The New Era of Metrology and Its Role in Information Technology: A Survey

Reham A. Abouhogail

Electrical Quantities Metrology Lab., National Institute of Standards (NIS), Egypt.
Corresponding author's email: reham.abdellatif@nis.sci.eg

Article Type: Review article
Received: 22/11/2023 **Accepted: 8/3/2024**

Abstract

Since the second half of the 20th century, in practically every sector of the economy, Information Technology (IT) has been a significant agent of change. National Metrology Institutes (NMIs) have a long history of ensuring the accuracy of measurement data, and they are currently attempting with IT capabilities by digitizing these processes. This study contributes to that goal by discussing some new fields in IT that contributes to developing the new metrology world. This study reviews IT capabilities and activities in measurement and testing, as well as identifies key terminology and concepts in IT metrology. Then, we conclude what is expected to happen in the field of metrology over the next 10 years according to the impact of IT. On the other side, you will find in this research the role of metrology in developing IT. The NMIs and the scientific measurement community have faced particular technological hurdles in building a solid measuring and testing infrastructure for IT due to the complexity and continuously changing nature of IT. This infrastructure for measuring and testing essential non-physical and non-chemical features associated with sophisticated IT systems is still in its infancy. Therefore, in this paper, the current challenges to developing IT system-based metrology concepts have been discussed.

Keywords: IT Metrology, Digital transformation, Digital System of Units, Digital Calibration Certificate, Smart Metrology.

1 Introduction

This survey is concerned with reviewing the interaction between metrology and information technology. In order to present this effect, we had to start with an introduction to each science clarifying the essential concepts. We can start to introduce metrology main concepts and main concepts in IT as follow.

1.1 Metrology

Metrology is the science of measurement where all aspects of the measurement process are related to it [1]. In engineering, metrology is responsible for a framework for creating the quality of measurement information used in decision making [2]. Every country should establish its own national metrology institute (NMI) to set its own standards. It should also create new standards and techniques to ensure that measurements are traceable to international primary standards. In Paris, The International Bureau of Weights and Measures (BIPM) organizes the development of worldwide standards. After that, these standards are tracked back to national standards until they reach the functioning standards. The establishment of accurate measurements through the definition of units and the creation of standards is the foundation of technological advancement. The value that was measured must be combined with the correct unit of measurement. Since its establishment in 1960 and recommendation at the 11th meeting of the General Conference on Weights and Measures (CGPM), the International System of Units (SI) has become the favorite system of units in the domains of research, technology, industry, and international trade. In the SI system, there are seven main units. All derived units of various quantities that can be computed from mathematical equations deduced from physical laws or regulations are derived from this unit [3]. The SI's base units are depicted in Fig. 1. The Meter Convention which is an international agreement selected the SI as its measurement system. Since its inception in 1960, it has served as the standard for measurement in research, technology, industry, and trade [3]. The development of new metrology tools can be difficult in some circumstances, such as when studying the lifetime and proficiency of batteries and solar cells with photovoltaic, where the characteristics are unknown. Others contain the development and implementation of trustworthy indicators that customers may use to recognize a product's environmental influence during both its manufacturing phases and its use [3].

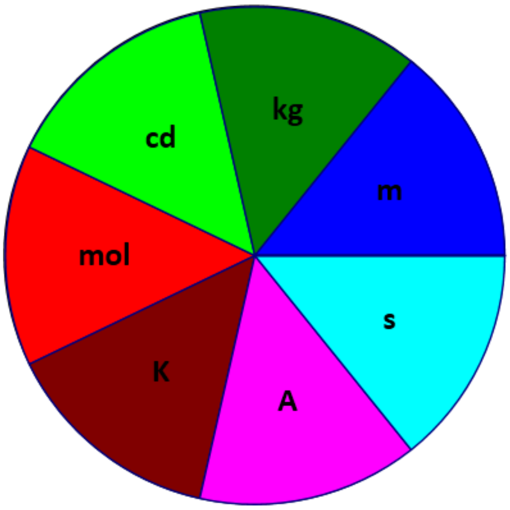

Figure 1: The SI units, redrawn from [3].

