IoT Fundamentals: Definitions, Architectures, Challenges, and Promises

Chapter · January 2020

DOI: 10.1007/978-3-030-30367-9_1

5 authors, including:

Farshad Firouzi
Duke University
51 PUBLICATIONS **917** CITATIONS
SEE PROFILE

Markus Weinberger
Hochschule Aalen
23 PUBLICATIONS **392** CITATIONS
SEE PROFILE

Fereidoon Shams Aliee
Shahid Beheshti University
123 PUBLICATIONS **665** CITATIONS
SEE PROFILE

Chapter 1
IoT Fundamentals: Definitions, Architectures, Challenges, and Promises

Farshad Firouzi, Bahar Farahani, Markus Weinberger, Gabriel DePace, and Fereidoon Shams Aliee

All compromise is based on give and take, but there can be no give and take on fundamentals. Any compromise on mere fundamentals is a surrender. For it is all give and no take.

Mahatma Gandhi

Contents

F. Firouzi (✉)
Department of ECE, Duke University, Durham, NC, USA

B. Farahani · F. S. Aliee
Shahid Beheshti University, Tehran, Iran

M. Weinberger
Aalen University, Aalen, Germany

G. DePace
University of Rhode Island, Kingston, RI, USA

F. Firouzi et al. (eds.), *Intelligent Internet of Things*,
https://doi.org/10.1007/978-3-030-30367-9_1

1.1 What Is IoT

By now, everyone has heard of the Internet of Things (IoT). Internet of Things has been defined as the next logical stage of the Internet and its extension into the physical world. It is the broad connection of devices that can interact with each other and share data to a larger network, where the shared data can be leveraged to extract value. All devices must have unique identifiers and use embedded technologies to sense and gather data about themselves and their environment and transfer that data to other devices or other hosts. Then these data must be correlated and analyzed to inform more intelligent decisions. The technical challenges are appealing in themselves, but from an industrial and business perspective, IoT presents a grand opportunity to leverage previously unknown information and insight to transform and create industrial processes and business models. This reality is a much greater opportunity than a simple connection. Several companies have defined the Internet of Things in their own terms, and it is instructive to examine these terms to see the similarities and differences.

- IBM defines the Internet of Things as "the concept of connecting any device (physical object) to the Internet and to other connected devices" [1]. IBM also writes that IoT refers to "the growing range of Internet-connected devices that capture or generate an enormous amount of information every day" [1].
- SAP defines the Internet of Things as "the vast network of devices connected to the Internet, including smartphones, and tablets and almost anything with a sensor on it – cars, machines in production plants, jet engines, oil drills, wearable devices, and more. These things collect and exchange data" [2].
- Gartner says "IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" [3].

- The Bosch corporation defines the Internet of Things as file sharing, e-commerce, social media, and the glue that connects things and devices. The devices can range from sensors and security cameras to vehicles and production machines. The connection of devices results in data that opens up new insights, business models, and revenue streams. The insights can lead to new services complementing conventional product business [4].
- Oxford Dictionary summarizes IoT as "a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data."
- Finally, IDC defines the Internet of Things as "a network of networks of uniquely identifiable endpoints that communicate without human interaction using IP connectivity (local or globally)" [5].

As you noticed, due to rapid emergence and convergence of technologies, the definition of IoT is evolving, and thus there are several definitions of IoT from different points of view. However, all of them have the following fundamental characteristics:

- *Things or Devices* – Things in IoT (also known as intelligent objects, smart objects, IoT devices, or IoT endpoints) are connected objects that can sense, actuate, and interact with other objects, systems, or people. In order to be a device on the Internet of Things, the device must have a processing unit, power source, sensor/actuator, network connection, and a tag/address so that it can be uniquely identified.
- *Connectivity* – Connectivity empowers the Internet of Things by enabling IoT things to be connected to the Internet or other networks. This implies that there must be a connectivity module in each IoT device as well as an appropriate communication protocol that the network and the device can both understand.
- *Data* – There is no IoT without ("big") data collected from IoT things and indeed "data is the new oil." Data is the first step toward action and intelligence. Sent information from IoT devices most often include environmental data, diagnostic, location data, or report on their status. The data also flows back to the device, for example, a command to tell it to sleep, or decrease power consumption.
- *Intelligence* – Intelligence is the key to unlock IoT potentials because of its ability to extract insights from IoT data. For example, the combination of artificial intelligence (AI), machine learning, data analytics, and IoT data can avoid unplanned downtime (i.e., predictive maintenance), increase operational efficiency, enable new and improved products and services, and enhance risk management [6].
- *Action* – Actions are the consequence of intelligence. It refers to the automated actions to be taken by the device or on the device, but also includes action from the stakeholders in the IoT ecosystem.
- *Ecosystem* – IoT has to be seen and analyzed through an ecosystem perspective. IoT things themselves, the protocols they use, the platforms on which they run, the communities interested in the data, as well as the goals and aims of interested parties all form the ecosystem.

- *Heterogeneity* – The Internet of Things is expected to be made up of heterogeneous devices, working on different platforms on different networks. Therefore, all the components should be interoperable, i.e., they must be able to connect, exchange, and present data in a coordinated manner based on a common reference model.
- *Dynamic Changes* – The state of devices, the contexts in which they operate, the number of connected devices, and the data they transmit and receive are all expected to change dynamically.
- *Enormous Scale* – The number of connected devices will be at least an order of magnitude more than current connections. This means there will be a commensurate increase in the amount of data generated by the devices, which in turn must be transferred and analyzed to be leveraged.
- *Security and Privacy* – Security and privacy are an intrinsic part of IoT. These issues are critical as personal data will be available online (e.g., in a healthcare system, IoT devices could be charting and sharing heart rate, blood glucose levels, sleep patterns, and personal well-being). This demands data sovereignty, secure networks, secure endpoints, and a scalable data security plan to keep all of this information safe.

The Internet of Things exists in an ecosystem, all the components and the environment that supports IoT and its aims. In an IoT ecosystem, there are four major components: *things*, *data*, *people*, and *process*. Let us examine each in turn (see Fig. 1.1) [7]. Of course, all four components, things, data, people, and process, must work in concert in order to achieve the promises of a more connected world.

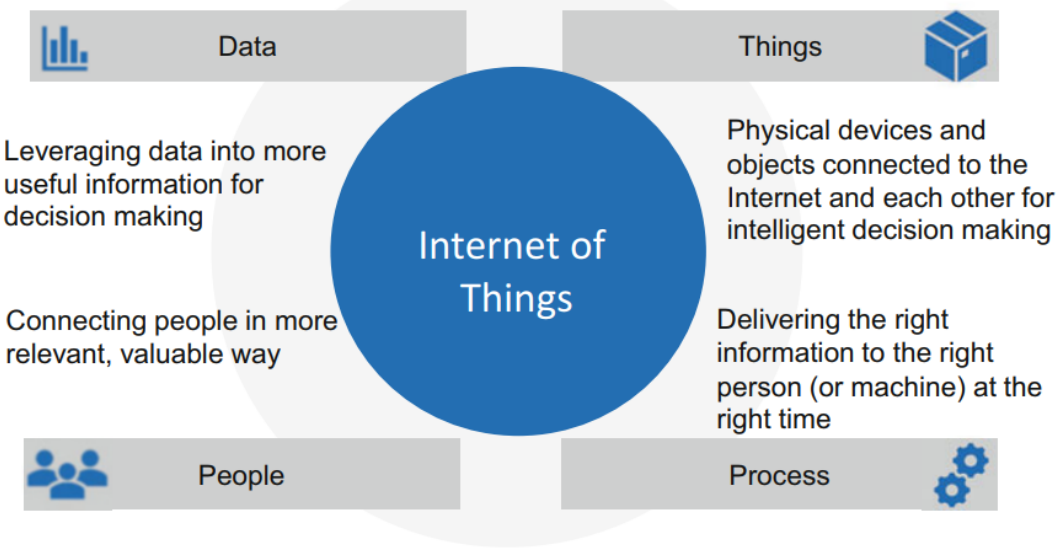

Fig. 1.1 IoT: The networked connection of people, things, data, and process

- *Things* – Things refers to the physical devices that operate as part of the Internet of Things. Each device must have the ability to connect to other devices or the network in general. This could be with a specialized communication protocol such as Zigbee or Bluetooth or the more general Internet Protocols (IP). The device needs the energy and processing power to handle that communication. Also, to be an IoT device, there must be some data to communicate. Most frequently, this is sensor data that is collected by the device itself. Some examples include image data from a security camera, temperature data from a thermometer, humidity or pressure data from a sensor on an industrial manufacturing machine, and so on. The thing or device may also be commanded to perform some action, perhaps sending specific data or moving an actuator or some other control motor. The device must be able to acknowledge these commands, perform these actions, and confirm with the remote controller that the desired action is performed. Routers, switches, and gateways are considered as part of the network but may also be classified as things. Devices must be equipped to survive the environmental conditions in which they are installed and have the necessary power, sensors, and communications to fulfill these roles.
- *Data* – The data component has been partially defined already, as those sensor data being sent from things as well as any commands being issued to the things. With the huge number of things producing data so often, it is easy to understand that the size of the data itself will be enormous. The raw data must be cleaned, that is, checked for errors and formatted, and then either stored for analysis or analyzed immediately. This task can be done at the edge of the network, close to the devices, or the data can be communicated to a more central collection point (e.g., cloud) where it is analyzed. The cost, relevance of the time of data to required actions, and communication barriers are some factors that determine the configuration of data processing. That being said, big data, collected from several IoT things, is most often stored and processed in the cloud.
- *People* – People are affected by the Internet of Things in at least two ways: as the agent of change who must work to make IoT function and as the beneficiary of its outcomes. Typically, people work in their own domain as a specialist at their job. With IoT, however, there is a much broader sense of interconnection between functions, and so people are increasingly finding themselves interacting with people in other business sectors. Sometimes this is a counterpart more or less with a similar function, or at a similar level, what we call horizontally located in the business, but other times it is a more vertical relationship, someone that operates at a lower or higher level. People must be interfacing in order to make sense of the data being collected and to determine the proper interpretation of the outcomes of the analysis of that data. Ultimately, it is people who create and maintain the Internet of Things, and their actions which can derive the most advantage from what IoT has to offer. The other side is the impact that the consumer sees from the IoT, meaning more informed decisions and targeted services from companies. People must also be aware of their personal data, who is collecting it and what is happening to it. Who owns this data? This is a question that has a complex and evolving answer.

- *Process* – The final component of the IoT ecosystem is process and that is where the benefits of intelligent automation, informed decision-making and control, and efficient procedures are realized. All of the methods, techniques, and processes currently used in vertical industries (e.g., manufacturing, logistics) can be made more efficient with the right information at the right time. Analyzing the data gathered from sensors and delivering this information to the appropriate stakeholders is the main idea of the process of IoT.

1.1.1 Internet of Things Terms and Acronyms

In this section, we review some fundamentals terms and explain how they relate to the Internet of Things.

- *Machine to machine communication (M2M)*: M2M is network communication between devices using any channel. Originally, it was used in an industrial context, but has come to mean that communication used to transmit data to personal appliances. Internet of Things is also communications between devices, but is used to also refer to vertical software stacks that automate and manage communications between multiple devices, and therefore refers to communication on a larger scale. Table 1.1 highlights the key differences between IoT and M2M.
- *Cyber-physical systems (CPS)*: The National Institute of Standards and Technology (NIST) has the following definition for CPS: "*Cyber-Physical Systems comprise interacting digital, analog, physical and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.*" Many manufacturing processes rely on cyber-physical systems as part of manufacturing. A cyber-physical system can also be found beyond manufacturing, for example, in the Smart Grid or in Smart Cities [8].

Table 1.1 The key differences between IoT and M2M

IoT	M2M
Devices communicate using IP networks, varying communications protocols possible	Point to point communications – embedded in hardware at the customer site
Data delivery is relayed through a middle layer in the cloud	Many devices use these protocols, over cellular networks or wired networks
Active Internet connection required	Not necessarily an Internet connection
Integration options are more varied, but management is necessary	Limited integration options; devices must have communications standards

- *Internet of Everything*: Cisco invented this term to mean the "people, process, data and things to make networked connections more relevant and valuable, turning information into actions' that improve everything." This terminology was abandoned sometime in 2017.
- *Social Internet of Things (SIoT)*: SIoT refers to an IoT in which things are able to create a network of social relationships with one another independent of human intervention. Objects are able to begin constructing social relationships based on the object's profile, interests (i.e., applications deployed, services used), and activities (i.e., movements). These social relationships can also be organized around events causing their creation. For example, a co-work relationship can be created between objects that work together to generate a common IoT application, such as objects that cooperate with each other to provide telemedicine or emergency response. A parental relationship may exist between objects that have the same manufacturer, are of the same model, or were constructed within the same period because they are part of the same batch. Social relationships are created between objects that are in contact occasionally or continuously because the object owners are in contact, and a co-ownership relationship may be created between heterogeneous objects that are owned by the same user. Adoption of the SIoT model offers many advantages [9]:
  - The social network created by the SIoT objects can be shaped as needed to ensure network navigability, the effective discovery of objects or services, and scalability similar to human social networks.
  - Trustworthiness can be created to balance the level of interaction among objects that are friends.
  - Models created to study social networks can be utilized to address IoT issues related to large networks of interconnected objects.

