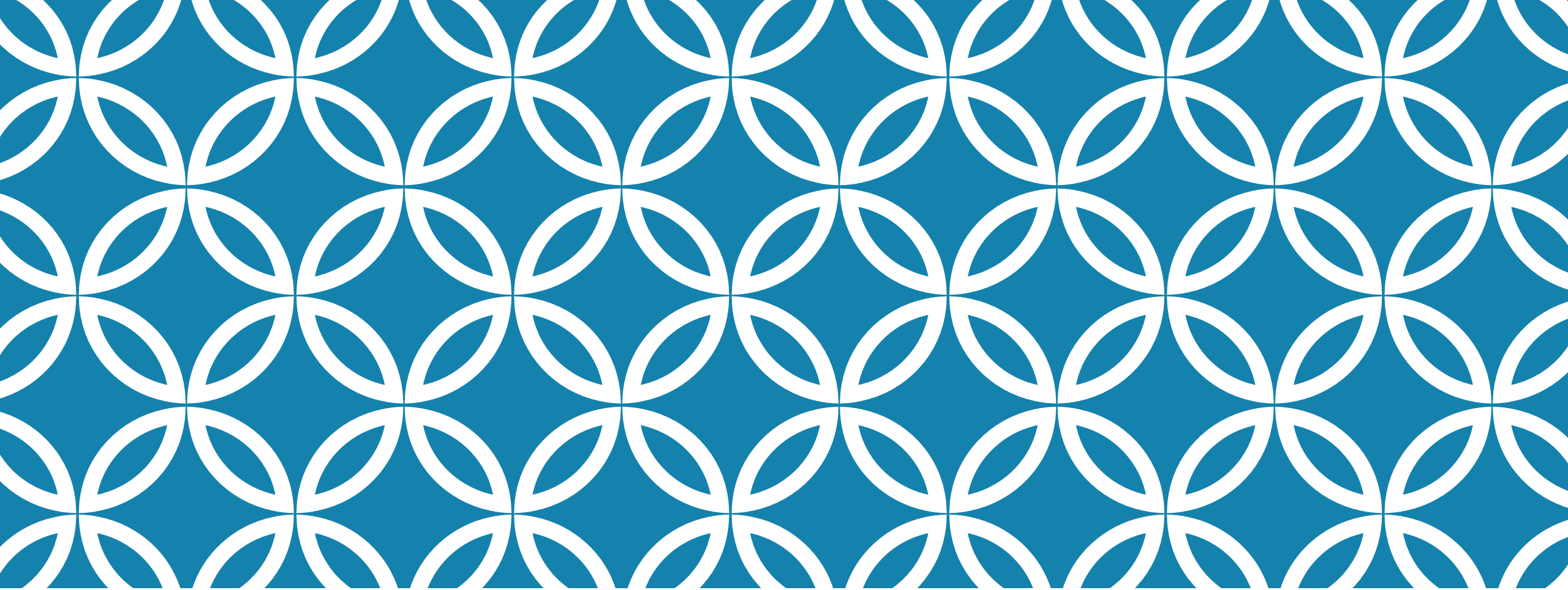
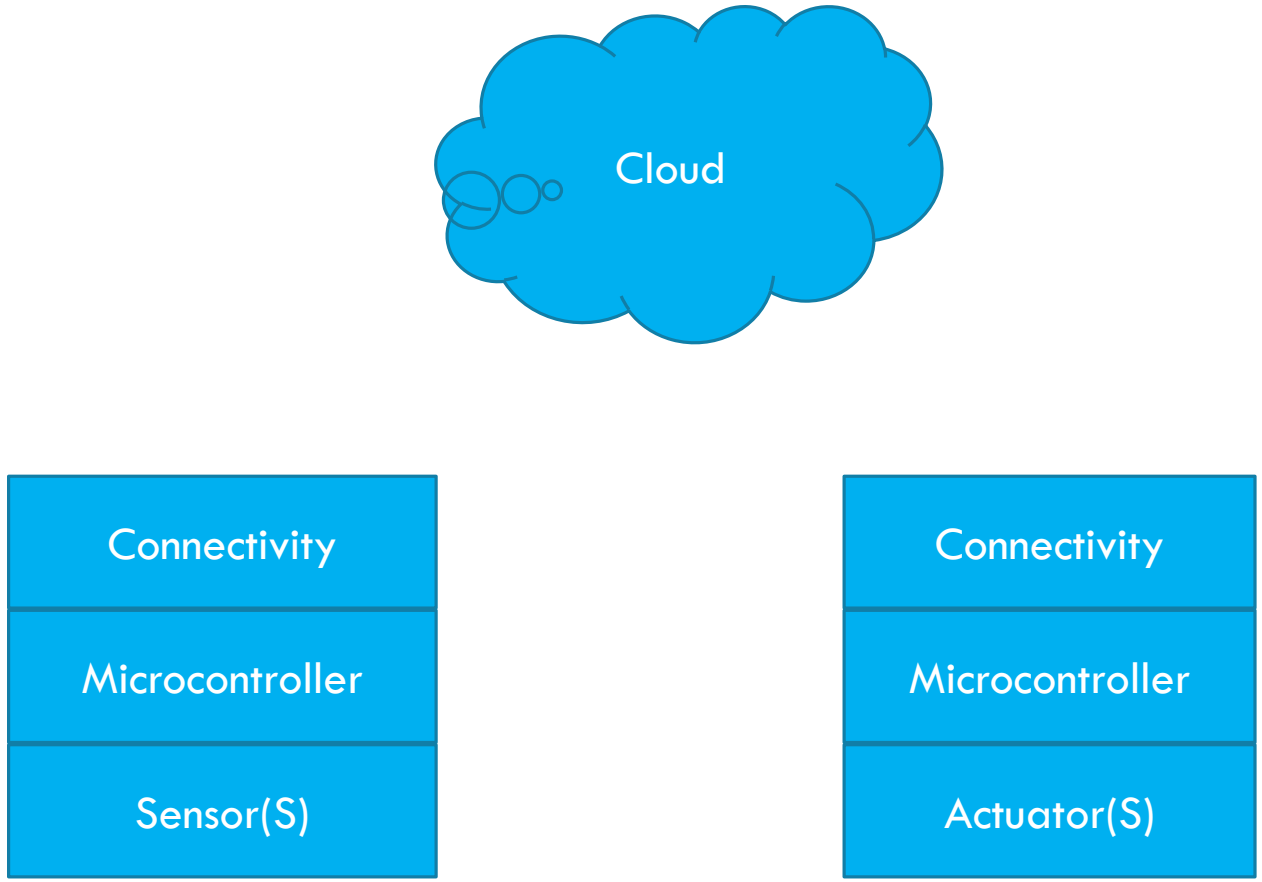


INTRODUCTION TO IOT

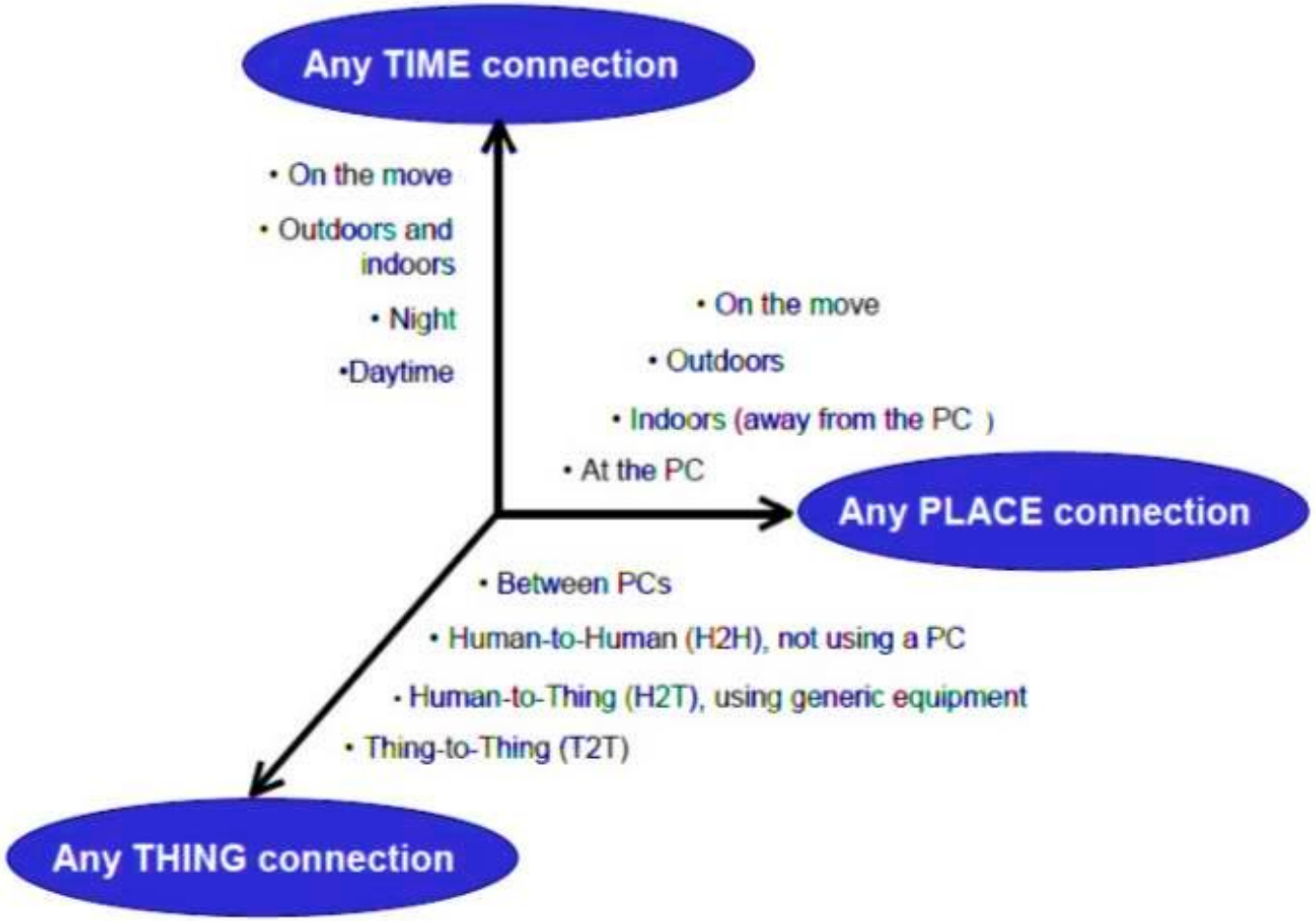
By Rahul Shrivastava

DEFINITION OF IOT

An internetwork of physical objects (Things) embedded with sensors, computers, connectivity & actuators that enables these objects to acquire data, transform it into knowledge, make intelligent decision and generate physical actions to manipulate the environment.



