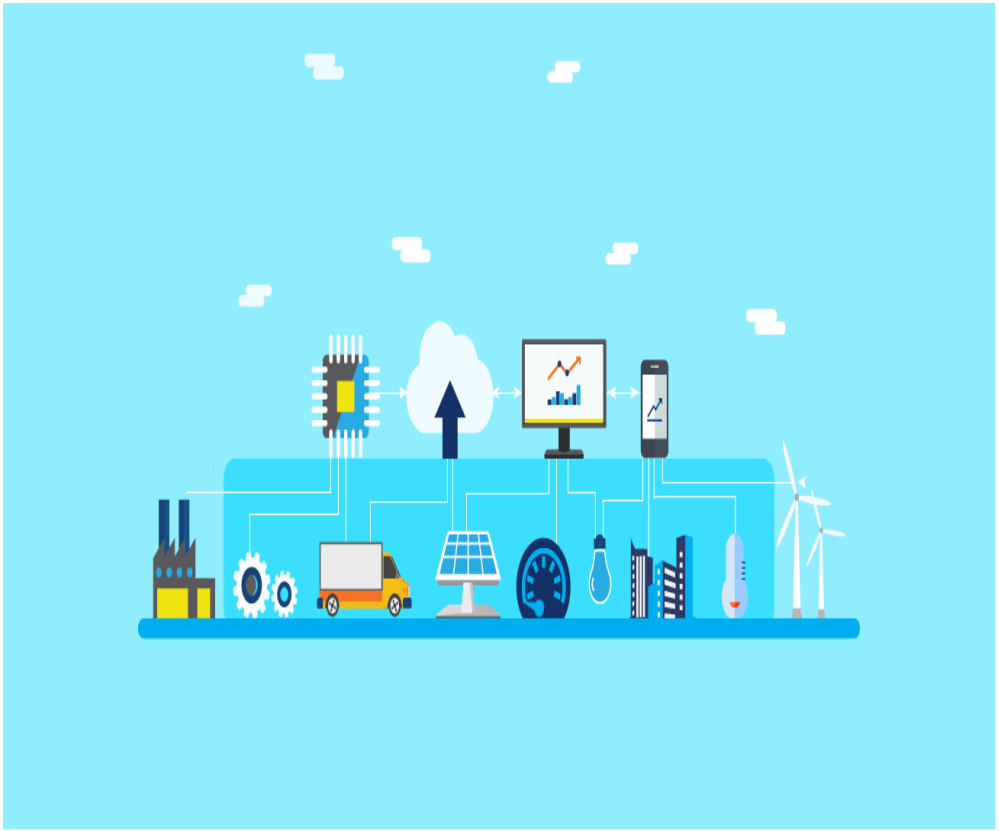
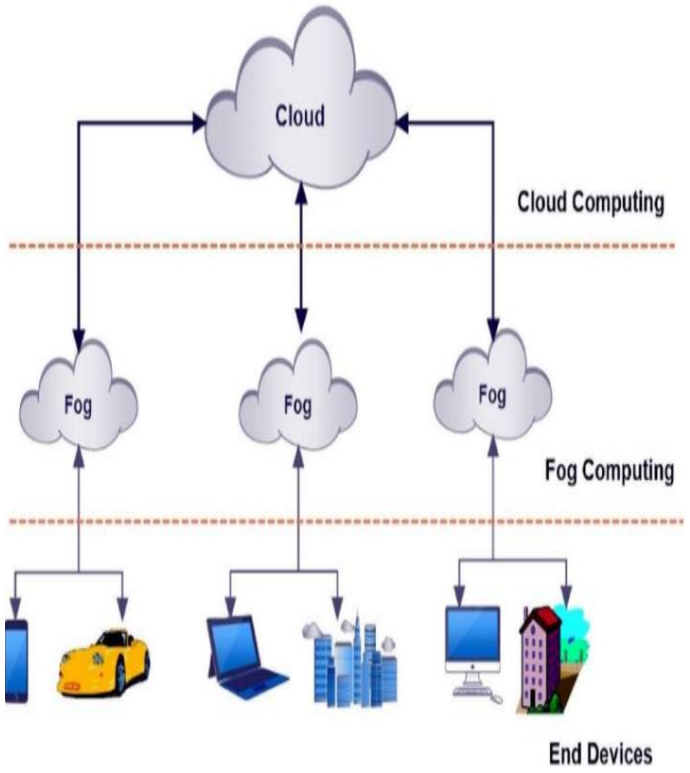




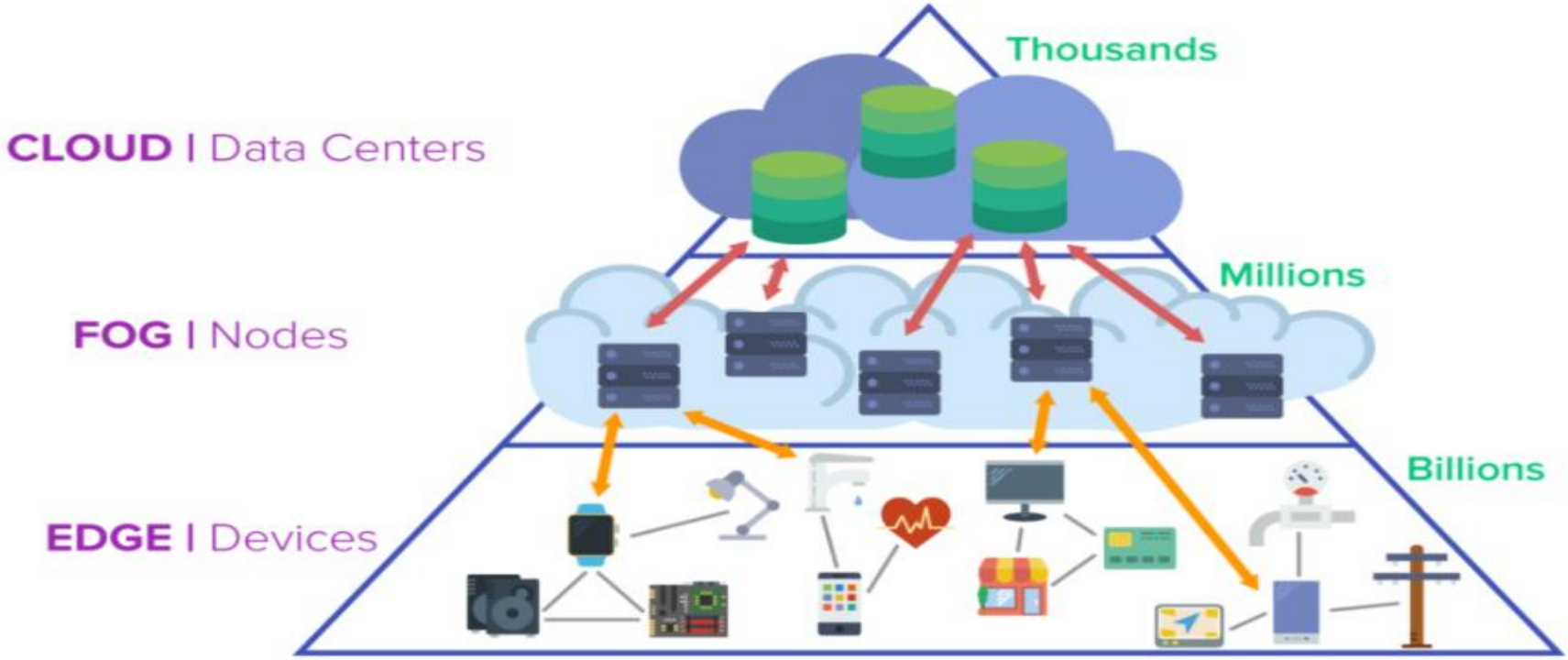
FOG AND CLOUD COMPUTING

UNIT 5

UNIT 5 FOG COMPUTING

- From Cloud to Fog
- Fog Computing architecture
- fog networks
- Principles of Edge/P2P networking
- Security and privacy in Fog

