Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.039736
Article

Evaluation of IoT Measurement Solutions from a Metrology Perspective

Donatien Koulla Moulla[1,2,*], Ernest Mnkandla[1] and Alain Abran[3]

[1]School of Computing, University of South Africa, Johannesburg, 1709, South Africa
[2]Department of Fundamental Sciences, University of Maroua, Maroua, 46, Cameroun
[3]Department of Software Engineering and Information Technology, École de Technologie Supérieure, Montréal, H3C 1K3, Canada
*Corresponding Author: Donatien Koulla Moulla. Email: moulldk@unisa.ac.za
Received: 13 February 2023; Accepted: 08 May 2023; Published: 28 July 2023

Abstract: To professionally plan and manage the development and evolution of the Internet of Things (IoT), researchers have proposed several IoT performance measurement solutions. IoT performance measurement solutions can be very valuable for managing the development and evolution of IoT systems, as they provide insights into performance issues, resource optimization, predictive maintenance, security, reliability, and user experience. However, there are several issues that can impact the accuracy and reliability of IoT performance measurements, including lack of standardization, complexity of IoT systems, scalability, data privacy, and security. While previous studies proposed several IoT measurement solutions in the literature, they did not evaluate any individual one to figure out their respective measurement strengths and weaknesses. This study provides a novel scheme for the evaluation of proposed IoT measurement solutions using a metrology-coverage evaluation based on evaluation theory, metrology principles, and software measurement best practices. This evaluation approach was employed for 12 IoT measure categories and 158 IoT measurement solutions identified in a Systematic Literature Review (SLR) from 2010 to 2021. The metrology coverage of these IoT measurement solutions was analyzed from four perspectives: across IoT categories, within each study, improvement over time, and implications for IoT practitioners and researchers. The criteria in this metrology-coverage evaluation allowed for the identification of strengths and weaknesses in the theoretical and empirical definitions of the proposed IoT measurement solutions. We found that the metrological coverage varies significantly across IoT measurement solution categories and did not show improvement over the 2010–2021 timeframe. Detailed findings can help practitioners understand the limitations of the proposed measurement solutions and choose those with stronger designs. These evaluation results can also be used by researchers to improve current IoT measurement solution designs and suggest new solutions with a stronger metrology base.

Keywords: Internet of Things; IoT measurement solutions; software engineering measurement; metrology; metrics

1 Introduction

The term 'Internet of Things' was coined by Kevin Ashton in 1999 while working at Procter and Gamble [1]. IEEE defines an Internet of Things (IoT) system as "a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating" [2]. Madakam et al. [3] defined IoT as "an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in the face of situations and changes in the environment".

IoT has shown potential benefits in several domains, including environmental, medical, industrial, transportation, manufacturing, and governance [4]. However, many research challenges still need to be addressed, such as privacy, energy management, information security, network, and information processing [5]. As in other disciplines, the availability of performance measures would enable planning and verification that an IoT system performs as desired and expected. IoT performance measurement solutions are important for managing the development and evolution of IoT systems, as they provide insights into performance issues, resource optimization, predictive maintenance, security, reliability, user experience, etc. An IoT system can be evaluated using many artifacts, such as software, service and application support layers, network, hardware, management and security capabilities [6].

A 2022 systematic literature review (SLR) in [5] identified 158 different IoT measurement solutions designed by researchers and proposed to practitioners. While this large number is interesting for the coverage of a variety of IoT measurable elements, without an understanding of their strengths and weaknesses, how can practitioners understand the limitations of the proposed measurement solutions and choose those with stronger designs? Similarly, how can researchers evaluate the current IoT measurement solution designs and suggest new solutions with stronger measurement designs? While previous studies proposed several IoT measurement solutions in the literature, they did not evaluate any individual one to figure out their respective measurement strengths and weaknesses. Because of the complexity and diversity of IoT systems, most of the related previous studies focused on specific metrics and, to the best of our knowledge, there has not yet been an independent evaluation, from either a theoretical or an empirical perspective, of the designs of the proposed IoT measurement solutions. This study evaluates the design of IoT measurement solutions using the metrology coverage evaluation method proposed by Abdallah et al. [7].

While a number of distinct approaches have been proposed in the literature for the validation of software metrics, such as in Card et al. [8], Fenton et al. [9], Zuse [10], and Schneidewind [11], the approach in Abdallah et al. [7] is based on the book 'Software Metrics and Software Metrology' [12], which consolidated these previous works and integrated the criteria from the classical metrology discipline applicable in all domains of science. This evaluation method was applied in the present study to evaluate 158 different IoT measurement solutions identified in 37 studies and three bibliographic references selected in the SLR from 2010 to 2021 [5].

The remainder of this paper is organized as follows. Section 2 provides an overview of related research, and Section 3 presents the method for evaluating metrology coverage. Section 4 presents a metrology evaluation of the selected studies on IoT measurement solutions. Section 5 looks at metrology coverage from four perspectives: an improvement over time, across IoT categories, within each study included in this study, and the implications for IoT practitioners and researchers. Section 6 concludes the paper with a summary of key findings and suggests potential areas of exploration for future work.

2 Related Work

Researchers have proposed IoT measurement solutions for software, security requirements, network, hardware, quality requirements, etc. A systematic literature review of IoT metrics in [5] reported that there are several studies on network metrics, whereas other categories have received less research attention. Zhang et al. [13] proposed an ontology model for IoT security to define the components of IoT security threats and inference rules for threat analysis. The model facilitates the implementation of security measures for the IoT but does not account for monitoring the overall security of the IoT. Fizza et al. [14] categorized Quality of Experience (QoE) metrics into four layers: device, network, computing, and user interface. Kuemper et al. [15] developed a framework for evaluating the quality of the information and data metrics in IoT systems. Klima et al. [16] conducted a literature review on the quality and test metrics in IoT systems, with some studies indicating that software characteristics play a significant role in determining the energy efficiency of a software system [17,18]. Quality of Service (QoS) evaluates the quality, efficiency, and performance of IoT devices, systems, and architectures [19]. Some QoS metrics, such as reliability, cost, energy consumption, security, availability, and service time, are essential and required for IoT services [20]. Pandey et al. [21] presented an approach for measuring the validity of data quality in IoT applications using metrics, such as usability, availability, timeliness, and completeness. da Cruz et al. [22] proposed a set of qualitative and quantitative metrics that can be used to compare the performances of different IoT middleware solutions.

Evaluating IoT systems has been found to be challenging owing to several issues such as the non-quantifiable values of some proposed measurement solutions [6], mathematical formulas, and measurement units at times unspecified or ill-defined, and some proposals are at odds with others. To address this issue, some researchers have suggested the use of weighting factors [6], including performance metrics pertaining to security and privacy threats [23,24] and those associated with energy efficiency [25].

Mustapää et al. [26] proposed an IoT digital validation system through a metrology-based data traceability chain from IoT devices to end users to ensure data trustworthiness for critical applications. Sousa et al. [27] used open standards such as IEC 62264 and ISO 23952:2020 to design a generic framework and interface for integrating measuring devices in an IoT architecture. An experimental case example within the steel manufacturing sector was used to validate the proposed approach, and the results indicated that the suggested generic interface can reduce product and process defects in the manufacturing industry.

