Capgemini engineering

EDGE IOT

Principles, challenges, drivers, and trends

Table of contents

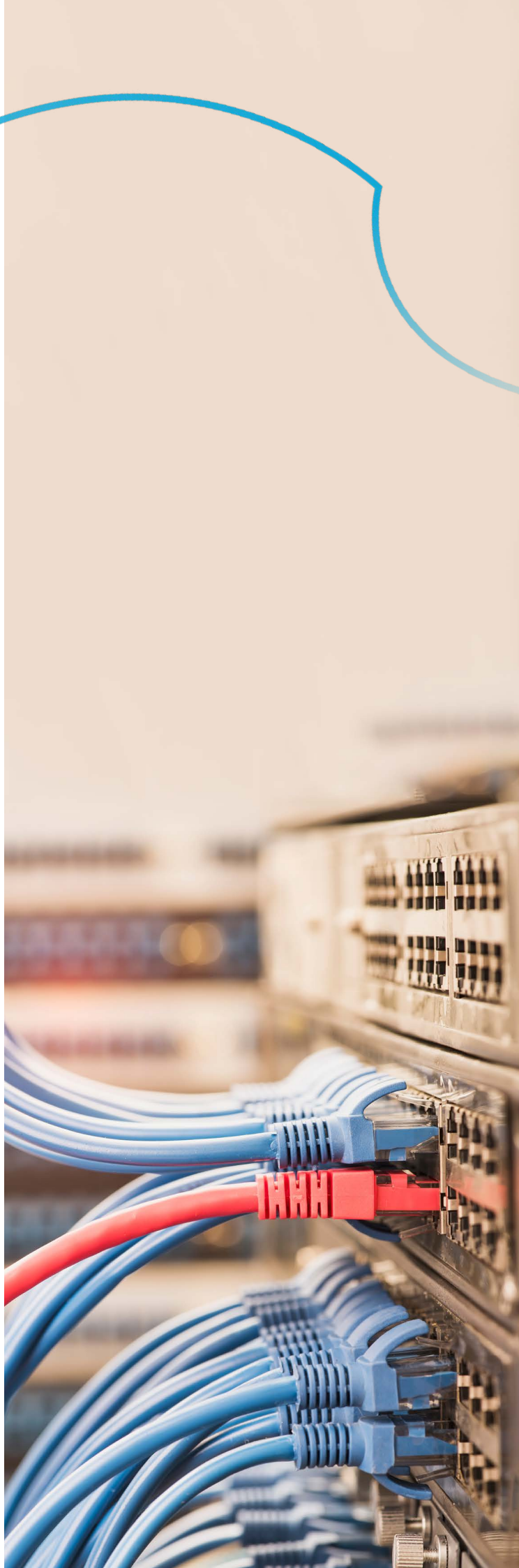
Executive summary

The way digital technology is evolving, edge compute and the internet of things (IoT) are destined to go hand-in-hand. The reason to consider edge in an IoT ecosystem is that killer applications and use cases in both the consumer and industrial sectors need to address the vast and varied requirements of low latency, quick data processing, better energy efficiency, zero-touch device provisioning, robust data security, and cost reduction.

Including edge in an IoT ecosystem addresses specific use cases, such as massive data processing and management of centralized gateways – for instance, in a car or an oil refinery – where multiple sensor nodes working on different technologies like Zigbee, Thread, Wi-Fi, BLE, and Z-Wave communicate to an edge gateway for quick data analytics and processing. Edge also supports both device and data security better with a zero-touch provisioning concept based on the GSMA IoT SAFE standard for e-SIM/i-SIM-based IoT devices.

Edge IoT is also becoming critical for 5G networks to enable new applications for massive machine-type communications (MMTC) and ultra-reliable low latency communications (URLLC) based on the evolving 3GPP R16/R17 standard. Edge will evolve its relationship with these emerging standards bodies.

This white paper provides insight into the dimensions of the challenges in consumer and industrial automation. It explores how edge wireless sensor nodes and edge gateway design elements can overcome IoT ecosystem challenges for specific use cases, such as video surveillance in residential communities, data management in connected cars, and security in the retail segment.



Introduction

The need for edge in the IoT ecosystem

Cities around the world are struggling to address challenges caused by growing populations and aging infrastructure. These trends are creating a variety of problems, including:

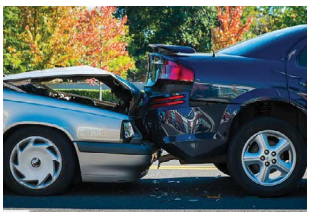
- Increasing pollution above acceptable levels set by state authorities
- Increasing traffic and congestion on poorly maintained roads
- More break-ins and robberies in commercial and residential areas
- More vehicle accidents, including with pedestrians
- Overloading power transformers that catch fire
- Petrochemical pipeline gas leaks and accidents
- Breakdown of waste removal services
- Breakdown of old sewer infrastructure and contamination of drinking water

IoT can be part of the solution to address these specifc challenges. Creating a framework with embedded intelligence and connectivity using a wide range of sensor nodes and end-devices makes the new system more intelligent and efficient.









IoT networks can help avoid accidents and manage day-to-day operations. The administrator can track worker productivity and efficiency in an industrial plant and optimize operational costs for different use cases in consumer and industrial markets.

An IoT ecosystem can create value and address many challenges, however, from a design perspective, most of today's IoT deployments rely on a centralized architectural design. In the cloud-based model, sensor nodes in the field transmit information to a cloud platform, where the data is processed and stored in a single location, thus simplifying data management and data post-processing. (See Figure 1.) However, the drawback of the cloud computing approach is that the massive amount of data transmitted to the IoT cloud platform constrains network bandwidth and causes higher latency. Also, data processing on an IoT cloud platform exclusively for time-sensitive applications is not an efficient solution for critical IoT applications like vehicle collision, intruder entry, fires, theft, etc.

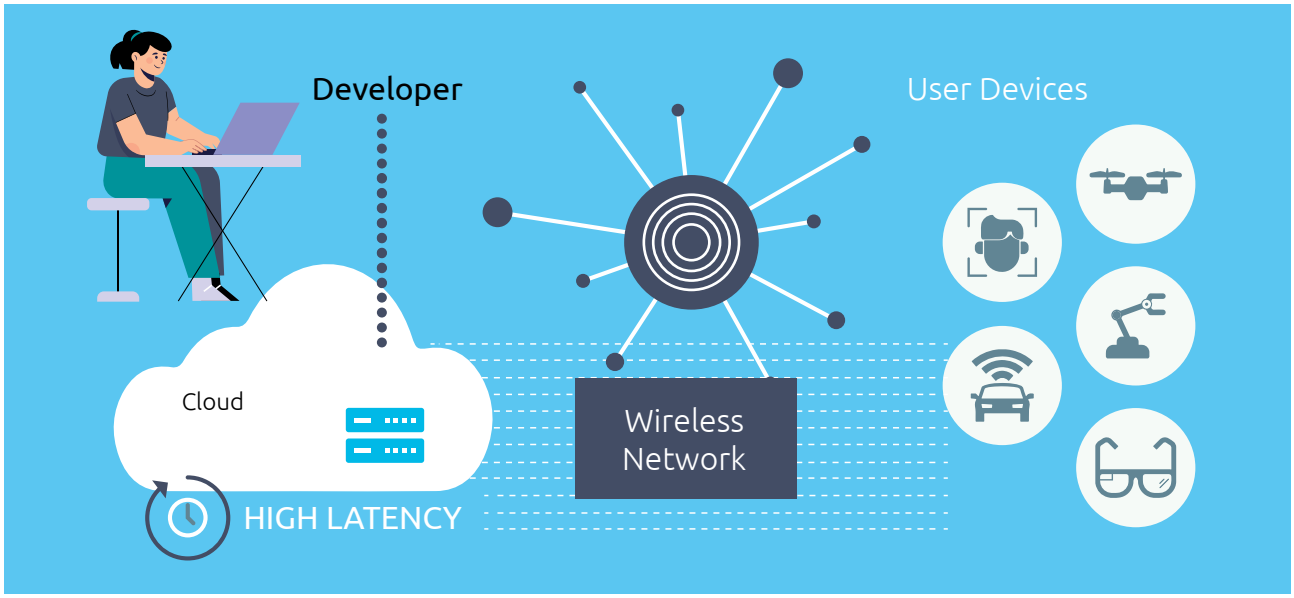


Figure 1. Cloud-based centralized model
Source: Capgemini Engineering

To overcome the existing challenges, there are specific parameters that require attention when designing the IoT solution.

- **Volume of data:** Smart buildings, connected vehicles, industrial IoT applications, and other IoT verticals generate vast amounts of data, leading to higher network bandwidth consumption, latency, and more data storage. Some of the data can be ignored at the source and does not need to be transmitted to the cloud
- **Privacy and security:** Ensuring data security is a significant challenge for the cloud-centric model as there is a real possibility that data transmitted over the internet could be hacked
- **Power:** Most sensor nodes deployed in IoT networks are battery-powered and need to conserve as much energy as possible. The energy consumed per bit for data transmission is a critical factor in the wireless node design. Therefore, it is essential to process data at the edge of the network to conserve energy instead of processing it in the data center on the cloud
- **Interoperability:** The IoT ecosystem needs support to increase interoperability between emerging connected devices and legacy devices by updating the communications protocols used by the older systems. Interoperability at the edge is the key to improving operational efficiency and enables error-free transmission and translation of messages and protocols

Overview

With the rapid growth of devices in the world today, the connectivity, security, and quality of service (QoS) are critical factors for many safety applications, where the data needs to be captured, processed, stored, and analyzed either at the sensor nodes or the edge of the IoT network. Each should be considered to ensure the IoT network operates efficiently and meets end-user expectations. One of the key metrics to manage critical IoT applications with many connected devices is latency. Edge-based solution design can address latency in real-time. Here are two examples:

- **Industrial automation in the oil and gas industry:** Managing critical equipment such as motors, valves, and flowmeters requires quick-turnaround data analytics to avoid significant damage. (See Figure 2.) There is a need for a mechanism to collect data from critical equipment, monitor and record information at the edge of the industrial network for quick analysis, and provide a warning at an early stage if there is an indication of a potential failure.

