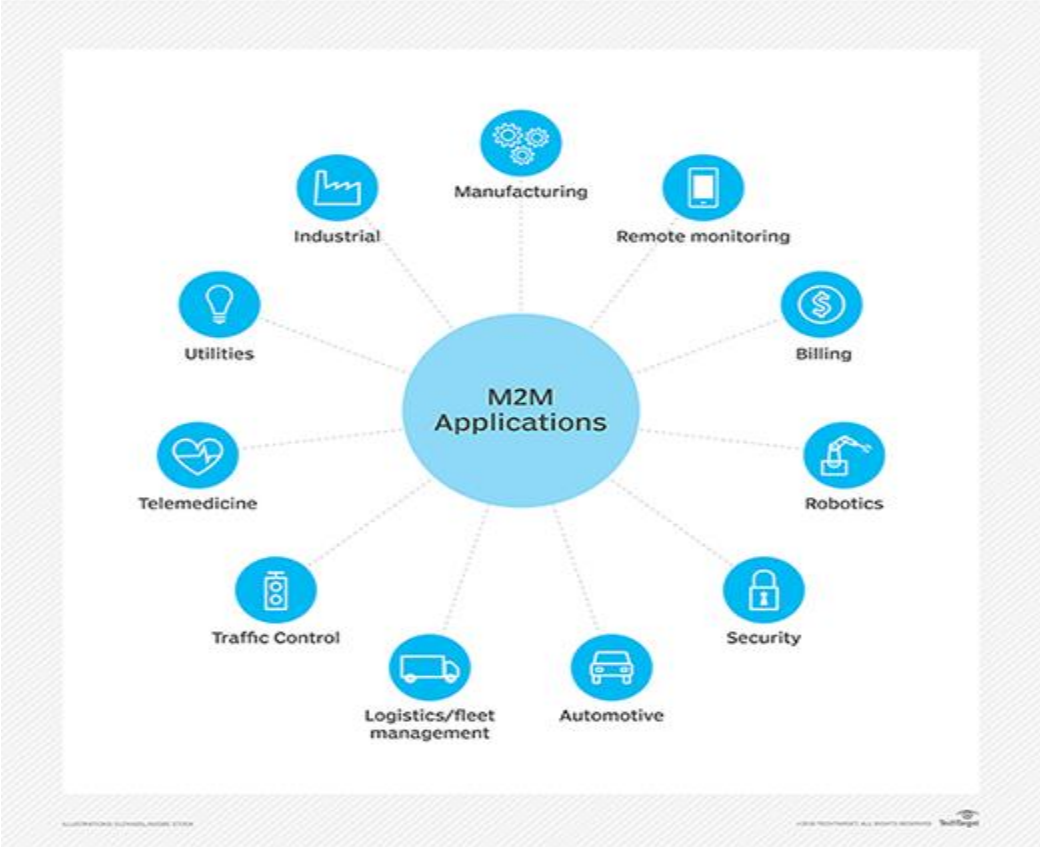
Beyond being able to remotely monitor equipment and systems, the top benefits of M2M include:

- reduced costs by minimizing equipment maintenance and downtime;
- boosted revenue by revealing new business opportunities for servicing products in the field; and
- improved customer service by proactively monitoring and servicing equipment before it fails or only when it is needed.

M2M applications

Machine-to-machine communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor's network, or *machine*, when a particular item is running low to send a refill. An enabler of asset tracking and monitoring, M2M is vital in warehouse management and supply chain management.

Utilities companies often rely on M2M devices and applications to not only harvest energy, such as oil and gas, but also to bill customers -- through the use of smart meters -- and to detect worksite factors, such as pressure, temperature, equipment status and more.



In telemedicine, M2M devices can enable the real-time monitoring of patients' vital statistics, dispensing medicine when required, or tracking healthcare assets.

M2M is also an important aspect of remote control, robotics, traffic control, security, logistics and fleet management, and automotive.

M2M vs. IoT

While many use the terms interchangeably, M2M and IoT are not the same. IoT needs M2M, but M2M does not need IoT.

Both terms relate to the communication of connected devices, but M2M systems are often isolated, stand-alone networked equipment. IoT systems take M2M to the next level, bringing together disparate systems into one large, connected ecosystem.

M2M systems use point-to-point communications between machines, sensors and hardware over cellular or wired networks, while IoT systems rely on IP-based networks to send data collected from IoT-connected devices to gateways, the cloud or middleware platforms.

Modbus

Modbus is a serial communication protocol for use with programmable logic controllers. It is typically used to transmit signals from instrumentation and control devices back to a main controller; or data gathering system, for example a system that measures temperature and humidity and communicates the results to a computer, according to Simply Modbus.

How does it work, and why use it for IoT?

The method is used for transmitting information over serial lines between electronic devices. The device requesting information is called "master" and "slaves" are the devices supplying information. In a standard Modbus network, there is one master and up to 247 slaves, each with a unique slave address from 1 to 247.

According to Intel, communication between a master and a slave occurs in a frame that indicates a function code. The function code identifies the action to perform, such as read a discrete input; read a first-in, first-out queue; or perform a diagnostic function. The slave then responds, based on the function code received, with a response indicated by a set of bytes. Slaves can therefore be intelligent devices or simple devices that represent a single sensor.
Because of this operation, systems based on the protocol are critical parts of the industrial "internet of things" for automation and control, housing valuable information that can be unlocked and used by analytics and enterprise systems.

The protocol is commonly used in IoT as a local interface to manage devices. It is an open protocol that is free for manufacturers to build their equipment into, and is now the most commonly available means of connecting industrial electronic devices, according to Simply Modbus.

Benefits of using Modbus

These are some advantages of using Modbus, as outlined by the Modbus Organization:

- If a Modbus driver is already installed and the user is familiar with Ethernet and TCP/IP sockets, a driver can be up and running and talking to a PC in a few hours. Development costs are said to be low; minimum hardware is required; and development is said to be easy under any operating system.
- There are no "exotic" chipsets required and the system can use standard PC Ethernet cards to talk to newly implemented device; as the cost of Ethernet falls, there should be a cost reduction in hardware; and users are not tied to one vendor for support, but can benefit from current developers.
- The specification is available free of charge for download, and there are no subsequent licensing fees required for using Modbus protocols.

- Interoperability among different vendors' devices and compatibility with an installed base of compatible devices.

KNX

KNX is a communication protocol developed for — and widely used in —home and building automation. It is a standardized (EN 50090, ISO/IEC 14543), OSI-based network communications protocol that is administered by the KNX Association.

The standard is based on the communication stack of the European Installation Bus (EIB) but enlarged with the physical layers, configuration modes, and application experience of BatiBUS and EHS.

KNX defines several physical communication media:

- Twisted pair wiring (inherited from the BatiBUS and EIB Instabus standards)
- Powerline networking (inherited from EIB and EHS– similar to that used by X10)
- Radio Frequency (KNX-RF)
- Infrared
- Ethernet (also known as EIBnet/IP or KNXnet/IP)

The Radio Frequency Versions: KNX RF, RF Ready, and RF Multi

Radio Frequency KNX is the wireless version of the KNX physical layers. KNX RF can share the application layers with the other media versions of KNX, so it's completely compatible on the application level, making KNX RF an ideal complement to wired or IP KNX.

Currently there are three variants of the KNX RF specification:

1. The original KNX RF.
2. KNX RF Ready, which added some features to be forward compatible with KNX RF Multi.
3. And KNX RF Multi, designed to meet some of the shortcomings of the previous protocol while improving reliability by using more than one RF channel.

The original KNX RF was specified in Supplement 22 of the KNX Specification 1.1 [KNX]. KNX RF operates at 868.3 MHz using FSK modulation at a data rate of 16.4 kbit/s. The PHY and MAC layers of KNX RF were defined jointly by the EN 13757-4:2005 (Wireless M-Bus) standard for wireless meter reading, allowing some degree of interoperability between the two protocols.

KNX RF allows unidirectional (transmit-only) devices, in addition to conventional bidirectional ones. By eliminating the receiver function, the device designer can extend the battery lifetime of building automation sensors.

KNX RF Device Addressing Scheme

Due to the nature of wireless communication and the support of transmit-only devices, KNX RF uses its own addressing scheme which is different from (although similar to) the standard KNX addressing scheme. Since RF is an open medium, the address spaces of neighboring installations would interfere with each other. Therefore it has to be guaranteed that each KNX RF installation has its own address space. Extended addresses are used for this purpose. An extended address is defined as the combination of the traditional KNX address and the serial number (SN) of the device.

KNX RF Multi: Expanding to Multiple Frequencies

Two new versions were added to the standard KNX RF Ready as an intermediate forward compatible version, and then finally the KNX RF Multi was released. The main difference between KNX RF Ready and KNX RF Multi is in the use of frequencies. KNX RF Ready can only communicate at a center frequency of 868.3 MHz, but it can co-operate with KNX RF Multi.

Switching Between Fast & Slow Channels in KNX RF Multi

With KNX RF Multi it is possible to switch between three “fast” and two “slow” channels. If there is interference, the KNX RF Mulit device will automatically change channel.

The fast channels are intended for human activities, such as switching on or dimming lights, that require fast response times. The slow channels are for applications which do not need low latency, such as heating, ventilation and air-conditioning (HVAC).

On the fast channels the data rate is 16.384 kbit/s and on the slow channels it’s 8.192 kbit/s. KNX RF Multi offers the further benefit of immediate acknowledgement of the telegrams sent. These are called »Fast Immediate Acknowledge« (IACK).

Wireless Range of KNX RF

The typical line-of-sight range of KNX RF at 868 MHz is 150 meters. Within a building the range very much depends on the actual environment, building materials, etc. Under good circumstances ranges of 30 meters are possible within a building. That said, device designers should conservatively plan on a range of 20 meters so that a “range reserve” is available. KNX RF also support multi-hop repeaters to extend the range.

Benefits of Using KNX RF

Intermediate Standard designed for Building Automation

Fully compatible on an application level with other KNX media: Twisted pair, PLC and Ethernet

Supports long-life b operation

Reliable radio protocol using listen-before-talk, multiple channels, repeaters, acknowledgement and re-transmissions

Hardware independent protocol

A single design commissioning to l (ETS is manufacturer-in lepende

A complete set of supported configuration modes (system and easy mode)

Any product labeled with the KNX trademark is conforming to the standard assured by KNX-accredited, third-party test lab

Examples of Building Automation Using KNX RF Networking

Bus devices can either be sensors or actuators needed for control of building management equipment such as:

- Lighting
- Blinds / shutters
- Security systems
- Energy management
- Heating, ventilation and air-conditioning systems (HVAC)
- Signaling and monitoring systems
- Interfaces to service and building control systems
- Remote control

- Metering
- Audio / video control
- White goods (refrigerators, washers, dryers, etc.)

Zigbee Architecture

In this present communication world there are numerous high data rate communication standards that are available, but none of these meet the sensors' and control devices' communication standards. These high-data rate communication standards require low-latency and low-energy consumption even at lower bandwidths. The available proprietary wireless systems' Zigbee technology is low-cost and low-power consumption and its excellent and superb characteristics makes this communication best suited for several embedded applications, industrial control, and home automation, and so on.

What is Zigbee Technology?

What is Zigbee Technology?

