Chapter 9
IoT Vertical Markets and Connected Ecosystems

The Internet of Things is expected to connect over 20 billion "things" to the Internet by 2020, covering a broad range of markets and applications. As IoT becomes more cost-effective and easier to deploy, new contenders and industry players are expected to enter the market. Hence, existing companies will be forced to disrupt or be disrupted. For the leaders of any of these companies, this begs two main questions: firstly, what new business models to employ in order to deliver better and cheaper service? And secondly, who to partner with to bring services to market quicker and at a lower cost?

In this chapter, we will first introduce, in Sect. 9.1, the key IoT application domains, which are often referred to in the literature as IoT verticals. Alphabetically, key verticals include agriculture and farming, energy, enterprise, finance, healthcare, industrial, retail, and transportations.

These verticals will include data sources (e.g., sensors, RFIDs, video cameras, etc.) producing wealth of new information about the status, location, behaviors, usage, service configuration and/or performance of systems, products, or devices. In Sect. 9.2, we will present the new business model which is mainly driven by the availability of new information, thereby offering extraordinary business benefits to the companies that manufacture, support, and service those systems, products, or devices, especially in terms of customer relationships. In Sect. 9.3, we will present the top requirements to deliver "anything as a service" in IoT followed by a specific use case.

Finally, the manifold IoT verticals in combination with the new business model will undeniably introduce opportunities for innovative partnerships. No single vendor will be able to address all business requirements. We will describe the requirements for such model in the last section.

A. Rayes, S. Salam, *Internet of Things From Hype to Reality*,
https://doi.org/10.1007/978-3-319-99516-8_9

9.1 IoT Verticals

There is no agreement across the industry on the number of IoT verticals. The number ranges from a few to over a dozen across various standards and marketing collaterals. The oneM2M and ETSI standard bodies have identified ten IoT verticals: agriculture and farming, energy, finance, healthcare, industrial, public services, residential, retail, and transportation. Other companies have used a slightly different categorization to include energy, transportation, education, healthcare, commerce, travel and tourism, finance, IT, and environment.

As we mentioned in the previous chapters, the objective is not to divide IoT into verticals and silos. On the contrary, the real impact of IoT will only occur when data from the silos is combined to create completely new types of applications. In other words, an IoT application should be able to manage IoT elements from many verticals with common parameters, open data models, and APIs. The collected data from IoT elements, combined with the new knowledge emerging in the area of "big data," will create the framework for many new types of applications. This progress will drive the growth of IoT.

In this chapter, we will describe IoT use cases using a modified version of the oneM2M and ETSI categorizations, as shown in Fig. 9.1. The IoT verticals include agriculture and farming, energy, oil and gas, enterprise, finance, healthcare, industrial, retail, and transportations.

It is important to note that some IoT standard bodies have used the term "energy" as a comprehensive label to include "energy consumption" in smart buildings/cities as well as "oil and gas" in the petroleum industry (e.g., to monitor oil rigs, pipelines, and emission). We believe IoT energy and IoT oil and gas are two separate verticals. Energy comes from oil and gas as well as other sources such as solar and winds. In

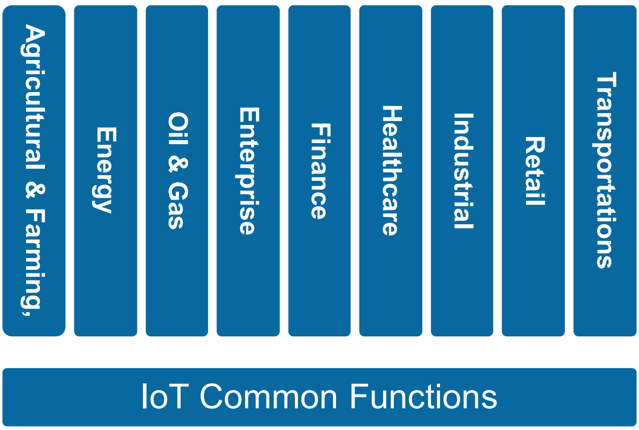

Fig. 9.1 IoT verticals

addition, energy is about managing smart meters, smart buildings, and smart cities, while oil and gas is more about process and asset management in the petroleum industry. More information will be provided in Sects. 9.1.2 and 9.1.3.

9.1.1 IoT Agriculture and Farming

According to the World Agriculture reports, global food consumption is expected to grow by 70% by 2050. IoT is well positioned to transform the agriculture industry and enable farmers to increase the quantity and quality of their crops at reasonable costs. IoT farming techniques are already increasing crop productivity and creating economies of scale for farmers. This is critical especially with the recent environmental challenges farmers are facing, such as increased water shortage in many regions of the world and the diminishing availability of farmland.

IoT sensor-based agriculture solutions are used to monitor soil moisture, crop growth, livestock feed levels, and irrigation equipment. The solutions utilize analytics to analyze operational data combined with weather and other information to improve decision-making.

Top IoT agriculture and farming use cases include:

- *Advanced yield monitoring:* Farming companies have introduced solutions to monitor and control various types of crops to deliver better results. For instance, wine quality is being monitored by installing sensors to monitor soil moisture and trunk diameter in vineries to optimize the amount of sugar in grapes. Similar techniques are used for water management by sensing the soil and determining the optimal amount of water required as part of green initiatives.
- *Optimal seeding:* Based on soil analysis and historical weather data, IoT-enabled solutions determine the best kind of seeds and optimal row spacing as well as seeding depth. They also produce soil fertilization recommendations that include the type and amount.
- *Optimal water usage:* Monitoring and controlling surrounding environmental conditions to determine water usage to capitalize on the production of fruits and vegetables. This includes utilizing weather forecast information to prevent damage due to ice formation, heavy rain, drought, snow, or strong wind. The humidity levels are also monitored in crops such as hay and alfalfa to avoid fungus and other bacterial contaminants.
- *Livestock monitoring:* Monitoring, tracking, and controlling farm animals (cows, goats, chickens, etc.) in open grasslands or indoor locations such as cages or stables. IoT is also used to monitor animal toxic gas levels, study ventilation, and warn on air quality to protect farm animals from harmful gases from excrements.
- *Farming as a service:* See Sect. 9.2.

9.1.2 IoT Energy Solutions

IoT energy covers smart buildings offering dynamic monitoring of overall energy consumption, thereby allowing their occupants or tenants to see when they are consuming power during peak hours at abnormally high rates. This allows the tenants to optimize energy usage while maintaining comfort. It also covers smart cities offering automatic dynamic optimization of global energy consumption on the streets, highways, and public facilities.

IoT energy use cases include:

- *IoT smart meters*: IoT smart meters record electrical power consumption on regular basis (e.g., hourly, every 15 min) and send collected information to the power company for monitoring and billing.
- IoT smart meters benefit power companies as well consumers. Power companies use the collected information to construct usage patterns and trend analyses to predict future energy usage especially during peak hours. They plan for such peaks with additional supply and by offering very attractive offers to customers to conserve energy. Customers use the information to view, typically on the portal of the power company, hourly electric and daily gas energy usage data. Consumers use the detailed hourly, daily, weekly, or monthly information to make smarter energy choices (e.g., use washing machine after 7 PM for cheaper rate).
- *Smart homes (connected home):* Connected home is defined as any home with at least one connected device (e.g., connected appliance, home security system, and door or motion sensor). Connected devices can learn usage patterns and enable remote operation to reduce energy consumption (e.g., water heaters, air conditioning, and lighting).
- Connected devices send information to service provider systems, which in turn, quickly analyze the data and notify homeowners if needed or directly send alerts to homeowners. The first model is often a subscription-based service in which a homeowner subscribes to a service (e.g., home security company), while the second model is non-subscription model (e.g., home security camera installed by homeowner and connected over the home Wi-Fi gateway). Can you name an example of model 2 (see Problem 8)?
- *Other cases:* IoT is also used to monitor and optimize solar energy plants' performance. How (see Problem 10)?
- To meet the IoT key promise of making human lives better, all connected home devices should come together into a single connected IoT system or connected service provider system offering the homeowner full and simple access and control.

9.1.3 IoT Oil and Gas Solutions

Ever since the explosion and sinking of the Deepwater Horizon oil rig in the Gulf of Mexico in April 2010, which was recognized as the worst oil spill in the US history, combined with the increase in strict government regulations, IoT has been at the core of the oil and gas industry transformation. It is not only enabling full real-time monitoring of oil rigs but also allowing contingent workforce to run near real-time maintenance of critical assets.

IoT oil and gas is used for predictive maintenance, pipeline monitoring, emission control, and location intelligence. It is also used for near real-time alert and trending analysis using sensors, installed on various equipments, and augmented with ERP (enterprise resource planning) data to trigger maintenance workflows for asset management and fleet operations monitoring.

