International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I2P213

Volume 69 Issue 2, 92-101, February 2021
© 2021 Seventh Sense Research Group®

Quality Assurance of IoT based Home Automation Application using Modified ISO/IEC 25010

Rohini Temkar[#1], Anand Bhaskar[*2]

[#1] *Department of Computer Science & Engineering*
[*2] *Department of Electronics & Communication Engineering*
Sir Padampat Singhania University, Udaipur-313601, Rajasthan, India.

[1] rohini.temkar@spsu.ac.in, [2] anand.bhaskar@spsu.ac.in

***Abstract** - With the development and emergence of technologies Internet of Things (IoT) is reaching maximum connectivity. The enormous and heterogeneous devices are responsible for producing and sharing a huge amount of data, which arises a need to focus on quality assurance of IoT applications. Traditional quality models are designed to evaluate the quality of software applications. Due to mobility and wireless connectivity in IoT applications, these quality models need to be enhanced. In order to focus on this need, in this paper, the modified ISO/IEC 25010 quality model for quality assurance of IoT applications is presented. The existing ISO/IEC model has been modified and formulated to incorporate the feature of IoT applications like software-hardware collaboration and networked, wireless mobile connectivity. The proposed model considers functionality, compatibility, security, performance, usability, reliability, maintainability, and portability. To evaluate the effectiveness and validate the performance of the proposed model, IoT-based home automation is simulated with five different scenarios. The validation of the various software quality metrics has shown improved quality scores over the existing quality assurance metrics.*

Keywords — *Quality Assurance, Internet of Things, Home Automation*

I. INTRODUCTION

Internet of Things (IoT) is a fusion of loosely-coupled, decentralized networks of wireless, mobile, and sensor-based intelligent heterogeneous devices. The IoT devices are capable of sensing, actuating, storing data, data and knowledge interpretation, and data exchange, in a situated context-aware manner. IoT has not only opened the door to new opportunities but also raised new questions. One of the significant questions is regarding the data access and quality of data. In the IoT environment, the data is being collected from heterogeneous devices where the software and hardware work together as a collaboration model. In such an environment, problem identification and its diagnosis become difficult. The way of defining the quality features of applications, including such devices, vary according to the functionalities of the system. Non-functional quality factors play a vibrant role in evaluating such systems due to their applicability and multiple functionalities at a given time [1]. The non-functional quality aspects such as performance, usability, timeliness, correctness, security are required to be tuned and should be traceable for the IoT systems. Thus, focus on addressing Quality of Service (QoS) issues becomes a crucial factor when designing quality models for IoT systems and the challenges that need to be addressed. As per the literature review, in 2020, there will be an estimated 50 billion devices connected to the IoT. A crucial factor is that the quality of service through quality governance software of IoT. The Software Quality Assurance Models for measuring the quality of software are available, but they are applicable to traditional software applications [2]. IoT applications arise the additional IoT characteristics. Hence the existing Software Quality models need to be improved and adapted to the characteristics of the IoT. The enhanced Software Quality Model can be further used as a basis for formulating the governance of IoT. In this paper, a modified ISO/IEC 25010 model is proposed to evaluate and validate the quality factors of IoT applications by formulating a quality metric for IoT applications. For the current work, IoT-based Home Automation Application is simulated using MATLAB Simulink software. Under this application, five different scenarios like IoT base water level control, automatic door lock system, automatic tube-light controller, smoke detector, and temperature-based fan controller are taken into consideration.

II. LITERATURE SURVEY

In this section, the literature survey is carried out in two perspectives IoT governance and quality assurance in IoT applications respectively.

A. IoT Governance

With rapid development in the Internet of Things and IoT characteristics, the traditional Internet Governance is required to enhance to support IoT. European Research Cluster on The Internet of Things focused on the issues of

IoT Governance, Privacy, and Security. They also provided a summary of the related work on Governance, Security, and Privacy. [3]. Weber expressed that the Internet of Things (IoT) is an emerging global Internet-based information architecture that faces many IoT issues like Privacy and Data Protection, Security and Safety, ethics, and interoperability which are considerably different than the traditional Internet due to enormous size and heterogeneity still a legal framework does not exist so far. [4]. Governance is changing under various situations of interconnectedness new rule-making structures need to be taken into consideration. The multi-stakeholder-approach in the governance process had become a topic of debate in Internet Governance. But the involvement of all stockholders with the necessary expertise is required to achieve high-level competence and expertise [5]. The goal of data governance is not just to clarify who "owns" data but also to optimize its value. The data itself is the important factor for improved business performance. Accordingly, the data governance has equal responsibility on businesses as it has on IT—and preferably more. This paper provides the necessary tools, framework, and vocabulary to educate business leaders about data governance. [6].

The quality of IoT based system directly affects the functionality and performance of the application. Bugs in the software module lead to violations of privacy, security, and compatibility. Due to the vast growth of the internet and data sharing capability, there is a need to maintain the privacy and security aspects of IoT-based systems. Software quality of IoT-based systems is directly related to processing quality, service quality, and information quality of IoT applications.

B. Quality Assurance in IoT Applications

IoT applications are a collaboration model of software and hardware. The data is collected from a variety of sensors and passes through various layers in IoT architecture. Not only the privacy and security of data but also the quality of data is also a crucial factor in the case of the IoT environment. Idri et al. have done a study to help quality managers to apply the ISO 9126 standard on software quality, particularly the External Quality model, to mobile environments. They evaluated the influence of the limitations of mobile technologies for each software quality characteristic. The External Quality model is used to assess the Reliability, Usability, and Efficiency characteristics of quality assurance [7].

