# CHAPTER 2 IoT Applications for Industry — Value Creation and Challenges

**IoT Applications**

Throughout the entire document the following pragmatic deﬁnition for IoT applications was used in order to focus the scope and to have a common understanding: IoT applications in the sense of this paper are solutions using IoT technologies capable to improve and easy adapt industrial manufacturing processes, enable new and efﬁcient ways to do operate and interact in pro- duction plants, create new service or supervision means for industrial instal- lations, offer an optimized infrastructure, reduce operational cost and energy consumption or improve human safety in industrial areas.

To start a project in industry environment the expected beneﬁt, the expected value to the company has to be estimated and later needs to be re-evaluated and

proved during operation. To deﬁne the value of an industrial IoT application or IoT project is difﬁcult. There are numerous reasons for that. The value typically shows up gradually with new process introduction and accumulates over time, the value is often difﬁcult to quantify due to multiple interactions and complex processes, it may contain hard but also soft beneﬁts difﬁcult to assess. Value can be generated and may show up as a result of a combination of IoT applications with other systems or processes, or can originate in new human behavior or new interactions. Fact is that value is the key element ﬁnally asked by the project stakeholders or owners.

There is no value but “values” each contributing to the total beneﬁt such as:

• Value from visibility identiﬁcation, location tracking

• Value form IoT-supported safety in hard industrial environments • Value from right information providing or collecting

• Value form improved industrial operation and ﬂows in industry • Value from reduced production losses

Value from reduced energy consumption

• Value from new type of processes made possible by IoT applica- tions

• Value form new type of maintenance and lifetime approaches • Value enabled by smart objects, connected aspects

• Value from sustainability.

**3.2 IoT Applications for Industry — Value Creation and Challenge**

Security and safety.

Security requirements are related to the cyber security threats and have to be part of the entire security strategy of the company.

Safety is mainly related to the device construction and the area of use but also to usability such that no safety threats occur due to use of the IoT applications and devices.

• Simple use.

Simple, intuitive use and (almost) self-explaining are important for the overall IoT application acceptance. The IoT application should ideally be context aware and adapt to the skills of the user and location or environment aspects.

• Optimal and adaptive set of features.

The IoT application should allow to perform desired task with the sufﬁcient, not-richer-then-necessary, set of features

• Low/No maintenance.

Maintenance free or reduced maintenance IoT applications and devices over operational life would be ideal. Maintenance over lifetime is an important aspect impacting the life cycle costs of IoT based solutions. It is affected by the sometimes high number of IoT devices in place, the fact that they are typically distributed over large areas, the required skills, tools and time needed for any type of IoT maintenance operation. This is valid for all devices but especially for active IoT devices or active wireless sensing. • Standardization.

IoT devices and applications should be using a set of standards to support interoperability of IoT devices, easy exchange and multi- vendor possibilities.

• Integration capabilities.

Easy integration in the IT and automation and process landscape of the industrial plant are required and may decide if a IoT solution will be used. This is particularly important for brown-ﬁeld projects but also for green ﬁeld in the view of future plant extensions. • Reach sensing and data capabilities.

IoT applications will relay more and more on complex sens- ing allowing distributed supervision and data collection and data capabilities. This is a chance in terms of additional data and

real-time information but also a challenge in terms of data and processing.

• Industry grade support and services.

The IoT applications should be supported over years in operation by a set of rich tools and continuously updated services. Typi- cally industry application requires also a centralized management of devices and systems, managed access rights, this might apply to some of IoT devices too.

Presently there are also numerous challenges to reach all the above.