1.2 Information Technology (IT)

The development, maintenance, and application of computer software, systems, and networks is referred to as information technology. It also involves their application in data processing and distribution. Information, facts, statistics, and other items acquired for reference, storage, or analysis are referred to as data [4]. Information technology has the potential to transform everything. Information technology advancements have opened up a whole new world of possibilities. The metrology industry has the potential to be transformed by IT. The shifts could be significant, requiring totally new methods to measuring and calibration services. The performance and efficacy of equipment and operations will be improved through on-line Measurement and remote calibration testing, repair, diagnostics, and maintenance. They'll make measuring knowledge available when and when it's required. In order to bridge the gap between IT and Metrology operations, we have to move forward to the digital transformation journey. When we speak about digital transformation, we listen two different words digitization and digitalization. Two letters make all the difference when it comes to digitization and digitalization. This isn't just a question of wordplay; this one is also a question of scale and prospective value to your company. Understanding the differences among these two methods is becoming increasingly important as the digital transformation gathers traction and firms turn to digital solutions to improve visibility and reduce inefficiencies.

The difference between Digitization and Digitalization is as shown in Table 1 and as follows [5]:

Analog-to-digital conversion of current information and documents is referred to as digitization. Consider scanning a photograph or creating a PDF from a paper report. The data is just encoded in a digital format rather than being modified. When digital data is used to automate processes and improve accessibility, it can save time and money; nevertheless, digitization does not strive to optimize processes or data. The use of digital technology to modify a business model and generate new income and value to produce opportunities is considered the process of shifting to a digital business. Beyond digitization, digitalization entails using digital information technology to completely overhaul a company's processes, including reviewing, reengineering, and reinventing how you do your business. Digitalization is a transformation of information and procedures, whereas digitization is a conversion of data and processes. Digitalization encompasses the capability of digital technology to gather information, develop trends, and create smarter business judgements, rather than simply digitizing current data. A paper would be digitized, but a factory would be digitalized, as SAP News points out. You would digitize a report in terms of reporting, but your organization's data collection method and workflows would be digitalized.

Table 1: *The difference between Digitization and Digitalization.*

	Digitization	**Digitalization**
Definitions	Converting analogue data documents and procedures to digital.	Using digital technologies to transform corporate operations, resulting in prospects for enhanced efficiency and revenue.
Examples	Creating a digital file by scanning an image. Creating a digital file, such as a PDF, from a paper report. Using a digital checklist software like Apple Reminders to convert an existing paper checklist. Turning actual sound into a digital file by recording a presentation or a phone call.	Finding new revenue sources by analyzing data collected by internet-connected gadgets. Using digital technology to revolutionize your reporting processes, gathering and analyzing data in real time, and leveraging insights to reduce risk and increase efficiency on future projects. Ex: Anyone can accomplish this by advising farmers and assisting them in maximizing crop yields using the collected data.

1.3 Automation in Metrology

Our main goal for using IT in metrology is to automate the metrology services and operations. But, the obstacle that stands in front of this process and other processes which are related to digital transformation is that metrology is controlled with standards and regulations which guarantee the quality of the presented services to different fields as health and international trade [2]. To start building an automated metrology system, we have to answer the three following questions.

1. What are the fundamentals of automation?

This question includes: what do you have the ability to automate? and what role does automation play in this?

2. How to create an NMI-wide automation strategy?

We can conclude the answer for this question in three steps: evaluation, planning, and adaptability.

3. How to put your automation approach into action?

Also, the answer to this question can be summarized by three steps: begin small, demonstrate value, and gradually develop.

In the next Section, we will introduce the influencing IT factors which contributes in the new generation of metrology as Cybersecurity, Blockchain, Artificial Intelligence (AI), Internet of Things (IoT), analysis of Big Data, and other essential aspects of the digital transformation. Then, in Section 3, we will speak about what is expected in the next generation metrology. Section 4 introduces the Metrology's role in IT. Finally, the paper is concluded in Section 5.

2 The Influencing IT Factors

Globally, researchers and industry experts are examining a range of digital technologies, including blockchain, cloud computing, artificial intelligence, Internet of Things (IoT), big data analytics, and more, to offer metrology solutions that lead to automated and paperless systems with improved customer support [6]. So, this section presents an analysis of the impact of IT on metrology by introducing the different influencing IT factors

2.1 Information Security

The processes and techniques devised and deployed to secure critical company information against modification, disruption, destruction, and examination are referred to as information security, or InfoSec. It exclusively pertains to data security processes Information Security Management System (ISMS) [7].