- *Connected oil and gas fields:* IoT sensors are being installed to monitor and control oil wellheads, pipelines, and equipment, to enhance the overall oil field remote operations, to enable predictive maintenance, and to provide comprehensive facility operations at reasonable costs, hence achieving better reliability and productivity from the fields.

- Also connected oil and gas fields reduce the need for site visits (e.g., site visits to unmanned offshore platforms), hence reducing the associated hazards and improving personnel safety.
- *Downstream applications:* IoT oil and gas also can play a role in downstream operations such as oil and gas storage, transportation, refineries, and distribution (e.g., petrol station fuel tanks can be monitored by distribution companies to dispatch tank trucks).

Oil and Gas Exercise

Chemical injection stations (Fig. 9.2) are used to dose corrosion inhibiting and biocide chemicals into oil pipelines. This eliminates the growth of organisms and reduces the corrosion rate of the pipelines in order to prolong their operational life.

One chemical station is required to dose at a rate of 0.4 gpm (gallons per minute) of chemicals per 10,000 bpd (barrels per day) of oil in the pipeline. In an existing plant, the station is set to dose at a constant 0.4 gpm. Considering the following pipeline flowrate profile during a day, calculate the quantity of chemicals saved per day by applying IoT to control the chemical injection station.

Answer

We only need to examine the part of the timeline where the flow within the pipeline drops below the 10,000 bpd threshold, as that's where the IoT solution will yield savings over the constant/static solution.

The flow within the pipeline drops to 8000 bpd for 12 h. During this time, the variable dosage supplied by the IoT solution drops to 8000/10000 * 0.4 gpm = 0.32 gpm.

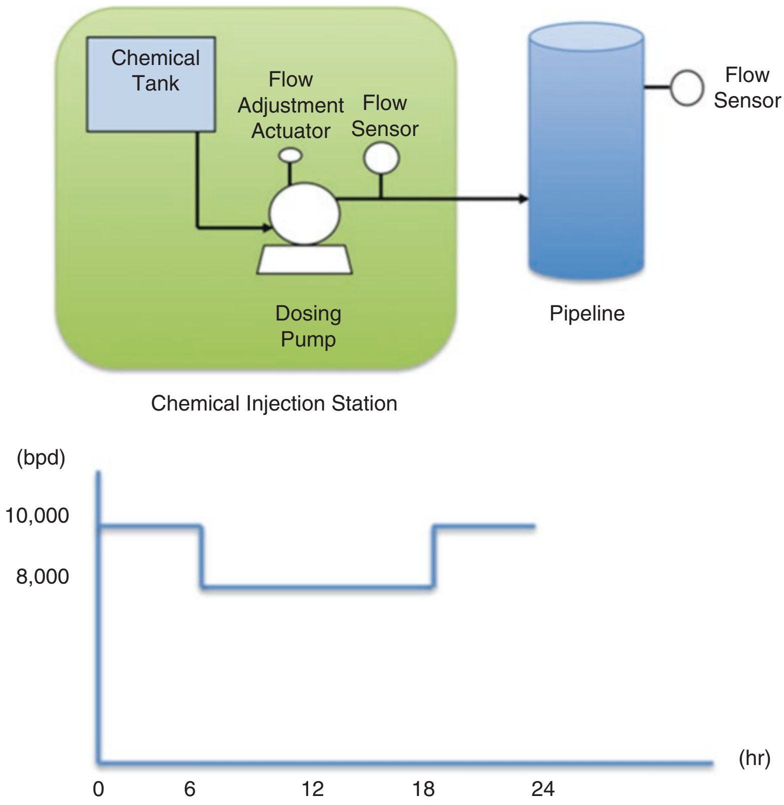

Fig. 9.2 Oil and gas exercise

The amount of chemical dispensed by the IoT solution for those 12 h = 0.32 gallons/minute * 12 h * 60 min/h = 230.4 gallons.

The non-IoT solution would have dispensed during the same time = 0.4 * 12 * 60 = 288 gallons.

The savings = 288–230.4 = 57.6 gallons.

9.1.4 IoT Smart Building Solutions

As with smart homes (under smart energy), smart buildings utilize sensors and controllers to monitor and automatically trigger services to save valuable time in cases of emergency (e.g., fire, intrusion, or gas leak). With the smart building system, services like video monitoring, light control, air-condition control, and power supply control are often managed from the same control center. In this section, we will focus on smart buildings as an enterprise solution, as specified in the oneM2M standards.

- *Safety monitoring and alerting:* Examples include *noise level monitoring* in urban zones and sounding alarms in real-time, *electromagnetic field level monitoring* by measuring the energy radiated by cell stations and other devices, *chemical leakage detection* in rivers by detecting leakages and wastes of factories in rivers, *air pollution* and control of CO_2 emission factors, pollution emitted by cars and toxic gases generated in farms, as well as *earthquake early detection.*
- *Smart lighting:* In smart lighting, IoT is used to minimize energy consumption, to provide weather adaptive lighting in streetlights, and to automate maintenance.
- *Flooding, water leakage, and pollution monitoring:* Monitoring of safe water levels in rivers, lakes, dams, and reservoirs. Detection of the presence of toxic chemical. Monitoring of tanks, pipes, and pressure variations. Real-time control of leakages and waste in the sea.
- *Detection of hazardous gases and radiation levels*: Detection of gas levels and leakages in and around industrial buildings and chemical factories. Monitoring of ozone levels during the meat drying process in food factories. Distributed measurement of radiation levels in the surroundings of nuclear power stations to generate leakage alerts.
- *Other use cases include* detection of garbage levels in containers to optimize the trash collection routes, preemptive monitoring of burning gases and fire conditions to define alert zones, snow level measurement to know in real time the quality of ski tracks and alert avalanche prevention security corps, monitoring vibrations and earth density to detect dangerous patterns in land conditions, and monitoring of vibrations and structural conditions in buildings and bridges.

9.1.5 IoT Finance

While IoT financial solutions are not as obvious as other IoT verticals, the financial industry has indeed benefited greatly from IoT. For many financial services businesses, the reality is that their business model is based on the flow of information, rather than on actual sensors and physical objects. As we mentioned in Chap. 1, some financial companies (e.g., Square, Intuit) have introduced IoT platform-based solutions connecting customers instantly with financial institutes and services. Such process used to be tedious and required time that often resulted in losing prospective deals to competitors. Banks are using IoT-based facial recognition solutions to identify important customers when they walk into the bank so they can be offered first-class treatment.

Auto insurance companies are working with technology companies and communication service providers to install sensor-based IoT telematics solutions in automobiles, to track driver behaviors in order to improve underwriting and pricing of policies. Other use cases include:

- *IoT usage-based auto insurance:* Sensors are installed in vehicles to track actual mileage, car location, and driving areas. In addition, IoT-based claim filing system is utilized allowing drivers to file claims using their smartphones eliminating the need for expensive agents and paperwork.
- *IoT solution to reduce fraud and liability:* In highly delicate work environments (e.g., chemical or nuclear plants, physical activities), smart sensors may be embedded in employees' uniforms. This allows the IoT solution to monitor employee whereabouts in high-risk areas, warn them in real time of any potential danger, and prevent them from entering restricted areas. This should result in safer work environments for the employees and reduce fraudulent workplace-related claims for the employer.
- *IoT safety solutions:* Sensors embedded in commercial infrastructure can monitor safety breaches such as smoke, mold, or toxic fumes, allowing for adjustments to the environment to head off or at least mitigate a potentially hazardous event.
- Other use cases include IoT-based commercial real estate building-management systems to speed up the overall building management processes, location-based near-field communication (NFC) payment processing, paperless mortgage applications including home inspection, and the approval process.

The progression of financial IoT is not without its challenges. Most driving consumers and corporations are uncomfortable with the notion of being "watched" at all time. Many have asked for limits on the collection and use of sensor-based data. This is a critical area for the industry to address by introducing balanced solutions that allow the collection of adequately limited data while protecting the interests of clients and markets. Full disclosure of collected data (what are you collecting about me?) as well as the secure handling and use of personal information (who has access to my data and how is it being used?) is already being demanded by consumers and corporations.

9.1.6 IoT Healthcare

Healthcare is considered as one of the most important verticals for IoT. Healthcare providers as well as patients are in great position to benefit from IoT. Intelligent IoT wearable devices in combination with mobile apps are allowing patients to capture their health data easily and send medical information for up to the minute analysis. Hospitals are using IoT for real-time tracking of important medical devices, personnel, and patients.

Examples of IoT healthcare use cases include:

- *Fall detection:* Fall detection is considered a main public health concern among senior citizens. The number of wearable medical devices, systems, and companies offering services intended at detecting falling has increased radically over recent years. Fall detection alert systems, typically worn around the waist or neck, include intelligent accelerometers that differentiae normal activities from actual falls. Fall detection solutions are already improving the quality of life of many elderly or disabled people living independently. It should be noted that smartphones also use accelerometers to determine vertical and horizontal display based on orientation.