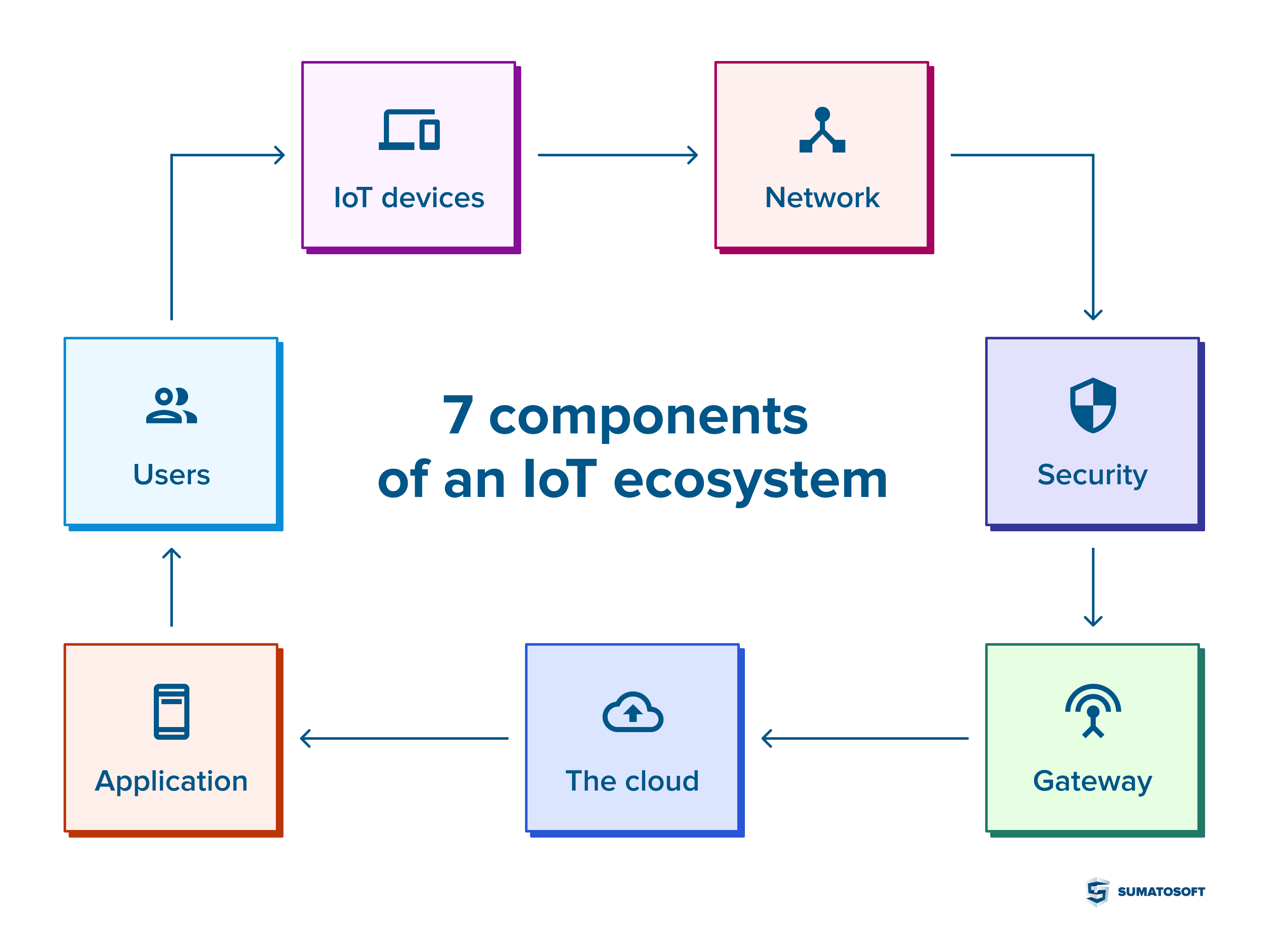
**Challenges faced by IoT industry applications**

The challenges for IoT industrial applications can be subject of a more extended treatment, however for the needs of present IoT applications and value creation they have been divided in 4 groups:

• IoT device technical challenges • Lifetime and energy challenge • Data and information challenge • Humans and business

The IoT devices technical challenges are numerous and subject of intense research. Some aspects will be addressed also in the following sections. A set of technical features will be especially needed in industrial applications, depending on application, such as extended capabilities for sensing in terms of sensor types and high sampling rate, communication, wireless data transfer and precise time synchronous collection of data both in single-hop and multi- hop industrial networks. Another aspect is related to the easy deployment, conﬁguration and re-use of non-permanently attached devices, such as the ones used for ad-hoc sensing. One critical and often neglected aspect is the device packaging for the industrial application needs which is essential for reliable operation.

