APPLIED COMPUTER SCIENCE

Applied Computer Science, vol. 19, no. 1, pp. 64–81
doi: 10.35784/acs-2023-05

Submitted: 2023-03-06 | Revised: 2023-03-18 | Accepted: 2023-03-21

Keywords: IoT metrics, Performance metrics, Software metrics, Energy consumption, Network metrics, Systematic literature review

Donatien Koulla MOULLA [0000-0001-6594-8378]*,**,
Ernest MNKANDLA [0000-0003-3989-5617]*, *Alain ABRAN* [0000-0003-2670-9061]***

SYSTEMATIC LITERATURE REVIEW OF IOT METRICS

Abstract

The Internet of Things (IoT) touches almost every aspect of modern society and has changed the way people live, work, travel and, do business. Because of its importance, it is essential to ensure that an IoT system is performing well, as desired and expected, and that this can be assessed and managed with an adequate set of IoT performance metrics. The aim of this study is to systematically inventory and classify recent studies that have investigated IoT metrics. The authors conducted a literature review based on studies published between January 2010 and December 2021 using a set of five research questions (RQs) on the current knowledge bases for IoT metrics. A total of 158 IoT metrics were identified and classified into 12 categories according to the different parts and aspects of an IoT system. To cover the overall performance of an IoT system, the 12 categories were organized into an ontology. The results show that the category of network metrics was most frequently discussed in 43% of the studies and, with the highest number of metrics at 37%. This study can provide guidelines for researchers and practitioners in selecting metrics for IoT systems and valuable insights into areas for improvement and optimization.

1. INTRODUCTION AND BACKGROUND

The expression "Internet of Things" was coined by Kevin Ashton in 1999 during his work at Procter & Gamble (Ashton, 2009). Although there is already a large body of literature on the design of the Internet of Things (IoT), investigating the performance of an IoT system has been much more challenging. Given the importance of IoT in industry and daily life, it is essential to ensure that an IoT system performs well as desired and expected. Many artifacts can be used to evaluate an IoT system, including software (IoT applications), service support and application support layer (data processing or data storage), network (networking capabilities and transport capabilities), hardware (devices capabilities), management capabilities, and security capabilities (Djam-Doudou et al., 2022).

* University of South Africa, School of Computing, Department of Computer Science, South Africa, moulldk@unisa.ac.za, mnkane@unisa.ac.za
** University of Maroua, National Advanced School of Mines and Petroleum Industries, Department of Fundamental Sciences, Cameroon, moulladonatien@gmail.com
*** École de Technologie Supérieure, Department of Software Engineering and Information Technology, Canada, alain.abran@etsmtl.ca

There are several issues related to the evaluation of IoT systems; for instance, some proposed measurement solutions are not quantifiable because of their non-quantifiable values (Voas et al., 2018). What is more, some formulas assigned to the metrics are inefficient and sometimes absent. Some proposals can be at odds with others, and to overcome this issue, some researchers have proposed weighting factors of importance applied to each individual metric (Voas et al., 2018), performance metrics related to security and privacy threats (Ahmed & Kannan, 2021; Kumar & Sharma, 2021; Yang et al., 2017; Zhou et al., 2017), and others related to energy efficiency (Magno et al., 2017; Zahoor & Mir, 2021). Other papers have proposed IoT metrics for hardware, software, network, quality requirements, security requirements, etc. An example of the latter is the study by Zhang et al. (2021) who proposed the IoT Security Threat Ontology (IoTSTO) as an IoT security ontology model to describe the elements of IoT security threats and threat analysis rules. Their model assists security managers in deploying IoT security solutions. However, their study did not consider monitoring the overall security of the IoT.

To ensure reliable IoT services, monitoring, measuring, and evaluating quality-relevant metrics are required. For instance, Fizza et al. (2021) presented a vision, survey, and future directions for Quality of Experience (QoE) research in IoT. They reviewed existing QoE definitions before conducting a literature review of techniques and approaches used to evaluate QoE in the IoT. They defined the quality metrics into four layers: device, network, computing, and user interface. Kuemper et al. (2018) proposed a framework based on quality information (QoI) metrics to assess the quality of heterogeneous data in IoT applications. Their study provided formulas for measuring the quality of information and data metrics for IoT systems.

To improve the efficiency and ensure the quality of Android applications for IoT systems, Cui et al. (2020) developed risk vulnerability prediction models based on machine learning techniques and software code metrics. However, in their study, the datasets used for building the models were relatively small.

Klima et al. (2020) reviewed the literature on quality and test metrics for IoT systems, and some studies have shown that software characteristics largely determine the energy efficiency of a software system (Hindle, 2015; Jagroep, 2017). Soubra and Abran (2017) presented the potential benefit of using functional size measurement based on the COSMIC – ISO 19761 method in the context of IoT for managing the energy consumption of IoT real-time embedded systems (RTES). Koçak (2018) explored the relationship between software code properties and energy consumption. Iwendi et al. (2020) investigated the minimization of the energy consumption of sensors in an IoT network to increase network lifetime.

In summary, a number of studies have proposed IoT metrics and their measurement automation; however, to the best of our knowledge, there has not yet been a systematic literature review (SLR) of IoT metrics which cover the different parts and aspects of an IoT system. This motivated the current SLR study of IoT metrics from 2010 to 2021. The rationale for the review is to systematically inventory and classify recent studies that have investigated IoT metrics, and therefore propose an ontology that establishes the relationships across each of the IoT performance metrics. Moreover, these metrics can help to evaluate the performance and effectiveness of IoT systems, depending on the specific use case, application, and system architecture and provide valuable insights into areas for improvement and optimization.

The rest of this paper is organized as follows. Section 2 presents the method used to conduct the SLR study. Section 3 presents the results and discussions. Section 4 concludes the paper with a summary of the key findings, study limitations, and directions for future work.

