National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

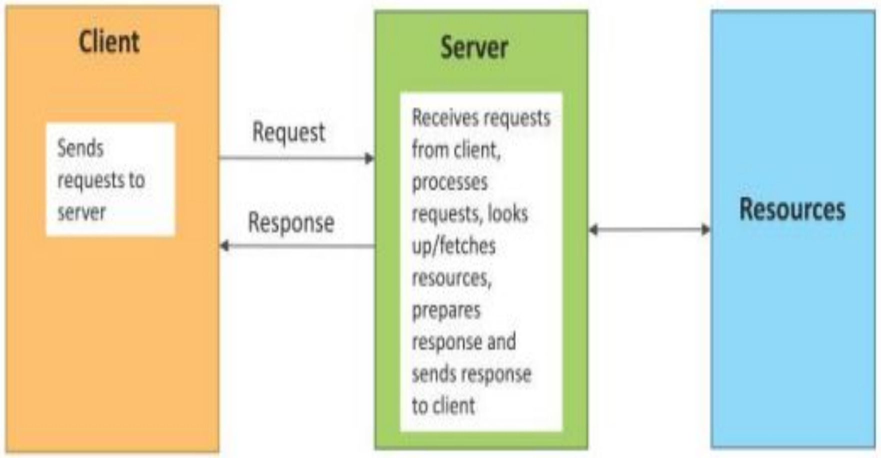
IoT Security and Forensics

Unit 1 - Introduction

- **DR. Madhavi Dave**
  Assistant Professor
  School of Cyber Security and Digital Forensics

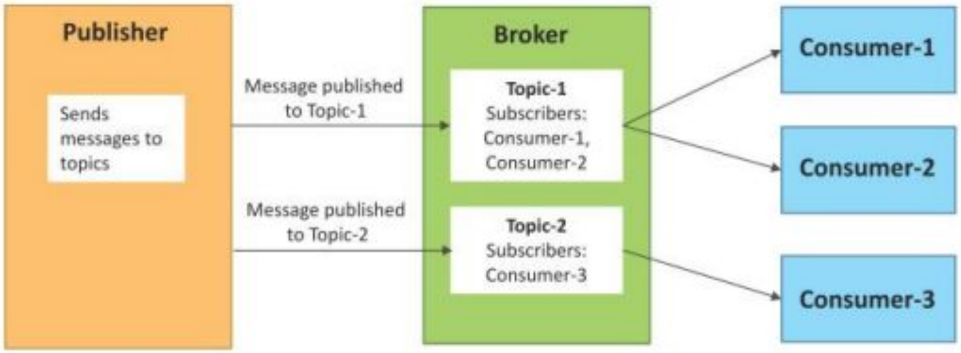
Request Response Communication Model

- Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests.
- When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.


Client
Sends requests to server
Request
Response
Server
Receives requests from client, processes requests, looks up/fetches resources, prepares response and sends response to client
Resources

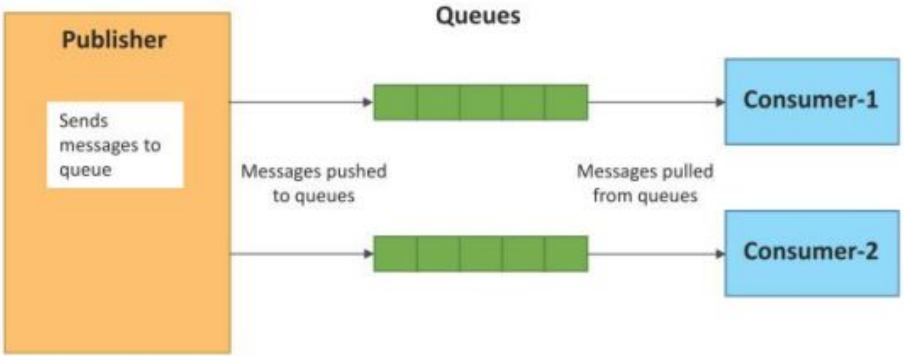
Publish Subscribe Communication Model

- Publish-Subscribe is a communication model that involves publishers, brokers and consumers.
- Publishers are the source of data. Publishers send the data to the topics which are managed by the broker.
- Publishers are not aware of the consumers.
- Consumers subscribe to the topics which are managed by the broker.
- When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers.