The study of the ISO 25010 model against existing open-source software quality models helps for better understanding and selection of quality models [8]. Kiruthika and Khaddaj introduced the functional and non-functional software quality issues. According to the authors, the functional software quality factors in IoT depend upon the functionalities of the system, and non-functional quality factors play a vital role in evaluating such systems. Addressing challenges in quality of service plays an important role in designing quality models [1]. Marwah et al. have done a comprehensive study and compared the various techniques and methodologies for IoT implementation on the basis of various software quality assurance factors. It has been observed that most of the techniques lack a tool to support and automation techniques. Therefore, there is a need for a generic methodology to implement IoT, which must be customizable to a specific domain. [9]. Kim developed a new quality model for IoT applications by quality attribute in ISO 9126. The effectiveness of the quality model for evaluating IoT applications is validated through case studies. However, ISO 9126 is the older reference model, which does not include the advanced quality factors [10]. Tambotoh et al. have presented the Software Quality Model for Internet of Things Governance. However, validation and measurements based on the formula are not yet done with this model. Still, this model is not yet used to formulate an IoT Governance (IoTGov) framework [2]. In [11], the author has proposed a multi-objective decision-making (MODM) based evaluation model of service quality by considering resource state and user preferences. In [12], the authors have done with performance analysis of radio frequency identification (RFID) networks, which is based on the binary tree medium access control (MAC) protocol. The network performance metrics like throughput, the average number of packets required to take a census of the RFID tags, and delay were considered for evaluation. In [13], authors have proposed a QoS model of grey decision-making from the view of IoT Global Infrastructure and built an adaptive service framework. In [14], a quality evaluation technique of RFID middleware according to ISO/IEC 9126 standard.

The complete performance of the IoT-based system encompasses the hardware and software quality of the product. Software quality of IoT-based systems directly affects the functionality and performance of the application. Bugs in the software module lead to violations of privacy, security, and compatibility. Due to the vast growth of the internet and data sharing capability, there is a need to maintain the privacy and security aspects of IoT-based systems. Software quality of IoT-based systems is directly related to processing quality, service quality, and information quality of IoT applications.

III. METRIC SUITE FORMULATION FOR QUALITY ASSURANCE

As compared to software applications IoT applications show additional characters due to the inclusion of smart devices.

1. Intelligent Hardware Devices: In IoT, various mobile and intelligent hardware devices participate in various activities. They are responsible for exchanging the information, make the decision intelligently and adapt to the environment.

2. Software-Hardware Collaboration Model: The devices collaborate with each other. This collaboration includes the

functionalities done by various software and hardware components.

3. Networked, Wireless, and Mobile connectivity: In IoT applications, the wireless and mobile connectivity among the devices serves the ease of access. With quality wireless, mobile and networked devices, diverse functions of IoT can be performed efficiently.

4. Remote Monitoring for IoT Devices: IoT applications come with an effective feature that can be monitored remotely. To achieve these characteristics, Computational intelligence is required.

5. Limited Battery and Memory: Limited battery lifetime and limited memory are considerable constraints in IoT applications. It can be overcome using adjusted transmission power.

The ISO/IEC 25010 model can be used to analyze the quality of the variety of software applications. It is an extended version of ISO/IEC 9126 with additional features such as compatibility and security. The above-mentioned IoT application characteristics can be mapped with ISO/IEC 25010 quality attributes. Figure 1 shows the mapping of IoT characteristics with quality attributes of ISO/IEC 25010.