Ačko et al. [28] and Eichstädt et al. [29] addressed the communication and data exchange issues in IoT environments. They used a formal framework for the transmission of metrological data that relies on the International System of Units (SI) to ensure clear, universal, secure, and standardized communication of metrological smart data in the IoT and Industry 4.0. Eichstädt et al. [30] discussed some of the main challenges and possible future impacts of metrology on digital transformations. They showed the importance of metrology in achieving trust and confidence in data and algorithms, cyber-physical systems, and quality infrastructure. According to Kuster [31], the adoption of a measurement information infrastructure (MII) and digital metrology can enable cost savings in infrastructure, which will improve the cost-risk balance specifically for IoT sensors.

Many working groups have worked on the standardization of IoT device measurements [6,32,33], but few have focused on the evaluation of IoT measurement solutions. Other researchers have provided quality models for evaluating the quality of IoT applications and services taking into account the characteristics of IoT systems [34–36].

Soubra [4] proposed an approach for defining universal metrics that can be applied to any IoT device based on the ISO 25023 standard and other metrics from the measurement literature. Aslanpour et al. [37] conducted a literature review related to user experience key performance indicators (KPIs) for industrial IoT systems and found that user experience KPIs measurement for industrial IoT systems is critical for ensuring the success and adoption of these systems.

In summary, several IoT performance measurements have been proposed, most of which focus on resource utilization, response time, energy consumption, cost, and network [5,38], and their strengths and weaknesses have not been independently evaluated. Each of the 40 studies in Table A1 in the Appendix section used a different approach to design individual IoT measurement solutions for different measurement needs. Do all of these measurement designs have the full set of strengths expected from measurement solutions? Do they have some weaknesses that make them less useful to practitioners, and even harmful in some instances? How can the IoT measurement solutions proposed in the literature be improved? While our previous work in [5] built an inventory of IoT measurement solutions in the literature and answered some research questions that spanned this set of primary studies, it did not evaluate any individual one to figure out their respective measurement strengths and weaknesses. In this study, we used a metrology-based approach for individual evaluation using explicit criteria from evaluation theory, metrology principles, and software measurement best practices.

3 Evaluation Method

The metrology coverage evaluation method proposed by Abdallah et al. [7] (see Fig. 1) consists of three steps: identification of the components of the metrology coverage method, definition of the criteria and principles for evaluating metrological coverage, and application of the proposed evaluation method. Abdallah et al. [7] originally applied this metrology coverage evaluation method to enterprise architecture measurement solutions. In our study, we applied this method to a different problem domain, that is, IoT measurement solutions.

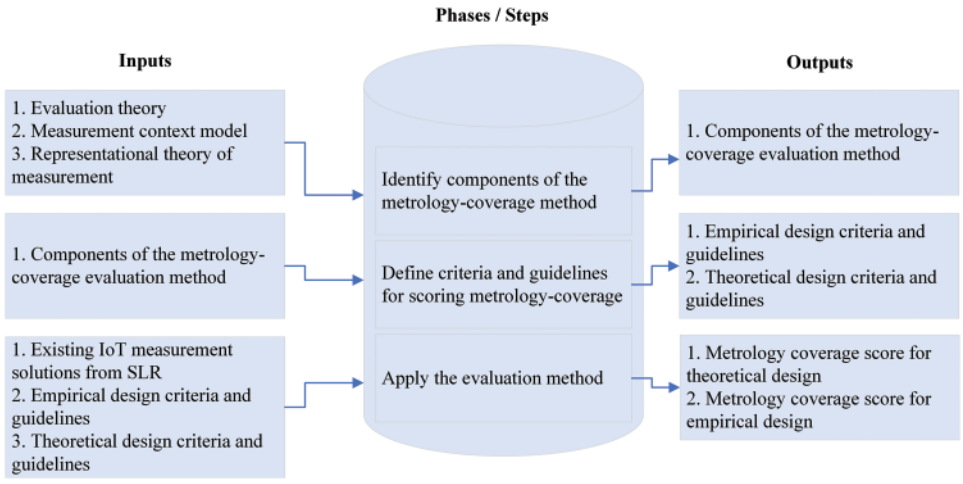

Figure 1: Methodology for designing a metrology coverage evaluation method [7]

3.1 Identification of the Components for the Metrology Coverage Method

Three components were used to design a method for evaluating the metrology coverage for IoT measurement solutions: evaluation theory [39], measurement context model [12], and representational theory of measurement [9,12].

3.1.1 Evaluation Theory

Fitzpatrick et al. [40] identified six categories of evaluation methods: objective, management, consumer, expertise, adversary, and participant-oriented. Fig. 2 presents the mandatory and basic components for conducting an evaluation using any of the methods listed.

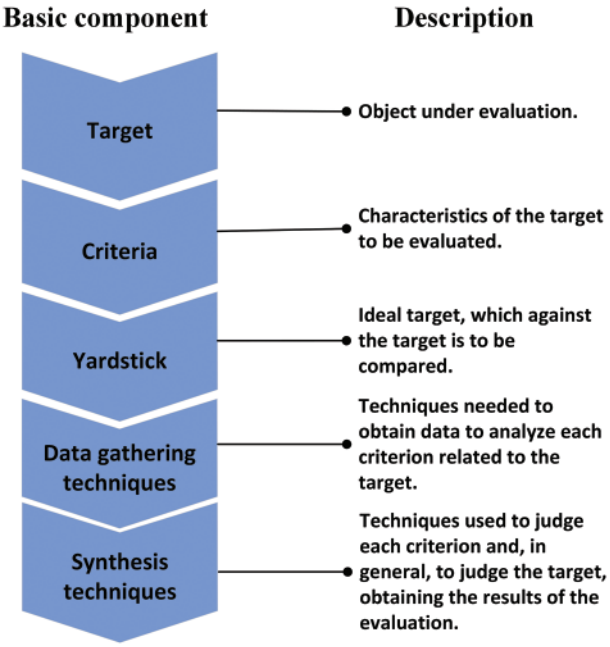

Figure 2: Basics components of evaluation methods [7]

Fig. 3 summarizes the key components of the IoT evaluation method along with a metrology coverage description for IoT measurement solutions proposed in the literature.

The components are:

- Target: Twelve categories of IoT measures as well as attributes and sub-attributes of each measured category identified in the SLR in [5]: network, energy, software, quality of experience, security, hardware, inference and data privacy, quality of an IoT service, quality of information and data quality, test, attacks and anomalies prediction, and privacy policies.
- Criteria: Measurement theory and measurement context model.
- Yardstick: Criteria of metrology and scoring guidelines.
- Data gathering techniques: Review of documentation based on the SLR in [5].
- Synthesis techniques: Presentation of the evaluation method's results.

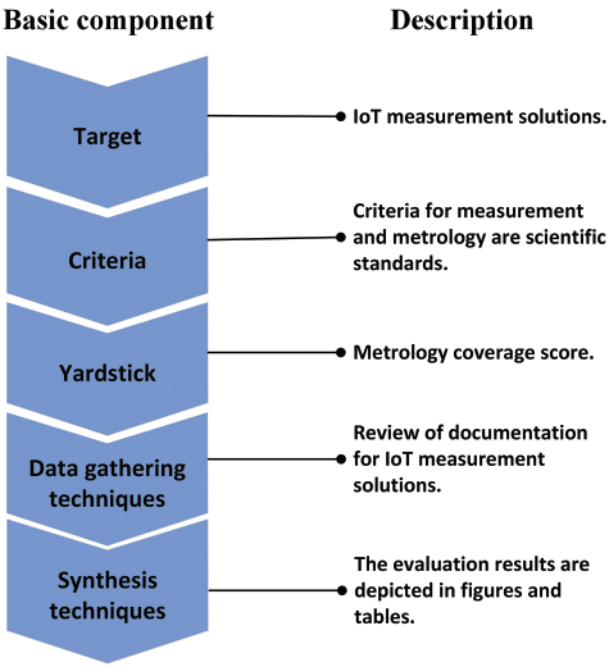

Figure 3: Key components for IoT evaluation method adapted from Abdallah et al. [7]

3.1.2 Measurement Context Model

The concept of measurement, as defined by the principles of metrology in [41], refers to the "measurement method," "application of a measurement method," and "measurement results". The measurement context model, as described by Abran [12], consists of three steps that provide the criteria for designing, applying, and exploiting the measurement results. The measurement context model includes the following criteria for the measurement method design:

1. Theoretical design criteria:
   - The attribute being measured should be clearly defined in the design.
   - The attribute being measured should be clearly decomposed in the design.
   - The relationship between the attributes and sub-attributes should be clearly defined.
   - The intended use of the measurement should be identified in the design.