FOG COMPUTING



- **Whereas Cloud is upwhere in the sky somewhere, distant and remote and deliberately abstracted**

- **Fog is close to the ground where things are getting done**

CLOUD COMPUTING : CHALLENGES

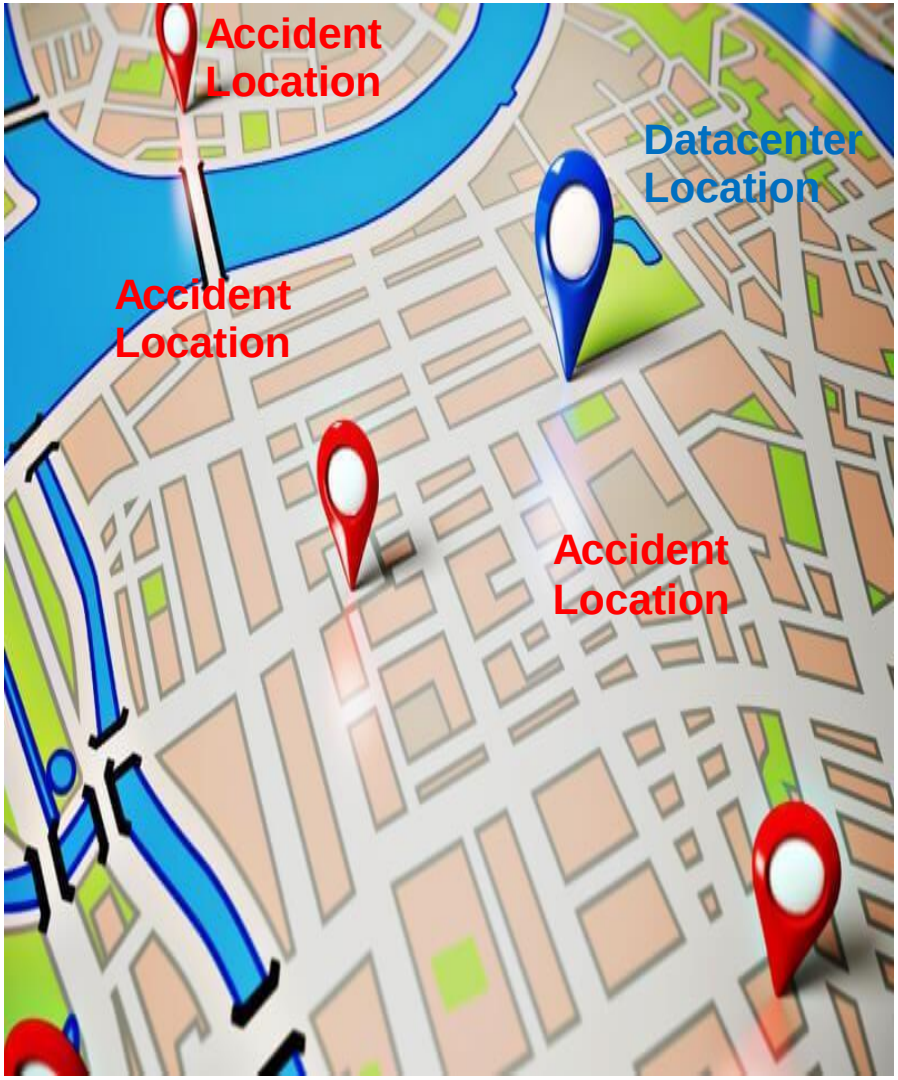
- Processing of huge data in a datacenter.
- Datacenter may be privately hosted by the organization (private cloud setup) or publicly available by paying rent (public cloud).
- All the necessary information has to be uploaded to the cloud for processing and extracting knowledge from it.

CLOUD COMPUTING –TYPICAL CHARACTERISTICS

- **Dynamic scalability**: Application can handle increasing load by getting more resources.
- **No Infrastructure Management by User:** Infrastructure is managed by cloud provider, not by end-user or application developer.
- **Metered Service**: Pay-as-you-go model. No capital expenditure for public cloud.

ISSUES WITH "CLOUD-ONLY" COMPUTING

- Communication takes a long time due to human-smartphone interaction.
- Datacenters are centralized, so all the data from different regions can cause congestion in core network.
- Such a task requires very low response time, to prevent further crashes or traffic jam.



FOG COMPUTING

- Fog computing, also known as fogging/edge computing, it is a model in which data, processing and applications are concentrated in devices at the network edge rather than existing almost entirely in the cloud.
- The term "Fog Computing" was introduced by the Cisco Systems as new model to ease wireless data transfer to distributed devices in the Internet of Things (IoT) network paradigm
- CISCO's vision of fog computing is to enable applications on billions of connected devices to run directly at the network edge.
  - Users can develop, manage and run software applications on Cisco framework of networked
    devices, including hardened routers and switches.
  - Cisco brings the open source Linux and network operating system together in a single networked device

FOG COMPUTING

Decentralization and flexibility are the main difference between fog computing and cloud computing. Fog computing, also called fog networking or fogging, describes a decentralized computing structure located between the cloud and devices that produce data. This flexible structure enables users to place resources, including applications and the data they produce, in logical locations to enhance performance.