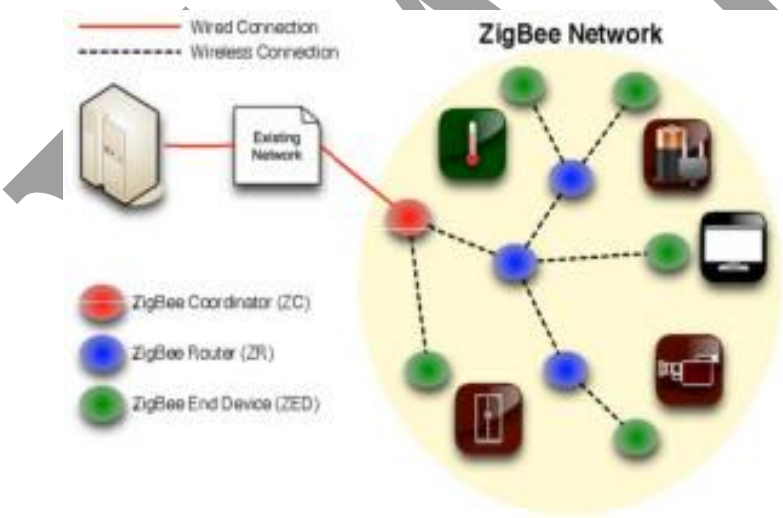
Zigbee communication is specially built for control and sensor networks on IEEE 802.15.4 standard for wireless personal area networks (WPANs), and it is the product from Zigbee alliance. This communication standard defines physical and Media Access Control (MAC) layers to handle many devices at low-data rates. These Zigbee's WPANs operate at 868 MHz, 902-928MHz and 2.4 GHz frequencies. The date rate of 250 kbps is best suited for periodic as well as intermediate two way transmission of data between sensors and controllers.

Zigbee is low-cost and low-powered mesh network widely deployed for controlling and monitoring applications where it covers 10-100 meters within the range. This communication system is less expensive and simpler than the other proprietary short-range wireless sensor networks as Bluetooth and Wi-Fi.

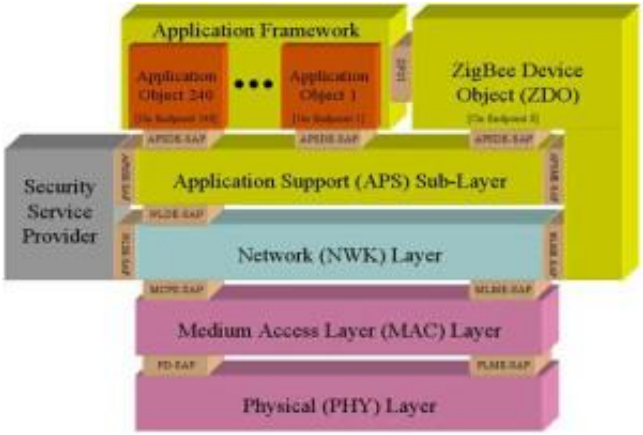
Zigbee supports different network configurations for master to master or master to slave communications. And also, it can be operated in different modes as a result the battery power is conserved. Zigbee networks are extendable with the use of routers and allow many nodes to interconnect with each other for building a wider area network.

Architecture

Zigbee system structure consists of three different types of devices such as Zigbee coordinator, Router and End device. Every Zigbee network must consist of at least one coordinator which acts as a root and bridge of the network. The coordinator is responsible for handling and storing the information while performing receiving and transmitting data operations. Zigbee routers act as intermediary devices that permit data to pass to and fro through them to other devices. End devices have limited functionality to communicate with the parent nodes such that the battery power is saved as shown in the figure. The number of routers, coordinators and end devices depends on the type of network such as star, tree and mesh networks.



Zigbee protocol architecture consists of a stack of various layers where IEEE 802.15.4 is defined by physical and MAC layers while this protocol is completed by accumulating Zigbee's own network and application layers.



Physical Layer: This layer does modulation and demodulation operations up on transmitting and receiving signals respectively.

MAC Layer: This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance (CSMA). This also transmits the beacon frames for synchronizing communication.

Network Layer: This layer takes care of all network related operations such as network setup, end device connection and disconnection to network, routing, device configurations, etc.

Application Support Sub-Layer: This layer enables the services necessary for Zigbee device object and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

Application Framework: It provides two types of data services as key value pair and generic message services. Generic message is a developer defined structure, whereas the key value pair is used for getting attributes within the application objects. ZDO provides an interface between application objects and APS layer in Zigbee devices. It is responsible for detecting, initiating and binding other devices to the network.

Network layer

Network is the OSI Level 3 layer and is the internet layer in the TCP-IP model. Like Physical and MAC layers, network layer is also part of the infrastructure layer in IOT reference architecture.

This layer is responsible for addressing and routing of data packets. At this layer, the datagram from transport layer are encapsulated to data packets and delivered to their destinations using IP addressing. IPv4 had been the standard protocol for network layer until now. The IPv4 has a limited address space which has been already exhausted and incapable

to cope up with the scalability of the IOT applications. The new IPv6 standard has been developed to accommodate address space sufficient to enable addressing the billions of IOT devices. There are also many protocol stacks which are based on IPv6 addressing that are developed considering IOT scenario. The popular network layer protocols are as follow -

- IPv4
- IPv6
- 6LoWPAN
- 6TiSCH
- 6Lo
- IPv6 over Bluetooth Low Energy
- IPv6 over G.9959

The network layer is divided into two sublayers: routing layer which handles the transfer of packets from source to destination, and an encapsulation layer that forms the packets.

RPL Protocol

RPL stands for *Routing Protocol for Low-Power and Lossy Network*. It is a distance-vector protocol that supports a varity of Data Link Protocols. RPL builds a **Destination Oriented Directed Acyclic Graph (DODAG)** which has only one route from each leaf node to the root. All the traffic in this DODAG is routed through the root. Initially, each node sends a DODAG Information Object (DIO) announcing them self as a root. This information travels in the network, and complete DODAG is gradually built. When a new node wants to join the network, it sends a DODAG Information Solicitation (DIS) request and root responds back with a DAO Acknowledgment (DAO-ACK) confirming the join.

CORPL Protocol

CORPL protocol is the extension of the **RPL protocol**, which is termed as **cognitive RPL**. This network protocol is designed for cognitive networks and uses DODAG topology. CORPL protocol makes two new modifications in the RPL protocol. It uses opportunistic forwarding to forward a packet between the nodes. Each node of CORPL protocol keeps the information of forwarding set rather than parents only maintaining it. Each node updates its changes to its neighbor using DIO messages. On the basis of this updated message, each node frequently updates its neighbor for constant forwarder set.

CARP Protocol

CARP (Channel-Aware Routing Protocol) is a distributed routing protocol. It is designed for underwater communication. It has lightweight packets so that it can be used for Internet of Things (IoT). It performs two different functionalities: network initialization and data forwarding. CARP protocol does not support previously collected data. Hence, it is not beneficial for those IoT or other application where data is changed frequently. The upgradation of CARP is done in E-CARP which overcomes the limitation of CARP. The E-CARP allows the sink node to save previously received sensory data.

6LoWPAN

The 6LoWPAN protocol refers to IPv6 Low Power Personal Area Network which uses a lightweight IP-based communication to travel over low data rate networks. It has limited processing ability to transfer information wirelessly using an internet protocol. So, it is mainly used for home and building automation. The 6LoWPAN protocol operates only within the 2.4 GHz frequency range with 250 kbps transfer rate. It has a maximum length of 128-bit header packets.

6LowPAN Security Measure

Security is a major issue for 6LowPAN communication Protocol. There are several attacks issues at the security level of 6LoWPAN which aim is to direct destruction of the network. Since it is the combination of two systems, so, there is a possibility of attack from two sides that targets all the layer of the 6LoWPAN stack (Physical layer, Data link layer, Adaptation layer, Network layer, Transport layer, Application layer).

APS layer

The application support sublayer (APS) provides services to the application layer and the network layer through the application support data entity (APSDE) and application support management entity (APSME).

The application support sublayer (APS) provides the services necessary for application objects (endpoints) and the ZigBee device object (ZDO) to interface with the network layer for data and management services. Some of the services provided by the APS to the application objects for data transfer are request, confirm, and response. Furthermore, the APS provides communication for applications by defining a unified communication structure (for example, a profile, cluster, or endpoint).

- **Application object (endpoint):** An application object defines input and output to the APS. For example, a switch that controls a light is the input from the application object, and the output is the light bulb condition. Each node can have 240 separate application objects. An application object may also be referred to as an endpoint (EP).
- **ZigBee device object (ZDO):** A ZigBee device object performs control and management of application objects. The ZDO performs the overall device management tasks:

  Determines the type of device in a network (for example, end device, router, or coordinator)

  Initializes the APS, network layer, and security service provider

  Performs device and service discovery

Initializes coordinator for establishing a network

Security management

Network management

Binding management

- **End node:** Each end node or end device can have multiple EPs. Each EP contains an application profile, such as home automation, and can be used to control multiple devices or a single device. More to the point, each EP defines the communication functions within a device
- **ZigBee addressing mode:** ZigBee uses direct, group, and broadcast addressing for transmission of information. In direct addressing, two devices communicate directly with each other. This requires that the source device has both the address and endpoint of the destination device. Group addressing requires that the application assign a group membership to one or more devices. A packet is then transmitted to the group address in which the destination device lies. The broadcast address is used to send a packet to all devices in the network.

Security

IoT security is the technology area concerned with safeguarding connected devices and networks in the internet of things (IoT).

IoT involves adding internet connectivity to a system of interrelated computing devices, mechanical and digital machines, objects, animals and/or people. Each "thing" is provided a unique identifier and the ability to automatically transfer data over a network. Allowing devices to connect to the internet opens them up to a number of serious vulnerabilities if they are not properly protected.

IoT security has become the subject of scrutiny after a number of high-profile incidents where a common IoT device was used to infiltrate and attack the larger network. Implementing security measures is critical to ensuring the safety of networks with IoT devices connected to them.

IoT security challenges

A number of challenges prevent the securing of IoT devices and ensuring end-to-end security in an IoT environment. Because the idea of networking appliances and other objects is

relatively new, security has not always been considered top priority during a product's design phase. Additionally, because IoT is a nascent market, many product designers and manufacturers are more interested in getting their products to market quickly, rather than taking the necessary steps to build security in from the start.

A major issue cited with IoT security is the use of hardcoded or default passwords, which can lead to security breaches. Even if passwords are changed, they are often not strong enough to prevent infiltration.

Another common issue facing IoT devices is that they are often resource-constrained and do not contain the compute resources necessary to implement strong security. As such, many devices do not or cannot offer advanced security features. For example, sensors that monitor humidity or temperature cannot handle advanced encryption or other security measures. Plus, as many IoT devices are "set it and forget it" -- placed in the field or on a machine and left until end of life -- they hardly ever receive security updates or patches. From a manufacturer's viewpoint, building security in from the start can be costly, slow down development and cause the device not to function as it should.

Connecting legacy assets not inherently designed for IoT connectivity is another security challenge. Replacing legacy infrastructure with connected technology is cost-prohibitive, so many assets will be retrofitted with smart sensors. However, as legacy assets that likely have not been updated or ever had security against modern threats, the attack surface is expanded.

In terms of updates, many systems only include support for a set timeframe. For legacy and new assets, security can lapse if extra support is not added. And as many IoT devices stay in the network for many years, adding security can be challenging.

IoT security is also plagued by a lack of industry-accepted standards. While many IoT security frameworks exist, there is no single agreed-upon framework. Large companies and industry organizations may have their own specific standards, while certain segments, such as industrial IoT, have proprietary, incompatible standards from industry leaders. The variety

of these standards makes it difficult to not only secure systems, but also ensure interoperability between them.