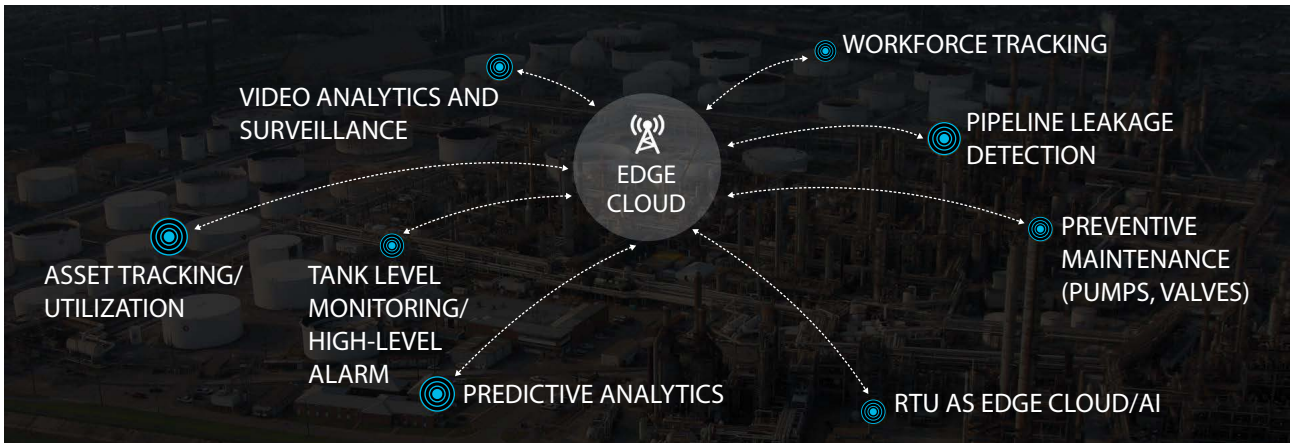


Figure 2. Oil and gas use of IoT and edge
Source: Capgemini Engineering

- **Residential communities:** Managing the day-to-day expectations of the people living in residential neighborhoods is complex. It includes monitoring and managing air quality, water quality, resident safety, especially at night, healthcare, especially for the elderly, electrical and wastewater management systems, and other functions. Connecting these systems to the edge will improve the safety and security of residents. (See Figure 3.)

Figure 3. Edge IoT can improve the management of residential communities
Source: Capgemini Engineering

To meet some of these expectations, the data generated at the source — a device or sensor node in an industrial automation system, residential community system, or a vehicle — is not required to travel to the cloud for processing. The data can be pre-processed and filtered by an edge device to remove noise and low-quality data. The device can also take care of privacy protection by truncating unauthorized data. Ideally, the data that gets processed at the edge provides a shorter response time, more efficient data processing, and data trimming with better security management, all with a limited burden on the network. Adding artificial

intelligence (AI) and machine learning (ML) inference at the edge of the network is another crucial element that makes the IoT ecosystem stronger and able to detect problems at an early stage.

In the IoT ecosystem, edge computing plays a significant role in the sensor node and the gateway that connects all the sensor nodes that work on different technologies and protocols. Figure 4 captures the essential features where edge delivers value in the IoT ecosystem.

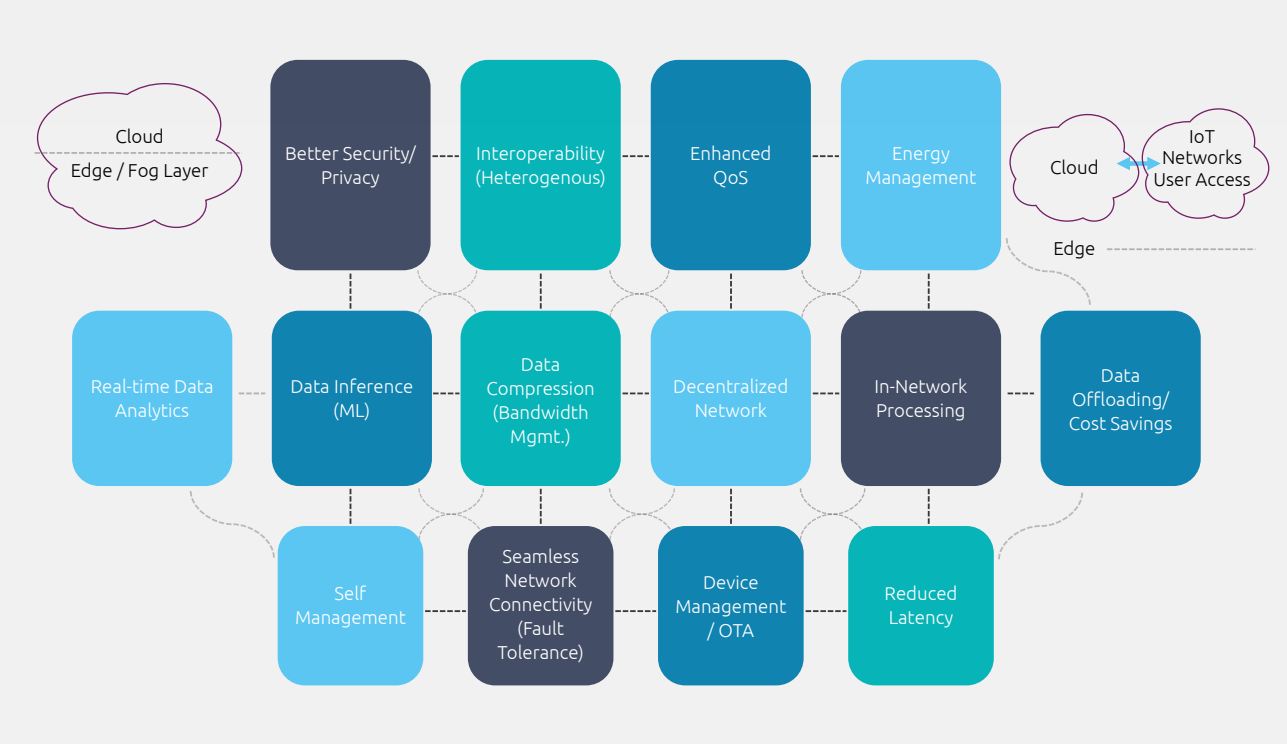


Figure 4. How edge delivers value in the IoT ecosystem
Source: Capgemini Engineering

Cloud computing is swinging back towards decentralized and distributed computing, and was the model used fifteen years ago. It highlights many value-add advantages that edge creates and is described below.

Data security: In the IoT ecosystem, security is a big challenge that includes data, device, and network security. In IoT network design, privacy is required to protect the data being transferred between the various sensor nodes of the IoT network, where hackers may try to eavesdrop on communications and inject false data into the IoT ecosystem. The integrity of data should always be maintained, as false data can change the IoT network design. For example, sensitive information like emergency alerts generated from a smart home or an industrial plant, where hackers can alter the data and create significant damage. To handle security challenges, edge acts as a crucial component on the southbound side by interfacing with various sensor nodes and on the northbound interface by connecting to different cloud platforms like AWS, Azure, and Google.

Quality of service: QoS is important for critical real-time applications. In IoT, data generated from the source nodes aggregate at the sink node and produce data traffic. So, the QoS should be designed to handle any constrained data traffic that flows through the IoT network. Also, QoS in the IoT network should not be affected by adding a new sensor node or removing existing sensor nodes. The IoT network should be able to support scalability without comprising the QoS. The edge sensor nodes and edge gateways play a crucial role in managing and providing a better QoS in the IoT network design.

Energy management: In the IoT ecosystem, the wireless sensor nodes require a significant amount of power to perform operations. Typically, most of the energy consumed by the battery-powered sensor nodes is for data collection, data processing, and data communications. And demand is growing. According to the International Energy Agency, more than 23 billion battery-powered IoT devices will exist by 2025.[1] Energy efficiency management is one of the critical requirements for edge-based node design, as many edge devices that are battery-powered today are located outdoors.

Consider Figure 5. To transmit data from sensor node 1 to the edge gateway requires node 5 to wake up to talk to node 10, so node 10 triggers node 12 to wake up and transmit the data to the edge gateway. These intermediate steps are adding no value but are consuming energy. Alternatively, the information that travels from node 1 to node 12 can be processed within the sensor node network by collaborating with other sensor nodes instead of having every node forward the data to the edge gateway, where the gateway needs to analyze and process the unwanted data.