Information Security Types [7]:

2.1.1 Security Applications

Security applications are considered a wide topic that includes software flaws in personal computers and mobile apps, as well as application programming interfaces (APIs). These weaknesses are identified in user authentication, code and configuration integrity, and well-developed rules and processes. Application flaws can serve as entrance points for large-scale data cracks. For Information Security, Application security is an essential part of boundary protection for Information Security.

2.1.2 Cloud security

Security for the cloud is concerned with the development and hosting of safe applications in cloud environments, as well as the secure usage of third-party cloud apps. The term "cloud" simply refers to a program that runs in a shared environment. In shared settings, businesses must ensure that separate operations are adequately isolated from one another.

2.1.3 Cryptography

Data confidentiality and integrity are improved by encrypting data in transit and at rest. In cryptography, digital signatures are often used to verify the validity of data. The importance of cryptography and encryption is growing. The Advanced Encryption Standard (AES) is a fantastic illustration of cryptography in action. The AES algorithm is a symmetric key method that is used to protect secret government data.

2.1.4 Infrastructure protection

It is for the internal and extranet networks, data centres, labs, mobile devices, servers and workstations, and are all protected by infrastructure protection.

2.1.5 Incident response

The function of incident response is to keep an eye out for and investigate possibly malicious conduct. IT workers should have an incident response plan in place to control the danger and restore the network in the event of a breach. The plan should also include a procedure for preserving evidence for forensic analysis and possible prosecution. This information can be used to avoid future breaches and assist employees in identifying the perpetrator.

2.1.6 Management of vulnerabilities

The technique of analysing an environment for fragile areas and ordering remediation based on danger is known as vulnerability management. Businesses are continually adding apps, users, infrastructure, and other features to various networks. As a result, it is critical to scan the network for probable vulnerabilities on a regular basis. Finding a vulnerability ahead of time can spare your company from the devastating implications of a data breach. When it comes to data quality, the Internet is not a harmless region. Data tampering, manipulation, and modification are all possibilities. Integrity and confidentiality are commonly certified today by associating a data source with the signature of a cryptographic key. One recommended practice [8] for devices is to attach a cryptographic identify with the device, and it is becoming gradually customary to utilize the public key as the identifier. Instead of using a name that can be readable by human, such as Device 12 on floor 2 of building 3, the public key (or a digital signature) can be used. However, because public keys don’t change with time, another party who has access to data continuously may be able to de-anonymize the source, posing a privacy risk. If an outsider discovers the identity of certain data source, that outsider can use the same public key to de-anonymize all past, present, and future data [2]. Decentralized identifiers (DIDs) [9] have recently been developed to address this issue, allowing data sources to modify their externally apparent identity over time while allowing intended users to reassemble an entire DataStream. Despite the relevance of data and calibration "freshness," a digital signature only can’t determine the time a piece of data was signed in. Distributed Ledger Technologies (DLTs) [10] have been used to address this problem.

Implementations of a DLT can be public, consortium, or private. Interledger solutions or blockchains [11] can also be used to connect distributed ledgers (DLT implementations), allowing the establishment of new middleware ledgers with quicker update cycles and lesser assurance. These methods serve noncritical, mid-latency applications since "slow" ledgers with great confidence give a cause of trust, however for temporally critical applications, lower confidence may have to be accepted. One low-hanging fruit of using DLTs to improve measurement security is to use them to store global, trustworthy, shareable lab notes [2]. Because the database is append-only, anything written to the notebook stays there indefinitely. For privacy and security reasons, it may be preferable to communicate signed fingerprints of data rather than simply writing measurements to a DLT, and then storing the findings in a time series database. These systems work together to verify when and with what instrument a measurement was taken, as well as the recorded value (s). In some circumstances, using numerous ledgers at the same time may be advantageous, such as having separate notebooks for various labs or initiating actions based on specified occurrences, such as when a measured value wanders outside its permissible limits [11].