2. Empirical design criteria-they should clearly describe:
   - The source of the input data should be clearly identified.
   - The input data type should be clearly identified.
   - The quantification rule should be clearly identified.
   - The mathematical operations should be mathematically valid.
   - The measurement unit should be clearly stated (internationally recognized).

3.1.3 Representational Theory of Measurement

Quantification rules must be identified and followed when mapping an attribute to a numerical world. For example, the software size in lines of code (LOC) is measured and converted into

another measurement unit (KLOC for Kilo lines of code). The mapped attribute must be based on a measurement scale type with a unit of measurement. Additionally, the mathematical operations performed on numbers must be permissible and conform to the quantification rules defined in [12].

3.2 Metrology Criteria Definition and Scoring Guidelines

3.2.1 Theoretical Design Criteria

The following theoretical design criteria were used:

- Definition of the attributes being measured.
- Decomposition of the attributes to a finer level to enable quantification.
- Definition of the sub-attributes.
- Usage identification of the measurement results.

Fig. 4 presents a description of the evaluation scoring guidelines for theoretical design.

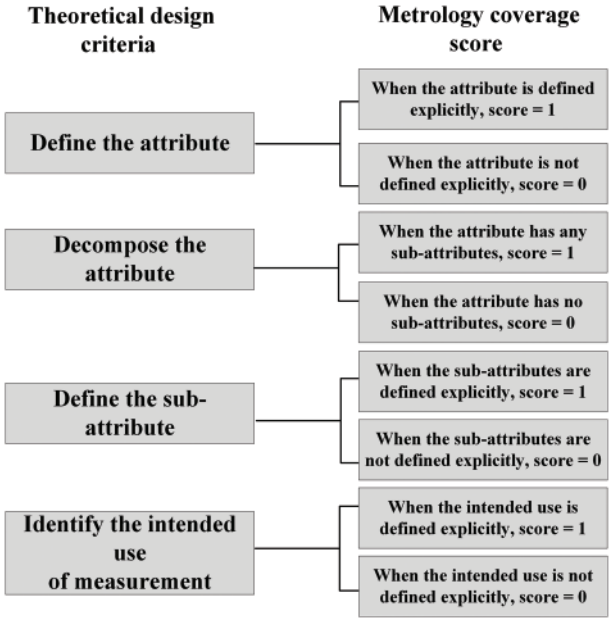

Figure 4: Theoretical design: Scoring guidelines for evaluation [7]

3.2.2 Empirical Design Criteria

The criteria of the empirical design are:

- Determination of data input.
- Identification of the data type.
- Identification of the quantification point of view.
- Identification of the rules for quantifying IoT measures and concepts.
- Determining if the collected input data was subjected to any mathematical operation before its use in the analysis models.
- Determining the use of an internationally recognized unit of measurement to quantify IoT measures.

Fig. 5 presents the evaluation scoring guidelines for empirical design.

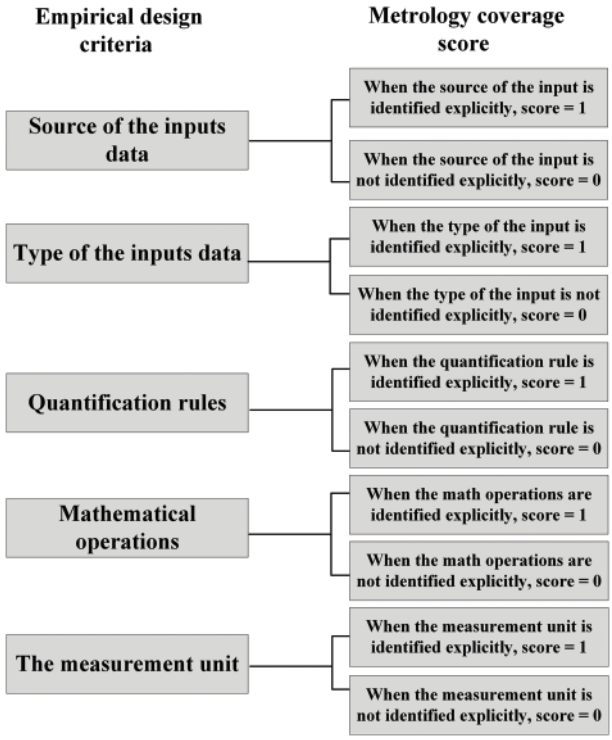

Figure 5: Empirical design: Scoring guidelines for evaluation [7]

3.2.3 Yardstick

The yardstick is used to determine whether IoT measurement solutions meet a set of metrology criteria, known as 'metrology coverage.' Metrology coverage was calculated as follows in [7]:

$$Metro\log y\ coverage = \frac{\sum_{i=1}^{n} Metro\log y\ coverage\ score}{n} \quad (1)$$

where:

- n = the number of metrology criteria.
- If a metrology criterion is met, the metrology coverage score is 1.
- If a metrology criterion is not met, the metrology coverage score is 0.

Fig. 6 summarizes the evaluation process.

4 Metrology Evaluation of the IoT Measurement Solutions

In our previous SLR study on IoT measurements [5], we identified a total of 158 measures and grouped them into 12 distinct categories. The following structure was used to evaluate each of IoT measurement solutions separately for each of the 12 categories:

- theoretical design evaluation;
- empirical design evaluation;
- attributes evaluation.

The metrology evaluation of the first category, energy measurement solutions is presented in detail, whereas the evaluations of the other 11 categories are provided in the supplementary file.

Four measurement solutions were proposed for the energy category in six studies, S1 to S6 [5] (see Table 1). S1 and S6 represent the ID of studies 1 and 6, respectively.