- *Tracking of medical devices:* Accurate tracking of expensive medical devices is very essential for hospitals especially in crowded emergency rooms with large medical staff. IoT solutions are being used to identify the exact location of such devices, identify last user, and then auto adjust the device setting, if applicable, based on the fingerprint of the current user.
- *Medical fridges for hospitals*: Sensors are being embedded in medical fridges for hospitals and medical offices to dynamically control temperatures inside mobile and stationary freezers filled with vaccines, medicines, and organic elements.
- Other use cases include measuring ultraviolet radiation and warning people of the hazard of sun exposure especially during certain hours.

As is the case with IoT financial, IoT healthcare has its own share of challenges. The security of IoT data and devices as well as government regulations is considered by many as the most important concern for patients and healthcare providers. Patients are concerned about employers gaining access to their medical records, especially when they register their BYOD mobile devices. Some physicians and healthcare IT departments are still adjusting to using and securing mobile devices in their operations. Finally the lack of standards and communication protocols around IoT puts the development of solutions at risk.

9.1.7 IoT Industrial

Industrial equipment and machines used in the overall manufacturing process, for instance, are becoming more digitized with capabilities to connect to the Internet. At the same time, manufacturers are looking at ways to advance operational efficiency such as supply chain and quality control, by utilizing such equipment to gather important data for their business to remain competitive and provide services at reasonable costs.

IoT is used to establish networks between machines, humans, and the Internet, thereby creating new ecosystems. It is also used to identify business gaps and opportunities, as we will cover in Sect. 10.3. Examples of industrial use cases include:

- *Predictive maintenance:* Predictive maintenance covers all connected assets in industrial plants (e.g., water treatment site). By utilizing real-time data collected from sensors and cameras, combined with advanced analytics, it is possible for companies to anticipate equipment failures and respond faster to critical situations. Advanced analytics is a hot research area that includes artificial intelligence and machine learning. With machine learning, computers can develop

algorithms on their own by analyzing data overtime. These algorithms can then be used to make predictions.
- *Connected factory:* As the name indicates, connected factory means connecting the entire factory network to the Internet with full monitoring and controlling solution. Connected factory typically includes mobile operation center for comprehensive and secure management.
- *Connected mine:* In connected mines, all mining vehicles, mining operation, mining asset tracking, and personal safety equipment are connected.
- *Supply chain control:* Monitoring of storage conditions along with the supply chain and product tracking for traceability purposes.

9.1.8 IoT Retail

According to a survey by Infosys, more than 80% of consumers are willing to pay up to 25% more for a better experience. This translates to a huge opportunity to be gained with IoT by collecting and analyzing information about products and customer interests and then gaining actionable insights from this information. Input sources include point of sale (PoS), supply chain sensors, RFID, as well as video cameras in the store.

- *Full tracking of products in stores:* With IoT, retailers have full visibility into products and merchandise with digital supply chains. This makes it possible for retailers to emphasize on top-selling products by offering more personal choices to fulfill and enhance the overall customer experience. It also makes it possible to determine under-selling products as well as overstocked and low stock products.
- *Full automation of product delivery:* The range of delivery options may be offered to the customers including pick up in store, home, or car delivery or retrieval from another location such as smart lockers from local 24-h stores. In the latter case, smart lockers are equipped with sensors that send automatic messages to customers reminding them to pick up.
- On the business side, some retailers have capitalized on IoT to redesign their distribution system to leverage larger stores as distribution centers. In this case, larger stores are used to offer a larger range of products to smaller stores for collection on the same day, thereby extending customers' choice of delivery and collection options.
- *Flexible shopping and loyalty programs*: Retailers are already using web technologies such as cookies, Wi-Fi, and video cameras to track customers' shopping behavior to enhance customer experience and send special offers based on buying patterns or even online browsing and search trends. For instance, retailers are using Bluetooth beacons in combination with shopping apps on customers' smartphones to generate heat maps that show how consumers move around stores (why would customer download retailer apps?—See Problem 13). For

customers who are not willing to download retailer apps, Wi-Fi triangulation is alternatively used to generate detailed heat maps.

- *Customer engagement suite:* As we mentioned in Chap. 1, some companies have introduced customer engagement tools that include email marketing services. These tools allow businesses to target specific customer segments with customized promotions based on actual purchase history. Square also introduced Square Payroll tool for small business owners to process payroll for their employees.
- *Interactive consumer engagement and operations:* Using real-time video cameras, in-store programmable devices and in-store display screens retailers can deliver smarter messaging based on what customers are looking at. This allows them to influence buying decisions, including up-sells.

9.1.9 IoT Transportation

As industry regulations force transportation and logistics organizations to do more with less, many companies have already discovered the benefits of using IoT to offer new services, improve efficiency and security, significantly gain real-time visibility of their operations, and save on fuel, just to name a few advantages.

Top use cases include:

- *Smart and connected parking:* Smart parking addresses one of the causes of pollution in urban areas. We all have been in situations where we drive back and forth looking for a parking spot. Smart and connected parking has addressed this problem very effectively. With smart parking service, drivers can easily find available parking spaces, pay parking fees, and even make advance reservations. Making parking reservations may be available for limited people such as VIPs or the disabled, since ordinary parking service needs to satisfy first-come-first-served rule.
- *Smart roads and traffic congestion:* Smart roads include intelligent highways with warning messages and diversions based on sensors capturing climate conditions and traffic events like accidents and traffic jams. Traffic congestion solutions monitor traffic as well as pedestrian levels to optimize driving and walking routes.
- *Connected rail:* Connected rail solutions are used to connect trains, tracksides, stations, and passengers. For instance, IoT is used to automatically alert passengers of scheduling and safety issues on their smart devices as well as offering onboard entertainment. IoT is also used to implement solutions to meet governmental and industrial safety compliance requirements at a minimum cost.
- Other use cases include continuous quality of shipment monitoring, which encompasses observing vibrations, location, temperature, strokes, container openings, and storage incompatibility detection, for instance, emission warning on containers storing flammable goods close to others containing explosive material. Control of routes followed for delicate goods like medical drugs, jewels, or dangerous merchandise are also included.

9.2 IoT Service Model: Anything as a Service

IoT-enabled devices and products will provide a wealth of information about their status, location, behaviors, usage, service configuration, and performance. This information, if leveraged correctly, offers extraordinary business benefits to the companies that manufacture, support, and service those products, especially in terms of customer satisfaction.

With the availability of such data combined with cost-effective Internet-based communications, many companies are starting to ponder why would they stop at selling a product and forgo very essential feedback information, when they can also sell a service with the right to monitor the actual usage and behavior of the product in the deployed environment. Usage information is not only used to service a product/device and prevent service deterioration by verifying contract service-level agreements (SLAs) but also to learn about the product in the field and determine the most essential set of future enhancements. Feedback information may be categorized by market segments but generally include common set of specific information such as which features are used the most, which features are used the least, and which features are never used and feature usage patterns (feature A is used with feature B).

IoT is bending the traditional linear value chain by allowing companies to economically connect to products and collect essential data. The data is then analyzed and correlated with business intelligence (BI) and intellectual capital (IC) and used to provide a proactive, predictive, and preemptive service experience. This is made possible with the creation of a "feedback loop" through which the heartbeats of manufactured objects continually flow back though the complex business systems that create, distribute, and service those products. Adopters of this new IoT service model are in a great position to deliver extraordinary business performance and break away from their competition.

With this model, many companies are already offering at least a form of their products (or main features of such products) as a service with an always-on connection to fully monitor actual usage and behavior in the deployed environment. Next we will present a few key examples.

9.2.1 Thrust as a Service

Aircraft engine manufacturers are moving from the business of selling engines to the business of selling thrust as a service. In fact, Rolls-Royce has been offering such services for the last several years. It sends jet engine telemetry data to data centers for full analysis and diagnostics. An inspection can be scheduled at the correct time, or spare parts can be directed to the right destination even before the pilots or the airline know that one of their engines has a problem.

Today most of Rolls-Royce engines are not sold but rented out on an hourly basis under their TotalCare® program, and a center is monitoring maybe hundreds or even thousands of engines at the same time. This model allows Rolls-Royce to accumulate a wealth of engine operational data and enables it to consult airlines on best practices. This makes it difficult for third parties to take maintenance business away from Rolls-Royce. Figure 9.3 illustrates the framework of “thrust as a service.”

Other aircraft engine manufacturers have similar programs. Airlines do not pay for the engines but for the time they are flying. With this model, engine manufacturers have a strong incentive to improve the reliability of their engines and drive out third-party maintenance providers.