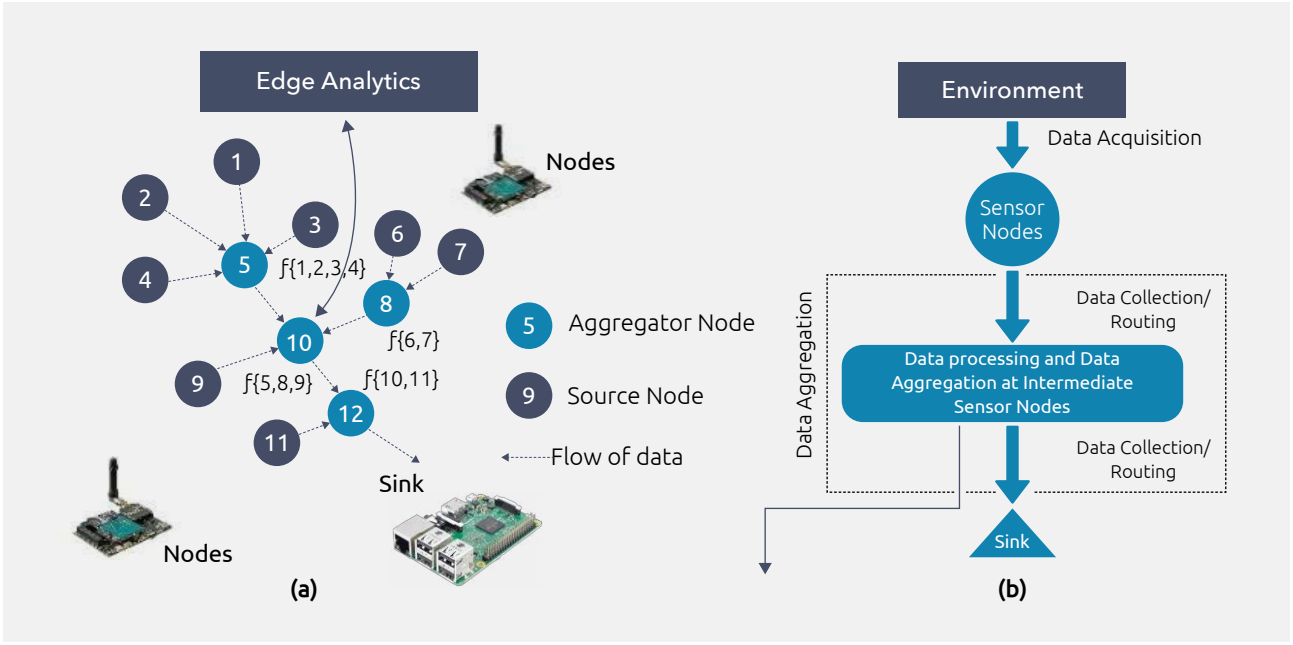


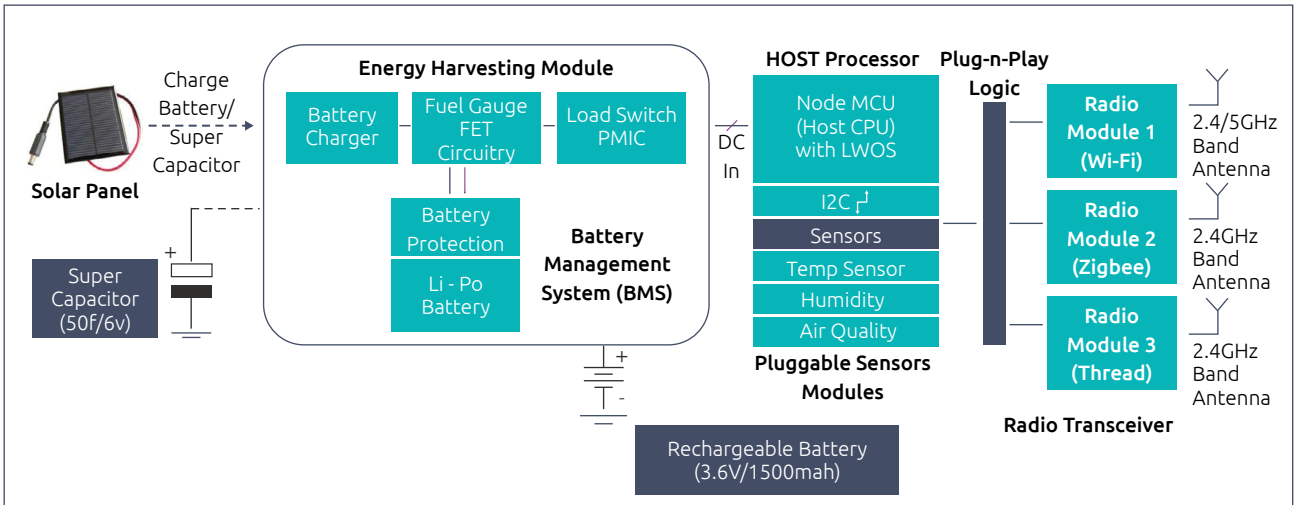
Figure 5. Transmitting data from a sensor node to the edge gateway is energy inefficient
Source: Capgemini Engineering

[1.] "Energy Harvesting Technologies for IoT," Jul. 2018, International Energy Agency

Handling data aggregation within the node network is called in-network processing (INP). It is a new concept in IoT network design, where the data generated from battery-powered sensor nodes can be aggregated, validated, and analyzed. When a node joins another node, the data is propagated. The nodes decide whether to transmit other sensor node data to the edge gateway, reducing the amount of data to be transmitted and lowering energy use.

On average, the energy spent transmitting one bit of information – the payload – between sensor nodes is crucial for the IoT network to work efficiently. Also, the components of the sensor nodes, such as the CPU and radio transceiver, require a large amount of power to listen to wireless transmissions, even in their idle state. Sometimes, it is difficult to recharge or replace the batteries in the nodes because of their location or environment.

Energy efficiency is one of the essential requirements to maximize the lifetime of the sensor nodes. Also, it is one of the most constraining requirements for the design and implementation of the edge nodes for various IoT applications. This is where the energy harvesting module plays a crucial role in supporting the battery and the supercapacitor for storing large amounts of energy. (See Figure 6.) The module allows the edge nodes to work in a more efficient way to handle energy management. While the existing method in the sensor node uses only batteries today to store energy, energy harvesting techniques using supercapacitors can extend battery life and increase the efficiency of the operational lifecycle of the wireless sensor node. Hence, the lifetime of a wireless sensor node becomes a very important factor for energy-efficient operation and has become mandatory for wireless sensor nodes in the IoT network.



In-Network Processing:

- Filtering: Used for reducing the amount of data being stored or transmitted
- Compression: Like filtering, it helps reduce the amout of data that is being transmitted or stored
- Aggregation: Amount of data is reduced by fusing the values measured across many sensors as it passes through the network
- Event Driven: Ability to autonomously scan the occurrence of predefined event; training, classification, interpretation and decision making are also considered to be in the form of INP

Figure 6. Energy harvesting at the edge

Source: Capgemini Engineering

The energy harvesting technique supports both the battery and supercapacitor and saves energy for the wireless edge node to operate more efficiently. In addition to the energy harvesting module, the data analytics on the edge node, which is part of INP, is another critical factor to consider. The emerging wireless sensor node design will have intelligence embedded – along with the energy management software algorithm – that will run jointly with the data analytics software capability and device management to manage the energy management functionality of the IoT network.

Interoperability: Edge plays a significant role in addressing the challenge of interoperability. There are many technologies and protocols that exist in the IoT world in both the consumer and industrial market segments. At the same time, there is a need for logic on the edge gateway to interconnect with various devices and sensor nodes that work on different technologies to provide smart services to the end-users. Interoperability is a crucial feature, as the end-user wants plug-n-play wireless sensor nodes and the other flavors of IoT devices to work together easily. (See Figure 7.)

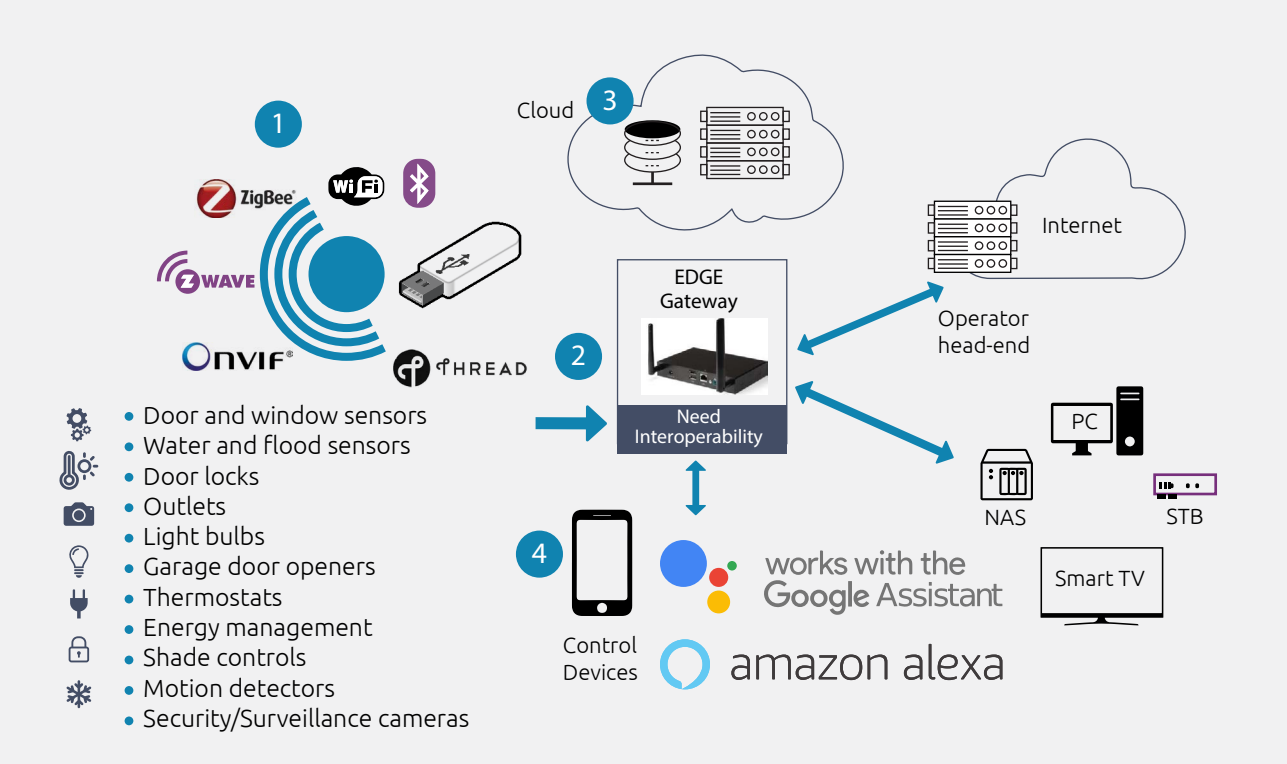


Figure 7. Interoperability challenges with different wireless technologies
Source: Capgemini Engineering

While connectivity opens a new door for highly differentiated IoT products, interoperability remains a core challenge. Edge brings a clear differentiated solution for interoperability by interconnecting different technologies such as Zigbee, Z-Wave, Thread, Bluetooth, Wi-Fi, LoRa, and IoT protocols and frameworks like MQTT, CoAP, and LWM2M. The edge IoT ecosystem can increase interoperability by converting the communication protocols of older legacy devices to a messaging format that the newer IoT devices understand.

