Software Quality Assurance testing methodologies in IoT

Mehreen Sirshar
Faculty Of Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
mehreensirshar@fjwu.edu.pk

Komal Naeem
Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
komiawan123@gmail.com

Mahnoor Khan
Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
semahnoor916@gmail.com

Tanzeela Akbar
Software Engineering
Fatima Jinnah Women University
Rawalpindi, Pakistan
tanzeelaakbar24@gmail.com

***Abstract*—IoT is a fast growing technology that has Promising potential for shaping our future. In this fast growing world of IoT, IoT systems are released without proper testing which effect its quality and does not guarantee user satisfaction. Different testing methodologies are carried out to ensure Quality assurance of IoT before releasing it to the market. In this paper we have reviewed different testing techniques using AI and different tools to ensure Quality of IoT. In this paper we have also reviewed different IoT challenges related to its quality.**

***Index Terms*—Internet of things (IoT), Quality Assurance, Testing, Artificial Intelligence (AI)**

I. Introduction

Software quality assurance is essential for developing any high market value product. Quality assurance is an organized way for ensuring conformance of services with user stated requirements. Ensuring software quality increases customer satisfaction and market value. Internet of Things reflects a basic concept of network devices capable of sensing and collecting data from around the globe and then exchanging data on the Internet where it can be interpreted and used for lots of interesting purposes. Manjunatha [14] stated in his study that IoT applications are becoming increasingly important day by day and organizations are focusing on revenue generation from IoT products. McKinsey found that by 2020, about 20 billion objects could be linked via IoT. So If a single hole exists in IoT network it can act as a weak point for IoT network and cause security issues, so it is important to test each IoT layer (Application, service, gateway and sensor layer) to ensure its quality. Testing IoT devices results in many challenges as IoT is an architecture in which software are closely intertwined with hardware. Testing each IoT layer is also a challenging task so many testing techniques like performance, interoperability, compliance, API, Benchmark, pilot and security testing etc. discussed are applied on these layers to overcome these challenges.

II. Literature Review:

In 2016, Abid Jamil et al. [1] addressed for better quality control purposes the current as well as improved testing techniques. Testing is primarily a process that includes the process of validation and verification. The types are white box testing which test the inside details of a system, black box testing that tests system functional details without knowing its internal details, and gray box testing which have combine features of both black and white box testing. Jamil have also discussed Software testing lifecycle phases and stages.Article further states that Testing is time consuming and therefore a complex process requires improved methods and creative methodologies.

In 2016, Bruce et al. [2] stated that to help developers cope with both technological and trust issues, quality assurance is required. It needs effective management of processes. Individuals need to be inspired to make an effort to control performance. SQA must start during the selection of requirements and protocols should be developed to ensure compliance with quality requirements is established.

In 2018, Miroslav Bures et.al [5] have address the current challenges related to the reliability of service, interoperability, security, integration and user's privacy in the QA of IoT. In this paper three areas are discussed 1) interoperability 2) IoT applications' behavior on a restraint connection 3) problems in testing which are caused by different version and variants of platform. IoT-specific testing methods can address the IoT applications' interoperability in two sentences. The first point raises demand of automated integration testing and simulation of IoT infrastructure parts. The second line raises unit-level integration testing and selection of suitable platform variants, and generation of efficient input testing data sets. This create opportunity for Constrained Interaction testing discipline.

In 2016, Harald et.al [6] carried his research in which they present challenges related to data science in order to enhance Internet of Things applications quality assurance. In this paper after describing the main characteristics of IoT, they provide data science application in software development areas. They first outline requirements for quality assurance that evolve with IoT, and these are categorized into six types: (Organizational, Environment, User,Data Security Management and Compliance Agreement). Lastly, four types of data science issues: Defect Prevention, Analysis, User Incorporation and Organizational which are derived from the six types of QA standards.

In 2019, the research carried out by Bestouns Ahmad et.al [7] is on the basis of latest recommendations on how systematic studies are mapped. A collection of questions about the performance aspects of IoT are carefully described in their research. In their paper they organize the different domain of the IOT which are frequently discussed based on the quality aspect. In which Wireless Sensor Networks (75 papers) followed by Health care system (29 papers), Smart City (20 papers) are the areas which are discussed frequently from quality viewpoint.

