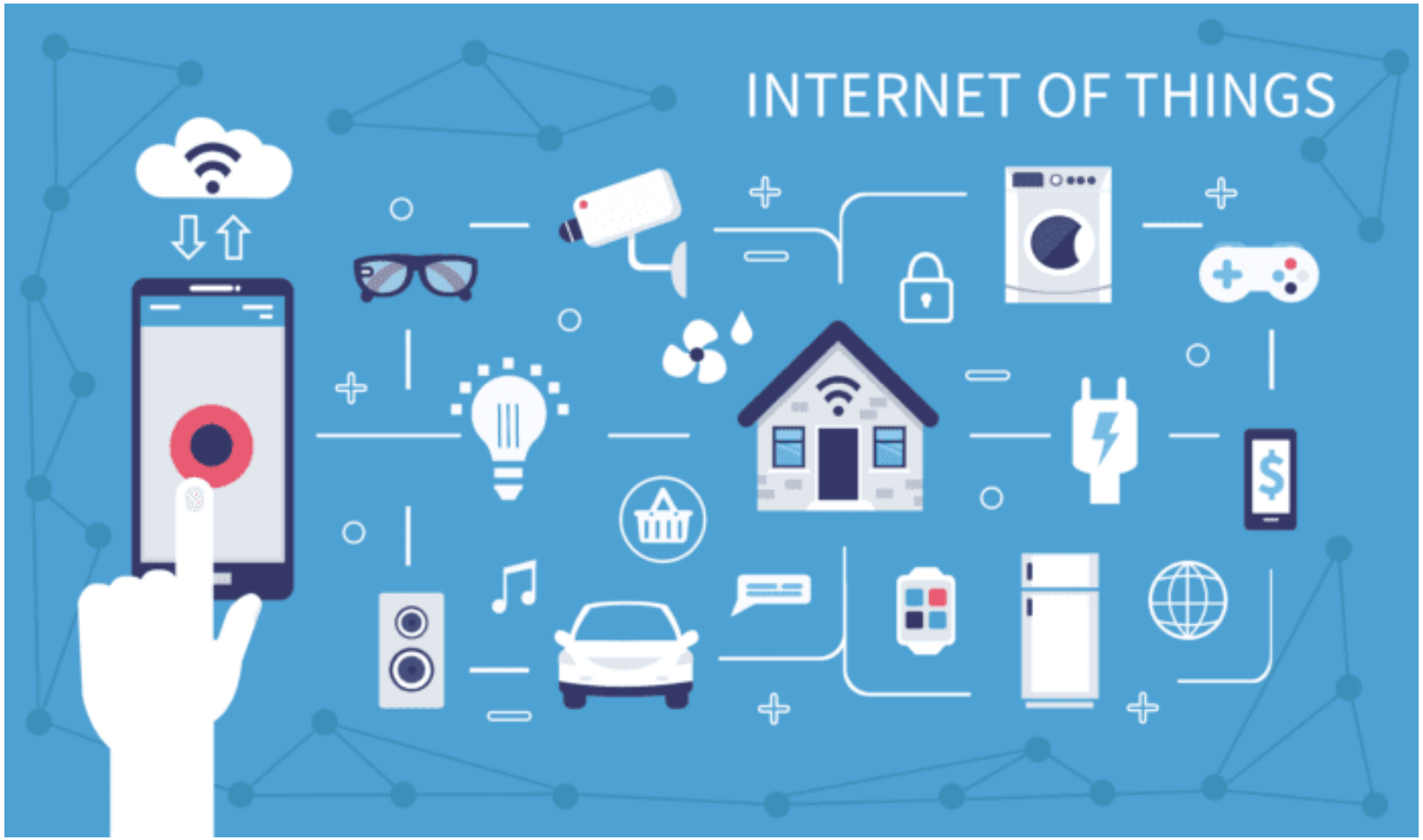
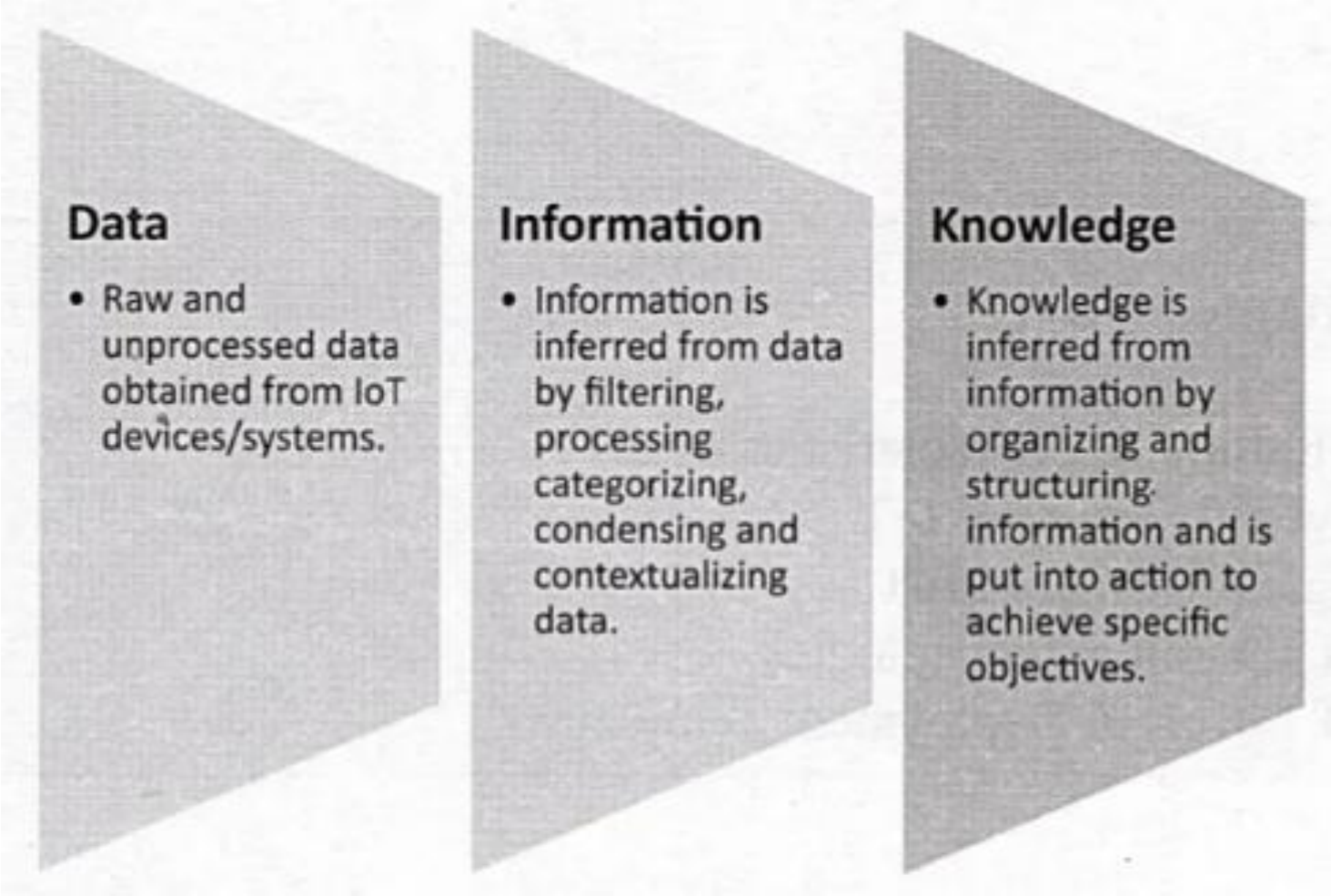