1.1.2 Impact of IoT

The estimated future impact of the Internet of Things is staggering. At the time of writing, it has been estimated that there are about 14 billion devices connected to the Internet. According to a Gartner forecast, it will go up to 25 billion by 2021. Cisco predicts that by 2020, that number will increase to 50 billion things. The government of the United Kingdom speculates twice that number, upward of 100 billion things. With this increased amount of connectivity, the way we interact with everyday objects will fundamentally shift. More of our choices can be driven by data instead of guesswork or habit. In our businesses, data-driven decision-making will prove more efficient and profitable. In our industries, processes and systems will be better managed and monitored, making us safer. Our quality of life will increase as these optimizations save us time, money, and energy. New services can be innovated from the data-rich environment, further improving our well-being.

1.1.3 Benefits of IoT

An organization that embraces the Internet of Things can expect greater safety, comfort, and efficiency. Hazardous environments and workspaces can be more carefully measured and the dangers more readily managed. The increased information about working conditions allows for decisions to improve comfort and consequently productivity, for example, a more localized thermostat can show the differences in the temperatures in specific offices. Adjustments for only those occupied spaces in temperature or lighting can lead to controlled energy costs and greater efficiency. Monotonous tasks can be automated, reducing downtime and yielding faster, more accurate, and greater results. Leveraging benefits like these can make the workplace more rewarding, and that improves employee satisfaction and retention and ultimately improved profits and reduces the necessary investment incurred by employee turnaround.

Organizations can also benefit from more information with which to make business decisions. Using large trends in empirical data means that fewer assumptions need to be made. It becomes possible to be more responsive to emerging trends. From a manufacturing standpoint, there is increased visibility into system behaviors. This can lead to shortened testing cycles and a more optimized production process. Revenue can also be increased or new streams can be realized by improving current procedures or making new ones from the increase in available information. IoT is a unique strategic advantage that early adopters will have over competitors who choose not to pursue digitalization. A few more benefits of IoT can be listed as below:

- *Efficiency*: More information about work/operation processes and rich data sets obtained from connected sensors leads to process streamlining. IoT enables great data sharing, and then manipulating the data as needed helps systems to work more efficiently and make smarter, more informed decisions in real time.
- *Transparency*: IoT digitizes every process and enables physical objects to remain connected, providing greater transparency. For example, IoT sensors can identify the status of the products in a production line or the location of assets in a field and track inventory and parcels.
- *Automation and control*: IoT enables the connection and digital control of physical objects, requiring extensive automation and control within the network. Without requiring human involvement, machines communicate with one another, resulting in more time-efficient output. Automation also ensures uniform completion of tasks and the quality of services provided. Human intervention may only be required in the case of an emergency.
- *Accuracy*: Monotonous tasks are automated, reducing downtime and errors.
- *Monitoring*: IoT provides the advantage of monitoring capabilities. Tracking supply quantities for business or monitoring the air quality of a home is easily accomplished and provides extensive information otherwise not easily obtained.

For example, knowing that the printer is almost out of paper or that you are running low on coffee can enable a user to consolidate shopping and avoid extra trips to purchase supplies. In addition, monitoring product expiration dates provide increased safety.

- *Information*: Access to additional information enables improved decision-making in a diverse array of areas, from everyday decisions like choosing what to purchase at the market to determine if a business has enough inventory. In each situation more knowledge gives the user greater power.
- *Time*: The integration of IoT has the potential to save large amounts of time, which is valuable to everyone.
- *Safety and comfort*: It can be difficult to imagine managing and monitoring hazardous environments requiring the consideration of multiple factors including human safety and optimizing the environment for productivity and comfort. Mundane tasks can be automated resulting in energy savings. For example, smart assembly lines can operate without human intervention and report errors immediately, resulting in greater productivity and less downtime. Automating monotonous tasks would also enable employees to engage in more rewarding work, resulting in increased employee satisfaction/retention and wider profit margins.
- *Security*: Security sensors (e.g., camera) as well as location-based sensors (such as GPS) have a significant ability to enhance security.
- *Cost/money*: The greatest advantage of IoT is the amount of money saved. Fewer errors, higher employee retention, improved processes, and energy-efficient behavior all reduce costs. IoT will be more widely utilized as long as the cost of monitoring equipment is less than the potential cost savings. IoT integration is proving highly useful in daily life as appliances communicate with one another, conserving energy and reducing costs.
- *Industry-specific view:* IoT can revolutionize several industries, for instance:
  - *Targeted marketing*: Greater information leads to individualized experiences, improving the interactions of customers with the company and bringing the company message to those more likely to become customers.
  - *Supply chain enhancements*: Asset tracking and management, security, optimized logistics, and transport all reduce costs of lost inventory, waiting times, and inventory mismatches.
  - *Health*: Individuals can get more information about their own bodies (heart rate, hours of sleep, etc.) to help in maintenance or identifying health problems.
  - *Smart building*: Workplace temperature, lighting, and air quality feedback can ensure a pleasant working environment, increasing satisfaction and productivity. In terms of security, connected cameras can detect the presence of unauthorized individuals.

1.1.4 IoT Challenges

Certainly, any changes bring not only benefits but also challenges that must be overcome. For any organization it is essential to determine which departments are responsible for which changes that must be made. Who will purchase and configure the needed IoT hardware (devices, gateways, etc.)? Who will install and run the needed software and troubleshoot the hardware and software? Who is responsible for networking? Which department will perform the analytics and deliver the reports and findings? There are also issues of what to do with legacy devices and other specialized solutions that will need to be found and addressed. Any potential solution must also be able to scale, to handle current needs but also those of the immediate future as the organization continues to adapt and grow. Through it all, ownership is necessary to maintain an adequate level of production quality, especially as several teams are usually called upon to work together. These are major issues that demand sound leadership in order to meet the challenges of implementing IoT for any organization.

Other challenges are more technical in nature. First of all, scalability and heterogeneity are intrinsic parts of IoT, which should be addressed via appropriate technologies. In this context, the necessary technology standards must be developed or updated including the network protocols and data aggregation standards. As mentioned before, a new connection paradigm will be needed and possibly described by these new protocols. At every stage from gathering data, to transmitting it, to storing and analyzing it, interoperability must be considered. Cloud Services are nonstandardized and non-unified, meaning that changing providers could incur the undue expense. There is currently no consensus on machine to machine protocols, and existing equipment uses a variety of operating systems and firmware technology. The surest way to mitigate these differences is to move computing tasks to the edge of the cloud and take advantage of fog computing models and IoT hubs. This will leave the cloud servers and services to handle the analytical and processing tasks for which they are best suited. Business must be prepared to handle these challenges with adequate planning and a solid business model. The revenue and profits will provide the motivation to invest in IoT and expand into vertical markets, horizontal markets, and consumer markets. If done properly, a market bubble will be avoided as well as regulatory and legal battles.

The final, and perhaps the most important, hurdle will be solving the issues associated with security. There have already been successful hacks, or unauthorized access to several devices on the Internet of Things. Since IoT will become a larger part of our daily lives, it should be obvious that the security of our sensitive information is becoming vital. Losing control of the radio in a car, or the transmissions of a baby monitor, or the home security cameras in a dwelling make for a frightening and compromising future. Controlling access to these and many other devices is a growing concern and is already being addressed.

In summary, the main challenges of IoT can be listed as below:

- *Scale*: Connecting to billions of active connected IoT devices is a big challenge, and the current communication models and technologies should be adjusted to address scalability challenges. In this context, emerging IoT technologies such as decentralized IoT network (e.g., edge/fog computing), peer-to-peer communications, and blockchain can be helpful.
- *Heterogeneity*: IoT in its nature consists of a plethora of devices with different interfaces and communication protocols, and thus there is a necessity to form a common way to abstract the underlying heterogeneity.
- *Privacy*: All the collected data must be kept secure and anonymous when necessary.
- *Data ownership*: Who is the owner of machine-generated data (MGD)? The entity that owns the IoT device or the manufacturer of the device (e.g., in connected cars)?
- *Cybersecurity*: Defeating attackers who seek to control, steal, or mislead is vital.
- *Legal liability*: Who is responsible when something goes wrong with an algorithm or an automated decision?
- *Sensors*: Technically, sensors must be inexpensive, accurate, and energy efficient.
- *Networks*: Transferring data and commands must be secure, reliable (correct and timely), and robust, despite operating in a noisy, busy, dangerous, or harsh environment.
- *Big data*: Connected devices continuously and simultaneously generate large volume and different varieties/forms of data, and thus IoT should be able to address time, resources, and processing capabilities.
- *Analysis*: The data must be properly interpreted and analyzed with fidelity to its meaning, especially if automated actions are taken based on data outcomes.
- *Interoperability*: There is a fierce competition to lead this burgeoning field, and all players must work together to be functional and to protect investments and must do so with fairness and integrity.

1.1.5 IoT and Big Data

Data coming from the Internet of Things is unlike data from the past in at least two important dimensions. First, the large amounts of data being generated demand a new data management approach. Traditional methods need to be adapted or entirely new approaches need to be discovered to handle diverse data constantly streaming from many sources. The second dimension is the nonuniformity of the data. Often the raw data is unstructured, or may come in several different formats, or may even change depending on the context. The new data management techniques must cope with these challenges. Up until now the discussion has been about big data without formally defining it. Big data is a large set of structured, unstructured, and

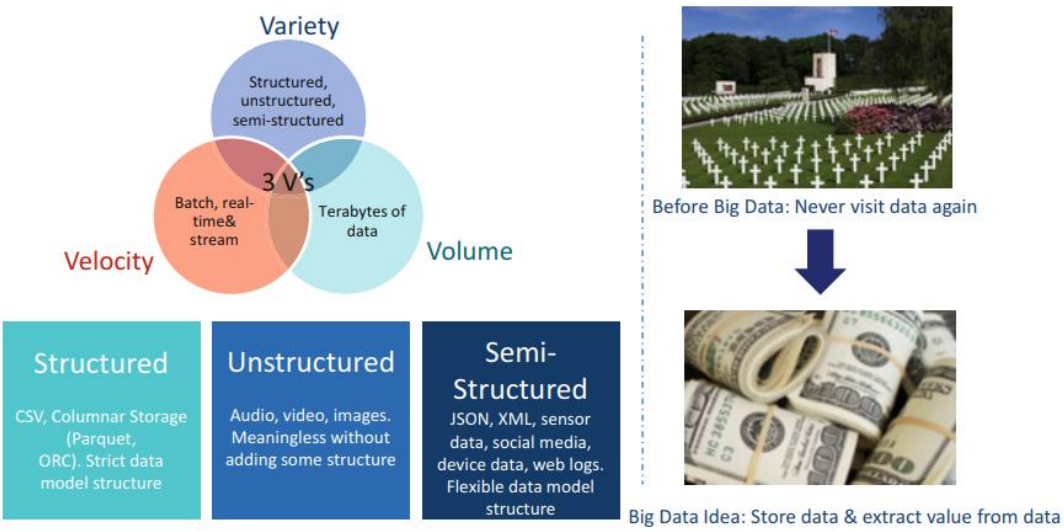

Fig. 1.2 The definition of big data

semi-structured data and the results of analyzing that data to gain insights. Doug Laney defined big data as the three V's (see Fig. 1.2):

- *Volume* – Storing large amounts of data.
- *Velocity* – The rate at which data is generated is high, so it must be stored or processed quickly.
- *Variety* – There are many possible formats of the data, from structured numeric to text, e-mails, video, audio, and so on.

Turning big data into tangible business insights is one of the major benefits of IoT. Most well-known approaches for dealing with IoT data include:

- *Analyzing data*: Before data becomes useful in making decisions, it must be analyzed. Traditional manual analytics, though powerful and informative, simply will not be practical in the face of the staggering amount of data that IoT will generate. Therefore, some automated analytics must be employed. These analytics need to provide descriptive reports of the environment, visualizations, dashboards, trigger alerts from data sources, and automated actions to be taken based on the data. They will also be used to detect patterns in the data, predict outcomes, and detect anomalies. There are open-source frameworks currently available for performing automated analytics. The two main approaches are to process the data in batches or to analyze the data as it is generated in real time. Which technique to use depends on the context of the problem as well as the resources available. The analytics can be run in a distributed fashion, also called in the cloud or at the edge, in servers nearer the sensors. First, the data is preprocessed, that is, duplicates are filtered out, and the data is possibly reordered, aggregated, and most likely normalized. These and other similar preprocessing tasks can be performed on the IoT device itself or on a gateway device before it is sent upstream. The most common automated analytics performed now are machine learning algorithms.

