Journal of Policy Research, 9(4), 9-18
https://jprpk.com
https://doi.org/10.61506/02.00121

An Efficient Systematic Approach for Adaptability Synthesis of IOT's Performance

Mehak Fatima[1]*, Hamayun Khan[2], Irfan uddin[3], Muhammad Nabeel Amin[4], Attiq Ur Rehman[5]

Abstract

The Internet of Things (IoT) has profoundly impacted various facets of contemporary society, transforming the ways in which individuals live, work, travel, and conduct business. Given its significance, it becomes imperative to ensure that IoT systems perform as intended and anticipated. This necessitates the availability of a comprehensive set of IoT performance metrics for assessment and management. This research endeavor's primary objective is to methodically catalog and categorize recent explorations into Internet of Things measurements. The writers executed a review of the literature encompassing research findings published from January 2010 until December 2021, guided by five research questions in all. Through this review, 158 in total distinct IoT measurements were unearthed and systematically grouped into 12 distinct groups, each pertaining to different facets and elements of IoT systems. To holistically assess IoT system performance, these twelve categories were carefully arranged in ontology. The outcomes unveiled the network metrics emerged as the most prevalent category of discussion, appearing 43 percent of the analyzed research, and boasting the greatest percentage of metrics, 37%. This research stands as a valuable resource for both researchers and practitioners, offering guidance when choosing the right metrics for Internet of Things systems. Additionally, it provides priceless insights into topics ripe for enhancement and optimization in the realm of IoT performance evaluation.

Keywords: Internet of Things, IoT Systems, IoT Metrics, Iot Measurements, IoT Security Metrics

1. Introduction

Kevin Ashton coined the term "Internet of Things" in 1999 while he was employed at Procter & Gamble (Ashton, 2009). Although a great deal has been published in the past about Internet of Things (IoT) design, evaluating an IoT system's performance has proven to be considerably more difficult making sure an IoT system functions as planned and anticipated is essential, especially given how important IoT is to business and daily life. Many objects of art, including software (IoT applications), equipment (gadgets abilities), management capacities, security abilities, network (networking and transport capabilities), administration support, application support layer by layer (information handling or information stockpiling), and equipment, can be used to evaluate an Internet of Things platform (Doudou and Djam-Doudou, 2022).

The evaluation of IoT systems presents several intricate challenges. Some proposed measurement solutions lack quantifiability due to the presence of values that cannot be quantified (Voas et al., 2018). Some measures can even be totally ineffectual or nonexistent. Since various proposals vary, a few researchers have recommended using weighting factors to focus on individual pointers (Voas et al., 2018). Notwithstanding these difficulties, various examinations ((Magno and colleagues, 2017; Zahoor and Mir, 2021) analyzed execution markers connected to security and protection issues notwithstanding energy proficiency (Ahmed and Kannan, 2021; Kumar and Sharma, 2021; Yang et al., 2017; Zhou et al., 2017). Various guidelines that cover equipment, programming, quality norms, network execution, and security necessities have likewise been proposed. Zhang et al. (2021) fostered Internet of Things Security Danger Cosmology (IoTSTO) as a worldview for IoT security dangers and proposals for danger investigation perception. Their work shows the opposite. Their methodology doesn't give total IoT security reconnaissance, yet it assists security overseers with executing IoT security arrangements.

Accomplishing reliable IoT administrations requires compelling quality-related measurements observing, estimation, and appraisal. For instance, Fizza et al. (2021) offered an extensive survey, evaluating the momentum status of the subject and framing future opportunities for Web of Things-related Nature of Involvement (QoE) research. They explored the meanings of QoE that had proactively been proposed prior to doing an exhaustive assessment of the strategies and approaches utilized in the IoT space to evaluate QoE. It's significant that they partitioned quality estimations into four classifications, with parts connected with PCs, organizations, gadgets, and UIs remembered for every classification. In all the while Kuemper et al.(2018) presented a methodology that is particularly planned to assess the nature of different information transfers in Web of Things arrangements. This strategy depends on great information (QoI) measurements. Their review yielded a bunch of conditions for deciding information quality as well as guidelines for information planned for Web of Things frameworks. This hypothetical system is a useful asset for surveying and maintaining information quality in the powerful Web of Things space. Cui et al.(2020) made

