International Journal For Technological Research In Engineering *ISSN (Online): 2347 - 4718*
International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - November 2016)

INTERNET OF THINGS (IOT): CHALLENGES FOR QA

Priyanka Rani
Asst. Professor, Computer Science &Engg

Abstract: Internet of Things is one of the next buzz words in the market, after evolution of.com. It is basically network of interconnected physical devices with sensors, which has dedicated IP address for internet connection and which are capable of communicating with other internet enabled devices. There are many challenges that each of the stakeholders (investors, device manufacturers, app developers, app testers and users) are facing for products developed based on IoT. In this paper, we will try to highlight the challenges that the QA person faces while testing the IoT based application/product and what best QA practices can be followed for a quality delivery of the IoT based applications.

Keywords: IoT, Internet of Things, IoT testing, IoT functional testing, QA challenges in IoT

I. INTRODUCTION

WITHmaturity of ".com", Internet has reached to smartphones and tablets. IoT is trying to further extend this connectivity to normal household devices or beyond them to all physical devices which can work with sensors and can connect with internet with the help of a dedicated IP address.

As an example consider a scenario that your alarm clock has the features that in parallel to waking you up, it informs your brewer to make a coffee, inform your geyser to start heating water and inform your toaster to start baking your breads. This is just one of the example of implementation of IoT, it can span across various objects like security systems, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more.

On a large scale, it can have involvement in healthcare, defence, weather forecasting or each and every other field that you can ever imagine. These things give a clear picture that why this topic is so hot and interesting.

People generally think IoT as an independent technology, which in actual is not true. Its actual is a combination of following existing technologies:

- Embedded Systems: The hardware and software part for any IoT based application is manufactured and developed using the existing technology stack of embedded systems, with extra involvement of sensors and ability to connect to internet.
- Communication infrastructure: It is the set of protocols and technologies which enables two physical devices to exchange data..

II. CHALLENGES OF IOT

Like any other new technology, there are many challenges that make the viability and feasibility of IoT doubtful. As they are too many devices which are candidate for IoT implementation, but there is no single unified platform of implementation, following can be few of the common challenges that the manufacturers and developers will face for implementation of IoT based systems:

- Security and Privacy concerns: As IoT needs interconnection of physical devices, but due to availability of so many devices in the market (even new are coming day by day), which are candidate for IoT implementation, thinking of a common security policy is really a tough job. If the IoT devices are poorly secured, it is very easy for the cyber attackers to use it as an entry point for the network and cause harm to the whole network. This will obviously lead to loss of lot of personal data and in turn deteriorate trust of all users using those devices.
- Lack of Open standards: As this is just the initial phases of IoT development, IoT consist of lot of individual devices with their own specifications. At this stage it hardly matters, but with time and growth, demand for standardization will increase.
- IoT is complex: As the development for IoT based applications is in initial phases only, so it's more of R&D, that's going on at the moment and only experts are putting their hands in scratch developments.
- Need for cloud and connectivity: As communication between devices is the major protocol for any IoT based application, availability of internet is the basic need and demand.

Considering the above challenges for any of the IoT application, its puts extra responsibility on a quality person to validate all the feasible loop holes that can compromise with the quality of the deliverable. In the following topics we will cover various challenges that a tester can face for various types of testing areas (As shown in below fig.) for an IoT application and then precautions that can be taken to avoid those challenges.

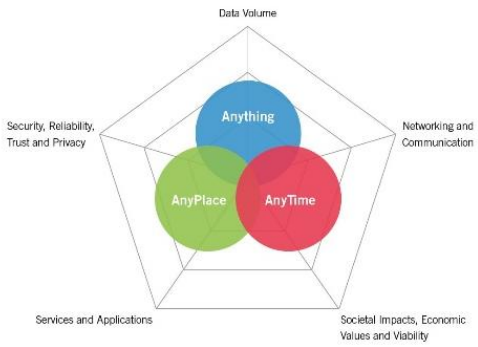

Figure 1 Testing areas impacted by IoT products

III. IOT: FUNCTIONAL TESTING CHALLENGES AND SOLUTIONS

Below are few of the major challenges that the QA involved in verification of IoT based applications will generally face while performing the functional testing:

- Too much money and time needed for a full-fledged environment setup.
- Various subcomponents and services needed for the product are owned by different vendors.
- Gathering of right test data from all dependent subsystems.
- Responsibility and ownership issues in case of segregated components.

A functional tester can take following steps to avoid these challenges and ensure for a quality deliverable:

- Service virtualization: Virtualizing the dependent services gives the flexibility of testing an independent component without worrying about the actual results provided by other dependent components. It will surely speedup things significantly by enabling testers to be less dependent on actual test infrastructure, evading the glitches of interconnectivity. So using service virtualization reduces dependency of availability of complete infrastructure for testing.
- Automating end to end: The stakes for effective test automation are high with the IoT because organizations are not only performing software testing but also vetting an entire ecosystem of connections, devices, and real-time scenarios. It demands for automating the end to end workflows, instead of just automating the software components.
- Real time operating systems: All the devices connected in an IoT system, depicts time based behaviors. So, it becomes very important to have validation of these components on actual real time operating systems, instead of normal operating systems.
- Crowdsourced testing: crowdsourced testing can be really helpful in case of IoT based system. Various folks can have access to independent components that are part of your IoT eco-system. Each one of them can be asked to test the whole system collaboratively. That will reduce overall burden of setting up of whole testing infrastructure at one place and will give more holistic and unbiased view when multiple folks are involved in validation of the system.