Seamless switching: To ensure always-on connectivity without interruption, the edge network should be enabled with end-to-end continuity. The seamless switching along with the session-persistence feature can ensure successful data transfer even when the underlying radio link connections are disrupted. (See Figure 8.) Seamless switching at the edge of the network – specifically on the edge gateway – monitors the existing connections on the northbound side and automatically switches to the available wireless or wired network without interruption based on priority and the user's choice of network selection. End-users will have the best available connection wherever they are (e.g., anywhere and anytime in a connected car, smart home, and smart retail store), including support functionalities such as:

- Continuous connectivity with a 3G, 4G, and 5G network
- Low latency
- Minimum packet loss

Figure 8: Seamless switching with session persistence based on the edge
Source: Capgemini Engineering

Localization: The deployment of wireless sensor nodes for smart-city initiatives and other applications is expected to grow in the near future. Each sensor node is expected to be enabled with its GPS receiver. However, high power consumption, high cost, and the need for line-of-sight connectivity make a GPS-based solution impractical for most IoT sensor nodes. Furthermore, GPS-based sensor nodes depend entirely on line-of-sight communications to the satellite, which may not always be available, such as when wireless sensor networks are deployed indoors or outdoors where line-of-sight is impossible, as in a heavily forested environment.

Deployment strategy of edge nodes: The wireless sensor nodes should remain functional, even if any of the other wireless sensor nodes fail within the network topology, and should have the in-built ability to be self-managing by changing the configuration of the sensor nodes in the network. Today, many wireless sensor nodes in the field, once deployed, are expected to operate autonomously and should be able to self-configure and adapt. When the wireless nodes are deployed, the nodes automatically handle the data distribution with other sensor nodes. The wireless edge nodes should have the intelligence to manage the various challenges on their own, such as:

- A self-healing edge node should allow other sensor nodes to discover, identify, and react to network disruptions
- A self-location edge node should be able to determine its geographical position using other network nodes' locations
- A self-managing edge node should be able to monitor its surroundings, adapt to changes in the physical environment, and cooperate with neighboring sensor nodes to form the IoT network topology and agree on data processing and communication strategies
- A self-organizing edge node should have the ability to adapt configuration parameters based on environmental conditions
- A self-optimizing edge node should have the ability to monitor and optimize the use of its own system resources
- A self-protecting edge sensor node should recognize and protect itself from intrusions and attacks

In energy-constrained wireless sensor nodes, the most important element is that all these self-management features must be designed and implemented to not suffer from excessive energy overhead.

Auto calibration: This feature is essential for edge sensor nodes, where manual calibration of wireless sensor modes (e.g., flow meters, pressure transmitters, temperature transmitters) in a larger industrial plant is expensive. Since it is a time-consuming process and difficult task, manual calibration of wireless sensor nodes in the field is too costly. So, auto-calibration and fine-tuning mechanisms are proposed for the wireless sensor nodes to be managed remotely and after calibration, the nodes are expected to provide accuracy and precision within +/- 0.1%, typically for different IoT applications.

Collaboration: It is highly recommended that wireless sensor nodes in large-scale IoT network deployments collaborate, where a single sensor in an IoT application may not be able to decide if an event generated is good or bad. In this case, several wireless sensor nodes within the IoT mesh network must collaborate to identify and detect an appropriate event. The joint data of many sensors can provide helpful information collaboratively to avoid any significant damage, especially in industrial automation systems.

Decentralized management: Today, most sensor nodes work in a star/mesh mode, where the IoT/M2M gateway collects information from all wireless sensor nodes. The gateway decides the routing path for each sensor node, based on the amount of energy available for each sensor node, and informs each sensor node of its routing path. However, if there are thousands or millions of nodes, the optimal paths would change frequently and would be difficult for the IoT gateway to process. For these reasons, a decentralized approach is recommended. This approach enables each sensor node to create and build its own routing decisions at the edge of the sensor node based on limited information, such as a list of the node's neighbors and the IoT gateway. A decentralized approach significantly reduces management overhead, and sensor node functions can be managed better on the edge node.

Other features such as data compression, ML with inference (e.g., the AWS Greengrass service on the edge), and device management/over-the-air (OTA) allow edge-based IoT designs to overcome challenges by maximizing network performance and providing better QoS for end-users.

Industry landscape

While edge computing is a critical element of the network infrastructure, both 5G and edge will significantly improve the performance of IoT applications as massive amounts of data is processed in near-real-time. 5G significantly increases speed over 4G, and edge significantly reduces latency by bringing network computation capabilities closer to the end-user. (See Figure 9.)

Edge is about the location of an asset, not the asset itself, and has a different meaning for different constituents:

- For the end-user, the IoT device is the edge
- For the telecom operator, the base station or cell tower is the edge
- For the cloud platform provider, the data center is the edge
- For the enterprise user, the supply chain is the edge

Edge Sensor Node

Good wireless sensor node design is essential for the efficient, autonomous edge sensor node to address the many challenges described in the previous section. (See Figure 10.) Most IoT sensor nodes are deployed in harsh, inaccessible environments - for example, smart-city applications - and are expected to work without maintenance or repair for five to ten years.

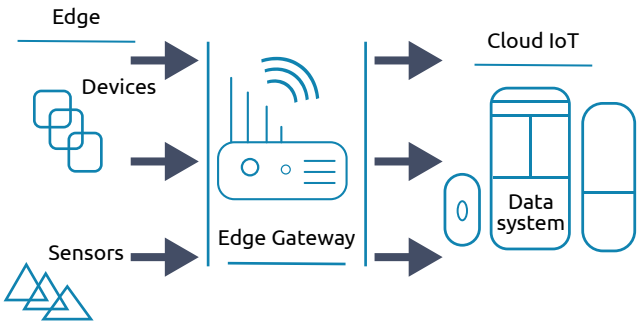


Figure 9. The three elements of the network
Source: IEEE

The limitations of wireless sensor nodes include:

- Small storage memory, where a few hundred kilobytes of data can be stored
- Operating frequencies between 16 and 40 MHz
- Operate in short-range between 10 and 100 meters
- Consume a lot of power during the transmission and reception of a single bit of data

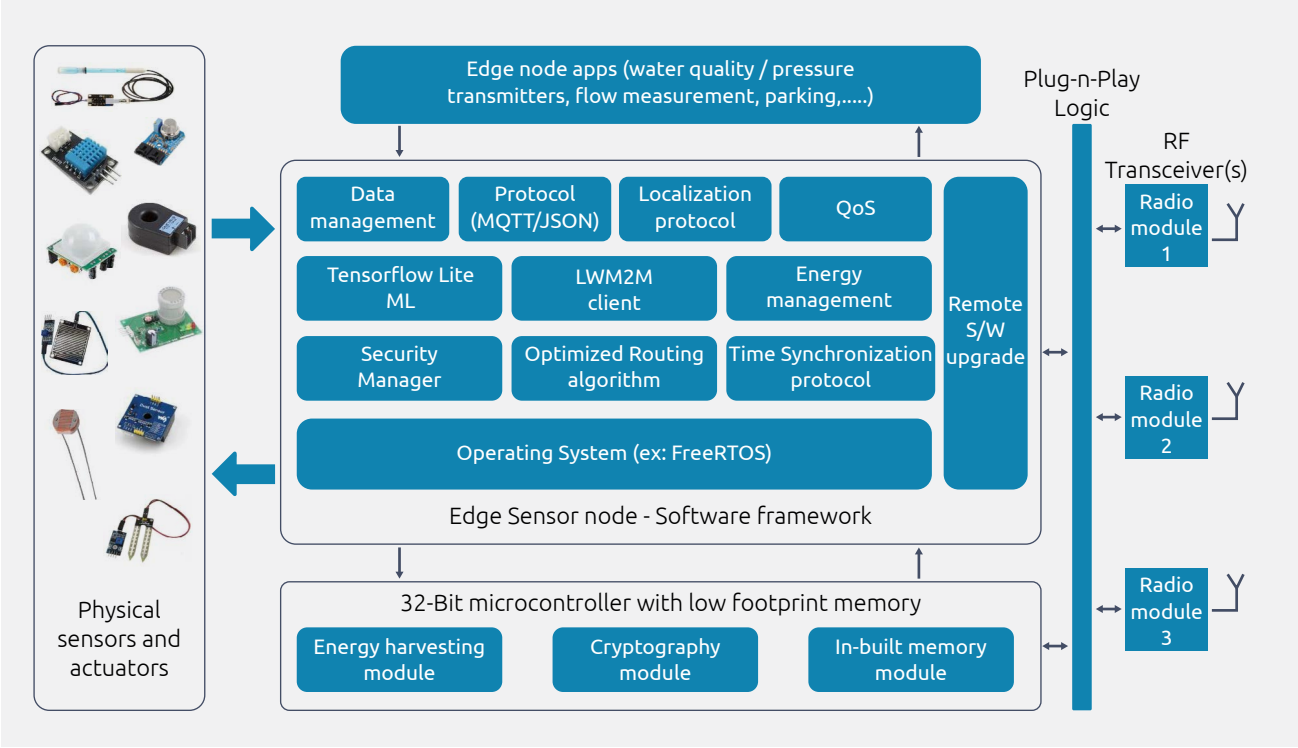


Figure 10. Edge sensor node software design model
Source: Capgemini Engineering

Today, 32-bit microcontroller SoCs have advanced features like inbuilt hardware accelerators, multi-radio RF transceivers, and low-power footprints. An edge-based sensor design could meet the IoT demands for the consumer and industrial market segments from the hardware perspective. OEMs' expectations for the wireless sensor node software design are increasing with the need for advanced features and high-level ideas for the software design of the sensor nodes. Their expectations include:

- Better energy-efficient algorithms
- Localization techniques
- Proactive routing
- Self-management and self-optimization
- Time synchronization
- QoS

Edge Gateway

Edge and 5G will be central to developing IoT networks in consumer and industrial market segments. With different technologies and protocols like LWM2M, software-defined networking (SDN), network function virtualization (NFV), MERN stack (MongoDB, Express.JS, React.JS, Node.js), Apache Spark, Kafka, Docker, Kubernetes, ELK stack (Elasticsearch DB, Logstash, Kibana), most of the cloud-based functions can be offloaded to the edge/IoT gateway. (See Figure 11.)