2.2 Artificial Intelligence (AI)

AI refers to a machine's capability to achieve tasks that would normally need human intelligence – such as pattern recognition, learning from knowledge, concluding, predicting the future, or taking any action – either digitally or as smart software in autonomous physical systems [12]. The availability of large data has fueled the development of AI as well as the need for it. Artificial intelligence technologies are shown to be important in the control, and operational observing of active measures in automation systems and mechanical engineering in context of Industry 4.0 [13]. In the domains of AI, machine learning, and deep learning, Neural Networks (NNs) mimic the function of the human brain, permitting computer programs to spot patterns and resolve problems [14]. Artificial neural networks (ANNs) and simulated neural networks (SNNs) are a subdivision of machine learning that are at the core of deep learning methods. Their name and construction are derived from the human brain, and they resemble the way biological neurons communicate with each another [15]. A node layer contains one input layer, more than or equal to one hidden layer, and an output layer in ANNs. Each node is connected to the others has a weightiness and threshold linked with it. If a node's output exceeds a certain threshold, the node is triggered, and data is sent to the next tier of the network. Else, no data is sent on to the network's next tier [15]. In [14], Machine learning and artificial intelligence key aspects and trends for optical measuring and inspection systems are presented and addressed. In [16], A spacecraft orbit control algorithm is being developed based Neural Networks. In [17] An Adaptive Neuro-Fuzzy Inference System (ANFIS)-based solution has been created as an alternative solution to traditional spacecraft attitude determination algorithms which suffers from a precision vs. computational load trade-off. As the complexity of an algorithm grows, so does its computing burden and accuracy which limits the application of the technique in a real-time (In-Orbit) setting.

2.3 Internet of Things (IoT) Applications

IoT is a network of interconnected calculating devices, machine-driven, digital machinery, items, may be animals, and people with single identifiers and the capability to transfer information devoid of requiring another interaction like human-to-human or human-to-computer [18]. A person who has a heart monitor implant, an animal which has a biochip transponder, a car with built-in sensors to aware the driver when tire pressure is under certain value, or any other natural or man-made item that can be given an Internet Protocol (IP) address and can transmit data through a network are all examples of things in the IoT [18].

Measurement equipment in industrial applications are frequently uncalibrated. Devices that require calibration may be calibrated in its place to save money and avoid calibration-related downtime. Inaccurately managed surroundings, on the other hand, endanger the calibration outcome. Many sensors can be employed for process observing to increase measurement accuracy, although the sensors utilized may be of poor quality due to cost restrictions [2].

These qualities provide further application-specific benefits, such as enhancing calibration processes by in situ built for calibration or through computational models, and optimizing production processes with higher quality sensor data [19]. Data fraud [20] and container ship capsizing [21] can both be avoided with the use of digital metrology. The drawbacks from using digital metrology will be presented in Subsection (3-5) [22, 23]. In [2], a digital validation system is proposed. A measurement quality metrics from metrology are brought to IoT data through a scheme that enables efficient measurement and device calibration methods. The system is based on two unique metrology solutions, Digital System of Unit (D-SI) and Digital Calibration Certificate (DCC) as well as a variety of digital security technologies, with a particular emphasis on Distributed Ledger Technologies (DLT).