2. THE REVIEW METHOD

To perform our systematic literature review (SLR), the authors followed the guidelines proposed by Kitchenham and Charters (2007) which can be summarized in six main stages: research questions, search strategy, study selection, quality assessment, data extraction, and data synthesis. The SLR protocol is illustrated in Figure 1.

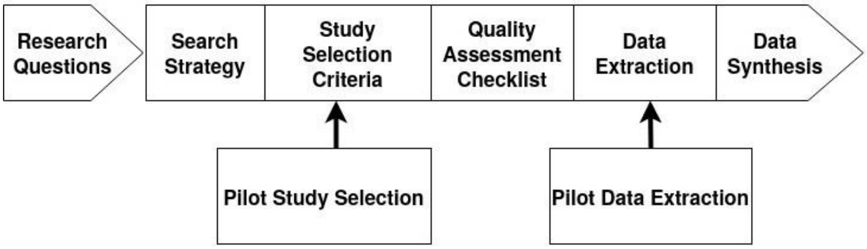


Fig. 1. The systematic review protocol

2.1. Research questions

The present SLR aims to identify and classify the different IoT metrics proposed in the literature and its current knowledge bases. Formulating the research questions is one of the important aspects of any SLR. The research questions judged relevant to this study were formulated as follows:

1. RQ1: Which are the dominant journals for papers reporting on IoT metrics?
2. RQ2: Which metrics have been used in IoT systems?
3. RQ3: What are the different categories / classification of IoT metrics?
4. RQ4: What other new metrics could be defined?
5. RQ5: What are the relationships between the different IoT metrics?

2.2. Search strategy

This section identifies the primary studies that address the research questions. The search strategy was conducted in two phases: search terms and data source. The search terms phase consisted of identifying the major terms from the selected research questions. The data source phase presents the databases used to search for and select relevant papers for our SLR.

2.2.1. Search terms

The search concentrated on key terms from the research questions as well as commonly used terms related to IoT and metrics. The research was written by combining the keywords relating to IoT and the keywords relating to metrics as follows: (“Internet of Things” OR

IoT OR “IoT systems”) AND (“IoT metrics” OR “IoT Measurement” OR “IoT performance metrics” OR “IoT network metrics” OR “IoT security metrics” OR “software metrics” OR “hardware metrics” OR “data quality metrics” OR “privacy metrics” OR “energy consumption metrics” OR “energy efficiency metrics” OR “Internet of Things metrics”).

2.2.2. Data source

The authors selected papers from five databases: Scopus, ScienceDirect, the ACM Digital Library, IEEE Xplore, and Springer. These databases were selected because they publish a significant number of research papers relevant to this study within the software engineering community. The constructed search terms were used to find journal papers, reviews, and conference papers. Because different databases' search engines use different syntax for search strings, the search terms were modified to accommodate them. A search was carried out on these five databases, focusing on the title, abstract, and keywords. To obtain relevant sources, searches on the five databases were conducted separately, and then we gathered the identified papers together. Duplicate papers were removed. To manage the search results, the Endnote reference management tool was used.

2.3. Study selection

A search from the five databases returned 180 papers. This section aims to identify next only the relevant papers that are useful to answer our research questions. Study selection criteria were used to determine which studies were included in or excluded from an SLR. For this purpose, the authors read the titles, abstracts, conclusions, or full text and applied the following inclusion and exclusion criteria to the 180 papers:

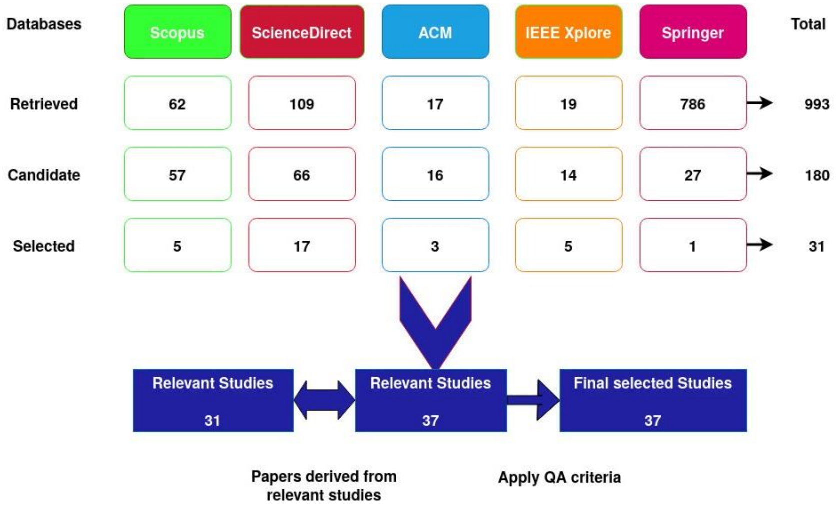
Inclusion criteria:

- The papers should be published between 2010 and 2021 and related to IoT metrics. The search was limited to this period because the IoT was launched around 2009 and we believe that a lot of research has been done in the last decade.
- The subject area should be computer science and informatics and the article types should be journals, reviews, or conference papers.

Exclusion criteria:

- Duplicated papers should be removed.
- Studies on the Internet of Things but not on IoT metrics were excluded.
- Studies not taking into account the inclusion criteria listed above were excluded.

After applying the selection criteria and quality assessment described in Section 2.4, 31 relevant papers were obtained. Then, the references of each relevant paper and identified additional papers that were not considered in the primary search, were reviewed. The selection criteria and quality assessment were also applied to these papers, and six relevant papers were returned. At the end, 37 papers were selected not including bibliographic references (see Appendix). In brief, Figure 2 provides an overview of the search, selection process, and number of selected studies retained.