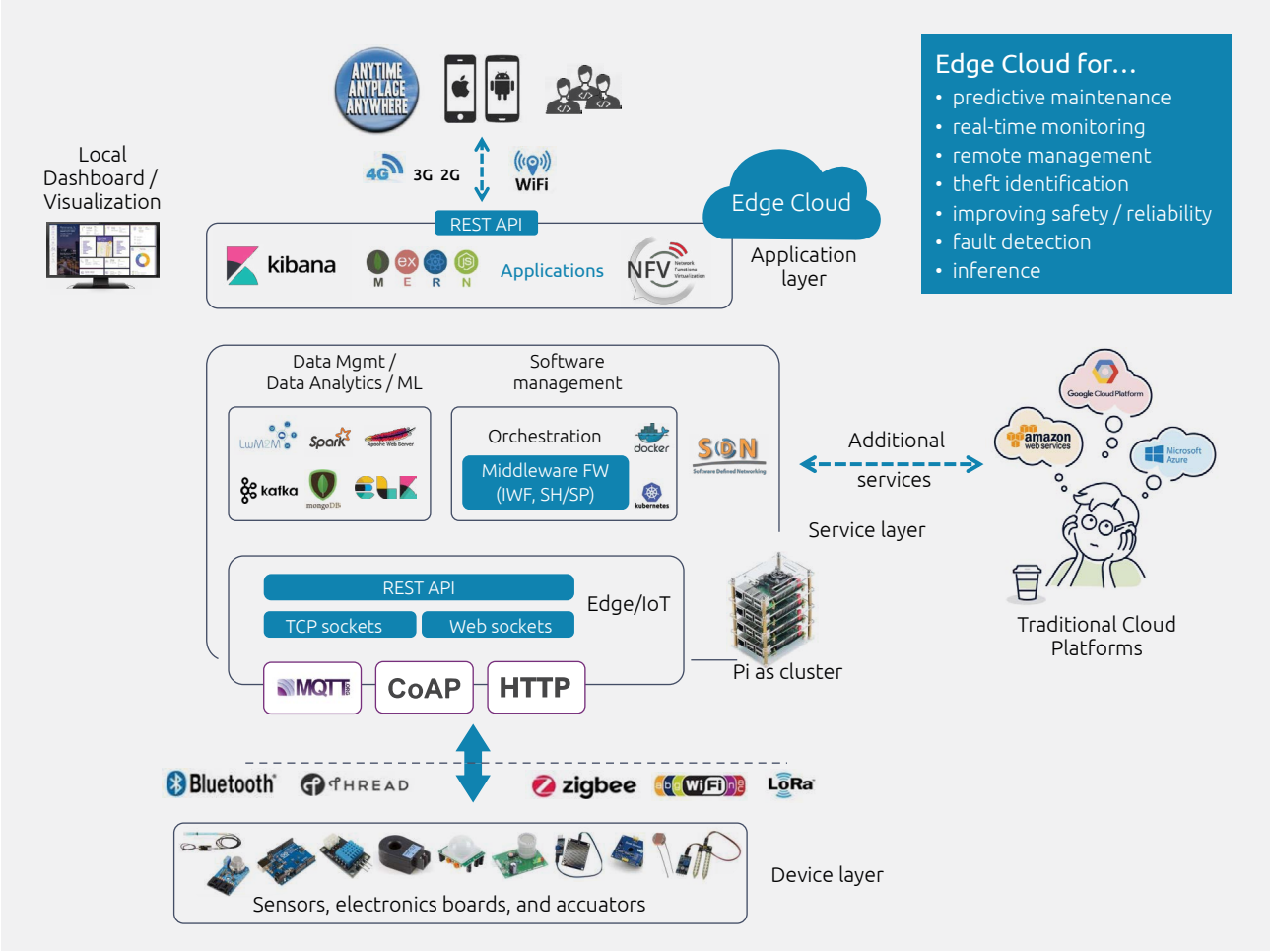


Figure 11. The edge gateway
Source: Capgemini Engineering

The edge gateways will be the critical enablers for predictive analysis in IoT network deployments. They can pre-process the data with efficient processing algorithms, secure the data, and detect any anomalies by reducing the computational latency. Shifting computing or offloading data from the cloud to the edge relieves the pressure on network bandwidth, processing speed, and responsiveness. As a result, it allows more bandwidth for technologies like augmented reality (AR) to accelerate with the emerging platforms and inbuilt support available today, such as:

- Google Coral with TensorFlow Lite support
- NVIDIA Jetson AI with TensorRT support
- Qualcomm Platform with Neural Processing SDK support
- Raspberry Pi 4 as a cluster or clusters

These embedded platforms can be used to build the edge gateway. They will help predict the problems in the IoT ecosystem at an early stage using data inference at the edge to make better business decisions.

Four challenges that edge-based solutions address

Challenge 1: Video surveillance in residential communities

Video surveillance systems are deployed in many residential communities and campuses. However, the physical security staff may not be highly alert at night, which creates problems when monitoring and tracking actual incidents captured on the camera feed. (See Figure 12.) One strategy is to place a greater dependency on cameras to generate critical alerts while monitoring sensitive locations. For example, services provided by Amazon such as GreenGrass and Kinesis can run on edge devices. Therefore, cameras can help address security issues by shifting the focus away from video surveillance to analytics and generating alerts for security staff.

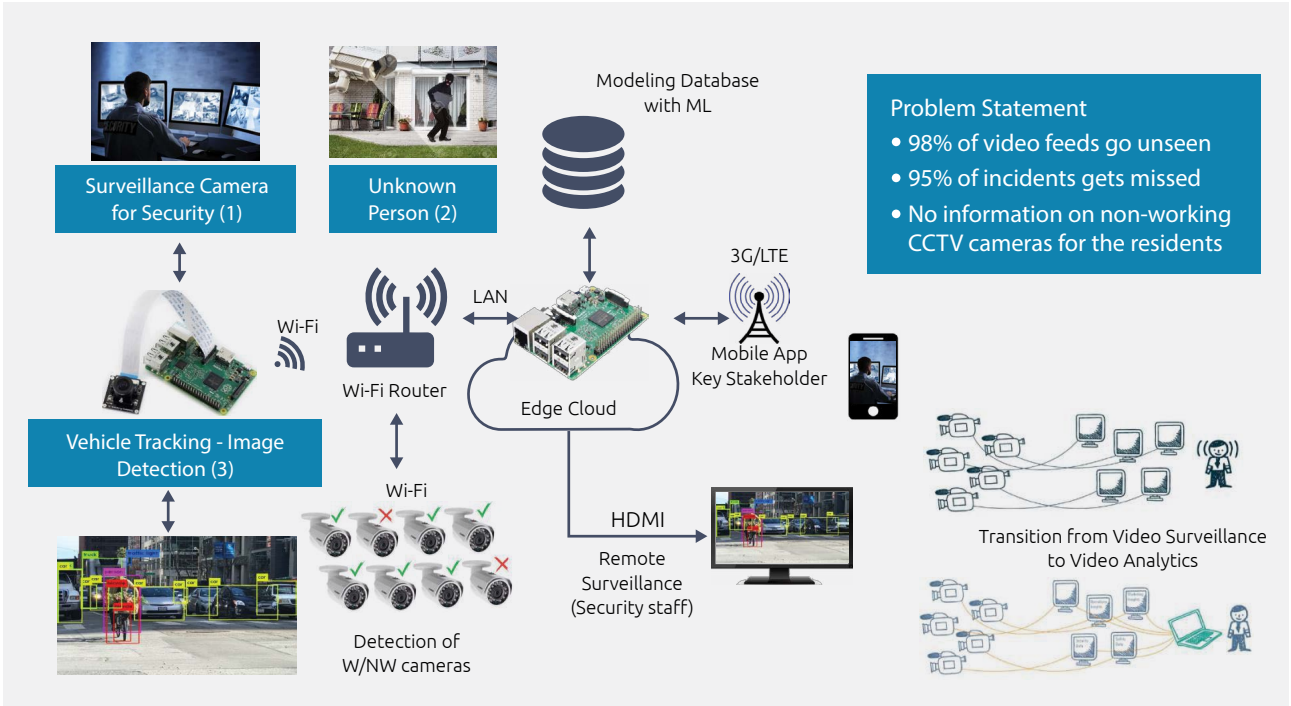


Figure 12. Residential community surveillance with an edge-based approach
Source: Capgemini Engineering

Video analytics of the camera feed acts as an edge device. The main advantages are a distributed system architecture and a massive reduction in bandwidth. Since the camera filters the unwanted information, it avoids transferring all the video data to the cloud platform, saving network bandwidth. That is one example of the use case of a camera functioning as an edge device to address a critical challenge faced in smart residential and campus applications.

Challenge 2: Seamless connectivity, session persistence and data management in the connected car

A significant challenge for the connected car is feature richness, which is the focus for many luxury car models. There are two immediate challenges carmakers face.

First, the most challenging part in the connected car is the amount of data processing required, generated from sensors such as electronic control units (ECUs), Lidar, radar, and cameras mounted on the car. (See Figure 13.)