2.4 Automation systems in Industry 4.0

The widespread adoption of digital technology has accelerated the industry's digital transformation, resulting in Industry 4.0. The notion of Industry 4.0 which is also known as the fourth industrial revolution has become a hot topic and is beginning to have an impact in industry. It is now a topic that academics, consultants, and, of course, businesses are interested in. It is also recognized that the majority of businesses and society are unaware of the ramifications and effects, as well as the hurdles that must be overcome in order to adopt it. The technical development from embedded systems to cyber physical systems (CPS) is referred to as Industry 4.0 or Smart Industry. It links embedded system production technologies and smart production processes to be ready for a new technical era that will employ automation technologies like CPS, IoT, and cloud computing to drastically change industry and production value chains and business models [24]. CPS are physical and engineered systems with operations which are observed, harmonized, controlled, and combined, as well as assisted by information and communication technology (ICT). ICT the interface with the physical world is possible with CPS [25]. Companies can use this new production system to establish the most appropriate manufacturing model and plan target roadmaps to solve the difficulties of the new industrial paradigm [26]. According to some researches, Industry 4.0 can increase manufacturing efficiency by 6% to 8% every year [27]. Industry 4.0's key goals in terms of inspection are to advance quality and maximize throughputs while lowering production prices, permitting for quicker and more precise procedures. In order for this to happen, virtual reality and augmented reality, the IoT, artificial intelligence and artificial vision, virtual assistants, Big Data, cloud computing, modern design programs and process simulation, 3D printing and security systems and services, Nano and biotechnology, or quantum computing, among other things, must be integrated. Metrology might be viewed as a challenge in ensuring part quality. As a result, more rigor is required to control 100 percent of production while maintaining the necessary flexibility to adjust the system to the various geometries of manufacturing components. Industry 4.0 necessitates significant modifications in metrology development. The following are some of the most important areas of research in relation to these changes: tackling metrological difficulties relating to measurement of multidimensional values (mostly non-physical ones), assurance of measurement results' reliability, securing and optimizing of measurement results flows in light of the expanding number of measuring instruments [28]. These variations are urgent and important; thus, it is necessary to manage the improvement of international standards governing the necessities of Industry 4.0 in order to apply correct techniques and implement the appropriate instruments and systems. The following concerns are between the most actual challenges in terms of metrological issues: The accuracy of the measurements gathered; the timeliness and security of the link to a data processer; and the formation of predictions of the process's path. To fully handle the aforementioned challenges, international standardization of feasible solutions, which are acknowledged by the metrological world, to these genuine metrology problems is required. The calibration procedure has traditionally relied on transmitting calibration artefacts from one location to another, which is effective yet inefficient. This technique is time-consuming and costly, with the constant risk that the calibration object will lose its accuracy through shipment If the calibration laboratories (reference) and customer laboratories may be linked via data transport rather than instrument transport, using industry 4.0 technologies, The data electronically transferred from one place (BIPM, NMI, or calibration laboratory) to another place (secondary calibration or customer laboratory) will permit a calibration process in various locations without transporting the calibration reference standard and the unit under test (UUT) to be in the same place at the same time. This can be accomplished by developing a procedure for producing, transferring, and controlling calibration data that will be matched with the reference values of the standards to the measured values from the UUT, without jeopardizing the accuracy and traceability required for calibration [29]. Nonetheless, the issue is to improve the flexibility of metrology systems that are close to the production line and can be quickly programmed to be user-friendly, allowing a non-expert to create and operate a new metrology structure. It is important to note that metrologies will be performed in an uncontrolled temperature and humidity environment, which distinguishes these circumstances from standard systems in controlled environments that provide a true measure in constant conditions [30]. Therefore, there is a need for a new digital quantity and new a unit measurement methodology to assist Industry 4.0. This is a critical requirement that must be met right away. Furthermore, digital transformation, with its massive data processing capability, opens the door to totally new applications driven by AI and machine learning, as well as hard realizations of metrological requirements as metrological traceability. Although these applications will take long time to occur, we have to prepare for them and establish setup to handle them. Expert knowledge on metrological principles, as well as knowledge from digital data experts, have to be aggregated to ensure that solid foundations for the SI Digital Structure are established. This has to be done right from the start to guarantee that a solid and dependable structure is built that will serve its goal well [31]. As part of the Industry 4.0 idea, main variations are occurring in industry, with a ubiquitous DT that intends to use huge sensor networks with wireless connectivity for enhanced decision-making.

This improved in metrological capabilities goes hand in hand with automation and the lightning-fast advancement of artificial intelligence algorithms. As a result, metrology tools that can deal with vast volumes of data and virtual things, as well as give trust in artificial intelligence choices, will need to be developed. All industrial processes are being disrupted by Industry 4.0, and This new 'wave' of rethinking industry is considered a challenge for metrology. Three examples of machine vision systems are presented in [30], and they are used to highlight some of the major challenges with which metrology must contend in this new paradigm. As a primary conclusion, each organization must develop its own roadmap for implementing the appropriate methodologies and processes in order to appropriately adapt and align with this new generation of metrology-related systems [30].