Karpagam Academy of Higher Education
Dept of CS
Subject: Internet of Things
Class: I M.Sc (CS) **Multiple Choice Questions**
UNIT-2

S.no	Questions	opt1	opt2	opt3	opt4	Answer
1	The equipment needed to allow home computers to connect to the Internet is called a	A Modem	B Gateway	C Monitor	D Peripheral	A Modem
2	The process of keeping addresses in memory for future use is called	A Routing	B Resolving	C Caching	D None of the above	C Caching
3	a	A Hub	B Host	C Gateway	D Repeater	B Host
4	A user can get files from another computer on the Internet by using	A HTTP	B TELNET	C UTP	D FTP	D FTP
5	The communication protocol used by Internet is:	A HTTP	B WWW	C TCP/IP	D FTP	C TCP/IP
6	The first network that planted the seeds of Internet was:	A ARPANET	B NSFnet	C Vnet	D Both (A) and (B)	A ARPANET
7	Which of the following protocols is used for WWW ?	A ftp	B http	C w3	D all of the above	B http
8	TCP is a commonly used protocol at	A Application layer	B Transport layer	C Network layer	D Data Link layer	B Transport layer
9	The first page that you normally view at a Website is its:	A Home page	B Master page	C First page	D None of the above	A Home page
10	Voice mail, E-mail, Online service, the Internet and the WWW are all example of	A Computer categories	B Connectivity	C Telecommuting	D None of the above	C Telecommuting

11	Which of the following layers of the OSI reference model resolve problems of damaged or lost or duplicate frames ?	A Data link layer	B Network layer	C Session layer	D None of the above	A Data link layer
12	X.25 protocol consists of	A Physical and frame levels	B Frame and packet levels	C Physical, frame and packet levels	D None of the above	C Physical, frame and packet levels
13	How much channel throughout of slotted ALOHA will be in comparison to pure ALOHA.	A Same	B Double	C Three times	D None of the above	B Double
14	X.21 is physical level standard for	A X.25	B CSMA/CD	C ATM networks	D None of the above	A X.25
15	X.25 LAPP uses a specific subset of	A CSMA/CD protocol	B HDLC protocol	C Token ring	D None of the above	B HDLC protocol
16	X.21 protocol consists of	A Physical and frame levels	B Frame and packet levels	C Physical, frame and packet levels	D Only physical level	D Only physical level
17	The shortest frame in HDLC protocol is usually the	A Information frame	B Management frame	C Supervisory frame	D None of the above	C Supervisory frame
18	and	A Pulse coding	B Shift keying	C Quantization	above	C Quantization
19	Which of the following encoding scheme is used by the physical layer of FDDI ?	A 3 out of 4	B 4 out of 5	C 5 out of 6	D None of the above	B 4 out of 5
20	What is the measure (unit) used to represent signaling rate per second	A Baud	B Hz	C Bps	D None of these	A Baud
21	The device operation at Data Link layer is	A Repeater	B Router	C Bridge	D None of these	C Bridge
22	In which ARQ, when a NAK is received, all frames sent since the last frame acknowledge are retransmitted	A Go back n	B Stop-and-wait	C Selective Reject	D Both A and B	A Go back n

23	XMPP Full form is _____	a) Extensible Messaging and Presence Protocol	b) Extensible Module and presence protocol	c) Extensible Messaging and Presence Protocol	d) Extensible Messaging and Presence Protocol	a) Extensible Messaging and Presence Protocol
24	XMPP is used for streaming which type of elements?	a) XPL	b) XML	c) XHL	d) MPL	b) XML
25	XMPP creates _____ identity.	a) device	b) email	c) message	d) data	a) device
26	XMPP supports _____	a) Structured data	b) Foundation	c) Federation	d) Jabber ID	c) Federation
27	Which protocol has a quality of service?	a) XMPP	b) HTTP	c) CoAP	d) MQTT	a) XMPP
28	The original transport protocol for XMPP.	a) FCP	b) TCP	c) MCP	d) HCP	b) TCP
29	Which XMPP core describes client server messaging?	a) RFC 6122	b) RFC 4854	c) RFC 6120	d) RFC 3923	c) RFC 6120
30	XMPP uses _____ architecture.	a) Decentralized client-server	b) Centralized client-server	c) Message	d) Public/subscriber	a) Decentralized client-server
31	XMPP implementation uses _____	a) CoAP	b) Gaming	c) Email	d) Polling	d) Polling
32	IRC stands for _____	a) Internet Reduce Chat	b) Interconnection Relay Chat	c) Internet Relay Chat	d) Interconnect Reduce Chat	c) Internet Relay Chat
33	SIP stands for _____	a) Session Initiation Protocol	b) Session Internet Protocol	c) Simple Initiation Protocol	d) Session Internet Protocol	a) Session Initiation Protocol
34	What Bigdata collects?	a) Human generated data	b) Sensor data	c) Machine generated data	d) Device data	a) Human generated data
35	What IoT collects?	a) Human generated data	b) Sensor data	c) Machine generated data	d) Device data	c) Machine generated data
36	Which requires data stream management?	a) Bigdata	b) IoT	c) Bigdata & IoT	d) Device data	b) IoT
37	Which requires Edge analytics?	a) Bigdata	b) IoT	c) Bigdata & IoT	d) Device data	b) IoT
38	The IoT operates at _____ scale.	a) Machine	b) Human	c) Device	d) Sensor	a) Machine

39	We need to invest in storage and prepossessing capacity to perform _____	a) C analytics	b) Bigdata analytics	c) Python analytics	d) IoT analytics	d) IoT analytics
40	IoT analytics was proposed by _____	a) Syntel	b) IBM	c) Accenture	d) Intel	d) Intel
41	Which page provides the number of last observations in the specific period?	a) Dashboard	b) GitHub	c) IoT analytics	d) Sensors	a) Dashboard
42	CoAP is specialized in _____	a) Internet applications	b) Device applications	c) Wireless applications	d) Wired applications	a) Internet applications
43	Which layer is CoAP?	a) Control layer	b) Transport layer	c) Service layer	d) Application layer	c) Service layer
44	CoAP provides which of the following requirements?	a) Multicast support and simplicity	b) Low overhead and multicast support	c) Simplicity and low overhead	d) Multicast support, Low over head, and simplicity	d) Multicast support, Low over head, and simplicity
45	The core of the protocol is specified in _____	a) RFC 7254	b) RFC 7252	c) RFC 7452	d) RFC 7524	b) RFC 7252
46	What is the RAM and ROM size in CoAP?	a) 100 KiB of RAM and 10 KiB of ROM	b) 10 KiB of RAM and 100 KiB of ROM	c) 10 KiB of RAM and 250 KiB of ROM	d) 250 KiB of RAM and 10 KiB of ROM	b) 10 KiB of RAM and 100 KiB of ROM
47	Which is an open standard?	a) HTTP	b) MQTT	c) XMPP	d) CoAP	d) CoAP
48	HART stands for_____	a) Highway Addressable Remote Transducer	b) High Addressable Remote Transducer	c) High Application Remote Transducer	d) Highway Application Remote Transducer	a) Highway Addressable Remote Transducer
49	LTP stands for _____	a) Lean Transducer Protocol	b) Lean Transport Protocol	c) Layer Transport Protocol	d) Layer Transducer Protocol	b) Lean Transport Protocol
50	URI and content type support is which protocol feature?	a) Http	b) UDP	c) CoAP	d) SPI	c) CoAP
51	Windows 10 IoT enterprise OS includes what?	a) Edge gateway	b) PI system	c) RAM	d) Data stream	a) Edge gateway

52	Types of gateway classes?	a) Only one	b) 3 types	c) 2 types	d) 4 types	c) 2 types

UNIT III

SYLLABUS

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 of Things: Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture.

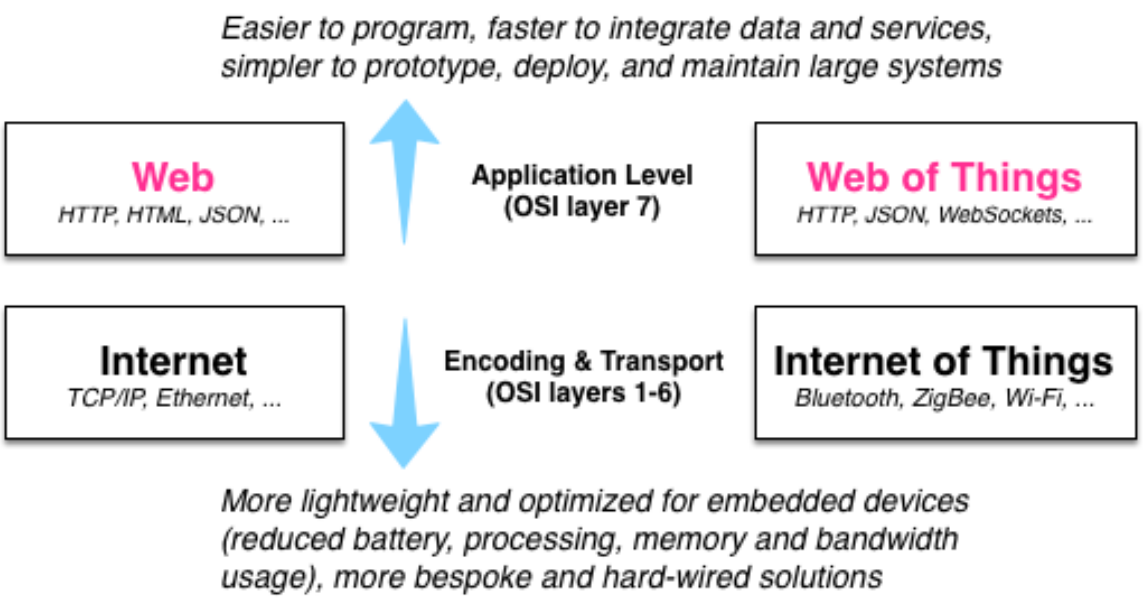
Web of Things versus Internet of Things

Contrasting the Current IoT and the WoT

As more everyday objects will be digitally augmented, the next logical step is to use the World Wide Web ecosystem and infrastructure to build applications for the IoT, effectively breaking this ongoing "one device, one protocol, one app" pattern. It would be particularly interesting to push down to each of those tiny devices the exact same technology that helped modern Web sites such as Facebook or Google scale to millions of concurrent users, without compromising on security or performance. The idea of maximizing existing and emerging tools and techniques used on the Web and apply them to the development of IoT scenarios is what we call the Web of Things.

While the IoT has been busy resolving networking problems, the Web of Things relies exclusively on application level protocols and tools. Mapping any device into a Web mindset makes the Web of Things agnostic to the physical and transport layer protocols used by devices. As you will learn to do in the book, pretty much any custom protocol or standard can be linked to the Web thanks to software or hardware "bridges" (via proxies or gateways).

bridges" (via proxies or gateways).



