International Journal of Engineering Technology and Management Sciences[IJETMS]

Website: ijetms.in Issue:1, Volume No.1, November-2017

Testing IoT: Novel Perspectives, Challenges, Future Work

Manas Kumar Yogi[1], K. Mahesh Kumar[2]

[1]*Asst. Professor ,CSE Dept. Pragati Engineering College, Surampalem ,A.P., India*
[2]*B.Tech III Year Student, CSE Dept. Pragati Engineering College, Surampalem ,A.P., India*

[1]manas.yogi@gmail.com
[2] maheshkumarkorukonda@gmail.com

***Abstract*— Our paper exposes testing aspects in IoT environment which are to be considered with any laxity. Our paper brings out the challenges faced when testing IoT based devices and the inherent IoT network itself. We concentrate on test cases in each aspect of the IOT network and which metrics can be applied to verify the functional aspect and also benchmark a value to indicate acceptable quality of service. We use a IoT testing framework to show which parameters effect the testing process and up to what extent they are useful. We also present in our work a scenario which illustrates how companies in future are gearing up to face the challenges in this field without compromising on the delivery of service quality thereby including a fair degree of justice in customers who use smart services for the betterment of their life.**

***Keywords*— IoT, Smart, M2M, Testing, MQTT**

INTRODUCTION

While we use phones, often termed as smartphones now-a-days, all the time they essentially happen to be just personal computers that all equip well in our hand and in our pockets. Our smartphones just connect us to the internet and with the people while the Internet of Things connect things to people through internet.

The term Internet of Things was coined in 1999 by Kevin Ashton, who is the co-founder of the Auto-ID centre at MIT. IoT encompasses a world in which devices are connected over a network with sensors enabling them to connect with each other and barter information.

These consists of your thermostat, lights in your home, your car and your washing machine too. As we know, all the above mentioned concepts existed way before the evolvement of internet but now we are adding internet to them. Nowadays people use smart watches which is a humongous example of IoT. These watches not only measure the length of our morning walk or run but also keep a track of our heartbeat, our location via GPS and now they even make calls. The experience with watch has gone to gross new level making our lives easier. The data collected from the smart watch can be used to track the location in case of emergency and measure heart beat which can be used for analysis while diagnosing during a cardiac failure.

Initially, the cost of these devices used to be enormous but now they have become cheaper so these types of devices can be used even by normal people. Now IoT devices are widespread and every household is having at least one IoT device. IoT is becoming something on which the world relies to drive. These optimize the performance and increase our productivity yet it still needs to be tested.

I. NEED OF IOT

Efficient Machine to Machine (M2M) correspondence which results in less human intervention.

Development of multiple protocols like Internet Protocol version 6 (IPv6), Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP) (D2S), Data Distribution Service(DDS) (D2D) etc which can used per requirement of the system. So, a far reaching conglomeration of technologies make IoT and productivity a lot easier and efficient.

Different technologies can be integrated into IoT such as Nano technology, embedded systems cloud computing etc which results in development of newer technologies.

