

Testing the Internet of Things – Are You Future Ready?

The mantra for testing an IoT Ecosystem to achieve success is to adapt well and avoid defects

- Sai Chintala, SVP-Enterprise Solutions, Cigniti Technologies

Imagine driving a car with an on-board chip to track your travel, process your toll gate, parking charges and traffic violations in addition to establishing connection to nearest emergency services in case you need road-side assistance. Now imagine the chip communicates with your smart phone through a mobile app that keeps you alert and updated. In machine-to-machine communication, data is communicated and the outcome is delivered to users in real-time. BTW, you actually need not imagine any of the above because these features are available in vehicles in many countries. This model is a classic example of the Internet of Things (IoT).

In layman's terms, IoT is a network of all components that leverage the Internet. Here are some interesting facts about IoT:

- According to Gartner, there will be over 26 billion devices on the Internet of Things by 2020.
- According to ABI Research, more than 30 billion devices will be wirelessly connected to the Internet of Things (Internet of Everything) by 2020.
- The market potential in this space is expected to be a 19 Trillion USD

Needless to say, testing IoT demands relevant domain expertise, infrastructure, and testing tools & techniques. The complex ecosystem of IoT and associated devices thrive on specialized testing.



Sai Chintala
SVP-Enterprise Solutions,
Cigniti Technologies

The Mantra for testing the IoT Ecosystem: Smart devices that do not hang

IoT involves billions of smart devices and the first step towards building a successful ecosystem is to ensure devices do not hang or crash. Today, leading smart devices have been found to present flaws long after adoption. In the context of IoT, even a minor defect can trigger a ripple effect and disrupt the businesses that leverage IoT.

There can be numerous reasons for these underlying flaws. To begin with, the device may not have been designed for the scale and possible variations of operations and use. In some cases, the inherent flaws in the device may snowball into major anomalies because of unintended or unexpected usage.

While malware has been attributed as one of the causes of device malfunction, a slowdown in functionality is typically attributed to the addition of a plethora of apps in application ecosystems where the smart devices interact with other components.

IoT is all about Scale: Testing needs to simulate realistic conditions

Devices in play are expected to accommodate traffic and environment estimated for peak usage. In simple words, the device has to sustain the functionality under a staggering array of permutations of expected and unexpected situations.

Security Testing of IoT

IoT essentially means more and more devices connected to other devices or networks/systems, which manage or monitor them. This trend demands new approaches and methods of security and testing procedures in order to protect both sides. The device usage side and the networks/systems side which monitor the device.

“According to Gartner, there will be over 26 billion devices on the Internet of Things by 2020”



Some key factors to be considered while testing IoT are:

1. Testing manufacturer's vulnerabilities
2. Check for security vulnerabilities due to diverse technologies in play
3. Application security and testing
4. Business integration testing
5. Governance for vendor and cross domain testing

IoT is all about Convergence – Testing needs to be Divergent

To validate the support for convergence, the testing strategy should consider a diverse matrix of technologies, devices, processes and scenarios that are applicable. The test strategy should include tools, techniques and resources with expertise over widely adopted devices, operating systems, networks and devices.

IoT is all about Speed – Testing needs to be Rapid

The configuration of the infrastructure, the development of the product/service/process and the UI are all streamlined to minimize the waiting period. Hence it's obvious that testing and associated test processes need to be agile with

rapid testing techniques, exploratory testing (repeatable) and overarching lean governance. Test reports and dashboards must be comprehensive and ought to be relayed in real-time.

IoT is all about Accuracy & Standardization – Testing needs to be apt & needs to ensure compliance

The ability to be precise in delivery is essential to succeed in the fast paced global economy, especially when each organization seems to having a different SDK / API which integrates with diverse components in the IT landscape.

The Testing (either an in-house team or your independent test service provider / partner) must include IoT specific test strategies, support SDLC under context, have access to on-demand test teams with requisite specializations. Success depends on the ability to leverage a dedicated infrastructure, cloud capabilities and a wide array of test tools (In-house, Open source, Commercial).

As enterprises leverage smart systems that 'sense' the environment and execute programmed actions, IoT driven testing is crucial to strengthen IT initiatives with security, intelligence and resilience.