Databases	Scopus	ScienceDirect	ACM	IEEE Xplore	Springer	Total
Retrieved	62	109	17	19	786	993
Candidate	57	66	16	14	27	180
Selected	5	17	3	5	1	31

Relevant Studies 31
Relevant Studies 37
Final selected Studies 37
Papers derived from relevant studies
Apply QA criteria

Fig. 2. Overview of search, selection process and results

2.4. Quality assessment

Quality assessment was used to discuss the relevance and credibility of the selected studies. The papers were selected from five well-known databases of papers reviewed by experts before their publication. In addition, for this SLR, we selected some quality evaluation questions proposed by Kitchenham and Charters (2007) that are the most appropriate for our research questions:

- Q1: Are the aims of study stated clearly?
- Q2: Are the metrics used in the study defined adequately?
- Q3: Are the findings clearly supported by the results reported?
- Q4: Are the limitations of study discussed?

Only papers that answered at least three of the above questions were selected.

2.5. Data extraction

The data extraction process allowed the extraction of the data items required to answer the research questions and study quality criteria. For each selected study, we extracted in a structured way the article title, author name, type of publication, date of publication, IoT metrics found, and the research questions addressed. It should be noted that not all of the studies selected addressed all the five research questions.

2.6. Data synthesis

Data synthesis aimed to collate and summarize the results of the included primary studies. We identified and grouped all relevant data to answer the research questions using descriptive synthesis. For descriptive statistics, we considered the number of IoT metrics found per study, the total number of IoT metrics according to the different parts and aspects of an IoT system, the relationships between the different IoT metrics, and the total number of studies per category/classification of IoT metrics.

3. RESULTS AND DISCUSSION

This section provides answers to the SLR research questions based on a synthesis of the selected studies.

3.1. RQ1: Which are the dominant journals for papers investigating IoT metrics?

Table 1 shows the distribution of the selected studies according to publication venue, type (journal or conference), and number of studies within a publication venue.

Tab. 1. Distribution of publication venues and type of the selected studies

Publication venue	Type of study	Number
Future Generation Computer Systems	Journal	3
IEEE Access	Journal	3
Wireless Network	Journal	3
IEEE Internet of Things Journal	Journal	2
Ad Hoc Networks	Journal	2
Journal of Network and Computer Applications	Journal	2
International Journal of Interactive Mobile Technologies	Journal	1
ACM Computing Surveys	Journal	1
Journal of Sensor and Actuator Networks	Journal	1
Pervasive and Mobile Computing	Journal	1
Information & Management	Journal	1
Computers & Electrical Engineering	Journal	1
Computer Networks	Journal	1
Computers & Security	Journal	1
Software Quality Journal	Journal	1
Simulation Modelling Practice and Theory	Journal	1
Physical Communication	Journal	1
International Conference on Body Area Networks	Conference	1
International Conference on Parallel and Distributed Systems	Conference	1
Annual Consumer Communications & Networking Conference	Conference	1
International Conference on Intelligent Environnements	Conference	1
International Conference on Communications, Computing, Cybersecurity, and Informatics	Conference	1
International Conference on Management of Emergent Digital EcoSystems	Conference	1
Conference on Business Informatics	Conference	1
International Workshop on Signal Processing Advances in Wireless Communications	Conference	1
Advances in Computer Science and Ubiquitous Computing	Conference	1
International Conference on Software Maintenance and Evolution	Conference	1
International Conference on Network Protocols	Conference	1

From Table 1, most of the studies were published in reputed journals with a percentage of 70% and 30% in conference proceedings. In this SLR, no journal has published more than 3 studies. As a complement to Table 1, Figure 3 presents the 2010-2021 timeline of the studies published, providing an overview of the evolution of research regarding IoT metrics.

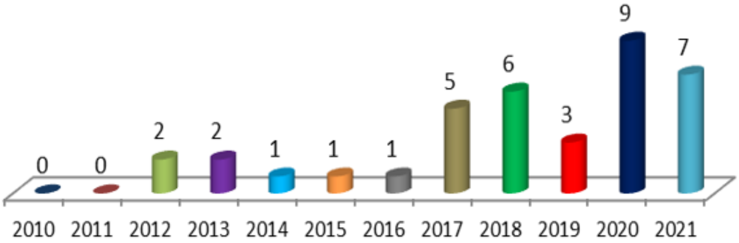


Fig. 3. Numbers of studies published per year

It has been noted that 81% of the studies have been published within the last five years and 53% of them were published in 2020 and 2021. Thus, we can conclude that IoT metrics have received increasing attention from researchers.

3.2. RQ2: Which metrics have been used in IoT systems?

The authors found from the selected studies (see Appendix), an inventory of 158 different metrics (see Table 2), of which some of these metrics have only been listed in previous studies (Cui et al., 2020; Fizza et al., 2021; Tavakolan & Faridi, 2020; Savola et al., 2012), others have been discussed in some depth (Klima et al., 2020; Kim et al., 2017), and others have been used in experiments to evaluate IoT systems (Gandotra & Jha, 2017; Hasan et al., 2019; Roy et al., 2021).

3.3. RQ3: What are the different categories / classification of IoT metrics?

According to the IoT reference model proposed by ITU-T Y.2060 (06/2012) and the different parts and aspects that affect the overall performance of an IoT system, we categorized the metrics into 12 categories: quality metrics of an IoT system or service, network metrics, quality of experience metrics, hardware metrics, energy metrics, quality of information and data quality metrics, software metrics, test metrics, attack and anomalies prediction metrics, privacy policies metrics categories, security metrics, and inference and data privacy metrics. Table 2 presents the metrics classified within each of the 12 categories. The second column in Table 2 lists the corresponding IoT metrics for each metric category.

