Roll No ....

CS-6005 (1) (CBGS)

B.E. VI Semester

Examination, May 2019

Choice Based Grading System (CBGS)

Internet of Things

Time : Three Hours

Maximum Marks : 70

Note: i) Attempt any five questions

ii) All questions carry equal marks.

1. a) Discuss area of development and standardization in Internet of things.

   b) Write in detail application of Internet of things.

2. What is Network Function Virtualization (NFV) based architecture to address connectivity and interoperability challenges in Internet of things?

3. a) What issues might affect the development and implementation of the IoT?

   b) Explain data storage in IoT.

4. a) What is IP Addressing? Why IPv6 are required to implement the concept of IoT?

   b) Explain media access control.

5. Explain following term
   i) Industrial and Automotive IoT
   ii) Wireless sensor network technology

6. a) Discuss the security and privacy issues in IoT.
   b) Discuss the role of sensors in IoT. Explain various types of sensors.

7. Discuss any one case study of IoT in detail.

8. Write a short notes (any two)
   a) RFID
   b) Web sockets
   c) M2M

******

Q. No.1 a) Discuss area of development and standardization in Internet of Things

Ans:

IoT(Internet of Things):

The Internet of Things (IoT) is the network of "things" or smart devices embedded with sensing, actuation, software, and network connectivity to sense and exchange data among the things, between the things, and with the outside world. The term IoT was coined in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors without requiring human intervention. Though the things were initially thought as machines, today, things are synonymous with any living entity including the human beings, animals, and any other device or element on earth. The "things" should not only be addressable but also reconfigurable, reusable, locatable, uniquely identifiable, and remotely controllable

Area of development:

The Internet of Things (IoT) is an emerging area of the modern technology which impacts use cases across governance, education, business, manufacturing, entertainment, transportation, infrastructures, health care, and so on. IoT promises an interconnected network of uniquely identifiable smart objects. This infrastructure creates the necessary backbone for many interesting applications that require seamless connectivity and addressability between their components. The range of IoT application domain is wide and encapsulates applications from home automation to more sophisticated environments, such as smart cities and e-government. Industry-focused applications include logistics and transportation, supply-chain management, fleet management, aviation industry, and enterprise automation systems. Healthcare systems, smart cities and buildings, social IoT, and smart shopping are a few examples of applications that try to improve the daily life of individuals, as well as the whole society. Disaster management, environmental monitoring, smart watering, and optimizing energy consumption through smart grids and smart metering are examples of applications that focus on environment.

Standardization:

Standardization is one of the most critical hurdles of the IoT evolution. Without global standards, the complexity of devices that need to connect and communicate with each other (with all the associated addressing, automation, quality of service, interfaces, data repository and associated directory services, etc.) will grow exponentially. The IoT promises billions of connected things which in turn require common standards in order to operate with an acceptable, manageable and scalable level of complexity.

Most of the existing Internet standards did not have the vision to include the IoT which is relatively a newer concept. Therefore, their scope is not sufficient to support the IoT technically and economically. Moreover, IoT architecture, use cases, devices, etc., are still evolving. Today, many IoT devices have been deployed with proprietary protocols. This makes the communication between multiple IoT devices difficult. However, in the era of digital revolution, with many vendors playing in the field, with researchers and entrepreneurs working hard to develop solutions and with government agencies trying hard to reach their citizens, the world has to agree to a common standard. Not only the hardware components related to the IoT, but also the software aspects of the IoT should also be standardized, creating standardized application programming interfaces (APIs) and software services such that future applications can be deployed in a level and uniform environment, thereby enabling easy migration across systems. Standardization is necessary to ensure

i) Interoperability across products, applications, and services that preclude vendor lock-in.
ii) Economy of scale, where the three sections of the society developer (researcher), government (regulator), and the user get benefited in a reasonable time frame.
iii) Security and privacy of the data and the users
iv) Space for the researchers to take our society to another height
v) Interoperation across physical communication systems, protocol syntax, data semantics, and domain information

