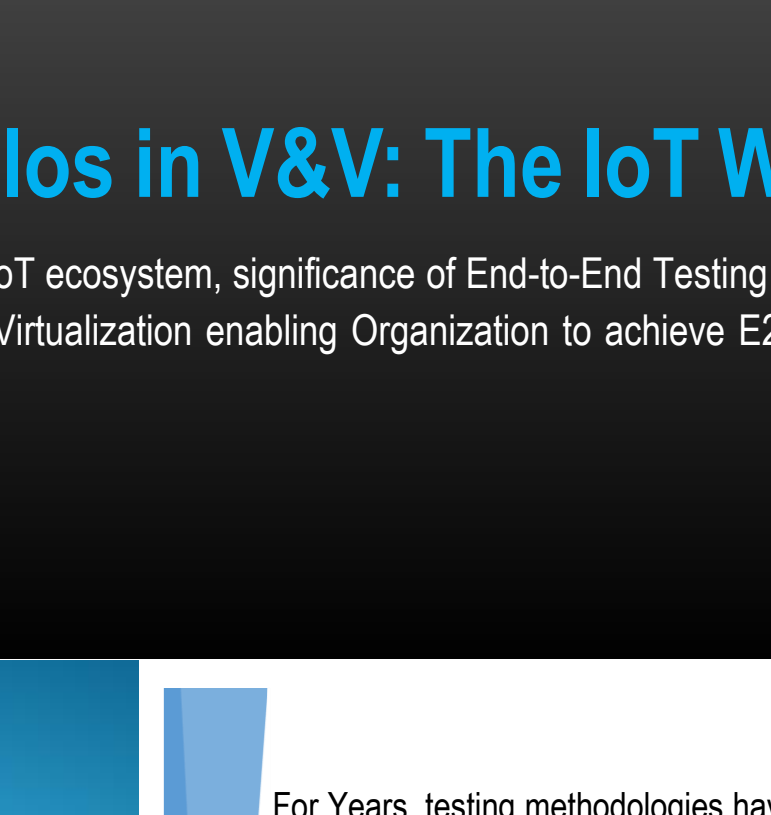


# Breaking the Silos in V&V: The IoT Way

A holistic view about the prevailing IoT ecosystem, significance of End-to-End Testing in this IoT era and the importance of Virtualization enabling Organization to achieve E2E Testing in an Agile way.



For Years, testing methodologies have focused on individual elements (Silos) of an organized, connected system. Testing is getting performed in isolation for front-end, back-end and field devices. The result – even though an individual element may work well, the chain of connected system may still appear to be broken due to flaws in integration points.

Because of this Silo'ed approach, the organizations in today's cut-throat competitive world are losing the advantage of providing an appealing experience at the moment of truth to the End User.

With IOT becoming Way of Life, the connected device technology is growing at a very fast pace, and soon would take over the basic human necessities. With this acknowledgement, it is imperative that much needed changes are brought to the testing methodologies, thereby removing the silos.

Executive Summary

Gamut of IoT Testing

Identified Key Silos

(Challenges/Gaps)

Introducing Virtualization

Continuous delivery – agile way

---

## Executive Summary

---

The **Internet of Things** is still in its infancy as a phenomenon. Despite this, its rate of expansion, adaptability, ingenuity and scope is startling. Companies are developing more and more ways for us to connect. Within the next five years, sensors will likely have permeated every aspect of our lives, from our refrigerators to our shoes. The world's IT infrastructure will be supporting a **trillion devices**, big and small.

**IoT is the next revolution**, which is swiftly transforming electronic products. In order to master and implement IoT, organizations need to work closely with mature vendors and overcome key hurdles such as:

- **Lack of consensus** on how to apply emerging standards and protocols to allow smart objects to connect and collaborate. It is difficult for organizations in integrating applications and devices that use multiple network technologies and operate on various networks.
- Testing IoT before launch can help **error detection** and avoid failure of IoT products.
- Capturing, Routing, Analyzing, and using the **insights of IoT data** in timely and relevant ways.
- **Privacy and security.** These two are major concerns in using IoT. As most of the devices have minimal human interference, there is a potential risk of security breaches or malfunctioning devices that may cause catastrophic failures in the IoT ecosystem. Continuous testing of devices is required to avoid security breaches and guard the systems from major damage from attacks.
- **Managing IoT complexities** and a large amount of data that sensors generate every millisecond. For implementing an efficient IoT, organizations require huge storage, strong data management, and analytical skills.

**Quality plays a key role in helping the IoT market succeed.** Testing IoT in addressing data management, security issues, and privacy concerns helps in offering trusted products. It is the backbone of the IoT ecosystem enablement.