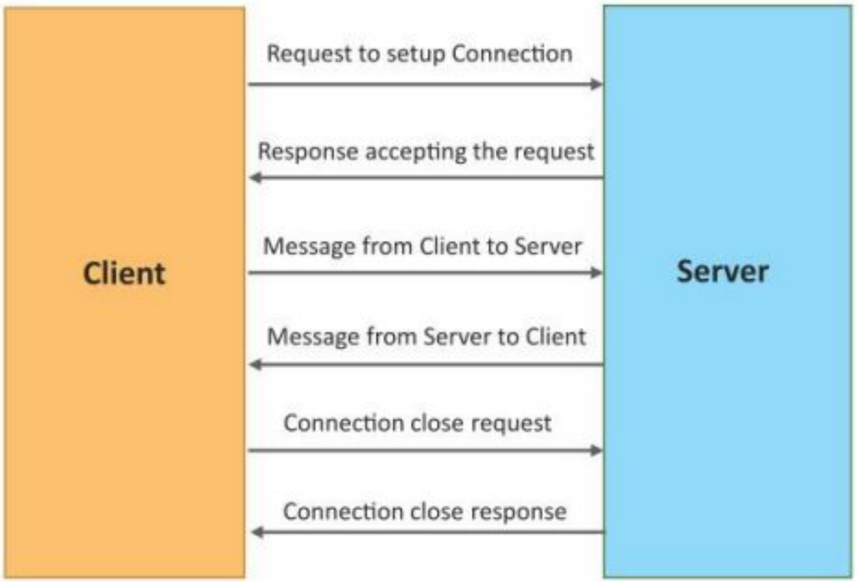
Push Pull Communication Model

- Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues.
- Producers do not need to be aware of the consumers.
- Queues help in decoupling the messaging between the producers and consumers.
- Queues also act as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate rate at which the consumers pull data.



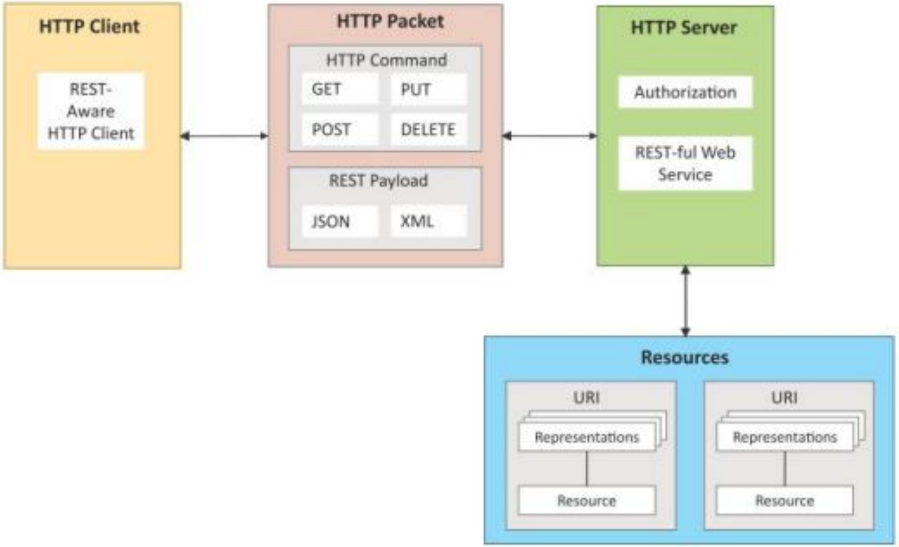
Exclusive Pair Communication Model

- Exclusive Pair is a bidirectional, full duplex communication model that uses a persistent connection between the client and server.
- Once the connection is setup it remains open until the client sends a request to