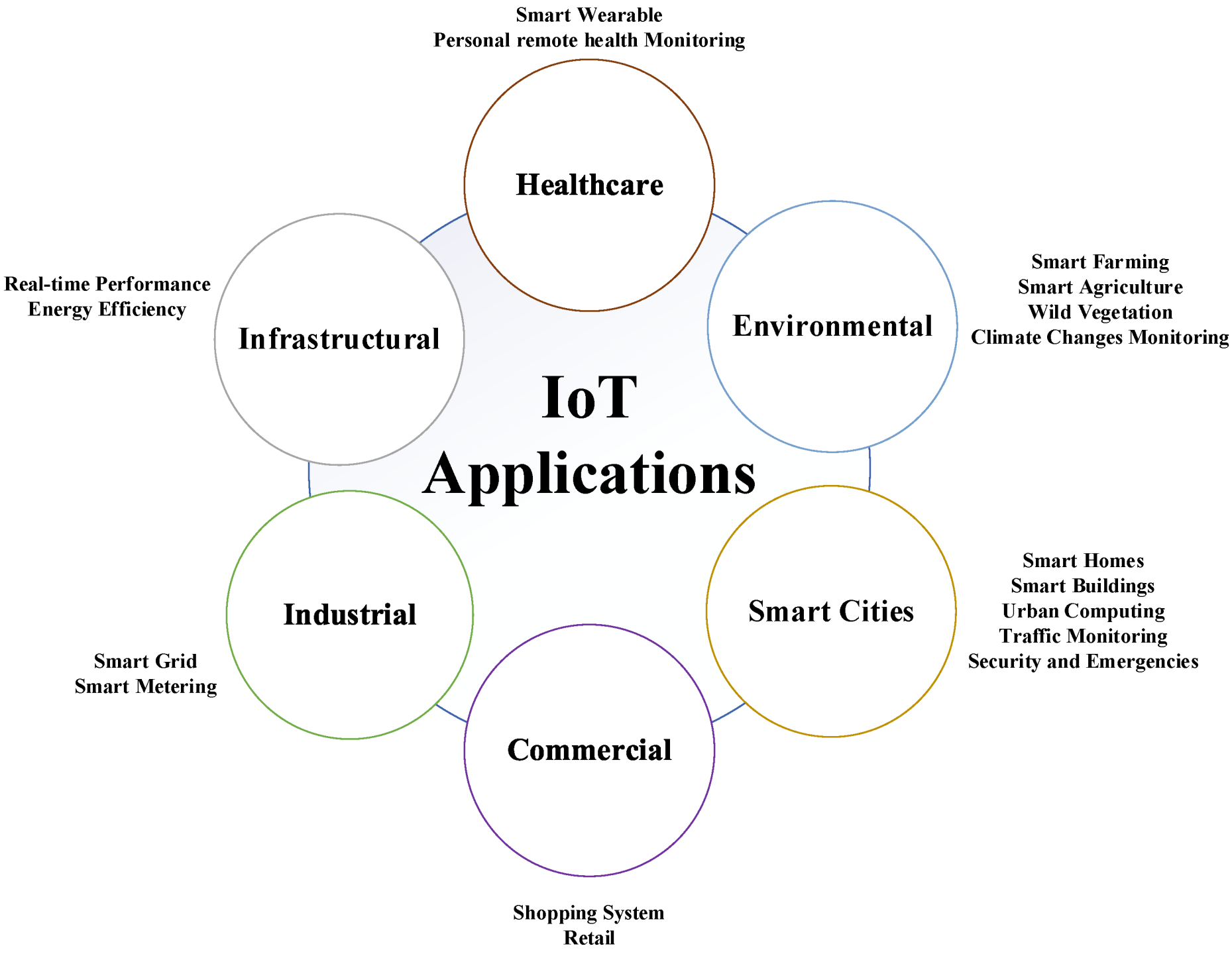
- Internet of Things(IoT) comprises **things** that have unique identities and are **connected to the internet.**
- Things?