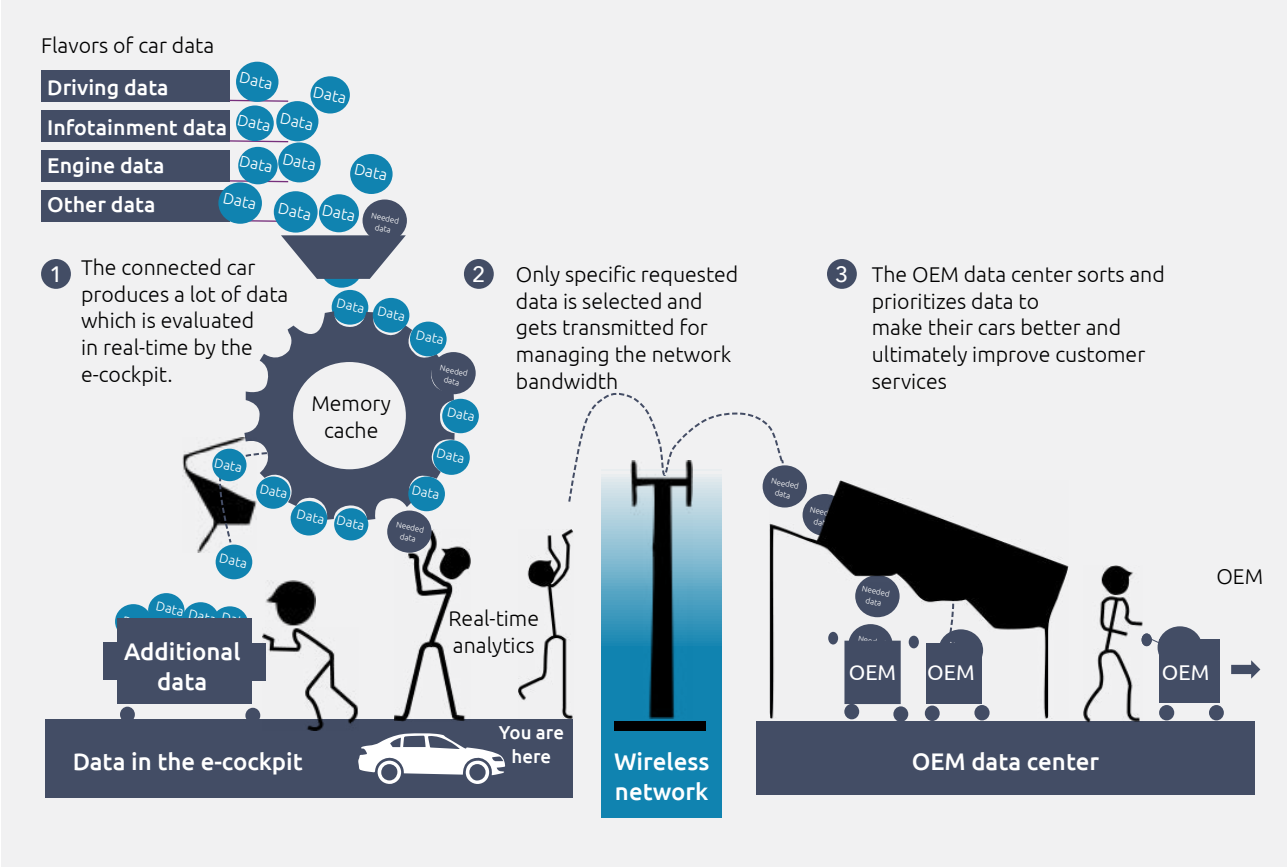


Figure 13: Flavors of car data
Source: Capgemini Engineering

The sensors located in the car produce various data, including telematics, drowsy driver, location, and surveillance, where the vehicle needs to analyze and respond to the data in nanoseconds. Edge plays a crucial role in the connected car ecosystem because it eliminates the need for a centralized data-processing warehouse in the OEM's data center and performs real-time analytics inside the car without a lag or the need for internet bandwidth. (See Figure 14.)

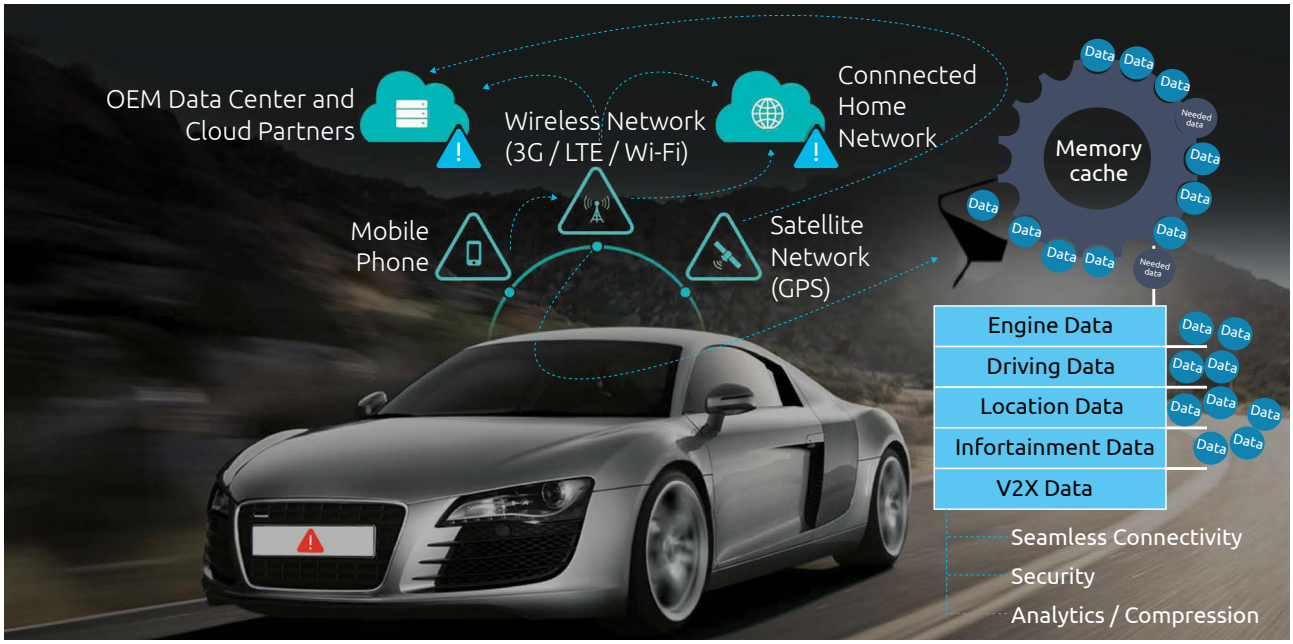


Figure 14. The auto ecosystem at the edge
Source: Capgemini Engineering

Another major challenge for the connected car is seamless network connectivity to share certain critical data with the OEM data center captured in the car network, and access the required services from service providers while driving. The advancements in telematics and security have become a requirement for remotely monitoring the connected car's performance and provide better service to end-users by both OEMs and mobile network operators (MNOs). The e-cockpit that acts as an edge gateway and resides inside the car should be intelligent enough to address the connectivity challenge based on the following:

- The car should be able to detect automatically the best available network based on user-defined policies and provide seamless connectivity, seamless switching, and seamless handoff across different network interfaces, including 3G, 4G, 5G, and Wi-Fi hotspots
- Avoid the ping-pong effect to reduce continuous handover between wireless networks
- The car should provide secure connectivity when switching between different wireless networks and maintain session continuity with persistence for all connected devices used by passengers connected over different devices in the car network
- QoS connections for different wireless networks should be continuously monitored. If the wireless network's performance does not meet the threshold for connectivity, network switching needs to have seamless connectivity to ensure the expected QoS of the end-users
- As the user preference would be more specific for different applications, such as telematics and safety-related applications, the connectivity should be provided more securely with less data and packet loss in the entire car's mobility landscape

Challenge 3: Data security and data aggregation in the retail segment

There are many compelling use cases in the retail market segment, such as smart inventory, smart shelf, and real-time tracking. At the same time, some challenges require a broader retail focus. (See Figure 15.) One major challenge for retailers is theft identification, especially in the jewelry market. Problems like burglary, worker theft, paperwork errors, vendor fraud, and monitoring shipments require quick real-time analytics instead of storing the data and analyzing it later with standard surveillance equipment.

Another challenge is spoilage, especially in the food retail sector. For instance, one large retail chain reported a nearly $2 billion loss due to wasted and spoiled food caused by a legacy refrigeration system. Specifically, alarms from the controllers on the refrigerators were slow to reach the operations and maintenance team.