In 2015, Marwah et.al [8] done the comprehensive analysis of IoT deployment techniques and methodologies against qulity assurance parameters and concluded that most strategies of IT implementation lack the aid of the tool and automation techniques. Therefore, they propose that IoT must be applied with a standard methodology.

In 2018, Bruno et. al [9] carried this research on studying IoT state from metrology perspective. IoT technologies are discussed like, RFID [9] , WSN [9] , LPWAN [9] and the forthcoming IoT 5 G network [9] . Bugs like Mikrotik routers [9] and IoT malware [9] created serious IoT security challenges. Their solution of self-calibration of instruments is completely hardware-based. In the future, sensors and actuators' remote recalibration is supposed to deliver the easiest and most effective way for solving data quality problem. In addition, algorithmic approach for data quality still present challenges of research, but results can be improved by collaboration with some sort of hardware like remote calibration.

V.Sathyavathy [10] showed how to use software testing techniques in IoT for the purpose of improving performance. The Internet of Things 'main goal and objective is to monitor, manage and organize different fields in a convenient, efficient and secure manner. This paper explores the types of software testing for home automation systems and how these systems can use the Artificial Intelligence techniques to generate test cases to improve their performance, energy, etc. Genetic algorithm is discussed as the most efficient algorithm for test case generation and in finding the feasible solution of a critical problem.

In 2018, Ghadeer Murad et.al [11] surveys different aspects of multiple IoT application software testing and methods, offering specific software testing like protection, usability, and connectivity. They also addresses the different kinds of problems which can occur during IoT system testing like network accessibility, automation, and user interface. In addition, they offers a wide range of applications and tools that are used for IoT testing such as Vector, Wireshark, and Shodan.

In 2017, John Esquiagola et.al [12] perform stress testing on using current version of IoT platform under different conditions. In this paper the authors have defined layers and related test phases that have to be tested. These layers are 1) Software Interaction Layer (Unit, integration, system and acceptance test) [12] 2) Hardware Interaction Layer (Performance, security and interoperability test) [12] 3) User Interaction Layer (Usability, Reliability, Conformance, and scalability test) [12] . Testing of software layers was performed using standard software frameworks such as Junit. While hardware layer was tested by using Tsung tool [12] . Initially the result show maximum request per second for each hardware device. The Intel NUC was the best performance system, followed by Intel Edison [12] and Intel Galileo [12] was the worst device.

In 2018, Svitlana Popereshnyak et.al [13] have presented some types of IoT architecture testing for ensuring the quality of IoT. 1) Device suitable for its intendent use 2) Test the existence of the network connection and scenario when there is no connection 3) Identify network problems that may contribute to disconnection and test routers and switches for IoT traffic sustainability 4) Operating system, Browser, their versions and communication mode 5) Static Test and Dynamic Test 6) users exploit the application in different ways and then express their views 7) Developed IoT framework, which has a certain functionality, should pass several compliance tests 8) To avoid possible errors while updating the application or the system as a whole, thorough testing is required.

In 2018, Pedro et al. [15] Enforces the concept of a model-based approach to IoT testing to systematize and simplify IoT environment testing and defines five IoT testing patterns consisting of Periodic Measurements, Triggered Measurements, Test Warnings, Test Activity and Test Sensors. These strategies are predicated on the idea that similar architectural systems need to share a similar test plan, i.e. following the same set of patterns of design. Identifying and recording these test trends would encourage standard test methods to be implemented, allowing developers and researchers to test IoT solutions using similar techniques to address similar needs, leading to improved IoT solutions reliability.

In 2019, this study is conducted by Hussam Hourani et.al [17] in which they discuss the key pillars of artificial intelligence that can be used in testing software. A brief overview on Machine learning and software testing has given

in the paper. The paper highlighted different methods and algorithms of AI used in Software testing areas. Scientists have suggested different Test Case Prioritization (TCP) methods to identify vulnerabilities in early stages. NLP was used to aid the techniques of TCP. It is concluded that these all approaches used can improve performance in testing of software. Software Testing related to AI will decrease market time and increase the organization's productivity in producing advanced softwares and smart automatic testing creation.

In 2017, Neha et al. [18] used AI-based evaluation methods to achieve software quality. There may be two forms of testing, i.e. manual testing and automated testing. Because of the need for indefinite time and resources, manual testing is not suitable for extensive projects. Automated testing is a technique where testing methods are used to run pre-determined computer scripts to detect defects. AI-based strategies include Ant Colony Optimization a metaheuristic optimization method, genetic algorithm heuristic search system, tabu search meta-heuristic algorithm, bee colony and data mining. Various tools are used to conduct automated testing including selenium, watir, ranorex and many more.

III. IoT Testing Techniques

Following are the testing types which are used to ensure the Quality assurance of Iot.

Usability Testing: It should be ensured that all devices connected to the network are available and perform well at all times.

Reliability Testing: Validating components of IoT like sensors in different conditions like operational and environmental.

Scalability Testing: Validate the IoT platform's ability to support multiple users at the same time without degrading performance.

Hardware-software Compatibility Testing: Validate the combination of different devices having different software and hardware configuration, protocol and product versions, and OS.

Security Testing: IoT is vulnerable to security issues such as missing data encryption, minimum password requirements, and password-free user interface access. So to secure IoT systems from these security testing is important.

Performance Testing : Validating the response time of sensors and application within the mentioned limit. One of the key aspects of IoT performance testing is validating information reading, writing and data retrieval speeds.

Connectivity Testing: Testing wireless signal to determine that what will happen if there is no/weak connection, or when many devices try to communicate with each other.

Benchmark Testing: The main task is to identify the problems associated with the network that can lead to the disconnection, as well as to test the routers and switches for IoT traffic sustainability.

Pilot Testing: It is done in the laboratory in order to allow us to conclude that the system is functional. In this a limited number of users are allowed to perform different task on the application and then express their opinion.

Functional Testing: Validate the correct functionalities of the IoT applications.

Network Testing: Testing the Iot Applications in different network and protocol connections to validate the connectivity across IoT platforms.

Interoperability Testing: Conducted to ensure the ability of different devices, other external devices and applications to support the necessary functionality between themselves.

API Testing: Testing the API directly or as component of an integration test to determine its features, robustness, and efficiency and safety demands.

IV. IoT Testing Platform

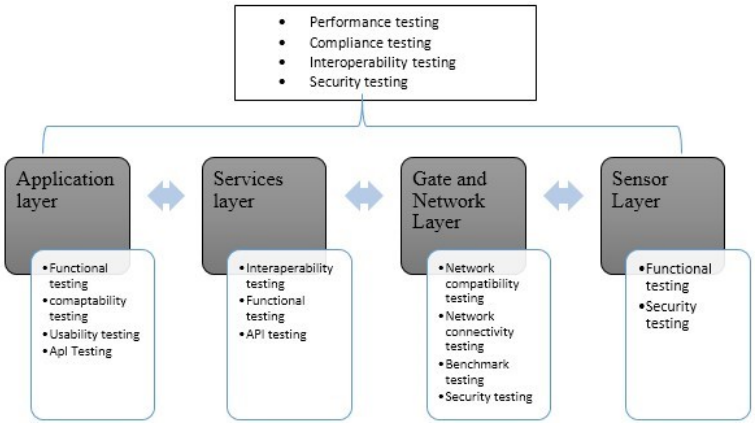

Fig. 1. IOT Testing Platform

V. Challenges in IoT Testing:

Iot is a collection of interlinked smart devices, physical and virtual machines, with distinctive identifiers and the ability to move data over a network without needing interaction between people and computer.IOT is encountering many challenges as it is extremely being used to develop better techniques and methods.

Table 1: General Challenges

Primary Challenges	Operational challenges
Dynamic Environment	Third part involvement in sub-systems
Real- time Complexity	Complex set of Use-cases
Scalability of the System	Hardware Quality & accuracy
	Security & Privacy Issues, Safety concerns

VI. Data Science Challenges and their identified Solutions

Quality assurance covers all the methods that we use to develop products in a way that increases our trust as well as the approaches of product evaluation. For the quality improvement of IoT applications, requirements are grouped into six types: • Organizational • Data Management requirements. • Environment • User • Compliance/Service Level Agreements • Security

Table 2:Data Science Challenges and their identified Solutions

Area	Challenges	Example	Solutions
IoT applications related to real world data generation	Real-time analysis is difficult due to the variety of possible case scenarios for real-time use and the difficulty that occurs in accordance with intelligence applications.	Stock exchange business processes	Over-the-air testing Automatic regression testing routines
	classical integration testing In the new IoT environment	IoT devices communication in real world	Field testing is performed by various users.
	Defect Prevention with emerging IoT	Defects in Data Science Field	Telemetry injection to detect anomalies

Also a regression model for negative binomial helps in estimating the number of faults in a large supply network by using previous releases of data. And a more successful approach is model for machine learning in locating code errors in software programs accurately. In addition, the identification of factors of defects is a useful way to apply data science techniques to avoid faults in IoT systems.

A. Metrological issues and Quality Assurance in IoT

A modern technique for recalibration is an algorithmic solution to the issue. Since the algorithm solution provides a vital estimation for inaccuracy of data obtained and recommends how to handle these deviations, it does not tackle the actual problem: the detector still gives wrong readings and is not stable. From above, its concluded that algorithm approach is expected to be helpful in giving accurate result if combined with some sort of hardware.

VII. IoT Testing Tools:

A. Software Tools

Following are the tools which are used for Iot Software testing.

Table 3: Software Tools

Tool	Use	Drawback
Wireshark:	Displaying TCP/IP and packet transfer of network	No network protection, only captures packet coming into network and store the data in uneditable archive so it is difficult to add comments
Tcpdump:	Displaying TCP/IP, packet transfer over network and source and destination host addresses.	No user interface (GUI), and analyze only TCP network traffic.
Shodan	To find IoT vulnerabilities.	There is a lack of results that you may need to evaluate the machine
Thingful	Allows IoT data owners to track how their data is used	Provides access to only those IoT devices that our central database is connected to.
MQTT Spy	Generally use for performance testing of IoT	Use for device which use MQTT protocol.

B. Hardware Tools Tools

Following are the tools which are used for Iot Hardware testing.

Table 4: Hardware Tools

Tool	Use	Drawback
JTAG Dongle	It is simply a means of communicating with the device's on-chip debug block and memory interface.	Single-step restrictions Memory access restrictions (speed and stability)
Logic Analyzer	Captures & displays multiple signals, decode them on bus, check sequence of events.	It does not focus on the signal's analog characteristics and specific values.
Digital Storage Oscilloscope	Stores & analysis signals digitally, check signal integrity, power supply glitches, timing of various events etc.	They are very sophisticated, and if damaged, they tend to be expensive to repair.

C. AI Testing Techniques in IoT QA

As AI helps in Testing of software, it also helps in testing of IoT softwares. Following are the AI techniques which are used in IoT testing.

Ant colony optimization	A population-based technique which can be used to locate estimated solutions to difficult optimization issues
Genetic Algorithm	Used for solving complex problems for machine learning and is also used for evolving simple test programs
Tabu search	Search methods used for mathematical optimization.
Artificial bee colony	Used for automatic generation of structural software test for the small information areas
Data mining	Process of mining the valuable information and knowledge from a huge database which is further useful for decision making.

VIII. Analysis:

In paper, we have discussed the types of testing used in IoT to ensure QA. IoT framework involves different layers therefore, fig 1 depicts mapping of testing techniques with these layers. Functional testing is done at three layers Application, Services and Sensor layer. While performance, Compliance, Interoperability and Security testing are done at all these four layers. As IoT devices and applications involve internet network, due to this if there is a single weak connection or a weakly secured device exist, they can make an entry point for the whole network and cause IoT system vulnerable to attacks and may cause privacy security issues. Weakly secured device can be a point of entry for the whole network. Therefore, security testing must be achieved at every layer of IoT Framework. From fig1, we have analyzed that the testing techniques which are used for the IoT QA are different from the classical testing techniques use for Software QA as IoT involves use of different protocols at its layers. In Table 1 2, We have analyzed the challenges that are faced during the testing of IoT applications and also discussed techniques to

solve them. Due to the emergence of real world data, Data Science has become a serious issue in maintaining the quality of IoT. Over-the-air, Regression testing and telemetry injection provides solution to overcome this issue. In Table 3 4, we have mentioned the testing tools like software and hardware testing tool for the IoT QA along with their drawbacks. Both Wireshark and Tcpdump done same job but Tcpdump is text based and have no user interface while Wireshark provide the user interface. Digital Storage Oscilloscope is considered the worst tool as compared to the other hardware tool. As it has the poorest drawback of being sophisticated, they tend to be expensive to repair if get damaged. In Table 5, AI techniques which are used to ensure the quality of IoT. The main advantages of using AI techniques in IoT testing, are improving accuracy, support both developers testers, provides automate testing and save time cost in overall test coverage.

IX. Conclusion

SQA is important to the production of technology that meets customer expectations and conforms to its requirements. The goal of every member of the software development company should be continuous improvement. Application testing is the application product verification and validation process. We can't make sure of the product's approximation without testing the value. High-quality product means better userfriendly applications. We have discussed various IoT challenges like operational, primary and challenges in data science. For assuring quality of IoT applications, various hardware software tools are used like Wireshark, Shodan, UART etc. Among AI testing techniques, data mining is the most used QA approach. Several techniques are used to achieve performance in software testing processes for test sequence generation, test automation, quality assessment, accuracy checking. For enhancement of quality of IoT applications, our study is concluded with a summary of the problems, tools and techniques used in IoT. Future research involves developing and evaluating new algorithms and techniques and their modern implementation to deal with the issues that have been identified.

References

[1] Jamil, M. A., Arif, M., Abubakar, N. S. A., Ahmad, A. (2016, November). Software testing techniques: A literature review. In 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M) (pp. 177-182). IEEE.

[2] Maxim, B. R., Kessentini, M. (2016). An introduction to modern software quality assurance. In Software Quality Assurance (pp. 19-46). Morgan Kaufmann.

[3] Peischl, B. (2015, April). Software quality research: From processes to model-based techniques. In 2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW) (pp. 1-6). IEEE.

[4] Kiruthika, J., Khaddaj, S. (2015, August). Software quality issues and challenges of Internet of Things. In 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES) (pp. 176-179). IEEE.

[5] Bures, M., Cerny, T., Ahmed, B. S. (2018, June). Internet of things: Current challenges in the quality assurance and testing methods. In International Conference on Information Science and Applications (pp. 625-634). Springer, Singapore.

[6] Foidl, H., Felderer, M. (2016, October). Data science challenges to improve quality assurance of Internet of Things applications. In International Symposium on Leveraging Applications of Formal Methods (pp. 707-726). Springer, Cham.

[7] Ahmed, B. S., Bures, M., Frajtak, K., Cerny, T. (2019). Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study. IEEE Access, 7, 13758-13780.

[8] Mateen, Q., Sirshar, M. (2015). Software QualityAssurance in Internet of Things. Int. J. Comput. Appl, 109, 16-24.

[9] Sandrić, B., Jurčević, M. (2018, January). Metrology and quality assurance in internet of things. In 2018 First International Colloquium on Smart Grid Metrology (SmaGriMet) (pp. 1-6). IEEE.

[10] Sathyavathy, V. Software Testing Techniques in IoT Applications.

[11] Murad, G., Badarneh, A., Quscf, A., Almasalha, F. (2018, July). Software Testing Techniques in IoT. In 2018 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 17-21). IEEE.

[12] Esquiagola, J., de Paula Costa, L. C., Calcina, P., Fedrecheski, G., Zuffo, M. (2017, April). Performance Testing of an Internet of Things Platform. In IoTBDS (pp. 309-314).

[13] Popereshnyak, S., Suprun, O., Suprun, O., Wieckowski, T. (2018, April). IoT application testing features based on the modelling network. In 2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH) (pp. 127-131). IEEE.

[14] Manjunatha Gurulingaiah Kukkuru, 2018. Testing IoT Applications – A Perspective

[15] Pontes, P. M., Lima, B., Faria, J. P. (2018, November). Test patterns for IoT. In Proceedings of the 9th ACM SIGSOFT International Workshop on Automating TEST Case Design, Selection, and Evaluation (pp. 6366). ACM.

[16] Ferry, N., Solberg, A., Song, H., Lavirotte, S., Tigli, J. Y., Winter, T., ... Aguirre, A. C. (2018, March). ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems. In International Workshop on Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment (pp. 112-127). Springer, Cham.

[17] Hourani, H., Hammad, A., Lafi, M. (2019, April). The Impact of Artificial Intelligence on Software Testing. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 565-570). IEEE.

[18] Bhateja, N., Sikka, S. (2017). Achieving quality in automation of software testing using Ai based techniques. Int. J. Comput. Sci. Mob. Comput, 6(5), 50-54.

[19] Sathyavathy, V., Priyaa, D. S. (2018, December). Software Testing Techniques with Artificial Intelligence in IoT Applications. International Journal of Recent Technology and Engineering (IJRTE), 7(4S2).