- *Machine learning (ML)*: Traditional mathematical statistical models analyze data by fitting the data to a model. Then the model is used to make predictions. This is a difficult process to follow especially when the data is dynamic or has many variables or the important points of the data are unknown. Machine learning is an algorithmic approach where the important parameters are extracted from the data in a process called learning. The data itself provides the structure of the mathematical model. Machine learning techniques can be applied to historical data or data taken in real time. The main way to think of it is that machine learning finds patterns or relationships or key variables in data. The model that is learned can be updated over time as more data is collected. One of the important applications of machine learning in the context of IoT is about finding patterns in the data, so that anomalies can be found quickly. Traditionally, anomalies were detected when certain values crossed thresholds. Machine learning allows for more complex patterns in the data to be identified as anomalous, therefore increasing speed and accuracy in detecting problems. The machine-learning-driven intelligence in IoT can be used for predictive analytics (what will happen), prescriptive analytics (what should we do next), and adaptive or continuous analytics (how can we adapt to the latest changes).
- *Edge analytics*: When analytics is applied at the edge of the network close to the IoT devices that generate the input data, it is referred to as edge analytics. Since network traffic is reduced, this is an attractive approach to reduce bandwidth and the latency from data gathering to a useful result. One drawback is that more processing power is needed in the devices and close to them, and cost or the particulars of the environment or device may make this prohibitive. On the other hand, sending large amounts of data across a network into the cloud may also be too expensive. Often a hybrid of edge and upstream analytics in the cloud is used to mitigate these costs.
- *Real-time analytics*: Any time that data is collected and immediately analyzed is known as real-time analytics. This is the best choice when a delay in the results of the analysis would reduce the value of the data. Time series data, rolling metrics, running averages, and any other occasion where the window of time analysis needs to be controlled are also good candidates for real-time analytics. Some real-time analytics frameworks available include Apache Storm, Apache Spark, and Flink frameworks.
- *Distributed analytics*: When the data sets are particularly large, too large to be handled by a single node (server), then distributed analytics can be used. As the name implies, the analysis tasks can be broken up and spread out to several compute nodes, possibly across multiple databases. If the data allows, it could be bucketed by time period and thereby effectively split up in order to make it more manageable. This is also an example of batch processing. Hadoop provides an ecosystem of frameworks for performing analytics. Apache Hadoop is used for batch processing and uses the MapReduce engine to process distributed data. Hadoop is a good open-source framework and one of the first to become available. It is used successfully for historical data analytics.

Data storage, besides the data processing, is another challenging issue in the era of big data. As more and more devices are connected to the Internet of Things, the amount of data they generate will drastically increase. They will be sending messages with their status, sensor outputs, metadata, and other messages. Despite the large amounts of data, it still must be stored. Two common methods are listed here, NoSQL databases and time series databases. Traditional techniques (SQL databases) are usually not feasible because of the amount of data being stored, with its varied and often unstructured nature. NoSQL databases offer high throughput and low latency of storage and retrieval. Since there is no schema, dynamic new data types are allowed. Couch Base, Apache Cassandra, Apache Couched, MongoDB, and Apache HBase (Hadoop) are examples of frameworks that use NoSQL. There is also a NoSQL in the cloud solution offered by IBM's Cloudant (a distributed database) and AWS' DynamoDB. A time series database can also be a NoSQL database or even a relational database. The indexing and queries are all based on timestamps in the data. Some frameworks using time series databases are InfluxDB, Prometheus, and Graphite.

1.1.6 IoT and Cloud Computing

The two worlds of IoT and Cloud experienced swift and independent progress. However, the complementary features of IoT and big data generated many new opportunities and advantages. Cloud computing is the solution to the increased demand for storage and processing. The cloud is defined as a group of servers and computers connected over the Internet in a large, distributed infrastructure. The concept is to deliver on-demand services over the Internet. The model is typically based on pay for the usage consumed (metered service), with the ability to scale up and down as needed (elastic resources). Amazon, Microsoft, and Google are dominating this *Infrastructure as a Service* (IaaS). They also provide *Platform as a Service* (PaaS) and *Software as a Service* (SaaS). The advantage to consumers is a lowered computation cost versus purchasing the hardware and then paying to operate and support it in-house. In summary, the main drivers for integration of IoT and Cloud are listed below [10]:

- *Device lifecycle management*: As the Internet of Things grows in size, the number of devices that need to be registered, managed, and updated while maintaining security requirements also grows and must be accommodated. It is possible for tools to configure and update firmware and software over the air (FOTA). The cloud platforms enable device lifecycle management, so devices can be connected, registered, on-boarded, updated remotely, and even remotely diagnosed should something need to be fixed. This reduces the operation and support cost of the devices. That means the enterprise Internet of Things is remotely managed, with minimal time and a reduced cost of ownership. In other words, a 360-degree view of the IoT devices is possible via the cloud.

- *Communication*: Cloud platform can be leveraged with the help of IoT to deliver scalable domain-independent services by providing appropriate service-oriented domain mediators.
- *Resource pooling*: Physical resources of IoT can be integrated into the cloud resource pool enabling us to allocate and share them on demand like regular Infrastructure as a Service (IaaS).
- *Storage*: IoT drives a real tsunami of big characterized by volume, variety, and velocity. In this context, IoT benefits from large-scale and long-lived storage of the cloud.
- *Computation*: Data processing is typically a very resource-hungry task. Therefore, IoT can benefit from virtually unlimited processing resource of cloud to aggregate data and execute batch and/or real-time analytics on the collected data.
- *Device shadowing or digital twin:* Another benefit available through cloud computing is device shadowing. The concept here is to have a backup of running applications and devices also running in the cloud. Any time there is a fault or failure in the original device or application; the twin can be examined to extract the result or to help in diagnosing the problem. System availability can be increased by using the digital twin as software redundancy. If the original system needs to be taken offline for maintenance, the twin can continue the operation uninterrupted; it can also provide system behavior statistics and behavior profiles for the original system at decreased risk.

1.1.7 IoT and Digitalization

Gartner defines "*digitalization*" as leveraging digital technologies to change business models and provide new revenue and value-producing opportunities. The process of updating a business to digital technologies is an evolutionary one and indeed has been happening for decades. The process is enabled by increased interoperability, information transparency across departments and industries, automated assistance and support, and a trend toward decentralized decision-making. In this context, IoT is considered as the major pillar for digitalization. The other important pillars are blockchain, big data, and machine learning.

1.1.8 IoT and Industry 4.0

The phrase "Industry 4.0" is rooted in a high-tech, German government research and development project in the manufacturing industry. It was initially coined at the Hannover Fair in 2011. Although there is some difference of opinion around the definition of historical industrial revolutions, Industry 4.0 is considered as the fourth industrial revolution. The initial industrial revolution occurred in the late 1800s and is responsible for mechanizing the power of steam and water. The second industrial

revolution began in the early 1900s and was characterized by the use of electricity to drive mass production through assembly lines and a reorganization of labor. The 1970s brought the third industrial revolution which utilized computers to automate production and processes. It is predicted that the coming fourth industrial revolution will fully utilize digital manufacturing in smart factories. Industry 4.0 is propelled by the merging of technologies such as:

- Industrial Internet of Things (IIoT) and extensive sensor use
- Analytics and big data
- Machine learning and artificial intelligence (AI)
- The convergence of IT/OT
- Augmented reality (AR)
- Advanced robotics
- Additive manufacturing

Benefits of Industry 4.0 Industry 4.0 will generate benefits in many areas. Product development will move more quickly due to analytics, and original equipment manufacturers (OEMs) will utilize analytics to understand better how consumers actually use products compared to a product's anticipated use. Sensor data will be used to optimize production through constant status updates that are compared to a digital twin (i.e., a perfectly efficient simulation which creates a virtual and digital replica of the target physical product/entity or process) to predict the physical counterpart's performance characteristics and guide corrective action and predictive maintenance needs. Additive manufacturing will become highly profitable based on highly flexible, small production capabilities. Augmented reality will drive learning and efficiency, and machines will assist humans with dangerous or complicated tasks as they gain autonomy. Many of these technological advancements are already occurring on a smaller scale. However, the guiding vision of Industry 4.0 is to revolutionize manufacturing and its connected industries. The main goal of the Industry 4.0 vision is to help manufacturing and its connected industries to evolve away from a logistics or end product focus. This revolution seeks to help these fields move toward an efficient customer-responsive business model that generates innovative revenue sources. Industry 4.0 also has the potential to revolutionize cities and utilities on a larger scale.

Industrial IoT The Industrial Internet of Things (IIoT) uses actuators and sensors to improve industrial and manufacturing processes. The IIoT is vital in many industries such as oil and gas, logistics, manufacturing, energy/utilities, transportation, resource mining, and aviation as well as other industrial fields or use cases common to these industries. However, there are some companies and professional researchers who consider Industry 4.0 and IIoT to be equivalent.

1.2 Architectures and Reference Models of IoT: A Layard View

1.2.1 IoTWF Reference Model of IoT

There are several standardizations in the IoT ecosystem. The IoT World Forum (IoTWF) is an exclusive annual industry event hosted by Cisco. As an outcome of their collaboration, they published a Standardized Architecture in 2014. The committee was comprised of Cisco, IBM, Rockwell Automation, and others. The proposed IoT Architecture is a seven-layer reference model, with control originating from the center (e.g., cloud) to the endpoint devices. Generally, data is gathered at the endpoint devices and is sent toward the center. The central processing can, in fact, be decentralized and implemented as a cloud service. The purpose of such a model is to give a common understanding of how the problem of creating IoT can be divided. With the different goals of each layer identified, and the interfaces specified, different companies can contribute pieces that will interoperate. Security can also be enforced at each layer of the model. These seven layers include (see Fig. 1.3) [11]:

1. *Physical devices and controllers (things)* – These are the physical devices, sensors, actuators, and controllers that form the Internet of Things. Their primary function is to collect data to transmit upstream, but they should also be capable of receiving commands, e.g., power down, etc.
2. *Connectivity (networking)* – This is the layer that serves as the medium to bring the sensor data from the devices to the upper layers where that data is cleaned and analyzed. The chief responsibility here is for reliable, secure, and timely delivery of data. This includes any switching or routing that is necessary as well as translation between protocols if necessary.

Fig. 1.3 IoT reference model by IoTWF

3. *Edge computing (data element analysis and transformation)* – This is also known as the fog layer because it is the layer where data cleaning, aggregation, and processing begin. It is the responsibility of this stage to prepare the data for analysis and storage. One of the methods to mitigate the enormous data flows is to start the analysis as early as possible. Data is evaluated, possibly reformatted or reordered, filtered, and checked for warning thresholds. Edge/fog computing facilitates data processing, data storage, and networking services between endpoint IoT devices and the center (e.g., cloud or data centers). The key idea of edge/fog is to process the data and make actions closer to where the data is created. This can ultimately result in reducing the traffic between IoT devices and real-time actions (i.e., respond fasters to events).
4. *Data accumulation (storage)* – This is the layer which prepares data to be stored in a database, whatever that format is. The key here is that after this layer, the data is expected to be able to be retrieved based on queries.
5. *Data abstraction (aggregation and access)* – Another layer that deals with the data. At this layer, the data is consistent, complete, and validated. In practice, data is often stored across multiple databases; the task of this layer is to ensure that the data is able to be queried and a unified, reliable result is returned.
6. *Application (reporting, analytics, control)* – This is where individual software applications can query the data to perform specific functions, such as reporting, monitoring, control of devices, visualizations, and analytics.
7. *Collaboration and processes (involves people and business processes)* – This is the layer that makes use of the outputs from the software applications of the previous layer. Data and conclusions from that data are shared with other entities or applications. The collaboration of several data sources illuminates new business practices, makes existing processes more efficient, and opens the doors to innovation. This is where the benefits of the Internet of Things are largely realized.

1.2.2 Simplified Reference Model of IoT

A simplified IoT architecture is comprised of the following layers (see Fig. 1.4) [12, 13]:

- *IoT Things Layer* – Consists of all IoT sensors and actuators.
- *IoT Network Layer* – Includes network components such as IoT gateways, switches, and routers responsible for transmitting data in a timely and dependable fashion. This layer also includes fog/edge nodes to perform data analysis and transformation and information processing as quickly and closely to the things as possible. This is very helpful in real-time applications such as IoT healthcare to be able to provide low-latency and faster responses to emergencies.

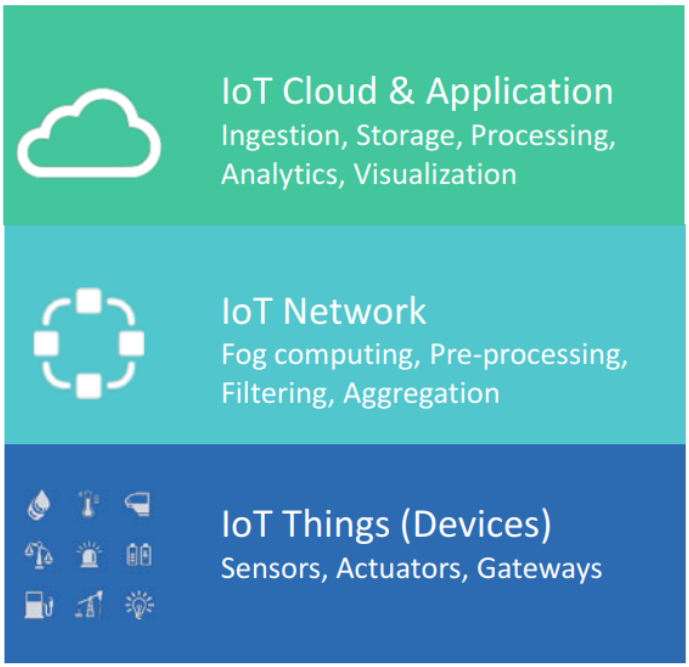

Fig. 1.4 Simplified IoT architecture

- *IoT Cloud and Application Layer* – Manages and processes IoT devices, as well as data created by the other two layers. It is also responsible for data ingestion, data interpretation through software applications, as well as integration with other platforms to improve business value.