II. Implicational Diversifications of IoT

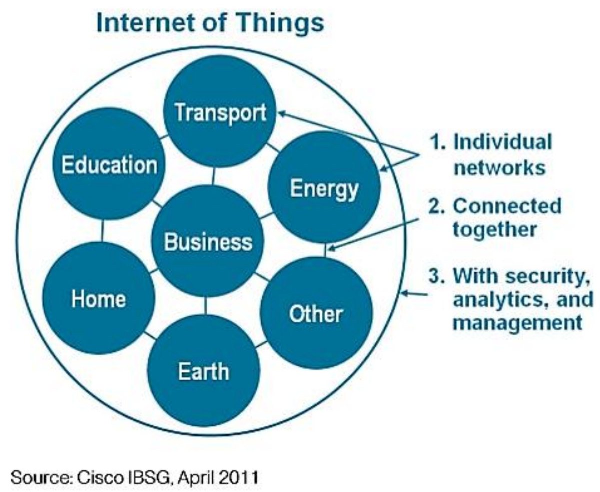

Fig.1: Implicational diversifications of IoT

III. Estimation of devices and Need for testing

Hans Vestburg, former CEO of Ericsson, stated in 2010 that there will be 50 billion connections by 2020. Cisco predicted that there will be 50 billion IoT devices connected by 2020 which is more than the world population. But the predictions have arguably gone down as of now. As of now the current count of IoT devices is around 6.4 billion which does not include smartphones, tablets and computers. With all of those included the figure goes to 17.6 billion according to IHS. Now Ericsson says that there will be 28 billion devices by 2021. IHS market estimates them to be 30.7 billion while Gartner predicts 20.8 billion excluding smartphones, tablets and computers.

However, the figures may vary, those still are more than the entire population on this planet. This raises the very need for testing as all this technology is new and not mastered yet. With these many devices there is a huge room for failures and they need to be tested until they meet the standards.

Nick Jones, vice president at Gartner said, "The IoT demands an extensive range of new technologies and skills that many organizations have yet to master. A recurring theme in the IoT space is the immaturity of technologies and services and of the vendors providing them. Architecting for this immaturity and managing the risk it creates will be a key challenge for organizations exploiting the IoT. In many technology areas, lack of skills will also pose significant challenges."

The need of IoT testing is clearly laid down in the above statement by Nick Jones. Even though IoT have a positive and bold effect on making out lives easier and efficient, it still requires companies offering the IoT services to pay even more attention to various elements like designing, security, risk and the architecture of their products.

On an yearly basis, every year enterprises and organisations all over the world are migrating towards IoT and developing, changing their products into IoT-enabled devices and rolling out into the market. With this focus of enterprises towards IoT and IoT-enabled products, there is a vast rise in the products related to healthcare, household, cars, utilities etc.

IV. Architectural Aspects of IoT

Following are the most used technologies in IoT:

1) *RFID:* RFID denotes Radio-frequency identification. It uses electromagnetic fields to identify the create and identify tags and has a great range when connected to a power source.
2) *NFC*: NFC is the short form for Near Field Communication. It enables two-way interaction between electronic devices mostly smartphones. It is mostly used for doing contactless payment transactions such as Apple pay, Google pay and debit at PoS transactions. The range of NFC is very low just a few millimetres.
3) *Bluetooth*: When short range communications are enough for the requirement of the system, Bluetooth comes into effect. This is used in wireless audio equipment and wearable devices.
4) *Z-Wave*: This consumes low power radio. This has low latency with date rates upto only 100kb/s and uses low frequency radio signals. Mostly used in home automation and is highly interoperable.
5) *Wi-Fi*: Wi-Fi stands for Wireless Fidelity. When it comes to IoT, the most used choice is Wi-Fi. It helps in transferring data, files and messages easily when on a Local network (LAN).

V. IoT Test Approaches

Following include some of the things to be considered while testing an IoT system. This includes an individual product or an entire system to be tested.

A. Usability

The usability of the IoT device is tested here. For example, the healthcare tracking devices should be portable so that it can transferred from one place to another. The device should be designed in a way that it should show warnings and error messages along with the notifications regarding healthcare.

B. Security

IoT is all based on data. The devices are driven by the data that is acquired by them.

This data is sent to other devices that connected on that particular IoT network. While transferring the data, there is a chance of it being hacked and accessed. During testing, data need to be checked whether it is encrypted i.e., when it gets transferred from one device to another device. If there is interface for accessing, then it should have password for authorizing it.

C. Connectivity

IoT is all a matter of connected devices. Connectivity is vital for transferring the data. Some organizations entirely depend on IoT, there the connection should be seamless without any interruption or else it will cause a huge loss to the organization. So testing should be done that the connection is always good and running. Also, we cannot be always sure that the connection is up and active. So testing also be done such that the device should prompt the user that the connection is offline so required action will be taken by user. Even though there is a connection failure or system failure data should not be lost. Even during offline mode there has to be some sort of technique that stores all the data generated by the system.