Client
Request to setup Connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection close response
Server

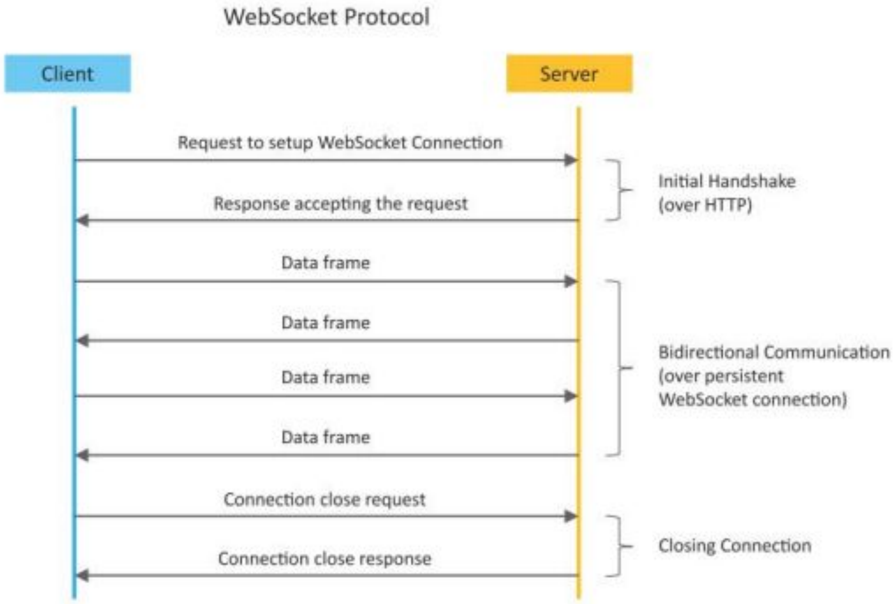
Rest based Communication API

- Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.
- REST APIs follow the request-response communication model.
- The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.



Web Socket Based Communication API

- WebSocket APIs allow bi-directional, full duplex communication between clients and servers.
- WebSocket APIs follow the exclusive pair communication model


WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake (over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication (over persistent WebSocket connection)
Connection close request
Connection close response
Closing Connection

IoT Levels & Deployment Templates

An IoT system comprises of the following components:

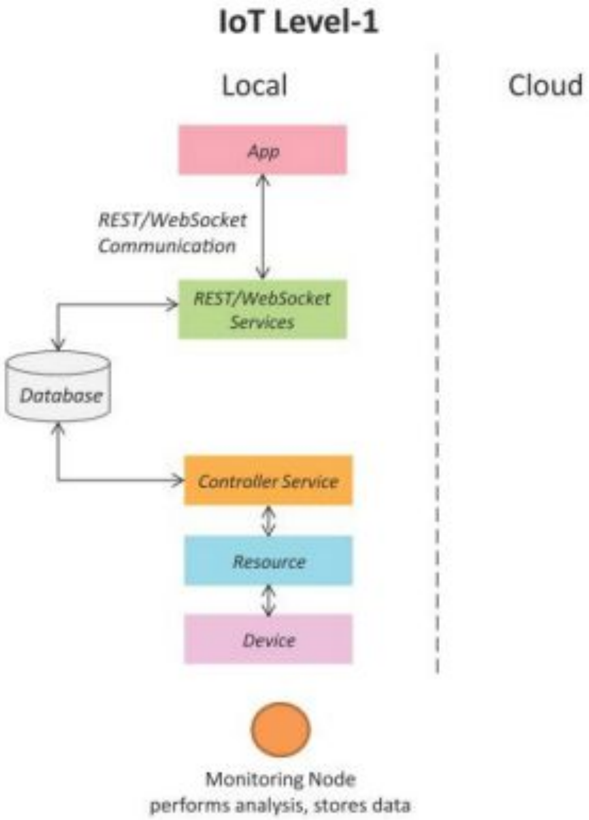
- Device: An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities. You learned about various examples of IoT devices in section
- Resource: Resources are software components on the IoT device for accessing, processing, and storing sensor information, or controlling actuators connected to the device. Resources also include the software components that enable network access for the device.
- Controller Service: Controller service is a native service that runs on the device and interacts with the web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.

