Top 6 Challenges of IoT Integration

TechRounder PDF Edition

Live article: https://www.techrounder.com/technology/top-6-challenges-of-iot-integration/

By Vipin PG | Published August 15, 2022 | Updated March 8, 2026 | Format: Article | 4 min read

In brief

IoT technology is gaining popularity for many reasons. For example, one of the many benefits of IoT technology is the ability to track cargo and play your favorite music in the shower using a waterproof Bluetooth speaker.

IoT technology is gaining popularity for many reasons. For example, one of the many benefits of IoT technology is the ability to track cargo and play your favorite music in the shower using a waterproof Bluetooth speaker.

Nonetheless, businesses face myriad challenges in IoT adoption to ensure the global device network is secure and functions efficiently.

These six factors pose severe concerns for the growth and development of the Internet of Things. Yet, they are the keys to achieving actual productivity and prosperity with these remarkable technologies.

Resource constraints

In this era of machine-generated and sensor-generated information, workloads' complexity, size, and attributes will reach massive scales. Unfortunately, today's edge network implementations are not large enough to handle incoming workloads. As a result, network limitations can cause performance issues and overload devices.

High IoT device density can lead to increased network congestion. In addition, it is impossible to detect the presence of certain IoT domains, which require everything to pass through an intelligent router or hub, making it difficult for humans to log, monitor, report, and perform other operations.

In operating environments that are resource-restained, an IoT device can face difficulties. However, there are special networking tools that a business can use that are specifically designed to work on the edge of the network.

Interoperability and compatibility among IoT systems

McKinsey market analysts estimate that between 40% and 60% percent of the total value depends on the interoperability among IoT systems. However, maintaining interoperability with different IoT system systems can be difficult due to the number of vendors, OEMs, service providers, and other parties involved.

IoT relies on sensors and networks. However, not all machines have the same advanced sensors or networking capabilities to share and communicate data. Additionally, legacy machines might not have the same sensors capable of providing the same results due to their different power consumption and security standards.

You could try adding external sensors to quicken the process, but this is difficult as it's hard to know which function or which part will communicate with the network.

IoT Regulations are not in place

Another feature of technological innovations is the slow pace with which government regulations catch up to current technology. Due to the rapid advancement in IoT technology, the government takes its time. As a result, it leaves businesses without the critical information they need to make decisions.

Because of weak IoT regulations, IoT still poses a significant security threat. And things may get worse as chances of major attacks are possible. Without enough rules and regulations, many disaster events may occur when cars and medical devices are connected to the internet.

IoT's quality control can prove challenging from a regulatory point of view. As a result, many experts call for robust and universal security standards for IoT technology.

Hardware compatibility issues

Data is captured primarily through sensors, PLCs, and other devices connected to IoT gateways, allowing data to be collected and sent to the cloud. Therefore, companies must carefully identify legacy equipment and hardware based on their business goals.

It becomes more challenging to implement IoT when there are legacy machines without the necessary PLCs and sensors. While adding external sensors can be done quickly, it is not 100% proof and will make it much more challenging. Therefore, it is essential to identify and resolve compatibility issues before IoT implementation.

Data security and privacy

IoT security has become a significant concern in prominent tech firms and federal agencies. Many of these concerns stem from the inextricable integration of devices within our environments.

Here are some alarming IoT statistics from 2021 which further add to security challenges:

IoT devices typically experience attacks five minutes after an internet connection, according to NETSCOUT Threat Intelligence.

74% of users worry they might lose their civil rights due to IoT, as reported by EIU.

48% admit they can't detect IoT security breaches on their network, reports Gemalto

Security concerns extend beyond the protection of sensitive data and privacy. As IoT devices become embedded in our daily lives, security attacks could also be directed at our health and routines.

To unlock the potential of IoT devices and protect them from security breaches by hackers, companies must develop privacy policies that ensure each individual is protected. Companies must plan, strategize, implement and monitor these policies while encouraging innovation in technology-related services.

Support and fragmentation

IoT devices will be a success if they can quickly identify, analyze, and correct problems. Unfortunately, the OEM warranties can be expensive, and IoT skills are scarce to manage billions of devices. SIs and ISPs share more responsibility for the performance of complex devices.

However, they also face a learning curve as well as skill shortages. In addition, companies have thousands of devices to support and millions of alerts daily, making it difficult for IT departments to detect, predict, and fix problems.

Conclusion

IoT workloads on large scales can prove challenging to manage. It is impossible to overcome the complexity and variability by hand or even with straightforward automation. Therefore, you should consider the advice above for IoT-driven workloads subject to these operational issues.

References

1. suse.com - products / k3s - https://www.suse.com/products/k3s/
2. finoit.com - blog / enterprise-challenges-in-iot - https://www.finoit.com/blog/enterprise-challenges-in-iot/