D. Performance

When we talk about performance, we need to look at scalability. The system must perform good under any circumstance with any amount of load. Consider a hospital management system which generally works with an average of 20 patients daily. All the patient data is transferred in the hospital and synced by various machines. Even if the number of patients increases to 50 the system should not fail and must be reliable for all the 50 patients. There should not be any errors and lags in transferring and syncing the data in the hospital. Tests should be done in a way that the system operates under a predictable amount of load at least.

E. Compatibility Testing

When we look at the architecture of an IoT system, we have different types of devices. Each device will have a different type of connection protocol, different version, different operating system also probably a different generation all together. Tests must be done that they are compatible with each other also are compatible with other similar types of devices in the market which is helpful in case of a failure for replacement. For example, different versions of Bluetooth such as 4.0 as currently 5.0.

F. Pilot testing

When it comes to IoT, pilot testing is thing to do for sure. Testing in lab gives assurance that the product works well. But we can’t be sure of that really as we can’t fully simulate the real-world scenarios in lab. Hence, the system or product is given to a limited number of users to use it in the real world. The feedback from these users help in making changes if required makes sure that out product works fine. This is pilot testing which is very essential for IoT systems/products.

G. Regulatory testing

Not every product we develop enters the market. The product needs to satisfy all the administrative needs as specified by the authorities. Tests must be done such that the product is compliant with all specifications set the regulatory body. By doing these tests we can be confident that our product will be certified and released.

H. Upgrade testing

Technology evolves, so is IoT. When we want better performance or efficiency, we upgrade specific parts of the system or the entire system. So regression testing should be done to handle the issues of upgrading issues.

VI. M2M INTERACTIONS

IoT is a system of connected devices. Machines communicate and work together without human involvement. So, we need to test Machine-to-Machine interactions as reports say that there will be billions of Machines in the very near future. These machines automate the work, increase efficiency and are more reliable than human also more economically viable. M2M interactions work as the heart of IoT. Given the growth of IoT devices and M2M interactions, every year human involvement is getting lesser. This causes the M2M interactions to be tested thoroughly.

A. Test environment management

Simulating the test environment including various devices of different types with different applications is not that easy. This difficulty increases with raise of the number of devices. So, having the appropriate test environment is a challenge for test engineers.

B. Test data management

All the difficulty in testing Machine to Machine interactions lies in testing the data and its management. Different devices will generate different types of data within the same environment which may be different behaviourally. Since the devices communicate making this data compatible and having it right is the important thing for testers.

C. Compatibility testing

As already mentioned above, a complex IoT architecture involves different devices, operating systems, messaging protocols, versions etc. So, making sure that the communication is done correctly despite these differences is key to the working of the system.

D. Performance testing

Performance testing is highly essential for organizations based on IoT. Since any delay in response time of Machine to Machine interactions can cause a loss to the organization. The lower the response time, the better the performance. Also including response time of the machine, there are other factors like memory usage, power usage and endurance. During times of failure disaster recovery is also vital for the success of the organization.

E. Accessibility testing

As more devices grow around us, accessibility testing grows. Every new system related to our system need to communicate with our system. For this our system need to be accessible only with required data with no issues for compatibility or accessing.

F. Security testing

Security is an important part of testing as data flows from one machine to another machine which needs to be protected. Also our IoT application need to secured with passwords and firewalls to prevented unauthorized access to data. Data which transfers from one device to another device need to be encrypted so that it won't be read by other devices.

G. Regulatory compliance testing

For every IoT device we use there are certain standards set by regulation authorities across the world. We need to rigorous testing of those standards and protocols so that our device will be compliant to those specifications.

These are a few test types which are basic and important. But depending upon the system or IoT product we need many other types of tests which assure the end to end functionality of the system.

Testing is generally done by test engineers but testing actually can be automated. Though we can't fully automate the testing, we can at least automatedly test some part of the system which reduces human effort and is more reliable. Following are some tools for IoT testing.