Source: Building the Web of Things: book.webofthings.io
Creative Commons Attribution 4.0

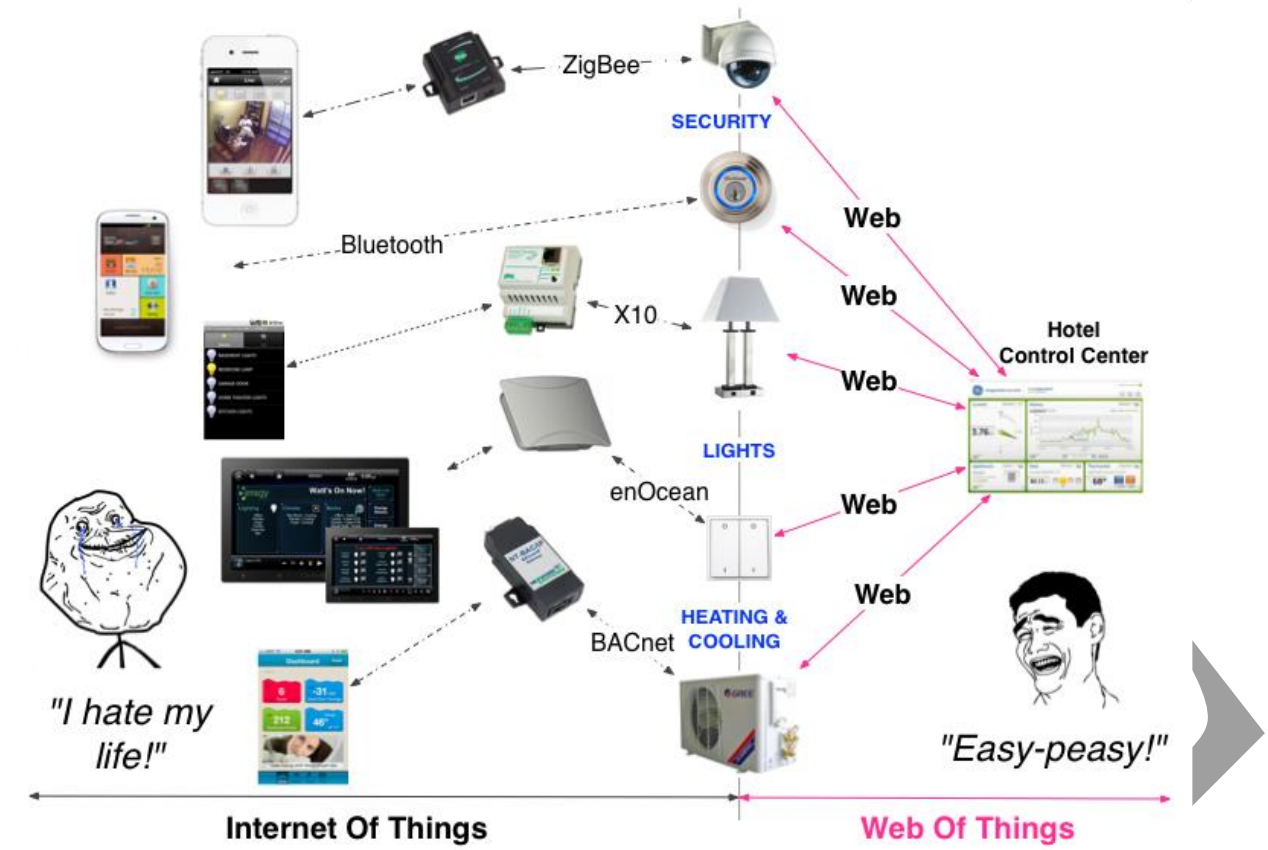
The Web of Things only deals with the highest OSI Layer (7), which handles applications, services and data. Working on such a high level of abstraction makes it possible to connect data and services from many devices regardless of the actual transport protocols used. In contrast, the Internet of Things does not advocate a particular application level protocol and is usually focusing on the lower layers of the OSI

stack.

Source: Building the Web of Things: book.webofthings.io
Creative Commons Attribution 4.0

The Web of Things is the ability to use modern Web standards directly on embedded devices. By leveraging all these standards for IoT scenarios, we both enable new types of interactive applications to be built, and also make sure that devices can be integrated with modern Web applications and services with minimal effort.

In the Web of Things, devices and their services are fully integrated in the Web because they use the same standards and techniques as traditional Web sites. This means that you can write applications that interact with embedded devices in exactly the same way as you would interact with any other Web service that uses Web APIs and in particular using RESTful architectures.



Source: Building the Web of Things: book.webofthings.io
Creative Commons Attribution 4.0

In the IoT, hundreds of incompatible protocols co-exist today. This makes the integration of data and services from various devices extremely complex and costly. In the Web of Things, any device can be accessed using standard Web protocols. Connecting heterogeneous devices to the Web makes the integration across systems and applications much simpler.

WoT Architecture

Like the OSI layered architecture organises the many protocols and standards of the Internet, the WoT architecture is an attempt to structure the galaxy of Web protocols and tools into a useful framework for connecting any device or object to the Web. The WoT architecture stack is not composed of layers in the strict sense, but rather of levels that add extra functionality, as shown in the figure below. Each layer helps to integrate Things to the Web even more intimately and hence making those devices more accessible for applications and humans.

Layer 1: Access

This layer is responsible for turning any Thing into a Web Thing that can be interacted with using HTTP requests just like any other resource on the Web. In other words, a Web Thing is a REST API that allows to interact with something in the real world, like opening a door or reading a temperature sensor located across the planet.

Layer 2: Find

This is where the second layer – Find – becomes interesting. This layer ensures that your Thing can not only be easily used by other HTTP clients but can also be findable and automatically usable by other WoT applications. The approach here is to reuse web semantic standards to describe things and their services. This enables searching for things through search engines and other web indexes as well as the automatic generation of user interfaces or tools to interact with Things. At this level technologies such as JSON-LD are in use: a language for semantically annotating JSON. This is also where standards such as the Web Things Model and the work of the W3C WoT group help: they define an abstract set of REST resources that Things should offer.

Layer 3: Share

The Internet of Things will only blossom if Things have a way to securely share data across services. This is the responsibility of the Share layer, which specifies how the data generated by Things can be shared in an efficient and secure manner over the web. At this level, another batch of Web protocols help. First, TLS, the protocol that makes transactions on the Web secure. Then, techniques such as delegated web authentication mechanisms like OAuth which can be integrated to our Things' APIs. Finally, we can also use social networks to share Things and their resources to create a Social Web of Things!.

Layer 4: Compose

Finally, once Things are on the Web (layer 1) where they can be found by humans and machines (layer 2) and their resources can be shared securely with others (layer 3), it's time to look at how to build large-scale, meaningful applications for the Web of Things. In other words, we need to understand the integration of data and services from heterogeneous Things into an immense ecosystem of web tools such as analytics software and mashup platforms. Web tools at the Compose layer range from web toolkits—for example, JavaScript SDKs offering higher-level abstractions

Karpagam Academy of Higher Education
Dept of CS
Subject: Internet of Things
Class: I M.Sc (CS) Multiple Choice Questions
UNIT-3

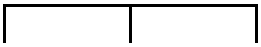
sno	Questions	opt1	opt2	opt3	opt4	Answer
1	_____ allows us to control electronic components	RETful API	RESTful API	HTTP	MQTT	RETful API
2	MQTT stands for _____	MQ Telemetry Things	MQ Transport Telemetry	MQ Telemetry Transport	MQ Transport Things	MQ Telemetry Transport
3	MQTT is _____ protocol.	Machine to Machine	Internet of Things	Machine to Machine and Internet of Things	Machine Things	Machine to Machine and Internet of Things
4	Which protocol is lightweight?	MQTT	HTTP	CoAP	SPI	MQTT
5	PubNub publishes and subscribes _____ in order to send and receive messages.	Network	Account	Portal	Keys	Keys
6	By clicking which key the PubNub will display public, subscribe, and secret keys.	Pane	Demo Keyset	Portal	Network	Demo Keyset
7	The messageChannel class declares the _____ class attribute that defines the key string.	command_key	command-key	commandkey	Key_command	command_key
8	_____ method saves the received arguments in three attributes.	__Init	Init__	__Init__	_init_	__Init__
9	_____ and _____ saves the publish and subscribe keys that we have generated with the PubNub Admin portal.	public_key and subscribe_key	Public-key and subscribe-key	publickey and subscribekey	Key_public and key_subscribe	public_key and subscribe_key

10	_____ specifies the function that will be called when there is a new message received from the channel.	Reconnect	Error	Connect	Callback	Callback
11	_____ specifies the function that will be called on an error event.	Callback	Error	Connect	Reconnect	Error
12	The equipment needed to allow home computers to connect to the Internet is called a	Modem	Gateway	Monitor	Peripheral	Modem
13	The process of keeping addresses in memory for future use is called	Routing	Resolving	Caching	None of the above	Caching
14	The server on the Internet is also known as a	Hub	Host	Gateway	Repeater	Host
15	A user can get files from another computer on the Internet by using	HTTP	TELNET	UTP	FTP	FTP
16	The communication protocol used by Internet is:	HTTP	WWW	TCP/IP	FTP	TCP/IP
17	The first network that planted the seeds of Internet was:	ARPANET	NSFnet	Vnet	Both (A) and (B)	ARPANET
18	Which of the following protocols is used for WWW ?	ftp	http	w3	all of the above	http
19	TCP is a commonly used protocol at	Application layer	B Transport layer	C Network layer	D Data Link layer	B Transport layer
20	The first page that you normally view at a Website is its:	Home page	Master page	First page	None of the above	Home page
21	Voice mail, E-mail, Online service, the Internet and the WWW are all example of	Computer categories	B Connectivity	C Telecommuting	D None of the above	C Telecommuting
22	Web site is a collection of	HTML documents	Graphic files	Audio and video files	All of the above	D All of the above

23	In MODEMS	Digital signal is amplified	B Several digital signals are multiplexed	C A digital signal changes some characteristic of a carrier wave	D None of the above	C A digital signal changes some characteristic of a carrier wave
24	In reality, Internet Protocol recognizes only	An IP address	B A location of the host	C A postal mail address	D None of the above	An IP address
25	The ground station in VSAT communication is called	HTTP	B Hub	C Multiplexer	D None of the above	B Hub
26	A small network making up the Internet and also having a small numbers of computers within it is called	Host	B Address	C Subdomain	D None of the above	C Subdomain
27	Computers on the Internet owned and operated by education institution form part of the	com domain	B edu domain	C mil domain	D None of the above	B edu domain
28	Which of the following networking solution is suitable for networking in a building?	WAN	B MAN	C LAN	D All of the above	C LAN
29	Which of the following topology share a single channel on which all station can receive and transmit?	Ring	Bus	Tree	Star	Bus
30	Main protocol used in Internet	X.25	IPX/SPX	TCP/IP	D Token Bus	TCP/IP
31	Cell based architecture is known as	ATM	B FDDI	LAN	D Client Server	ATM
32	The network where all the nodes are around a central server is a	Bus network	B Star network	C Ring network	D None of the above	B Star network
33	Which of the following topology is least affected by addition/removal of a node?	RING	B BUS	C STAR	D None of the above	RING
34	In which cases gateway will appear?	a) Industrial Automation	b) Building automation	c) Transportation	d) Industrial & Building Automation	d) Industrial & Building Automation

35	The agent running as a _____ on a device.	a) SSH Terminal	b) Yocto Linux	c) Daemon	d) Local agent	c) Daemon
36	_____ command line utility allows us to perform specific interactions with Intel IoT Analytics.	a) Iotkit-admin	b) SSH Terminal	c) Local agent	d) Daemon	a) Iotkit-admin
37	We will not use command line utility to perform _____	a) proper communication with Intel IoT analytics	b) Obtain device id	c) Activate device	d) Send observations	d) Send observations
38	Build: 0.14.5 defines what?	a) Ip Address	b) Medium	c) Address	d) Version	d) Version
39	Command line to obtain the device Id?	a) iotkit-admin device-id	b) iotkit-admin deviceid	c) Iotkit – admin device-id	d) Iotkit – admin device – id	a) iotkit-admin device-id
40	Default, device Id is equal to _____	a) IP Address	b) MAC Address	c) ISP	d) UI	b) MAC Address
41	Which protocol is used to link all the devices in the IoT?	a) TCP/IP	b) Network	c) UDP	d) HTTP	a) TCP/IP
42	_____ enables seamless integration of LoWPAN devices with internet leveraging.	a) IETF 6LoWPAN	b) IEFT CoAP	c) RFID/NFC	d) IEEE 802.15.4.LoWPAN	a) IETF 6LoWPAN
43	enables open application layer for constrained nodes.	a) IETF 6LoWPAN	b) IEFT CoAP	c) RFID/NFC	d) IEEE 802.15.4.LoWPAN	b) IEFT CoAP
44	_____ tags, devices, smart phones useful in identification.	a) IETF 6LoWPAN	b) IEFT CoAP	c) RFID/NFC	d) IEEE 802.15.4.LoWPAN	c) RFID/NFC
45	_____ supports low energy radio operation.	a) IETF 6LoWPAN	b) IEFT CoAP	c) RFID/NFC	d) Bluetooth	d) Bluetooth
46	_____ specification defining the PHY and MAC layer of low power devices.	a) IETF 6LoWPAN	b) IEFT CoAP	c) RFID/NFC	d) IEEE 802.15.4.LoWPAN	d) IEEE 802.15.4.LoWPAN