DEFINITION OF IOT



CHARACTERISTICS OF IOT

- **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- **Things-related services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.
- **Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

CHARACTERISTICS OF IOT

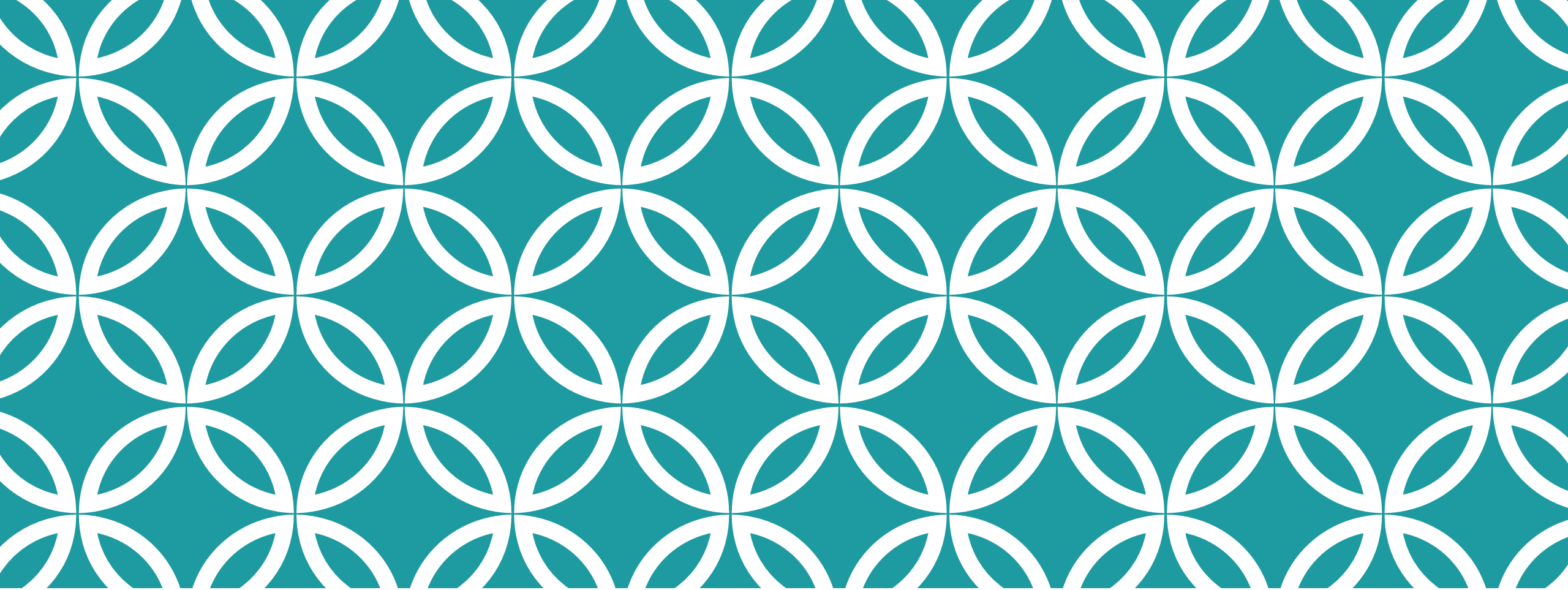
Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

Safety: As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

CHARACTERISTICS OF IOT

Connectivity: Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

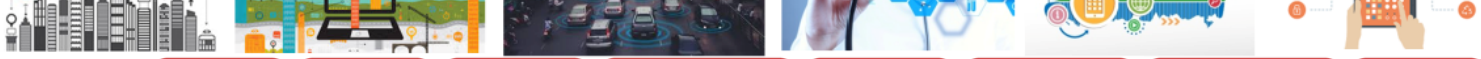


IOT ARCHITECTURAL VIEW

IOT ARCHITECTURAL VIEW

IoT architecture consists of different layers of technologies supporting IoT. It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IoT deployments in different scenarios.

IOT ARCHITECTURAL VIEW



SMART LIVING | SMART CITIES | SMART ENERGY | SMART TRANSPORT | SMART HEALTH | SMART INDUSTRY | SMART BUILDINGS | SMART HOMES

APPLICATION LAYER

IOT APPLICATIONS

SERVICE SUPPORT & APPLICATION SUPPORT LAYER

- VIRTUAL ENTITY
- VIRTUAL ENTITY & IOT SERVICE MANAGMENT
- VIRTUAL ENTITY SERVICE
- IOT BUSINESS PROCESS MANAGMENT
- BUSINESS PROCESS EXECUTION
- BUSINESS PROCESS MODELING
- MANGMENT CAPABILITIES
- GENERIC/SPECIFIC MANAGMENT
- DEVICE MANAGER
- QOS MANAGER
- SECURITY
- AUTHENTICATION
- IDENTITY MANGMT
- ACEESS CONTROL
- ENCRYPTION
- DATA MANGMENT
- DATA GOVERNENCE
- DATA QUALITY MANGMT
- DATA MINING
- ANLYTICS PLATFORM
- IN MOTION ANALITICS
- PREDICTIVE ANALITICS
- STATISTICAL ANALITICS

NETWORK / COMMUNICATION LAYER

- NETWORKING CAPABILITY
- TRANSPORT CAPABILITY
- GATEWAY NETWORK: WI-FI | GSM/GPRS | LTE | ETHERNET
- GATEWAY: EMEDDED & SIGNALPROSESSOR | OS | SIM MODULE | MICROCONTROLLER

SMART DEVICE / SENSOR LAYER

SENSOR NETWORKS

WI-FI | ZigBee | ETHERNET | BLUETOOTH | UWB | WIRED

SENSORS: ANALOG | DIGITAL | RFID | ELECTRO-MECH | PHOTO-ELECTRIC | GPS | SOLID STATE | INFRA-RED | GYROSCOPE | ELECTRO-CHEMICAL

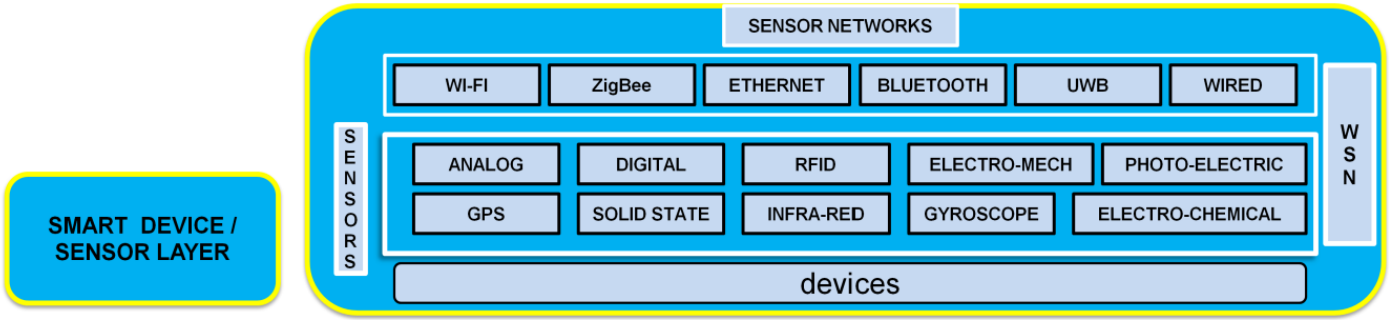
WSN

devices

IOT ARCHITECTURAL VIEW

SMART DEVICE / SENSOR LAYER

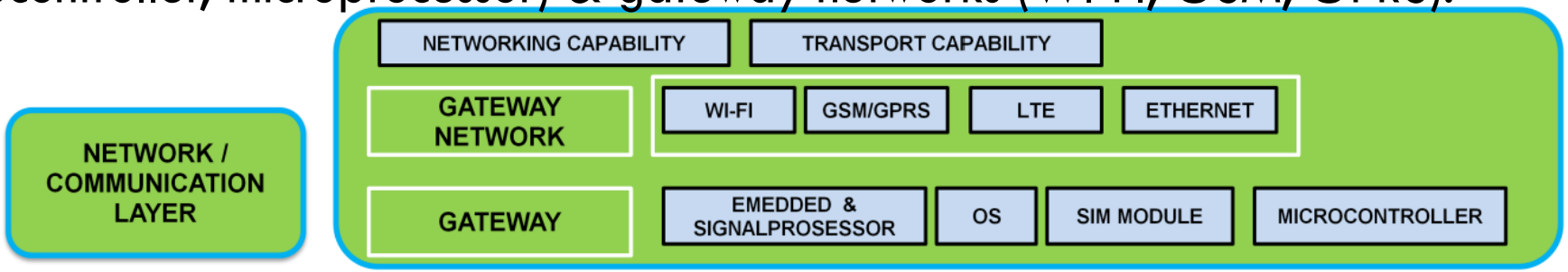
Smart device / sensor layer: The lowest layer is made up of smart objects integrated with sensors. The sensors enable the interconnection of the physical and digital worlds allowing real-time information to be collected and processed. There are various types of sensors for different purposes. The sensors have the capacity to take measurements such as temperature, air quality, speed, humidity, pressure, flow, movement and electricity etc. In some cases, they may also have a degree of memory, enabling them to record a certain number of measurements. A sensor can measure the physical property and convert it into signal that can be understood by an instrument. Sensors are grouped according to their unique purpose such as environmental sensors, body sensors, home appliance sensors and vehicle telemetric sensors, etc