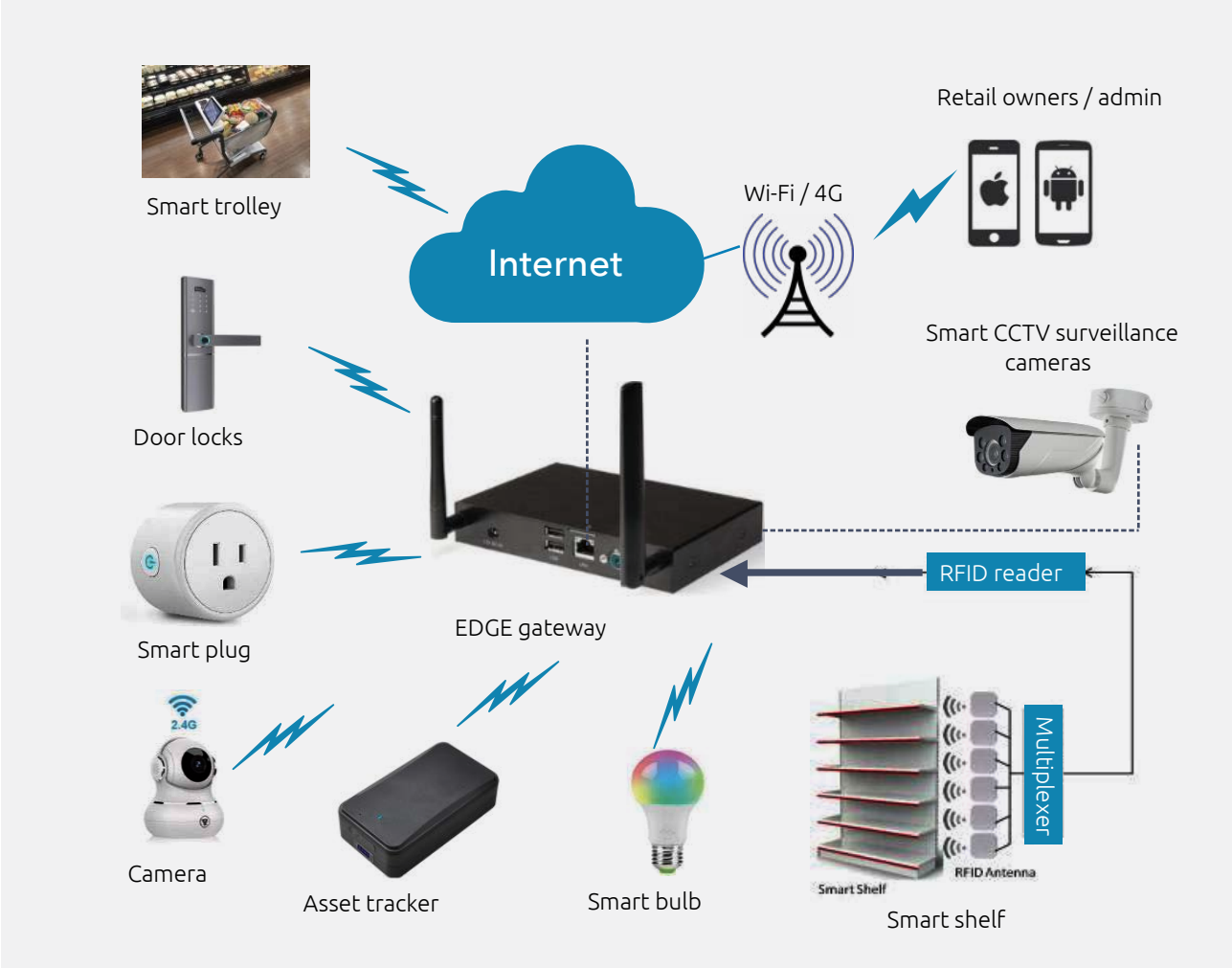


Figure 15. Data security in retail
Source: Capgemini Engineering

Another challenge in the retail business is the cost associated with operating equipment. More efficient and connected energy management systems and maintenance can reduce costs in three areas:

- Refrigeration
- Lighting
- Heating and air conditioning

Other challenges that edge can address include:

- User behavior analytics in a crowded area for a new product launch
- In-store navigation is a critical need in retail stores, especially during expansion. An example is the digitization of physical assets and end-products
- Maintaining social distance between workers and customers during the Covid-19 pandemic

Addressing retail challenges with data collection, processing, and management, and supporting various technologies, protocols, and devices is a significant task and needs to be managed by a single entity called the edge gateway, located on the retail premises. With an edge-based model, retailers can improve store operations and enhance the customer experience to drive purchases.

Challenge 4: Condition-based monitoring for Industry 4.0

Condition-based monitoring (CBM) is a maintenance strategy used in factories and automated processing plants such as chemical and oil-and-gas facilities to monitor critical operational parameters of assets to determine their changes under various conditions. CBM typically measures process parameters such as pressure, temperature, pH, noise, vibration, flow, misalignments, motor bearing failures, and more. Also, samples are measured, such as the condition of the oil, electric motors, engines, gearboxes, fans, electrical control panels, compressed air, and hydraulic systems. (See Figure 16.) The measurements taken from this sophisticated equipment are called "conditional measurements" and are essential for identifying the condition of the equipment being monitored regularly.

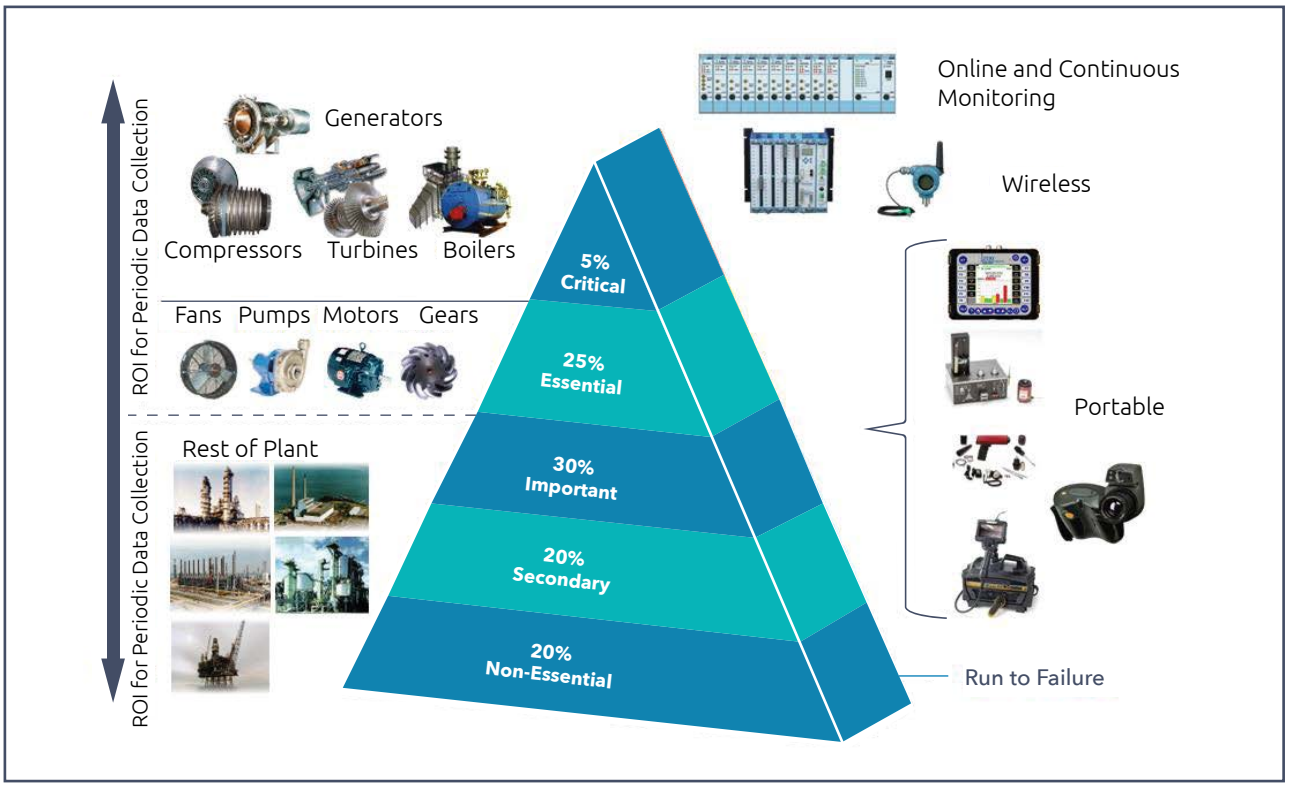


Figure 16. Condition-based monitoring in industrial plants
Source: IEEE

Condition-based monitoring is an element in large factory-based environments to handle predictive maintenance and monitoring. It is essential to take measurements regularly and quickly assess the data generated closer to the equipment to manage critical operations. The edge gateway interfaces with various sensor-node data streams to monitor equipment in real-time, evaluate conditions, generate alerts, and trigger maintenance immediately to avoid damage to the equipment or plant.

The field technicians working in the plant can monitor equipment performance with the help of the edge gateway to reduce the risk of equipment downtime or failure. The collection and analysis of specific data at the edge of the network can accurately diagnose the problem more quickly than managing and monitoring via a cloud platform. The maintenance team can also plan for appropriate maintenance actions to prevent failure and ensure continuous operations of the equipment, which saves money, improves labor efficiency, and creates new revenue streams based on the data monitored and analyzed. With CBM, the field engineers can measure the equipment's health, performance, reliability, and integrity and predict and prevent significant failures before they happen.

Embedded platforms for the edge

Today, several embedded platforms are being used to develop edge solutions for IoT applications. Some platforms are ruggedized commercial platforms, while others are emerging AI-based embedded platforms used to create edge-based IoT solutions. Figure 17 shows some of the leading platforms for building edge-based IoT solutions in various market segments.

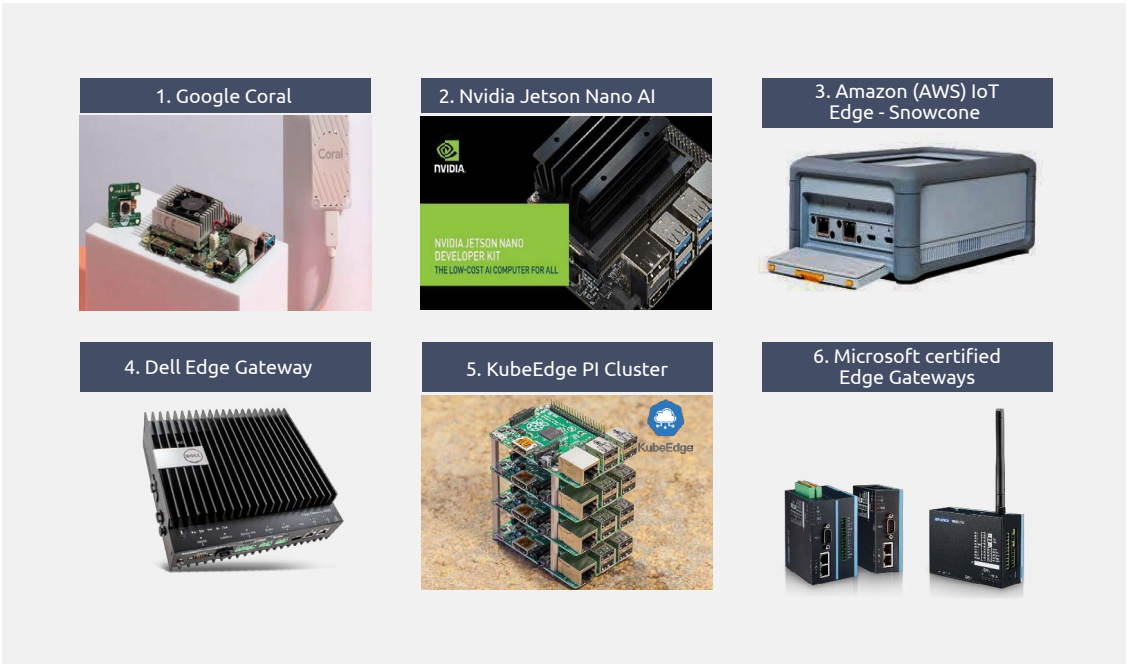


Figure 17. AI-based embedded edge IoT platforms
Source: Amazon, Dell, Google, Microsoft, Nvidia, KubeEdge

Point of view

Capgemini Engineering believes that edge-based IoT-solution design covering sensor nodes and gateways can bring many advantages to the consumer and industrial market segments. (See Figure 18.)

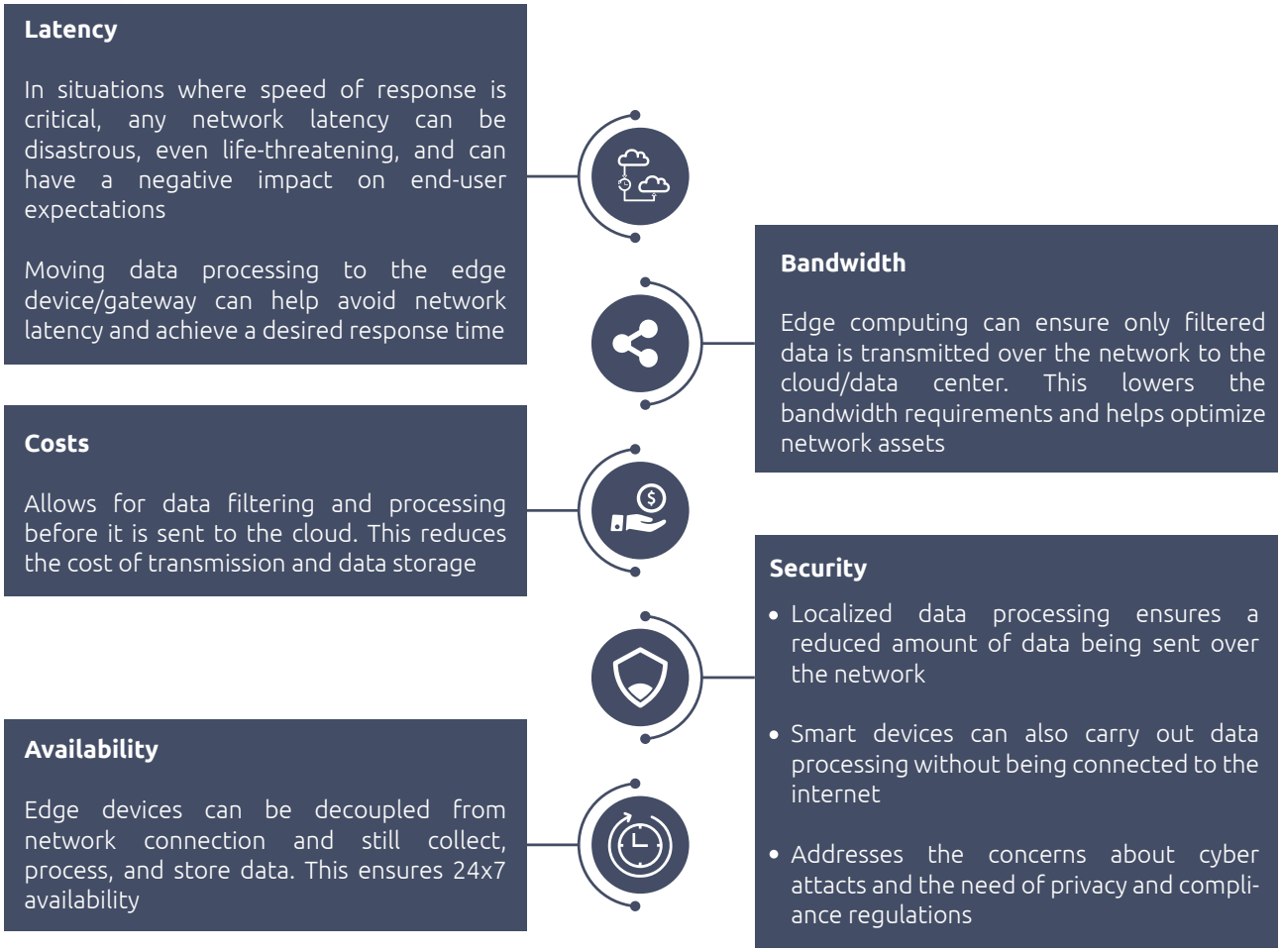


Figure 18. The benefits of edge-based IoT solutions
Source: Capgemini Engineering

Edge is a significant step in the emergence of IoT networks that enable interoperability between short-range networks like Wi-Fi, Zigbee, and Bluetooth, and long-range networks like 4G and 5G networks. Edge is used in many industry sectors to address user-driven applications. 5G is an enabling technology for IoT in the near term. For example, today, IoT is a crucial enabler of smart-city initiatives. With 5G, smart cities will be linked together in a more extensive infrastructure deployment based on advanced 5G feature support like mMTC and URLLC.

Conclusion

The edge-based deployment model will be essential for future IoT network deployment along with emerging technologies like 5G. Also required is support from technologies and protocols like LWM2M, energy harvesting, AI, Apache Spark, Tensor Flow Lite, MongoDB, Docker, Kubernetes, MERN, Kafka, SDN, NFV, and others for managing the design of edge-based devices, wireless sensor nodes, and gateways. (See Figure 19.) Shifting data processing and data offloading to edge sensor nodes, or the edge gateway simplifies the pressure on network bandwidth, and speeds processing and responsiveness. Here, there is less dependency on the cloud platform provider, except for storing a massive quantity of data for analysis in the long term.

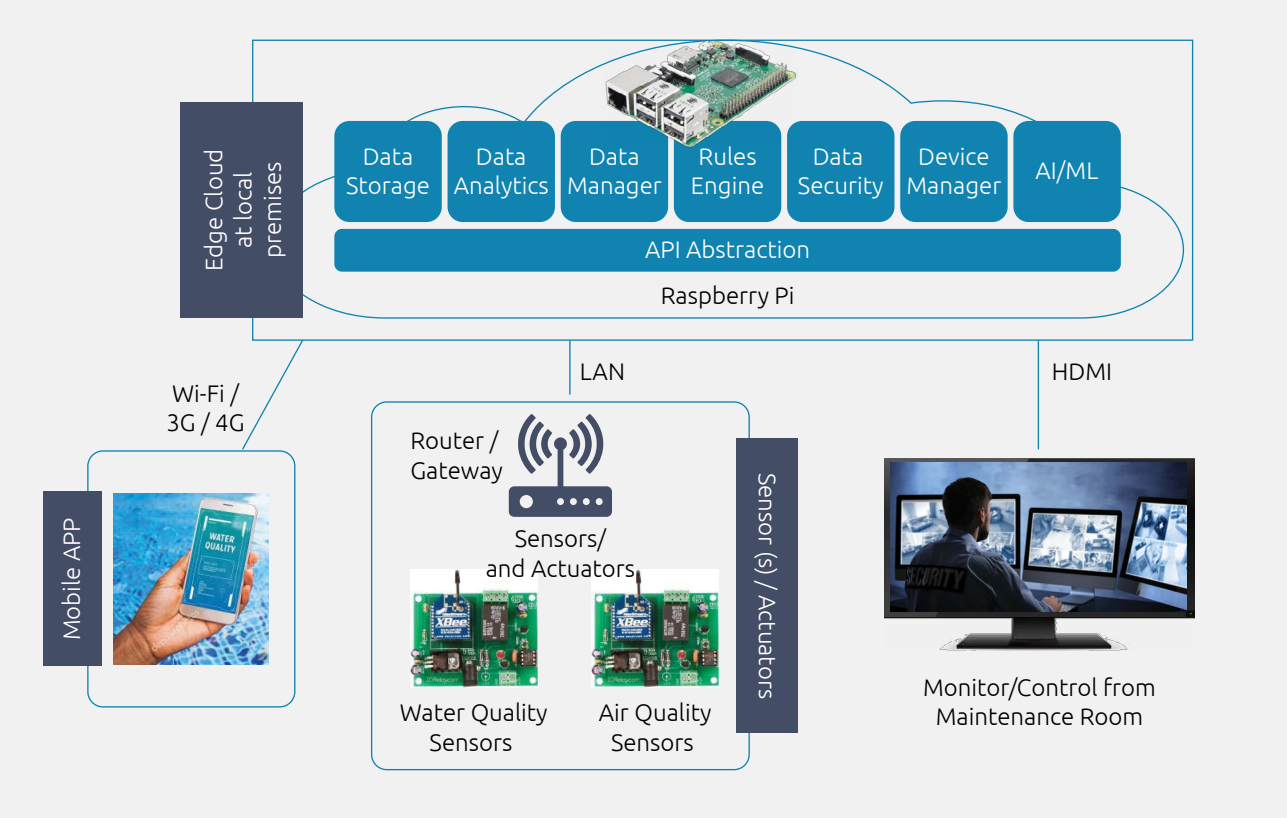


Figure 19. Edge Cloud design
Source: Capgemini Engineering
Image Source: Google

In addition to reduced latency, cost reduction, efficient energy management, less bandwidth, and improved privacy and security – which are critical benefits of edge in the IoT ecosystem – edge also addresses other important factors such as self-healing edge nodes and the seamless convergence of IT and OT.

Author

Vijay Anand

Assistant Vice President,
Technology, and Chief IoT Architect,
Capgemini Engineering

Vijay plays a strategic leadership role building connected IoT solutions in a number of market segments including consumer and industrial IoT. He has over 25 years of experience and has published 19 research papers, including IEEE award-winning articles. He is currently pursuing a Ph.D. at the Crescent Institute of Science and Technology, India.

Capgemini engineering

About Capgemini Engineering

Capgemini Engineering combines, under one brand, a unique set of strengths from across the Capgemini Group: the world leading engineering and R&D services of Capgemini Engineering – acquired by Capgemini in 2020 - and Capgemini's digital manufacturing expertize. With broad industry knowledge and cutting-edge technologies in digital and software, Capgemini Engineering supports the convergence of the physical and digital worlds. We help clients unleash the potential of R&D, a key component of accelerating their journey towards Intelligent Industry. Capgemini Engineering has more than 52,000 engineer and scientist team members in over 30 countries across sectors including aeronautics, space and defense, automotive, railway, communications, energy, life sciences, semiconductors, software, and internet and consumer products.

For more details, contact us :

www.capgemini-engineering.com

Write to us at:

engineering@capgemini.com