*[1] Department of Computer science, Superior University Lahore, Pakistan. Mehakkfatimaa555@gmil.com
[2] Department of computer Science, Faculty of Computer Science & IT, Superior University Lahore, Pakistan
[3] Faculty of Computer Science & IT, Department of computer Science, Superior University Lahore, Pakistan
[4] Department of Computer Science, Superior University Lahore, Pakistan
[5] Department of Computer Science, Superior University Lahore, Pakistan

expectation models for hazard and weakness fully intent on upgrading the adequacy and nature of Android applications for Web of Things (IoT) frameworks. These models were assembled utilizing programming code measurements and AI draws near. It's memorable's essential that the investigation of these forecast models was confined by the minuscule datasets that were used to fabricate them. This information size limitation might affect their gamble weakness assessments' power and the capacity to be general. A careful writing survey on test measurements and quality was led by Klima et al.(2020) against the foundation of IoT frameworks. Strikingly, as studies like Jagroep (2017) and Hindle (2015) show, some exploration has proposed that a product program's elements might significantly affect how energy-proficient it is.

The thought of utilizing Enormous - ISO 19761 strategy based useful size estimation in the Web of Things was first proposed by Soubra and Abran (2017). They underlined the potential benefits of applying this technique to ongoing implanted framework (RTES) energy the board in Web of Things applications. To reveal insight into the perplexing linkages between programming plan and energy effectiveness, Koçak (2018) analyzed the connection between programming code quality and their effect on energy use. To build the helpful existence of the organization, Iwendi et al.(2020) focused on advancing energy productivity in Web of Things sensor hubs. In order to promote longer network durability, their work tackled the vital issue of energy preservation in Internet of Things networks.

All things considered, A few of research has suggested IoT measurements and the automation of their assessment; yet, as far as we are aware, no comprehensive systematic literature review (SLR) has been conducted on IoT metrics that covers every part and component of an Internet of Things system. This served as the inspiration for the present-day SLR research of IoT indicators from 2010 and 2021. The evaluation's objective is to create an ontology that illustrates the connections between each IoT indicator of performance by methodically gathering and categorizing current research that have looked at IoT metrics. Furthermore, based regarding the specific application, use scenario, and system architecture, these metrics can aid in assessing the efficacy and performance of IoT systems and offer insightful information about areas in need of adjustment.

Table 1. Overview of IoT Metrics and Research (1999-2023)

Category	**Key Terms/Phrases**
Background	Kevin Ashton, Procter & Gamble, Internet of Things (IoT)
Creation of Term	Kevin Ashton, 1999, "Internet of Things"
IoT System Components	Software, Hardware, Management, Security, Network, Service
Challenges in Evaluation	Non-quantifiable values, Inefficient metrics, Weighting factors, Security and privacy concerns, Energy efficiency
Security Metrics	Security monitoring, IoT Security Threat Ontology (IoTSTO)
Quality Metrics (QoE)	Fizza et al. (2021), Device, Network, Computing, and User Interface are the four levels.
Quality Information (QoI)	Kuemper et al. (2018), Data stream quality metrics, IoT applications
IoT Applications for Android	Cui and associates (2020), prediction of risk vulnerability, Software code metrics, machine learning, and small datasets
Literature Review on Quality and Test Metrics	Klima et al. (2020), Energy efficiency, Software characteristics, COSMIC - ISO 19761 method, Real-time embedded systems (RTES)
Functional Size Measurement in IoT	Soubra and Abran (2017), COSMIC - ISO 19761 method, Energy consumption, Real-time embedded systems (RTES)
Properties of Software Code and Energy Use	Koçak (2018), Software code attributes and energy efficiency: a relationship
Optimization of Energy Consumption in IoT Sensor Nodes	Iwendi et al. (2020), Energy consumption optimization, IoT sensor nodes, Prolonged network longevity
SLR on IoT Metrics (2010-2021)	Ontology creation, Connections between IoT performance indicators, Use case, Application, System architecture
2023 IoT Metrics	Ongoing research, Future developments, Evolving metrics landscape

This is how the remainder of the paper is structured. The SLR study's methodology is presented in Section 2. The findings and discussions are presented in Section 3. The paper's final section provides an overview of the major conclusions, limitations of the study, and recommendations for further research.

2. Review Method

The criteria provided research themes, search approach, research selection, assessment of quality, extraction of data, and synthesis of data, which may be summed up in six main stages by Kitchenham and Charters (2007), were followed by the authors to conduct our systematic literature review (SLR). Figure 1 is an illustration of the SLR protocol.

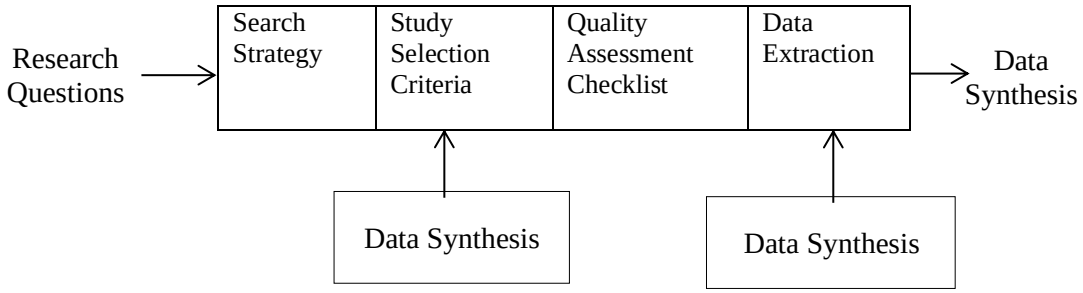

Fig. 1. The protocol for systematic reviews

2.1. Research Questions

The current SLR seeks to classify and identify the numerous IoT measurements suggested in the body of publications and information repositories that already exist. Developing the inquiry for the study is a crucial component of any methodical writing survey. The following formulations of research questions were deemed pertinent to this study:

RQ1: In terms of publications reporting on IoT indicators, which journals predominate?
RQ2: What metrics have Internet of Things systems used?
RQ3: What classifications or categories exist for IoT metrics?
RQ4: What further novel metrics might be established?
RQ5: How do the various IoT measurements relate to one another?

2.2. Search strategy

The original researches that answer the inquiries for the research are listed in this section. The search parameters and the data source parts of the approach were carried out in two stages. Finding the key terms from the chosen research topics comprised the search terms phase. The databases utilized to find and choose pertinent papers for our SLR are displayed in the data source phase.

3. Data Source

Five databases were used by the authors to choose their papers: IEEE Xplore, Springer, Digital Library of ACM, ScienceDirect, and Scopus. These repositories were chosen because the software engineering community publishes a sizable quantity of research articles that are pertinent to this study. We found journal publications, reviews, and conference papers using the created search keywords. The search terms were changed to account for the fact that search engines from different databases have varied syntactic requirements for search strings. These five databases were searched, with special attention paid to the title, abstract, and keywords. We individually searched each of the five databases to find pertinent sources, and then we collected the papers that were found. Paper copies were eliminated. The Endnote reference management application was utilized in order to organize the search results.

3.1. Study Selection

180 papers were found after a search across the five databases. The purpose of this part is to list only the pertinent publications that can be used to address our research concerns. Which studies were included in or omitted from a systematic literature review (SLR) were decided using study selection criteria. The authors utilized the subsequent requirements for inclusion and exclusion in the 180 publications after reading the titles, abstracts, conclusions, or complete texts for this purpose:

3.2. Inclusion Criteria

- The articles on IoT measurements should be released between 2010 and 2021. Since the Internet of Things was introduced in 2009, and since we think a lot of research has been done in the last ten years, the search was restricted to this time frame.
- The articles should be published in journals, reviews, or conference proceedings, with computer science and informatics as the subject matter.

3.3. Exclusion Criteria

- Paper copies ought to be disposed of.
- Research within the Internet of Things that did not focus regarding IoT metrics was disregarded.
- Research that did not consider the previously mentioned inclusion criteria was not accepted.

Thirty-one suitable papers were obtained after the quality evaluation and selection criteria outlined in Section 2.4 were applied. Subsequently, all pertinent publications' references were examined, and supplementary papers that were missed during the initial search were found. Six pertinent papers were returned after these were subjected to the selection criteria and quality assessment. 37 papers were chosen in the end; the bibliographic references are not included.

3.4. Quality Assessment

The discussion of the chosen studies' legitimacy and applicability was conducted using quality assessment. The papers were chosen from five reputable databases of articles that had been pre-publication evaluated by professionals. Additionally, we chose a few Kitchenham and Charters (2007) quality evaluation criteria for this SLR since they best

fit our study topics
Q1: Are the study's objectives clearly stated?
Q2: Are the measures employed in the research sufficiently specified?
Q3: Do the results reported clearly support the findings?
Q4: Are the study's limitations discussed?
Only submissions that addressed a minimum of three of the aforementioned queries were chosen.

3.5. Data Extraction

The procedure for extracting data made it possible to retrieve the information needed to address the study's quality standards and research questions. We methodically extracted the paper for every study we selected, we included information such as the title, creator name, distribution type, distribution date, IoT measurements found, and exploration concerns tended to. Know that not all five research concerns were covered by every paper that was selected.

3.6. Data Synthesis

The goal of data synthesis was to compile and condense the findings of the main research that were included. Using descriptive synthesis, we found and categorized all pertinent data to address the study questions. For the purpose of illustrative insights, we considered the overall number of IoT metrics categorized by the several sections and attributes of an IoT system, the all-out number of review found for every class or characterization of IoT measurements, and the connections among the different IoT metrics.

4. Results and Discussions

Based on a summary of the chosen studies, this part offers responses to the SLR research questions.

RQ1: In terms of publications reporting on IoT indicators, which journals predominate?

The arrangement of the chosen research, in accordance with the type of being published (a conference or magazine), quantity of research within a publication venue, and publication venue is displayed in Table 1.

Table 2. Distribution of publishing outlets and the nature of the chosen studies

Publication Site	Kind of Research	Number
Future Generation Computer Systems	Journal	1
IEEE Access	Journal	1
Wireless Network	Journal	1
IEEE Internet of Things Journal	Journal	1
Ad Hoc Networks	Journal	1
Journal of Network and Computer Applications	Journal	1
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 Environments	Conference	1
International Conference on Communications, Computing, Cyber security, and Informatics	Conference	1
International Conference on Management of Emergent 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

According to Table 2, 70% of the research was released in reputable journals, while 30% were released in the proceedings of the conference. No publication has released more than three papers in this SLR.

RQ2: What metrics have Internet of Things systems used?

The authors identified 158 unique metrics (see Table 2) from the selected studies Of these, some have just been referred to in past examinations (Cui et al., 2020; Fizza et al., 2021; Tavakolan and Faridi, 2020; Savola et al., 2012), others have been the subject of inside and out research (Klima et al., 2020; Kim et al., 2017), despite everything others have been utilized in trials to assess IoT frameworks (Gandotra and Jha, 2017; Hasan et al., 2019; Roy et al., 2021).might be useful for little models (Kim, 2013).

RQ3: What classifications or categories exist for IoT metrics?

In light of the ITU-T Y.2060 (06/2012) IoT reference model and the different parts and perspectives that influence the general exhibition of an IoT framework, we partitioned the measurements into 12 classes: quality measurements of an IoT framework or administration; network measurements; nature of involvement measurements; equipment measurements; energy measurements; nature of data and information quality measurements; programming measurements; test measurements; assault and irregularities expectation measurements; security approaches measurements classes; security measurements; what's more, deduction and information security measurements. The measurements characterized into every one of the 12 classifications are displayed in Table 2. For each metric classification, the connected IoT measurements are recorded in Table 2's subsequent section.

Table 3. IoT metrics classification and category

Type of IoT Measurements	IoT Metrics
Measures of an IoT system's or service's quality	availability, user mistake rate, responsiveness, security, functionality, appropriateness, interoperability, development, mean stretches between disappointments, recoverability, productivity, consistence, utilitarian rightness, transportability, secrecy, maturing flaws, trustworthiness, and security?
Network parameters	Proficiency, framework solidness, bundle misfortune proportion, accessibility, crash likelihood, and Organization lifetime, information move size, handling speed, parcel conveyance proportion, start to finish delay, memory space, union time, idleness, network over-burden, jump delay, data transfer capacity, significance, bundle mistake proportion, routineness, cutoff time, bit blunder rate, and shortcoming recuperation are a portion of the elements that influence parcel transmission deferral, inertness, and transmission cycle. factor for door load balance, run of the mill connect dormancy, Transmission power, control above, throughput, information rate, message size, information extraction rate, and the quantity of contentions Memory utilization, parcel delay, expected transmission delay, control message above, "SNR," or motion toward commotion proportion, time spent in bundle air Coding rate, spread element, and availability range Adaptability, proficiency of the range, "RSSI" (got signal strength marker), load, intricacy of execution, network aspects, proficient utilization of the channels, examining span, Pace of information misfortune, blockage, jitter in delays, The amount of live hubs
Experience metrics' quality	Surveys mean opinion score.
Hardware measurements	Expenditure of energy, sensor accuracy, the quality of the cameras, length of time that the sensor is detecting
Measures of energy	Power consumption, residual energy, energy efficiency, and energy consumption
Metrics for data quality	Effectiveness, credibility, superficiality, consistency, and coherence.
Software measurements	Cohesion, code complexity, and code redundancy Readability of code, Remark about line density Absolutely awful behavior, Calculation time, Crucial exercise, duplicate lines, files, blocks, and other data Component coupling extent, File, memory usage, and interceptor practice Approach, The quantity of classes, the quantity of lines in the comments, first instruction, Caliber of the code secondary methodology, Unit interface size, code volume, and code size.
Examine metrics	Test Case Review Imperfection Thickness, Deformity Spillage, Imperfection Dismissal Rate, Deformity Re-open Rate, Imperfection Disclosure versus Imperfection Fix Rate, Test Efficiency, Test Execution Rate, Test Prearranging Efficiency, Test to Abscond Proportion, Substantial Deformities, Viable Imperfection Thickness, and Requirement Coverage in Regression Tests

Type of IoT Measurements	IoT Metrics
Attacks and prediction metrics for anomalies	Receiver operating characteristic curve, F1 score, confusion matrix, accuracy, precision, recall.
metrics categories for privacy policies	Selectivity, obligation, disclosure, and collection.
Metrics for security	Attack success probability, attack cost, and Rate of compromise, As you wait for a compromise, The quantity of connections both inbound and outbound, the number of active services, Password Durability percentage of assaults that succeed, Peril.
Metrics for data privacy and inference	Utility, mutual information, identification, data misfortune, data security, differential protection, normal data spillage, and reliability.

RQ4: What further novel metrics might be established?

Although there were only 37 papers in total that were utilized to build the SLR, over the course of ten years, this quantity was comparable to previous SLR on novel themes (Enholm et al., 2021; Taylor et al., 2020; Wu et al., 2016). Nonetheless, this pertinent sample can offer a quantitative and objective perspective on IoT measurements research, from which we can extract insightful knowledge for practitioners and researchers alike, such as pinpointing metric coverage gaps within a certain IoT metrics category. Given that this category has the most measurements; it makes sense that the majority of the research has addressed network metrics. However, in contrast to the organization classification, different classes equipment measurements, derivation and information protection measurements, quality measurements, data quality and information quality measurements, test measurements, assaults and peculiarities expectation measurements, and security approaches measurements classifications—have gotten less research attention. It should be mentioned that a study may include multiple categories.

Furthermore, the categories with the highest percentage of formula-containing metrics are quality, energy, equipment, assaults and abnormalities forecast, and test measurements; the categories with the lowest percentage of formula-containing metrics are security and induction and information protection measurements.

Our SLR only contains metrics that are classified; it does not contain any metrics related to privacy policies. As a result, new measurements pertaining to privacy concerns and metrics lacking formulas must be researched. It's also important to investigate other types of indicators, such as those related to finances, user satisfaction, convenience, and safety.

RQ5: How do the various IoT measurements relate to one another?

In our research, we observed a critical gap in existing studies where the relationships between various components influencing the overall performance of an IoT system were not adequately identified. To address this deficiency, we propose the development of ontology, serving as a comprehensive framework that consolidates and organizes diverse performance metrics within the IoT ecosystem. Our approach involves establishing hierarchically interconnected relationships among these metrics to offer a more nuanced understanding of their dependencies and interactions. The ontology, depicted in Figure 6, employs a categorical structure to encapsulate key facets of IoT performance. Notably, it includes network metrics, encompassing crucial parameters like energy metrics, and software metrics, which, in turn, incorporate pivotal elements such as security metrics. This hierarchical representation ensures a systematic and thorough analysis of the intricate connections between different IoT metrics, thereby contributing to a more holistic evaluation of the overall system performance.