VII. IoT Testing Tools:

A. Software

1) Wireshark**:** Wireshark is a network analyser. It is open source and free. It is used for analysis and troubleshooting of network. It is cross platform and can be used on windows. BSD, Linux, macOS. It has GUI interface and command line interface(TShark). This utility can be used in testing packets in network of the IoT system.
2) Tcpdump**:** This is also a network analyser just like Wireshark but unlike Wireshark, tcpdump doesn't has a GUI. It runs on a command line interface. This is also a free software for analysing the network for displaying the packets received and transmitted over the network. It works on most operating systems.

B. *Hardware*

1) JTAG Dongle**:** JTAG name comes from Joint Test Action Group. This is an industry standard. This is used for testing and checking PCBs (Printed Circuit Board). It is now used for debugging embedded systems. Since JTAG accesses the blocks of ICs of a system, it is used for testing IoT systems.
2) DSO (Digital Storage Oscilloscope)**:** DSO is used to measure power supply and signals digitally unlike analog oscilloscope which uses analog techniques. It stores the received signal and then displays the it. Any issues in power supply and integrity of signal can be checked using DSO.
3) Software Defined Radio**:** This emulates components of hardware used in the system using software on computer. Signal processing which is typically done by hardware can be done using Software Defined Radio.

VIII. Challenges in IoT testing:

Testing is not easy and IoT testing is way more difficult. We have various problems in IoT testing some of which are discussed below.

1) Hardware-Software Mesh:

IoT contains physical hardware devices like sensors, transistors, ICs etc and also various software components like user interfaces, firewalls, logins etc. Both play a vital role in the functioning of the system. We can test the hardware and software separately, but they in a real time environment they always depend each other. So testing only the functionality is not enough. So it is a difficult thing to test unlike a traditional hardware/software system. Many of the issues we encounter in real world cannot be simulated during testing phase.

a) Device Interaction module:

Since IoT contains a lot of devices of various architectures, it is difficult to integrate one device with each other having different configurations. There need to be communication between these devices which is mandatory for working of the system. But to make the data transfer (communication) happen as intended they need to be integrated in a way that there won't be any compatibility issues, security issues and upgrade issues. Also these devices need to be backward compatible.

b) Real-time data testing:

For correct working of any IoT system it needs to be pilot tested which is compulsory for rectifying the errors if encountered any. But setting the system in the pilot is very difficult. And it gets difficult to get the required data which causes the failure as we exactly can't know how the failure occurred. So real time data testing comes as a big challenge to the testers.

c) UI:

IoT devices are spread across every platform both in computers and mobile devices. For any IoT device/system there will be a separate User Interface on various Operating Systems like Windows, Linux, Android, ios, Raspberry pi etc. We can test the UI on a specific device but we cannot test all the devices that are available out there in the world. But the fact is we can't omit the possibility that a specific device is not used by a user in the real world. So the challenge is testing the UI on various devices which is not possible and tough to overcome.

d) Network availability:

In IoT, all the devices communicate by transferring data over a network. The communication need to be faster for good performance. IoT produces results only when the network is available. Depending upon the speed of the network, it should work even if the speed of network is slow or worse. So the system need to tested by simulating various network connection speeds. We can test this scenario by used virtual network simulators by varying the connectivity, load and stability. However, the real world connectivity environment is always a new scenario which is the challenge for testing.

IX. CASE STUDY

Infosys, the world leader in software services, has developed a comprehensive framework for validation of IOT applications. Testing can be performed easily with this solution across various IOT protocols, hardware platforms. It can test the functionality, load, security of any IOT application. As claimed by the Infosys service managers, this framework can save 80-90% tool cost and reduce the go-to-market time by 20% after validation is performed.