IV. IOT: SECURITY TESTING CHALLENGES AND SOLUTIONS

We're already hearing horror stories about car and home automation systems being hacked. In the rush to get these products to market, many manufacturers have forgotten about security testing. Few of the major challenges faced during security testing of IoT based systems are:

- No standard protocol of security for multiple devices involved in the IoT stack.
- Networks involved are third party and involve chance of vulnerability.
- Authentication missing between devices.
- Hacking of social authentication.

Following are few of the areas that need to be thoroughly validated for implementation of a secured IoT infrastructure:

- Encrypted data transfer: Data transfer to the backend and between devices should always be in encrypted form. This should be part of basic validation that no unencrypted data should flow through the network.
- Usage of legitimate devices: Only legitimate devices should be allowed to be part of the network for IoT based products. A proper validation should be done to ensure that not any of the devices come and become part of network, there should be formalized way to first ensure authentication of the device and then only the same should be allowed to be part of the network.
- Ensuring no data loss during network interruption: If the network connection breaks during communication, it should be ensured that the data is not lost and is being saved in some cloud service, which can be gathered later once the network services resumes for the devices.
- Coverage for security testing of all independent components: IoT security testing must be run for common Web application vulnerabilities such as cross-site scripting and cross-site request forgery, make use of public encryption algorithms when possible, and try to make the most out of firewall protection as certain devices may not support it. On the software side, make sure patches and updates can be digitally signed to prove legitimacy to the device. Devices should not assume all patching attempts are legitimate; an apparent patch could be a piece of malicious code.

V. IOT: PERFORMANCE TESTING CHALLENGES AND SOLUTIONS

Below are few of the major challenges that QA will face while planning for performance testing of IoT based applications/products:

- One of the biggest challenges that testers will face is the involvement of all types of devices .Eg, one IoT product can have involvement of smartphone, AC, refrigerator and many more devices. Now a performance and load tester may be familiar with recording traffic from web browsers, mobile devices, etc., but testing new objects that do not allow a change of settings might prove inconvenient.
- Understanding exact impact of factors such as latency, packet loss, network bandwidth, load, etc.
- Usage conditions and network availability can also be one of the factors impacting performance of the

product.

As a performance QA engineer, a tester can use below methodologies to eliminate above risks:

- Real world testing instead of CPU testing: A careful test plan should be created by properly examining the factors that how the devices are used in real world. This can certainly have an impact on how the device should be performance tested and monitored. For example, a fitness tracker band needs to accurately measure input from things like the wearer's pulse, range of motion, and movement speed which are all things that are difficult to simulate without actually performing real world use tests.
- Verification at various network speeds: As communication is the major part for any IoT based product, so it needs a proper validation of all the subcomponents, how they are behaving at various network speeds and at least should ensure that there shouldn't be any packet loss, no matter how low is the network speed.
- Backend load and performance testing: As a performance QA, primary responsibility should be to validate that backend is able to handle the load as stimulated with no degradation in performance. A string backend will ensure that all frontend devices are able to handle all communication properly.
- High volume and growth explosion verification: QA engineers can use virtualization to run performance testing on the servers to see how well they hold up under pressure. IoT developers need to be aware of thresholds where the infrastructure will start demonstrating a degraded user experience.

VI. IOT: USABILITY TESTING CHALLENGES AND SOLUTIONS

As there are multiple devices involved in any of the IoT based product, so usability can be one of the major issues for any of the IoT based product. To ensure that the product is simple enough to use, following testing techniques can be used before actually launching the product in market:

- Test by Customer: Beta testing can be very useful in case of IoT based products, as users will provide an early feedback about usability and interfaces of product. Floating down the product to a small subset of actual users, will really help is providing some early and useful feedback that can be incorporated before delivering the actual product to a larger domain of users.
- Testing the human experience:The test approach for Human Experience testing involves not only "field" testing, but testing in the real world of the user. The most effective way to design human experience tests is using human computer interaction design principles. By developing "Personas", we delve into the users' personalities and characteristics and we begin to understand their expectations of the device. Then we create "User Value Stories" to test the ways in which the human user will achieve value from the device.

VII. CONCLUSION

IoT being a new field have lot of challenges from manufacturers to developers to testers. From a test perspective, it possesses lots of challenges and responsibilities for making sure of a quality deliverable. Due to involvement of various types of devices and networks, the overall scope of testing has grown a lot in case of IoT devices. So, an IoT tester need to ensure that he/she use the methodologies for various types of testing as mentioned in this white paper, for making sure of a quality deliverable within stipulated time frame.

REFERENCES

[1] http://internetofthingswiki.com/internet-of-things-definition/
[2] http://www.datamation.com/data-center/the-internet-of-things-7-challenges.html
[3] http://internetofthingswiki.com/internet-of-things-definition/
[4] http://www.ti.com/tool/cc2650stk#video
[5] http://www.ti.com/ww/en/internet_of_things/iot-challenges.html
[6] http://nordicapis.com/automated-testing-for-the-internet-of-things/
[7] https://devops.com/2015/02/24/functional-testing-iot/
[8] https://dzone.com/articles/update-your-testing-strategy-for-the-iot-with-auto
[9] http://www.softwaretestingclass.com/internet-of-things-iot-testing-challenges-applications-and-sample-test-cases/
[10] http://internetofthingsagenda.techtarget.com/feature/IoT-security-testing-Cover-all-your-bases
[11] http://www.gallop.net/blog/performance-testing-for-internet-of-things-challenges/