Information and communication technologies (ICTs), particularly the IoT are becoming unavoidable in industry, owing to their importance in enhancing organizational efficiency and competitiveness [32]. The ICT and IoT are pushed in almost all aspects of industry, resulting in the emergence of Industry 4.0 which is also known as the Industrial Internet of Things (IIoT). Specifically, through the combination of manufacturing, ICT, and CPS, industry 4.0 aims to redefine the relationship between workers and machines. Security plays an important role when improving and deploying production mechanism [33, 34]. So, adding automation, communication with internet, and data analysis to industry and manufacturing improves total efficiency, optimizes processes, and revolutionizes business while simultaneously posing security issues to ensure overall system dependability and integrity. As a result, this new environment introduces crucial elements that may alter the current state of metrology and metrology systems. In this context, metrology is defined as the systematic and extremely accurate collection of information in time and space [35]. Therefore, metrology has a challenge not only by the large amount of data gathered throughout the life-cycle of production, but also by the guarantee required for all sensor measurements as part of the operations of the day in the factory of the future (FOF) [36]. If detailed studies and/or very precise measurements are necessary, i.e. to address a quality problem whose source is unidentified, to advance a design, or to confirm the quality of extremely sensitive items, questions will arise. It should be emphasized, however, that time does not stop in the measuring room. Despite some obstacles, robotics and machine vision schemes may be the key to attaining local victories, and it is critical to combine these inaccessible solutions into a comprehensive industrial vision. The authors in [30] to illustrate these challenges presented three machines vision-based quality control schemes, performing a 100% review of production, conveying data about welding dimensions and object divergence in reference to the theoretical definition [30].

2.5 Digital Twins

The virtual equivalent of a physical object, such as an IoT gadget, is referred to as a "digital twin" The word was mentioned in a Nature comment [37], and a Scopus search for "Digital Twin" on February 7, 2020 yielded 819 results, up from two in 2014. The basic idea has been around for a long time [38]. Digital Twins and similar notions have produced plenty of new names of art [39, 40]. A Data Proxy, for example, is a Digital Twin which based on previously estimated data that saves system resources and improves the level of security while meeting application expectations, however a traditional Digital Twin mirrors data as closely as feasible [40, 41]. Digital Twins built for calibrated measurement equipment that operate as essential communication components to other entities [42] and incorporate a DCC and other important metrology data [43] have been proposed by metrology practitioners. By combining their calibrated data with physics-based modelling, metrology enhanced twins can improve manufacturing quality [43]. Digital twins will become a more important aspect of IoT solutions in the future. Digital twins will manage all data flow between distant computing environments and devices, as well as within devices [38], [40], allowing for total device optimization. To improve the life time of battery and other data, for example. Saturating twins with measurement quality data through a DCC or through otherwise will boost their usefulness by allowing them to serve a wider range of future applications, some of which may be important [2].

2.6 Blockchain

Blockchain is a chain of blocks that stores transactions data as shown in Fig. 2. The term "blockchain" initial appears in Satoshi Nakamoto's white paper on Bitcoin, which defines a different decentralized cryptocurrency [44]. Bitcoin pushes blockchain technology to its limit and has a lot of attention. Following that, a slew of cryptocurrencies and blockchain-based projects emerge.

As a result, blockchain has become a popular topic. Surprisingly, the blockchain's technology is not brand new. Security, distributed system, peer-to-peer networking, and other technologies are all combined in blockchain. Furthermore, blockchain provides a safe framework for cryptocurrencies, in which no one can tamper with transaction content and all nodes participate anonymously in transactions. As a result, blockchain technology has a wide range of applications, including financial services, medical systems, supply chains, and the IoT [45].

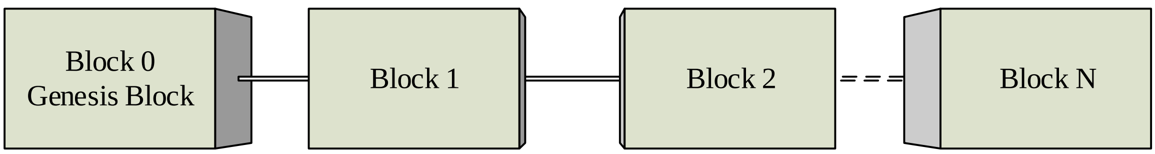

Figure 2: Blockchain is a chain of blocks that stores transactions data.

The organizations which are in the same supply chain see data and accuracy of data as critical to their success, but they are typically hesitant to share or use information when they don't trust one another. Despite the fact that firms may have access to the data of their supply chain partners, trust difficulties persist because they may intentionally or subconsciously deceive them with inaccurate, incorrect, or counterfeit data that does not indicate the genuine information. Companies and others are searching for ways and solutions that will allow them to securely communicate data and examine the origin, validity, and integrity of data over time in order to develop more dependable and trusted plans and projections. Blockchain is an ideal answer to these issues since it creates a single, irreversible record of information that can be read by anyone with permission to view but it can't be changed. Despite the fact that blockchain's adoption in finance has been swift, businesses claim to know little about it because of its novelty and a dearth of use cases and studies in the literature which illustrate blockchain's benefits.