In order to achieve a seamless integrated testing of IoT systems, **Virtualization** becomes need of the hour, not only to achieve end-to-end testing with integrated approach but also to optimize the test environment usage by lowering the infrastructure setup costs. Virtualization lets you simulate software components and hardware set-up and becomes helpful in testing holistically; eliminating dependencies on hardware devices, bringing hidden defect early and ropes in faster go to market of the product.

**This whitepaper aims to provide view on:**

**“Seamless Integration testing of Various IoT Components through Virtualization in an agile way”**

## Gamut of IoT Testing

Though multiple definitions exist for IoT, we define it as a network of physical objects that contains sensors or embedded technologies to interact with the internal or external environment and to take intelligent decisions. One of the most significant impacts of the IoT is that organizations are noticing a change in consumer behavior and expectations. This means frequent updates, upgrades, and a slick user experience.

Core components of IoT include three different components: things, communication and computing.

1. **Things:** Smart, connected products and other Things combine processors, sensors and software with connectivity.
2. **Communication Infrastructure:** Wired and wireless (Wi-Fi, 4G, Bluetooth, Zigbee) networks connect Things to the Internet and each other.
3. **Computing Infrastructure:** Data capture and analytics tools, and new business and software applications create new forms of value

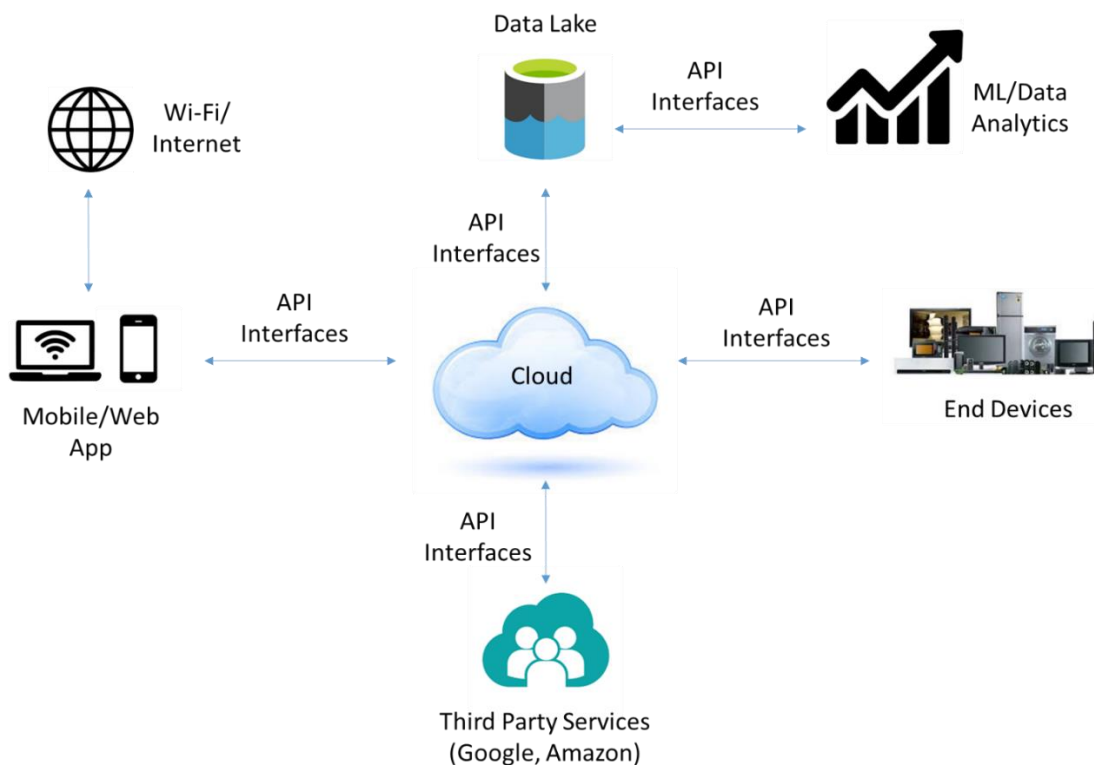


Figure 1: Impression of Typical IoT Ecosystem

Figure 1 depicts a typical IOT platform setup with various components contributing for the processing of business workflow. Each of the component is termed as Silo (Mobile, Cloud, Data Lake, Third party Services, End Devices, and Analytics etc.).

It is important that each of these Silos be tested independently as well as in an integrated manner to achieve the objective of E2E testing. A typical business case cannot be justified unless all the components (silos) are tested in an integrated way

## Identified Key Silos (Challenges/Gaps)

### KEY CHALLENGES

Gartner says, “more than 7.5 billion Internet of Things (IoT) devices will be in use in 2019, and that number will grow to more than 20 billion by 2026.”