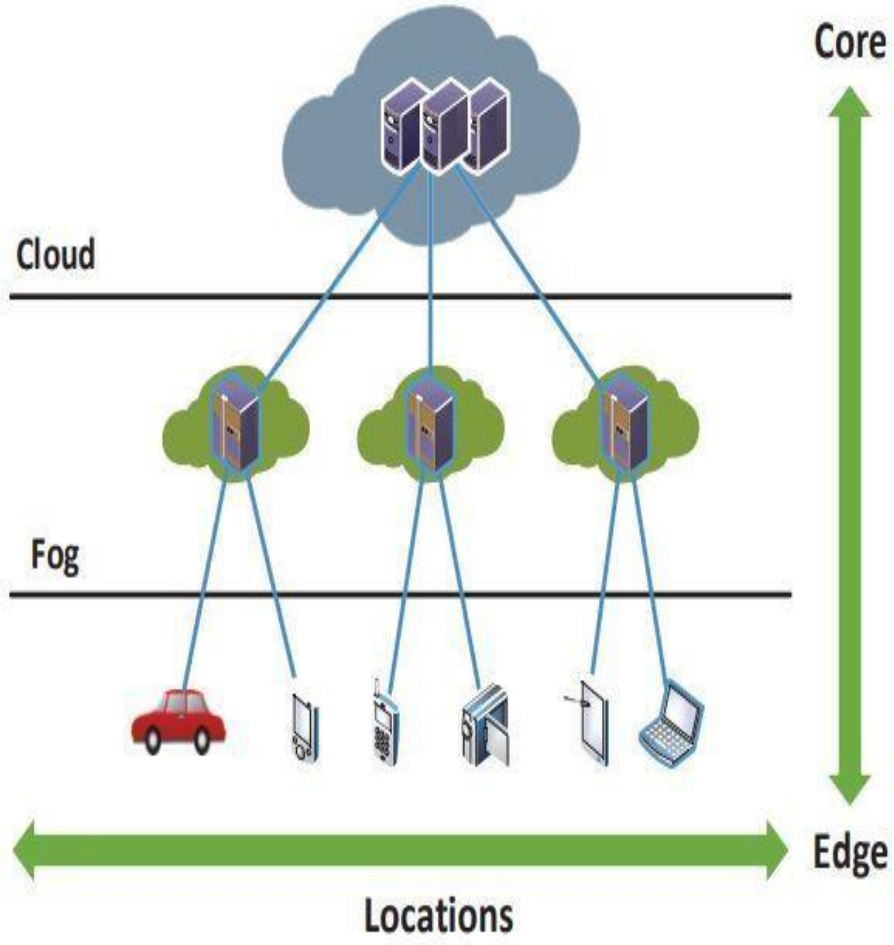
The structure's goal is to locate basic analytic services at the edge of the network, closer to where they are needed. This reduces the distance across the network that users must transmit data, improving performance and overall network efficiency.

Fog computing security issues also provide benefits for users. The fog computing paradigm can segment bandwidth traffic, enabling users to boost security with additional firewalls in the network.

Fog computing maintains some of the features of cloud computing, where it originates. Users may still store applications and data offsite, and pay for not just offsite storage, but also cloud upgrades and maintenance for their data while still using a fog computing model. Their teams will still be able to access data remotely

FOG COMPUTING

- Bringing intelligence down from the cloud close to the ground/ end-user.
- Cellular base stations, Network routers, WiFi Gateways will be capable of running applications.
- End devices, like sensors, are able to perform basic data processing.
- Processing close to devices lowers response time, enabling real-time applications.



FOG COMPUTING

- Fog computing enables some of transactions and resources at the edge of the cloud, rather than establishing channels for cloud storage and utilization.

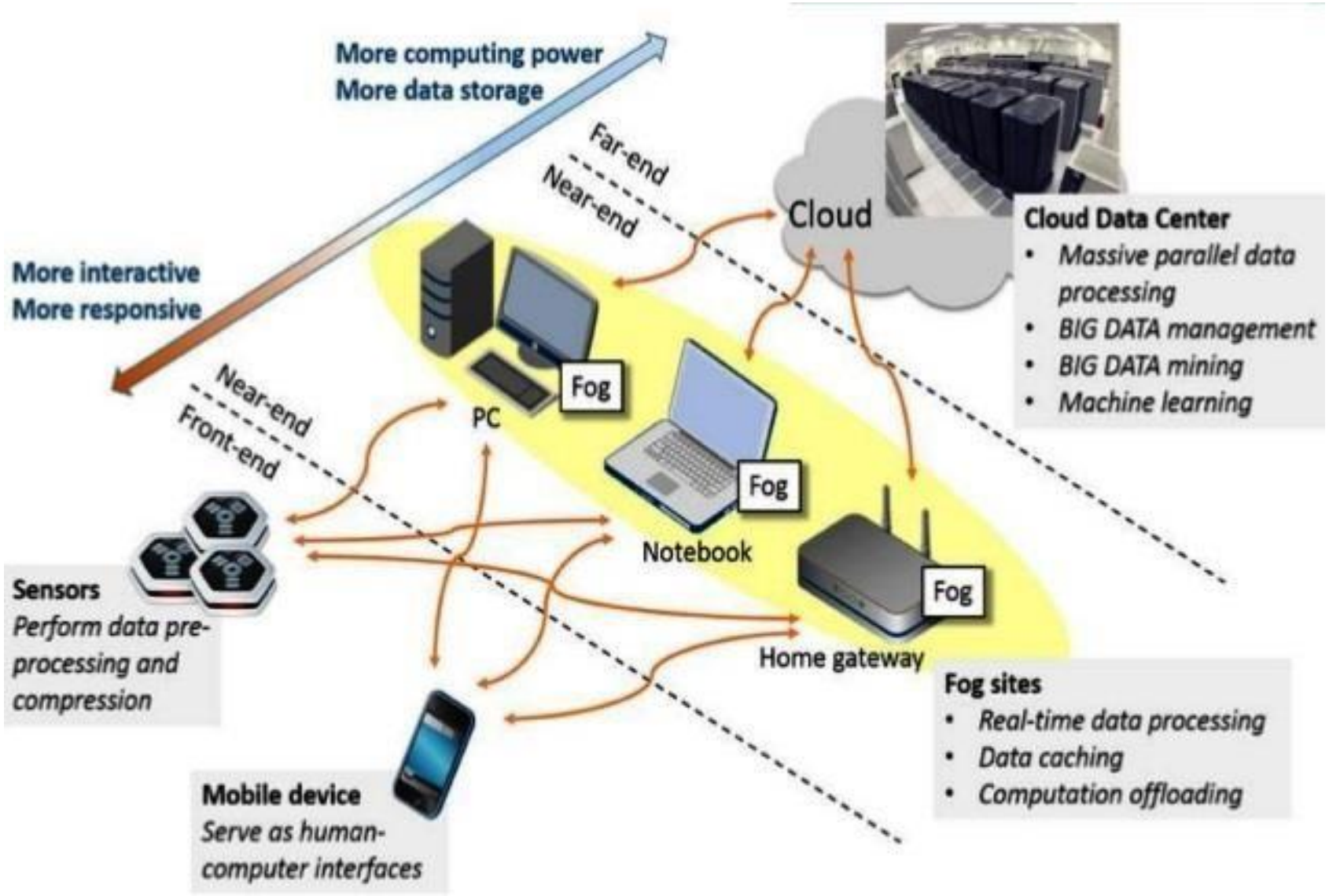
- Fog computing reduces the need for bandwidth by not sending every bit of information over cloud channels, and instead aggregating it at certain access points.

- This kind of distributed strategy, may help in lowering cost and improve efficiencies.