Tab. 2. Category / classification of IoT metrics

Category of IoT metrics	IoT metrics
Quality metrics of an IoT system or service	availability, rate of user error, responsiveness, security, functionality, suitability, interoperability, maturity, mean time between failures, recoverability, reliability, efficiency, conformance, functional correctness, portability, confidentiality, flaws over time, integrity and safety.
Network metrics	GoodPut, reliability, collision probability, availability, packet loss ratio, network stability, Packet Transmission Delay, packet latency, Transmission Cycle, network lifetime, data transfer size, processing speed, packet delivery ratio, End-to-end delay, Memory space, convergence time, latency, network overload, hop delay, bandwidth, priority, packet error ratio, periodicity, deadline, bit error rate, fault recovery, Gateway Load-Balanced factor, Average Link Delay, Throughput, data rate, Message size, Data Extraction Rate, number of collisions, control overhead, transmission power, Expected Transmission Delay, packet delay, Memory utilization, control message overhead, Signal to noise ratio "SNR", Packet time on air, Connectivity range, Spreading factor, Coding rate, Spectrum efficiency, scalability, Received signal strength indicator "RSSI", Load, Implementation complexity, Network size, Effective utilization of channels, Sampling frequency, Data loss rate, Congestion, delay jitter, Number of alive nodes, Temperature, maintainability, Packet creation time.
Quality of experience metrics	Mean opinion score, Surveys.
Hardware metrics	Energy consumption, Accuracy of sensors, Resolution of camera devices, Time duration for which sensor is sensing.
Energy metrics	Energy efficiency, energy consumption, residual energy, Power Consumption.
Quality of information and data quality metrics	Completeness, Timeliness, Plausibility, Artificiality, Concordance.
Software metrics	Code complexity, Code redundancy, Cohesion, Code readability, Comment line density, Completely bad practice, Computation time, Critical practice, Duplicated blocks, Duplicated Files, Duplicated lines, Extent of component coupling, File, Interceptor practice, memory consumption, Method, Number of classes, Number of comment lines, Number of lines, Primary training, Quality of code, Secondary practice, Size of code's units, Unit interface size, Volume of code.
Test metrics	Defect Density of Test Case Review, Defect Discovery vs Defect Fix Rate, Defect Leakage, Defect Rejection Rate, Defect Re-open Rate, Effective Defect Density, Requirement Coverage, Test Case Reuse in Regression Tests, Test Execution Productivity, Test Execution Rate, Test Scripting Productivity, Test to Defect Ratio, Valid Defects.
Attacks and anomalies prediction metrics	Confusion matrix, Accuracy, Precision, Recall, F1 score, Receiver operating characteristic curve.
Privacy policies metrics categories	Obligation, disclosure, collection, and selectivity.
Security metrics	Attack cost, Attack success probability, Compromise rate, Mean-time-to- compromise, Number of Active Services, Number of Inbound and Outbound Connections, Password Strength, Percentage of successful attacks, Risk.
Inference and data privacy metrics	Utility, information loss, trustworthiness, information privacy, differential privacy, average information leakage, local differential privacy, identifiability, mutual information.

Figure 4 shows the distribution of metrics per category found in the literature over the past one decade.

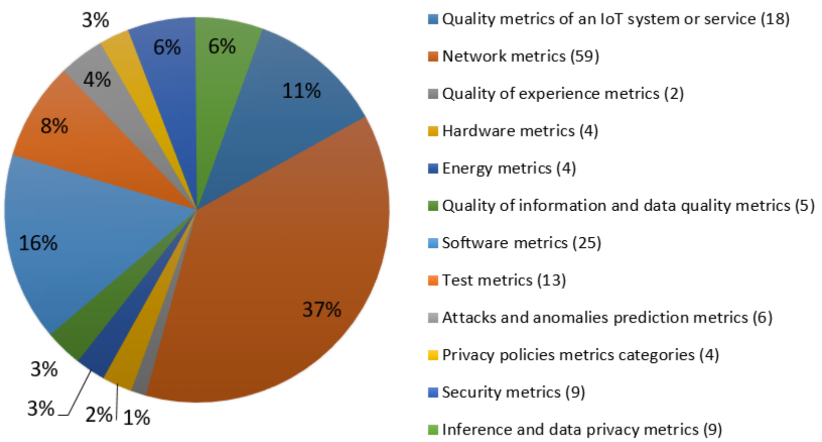


Fig. 4. Distribution of the IoT metrics per category

From Figure 4, the categories of network, software, and quality metrics have the highest number of metrics with 59, 25, and 18, respectively, whereas the categories of quality of experience, hardware, energy, and privacy policies metrics have, by far, the lowest number of metrics with 2 and 4, respectively.

3.4. RQ4: What other new metrics could be defined?

Figure 5 presents, in terms of number of studies, the amount of research attention given to each category of metrics from 2010 to 2021.