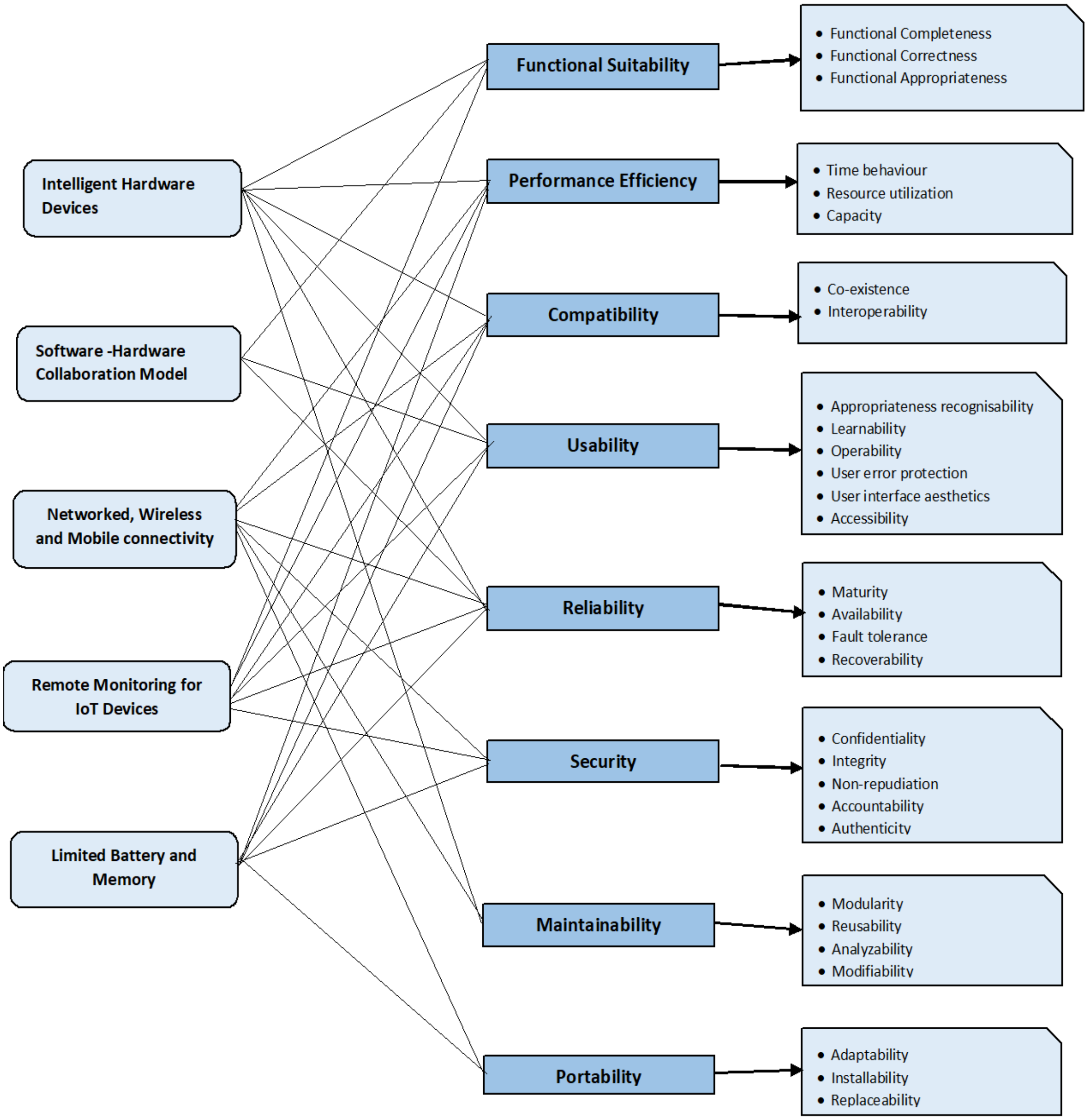

Figure 1. Mapping of IoT characteristics with Quality Attributes in ISO/IEC 25010 Quality Model.

TABLE 1. FORMULATION OF METRIC SUITE FOR QUALITY ASSURANCE IN IOT APPLICATIONS

Characteristics	**Sub characteristics**	**Description**	**Formula**
Functional Suitability	Functional completeness	The ratio of the number of functions completed against the number of functions stated.	X=A/B A= number of functions completed. B= number of functions stated.
	Functional correctness.	The ratio of a number of functions correctly implemented with the needed degree of precision against the number of functions completed.	X=A/B A=Number of functions correctly implemented needed degree of precision B= Number of functions completed.
Performance efficiency	Time behavior	It can be measured as response time, Throughput, Turnaround time, Network delay. Response time: Duration from the request made to the first response.	X= Response Time/ Throughput/Turnaround Time/ Network Delay
	Resource utilization	The number of resources used to complete IoT applications. Resources can be Memory requirement, I/O Device requirement, Bandwidth requirement, Energy Consumption.	X= Number of resources used to complete IoT application
	Capacity	The degree to which the maximum limits of a product or system parameter meet requirements. The system parameters can be Maximum The number of items that can be stored, maximum number of concurrent users, the highest communication bandwidth, throughput of transactions, and size of the database.	X= System parameter that reaches Maximum limit which meets the requirements.
Compatibility	Co-existence	A number of IoT devices share a common environment.	X= Number of IoT devices shares common environment.
	Interoperability	The degree to which heterogeneous IoT devices share information with each other	X=Number of cases where IoT Devices share information without failure.

Usability	Appropriateness recognizability	The ratio of functions recognized as appropriate by the user against all completed functions	X=A/B
			A= Functions recognized as appropriate by the user.
			B=All completed functions.

	Learnability	The ratio of functions learnt/ understood by the user against all completed functions	X=A/B
			A= Functions learnt/ understood by user
			B=All completed functions.

	Operability	The ratio of functions that are easy to operate against all completed functions.	X=A/B
			A= Functions which are easy to operate
			B=All completed functions.

Reliability	Maturity	The ratio of functions/components the meet needs of reliability against the total number of implemented functions.	X=A/B A= Functions/components the meet needs of reliability B= Total number of implemented functions.
	Availability	The ratio of the number of times the system was available/accessible to use against the number of times the system was required to use.	X=A/B A= Number of times the system was available/accessible to use B=All completed functions needs.

	Fault tolerance	The ratio of the number of times the system was operable even if there was a fault against the number of times faults occurred.	X=A/B A= Number of times the system was operable even if there was a fault B= Number of times faults occurred.
	Recoverability	The ratio of the number of times the system was recovered from fault against the number of times faults occurred.	X=A/B A= Number of times the system was recovered from fault. B= Number of times faults occurred.
Security	Confidentiality	The degree to which functions used to control illegal access work fine.	X= percentage that application works against illegal access.
	Integrity	The degree to which functions used to prevent modifications works fine.	X= percentage that application works against illegal modification in the system.
	Accountability	No of the functions are themselves accountable for the malicious action.	X= No of functions that are themselves accountable for the malicious action.
	Availability	The degree to which functions make data available when required.	X=percentage that application works against denial of service attack.
Maintainability	Modularity	The ratio of the number of modified functions with minimal impact on other functions against the total number of modified functions.	X=A/B A= Number of modified functions with minimal impact on other functions. B= Total number of modified functions.
	Reusability	A number of other systems where components are reused.	X=Number of other systems where components are reused.
	Modifiability	The ratio of the number of modified functions without degrading performance against the total number of modified functions.	X=A/B A= Number of modified functions without degrading performance. B= Number of modified functions.
Portability	Adaptability	The percentage with which the system can be adapted to changes.	X= percentage with which system can be adapted to changes.
	Installability	The percentage with which the system can be installed/uninstalled in a specific environment.	X= percentage with which system can be installed/uninstalled in a specific environment.
	Replaceability	The percentage with which the system positively works with the replaced component.	X= percentage with which system positively works with the replaced component.