FOG COMPUTING - MOTIVATION

- Fog Computing is a paradigm that extends Cloud and its services to the edge of the network
- Fog provides data, compute, storage and application services to the end-user
- Recent developments: Smart Grid, Smart Traffic light, Connected
  Vehicles, Software defined network

FOG COMPUTING



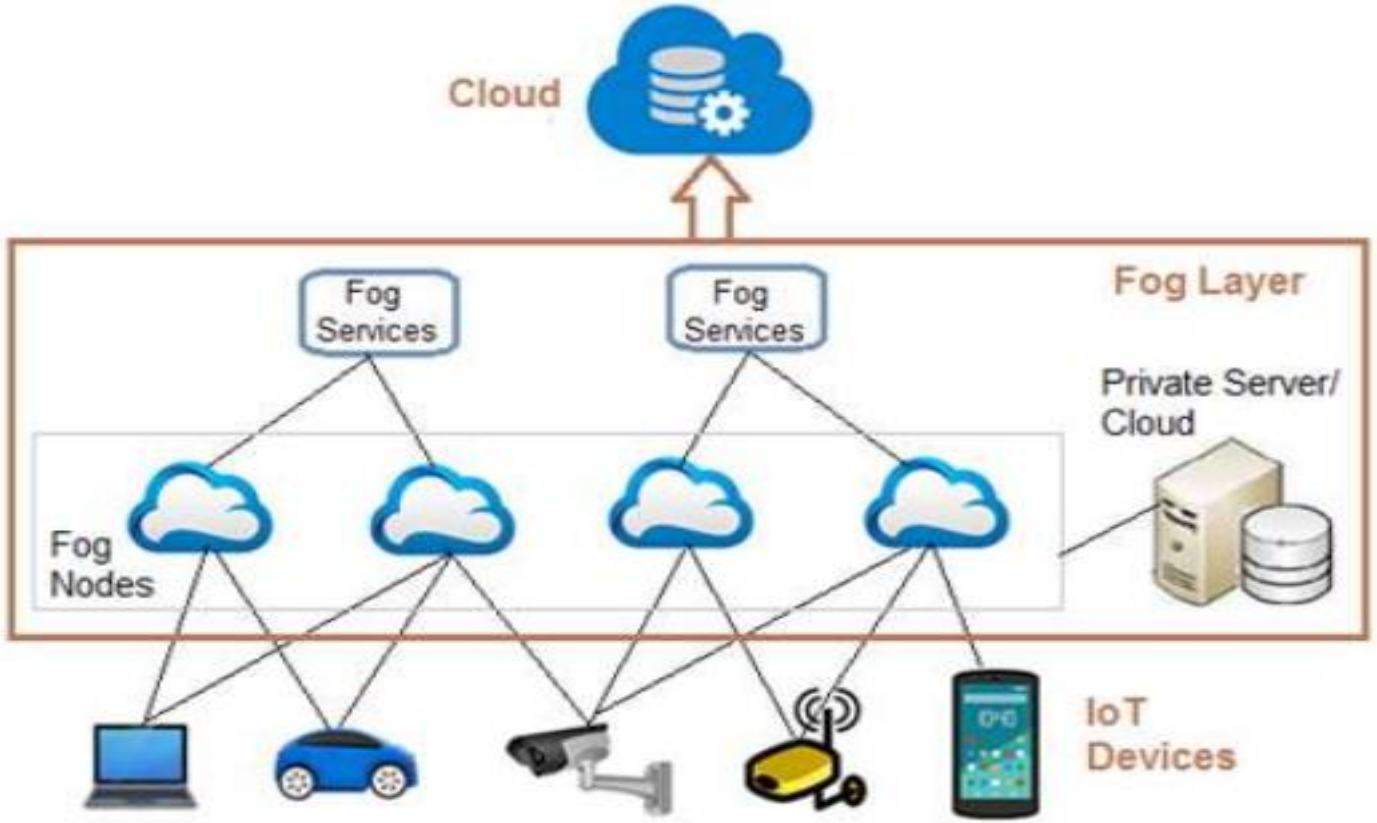
FOG COMPUTING -ENABLES

- **Virtualization :** Virtual machines can be used in edge devices.
- **Containers:** Reduces the overhead of resource management by using light-weight virtualizations. Example: *Docker* containers.
- **Service Oriented Architecture:** Service-oriented architecture (SOA) is a style of software design where services are provided to the other components by application components, through a communication protocol over a network.
- **Software Defined Networking:** Software defined networking (SDN) is an approach to using open protocols, such as OpenFlow, to apply globally aware software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware.

FOG COMPUTING - NOT A REPLACEMENT OF CLOUD COMPUTING

- Fog/edge devices are there to help the Cloud datacenter to better response time for real-time applications. Handshaking among Fog and Cloud computing is needed.
- Broadly, benefits of Fog computing are:
  - Low latency and location awareness
  - Widespread geographical distribution
  - Mobility
  - Very large number of nodes
  - Predominant role of wireless access
  - Strong presence of streaming and real time applications
  - Heterogeneity

FOG COMPUTING - ARCHITECTURE



- The Fog computing architecture consists of physical and logical elements in the form of hardware and software to implement IoT (Internet of Things) network.
- It is composed of IoT devices, fog nodes, fog aggregation nodes with the help of fog data services, remote cloud storage and local data storage server/cloud. Let us understand fog computing architecture components.

FOG COMPUTING - ARCHITECTURE

• **IoT devices**: These are devices connected on IoT network using various wired and wireless technologies. These devices produce data regularly in huge amount.

There are numerous wireless technologies used in IoT which include Zigbee, Zwave, RFID, 6LoWPAN, HART, NFC, Bluetooth, BLE, ISA-100.11A etc. IoT protocols used include IPv4, IPv6, MQTT, CoAP, XMPP, AMQP etc.

• **Fog Nodes:** Any device with computing, storage and network connectivity is known as fog node. Multiple fog nodes are spread across larger region to provide support to end devices. Fog nodes are connected using different topologies.

The fog nodes are installed at various locations as per different applications such as on floor of a factory, on top of power pole, along side of railway track, in vehicles, on oil rig and so on.

Examples of fog nodes are switches, embedded servers, controllers, routers, cameras etc. High sensitive data are processed at these fog nodes.

FOG COMPUTING - ARCHITECTURE

- **Fog aggregate nodes**: Each fog nodes have their aggregate fog node. It analyzes data in seconds to minutes. IoT data storage at these nodes can be of duration in hours or days. Its geographical coverage is wider. Fog data services are implemented to implement such aggregate node points. They are used to address average sensitive data.

- **Remote Cloud**: All the aggregate fog nodes are connected with the cloud. Time insensitive data or less sensitive data are processed, analyzed and stored at the cloud.

- **Local server and cloud:** Often fog computing architecture uses private server/cloud to store the confidential data of the firm. These local storage is also useful to provide data security and data privacy.

FOG COMPUTING WORKING OPERATION

•There are three types of data 1. most time sensitive data, 2.less time sensitive data and 3.time-insensitive data.

Fog computing architecture works based on type of data it receives. Nearest fog nodes takes data input from the devices.