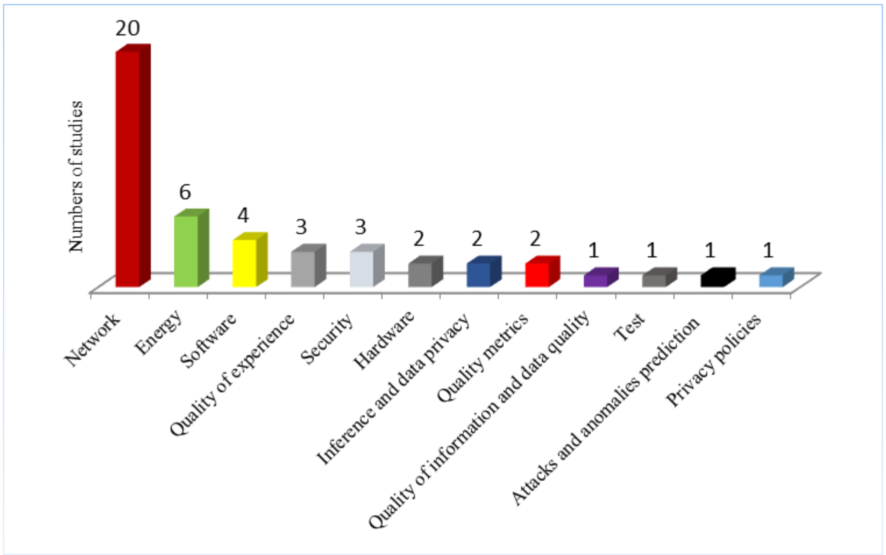


Fig. 5. Numbers of studies per category of IoT metrics

The total number of studies used to construct the SLR was relatively small (37 papers), but for a decade, this number was similar to other SLR on new topics (Enholm et al., 2021; Taylor et al., 2020; Wu et al., 2016). However, this relevant sample can provide an objective and quantitative view of the research on IoT metrics, from which we can derive valuable insights for both practitioners and researchers, including identifying gaps in metric coverage within a category of IoT metrics.

As shown in Figure 5, on the one hand, most of the studies discussed network metrics and this is also justified by the highest number of metrics for this category. On the other hand, compared to the network category, the other categories have received less research attention, specifically hardware metrics, inference and data privacy metrics, quality metrics, quality of information and data quality metrics, test metrics, attacks and anomalies prediction metrics, and privacy policies metrics categories. It should be noted that a study can discuss more than one category (in Figure 5, the sum of the numbers of studies is 46).

Moreover, the categories of quality, energy, hardware, attacks and anomalies prediction, and test metrics have the highest percentage of metrics with formulas, whereas the categories of security and inference and data privacy metrics have the lowest percentage of metrics with formulas.

There are no privacy policies metrics found in our SLR; only categorization of the metrics exists. Therefore, new metrics need to be investigated for privacy issues and for metrics with no formulas. In addition, other categories of metrics, such as financial metrics, metrics for user satisfaction, convenience and safety, should be explored.

3.5. RQ5: What are the relationships between the different IoT metrics?

It is worth noting that IoT metrics are used to measure the overall performance of an IoT system. All of these metrics aim to ensure that an IoT system performs as desired and expected, and therefore should be related. The selected and analyzed studies (see Appendix) do not identify the relationships between the different parts that affect the overall performance of an IoT system. Therefore, we propose an ontology that brings together all these performance metrics. We determined the relationships between metrics using a set of hierarchically interconnected IoT metrics. These relationships between different IoT metrics have been represented with the ontology structure shown in Figure 6 using categories such as: network metrics which include energy metrics and, software metrics which include security metrics.

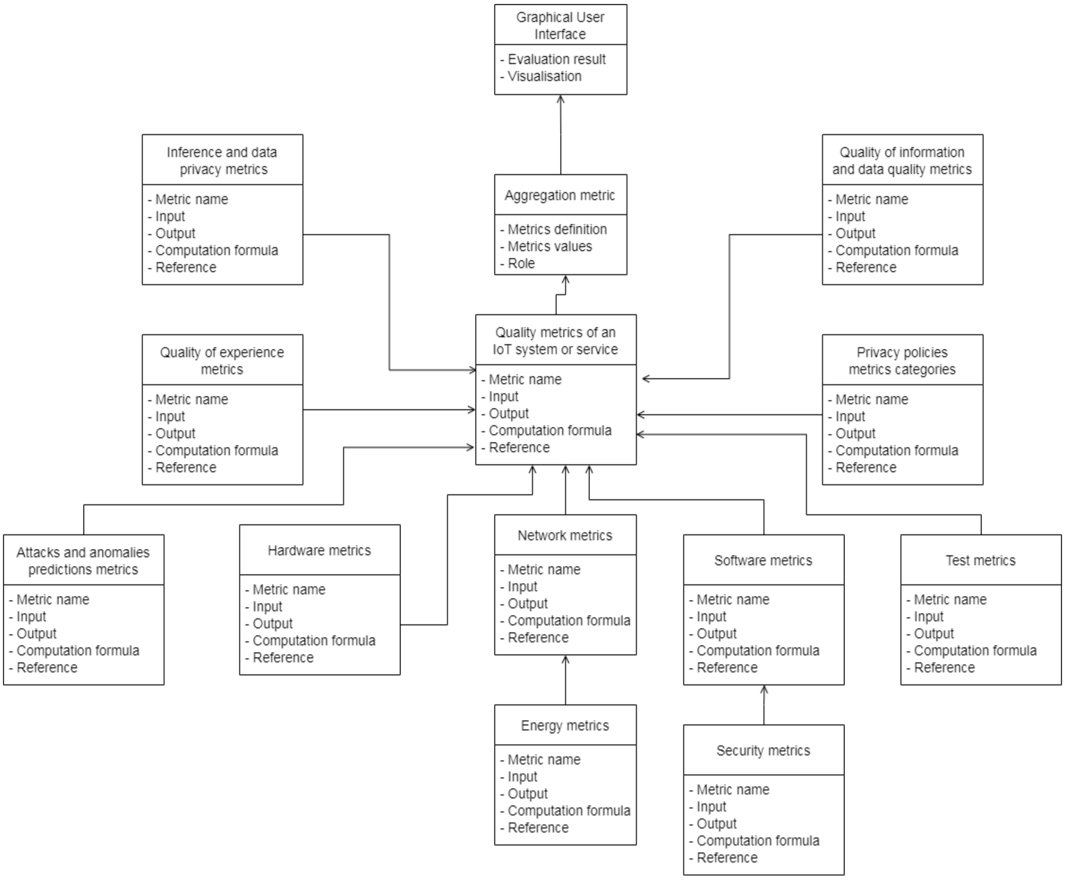


Fig. 6. Relationships between the categories / classes of metrics

Figure 6 shows the organization of different IoT metrics, considering their nature as classification criteria. IoT metrics identified in each category were described by their respective name, input, output, computation formula and the reference where they have been identified. The aggregation metric consists of evaluating the overall IoT performance system by taking into account the metrics definition, the metrics values and the role for each category. The graphical user interface allows the evaluation result and its visualization. It should be noted that all these metrics aim to contribute to ensuring quality services in an IoT system.