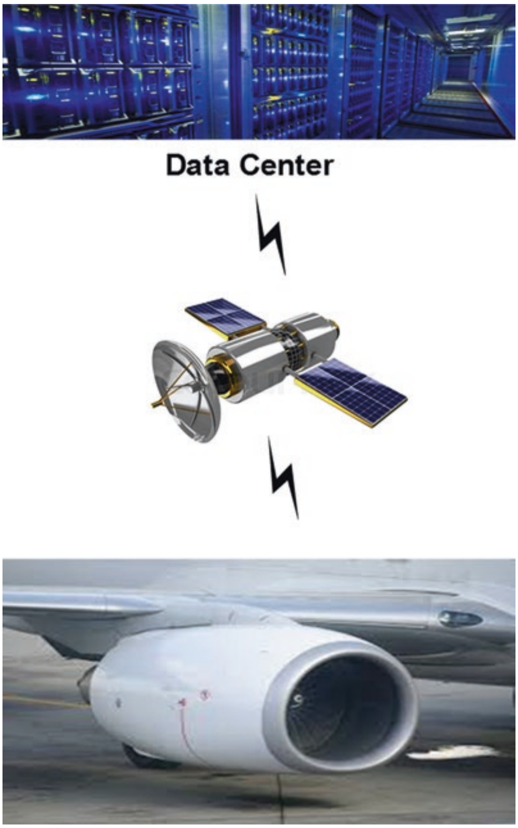

Fig. 9.3 Connected jet engine

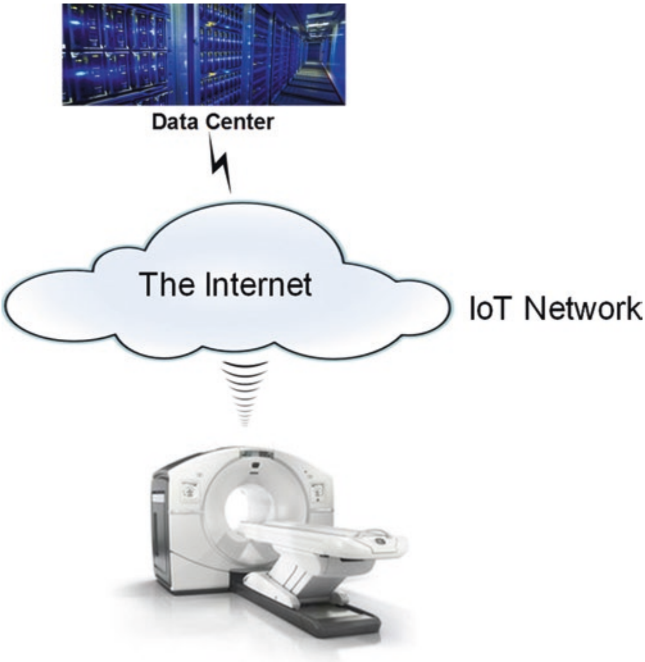

Fig. 9.4 Example of CT machine connected to a data center

9.2.2 Imaging as a Service

Hospitals and large medical facilities worldwide are being challenged with high cost of medical equipment and increased government regulations. Vendors of medical imaging machines (e.g., magnetic resonance imaging (MRI) machines, computed tomography (CT) scanners, and X-ray machines) are taking advantage of such challenges and offering "imaging as service" provisions. The new connected "as a service" business model is not only reducing imaging equipment operational costs but also offering equipment manufacturers, service providers, and hospitals new revenue streams. Figure 9.4 depicts an example of imaging as a service.

9.2.3 Farming as a Service

Agriculture machinery and chemical companies are also realizing the value of the new IoT service model. Tractors and many farming machines are being equipped with sensors and actuators. Agriculture machinery and chemical companies are partnering together to offer farming as a service (FaaS) where the farming machines are brought to a farm during seeding seasons. The machines analyze the soil square feet by square feet and send the data back to the agriculture machinery company

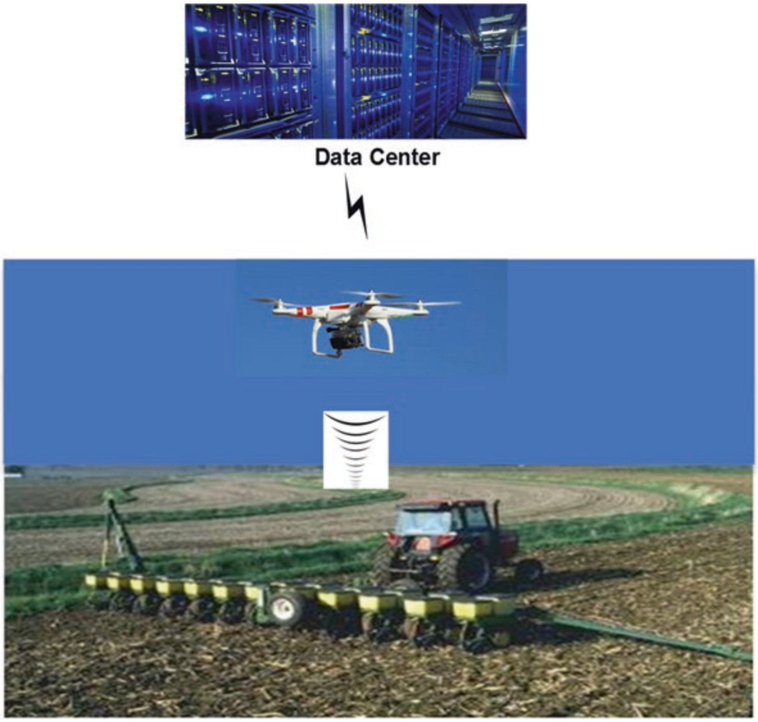

Fig. 9.5 Farming as a service (FaaS)

data centers, where the data is analyzed in real time, and the result is sent to actuators to release into the soil the best matching kinds of seeds and the right amount of fertilizers.

Farming machines (e.g., tractors) may be connected over cellular (e.g., 4G) networks or drones as shown in Fig. 9.5. In the latter case, drones are deployed by agriculture machinery companies just for the duration of seeding. Drones are typically used when the cellular signal is weak. What is another method of connecting agriculture machinery to the network (see Problem 7)?

9.2.4 IT as a Service

Another and perhaps less obvious example is the IoT network provider itself. Virtually all modern businesses/enterprises are powered by technologies, and visibility into the underlying infrastructure is mission critical. In the past, businesses relied on IT to deliver mission-critical business functions (e.g., customer portals, financial applications, email, supply chain systems, and a myriad of other crucial services that need to work flawlessly to prevent any impact on services and customers).

Today, businesses can no longer afford waiting for IT to provide all infrastructure capabilities.

As IT infrastructure continues to grow and becomes more complex, especially with the proliferation of hardware, software, applications, VMs, cloud services, and mobile devices, providing visibility into that infrastructure is a constant moving target.

Vendors of IoT hardware and software solutions (e.g., sensors, gateways, routers, switches, platforms) are also offering "feature as a service." For instance, a network vendor may own IoT getaways (or IoT routers and switches) and simply offers connection services with guaranteed SLAs (service-level agreements). As with previous examples, the networking vendor can only do so by enabling its IoT elements (e.g., gateways, routers, switches) to collect and send data to the vendor's data centers for service monitoring, analysis, and diagnostic. Such model also allows the vendors to gather a wealth of operational data and enables them to offer consultation to other enterprises on best practices (Fig. 9.6).

It should be noted that in all of the above examples:

- Any device or system (e.g., jet engine, medical imaging equipment, IoT gateways) downtime represents a loss of revenue or time, none of which airlines, hospitals, or IoT service providers are willing to lose. With IoT "as service" model, jet engines, medical imaging equipment, as well as IoT network elements

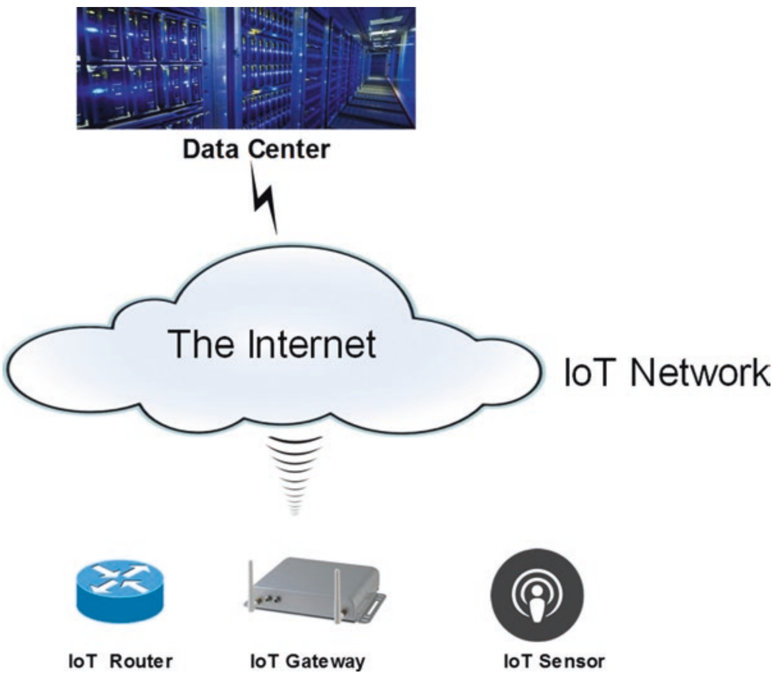

Fig. 9.6 IT as a service

are covered via service contracts with the original equipment manufacturers. Through remote predictive monitoring and maintenance, service contract providers can fix problems before the service is even impacted.