➡**Most time sensitive data** are handled by nearest fog node to end device which has generated the data. After the received data is analyzed, decision or action is transmitted to the device. After this, fog node sends and stores summary to the cloud for future analysis. The data at fog node is analyzed in fraction of a second.

➡**Less time sensitive data** are sent to aggregate node for analysis. After analysis is performed, aggregate node sends decision or action to the device through nearest node. Aggregate fog node takes seconds or minutes to complete the analysis. The aggregate node later sends the report to cloud for future analysis purpose.

➡**Time insensitive data** can wait for longer duration (in hours, days or weeks). The data is sent to cloud for storage and future analysis.

FOG COMPUTING –PROS (ADVANTAGES OR BENEFITS)

- It offers better security.
- It saves network bandwidth and hence reduces operational costs.
- It reduces latency.
- It offers better privacy.
- It is easy to develop fog applications.
- Fog nodes are mobile in nature.
- Fog nodes can withstand any harsh environment conditions.

FOG ADVANTAGES

- Fog can be distinguished from Cloud by its proximity(nearness or closeness) to end-users.
- Dense geographical distribution and its support for mobility.
- It provides low latency, location awareness, and improves quality-of- services (QoS) and real time applications.

FOG COMPUTING CONS (DISADVANTAGES OR CHALLENGES)

• It is difficult for any arbitrary devices to exchange the data on fog computing networks.
• There are security concerns due to wide use of IoT based wireless networks, IP address spoofing etc.
• Data consistency and data management in fog computing is a challenge.
• Trust and authentication are major concerns.
• Scheduling is complex as tasks can move between clients, fog nodes and back end servers.
• Power consumption is higher due to de-centralized architecture.

SECURITY ISSUES

- Major security issues are authentication at different levels of gateways as well as in the Fog nodes
- Man-in-the-Middle-Attack
- Privacy Issues
- *In case of smart grids, the smart meters installed in the consumer's home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses.*

LIMITATIONS OF CLOUD COMPUTING

- High capacity(bandwidth) requirement
- Client access link
- High latency
- Security

"Fog" Solution

- Reduction in data movement across the network resulting in reduced congestion
- Elimination of bottlenecks resulting from centralized computing systems
- Improved security of encrypted data as it stays closer to the end user

FOG COMPUTING AND CLOUD COMPUTING

Requirement	Cloud computing	Fog computing
Latency	high	low
Delay jitter	High	Very low
Location of server nodes	With in internet	At the edge of local n/w
Distance between the clie nt and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data enrouter	High probability	Very Less probability
Location awareness	No	Yes

FOG COMPUTING AND CLOUD COMPUTING

Requirement	Cloud computing	Fog computing
Geographicaldistribution	Centralized	Distributed
No. of server nodes	Few	Very large
Support for Mobility	Limited	Supported
Real time interactions	Supported	Supported
Type of last mile connecti vity	Leased line	Wireless

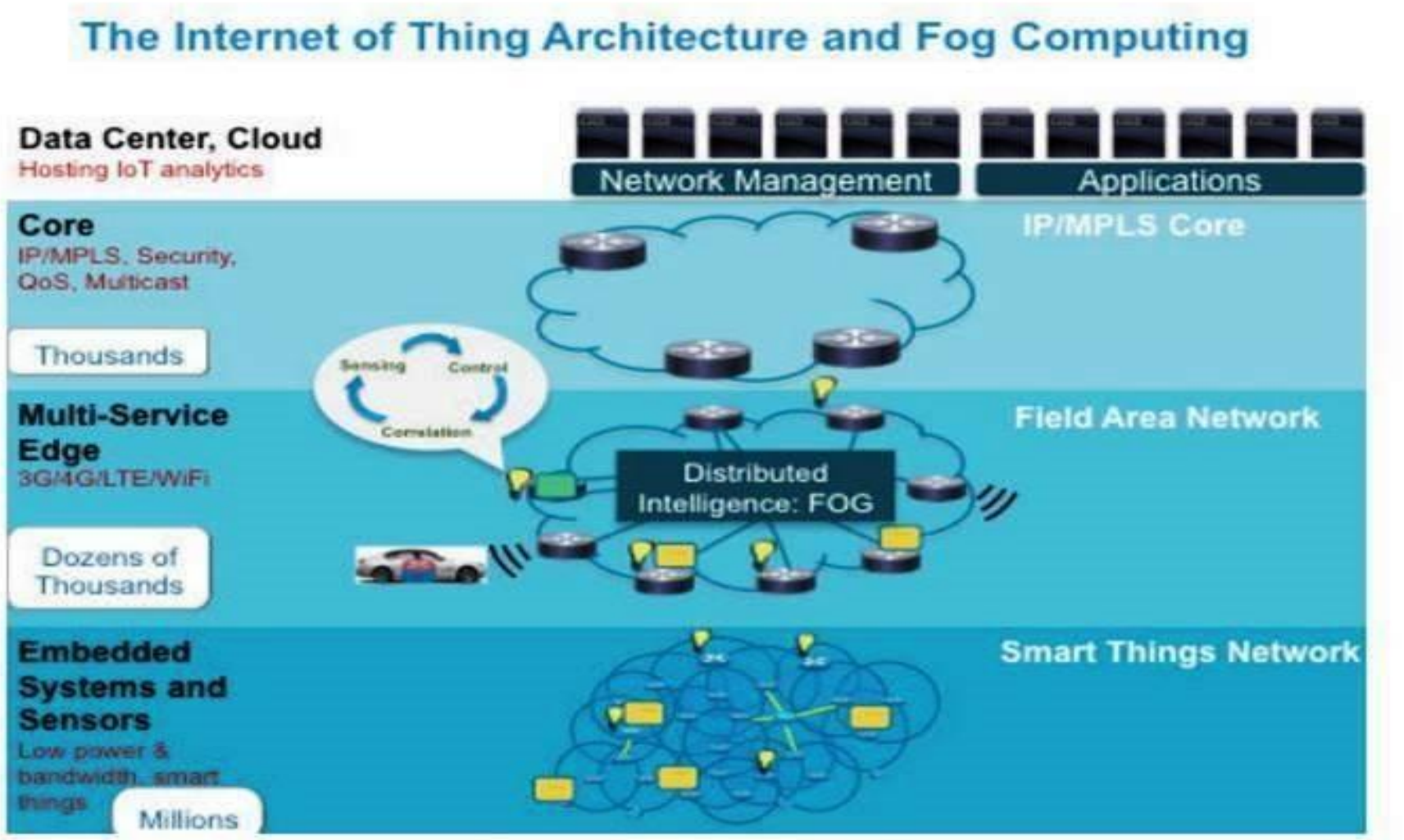
FOG COMPUTING USE-CASES

- **Emergency Evacuation Systems:** Real-time information about currently affected areas of building and exit route planning.
- **Natural Disaster Management:** Real-time notification about landslides, flash floods to potentially affected areas.
- Large sensor deployments generate a lot of data, which can be pre- processed, summarized and then sent to the cloud to reduce congestion in network.
- **Internet of Things (IoT)** based big-data applications: Connected Vehicle, Smart Cities, Wireless Sensors and Actuators Networks(WSANs) etc.

