Software Quality Model for Internet of Things Governance

Johan J.C. Tambotoh
Doctor of Computer Science
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.

Information System Department
Satya Wacana Christian University
Salatiga - Indonesia
johan.tambotoh@staff.uksw.edu

Sani M. Isa
Master in Computer Science
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.
sani.m.isa@binus.ac.id

Ford Lumban Gaol
Doctor of Computer Science
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.
fgaol@binus.edu

Benfano Soewito
Binus Graduate Program
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.
bsoewito@binus.edu

Harco Leslie Hendric Spits Warnars
Doctor of Computer Science
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.
shendric@binus.edu

***Abstract*— Despite the growth of the implementation of the Internet of Things (IoT) in the last decade, the IoT still continues to rise. In 2020 there will be an estimated 50 billion devices connected to the IoT. A crucial factor is the quality of service through quality governance software of IoT. The various traditional approaches of measuring the quality of software needs to be improved and adapted to the characteristics of the IoT. This study aims to provide an overview of software quality model for IoT based on ISO/IEC 25010 and information quality attributes of COBIT 4.1. Through literature review approach, we found the mapping and relationship between IoT characteristics and quality characteristics of software based on the quality of information. These results will be used as a basis for formulating the governance framework of IoT.**

Keywords—Software Quality Model; Internet of Things; ISO/IEC 25010, COBIT 4.1

I. Introduction

The convergence and proliferation of information technology trough key technologies of digital businesses have increased. Ross [1] uses the acronyms SMACIT (Social, Mobile, Analytics, Cloud and Internet of Things) to describe today's key technologies that give various benefits for businesses and organizations. SMACIT strategy promotes a digital transformation in every aspect of human life; Smart and connected products, capabilities of powerful, accessible technologies, integrated business capabilities rapidly growing new functions and changing business conditions [2].

Internet of Things (IoT), as a part of SMACIT strategy, is rising very fast. The concept of IoT originated by Auto-ID Center at MIT in 1999 [3]. The beginning of the IoT implementation is Radio Frequency Identification Systems (RFID) that connected devices and transmited information through a frequency to the internet to one achieve intelligent identification and management. The IoT implementation supported Supply Chain Management (SCM) application [4]. Formally, the IoT term was introduced in World Summit on the Information Society (WSIS) Tunisia in 2005. International Telecommunication Union (ITU) has released the Internet of Things report as the 7th series internet report of ITU [5]. During the last decade, the IoT has been implemented in the various field, including smart manufacturing [6][7], health [8], smart agriculture [9][10], smart home [11] and smart city [12][13].

The implementation of IoT has an impact on the entire system of the object associated with the internet. The governance of IoT (or IoTGov), as a part of Information Technology Governance (ITG), can help to convert the enterprise goals to the IoT goals [14]. The IoTGov is important to meet stakeholders needs and expectations, set directions and control the IoT performance. IoTGov issues such as trust, safety, compliance, and risks are an invasion of privacy and exposure of proprietary data and information. IoT operates in a complex ecosystem because an IoT application touches various layers of technology [15].

More connected devices means more entry points for potential hackers. Considering the complexity of the IoT, it is not easy to bridge the gap between governance and management aspects of IoT in the real implementation. Consequently, the IoTGov must pay attention to the sharing of resources, dynamic changes, distribution of devices and also the amount of data to manage IoT applications. To support the IoTGov, the critical issue is about software quality. Quality assurance for the IoT applications is important to make the user safer and more secure when using IoT applications. With several millions of software and hardware that connected to the object, it needs performance testing and predicting performance.

This paper is an initial research work of the IoTGov framework development. Through a literature review, this paper will describe the relationship between IoT characteristics with software quality model like ISO / IEC 25010. This model will be combined with information quality attributes in ITG framework as described in Control Objectives for Information and Related Technologies (CobiT) 4.1.

II. Literature Review

A. Internet of Things Governance

Currently, IoT governance and management are probably the most challenging topics in the IoT research area. Some issues, such as compliance, accountability, privacy, legitimacy, the uniqueness of identifiers, data control, security, and others are identified as critical factors in IoT implementation. Weber

978-1-5090-5671-2/16/$31.00 ©2016 IEEE

[16] [17] explains that the further substantial governance principle in the implementation of the IoT includes security aspects, confidentiality, privacy and data protection.