Organization Name	Outcome
Internet of Things Global Standards Initiative (IoT-GSI)	JCA-IoT
Open Source Internet of Things (OSIoT)	Open Horizontal Platform
IEEE	802.15.4 standards, developing a reference architecture
Internet Engineering Task Force (IETF)	Constrained RESTful Environments (CoRE), 6LOWPAN, Routing Over Low power and Lossy networks (ROLL), IPv6
The World Wide Web Consortium (W3C)	Semantic Sensor Net Ontology, Web Socket, Web of Things
XMPP Standards Foundation	XMPP
Eclipse Foundation	Paho project, Ponte project, Kura, Mihini/M3DA, Concierge
Organization for the Advancement of Structured Information Standards	MQTT, AMPQ

Figure-1showing IoT Standards

Though there is no single body which is responsible for making IoT standards, there are considerable efforts at national and international level, at government level, and at different organizational levels for IoT standardization. Alliances have been formed by many domestic and multinational companies to agree on common standards and technology for the IoT. However, no universal body has been formed yet. While organizations such as IEEE, Internet Engineering Task Force (IETF), ITU-T, OneM2M, 3GPP, etc., are active at international level, Telecommunication Standards Development Society, India (TSDSI), Global ICT Standardization Forum for India (GISFI), Bureau of Indian Standards (BIS), Korean Agency for Technology and Standards (KATS) etc., are active at national level and European Telecommunications Standards Institute (ETSI) in the regional level for standardization.

Let's take a simple transaction: data is typically collected by sensors within IoT devices, transmitted via wireless and wired networks to data and application warehouses virtualized in the cloud, and aggregated for analysis to determine information such as usage patterns through analytics and business intelligence applications. Standardizing is not particularly important to solve interoperability, as this can always be achieved through multiprotocol gateways. Standardization across the IoT landscape is important because this reduces the gaps between protocols (and associated security holes and issues). It also reduces the overall cost of data, associated transport costs and the cost of manufacturing of individual components. This is because fewer standards enable more compatible components, which all leads to reduced cost of design, manufacturing and a reduced time to market. Standardization also streamlines the overall integration at an application level (aggregation of data, interoperability of data, reports and business processes) without being concerned with individual IT devices, unique protocols and non-standard data formats.

Standardization and the limitation caused by regulatory policies have challenged the growth and adoption rate of IoT and can be potential barriers in embracing the technology. Defining and broadcasting standards will ease the burden of joining IoT environments for new users and providers. Additionally, interoperability among different components, service providers, and even end users will be greatly influenced in a positive way, if pervasive standards are introduced and employed in IoT. Even though more organizations and industries make themselves ready to embrace and incorporate IoT, increase in IoT growth rate will cause difficulties for standardization. Strict regulations about accessing radio frequency levels, creating a sufficient level of interoperability among different devices, authentication, identification, authorization, and communication protocols are all open challenges facing IoT standardization.

Q1(b) Write detail application of Internet of Things

Answer:

The Internet of Things (IoT) is an emerging area of the modern technology which impacts use cases across governance, education, business, manufacturing, entertainment, transportation, infrastructures, health care, and so on. IoT promises an interconnected network of uniquely identifiable smart objects. This infrastructure creates the necessary backbone for many interesting applications that require seamless connectivity and addressability between their components. The range of IoT application domain is wide and encapsulates applications from home automation to more sophisticated environments, such as smart cities and e-government. Industry-focused applications include logistics and transportation, supply-chain management, fleet management, aviation industry, and enterprise automation systems. Healthcare systems, smart cities and buildings, social IoT, and smart shopping are a few examples of applications that try to improve the daily life of individuals, as well as the whole society. Disaster management, environmental monitoring, smart watering, and optimizing energy consumption through smart grids and smart metering are examples of applications that focus on environment.

In a broader magnitude, Gascon and Asin classified IoT applications under the following categories: smart environment, smart cities, smart metering, smart water, security and emergencies, retail, logistics, industrial control, smart agriculture, smart animal farming, domestic and home automation, and eHealth. IoT applications based on their usage domain fall into the following three categories: (1) monitoring and actuating, (2) business process and data analysis, and (3) information gathering and collaborative consumption.