IV. RESULT AND DISCUSSION OF CASE STUDY

For the experimental evaluation, a simulation of home automation using IoT is considered. The proposed IoT scenario is implemented using MATLAB Simulink software on a personal computer with a Core i3 processor, 4GB RAM, and Windows 8 operating system. Five home automation applications such as temperature-based fan regulator, face recognition-based door lock system, tube-light switching, automatic water level controller, and smoke detector are considered. For communication purposes, Bluetooth and IEEE 802.15.4 (Zigbee) communication model. For the implementation of the multi-level controlling action, Fuzzy Logic is used. The fuzzy controller will act as the software module to control the home appliances based on the specific inputs. Fuzzy logic converts the input variables into crisp variables and, based on rule base, generates the control action [25]. The process of quality assurance of IoT-based home automation is shown in Fig. 2. In the initial stage, all the control parameters and system configurations are required for the home automation systems. The performance of the face recognition and speech recognition based door lock system and light control system is evaluated on the basis of accuracy, recognition time, response time, spoofing attack on the software model. The score of various software quality assurance attributes is measured for every home automation application using the metrics given in table 1. Fig. 3 shows the simulation of IoT-based home automation for controlling five different home appliances. The face recognition based door lock system is based on the Local Binary Pattern algorithm (LBP) for the face recognition [26], and the hand clap detection algorithm uses Mel Frequency Cepstral Coefficients (MFCC) and K-Nearest Neighbor (KNN) classifier for switching of tube-light [27][28]. The door lock access is given to five-person and hence face recognition system is implemented for the five subject's database. Face recognition-based door-lock system is person dependent and considers the security aspect of the IoT software. At the same time, a handclapping-based tube light control system is person-independent. The proposed implementation shows perfect functional completeness and appropriateness. The correctness is achieved for ten iterations for an average of four home automation functions that causes a practical correctness value equal to 0.8. Fig 3 and Fig 4 show the room temperature-based fan controller and smoke controller. The weights of the quality matrix are divided into three parts such as 0.3 (high), 0.2 (medium), and 0.1 (low). The evaluation of various ISO/IEC 25010 for home automation systems using IoT is shown in Table 2.

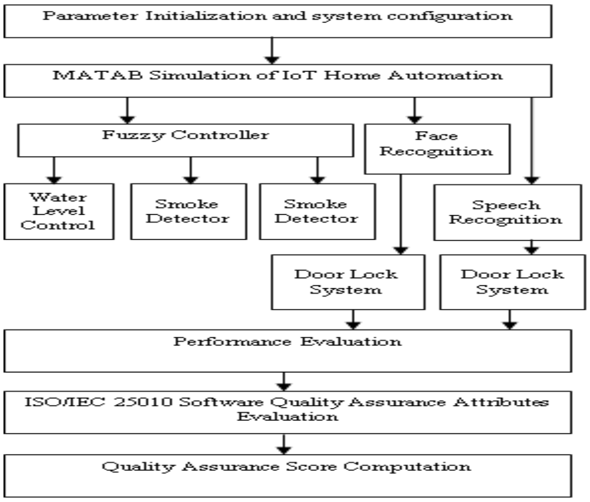
Parameter Initialization and system configuration
MATAB Simulation of IoT Home Automation
Fuzzy Controller
Face Recognition
Water Level Control
Smoke Detector
Smoke Detector
Speech Recognition
Door Lock System
Door Lock System
Performance Evaluation
ISO/IEC 25010 Software Quality Assurance Attributes Evaluation
Quality Assurance Score Computation