1.3 IoT Frameworks and Platforms

1.3.1 FIWARE

FIWARE is funded by the European Union (EU) to be an open-source middleware platform. This means that it specifies interfaces for application programmer interfaces, allowing anyone to be able to connect devices to a catalog hosted in the cloud. The idea is to simplify the task of integrating devices into IoT and enable an economy based on data. Since it is a standard, it relies on participation and adoption, but the promise of interoperability is real and appealing. To that end there is an active and well-funded community surrounding the platform and encouraging participation [14].

1.3.2 SmartThings

SmartThings is a cloud-based platform offered by Samsung that focusses on building and running an IoT-driven smart home. The application management system is used to process subscriptions from device type handlers. Over 300 different

devices are supported in the system, to allow the user control over objects in the home. From dimmer switches to sensors and alarm systems, SmartThings offers integration of varied devices with third-party assistants such as those produced by Amazon or Google. The system can increase security and convenience in any home by providing a common connection and integration of devices found there.

1.3.3 AWS IoT

With Amazon Web Services (AWS) IoT, Amazon offers a managed, cloud-based solution. Platforms and software are all offered as a service, with the ability to scale and use its analytics tool on IoT data. Things can be registered as devices, and the architecture features a Message Broker, Thing Registry, Thing Shadows (Digital Twins), and Rules Engine in addition to Security and Identity components. AWS is aimed at home users as well as industrial users with its mix of device software, control, and data services. Amazon machine learning provides analytics and visualization tools as a service. Users can make use of the same technology used by Amazon data scientists internally, but with a friendlier wizard-style interface to begin. Getting started building and performing IoT tasks or data science functions are painless. The services scale as your needs or businesses grow, and stopping is just easy since no capital investment is required [15].

1.3.4 Microsoft Azure IoT

The Azure Internet of Things (IoT) is a collection of services that is capable of connecting, controlling, and tracking billions of IoT devices. Available services in Microsoft IoT include [16]:

- Azure Internet of Things (IoT) Hub
- Azure IoT Edge
- Azure Stream Analytics
- Azure Machine Learning
- Azure Logic Apps

1.3.4.1 Azure Internet of Things (IoT) Hub

The Azure IoT hub is a cloud-hosted service that functions as a centralized, bidirectional message hub for an IoT application and its connected devices. It can be used to build dependable and secure communications among millions of IoT devices and back-end solutions hosted by the cloud. Almost any device can be virtually connected to the IoT hub, which supports communication coming from the device to the cloud and vice versa. IoT hub is able to support different message

patterns used to manage devices including file uploads from devices, device-to-cloud telemetry, and request-reply methods. IoT hub monitoring is useful for supporting solution health because it monitors events including device connections, failures, and connections. The IoT hub provides a secure channel for devices to communicate and send data [16]:

- Individual device authentication allows each device to connect to the hub securely and to be controlled securely.
- The IoT hub provides total control over device access and can manage each per-device connections.
- When a device initially boots up, the *IoT Hub Device Provisioning Service* automatically provisions devices to the correct IoT hub.
- Various device capabilities are supported by multiple authentication types:
  - SAS Token-Based Authentication
  - Individual X.509 Certificate Authentication
  - The X.509 CA Authentication IOT hub connects devices using the following protocols: AMQP, AMQP over WebSocket, HTTPS, MQTT, MQTT over WebSocket

IoT hub also includes built-in message routing which provides the flexibility to create a rules-based, automated message fan-out. Additionally, the IoT hub can be combined with additional Azure services to create comprehensive solutions such as:

- *Azure Logic Applications* – Business process automation
- *Azure Machine Learning* – Adds AI models and machine learning to solutions
- *Azure Stream Analytics* – Provides real-time data analytics on data streaming from devices

There are two available Software Development Kit (SDK) categories used with the IoT hub:

- *IoT Hub Device SDKs* – Allow one to create IoT applications to be executed on IoT devices. These applications can send telemetry to the IoT hub and include the option to receive messages, method, job, or updates from the hub. Compatible languages include Python, Node.js, Java, C#, and C/C++.
- *IoT Hub Services SDKs* – Allow a developer to create back-end applications that manage the hub and schedule jobs, send messages, invoke other functions, or send updates to IoT modules or devices.

1.3.4.2 Azure IoT Edge

Edge enables an organization to focus on business insights rather than focusing on data management by transferring cloud analytics and some business logic from cloud to edge. Azure IoT Edge has three main components (see Fig. 1.5) [16]:

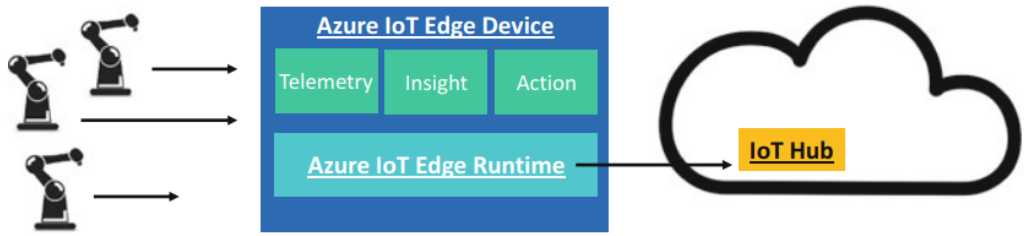

Fig. 1.5 The architecture of Azure IoT Edge

- *IoT Edge Modules* – These are the fundamental execution units that run the business logic of the system at the edge. These modules are implemented as Docker-compatible containers. There is a possibility to create more complex data processing pipeline by connecting several containers to each other. IoT Edge allows you to create custom modules or bundle different Azure services into modules able to extract insights from IoT data offline at the edge.
- *IoT Edge Runtime* – It is located in the edge and provides cloud and custom business logic for IoT Edge. In addition, it performs communication and management operations including:
  - Manages workload installation and updates
  - Manages Azure IoT Edge Security Standards
  - Ensures IoT Edge Modules are running
  - Monitors and reports module health remotely
  - Manages communication and handles communication between downstream endpoint IoT devices and IoT Edge, between modules, and between the cloud and IoT Edge devices
- *IoT Cloud Interface* – It sits in the cloud and allows remote management and monitoring of IoT Edge devices from the cloud.

1.3.4.3 Azure Stream Analytics

As an event-processing engine, Azure Stream Analytics enables you to monitor large-volume streaming data coming from IoT devices as well as data from social media feeds, applications, web sites, etc. You can also use Azure Stream Analytics to visualize relationships and find patterns in streaming data. Once identified, data patterns can be used to drive downstream actions like sending information to reporting tools, storing data, or creating data alerts [16].

Azure Stream Analytics utilizes a source of streaming data that is ingested into the Azure IoT hub, Azure event hub, or from Azure storage. To evaluate the data streams, you must create an analytics job that identifies the input data stream source and uses a transformation query to determine how to search for data relationships or patterns. When analyzing incoming data is done, you are able to identify the desired output and then determine how to respond to the analyzed information. For example, you can take follow-up actions including:

- *Trigger Alerts/Customized Workflows* – Triggers a specific process or function in response to an input pattern.
- *Visualize Data* – Data is sent to a Power BI (a business intelligence framework) dashboard to allow real-time data visualization.
- *Store Data* – Utilizes Azure storage system to store the data; therefore, you can perform batch analytics or train holistic machine learning models based on historical data.

1.3.4.4 Azure Machine Learning

Azure Machine Learning is a cloud-based service supportive of open-source technology and useful for large-scale training, deploying, automating, and managing machine learning models. Azure Machine Learning enables the user to access thousands of open-source Python packages that include machine learning components such as PyTorch, Scikit-learn, and TensorFlow. Microsoft also offers another framework called Azure Machine Learning Studio, a drag-and-drop, a collaborative area that allows you to create, test, and deploy machine learning solutions without writing code. This workspace also provides preconfigured and pre-built algorithms as well as data management modules that make experimenting with machine learning modules quick and uncomplicated. Azure Machine Learning Service is beneficial instead of Azure Machine Learning Studio, when greater control over the details of the machine learning algorithms is needed or you need the flexibility to utilize open-source machine learning libraries [16].

1.3.4.5 Azure Logic Apps

Azure Logic Apps is a cloud service used to arrange or automate tasks, workflow, or business processes when data, applications, systems, or services must be integrated across large enterprises. One of the main benefits of Azure Logic Apps is that it makes the designing and implementation of scalable data integration, applications, and other system solutions including business-to-business (B2B) communication within the cloud or on premises (or both) easier and more straightforward. Below you will find examples of workloads that is possible to automate using Azure Logic Apps [16]:

- *Event Processing* – Events can be processed and routed across cloud services and on-premises systems.
- *Email Notification* – Email notification can be automatically sent via Office 365 when an event occurs in an app, service, or system.
- *File Transfer* – Uploaded files can be transferred from FTP or SFTP servers to Azure storage.
- *Tweet Monitoring* – Tweets can be reviewed by subject or analyzed based on sentiment and alerts or tasks can be created if the additional inspection is required.

1.4 IoT Applications in Vertical Markets

There are many areas where the Internet of Things will have a major impact. What follows is a sampling and a brief discussion of some of these IoT application areas.

1.4.1 Smart Agriculture

Also known as precision farming, since the power of data is brought to bear on agricultural decisions, instead of the traditional wisdom and guesswork.

- *Smart Greenhouses:* An IoT-enabled greenhouse will allow for the finer automation and control of environmental parameters. As expected, all aspects of the greenhouse can be monitored and recorded, including temperature, sunlight, air quality, humidity, and air flow. Adjustments to the environment can be recommended or automatically carried out depending on the recommendations of cloud servers.
- *Livestock Monitoring:* Cattle and other livestock can be monitored with IoT sensors to determine their location and vital signs to determine their health. Those animals with warning signs of sickness can be identified, quarantined to protect the others, and treated to overcome the sickness. This process saves on labor costs, improves the health of the overall herd, and reduces the risk to the animals and farmers.
- *Agricultural Drones:* In addition to placing sensors at key points, farmers can use airborne drones to monitor much larger and widespread areas. These drones can be recruited to plant seeds, spray existing crops, take soil samples, assess the health of crops, or even monitor fields or assets for security purposes simply. Historical records of crops can be more easily kept with drones assisting. They could also be used for integrated GIS mapping and visualization. All of these data points can ease the burdens on farmers, saving time and money and potentially increasing the agricultural output of the farm.

As an example of IoT in agriculture, we can name Cropx company. This company installs sensors to understand better water usage in fields growing crops. The data are used to conserve better and utilize irrigation. The company also advises on the type and use of pesticides and fertilizers to maximize the yields of crops. They do this by collecting data on soil, air quality, crop maturity, and even weather and then using algorithms and machine learning techniques to determine when and where to intervene.

1.4.2 Logistics and Transportation

Logistics is all about moving items from one place to another. Warehouses are used to store the items temporarily until they can be loaded onto vehicles and moved

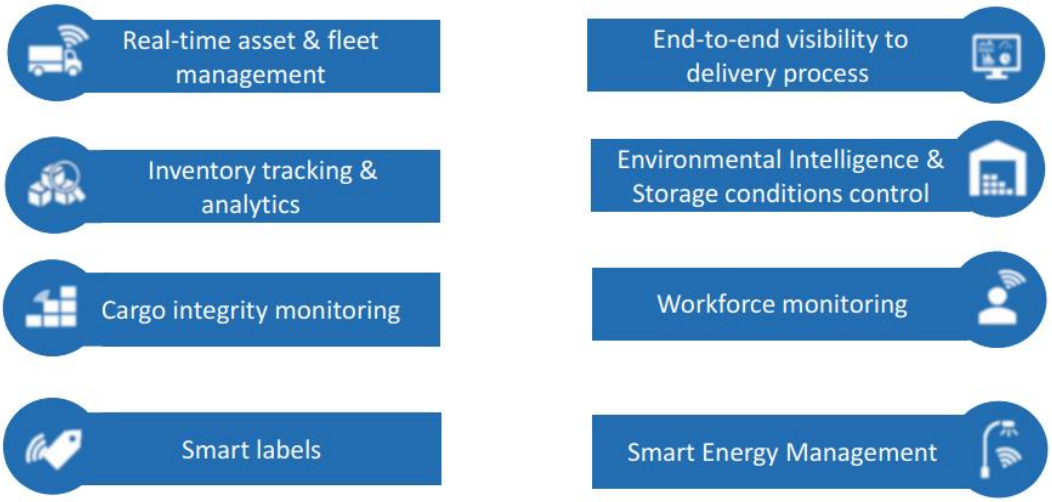

Fig. 1.6 A few use cases of IoT in logistics

further along toward their destination. The vehicles use the transportation network to maneuver between endpoints and warehouses. Generally, suppliers are the ones that dispatch these vehicles to deliver the items to customer locations. To succeed at logistics, it is important to reliably, safely, and predictably deliver items from suppliers to customers. All stakeholders also want to know the status and position of the items in the transportation network and to be able to forecast how long it will take to receive these items through borders, customs, or other checkpoints. This means that a quality logistics operation has mastery over the capacity of each stage in the transport and can optimize vehicle routes between endpoints in an energy-efficient and proactive manner. IoT can assist with all of these goals, from real-time traffic and environmental conditions for vehicles, to real-time monitoring of vehicle and warehouse capacity, to sensors to locate and verify that items are in good condition and route. The value of items is linked to the length of time they are in transit, so minimizing risk in damage or delay is another prime concern, and another one that can be addressed with the data that IoT delivers. The vehicle fleet itself can also be monitored to ensure that timely maintenance is being done, increasing its availability and longevity. Fuel and time can be saved by re-routing around bad weather or accidents, and theft and loss can be prevented and stopped with cargo validation and monitoring. There may be other business innovation opportunities when the IoT is fully leveraged in this field. A few more uses cases of IoT in logistics/transportation are shown in Fig. 1.6.

