A Catalog of Consumer IoT Device Characteristics for Data Quality Estimation

VALENTINA GOLENDUKHINA, HARALD FOIDL, and DANIEL HÖRL, University of Innsbruck, Innsbruck, Austria
MICHAEL FELDERER, German Aerospace Center (DLR), Cologne, Germany, University of Cologne, Cologne, Germany, and University of Innsbruck, Innsbruck, Austria

The Internet of Things (IoT) is rapidly growing and spreading across different markets, including the customer market and consumer IoT (CIoT). The large variety of gadgets and their availability makes CIoT more and more influential, especially in the wearable and smart home domains. However, the large variety of devices and their inconsistent quality due to varying hardware costs have an influence on the data produced by such devices. In this article, a catalog of CIoT properties is introduced, which enables the prediction of data quality. The data-quality catalog contains six categories and 21 properties with descriptions and trust score calculation methods. A diagramming tool is implemented to support and facilitate the process of evaluation. The tool was assessed in an experimental setting with 14 users and received positive feedback. Additionally, we provide an exemplary application for smartwatch devices and compare the results obtained with the approach with the users' evaluation based on the feedback from 158 smartwatch owners. As a result, the method-based ranking does not provide similar results to the regular users. However, it yields comparable outcomes to the assessment conducted by experienced users.

CCS Concepts: • **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability;

Additional Key Words and Phrases: IoT, CIoT, internet of things, consumer IoT, data quality, wearable devices

ACM Reference Format:
Valentina Golendukhina, Harald Foidl, Daniel Hörl, and Michael Felderer. 2024. A Catalog of Consumer IoT Device Characteristics for Data Quality Estimation. *ACM J. Data Inform. Quality* 16, 4, Article 21 (December 2024), 25 pages. https://doi.org/10.1145/3639708

1 INTRODUCTION

Consumer Internet of Things (CIoT) devices have gained significant popularity, transforming the way individuals interact with technologies in their daily lives. CIoT is human-centered and exhibits multifaceted utility across various domains [42]. For instance, it plays a pivotal role in smart home management, furnishing invaluable environmental data, and finds application in

Authors' addresses: V. Golendukhina, H. Foidl, and D. Hörl, University of Innsbruck, Innsbruck, Austria, 6020; e-mails: {valentina.golendukhina, harald.foidl}@uibk.ac.at, daniel.hoerl@student.uibk.ac.at; M. Felderer, German Aerospace Center (DLR), Cologne, Germany, 51147 and University of Cologne, Cologne, Germany, 50923 and University of Innsbruck, Innsbruck, Austria, 6020; e-mail: michael.felderer@dlr.de.

ACM 1936-1955/2024/12-ART21
https://doi.org/10.1145/3639708

healthcare for tracking vital metrics like heart rate and user-specific habits [1]. CIoT devices enable consumers to enhance their quality of life, optimize resource utilization, and personalize their experiences [42]. With the increasing adoption of CIoT devices, a massive amount of data is being generated by consumers and transmitted through interconnected networks. According to several studies in medicine, sports, and psychology, CIoT devices and especially wearables can have a significant impact on future research [8, 27, 34]. However, the quality of the data is crucial to ensure reliable and meaningful outcomes.

However, due to limitations in hardware and software, the produced data is often noisy and erroneous, which can lead to false analysis, affect the decision-making process, and compromise system performance [40]. Furthermore, despite the wide adoption of CIoT in everyday life, there is a lack of studies examining the accuracy of the data collected by **Consumer Wearable Health Devices (CWHDs)** [26].

Data quality is an essential factor in the success of CIoT systems. High-quality data ensures accurate insights, reliable automation, and personalized experiences for consumers. Several studies have focused specifically on data quality for **Internet of Things (IoT)** devices [31, 36], but existing research is limited to the examination of the quality of already produced data and does not consider the device properties. Moreover, there is a need for further research on the data quality assessment of person-generated wearable device data [9]. Since millions of CIoT devices exist, a trust score describing their data's expected quality can be used as a marker of the trustworthiness of the analysis made with such data and an important decision parameter for the purchase or implementation of such devices based on their purpose and sensitivity of the final data.

Foidl and Felderer have proposed an approach for assessing **industrial IoT (IIoT)** data sources [13]. By analyzing various characteristics, such as sensor types, data transmission protocols, and machinery capabilities, their proposed approach enables the estimation of data quality before its actual production. However, different IoT devices have their specific parameters and require different approaches to their assessment. Unlike industrial IoT, CIoT is widespread among consumers and does not follow the same high standards as IIoT. Moreover, the large number of different devices and their frequent updates complicate the development of quality standards. In addition, CIoT often functions wirelessly, which increases the likelihood of connectivity issues. All these factors lead to a potential decrease in data quality that cannot be captured by the approach for IIoT. To address this issue, this article provides CIoT-specific data-quality properties.

This article adapts and extends the catalog developed in Reference [13] to assess the quality of CIoT. To enhance the practical application of the catalog, we have developed a web-based tool that facilitates the utilization of the catalog and provides users with an accessible and user-friendly interface for their assessments. Additionally, we show an example of the catalog application in the smartwatch domain by modeling 11 devices and comparing the obtained ranking with the data quality assessment by 158 users. Therefore, this work makes the following contributions:

— an approach for data-quality assessment based on CIoT;
— a supporting tool for CIoT evaluation;
— an exemplary smartwatch evaluation and its comparison with the ranking by 158 users.

The remaining article is structured as follows. Section 2 provides the necessary background information and describes the related literature. Section 3 describes the process of catalog development, implementation of the supporting tool, and survey design for smartwatch evaluation. Section 4 presents the data-quality catalog, its software implementation, and evaluation of the tool. Section 5 presents the case of catalog application and its comparison to the users' assessment. Section 6 discusses the findings, threats to validity, and future work, and Section 7 concludes the article.

2 BACKGROUND

This section first provides background information on CIoT and data quality. Afterward, related work on data quality, data trustworthiness, and data source assessment in the realm of the IoT is discussed.

2.1 Consumer Internet of Things

The IoT has emerged as a significant technological advancement in recent years, connecting a vast network of devices and systems to the internet [15, 24]. Typical technologies involved include communication technologies, cloud computing, advanced analytics, and machine learning. The IoT has many applications, from industrial and healthcare to transportation and smart cities. However, one of the most prominent and rapidly growing areas of the IoT is the CIoT.

The CIoT refers to the network of everyday objects that are connected to the internet and can communicate with each other, such as smart home devices or wearables [5, 42]. These devices collect and utilize data to automate tasks, offer personalized experiences, and enhance awareness of the environment, resulting in time and cost savings [42]. Accordingly, the CIoT can be described as human-centric aiming to enable consumer-oriented applications.

A second prominent representative of the IoT is the industrial IoT [41, 42], with which we want to briefly compare the CIoT in the following. While the CIoT is focused on the consumer market, the IIoT is used in industrial applications where reliability and performance are critical. IIoT devices must be able to operate reliably even under harsh conditions and with minimal human intervention. Moreover, the IIoT has more connectivity standards and higher data volumes compared to CIoT. A further difference is that IIoT is mission-critical with timing requirements, while CIoT is less time-sensitive. While the CIoT usually relies on wireless communication, the IIoT includes both wireless and wired communication infrastructures.

2.2 Data Quality

Over time, multiple data quality definitions and characteristics have emerged from different domains. The most prominent definition of data quality may be attributed to Wang and Strong [47] who defined it as "data that are fit for use by data consumers." In simple terms, this definition emphasizes the importance of the intended usage of the data, meaning that only the data consumer can judge whether the data are fit for use or not.

In this work, we base our understanding of data quality on ISO/IEC's [19] definition, which is closely related to that of Wang and Strong. According to the standard, data quality is the degree to which data meets specified requirements. The standard also categorizes data-quality characteristics into two main categories: system-dependent data quality and inherent data quality. The system-dependent category considers the technological domain in which data is used and defines data quality as the extent to which it is achieved and maintained within computer systems. However, inherent data quality refers to the characteristics of the data itself, such as accuracy, completeness, consistency, credibility, and currentness. These characteristics are directly related to the values of the data and are used in the remaining article when we talk about data quality.

2.3 Related Work

There is a considerable amount of research on data quality in the field of the IoT [25]. Contributions vary depending on their perspective taken such as filtering data [22], detecting anomalies [14], or proposing new techniques for improving data quality [33]. In this section, we limit ourselves to work closest to this article. We first discuss contributions that investigate IoT-related criteria or

factors likely to affect data quality. Then, relevant research on data trustworthiness, which is often seen as a proxy measure of data quality, is presented.

2.3.1 IoT Data Quality. In 2016, Karkouch et al. [20] proposed several general factors that may affect data quality within the IoT. These factors include vandalism, resource constraints, environmental factors, issues with sensors or networks, security and privacy concerns, data stream processing, and the challenges of deploying IoT devices on a large scale.

Wearable devices have been widely studied in the field of IoT data quality. In the remaining section, we will focus specifically on research in this area, as it is particularly relevant to our own work. For example, Mahloko and Adebesin [26] focused in their work on factors that influence the data accuracy of consumer wearable health devices. They identified the tracker and sensor type, the algorithm used in the device, and limitations in the design, energy consumption, and processing as the main influencing categories. Further, a recent study by Cho et al. [9] identified device- and technical-related factors, user-related, and data governance-related factors likely to affect the data quality of person-generated wearable device data. Böttcher et al. [6] collected wearable data about more than 600 persons. One of their findings was that the data streaming resulted in a much higher loss of data compared to onboard device recording. Canali et al. [7] found that the device's location on the body is a critical factor to consider. Further, the authors highlight that the used sensors and techniques for recording data are critical for reliable data collection. They conclude that the variability of sensors and the data collection practices as well as concrete contextual information are essential characteristics in this regard that can influence data quality.

Concluding, there is a huge body of literature that highlights the importance of the intrinsic characteristics of IoT data sources regarding affecting their provided data quality.

2.3.2 Data Trustworthiness. Further contributions worth mentioning are situated in the field of data trustworthiness. Research in this area, e.g., References [2, 4, 39, 45], tries to develop approaches or methods to determine the trustworthiness of the data provided. The trustworthiness of data is closely linked to the concept of data quality, although the history of data (i.e., its origin, trace of operations, and movement) is more considered in data quality. Most research on data trustworthiness, in contrast to our aim, solely relies on data values themselves to reason about the data quality. However, there are some approaches that include characteristics of the sources providing the data.

One such approach was proposed by Tang et al. [44]. The authors present a framework to identify trustworthy sensor alarms within cyber-physical systems. They use the reliability of a sensor as a factor that impacts the data quality of the sensor to improve their proposed trustworthiness inference. However, the computation of sensor reliability is based solely on data items and does not take into account sensor-specific properties. Further, Dai et al. [11] present a framework to determine the trustworthiness of data and data providers. While the approach initially uses unspecified criteria to determine the trustworthiness of data providers, it is later recomputed based on the average trustworthiness of the data provided by those providers.

2.3.3 Data Source Assessment Approach. In a recent study, Foidl and Felderer [13] addressed the issue that many data trustworthiness approaches rely solely on the data values themselves, without taking into account the intrinsic characteristics of the sources providing the data. The authors developed an approach that separates data sources in data stores (e.g., databases) and data providers (e.g., sensors) to use their characteristics for reasoning about the data quality provided. Foidl and Felderer focused on the IIoT and proposed a catalog of data provider criteria likely to affect the quality of data produced. They further proposed a set of general quality characteristics

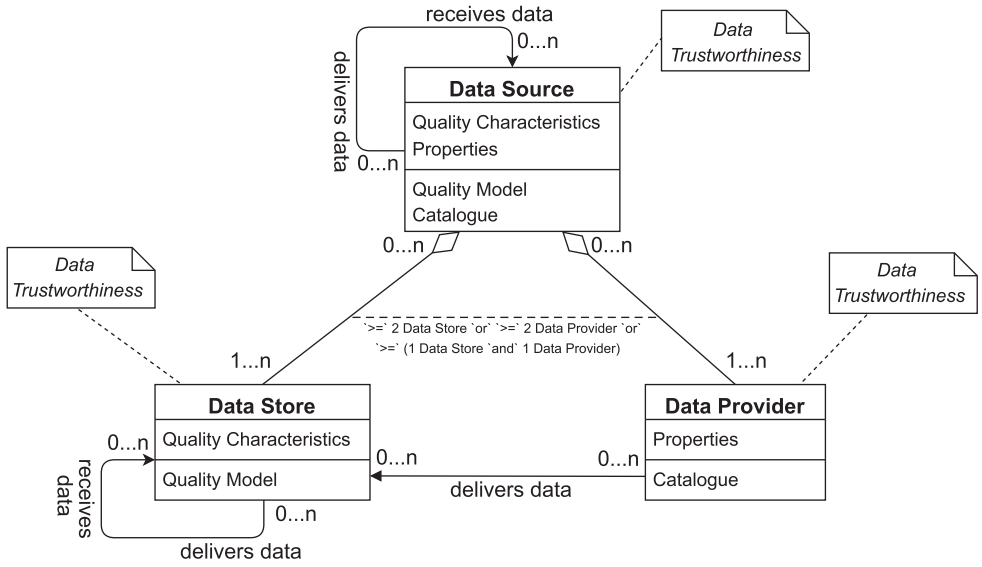

Fig. 1. Data source assessment meta-model (UML notation) [13].

that may affect the data quality of data stores. The underlying idea of their approach is to assess these characteristics and properties to infer the provided data quality of data stores and providers.

To model dataflows they proposed a meta-model, which is shown in Figure 1. The model consists of three components: data stores, data providers, and data sources (a collection of at least two of the former components). Data stores represent storages such as databases, files, or data lakes, whereas data providers represent sensors or devices that deliver data. The central idea of the model is that data providers deliver data to data stores. Foidl and Felderer proposed a quality model for assessing the quality characteristics of data stores and a catalog for assessing the properties of data providers. Whereas the data store quality characteristics are generally applicable, the data provider properties are domain-dependent. In our work, we aim to reuse their approach and develop a specific property catalog of CIoT data providers.

To be able to reason about the provided data quality, Foidl and Felderer proposed a calculation scheme to compute scores for data stores, data providers, and data sources based on the assessments. The authors developed checklists with points to conduct the assessment and used these results for score calculation. The score calculation is described in more detail in Section 3.3.

3 METHODOLOGY

To create a comprehensive catalog for evaluating data sources, our approach primarily involved researching relevant literature to identify various factors related to data quality. The extracted factors were analyzed and synthesized to construct the catalog. Additionally, we leveraged these findings to develop a diagramming tool that assists in evaluating CIoT systems. Last, we employed the catalog in a practical case study focused on wearable devices. The subsequent sections of the article detail the step-by-step process and scientific methodologies employed to achieve these objectives.

3.1 Literature Collection

One of the main objectives of the data-quality catalog is to include all relevant and critical for the assessment categories. To achieve this, we conducted a literature review including both grey and

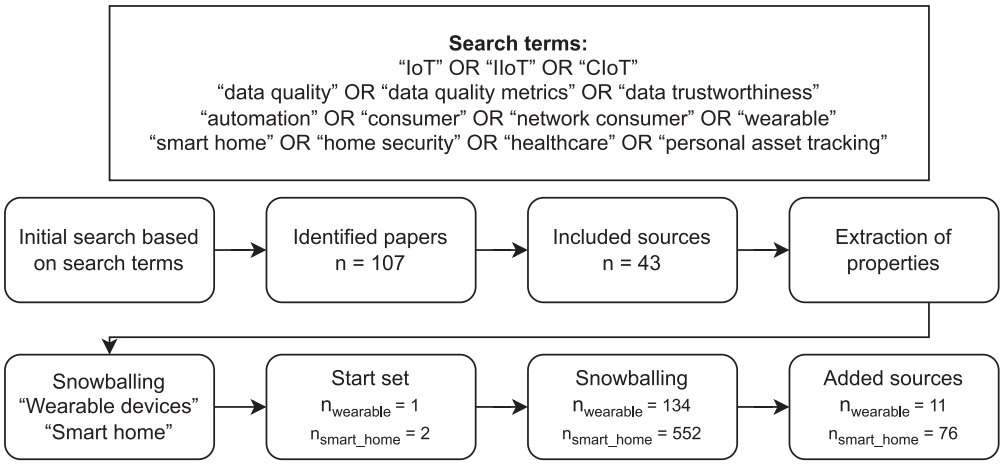

Fig. 2. Literature review procedure.

Table 1. Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
The paper mentions factors influencing the accuracy of devices	Full text of the paper is not accessible
The paper describes the general advantages or disadvantages of certain sub-properties of devices	The paper is not in English

white literature. Since CIoT is characterized by a large variety of devices and application areas, it was necessary to examine the overall and specific attributes of CIoT devices. The literature review process is presented in Figure 2.

An initial topic overview allowed us to recognize the main areas of application of CIoT and tailor the search string. To collect the set of search terms, we conducted an overview of the current research and applications of CIoT using the keywords "IoT," "CIoT," "Data quality," and "Data quality metrics" in Google Scholar. As a result, the identified areas of CIoT applications included smart home, home security, wearable, healthcare, and personal asset tracking [18]. A further search included each of these categories and such keywords as automation, consumer, and network consumer. Using the different search terms, we found literature on the identified categories to explore the general characteristics of the CIoT devices and collect data quality-related properties. To proceed with the relevant papers, we applied the inclusion and exclusion criteria provided in Table 1.

After further examination and application of exclusion and inclusion criteria, the identified literature was used to extract the general properties.

To ensure that all important categories were added, we further applied forward snowballing with a focus on wearables and smart home devices as one of the most researched areas, which are also ranked as the most popular in Google search [23]. This process was conducted for both areas, wearables, and smart home, separately following the guidelines for snowballing in systematic literature studies [48]. The starting set consisted of one literature review on wearable devices [26] and two literature reviews on IoT for smart homes [37, 43]. The snowballing iterations continued until no new papers were found.

After four iterations, we identified 134 papers on wearable devices and 552 papers on smart home topics based on the title and abstract. Following a more thorough evaluation of the papers during

the second round of selection, we narrowed down our focus and identified 11 papers relevant to wearable devices and 76 papers related to home devices that were deemed suitable for inclusion in the data-quality catalog. Furthermore, our snowballing search method yielded three additional properties that were considered valuable additions to the catalog.

3.2 Catalog Creation

As a base of the data-quality catalog, we used the catalog developed by Foidl and Felderer for IIoT assessment [13]. The required CIoT-specific properties and characteristics for the catalog were extracted and processed from the set of related literature defined in the previous section.

To obtain a comprehensive list of properties, all significant text sections containing related characteristics were extracted. To control if these characteristics have an influence on the data quality, we used the five inherent data-quality characteristics from the ISO 25012 standard [19]: accuracy, completeness, consistency, currentness, and credibility. If a data provider property is able to influence at least one of these characteristics, then it is included in the final set of properties for the data-quality catalog.

During the literature analysis process, we reviewed over 50 characteristics, which were then synthesized to 28 CIoT properties, of which 25 had a direct influence on data quality. We analyzed the final set of properties and united the similar ones so that the properties tend to a higher level of generality but maintain their specific characteristics regarding CIoT data providers. This process resulted in six categories and 21 properties.

To achieve this, we followed a thematic synthesis approach [10]. As a result of the iterative process of synthesis and revision of the catalog by other researchers, we distinguished six categories (connectivity, general, hardware, market standpoint, mobility, and security) and their consecutive CIoT data provider properties. To be able to use them for the evaluation of CIoT devices, each category provides a description, an example of use, and evaluation options in the form of a 3-point Likert scale describing the level of influence on data quality.

3.3 Trust Score Computation

To calculate the trust score τ, we used the method proposed by Foidl and Felderer [13]. A score τ describes to which extent the source could be trusted, ranging from 1 (100%) to 0 (0%).

For data providers, the score τ is computed in the following way:

$$\tau(Data\ Provider) = 1 - \frac{\sum selected\ option\ score_i}{maximal\ score\ possible}. \tag{1}$$

The score τ for the data store gets calculated using the **Quality Score (QS)**:

$$\tau(Data\ Store) = \frac{QS(Data\ Store)}{max\ QS(Data\ Store)}. \tag{2}$$

Both scores are incorporated as an average trust score $\bar{\tau} = \frac{\sum_{i=0}^{n} \tau_i}{n}$, into the overall trust score for a specific data source, whereas j determines the number of distinct data sources:

$$\tau(Data\ Source) = \frac{\bar{\tau}(Data\ Store) + \bar{\tau}(Data\ Provider)}{j}. \tag{3}$$

Based on the value of the trust score τ, the corresponding trust level can be identified. One of the interpretation strategies includes low, medium, and high trust categories. In this categorization, devices with τ less than 0.4 are considered as low trust, τ equal to 0.4 to 0.8 represent medium trust devices, and devices of high trust have a trust score of more than 0.8.

The scores are based on the six identified categories and 21 properties. Such calculation can become a complex and error-prone task. To address this challenge, the equations were implemented in the digital tool to automate the trust score τ computation.

3.4 Tool Support and Evaluation

To facilitate the use of the CIoT data-quality catalog, we provide digital tool support. The application is developed using the client-side JavaScript diagramming library mxGraph.[1] The full functionality of the library is demonstrated with diagrams.net.[2] The library provides functionality to build and manipulate graphs and is adaptable for the purposes of this article.

To estimate ease of use, we conducted an experiment with 14 students. In the experiment, the respondents were asked to execute a given task scenario and estimate the quality of a given data provider using the tool. The participants were provided with a list of actions they needed to accomplish to complete the task. Afterward, the participants were asked to complete a questionnaire to evaluate the software tool's usability. The questions were designed to measure the ease of use of the software on a 6-point Likert scale ranging from 1 (extremely likely) to 6 (extremely unlikely). Feedback was collected throughout the experiment to improve usability as part of future work.

3.5 Case Study

To demonstrate how the catalog can be applied and evaluate the results, we focused on the data generated by smartwatches. We conducted a survey to gather the users' opinions regarding the data quality of their wearable devices. Then, the data quality of the most represented watches was modeled using the tool. The next sections describe the survey design process, application of the catalog, and data analysis procedures.

3.5.1 Survey Design. The survey consisted of 15 questions and contained questions on the type of device, the experience of the users, and different data-related issues. To avoid misinterpretation, each question related to possible problems had several examples in the description. Questions and examples are listed in Table 2.

The first question aims to examine the experience of the participants with the device and their awareness of the produced data. Possible answer options include basic settings; customized options; new user-defined functions; export, import, and data evaluation by the participant.

Data-related issues were formulated based on the problems reported by users of smartwatches. Such reports were collected from users' reviews on various smartwatch devices on Amazon.[3] The process consisted of the following steps. Using the keywords "smartwatch" and "fitness tracker," the first page results were collected. The resulting devices provided a plethora of negative reviews, of which informative reviews were selected. After a revision of all selected comments, related data points were identified and summarized into failures used for the survey. The questions were formulated in such a way that they cover all data-quality dimensions, i.e., completeness (questions 5, 7, 8, 13), accuracy (questions 9, 10, 11), credibility (questions 4, 6, 12), currentness (question 15), and consistency (question 14). The evaluation is done using a 4-point Likert scale with the options never, rarely, often, and always.

The survey was created on the Limesurvey platform[4] and distributed among the students and employees of an Austrian university. The target group of the survey was people who have and

[1] https://github.com/jgraph/mxgraph
[2] https://diagrams.net
[3] www.amazon.com
[4] https://www.limesurvey.org

Table 2. Survey Questions

#	Survey question	Example	Question type
1	How familiar are you with your device? To what extent have you customized/utilized your device?	Customizations include adding detailed data about yourself, setting specific training modes, and changing the accuracy of GPS measurements	Single choice
2	Which device do you own?	—	Single choice or free text
3	Have you performed the same/same activities multiple times using the equipment?	—	Single choice
The core questions: have you experienced the mentioned problems related to your device?			
4	My device does not measure similar data to other known devices/references	Treadmill at the gym, devices at the doctor's office, Google GPS distance data of track	4-point Likert scale
5	My device is not continuously tracking activities when required	Stops tracking in the middle of an activity, requires manual changing of tracking activity, randomly slows down	4-point Likert scale
6	My device is not assigning the correct activity when used.	Swimming activity recognized while sweating on a hot day, running while walking, sleeping while awake	4-point Likert scale
7	My device reboots automatically during a workout	Resulting in missing data points	4-point Likert scale
8	My device loses complete recorded measurements of a route/exercise/ measurement	On synchronization, reboot	4-point Likert scale
9	My device has problems detecting high and low readings correctly	Workouts produce high heart rates	4-point Likert scale
10	My device is measuring data that does not match the performed activity	Floor climbing while walking flat, tracking sleep hours when awake, and the opposite	4-point Likert scale
11	My device has unrealistic measurement outliers	Unrealistically low/high values	4-point Likert scale
12	My device captures motion data, although no activities are performed	Step counting during sedentary activity or the charging process	4-point Likert scale
13	My device is losing data during recordings	GPS coordinates, heart rate measurements	4-point Likert scale
14	My device measures different values for identical activities	Different GPS data on the same running track	4-point Likert scale
15	My device is not providing me with the measurements in a timely manner	Delayed heart rate changes during high-intensity training; not providing data until a certain continuous sleep amount is reached	4-point Likert scale

actively use a smartwatch of any brand. In total, we received 543 responses to the survey, of which 297 were full responses.

3.5.2 Data Analysis. Only completed responses were considered for the analysis. To enhance the quality of the results, the data entries were sorted out if an invalid device name was given, no device name was given, company name only was given, or less than 50% of core questions for data quality assessment were filled out. Additionally, if two models of a device had the same technical specifications, devices were merged into one model to increase the number of responses per device. To avoid polarized opinions and outliers, we calculated the standard deviation to see the difference in the final scores among the users of the same devices. As a result, we collected information about 62 different devices, of which 11 devices from five brands were used for the final evaluation. Each device score was based on at least four responses from different users.

Since technical issues can differ per device and can be influenced by external factors, the overall data quality was derived from the frequency of errors, and individual errors were omitted for

simplification, i.e., each issue was given equal weight and the summary of issues was considered as the users' score.

3.5.3 Catalog Application. Once the devices with the highest response rates and the most reliable user assessments were identified, we proceeded to model for the selected smartwatches, utilizing the catalog and the developed tool. To ensure the objectivity and accuracy of the trust score calculation, a smartwatch-specific scoring schema was employed (see Figure 5). This schema was created based on extensive research into field-specific forums, internet sources, and examination of smartwatch documentation.

When modeling the devices inside the tool, all information about the devices was taken from open sources including device documentation from manufacturers and distributors. For the modeled sources, all premium services are assumed to be activated to enable the full feature set. A detailed listing of the set-up rules for catalog properties is described in Section 5.

The results from the survey were then compared to the trust score (τ) modeled with the tool leading to the creation of two distinct rankings that could be visually compared. To quantitatively measure the relationship between the modeled scores and the perception of the participants, Spearman's rank correlation coefficient was used.

4 DATA-QUALITY CATALOGUE

After examining the related literature and synthesizing the data, all properties were grouped into six categories: connectivity, general, hardware, market standpoint, mobility, and security. In this section, we describe the properties of each category, introduce the data provider quality catalog, and present the web-based tool and its evaluation.

4.1 Influence on Data Quality

Overall, 21 properties were extracted from the literature. Although the categories have similarities with the catalog of industrial IoT [13], we identified some categories important specifically for CIoT, e.g., market standpoint and security. Since CIoT data providers are more human-centric, in contrast to the IIoT provider type, a more detailed examination of the nature of human input, e.g., updates, configuration, and so on, was made. It is crucial to consider mechanisms for validating and verifying user input to maintain high-quality data. Moreover, the competitive market leads to ecosystems of large companies, directly influencing the interoperability of those devices across each other and defining the software produced for different ecosystems. All categories were checked against the five data-quality dimensions: completeness, accuracy, credibility, currentness, and consistency. Table 3 presents the CIoT-related properties and their effect on the dimensions of data quality.

Challenges related to device mobility, connectivity, and user interaction can impact data completeness. Inconsistent data collection intervals, missing or incomplete data due to network disruptions or device failures, and limitations in capturing specific data types can affect the completeness of CIoT data.

The accuracy of CIoT data is influenced by various factors, including device sensors, signal noise, calibration, and environmental conditions. Robust sensor calibration, quality control measures, and user feedback mechanisms are vital for ensuring accurate CIoT data.

Data credibility refers to the degree of trustworthiness, reliability, and authenticity of the data collected from CIoT devices. CIoT introduces new challenges to data credibility due to the heterogeneity of devices, user-generated content, and the potential for data tampering.

Finally, CIoT data needs to be timely and up-to-date to support real-time decision-making and enable dynamic applications. However, factors like device mobility, network latency, and battery

Table 3. Influence of Properties on Data Quality

Category	Property	Completeness	Accuracy	Credibility	Currentness	Consistency
Connectivity	Integration flexibility [38]	x				x
Connectivity	Communication quality [38]			x		x
Connectivity	Connection latency [13] [32]				x	
Connectivity	Secured device accessibility [38]	x	x	x		x
General	Amount of Data collection [26][12]		x	x		
General	Device compatibility [3]	x				x
General	Usability [35][17]	x	x	x		x
General	Device Age [13]	x	x	x	x	x
General	Data validation option [35][21]	x		x		
General	Certification [21]	x	x	x		
Hardware	Power source longevity [26][13]	x		x	x	x
Hardware	Power source power supply [13] [3]	x		x	x	x
Hardware	Power source time per charge [26][13]	x	x	x	x	x
Hardware	The tracker and sensor types [26]	x	x	x	x	x
Market standpoint	Application quality [3]	x	x			
Market standpoint	Manufacturer prominence [26]		x	x		
Market standpoint	Price category [3] [32]	x	x	x		x
Mobility	Movement amount [13][35]	x	x		x	x
Security	Security configurations [30]	x		x		x
Security	Software update currentness [3] [26] [30]	x	x	x	x	x
Security	Encrypted communication security [30]	x	x	x		x

longevity can impact data currentness. Inconsistencies in data formats, semantics, or standards across different devices and platforms can affect data consistency.

4.2 Catalog Elements

The final CIoT data provider catalog has the form of a questionnaire where each question describes a certain property of the data provider. This catalog consists of six main categories, encompassing a total of up to six properties within each category. For ease of comprehension, each category and property in the catalog is accompanied by a descriptive explanation. The full catalog is presented in Table 4.

The catalog introduces a standardized method for determining the level of each property. By offering three options with accompanying examples, users can effectively assess and rate the performance and capability of each property. This enables a more accurate evaluation of the data quality provided by CIoT devices and enhances the overall trustworthiness and reliability of the assessment.

Once all the questions in the catalog are answered, the assigned points for each property are aggregated to generate a trust score for the device. The trust score τ is calculated based on

Equation (1) and aims to provide an objective measure of the data quality that can be expected from the corresponding data provider.

The following sections describe the catalog structure, define its elements, and present the digital assessment tool.

4.2.1 Connectivity-related Properties. The reliability of connectivity affects the consistency and availability of data, with unreliable or intermittent connectivity leading to data loss and incomplete or inconsistent data. Latency, or data transmission delay, can impact the timeliness and currentness of data, especially in real-time applications. Furthermore, bandwidth limitations can affect the speed and capacity of data transfer, potentially leading to delays and reduced data quality.

These connectivity-related factors collectively influence the overall data quality of CIoT devices and can impact the reliability, responsiveness, and effectiveness of CIoT applications and services. Connectivity-related properties comprise four properties: integration flexibility, communication quality, and connection latency. Their description is presented in Table 5.

4.2.2 General Properties. General properties encompass various CIoT-specific aspects that can significantly impact data quality. They are derived from user reviews or more sophisticated technical reviews when filling out the data provider catalog. All assigned properties and their descriptions can be found in Table 6.

The age of the devices has a major impact, as older devices do not receive the same support service and updates. Moreover, newer devices become a quality advantage due to newer technologies used.

The competitive market in CIoT can result in different ecosystems and platforms developed by large companies. Interoperability becomes important for seamless integration and communication between devices from different manufacturers. Incompatibility or lack of standardization can impact data quality by introducing inconsistencies or limitations in data exchange.

Additionally, the general category takes into account the amount of fine-tuning and usability to which those devices can be used. A wrong setup of the device does not return quality data [8], e.g., changing indoor/outdoor location, training set, and other factors can lead to possible errors.

4.2.3 Hardware-related Properties. Regarding hardware constraints, only the most common factors including battery and sensor/tracker type are mentioned as separate properties. In general, the previously mentioned hardware constraints regarding energy, memory, communication, storage, processing power, and cost constraints [22, 46] are included in diverse categories, not specifically targeting only hardware.

The hardware category includes more general properties relevant to most CIoT devices. For example, devices are often battery-powered. When a device is not connected directly to a power source, the battery plays a crucial role in terms of hardware. Since data can only be collected when the device has enough energy this has a crucial impact on the data quality. Power loss plays a vital role in long-term monitoring when interruption can affect data accuracy or lead to the loss of data [16]. All properties and their definitions are listed in Table 7.

4.2.4 Market Standpoint-related Properties. The market standpoint category indicates the perspective and requirements of the consumer market. It can influence data quality by determining the level of demand for accurate and reliable data. Higher market expectations can drive CIoT providers to ensure better data quality to meet consumer needs. Furthermore, price, manufacturers, and application quality play a significant role in defining device quality and, thus, the quality of produced data. For instance, price category and manufacturer prominence can partly reflect the quality of the used components, which has an influence on the performance of wearable devices [26], completeness, and accuracy.

Table 4. Data Provider Property Catalog

Category	Properties	Details/Examples	Subproperties (checkboxes)	Subproperty description	Points
Connectivity	Integration flexibility	CoAP, MQTT, XMPP, AMQP	low medium high	able to communicate with new standards able communicate with most standards supports legacy communication standards	5 3 0
Connectivity	Communication quality	NFC, Bluetooth, Wlan	low medium high	no stable connection can be accomplished most of the time the connection can be kept up stable connection	5 3 0
Connectivity	Connection latency		low medium high	asynchronus communication (e.g. Synchronizing after manual adjustments) communication in bulks communication data is always transfered	5 3 0
Connectivity	Secured device accessibility	Open ports, administration interface, only connected through a gateway	full restricted only over specified resource	knowing the device address, data can be accessed An admin interface keeps the user from connecting to the device. an admin interface keeps the user from connecting to the device. (with block list)	5 3 0
General	Amount of Data collection	Wearable device: heart rate, speed, GPS data ...	low medium high	data is collected from more or less one source multiple data direct data information is collected also coupled metadata is considered	5 3 0
General	Device compatibility		limited mostly seamlessly	only in the intended infrastructure can be included into a more diverse infrastructure after some configuration can be included in any infrastructure without effort	5 3 0
General	Usability		hard medium easy	not possible or only "experts" can configure the device to its full extend after some effort it is possible to configure the optimal settings no knowledge needed e.g. autoconfiguration	5 3 0
General	Device Age	Sensors, Communication protocols, wireless technologies	old middle new	legacy technology common on the consumer market new technology	5 3 0
General	Data validation option	Recordings like running tracks GPS data log data etc. can be validated	low medium high	data cannot be altered afterwards data collection available in blocks that could be deleted correcting, deleting and adding of missing or errorneous data	5 3 0
General	Certification	no official certification is available complies to commission rules etc. FDA or CE approval	not available market or regulatory certificates medical or industry grade certificates	no certificate given for example complies with Federal Communications Commission (FCC) Rules FDA or CE approval	5 3 0
Hardware	Power source longevity	LiMnO_2 225 mAh, Lithium polymer battery, Lithium-ion polymer, CR2032 coin cell	less than 4 months 4 months over 6 months	short amount of time medium can be used over a long period of time	5 3 0
Hardware	Power source power supply	LiMnO_2 225 mAh, Lithium polymer battery, Lithium-ion polymer, CR2032 coin cell	reduced performance nearly stable performance always full performance	some components are kept on standby and do not always gather data no standby but some components are throttled and those dont gather data as accurately as possible all components are used to their full extend to gather data	5 3 0
Hardware	Power source time per charge	LiMnO_2 225 mAh, Lithium polymer battery, Lithium-ion polymer, CR2032 coin cell	low medium high	the power source must be exchanged often the power source must be exchanged on regular basis the power source must be exchanged after a long period of time or not at all	5 3 0
Hardware	The tracker and sensor types	Device for heart rate measurement. For example Photoplethysmography (PPG) sensors for heart rate, Pedometer and accelerometer, etc.	low quality general purpose specialized	low quality sensor or misplaced e.g. misused sensor (accelerometer for detecting wakefulness) appropriate sensor with perfect placement	5 3 0
Market standpoint	Application quality	Crashes, Apple / Android Store rating, usability	low medium high	application is full of software bugs and nearly unusable application fulfils its purpose, but has some drawbacks application is fully tested and runs smoothly	5 3 0
Market standpoint	Manufacturer prominence	Vates, Softengi, R-Style Lab	sparse mediocre wide spread	unknown to the market. Niche product or newly entering the markt. known to most of the IoT consumer market even known to consumers, which are not engaged in the IoT market	5 3 0
Market standpoint	Price category	Smartlight bulbs, thermostat	cheap average high	considerably cheaper than the average market value more or less the average market value a higher price than the average market value	5 3 0
Mobility	Movement amount	Smart watch, Amazon echo, smart thermostat, doorbell, garden robot etc.	often partly static	moved during its whole operation (wearable) mostly static but moved sometimes (audio interface) never moved after installation (thermostat)	5 3 0
Security	Security configurations	Manufacturer settings an passwords are pushed without consence onto the devices, basic settings like password, fully cosumizable settings	no configuration possible basic settings like password fully configurable	manufacturer doesn't give any possibility to configure the device basic security settings like passwords are possible manyfold advanced security option	5 3 0
Security	Software update currentness	Firmware updates, User software updates etc.	never regularly very often	device is shipped with static software updates are made on regular basis, although some important updates may be delayed to a day as soon as possible important updates are pushed to the device	5 3 0
Security	Encrypted communication security		encrypted only after upload partly encrypted beforehand fully encrypted communication	unencrypted internal communication encryption of critical data occurs all communication data is encrypted	5 3 0

Table 5. Connectivity-related Properties

Properties	Description
Integration flexibility	Describes to which extend the device is compatible with other communication standards.
Communication quality	Most of the devices are wireless. Describes the quality of their wireless connection. This includes aspects like range, transfer rate, and amount of disconnects.
Connection latency	Latency for data communication. May be triggered by the connection or the speed of data processing.
Secured device accessibility	Describes to which extend data can be accessed over the internet.

Table 6. General Properties

Properties	Description
Amount of data collection	Describes how many different data points/sources are collected on the device for a given function.
Device compatibility	Describes if a device can be added to current IoT infrastructure, is isolated from other manufacturers, or requires some adaptation.
Usability	Describes to which extent the user can use the device with its most accurate settings. Takes into account the learning curve, autoconfiguration, and user interface usability.
Device Age	Describes how old the device is. This takes into account if new releases of the same device category occurred after the release.
Data validation option	Degree to which user can alternate data before it gets used by subprocesses.
Certification	Certificates, approvals, or other commission validations.

Table 7. Hardware-related Properties

Properties	Description
Power source longevity	Describes whether a battery is used and what type of battery is used. Takes into account the long-term longevity of the battery.
Power source power supply	Takes into account the power provided to the given device. Describes if the given power is sufficient for the device.
Power source time per charge	Takes into account power supply, and usable time per charge.
The tracker and sensor types	Describes the type of attached sensors.

The overview of the identified properties is shown in Table 8.

4.2.5 Mobility-related Properties. The mobility category includes only one property, which is the movement amount. Nevertheless, it was added in a separate category as mobility is specific to CIoT and has a significant effect on the final data quality. The requirement of continuously delivering services to mobile users leads to another challenge. The description is presented in Table 9.

Table 8. Market Standpoint-related Properties

Properties	Description
Application quality	Describes the quality of the application itself. This includes firmware, user feedback, store rating, and general quality of the applications for the IoT devices.
Manufacturer prominence	Describes how well the manufacturer is spread inside the IoT market for this type of device. This takes into account marketing experience, software design, and manufacturing experience.
Price category	Describes the number of flaws by reducing costs or rushing the product onto the market.

Table 9. Mobility-related Properties

Properties	Description
Movement amount	Refers to the patterns and behaviors associated with the mobility, or lack thereof, of devices within the CIoT ecosystem.

Table 10. Security-related Properties

Properties	Description
Security configurations	Describes to which extent the security settings can be modified or updated by the device owner.
Software update currentness	Describes how often the device receives important updates.
Encrypted communication security	Reduced risk of data manipulation.

The mobility of CIoT devices can affect data accuracy, particularly in scenarios where the device's location is critical to the data's meaning or context. For example, location-based data, such as GPS coordinates or environmental monitoring data, relies on accurate positioning. Any inaccuracies in the device's mobility tracking or positioning systems can lead to erroneous or misleading data. Furthermore, mobility introduces challenges in maintaining a reliable and uninterrupted connection between CIoT devices and the network infrastructure they rely on.

4.2.6 Security-related Properties. Security is a critical aspect of CIoT, as consumer devices often handle sensitive personal data. The security property can greatly impact data quality by addressing vulnerabilities and protecting against data breaches, unauthorized access, or tampering. Insecure CIoT devices might threaten other connected devices [29]. Due to the increasing number of connected devices, there are chances of exploitable cyber-physical security vulnerabilities. Ensuring robust security measures enhances data integrity and reliability. The security category includes properties related to security configurations, software update currentness, and encrypted communication security. The definitions are provided in Table 10.

4.3 Tool Implementation

The data provider quality catalog is accompanied by a digital assessment tool named graphted.[5] This tool streamlines the assessment process, allowing users to conveniently navigate and

[5]https://graphted.github.io/graphted/

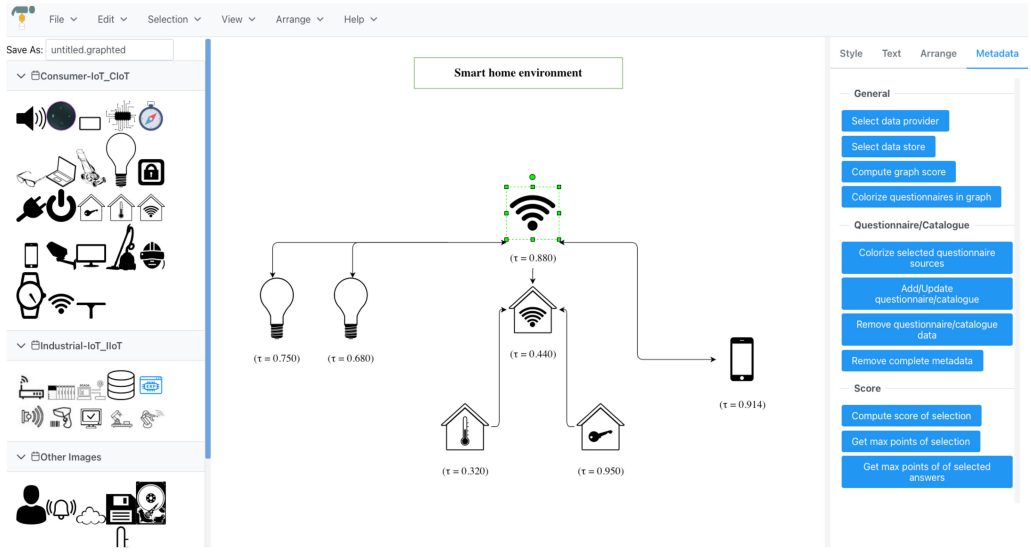

Fig. 3. Software-based assessment tool for the data provider quality catalog.

complete the questionnaire. By digitizing the catalog, users can easily access, track, and analyze their assessments, further enhancing the efficiency and effectiveness of the evaluation process. The underlying computations of trust score τ are based on the equations from Section 3.3.

To make it universally available and avoid a large setup, a web application is chosen as a target platform. The front end of the tool was implemented as a client-side web application representing a minimal graph editor **User Interface (UI)**. The tool can assist in the evaluation of one device but also supports the assessment of several connected devices, which is often the case with CIoT, e.g., a smart home system must contain several sensors and devices to function properly. Figure 3 presents the modeling process of a smart home network consisting of several elements, where for each element trust score τ is calculated.

The underlying IoT environment is modeled as a graph. Each vertex can represent a component type from the corresponding meta-model as shown in Figure 1. These components were modeled as vertices or groups of vertices inside the application, where each vertex is assigned to its corresponding catalog. As an example, the CIoT data provider catalog contains categories, properties, descriptions, options, and additional descriptions as presented in Table 4. Similar catalogs exist for the data store component (used by both IIoT and CIoT) and the data provider component for IIoT. The last component type, data source, represents a group of at least two elements of the aforementioned component types. The tool calculates the trust score τ based on the filled-out questionnaire for each vertex. The calculations are based on Equations (1), (2), and (3). Multiple vertices can then be used to calculate the overall trust score for the modeled graph. For visibility, each data source component could be highlighted by a distinct border color.

The tool interface consists of four main sections.

— *Menubar* provides a collection of functionalities including saving, graph editing options, and so on
— *The left side area* includes project name and icon collections for vertices to drag and drop into the graph area.
— The section containing *the graph building area* is located in the center

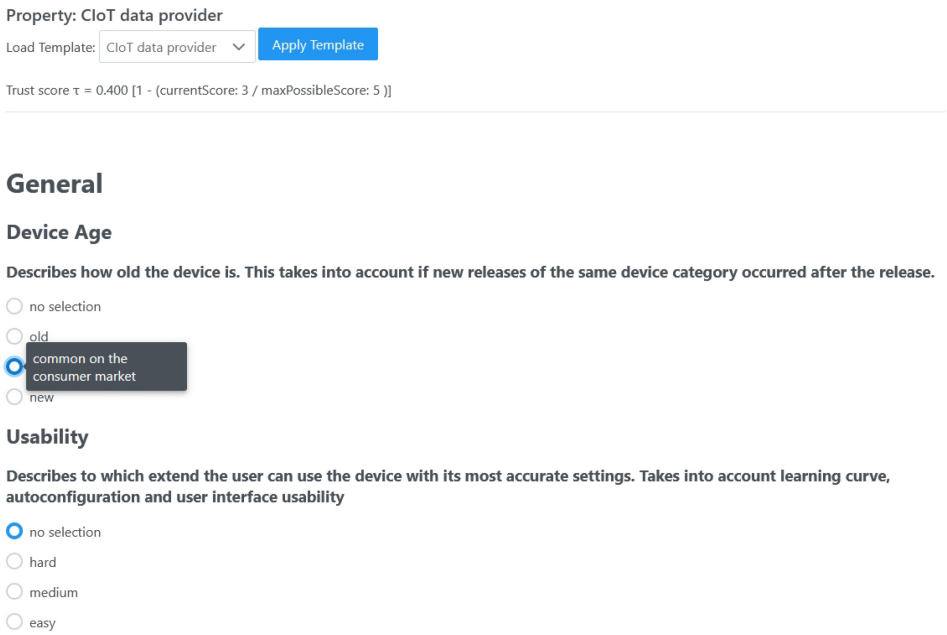

Fig. 4. Snippet of CIoT data provider catalog questionnaire.

— The right side area provides *editing options*. These options change based on the current selection in the graph. This area also contains the "Metadata" tab containing the buttons for the data source assessment.

To enable quality assessment within the tool, the following functionalities were implemented:

— Handling the questionnaire from its JSON format including loading, saving, rendering as a form, and editing.
— Dynamic calculation of the trust score based on the selection.
— Additional interaction with the graph editor.

An exemplary snippet of evaluation of one of the properties of the data provider catalog is shown in Figure 4. The trust score τ is shown at the top followed by the questionnaire. While the assigned questionnaire is being filled out, the associated trust value τ is calculated dynamically. When completing the survey, additional tips are shown to facilitate the understanding of the properties.

Additionally, the tool supports the calculation of the trust score over a net of connected devices. When several IoT elements are selected, their calculated scores are combined into an overall trust score for multiple nodes. Consequently, the overall trust score computation can be adapted in two ways. The first option is to change it to the selected nodes, the second option is to update or remove the underlying questionnaires of the selection.

4.3.1 Tool Evaluation. To evaluate the usability of the tool, we conducted an experiment with 14 students and evaluated their experience afterward with a questionnaire. The subjects were between 18 and 24 years old, and currently enrolled in a Software Engineering Master's study program. Participants were instructed to select the response option that best represented their experience with the provided software by choosing a number between one and six. Higher scores indicate a stronger disagreement, while lower scores indicate a higher agreement or likelihood. The medians of students' responses to each question are presented in Table 11. At least half of the

Table 11. Usability Evaluation of the Tool

Question	Median
Learning to operate the diagramming tool would be easy for me.	2.00
I would find it easy to get the diagramming tool to do what I want it to do.	2.50
My interaction with the diagramming tool would be clear and understandable.	3.00
I would find the diagramming tool to be flexible to interact with.	2.00
It is easy to remember how to perform tasks using the diagramming tool.	2.00

1—Extremely likely; 6—extremely unlikely.

participants answered that it is extremely likely or quite likely to learn how to operate the tool and remember how to use it.

During the experiment, most users could complete all task scenarios indicating that the tool is usable, and the tasks were formulated understandably. The users found it quite likely to remember how to perform tasks using the tool and slightly likely how to operate the tool, getting the tool to do what they want to do and being flexible to interact with. More detailed results for every question are shown in Table 11. Open-ended questions during and after the survey revealed that the area where the tool can be improved the most is in the interaction with the diagram, i.e., the unclear navigation around the diagram and unclear handling of drawing edges.

5 APPLICATION

This section presents an example of data providers' quality catalog application and compares the modeled results with the collected users' experience. For this purpose, smartwatches were chosen as one of the most widely used CIoT devices. First, we present the results of the survey designed to collect feedback from the smartwatch users. Smartwatches with more than four responses and high agreement scores were then modeled using the developed quality catalog and supporting tool. The results are then compared against each other.

To ensure the anonymization of results and not promote any brands in this article, we do not provide models and brands of the examined smartwatches. Overall, our sample consisted of devices of two brands represented by five and three models, and three other brands represented by one model.

5.1 Users' Evaluation

Overall, the respondents reported 62 different smartwatch models. After data cleaning, elimination of outliers and invalid results, and standardizing smartwatch brand and model names, only smartwatches with four or more answers were selected for further analysis, which resulted in 158 responses on 11 smartwatch models from five different brands. Of the respondents, 16% use the basic settings, 45% make some customizations, 23% use new user-defined functions, and 15% export and evaluate data by themselves.

The mean results of each respondent's answers on the same device did not show large differences. The standard deviation of each device assessment varies from 0.04 to 0.16.

The issues that were the least reported by the participants were losing complete recorded measurements of an exercise and measuring different values for identical activities. More than 80% of the participants stated that it never happened to them. The most frequently reported issues are losing data during recordings, measuring data that does not match the performed activity, rebooting automatically during a workout, and presenting unrealistic measurement outliers. More than 50% of the respondents answered that they face such problems rarely or often.

To calculate the users' score for each device, the points for all 12 core questions were summarized for each respondent and the mean value among the users of the same smartwatch was calculated. With the maximum possible score of 36, the scores for different devices ranged from 27 to 31.

Category	Property	Description	Option	Additional Description	Points
Connectivity	Integration flexibility	By common protocols (Wifi 2.5GHz/5GHz; Bluetooth, manufacturer specific protocols compatible with other devices)	Low	Only newest Wifi and Bluetooth supported (require high OS version for coupled devices)	5
			Medium	Default (Wifi and Bluetooth support)	3
			High	UMTS and default (Wifi and Bluetooth support)	0
	Communication quality	By quick search findings of disconnects, pairing errors, etc.	Low	Multiple kinds of error occurs were found through a quick search	5
			Medium	One kind of error was found through a quick search	3
			High	No findings in a quick search	0
	Connectivity latency	Quick search findings of device lags	Low	Multiple findings occur through a quick search	5
			Medium	One issue was found during a quick search	3
			High	No findings in a quick search	0
General	Amount of data collection	The number of sensors in relation to accessible data	Medium	Default (using multiple sensors for functions like sleep detection is standard)	3
			High	High: all sensor data available (might include even activity-related processing)	0
	Device compatibility	By prominent OS: smartphone (Android and IOS support), computer (Mac and Windows support)	Medium	Limited support of OS	3
			High	All prominent OS supported	0
	Device age	Resease date	Old	2015 - 2017	5
			Medium	2018 - 2020	3
			New	2021 - 2022	0
Hardware	Power source poiwer supply	Can be energy-saving options edited to force the full device performance	Reduced performance	Device performance limited for improved battery	5
			Nearly stable performance	Full device performance except in power saving	3
			Always full performance	Force the full device performance	0
	Power source time per charge	Battery time per charge	Low	< 13h	5
			Medium	13 - 20h	3
			High	> 20h	0
	The tracker and sensor types	All devices are smartwatches	General purpose		3
Market standpoint	Application quality	Based on application rating of related app stores (smartphone and computer)	Low	1-2 stars	5
			Medium	3-4 stars	3
			High	5 stars	0
	Manufacturer prominence	Based on the market share of the company	Sparce	Niche no-name manufacturer with new devices	5
			Medium	A bigger manufacturing company	3
			Widespread	One of the major players in the market	0
	Price category	Based on common smartwatch prices of results	Cheap	< 140$	5
			Medium	140$ - 190$	3
			High	> 190$	0
Mobility	Movement amount	Typical for smartwatches	Often		3
Security	Encrypted communication security	Derived based on the difficulty of data extraction	Encrypted only after upload	Direct access in same Wireless Local Area Network (WLAN) or possible without any keys	5
			Partly encrypted beforehand	Non of the other options. Some other kind of access (e.g. partial data through Universal Serial Bus (USB); WLAN)	3
			Fully encrypted communication	Any data access requires a key	0

Fig. 5. Smartwatch evaluation criteria.

5.2 Tool Evaluation

For the modelled sources, all premium services are assumed to be activated to enable the full feature set. The properties "Usability," "Secured device accessibility," "Security configurations," and "Software update currentness" were used in the way they are described in the catalog from Table 4, other properties and possible options had to be adapted to smartwatch devices. The adapted properties and options are listed in Figure 5. The 11 devices identified from the survey responses were individually modeled with the tool. Information about the devices was collected from open sources and documentation. Each device was evaluated based on the defined properties on a scale from zero to five. The trust score τ was calculated using the equations in Section 2.

The trust scores τ ranged from 0.42 to 0.76, which shows a wider range than the users' assessment. According to the catalog evaluation, none of the represented smartwatches achieved a high trust level, all watches can be considered as devices with moderate trust level.

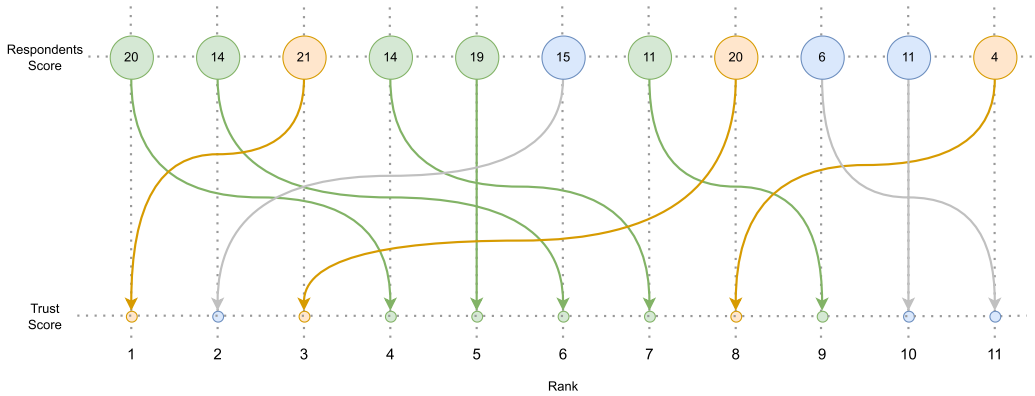

Fig. 6. Comparison of the scores. Each circle represents an individual device, and the number of answers is indicated inside the circles. The devices from the same brand are colored green and yellow. Within the devices colored in blue, each represents a different brand.

5.3 Comparison

The results gathered from the respondents and the scores modeled using the tool were used to create smartwatch rankings, which were then compared against each other. The change in the ranking is presented in Figure 6. The correlation between the two rankings was measured with Spearman's rank correlation coefficient.

Overall, when comparing all the answers and the modeled scores, the users' evaluation differs as shown in Figure 6. We discovered a low correlation of 0.5 with no significance (p-value of 0.9). However, when checked for the experience of the users, i.e., question 1 of the survey (see Table 2), we found that the correlation increases with the experience of the respondents. The highest correlation with the CIoT catalog approach was discovered in the group of experienced participants who export and evaluate data by themselves. The correlation coefficient in this group equals 0.66 and is significant (p-value 0.03).

As depicted in Figure 6, there is a notable disparity between the overall rankings derived from respondents' scores and trust scores. Nevertheless, when we narrow our focus to the comparison of devices from the same brand, a significant alignment emerges. Specifically, when examining a brand comprising five distinct smartwatch models, and another brand featuring three distinct models, the users' ranking corresponds closely with the trust score-based ranking. When considering solely the former brand within the ranking highlighted in green in Figure 6, the users' ranking follows a similar order as the catalog-based method, with only a single model being differently positioned, i.e., a model that takes place five in both rankings. Likewise, for the brand represented by three models highlighted in yellow, the users' ranking aligns precisely with the trust score-based ranking.

6 DISCUSSION

This article extends the developed approach for IIoT data source assessment [13] to the CIoT domain, which results in similar categories in both catalogs. However, the CIoT catalog considers specific CIoT characteristics such as customer orientation, wireless connections, or influence of market standpoint.

The wide variety of CIoT devices makes evaluating data sources for consumer devices a complicated task. There are various products for each type of device, but their settings and software

used change frequently. This fast-paced market makes it difficult to gather an up-to-date and sophisticated knowledge base, and experts for various devices are missing.

The aim was to ascertain the individual properties with maximum precision while maintaining an abstract nature to apply to the diverse range of devices, ensuring comprehensive coverage. Since CIoT data providers are more human-centric, in contrast to the IIoT provider type, a more detailed examination of the nature of human input, e.g., updates and configuration, was made. The general category takes into account the amount of fine-tuning and usability to which those devices can be used. The developed data provider catalog for CIoT serves as a guideline for assessing consumer devices.

Regarding the tool support, the visualization and assisted process allow for basic tool assistance but no advanced options such as weights or trust profiles were implemented. The "ease of use" feedback and successful creation of small example CIoT systems by the participants confirm that a diagramming application can be used to model IoT systems and calculate their predicted data quality. Due to the limited time and resources, we only focused on ease of use and not usability, since the domain experts are required for the latter. Nonetheless, we collected valuable feedback for further improvements.

When we examine the alignment between the scores given by experienced users and the trust score ranking, we find a notable correlation of 0.66. This finding is consistent with the work of Foidl and Federer, who identified a substantial correlation of 0.69 in their assessment of IIoT [13]. These results suggest that device characteristics identified in the catalog play a significant role in predicting data quality. Nonetheless, it is important to acknowledge that there are additional factors that should also be taken into account.

The evaluation of the devices using the approach does not fully match the users' evaluation and there might be several reasons for that. When comparing the users' evaluation of the devices with the CIoT catalog-based evaluation, the latter provides a ranking that is closer to the ranking of experienced users with data knowledge. Such users are more aware of the data issues in their tools. In contrast, the results of the regular users cannot be directly compared, since the regular users might miss data-quality issues due to the low attention to such data or no benchmarks provided.

Another finding is the possible importance of the brand for the users. Smartwatches of prominent brands can be ranked higher due to their reputation and unconscious attitudes. A similar effect of brand familiarity on the users' perception was described by McClure et al. [28]. As the comparison of the rankings showed, one brand was constantly under-ranked, while the devices of another brand were ranked two to three positions higher by users than when the catalog was applied. Thus, using the catalog for the data-quality prediction might enforce a less biased evaluation of the devices.

6.1 Threats to Validity

One of the characteristics specific to CIoT is the large variety of devices and quick development of new devices. Generally, the area of IoT constantly develops and new technologies are being implemented quickly. Thus, it is hard to stay up-to-date in this ever-changing domain, and the complete coverage of the literature is not assured. The second round of literature search focused on the most common sub-areas, "wearable" and "smart home," to control the identified properties and supplement the missing ones.

A potential threat to validity arises from our exclusive reliance on white literature when constructing the catalog to ensure generalizability and credibility, neglecting grey literature sources. This limitation could result in the omission of important device properties not covered in academic research, potentially impacting the comprehensiveness of our catalog. To mitigate this potential

limitation, future research could consider incorporating grey literature sources, industry reports, and non-academic documents into the catalog-building process.

The categories and properties were extracted and synthesized by one researcher. The accuracy and validity of these assessments may be influenced by subjective biases and variations in individual interpretations. To ensure the process, the categories were then iteratively overviewed by two other researchers.

The catalog and tool developed in this study may have limitations in their applicability to all CIoT data sources. However, we tried to cover as many general properties as possible to make the catalog easily adaptable to different types of devices.

The application of the catalog and its comparison to users' assessment was only considering a limited number of smartwatch devices. Further investigations are needed to understand the factors contributing to data quality in CIoT and to enhance the predictive capabilities of the catalog.

6.2 Future Work

Overall, the CIoT device market is wide and does not allow for a precise data provider catalog applying granular grades to each device. The developed catalog could be merged with similar work specific to a particular type of CIoT device, such as that used by Foidl and Felderer [13]. Observing the behavior of different types of devices could develop the weighted scores over time, providing insight into which features are more influential.

"Wearable" and "smart home" device groups were chosen, since they had the most information available in relation to data quality and their device properties during the general search process. However, the CIoT is not limited by devices from these two groups. More work can be done to generalize it to the other categories.

The provided software is a prototype targeted towards the desktop use of the application to achieve the minimum requirements for computing the trust score τ and creating the underlying meta-model. Thus, the focus lies on basic graph options like navigation, basic editing, save and load operations, and processing the given data sources. In future work, mobile application usage, more intuitive UI, performance, and advanced options for power users could be targeted.

7 CONCLUSION

This article presents a catalog for assessing CIoT data providers and a tool to support this process for CIoT and IIoT data sources.

A questionnaire-based catalog was developed to assess CIoT data providers and predict the quality of the produced data. This questionnaire includes device properties that could affect data quality. Those properties were collected through a search across academic and non-academic sources for general focus points of CIoT, followed by two individual in-depth searches using the snowballing approach to search for device properties of "wearable" and "smart home"-related devices.

An extended diagramming application was developed to assist the data source assessment process. The tool allows the user to model an underlying CIoT system as a graph, representing each component as a separate node. The data source assessment for CIoT data sources was integrated into the developed tool. During a usability experiment, ten participants positively evaluated the "ease of use" of the tool.

The proposed approach was applied to model 11 smartwatches. The results were then compared against the user evaluation obtained via a survey. The results do not show a significant correlation between the regular respondents' evaluation and catalog-based evaluation. However, the experienced users ranking shows a correlation of 0.66 with the ranking based on the approach. Moreover, there is a possible influence of brands on the users' evaluation, which might make a catalog-based assessment less prone to marketing-imposed biases.

REFERENCES

[1] Tejasvi Alladi, Vinay Chamola, Biplab Sikdar, and Kim-Kwang Raymond Choo. 2020. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electr. Mag.* 9, 2 (2020), 17–25.

[2] Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, Nabil El Ioini, Mehdi Elahi, and Claus Pahl. 2021. From trustworthy data to trustworthy IoT. *ACM Trans. Cyber-Phys. Syst.* 5, 1 (2021), 1–26. https://doi.org/10.1145/3418686

[3] Sharu Bansal and Dilip Kumar. 2020. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *Int. J. Wireless Info. Netw.* 27 (2020), 340–364.

[4] Elisa Bertino. 2015. Data trustworthiness—Approaches and research challenges. In *Proceedings of the International Workshop on Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri (Eds.). Lecture Notes in Computer Science, Vol. 8872. Springer International Publishing, Cham, 17–25.

[5] Elisa Bertino. 2018. Security and privacy in the IoT. In *Proceedings of the International Conference on Information Security and Cryptology*, Xiaofeng Chen, Dongdai Lin, and Moti Yung (Eds.). Springer International Publishing, Cham, 3–10. https://doi.org/10.1007/978-3-319-75160-3_1

[6] Sebastian Böttcher, Solveig Vieluf, Elisa Bruno, Boney Joseph, Nino Epitashvili, Andrea Biondi, Nicolas Zabler, Martin Glasstetter, Matthias Dümpelmann, Kristof Van Laerhoven et al. 2022. Data quality evaluation in wearable monitoring. *Sci. Rep.* 12, 1 (2022), 21412.

[7] Stefano Canali, Viola Schiaffonati, and Andrea Aliverti. 2022. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLOS Dig. Health* 1, 10 (2022), e0000104.

[8] Bryson Carrier, Brenna Barrios, Brayden D. Jolley, and James W. Navalta. 2020. Validity and reliability of physiological data in applied settings measured by wearable technology: A rapid systematic review. *Technologies* 8, 4 (2020), 70. https://doi.org/10.3390/technologies8040070

[9] Sylvia Cho, Ipek Ensari, Chunhua Weng, Michael G. Kahn, and Karthik Natarajan. 2021. Factors affecting the quality of person-generated wearable device data and associated challenges: Rapid systematic review. *JMIR mHealth uHealth* 9, 3 (2021), e20738. https://doi.org/10.2196/20738

[10] Daniela S. Cruzes and Tore Dyba. 2011. Recommended steps for thematic synthesis in software engineering. In *Proceedings of the International Symposium on Empirical Software Engineering and Measurement*. IEEE, 275–284.

[11] Chenyun Dai, Dan Lin, Elisa Bertino, and Murat Kantarcioglu. 2008. An approach to evaluate data trustworthiness based on data provenance. In *Proceedings of the Conference on Secure Data Management*, Willem Jonker and Milan Petković (Eds.). Lecture Notes in Computer Science, Vol. 5159. Springer, Berlin, 82–98.

[12] Chris Evans. 2018. Internet of Things Challenges in Storage and Data. Retrieved from https://www.computerweekly.com/news/252450705/Internet-of-things-challenges-in-storage-and-data

[13] Harald Foidl and Michael Felderer. 2023. An approach for assessing industrial IoT data sources to determine their data trustworthiness. *Internet Things* 22 (2023), 100735. https://doi.org/10.1016/j.iot.2023.100735

[14] Haitham Ghallab, Hanan Fahmy, and Mona Nasr. 2020. Detection outliers on internet of things using big data technology. *Egypt. Inform. J.* 21, 3 (2020), 131–138. https://doi.org/10.1016/j.eij.2019.12.001

[15] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of things (IoT): A vision, architectural elements, and future directions. *Future Gen. Comput. Syst.* 29, 7 (Sept. 2013), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

[16] Mostafa Haghi, Kerstin Thurow, and Regina Stoll. 2017. Wearable devices in medical internet of things: scientific research and commercially available devices. *Healthcare Inform. Res.* 23, 1 (2017), 4–15.

[17] Sophie Huhn, Miriam Axt, Hanns-Christian Gunga, Martina Anna Maggioni, Stephen Munga, David Obor, Ali Sié, Valentin Boudo, Aditi Bunker, Rainer Sauerborn, Till Bärnighausen, and Sandra Barteit. 2022. The impact of wearable technologies in health research: Scoping review. *JMIR mHealth uHealth* 10, 1 (2022), e34384. https://doi.org/10.2196/34384

[18] i scoop. N/A. What is Consumer Internet of Things (CIoT)? Retrievedfromhttps://www.i-scoop.eu/internet-of-things-iot/what-is-consumer-internet-of-things-ciot/. Accessed on May 22, 2023.

[19] International Organization for Standardization. 2008. ISO 25012:2008—Software engineering—Software product Quality Requirements and Evaluation (SQuaRE)—Data quality model. Retrievedfromhttps://www.iso.org/standard/35736.html ISO Standard 25012:2008.

[20] Aimad Karkouch, Hajar Mousannif, Hassan Al Moatassime, and Thomas Noel. 2016. Data quality in internet of things: A state-of-the-art survey. *J. Netw. Comput. Appl.* 73 (2016), 57–81.

[21] Iqra Khan, Salman Akhtar, and Mohammad Kalim Ahmad Khan. 2021. Lifestyle-based health awareness using digital gadgets and online interactive platforms. *NeuroPharmac* 6, 3 (2021), 295–310. https://doi.org/10.37881/1.638

[22] Dae-Young Kim, Young-Sik Jeong, and Seokhoon Kim. 2017. Data-filtering system to avoid total data distortion in iot networking. *Symmetry* 9, 1 (2017), 16. https://doi.org/10.3390/sym9010016

[23] Asif Ali Laghari, Kaishan Wu, Rashid Ali Laghari, Mureed Ali, and Abdullah Ayub Khan. 2021. A review and state of art of Internet of Things (IoT). *Arch. Comput. Methods Eng.* 29 (2021), 1–19.
[24] In Lee and Kyoochun Lee. 2015. The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons* 58, 4 (July 2015), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008
[25] Caihua Liu, Patrick Nitschke, Susan P. Williams, and Didar Zowghi. 2020. Data quality and the Internet of Things. *Computing* 102, 2 (2020), 573–599.
[26] Lerato Mahloko and Funmi Adebesin. 2020. A systematic literature review of the factors that influence the accuracy of consumer wearable health device data. In *Responsible Design, Implementation and Use of Information and Communication Technology*, Marié Hattingh, Machdel Matthee, Hanlie Smuts, Ilias Pappas, Yogesh K. Dwivedi, and Matti Mäntymäki (Eds.). Springer International Publishing, Cham, 96–107. https://doi.org/10.1007/978-3-030-45002-1_9
[27] Ryan Mattfeld, Elliot Jesch, and Adam Hoover. 2021. Evaluating pedometer algorithms on semi-regular and unstructured gaits. *Sensors* 21, 13 (2021), 4260. https://doi.org/10.3390/s21134260
[28] Samuel M. McClure, Jian Li, Damon Tomlin, Kim S. Cypert, Latané M. Montague, and P Read Montague. 2004. Neural correlates of behavioral preference for culturally familiar drinks. *Neuron* 44, 2 (2004), 379–387.
[29] Jordan Melzer, Jacques Latour, Michael Richardson, Aisha Ali, and Wahab Almuhtadi. 2020. Network approaches to improving consumer IoT security. In *Proceedings of the IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 1–6.
[30] Markus Miettinen, Paul C. van Oorschot, and Ahmad-Reza Sadeghi. 2018. Baseline functionality for security and control of commodity IoT devices and domain-controlled device lifecycle management. *arXiv preprint arXiv:1808.03071* (2018).
[31] Mrs. Nazleeni Haron, Dr. Jafreezal Jaafar, Dr. Izzatdin Abdul Aziz, Mr. Mohd Hilmi Hasan, Dr. Ibrahim Shapiai. 2017. Data trustworthiness in internet of things: A taxonomy and future directions. In *Proceedings of the IEEE Conference on Big Data and Analytics (ICBDA'17)*. IEEE, 25–30. https://doi.org/10.1109/ICBDAA.2017.8284102
[32] Mehar Mutreja, Kunal Khandelwal, Hridya Dham, and Pronika Chawla. 2021. Perception of IOT: Application and challenges. In *Proceedings of the 6th International Conference on Communication and Electronics Systems (ICCES'21)*. IEEE, 597–603.
[33] Farid Naït-Abdesselam and Chafiq Titouna. 2020. Data quality improvements for internet of things using artificial neural networks. In *Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 1–6.
[34] Benjamin W. Nelson, Carissa A. Low, Nicholas Jacobson, Patricia Areán, John Torous, and Nicholas B. Allen. 2020. Guidelines for wrist-worn consumer wearable assessment of heart rate in biobehavioral research. *NPJ Dig. Med.* 3 (2020), 90. https://doi.org/10.1038/s41746-020-0297-4
[35] Aleksandr Ometov, Viktoriia Shubina, Lucie Klus, Justyna Skibińska, Salwa Saafi, Pavel Pascacio, Laura Flueratoru, Darwin Quezada Gaibor, Nadezhda Chukhno, Olga Chukhno, Asad Ali, Asma Channa, Ekaterina Svertoka, Waleed Bin Qaim, Raúl Casanova-Marqués, Sylvia Holcer, Joaquín Torres-Sospedra, Sven Casteleyn, Giuseppe Ruggeri, Giuseppe Araniti, Radim Burget, Jiri Hosek, and Elena Simona Lohan. 2021. A survey on wearable technology: History, state-of-the-art and current challenges. *Comput. Netw.* 193 (2021), 108074. https://doi.org/10.1016/j.comnet.2021.108074
[36] Hafiz ur Rahman, Guojun Wang, Md Zakirul Alam Bhuiyan, and Jianer Chen. 2019. Trustworthy data collection for cyber systems: A taxonomy and future directions. In *Proceedings of the International Conference on Smart City and Informatization (ISCI'19)*. Springer, Singapore, 152–164. https://doi.org/10.1007/978-981-15-1301-5_13
[37] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *J. Clean. Prod.* 140 (2017), 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006
[38] Sana Sabah Sabry, Noor Ahmed Qarabash, and Hadeel S. Obaid. 2019. The road to the internet of things: A survey. In *Proceedings of the 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*. IEEE, 290–296.
[39] Abdus Satter and Nabil Ibtehaz. 2018. A regression based sensor data prediction technique to analyze data trustworthiness in cyber-physical system. *Int. J. Info. Eng. Electr. Bus.* 10, 3 (2018), 15–22. https://doi.org/10.5815/ijieeb.2018.03.03
[40] Samad Sepasgozar, Reyhaneh Karimi, Leila Farahzadi, Farimah Moezzi, Sara Shirowzhan, Sanee M. Ebrahimzadeh, Felix Hui, and Lu Aye. 2020. A systematic content review of artificial intelligence and the internet of things applications in smart home. *Appl. Sci.* 10, 9 (2020), 3074.
[41] Shakir Khan. 2018. Modern internet of things as a challenge for higher education. *Int. J. Comput. Sci. Netw. Secur.* 18 (Dec. 2018), 34. https://doi.org/10.14569/IJACSA.2018.091108
[42] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund. 2018. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Industr. Inform.* 14, 11 (Nov. 2018), 4724–4734. https://doi.org/10.1109/TII.2018.2852491
[43] Yi Sun and Shihui Li. 2021. A systematic review of the research framework and evolution of smart homes based on the internet of things. *Telecommun. Syst.* 77, 3 (2021), 597–623. https://doi.org/10.1007/s11235-021-00787-w

[44] Lu-An Tang, Xiao Yu, Sangkyum Kim, Quanquan Gu, Jiawei Han, Alice Leung, and Thomas La Porta. 2013. Trustworthiness analysis of sensor data in cyber-physical systems. *J. Comput. Syst. Sci.* 79, 3 (2013), 383–401.

[45] Hai Tao, Md Zakirul Alam Bhuiyan, Md Arafatur Rahman, Tian Wang, Jie Wu, Sinan Q. Salih, Yafeng Li, and Thaier Hayajneh. 2020. TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system. *IEEE Trans. Industr. Inform.* 16, 5 (2020), 3311–3321. https://doi.org/10.1109/TII.2019.2950192

[46] Sandip Thite and Devendrasingh Thakore. 2020. A survey on the internet of things: Applications, challenges and opportunities with india perspective. In *Proceedings of the International Conference on Data Science, Machine Learning and Applications (ICDSMLA'19)*. Springer, Singapore, 1263–1272.

[47] Richard Y. Wang and Diane M. Strong. 1996. Beyond accuracy: What data quality means to data consumers. *J. Manage. Info. Syst.* 12, 4 (1996), 5–33. https://doi.org/10.1080/07421222.1996.11518099

[48] Claes Wohlin. 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*. ACM, London, UK, 1–10.

Received 31 May 2023; revised 5 October 2023; accepted 29 November 2023