We simulated few IOT jobs on a popular framework called as IOTify. We simulated 8 jobs varying no. of clients up to 100 clients maximum. MQTT protocol was used and we also tuned the repeat interval between the clients for each message. What we observe from this experiment is that even with 5% packet drop rate and 10% packet drop rate, the average time to deliver per message decreased from 0.289ms to 0.240ms keeping other network parameters constant. So, we can easily infer that in IOT environment, packet drop rate should be minimum and to test this aspect test cases at monitoring packet drop rate should be developed with great care. Also, aspect to be tested if reordering of packets should not consume much time for acceptable QoS and also duplication of packets should not happen. If duplicate packets arrive at clients, memory space at such clients decrease thereby slowing down the processing ability at such clients.

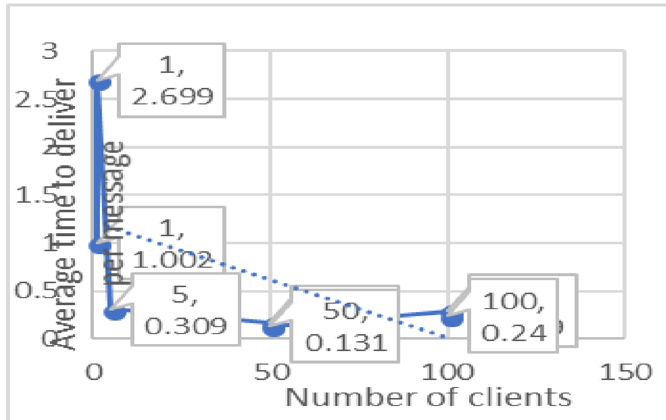

Fig.**2.** Performance of IoT framework with no. of clients versus Average time per message

From above graph, we observe that for same no. of clients the average time/message decreases, if the interval time decreases and repeat frequency increases. So, while testing IOT clients the above case can be tested for expected positive results. In case such result is not obtained, we can say the IOT clients have failed against expected result and suitable corrections can be made. Yet another observation is that keeping no. of clients, repeat frequency interval of messages same, the average time/message is almost same irrespective of packet drop rate.

X. CONCLUSION

Due to heavy competition in IOT market companies are concentrating more on performance, cost issues rather than working on security issues. It is not the case that such companies are totally disregarding security, privacy concerns but they still have a scope to improve in this regard. This paper is a sincere attempt to present where in IOT network testing activities have to be focused and which factors are to be considered while testing. Our paper discusses the very purpose of IOT testing and represents the approaches which can be effectively applied to test the IOT environment. All the approaches take into account the cost effectiveness of the IOT system because users always prefer a low-cost as well as robust system to work on. We conclude this paper by advocating the principle of fair usage of IOT without hindering the technological advancements in IOT domain.

References

1. Eriksson, J., Osterlind, F., Finne, N., Tsiftes, ¨ N., Dunkels, A., Voigt, T., Sauter, R., and Marron, P. J. ´ COOJA/MSPSim: Interoperability testing for wireless sensor networks. In Proc. Simutools (2009), ICST, pp. 27:1–27:7.

2. Okola, M., and Whitehouse, K. Unit testing for wireless sensor networks. In Proceedings of the 2010 ICSE Workshop on Software Engineering for Sensor Network Applications (2010), SESENA '10, ACM, pp. 38–43.

3. Quereilhac, A., Lacage, M., Freire, C., Turletti, T., and Dabbous, W. NEPI: An integration framework for network experimentation. In Proc. of SoftCOM (2011), pp. 1–5.
4. Rakotoarivelo, T., Ott, M., Jourjon, G., and Seskar, I. Omf: A Control and Management Framework for Networking Testbeds. SIGOPS Oper. Syst. Rev. 43, 4 (Jan. 2010), 54–59.
5. Amazon Mechanical Turk, Available: www.mturk.com/mturk/welcome .
6. Constantinos Marios Angelopoulos, et al., "Characteristic Utilities, Join Policies and Efficient Incentives in Mobile Crowdsensing Systems", Wireless Days, Rio de Janeiro, 2014
7. Sotiris Nikoletseas, et al., "Decentralizing and Adding Portability to an IoT Test-bed through Smartphones", 2nd International Workshop on Internet of Things – Ideas and Perspectives, CA USA, (IoTIP 2014)