Challenges of Quality Assurance in IoT

Mehreen Sirshar
Department of Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
msirshar@gmail.com

Dur e Shahwar Zahra Tallat
Department of Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
dszt37@gmail.com

Maryam Khan
Department of Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
maryamkhan.fjwu@gmail.com

Asma Arshad
Department of Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
noorturk16@gmail.com

***Abstract*—Immense challenges arise in the Quality Assurance area due to contemporary development in Internet of Things (IoT) technology. Current issues are mainly related to test coverage, test diversity, IoT Stability, Use of Cellular Networks in IoTs, IoT Devices updates, Security, Data Integration, and interoperability. In this paper, we present all those issues with suggestions for tackling those issues.**

***Index Terms*—Internet of Things(IoTs); Challenges; Test Strategies; Quality Assurance; Suggestion; Interoperability; Security**

I. Introduction

Over the last two decades, solutions related to Internet of Things has begin to come out from basics to advanced level of solutions, which can be seen in our everyday lives. These advancement also brings many challenges. For example insufficient standardization and updation, security and privacy concerns, testing, Data integration and interoperability.
This paper mainly focuses on quality assurance and different testing procedures in Internet of Things. Also the main challenges faced along with the suggestions. This paper identifies the areas considered relevant by us for further research

II. Literature Review

With the IOTs, the physical objects are integrated into the virtual entities. IOTs is the troublesome technological innovation, for the future information technology integration and the optimization. It is the implementation which serves as a core of the industrial growth. It helps to provides linkage of the things in a real world with the people, through the internet and brings process data in the form of information for making decision. This growing technology helped people to create Smart home systems, Hybrid cars, fascinating Smart wearables and healthcare system. It joins and connects billions of the devices through the internet. The rise in the Internet-connected structures or systems and accompanying, increase in the Internetwork attack surface can be easily represented by the several tiers of the expanded surface complexity. However, also growing technologies that do not need human interaction and capability to produce and also consume network information. By 2020, there are going to be over trillion these systems. The smart, and these connected objects will populate IOTs that will interact with the both humans and human environment by delivering all kind of information. The paper attempts to contribute to literature that addresses the primary IOT problems with impact on quality assurance.

III. Primary IOT problems with impact on quality assurance

A very large number of studies have been performed concerning IoT problems and issues. In the following analysis section, we have identified many distinctive issues of IoT solutions. Table 1 identifies issues along with their direct effect they put on testing and also on the quality assurance.

A. Test Coverage

Because of fragmentation, or the multiplicity of the smartphone market based on brand, operating system, versions of the operating system, size of the screen, model ,and other elements, its a challenge to develop an IoT that can operate perfectly across incalculable devices [1].

Suggestion

So, it is beneficial to test IoTs across numerous devices to confirm their worth, quality and reveal bugs that can hamper functions. For companies without a relevant testing devices, the efficiency of a quality assurance campaign can be watered down by an inadequate test coverage.

B. Test Diversity

The testing of an IoT involves more than just testing an actual device. It also covers, the testing the mobile application on variety of devices to detect bugs that can lead to damage, upset and ruin brand image, and affects consumer confidence [2].

Suggestion

Some testing techniques can focus on determining the key functions, others are better to assess other important features like UX and accessibility. So, without the right testing expertise, it is very difficult to make plan, proper design, and execute test.So, we should have a good testing proficient workforce.

C. IoT Stability

The IOT can connect to other devices via Bluetooth or a WIFI network. Connecting or staying connected to other devices or network is so complex and sometimes difficult. Connection issues can make an IoT useless if it is prevented from sharing data [3].

Suggestion

To overcome these kind of difficulties, it is beneficial to test ability of internet of things to connect to other devices. The type of connection in a test should reflect the all abilities of an IoT device. Furthermore, testing an IOT should be accompanied over a huge time and also with a diverse devices with different bluetooths and WIFI configurations.

D. Use of Cellular Networks in IoTs

Use of the cellular gateway in order to connect to IoT devices sounds awesome, but its users are unable to get the phone reception at some of the remote areas. The construction of the infrastructure can be vey expensive [4].