4. CONCLUSION AND FUTURE WORK

4.1. Summary of findings

A number of issues in the IoT have been investigated over the years, but relatively few have focused on IoT metrics, and this knowledge has not yet been inventoried and categorized. This 2010-2021 SLR in recent studies proposing IoT metrics followed the guidelines proposed by Kitchenham and Charters (2007). First, 37 studies were selected from the ACM Digital Library, Springer, IEEE Xplore, ScienceDirect, and Scopus databases to address our research questions using specified inclusion and exclusion criteria and then analyzed to answer the research questions.

The SLR findings can be summarized as follows:

- RQ1: Most of the selected studies were published in journals, and the remaining studies were published in conference proceedings. In addition, no specific journal has published more than three studies. Most of the studies are fairly recent and have been published over the past five years (81% from 2017 to 2021). This indicates that IoT metrics have gained increasing attention from researchers.
- RQ2: We identified 158 different metrics, some of which are listed only, others are discussed in more depth, and some are used in experiments to evaluate IoT systems.
- RQ3: We categorized IoT metrics into 12 categories. The categories of network, software, and quality metrics presented the highest number of metrics, whereas the categories of quality of experience, hardware, energy, and privacy policies metrics had the lowest number of metrics.
- RQ4: New metrics could be defined for privacy issues and metrics such as convenience and safety, financial metrics, metrics for user satisfaction should be introduced. There are no formulas for the categories of security, and inference and data privacy metrics.
- RQ5: We determined the relationships between metrics through a set of hierarchically interconnected IoT metrics and represented them as an IoT metric ontology.

One of the most interesting findings of our study was that the extracted metrics could be used to evaluate the overall performance of an IoT system through the proposed IoT metrics ontology. This research is also of interest to both researchers and practitioners and contributes to consolidating the current knowledge bases for IoT metrics, and should guide in the selection of the appropriate metrics for IoT systems.

4.2. Study limitations

Limitations refer to influences or shortcomings that are beyond the researchers' control and place restrictions on the methodology and analysis of research data (Filippova et al., 2017). The limitations of this study related to the research problem under investigation may include the following:

- Search strings derived from the research questions. Studies that did not include our search terms in their titles, abstracts, and keywords may not have been considered.
- The assumption used to assess the relevance and credibility of primary studies may be incorrect and may have excluded other relevant papers.

To conduct this SLR, reputed journals and international conferences were used to ensure the selection of relevant primary empirical studies. Regardless of the number of studies selected, we believe that this study provides a reliable basis for further research on the IoT metrics.

4.3. Future work

Further empirical studies can be conducted on IoT metrics using our study as a baseline for comparison. In this paper, we point out that few studies have focused on the IoT metrics. To fill the gaps identified in this SLR, researchers could propose other metrics such as privacy metrics, financial metrics, user satisfaction metrics, convenience, and safety metrics. Furthermore, the IoT metrics ontology framework proposed in this SLR can be extended and improved.

Funding

This research was funded by the University of South Africa under Grant 409000.

Conflicts of Interest

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

REFERENCES

Ahmed, M. I., & Kannan, G. (2021). Secure and lightweight privacy preserving internet of things integration for remote patient monitoring. *Journal of King Saud University - Computer and Information Sciences, 34*(9), 1319-1578. https://doi.org/10.1016/j.jksuci.2021.07.016

Ashton, K. (2009). *That 'Internet of Things' Thing*. Retrieved March 31, 2022 from https://www.rfidjournal.com/that-internet-of-things-thing.

Cui, J., Wang, L., Zhao, X., & Zhang, H. (2020). Towards predictive analysis of android vulnerability using statistical codes and machine learning for iot applications. *Computer Communications, 155*, 125-131. https://doi.org/10.1016/j.comcom.2020.02.078

Djam-Doudou, M., Ari, A. A. A., Emati, J. H. M., Njoya, A. N., Thiare, O., Labraoui, N., & Gueroui, A. M. (2022). A certificate-based pairwise key establishment protocol for IoT resource-constrained devices. *Proceedings of the 2nd International Conference of Pan-African Artificial Intelligence and Smart Systems (PAAISS)* (pp. 3-18). Springer. https://doi.org/10.1007/978-3-031-25271-6_1

Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2021). Artificial Intelligence and Business Value: a Literature Review. *Information Systems Frontiers*, *24*, 1709–1734. https://doi.org/10.1007/s10796-021-10186-w

Filippova, A., Trainer, E., & Herbsleb, J. D. (2017). From diversity by numbers to diversity as process: Supporting inclusiveness in software development teams with brainstorming. *Proceedings of the 39th International conference on software engineering* (pp. 152–163). IEEE. https://doi.org/10.1109/ICSE.2017.22

Fizza, K., Banerjee, A., Mitra, K, Jayaraman, P. P., Ranjan, R., Patel, P., & Georgakopoulos, D. (2021). QoE in IoT: a vision, survey and future directions. *Discover Internet Things*, *1*(4), 1-14. https://doi.org/10.1007/s43926-021-00006-7

Gandotra, P., & Jha, R. K. (2017). A survey on green communication and security challenges in 5G wireless communication networks. *Journal of Network and Computer Applications*, *96*(C), 39-61. https://doi.org/10.1016/j.jnca.2017.07.002

Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*, 100059. https://doi.org/10.1016/j.iot.2019.100059