1.4.3 Smart Grid

The traditional power grid consists of monolithic power generation plants that deliver electricity across transmission lines to power substations where electricity is

distributed to customers via distribution lines. The customers had meters to record the use of the electricity, and these meters needed to be visited to be read. The next generation of power grid adds intelligence at the customer end by making those meters able to communicate their readings back to the power company. Further, with advanced metering, they can be updated in real-time to reflect changing tariffs on power based on loading and time factors. Demand can be better understood making power generation timelier and more efficient. Energy spikes, equipment failure, and power failures can be detected more quickly with smart sensors and the response can be more rapid with the automatic dispatch of engineers or even an automated restoration. Power outages and interruptions cost several billion dollars every year, so finding solutions to reduce and eliminate the occurrences improves quality of life and makes financial sense. Generators of electricity can better understand where, how, and how much electricity is used on the grid, enabling them to be more adaptive and responsive. Especially as the move is toward renewable energy sources and decentralization of electricity generation, smart technologies are vital to unlocking wind, solar, and tidal power to its full potential.

On the consumer side, understanding when and how electricity in the home is used can lead to better choices. Home automation can activate appliances during off-peak times, and thermostats can control home heating and cooling depending on the time of day and occupancy to maximize comfort and energy savings. Electric vehicles can serve as power storage for a smart grid, or a micro-grid for the neighborhood, being charged during off-peak times, and returning power to the grid during the times of highest demand. To address the above challenges, research and development to design IoT-driven power grid as a robust, reliable, and secure infrastructure is critical to the future of technological advances, since it powers all the other technologies.

1.4.4 Smart Building

Large buildings are currently outfitted with proprietary solutions to assist in solving the problems faced by facilities managers. They need information about how the building is functioning, the heating, ventilation and air conditioning system, the boilers, the power, the security system, and many other systems and subsystems that make up a modern building. While some management systems do a good job, they are often difficult to integrate with other solutions. Since they are often hardware based, once they become obsolete, it can be costly to update them, making them inflexible. Legacy buildings are a significant contributor to the increase in greenhouse gases in the atmosphere, with some estimates as high as 36 percent of CO2. Forty percent of total energy consumption is from the maintenance of buildings, with as much as 75 percent of current structures being inefficient. In 2016, the Paris Climate Agreement specifically targeted reducing the high energy consumption of buildings as an excellent method for addressing climate change.

IoT will bring greater interoperability to these older, disparate systems and, through the cloud, allow for greater remote management, improving efficiency and

response time. The sensors in an IoT-enabled building can collect the traditional information but also many other pieces of information not currently monitored, like air quality and occupancy. Using this data, building services could be improved to make occupants more comfortable and safer and also to use less energy. Workers who have greater peace of mind are able to concentrate better and be more productive. A smart building can offer this increased comfort with targeting thermostats to maintain more consistent temperatures. This results in more employee satisfaction, but also in a reduction in facilities calls to come and adjust the thermostat. Smart lighting can adjust light levels based on time of day and the presence of people needing that light, resulting in added savings. As systems change and adapt, software-based solutions will more easily adapt to them. The output of the sensors and detectors can be collected and visualized for facilities managers, to improve maintenance timing and effectiveness. Several companies are working for IoT-integrated solutions for the smart building, including Intel.

A case study in the possible energy conservation is that of a conference room. These rooms are important locations for productive meetings and a valuable space in which to work, but whether they are actually being used or not, traditionally they receive HVAC services. Intel performed a study using its smart building product and showed in its report that it was able to save 4 percent on HVAC costs in conference rooms in its subject building. With LED lighting and occupancy detection, it was able to reduce lighting wattage used per square foot from 1.09 to 0.39. Through analyzing other data points, there is room to innovate other cost savings in offices and shared spaces in buildings.

Power companies incentivize customers to reduce consumption during peak times by offering lower rates or credits called Automated Demand Response. IoT-driven smart buildings can take advantage of this by knowing the current building power usage and the grid rates and adjusting the load accordingly. There may be some load devices whose use can be delayed until an off-peak time, for example. If more power is demanded, then solar panels on the building, batteries or fuel cells in the building, or even a local power generator (diesel perhaps) could be utilized to make up the shortfall. This process can be automated via IoT solutions to optimize the cost of power to the building.

1.4.5 Smart Factory

Like IoT and other emerging technologies, there is not a unique and universally accepted definition for smart factory. However, smart manufacturing or smart factories can be explained by their main characteristics and core contributing technologies such as IoT, machine learning, 3D printing, cyber-physical system, robotics, big data, and blockchain. In the context of IoT, smart factories are manufacturing plants that incorporate IoT technologies into their processes to improve and optimize each and every aspect of the factory.

1.4.5.1 Current Manufacturing Model

The current manufacturing automation is based on a hierarchical architecture consisting of the following layers:

- *Level 1: Sensor and Actuator Layer* – This is the base level where the devices, sensors, and actuators exist on the plant/shop floor to perform different manufacturing process. This layer is a part of Operational Technology (OT).
- *Level 2: Field Automation Layer* – This layer (mostly based on PLC: Programmable Logic Controller) monitors and controls the devices that are attached to. This layer is also a part of Operational Technology.
- *Level 3: Supervisory and Integration Layer* – This layer mainly addresses supervisory control of the whole production process in the shop floor, shop floor monitoring, data acquisition, and data storage. It also functions as a multi-protocol intermediate gateway between the underlying industrial systems and the upper enterprise systems. This layer is usually implemented by Manufacturing Executive Systems (MESs), and Supervisory Control and Data Acquisition systems (SCADA). Level 3 is also a part of Operational Technology.
- *Level 4: Enterprise Layer* – Finally, decisions at this level concern the business planning, customer orders, material acquisition, and administration. Note that this layer is classified as an Information Technology (IT) layer.

Three important points should be noted here. The first point is that the above layers sometimes melt into each other in a way that some functions can be implemented at multiple levels. Second, many existing factories have not integrated the integration of Information Technology (Layer 4) with Operational Technology (Layer 1–3) yet. The third point is that the above model is rigidly structured to some extent, meaning that in the first two layers, there is almost a strict master-slave communication paradigm, with the master taking charge. According to Industry 4.0, the above model can be evolved toward a more decentralized model, allowing for more autonomy. In Industry 4.0, the decentralization allows for more flexibility, self-governance, self-organization, self-maintenance and self-repair. These are all goals of smart manufacturing, and is not surprising as Industry 4.0 is a much more recent standard.

1.4.5.2 Potential Use Cases

Here are the most popular IoT applications that are reshaping manufacturing and factories:

Operating Efficiency IoT-based smart factories are more responsive to changes in the environment and armed with more detailed and timely data are poised to proactively address potential problems or events as soon as they occur or even before they occur. In addition, traditional manufacturing plants depend on the skill and training of the operators and technicians to produce their output. For decades,

manufacturing has worked to increase the amount of automation in the process. Some benefits were realized, but often new technicians were needed to ensure the automation was working optimally. The Internet of Things should improve this situation as automation can be better monitored and controlled. A networked control system can sense, visualize and control every aspect of the manufacturing process even remotely. The smart factory can deliver a cost-effective, efficient, sustainable, and safe manufacturing system.

Real-Time Quality Control Manufacturing business success is dependent upon a rigorous inspection process applied across each production phase. IoT enables manufacturers to program equipment and utilize big data analytic frameworks within factories to effectively monitor the manufacturing line, equipment, raw materials quality, and the quality of completed products at each point in the manufacturing process. Integrating IoT in this manner provides the following benefits to the quality control process:

- Enabling real-time action in alignment with the manufacturing process
- Optimizing in-process manufacturing using production engineering insights
- Continuous adaptation and learning based on production output
- Continuous optimization to address process drift or production variance

Predictive Maintenance The ability to predict difficulties or perform predictive maintenance is an advantage with increased uptime and safety. Predictive maintenance is repairing or replacing equipment or components before predicted failures. Traditionally, historical mean time between failure data was used to schedule this maintenance, but with more accurate and timely data from IoT devices, a more specific time can be found, meaning good parts are not replaced, or unexpected weaknesses can be located and addressed before catastrophic failure. Of course, the data must be analyzed to extract these benefits, using machine learning and other data analytics techniques as mentioned earlier.

Safety Employee safety is another area that can be improved with IoT devices. Workers can be observed to find lapses in focus or other mistakes, and preventative action can be taken. With increased knowledge of activities on the floor, should there be a problem, help can be dispatched more quickly and accurately. When all activities are analyzed, it is possible to discover new processes or methods to use during the manufacturing itself. There is the potential to improve efficiency with these process ideas or with real-time solutions as situations develop in the plant.

Supply Chain Management IoT can help with supply chain management, as sensors track and help manage the location and condition of inventory, management can better plan, and schedules can be adjusted to optimize output. In addition to sensors, IoT devices can be used directly for automation. Integrating robotics can improve worker safety and factory throughput and reduce costs by increasing efficiency.

Machine as a Service (MaaS) This approach will allow updated machines to be deployed from the cloud, with remote configuration, connectivity, and monitoring.

Services such as these will allow for 100% uptime and zero-touch deployment, two desirable goals for manufacturers.

IT/OT Convergence Since the 1970s, there has been an increase in automation in the manufacturing sector. This trend continues as operational technology (OT) and information technology (IT) converge with programmable logic controllers, computers, networking, and connected devices and sensors. IoT brings manufacturing technology and enterprise networks together, eliminating technological silos. These improvements will lower costs with scaled, automated, and platform-based machine connectivity that will increase monitoring and optimization. It can be claimed that the main driving factor in IIoT and IoT in the manufacturing industry is the convergence of IT/OT. There are two terms that must be understood before discussing the convergence of IT/OT:

- *Information Technology (IT)* – Using computers, hardware/software, and other telecommunications devices to complete business operations. IT is mainly linked with the back-end functions required to handle operations including billing, resource planning, asset monitoring, accounts receivable/payable, and maintaining client information.
- *Operational Technology (OT)* – The foundation of modern smart factories. Manages infrastructures powering manufacturing plants and ensures factory lines keep running. The value of OT is amplified as additional machines or components are connected.

IT/OT convergence means operational technologies such as meters, sensors, programmable logic controllers, and SCADA are integrated to work together in near real time or real time with IT systems. The fields of OT and IT have existed side by side since the beginning of modern manufacturing. However, they have been siloed, with minimal interaction, resulting in a lack of understanding about how individual departments fit into the manufacturing process. Before IT/OT convergence, data sharing among departments was guided by the calendar, but the birth of the IIoT has vastly reduced the gap between IT and OT. Therefore, in a post-integration era, both IT and OT can share data in real time. There are several main benefits to IT/OT convergence, including agility, performance, productivity, cost, and agility. Combining IT and OT generates a complete picture of operational improvement opportunities and challenges facing manufacturers. This increased transparency helps IT and OT teams to better define their roles in light of a clearer team goal or purpose.

- *Cost*: The benefit that most often overlies both IT and OT departments is cost. In the area of IT, the cost is tied to predicting or illustrating profitability while the cost is generally linked to reducing production expenses in the area of OT. In both departments, reducing costs is good for the organization's profit margin.
- *Performance and productivity*: The benefits of improved performance and productivity are connected. Businesses can enable IT and OT to collaborate through a common platform to create accurate key performance indicators (KPIs) that

equip both departments to work toward common goals together while improving company-wide visibility.
- *Agility*: When an organization does a better job of controlling costs and analyzing KPIs, it is better able to act with agility to reduce production time and make space for innovation, which was a highly difficult task in a siloed IT/OT environment.

1.4.5.3 Major Challenges

There is the perception of several barriers that must be overcome in order to evolve manufacturing plants to smart factories. A recent survey of manufacturing executives by Cisco ranked these problems for IoT in manufacturing, starting from the most serious [17]:

- Lack of supply chain visibility
- Lack of visibility of plant floor KPIs
- Inability to access data within production
- Lack of common metrics across plants
- Plant floor IT apps in silos
- Employee skills gap
- The complexity of manufacturing operations
- Inflexible automation
- Lack of understanding the plant floor
- Lack of reliable plant floor network
- The process not automated (manual)
- Lack of clear manufacturing strategy
- Unable to justify return on investment (ROI)
- Insufficient investment to modernize
- Security threat or fear

1.4.6 Smart City

People have lived in cities for centuries, but only relatively recently, the mass migration from rural areas to cities has intensified worldwide. In 1950, less than one-third of the world's population lived in cities; that fraction is expected to increase to two-thirds by 2050. In raw numbers, that was fewer than 1 billion people, to upward of 4 billion people. As these populations increase, it puts tremendous pressure on the local environment. The amount of energy consumed, the amounts of food and products that must be brought into the city, and waste that must be removed strain the transportation system and the city itself. The world's cities use 60–80% of the energy used in the world. They also contribute the most to greenhouse gas emissions. Cities consume 60% of potable water in the world, wasting an estimated 20% in leakage. It is important to optimize the use of these critical resources and maximize their conservation [18].