IOT ARCHITECTURAL VIEW

NETWORK / COMMUNICATION LAYER

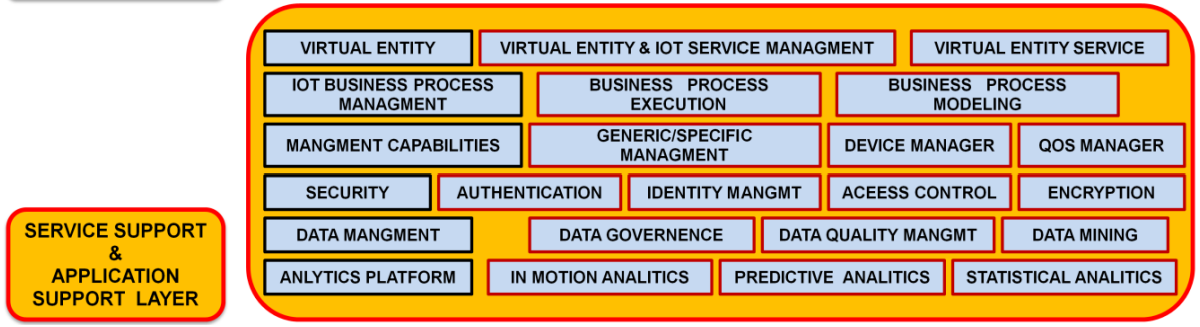
Network / Communication Layer: Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Current networks, often tied with very different protocols, have been used to support machine-to-machine (M2M) networks and their applications. With demand needed to serve a wider range of IoT services and applications such as high speed transactional services, context- aware applications, etc, multiple networks with various technologies and access protocols are needed to work with each other in a heterogeneous configuration. These networks can be in the form of a private, public or hybrid models and are built to support the communication requirements for latency, bandwidth or security. Various gateways (microcontroller, microprocessor) & gateway networks (WI-FI, GSM, GPRS).



IOT ARCHITECTURAL VIEW

MANAGEMENT SERVICE LAYER

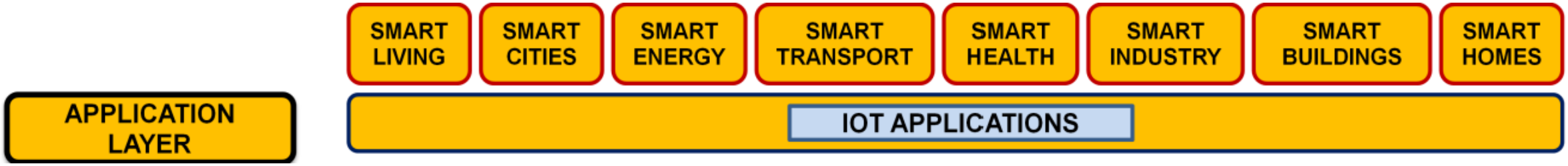
Management Service Layer: The management service renders the processing of information possible through analytics, security controls, process modeling and management of devices. One of the important features of the management service layer is the business and process rule engines. IoT brings connection and interaction of objects and systems together providing information in the form of events or contextual data such as temperature of goods, current location and traffic data. Some of these events require filtering or routing to post-processing systems such as capturing of periodic sensory data, while others require response to the immediate situations such as reacting to emergencies on patient's health conditions. The rule engines support the formulation of decision logics and trigger interactive and automated processes to enable a more responsive IoT system.

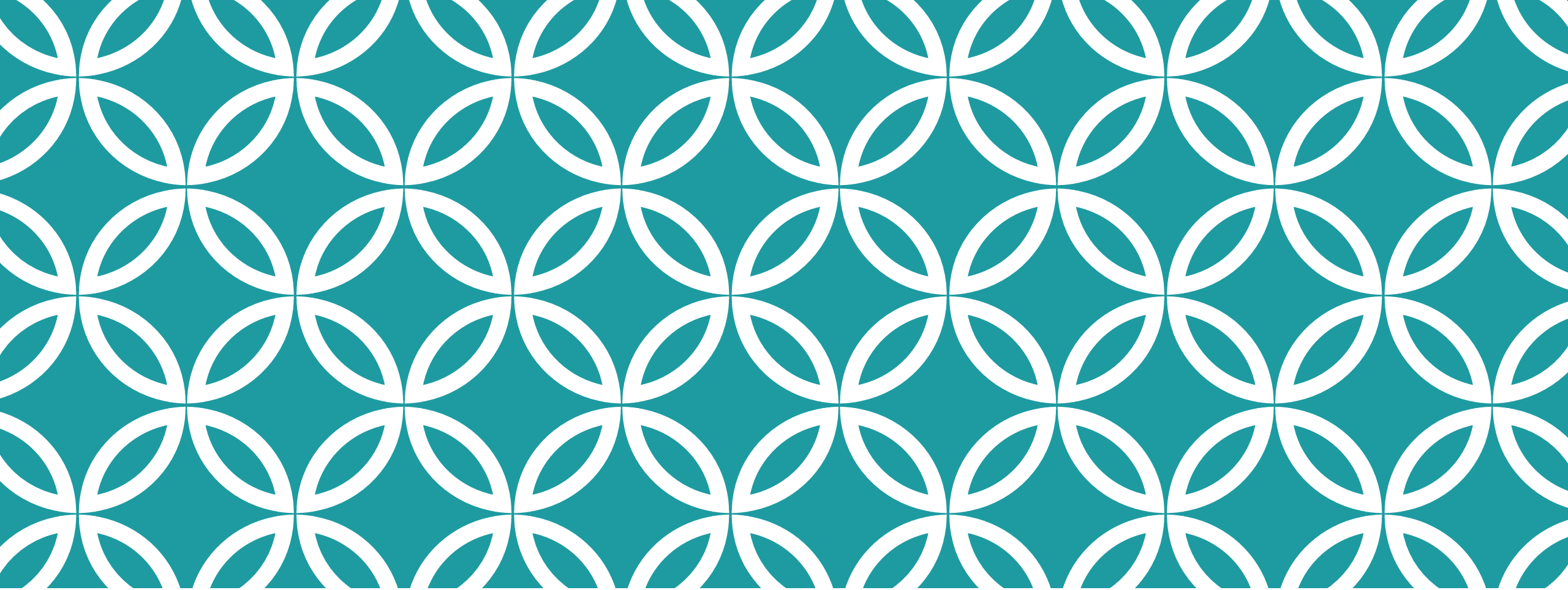


IOT ARCHITECTURAL VIEW

APPLICATION LAYER

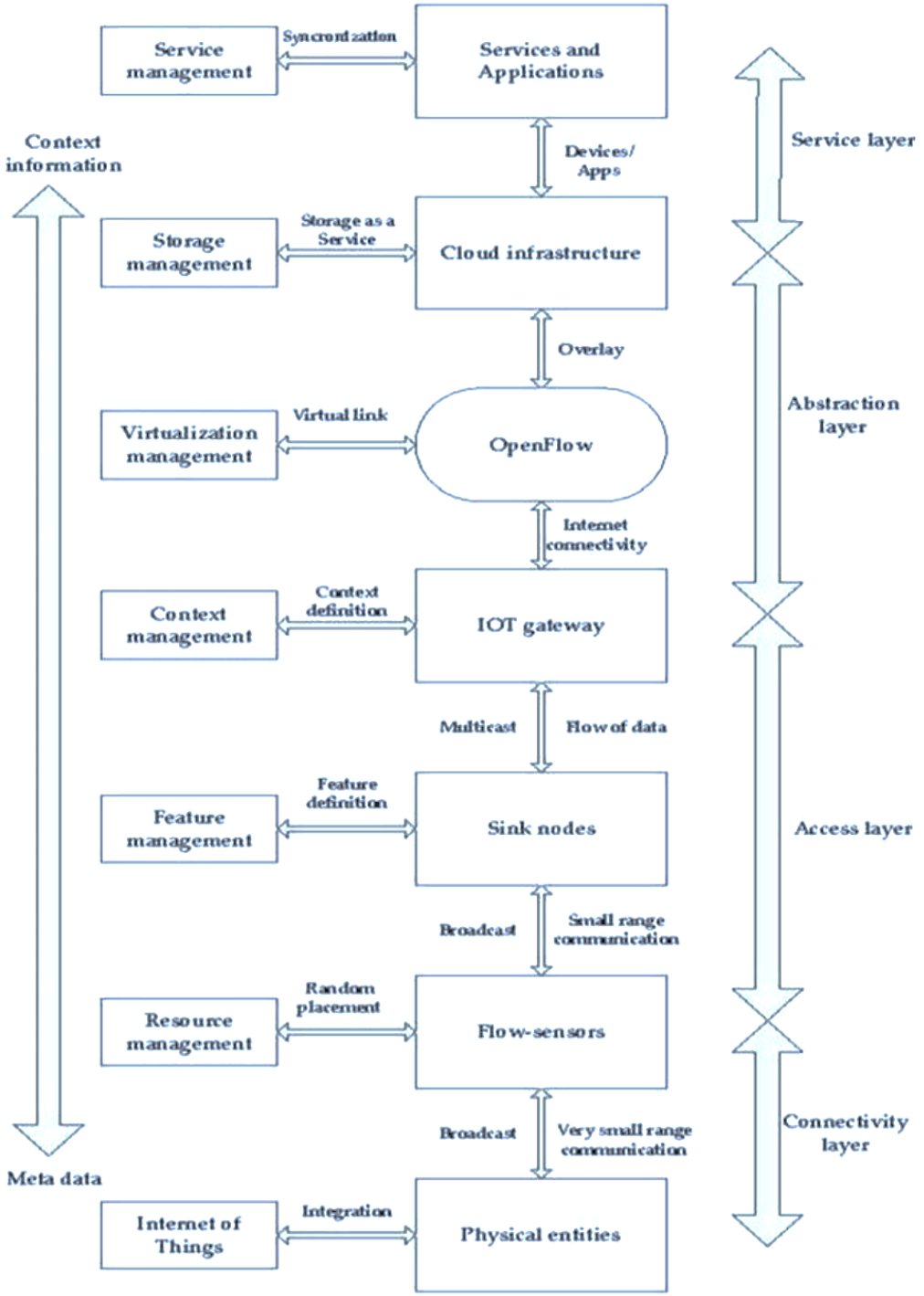
Application Layer-The IoT application covers "smart" environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy.





