

Top 10 IoT Challenges and Their Solutions

The Internet of Things has become one of the fastest emerging tech trends in the past few years, especially with the growing advancements in sensor technology concerning speed, sensitivity, and network coverage. Given the impact of COVID-19, companies that implemented IoT have started to perform exceedingly well.

As per a research report by Aruba, **83% of organizations that employ IoT technology have reported a significant increase in business efficiency.**¹ This also involves better visibility across the organization and easier expansion into other markets.

Along with generating insights and reducing operational costs, IoT is providing valuable services to customers. However, as IoT applications proliferate, industry leaders must address the engineering, technical, and implementation challenges from the early design phase to manufacturing outcomes.

In this article, we discuss the top 10 IoT challenges and solutions to overcome them. Addressing these challenges saves your organization from quality issues, project failures, budget overruns, and long completion times.

1. Compatibility and Integration.

Big vendors like Amazon (AWS IoT), Google (Brillo), Microsoft (Azure IoT), etc. have rapidly grown in the IoT market in the last few years. Each of these platforms promotes its own IoT infrastructure, proprietary protocols, and interfaces, making it extremely difficult for these solutions to work together seamlessly. Nevertheless, the necessity to maintain integration between IoT systems is growing.

In fact, a McKinsey analysis states that **40% of the potential benefits of IoT are obtained with the interoperability** between IoT systems.² Connecting devices, networking, and exchanging data is the integral component of IoT to work as one. Therefore, each IoT vendor must prepare its network for integration right from the start.

Here are the three compatibility and integration guidelines to follow when trying to fit in an IoT landscape.

1. The systems should be built within the universal framework to establish an open standard and promote global transparency for the industries.

2. [IoT devices](#) work much better with one another when developed with software-driven technologies instead of hardware-driven technologies. This allows adjustments for needed enhancements along the way.
3. The devices should maintain an open-sourced messaging protocol for effective data transfer even when different user applications are used.

2. Identifications and Authentication of Devices.

There are predicted to be 46 billion connected devices for the year 2021 alone, and by the end of the year, 31 billion devices will be installed worldwide.³ This myriad of devices is an invitation to [IoT security risks](#) and complexity. This is the very reason for strong authentication and identification of devices.

Authentication of IoT devices ensures that connected devices can be trusted to communicate securely with other devices as well as the backend infrastructure. Consequently, they need a unique identity of each IoT device to connect to a gateway or central server. This assists IT, system administrators, with tracking each device throughout its lifecycle, communicating with it securely, and preventing it from any harmful behavior.

3. Lack of IoT Integration.

Capturing the full potential of IoT requires integration to be at the epicenter of the project. [IoT integration](#) captures data from smart devices and moves it into business applications for better results. This helps to automate processes, support real-time monitoring, and apply analytics for insights.

However, in a Gartner Research Circle survey on IoT, ***companies implementing IoT ranked integration as one of their top three technical challenges.***⁴ A lack of proper integration could lead to abnormalities in functions, and the inefficiency to deliver value to the customers. It further involves three types of integration challenges related to device, data, and application & processes.

Research vice president at Gartner, Benoit Lheureux, advises limiting the scope, scale, and complexity of initial IoT projects. Utilize built-in IoT integration capabilities at first, and then extend those with best-of-breed integration solutions. To quote him,

*“This allows you to quickly capitalize on initial IoT projects, and then incrementally utilize new integration skills and technologies to address your expanding integration requirements later.”*⁵

4. Connectivity Challenges.

Wireless connectivity is highly complex, and so are the fast-evolving wireless standards. **The** global mobile satellite company, Inmarsat, revealed that **4% find connectivity issues one of the biggest challenges in IoT deployment.**⁶

Yet, mission-critical devices are expected to enable a seamless flow of data back and forth from a device, an infrastructure, the cloud, and applications. They have to work reliably even in the toughest environment without any failure.

The best way to respond to connectivity challenges is to incorporate highly flexible, configurable, and upgradeable designs. These designs should be able to be used in both manufacturing and R&D and meet future needs. This will help companies minimize measurement of the correlation issues across the different phases of development.

5. Data Security and Privacy Issues.

IoT security has already turned into a serious concern across prominent tech firms and federal agencies. Much of this stems from integrating devices into our environments without our knowledge.

Here are some of the alarming IoT statistics of 2021 that is further adding to the security challenge:

- IoT devices are typically attacked within five minutes of connecting to the internet. – [\(NETSCOUT Threat Intelligence Report\)](#)⁷
- 74% of global consumers worry about losing their civil rights because of IoT – [\(EIU\)](#)⁸
- 48% of businesses admit they are unable to detect IoT security breaches on their network. – [\(Gemalto\)](#)⁹

Concerns are no longer limited to the protection of our privacy and sensitive data. As IoT devices become ingrained in our lives, our very health and habits can become the target of a security attack.