MONITORING AND ACTUATING

Monitoring devices via APIs can be helpful in multiple domains. The APIs can report power usage, equipment performance, and sensor status, and they can perform actions upon sending predefined commands. Real-time applications can utilize these features to report current system status, whereas managers and developers have the option to freely call these APIs without the need for physically accessing the devices. Smart metering, and in a more distributed form, smart grids, can help in identifying production or performance defects via application of anomaly detection on the collected data, and thus increase the productivity.

Likewise, incorporating IoT into buildings, or even in the construction process, helps to move toward green solutions, save energy, and, consequently, minimize operation cost. Another area that has been under focus by researchers is applications targeting smart homes that mainly target energy-saving and monitoring. Home monitoring and control frameworks like the ones developed by Verizon and Boss support different communication protocols (Wi-Fi, Bluetooth, etc.) to create an interconnected network of objects that can control desired parameters and change configurations based on the user's settings.

Business Process and Data Analysis

Riggins categorized the level of IoT adoption through Big Data analytics usage to the following categories:

- Society level, where IoT mainly influences and improves government services by reducing cost and increasing government transparency and accountability
- Industry level, in which manufacturing, emergency services, retailing, and education have been studied as examples
- Organizational level, in which IoT can bring the same type of benefits as those mentioned in society level Individual level, where daily life improvements, individual efficiency, and productivity growth are marked as IoT benefits

The ability to capture and store vast amounts of individual data has brought opportunities to healthcare applications. Patients' data can be captured more frequently, using wearable technologies such as smart watches, and can be published over the Internet. Later, data mining and machine-learning algorithms are used to extract knowledge and patterns from the raw data and archive these records for future reference. Healthsense eNeighbor developed by Humana is an example of a remote controlling system that uses sensors deployed in houses to measure frequent daily activities and heath parameters of occupants. The collected data is then analyzed to forecast plausible risks and produce alerts to prevent incidents. Privacy and security challenges are two main barriers that refrain people and industries from embracing IoT in the healthcare domain.

Information gathering and collaborative consumption

Social Internet of Things (SIoT) is where IoT meets social networks, and, to be more precise, it promises to link objects around us with our social media and daily interaction with other people, making them look smarter and more intractable. SIoT concept, motivated by famous social media like Facebook and Twitter, has the potential to affect many people's lifestyles. For example, a social network is helpful for the evaluation of trust of crowds involved in an IoT process. Another advantage is using the humans and their relationships, communities, and interactions for effective discovery of IoT services and objects.

Q2 Network Function Virtualization (NFV) based architecture to address connectivity and interoperability challenges in Internet of Things.

Answer:

Network functions virtualization (NFV) replaces the traditional network by virtualizing network services rather than operating them on proprietary dedicated hardware. That hardware is now just commodity hardware that runs software to accomplish functions such as routing, and firewalls. Classical MNO's network is crowded with a variety of proprietary hardware elements e.g. routers, switches, Packet Core nodes, and Access nodes. Whenever it wants to launch a new network service it often requires yet another hardware element. Finding the space and power to accommodate this new hardware is becoming increasingly difficult, compounded by the increasing costs of energy, capital investment challenges and the rarity of skills (necessary to design, integrate and operate increasingly complex hardware-based appliances).

Moreover, hardware-based appliances have an end of life i.e. 5 years or 10 years, which puts an additional burden of a procure-design-integrate-deploy cycle with little or no revenue benefits on the service provider. Hardware life cycles are becoming shorter as technology and services innovation accelerates, slow down the roll out of new revenue earning network services and restricting innovations in a network-centric connected world.

NFV Definition

The Network Functions Virtualization (NFV) is a network architecture or concept that utilizes the IT technology fundamentals to virtualize entire network node functions onto industry standard high volume servers, switches and storage, which could be located in Data centers or centralized locations. Network Nodes are in the end user premises to create communication services and illustrated in Figure 2.

It involves implementing network functions in a software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as in when required, without the need to install new hardware equipment.