Figure 2. The process of quality assurance of IoT based home automation

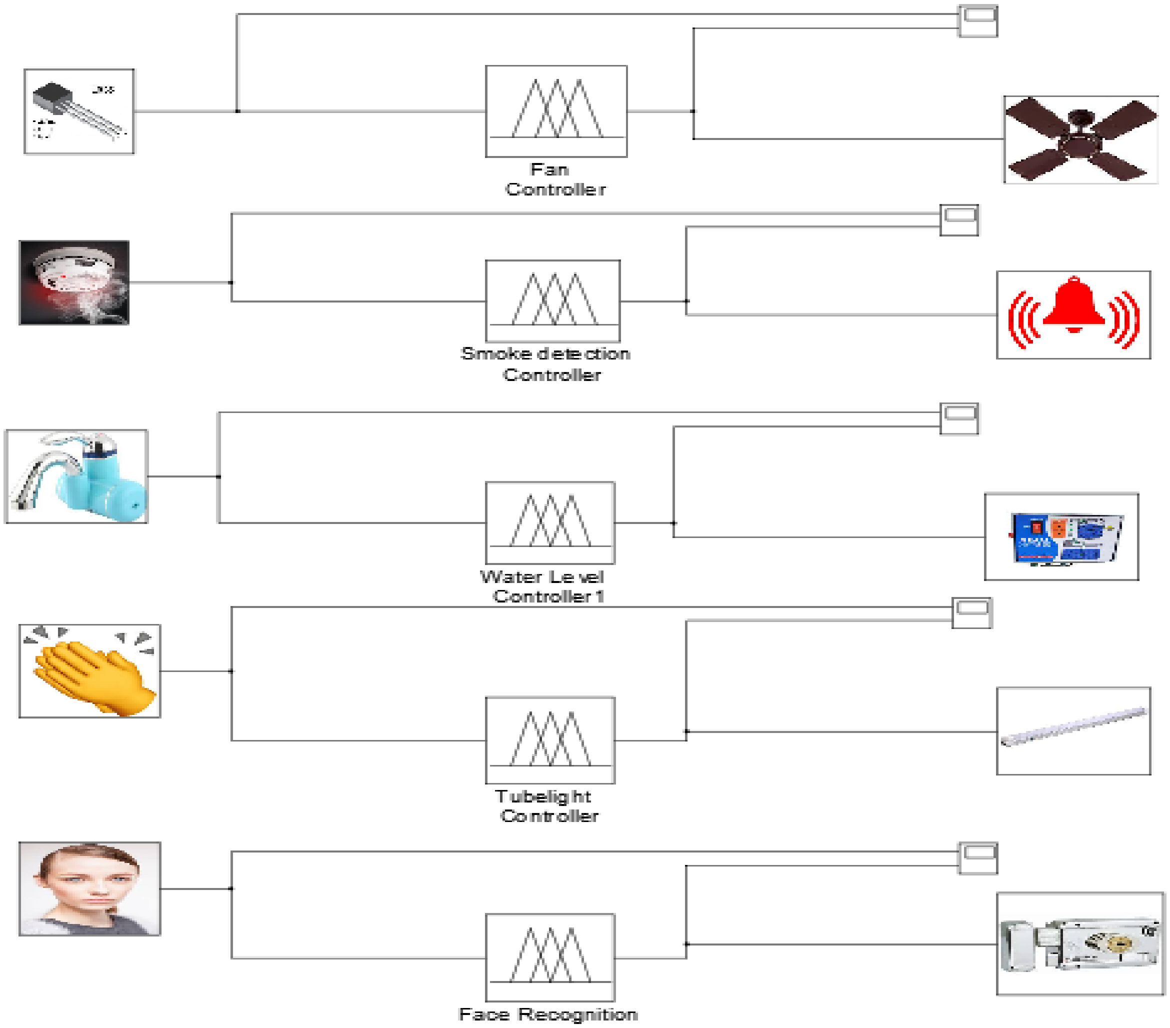

Figure 3. Simulation of IoT based home automation system using fuzzy logic

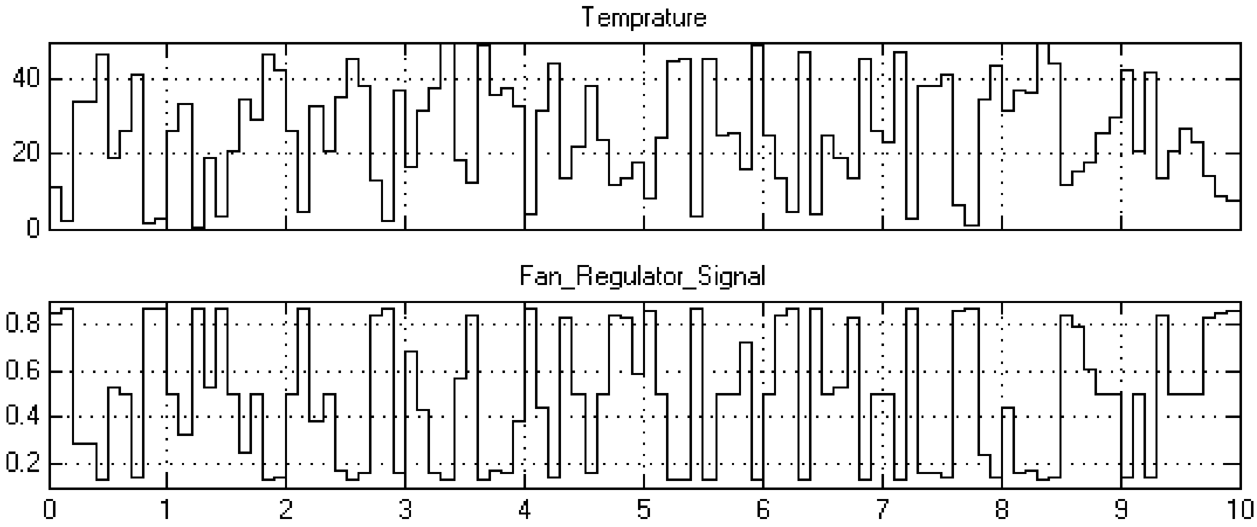

Figure 4. Simulation of room temperature based fan controller

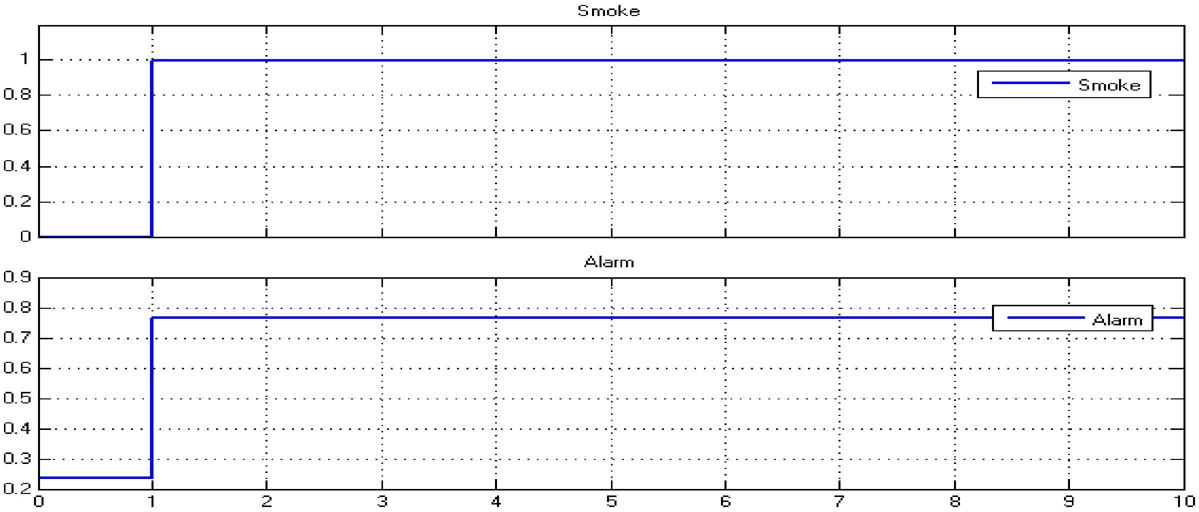

Figure 5. Simulation of smoke Controller

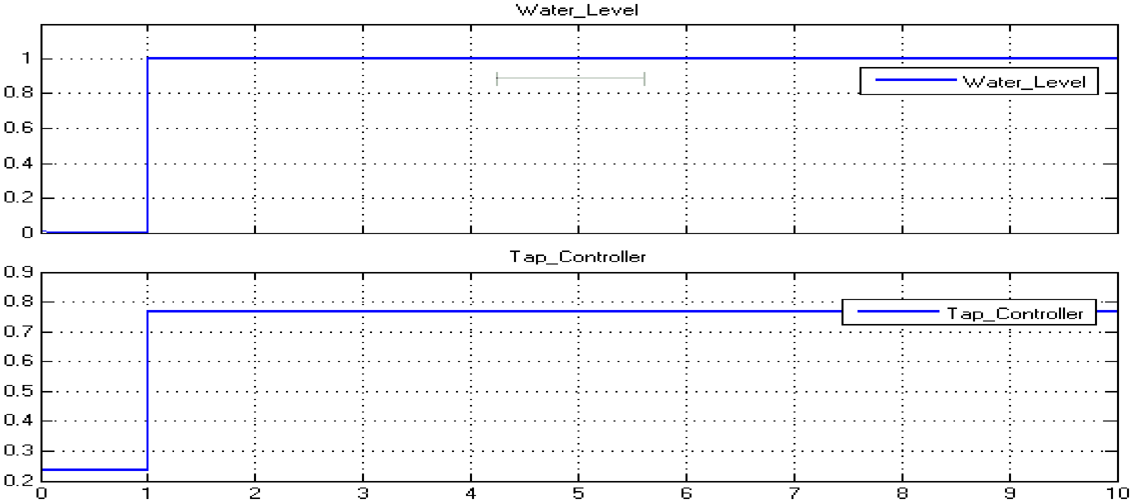

Figure 6. Simulation of water level controller

TABLE II. VARIOUS ISO/IEC 25010 ATTRIBUTES CALCULATION

Characteristics	**Sub - characteristics**	**Fan Controller**	**Smoke Detector**	**Water Level Controller**	**Door Lock System**	**Tube-light Controller**	**Final Score**	**Average Score**
Functional Suitability	Functional completeness	High	High	High	High	High	1	0.9
	Functional correctness.	High	High	High	Medium	High	0.8.	
Performance efficiency	Time behavior	High	High	High	Medium	High	0.8	0.93
	Resource utilization	High	High	High	High	High	1	
	Capacity	High	High	High	High	High	1	
Compatibility	Co-existence	High	High	High	High	High	1	0.8
	Interoperability	High	High	High	Low	Low	0.6	
Usability	Appropriateness recognisability	High	High	High	High	High	1	0.8
	Learnability	High	High	High	Low	Low	0.6	
	Operability	High	High	Low	Low	High	0.8	
Reliability	Fault tolerance	Medium	Low	Low	High	High	0.6	0.6
	Recoverability	High	High	High	High	High	0.6	
Security	Confidentiality	Low	Low	Low	High	Medium	0.4	0.4
	Integrity	Low	Low	Low	High	Medium	0.4	
	Accountability	Low	Low	High	High	High	0.4	
	Availability	High	Low	Low	High	High	0.6	
Maintainability	Reusability	High	High	High	Low	High	0.8	0.6
	Modifiability	Low	Low	Low	High	High	0.4	
Portability	Adaptability	High	High	High	Low	Low	0.6	0.6
	Installability	High	High	High	Low	Medium	0.6	
	Replaceability	High	High	High	Low	Low	0.6	
							Average Score	5.63