- The ability for manufacturers to connect and pull intelligence from their systems (e.g., jet engine, medical imaging equipment, IoT gateways) has been available for some time now, primarily as an outgrowth from their own support and maintenance service offers. With IoT, a new “as a service” model is being realized. Services on top of connectivity are improving equipment ROI and competitiveness for equipment vendors and stakeholders (e.g., hospitals, OEMs, and service providers). Also, in existing solutions, connectivity may not be realized over the Internet, rather over dedicated links and proprietary networks. However, many vendors are indeed building IoT platforms to transition from propriety rigid and expensive solutions into open economical IoT-based solutions.

9.3 Enabling “Anything as a Service”

In this section, we will describe the requirements for end-to-end intelligent service automation. This includes the basic requirements for specific instrumentation and telemetry data to be provided by the product, embedded management capabilities, as well as vertical-specific intellectual capital to provide a proactive, predictive, and preemptive service experience addressing the operations and health of the product.

Regardless of IoT verticals or underlying technologies, “anything as a service” can only be realized with several key capabilities. In this section, we will list these capabilities in ten main areas. Once the capabilities are enabled across the IoT layers, systems (e.g., IoT platform as we specified in Chap. 7) are required to automate the end-to-end functionalities.

Given the difficulties with providing generic answers across IoT verticals, we’ll use the thrust as a service as the guiding example for illustrations.

1. Which data to collect and from which entities? For example, for the thrust as a service example, the data includes jet engine operational parameters including engine RPM (revolutions per minute), fuel consumption, temperature, pressure, aircraft aerodynamic, and mechanical operational parameters such as wind speed, ground speed, positions of flaps, positions of slats, positions of spoilers, positions of ailerons, positions of rudders, positions of elevators, positions of horizontal stabilizers, fuel level, etc.
2. How to collect (or sense) such data? For example, use embedded pressure, temperature, or speed sensors or tap into aircraft control bus messages, etc.
3. Once the data is collected and while it is in the fog layer, what type of local analysis (e.g., by the collection agent itself) is required? For example, an hour of flight generates terabytes worth of data. It makes sense to compress this data by filtering out and compacting duplicate sensor readings before transporting the data over expensive satellite links.

4. How to transmit the collected (or locally analyzed) data from the device to backend data centers securely and with minimum impact on the network? For example, utilize satellite links for critical data that needs to be delivered in real time and airport Wi-Fi while the aircraft is docked at the gate for noncritical data.
5. How to entitle, validate parse, and analyze the collected data once it is received by the backend system? Hence, entitlement, data validation, data parsing, and data analysis require interactions with the supplier/partner backend systems and databases including intellectual capital information, e.g., matching the data with the correct models based on the jet engine model and aircraft type, segregating one airline's flight data records from those of another airline, etc.
6. Which service-based performance (e.g., end-to-end delay), diagnostic, and security compliance measures should be calculated at the backend and by which algorithms? For example, fuel economy can be a function of the engine RPM, wind speed and direction (head vs. tail), flaps/slats positions, etc. Complex algorithms come into play for that single performance metric.
7. Which thresholds (e.g., quality of service, grade of service) should step #6 estimated measures be evaluated against?
8. If step #6 estimated measures are above the threshold, what type of real-time and none-real-time actions should be taken in the impacted device and/or the network? Which algorithms? For example, suggest alternate flaps/slats settings on takeoff or landing to minimize fuel consumption.
9. If action is needed, which secure protocol should be used to access the device/network from the backend system and take action? For example, use secure socket layers (SSL) to encrypt communication between the aircraft and data centers.
10. Finally, which trending algorithms should be used to predict future measures?

Determining the required feature data (Question 1) is considered to be the most critical and difficult question especially for new technology. Feature data can only be defined if the performance measures and trending algorithms are well defined and understood.

Example: IoT IT Services
We will use the example of IT infrastructure as a service. Specifically, we will assume an IT infrastructure (e.g., IoT gateways and network switches) is deployed by an IT company to provide "IT service" to a transportation company.

IoT-based IT service requires identifying every managed entity with an IP address, collecting data from these managed entities, and performing event correlation based on vendor best practices and intellectual capital. Such information is used to proactively predict network and service performance and to provide information about future trends and threats to enable proactive remediation. This way, network planners/administrators can take action before a problem occurs, thereby preventing risk-inducing conditions from occurring at all.

The most essential input for an IT service is well-defined standardized embedded measurements to be collected from the network devices. This includes data subscribing to the standardized YANG (Yet Another Next Generation), data modeling language for the Network Configuration Protocol (NETCONF), or Simple Network Management Protocol (SNMP) MIBs. NETCONF and the older SNMP are network management protocols developed and standardized by the Internet Engineering Task Force (IETF).

NETCONF and SNMP are essential for FACPS (Fault, Accounting, Configuration, Performance, and Security) management. When NETCONF and SNMP data is not sufficient, “syslog” and the output of command-line interface (CLI) commands are also utilized. In fact, many network devices are configured to send syslog messages to an event collector, such as a syslog server, in response to specific events. The syslog protocol separates the content of a message from the transport of the message. In other words, the device sending the syslog message does not require any communication from the devices transporting or logging the message. This enables devices, which would otherwise be unable to communicate, to notify network administrators of problems. The syslog standard is documented in Request for Comments (RFC) 3164 and RFC 5424 of the IETF.

It should be noted that unlike the jet engine and medical machine examples (Sect. 9.2), which mainly employ mechanical or external sensors, IT services rely on embedded software to sense and collect data from the device. Other embedded measurements include IP SLA and Netflow as mentioned in Chap. 1.

The collected statistics are then consumed by various algorithms, utilizing the intellectual capital (IC) information[1] to calculate management and contract renewal-related measures as outlined in steps 3–6 above. IC is another critical input for IP-based smart services.

Figure 9.7 shows an overview of IoT IT services. A service becomes proactive by adding advanced software analytics algorithms to the collected data, and then delivering this results in an actionable way that provides critical value for the customers. IoT services provide a proactive, predictive, and preemptive service experience that is automated and intelligence-based to address the operations, health, performance, and security of the network. It securely automates the collection of device, network, and operations information from the network. The collected information is analyzed and correlated with the vendor’s vast repository of proprietary intellectual capital turning it into actionable intelligence to aid network planners/administrators increase IT value, simplify IT infrastructure, reduce cost, and streamline processes.

IoT IT services enable network vendors and technology service providers to provide solutions through machine-to-machine[2] interactions that automatically provide real-time visibility and issue resolution. Such intelligence enables people-to-people

[1] IC information is typically captured by analyzing collected data overtime against the supplier intelligence and data bases (e.g., Microsoft collects and analyzes data from its Windows customers over the Internet).

[2] The term “machine” refers to managed entity with an IP address such as router, switch, and router interface.

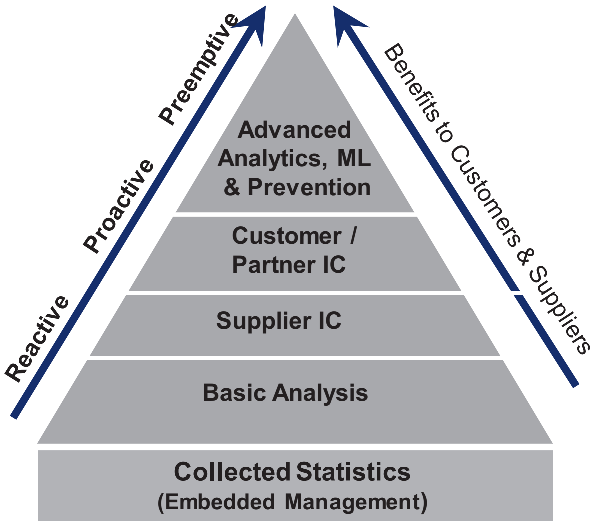

Fig. 9.7 Overview of IoT IT services

interactions and enhanced social media collaboration. The interactions enable vendors and service providers to continue growing their critical intellectual capital.