The main reason cities have not been well designed is because they grew organically in response to increases in population. When the population increases rapidly, then urban planning cannot keep pace. The other problem is that city services are independent of each other, not communicating to solve problems together. The way cities are organized prevents collaboration, with each service or department getting their own funding and incentivized to solve their narrow problems. This leads to redundancy, waste, and shortcomings in meeting the needs of the city population. What is needed is a more scalable, collaborative, efficient system of city management and improvement. The Internet of Things can provide a city with more detailed and timely information and facilitate better solutions to the inefficiencies of modern cities.

1.4.6.1 Smart City Layers

As proposed by Cisco, an IoT solution for a smart city can be described with four general layers [17]:

- *Street Layer*: At the base is the street layer. This is where devices and sensors are placed in various parts of the city to collect data and take automated or commanded actions resulting from the analyzed data. The sensors used will depend on the location and function expected of them.
  - Video cameras are currently in widespread use in cities for various reasons. Some are aimed at highway sections, interchanges, or some city street intersections, and these are used to determine and report traffic conditions primarily. Other cameras are mounted at street level and are intended to monitor pedestrian behavior or are used for security purposes. The improvements in video recognition technology mean that these can be automated to perform facial recognition and vehicle recognition and make automated reports for security, traffic, and accidents.
  - Device counters or vehicle detectors are used to count the number of vehicles passing a certain area, or that are parked on streets or in structures. This is another technology that has been in use for many years to great benefit. Its use can be expanded to make parking counts more available to private drivers and their applications to better coordinate parking. They can also be adapted to count other things such as birds behaving as pests in public areas.
  - Magnetic sensors are able to detect the presence of vehicles in specific locations. This is another sensor that can be applied to the parking problem. It can also be used to make traffic lights more responsive.
  - An air quality sensor can be used to measure the amounts of particulate matter present in the atmosphere. This data can be used to give warnings to citizens when air quality is bad or to detect the culprits of high levels of pollution in order to improve air quality.

  - There are other sensors and controllers available and the choice of which one to be used depends on the problem to be solved and the resources available. There are several factors to consider when selecting a sensor. What are its lifetime maintenance costs? Can it be mounted on existing infrastructure? What is the cost of operation? Can it store its own data, or must it be transmitted to the cloud immediately? If such a connection is needed, is it available? How can this sensor interoperate with other such sensors? Can it scale? Once these questions are answered, then a tradeoff analysis can be conducted and the appropriate sensors can be selected. This is another reason why it is more efficient for the different departments of a city to work in concert, as they can leverage sensors and infrastructure to solve multiple problems.

- *City Layer*: The next layer is the city layer. This is above the street layer and provides the connectivity for the myriad devices in use at the lower layer. This means the network routers and switches are at this layer along with the communications protocols that allow the connected devices to exchange data. This is also the edge layer and the start of data processing. Some sensor data will be time sensitive, while others must be cleaned or reordered before transmission to the higher levels. A resilient and reliable network is therefore a necessity at this layer. Often, the networking equipment will be placed outdoors or in a harsh environment and therefore must be designed to work under inhospitable conditions. A malfunction at this layer may cause automated false alarms due to missing or mishandled data.
- *Data Center Layer*: When the data has been collected at the edge and transmitted, possibly over different transport protocols, it is delivered to the next layer up, the data center layer. This is where the final analysis is performed, and the results of these analytics are stored for further use. Therefore, analytics, storage, and some method of making results available are the primary functions at this layer. As previously discussed, the cloud plays a major role at this stage, providing the required storage and processing power.
- *Services Layer*: The services layer is the final layer in the Internet of Things smart city model. At this point, the results of the sensor data are provided to applications that make use of it – for example, a visualization tool to show the real-time status of traffic in the city. City managers, law enforcement, and private citizens should all have access to the data. City managers will want to ensure that the city is running smoothly and could use the data to find opportunities to conserve energy, for instance, or to check on the status of waste removal in a given neighborhood. Law enforcement could be verifying that tolls were paid or the payment made for the use of a public parking space, among other things. A private citizen could be looking for an open parking space or for the speediest path to the other side of the city. Once the sensors are in place and the data made available, then the city is ready to reap the benefits of the Internet of Things.

1.4.6.2 Applications of IoT in Smart City

Here is a sample of some areas where the Internet of Things is making a positive impact on smart cities.

- *Smart Lights* – Public outdoor lighting is beneficial to society as it makes public spaces safer to live and work. Unfortunately, it is also expensive to operate and often wasteful. Many systems merely use a timer to activate and deactivate the lights at certain hours of the day. The Internet of Things can make the system more efficient. Using sensors to monitor usage and activity at the lights, they can be directed to activate the lights only when needed. They can adapt the lighting settings to environmental conditions, such as fog or rain, when visibility has decreased. Lights can also be used to assist emergency responders or law enforcement by providing more lights in high-crime areas or when an accident has occurred. Real-time data about the lights themselves can provide operational status, making maintenance and replacement tasks proactive. This can increase the longevity and operational time of the lights while reducing maintenance costs.
- *Traffic* – Traffic lights can also benefit from the sensing and command possibilities of being connected by the Internet of Things. Real-time traffic data can be used to smooth traffic loads throughout cities. The goals are to reduce idling time, to improve flow and runtimes through the city, and to reduce pollution and fuel use. The data can be collected from cameras and correlated with data from vehicle counters. The ideal system would integrate traffic data with private navigation applications, so that a centralized view of the city can help direct drivers to balance routes. With smart traffic light technology and sensors on roadways, vehicle accidents can be detected more quickly, and assistance can be dispatched to the scene more efficiently. The path of the responders (e.g., police, ambulance) can be expedited, and even emergency rooms can be alerted so they can be prepared to receive victims. These efficiencies will help to make our roads safer.
- *Smart Parking* – Parking in a congested city can be frustrating and wasteful. With access to data about traffic patterns and open parking spots, applications can help citizens to locate and travel to available parking more efficiently. Kansas City in the United States and Paris in Europe have already implemented IoT smart parking solutions.
- *Smart Water* – Every city needs to manage its water supply. Water treatment plants must treat potable water for citizens, and a distribution system must deliver this water to residents. Currently, up to 20% of water is lost from the network because of leaks. It is difficult to predict water demand, and without accurate predictions, treatment plants can run inefficiently. The Internet of Things sensors can be used to improve water metering, leakage detection, planning for increased distribution, and understanding water use. Having better, more accurate data helps when creating water usage models, which improves predictions. More accurate water meters make water bills more accurate and build trust between

city water authorities and customers. Water is a precious commodity for us and it is vital that we manage it in an informed, thoughtful and efficient manner.

- *Smart Waste* – All cities produce waste and managing that waste is a difficult challenge. The most used current solution to the waste problem is to use manual collection based on a schedule set by a waste management company. The schedule may or may not be effective as it depends on the details of the waste management contract. The scope of the waste problem includes the collection, transport, processing, and disposal of the various kinds of waste generated by a city's population. Some waste can be recovered by recycling techniques, but this must be identified and separated and then transported to a recycling facility for processing. The entire process must be managed and monitored all at the cost of time, money, and labor. Improvements in the process can benefit all the stakeholders, the city council, manufacturing plants and other companies, health and safety authorities, and the people themselves. Using the Internet of Things to improve the process involves adding sensors in the waste receptacles and in the waste removal vehicles. These sensors can detect the amounts of garbage and the types of garbage present. In this way, a logistics platform can match the collection agents to the receptacles that are at or near capacity. The routes that collection trucks use can be optimized for efficiency.

1.4.6.3 Examples of Smart City

There are some cities that are already embracing transformative IoT technologies to improve the well-being of their citizens. For example, in Stockholm, a smart management system in conjunction with smart applications has addressed traffic and environmental issues in the city. The city implemented a policy of a shared waste management vehicle fleet that resulted in better waste collection routes and improved waste collection.

In Helsinki, the collective inputs of the citizens were leveraged by making over 1 thousand databases publicly available. The data concerned transport, economics, employment, and overall well-being of the people in the city. This was done via an open urban data platform, called the Helsinki Region Infoshare Project. The project won the European Prize for Innovation in Public Administration for empowering the citizens of the city. One of the chief results was to foster more public involvement in policy- and decision-making in the city.

1.5 IoT Business Implications and Opportunities

Internet of Things is seen as a strategic topic in many industries. For example, in 2018 the number of job postings related to IoT in Germany doubled compared to 2017 [19]. Bain & Company projected the global IoT market to reach $318 billion by 2021. Expectations are high regarding future IoT-based turnover [20]

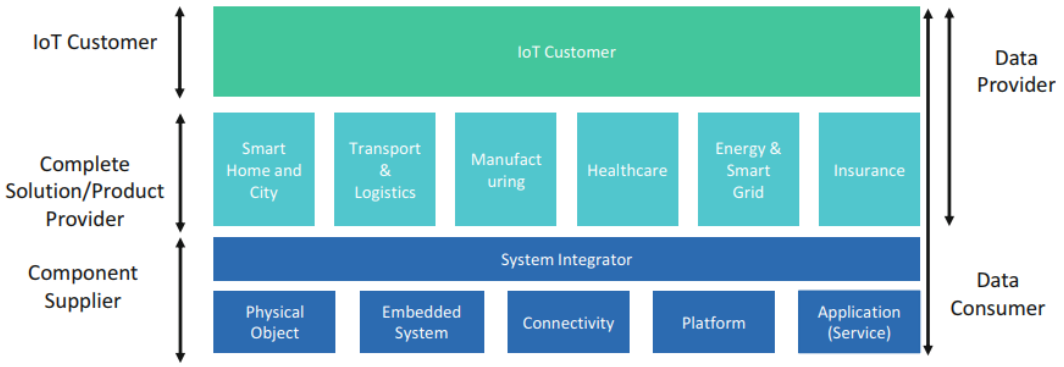

Fig. 1.7 Three basic IoT business opportunities

and emerging new business models [21]. Despite those huge expectations, many companies, especially small- and medium-sized enterprises, struggle to identify promising business models and solid use cases [22]. To be able to design new business models and draft business cases, the key business opportunities that IoT provides for a specific company should be analyzed and evaluated. In this context, we also need to understand the IoT business ecosystem, the stakeholders, as well as their motives. As shown in Fig. 1.7, three business opportunities and stakeholders can and should be distinguished when discussing the strategic impact of IoT from a company's point of view:

- *Complete Product and Solution Provider (Vendor):* These stakeholders aim at creating additional revenue streams from smart products/services which comprise the hybrid value proposition of IoT solutions [23].
- *IoT Customer*: The customer of an IoT solution on the other side is ultimately looking for optimization and cost reductions within its own operations. The IoT solution makes the operations of IoT customers smarter and optimized. The fundamentally different perspectives of IoT provider and IoT customer and their relation can be illustrated better by an example. John Deere is an international corporation that manufactures agricultural, construction, and forestry machinery. The so-called field connect system from John Deere allows for monitoring the moisture levels on various depths of a farmer's field [24]. The IoT provider (John Deere) intends to create additional revenues from an innovative offering based on IoT, which he did not sell before. The farmer (IoT customer) on the other hand invests money in an IoT solution hoping to reduce the cost for monitoring moisture manually on site and waste of water.
- *Component Supplier*: Many companies could leverage the third strategy as well. A component supplier facilitates the design and deployment of the Internet of Things. In this case, no complete IoT solutions are involved, but just IoT components. These might be technical components on a single layer of the IoT technology stack (e.g., IoT device, gateway, connectivity, and cloud platform) or components from two or more layers.

1.5.1 Component Supplier: Component Business

While a complete IoT solution comprises the whole IoT stack, IoT components relate to one or at maximum three layers of the IoT stack. A company could focus on selling such IoT components to complete IoT solution providers who intend to build and release complete IoT solutions. Let us examine each layer of the IoT value stack and their corresponding stakeholders using a connected electric bike (e-bike) example [25]:

- *Physical Object* – The physical object (i.e., e-bike) provides the initial direct benefit for the user. As with traditional bicycles, the e-bike provides an eco-friendly, healthy mode of transportation while also enabling motorized cycling.
- *Embedded System* – In this layer, the physical thing is equipped with a processing unit (e.g., a microcontroller), a connectivity module (e.g., 3G, 4G, NB-IoT), sensors, and actuating components to become smart. These pieces operate locally by gathering data and providing localized benefits. In our example, sensors are responsible for monitoring battery status or sensing when motorization is required. An example of an embedded system provider is Bosch which designs and provides several IoT sensors for years.
- *Connectivity* – In this layer the smart object and its functions/status (e.g., battery status) can be accessed online globally with the help of network providers/operators. Moreover, new services could be added to the system e.g., online location monitoring or theft prevention. In many IoT solutions such as e-bike, we can use SIM cards and mobile networks to be connected to the Internet. Indeed, already in the first quarter of 2016 in the United States, 69% of newly activated SIM cards were related to non-phone devices, like cars, dog collars, etc. Thus, all major mobile network operators aim at selling SIM cards as IoT components.
- *Platform (Cloud)* – Platforms are one of the central foundations of IoT as they unite connectivity, service providers, applications, and embedded systems to create specialized IoT solutions for diverse industries. Platform providers offer data ingestion, data storage, data analytics, data visualization, device/user management, and integration with other third parties through SDK or APIs. In our e-bike IoT solution, this layer enables one to track the movement patterns of e-bike users, study the difficulty levels of specific cycling routes to understand motorized support demand better, or discover the location of stolen e-bikes in real time. An example of the platform layer could be Amazon. With Amazon Web Services (AWS), the company has been successful in the cloud computing business. Indeed, Amazon is now offering an IoT component (i.e., AWS) that can be used to build IoT solutions.
- *Application (Service)* – This final layer combines the options and features provided by the prior layers to structure digital services. Users can receive digital services in appropriate formats that are independent of location via mobile applications or web tool. In our example, this feature enables customers to find e-bikes in the case of theft or provides pertinent location information to law enforcement.