Last but not least is the heterogeneity aspect which is a problem even today. In industrial environments often encountered are combinations of one or more of: of passive and active RFID with or without sensing, various ﬁx or mobile RFID readers, wireless sensor nodes and networks, wired and wireless technologies in factory automation, use of different frequency bands.



**IoT Today**

The fact is, landlines are becoming obsolete. IOT Today uses cellular technology. More reliable, with better coverage, and with faster alert response times. Be alerted instantly if there is an emergency and monitor the situation and even lock your doors and arm your alarm remotely. With only your cell phone, you can know what's happening in your home.

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Currently, the applications of IoT cover adverse areas including manufacturing or the industrial sector, agriculture, health sector, smart cities, security, and emergency services among many others.

With IoT, Companies can automate processes and save labor costs. It also reduces waste and improves service delivery, making it cheaper to manufacture and deliver goods and ensuring transparency in customer transactions  
The Next Generation Internet of Things (NGIoT) initiative is a growing community of projects and related initiatives at work to maximise the power of IoT made in Europe. NGIoT works to lower the barrier for adoption and development of IoT-empowered solutions, by supporting business models, innovation and skills.

**IoT Tech Trends:**

1. Remote Monitoring

2. Modular Smart Technologies Solutions

3. Data Analysis

4. Artificial Intelligence, Machine Learning, and Visual Inspection

5. Advanced Networks

6. Smart Buildings, Smart Cities

7. Digital Twins

8. Fintech

## 4 Types Of IOT Networks

### 1. Cellular

Cellular networks use the same mobile networks as smartphones to allow IoT devices to communicate. Because these networks were originally designed for power-hungry devices like smartphones, they weren’t always considered the best fit for IoT devices. Eventually, the cellular industry developed new technologies that were more appropriate for IoT use cases. Today, this type of wireless network is very popular, and is considered a reliable and secure method of IoT connectivity. Cell service is available in most locations in the U.S., and this type of network covers a very large area. However, cell connectivity often isn’t available in the places that most need monitoring sensors—for example, inside utility closets, elevator shafts, basements, etc. (Another IoT wireless technology class, LPWAN, might be a better fit for these locations.) And even though cellular connectivity is now less expensive and more power efficient than traditional telecom standards, cellular-connected IoT devices still require a great deal more power and energy than some other types of wireless networks.

Two cellular IoT wireless protocols currently vying for dominance are [**LTE-M** and **Narrowband IoT (NB-IoT).**](https://www.iotacommunications.com/blog/lte-m-vs-nb-iot/) LTE-M is a great option for IoT connectivity if you’re willing to pay the price, and if your use case requires low power. In addition, LTE-M networks are already in place in the U.S., which means you can start taking advantage of this option today. NB-IoT is somewhat less costly than LTE-M and uses less battery power, but there’s not enough coverage everywhere to reliably deploy an NB-IoT solution yet.

### 2. Local and Personal Area Networks (LAN/PAN)

Networks that cover fairly short distances are called personal area networks (PAN) and local area networks (LAN). PAN and LAN networks are considered to be fairly cost-effective, but the transfer of data can sometimes be unreliable.

Wireless personal and local area network technologies that are commonly incorporated into IoT connectivity solutions are **WiFi**and **Bluetooth.** WiFi can be used for applications that run in a local environment, or in a distributed setting if there are multiple access points integrated into a larger network. One downside to WiFi is that it works only if the signal is strong and you’re close to the access point. Also, WiFi is generally more power-hungry than people think, but it is possible to operate it in a way that’s a little more power-efficient (for example, your device only connects periodically to send data, then goes back to sleep).

Bluetooth Low Energy (BLE) is a more energy-efficient wireless network protocol—if you’re not receiving data constantly, a single battery running BLE could last up to five years. However, compared to WiFi it is slower to transmit and is more limited in the amount of data it is capable of sending.

Both WiFi and Bluetooth are easy to connect in most cases, although WiFi does have some security challenges that may be difficult to overcome.