Another essential requirement for IoT IT services is the smart agent with automated two-way-always-on connectivity between the device (or the network) and service management backend systems that typically reside in the network operation center (NOC), at the network supplier, or at the managing partner. This connection is used to (a) send uninterrupted near-real-time device/network intelligence from the device/network to the service management system(s) and to (b) allow network management system(s) to connect to the device/network to take action to prevent service outage or service deterioration.

Thus, one of the key differences between traditional network management and IoT IT service is the fact that IoT IT services utilize uninterrupted, persistent machine-to-machine or machine-to-person diagnostics, fortified with intellectual capital and best practices, in a blend designed to give network administrators deep visibility into the network. Network management solutions themselves may be connected to backend services.

With IoT IT services, network administrators have direct view and intelligence at the device, network, operations, and application layer providing automated reports and recommendations. This end-to-end approach results in network intelligence that enables network vendors (typically responsible for network and service warranty), customers/clients (network owners), and partners (typically responsible for operating, monitoring, and maintaining the network by working with vendors and customers) to deliver proactive services including regular monitoring, proactive notification, and remote remediation to enhance the customers' network availability and performance.

9.4 Connected Ecosystems

As was mentioned in quite a few chapters in this book, the number of devices connected to the Internet is already in billions and expected to reach over 20 billion in just a few years. Each of these devices is in a position to create a set of new automated services that are essential to business as well as the advancement of the world economy. Today's businesses are already requiring manufacturers to supplement their products with intelligence and connectivity. With such capabilities, IoT layers and domains will be drivers for major software development as well as services support in devices, infrastructure, platforms, and applications. No single vendor will be able to handle a complete IoT vertical, let alone offering an end-to-end solution. IoT go to market will be driven by complex partnerships that includes a combination of original equipment manufacturers (OEM), value-added resellers (VAR), systems integrators (SI), and independent software vendors (ISV). IoT products, hardware, and software, as well as end-to-end solutions, will be developed in multidimensional partnerships, meaning that they're developed to integrate into IOT devices, networks, platforms, applications, and/or service. They will also be utilized to extend an IoT-enabled service portfolio.

On the device and network side, for instance, suppliers have been exploiting the device embedded intelligence and connectivity capabilities to offer IoT-based services changing the traditional maintenance and support from reactive to proactive approach. These services are typically offered as part of remote management of network equipment and assets, which provides proactive network monitoring, health checkups, diagnostics, and software repairs in addition to technical support.

Suppliers are also realizing that connected devices continue to generate information value not just for services but over their lifespans. They now know the current location of the device, when it was first installed, important specifications, diagnostics, availability of spares, replacement alternatives, repair instructions, support status, and so on. This information can then be used by manufacturers and their partners for sales and marketing efforts, product development, and new customer services.

Analysts believe that manufactures who have been exposed to the values driven by connected device have a superior advantage. Their businesses will be shaped by new, significant revenue opportunities emerging from the availability of the information provided by these newly connected devices.

In the reaming of this chapter, we'll describe the new IoT ecosystem-based business model, using IT use cases for illustration, and then describe the key gaps to allowing OEM,VAR, SI, and ISV to form partnership to develop end-to-end IoT solutions.

9.4.1 IoT Services Terminologies

As we just mentioned in Sect. 9.2, suppliers have been able to connect their devices (e.g., jet engines) to send information to their data centers for some time even before IoT is fully materialized. However, proprietary communication protocols and algorithms were often utilized. The proprietary algorithms where used by tools to sense, collect, store, analyze, and transport the data. Proprietary systems are rigid in nature, developed to support a single solution, and are prohibitory expensive to support and maintain (e.g., over satellites).

IoT promises to provide an open and efficient solution that can be utilized across multiple environments and technologies. The Internet Protocol itself has been shown to present a proficient and open approach to support “as a service” model as illustrated in Chap. 2.

Before we introduce IoT ecosystem solutions, however, we will define the key terminologies to be used in the rest of this chapter.

- Product, device, or machine refers to an “entity to be managed” such as IoT gateway, router, switch, card on the switch, platform, application, and network management system. Such entity is expected to have a unique identifier (i.e., IP address).
- Supplier (or vendor) refers to the company that manufactures, sells, and/or leases the device/machine. For example, Cisco is a supplier of networking devices, Rolls-Royce or GE is a supplier of jet engines, and Caterpillar is a supplier of heavy machinery.
- Enterprise (or network owner) refers to a business/company that has purchased services and purchased or leased the required devices/products that are required to run the services. For example, AT&T is a customer of Cisco and Owner of AT&T network. An end subscriber to AT&T services is a customer of AT&T and an owner of a device managed by AT&T.
- Partner refers to the third-party company that partners with a vendor to service a customer network. The partner may be an OEM, VAR, SI, ISV, or business partner on the service level, for example, IBM is a partner of Cisco that may be hired by AT&T to manage/service AT&T network.

9.4.2 IoT Connected Ecosystems Models

In this section, we will describe multiple flavors of ecosystem models that have resulted from the IOT models with connectivity and device intelligence. But first, we will describe the traditional model. Historically, vendors have sold their products to an enterprise. The enterprise fully manages the products on their own, as shown in Fig. 9.8, or the enterprise outsources the management of such products to a single or multiple partners, as shown in Fig. 9.9.

In IoT, the support paradigm is expected to be a combination of the above two models. We will refer to this model as a full ecosystem model which has been empowered by virtualization and cloud computing. Figure 9.10 shows a flavor of such model with customer-partner-supplier relationships. In this model, network vendors and/or their partners are often contracted by the network owners to manage the network as well as the services that are offered on the networks.

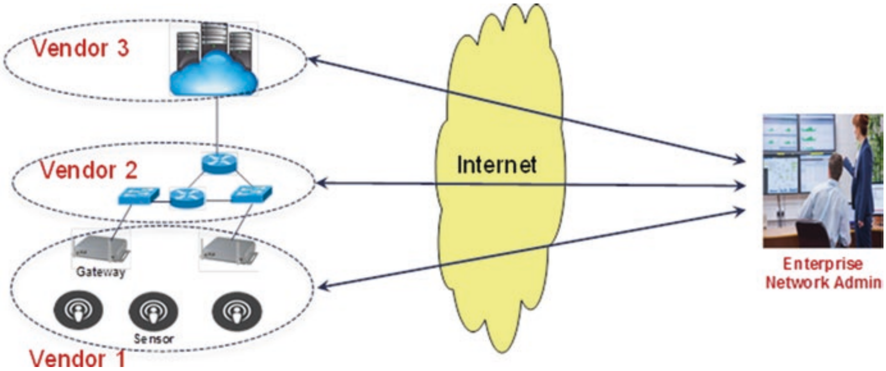

Fig. 9.8 Traditional support model: Limited to vendors and enterprises

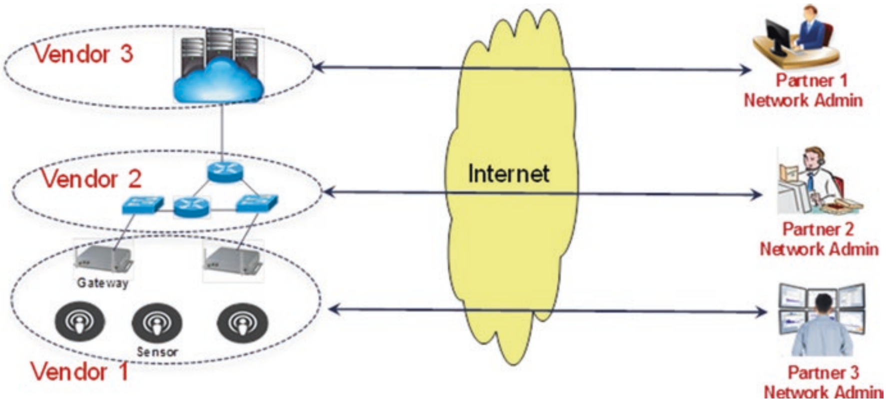

Fig. 9.9 Traditional support model: Limited to vendors and partners

The depth of such contracts varies between companies and typically depends on the structure, resources, and expertise of the client. It can range from a limited device warranty service where vendors are responsible for the health of their devices by providing TAC (technical assistance center) support and RMA (return material authorization) to full managed service where the network vendor and/or its partner is responsible for the comprehensive management functions as well as the end-to-end services offered by the network owner to end customers. In this case, the enterprise may own some aspect of the service management (e.g., in charge of monitoring and fixing level 0 and level 1 problems). The partner owns more complex aspects of service management (e.g., level 2), and the vendor is responsible for levels 3 and 4 which may include fixing defects by subject matter experts as well as RMAs and firmware update support.

It should be noted that:

- Level 0 typically means self-support by searching support documentations such as FAQs and information from the Internet. It allows users to access and resolve

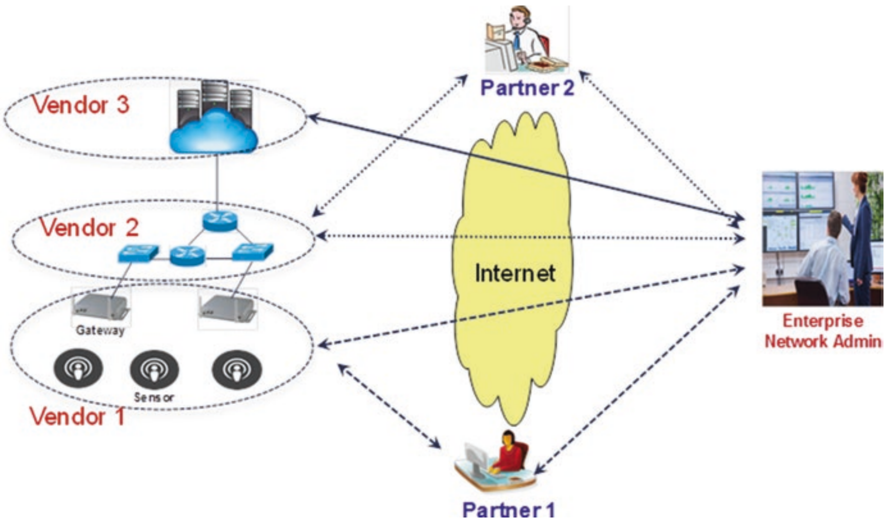

Fig. 9.10 Full ecosystem model with customer-partner-supplier relationships

issues on their own without contacting a local helpdesk or service desk for resolution.

- Level 1 is the initial support level responsible for basic customer issues.
- Level 2 is a more in-depth technical support level than level 1 with more experienced technicians with knowledgeable on a particular product or service.
- Level 3 is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced problems.
- Level 4: While not universally used, a fourth level often represents an escalation point beyond the organization, for example, the research and development organization that have developed the code and algorithms.

Other flavors of the full ecosystem model include multiple partners and even vendors for the same IoT layer (e.g., sensors from multiple vendors). In this case, data integrity is very essential to prevent partner 1, for example, from accessing data managed by partner 2 especially when partners 1 and 2 are competitors.

In all of these three cases (Figs. 9.8, 9.9, and 9.10), the value of an IT product has been limited to the product itself and a traditional maintenance and support contract. With IoT, these support and "break-fix" contracts provide a valuable augmentation to the product for customers and have a potential to grow to a considerable scale.

9.4.3 IoT Connected Ecosystems Models Key Capabilities

The IoT ecosystem model cannot work properly without addressing data privacy, standardization, and security.

Data privacy is vital to prevent data from being exposed to hackers and competitors. Data privacy is very delegate in IoT connected ecosystem model: data must be shared but only with the appropriate vendors and/or partners to speed up the discovery of any potential issue. With multiple partners managing, the three-way ecosystem model that includes vendor-partner-enterprise (Fig. 9.9) required a full-proof secure system that guarantees sensitive data does not fall into the wrong hands.

Security is important for every player including the enterprises, vendors, partners, and of course the end customers. Ecosystem players are not willing to risk investments unless standard technologies and methodologies are first established.

Standardization is essential to deliver scalable and flexible solutions to the market at reasonable price. It makes it possible for individual stakeholders to partner and work with IoT hardware (e.g., sensors, getaways) and software (e.g., IoT platform and applications) vendors, application developers, solution integrators, data content owners, and connectivity providers.

Outsourcing the management and operation of the network is gaining significant attractiveness in recent years. It benefits the enterprises in so many ways. Examples of such benefits include:

A. Allowing enterprises to concentrate on their own business and leave IT-related functions to the experts. This is especially important for small or medium business (e.g., small banks, retailers) with limited IT resources.
B. Allowing network owners to introduce and deploy new technologies quickly. Network owners do not need to hire or train subject matter experts every time a new service/technology is introduced.
C. Allowing enterprises to take more intelligent risks (e.g., trying multiple technologies at the same time) by taking advantage of cloud computing to lease required infrastructures only for the duration of service.
D. Allowing network vendors and partners to manage the full lifecycle of the products and use the collected information to develop smarter products customized for the customer. For example, a farming equipment company may offer embedding soil analysis system that analyzes farm soil in real time and determines the best type and amount of fertilizer, in addition to the business of selling faming traditional equipment.
E. Allowing network vendors and partners to compare the network health and KPI (key performance indicators) with other networks of the same type and provide reports to the customers to repair and/or improve the network and service performance.

Key capabilities to enable connected ecosystem models include:

A. Ability to acquire essential data from managed devices or products in timely fashion. Depending on the specific IoT vertical, such capability requires agreements on the data to be collected, APIs and embedded storage via smart agents, for instance. Smart agent may be defined as capability that resides on the device or product to collect the required data on regular basis or on demand. It should also have the ability to notify northbound applications based on programmed conditions (e.g., notify northbound application when the temperature change is more than 1 degree).

B. Ability for supplier or partner to analyze the data in timely fashion with a service platform as we mentioned in Chap. 7.
C. Ability for suppliers or partners to correlate collected data against intellectual capital (IC) and business intelligence rules and other databases to produce actionable results.
D. Two-way connectivity: Connectivity allowing devices and products to send data securely to the supplier and/or partner service platform systems. It also allows the service platform system to access the device or product secularly to take action when required.
E. Secure entitlement and data transfer capability to register and entitle customer networks and communicate securely (via encryption and security keys) with service providers or network vendors as we mentioned in detail in Chap. 8.

With the above capabilities, services will be transitioned from being reactive to being proactive and predictive.

9.5 Summary

This chapter introduced key IoT verticals that included agriculture and farming, energy, oil and gas, enterprise, finance, healthcare, industrial, retail, and transportations.

Some standard bodies have used the term “energy” to include energy consumption in smart cities as well as “oil and gas” in the petroleum industry. We believe “IoT energy” and “IoT oil and gas” should be treated as two separate verticals. This is due to the fact that energy is produced from many other sources (e.g., winds, solar) with focus on energy consumption. However, oil and gas focuses more on process and asset management for the petroleum industry.

The chapter then presented a new IoT business model, driven by the availability of new information, and offering key business benefits to the companies that manufacture, support, and service those systems, products, or devices.

Next the chapter presented the top requirements to deliver “anything as a service” that include ability to determine: which data is needed? How to capture the data? What type of local analysis is needed? How to transmit the data? Hoe to entitle, validate, parse, and analyze the collected data once it is received by the backend system? Which service-based performance? Which QoS and GoS thresholds? What type of real-time and none-real-time actions should be taken in the impacted device and/or the network and which algorithms? Which secure protocol should be used access the device/network from the backend system and take action? And which trending algorithms should be used to predict future measures?

Multiple IoT verticals in combination with the new ecosystem business model were also introduced. The chapter clearly showed that no single vendor would be able to address all business requirements. Finally the chapter listed the key benefits of the proposed IoT ecosystem partner and the capabilities to enable connected ecosystem models to function properly.

Problems and Exercises

1. What are the top ten IoT verticals as defined by oneM2M and ETSI standard bodies?
2. This chapter stated that the real impact of IoT will only occur when data from the silos is combined to create completely new types of applications. What does this mean? Why is it important?
3. What are the top two challenges to the farming industry? Why does IoT address these challenges?
4. Some companies identified the six-pillar for IoT to include connectivity, fog computing, security, data analytics, management and automation, and application engagement platform. What is meant by each area? Why each of these areas is essential?
5. Complete the following tables.

IoT solution	Definition	IoT vertical
Smart and connected parking		
Structural health		
Noise urban maps		
Smartphone detection		
Electromagnetic field levels detection		
Traffic congestion		
Smart lighting		

6. Three main use cases were listed for IoT agriculture and farming. List another use case.
7. What is the definition of a connected home? Provide an example.
8. Devices in connected homes can send information to service providers or directly to homeowners. List example for each case.
9. In the farming as a service (FaaS), agriculture machinery companies are utilizing drones when the cellular coverage is not available.
   (a) Beside drones, what other technology may be used?
   (b) How does drone technology work?
   (c) Compare pros and cons of drones vs. the other technology in part (a).
10. Describe how IoT is used to monitor and optimize solar energy plants?