Hindle, A. (2015). Green mining: a methodology of relating software change and configuration to power consumption. *Empirical Software Engineering*, *20*(2), 374-409. https://doi.org/10.1007/s10664-013-9276-6

Iwendi, C., Maddikunta, P. K. R., Gadekallu, T. R., Lakshmanna, K., Bashir, A. K., & Piran, M. J. (2020). A metaheuristic optimization approach for energy efficiency in the IoT networks. *Software: Practice and Experience, 51(*12), 2558– 2571. https://doi.org/10.1002/spe.2797

Jagroep, E., Broekman, J., van der Werf, J. M. E. M., Lago, P., Brinkkemper, S., Blom, L., & Vliet, R. (2017). Awakening awareness on energy consumption in software engineering. *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)* (pp.76–85). IEEE. https://doi.org/10.1109/ICSE-SEIS.2017.10

Kim, M., Park, J. H., & Lee, N. Y. (2017). A Quality Model for IoT Service. In: J. Park, Y. Pan, G. Yi & V. Loia (Eds.), *Advances in Computer Science and Ubiquitous Computing. UCAWSN CUTE CSA 2016 2016 2016. Lecture Notes in Electrical Engineering* (vol. 421, pp. 497-504). Springer. https://doi.org/10.1007/978-981-10-3023-9_77

Kitchenham, B. A., & Charters, S. (2007). *Guidelines for performing systematic literature review in software engineering.* Keele University.

Klima, M., Rechtberger, V., Bures, M., Bellekens, X., Hindy, H., & Ahmed, B. S. (2020). Quality and Reliability Metrics for IoT Systems: A Consolidated View. In S. Paiva, S. I. Lopes, R. Zitouni, N. Gupta, S. F. Lopes & T. Yonezawa (Eds.), *Science and Technologies for Smart Cities*. SmartCity360° *2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 635-650). Springer. https://doi.org/10.1007/978-3-030-76063-2_42

Koçak, S. A. (2021). *Software energy consumption prediction using software code metrics* (PhD disertation), Environmental Applied Science and Management, Ryerson University, Canada. https://doi.org/10.32920/ryerson.14666424.v1

Kuemper, D., Iggena, T., Toenjes, R., & Pulvermueller, E. (2018). Valid.IoT: a framework for sensor data quality analysis and interpolation. *Proceedings of the 9th ACM Multimedia Systems Conference* (pp. 294-303). The ACM Digital Library. https://doi.org/10.1145/3204949.3204972

Kumar, R., & Sharma, R. (2021). Leveraging blockchain for ensuring trust in IoT: A survey. *Journal of King Saud University - Computer and Information Sciences, 34*(10), 1319-1578. https://doi.org/10.1016/j.jksuci.2021.09.004

Magno, M., Aoudia, F. A., Gautier, M., Berder, O., & Benini, L. (2017). WULoRa: An Energy Efficient IoT End-Node for Energy Harvesting and Heterogeneous Communication. *Proceedings of IEEE/ACM Design, Automation & Test in Europe Conference & Exhibition* (pp. 1528-1533). IEEE. https://doi.org/10.23919/DATE.2017.7927233

Roy, S., Mazumdar, N., & Pamula, R. (2021). An energy optimized and QoS concerned data gathering protocol for wireless sensor network using variable dimensional PSO. *Ad Hoc Networks, 123*(C), 1-19. https://doi.org/10.1016/j.adhoc.2021.102669

Savola, R., Abie, H., & Sihvonen, M. (2012). Towards metrics-driven adaptive security management in E-health IoT applications. In I. Balasingham (Ed.), *Proceedings of the 7th International Conference on Body Area Networks (BodyNets '12)* (pp. 276–281). The ACM Digital Library. https://dl.acm.org/doi/abs/10.5555/2442691.2442753

Soubra, H., & Abran, A. (2017). Functional Size Measurement for the Internet of Things (IoT): An example using COSMIC and the Arduino open source platform. In M. Staron &W. Meding (Eds.), *Proceedings of the International Workshop on Software Measurement and the International Conference on Software Process and Product Measurement* (pp. 122-128). The ACM Digital Library. https://doi.org/10.1145/3143434.3143452

Tavakolan, M., & Faridi, I. A. (2020). Applying privacy-aware policies in IoT devices using privacy metrics. *Proceedings of the International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)* (pp.1-5). IEEE. https://doi.org/10.1109/CCCI49893.2020.9256605

Taylor, P. J., Dargahi, T., Dehghantanha, A., & Parizi, R. M. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147-156. https://doi.org/10.1016/j.dcan.2019.01.005

Voas, J., Kuhn, R., & Laplante, P. A. (2018). IoT metrology. *IT Professional, 20*(3), 6-10. https://doi.org/10.1109/MITP.2018.032501740

Wu, H., Shi, L., Chen, C., Wang, Q., & Boehm, B. (2016). Maintenance Effort Estimation for Open Source Software: A Systematic Literature Review. *Proceedings of the International Conference on Software Maintenance and Evolution*, (pp. 32-43). IEEE. https://doi.org/10.1109/ICSME.2016.87

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE *Internet of Things Journal, 4*(5), 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

Zahoor, S., & Mir, R. N. (2021). Resource management in pervasive Internet of Things: A survey. *Journal of King Saud University - Computer and Information Sciences, 33*(8), 921-935. https://doi.org/10.1016/j.jksuci.2018.08.014

Zhang, S., Bai, G., Li, H., Liu, P., Zhang, M., & Li S. (2021). Multi-Source Knowledge Reasoning for Data-Driven IoT Security. *Sensors, 21*(22), 7579. https://doi.org/10.3390%2Fs21227579

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: challenges. *IEEE Communications Magazine, 55*(1), 26-33. https://doi.org/10.1109/MCOM.2017.1600363CM

Appendix – selected primary studies.