APPLICABILITY

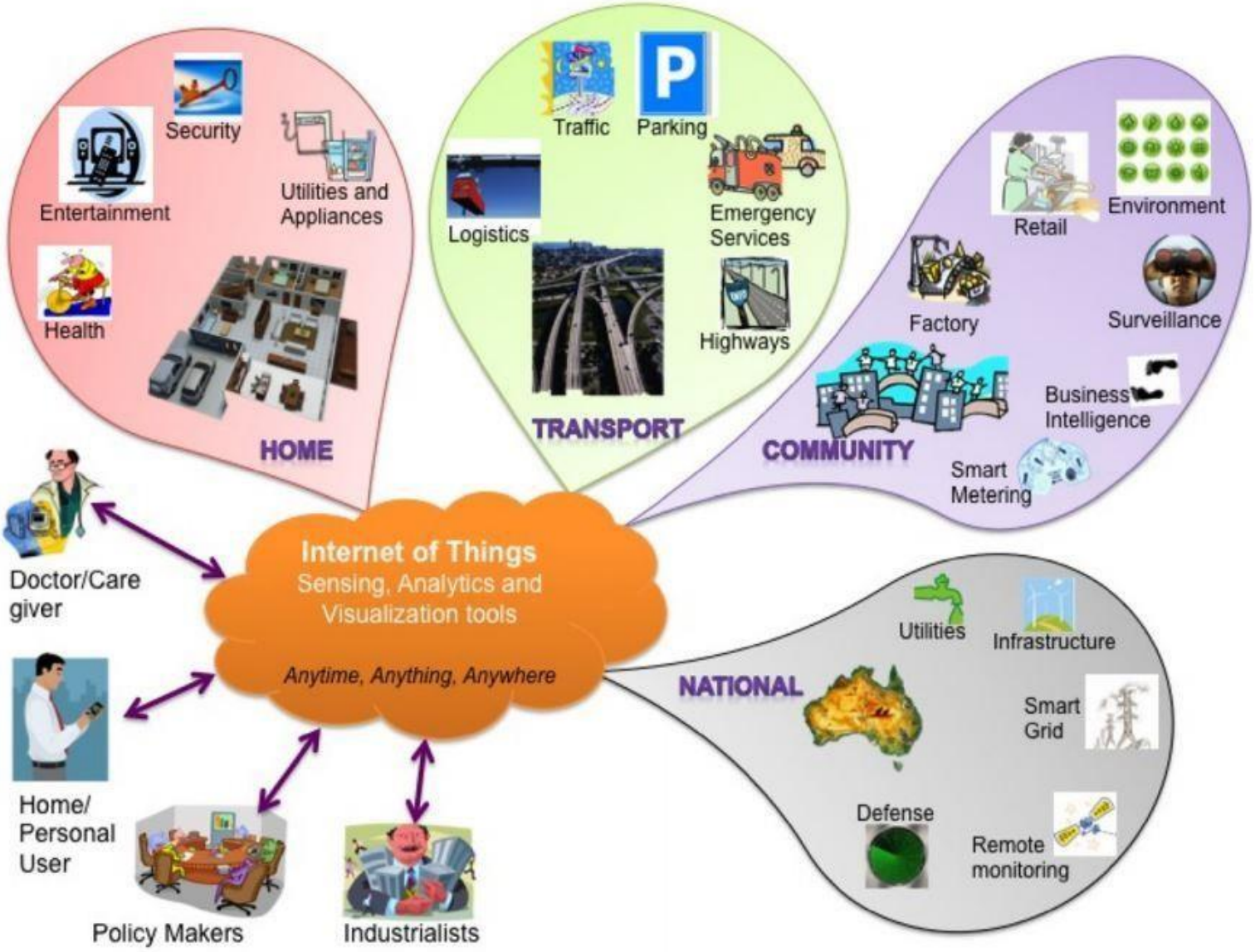
- Smart Grids
- Smart Traffic Lights
- Wireless Sensors
- Internet of Things
- Software Defined Network

FOG COMPUTING AND IOT (INTERNET OF THINGS)



MPLS- Multi Protocol Label Switching- provides a mechanism for forwarding packets for any network protocol