Suggestion

Even though the LTE-M and LTE-NB are using the existing cellular towers, but still these low-powered, and the wide-area networks provides larger coverage. Even when user is not receiving stronger signals for the voice calls or a 4G-LTE data, they can even then access LTE-M.

E. IoT Devices updates

Another problem is less possibility to configure and update several kinds of IoT devices. It can be due to the lower production costs and budget or the energy consumption problems. It's not plausible for updating certain kinds of different devices, which is also standard for the sensor networks. [5].

Suggestion

All these variables needs testing, that certainly arises costs of test-bed and the number of variables to test.

F. Use of proprietary protocols in IoTs

Comparison with some and common website related internet solutions, the testing of IoT solution is much more specific from other perspective. While testing website systems, we typically presume, the physical layers such as the hardware, the networking protocols, the OS, and the application servers, are tested by suppliers. So, we just focus on the system testing specifically on the integration and on application levels. [6].

Suggestion

In the IoT, the condition is totally dissimilar. There are already much more variety of the conventional standard protocols as compared to the web solutions. However, a many different protocols are being used in present internet of things [7]. So, testing of IoT essential services involves testing lower layers of the system; when this service includes development of the IoT instruments, we also requires to examine the hardware.

G. IoT security

The progression of IoT and amount of under-secured end-points is too greater than any of the traditional Information technology network, and security risk is also much bigger. Considering critical sectors, IoT devices already work or serve healthcare, emergency services, banking. The IoT security cannot be underestimated any longer. IoT security problems currently comes from these three main sources: Network hacks, Distributed Denial of Service (DDoS) attacks, Radio frequency (RF) jamming [8].

Suggestion

The IoT devices are associated to the back-end systems that are connected already to Internet via IoT network. The IoT network performs crucial role in smooth operation of the IoT devices. To sustain smooth operation, IoT network should be protected and secured. By using endpoint security features or techniques like anti-malware,, intrusion prevention, antivirus and firewalls, you can efficiently protect the whole network and secure the network against attacks [9].

H. Data Integration in IoT

The problem of data integration in IoT is among the biggest hurdles to IoT adoption that businesses across the world are experiencing with the continued propagation of the technology. Solving this challenge may require technology leaders to rethink and revamp their traditional IT infrastructures [10].

Suggestion

In order to overcome data integration challenges one must create a well-defined strategy for IOT in data integration, also take an API eccentric approach in inter device communication. And adopt integration platform as service for network integration.

I. Lack of Uniform Standards

As companies of all shapes and sizes create new gadgets for IoTs, one spiking factor has turn out to be more and more clear i.e., there is an extensive lack of uniform standards. If the entire notion behind the IoT is to create a world where everyone is capable to communicating with every other, this barrier is possibly one of the biggest barriers of all. [11].

Suggestion

One answer to this trouble is to create hub devices, permitting the consumer to control a variety of different IoT devices from one central gadget. But even this answer has some great hurdles. Companies would want to be the preferred choice of IoT gatekeeper. Another method called the access control mechanisms, it limit the rights of device or applications so that they will be able to only access the resources required by them to perform their specific tasks. One of its major advantage is that even if a device is compromised, the intruder will not have the rights to access sensitive data. [12]

J. Data Silos

Possibly the most instant challenge for the agencies shifting in the direction of IoT have to deal with is the concept of data

silos. Data is not of any value to any business enterprise if it exists in a vacuum. [13].

Suggestion

While addressing this challenge, corporations usually have two predominant choices available. Either they can select to purchase or create a new, end-to-end answer from the ground up, or they can incorporate and integrate IoT functionality into their current infrastructure. The first solution is costly, thus many companies tend to choose the second. Regardless of which route you choose, it is clear that integrating data from current systems is definitely a step really worth taking.

K. Securing the Edge

Security is the best challenge related to IoT development. As each and every gadget is related to wider computing network, attack surface is enormous larger than the typical network architecture. More worse, many gadgets are traveling between variety of networks, possibly picking up malware alongside them, which helps cybercriminals to skip some security measures. Many IoT devices are independent, which can cause those devices to act in ways that when evaluating risks, standard network protection protocols may not take them in account. [14].

Suggestion

To shield towards doable threats, corporations ought to construct their networks with the assumption that any system linked to it is already compromised in some way. In this way, they will definitely make the protocols and authentication criteria to deny the automatic access to sensitive data.

L. Government Guidelines

Data facilities and most tech companies are used to dealing with legislation. But the rollout of IoT devices has befell so rapidly that the legal allegations to this new technology have yet to be established. Even legal requirements related to purchaser records are continuing to grow. Companies that are integrating IoT devices into their network, strategies must be made and legal requirements must be taken in consideration on how it could have impact on their incorporation in the future. [15].

Suggestion

One of the exceptional choices for IoT companies searching to keep away from these challenges is to accomplice with a data center that accommodates into each and every and each issue of its operations. These facilities are already searching in advance to find a way that how records accumulated by means of IoT devices will be handled and secured.

M. Environment

With the development of IoT, the environment is completely changing in which testing activities and quality assurance are being implemented. Normally these activities are performed in a specified environments (for example; PC with specified OS and network connection), which alternatively be implemented in a complicated and dynamic environment. [16].

Suggestion

Developers should apprehend the building of the used third party hardware for developement of IoT applications. He should also test implementations and check if the required functionality is supported via the other external devices.

N. Interoperability

It is very important for a developer that he must have the ability to test all the changes in code against the other executions. Though, if testing for interoperability of network level, it requires each and every probable hardware and software amalgamations to be there at one single place. [17].

Suggestion

Conformance testing should be done against both: specification and the plugtest-events (technology implementers physically meet, then each party bring their systems in order to test against systems brought by the other parties).

O. IoT sensors

A substantial test setup adaptations is needed by the new sensor applications. If we want to integrate several sensors in single package it requires different types of stimulant which is very expensive, unless different stimuli combined in a single system. [18].

Suggestion

To overcome this issue we will need dynamic market which includes new wireless protocols, protocol-based programming and new sensor functions which ultimately means we will require a whole new setup.

P. Customer Uncertainty

According to a study carried out by the Dutch cybersecurity affiliation Gemalto, ninety percentage of customers lack confidence in IoT security, with sixty five percent concerned that hackers might manipulate their devices. Considering that many IoT devices are intended to use in home, its essential for agencies to tackle these concerns. [19].

Suggestion

Transparency start when it comes to earning the trust of customers. As they will prefer to know that what information is being gathered from them, how its being used, the vicinity its being stored, and how its being protected. They will want to be aware of what occurs if one of their devices is compromised and what alternative is available if the companys servers go through a data breach. Disseminating this information obviously and proactively will eliminate any misconceptions about IoT safety and therefore prevailing the trust of consumers.

As IoT revolution is already here, companies must not take the challenges related to implementation for granted. Failing to address these areas could lead to uncomfortable situations including useless products, making it crucial for organizations to put a great deal out of it or making a groundbreaking technology. By working closely with a data center, they can build positive frameworks that allow them to deliver the type of groundbreaking offerings clients assume. [20]

Table 1. Consequences of IoT issues for testing and quality assurance process.

Challenge	Consequences for testing and quality assurance process.
5,6,12	Demand for a method to define effective test strategy for the IOT solution.
7,8,9,10,11,16	Increased necessity of security testing, which also contains privacy aspects.
1,2	Test IoT's across numerous devices to confirm their worth, quality and reveal bugs that can hamper functions
6,5,14,15	Increased need for more effective integration testing, if possible, automated
6,5	Test automation in general, as the number of variants seems not feasible to be tested manually
3	Test of behavior of IoT solutions under the limited connection and several edge conditions are needed, especially for the life-critical systems
4,13	Need for wide-area networks provides larger coverage such as LTE-M.

IV. Conclusion

In spite of the fact, that the IoT is representing the prime and noteworthy flow in present technology development, the work related to IoT testing is limited. During the analysis, we established different principal fields, which could be basis of future research related to IoT testing techniques. Due to the development in IoT technology and current researches, we can anticipate further techniques to be initiated and made by different research groups. More-over, at present, these areas gives future research chances and opportunities.

References

[1] I. L. K. Lee, "The internet of things (iot): Applications, investments, and," 2015. [Online]. Available: www.googleschlor.com.