47	6LoWPAN Adaption layer contains?	a) Header compression	b) Fragmentation	c) Layer 2 forwarding	d) Header compression, Fragmentation, and Layer 2 forwarding	d) Header compression, Fragmentation, and Layer 2 forwarding
48	_____ is an application layer protocol for resource constrained devices.	a) CoAP	b) HMTP	c) MQTT	d) TCP/IP	a) CoAP
49	Adheres to _____ approach for managing resources and support mapping to HTTP.	a) RETful	b) IoT	c) Restful	d) RESTful	d) RESTful
50	How many messages types are there in CoAP?	a) 2	b) 5	c) 3	d) 4	d) 4
51	Number of methods in CoAP?	a) 2	b) 5	c) 4	d) 3	c) 4
52	WSN stands for _____	a) Wired Sensor Network	b) Wireless Sensor Network	c) Wired Service Network	d) Wireless Service Network	b) Wireless Sensor Network
53	ITS stands for _____	a) Internet Travel Services	b) Internet Transportation Security	c) Intelligent Transportation Security	d) Intelligent Transportation Services	d) Intelligent Transportation Services
54	An IoT _____ center is envisaged as an important part of the generic IoT platform to unify the organization.	a) Individual Information	b) Individual Integration	c) Integrated Information	d) Individual and Integrated Information	c) Integrated Information
55	The core element is operated by _____	a) PaaS	b) IoT service Provider	c) SaaS	d) IaaS	b) IoT service Provider



UNIT IV

SYLLABUS

Integrating IOT: 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.

Integrating IOT: Integrated Billing Solutions in the Internet of Things Business Models for the Internet of Things

The evolution of Internet of Things has rapidly transformed the world of communications by not only enabling devices interact with humans but also with other devices and the external environment.

This revolution in the IT world is creating new experiences, changing lives and creating the impact on businesses by engulfing almost every field which includes transportation, agriculture, insurance, healthcare, retail, manufacturing and much more.

Gartner predicts that there will be 26 billion connected devices by 2020. This innovative and burgeoning Internet of Things technology has enabled vendors to trot out new products and applications to address specific requirements across verticals which include Fleet Management, Health Monitoring, Smart Grid Applications, Soil Monitoring, Smart Payments and others.

These applications not only generate value to businesses and customers but also enable monetize these services. It is also said that IoT product and service suppliers will generate incremental revenue exceeding $300 bn mostly in services in 2020, by Gartner.

The evolving sophistication in the Internet of Things world provides a major opportunity for service providers to capture new business models, generate new revenue streams and develop new pricing strategies.

As these services scale up, service providers need to address their business challenges for better monetization, increased ARPU, ease of managing complex pricing plans which support bundling of services.

To succeed in the IoT market, you need a billing solution which is not only flexible but also agile in order to handle ever evolving complex business models. You need a system that is scalable to growing markets and can offer new deals, bundled services and a real time usage based pricing and charging models to keep up the pace with the fast growing IoT technology.

- **Improve monetization:** A flexible system able to manage all existing and innovative IoT monetization techniques be it pre-paid, Pay-per-use, Pay-for-privacy, Ad supported, Add-on capabilities, service subscription, Lending/leasing/renting, Digital/physical freemium hybrid etc.
- **Streamline customer onboarding:** The Full-featured system supports the automation of complete customer life cycle right from customer portal sign up to installing hardware at customer's location. Thus, ensuring delivery of best in class support and reduced operational costs.
- **Quickly and efficiently resolve customer requests:** Sensors installed in the machine continuously track for device performance and in the case of breakdown, triggers an event. Now, SURE! Trouble Ticket Management solution detects the event and based on the type of event automatically creates a service ticket and routes it automatically to the right service engineer.
- **Manage Partners and Distribution Channels across globe:** A powerful partner management solution that Manage-Track-Settle complex bills and revenue sharing between you and your partner taking in effect of local taxes as applicable.
- **Scalable solution:** Able to manage growing customer base, supports high volumes of billing and multiple applications while preventing revenue leakages.
- **Quickly integrate with IoT platforms:** Through Our REST and Open APIs, you can quickly integrate SURE! IoT Monetization engine with any IoT platforms. SURE! IoT monetization engine is pre-integrated with all leading IoT platforms.
- **Business Benefits:**
- Strengthens your competitiveness by quickly developing new packaging and pricing models that are specific to your customer preferences.
- Flexibility and efficiency to meet market demands
- Reduced time to market
- Reduced operational costs and revenue leakages
- Real time service enablement
- Future proof solution for evolving complex business models

Network Dynamics: Population Models

Information cascade

In an information cascade, people observe the of choices of others and make their own decisions based on that observation while ignoring their personal knowledge or getting more information. It's a theory used in the field of behavioral economicsand other social sciences.

Informational cascades can be observed in many areas, including financial markets. Recognizing and avoiding this behavior can help people make better financial decisions.

How an Information Cascade Works

Information cascades usually develop when there's no direct verbal communication between individuals. For this example, let's assume that there are four individuals, **M**, **N**, **O**, and **P**. They're faced with two choices: either accepting or rejecting. Each person sequentially makes their choice.

M is the first decision maker, and as such will make a decision based on personal knowledge. Let's suppose **M** accepts.

N is the second decision maker and has the public knowledge that **M** made a decision to accept. **N** may choose to either accept or reject based on both personal knowledge and public knowledge. **N** chooses to accept.

Now, let's assume that **O** ignores their personal knowledge and accepts only because both **N** and **M** already accepted. This forms an information cascade. **O** is just imitating the others and isn't adding new information to the cascade.

P observes the choices of **M**, **N**, and **O** and imitates them by making the same choice to accept.

Key Characteristics

Herd behavior. After a point, very little new information is added to the cascade, and individuals just imitate others based on a belief that such a large number of people can't be wrong. This is referred to as herd behavior. This imitation can lead to erroneous behavior on a massive scale.

Fragility. Information cascades are generally very brittle by nature, as individuals may be reacting only to hearsay and public observation. Any new public information or a more precise information source can change the actions, as well as the direction of the cascade.

Disappearance of external information. When people make decisions based on the actions of others, they're not adding new information to the public's knowledge base.

Examples in Financial Markets
Information cascades can be common in financial markets. An example: An average person might think that a financial pundit has more knowledge and information than they do. Because of that, they imitate the pundit's stock picks.

Maybe that person's neighbor observes them boasting about their stock picks, and so the neighbor also picks the same stocks. Another neighbor notices that both people chose the same stocks and assumes that those stocks must be good picks, simply because more than one person has picked them.

Network Effects

There can be no Internet of Things (IoT) without the network to support it. Sensors and gadgets will gather increasingly vast amounts of data. But the Internet of Things is about more than just gadgets and displays; the amount of data gathered will seriously impact the network, and the networking industry needs to evaluate possible implications.

Three areas of the IoT that will impact the network are data analytics, the need for network agility, and security. Let's take a closer look at these three areas.

Data analytics

Data without analytics is relatively useless. The influx of sensors will create vast amounts of data that will need to be processed. For manufacturers, post-sale service or warranties can be continuously tracked in real-time using machine-to-machine sensors to identify malfunctions or warranty issues. Real-time promotions can be sent by analyzing sensor data and customers' buying preferences.

These newfound capabilities made available across industries will not only increase the amount of data, but also significantly increase the demand for business intelligence. It's important to think about the backend implications this will present to the network.

The sheer volume of data will increase the drive toward a cloud-based data center as moving data efficiently to the cloud and extracting intelligence become very critical tasks.

Agile networking

The IoT will impact everyone at the professional and individual levels; whole industries will leverage the availability of sensors and machine-to-machine communication. In agriculture, irrigation systems will function based on a multitude of inputs, including weather forecasts

and data from moisture sensors. Manufacturing plants will be totally wired on sensor networks, as will oil drilling equipment. Drilling times will be reduced by the use of advanced analytics that can predict conditions and improve operation based on previous events.

The sheer volume of data created by the IoT will have unfathomable impact on the networking systems used today. Deep analytics will require distributed datacenters and real-time response to events. Fast, agile networks are crucial to enable the real-time analysis of sensor data. Given these requirements, it is very unlikely that today's networks will stand up to the demands of 2020.

As a potential solution, even software-defined networking only begins to address some of these needs in the cloud data center. However, it's a strong start in the right direction.

Security

Hyper-connectivity will threaten the individual in more ways than currently acknowledged. We need to think about how to protect against inevitable threats to the system. Power grids will be more efficient, and consumer interactions such as net metering will drive the integration of operational technology (OT) and information technology (IT).

However, the integration of OT and IT opens the door for external threats. Cars will be able to drive themselves, controlled by applications. Having your networked garage recognize whether or not your car is in the garage is useful, but it also creates opportunity for hackers. Businesses and homes will become increasingly targeted and hackable. It's important that the networking industry works now to ensure security within these networks of tomorrow.

The Internet of Things represents huge changes underway across all industries. As sensors become more common in the home and at work, it's easy to imagine a future overtaken by connected objects and devices and a network that is unprepared for it. We need to think proactively about our role as an industry and start solving today the problems of a not-too-distant tomorrow.

Structural Models

The expected flood of data from billions of connected devices is raising many challenges for how IoT solutions will be architected. Common design paradigms from device-to-cloud will allow more flexibility on how compute will best be utilised for data analytics. A big challenge is where do we place data analytics: on device, at the edge, or in the cloud?

Just what role does data analytics play in the Internet of Things? Whilst there is no single definition of IoT, it is good to define IoT from a Data Analytics (DA) perspective – "Applying algorithms to data from smart devices that leads to process (industrial IoT)

and life (consumer IoT) optimisation." IoT is the train that data analytics was waiting all these years for. Billions of devices producing data. A marriage made in heaven.

Where the Challenges Lie

Two frequent problem statements from developers working on data analytics use cases in IoT are 1: "I can't place any analytics on the device or gateway as it just doesn't have the resources to cope with the amount of data," and 2: "How do we store and process all the data?"

Looking at 1, if developers could look to classify the data into two buckets at edge and device, namely (1) use now data and (2) use later data, then it can begin to perform local data reduction by pre analytics. This will ensure we can minimise data storage and transfer rates, and free up compute for device based analytics.

Looking at 2, the first step for any data scientist af ter getting a data set is to cleanse it. This by its very existence should suggest that we don't need all the data to make the decision required for business impact, as there is still a lot of junk data being generated by these IoT devices.

Introducing Haze Computing

IoT edge gateways are now an essential part of IoT applications. But where does the edge begin and end? Compute exists right from the devices all the way to cloud, so why should the gateway be treated any differently? In fact, in lots of cases the pooled compute of the devices that are connected to the gateway can exceed what is available at the edge gateway. The challenge is how devices are configured in Machine to Machine (M2M). It is predicted here that the classic gateway will be squeezed from above by cloud and below from devices, and it may become distributed by design.