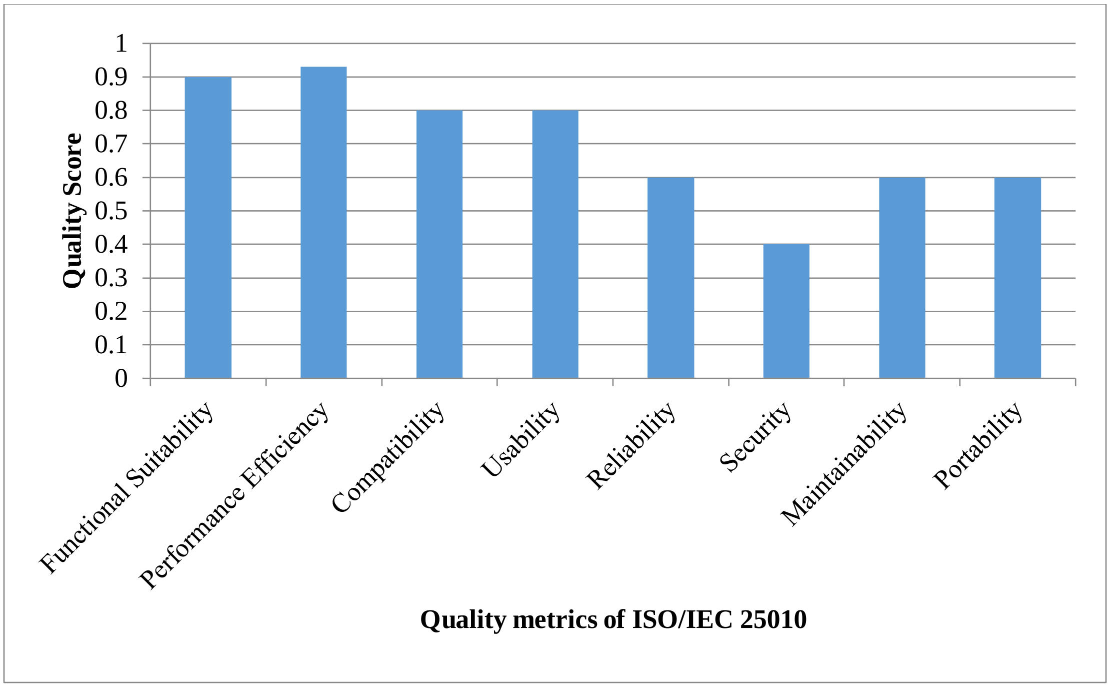

Figure 7. Overall quality measures for the various evaluation metrics of the ISO/IEC 25010

Figures 4, 5, and 6 show the simulation results of the room temperature-based fan controller, smoke controller, and water level controller. Face recognition based system is more secure among all the implemented applications, whereas other applications are sensitive to external disturbances and interferences. The proposed method has shown better performance efficiency, functionality suitability, compatibility, and usability. Fig. 7 shows overall quality measures for the various evaluation metrics of the ISO/IEC 25010 for IoT-based home automation systems. The average quality score of the proposed evaluation is 5.63. Table 3 shows the comparison of the proposed quality model with the existing system. The proposed study has considered compatibility, security, and maintainability as the new measures for the software quality assurance of IoT-based applications. The evaluation of various quality metrics has shown improvement in the quality metrics of the IoT-based systems.

TABLE III. PERFORMANCE COMPARISON WITH EXISTING METRIC

Sr. No	Quality Metrics	Oh Gioug et al. [24]	Mi Kim [10]	Proposed Method
1	Functional Suitability	Yes	Yes	Yes
2	Performance Efficiency	Yes	Yes	Yes
3	Compatibility	No	No	Yes
4	Usability	Yes	No	Yes
5	Reliability	Yes	Yes	Yes
6	Security	No	No	Yes
7	Maintainability	No	No	Yes
8	Portability	Yes	Yes	Yes

V. CONCLUSION

The current research work has introduced an approach to design Quality Assurance to evaluate the quality factors of IoT applications based on the modified ISO/IEC 25010 Quality Model. It will help to evaluate the non-conventional features of IoT applications. A virtual environment of the Home Automation Application has been created using MATLAB Simulink to evaluate quality attributes. Five scenarios for home automation using the fuzzy controller and machine learning-based algorithms are considered. The quality is evaluated using eight significant characteristics of the modified ISO/IEC 25010: compatibility, functional suitability, maintainability, portability, reliability, security, and usability. It is observed that the proposed modified ISO/IEC 25010 models help to evaluate the proper quality assurance of IoT-based systems. In the future, the proposed model can be extended for the quality assurance of the real-time android based IoT applications. This approach further can be used to incorporate in the framework of IoT Governance.

REFERENCES

[1] Kiruthika, J; and Khaddaj, S., Software Quality Issues and Challenges of Internet of Things. Proc. IEEE DCABES, China. August 18-24(2015) 176-179.

[2] Tambotoh, Johan J.C.; Isa Sani M., Software quality model for the Internet of Things governance. Proc. IEEE ICoDSE, Indonesia. (2016) 26-27.

[3] European Research Cluster., Internet of Things: IoT Governance, Privacy and Security Issues. European Research Cluster of Internet Things, (2015) 1-128.

[4] Weber, R. H., Internet of things - Governance quo Vadis? Computer law & security review 29(2013) 341–347.

[5] Weber, R. H. (2011): Shift of legislative powers and multi-stakeholder governance. International Journal of Public Law and Policy, 1(1).