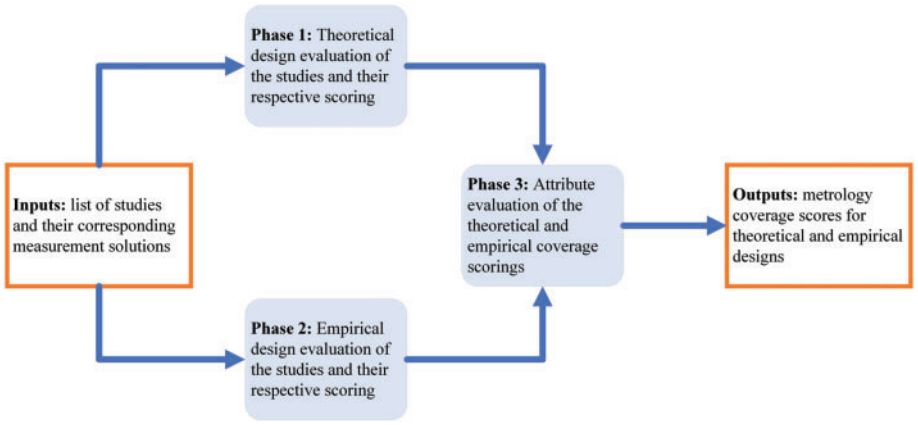

Figure 6: Metrology coverage evaluation process

Table 1: Energy measurement solutions in 6 studies

Study Id	Energy efficiency	Energy consumption	Power consumption	Residual energy
S1	✓			
S2	✓			
S3		✓		
S4	✓		✓	
S5				✓
S6			✓	✓

4.1 Theoretical Design Evaluation

Fig. 7 shows the evaluation results for each theoretical design criterion and lists above each scoring the related studies (Si). For instance, for the "define the sub-attributes" criterion, scoring = 1 for S4 and S6 and, scoring = 0 for S1, S2, S3 and S5. The metrology coverage for this criterion was calculated as follows:

$$Metro\log y\ coverage = \frac{\sum_1^6 0+0+0+1+0+1}{6} \tag{2}$$

The metrology coverage evaluation showed that 33% of the studies defined sub-attributes (S4 and S6).

From Fig. 7, the theoretical design strengths (in blue) and weaknesses (in red) are depicted, as follows:

1. Design strength:
   - Eighty-three percent of the studies met the fifth criterion ("identify the intended use of measurement").

2. Design weaknesses:
    - Half of the studies failed to satisfy the first and second criteria;
    - Sixty-seven percent of the studies failed to satisfy the third criterion.

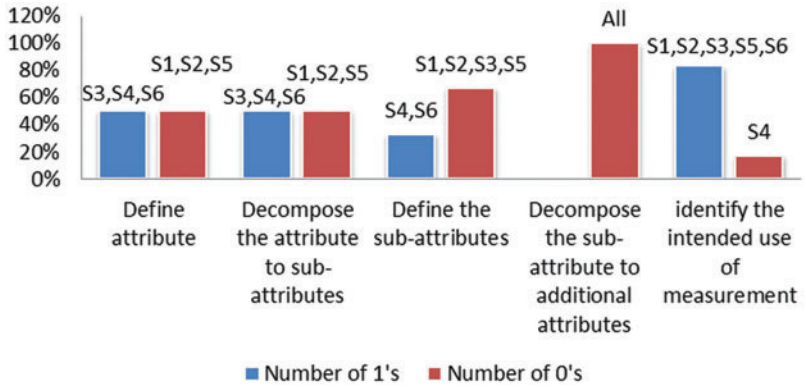

Figure 7: IoT energy measurement–heoretical design: Metrology coverage

4.2 Empirical Design Evaluation

Fig. 8 shows the evaluation results for each empirical design criterion and lists above each scoring the related studies (Si). For instance, the "Identify quantification rule" criterion was scored 1 for S4 and 0 for S1, S2, S3, S5, and S6 (see Fig. 8). The metrology coverage for this criterion was calculated as follows:

$$Metrology\ coverage = \frac{\sum_1^6 0+0+0+1+0+0}{6} \tag{3}$$

Metrology coverage evaluation showed that 17% of the studies identified the quantification rules (S4).

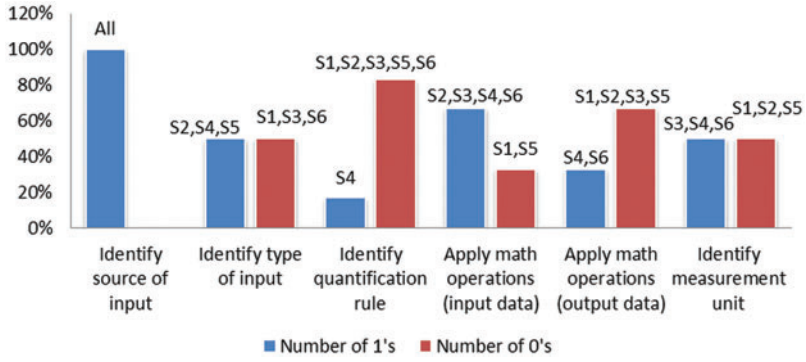

Figure 8: IoT energy measurement–empirical design: Metrology coverage

A summary of the strengths and weaknesses of each metrology criterion for the analyzed measurement solutions is presented as follows:

1. Design strengths:
    - All of the studies met the first criterion ("identify source of input");

- Sixty-seven percent of studies met the fourth criterion.

2. Design weaknesses:
   - Half of the studies failed to satisfy the second and sixth criteria;
   - Eighty-three percent of the studies failed to satisfy the third criterion.

4.3 IoT Energy Attributes Evaluation

In Fig. 9, the coverage scores for both theoretical and empirical energy attributes are depicted within each related paper from the SLR [5].

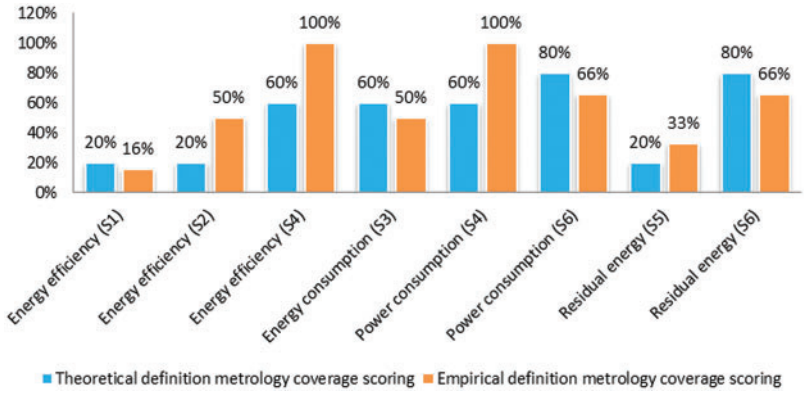

Figure 9: IoT energy attributes-theoretical and empirical metrology coverage

To summarize:

- Energy efficiency and power consumption: Their theoretical design received a significantly lower coverage score in comparison to their empirical design.
- Energy consumption and residual energy: The theoretical design achieved a higher coverage score compared to the empirical design.

5 Discussions

The evaluation of IoT measurement solutions is discussed in this section through the following four questions:

1. Has the metrology coverage improved over time?
2. How does the metrology coverage vary across IoT categories?
3. Which studies provide the highest metrology coverage?
4. What are the implications for IoT practitioners and researchers?

5.1 Has the Metrology Coverage Improved Over Time?

To conduct a timeline analysis of the metrology coverage over the 2010–2021 timeframe, the median and mean of the scoring data from 37 studies and three bibliographic references selected in an SLR from 2010 to 2021 were calculated. The medians were greater than the mean for the theoretical (60 and 57.84) and empirical (50 and 47.24) design metrology coverages, indicating that the scoring data were not normally distributed. Next, we used Spearman's correlation to determine the relationship between metrology coverage and time for both the theoretical and empirical designs. The Spearman

correlation test is commonly used for an ordinal or nominal type of data, based on the rank nature of the data. Spearman's coefficient can be interpreted as follows:

- Coefficient correlation of (1): The two variables have a strong positive relationship.
- Coefficient correlation of (−1): The two variables have a perfectly negative relationship.
- Coefficient correlation of 0: there is no relationship between the two variables.