### 3. Low Power Wide Area Networks (LPWAN)

IoT devices that run on LPWANs send small packets of information infrequently and over long distances. This type of wireless network was developed in response to the early challenges of cellular connectivity. Proponents of LPWAN position it as longer-range than WiFi and Bluetooth, but using less power than cellular. Sigfox built the first LPWAN network in France and is considered the driving force behind its growth (despite the fact that [Sigfox never took off](https://www.iotacommunications.com/blog/sigfox-usa/) in the U.S.).

A well-known and commonly used IoT network protocol in this category is **LoRaWAN** (long range wireless area network), which runs on the [LoRa](https://www.link-labs.com/blog/what-is-lora) (long range) communication network. Advantages of LoRaWAN for IoT devices are its low power requirement (for long battery life) and relatively low-cost chipsets. Plus, under the right conditions, a single base station or gateway running on a long-range network is capable of providing service to a very large area—a few kilometers in dense urban areas and up to 15–30 kilometers in rural areas.

### 4. Mesh Networks

Mesh networks are best described by their connectivity configuration—how the components communicate with each other. In mesh networks, all the sensor nodes cooperate to distribute data amongst each other to reach the gateway. (A star topology, in contrast, is where all sensor nodes communicate to a central hub.)

**Zigbee** is one example of an IoT wireless network technology. Mesh networks are very short range and may require extra sensors throughout a building or the use of repeaters to get the coverage your application needs. Also, the nature of the way these networks communicate can result in high power consumption, especially if you need instant messaging, such as for a smart lighting application. (IoT applications that require only occasional information updates use less power.) However, mesh networks are also fairly robust, able to find the fastest and most reliable paths to send data, and easy to install, making them a popular choice for in-building use.

# Why is IoT so Important?

IoT illustrates the network of signal-enabled devices connected to the internet and sharing data with other devices over the internet for the purpose of accomplishing tasks. The IoT devices are installed with technologies capable of sending and receiving data. These “things” range from home gadgets, wearables, lightbulbs, speakers, cars, cellphones to complex networks of industrial machines.

Daniel Burrus, founder, and CEO of Burrus Research, Inc., defined IoT as follows:

“The Internet of Things is a combination of networked sensors and machines that enable machine-to-machine communications. Enabling technologies to include the internet, advanced cloud services, wired and wireless networks, and data-gathering sensors, making the system instantaneous anywhere, anytime.”

IoT is so important because the use of internet-connected devices has become mainstream, and companies in diverse industries are adopting this technology so as to be more efficient, productive, and competitive. [According to Statista](https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/), the installed base of active Internet of Things connected devices is forecast to reach 30.9 billion units by 2025.

“The IoT is a giant network of connected “things” (which also includes people). The relationship will be between people-people, people-things, and things-things.” writes Jacob Morgan, an author and futurist.

IoT has revolutionized how we live, interact with our environment and work in the 21st century. Today, almost everyone uses smart devices or makes use of a service that leverages the Internet of Things.

Over the years, there has been a gradual but steady improvement in internet technologies. Internet broadband is more readily available, signal-enabled devices are common, and the cost of creating networks of “things” is no longer as exorbitant as before. As a result, people now rely on IoT-enabled devices and environments for their day-to-day routines.

**IoT: Critical for Human Progression**

Applying Internet of Things in a particular country or cities is a big help imagine using unique centralized system that can minimize traffic, detect crime easily or even accident can be detected in a real time with a fast response from the respective supports. It can also help strengthen our economy through machines that works autonomously without needing human intervention. All the other support will greatly describe things that are made possible by the IoT. So Connected Home, Car, Mobile Phones, and other appliances and device that can be connected a network in some way. Think of if a world of urbanized and industrialized equipped with those technologies that is interconnected together can simply help us in all our day to day activity. Even doing a laundry while doing a multi tasking activity at work and at home can be done simultaneously using this type of technology. We need to decide how much in favor of this advancement will control us . IoT improves the quality of life.

IoT can also solve major problems like Security Management that use sim cards or chips that can act as a sensors such as clothing with biometric sensors, facial recognition, footprint sensors, and more to increase the security of homes, offices, and buildings so with these trends it can minimize security problems like robbery or even murder. Another good thing with the IoT is can also interconnect with hospital equipment for health emergencies for example a patient with a heart ailment connected directly to the hospital can easily be addressed and save lives even in Road Traffic can minimized congested path by using an IoT sim cards such as traffic lights, smartphones, cars, GPS devices, and cameras can be used to monitor traffic patterns , inform drivers of traffic situations can easily help our enforcers , government and the constituents . Another Thing is it can also help conserved energy consumption of home or work and in terms of agricultural matters it can also support by using a sensor that can detect the environmental problems. IoT is more sophisticated but it can lead to a better life and better business opportunities.

# Challenges in Internet of things (IoT)

The Internet of Things (IoT) has fast grown to be a large part of how human beings live, communicate and do business. All across the world, web-enabled devices are turning our global rights into a greater switched-on area to live in.  
There are various types of challenges in front of IoT.

**Security challenges in IoT :**

1. **Lack of encryption –**  
   Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security challenges.  
   These drives like the storage and processing capabilities that would be found on a traditional computer.  
   The result is an increase in attacks where hackers can easily manipulate the algorithms that were designed for protection.
2. **Insufficient testing and updating –**  
   With the increase in the number of IoT(internet of things) devices, IoT manufacturers are more eager to produce and deliver their device as fast as they can without giving security too much of although.  
   Most of these devices and IoT products do not get enough testing and updates and are prone to hackers and other security issues.
3. **Brute forcing and the risk of default passwords –**  
   Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute force.  
   Any company that uses factory default credentials on their devices is placing both their business and its assets and the customer and their valuable information at risk of being susceptible to a brute force attack.
4. **IoT Malware and ransomware –**  
   Increases with increase in devices.  
   Ransomware uses encryption to effectively lock out users from various devices and platforms and still use a user’s valuable data and info.  
   **Example –**  
   A hacker can hijack a computer camera and take pictures.  
   By using malware access points, the hackers can demand ransom to unlock the device and return the data.
5. **IoT botnet aiming at cryptocurrency –**  
   IoT botnet workers can manipulate data privacy, which could be massive risks for an open Crypto market. The exact value and creation of cryptocurrencies code face danger from mal-intentioned hackers.  
   The blockchain companies are trying to boost security. Blockchain technology itself is not particularly vulnerable, but the app development process is.

**Design challenge in IoT :**

1. **Battery life is a limitation –**  
   Issues in packaging and integration of small-sized chip with low weight and less power consumption. If you’ve been following the mobile space, you’ve likely see how every yr it looks like there’s no restriction in terms of display screen size. Take the upward thrust of ‘phablets’, for instance, which can be telephones nearly as huge as tablets. Although helpful, the bigger monitors aren’t always only for convenience, rather, instead, display screen sizes are growing to accommodate larger batteries. Computers have getting slimmer, but battery energy stays the same.
2. **Increased cost and time to market –**  
   Embedded systems are lightly constrained by cost.  
   The need originates to drive better approaches when designing the IoT devices in order to handle the cost modelling or cost optimally with digital electronic components.  
   Designers also need to solve the design time problem and bring the embedded device at the right time to the market.
3. **Security of the system –**  
   Systems have to be designed and implemented to be robust and reliable and have to be secure with cryptographic algorithms and security procedures.  
   It involves different approaches to secure all the components of embedded systems from prototype to deployment.

**Deployment challenges in IoT :**

1. **Connectivity –**  
   It is the foremost concern while connecting devices, applications and cloud platforms.  
   Connected devices that provide useful front and information are extremely valuable. But poor connectivity becomes a challenge where IoT sensors are required to monitor process data and supply information.
2. **Cross platform capability –**  
   IoT applications must be developed, keeping in mind the technological changes of the future.  
   Its development requires a balance of hardware and software functions.  
   It is a challenge for IoT application developers to ensure that the device and IoT platform drivers the best performance despite heavy device rates and fixings.
3. **Data collection and processing –**  
   In IoT development, data plays an important role. What is more critical here is the processing or usefulness of stored data.  
   Along with security and privacy, development teams need to ensure that they plan well for the way data is collected, stored or processed within an environment.
4. **Lack of skill set –**  
   All of the development challenges above can only be handled if there is a proper skilled resource working on the IoT application development.  
   The right talent will always get you past the major challenges and will be an important IoT application development asset.