What is being proposed here is to create a dynamic model for your analytics applications, which I name presently as Haze Computing (named due to coverage from device to cloud), where you begin with a pooled view of your resources. Each DA app that you build analyses the local and global compute available to it across cloud, edge and device(s), and the haze data management controllers (DMC) aggregate and design how and where analytics take place in a dynamic fashion.

By being a little more clever at the data source, one can both reduce the amount of data being kept locally and pushed to cloud by designing a data consistency aware messaging service from cloud to device that serves a series of DMC that are in sync and take control over other messaging communication for IoT. Each IoT application for a single device would have its

own cloud DMC, device DMC and edge DMC. Their purpose is to manage the data's 3V's (velocity, volume, variety) and the application of analytics apps on the data stream at predefined intervals. Having this type of architecture will ensure you can scale your applications and services across cloud, edge, and device.

Security

The single view per IoT application ensures that security can be better managed across device, edge, and cloud. Security and privacy are still the main concerns for IoT practitioners across the industry. Applying a more holistic architecture design makes implementing next generation security topologies much easier. One such topology is blockchain, of bit coin fame. If you consider that the cloud application can act as the parent blockchain that can spawn multiple sidechains at the edge, which can in turn manage device based sidechains, then you can create a security ecosystem that is automatic, based on consensus, and fully auditable.

Energy Efficiency

If developers can become more conscious and implement green computing paradigms at the haze level, where energy usage rates are much more visible, then best practices can be designed and built much easier. Normally the more data we have to process, store, and transfer means the more energy that will be consumed. This architecture ensures you can reduce the energy use as each DMC acts as a data filter point.

Reduce Complexity

It is common for developers to be slightly behind in where the trends are within the IoT landscape. One main reason for this is normally we have experts in one of the areas required to build full breadth IoT applications, and there are a myriad of technologies with various design practices that are not in sync. This architecture will allow developers to eliminate design chasms across edge, device and cloud, and introduce simplicity in IoT standards being driven by the IIC and OPC.

Cascading Behavior in Networks

Cascading hubs is a term that describes the action of adding additional physical ports when an existing hub or switch has run out of physical connections. To do this, a new hub or switch is connected to an existing hub or switch uplink portusing a network (Cat 5) cable.
When people are connected by a network, it becomes possible for them to influence each other's behavior and decisions. This basic principle gives rise to a range of social processes

in} which networks serve to aggregate individual behavior and produce population-wide, collective outcomes.

There are many settings in which it may be rational for an individual to imitate the choice of others Two distinct reasons can be identified:} Information effects} choices made by others can provide information about what they know} Direct-benefit effects} there are direct benefits from copying the decisions of others} Information effects may entail making choice contrary to one's own} information Example: restaurant choice} This results in a phenomenon called herding or information cascade} Information cascade has the potential to occur when people make} decisions sequentially, with later people watching the actions of earlier people and making inferences.

Diffusion in Networks

When we model processes by which new ideas and innovations are adopted by a population, the underlying social network can be considered at two conceptually very different levels of resolution: Network viewed as a relatively amorphous population of} individuals and look at effects in aggregate Look closer at the fine structure of the network and consider how} individual nodes are influenced by their network neighbors The second view addresses a number of phenomena that cannot be} modeled well at the level of homogenous populations.

Cascading behavior

In any network, there are two obvious equilibria to the} network-wide coordination game:

Everyone adopts A

Everyone adopts B

We want to understand: How easy it is to "tip" the network from one of these equilibra} to the other.

What other intermediate equilibria look like (states of coexistence where A is adopted in some parts of the network and B is adopted in others.)

The Small-World Phenomenon

The small-world phenomenon -- the principle that we are all linked by short chains of acquaintances, or "six degrees of separation" -- is a fundamental issue in social networks; it is a basic statement about the abundance of short paths in a graph whose nodes are people, with links joining pairs who know one another. It is also a topic on which the feedback between social, mathematical, and computational issues has been particularly fluid.

The problem has its roots in experiments performed by the social psychologist Stanley Milgram in the 1960s; to trace out short paths through the social network of the United States, he asked participants to forward a letter to a "target person" living near Boston, with the restriction that each participant could advance the letter only by forwarding it to a single

acquaintance. Milgram found that the median completed chain length was six. Why should a social network contain such short paths?

Working much more recently, applied mathematicians Duncan Watts and Steve Strogatz proposed thinking about networks with this small-world property as a superposition: a highly clustered sub-network consisting of the "local acquaintances" of nodes, together with a collection of random long-range shortcuts that help produce short paths.

In addition to empirical studies of social, technological, and biological networks, Watts and Strogatz considered the following simple model system: Start with a *d*-dimensional lattice network, and add a small number of long-range links out of each node, to destinations chosen uniformly at random. A network created by this superposition will have local clustering and short paths, just like many of the networks found in the real world. (See Figures 1 and 2.)

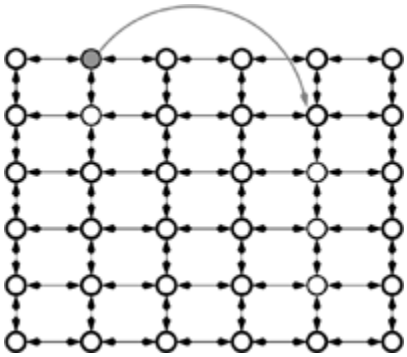


Figure 1. Two-dimensional grid with a single random shortcut superimposed.

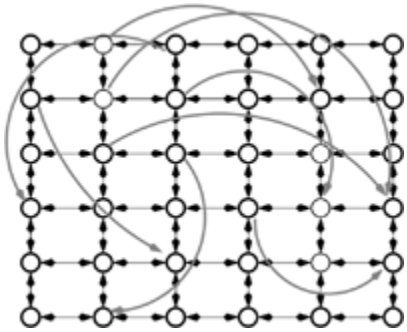


Figure 2. Two-dimensional grid with many random shortcuts superimposed (as in the Watts-Strogatz model).

But Milgram's experiment really led to two striking discoveries, of which the existence of short paths was only the first. The second was that people in society, with knowledge of only their own personal acquaintances, were collectively able to forward the letter to a distant target so quickly. Viewed in computational terms, this is a statement about the power of a routing algorithm, equipped with purely local information, to find efficient paths to a

destination; that such a decentralized routing scheme is effective says something striking about the underlying social network.

Modeling this aspect of the small-world phenomenon poses further challenges: Can we find model systems for which it can be proved that Milgram-style decentralized routing will produce short paths? Here, mathematical analysis of the Watts-Strogatz model and its variants yields some surprises. For one, it is possible to prove that in the model of a *d*-dimensional lattice with uniformly random shortcuts, no decentralized algorithm can find short paths; this, then, is a concrete example of a network in which short paths exist, but local knowledge does not suffice to construct them.

Exploring further, though, we find that a subtle variant of the Watts-Strogatz network will in fact support efficient search: Rather than adding the long-range shortcuts uniformly at random, we add links between nodes of this network with a probability that decays like the *d*th power of their distance (in *d* dimensions). Moreover, this is the only link distribution of this form for which efficient search is possible. The intuition here is that a probability decaying like the dth power of the distance is in fact uniform over all "distance scales" -- a node is roughly as likely to form links at distances 1 to 10 as it is at distances 10 to 100, 100 to 1000, and so on. (See Figure 3.)

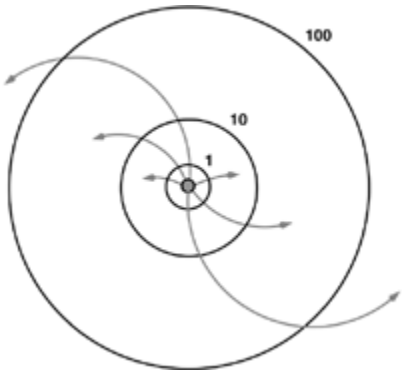


Figure 3. A node with several random shortcuts spanning different distance scales.

The ability to construct a searchable network in this way, with long-range links whose probabilities decay with distance, has proved useful in the design of peer-to-peer file-sharing systems on the Internet, where content must be found by nodes consulting one another in a decentralized fashion. In other words, nodes executing these look-up protocols are behaving very much like participants in the Milgram experiments -- a striking illustration of the way in which the computational and social sciences can inform one another, and the way in which mathematical models in the computational world turn into design principles with remarkable ease.

Karpagam Academy of Higher Education
Dept of CS
Subject: Internet of Things
Class: I M.Sc (CS) Multiple Choice Questions
UNIT-4

sno	Questions	opt1	opt2	opt3	opt4	Answer
1	What is pipe lining?	a) Non linear	b) Linear	c) Linear and Non linear	d) Sometimes both	b) Linear
2	Using what the processor wake-up from power-down?	a) External Interrupts	b) Internal interrupts	c) Serial Programming	d) Program Counter	a) External Interrupts
3	What is the size of ADC and DAC?	a) 16 bit	b) 10 bit	c) 8 bit	d) 32 bit	b) 10 bit
4	How many processors are used in the Instruction pipelining?	a) One	b) Two	c) Three	d) Four	a) One
5	The ARM7TDMI-S uses which pipelining?	a) 2-Stage	b) 3-Stage	c) 4-Stage	d) 5-Stage	b) 3-Stage
6	Arduino shields are also called as _____	a) Extra peripherals	b) Add on modules	c) Connectivity modules	d) Another Arduinos	b) Add on modules
7	Which is the software or a programming language used for controlling of Arduino?	a) Assembly Language	b) C Languages	c) JAVA	d) Any Language	d) Any Language
8	_____ are pre built circuit boards that fit on top of Android.	a) Sensor	b) Data types	c) Breadboard	d) Sheilds	d) Sheilds
9	_____ is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission	IPv6	IPv4	IPv5	IPv7	IPv6
10	_____ protocol provides communications privacy for datagram protocols.	FTP	DTLS	SMTP	POP	DTLS

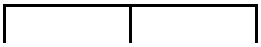
11	_____ Resolves host names to IP addresses within small networks that do not include a local name server.	DTLS	SMTP	IPv6	mDNS	mDNS
12	_____ is an application layer protocol that is intended for use in resource-constrained internet devices	CoAP	MQTT-SN	MQTT	IPv4	CoAP
13	A _____ is a C-based CoAP stack which is suitable for embedded environments.	SMTP	SMCP	DTLS	IPv6	SMCP
14	The first open international middleware standard directly addressing publish-subscribe communications is	DDS	AMQP	LLAP	JMS	DDS
15	_____ open source software framework that makes it easy for devices and apps to discover and communicate with each other.	IPSO	OMA	Alljoyn	IEEE P2413	Alljoyn
16	_____ is to manage security configuration in a Trusted Execution Environment	OTrP	X.509	CoAP	MQTT	OTrP
17	_____ systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.	SMCP	SCADA	DTLS	MQTT-SN	SCADA
18	SCADA systems were first used in _____	1960s	1980s	1970s	1950s	1960s
19	_____ contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.	Level 0	Level 1	Level 2	Level 3	Level 0

20	_____ contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors.	Level 0	Level 1	Level 2	Level 3	Level 1
21	_____ contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.	Level 0	Level 1	Level 2	Level 3	Level 2
22	_____ is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.	Level 0	Level 1	Level 2	Level 3	Level 3
23	_____ is the production scheduling level	Level 4	Level 1	Level 2	Level 3	Level 4
24	____ uses electromagnetic fields to automatically identify and track tags attached to objects.	DTLS	RFID	IPv5	X.509	RFID
25	A radio-frequency identification system uses	tags	active	reader	progress	tags
26	_____ has a small battery on board and is activated when in the presence of an RFID reader.	BAP	ISO/IEC 18000	ISO/IEC 29167	ISO/IEC 20248	BAP
27	CCN stands for _____.	Content-concentric Networking	Content-Centric Networking	Content-Centric	Centric-Centric Networking	Content-Centric Networking
28	TSMP stands for _____.	Time Synchronized Mesh Protocol	Transport Synchronized Mesh Protocol	Time Sequence Mesh Protocol	Time Synchronized Mass Protocol	Time Synchronized Mesh Protocol