IoT Levels & Deployment Templates (cont..)

- Database: Database can be either local or in the cloud and stores the data generated by the IoT device.
- Web Service: Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).
- Analysis Component: The Analysis Component is responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.
- Application: IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed data.

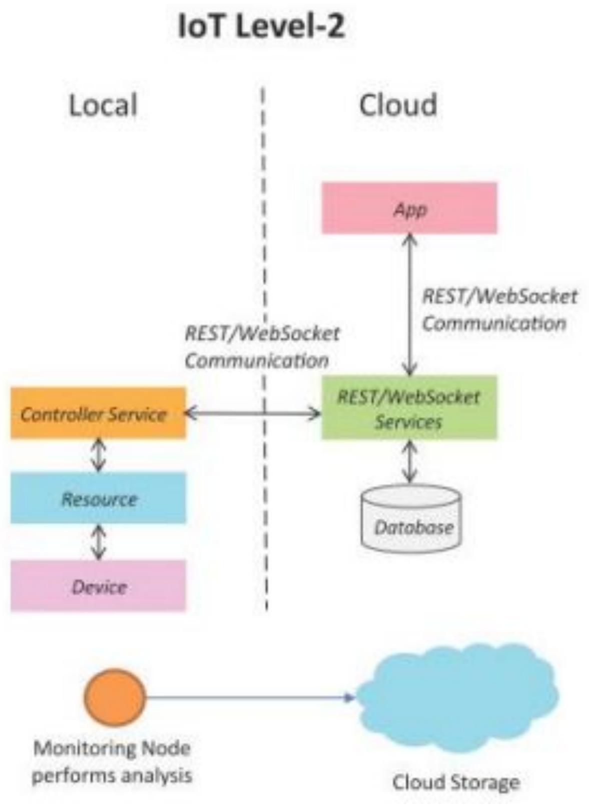
IoT Level - 1

- A level-1 IoT system has a level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application
- Level-1 IoT systems are suitable for modeling low- cost and low-complexity solutions where the data involved is not big and the analysis requirements are not computationally intensive.