To realize the true potential of IoT devices and save them from security breaches, companies need to develop policies that respect every individual's privacy. In addition, they need to plan, strategize, and implement these policies while fostering innovation in both technology and services.

6. No Testing or Updates.

Another critical way to resolve vulnerabilities is revisiting IoT devices for updates after deployment. Over-the-air (OTA) updates allow continuous improvements of devices even after they are in the hands of the consumers. An OTA update provides designers and developers with the means to implement new functionalities to their products. They can increase the product's scalability by adding new features and infrastructure after its launch.

Similarly, the software and operating systems of devices need a version update to function with improved performance. Simply put, updates keep the IoT devices robust and ensure data protection. They also reduce maintenance costs as an update can be deployed in phases.

Additionally, there are no limitations on the number of updates to be released in a year. Companies can work on the testing and then roll out a proven, ready-to-launch service. This not only helps solve security errors but gains time in the programming process and time to market to push sales.

7. Bandwidth Limitations.

Inadequate device bandwidth is one of the other challenges expected to increase this year. With the number of devices connecting to the IoT environment and the increase in data generation, the devices need a broader bandwidth to function and sustain development processes.

Low battery life, transmission range, capacity, and bandwidth can disrupt services such as data transmission, processing, and delivery. As the device load escalates and project activity volumes, enhanced management will allow a seamless transfer of data between devices and servers.

8. Intelligent Analytics.

Big data is the fuel of IoT devices. It helps them generate intelligent insights, make smarter decisions, and open doors to new opportunities. However, a flaw in the data could lead to false positives and false negatives, exposing algorithmic limitations. Based on a report by HubSpot, it is apparent that 44% of IoT stakeholders face difficulty in capturing data, and 30% confirm that their analytics capabilities are not strong and flexible.¹⁰

Other challenges include legacy systems' ability to analyze unstructured data and manage real-time insights, slow adoption of technology, and lack of skilled professionals. One way to

solve the IoT analytics challenges is to consider a possible IoT deployment. All that matters is how we convert data into insights, insights into actions, and actions into profit.

9. Operating Environment Concerns.

The physical environment where the smart device operates is a key factor in defining its functionality, and therefore, it is the key concern. IoT devices face several hindrances depending upon the operating environment in which they are set up or the locality and the region in which they are deployed.

The IoT systems can have uptime issues due to extreme temperature, overheating, rough handling, wear and tear due to wind, or simply due to pedestrian activities, not to mention device theft, poor connectivity, and delay in data transmissions. All these operating environment concerns deter IoT devices from delivering their full performance.

The best way to resolve operating challenges is to design an IoT device intended for the environment. Special design and testing guidelines must be followed to make sure installed devices function properly for the required operating lifetime.

10. Lack of IoT Device Management.

IoT device management provides administrative access to a deployed network of IoT devices and automated processes. This means enabling relevant tools, infrastructure, operational protocols, and workflows for more optimized performance of devices and systems. Organizations looking to adopt IoT solutions are often unaware of why they need IoT administration in the first place.

Monitoring these connected devices improves security and enhances their tasks such as data collection, data routing, and edge computing. The management sends notifications to the administrator who can securely access these devices, troubleshoot any error, update their firmware, and then reboot them – if needed, without individually logging in to each device. A holistic approach to managing smart devices ensures that IoT goals are met and achieved.

Wrapping Up

These were the top 10 IoT challenges revolving around adoption, growth, and mainly results. No doubt, IoT can add tremendous value to business operations, and connected products are the new normal. All you need is a deeper understanding of these challenges and knowing what key

steps should be considered. Using the right design, compliance, manufacturing, and security tools will help you build a strong IoT foundation that delivers on its promise.

What do you think?

Endnotes

1. <https://dataprot.net/statistics/iot-statistics/>
2. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>
3. <https://techjury.net/blog/how-many-iot-devices-are-there/#gref>
4. [IoT Integration Questions](#)
5. <https://www.gartner.com/smarterwithgartner/iot-integration-questions/>
6. <https://www.inmarsat.com/en/news/latest-news/enterprise/2017/connectivity-challenges-threaten-to-derail-logistics-sectors-iot-ambitions.html>
7. <https://findstack.com/internet-of-things-statistics/>
8. <https://findstack.com/internet-of-things-statistics/>
9. [https://www.sciencedirect.com/science/article/abs/pii/S1353485819300182#:~:text=Nearly%20half%20\(48%25\)%20of.being%20part%20of%20a%20botnet.](https://www.sciencedirect.com/science/article/abs/pii/S1353485819300182#:~:text=Nearly%20half%20(48%25)%20of.being%20part%20of%20a%20botnet.)
10. <https://blog.hubspot.com/marketing/internet-of-things-iot>