In 2011, the Technology Strategy Board [18] proposed an IoT governance research roadmap. They classified IoTGov research focus in 6 priority areas for research. They are (a) Ethical implications; (b) Accountability and liability; (c) Regulatory and standards issue; (d) Digital life and death; (e) Ownership and intellectual property rights; and (f) Aligning local, national, regional and global practices and policies.

It is not surprising that factors like ethics, accountability, compliance to standard, privacy, security and ownership become significant dimensions within IoTGov. Similar to the "traditional principle" in ITG, there are many aspects of governance structure and capability that are necessary for relation to IoT development and delivery [19]. Almeida [20] explains that IoTGov must focus on people as a central of IoTGov. To support the implementation of IoTGov, it is essential to build trust for IoT as an ecosystem, also making it compatible with human rights and ensuring that it is drafted at the measure.

European Commission (EC) has initiated a public consultation to identify those areas where public intervention would be required to allow the relevant benefits of IoTGov. This research was conducted between April and July 2012 [21]. The majority of respondents agreed that the implementation of the IoT as a physical world infrastructure and the environmental bring impact of IoT deployment. It should be addressed by specific IoT governance. They insisted that IoT governance must be defined and clear before IoT is widely implemented.

Although relatively new, the study of IoTGov has been discussed extensively. Nastic [22], [23] proposed rtGovOps as a framework for daily operational governance of IoT applications in the cloud system. This framework provides detailed mechanisms and enabling ways to reduce the complexity of IoT operational governance. This framework is expected to enable operations managers to perform custom operational governance processes more efficiently in large-scale IoT cloud systems. This framework is used on the operational side, therefore Nastic [23] suggests to use other governance approaches like CobiT to achieve the governance objectives. CobiT can be the complementary to rtGovOps and can be used to manage and trace the governance objectives. Another recommendation from this research is to make a quality assurance as a quality of services (QoS). Therefore, we propose a software quality model for IoT implementation based on ISO/IEC 25101:2011 and to use information quality attribute based on CobiT.

B. *Software Quality for IoT*

As an internet-enabled revolutionary computing technology, IoT software development and validation is critical and complex. An IoT software should be able to run between Machine to Machine (M2M), machine to the cloud, machine to objects, and much more. With the various objects and things, it makes a number of heterogeneous interconnected devices in IoT. It raises risks associated with security, quality of data, and privacy. It is the underlying concept why aspects of software quality measurement are studied early in the development IoTGov framework.

IoT application development often attracts less attention to the security implications. In fact, inline with the basic principles of application development, efforts to identify and how to overcome them need to be considered from the beginning. In 2013, the Information Systems Audit and Control Association (ISACA) conducted a survey to determine the impact of IoT on overall ITG aspects [24]. The survey conducted on 2,013 ISACA members from 110 countries. The study focused on attitudes toward privacy and safety of devices and applications connected to the IoT. Most of them argued that the information is vulnerable to be stolen (US: 90%, Mexico: 91%, India: 88%, UK: 86%). However, more than 50% believed that IoT will provide benefits. Hence the attention to devices security and the information is important. Through software quality assurance, as part of IoTGov, it concerns over the potential theft of data and information can be minimized.

Software quality assurance in IoT must consider the amount of data received, the speed of sensors, and the process of data input via tapping and typing, and various other factors. The IoT software quality assurance is a systematic way to check whether the software product meets certain requirements and standards and achieve its desired level. Several studies have linked to IoT quality software, including Hummel [25] who used incremental software quality analysis for embedded systems, Evdokimov [26] who introduced discovery services to IoT based on based on the ISO/IEC 9126, Peischl [27] who used the model-based testing for IoT software quality, and Kiruthika [28] who described some factors that influenced when designing quality models for IoT system, and Marwah [29] who performed a literature review on IoT software quality assurance.

C. *ISO/IEC 25010 – System and Software Quality Model*

As described previously, the software quality process is to assess a number of attributs and variables. The variables can be divided into two criteria, internal and external quality criteria. External quality is the user experiences when running the software in the implementation phase. Internal quality refers to the internal aspects of software, that is only seen by developers. External quality is very important for the users, while the internal quality is important to software developers [30].

In this paper, we use a model of software quality based on ISO/IEC 25010:2011–*Software Engineering: Software Product Quality Requirements and Evaluation* (SQuaRE). This standard offers a generic model that can be utilized in a variety of software quality measurement [31]. This model is the improvement and enhancement version of the ISO/IEC 9126, by adding two characters, compatibility and security.

This model is used to support the evaluation of software from different perspectives. The perspective of acquisition, development, implementation, maintenance, and evaluation or audit software are combined and interacting one to another. ISO/IEC 25010:2011 categorizes quality model internally and externally. This model consists of eight characteristics, which are further subdivided into sub-characteristics that can be measured internally and externally. These are the characteristics of this model: functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability. Measurements are performed at the level of quality attributes that exist in every sub-characters.

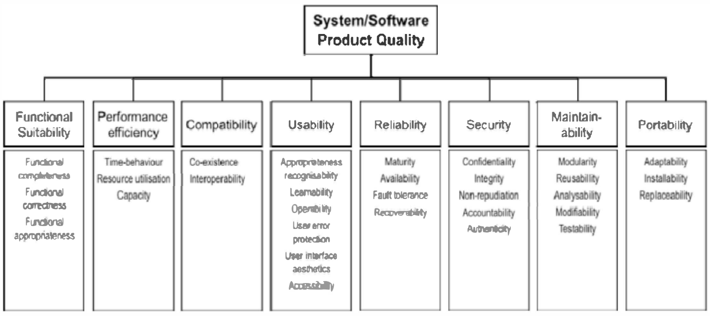

Fig. 1. Software Quality Model based on ISO/IEC25010 [30]

In this model, the software product is determined by the inherent nature of the functions, where quality is determined by the extent to which the software is able to provide certain services. The nature of the inherent quality of software products and systems are interrelated and interacting to each other. This is in accordance with the characteristics and functions in a variety of applications and devices on the IoT.

This research will explain the metric on attribute based on the criteria of information quality as shown in Fig.1. This study focuses on measuring attributes that are tailored to the nature and characteristics of the IoT. Utilization of the quality of information derived from CobiT 4.1 framework is intended to get the perspective of ITG in general. The following describes the attributes related to the quality of information that will be used in the metric.

D. *Attributes of Information Quality*

The attributes of information quality is one of the critical aspects in assuring the quality of the software. This is in accordance with the model of ISO / IEC 25010 that stresses the aspects of quality software and services. Chitumaskul [32] argues that the quality of the software is determined by the quality of process, quality of service and quality of information as shown in Fig. 2. This model is an enhancement of the Information System Success Model by DeLone and McLean [33].

Fig. 2. Relationship Between Software Quality and Information Quality [32]

Therefore this study includes information quality aspects as quality attributes, along with the attribute information on each sub-characters on ISO / IEC 25010. This is important because the characteristics of the IOT software integrates with a variety of devices and interact with each other. The quality of information used comes from IT governance framework, the COBIT 4.1. The followings are the attributes of information quality :

- The effectiveness of the information that directs the impact on the objectives of defining the IT strategic plan, which is relevant to the organization in the right time, the right way, consistent, and appropriate;
- Efficiencies that impact indirectly on the target destination controls the provision of information for defining the IT strategic plan through the optimal use of resources (the most productive and economical);
- Confidentiality of information defining the protection of sensitive IT strategic plan that should be used or not in the target purposes;
- The integrity of the accuracy and completeness of information in defining the IT strategic plan. Also to the appropriate validity values and expectations of the organization, that may have an impact or no impact on the target purposes;
- Availability could impact on the goals of the control of the IT strategic plan information as required by the organization today and in the future. Also, involves securing the necessary resources and associated capabilities;
- Compliance that impact indirectly on goals of the review of the control and management of strategic IT plan. This includes the laws, regulations, and an agreement covering the organization process, also the applicable criteria of external organizations and internal policies;
- Reliability that may affect the target control of the availability of information for defining the IT strategic plan that is appropriate for management in order to operationalize the entity and for management and governance.

III. METHODOLOGY

This study uses literature review approach to examine the attributes metric on ISO/IEC 25010 and information quality metric on CobiT 4.1. The first step is determining and mapping up the characteristics of the IoT with sub-characteristics and attribute in the ISO/IEC 25010. The second step is identifying the quality attributes that is consistent with the information quality on COBIT 4.1. After that, we create the formula and scale of quality measurement metrics. The final result is a formula that is a model of quality metrics for IoT. This model becomes part of the framework IoTGov that will be proposed in future studies.

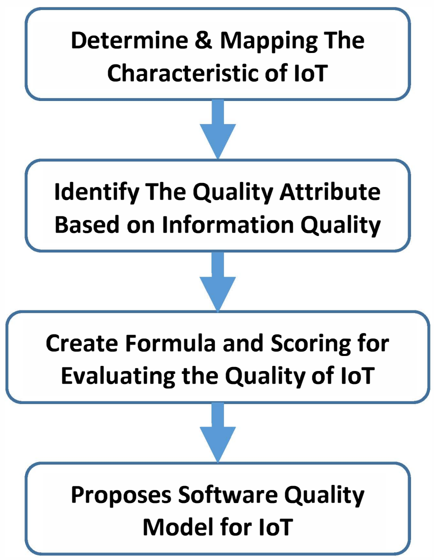

Fig. 3. Research Stages

IV. Results and Analysis

Since first introduced in a decade ago, the IoT-based applications have different characteristics than the application in general. Various studies have been conducted to etermine the characteristics of the IoT. Therefore, in this study we propose the characteristics of the IoT, based on research conducted by Khalefa [34], Idri [35], Crews [36] and Rose [37]. We categorize the IoT characteristics into 5 (five) categories as follows:

1. Embedded and adaptive devices.
   IoT device is equipped with an embedded and adaptive device that has the ability to exchange information and make an intelligent decision. This device generates large volumes of data. The IoT devices consist of two parts: software and hardware components.
2. Collaboration model and natural human interface.
   Devices collaborate with each other in IoT applications, each typically consists of multiple business processes and workflows. The collaboration includes hardware and software functions. Even some of the devices can perform the function of human nature through a special application. These interactions should consider the function of hardware and software.
3. Networked, mobility, and wireless.
   The ability of applications to mobility refers to the ease of use IoT applications. It is necessary for a quality wireless network connectivity and software to have the ability to efficiently execute some diverse functions.
4. Design to monitoring IoT devices.
   IoT device has the characteristics that can be monitored remotely. Computational intelligence is needed to ensure the implementation of this function. Software must also be able to provide real-time accurate and quality processing.
5. Always on and limited resources.
   The biggest problem IoT devices and applications are limited energy and resources. There are limitations on memory and computing power. IoT for that software should be designed efficiently but does not reduce the functions.

Based on the characteristics of the IoT, Figure 4 shows the mapping between the characteristics of the IoT, characteristics, sub-characteristics of software quality of based on ISO / IEC 25010 and information quality attributes. Every characteristic of the IoT has relationship with the character of software quality. The following is an explanation of each quality of the software.

1. Functional suitability (FS): Focus on examination function output based on input at IoT applications. To measure the extent to which the product or IoT applications can provide functionality that meets the needs that exist in certain circumstances.
2. Performance efficiency (PE): Focus on a performance of

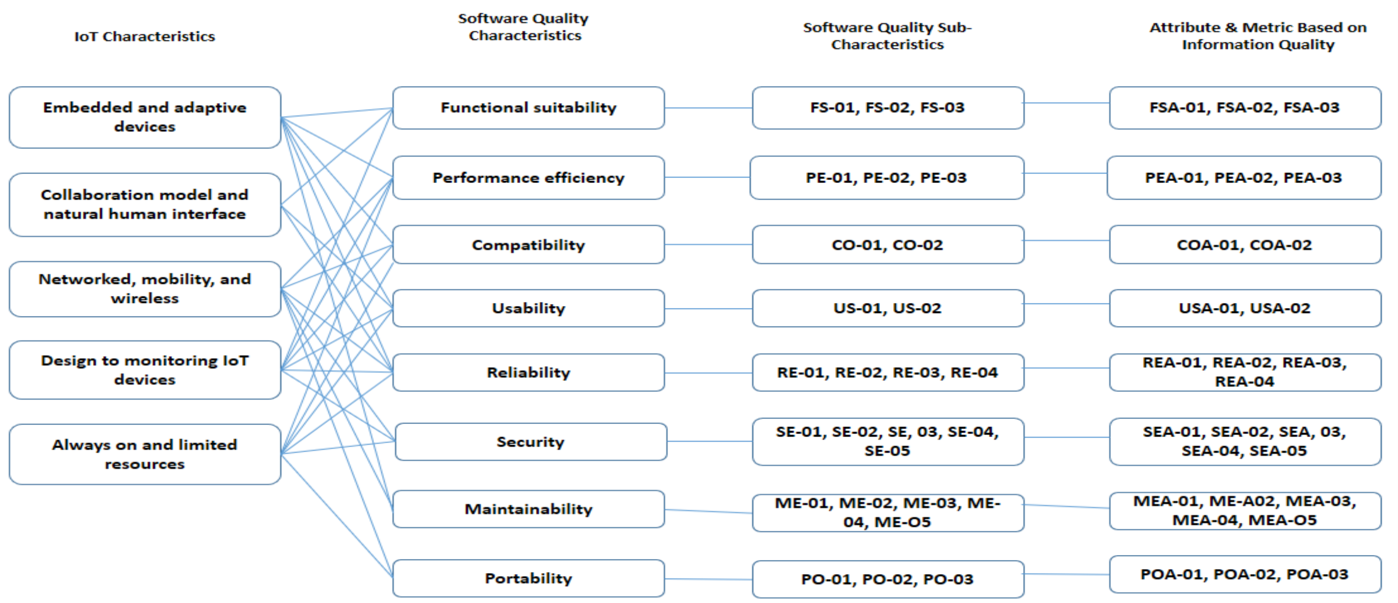

Fig 4. Mapping The IoT Characteristics of IoT and Software Quality

the IoT resources in certain circumstances. The performance measured by the response time when the application is accessed by the user, to optimize program performance, anticipation when a lack of memory, a weak battery and rapid transition to a different network.

3. Compatibility (CO): Focus on measuring the extent which components and applications can exchange the information when products, systems, and other components are interconnected. This is important because the IoT able to share information between hardware or software in the same environment.
4. Usability (US): Focus on measuring the extent to which the product or IoT-based system can be used by specified users to achieve certain goals by meeting the rules of effectiveness, efficiency, and satisfaction in a specified context. It could verify user experience of IoT applications, with respect to its usage, visibility of text, appeal, and usefulness of the content to the end user.
5. Reliability (RE): Degree to which system, product performance or components of IoT can specify the functions under specified conditions for a specified period of time.
6. Security (SE): Focus on measuring product or system on IoT to protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization. Validate privacy of data, reliability of IoT app, verification, availability, and authorization are the factors that need to be considered
7. Maintainability (MA): Focus on measuring effectiveness and efficiency with a product or system can be modified by the intended maintainers in IoT ecosystems. To verify behavior of IoT applications when battery is fully discharged, when updated version applications and get installed, or for any interruption of message or call received.
8. Portability (PO): Focus on effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment of IoT to another things or objects.

The next step in this research is to determine the measurement formula for each attribute. This formula is based on the calculation of the ratio as defined by the criteria of each sub-character ISO / IEC 25010. The following Table 1 is the formulas for each the attribute.

TABLE I. THE FORMULA OF IOT SOFTWARE QUALITY*

Sub-Char	Metrics and Attributes		Formula
(1)	(2)	(3)	(4)
FS-01: Functionality	Complete-ness of functional implemen-tation	Ratio of the number of functions correctly implemented with no omissions against the number of functions stated in the requirement spec.	X=1 – (A/B) A= Number of functions in which problems are detected in evaluation B= Number of functions checked
PE-01: Time behavior	Response time	Duration from giving an instruction to starting a batch of tasks till receiving the first response	X=time (calculated or simulated)
CO-01: Interoperability	Connection with external system	The number of cases where information is exchanged with external system or component	No. of external systems
US-01: Appropriateness recognizability	Description complete-ness Ratio	Ratio of the functions (or types of functions) stated in the manual against all usable functions	X= A/B A= Number of functions (or types of functions) B= Total number of functions (or types of functions)
RE-01: Maturity	Test appropriate ness	Ratio of the number of tests actually performed (or reviewed) against the number of tests that should be performed in order to meet the requirements	X= A / B A= Number of actually performed test cases representing operation scenario during testing. B= Number of test cases to be performed
SE-01: Confidentiality	Illegal access control performan-ce	Ratio of the number of implemented functions against the number of functions used to control illegal access	X= A / B A= Number of detected illegal operations B= Number of illegal operations anticipated in specification
MA-01: Modularity	Condensa-bility	Degree of the relational strength between the function factors and information factors in a class or package	LCOM* (Lack of Cohesion in Methods) is an index to measure condensability of source code of the object-oriented language
PO-01: Accessibility & Installability	Ease of implement ation performan-ce	Ratio of correct implementation of a system It	X = A/B A = No. of operations performed by changing the procedures at implementation B = A series of total number of operations required for implementation

**example for each sub-characteristics.*

V. CONCLUSIONS & FUTURE WORKS

Based on the results of this study, it shows the relationship between the characteristics of the IoT with the characteristics of software and information quality. As mentioned earlier, this model is one part of the IoTGov framework that will be proposed in next research. Aspects of data security and confidentiality of data and the information quality are shown in the mapping and the metrics described above. The limitation of this study was the model has not been validated. Future studies will focus on validation and measurements based on a formula and formulate a framework IoTGov simultaneously with implementation guideline.

REFERENCES

[1] J. W. Ross, I. Sebastian, and N. O. Fonstad, "Define Your Digital Strategy - Now," *Cent. Inf. Syst. Res. - MIT Sloan Manag.*, vol. XV, no. June 2015, pp. 1–4, 2015.

[2] J. W. Ross, I. M. Sebastian, and C. M. Beath, "How To Create a Great Digital Strategy," 2016.

[3] S. Sarma, D. Brock, and K. Ashton, "The networked physical world.TR MIT-AUTOID-WH-001 MIT Auto-ID Centre," *Auto-ID Cent. White Pap. MIT- …*, pp. 1–16, 2000.

[4] F. Wang, L. Hu, J. Hu, J. Zhou, and K. Zhao, "Recent Advances in the Internet of Things : Multiple Perspectives," *IETE Tech. Rev.*, vol. 4602, no. April, pp. 1–11, 2016.

[5] International Telecommunication Union, "The Internet of Things," 2005.

[6] C. Yang, W. Shen, T. Lin, and X. Wang, "IoT-enabled dynamic service selection across multiple manufacturing clouds," *Manuf. Lett.*, vol. 7, pp. 22–25, 2016.

[7] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Trans. Ind. Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[8] H. J. La, "A conceptual framework for trajectory-based medical analytics with IoT contexts," *J. Comput. Syst. Sci.*, vol. 82, no. 4, pp. 610–626, 2016.

[9] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Comput. Electron. Agric.*, vol. 118, pp. 66–84, 2015.

[10] Y. Liu, W. Han, Y. Zhang, L. Li, J. Wang, and L. Zheng, "An Internet-of-Things Solution for Food Safety and Quality Control: A Pilot Project in China," *J. Ind. Inf. Integr.*, 2016.

[11] K. K. Du, Z. L. Wang, and M. Hong, "Human machine interactive system on smart home of IoT," *J. China Univ. Posts Telecommun.*, vol. 20, no. SUPPL. 1, pp. 96–99, 2013.

[12] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 3, pp. 81–93, 2014.

[13] V. Scuotto, A. Ferraris, and S. Bresciani, "Internet of Things: Applications and challenges in smart cities: a case study of IBM smart city projects," *Bus. Process Manag. J.*, vol. 22, no. 2, pp. 357–367, 2016.

[14] ISO/IEC, "Internet of Things (IoT) Preliminary Report 2014," 2015.

[15] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, no. November, pp. 146–164, 2015.

[16] R. H. Weber, "Internet of things – Need for a new legal environment?," *Comput. Law Secur. Rev.*, vol. 25, no. 6, pp. 522–527, 2009.

[17] R. H. Weber, "Internet of things - Governance quo vadis?," *Comput. Law Secur. Rev.*, vol. 29, no. 4, pp. 341–347, 2013.

[18] R. Tafazolli, H. Aghvami, W. Dutton, and U. Colin, "A Roadmap for Interdisciplinary Research on the Internet of Things," 2012.

[19] Internet of Things European Research Cluster, *Internet of Things 2012 New Horizons.* PlatinumPrint, 2012.

[20] V. A. F. Almeida, D. Doneda, and M. Monteiro, "Governance Challenges for the Internet of Things," *IEEE Internet Comput.*, vol. 19, no. 4, pp. 56–59, 2015.

[21] European Commission, "Report on the Public Consultation IoT Governance," 2013.

[22] S. Nastic, C. Inzinger, H.-L. Truong, and S. Dustdar, "GovOps: The Missing Link for Governance in Software-defined IoT Cloud Systems," *10th Int. Work. Eng. Serv. Oriented Appl. conjunction with ICSOC 2014*, p. to appear, 2014.

[23] S. Nastic, M. Vögler, C. Inzinger, H.-L. Truong, and S. Dustdar, "rtGovOps: A Runtime Framework for Governance and Operations in Large-scale IoT Cloud Systems," in *Proc. Intl. Conf. on Mobile Cloud Computing, Services, and Engineering*, 2015, no. JANUARY, pp. 24–33.

[24] ISACA, "Risks and Rewards of the Internet of Things," 2013.

[25] B. Hummel and T. Kinnen, "Incremental Software Quality Analysis for Embedded Systems," in *EmbeddedWorld2015*, 2015, pp. 1–5.

[26] S. Evdokimov, B. Fabian, S. Kunz, and N. Schoenemann, "Comparison of Discovery Service architectures for the Internet of Things," in *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, UMC 2010 - 2010 IEEE International Workshop on Ubiquitous and Mobile Computing*, 2010, pp. 237–244.

[27] B. Peischl, "Software quality research: From processes to model-based techniques," in *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2015, no. 1, pp. 1–6.

[28] J. Kiruthika and S. Khaddaj, "Software Quality Issues and Challenges of Internet of Things," *2015 14th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci.*, pp. 176–179, 2015.

[29] Marwah, Q. Mateen, and M. Sirshar, "Software Quality Assurance in Internet of Things," *Int. J. Comput. Appl.*, vol. 109, no. 9, pp. 16–24, 2015.

[30] C. Moturi and P. Mbiwa, "An evaluation of the quality of management information systems used by SACCOs in Kenya.," *TQM J.*, vol. 27, no. 6, pp. 798–813, 2015.

[31] J. Heidrich, D. Rombach, and M. Klas, "Software Project Management in a Changing World," in *Software Project Management in a Changing World*, 2014, pp. 1–32.

[32] W. Chutimaskul, S. Funilkul, and V. Chongsuphajaisiddhi, "The quality framework of e-government development," *Proc. 2nd Int. Conf. Theory Pract. Electron. Gov. - ICEGOV '08*, p. 105, 2008.

[33] S. Petter, W. DeLone, and E. McLean, "Information Systems Success: The Quest for the Independent Variables," *J. Manag. Inf. Syst.*, vol. 29, no. 4, pp. 7–62, 2013.

[34] M. S. Khalefa, M. A. Jabar, W. N. Hussein, H. A. Alasad, and H. F. Zmezm, "The Internet of Things Software Architectural Solutions," *Aust. J. Basic Appl. Sci.*, vol. 9, no. 33, pp. 271–277, 2015.

[35] A. Idri, K. Moumane, and A. Abran, "On the use of software quality standard ISO/IEC9126 in mobile environments," in *Proceedings - Asia-Pacific Software Engineering Conference, APSEC*, 2013, vol. 1, pp. 1–8.

[36] B. Crews and S. Mangal, "The Internet of Things and Its Impact on Testing," no. January. pp. 1–26, 2012.

[37] K. Rose, S. Eldridge, and C. Lyman, "The internet of things: an overview," 2015.