5. Conclusion and Future Work

5.1. Summary of Findings

Over the years, many IoT-related issues have been studied; however, only a small number of these studies have concentrated on IoT metrics, and this knowledge has not yet been compiled and arranged. In recent research that suggested IoT metrics, the 2010–2021 SLR adhered to the recommendations made by Kitchenham and Charters (2007). Using predetermined inclusion and exclusion criteria, 37 studies were first chosen to address our research questions from the ACM Digital Library, Springer, IEEE Xplore, ScienceDirect, and Scopus databases. The studies were then examined to provide answers to the research questions.

RQ1: The majority of the chosen research was published in journals, while the remainder was published in proceedings from conferences. Furthermore, no particular journal has released more than three studies. Eighty-one percent of the papers were published between 2017 and 2021, making them the majority of fairly recent research. This suggests that academics are paying more and more attention to IoT metrics.

RQ2: A total of 158 metrics were found; some are merely stated, some are extensively explored, and some are utilized in experiments to assess Internet of Things systems.

RQ3: We divided the IoT measurements data into 12 groups. The most metrics were found in the network, software, and quality metrics categories; the fewest measurements were found in the hardware, energy, privacy rules, and quality of experience metrics categories.

RQ4: Financial metrics, convenience and safety measures, metrics for user happiness, and metrics for privacy concerns could all be given new definitions. The metrics related to data privacy, inference, and security is not standardized.

RQ5: Using a collection of IoT measures that are hierarchically interconnected, we were able to ascertain the relationships between the metrics and expressed them using an IoT metric ontology. One of the most fascinating findings from our study was the adaptability of the extracted metrics, which, when arranged according to the suggested IoT metrics ontology, may be utilized to provide a thorough evaluation of an IoT system's overall performance. This research has implications for the academic community as well as industry professionals because it adds to the body of knowledge already available on IoT metrics and offers helpful advice on how to choose the best metrics for an efficient assessment of IoT systems.

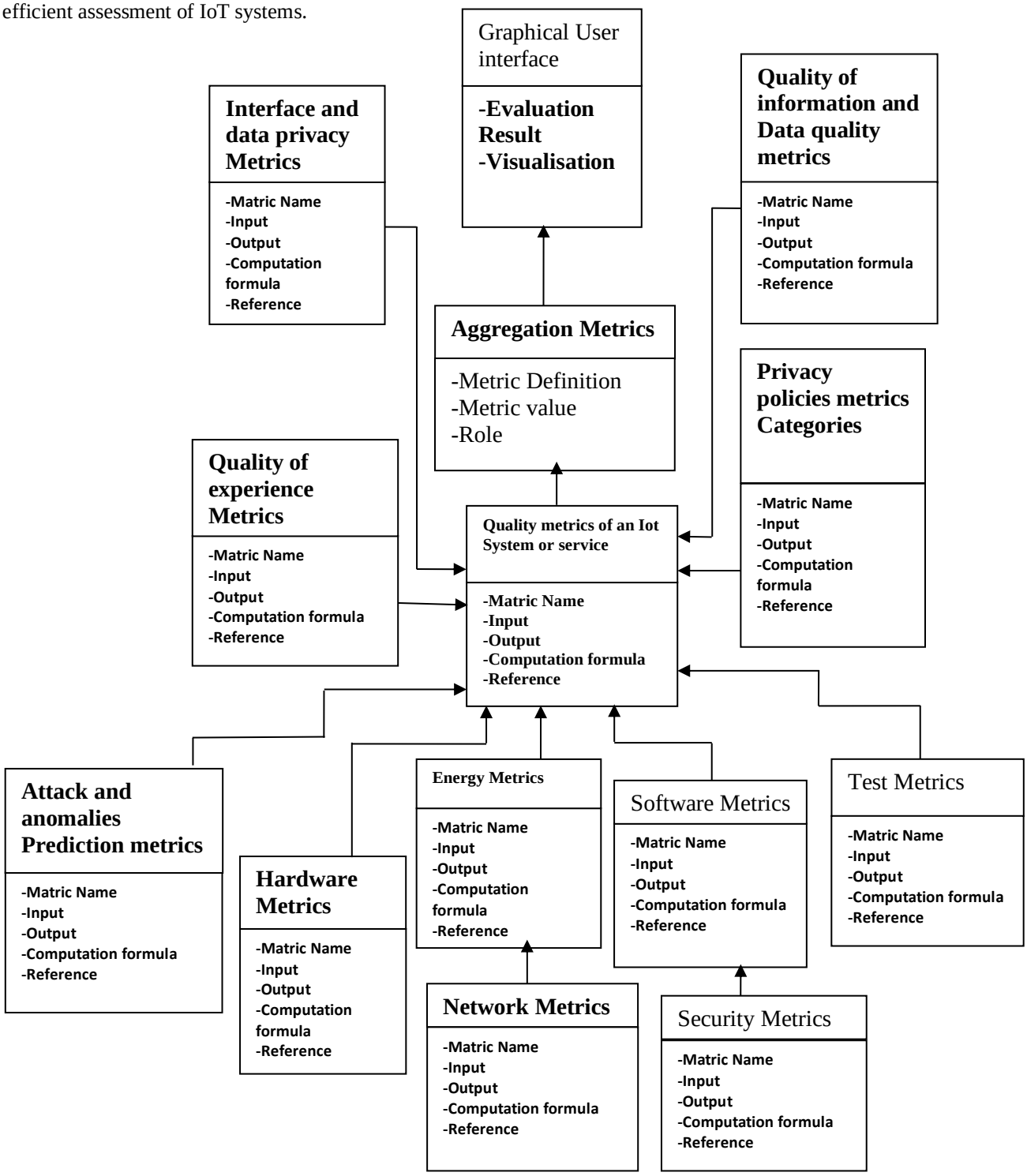

Fig. 2. Relationships between the categories / classes of metric

Table 4. IoT metrics classification and category

Aspect	Summary
Background	Over the years, numerous IoT-related issues studied, but focus on IoT metrics limited. Lack of compiled and arranged knowledge.
SLR Methodology	2010–2021 SLR followed Kitchenham and Charters (2007) recommendations. 37 studies selected using predetermined criteria from ACM Digital Library, Springer, IEEE Xplore, ScienceDirect, and Scopus.
RQ1: Publication Trends	Majority research in journals; conferences also used. No single journal exceeds three studies. 81% of papers (2017–2021), indicating increasing academic attention to IoT metrics.
RQ2: Number of Metrics	Identified 158 metrics – various levels of exploration and experimental usage in IoT system assessments.
RQ3: Metric Categories	IoT measurements categorized into 12 groups. Network, software, and quality metrics most prevalent; hardware, energy, privacy rules, and quality of experience metrics least prevalent.
RQ4: Metric Definitions	Potential new definitions for financial metrics, convenience, safety, user happiness, and privacy metrics. Lack of standardization in data privacy, inference, and security metrics.
RQ5: Metric Relationships	Developed a hierarchical IoT metric ontology, revealing interconnections between metrics for comprehensive system evaluation.
Key Finding	Adaptability of extracted metrics, organized by IoT metric ontology, facilitates thorough IoT system performance evaluation.
Implications	Significant implications for academia and industry, expanding IoT metric knowledge, and providing guidance on efficient metric selection for IoT system assessment.

5.2. Study Limitations

In research, limitations are restrictions or circumstances that are beyond the researcher's control and may affect the methodology and data analysis. Within the framework of this investigation, a number of constraints are noteworthy:

- The research questions served as the basis for the search terms that were utilized to find pertinent studies. This implies that research that did not specifically include these search terms in their abstracts, titles, or keywords might have slipped through the cracks during the selection procedure.
- Other relevant research papers may be excluded as a result of the imperfection of the criteria used to evaluate the relevance and trustworthiness of primary studies.

To ensure that the chosen studies were reliable and pertinent, it is crucial to stress that our systematic literature review painstakingly obtained primary empirical studies from respectable publications and international conferences. Notwithstanding these drawbacks, we believe that this work provides a solid basis for future investigation into IoT measurements.

5.3. Future Work

Building on the insights offered, future empirical research in the field of IoT measurements can utilize our work as a standard for comparative analysis. We draw attention to a significant vacuum in the literature on IoT measures, which present a chance for researchers to develop new metrics that include topics such as privacy, financial performance, convenience, safety, and user happiness. Furthermore, there is room for improvement and development in the IoT metrics ontology framework presented in this systematic literature analysis, providing the possibility of more thorough and sophisticated evaluation criteria.

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

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

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

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