This appendix contains the supporting documentation for our article. The list of the 37 selected studies and three additional bibliographic references selected to perform the SLR are presented in Table 1.

Tab. 1. Selected primary studies

IoT Category	Study Id	Authors	Title	Source
Energy	S1	Georgiou et al.	Software Development Lifecycle for Energy Efficiency: Techniques and Tools	ACM Comput. Surv.
	S2	Huang et al.	Building Energy Efficient Internet of Things by Co-Locating Services to Minimize Communication	Association for Computing Machinery
	S3	Filho et al.	A fog-enabled smart home solution for decision-making using smart objects	Future Generation Computer Systems
	S4	Gandotra & Jha	A survey on green communication and security challenges in 5G wireless communication networks	Journal of Network and Computer Applications
	S5	Lin et al.	Zigbee-based Internet of Things in 3D Terrains	Computers & Electrical Engineering
	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
Network	S7	Amini et al.	Availability-Reliability-Stability Trade-Offs in Ultra-Reliable Energy-Harvesting Cognitive Radio IoT Networks	IEEE Access
	S8	Amini et al.	Performance Analysis of URLL Energy-Harvesting Cognitive-Radio IoT Networks With Short Packet and Diversity Transmissions	IEEE Access
	S9	Li et al.	Enhancing the Performance of 802.15.4-Based Wireless Sensor Networks With NB-IoT	IEEE Internet of Things Journal
	S10	Shahzad et al.	IoTm: A Lightweight Framework for Fine-Grained Measurements of IoT Performance Metrics	Conference on Network Protocols
	S11	Al-Roubaiey et al.	EATDDS: Energy-aware middleware for wireless sensor and actuator networks	Future Generation Computer

				Systems
	S12	Lima et al.	Adaptive priority-aware LoRaWAN resource allocation for Internet of Things applications	Ad Hoc Networks
	S5	Lin et al.	Zigbee-based Internet of Things in 3D Terrains	Computers & Electrical Engineering
	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
	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
	S14	Roy et al.	An energy optimized and QoS concerned data gathering protocol for wireless sensor network using variable dimensional PSO	Ad Hoc Networks
	S15	Xu et al.	Enabling robust and reliable transmission in Internet of Things with multiple gateways	Computer Networks
	S16	Yuan et al.	Instrumenting Wireless Sensor Networks — A survey on the metrics that matter	Pervasive and Mobile Computing
	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
	S18	Ramli et al.	A Study on the Impact of Nodes Density on the Energy Consumption of LoRa	International Journal of Interactive Mobile Technologies
	S19	Paschou et al.	Health Internet of Things: Metrics and methods for efficient data transfer	Simulation Modelling Practice and Theory
	S20	Sallum et al.	Improving Quality-Of-Service in LoRa Low-Power Wide-Area Networks through Optimized Radio Resource Management	
	S21	Olapure et al.	Design and analysis of RPL objective functions using variant routing metrics for IoT applications	Wireless Netw.
	S22	Rani et al.	A hybrid approach for the optimization of quality of service metrics of WSN	
	S23	Dvornikov et al.	QoS Metrics Measurement in Long Range IoT Networks	Conference on Business Informatics
	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
Inference and data privacy	S25	Abdelhameed et al.	Privacy-preserving tabular data publishing: A comprehensive evaluation from web to cloud	Computers & Security
	S26	Sun et al.	Inference and data privacy in iot networks	Workshop on Signal Processing

				Advances in Wireless Communications
Hardware	S16	Yuan et al.	Instrumenting Wireless Sensor Networks — A survey on the metrics that matter	Pervasive and Mobile Computing
	Ref9	Fizza et al.	QoE in IoT: a vision, survey and future directions	Discover Internet Things
Quality	S27	Kim et al.	A Quality Model for IoT Service	Advances in Computer Science and Ubiquitous Computing
	Ref12	Klima et al.	Quality and reliability metrics for IoT systems: a consolidated view	Summit Smart City
Test	Ref12	Klima et al.	Quality and reliability metrics for IoT systems: a consolidated view	Summit Smart City
Software	S28	Baggen et al.	Standardized code quality benchmarking for improving software maintainability	Software Quality Journal
	S29	Pantiuchina et al.	Improving code: The (mis) perception of quality metrics	Conference on Software Maintenance and Evolution
	Ref11	Cui et al.	Towards predictive analysis of android vulnerability using statistical codes and machine learning for iot applications	Computer Communications
	Ref12	Klima et al.	Quality and reliability metrics for IoT systems: a consolidated view	Summit Smart City
Quality of information and data quality	S30	Eushay et al.	Domain agnostic quality of information metrics in iot-based smart environments	Conference on Intelligent Environments
Privacy policies	S31	Tavakolan	Applying privacy-aware policies in iot devices using privacy metrics	Conference on Communications, Computing, Cybersecurity, and Informatics
Attacks and anomalies prediction	S32	Hasan et al.	Attack and anomaly detection in iot sensors in iot sites using machine learning approaches	Internet of Things
Security	S33	Setzler et al.	IoT Metrics and Automation for Security Evaluation	Consumer Communications & Networking Conference
	S34	Savola et al.	Towards metrics-driven adaptive security management in E-health IoT applications	Conference on Body Area Networks
	S35	Ge et al.	A Framework for Modeling and Assessing Security of the Internet of Things	
Quality of experience	S36	Shin, D-H	Conceptualizing and measuring quality of experience of the internet of things: Exploring how quality is perceived by users	Information & Management
	S37	Suryanegara et al.	A 5-step framework for measuring the quality of experience (QoE) of Internet of Things (IoT) services	IEEE Access

	Ref9	Fizza et al.	QoE in IoT: a vision, survey and future directions	Discover Internet Things