29	DNS stands for _____.	Data Name System	Domain Name Server	Domain Name System	Domain Name Service	Domain Name System
30	An open, lightweight JSON-based hypermedia catalogue format is	HyperCat	UPnP	MQTT	Telemetry	HyperCat
31	_____ is an application layer protocol that is intended for use in resource-constrained internet devices	MQTT-SN	IBM	CoAP	HTTP	CoAP
32	_____ protocol enables a publish/subscribe messaging model in an extremely lightweight way.	IBM	CoAP	HTTP	MQTT	MQTT
33	_____ enables you to see a list of URLs being broadcast by objects in the environment	CoAP	HTTP	MQTT	Physical Web	Physical Web
34	_____ is a C-based CoAP stack which is suitable for embedded environments	SMCP	IBM	CoAP	HTTP	SMCP
35	_____ is an open standard application layer protocol for message-oriented middleware	IBM	AMQP	MQTT	Telemetry	AMQP
36	_____ is directly addressing publish-subscribe communications for real-time and embedded systems	CoAP	DDS	HyperCat	UPnP	DDS
37	_____ API is for sending messages between two or more clients.	JMS	MQTT-SN	IBM	CoAP	JMS
38	_____ is a simple short message that is sent between inteligent objects using normal text	CoAP	HTTP	LLAP	IBM	LLAP
39	_____ is a simple communications protocol designed for data transfer between computers	IBM	SSI	CoAP	DDS	SSI

40	An open source software framework that makes it easy for devices and apps to discover and communicate with each other.	IBM	CoAP	IEEE P2413	Alljoyn	Alljoyn
41	A protocol to install, update, and delete applications and to manage security configuration	OTrP	DDS	HyperCat	UPnP	OTrP
42	Standard for public key infrastructure (PKI) to manage digital certificates	MQTT-SN	IBM	X.509	Telehash	X.509
43	_____ systems are used to monitor and control a plant or equipment in industries.	SCADA	HMI	M2M	DDS	SCADA
44	_____ contains the field devices such as flow and temperature sensors	Level 1	Level 0	Level 2	Level 3	Level 0
45	_____ contains the industrialised input/output (I/O) modules	Level 1	Level 0	Level 2	Level 3	Level 1
46	_____ contains the supervisory computers, which collate information	Level 1	Level 0	Level 2	Level 3	Level 2
47	_____ is the production control level, which does not directly control the process	Level 1	Level 0	Level 2	Level 3	Level 3
48	_____ is the production scheduling level.	Level 1	Level 0	Level 2	Level 4	Level 4
49	_____ uses electromagnetic fields to automatically identify and track tags attached to objects.	RFID	SCADA	HMI	M2M	RFID

50	_____ part includes the form and design of the products	Connectivity	Platform	Business Model	Killer Applications	Platform
51	_____ phase includes all parts of the consumer's day and night routine	Connectivity	Platform	Business Model	Killer Applications	Connectivity
52	_____ is a big motivation for starting, investing in, and operating any business	Connectivity	Platform	Business Model	Killer Applications	Business Model



UNIT V

SYLLABUS

Applications: 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. Applications - Smart Grid – Electrical Vehicle Charging - Case studies: Sensor body-area-network and Control of a smart home.

Collaborative Production Environments

Market structures underlie a continuous process of change, caused by innovations of enterprises, technical improvements, new market participants, amendments, or changes in society's values. The concerned enterprises need to react to these changes and need to adapt their services and products in a quick and adequate manner in accordance with the new market conditions. The rate of market changes grew steadily over the previous decades, especially due to the improvement as well as the development of existing and new information and communication technologies (ICT).

Fulfilling the demands of the market is a bigger challenge than ever before – within very small time intervals a market can change fundamentally. The automotive industry can serve as an example: within a few years the demand for powerful and fast cars has decreased significantly, while the customers' sensitivity for ecological fuel-saving cars has increased noticeably – that was much faster than the leading automakers had expected and taken into account within their product ranges and corporate structures

The Internet of Things underlies different definitions, but mainly the term describes the increasing interconnectedness of electronic devices, using a common information infrastructure. Sometimes the Internet of Things is depicted as an unclear vision of unknown technologies; but it is neither a future vision, which is far away like a utopia, nor a technological breakthrough, like the invention of the radio or television was; it is a realistic prediction of the future convergence of present technological developments, the infrastructural expansion and the general trend of ubiquitous online accessibility.

The future Internet of Things will use protocols and algorithms which will be based on those we use in the Internet today; it will just extend the capabilities of a more extensive machine-to-machine and human-to-machine communication, resulting in a higher number of

specialised communication participants within the Internet. Autonomous objects are objects which are equipped with intelligence (small central processing units (CPUs) and algorithms) to be capable of making contextual routing decisions or handling activities. Both, the Internet of Things concepts and the autonomous objects, are complementary.

The Internet of Things acts as an infrastructure and helps to realise the new systemic characteristics of autonomy and agility by providing object-oriented information architecture for precise real-time data and ubiquitous Internet access. When applying the described concepts consequently, several existing paradigms of production environments are affected. Paradigms like "Just in Time" are no longer applicable, for instance. Most of the existing paradigms have in common that they require deterministic environments. Introducing a high degree of freedom leads to non-deterministic environments and, as a result, state-of the-art methods have to be extended.

This contribution investigates the suitability and cooperation of the Internet of Things and autonomous objects for autonomic and agile processes in collaborative production environments. Automotive supply chains are typical collaborative production environments, in which different companies participate in producing a final product. Hence, varying the product range or changing the corporate structure of a central supply chain member, like automakers, always affects the processes and structures of its supply chain partners. The transmission of the need for changes from partner to partner and the detection of the individual modifications in processes and structures require a long time.

Thus, an improvement of the network-wide reaction time offers a high potential to save and to strengthen the market position. To reduce the time gap between the detection of change and the necessary adjustments in production, it is necessary to find technologies and methods which enable the production networks to react autonomously for developing an agile supply chain coordination design.

Resource Management in the Internet of Things: Clustering

Techniques like clustering, software agents and synchronisation are used in order to overcome the challenges of managing the resources of the Internet of Things objects. Clustering is beneficial to reduce the energy expenditure and improve the scalability and robustness of the object networks. IoT objects are grouped into clusters in order to overcome scalability, energy efficiency and robustness issues. Clustering allows of Wireless Sensing Networks to be more hierarchical.

Clustering is the concept where your IOT devices are linked to a gateway in a particular area. This is opposed to the use of "meshing" technology whereby the devices are interconnected and communicate with each other and spread out the "signal" that way. Clustering is argued as more reliable method of communications as it requires less power than Meshing and will not be let down necessarily by a group of IOT devices. It is similar to the concept of Star Distribution vs interconnection. It uses a hub in each geographical area meaning that there is

a single point of failure and the hub or gateway can communicate where the issue is when your IOT devices fail.

Everyone, from consumers to corporates, is embracing the changes brought by the revolution called the Internet of Things (IoT). It has changed the world in more ways than we could imagine until a few years back. And the changes and advancements will continue in future as well, in fact, Internet of Things (IoT) will shape our future. Already the numbers are staggering; billions of sensors connected with billions of devices are redefining almost everything under the sun. It is estimated that around 75 Billion devices will be interconnected by 2025.

Around $6 Trillion is estimated to be spent on the Internet of Things (IoT) solutions in the next five years. No price for guessing that the reason this amount is expected to be spent on IoT is that IoT has already shown a lot of potential in a very short time and it has just begun. There is not a single industry that is not impacted by IoT by now. Some have already had a major influence of IoT while some are just beginning to realise its importance.

Retail companies are investing heavily in IoT as they understand the importance of data-driven analytics and also to further improve customer experience. Customers, on the other hand, are enjoying the new experiences made possible because of IoT. Data-driven analytics based on the data gathered from billions of sensors to reach the potential customers and for better marketing will be very common in 2018. Although in very early stages, Amazon's drone delivery system is completely powered by IoT and is expected to be a ground-breaking innovation.

IoT is reshaping healthcare as well. Wearable technology to monitor your condition at any time and anywhere is very common now. Sensors are collecting data and at the same time, the data can be visible to doctors. This is helping doctors closely monitor crucial patients from far away.

The manufacturing industry is making use of smart machines to improve the overall manufacturing process and to produce better goods. IoT has something to offer to everyone, it has completely changed the way we used to do business, socialize and have fun

Synchronization and Software Agents

The metaphor of "intelligent software agents" as basic building blocks for the development of new generation intelligent software systems triggered both theoretical and experimental computer science research aiming to develop new programming languages for agent systems. In our opinion, the main achievement of this trend of research was the development of new programming models that address both the basic features of agenthood (autonomy, reactivity, proactivity and social abilities) as well as more advanced, human-like features usually collectively coined in the agent literature as "mental attitudes" (beliefs, desires, intentions, commitments), following the model of "intentional systems" introduced by the philosopher Daniel Dennett in 1971 to explain behavior of rational agents.

Agent oriented technologies, engineering of agent systems, agent languages, development tools and methodologies are an active and emergent research area and agent development is getting more and more interesting. There are many approaches, theories, languages, toolkits, and platforms of different quality and maturity which could be applied in different domains. Our motivation and the main goal of the paper are to bring a survey in the field of agent technology and to cover different aspects of agents.

Agents, agent-oriented programming (AOP), and multi-agent systems (MAS) introduce new and unconventional concepts and ideas. Still, there is a number of definitions of the term 'agent' that include a property common to all agents: agent acts on behalf of its user, as well as a lot of additional properties: agent communicates with other agents in a multi-agent system; acts autonomously; is intelligent; learns from experience; acts proactively as well as reactively; is modeled and/or programmed using human-like features (beliefs, intentions, goals, actions, etc.); is mobile, and so on.

Applications - Smart Grid

Fault Detection

Traditionally, electric utilities have largely relied on faulted circuit indicators (FCIs) to detect and locate outages within their systems. This approach has its roots in what is now considered aging technology. These older grid systems have fallen behind in large part because they were only updated every few decades. As a result, the electric utility industry is built on an infrastructure dominated by legacy and proprietary systems.

Modern telecommunication technologies have evolved to open standards-based paradigms that facilitate moving to a modern smart grid. Standards-based protocols and platforms help the grid stay up to date with software updates instead of sending field service crew to change hardware.

The Gateway

Fault detection sensors are used on existing grid infrastructure. They're designed to indicate and locate both permanent and momentary faults accurately and reliably. Many of them have 3G. Some even have LPAN radios built into them for communication. As the 3G network sunsets, the fault sensor can continue to operate until the end of its life with an IoT gateway.

The gateway allows the sensor to connect via Bluetooth Low-Energy (BLE) and then transport data over the grid's cellular network. The newly-smart fault sensor then continues to help electric utilities improve reliability while reducing operating and maintenance costs.