[2] O. Y. A. N. Al-Falahy, "Technologies for 5G networks: Challenges and opportunity," 2017. [Online]. Available: www.googleschlor.com.

[3] J. Parmar, "IoT: Networking Technologies and Research Challenges," 2016. [Online]. Available: https://scholar.google.com/.

[4] M. C. A. Z. L. V. M. Z. A. Biral, "The challenges of M2M massive access in wireless cellular networks," 2015. [Online]. Available: www.googleschlor.com.

[5] G. A. S. M. O. F. U. G. A. Ali, "Technologies and challenges in machine-to- machine applications," 2017. [Online]. Available: www.googleschlor.com.

[6] J. M. G. M. L. W. a. K. P. Batalla, "Implementation and performance testing of ID layer nodes for hierarchized IoT network.," 2015. [Online]. Available: www.googleschlor.com.

[7] Q. S. Marwah, "Software quality assurance in Internet of Things. Int. J.," 2015. [Online]. Available: www.googleschlor.com.

[8] C. P. J. A. M. M. J. Frahim, "Securing the internet of things,A proposed framework," 2015. [Online]. Available: www.googleschlor.com.

[9] Z. C. X. D. A. V. V. J. Zhou, ";Security and privacy for cloud-based IoT:Challenges," 2017. [Online]. Available: www.googleschlor.com.

[10] H. F. M. Foidl, "Data science challenges to improve quality," 2016. [Online]. Available: www.googleschlor.com.

[11] P. Worthy, B. Matthews and S. Viller, "Trust me: doubts and concerns living with the Internet of Things.," in In Proceedings of the 2016 ACM Conference on Designing Interactive Systems, 2016, June.

[12] E. Bertino, K. K. R. Choo, D. Georgakopoplous and S. Nepal, "Internet of things (iot): Smart and secure service delivery.," p. 7, December 2016.

[13] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello and A. Ceon-Porisini, "A secure and quality-aware prototypical architecture for the Internet of Things.," pp. 43-55, 2016.

[14] M. Bures, T. Cerny and B. S. Ahmed, "Internet of things: Current challenges in the quality assurance and testing methods. In International Conference on Information Science and Applications.," Singapore, 2018, June.

[15] V. Desnitsky and I. Kotenko, "Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge.," Journal of ambient intelligence and humanized computing, pp. 705-719, 2016.

[16] H. Foidl and M. Felderer, "Data science challenges to improve quality assurance of Internet Things applications.," in In International Symposium on Leveraging Applications of Formal Methods, Cham, 2016, October.

[17] P. Rosenkranz, M. Wahliseh, E. Baccelli and L. Ortmann, "A distributed test system architecture for open-source IoT software.," in In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, 2015, May.

[18] E. J. Marinissen, Y. Zorian, M. Konijnenburg, C. T. Huang, P. H. Hsieh, P. Cockburn and I. Verbauwhede, "IoT: Source of test challenges.," in 21th IEEE European Test Symposium (ETS), 2016, May.

[19] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications.," in IEEE communications surveys tutorials, 2015.

[20] J. Kiruthika and S. Khaddaj, "Software quality issues and challenges of Internet of Things.," in In 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), 2015, August.

[21] F. H and F. M, "Data Science Challenges to Improve Quality Assurance of Internet of Things Application," p. 20, 2016.

[22] Alur and R. , "Systems computing challenges in the Internet of Things," 2016.

[23] H. Foidl and M. Felderer, "Challenges to improve quality assurance of Internet of Things," 2016.

[24] M. Hossain, M. Fotouhi and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," pp. 21-28, 2015.

[25] J. Sifakis, "System Design in the Era of IoT—Meeting the Autonomy Challenge," 2018.

[26] R. B and A. H, "Internet of things: trends, opportunities, and challenges," pp. 89-95, 2017.

[27] A. Alkhalil and R. Ramadan, "IoT data provenance implementation challenges," 2017.

[28] Sha, W. Y. W. and S. , "On security challenges and open issues in Internet of Things," p. 10, 2018.

[29] Malik and S. Singh, "Security risk management in IoT environment," p. 12, 2019.

[30] Casale and Giuliano, "Current and future challenges of software engineering for services and applications," 2016.