UNIT II
Identification of IoT Object and Services

Identification codes can be classified as

(i) object IDs (OIDs)
(ii) communication IDs.

Examples radio frequency identification (RFID)/electronic product code (EPC), content ID,1telephone number, and uniform resource identifier (URI)/uniform resource locator (URL);media access control (MAC) address, network layer/IP address, and session/protocol ID.

All objects to have a permanent unique identifier, an OID.All end-point network locations and/or intermediary-point network locations to have a durable, unique network address (NAdr) using IPv6When objects that have enough intelligence to run a communications protocol stack (so that they can communicate), are placed on a network, these objects can be tagged with a NAdr.

Every object then has a tuple (OID, NAdr) that is always unique, although the second entry (NAdr) of the tuple may change with time, location, or situation.In a stationary, non-variable, or mostly static environment, assigns the OID to be identical to the NAdr where the object is expected to attach to the network; that is, the object tuple (NAdr, NAdr).In case the object moved, the OID could then be refreshed to the address of the new location; that is, the object tuple (NAdr', NAdr').In general trend toward object mobility, giving rise to a dynamic environment; hence, to retain maximal flexibility, it is best to separate, in principle, the OID from the NAdr

Identification scheme is that it affords global uniqueness.It is useful to have mechanisms for hierarchical grouping to deal with large populations.The feature of IPv6 address provides such hierarchical grouping. For a number of applications, there is a need to map/bind IP addresses (communications IDs) with other relevant OIDs.Modern layered communication architectures also require addressing and processing capabilities at several layers,For example, at the Data Link Layer, at the Network Layer, at the Transport (Protocol ID), and at the session/application layer.Some argue that different identification schemes are required for different applications.For example, the information related to things such as books, medicine, and clothes may not require global identification because revocation lists are required

An EPC (electronic product code) is a number assigned to an RFID tag representative of an actual EPC.Each number is encoded with a header, identifying the particular EPC version used for coding the entire EPC number.An EPC manager number is defined, allowing individual companies or organizations to be uniquely identified; an object class number is present, identifying objects used within this organization, such as product types EPC uses a numerical system for product identification, but its capabilities are much greater.An EPC is actually a number that can be associated with specific product information, such as date of manufacture and origin and destination of shipment. This provides significant advantages for businesses and consumers.The EPC is stored on an RFID tag, which transmits data when prompted by a signal emitted by a special reader.Note that EPC and RFID are not interchangeable

OID may be replaced by object namingDomain name system (DNS) is a mechanism for Internet-based namingIn the IoT context, the advantages of identifying information by name, not by node address.DNS is used to map the "human-friendly" host names of computers to their corresponding "machinefriendly" IP addresses. E.g.Object name service (ONS) will also be important in the IoT to map the "thing-friendly" names of object which may belong to heterogeneous name spaces (e.g., EPC, uCode, and any other self-defined code) on different networks (e.g., TCP/IP network) into their corresponding "machine-friendly" addresses or other related information of another TCP/IP network.This naming system can used for set of systems as object name should disclose its identity.

For some applications, especially where there is a need for simple end-user visibility of a small set of objects (i.e., where the objects are few and discretely identifiable a home's thermostat, a home's refrigerator, a home's lighting system, a pet of the owner), the object may be identified through Web Services (WSs).WSs provide standard infrastructure for data exchange between two different distributed applications.Lightweight WS protocols for the representational state transfer (REST) interface may be useful in this context.REST is a software architecture for distributed systems to implement WSs. REST is good compared to simple object access protocol (SOAP) and web services description language (WSDL) due to its relative simplicity.

IoT objects and IoT applications (e.g., grid control, home control, traffic control, and medical monitoring), security and privacy in communications and services become absolutely critical.Strong authentication, encryption while transmitting, and also encryptions for data at rest is ideal; however, the computational requirements for encryption can be significant.At the central/authenticating site,

rapid authentication support is desirable; otherwise objects would not be able to authenticate in large-population environments.

Tracking the object using GPS is costlyBut worst when tracking more than one object.There is a need to maintain ubiquitous and seamless communication while tracking the location of objects.

Capabilities for scalability are important in order to be able to support an IoT environment where there is a large population that is highly distributed.Locator/identifier separation.Basic idea behind the separation is that the Internet architecture combines two functions, routing locators (where one is attached to the network) and identifiers (where one is located), in one number space: the IP address.Proponents of the separation architecture postulate that splitting these functions apart will yield several advantages, including improved scalability for the routing system.The separation aims to decouple locators and identifiers, thus allowing for efficient aggregation of the routing locator space and providing persistent identifiers in the identifier space.The protocol called locator/ID separation protocol (LISP)

LISP aims for an incrementally deployable protocol.The LISP WG (Working Group) frame that include(i) an architecture description, (ii) deployment models,(iii) a description of the impacts of LISP, (iv) LISP security threats and solutions,(v) allocation of end-point identifier (EID) space, (vi) alternate mapping system designs(vii) data models for management of LISP.