- *System Integration* – The stakeholders of this layer play a large role in the IoT ecosystem because not all IoT components are plug-and-play right out of the box. Therefore, system integrators are needed to enable individual IoT components to collaborate in the best possible way. System integrators should identify a specific niche and then make partnerships with other stakeholders.

1.5.2 Complete Solution and Product Provider: Additional Revenue

IoT solutions are addressing business problems across several vertical markets from health to smart building, transportation/logistics, energy, and manufacturing. In this context, many companies, incumbents and startups, seek to create revenues from smart connected products. This could include enhancing the companies' already existing products with embedded systems (e.g., sensors, connectivity, etc.) in order to enable new features or digital services. But it could also mean developing entirely new connected offerings.

One of the main challenges for such an endeavor lies in handling the rather complex IoT value stack. A company from the digital or Internet world or a startup would need to develop and produce the connected thing, which would mean to enter the hardware world, with comparatively high upfront investments for development and production setup. A manufacturing company needs to complement its hardware expertise with the required skills on the connectivity, analytics, and service layer, which includes user front ends like apps as well. A second aspect which might be new for many manufacturing companies is the fact that servers and their software, as well as apps and other user front ends, need to be operated and maintained throughout the whole usage phase. This poses two challenges. On the one hand, the organization has to bear operating cost over the whole lifetime of the offering. And, on the other hand, the organization needs to have the capability to perform the abovementioned operations. Especially manufacturing companies might need to install new units taking care of those tasks [26].

The upside of smart connected products is new revenue sources which wait to be captured by an appropriate business model [23]. It provides a hybrid value proposition consisting of physical and digital parts. Both parts can be monetized either in a product (one-time payment and transfer of ownership) or service manner (continuous payments and usage rights). This opens up a space of four potential revenue sources. Especially in B2B scenarios, vendors manage to monetize two or more of those revenue sources. But even if only the hardware is being monetized, prices for connected products are, in many cases, much higher compared to similar non-connected products. For example, connected Philips Hue light bulbs sell for much higher prices compared to not connected light bulbs [27].

It should be noted that the creation of IoT products currently is not directed by specific guidelines or a systematic method. The application of a traditional

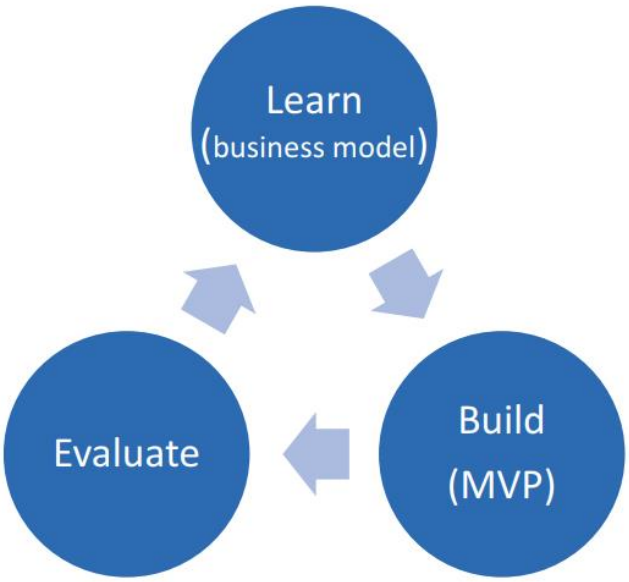

Fig. 1.8 Phases of IoT product development

legacy product development paradigm to IoT products is generally ineffective and disadvantageous. Agile methodology and in particular Lean model is typically considered a good fit for many organizations working in the IoT domain. According to this model, when developing an IoT product, there are three main stages that are important to constructing a competitive and sustainable IoT solution (see Fig. 1.8):

- *Learn* – Develop an innovation plan and construct or revise the business model.
- *Build* – Implement and build a minimum viable product (MVP).
- *Evaluate* – Measure and evaluate the product and provide feedback to the first stage.

1.5.3 IoT Customer: Optimization and Cost Reduction

While IoT consumers might buy an IoT solution in order to increase their comfort, for the peace of mind or just for fun, in business to business cases, the customer always calculates a return on investment. For IoT solutions, this usually translates into expected cost reductions that amortize the investment. Among the most popular approaches to realize IoT-based cost reductions is condition monitoring [28]. Critical parameters in the production process, like soil moisture in the John Deere example, are being monitored and optimized in order to reduce waste, or equipment is being monitored with the aim to reduce downtime. Other approaches include optimizing the supply chain. IoT, in terms of RFID technology being applied in a warehouse for example, could lead to a much more detailed picture of the actual inventories of raw material. This in return could allow for reducing the warehouse stocks, which leads to cost reductions as well.

In general, the Internet of Things helps to gather data regarding the status of the physical world. This could be the condition of machines or other equipment, inventories in a warehouse/whereabouts of goods. Those data can be analyzed and leveraged by advanced machine learning algorithms and big data analytics algorithms to optimize a company's operations.

1.5.4 Important Aspects of Implementation

The three IoT-based business opportunities pose different challenges for companies. But in general, they require a significant change in the company's business model. While changing a business model is a serious management challenge already, business model innovation poses various additional challenges. Bilgeri et al. identified 16 barriers to IoT business model innovation. They are distributed along with the following innovation phases: idea generation, concept development and evaluation, technical implementation, and commercialization. Many of these issues are related to organizational questions. As already discussed, IoT solutions require continuous efforts, e.g., in back-end operations, maintenance, and development of new features throughout the whole lifecycle. Most incumbents from the manufacturing industry do not have units for these tasks in their organization yet. To name another example, IoT solutions provide the opportunity to sell services in addition to or rather than products. However, selling services requires different skills as well as controlling and financial mechanisms compared to selling products.

1.5.5 Data Monetization

Transforming IoT data into a marketable product is a fast-growing trend many companies are considering as a secondary revenue source; however, the idea of selling data is not a new one. Gartner has labeled the creation and utilization of data or information with the term, "*infonomics*" [29]. With millions of smart devices connecting to the IoT and collecting data, a new market based on data providers and data customers has been born (see Fig. 1.7). Profiting from IoT data can be approached in two ways [30]:

- *Direct Data Monetization* – Regardless of why you may be willing to offer your raw data, there are probably consumers interested in using and paying for your data. While there are many ways to sell data, a primary means is through a data marketplace. When selling data, direct monetization is generally separated into two categories [30]:
  - *Selling Raw Data* – Direct access to data (i.e., APIs or data sets) is provided in trade for cryptocurrency or money. There are two general marketplaces from

which you can choose and the appropriate choice depends on your strategic requirements [30].

  - *Centralized Marketplace* – This is a platform owned by one party that serves as a centralized location to exchange multiple kinds of data among diverse participants. In this marketplace, both metadata and raw data are stored.
  - *Decentralized Marketplace* – This is a platform where participants are able to exchange data directly in peer-to-peer transactions. In this context, the marketplace only stores the metadata to enable data consumers to find the provider/owner of the data.

- *Selling Data Insights or Analysis* – Performing data analytics on raw data improves the quality of the information being sold. Not all companies have the capability to analyze data, creating an opportunity for monetization that is beneficial for both sides of the transaction. Analysis services can be offered in marketplaces or through other channels.

- *Indirect Data Monetization* – Data can be used to improve business intelligence and function, generate new products or services, and create new business models. Generally, there are two approaches to making good use of your own data [30]:

  - *Data-Driven Optimization* – Utilizing data in this way decreases cost and increases the effectiveness and efficiency of business processes. This optimization is applicable across many fields. For example, manufacturing test benches could be optimized by shortening the testing time or field data could be utilized to improve the design of a product.
  - *Data-Driven Business Models* – Monetizing by employing this strategy means that process or product data is used to generate new business opportunities or attract new customer groups through the development of new services or products or by improving existing products or services. Building a data-driven business model enables you to uncover innovative, new businesses rather than adjacent businesses. These models are also important for diversifying revenue streams. For example, Bosch makes use of manufacturing data to create customized subscription-based services that monitor the conditions of hydraulic systems.

The market of IoT data will keep growing as companies learn how powerful it can be to provide data to others and how much others are willing to pay to obtain data. The primary challenges around monetizing IoT data include [29]:

- *Ensuring Data Quality* – In order for customers to trust the data provided, it must be of high-quality and complete. The data should also be accurate and timely and have been obtained ethically.
- *Determining Information Type* – Providers of data will need to adapt and flex to customer needs as companies may require IoT data in diverse forms or

may consider data that was not originally fit to their particular business model. Customers may seek additional information for data points that were not initially recorded.

- *Traditional Product Management and Marketing* – IoT data is not like a traditional physical product. Therefore, companies may need to forego the usual activities that help sell physical products such as research, design, development, promotions, packaging, or marketing support.
- *Protecting Against Unlicensed Use* – It is very important to ensure data sovereignty for the creator of the data. It is easy to copy data, and thus it can become difficult to make sure customers are not utilizing data in unintended manners. Therefore, we need to consider contracts that ensure a licensed user understands the appropriate and ethical handling of information products, how to audit usage, etc.

1.5.6 Business Model

It is important to understand the basic business model before attempting to create an IoT Solution. The term "*business model*" was born toward the end of the 1990s when it became a buzzword in popular media. Since that time, it has received significant attention from scholars and business practitioners and currently exists as a clear point of interest in many areas of IoT. Typically, the business model is defined as an analytical model used to determine how a business functions. The available literature regarding the business model has not yet reached an agreement regarding which elements are vital to the creation of a business model. However, two widely known tools currently exist to illustrate business models: *St. Galler Magic Triangle* and *Osterwalder Business Model Canvas*.

The St. Galler Magic Triangle is comprised of four dimensions and is illustrated using a triangle shape (see Fig. 1.9) [31]:

- *Who*
  - Who are the target customers?
  - How can customers be classified into groups?
  - What are the basic demographics and shared characteristics of customers?
- *What*
  - What is the opportunity being offered to the customer?
  - What value is being added for the customer? (value proposition)
  - What combination of services or products make up the opportunity?
- *How*
  - How is the value proposition created, applied, and distributed?

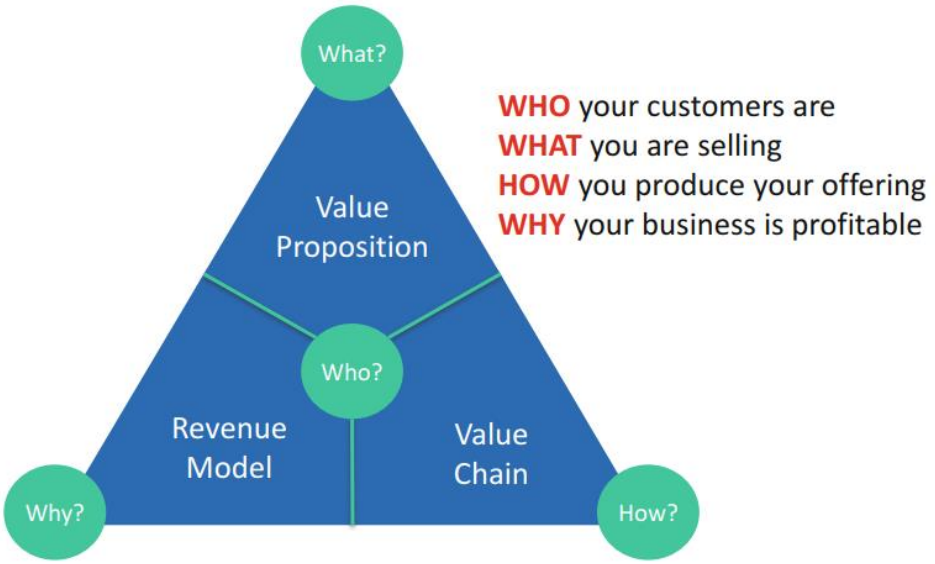

Fig. 1.9 St. Galler Magic Triangle

- How will the activities and processes need to provide the product look?
- What kind of resources will be needed?
- Which IoT business ecosystem stakeholders will be needed and how should they be organized?

- *Revenue*
  - Does it look as though the opportunity will be financially sustainable?
  - What does the cost structure look like?
  - What revenue mechanisms will be applicable?
  - How can the value proposition be monetized?

Thoughtfully answering the questions in each of the four areas noted above creates a solid business model and a foundation for further innovation in IoT ecosystem.