INTERNET OF THINGS

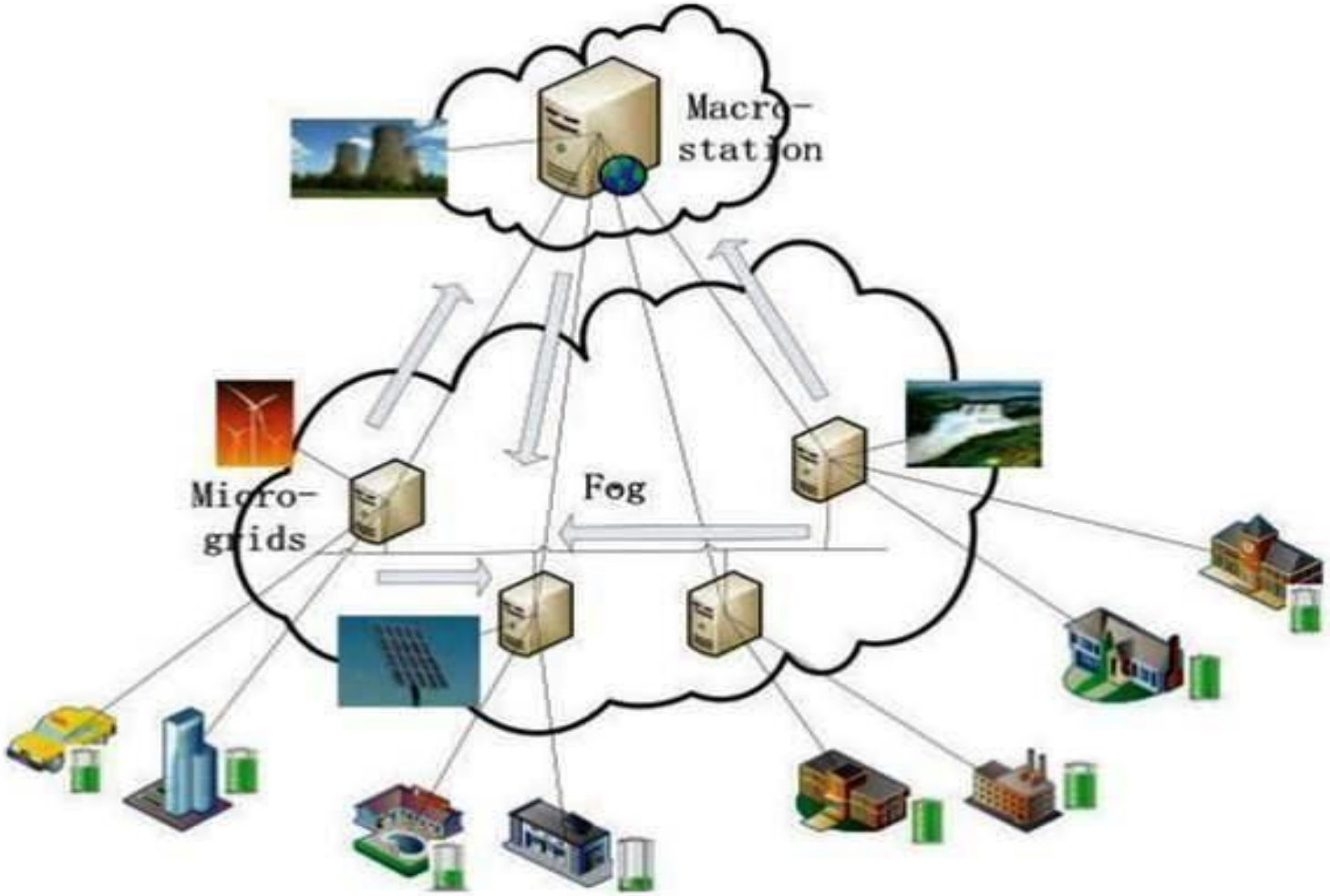


CONNECTED VEHICLE (CV)

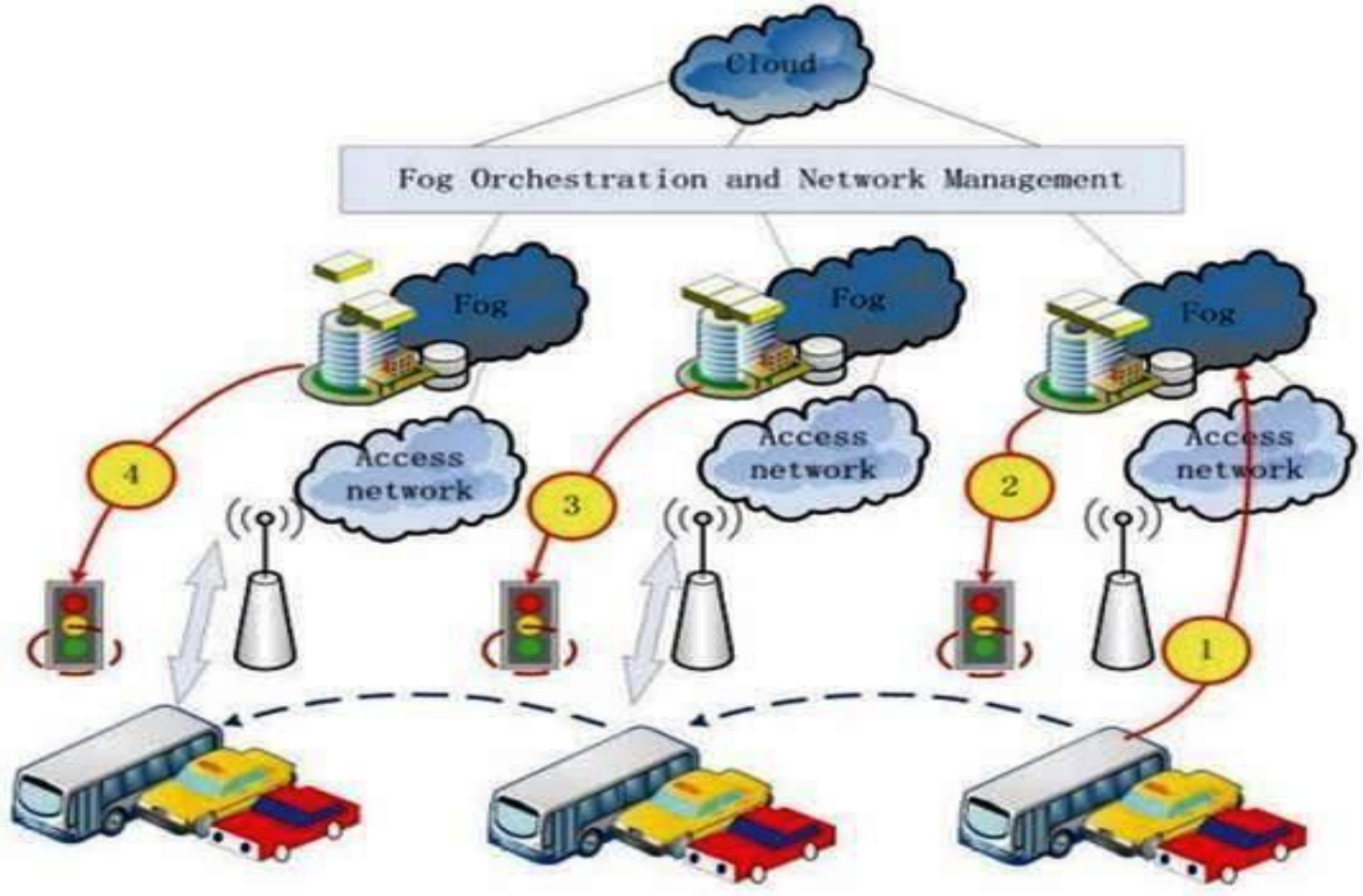
- The Connected Vehicle deployment displays a rich scenario of connectivity and interactions: cars to cars, cars to access points (Wi-Fi, 3G, LTE, roadside units [RSUs], smart traffic lights), and access points to access points.

- The Fog has a number of attributes that make it the ideal platform to deliver a rich menu of SCV services in infotainment, safety, traffic support, and analytics: geo-distribution (throughout cities and along roads), mobility and location awareness, low latency, heterogeneity, and support for real-time interactions.

SMART GRID AND FOG COMPUTING



FOG COMPUTING IN SMART TRAFFIC LIGHTS AND CONNECTED VEHICLES



FOG COMPUTING USE-CASES

- **Emergency Evacuation Systems:** Real-time information about currently affected areas of building and exit route planning.
- **Natural Disaster Management:** Real-time notification about landslides, flash floods to potentially affected areas.
- Large sensor deployments generate a lot of data, which can be pre-processed, summarized and then sent to the cloud to reduce congestion in network.
- **Internet of Things (IoT)** based big-data applications: Connected Vehicle, Smart Cities, Wireless Sensors and Actuators Networks(WSANs) etc.