A positive correlation indicates that metrology coverage improves over time. We also defined the null and alternative hypotheses as follows:

- Null hypothesis: There is no correlation between the metrology coverage criteria and time (rs = 0 and *P*-value > 0.05).
- Alternative hypothesis: There is a correlation between the metrology coverage criteria and time (rs $\neq$ 0 and *P*-value < 0.05).

The statistical analysis results of the theoretical and empirical metrology coverage criteria showed a weak correlation:

- rs = +0.35 and *P*-value = 0.98 for theoretical;
- rs = +0.23 and *P*-value = 0.92 for the empirical.

Because the *P*-value is greater than the level of significance (P-value > 0.05) for the metrology coverage of the theoretical and empirical designs, the null hypothesis is accepted for both metrology coverage designs, and we can conclude that there has been no improvement in the metrology coverage for both the theoretical and empirical designs over time.

5.2 How Does the Metrology Coverage Vary Across IoT Categories?

Fig. 10 compares the coverage scores of the theoretical and empirical designs for the 12 categories based on their median coverage scores.

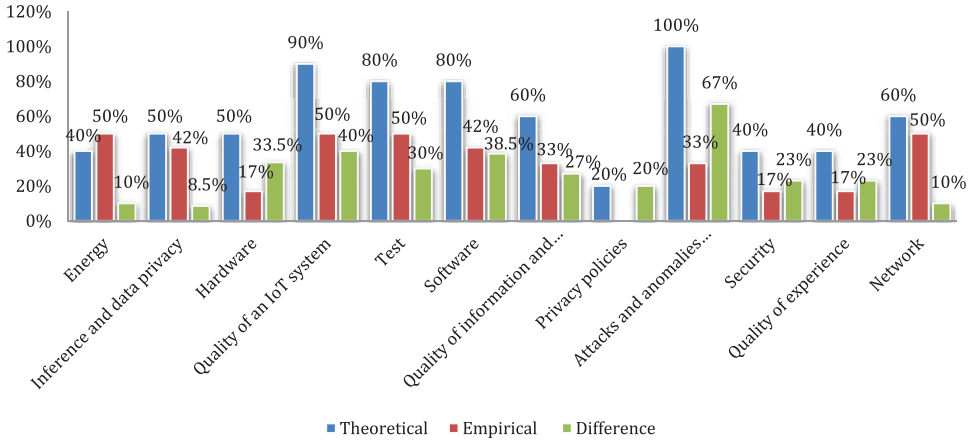

Figure 10: Comparison of theoretical and empirical metrology coverage

From Fig. 10, it can be observed that:

- The categories of quality of an IoT system, test, software, and attacks and anomalies prediction measurement solutions present the highest theoretical metrology coverage at 80% or more, whereas the categories of privacy policies, quality of experience, security, and energy presented the lowest theoretical metrology coverage at no more than 40%.

- The metrology coverage of the empirical design was relatively low for all categories (not more than 50%).

Table 2 provides the ranking of each IoT category based on theoretical and empirical definitions, which were obtained by calculating the median of its metrology coverage scores for each category.

Table 2: Ranking by IoT category of measurement solutions

IoT category	Theoretical design		Empirical design	
	Metrology Coverage (median %)	Rank of IoT category	Metrology Coverage (median %)	Rank of IoT category
Attacks and anomalies prediction	100%	1	33%	8
Quality of an IoT system	90%	2	50%	2
Test	80%	3	50%	3
Software	80%	4	42%	6
Quality of information and data	60%	5	33%	7
Network	60%	6	50%	4
Inference and data privacy	50%	7	42%	5
Hardware	50%	8	17%	9
Energy	40%	9	50%	1
Security	40%	10	17%	10
Quality of experience	40%	11	17%	11
Privacy policies	20%	12	0%	12

From Table 2, it is noted that:

1. Theoretical designs:
   - The attacks and anomalies prediction category presents the highest rank = 1, which satisfies the set of metrology criteria.
   - The privacy policies category presents the lowest (rank = 12) set of metrology criteria.
2. Empirical designs:
   - The energy category presents the highest (rank = 1) set of metrology criteria.
   - The privacy policies category presents the lowest (rank = 12) set of metrology criteria.

From Table 2, when both theoretical and empirical rankings are taken into account the 'IoT quality' category (with the 2nd ranking on both types of criteria) has a somewhat higher metrology coverage than the 'attacks and anomalies prediction' category that ranked 1st on theoretical criteria but 8th on empirical criteria.

5.3 Which Studies Present the Best Metrology Coverage?

This section presents studies with the highest theoretical and empirical metrology coverage for each category of measurement solutions.

5.3.1 Theoretical Design Evaluation

Table 3 summarizes the evaluation results of the theoretical design of each study's measurement solutions. The highlighted lines in Table 3 indicate studies with metrology coverage of 80% or more.

Table 3: Results of the theoretical designs evaluation in each study

IoT category	Study ID	Define the attribute	Decompose the attribute	Define the sub-attribute	Decompose sub-attribute to additional attributes	Identify the intended use of measurement	% metrology coverage
Energy	S1	0	0	0	0	1	20%
	S2	0	0	0	0	1	20%
	S3	1	1	0	0	1	60%
	S4	1	1	1	0	0	60%
	S5	0	0	0	0	1	20%
	S6	1	1	1	0	1	80%
Inference and data privacy	S25	0	0	0	0	1	20%
	S26	1	1	1	0	1	80%
Hardware	S16	1	1	0	0	1	60%
	Ref9	1	0	0	0	1	40%
Quality	Ref12	1	1	1	0	1	80%
	S27	1	1	1	1	1	100%
Test	Ref12	1	1	1	0	1	80%
Software	Ref11	0	0	0	0	1	20%
	Ref12	1	1	1	0	1	80%
	S28	1	1	1	0	1	80%
	S29	1	1	1	0	1	80%
Quality of information and data quality	S30	1	1	0	0	1	60%
Privacy policies	S31	0	0	0	0	1	20%
Attacks and anomalies prediction	S32	1	1	1	1	1	100%
Security	S33	1	1	1	1	1	100%
	S34	0	0	0	0	0	0%
	S35	1	0	0	0	1	40%
Quality of experience	Ref9	1	0	0	0	1	40%
	S36	1	0	0	0	1	40%
	S37	1	1	1	0	1	80%

(Continued)

Table 3 (continued)

IoT category	Study ID	Define the attribute	Decompose the attribute	Define the sub-attribute	Decompose sub-attribute to additional attributes	Identify the intended use of measurement	% metrology coverage
	S7	1	1	1	1	1	100%
	S8	1	1	1	1	1	100%
	S9	1	1	1	1	1	100%
	S10	1	1	0	0	1	60%
	S11	1	0	0	0	0	20%
	S12	1	1	1	1	1	100%
	S5	1	1	1	1	1	100%
	S6	1	0	0	0	1	40%
Network	S13	1	1	1	1	1	100%
	S14	1	1	1	1	1	100%
	S15	1	1	1	0	0	60%
	S16	1	0	0	0	1	40%
	S17	1	0	0	0	0	20%
	S18	1	1	0	0	1	60%
	S19	1	1	1	0	1	80%
	S20	1	0	0	0	1	40%
	S21	1	1	0	0	1	60%
	S22	0	0	0	0	1	20%
	S23	0	0	0	0	1	20%
	S24	1	0	0	0	1	40%

The following studies provide the best metrology coverage by IoT category:

- Energy: S6;
- Inference and data privacy: S26;
- Quality: Reference 12, S27;
- Test: Reference 12;
- Software: Reference 12, S28, S29;
- Attacks and anomalies prediction: S32;
- Security: S33;
- Quality of experience: S37;
- Network: S5, S7, S8, S9, S12, S13, S14, S19.

These studies with the highest theoretical metrology coverage could be used by practitioners with greater confidence. Researchers can also identify in these studies some of the best practices for designing measurement solutions. Similarly, studies with lower scores allow researchers to identify theoretical metrological gaps in the proposed measurement solutions, which can be considered as research opportunities that can be addressed using the best practices proposed in studies with stronger metrology coverage.

5.3.2 Empirical Design Evaluation

Table 4 presents the empirical design evaluation results of the proposed measurement solutions for each study. The highlighted lines represent studies with an empirical metrological coverage of 80% or more.

Table 4: Results of the empirical designs evaluation in each study

IoT category	Study ID	Identify the source of input	Identify the type of input	Identify quantification rule	Apply math operations (input data)	Apply math operations (output data)	Identify measurement unit	% metrology coverage
Energy	S1	1	0	0	0	0	0	17%
	S2	1	1	0	1	0	0	50%
	S3	1	0	0	1	0	1	50%
	S4	1	1	1	1	1	1	100%
	S5	1	1	0	0	0	0	33%
	S6	1	0	0	1	1	1	67%
Inference and data privacy	S25	1	0	0	1	0	0	33%
	S26	1	0	1	1	0	0	50%
Hardware	S16	1	0	0	0	0	1	33%
	Ref9	0	0	0	0	0	0	0%
Quality	Ref12	1	0	1	1	0	0	50%
	S27	1	0	1	1	0	0	50%
Test	Ref12	1	0	1	1	0	0	50%
Software	Ref11	0	0	0	0	0	0	0%
	Ref12	1	0	1	1	0	0	50%
	S28	1	0	0	1	0	0	33%
	S29	1	0	1	1	0	1	67%
Quality of information and data quality	S30	1	0	0	1	0	0	33%
Privacy policies	S31	0	0	0	0	0	0	0%
Attacks and anomalies prediction	S32	1	0	0	1	0	0	33%
Security	S33	1	1	0	1	0	0	50%
	S34	0	0	0	0	0	0	0%
	S35	1	0	0	0	0	0	17%
Quality of experience	Ref9	0	0	0	0	0	0	0%
	S36	1	0	0	0	0	0	17%
	S37	1	1	0	1	0	1	67%
Network	S7	1	1	0	1	1	1	83%
	S8	1	1	0	1	1	1	83%
	S9	1	0	0	1	0	1	50%
	S10	1	0	0	1	0	1	50%
	S11	1	0	0	0	0	1	33%
	S12	1	0	0	1	1	1	67%
	S5	1	0	0	1	1	1	67%
	S6	0	0	0	0	0	0	0%
	S13	1	0	0	1	1	0	50%
	S14	1	1	1	1	1	1	100%
	S15	1	1	1	1	0	1	83%
	S16	1	0	0	0	0	1	33%

In Table 4, the following studies provide the highest empirical metrology coverage by IoT category:

- Energy: S4;
- Network: S7, S8, S14, S15, S18, S19.

5.3.3 Summary of the Findings

From Tables 3 and 4, it can be observed that:

- The most strongly met theoretical design metrology criterion is: "Identify the intended use of measurement," which was covered in 35 of the 37 selected studies.
- The most poorly met theoretical design metrology criterion is: "Decompose sub-attribute to additional attributes," which was absent in 27 of the 37 selected studies.
- The most strongly met empirical design metrology criterion is: the "Identify source of input," which was covered in 35 of the 37 selected studies.
- The most poorly met empirical design metrology criterion is: "Identify quantification rule," covered only in 8 of the 37 selected studies.

The studies highlighted in Tables 3 and 4 will allow practitioners and researchers to find stronger theoretical and empirical designs for measurement solutions, which can be implemented with more confidence. The best practices proposed in studies with stronger metrological coverage can be used to improve other studies with lower scores.

5.4 What are the Implications for IoT Practitioners and Researchers?

The study's key findings can help practitioners understand the limitations and metrology strengths and weaknesses of IoT measurement solutions and choose those with stronger designs. In Tables 3 and 4, practitioners can identify and implement stronger metrology designs from the studies that present the best rankings. This research is also valuable for both researchers and practitioners and contributes to consolidating the current knowledge bases for IoT measurement solutions, and offers guidance on selecting suitable measures for IoT systems.

Table 5: Key metrology evaluation findings by IoT category

IoT category	Theoretical design		Empirical design	
	Key strengths	Key weaknesses	Key strengths	Key weaknesses
Energy	Most of the studies specify how measurement results will be used.	Sub-attributes are never decomposed into additional ones.	The sources of inputs are always identified.	Types, quantification rules, and measurement units are not identified. Mathematical operations applied to the outputs are not based on a metrology standard.
Inference and data privacy		Most of the criteria are not met.	Sources of the measurement inputs are always identified. Mathematical operations applied to the inputs are always based on a metrology standard.	Types and measurement units of the measurement inputs are never identified. Mathematical operations applied to the outputs do not follow a metrology standard.

(Continued)

Table 5 (continued)

IoT category	Theoretical design		Empirical design	
	Key strengths	Key weaknesses	Key strengths	Key weaknesses
Hardware	Attributes are completely defined. How measurement results will be used is always described.	Sub-attributes are never defined and decomposed into additional attributes.		Most of the criteria are not met.
Quality of an IoT system	Most of the criteria are met.			Most of the criteria are not met.
Test	Most of the criteria are met.		Most of the criteria are met.	
Software	Most of the criteria are met.			Most of the criteria are not met.
Quality of information and data quality	Attributes are always defined and decomposed. Intended usage of Measurement results are always identified.	Sub-attributes are never defined and decomposed into additional attributes.		Most of the criteria are not met.
Privacy policies		Most of the criteria are not met.		All of the criteria are not met at all.
Attacks and anomalies prediction	All criteria are met.			Most of the criteria are not met.
Security		Most of the criteria are not met.		Most of the criteria are not met.
Quality of experience		Most of the criteria are not met.		Most of the criteria are not met.
Network		Most of the criteria are not met.	Most of the criteria are met.	

6 Conclusion and Future Work

Several IoT performance measurement solutions have been proposed; however, their strengths and weaknesses have not been independently evaluated. This study used a novel approach to evaluate 158 IoT measurement solutions using a metrology-coverage evaluation method. The findings can be summarized as follows:

- The metrological coverage varies significantly across IoT measurement solution categories. The metrological theoretical and empirical strengths and weaknesses of the IoT categories are summarized in Table 5.
- Practitioners can find in Tables 3 and 4 the studies that proposed an IoT measurement solution by category type, as well as their metrology coverage, providing them with an initial understanding of related strengths and gaps in terms of both theoretical and empirical limitations.

- The metrological coverage of IoT measurement solutions did not show improvement over the 2010 to 2021 timeframe.

This research work and related findings are not based on a set of assumptions, but rather on a set of explicit criteria derived from evaluation theory, metrology principles, and software measurement best practices. In terms of limitations this research work, while it identifies which limitations in terms of theoretical and empirical metrology criteria are not addressed in the primary studies, does not propose specific improvements to the weaknesses identified in the IoT measurement solutions proposed in the literature: this is best left to researchers with domains expertise.

The findings of this research can offer valuable insights for researchers and practitioners, enabling them to understand the limitations and metrology weaknesses of IoT measurement solutions and choose those with more robust designs.

Further studies should be conducted on IoT measurement solutions using our study to:

- Find the best design practices of measurement solutions in studies with the highest rankings.
- Improve previously published measurement solutions with lower scores by implementing the best practices reported in studies with stronger metrological coverage.
- Develop new ones with a stronger metrological foundation.

Funding Statement: This research was supported by the University of South Africa under Grant No. 409000.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Ashton, "That 'Internet of Things' thing," 2009. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[2] IEEE 2413-2019, *IEEE Standard for an architectural framework for the Internet of Things (IoT)*. New Jersey, USA: IEEE Standards Association, pp. 269, 2020.

[3] S. Madakam, R. Ramaswamy and S. Tripathi, "Internet of Things (IoT): A literature review," *Journal of Computer and Communications*, vol. 3, no. 5, pp. 164–173, 2015.

[4] H. Soubra, "Towards universal IoT metrics automation," in *Proc. Int. Workshop on Software Measurement and Int. Conf. on Software Process and Product Measurement (IWSM/MENSURA)*, Izmir, Turkey, pp. 1–12, 2022.

[5] D. K. Moulla, E. Mnkandla and A. Abran, "Systematic literature review of IoT metrics," *Applied Computer Science*, vol. 19, no. 1, pp. 64–81, 2023.

[6] J. Voas, R. Kuhn and P. A. Laplante, "IoT metrology," *IEEE IT Professional*, vol. 20, no. 3, pp. 6–10, 2018.

[7] A. Abdallah, A. Abran and M. Villavicencio, "Measurement solutions in the enterprise architecture literature: A metrology evaluation," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 9, pp. 2935–2957, 2022.

[8] D. Card and R. L. Glass, *Measuring Software Design Quality*. New Jersey, USA: Prentice Hall, 1990.

[9] N. Fenton and J. Bieman, *Software Metrics: A Rigorous and Practical Approach*, 3rd ed., Florida, USA: CRC Press, Inc, pp. 617, 2014.

[10] H. Zuse, *A Framework for Software Measurement*. Berlin, Germany: Walter de Gruyter, pp. 755, 1997.

[11] N. Schneidewind, "Validating software metrics: Producing quality discriminators," in *Proc. Int. Symp. on Software Reliability Engineering (ISSRE)*, Austin, TX, USA, pp. 225–232, 1991.

[12] A. Abran, *Software Metrics and Software Metrology*. New York: John Wiley & Sons Interscience and IEEE-CS Press, pp. 328, 2010.

[13] S. Zhang, G. Bai, H. Li, P. Liu, M. Zhang *et al.,* "Multi-source knowledge reasoning for data-driven IoT security," *Sensors*, vol. 21, no. 22, pp. 1–19, 2021.

[14] K. Fizza, A. Banerjee, K. Mitra, P. P. Jayaraman, R. Ranjan *et al.,* "QoE in IoT: A vision, survey and future directions," *Discover Internet of Things*, vol. 1, no. 4, pp. 1–14, 2021.

[15] D. Kuemper, T. Iggena, R. Toenjes and E. Pulvermueller, "Valid.IoT: A framework for sensor data quality analysis and interpolation," in *Proc. ACM Multimedia Systems Conf. (MMSys'18), Association for Computing Machinery*, New York, pp. 294–303, 2018.

[16] M. Klima, V. Rechtberger, M. Bures, X. Bellekens, H. Hindy *et al.,* "Quality and reliability metrics for IoT systems: A consolidated view," In: S. Paiva, S. I. Lopes, R. Zitouni, N. Gupta, S. F. Lopes, *et al.,* (Eds.), *Science and Technologies for Smart Cities. SmartCity360° 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 372, Berlin/Heidelberg, Germany: Springer, 2020.

[17] A. Hindle, "Green mining: A methodology of relating software change and configuration to power consumption," *Empirical Software Engineering*, vol. 20, no. 2, pp. 374–409, 2015.

[18] E. Jagroep, J. Broekman, J. M. E. M. van der Werf, S. Brinkkemper, P. Lago *et al.,* "Awakening awareness on energy consumption in software engineering," in *Proc. Int. Conf. on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)*, Buenos Aires, Argentina, pp. 76–85, 2017.

[19] N. Temglit, A. Chibani, K. Djouani and M. A. Nacer, "A distributed agent-based approach for optimal QoS selection in web of object choreography," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1655–1666, 2018.

[20] L. Huo and Z. Wang, "Service composition instantiation based on cross-modified artificial Bee Colony algorithm," *China Communications*, vol. 13, no. 10, pp. 233–244, 2016.

[21] R. D. Pandey and I. Snigdh, "Validity as a measure of data quality in Internet of Things systems," *Wireless Personal Communications*, vol. 126, pp. 933–948, 2022.

[22] M. A. A. da Cruz, J. J. P. C. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi and V. Korotaev, "Performance evaluation of IoT middleware," *Journal of Network and Computer Applications*, vol. 109, pp. 53–65, 2018.

[23] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in Internet of Things using the optimum authentication key," *International Journal of Computers and Applications*, vol. 42, no. 3, pp. 306–314, 2020.

[24] J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[25] M. Magno, F. A. Aoudia, M. Gautier, O. Berder and L. Benini, "WULoRa: An energy efficient IoT End-Node for energy harvesting and heterogeneous communication," in *Proc. IEEE/ACM Design, Automation & Test in Europe Conf. & Exhibition*, Lausanne, Switzerland, pp. 1528–1533, 2017.

[26] T. Mustapää, J. Autiosalo, P. Nikander, J. E. Siegel and R. Viitala, "Digital metrology for the Internet of Things," in *Proc. Global Internet of Things Summit (GIoTS)*, Dublin, Ireland, pp. 1–6, 2020.

[27] J. Sousa, J. P. Mendonça and J. Machado, "A generic interface and a framework designed for industrial metrology integration for the Internet of Things," *Computers in Industry*, vol. 138, pp. 103632, 2020.

[28] B. Ačko, H. Weber, D. Hutzschenreuter and I. Smith, "Communication and validation of metrological smart data in IoT-networks," *Advances in Production Engineering & Management*, vol. 15, no. 1, pp. 107–117, 2020.

[29] S. Eichstädt and B. Ludwig, "Metrology for heterogeneous sensor networks and industry 4.0," *Automatisierungstechnik*, vol. 68, no. 6, pp. 459–464, 2020.

[30] S. Eichstädt, A. Keidel and J. Tesch, "Metrology for the digital age," *Measurement: Sensors*, vol. 18, pp. 100232, 2021.

[31] M. Kuster, "A measurement information infrastructure's benefits for industrial metrology and IoT," in *Proc. IEEE Workshop on Metrology for Industry 4.0 & IoT*, Roma, Italy, pp. 479–484, 2020.

[32] A. Ebraheem and I. Ivanov, "IoT standardization: An overview of organizations and standards," in *Proc. Moscow Workshop on Electronic and Networking Technologies (MWENT)*, Moscow, Russian Federation, pp. 1–5, 2022.

[33] M. C. Kaya, M. Saeedi Nikoo, M. L. Schwartz and H. Oguztuzun, "Internet of measurement things architecture: Proof of concept with scope of accreditation," *Sensors*, vol. 20, no. 2, pp. 1–20, 2020.

[34] M. Kim, "A quality model for evaluating IoT applications," *International Journal of Computer and Electrical Engineering*, vol. 8, no. 1, pp. 66–76, 2016.

[35] M. Kim, J. H. Park and N. Y. Lee, "A quality model for IoT service," in *Advances in Computer Science and Ubiquitous Computing*, vol. 421. Singapore: Springer, pp. 497–504, 2017.

[36] M. Abdallah, T. Jaber, N. Alabwaini and A. A. Alnabi, "A proposed quality model for the Internet of Things systems," in *Proc. Jordan Int. Joint Conf. on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, pp. 23–27, 2019.

[37] M. S. Aslanpour, S. S. Gill and A. N. Toosi, "Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research," *Internet of Things*, vol. 12, pp. 1–20, 2020.

[38] A. Trendowicz, E. C. Groen, J. Henningsen, J. Siebert, N. Bartels *et al.,* "User experience key performance indicators for industrial IoT systems: A multivocal literature review," *Digital Business*, vol. 3, no. 1, pp. 1–26, 2023.

[39] M. López, *An Evaluation Theory Perspective of the Architecture Tradeoff Analysis Method (ATAM) (Technical Report CMU/SEI-2000-TR-012)*. Pittsburgh, PA: Software Engineering Institute, Carnegie-Mellon University, 2000.

[40] J. L. Fitzpatrick, B. R. Worthen and J. R. Sanders, *Program Evaluation: Alternative Approaches and Practical Guidelines*. Boston, USA: Pearson/Allyn and Bacon, pp. 559, 2010.

[41] ISO/IEC Guide 99:2007, *VIM ISO/IEC Guide 99 International Vocabulary of Metrology—Basic and General Concepts and Associated Terms (VIM)*. Geneva: International Organization for Standardization—ISO, 2007.

Appendix. 37 Selected primary studies and 3 additional references

Table A1: Selected primary studies

Study Id	Authors	Title	Source	Year
S1	Georgiou et al.	Software development lifecycle for energy efficiency: techniques and tools	ACM Comput. Surv.	2019
S2	Huang et al.	Building energy efficient Internet of Things by co-locating services to minimize communication	Association for Computing Machinery	2014
S3	Filho et al.	A fog-enabled smart home solution for decision-making using smart objects	Future Generation Computer Systems	2020

(Continued)

Table A1 (continued)

Study Id	Authors	Title	Source	Year
S4	Gandotra et al.	A survey on green communication and security challenges in 5G wireless communication networks	Journal of Network and Computer Applications	2017
S5	Lin et al.	Zigbee-based Internet of Things in 3D terrains	Computers & Electrical Engineering	2013
S6	Sarwesh et al.	ETRT–Cross layer model for optimizing transmission range of nodes in low power wireless networks–An Internet of Things perspective	Physical Communication	2018
S7	Amini et al.	Availability-reliability-stability trade-offs in ultra-reliable energy-harvesting cognitive radio IoT networks	IEEE Access	2020
S8	Amini et al.	Performance analysis of URLL energy-harvesting cognitive-radio IoT networks with short packet and diversity transmissions	IEEE Access	2021
S9	Li et al.	Enhancing the performance of 802.15.4-based wireless sensor networks with NB-IoT	IEEE Internet of Things Journal	2020
S10	Shahzad et al.	IoTm: A lightweight framework for fine-grained measurements of IoT performance metrics	Conference on Network Protocols	2018
S11	Al-Roubaiey et al.	EATDDS: energy-aware middleware for wireless sensor and actuator networks	Future Generation Computer Systems	2019
S12	Lima et al.	Adaptive priority-aware LoRaWAN resource allocation for Internet of Things applications	Ad Hoc Networks	2021
S13	Pundir et al.	A systematic review of quality of service in wireless sensor networks using machine learning: recent trend and future vision	Journal of Network and Computer Applications	2021

(Continued)

Table A1 (continued)

Study Id	Authors	Title	Source	Year
S14	Roy et al.	An energy optimized and QoS concerned data gathering protocol for wireless sensor network using variable dimensional PSO	Ad Hoc Networks	2021
S15	Xu et al.	Enabling robust and reliable transmission in Internet of Things with multiple gateways	Computer Networks	2018
S16	Yuan et al.	Instrumenting wireless sensor networks — A survey on the metrics that matter	Pervasive and Mobile Computing	2017
S17	Aimtongkham et al.	Multistage fuzzy logic congestion-aware routing using dual-stage notification and the relative barring distance in wireless sensor networks	Wireless Networks	2021
S18	Ramli et al.	A Study on the impact of nodes density on the energy consumption of LoRa	International Journal of Interactive Mobile Technologies	2021
S19	Paschou et al.	Health Internet of Things: metrics and methods for efficient data transfer	Simulation Modelling Practice and Theory	2013
S20	Sallum et al.	Improving quality-of-service in LoRa low-power wide-area networks through optimized radio resource management	Journal of Sensor and Actuator Networks	2020
S21	Olapure et al.	Design and analysis of RPL objective functions using variant routing metrics for IoT applications	Wireless Netw.	2020
S22	Rani et al.	A hybrid approach for the optimization of quality of service metrics of WSN	Wireless Netw.	2020
S23	Dvornikov et al.	QoS metrics measurement in long range IoT networks	Conference on Business Informatics	2017

(Continued)

Table A1 (continued)

Study Id	Authors	Title	Source	Year
S24	Faheem et al.	Mqrp: mobile sinks-based QoS-aware data gathering protocol for wireless sensor networks-based smart grid applications in the context of industry 4.0-based on internet of things	Future Generation Computer Systems	2018
S25	Abdelhameed et al.	Privacy-preserving tabular data publishing: a comprehensive evaluation from web to cloud	Computers & Security	2018
S26	Sun et al.	Inference and data privacy in IoT networks	Workshop on Signal Processing Advances in Wireless Communications	2019
S27	Kim et al.	A quality model for IoT service	Advances in Computer Science and Ubiquitous Computing	2016
S28	Baggen et al.	Standardized code quality benchmarking for improving software maintainability	Software Quality Journal	2012
S29	Pantiuchina et al.	Improving code: the (mis) perception of quality metrics	Conference on Software Maintenance and Evolution	2018
S30	Eushay et al.	Domain agnostic quality of information metrics in IoT-based smart environments	Conference on Intelligent Environments	2020
S31	Tavakolan	Applying privacy-aware policies in IoT devices using privacy metrics	Conference on Communications, Computing, Cybersecurity, and Informatics	2020
S32	Hasan et al.	Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches	Internet of Things	2019

(Continued)

Table A1 (continued)

Study Id	Authors	Title	Source	Year
S33	Setzler et al.	IoT metrics and automation for security evaluation	Consumer Communications & Networking Conference	2021
S34	Savola et al.	Towards metrics-driven adaptive security management in E-health IoT applications	Conference on Body Area Networks	2012
S35	Ge et al.	A framework for modeling and assessing security of the Internet of Things		2015
S36	Shin, D-H	Conceptualizing and measuring quality of experience of the Internet of Things: exploring how quality is perceived by users	Information & Management	2017
S37	Suryanegara et al.	A 5-step framework for measuring the quality of experience (QoE) of Internet of Things (IoT) services	IEEE Access	2019
Ref9	Fizza et al.	QoE in IoT: a vision, survey and future directions	Discover Internet Things	2021
Ref11	Cui et al.	Towards predictive analysis of android vulnerability using statistical codes and machine learning for IoT applications	Computer Communications	2020
Ref12	Klima et al.	Quality and reliability metrics for IoT systems: a consolidated view	Summit Smart City	2020