- The scope of IoT is not limited to just connecting things to internet. IoT allows these things to communicate and exchange data while executing meaningful applications towards a common user or machine goal.




Smart Wearable
Personal remote health Monitoring
Healthcare
Real-time Performance
Energy Efficiency
Infrastructural
Environmental
Smart Farming
Smart Agriculture
Wild Vegetation
Climate Changes Monitoring
IoT
Applications
Industrial
Smart Grid
Smart Metering
Smart Cities
Smart Homes
Smart Buildings
Urban Computing
Traffic Monitoring
Security and Emergencies
Commercial
Shopping System
Retail

- **Definition of IoT:**

“A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network, often communicate data associated with users and their environments.”

Characteristics of IoT:

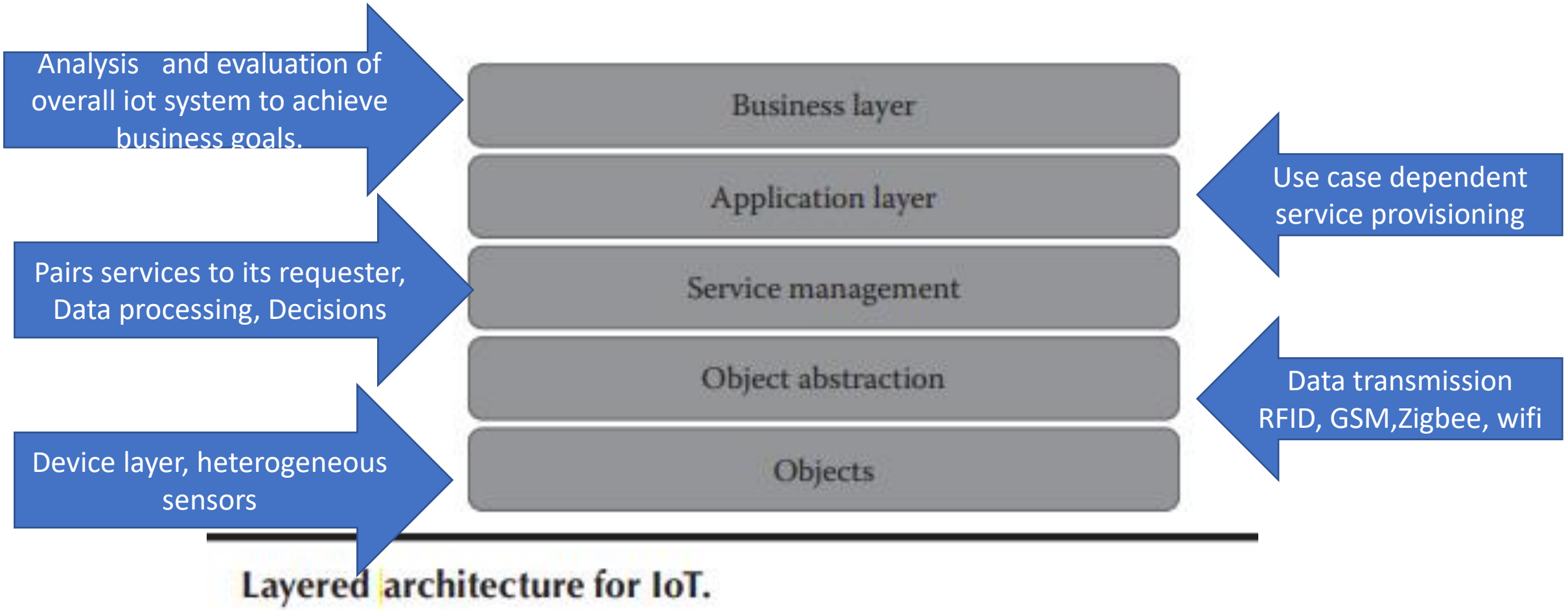
- Dynamic & Self-Adapting: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context, or sensed environment. For example, surveillance system.
- Self-Configuring: These devices have the ability configure themselves (in association with the IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.
- Interoperable Communication Protocols: IoT devices may support a number of interoperable communication protocols and can communicate with other devices and also with the infrastructure.
- Unique Identity: Each IoT device has a unique identity and a unique identifier (such as an IP address or a URI).
- Integrated into Information Network: IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

The IoT Challenges and the Research Domains

- The current IoT environments are bound to face a variety of shortcomings for **storing the massive amount of IoT data** and for subjecting the collected IoT **data appropriate analytics to extract timely and actionable insights**.
- International Data Corporation (IDC) has clearly visualized and portrayed the following critical and crucial challenges for IoT for the envisioned IoT days.
- We need elastic **compute servers, storage appliances, and network connectivity solutions on the infrastructure front.**
- On the platform side, we need highly synchronized platforms for simplifying **data cleansing, translation, aggregation, mining, and processing**. Further, **knowledge discovery and dissemination platforms** are insisted on sharing what is extracted out of IoT data.
- Data centers are transitioning toward cloud centers (cloud 1.0) and the next evolution is cloud enabled data centers (cloud 2.0) through the incorporation of powerful concepts such as software defined compute, storage, and networking. That is, **future data centers will be software-defined, automated, optimized, and virtualized**.

The Research Domains

- Energy-efficient device architectures: Energy harvesting and novel hardware designs for energy optimization
- Elastic IoT infrastructures: accommodative to have a large number of communicating devices and digitized objects
- Highly optimized communication protocol
- Data deduplication and compression mechanisms
- Device security



Layered architecture for IoT.

IoT vs. M2M

- M2M describes the technology that enables the communication between two or more machines.
- With M2M, one could connect machines, devices, and appliances in a wired or wireless fashion via a variety of communications techniques to deliver services with limited human intervention
- The main objective of M2M is to connect a machine/device to another machine (typically in an industrial setting) via cellular or wired network so that its status can be monitored and its data can be collected, remotely.
- IoT is more of a universal market technology that aims at serving consumers, industries, and enterprises.
- M2M relies on point-to-point communications enabled by dedicated hardware components integrated within the machine. IoT, on the other hand, typically uses IP networks and integrates web applications to interface device/machine data to a middleware, and in the majority of cases, to cloud.

IoT vs. M2M

- M2M is part of the IoT, while M2M standards have a prominent place in the IoT standards landscape.
- However, IoT has a broader scope than M2M, since it comprises a broader range of interactions, including interactions between devices/things, things and people, things with applications and people with applications.
- It also enables the composition of workflows comprising all of the above interactions.
- IoT includes the notion of internet connectivity (which is provided in most of the networks outlined above), but is not necessarily focused on the use of telcom networks.