[6] Informatica., Holistic Data Governance: A Framework for Competitive Advantage. Retrieved from http://www.citia.co.uk/content/files/holistic-data-governance-a-framework-for-competitive-advantage_85567506.pdf., (2012).

[7] Idri, A.; Moumane, K.; and Abran, A. (2013): On the use of software quality standard ISO/IEC9126 in mobile environments. Proc. IEEE, APSEC, Thailand. 2-5,1-8.

[8] Adewumi, A.; Misra, S.; and Omoregbe, N., Evaluating Open Source Software Quality Models Against ISO 25010. Proc. IEEE CIT/IUCC/DASC/PICOM, UK. 26-28,872–877.

[9] Marwah; Mateen, Q.; and Sirshar, M., Software Quality Assurance in the Internet of Things. International Journal of Computer Applications, 109(9)(2015) 16–24.

[10] Kim, M., A Quality Model for Evaluating IoT Applications. International Journal of Computer and Electrical Engineering, 8(1), 66-76. doi: 10.17706/ijcee.2016.8.1. (2016).

[11] Fan, S. S., Shi, W. X., Wang, N., & Liu, Y., MODMbased evaluation model of service quality in the internet of things. Procedia Environmental Sciences, 11(2011) 63-69.

[12] Ferrari, G., Cappelletti, F., & Raheli, R., Simple performance analysis of multiple access RFID networks based on the binary tree protocol. International Journal of Sensor Networks, 4(2008) 194-208.

[13] Liu, J. H., & Tong, W. Q., Adaptive service framework based on grey decision-making in the internet of things. Proceedings of 2010 6th International Conference on Wireless Communications, Networking and Mobile Computing., (2010).

[14] Oh, G., Kim, D. Y., Kim, S. I., & Rhew, Y., A quality evaluation technique of RFID middleware in ubiquitous computing. Proceedings of International Conference on Hybrid Information Technology: 2(2006) 730-735.

[15] Bures, Miroslav, Tomas Cerny, and Beston S. Ahmed. Internet of things: Current challenges in the quality assurance and testing methods., In International Conference on Information Science and Applications, 625-634. Springer, Singapore, (2018).

[16] European Commission, Report on the Public Consultation on IoT Governance, (2013)1-26.

[17] Tafazolli, R.; Aghvami, H.; Cooper, R.; Dutton, W. and Dr. Upstill C., A Roadmap for interdisciplinary research on the Internet of Things. Report by Technology Strategy Board UK, (2013) 20.

[18] Almeida, V. A. F.; Doneda, D.; and Monteiro, M., Governance Challenges for the Internet of Things. IEEE Internet Computing, 19(4)(2015).

[19] Nastic, S.; Inzinger, C.; Truong, HL. and Dustdar S. (2015a): GovOps: The Missing Link for Governance in Software-Defined IoT Cloud Systems. ICSOC Workshop, Lecture Notes in Computer Science, Springer,8954.

[20] Nastic, S.; Vogler, M.; Inzinger, C.; Truong, H. L., and S. Dustdar. , RtGovOps: A runtime framework for governance in large-scale software-defined IoT cloud systems. Proc. MobileCloud, USA. March 30- April 3(2015B) 24-33.

[21] Al-Ruithe, M.; Benkhelifa, E.; and Hameed, K, A Conceptual Framework for Designing Data Governance for Cloud Computing. Proc. MobiSPC, Canada. August 15-18(2016a) 160–167.

[22] Al-Ruithe, M.; Mthunzi, S.; and Benkhelifa E., Data governance for security in IoT & cloud converged environments. Proc. AICCSA, November 29 - December 2, (2016b)1-8.

[23] Miguel, J. P.; Mauricio, D.; and Rodríguez, G., A Review of Software Quality Models for the Evaluation of Software Products. International Journal of Software Engineering & Applications (IJSEA), (2014)5(6).

[24] Ashok Kumar Renganathan, Nethaji Kochadai, Sakthimurugan Chinnaramu , IoT – An Intelligent Design and Implementation of Agent Based Versatile Sensor Data Acquisition and Control System for Industries and Buildings, International Journal of Engineering Trends and Technology 68(5) (2020) 46-53.

[25] Oh, GiOug, Doo Yeon Kim, Sang Il Kim, and Sung Yul Rhew., A quality evaluation technique of RFID middleware in ubiquitous computing., In 2006 International Conference on Hybrid Information Technology,2(2006) 730-735. IEEE.

[26] Abdygalievich, Abdymanapov Sarsengali, Alibek Barlybayev, and Kuzenbaev Batyrkhan Aman zholovich., Quality evaluation fuzzy method of automated control systems on the LMS example., IEEE Access 7(2019) 138000-138010.

[27] Bhangale, Kishor B., Kamal M. Jadhav, and Yogesh R. Shirke. "Robust Pose Invariant Face Recognition using DCP and LBP., Int. Journal of Mgmt., Tech. And Engg 8(11)(2018) 1026-1034.

[28] Bhangale, Kishor B., Prashant Titare, RaosahebPawar, and SagarBhavsar., Synthetic Speech Spoofing Detection Using MFCC And Radial Basis Function SVM., IOSR Journal of Engineering (IOSRJEN) 8(6)(2018) 55-62.

[29] Bhangale, KishorBarasu, and K. Mohanaprasad., A review on speech processing using machine learning paradigm., International Journal of Speech Technology (2021) 1-22.