Testing these devices will be one of the biggest challenges to face device manufacturers and integrators in the coming years.

### Diversified Combination of Hardware-Software

IoT platform includes variants of devices, which connect to servers (on-premises or in the cloud) over near real-time networks. Server infrastructure is built on multiple interconnected services and applications from different vendors. Testing such a complex, multivendor environment and simulating real-time situations is always a challenge.

### Complex Connectivity of Hardware-Software

Testing an IoT solution requires an integrated approach to test software and hardware in a dynamic environment. Testing inter-communication between hardware and software layers is a challenge. In addition to testing functionality of each of the components, it is important to test business scenarios involving interactions between hardware and software which is a complex process.

### Varied Communication Channels

IoT ecosystem already includes multiple components (Silos) and these Individual components further use varied communication protocols to interact with each other. Protocols such as Message Queuing Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP) and Constrained Application Protocol (CoAP) are others. This requires testing of varied combinations, which is not practical.

## **Availability of third party services**

Testers must have a strong test strategy, have a good understanding of the architecture, and ensure that the devices and software under test are always configured with the correct version. If the system depends on third-party services, tests may fail if that third-party service changes. If the third-party service is unavailable, one cannot complete testing of business functions which connects to the external services.

## **Fast-moving real-time data**

Connected IoT devices rely on fast communication. Varied connected devices sharing tons of data places a significant load on the network. Consequently, network status can have a significant effect on device performance. Smart devices often experience problems with network infrastructure, such as overburdened WiFi channels, unreliable network hardware, and slow or inconsistent Internet connections. Since these devices are mostly remotely connected, such situations will impact user experience.

## Virtualization – Connecting the Silos

These are some of the hard pressing challenges for IoT testing. Apart from these, the requirements to test end-to-end use cases to deliver great user experience in a live environment of IoT ecosystem shoots up the test infrastructure costs in the form of test labs.

Virtualization in such a scenario becomes helpful to optimize the test environment usage and lower setup costs. Virtualization lets you simulate software components and hardware set-up for testing applications (which are dependent on these components) when these components are not accessible for testing. Interestingly, it emulates the dependencies to help imitate the behavior and data interaction to derive the actual testing output. It is also one of the best ways to speed up testing and time-to-market.

When it comes to implementing virtualization, there are various components that play different roles. Below are the components of setting up a virtualized test environment for IoT platform.

### 1. Sensor Virtualization

Sensors can be virtualized by deploying

firmware on low cost USB sticks and using Raspberry Pi for computational needs. These virtualized sensors can then pass signals to the server through a gateway for end-to-end testing. Applications can be tested at length with all possible versions of virtualized hardware.

### 2. Service Virtualization

Virtualizing Cloud APIs, web services, backend, messaging protocols, IoT endpoints in the cloud, network services removes functional testing and integration testing service component dependencies and ensures total system testing coverage early in the development cycle rather than waiting for the end product. It also keeps the continuous integration/continuous delivery pipeline intact, virtualizing the constrained components.

### 3. Device Virtualization

Devices can be modelled by integrating simulated ECUs with HMIs or other displays. The virtualized device can be connected to cloud using standard protocols (MQTT, HTTPs, Web Sockets etc) and act as an actual device in field to test integrated workflows.

## Case in Point

A Typical use case where virtualization can aid is of smart city solution requiring hundreds of field video nodes to supply the right video input to the platform. Video node virtualization using Raspberry Pi and API virtualization to capture the video input ensures continuous testing and monitoring, improving the uptime.

Virtualization can also lend a path to analytics, where the volume of data collected increases significantly due to a number of iterations and scaling it enables. This data can then be analyzed and fed back to the various test scenarios.

Virtualization forms a major part of automating the regression test cases of an IoT system that takes as much as 30% of overall testing efforts, typically during any particular release. It helps in reducing risk, time, and cost and achieving scale. In addition, virtualization enables continuous testing of applications





## Continuous Delivery – An Agile Way

Continuous delivery and automation are the key to IoT success. Continuous delivery is possible because of the availability of virtualization for e2e test automation.

Agile methodologies and continuous delivery, on the other hand, are particularly well equipped for dealing with the demands of the connected device. With agile, frequent updates are essentially a requirement. This satisfies the end user's desire for a constantly updated device, the developer's need for a manageable development schedule, and the business requirements to respond quickly to market needs.

Agile methods also support the use of automating the software delivery pipeline: from software builds, testing, and all the way through deployments and product updates. This is useful in the world of connected devices for two reasons. First, it means that many tests (particularly those required for security purposes) can be automated, which leads to a reduced risk of security flaws and to a better, more stable end-product. Second, by automating releases of software updates and simplifying the operations that go into deployments, the developer's time is freed up to create new features to improve the product.