11. Experts believe that the lack of IoT standards and communication protocols is putting development in risk especially in healthcare and financial. Why is that?
12. Define the top requirements and framework to introduce "heat as a service" under smart building?
13. In IoT retails use cases, retails use customer smartphones to generate heat maps that show how consumers move around stores. Why would a customer download retailer apps? What can the retailer do if customers are not willing to download the app?
14. In a table format, compare the transport, end device, and place of analytics for thrust as a service, imaging as a service, farming as a service, and IT as a service.
15. It was mentioned in Sect. 9.3 that the IT infrastructure for business is growing and becoming a moving target with complexity. How is the infrastructure becoming more complex? Provide examples.
16. Describe the operational model of IT as a service (ITaaS)? Which organization is delivering the service? Which organization is receiving the service? How is the service delivered?
17. With the availability of IoT data combined with cost-effective Internet-based communications, many companies starting to contemplate why they would they stop at selling a product and forgo very essential feedback information, when they can also sell a service with the right to monitor the actual usage and behavior of the product in the deployed environment. Usage information are not only used to service a product/device and prevent service deterioration by verifying contract level service-level agreements but also to learn about the product in the field and determine the most essential set of future enhancements. Provide an example.
18. With IoT, who do service providers determine which features, of a particular product, are used the most?
19. What is IoT-based IT service? What are to tow top requirements for IoT-based IT and why are they needed?
20. What are the key differences between traditional network management and IoT IT service?
21. (1) Why businesses are requiring manufacturers to supplement their products with intelligence and connectivity? (b) Why is it difficult for single vendor to provide a complete IoT solution? (c) List three typical partnerships that vendors needs to establish to provide complete IoT solutions.
22. Some IoT standard bodies have combined "IoT energy" and "IoT oil and gas" into one vertical called "energy." However, the authors have decided to keep "IoT energy" and "IoT oil and gas" as two separate verticals. What was their arguments based upon?
23. What is the 80–20 business rule? Which IoT businesses does it apply to?
24. Why many suppliers are utilizing IoT connectivity to generate information value not just for services but over their lifespans? Provide examples of such information.

25. What level 0–4 support in technical services? Is there a level 0? If so, what is it?
26. What is IoT full ecosystem model? Which major technology has made make such model feasible?
27. What are the top three requirements that are required for the IoT connected ecosystems model to work? Provide a brief summary of each requirement?
28. Why outsourcing the management and operation of an IoT network is gaining significant attractiveness in recent years?
29. What are the top five capabilities to enable connected ecosystem model for IT-based service?

References

1. OneM2M White Paper, The Interoperability enabler for the entire M2M and IoT Ecosystem, Jan 2015, Online: http://www.onem2m.org/images/files/oneM2M-whitepaper-January-2015.pdf
2. OneM2M Technical Report: OneM2M-TR-0001-UseCase, Sept 23, 2013
3. TM Forum Vertical Markets and connected Ecosystems, Online: https://www.tmforum.org/vertical-markets-connected-ecosystems/
4. Internet of Things World Forum Cisco Day 1 Presentation, Oct 14, 2014, Online: http://www.slideshare.net/BessieWang/iot-world-forum-press-conference-10142014
5. A. Slaughter, G. Bean, A. Mittal, *Connected Barrels: Transforming Oil and Gas Strategies with the Internet of Things*, Deloitte University Press, August 12, 2015. Online: http://dupress.com/articles/internet-of-things-iot-in-oil-and-gas-industry/
6. SAP, The CEO Perspective: Internet of Things for Oil and Gas Top Priorities to Build a Successful Strategy, 2014, Online: https://www.sap.com/bin/sapcom/en_us/downloadasset.2014-10-oct-30-20.the-ceo-perspective-internet-of-things-for-oil-and-gas-pdf.html
7. 5Liblium, 50 Sensor Applications for a Smarter World, Online: http://www.libelium.com/top_50_iot_sensor_applications_ranking/
8. Rolls-Royce Total care: Meeting the needs of Key Customers, Executive Briefing #6, March 2013, Online: http://www.som.cranfield.ac.uk/som/dinamic-content/media/Executive%20Briefing%206%20-%20RR%20Totalcare%20-%20Mtg%20the%20Needs%20of%20Key%20Customers%20%20-%208%20Mar%2010%20v9.pdf
9. Driven by Increased Demands on Healthcare Suppliers, Connected Medical Imaging Equipment to Grow at a 17% CAGR, ABI Research, Mach 20, 2015, Online: https://www.abiresearch.com/press/driven-by-increased-demands-on-healthcare-supplier/
10. IoT Services for Medical Imaging Equipment Market: MRI, X-ray, CT Scanners, and Tomography, ABI Research, Online: https://www.abiresearch.com/market-research/product/1021023-iot-services-for-medical-imaging-equipment/
11. Federal energy Regulatory Commission Assessment of Demand Response and Advanced Meeting Staff Report, December 2008, Online: http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf
12. J. Eckenrode, The Internet of Things and financial services: Too much—or not enough—of a good thing? Deloitte Quick Look Blog, Oct 7, 2015, online: https://quicklookblog.com/2015/10/07/the-internet-of-things-and-financial-services-too-much-or-not-enough-of-a-good-thing/
13. Technology Target, A guide to healthcare IoT possibilities and obstacles, Online: http://searchhealthit.techtarget.com/essentialguide/A-guide-to-healthcare-IoT-possibilities-and-obstacles

14. The IoT, in *What the IoT Means for the Public Sector*, Hitachi Data Systems, Online: http://www.isaca.org/Groups/Professional-English/cybersecurity/GroupDocuments/IoT%20in%20the%20Public%20Sector.pdf
15. A. Rayes, Book Chapter: IP-Based Smart Services, Network Embedded Management and Applications, Springer, 2012, http://www.springer.com/engineering/signals/book/978-1-4419-6768-8
16. C. Chen, L. Yuan, A. Greenberg, C. Chuah‡, P. Mohapatra , Routing-as-a-service (RaaS): a framework for tenant-directed route control in data center. IEEE/ACM Trans. Networking, **22**(5), 1401 (2014)
17. K. Lakshminarayanan, I. Stoica, S. Shenker, J. Rexford, Routing as a service, Online: http://www.icsi.berkeley.edu/pubs/networking/routingservice04.pdf
18. Real-World IoT Case Studies, Best Practice and IoT Methodology, entrsise-iot.org, Online: http://enterprise-iot.org/
19. Internet of Things: http://www.mckinseyquarterly.com/The_Internet_of_Things_2538
20. The Internet of Things: How the Next Evolution of the Internet Is Changing, Cisco IBSG white Paper, Dave Evans, Apr 2011
21. P. Marshall, The 80/20 rule of time management: stop wasting your time, Online: https://www.entrepreneur.com/article/229813
22. GE Services: http://www.geaviation.com/services/index.html
23. Boeing commercial Aviation Services: http://www.boeing.com/commercial/aviationservices/index.html
24. Boeing Gold Care Solution: http://www.boeing.com/commercial/goldcare/index.html
25. Caterpillar Services: http://www.cat.com/parts-and-service
26. John Deere Services and John Deere Farm Sight: http://www.deere.com/wps/dcom/en_US/services_and_support/services_support.page, http://www.deere.com/en_US/CCE_promo/farmsight/index.html
27. Go Green Intuitive, June 2016, Online: https://gogreeninitiative.org/wp/
28. J.F. Kurose, K.W. Ross, *Computer Networking: A Top-down Approach*, 5th edn. (Addison Wesley, Boston)
29. G. Allmendinger, R. Lombreglia, Four Strategies for the Age of Smart Service*:* http://hbr.org/product/four-strategies-for-the-age-of-smart-services/an/R0510J-PDF-ENG
30. J. Case, et al., Simple Network Management Protocol (SNMP), RFC 1157 (1990)
31. R. Presuhn, et al., Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), ed: STD 62, RFC 3418 (2002)
32. L. Steinberg, *Troubleshooting with SNMP and Analyzing MIBS*, ed (McGraw-Hill Companies, 2000)
33. Alfa Images Online: http://alfa-img.com/show/farm-planters.html
34. The Internet of Everything – Vision and Strategy, Cisco Systems, Mar 2013, Online: http://www.slideshare.net/Cisco/2-internet-of-everything-vision-and-strategy-rob-lloyd-final
35. Integrated Framing Systems, Online: http://www.monsanto.com/investors/documents/whistle%20stop%20tour%20vi%20-%20aug%202012/wst-ifs_posters.pdf
36. How the Internet of Things is Reinventing Retail, Position Paper by ComQi, July 2015, Online: http://www.comqi.com/internet-things-reinventing-retail/
37. Infosys Study, Rethinking Retail Insights from consumers and Retail into an Omi-Channel Shopping Experience, 2014, Online: https://www.infosys.com/newsroom/press-releases/Documents/genome-research-report.pdf
38. How the Internet of Things Is Improving Transportation and Logistics, Supply Chain 247, Sept 9, 2015, Online: http://www.supplychain247.com/article/how_the_internet_of_things_is_improving_transportation_and_logistics/zebra_technologies