IOT CONCEPTUAL FRAMEWORK

IOT CONCEPTUAL FRAMEWORK

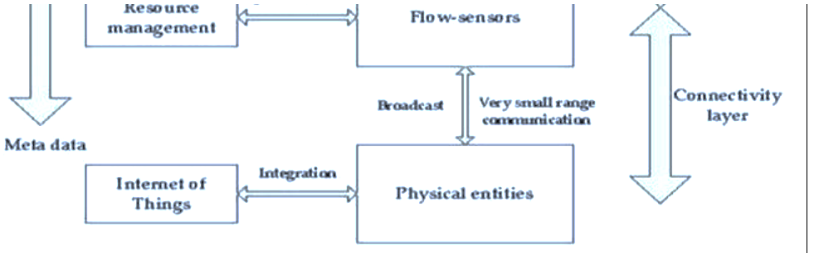


IOT CONCEPTUAL FRAMEWORK

- The main tasks of this framework are to analyze and determine the smart activities of these intelligent devices through maintaining a dynamic interconnection among those devices.
- This model is capable of logical division of physical devices placement, creation of virtual links among different domains, networks and collaborate among multiple application without any central coordination system. IaaS can afford standard functionalities to accommodate and provides access to cloud infrastructure.
- Total infrastructure system can be categorized into 4 layers

IOT CONCEPTUAL FRAMEWORK

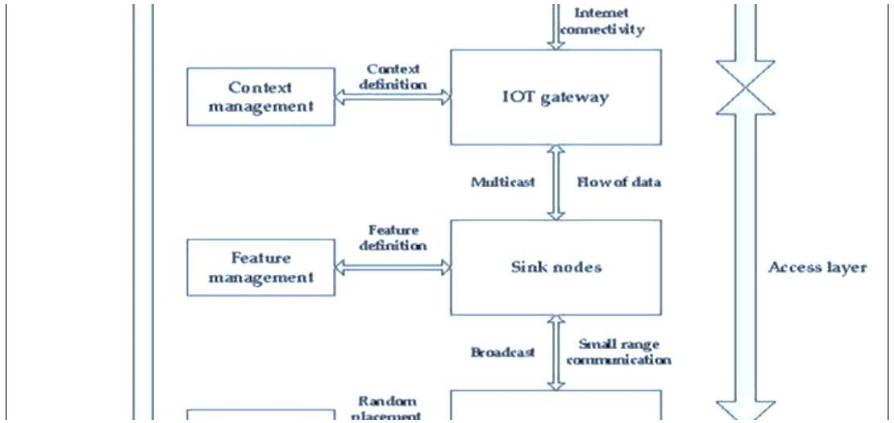
1. CONNECTIVITY LAYER



- This layer includes all the physical devices involved in the framework and the interconnection among them.
- Future internet largely depends on the unification of these common objects found everywhere near us and these should be distinctly identifiable and controllable.
- This layer also involves assigning of low range networking devices like sensors, actuators, RFID tags etc and resource management checks the availability of physical resources of all the devices and networks involved in the underlying infrastructure.
- These devices contain very limited resources and resource management ensures the maximum utilization with little overhead. It also allows sharing and distribution of information among multiple networks or single network divided into multiple domains.

IOT CONCEPTUAL FRAMEWORK

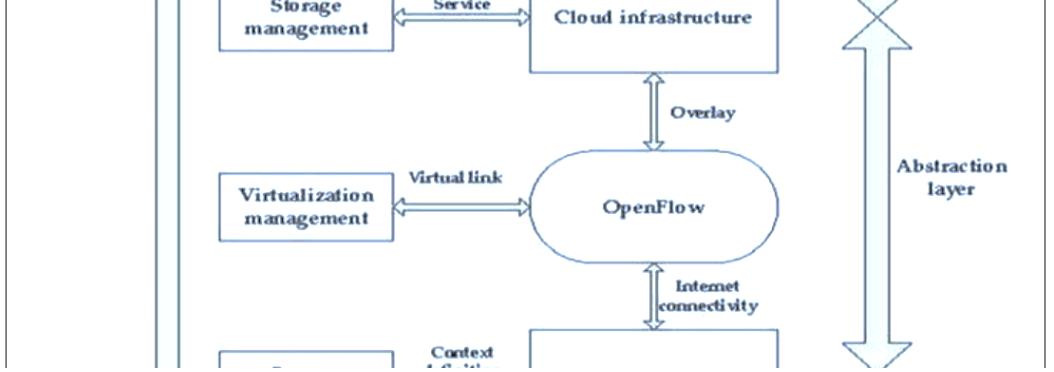
2. ACCESS LAYER



- Context Data will be reached to internet via IoT Gateway as captured by short range devices in form of raw data.
- Access layer comprises topology definition, network initiation, creation of domains etc.
- This layer also includes connection setup, intra-inter domain communication, scheduling, packet transmissions between flow-sensors and IoT gateway.
- Feature management contains a feature filter which accepts only acceptable context data and redundant data are rejected
- Large number of sensor maintains lots of features but only a small subset of features is useful generate a context data.
- Feature filter helps to reduce irrelevant data transmission, increases the data o transfer rate of useful data and reduce energy and CPU consumption too

IOT CONCEPTUAL FRAMEWORK

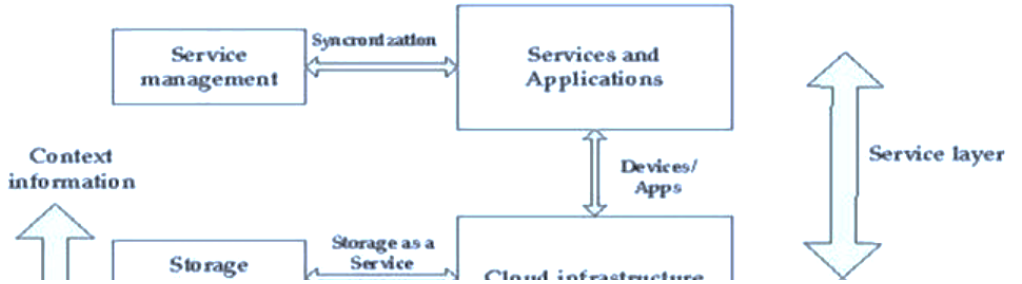
3. ABSTRACTION LAYER



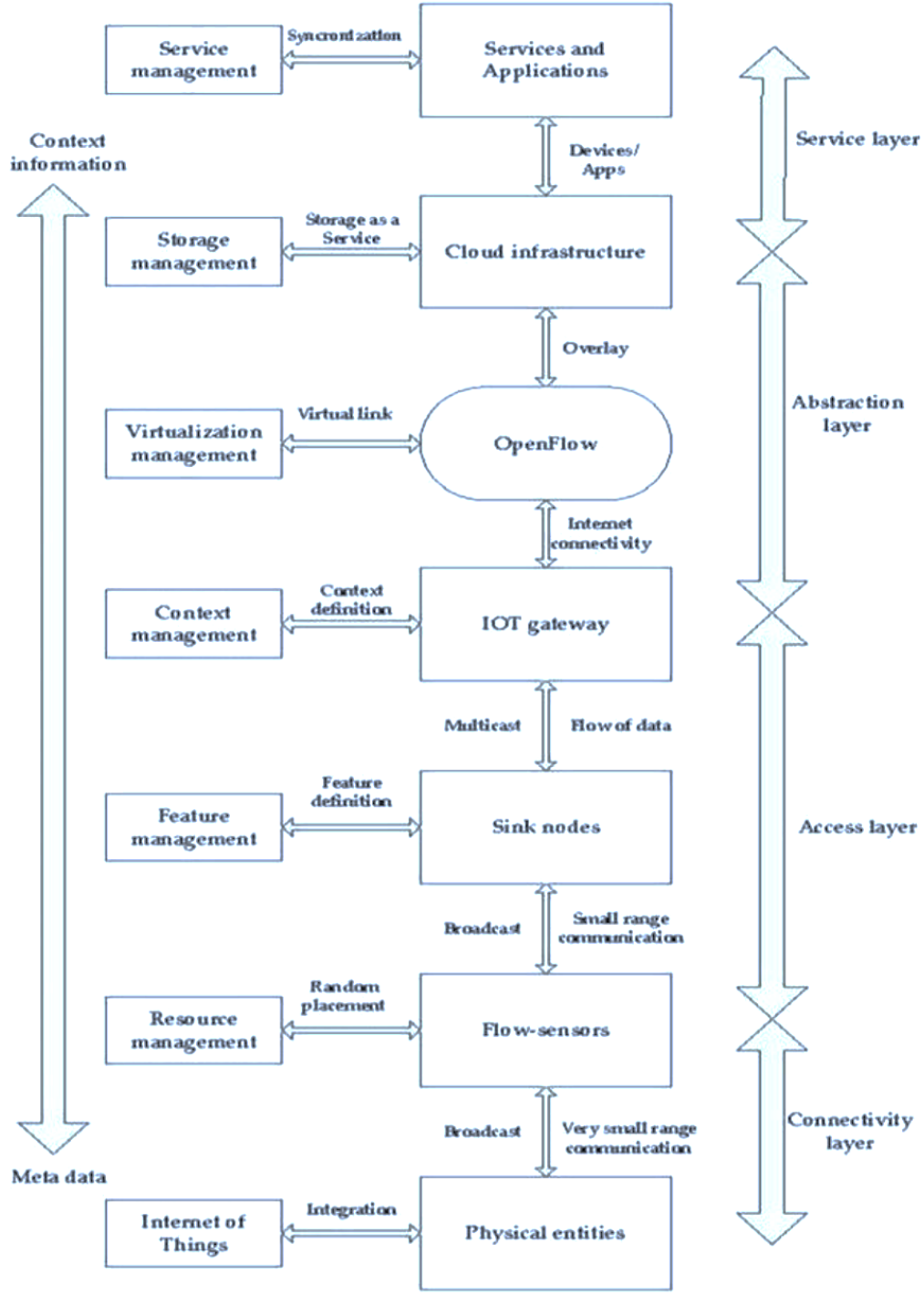
- One of the most important characteristics of Open Flow is to add virtual layers with the preset layers, leaving the established infrastructure unchanged.
- A virtual link can be created among different networks and a common platform can be developed for various communication systems.
- The system is fully a centralized system from physical layer viewpoint but a distribution of service (flow visor could be utilized) could be maintained.
- One central system can monitor, control all sorts of traffics. It can help to achieve better band-width, reliability, robust routing, etc. which will lead to a better Quality of Services (QoS).