Making a Smart Grid IoT Application

Connecting legacy equipment to smart grid IoT applications allows electric utilities to:

- **Push Data in Real Time –** Relying on centralized polling of data causes significant latency and limited ability to scale. Many IIoT gateways poll data locally and create data models that can communicate with traditional SCADA systems as well as cloud-based platforms to take advantage of modern web services.
- **Leverage Cellular Infrastructure –** IIoT gateways allow grid monitoring devices to take advantage of cellular connectivity, forming secure connections with multiple backends or cloud systems.
- **Enhance Sensing with Low Power Sensors –** IIoT gateways can convert LPWAN sensor data from legacy protocols such as DNP3 or newer cloud protocols.
- **Leverage the Cloud –** As distributed grids become increasingly complex with many more devices to manage, IIoT gateways are able to connect to cloud-based infrastructure and share real-time data and analytics with users through cloud-managed dashboards.
- **Enhanced Grid Security –** Legacy grid monitoring systems (when IP-networked) are vulnerable to cyber attacks. They lack robust cybersecurity capabilities because the legacy protocols were not designed with modern threats in mind. IIoT gateways can minimize security risks using the latest security methodologies and update and patch security features to adapt to ever-changing cybersecurity threats.

Electrical Vehicle Charging

Two key technologies which will transform our future energy systems are IoT-enabled smart grids and advancements in battery storage. Together, they will help to improve energy distribution and storage in smart cities.

The installation of smart grids, enabled by the IoT, will change the way energy is distributed and consumed. Powered by demand-response systems, which allow for real-time monitoring of customer requests, smart grids can autonomously react to energy supply and demand.

Smart grids can also adjust the distribution of energy, controlling demand more efficiently and sharing it more effectively. Smart meters, which are currently being installed in urban buildings across the globe, will support this change by autonomously

reporting customer demands to suppliers, who in turn can react and optimize how much energy is required.

In parallel to the development of smart grids is the creation and implementation of battery storage. A vital part of a renewable energy system, batteries help manage energy supply and demand by storing generated energy until it is required for use, thus avoiding waste. Battery storage technology, such as Hitachi's CrystEna facilitator, is improving rapidly and is able to regulate how much energy is used.

Many governments and businesses have begun to implement smart energy systems using renewable energy. As part of the Smart Energy Islands project, Hitachi has partnered with the EU and the main stakeholders on the Isles of Scilly – including the council, local businesses, the Duchy of Cornwall and Tresco Island – to create a smart energy system using the IoT.

The programme is investigating whether renewable technology, such as solar panels and batteries, can be used more efficiently by connecting to smart energy systems via an IoT platform. Hitachi is involved in the development and management of the supply, storage and demand of electricity in this partnership and its work aims to help reduce the price of energy on the Isles of Scilly by 40 per cent. This Smart Islands Partnership has begun testing its research on a smaller energy capacity, in the hope that it can be scaled up and impact larger areas, such as cities.

The installation of this technology demonstrates that by harnessing the power of data, new energy technology can provide cities with a more efficient and cleaner energy system.

SMARTER ENERGY USAGE

Transport is the largest energy consuming sector in the UK, representing 40 per cent of total energy consumption in 2016 and making it a vital component in the drive to make energy smarter. For city dwellers, concerns about pollution, congestion and the cost of transport are high on the priority list.

Here, smart technology can have a positive impact with the development of electric vehicles (EVs), their charging points and connected vehicles. In fact, the International Energy Agency predicts that there could be between 40 million and 70 million EVs on the roads by 2025. If these figures prove to be correct, there will undoubtedly be a reduction in the level of carbon-intensive fumes in our densely populated cities.

However, EV charging depends on the efficient distribution of energy. Smart grids, in conjunction with charging infrastructure, therefore play a key role in smart cities' future. Consequently, we have seen an increase in the amount of EV infrastructure investment. France is currently leading the way in Europe, installing 11,987 charging points in the past year with numbers set to grow. By running on electricity distributed from smart grids, EVs will also develop a second purpose as batteries. When fully charged and linked to buildings, the cars would release energy back from their internal storage.

There are further exciting opportunities for transport in the area of efficiency. With more than 50 billion IoT-enabled devices expected by 2025, Vehicle to Everything systems will link our vehicles to related infrastructure – such as traffic lights and public transport timetables – increasing the level of control authorities will have over traffic. It is predicted that this technology will reduce emissions by 10 per cent, primarily through reduced congestion and, therefore, the time vehicles spend idling.

To solve the issues raised by greater demand in energy, smart tech is providing targeted solutions to make city energy systems cleaner and efficient. The impact of big data and smart tech has reached beyond energy systems to our transport links and is predicted to continue to grow, solving the wider societal issues of our future cities, too.

Karpagam Academy of Higher Education
Dept of CS
Subject: Internet of Things
Class: I M.Sc (CS) Multiple Choice Questions
UNIT-5

sno	Questions	opt1	opt2	opt3	opt4	Answer
1	A Java Message Oriented Middleware API for sending messages between two or more clients.	a)Java Message Service	b)Java Development kit	c)Java Middleware Service	d)Java Development Environment	a)Java Message Service
2	Standard for public key infrastructure (PKI) to manage digital certificates and public-key encryption	a)X.504	b)X.509	c)X.507	d)X.502	b)X.509
3	A computer system for gathering and analyzing real time data	a)SCADA	b)RFID	c)M2M	d)RTU	a)SCADA
4	Radio-frequency identification (RFID) uses _____ fields to automatically identify and track tags attached to objects.	a)magnetic	b)electromagnetic	c)radio waves	d)neutron	b)electromagnetic
5	_____is one method for Automatic Identification and Data Capture (AIDC)	a)SCADA	b)RFID	c)M2M	d)RTU	b)RFID
6	what is W3C?	a)World Wide Web count	b)World Wide Web Consortium	c)World Wide Web Control	d)World Wide Web Console	b)World Wide Web Consortium
7	Which can be affixed to an object and used to track and manage inventory, assets, people, etc.	a)RFID tag	b)GPS	c)IC	d)Camera	a)RFID tag
8	IOT needs _____,but M2M don't need IOT	a)M2M	b)RFID	c)SCADA	d)Modbus	a)M2M

9	which is data communication protocol for automtion and conrol networks.	a)CIAP	b)TCP	c)BACNET	d)IMAP	c)BACNET
10	When the two computers connected directly and is also known as RFC1661	a)UDP	b)TCP/IP	c)machine to machine protocol	d)point to point protocol	d)point to point protocol
11	which protocol is mainly used for providing industrial solutions?	a)LAN	b)Ethernet	c)VPN	d)WAN	b)Ethernet
12	which is used by email clients to retrieve email messages from a mail server.	a)BACNET	b)IMAP	c)CIAP	d)SMTP	c)CIAP
13	which architecture enables user to send and receive emails through server without any devices.	a)CIAP	b)SMTP	c)IMAP	d)BACNET	c)IMAP
14	this technology is used for manufacturing and industrial settings	a)Iot	b)M2M	c)WOT	d)RFID	b)M2M
15	This is serial communication protocol used with PLC.	a)M2M	b)IMAP	c)Modbus	d)RFID	c)Modbus
16	how many varients in KNX protocol?	a)4	b)6	c)1	d)3	d)3
17	which architecture is most suitable for embedded applications?	a)ZigBee	b)M2M	c)BACNET	d)Bluetooth	a)ZigBee
18	which is not a part of zigbee architecture?	a)coordinator	b)routers	c)end devices	d)security system	d)security system
19	How many layers in zigbee architecture?	a)7	b)6	c)4	d)5	d)5
20	collection of software and hardware elements used or supervisory and data acquisition	a)BACNET	b)SCADA	c)RFID	d)IOT	b)SCADA
21	protocols are divided into how many layers?	a)7	b)8	c)6	d)5	b)8
22	Web of Things relies exclusively on _____ level protocols and tools.	a)network	b)presentation	c)data link	d)application	d)application
23	which is only relies on the application level protocols and tools.	a)IOT	b)WOT	c)web	d)internet	b)WOT

24	Which is only deals with the highest OSI Layer (7), which handles applications, services and data.	a)web of things	b)internet of things	c)HTTP	d)web sockets	a)web of things
25	which has the ability to use modern Web standards directly on embedded devices.	a)wot	b)iot	c)web	d)internet	a)wot
26	WoT architecture is an attempt to structure the galaxy of _____ protocols and tools into a useful framework for connecting any device or object to the Web	a)internet	b)standard	c)web	d)IT	c)web
27	The WoT architecture stack is not composed of _____ in the strict sense	a)sessions	b)layers	c)protocols	d)hierarchy	b)layers
28	In WOT architecture which is not a layer in following	a)find	b)access	c)session	d)share	c)session
29	Which layer ensures that your Thing can not only be easily used by other HTTP clients but can also be findable and automatically usable by other WoT applications.	a)access	b)find	c)share	d)compose	b)find
30	Which layer is responsible for turning any Thing into a Web Thing?	a)find	b)share	c)access	d)compose	c)access
31	which layer specifies how the data generated by Things can be shared in an efficient and secure manner over the web	a)find	b)share	c)access	d)compose	b)share
32	ICT stands for	information and communication technologies	interpretation and communication technologies	information and consolidation technologies	information and communication transport	information and communication technologies
33	_____overcomes the challenges of managing the resources of the Internet of Things objects	Remote	clustering	Accessing	Platform	clustering

34	Clustering is the concept where your IOT devices are linked to a _____	System	Machine	gateway	Software	gateway
35	Clustering is argued as more reliable method of communications as it requires less power than _____	Meshing	b)access	b)layers	c)session	Meshing
36	AOP stands for _____	access-oriented programming	aquire-oriented programming	application-oriented programming	agent-oriented programming	agent-oriented programming
37	MAS stands for _____	multi-agent systems	multi-access systems	multi-app systems	multi-application systems	multi-agent systems
38	FCI stands for _____	false circuit indicators	faulted circuit inspections	faulted circuit indicators	faulted circumference indicators	faulted circuit indicators
39	BLE stands for _____	Bluetooth Low-Energy	Bluetooth Light-Energy	Bluetooth Low-Efficient	Bandwidth Low-Energy	Bluetooth Low-Energy
40	_____ allows the sensor to connect via BLE and then transport data over the grid's cellular network.	gateway	clustering	Platform	clustering	gateway
41	_____ isrelying on centralized polling of data causes significant latency and limited ability to scale.	multi-access systems	Push Data in Real Time	multi-application systems	access-oriented programming	Push Data in Real Time
42	Legacy grid monitoring systems (when IP-networked) are vulnerable to cyber attacks is dealt with _____.	Enhanced Grid Security	faulted circuit inspections	multi-app systems	access-oriented programming	Enhanced Grid Security
43	In _____ people observe the of choices of others and make their own decisions based on that observation	information security	b)World Wide Web Consortium	information cascade	c)M2M	information cascade
44	Information cascades are generally very brittle by nature, as individuals may be reacting only to hearsay and public observation is called:	Accessibility	Fragility	b)standard	clustering	Fragility

45	OT stands for _____	operations technology	operation technique	operational technology	operational transmission	operational technology
46	DA stands for _____	Design Analytics	Detailed Analytics	Data Analogy	Data Analytics	Data Analytics
47	DMC stands for _____	design management controllers	data management controllers	data maintain controllers	data management consortium	data management controllers
48	_____ layer is responsible for turning any Thing into a Web Thing	share	maintain	Access	find	Access
49	_____layer ensures that your Thing can not only be easily used by other HTTP clients.	share	maintain	Access	find	find
50	_____ connects different, often complex and already existing programs that were not originally designed to be connected.	Middleware	Fragility	standard	clustering	Middleware
51	____ is the contract between applications and the runtime system of a Servient, the so-called WoT Runtime.	WoT Web	WoT Runtime	WoT machine	WoT Scripting API	WoT Scripting API
52	_____ are implementations of the Binding Templates.	Protocol Bindings	System	System App	API	Protocol Bindings
53	_____ comprises the strategies and technologies used by enterprises for the data analysis of business information.	clustering	Business intelligence	c)RFID	d)IOT	Business intelligence
54	_____ is a network based computational model that has the ability to process large volumes of data	Grid computing	system computing	machine computing	computing	Grid computing