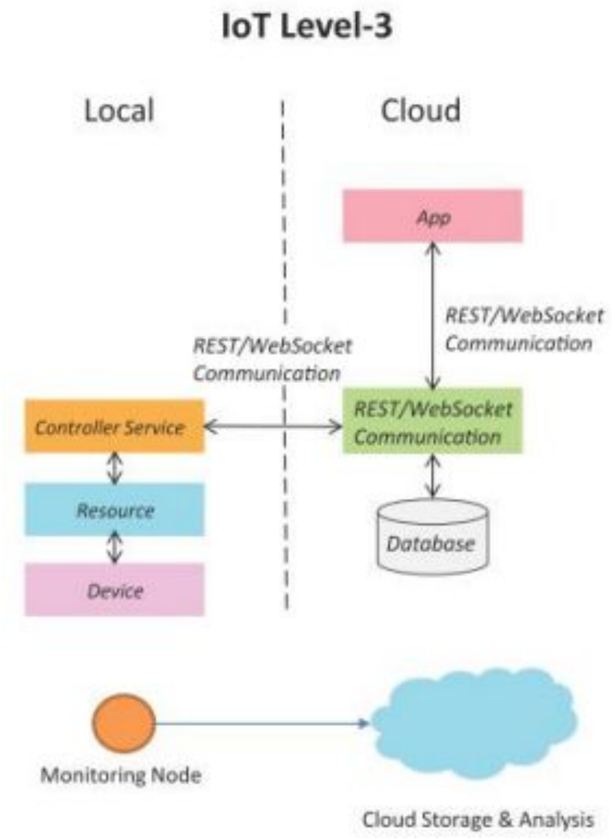
IoT Level - 2

- A level-2 IoT system has a single node that performs sensing and/or actuation and local analysis.
- Data is stored in the cloud and application is usually cloud- based.
- Level-2 IoT systems are suitable for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.



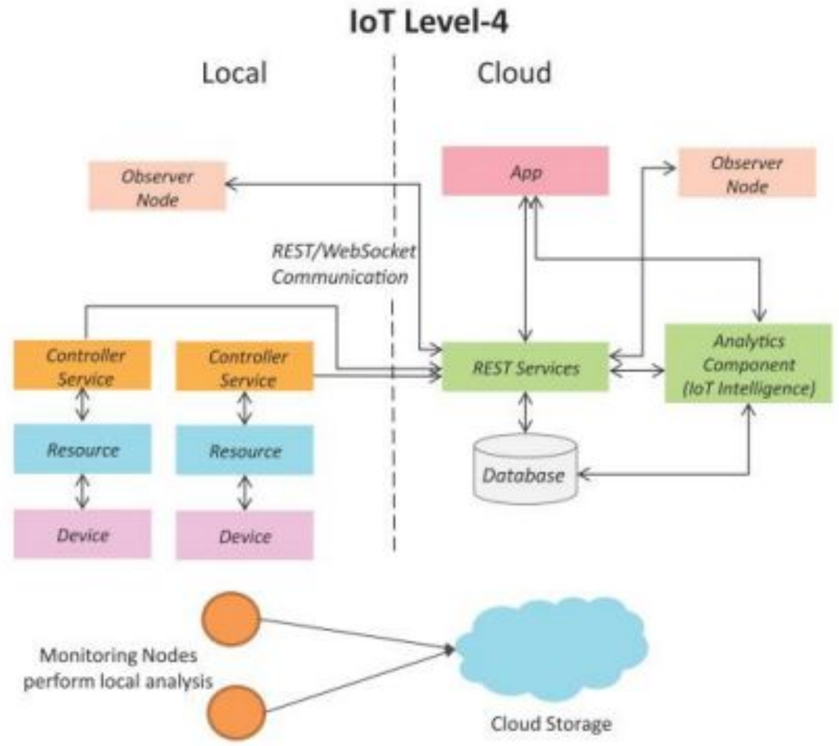
IoT Level - 3

- A level-3 IoT system has a single node. Data is stored and analyzed in the cloud and application is cloud- based.
- Level-3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.