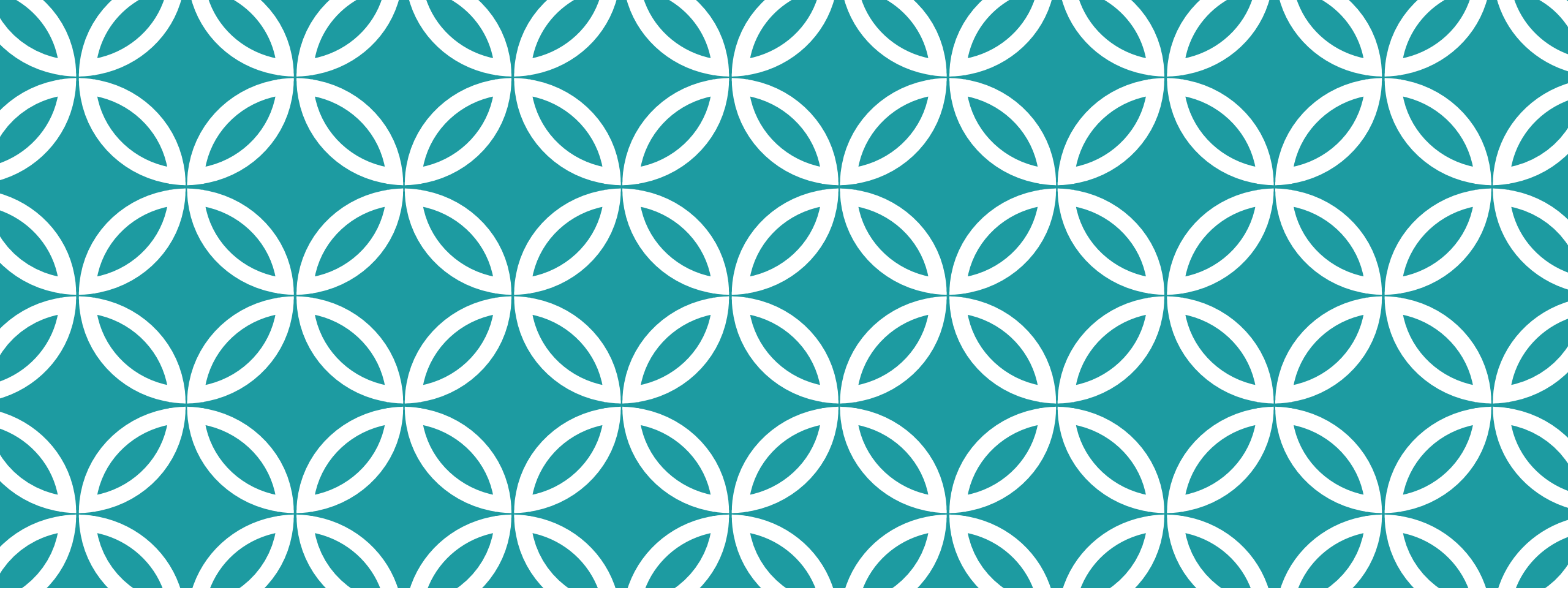
IOT CONCEPTUAL FRAMEW

4. SERVICE LAYER



- It is not only responsible for storing data but also to provide security along with it. It also allows accessing data effectively.
- integrating data to enhance service intelligence, analysis based on the services required and most importantly increases the storage efficiency.
- Storage and management layer involves data storage & system supervision, software services and business management & operations.
- Though they are included in one layer, the business support system resides slightly above of cloud computing service whereas Open-Flow is placed below of it as presented to include virtualizations and monitor management.
- Service management combines the required services with organizational solutions and thus new generation user service becomes simplified.


Service management
Syncronization
Services and Applications
Service layer
Context information
Devices/ Apps
Storage management
Storage as a Service
Cloud infrastructure
Overlay
Virtualization management
Virtual link
OpenFlow
Abstraction layer
Internet connectivity
Context management
Context definition
IOT gateway
Multicast
Flow of data
Feature management
Feature definition
Sink nodes
Access layer
Broadcast
Small range communication
Resource management
Random placement
Flow-sensors
Broadcast
Very small range communication
Connectivity layer
Meta data
Internet of Things
Integration
Physical entities



PHYSICAL DESIGN OF IOT

PHYSICAL DESIGN OF IOT

- The Internet of Things will become part of the fabric of everyday life.
- It will become part of our overall infrastructure just like water, electricity, telephone, TV and most recently the Internet.
- Whereas the current Internet typically connects full-scale computers, the Internet of Things (as part of the Future Internet) will connect everyday objects with a strong integration into the physical world.

PHYSICAL DESIGN OF IOT

1. PLUG AND PLAY INTEGRATION

- If we look at IoT-related technology available today, there is a huge heterogeneity.
- It is typically deployed for very specific purposes and the configure requires significant technical knowledge and may be cumbersome.
- To achieve a true Internet of Things we need to move away from such small- scale, vertical application silos, towards a horizontal infrastructure on which a variety of applications can run simultaneously.
- This is only possible if connecting a thing to the Internet of Things becomes as simple as plugging it in and switching it on.
- Such plug and play functionality requires an infrastructure that supports it, starting from the networking level and going beyond it to the application level. This is closely related to the aspects discussed in the section on autonomy.

PHYSICAL DESIGN OF IOT

1. PLUG AND PLAY INTEGRATION

- On the networking level, the plug & play functionality has to enable the communication, features like the ones provided by IPv6 are in the directions to help in this process.
- Suitable infrastructure components have then to be discovered to enable the integration into the Internet of Things. This includes announcing the functionalities provided, such as what can be sensed or what can be actuated.

PHYSICAL DESIGN OF IOT

2. INFRASTRUCTURE FUNCTIONALITY

- The infrastructure needs to support applications in finding the things required.
- An application may run anywhere, including on the things themselves.
- Finding things is not limited to the start-up time of an application.
- Automatic adaptation is needed whenever relevant new things become available, things become unavailable or the status of things changes.
- The infrastructure has to support the monitoring of such changes and the adaptation that is required as a result of the changes.

PHYSICAL DESIGN OF IOT

3. SEMANTIC MODELING OF THINGS

- To reach the full potential of the Internet of Things, semantic information regarding the things, the information they can provide or the actuations they can perform need to be available.
- It is not sufficient to know that there is a temperature sensor or an electric motor, but it is important to know which temperature the sensor measures: the indoor temperature of a room or the temperature of the fridge, and that the electric motor can open or close the blinds or move something to a different location.
- As it may not be possible to provide such semantic information by simply switching on the thing, the infrastructure should make adding it easy for users.
- Also, it may be possible to derive semantic information, given some basic information and additional knowledge, e.g. deriving information about a room, based on the information that a certain sensor is located in the room. This should be enabled by the infrastructure.

PHYSICAL DESIGN OF IOT

4. PHYSICAL LOCATION AND POSITION

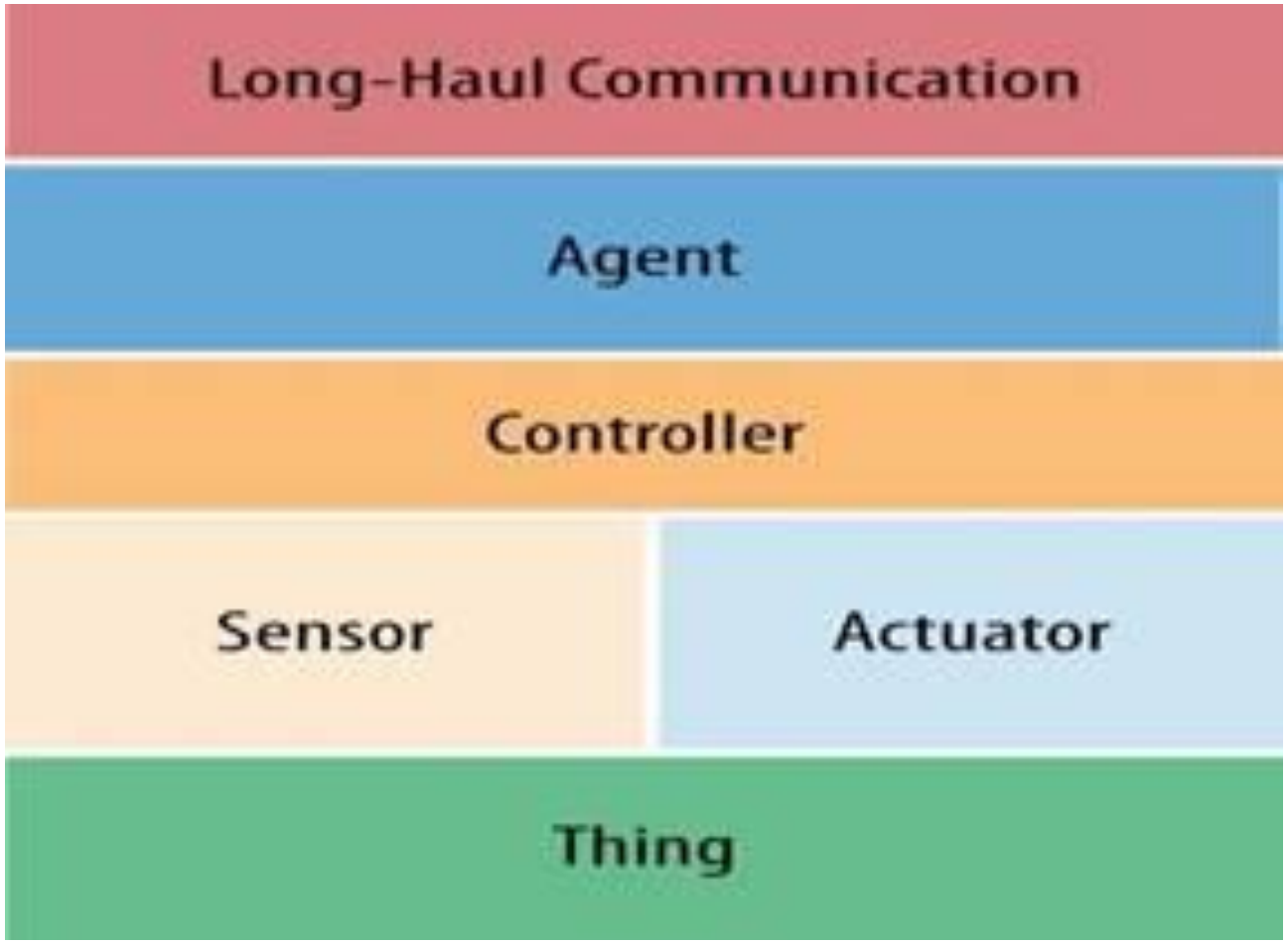
- As the Internet of Things is strongly rooted in the physical world, the notion of physical location and position are very important, especially for finding things, but also for deriving knowledge.
- Therefore, the infrastructure has to support finding things according to location (e.g. geo-location based discovery). Taking mobility into account, localization technologies will play an important role for the Internet of Things and may become embedded into the infrastructure of the Internet of Things.

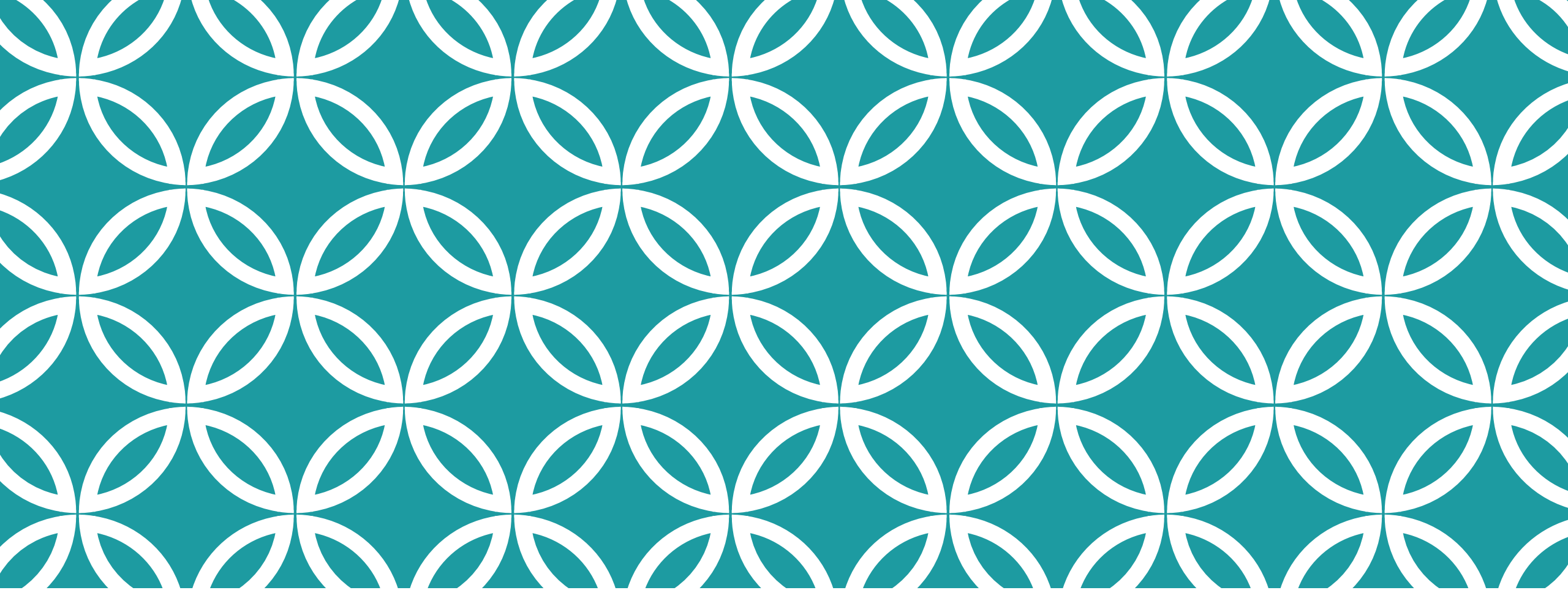
PHYSICAL DESIGN OF IOT

5. SECURITY AND PRIVACY

- In addition, an infrastructure needs to provide support for security and privacy functions including identification, confidentiality, integrity, non-repudiation authentication and authorization.
- Here the heterogeneity and the need for interoperability among different ICT systems deployed in the infrastructure and the resource limitations of IoT devices (e.g., Nano sensors) have to be taken into account.

LOGICAL IOT ARCHITECTURE





IOT APPLICATIONS

IOT APPLICATIONS

The IoT application covers smart environments/spaces in domains such as:

Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy.

Following are some of the IoT applications.

IOT APPLICATIONS

IOSL (INTERNET OF SMART LIVING)-REMOTE CONTROL APPLIANCES

- Weather: Displays outdoor weather conditions such as humidity, temperature, pressure, wind speed and rain levels with ability to transmit data over long distances
- Smart Home Appliances: Refrigerators with LCD screen telling what's inside, food that's about to expire, ingredients you need to buy and with all the information available on a Smartphone app.
- Washing machines allowing you to monitor the laundry remotely, and Kitchen ranges with interface to a Smartphone app allowing remotely adjustable temperature control and monitoring the oven's self-cleaning feature
- Safety Monitoring: cameras, and home alarm systems making people feel safe in their daily life at home,
- Intrusion Detection Systems: Detection of window and door openings and violations to prevent intruders
- Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.

IOT APPLICATIONS

IOSC (INTERNET OF SMART CITIES)

- Structural Health: Monitoring of vibrations and material conditions in buildings, bridges and historical monuments
- Lightning: intelligent and weather adaptive lighting in street lights
- Safety: Digital video monitoring, fire control management, public announcement systems,
- Transportation: Smart Roads and Intelligent High-ways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams
- Smart Parking: Real-time monitoring of parking spaces availability in the city making residents able to identify and reserve the closest available spaces
- Waste Management: Detection of rubbish levels in containers to optimize the trash collection routes. Garbage cans and recycle bins with RFID tags allow the sanitation staff to see when garbage has been put out.

IOT APPLICATIONS

IOSE (INTERNET OF SMART ENVIRONMENT)

- Air Pollution monitoring: Control of CO2 emissions of factories, pollution emitted by cars and toxic gases generated in farms
- Forest Fire Detection: Monitoring of combustion gases and preemptive fire conditions to define alert zones
- Weather monitoring: weather conditions monitoring such as humidity, temperature, pressure, wind speed and rain, Earthquake Early Detection
- Water Quality: Study of water suitability in rivers and the sea for eligibility in drinkable use
- River Floods: Monitoring of water level variations in rivers, dams and reservoirs during rainy days
- Protecting wildlife: Tracking collars utilizing GPS/GSM modules to locate and track wild animals and communicate their coordinates via SMS.

IOT APPLICATIONS

IOSI (INTERNET OF SMART INDUSTRY)

- Explosive and Hazardous Gases: Detection of gas levels and leakages in industrial environments, surroundings of chemical factories and inside mines, Monitoring of toxic gas and oxygen levels inside chemical plants to ensure workers and goods safety, Monitoring of water, oil and gas levels in storage tanks and Cisterns,
- Maintenance and repair: Early predictions on equipment malfunctions and service maintenance can be automatically scheduled ahead of an actual part failure by installing sensors inside equipment to monitor and send reports.

IOT APPLICATIONS

IOSH (INTERNET OF SMART HEALTH)-PATIENTS SURVEILLANCE:

- Monitoring of conditions of patients inside hospitals and in old people's home, Medical Fridges: Control of conditions inside freezers storing vaccines, medicines and organic elements
- Fall Detection: Assistance for elderly or disabled people living independent,
- Physical Activity Monitoring: Wireless sensors placed across the mattress sensing small motions, like breathing and heart rate and large motions caused by tossing and turning during sleep, providing data available through an app on the Smartphone.

IOT APPLICATIONS

IOSA (INTERNET OF SMART AGRICULTURE)-GREEN HOUSES:

- Control micro-climate conditions to maximize the production of fruits and vegetables and its quality
- Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc.
- Animal Farming/Tracking: Location and identification of animals grazing in open pastures or location in big stables, Study of ventilation and air quality in farms and detection of harmful gases from excrements
- Field Monitoring: Reducing spoilage and crop waste with better monitoring, accurate ongoing data obtaining, and management of the agriculture fields, including better control of fertilizing, electricity and watering.

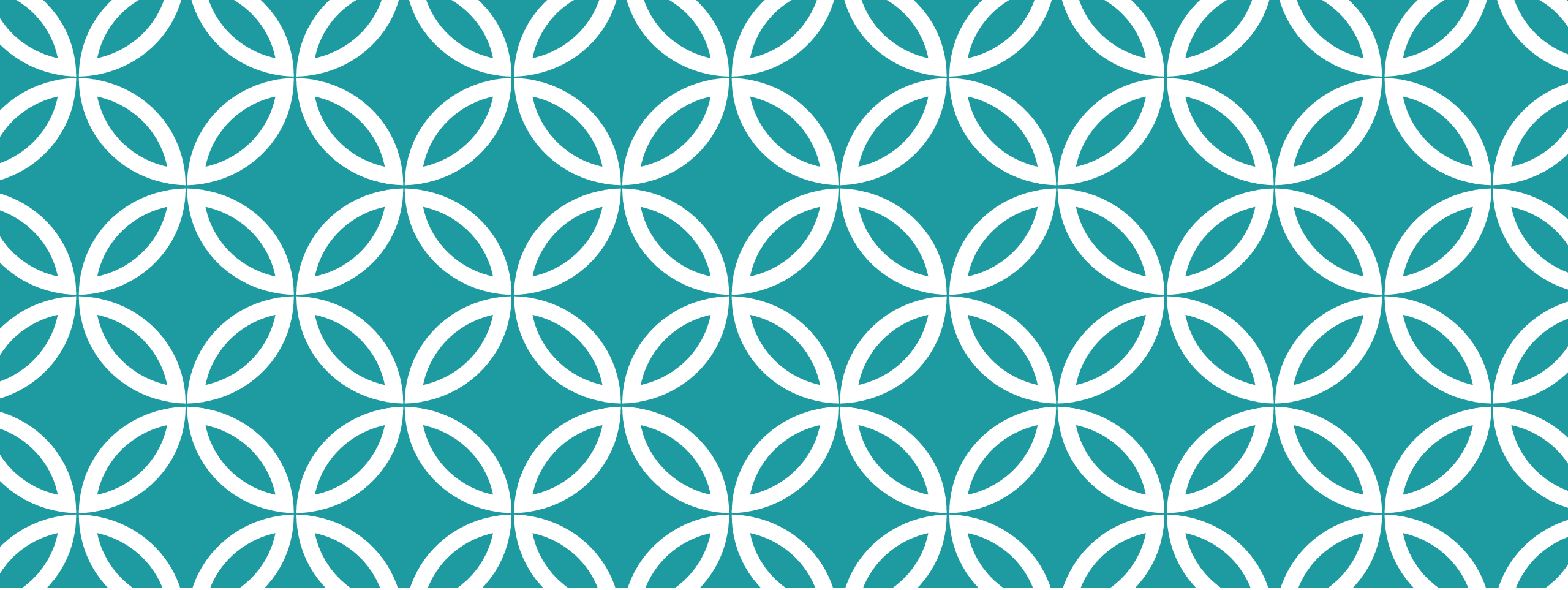
M2M

MACHINE-TO-MACHINE (M2M)

- Machine to machine (M2M) is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.
- M2M communication is often used for remote monitoring. In product restocking, for example, a vending machine can message the distributor when a particular item is running low.
- M2M communication is an important aspect of warehouse management, remote control, robotics, traffic control, logistic services, supply chain management, fleet management and telemedicine.

MACHINE-TO-MACHINE (M2M)

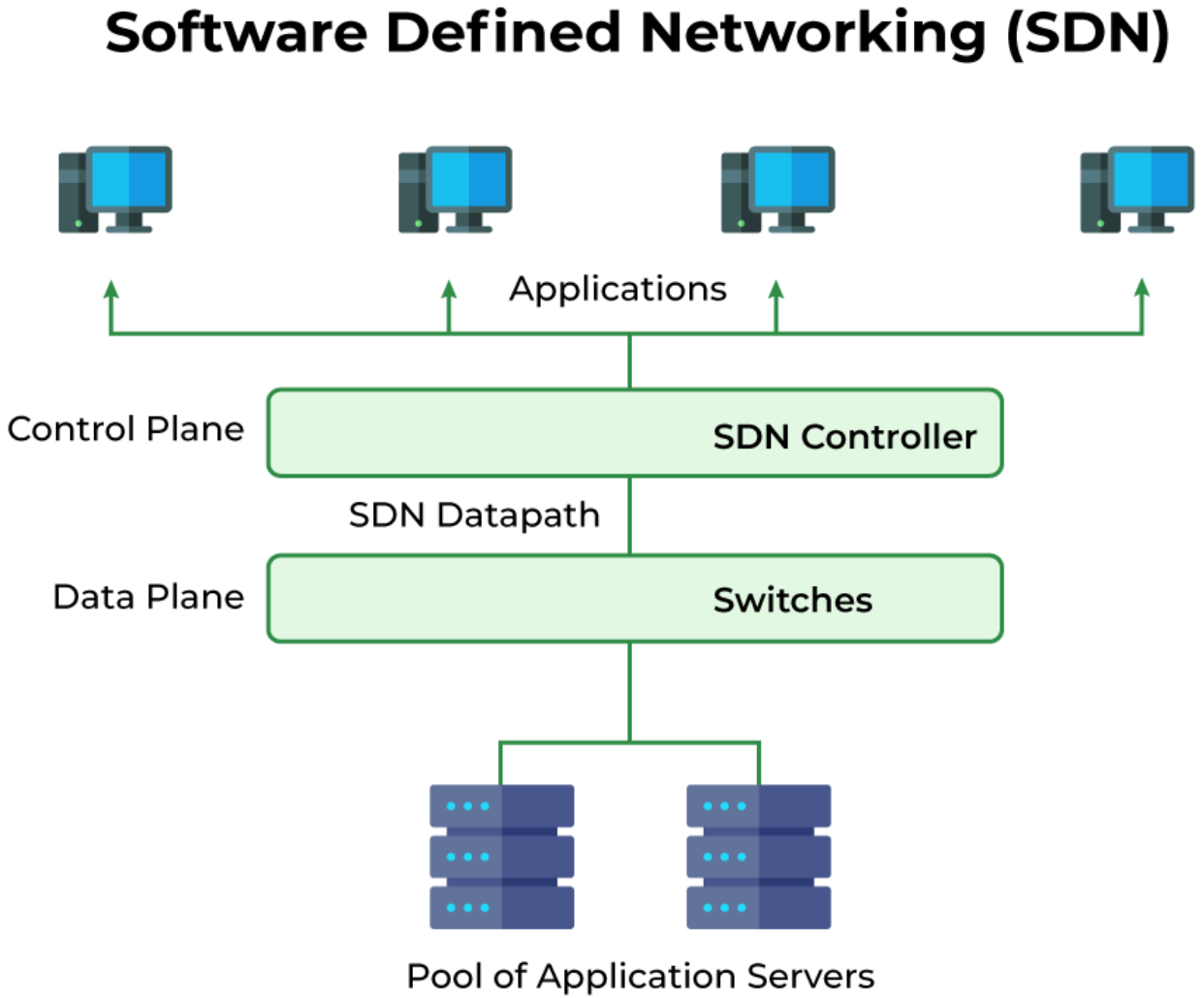
- It forms the basis for a concept known as the Internet of Things (IoT).
- Key components of an M2M system include sensors, RFID, a Wi-Fi or cellular communications link and autonomic computing software programmed to help a networked device interpret data and make decisions.
- The most well-known type of M2M communication is telemetry, which has been used since the early part of the last century to transmit operational data.
- Pioneers in telemetric first used telephone lines and later, on 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 like home heating units, electric meters and Internet-connected appliances.
- Products built with M2M communication capabilities are often marketed to end users as being smart.



SOFTWARE DEFINE NETWORK (SDN)

SOFTWARE DEFINED NETWORK

- Software-Defined Networking (SDN) in the context of the Internet of Things (IoT) is a network architecture that allows for more flexible and efficient management of IoT devices and their communication within a network. SDN is a technology that separates the control plane (the decision-making part of the network) from the data plane (the part that forwards data packets).



SOFTWARE DEFINED NETWORK

Centralized Network Control: SDN centralizes the control of the network through a software controller. This controller can dynamically configure and manage network resources, making it easier to adapt to the changing demands of IoT devices. In an IoT ecosystem, where devices can be numerous and varied, this centralized control is invaluable.

Traffic Optimization: SDN enables intelligent routing and traffic optimization. IoT devices often have diverse requirements, with some requiring low-latency communication, while others need high bandwidth. SDN can route traffic efficiently based on these requirements, ensuring that critical IoT applications perform as expected.

SOFTWARE DEFINED NETWORK

Security: IoT devices are often vulnerable to various security threats. SDN can implement security policies and access controls at a centralized level, making it easier to monitor and respond to security incidents. It can isolate and segment IoT devices to prevent unauthorized access and minimize attack surfaces.