APPLICABILITY

- Smart Traffic Lights
- Connected Vehicles
- Smart Grids
- Wireless Sensors
- Internet of Things
- Software Defined Network

FOG CHALLENGES

- Fog computing systems suffer from the issue of proper resource allocation among the applications while ensuring the end-to-end latency of the services.
- Resource management of the fog computing network has to be addressed so that the system throughput increases ensuring high availability as well as scalability.
- Security of Applications/Services/Data

RESOURCE MANAGEMENT OF FOG NETWORK

- Utilization of idle fog nodes for better throughput
- More parallel operations
- Handling load balancing
- Meeting the delay requirements of real-time applications
- Provisioning crash fault-tolerance
- More scalable system

RESOURCE MANAGEMENT – CHALLENGES

- Data may not be available at the executing fog node. Therefore, data fetching is needed from the required sensor or data source.
- The executing node might become unresponsive due to heavy workload, which compromises the latency.
- Choosing a new node in case of micro-service execution migration so that the response time gets reduced.
- Due to unavailability of an executing node, there is a need to migrate the partially processed persistent data to a new node. (State migration)

RESOURCE MANAGEMENT – CHALLENGES

- Due to unavailability of an executing node, there is a need to migrate the partially processed persistent data to a new node. (State migration)
- Final result has to transferred to the client or actuator within very less amount of time.
- Deploying application components in different fog computing nodes ensuring latency requirement of the components.
- Multiple applications may collocate in the same fog node. Therefore, the data of one application may get compromised by another application. Data security and integrity of individual applications by resource isolation has to be ensured.

RESOURCE MANAGEMENT – APPROACHES

- Execution migration to the nearest node from the mobile client.
- Minimizing the carbon footprint for video streaming service in fog computing.
- Emphasis on resource prediction, resource estimation and reservation, advance reservation as well as pricing for new and existing IoT customers.
- Docker as an edge computing platform. Docker may facilitate fast deployment, elasticity and good performance over virtual machine based edge computing platform.

RESOURCE MANAGEMENT – APPROACHES

- Resource management based on the fluctuating relinquish probability of the customers, service price, service type and variance of the relinquish probability.
- Studying the base station association, task distribution, and virtual machine placement for cost-efficient fog based medical cyber-physical systems.
- The problem can be formulated into a mixed-integer non-linear linear program and then they linearize it into a mixed integer linear programming (LP).
- LP- based two-phase heuristic algorithm has been developed to address the computation complexity.

FOG - SECURITY ISSUES

- Major security issues are authentication at different levels of gateways as well as in the Fog nodes
- Man-in-the-Middle-Attack
- Privacy Issues
- *In case of smart grids, the smart meters installed in the consumer's home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses.*

SECURITY AND PRI VAC Y ISSUES AND SOLUTIONS OF FOG COMPUTING

Due to its location (ie, close to IoT devices which means protection and surveillance are relatively weak), the Fog will be easier and more accessible than the Cloud, which increases the probability of attacks.

Fog nodes may encounter several malicious attacks (eg, man-in-the-middle, authentication, distributed denial of services DDOS attacks, access control, and fault

tolerance) and new security and privacy challenges. Moreover, while the Cloud has standard security and privacy measures and certifications, the Fog does not have such standards. Hence, the available security and privacy solutions that work for the Cloud may not work efficiently for the Fog.

Fog nodes are an attractive target for many types of attacks.

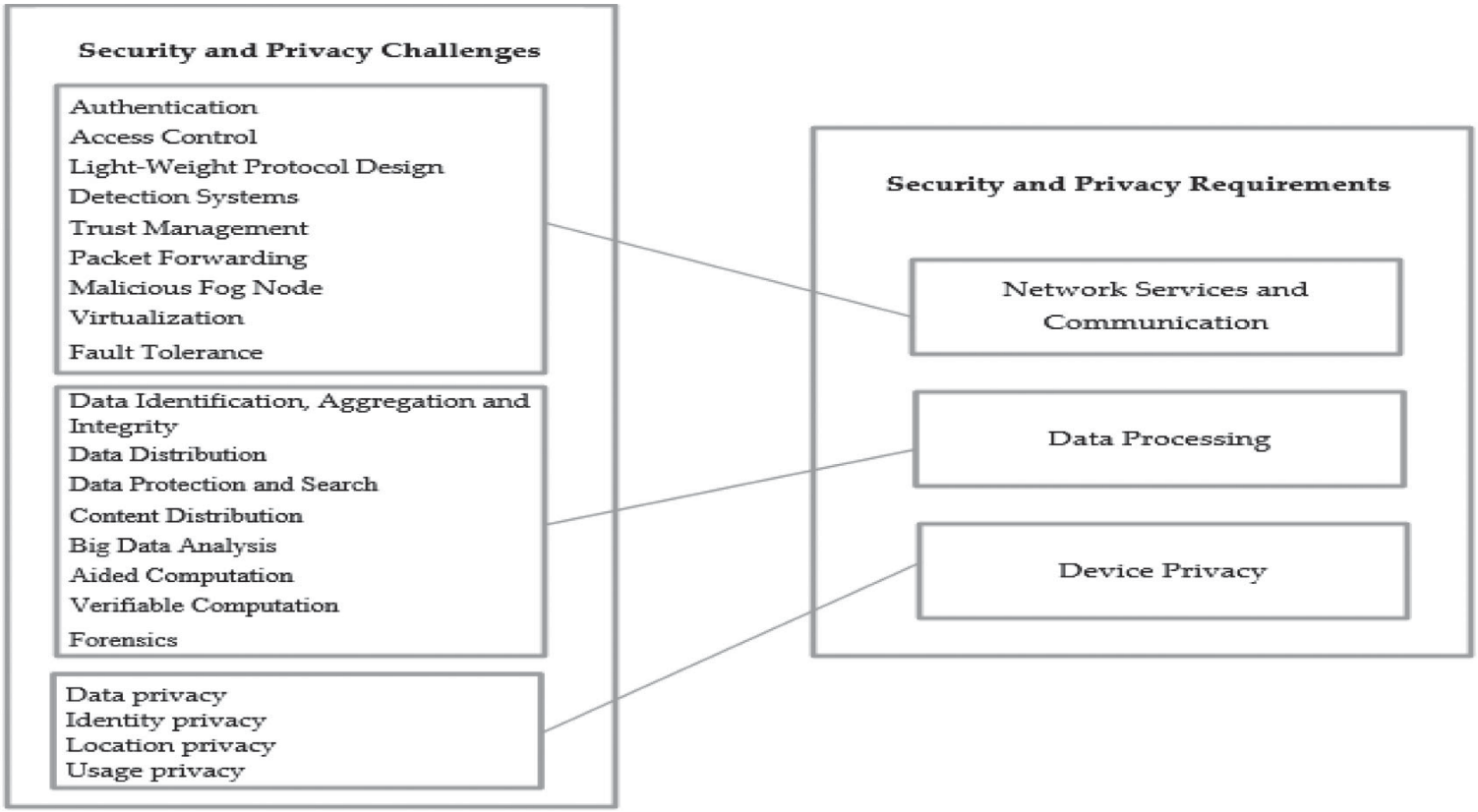
Security and privacy threats

Since the Fog is an extension to Cloud computing, it inherits many threats from the Cloud.Moreover, Fog nodes are “honest but curious” in general.
This is because these nodes are deployed by Fog vendors who are honest in providing certain services to end-users.

However, they may snoop on the content and personal data of the end-users. The providers of Fog may ask the end-users for personal information in order to maintain or fix some issues, which might lead to leakage in the user’s privacy.

Fog nodes are an attractive target for many types of attacks.

Security and Privacy Requirements



THANK YOU

QUIZ

Does fog support IoT concepts.

a) True

b) False