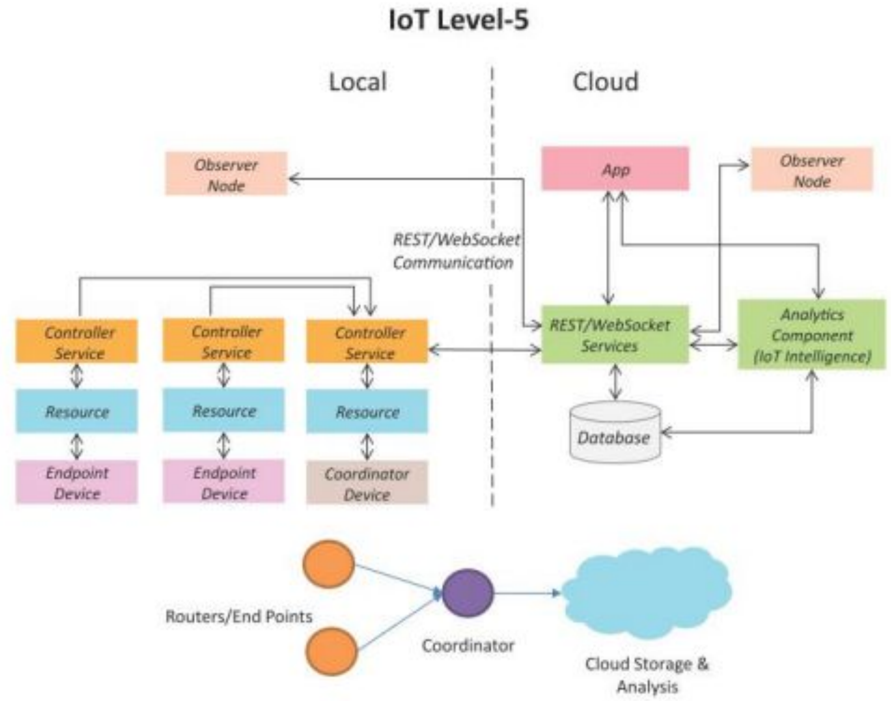
IoT Level - 4

- A level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud-based.
- Level-4 contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- Level-4 IoT systems are suitable for solutions where multiple nodes are required, the data involved is big and the analysis requirements are computationally intensive.



IoT Level - 5

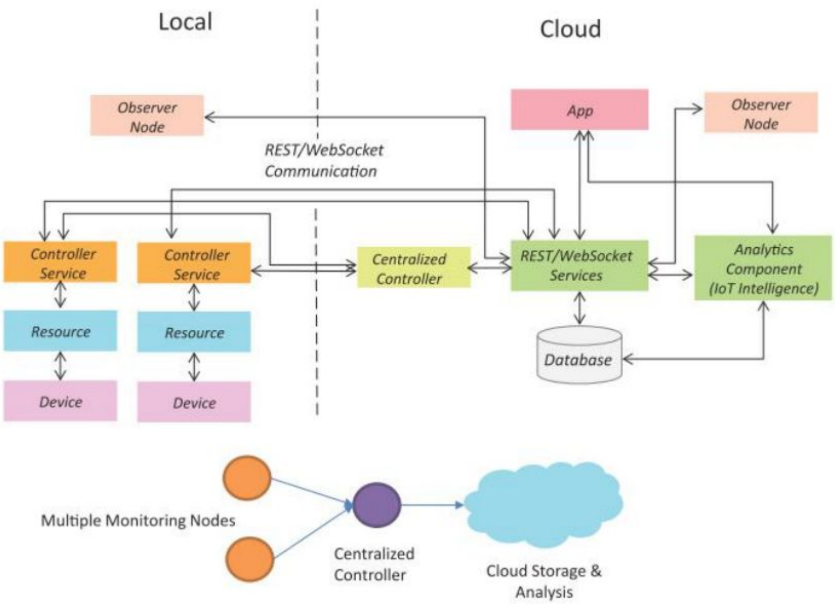
- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes that perform sensing and/or actuation.
- Coordinator node collects data from the end nodes and sends to the cloud.
- Data is stored and analyzed in the cloud and application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.



IoT Level - 6

- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and application is cloud-based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.

IoT Level-6



Security, Privacy & Trust

- There are a number of specific security, privacy and trust challenges in the IoT, they all share a number of transverse non-functional requirements:
  - Lightweight and symmetric solutions
  - Support for resource constrained devices
  - Scalable to billions of devices/transactions
  - Solutions will need to address federation/ administrative co-operation
  - Heterogeneity and multiplicity of devices and platforms
  - Intuitively usable solutions seamlessly integrated into the real world

Trust for IoT

- There is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged can indeed be relied upon.
- The trust framework needs to be able to deal with humans and machines as users.
- The development of trust frameworks that address this requirement will require advances in areas such as:
  - Lightweight Public Key Infrastructures (PKI) as a basis for trust management.
  - Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources.
  - Quality of Information is a requirement for many IoT-based systems.