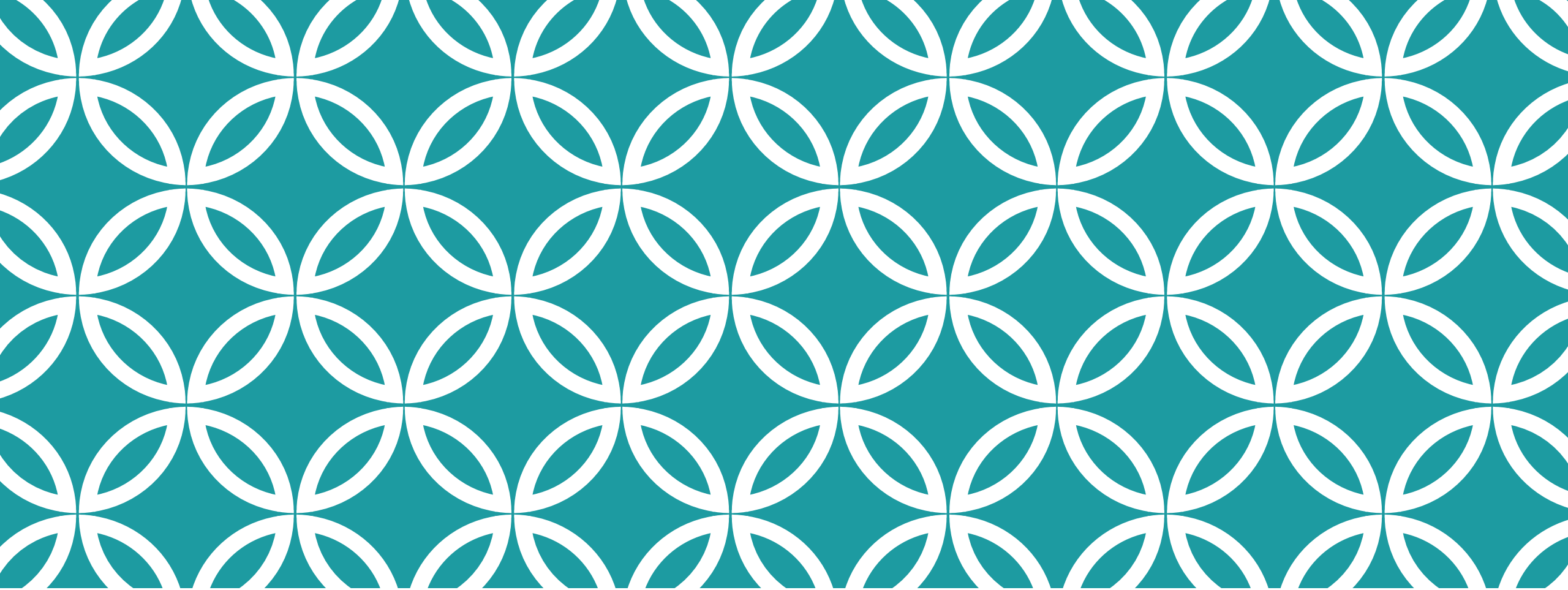
Resource Management: IoT networks may involve devices with varying computational and communication capabilities. SDN can allocate network resources dynamically based on device requirements, ensuring that resources are efficiently used while guaranteeing quality of service (QoS) for critical applications.

SOFTWARE DEFINED NETWORK

Scalability: IoT networks can grow rapidly. SDN's flexible architecture allows for easier scaling of the network infrastructure to accommodate the increasing number of IoT devices without the need for extensive hardware upgrades.

Programmability: SDN is highly programmable, allowing network operators to define policies and rules through software. This programmability is beneficial for IoT applications because it enables quick adaptation to changing requirements or the introduction of new services and applications.

Visibility and Analytics: SDN provides detailed visibility into network traffic, which is crucial for monitoring and analyzing IoT device behavior. This visibility can be used to identify performance issues, troubleshoot problems, and gather data for analytics and optimization.



NETWORK FUNCTION VIRTUALIZATION (NFV)

NETWORK FUNCTION VIRTUALIZATION (NFV)

Network Function Virtualization (NFV) is a technology that virtualizes and abstracts network functions traditionally performed by dedicated hardware devices, such as routers, firewalls, load balancers, and more. NFV aims to replace these hardware appliances with software-based virtualized instances that can be deployed and managed more flexibly.

NETWORK FUNCTION VIRTUALIZATION (NFV)

Resource Optimization: IoT deployments often involve a diverse set of network functions to support various devices and applications. NFV allows these functions to be instantiated as virtual network functions (VNFs) on shared hardware, leading to better resource utilization and cost savings.

Scalability: IoT networks can scale rapidly, with fluctuating demands. NFV enables easy scaling by creating or removing virtual instances as needed, without the need for physical hardware procurement and installation.

Service Chaining: NFV makes it easier to chain network functions together to create customized service paths for IoT traffic. This is particularly useful when different IoT devices require different services, such as security, optimization, or monitoring.

NETWORK FUNCTION VIRTUALIZATION (NFV)

Rapid Deployment: VNFs can be deployed quickly and remotely, which is advantageous in IoT scenarios where devices may be geographically dispersed. This agility helps in deploying network services as needed, even in remote locations.

Network Function Orchestration: NFV is often used in conjunction with Network Function Orchestration (NFO) to automate the provisioning, scaling, and management of virtual network functions. This is critical in IoT, where automation can help in handling the large number of devices and their dynamic requirements.

Cost Reduction: By replacing specialized hardware with virtualized instances, NFV can lead to cost savings in terms of capital expenditures (CapEx) and operational expenditures (OpEx). This is especially relevant in IoT deployments where cost-efficiency is a concern.

NETWORK FUNCTION VIRTUALIZATION (NFV)

Flexibility: IoT networks may require different network functions for various use cases (e.g., industrial IoT, smart cities, healthcare). NFV's flexibility allows network operators to adapt and reconfigure network services quickly to meet these diverse requirements.

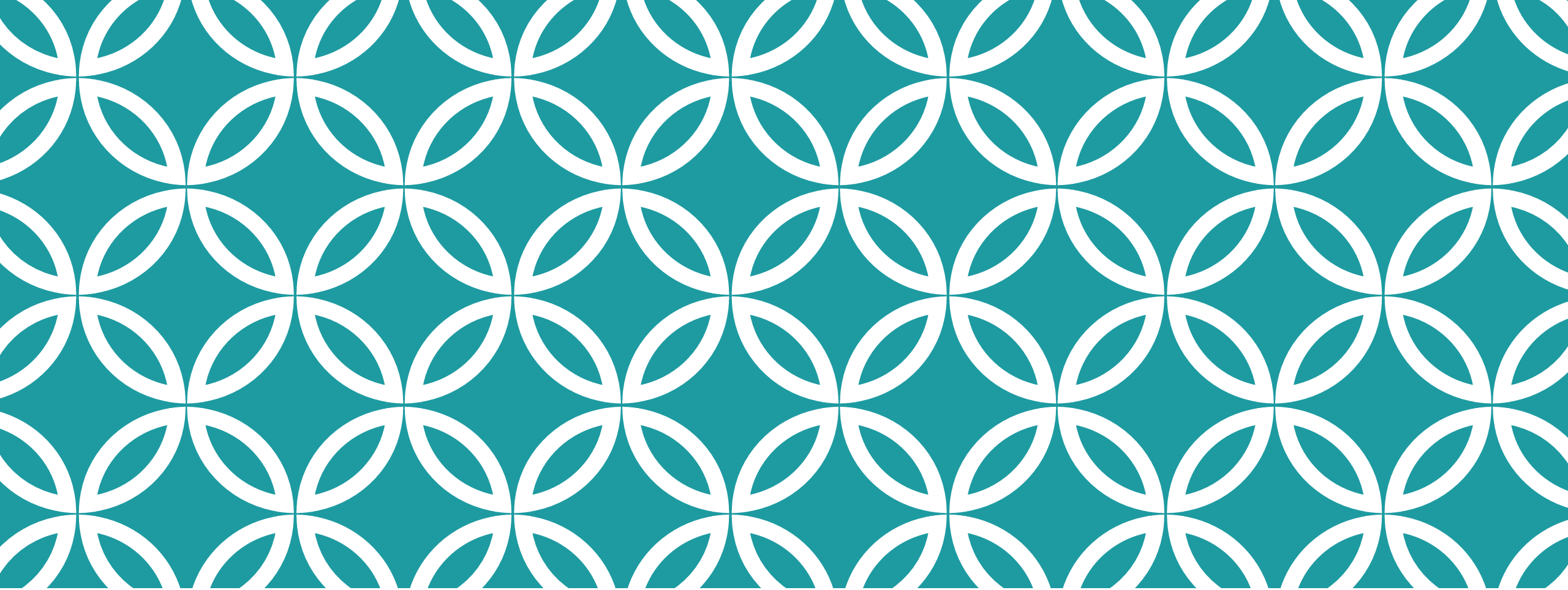
Security: NFV enables the deployment of virtualized security functions, such as firewalls and intrusion detection systems, which can be dynamically adapted to protect IoT devices and data from emerging threats.

Traffic Optimization: Virtualized network functions can be optimized to handle IoT-specific traffic patterns, ensuring low latency and efficient data routing for time-sensitive applications.

NETWORK FUNCTION VIRTUALIZATION (NFV)

Analytics and Monitoring: NFV can provide visibility into network traffic, allowing for real-time monitoring and data analytics, which is valuable for gaining insights into IoT device behavior and performance.

In summary, NFV can enhance the scalability, agility, cost-effectiveness, and security of IoT networks by virtualizing and abstracting network functions. It enables the efficient deployment and management of network services in response to the dynamic and diverse requirements of IoT deployments.



IOT CLOUD BASED SERVICES

IOT CLOUD BASED SERVICES

Amazon Web Services IOT Platform-Amazon dominates the consumer cloud market. They were the first to really turn cloud computing into a commodity way back in 2004. “ince then they’ve put a lot effort into innovation and building features, and probably have the most comprehensive set of tools available.

Microsoft Azure IoT Hub-Microsoft is taking their Internet of Things cloud services very seriously. They have cloud storage, machine learning, and IoT services, and have even developed their own operating system for IoT devices. This means they intend to provide a complete IoT solution provider.

IBM Watson IoT Platform-IBM is another IT giant trying to set itself up as an Internet of Things platform authority. They try to make their cloud services as accessible as possible to beginners with easy apps and interfaces. You can try out their sample apps to get a feel for how it all works. You can also store your data for a specified period, to get historical information from your connected devices.

IOT CLOUD BASED SERVICES

Google Cloud Platform-Search giant Google is also taking the Internet of Things very seriously. They claim that Cloud Platform is the best place to build IoT initiatives, taking advantage of Google's heritage of web-scale processing, analytics, and machine intelligence.