Osterwalder Business Model Canvas, created by Osterwalder in 2010, serves as an alternative method to the St. Galler Magic Triangle for illustrating a business model (see Fig. 1.10) [32]. It provides a well-known guide for explaining a business model in only one page. This model includes the following components [32]:

1. *Key Partners*: Who are the key partners and suppliers?
2. *Key Activities*: What key activities (e.g., marketing, designing, producing) our value propositions, distribution channels, customer relationships, and revenue streams need? What tasks does the company need to perform to fulfill its business purpose [32]. Some typical key activities in IoT business model include *Research & Development*, *Production*, *Marketing*, and *Sales & Customer Services*.

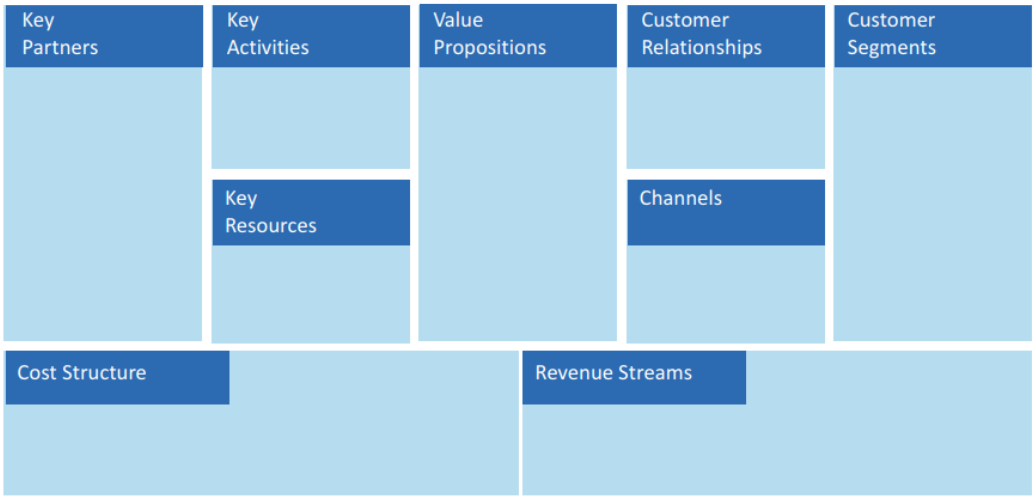

Fig. 1.10 Osterwalder Business Model Canvas

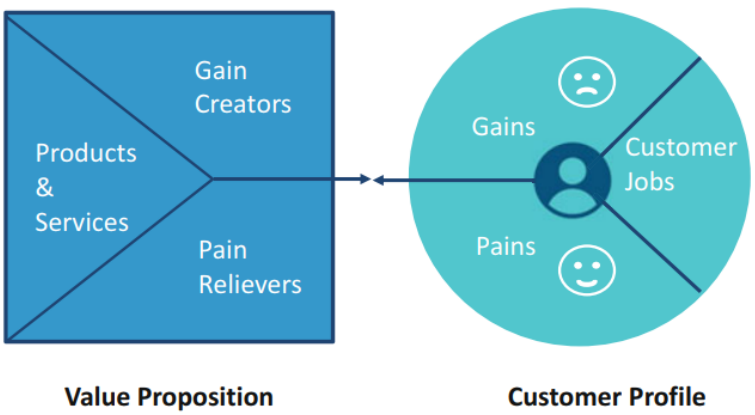

Fig. 1.11 Value Proposition Canvas

3. *Key Resources*: What key resources (e.g., *physical resources*, *intellectual resources*, *human resources*, *financial resources*) do our value propositions, distribution channels, customer relationships, and revenue streams require [32]?
4. *Key Propositions*: What value do we deliver to our customers? What bundles of products/services do we offer? Which problems of the customer are solved by our products/services? To find the key proposition, one can use the Value Proposition Canvas [32]. As shown in Fig. 1.11, the Value Proposition Canvas consists of two building blocks to be able to model and visualize the relationship between product/service and customer/market [32]:

   - *Customer Profile*: This shows the task/job a customer needs to get done, potential pains that the customer might face during and after the job, and benefits that a customer expects from the product/service.

- *Value Proposition*: This shows the list of products/services, explains how they can kill the pains of the customer, and demonstrates how the offered products/services can create customer gains.

5. *Customer Relationship*: What type of relationship does each of our customer segments expect us to establish and maintain a long-term relationship with them? The most common types of customer relationships include transactional, personal assistance, self-service, automated services, communities, and co-creation. Note that these types of relationships can coexist in a company's relationship [32].
6. *Channels*: Through which channels (e.g., website, email) do our customer segments want to be reached [32]?
7. *Customer Segments*: From whom are we creating value? Who are our most important customers [32]?
8. *Cost Structure*: What are the most important costs inherent in our business model? Which key resources/activities are the most expensive [32]?
9. *Revenue Streams*: For what value are our customers really willing to pay? For what do they currently pay? How are they currently paying? How would they prefer to pay? How much does each revenue stream contribute to overall revenues [32]?

1.5.7 Minimum Viable Product (MVP)

The concept of a *minimum viable product* (MVP) was first introduced in Eric Ries' popular book, *The Lean Start-Up*, in 2001. The goal of an MVP is to evaluate if the product fits in the market with the smallest possible amount of risk. In this approach, a new product is created with features adequate to satisfy the earliest users. The final features are not developed until feedback from initial users can be evaluated. In short, the main idea is to construct a very simple, testable version of the product. The results of testing can be included in the next stage of development during the scaling phase or for revising the business model. A "build, evaluate, and learn" approach enables the solution provider to build the more important and viable basics into the product as quickly as possible. At the start of the process, there is usually a large-scale, almost unreachable vision of what the finished product will be, and shaping the vision at such a high level can consume large amounts of time and considerable resources. It is important to avoid the pitfall of trying to create a *perfect IoT product*. Instead, one should focus on creating a *possibly viable IoT product* with the potential to focus team creativity and original ideas throughout the process, while addressing the question of whether the product should even be created at all or not. In order to choose the most significant value proposition for creating the MVP, the company must concentrate on the specific intersection of the customer's wants and the value of the product as illustrated in Fig. 1.12. As shown in this figure, to be able to define the list of important features which should be

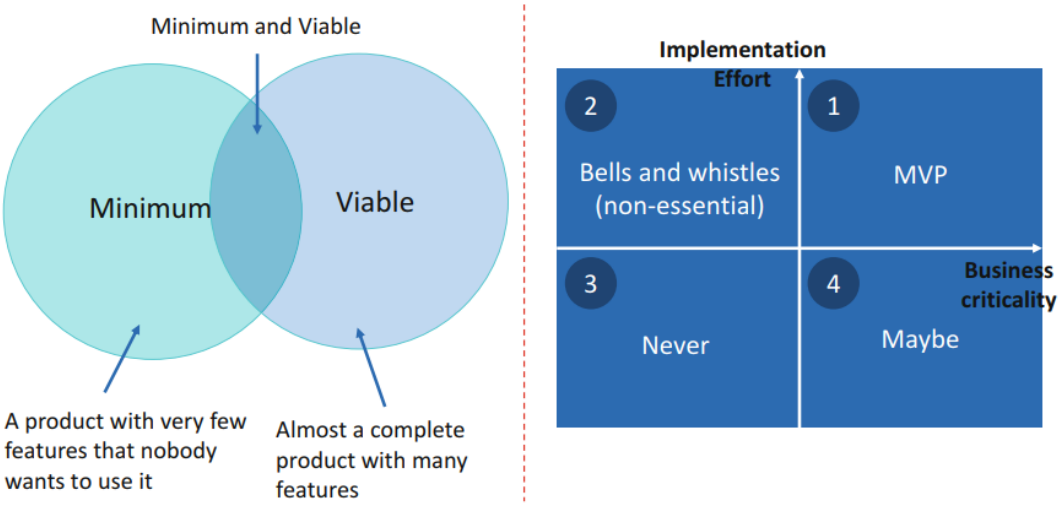

Fig. 1.12 Minimum viable product (MVP)

included in the MVP, we can classify the product features based on two dimensions, namely, implementation effort and business criticality.

- *Quadrant I* – Features in this area are vital to the MVP because they are critical to business success and are usually more straightforward to implement.
- *Quadrant II* – These features are nice, but they are not vital and are still easy to implement. Leaving these out of the MVP saves both time and resources.
- *Quadrant III* – Features in this area are trivial and can be hard to implement. They should be avoided in an MVP and in the following product iterations.
- *Quadrant IV* – These features are business critical, but are also arduous to implement. The elements in this quadrant need a maximum amount of deliberation and thought.

1.6 Summary

This chapter introduced the Internet of Things (IoT) with several definitions and discussed the benefits and challenges of establishing the IoT. There are advantages to be gained in the personal lives of individuals as well as the operations of businesses and manufacturers. This chapter discussed all the promises and challenges of IoT. The complete IoT stack from the sensors and devices, to the fog, and to the cloud has also been explained. There are several commercial frameworks, cloud technologies, and IoT-enabled devices and ecosystem providers, which we presented their offerings briefly. Next, some examples of the applications of IoT technology have been listed with their expected impacts to varied sectors of our society, from agriculture to the cities in which we live. Finally, the details of the business implications, business models, and opportunities of IoT have been addressed.

References

1. IBM. Available from: https://www.ibm.com
2. SAP. Available from: https://www.sap.com/
3. Gartner
4. Bosch. Available from: https://www.bosch.com/
5. IDC. Available from: https://www.idc.com
6. Intelligent IoT. Available from: https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/intelligent-iot-internet-of-things-artificial-intelligence.html
7. A. Rayes, S. Salam, *Internet of Things—From Hype to Reality* (The road to Digitization. River Publisher Series in Communications, Springer, Denmark, 2017), p. 49. https://www.amazon.de/Internet-Things-Hype-Reality-Digitization/dp/3319448587
8. NIST: National Institute of Standards and Technology. Available from: https://www.nist.gov/
9. P. Raj, A.C. Raman, *The Internet of Things: Enabling Technologies, Platforms, and Use Cases* (Auerbach Publications, 2017)
10. A. Botta et al., Integration of cloud computing and internet of things: a survey. Futur. Gener. Comput. Syst. **56**, 684–700 (2016)
11. Internet of Things World Forum. Available from: https://www.iotwf.com/
12. F. Firouzi et al., Keynote paper: from EDA to IoT eHealth: promises, challenges, and solutions. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **37**(12), 2965–2978 (2018)
13. B. Farahani et al., Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. Futur. Gener. Comput. Syst. **78**, 659–676 (2018)
14. FIWARE. Available from: https://www.fiware.org/
15. AWS IoT. Available from: https://aws.amazon.com/iot/
16. Microsoft Azure IoT. Available from: https://azure.microsoft.com/en-us/services/iot-hub/
17. D. Hanes et al., *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things* (Cisco Press, 2017)
18. I.A.T. Hashem et al., The role of big data in smart city. Int. J. Inf. Manag. **36**(5), 748–758 (2016)
19. Diese Digitalexperten sind bei deutschen Firmen besonders begehrt. Available from: https://www.handelsblatt.com/unternehmen/beruf-und-buero/digitaler-jobindex/digitaler-job-monitor-diese-digitalexperten-sind-bei-deutschen-firmen-besonders-begehrt/22957856.html?ticket=ST-1817019-o0qDpTQqZsW0sFKadd20-ap
20. Roundup of Internet of Things Forecasts. Available from: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6a7ab8041480
21. E. Fleisch, M. Weinberger, F. Wortmann, *Business Models and the Internet of Things, Bosch IoT Lab Whitepaper* (Bosch Internet of Things and Services Lab, 2014)
22. Businesses are Expected to Continue IoT Adoption Despite Security Risks, Survey Says. Available from: https://biztechmagazine.com/article/2017/02/businesses-are-expected-continue-iot-adoption-despite-security-risks-survey-says
23. F. Wortmann et al., Ertragsmodelle im Internet der Dinge, in *Betriebswirtschaftliche Aspekte von Industrie 4.0*, (Springer, 2017), pp. 1–28
24. John Deere, John Deere Prescision Ag Technology, Brochure. Available from: https://www.deere.com/assets/publications/index.html?id=004d03e7#36
25. D. Bilgeri, et al., *The IoT business model builder.* A White Paper of the Bosch IoT Lab in collaboration with Bosch Software Innovations GmbH, 2015
26. D. Bilgeri, F. Wortmann, E. Fleisch, How digital transformation affects large manufacturing companies' organization. 2017
27. E. Fleisch et al., *Revenue Models and the Internet of Things? A Consumer IoT-based Investigation* (ETH Zurich, 2016)
28. How the Internet of Things is driving cost-saving efficiencies for manufacturers, The shi blog. Available from: https://blog.shi.com/hardware/internet-things-driving-cost-saving-efficiencies-manufacturers/

29. D.B. Laney, *Infonomics: How to Monetize, Manage, and Measure Information as an Asset for Competitive Advantage* (Routledge, 2017)
30. A guide to data monetization. Available from: https://blog.bosch-si.com/business-models/a-guide-to-data-monetization/
31. O. Gassmann, K. Frankenberger, M. Csik, The St. Gallen business model navigator. 2013
32. Osterwalder Business Model Canvas. Available from: http://alexosterwalder.com/