- Decentralized and self-configuring systems as alternatives to PKI for establishing trust.
- Novel methods for assessing trust in people, devices and data, beyond reputation systems.
- Assurance methods for trusted platforms including hardware, software, protocols, etc.
- Access Control to prevent data breaches.

Security for IoT

- As the IoT becomes a key element of the future Internet and a critical national/international infrastructure, the need to provide adequate security for the IoT infrastructure becomes ever more important.
- Advances are required in several areas to make the IoT secure from those with malicious intent, including:
  - DoS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms.
  - General attack detection and recovery/resilience to cope with IoT specific threats, such as compromised nodes, malicious code hacking attacks.
  - Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored.
  - The IoT requires a variety of access control and associated accounting schemes to support the various authorization and usage models that are required by users.
  - The IoT needs to handle virtually all modes of operation by itself without relying on human control.

Privacy for IoT

- As much of the information in an IoT system may be personal data, there is a requirement to support anonymity and restrictive handling of personal information.
- There are a number of areas where advances are required:
- Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.
- Techniques to support Privacy by Design concepts, including data minimisation, identification, authentication and anonymity.
- Fine-grain and self-configuring access control mechanism emulating the real world.

- There are a number of privacy implications arising from IoT devices where further research is required, including:
  - Preserving location privacy, where location can be inferred from things associated with people.
  - Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.
  - Keeping information as local as possible using decentralized computing and key management.
  - Use of soft identities, where the real identity of the user can be used to generate various soft identities for specific applications.

IoT Related Standardizations

- Standards are needed for interoperability both within and between domains.
- Within a domain, standards can provide cost efficient realizations of solutions, and a domain here can mean even a specific organization or enterprise realizing an IoT.
- Between domains, the interoperability ensures cooperation between the engaged domains, and is more oriented towards Internet of Things applications.
- Significant attention is given to the "pre-selection" of standards through collaborative research, but focus should also be given to regulation, legislation, interoperability and certification as other activities in the same life-cycle.
- It would be beneficial to develop a wider approach to standardization and include anticipation of emerging or on-going policy making in target application areas.

- The standardisation bodies are addressing the issue of interoperable protocol stacks and open standards for the IoT.
- This includes as well expending the HTTP, TCP, IP stack to the IoT-specific protocol stack.
- This is quite challenging considering the different wireless protocols like ZigBee, RFID,Bluetooth, BACnet 802.15.4e, 6LoWPAN, RPL, and CoAP.
- Agreed standards do not necessarily mean that the objective of interoperability is achieved.
- The mobile communications industry has been successful not only because of its global standards, but also because interoperability can be assured via the certification of mobile devices and organizations.

- From the point of view of standardisation IoT is a global concept, and is based on the idea that anything can be connected at any time from any place to any network, by preserving the security, privacy and safety.
- Interoperability is a key challenge in the realms of the Internet of Things.
- This is due to the intrinsic fabric of the IoT as:
  - High–dimensional
  - Highly-heterogeneous
  - dynamic and non-linear
  - hard to describe/model.

Interoperability in IoT

- The Internet of Things is shaping the evolution of the future Internet.
- After connecting people anytime and everywhere, the next step is to interconnect heterogeneous things/machines/smart objects both between themselves and with the Internet.
- As for the IoT, future networks will continue to be heterogeneous, multi-vendors, multi-services and largely distributed.
- Consequently, the risk of non-interoperability will increase. This may lead to unavailability of some services for end-users.
- The framework for sustainable interoperability in Internet of Things applications needs (at least) to address the following aspects:
  - Management of Interoperability in the IoT
  - Dynamic Interoperability Technologies for the IoT
  - Measurement of Interoperability in the IoT
  - Interaction and integration of IoT in the global Internet

Device Level Energy Issues

- Challenges in IoT is how to interconnect “things” in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices