Mustapää, Tuukka; Autiosalo, Juuso; Nikander, Pekka; Siegel, Joshua E.; Viitala, Raine

Digital Metrology for the Internet of Things

Published in:
GIoTS 2020 - Global Internet of Things Summit, Proceedings

DOI:
10.1109/GIOTS49054.2020.9119603

Published: 17/06/2020

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Published under the following license:
Unspecified

Please cite the original version:
Mustapää, T., Autiosalo, J., Nikander, P., Siegel, J. E., & Viitala, R. (2020). Digital Metrology for the Internet of Things. In *GIoTS 2020 - Global Internet of Things Summit, Proceedings* Article 9119603 IEEE. https://doi.org/10.1109/GIOTS49054.2020.9119603

Digital Metrology for the Internet of Things

Tuukka Mustapää
Dept. of Mechanical Engineering
Aalto University School of Engineering
Espoo, Finland
tuukka.mustapaa@aalto.fi

Juuso Autiosalo
Dept. of Mechanical Engineering
Aalto University School of Engineering
Espoo, Finland
juuso.autiosalo@aalto.fi

Pekka Nikander
Dept. of Communication and Networking
Aalto School of Electrical Engineering
Espoo, Finland
pekka.nikander@aalto.fi

Joshua E. Siegel
Dept. of Computer Science and Engineering
Michigan State University
East Lansing, Michigan
jsiegel@msu.edu

Raine Viitala
Dept. of Mechanical Engineering
Aalto University School of Engineering
Espoo, Finland
raine.viitala@aalto.fi

***Abstract*—Internet of Things (IoT) device data enables diverse applications. However, the quality of data are non-standardized and difficult to quantify. While poor quality data may be usable, establishing error bounds supports IoT's use in critical applications. National Metrology Institutes (NMIs) have long tradition in making measurement data trustworthy, and they are now working to digitalize these practices. This paper forwards that agenda by presenting a Distributed Ledger Technology (DLT) based concept to leverage digital metrology for IoT data and devices. Digital Calibration Certificates (DCCs) offer a solution for describing, certifying, authenticating, and securing IoT data quality. With DCCs, measurement device (sensor) calibration information may be included as metadata alongside samples captured by a device. Metadata may include device identification, which serves as proof-of-origin for measurements and samples, and timing data, to ensure its "freshness." DCCs enhance communicating the quality of captured information among devices, services, and applications, thereby supporting IoT's use in domains with strict error constraints. Our proposed concept securely validates DCC-based (meta)data traceability chain from NMIs and devices to data end-users with cryptographic measures, rendering IoT data trustworthy for critical applications.**

***Index Terms*—IoT, metrology, digital calibration certificate, security, Digital Twin**

I. Introduction

Internet of Things (IoT) device sensors produce abundant data, with falling costs allowing device distribution across increasingly diverse environments and contexts. However, while data volume has increased, its veracity has not. Data captured by IoT devices is not inherently trustworthy and therefore may not support critical applications. Improved knowledge of system or sample metadata, coupled with device- and application-specific optimized sampling, could improve system performance and data usability. Solutions drawn from the field of (analog) metrology serve as a jumping-off point for ensuring high quality measurements and effective communication of data quality so that critical applications may rely on the IoT.

This work was supported by EURAMET under Grant 17IND02 "SmartCom" and Business Finland under Grant 8205/31/2017 "DigiTwin."

As industrial digitalization takes hold, metrology and its related discipline of calibration have adopted such technologies slowly. For example, datasheets for measurement quality or calibration details are captured on paper [1]. The slow adoption of digital technologies in metrology may stem from its tradition of providing standards and measurement services that underpin critical elements of society, the responsibility for which makes change a slow and deliberate process to avoid "breaking" essential capabilities responsible for financial livelihood or even health and wellness.

The systems used by the National Metrology Institutes NMI may also lack the tools or support required for digital cryptography to reliably authenticate the origin and secure the integrity of electronic documents such as calibration certificates. However, creating and distributing strongly-secured electronic documents is an established practice with the potential to meet or exceed the security of paper documents. Perhaps soon, NMIs will provide secure and traceable Digital Calibration Certificates (DCCs) [1].

The capabilities enabled by digital metrology have the potential to enhance opportunities for data reuse and improve businesses by creating new opportunities for product or service creation and uses for trustworthy data. They enable new development directions such as instant traceability from measurement to sampling conditions through to global measurement standards, or the creation of high-quality, certified data markets.

Benefits of introducing digital metrology for IoT measurements include:

- Knowledge about the uncertainties of measurement devices and their measurement results is increased
- Quality metrics of data are quantified as metadata
- Traceability of data quality through certification of origin, integrity, and metrological quality of measurement data
- Market value of data is heightened thanks to the aforementioned reasons
- Cost savings in cases where calibration is a legal obligation, enabled by automatic data processing

Further application-specific benefits are enabled by these characteristics, for example optimizing production processes with higher quality sensor data, and improving calibration processes through in-situ calibration or computational models [2]. Digital metrology practices can even help prevent data frauds [3] and container ship capsizing [4].

Downsides of digital metrology may include the introduction of systemic errors stemming from reduced human supervision, possible privacy erosion, and increased costs of implementation (initially).

Countermeasures include artificially-intelligent supervisors [5] privacy-preserving, decentralized identifiers [6] and storing cryptographic fingerprints rather than raw data.

In this paper, we propose a digital validation system that enables efficient measurement and device calibration practices brings quantified measurement quality metrics from metrology to IoT data. The system relies on two novel metrology solutions, Digital Calibration Certificates (DCC) and Digital System of Units (D-SI), and various digital security technologies with the main focus on Distributed Ledger Technologies (DLT). The concept is presented for a system comprising a single measurement device in Figure 1.

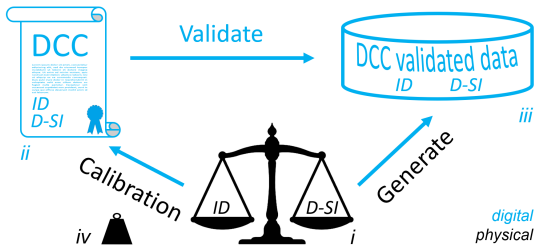

Fig. 1. Calibration information of a measurement device *i* is stored in a DCC *ii* which validates the data *iii* generated by the device. The calibration is performed using an artefact *iv* (or device) that has higher metrological properties than the calibrated device. Device identifier (ID) is used in all three components *i-iii* and data is stored in D-SI format.

The paper is organised as follows: Section II provides the relevant background for the proposed concept described in Section III. Potential use cases in regulated production calibration and container ship stowage are presented in Section IV and challenges and opportunities are discussed in Section V. Section VI concludes the paper.

II. Background

Our proposed innovation draws upon concepts from metrology and the Internet of Things, including Digital Twins, which provide a compelling use-case for digital metrology in cyberphysical systems. Metrology ensures many safety critical operations, rendering data origin and integrity as essential components for our solution.

A. Metrology

Metrology is the scientific study of measurement. In engineering, metrology provides a framework for establishing the quality of measurement data used in decision making. This framework is supported by the global cooperation of NMIs, each of which maintains traceable national measurement standards (e.g. SI units), physical constants, and standards (e.g. those by ISO).

The comparability of measurement data provided by different instruments requires that data are traceable to the same measurement standard of the specific physical quantity. In metrology, traceability is defined as the property of a measurement result whereby the result can be related to a reference through a documented unbroken chain of calibrations, each contributing to the measurement uncertainty [7].

Scheduled calibration is required for verifying that measurement instruments function within the allowed margin for uncertainty, as aging and wear can cause negative effects on the instruments.

Calibration regulations demand that the calibrations of individual instruments must be documented with calibration certificates. The requirements for calibration intervals and limits of acceptable measurement uncertainties vary based on the laws and regulations in different countries and industries. Currently, calibration certificates are paper documents or PDF files that include the information specified in the relevant standards e.g. ISO 17025 or other industry specific standards.

The global acceptance of calibration certificates is based on mutual agreements such as the International Committee of Weights and Measures' (CIPM) Mutual Recognition Agreement (MRA). In addition to NMIs, there are accredited calibration laboratories that provide standardized calibration services.

To better-meet the needs of calibrators, standards bodies, and data consumers, there is an opportunity to modernize these certificates to improve their utility.

B. IoT Applications

In industrial applications, measurement devices are often uncalibrated. For those requiring calibration, devices may be calibrated on site to reduce costs and limit calibration-related stoppages. However, loosely-controlled environments compromise the achievable calibration result. Multiple sensors may be used for process monitoring to improve measurement fidelity through data filtering and sensor fusion, though cost constraints mean the sensors used may be of poor quality.

C. Digital Twins

"Digital Twin" is a term for the virtual counterpart of a physical product such as an IoT device. The term was featured in a Nature comment [8], and a Scopus search on 7th February, 2020 for "Digital Twin" shows an increase from two results in 2014 to 819 in 2019. The underlying concept has been around longer [9].

Many terms of art have been introduced for Digital Twins and related concepts [10]–[12]. Though the concept of remotely-mirroring a system is constant, these terms are not interchangeable. For example, a Data Proxy is a Digital Twin based on estimated data designed to conserve system resources and improve security while respecting application demands, whereas a conventional Digital Twin mirrors data as faithfully

as possible [12], [13]. For the sake of simplicity, we refer to Digital Twins in this paper, but the concepts introduced apply to related mirroring approaches.

Metrology practitioners have proposed Digital Twins for calibrated measurement instruments that act as central communication elements to other parties [14] and include a DCC and other metrology data [1]. Metrology enhanced twins can increase production quality by combining their calibrated data with physics based simulation [1].

Digital Twins will increasingly become a crucial part of IoT implementations. Twins will handle all information flow between remote computing environments and devices, and among devices themselves [9], [12], allowing comprehensive device optimization. e.g. to enhance battery life and/or data fidelity. Imbuing twins with measurement quality information (via a standardized DCC or otherwise) will increase their utility by supporting diverse and potentially-critical future applications.

D. Data origin and integrity

The Internet is not a safe place when data quality is concerned. Tampering, data modification, and alteration are omnipresent risks. Today, data origin and integrity are typically validated through the association of a data source by signing a cryptographic key [15].

For devices, one recommended practice [16] has been to associate a cryptographic identifier with the device itself and it is increasingly common practice to use the public key as an identifier for the key holder. That is, instead of using a human readable name, such as *Device 123 at floor 4 of building 5*, the public key (or a digital fingerprint thereof) is used directly.

However, public keys are time-invariant, so an external party able to view data over time could potentially de-anonymize the source, creating a privacy problem. If an outsider finds out the identity of one data provider, this outsider may de-anonymize all past, present, and future data with the same public key. .

This has recently been addressed with decentralised identifiers (DIDs) [6], which allow the data source to change their externally-visible identifier over time while allowing intended recipients to reconstruct a full datastream.

At the same time, a digital signature alone does not prove *when* a piece of data was signed, despite the importance of data and calibration "freshness." To address this issue, Distributed Ledger Technologies (DLTs) [17] have been applied. A DLT can have *public*, *consortium*, or *private* implementations. Distributed ledgers (DLT implementations) can also be interconnected with interledger solutions [18], allowing the creation of additional middleware ledgers that provide faster update cycles with lower confidence. These solutions support non-critical, mid-latency applications, as "slow" ledgers with high confidence provide a root of trust, whereas lower confidence may have to be accepted for temporally critical applications.

A low-hanging fruit of enhancing measurement security with DLTs is to leverage them for keeping global, trustworthy, shared lab notebooks. Anything written to the notebook stays there forever, as the database is append-only. For privacy and security reasons, one may not want to write measurements directly to a DLT, but share instead signed fingerprints of data, storing the results in a time series database. These systems jointly enable verification of when and with what device a measurement was captured, along with the recorded value(s).

In other cases, it may be beneficial to use multiple ledgers simultaneously, e.g. unique notebooks for different labs or for triggering actions on specific events, such as when a measured value drifts outside its allowed ranges [18].

III. Proposed concept

Our concept combines ongoing development of DCCs, Digital System of Units (D-SI), device identities, DLTs, and IoT devices to meet this underaddressed need. The concept is presented in Fig. 3 and III-F.

A. Digital Calibration Certificates (DCC)

Digital Calibration Certificates were originally presented by PTB [1]. They proposed an XML structure designed to support existing standards and meet recommendations for presenting metrological data. A DCC can be used to present administrative data and measurement results from a machine's current calibration certificates in a computer-readable format secured by a digital signature or issuer's seal. The concept is being further developed in EMPIR project "SmartCom," funded by the EU Horizon 2020 programme.

XML was selected as the initial format for DCCs, though these could be implemented in formats offering lower overhead and improved human-readability, such as JSON.

In our concept, a DCC conveys the measurement uncertainty of an IoT device and provides a reference to its verified traceability chain. A link to the DCC can be included in a measurement's metadata. DCCs form a backbone rooted at the NMIs enabling the development of system-level digital metrology for IoT.

B. Digital System of Units (D-SI)

To present measurement data in the calibration certificates in a machine-readable format, a new XML format was developed as a part of the SmartCom project: a Digital System of Units (D-SI) [19]. Relevant information includes numerical values for measurement results, units related to the values, and measurement uncertainties including both the value of the uncertainty and its distribution. The D-SI data model is presented in Fig. 2. D-SI is further developed in "CIPM Task Group on the Digital SI" [20].

C. Secure digital device identities

Secure digital traceability of a measurement, from NMI to an end user, can only be guaranteed if a calibrated device can be securely linked to the DCC. To fulfill this need, our proposed solution leverages secure digital device identities. IEEE 802.1AR-2018 [16] defines a secure device identifier cryptographically-bound to a device and supporting authentication of the device's identity. Each identifier consists of an X.509 key certificate that identifies the subject device and a corresponding private key securely embedded in the device.

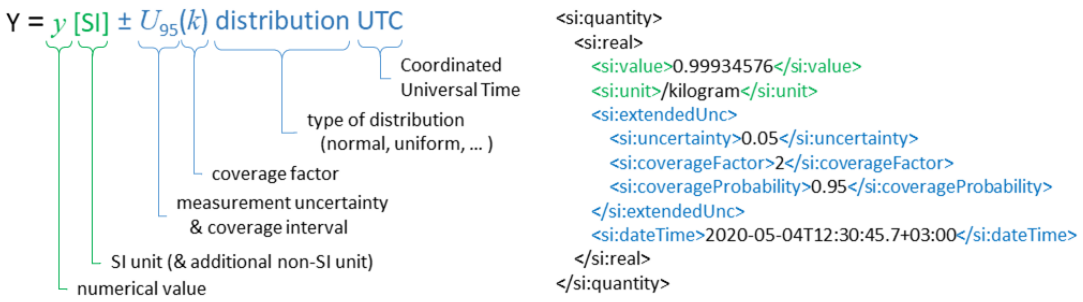

Fig. 2. The D-SI data model (left) and sample data (right). The data model covers requisite information to ensure the correct presentation of both metrological information (green) and metadata (blue)

We propose initially using 802.1AR device identifiers and including such an identifier in the DCC (the location of the secure device identification information could vary based on application requirements). Once W^{3}C has standardized Decentralized Identifiers (DID), these may be used in addition to the 802.1AR identifiers [21].

D. DLT-validated DCC

The integrity of a DCC must be validated to maximize its utility to a data consumer or viewer. Validation can be implemented with a system accessible by a limited group of stakeholders or one with public access. In either case, the use of a DLT may increase the solution's feasibility.

We propose using a consortium ledger whose administration stakes are divided between NMIs and that can be used by anyone for validating a DCC worldwide. We will first build a DCC-validating consortium ledger administrated by NMIs and work gradually towards a worldwide solution. NMIs represent a natural calibration authority suitable for supporting DCC validation ledgers.

The DLT can store DCCs and DCC-validated data, or as a more efficient and privacy preserving solution, only their cryptographic fingerprints.

E. DCC-enabled IoT device

IoT data are currently underutilized, in part because it is difficult to establish their provenance. The lack of reliable information about data origin, accuracy, and timestamping stifles the growth of data marketplaces.We propose including the DCC and accompanying quantified data quality metadata to improve data portability and (re)usability.

Provenance metadata, including timing information and device identification, describe the data from a specific measurement device in detail and therefore support their use in applications where input quality may matter (e.g. critical applications such as healthcare, utilities, manufacturing, automated driving, etc).

F. Overall solution

The proposed solution is depicted in Figure 3. The DCCs of a calibration chain from NMI to measurement instrument are stored in the DCC-DLT cloud, with multiple DLTs connected by interledger solutions.

The DCC of a measurement device can be used to verify the quality of a measurement result, creating a DCC-validated data marketplace. The end user can (re)certify their purchased data with the DCC-DLT cloud. The DCC-validated data also includes metrology-based quality of data metrics that describe the measurement uncertainty of the data and potentially other metadata.

Normally, the DCC-DLT cloud acts as a passive element storing and validating DCCs and data. When past calibration activity must be revoked, the cloud can send notifications to users of data and devices in the DCCs affected calibration chains of the DCCs withdrawal, and the calibration withdrawal appended to the end of the chain.

IV. Use cases

We now demonstrate representative use cases of digital metrology for regulated production calibration and container ship stowage.

A. Regulated production calibration

Today's consumer products involve complex subcontracting networks, with global materials and components used in assembly. Ensuring the quality and compatibility of the components requires components to meet tolerances set in the design specification. It is essential that the quality-related measurements from the entire supply chain network are comparable and traceable to equivalent measurement standards.

Data integrity plays a role in industries with strictly-regulated quality management. The pharmaceutical industry is one such an example. In order to access certain markets, pharmaceutical companies must have their manufacturing processes audited by regulators. To ensure that measurement instruments used for controlling production processes meet specified tolerances, they must be calibrated regularly. The calibrations are often carried out in the production environment by accredited external calibrators, who provide the calibration certificates to the facility owner. The information on paper-based certificates has to be manually imported to data management systems. Additionally, original documents must be

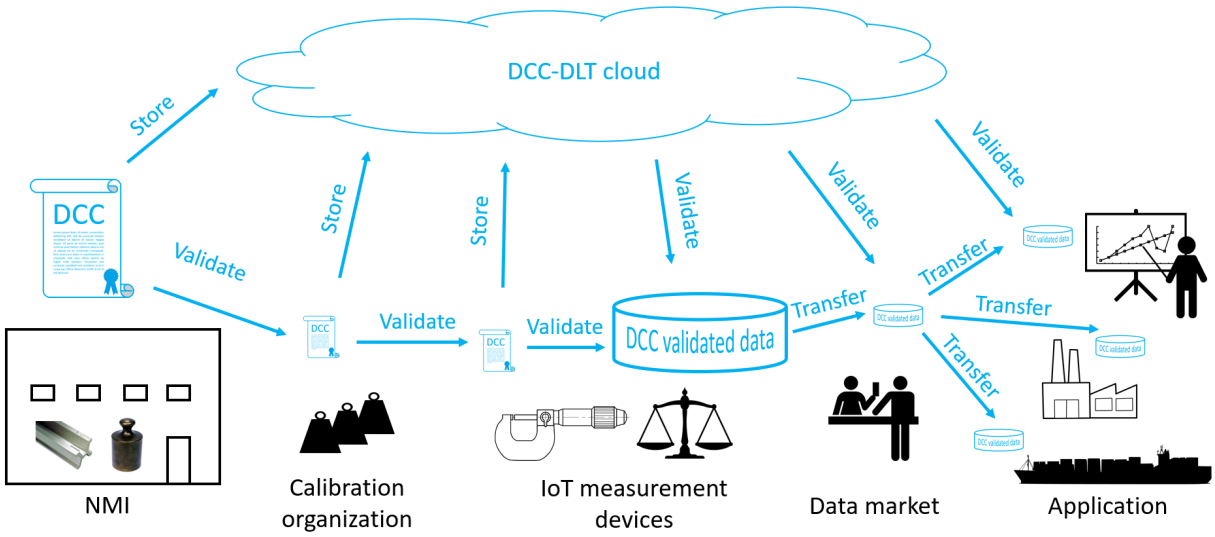

Fig. 3. The proposed solution for DCCs and data provenance sharing. DCC of an NMI provides the root of measurement trust for calibration organization(s) and further to IoT measurement devices. Devices generate DCC validated data which is transferred to end-user, potentially via a data market. DCC-DLT cloud is a combination of DLT and traditional trusted cloud solutions that provides storage and integrity across the traceability system, namely storing DCCs and validating measurement data.

filed and preserved in a space that is safe in emergencies. The human resource needs for calibration and calibration data management are high due to the amount of equipment in complex manufacturing environments.

If assembly components are not compliant and the traceability of the supply chain is lacking readable documentation, analysing and correcting the problem is challenging. With comprehensive digital documentation, finding problems can be unambiguous and more efficient.

B. Container ship stowage

Millions of tons of goods are transported daily via containers loaded and unloaded in harbours. The SOLAS convention, which regulates the minimum safety standards related to the construction, equipment and operation of merchant ships, requires that the weight of the containers must be shared with carriers. Weights may be determined weighing the container before it is loaded onto the ship, or if the exact weights of the container and cargo are known, it may be declared [22]. Knowing the weights of individual containers is essential for optimizing the ship's weight distribution and stability. In the worst case, an unevenly-loaded ship may capsize due to inaccurate container weight declarations [4].

Current cargo weighing systems, which are integrated into the cranes used in harbours, do not include uncertainty or identification metadata. Adding this functionality would allow better analysis of the weight distributions for stowage plans improving safety, stability, and efficiency.

Additionally, cryptographic methods and DLTs could be used to help improve the security of the transportation as content modification could be noticed through changes in the weight of the containers loaded or unloaded to or from a ship. Fingerprints of the information of individual containers could be stored in distributed ledgers to prevent forging these data.

V. Discussion

We discuss the proposed concept from the viewpoints of challenges and opportunities.

A. Challenges

Metrologically, the transition from current practices to a digitized solution is a significant challenge. The standardization of a new calibration data format will be slow, requiring global consensus and mutual agreements before DCCs reach full potential.

In addition to DCC and D-SI formats, additional standards for metadata are needed to support and further improve the applicability of the digital metrology infrastructure across application areas.

As an alternative to a DLT-based DCC cloud, the cloud can be implemented with more traditional technologies that are not based on DLT solutions. With a non-DLT DCC cloud, a solution comparable to the traditional electronic banking systems must be implemented, i.e. it will need a single central authority that is able to manipulate all contents of the cloud. Such a central authority would become an attractive target for malicious actors. A successful attack could bring down the whole calibration system. A DLT-based DCC cloud would require more effort to compromise, and is therefore the preferred embodiment.

B. Opportunities

With the global adoption of our proposed concept, future data will be more usable across industries as DCCs enhance trust in the accuracy, precision, and timeliness of measurement data. Today, unless we control a system end-to-end (we produce the hardware, software, and installation) we assume low confidence irrespective of the system embodiment because we can't afford to make important decisions on poor-quality

data. Improved certification means we can create applications for critical domains that trust data generated by specific types and configurations of sensors.

Machine learning is particularly dependent on data quality. Although machine learning can effectively process data e.g. for filtering inaccurate measurements or timestamps, some systematic errors are caused by the aging of the measurement devices might end up going unnoticed.

Introducing metrology to IoT measurements increases the usability of the data for targeted applications and external parties. Trusted data will also be an enabler of a data economy where marketplaces can guarantee the quality of data sold. Consequently, the overall flow of trustworthy information will be increased, benefiting all stakeholders.

Modern organizations rely on data to make informed decisions. Trustworthy IoT sensor data provides a deeper insight of operations, enabling management to do more accurate decisions. Therefore, introducing metrology-based data quality metrics to IoT sensors can provide broader societal impact.

Additional efforts are required to enable the opportunities. These include e.g. validating the DCC in real use cases, establishing the system for storing and distributing DCCs, and securing the physical to digital traceability chain, potentially with Digital Twins.

VI. Conclusion

This paper presented a conceptual mission-statement to bring metrology practices to IIoT sensors. The proposed DLT-based DCC cloud facilitates metrologically-validated data at a scale infeasible with current solutions, but suitable for IoT's growing reach. The cloud allows instant and worldwide validity checks of DCCs and DCC-validated data, and implications of the implementation of such a solution will increase the impact of the IoT. For example, an increase overall trust in IoT measurement data may enable *trustworthy* data markets, or the use of information in novel, mission-critical applications.

Bringing digital metrology to IoT contributes to a range of industries and applications by allowing the use of trustworthy, accurate, precise, and appropriately timestamped measurements. Implications range from communicating standardized metrics across industries worldwide, to enabling B2B and B2C IoT data markets with quantified error metrics. In regulated environments, DCCs reduce costs and increase data integrity through automatized calibration information processing. The applications of such information may have impact ranging from lower cost of manufacturing, to higher production quality, to more stable cargo carrier ships on the sea and beyond. In essence, adding validation metadata to IoT-sourced information allows for the first time the appropriate use of data originating from mega-scale distributed sensing systems in applications for which outcomes are critical.

Our proposed solution provides one means of validating metrological data for IoT devices, and the concepts are applicable outside of manufacturing and industrial applications. DCCs have the potential to change how we see the data generated by the IoT, leading to cross-industry revolution.

References

[1] S. Hackel, F. Härtig, J. Hornig, and T. Wiedenhöfer, "The digital calibration certificate," vol. 127, no. 4, pp. 75–81. [Online]. Available: https://www.ptb.de/cms/de/presseaktuelles/zeitschriften-magazine/ptb-mitteilungen/verzeichnis-der-ptb-mitteilungen/ptb-mitteilungen-2017/heft-4-metrologie-fuer-die-digitalisierung-von-wirtschaft-und-gesellschaft.html

[2] J. M. Barcelo-Ordinas, M. Doudou, J. Garcia-Vidal, and N. Badache, "Self-calibration methods for uncontrolled environments in sensor networks: A reference survey," vol. 88, pp. 142–159. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870518306115

[3] Y. Obayashi, "Kobe steel admits data fraud went on nearly five decades, CEO to quit." [Online]. Available: https://www.reuters.com/article/us-kobe-steel-scandal-ceo-idUSKBN1GH2SM

[4] Standing Commission for Maritime Accident and Incident Investigations, Technical report a-20/2012 Investigation of the capsizing of merchant vessel DENEB at the Port Algeciras on June 2011. [Online]. Available: https://www.mitma.gob.es/recursos_mfom/ita202012denebingoptimizadoweb.pdf

[5] J. Siegel and S. Sarma, "A cognitive protection system for the internet of things," vol. 17, no. 3, pp. 40–48.

[6] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," vol. 30, pp. 80–86. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574013718301217

[7] JCGM 200:2012, International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM), 3rd edition. [Online]. Available: https://www.bipm.org/utils/common/documents/jcgm/JCGM_200_2012.pdf

[8] F. Tao and Q. Qi, "Make more digital twins," vol. 573, no. 7775, pp. 490–491, number: 7775 Publisher: Nature Publishing Group. [Online]. Available: https://www.nature.com/articles/d41586-019-02849-1

[9] J. Autiosalo, J. Vepsäläinen, R. Viitala, and K. Tammi, "A feature-based framework for structuring industrial digital twins," vol. 8, pp. 1193–1208.

[10] J. Autiosalo, "Platform for industrial internet and digital twin focused education, research, and innovation: Ilmatar the overhead crane," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 241–244.

[11] M. Langheinrich, F. Mattern, K. Rmer, and H. Vogt, "First steps towards an event-based infrastructure for smart things," p. 34.

[12] J. E. Siegel, S. Kumar, and S. E. Sarma, "The future internet of things: Secure, efficient, and model-based," vol. 5, no. 4, pp. 2386–2398.

[13] J. E. Siegel, "Data proxies, the cognitive layer, and application locality: enablers of cloud-connected vehicles and next-generation internet of things," Ph.D. dissertation, Massachusetts Institute of Technology, 2016.

[14] F. Thiel, "Digital transformation of legal metrology - the european metrology cloud," vol. LIX, no. 1, p. 12.

[15] W. Diffie, "The first ten years of public-key cryptography," vol. 76, no. 5, pp. 560–577, conference Name: Proceedings of the IEEE.

[16] "IEEE std 802.1ar-2018: Secure device identity." [Online]. Available: https://1.ieee802.org/security/802-1ar/

[17] H. Natarajan, S. Krause, and H. Gradstein, *Distributed ledger technology and blockchain*. World Bank.

[18] P. Nikander, J. Autiosalo, and S. Paavolainen, "Interledger for the industrial internet of things," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, vol. 1, pp. 908–915, ISSN: 1935-4576.

[19] D. Hutzschenreuter, F. Härtig, W. Heeren, T. Wiedenhöfer, A. Forbes, C. Brown, I. Smith, S. Rhodes, I. Linkeová, J. Sýkora, V. Zelený, B. Ačko, R. Klobučar, P. Nikander, T. Elo, T. Mustapää, P. Kuosmanen, O. Maennel, K. Hovhannisyan, B. Müller, L. Heindorf, and V. Paciello, "SmartCom digital system of units (d-SI) guide for the use of the metadata-format used in metrology for the easy-to-use, safe, harmonised and unambiguous digital transfer of metrological data." [Online]. Available: https://zenodo.org/record/3522631#.XlThh1BS9hE

[20] CIPM Task Group on the Digital SI. [Online]. Available: https://www.bipm.org/en/committees/cc/wg/cipm-tgdsi.html

[21] W3C DID Working Group. [Online]. Available: https://www.w3.org/2019/did-wg/

[22] International Maritime Oraganization, Verification of the gross mass of a packed container. [Online]. Available: http://www.imo.org/en/OurWork/Safety/Cargoes/Containers/Pages/Verification-of-the-gross-mass.aspx