The role of blockchain as a certifying authority that ensures the authenticity, integrity and origin of data held off-chain was proposed in some studies [46]. To that aim, a software connector module has been created to allow an enterprise information system to interact with an Ethereum-like blockchain. The application study demonstrates that blockchain technology is a useful tool for overcoming cooperation and trust subjects in a supply chain, improving overall supply chain efficiency, minimizing the negative values of data asymmetry across supply chain levels, and discouraging companies from engaging in any misbehaviour (e.g. counterfeiting information or low information accuracy). Because blockchain research in supply chain management is still in its beginning, it's worth looking into potential uses and benefits that might persuade supply chain managers to apply this technology and function in a trust-based environment. This research encourages the investigation of further supply chain phenomena through the use of a blockchain-enabled simulated supply chain, that serves as the ideal test environment for examining the true benefits of blockchain technology [46]. In the coming years, not only with other NMIs around the world, but also with health care authorities and research institutions with expertise in different science fields like medicine, biology, and chemistry, the traceability of measurements which is connected with quality of life, Nano medicine, and health in overall, will need to be improved in collaboration. This will be accomplished by looking for collaborations on a national and international level, as well as through European technological platforms [3].

Authors in [47] utilize blockchain capabilities to create a tamper-proof, traceable, trackable, accessible, immutable, resilient, and trustworthy spare part inventory system. To store and share spare parts data, the suggested system includes decentralized storage of interplanetary file systems (IPFS). Many proposed ideas during the recent years were to develop the important systems in the metrology field as the measurement systems or calibration systems and others as in [48-50] by using blockchain technologies as smart contracts. [48] proposes a mechanism dubbed "the system of recording calibration certifications." It's thought to be a blockchain-based application for metrology traceability. Takatsuji et al. use blockchain technology in [48] to allow the certificate owner to see the chain of calibrations all the way to the primary standard. Each laboratory in their proposed scheme has its own unique identifier, as well as a separate identifier for each calibration. According to the system, in order to locate a calibration anywhere in the globe, we must first locate the laboratory and the calibration. The method suggests that the transaction be split into two parts: a record of the most recent certificate and encrypted data about the initial certificates. However, in order for this proposed system to function successfully, all calibration laboratories in the traceability chain must employ it. As a result, this system cannot be used immediately. It can be utilized in a closed environment, such as a corporate [48]. The WELMEC 7.2 Software Guide [51] is cited by Peters et al. in [52] to define the main needs for legal metrology software.

The following are some of these requirements:

- The outcome is repeatable.
- Software durability of the measuring instrument.

- The output of the measuring instrument must include a software identity to confirm that the program has not been tampered with.
- The metrological features of a measuring equipment must be protected from any inadmissible effect.
- Measurement data, metrological critical parameters, and software are all protected from either accidental or intentional corruption.
- Once the measurement is performed, proof of the measurement result and the essential information to calculate the transaction should be provided on demand.

According to Peters et al. [52], the blockchain will be the expected technology that can satisfy the requirements of measuring devices. In [52], Peters et al. give several examples of blockchain applications that are appropriate for legal metrology, like Update Mechanism, Billing System and Decentralized Audit Trail. Finally, Peters et al. in [52] suggest that the private blockchain kind is the best for legal metrology.

2.7 Big Data Analysis

Big data analysis is often the hard process to analyse large amounts of data in order to identify information like market trends, identifying hidden patterns, correlations, and client preferences can help firms make better judgments. [53]. Big Data analysis tools and approaches provide organizations with a way to evaluate data sets and obtain new information on a large scale. Basic questions regarding business operations and performance are answered by business intelligence (BI) queries [53]. Big data analytics is a type of advanced analytics that entails complicated applications that use analytics systems to power aspects like predictive models, statistical algorithms, and what-if analyses [53]. Big data analytics technologies and software can help businesses make data-driven decisions that improve business outcomes. More effective marketing, additional revenue opportunities, customer personalization, and increased operational efficiency are all possible benefits. These advantages can provide competitive advantages over competitors with the right strategy.

2.8 Digital Transformation

Because every company's digital transformation will be distinct, it's difficult to come up with a universal description. However, we describe digital transformation in broad terms as the integration of digital technology into all aspects of a business, resulting in profound changes in how firms function and give value to consumers. Beyond that, it's a culture shift that necessitates firms challenging the status quo on a regular basis, experimenting frequently, and becoming comfortable with failure. This may include abandoning long-established business processes on which organizations were founded in favor of relatively fresh methods that are still being defined.

We've seen the COVID-19 epidemic issue reshapes both the what and how of firms' digital transformation goals in a matter of weeks. So, what is the best way to get started with digital transformation? First: 8 people you'll need for digital transformation dream teams as follows [54].

1. The leader of the digital transition

This key individual possesses strong soft skills, responsibility, and a track record of successfully leading digital transformations.

2. The agent of change

Communication, cultural transformation, and organizational change are all skills that this one-of-a-kind person should possess. The successful ones, have a decent presence that allows them to influence business officials as well as communicate with employees at all levels in order to push for change. These evangelists will market and sell digital capabilities both inside and internationally.

3. The engineer with technical knowledge

These people are in charge of defining the project's IT architecture. They are not only familiar with today's technology stack, but also with what it should be like in the future. They have an excellent awareness of diverse technology architectures and integration patterns to exploit existing capabilities. They can plug-in and plug-out both internal and external capabilities.

4. The expert in business

This is the person who knows everything there is to know about the function or process being altered. This lineup member also acts as a conduit for bringing in more specialists on demand. This person becomes the company's voice, collaborating with the technical expert to ensure that all business requirements are met. They have the ability to describe company issues, opportunities, and value. They take charge of defining required capabilities, encouraging experimentation and making quick decisions on what works and what doesn't.

5. The information architect

According to Kothari [54], this key actor will explain the many uses cases for data collecting and provide guidance on how analytics projects will be applied across the firm.

6. The financial analyst

This team member is in charge of creating the initiative's business case and financial-value framework. The relationship between your entire team and this player, as well as your organization's bigger group of finance professionals, should be a top focus; digital project funding depends on it. The first stage is to present all of the IT initiatives.

7. The serious hacker

These professionals have a penchant for breaking things and delivering constructive critique. They'll make sure the functionality is ready for pilots and meets the success criteria set by the project or program's owners. In the next Section, we conclude what is expected to happen in the field of metrology over the next 10 years according to the impact of IT.

The digitalization of goods and the use of digital procedures in conformity assessment are creating a slew of new issues (such as, in the calibration process) that necessitate the digitalization of the entire traceability chain. The use of intelligent sensors as a product in quality infrastructure necessitates appropriate traceability, which takes into consideration both the physical qualities of the transducer, as well as the measurement data's incorporated digital pre-processing. Simultaneously, the digital transformation of administrative operations in the traceability chain, accreditation, and conformity assessment necessitates suitable standardization and the validation of digital calibration certificates by a centralized, trustworthy institution. NMIs are confronted with various new issues as a result of the rapidly advancing digital transformation, which the clear majority of them regard as the greatest essential challenge to retaining their own effectiveness. It is clear that the demands imposed on NMIs to carry out this digital transformation are mostly in the following areas:

- IT and software capabilities;

- Modeling and measuring in the virtual world processes or as we say "digital twins";
- Cloud computing and real-time data storage;
- Autonomous systems;
- Integration and application development;
- Creating a link between the physical and virtual world (CPS).

Sensor data is continuously reviewed and compared as a result of this. In metrology, a data correlation study of solar modules along their value chain is an example. Data analysis procedures can be produced by providing suitable measurement and traceability methods, which would enable a quick reaction in the case of a defect and allow a link to be made between reduced efficiency in a solar park and wafer manufacture as an example. Because this necessitates in-depth knowledge and developments in measurement processes, as well as the improvement of appropriate mathematical and statistical procedures, mutual research between the departments of "Photometry and Applied Radiometry" and "Mathematical Modelling and Data Analysis" is required. Many domains of Nanometrology have examples of high-dimensional measurement results, such as signal contrast modelling using Monte Carlo techniques for the assessment of measurements on Nano-objects in scanning electron microscopes. Moreover, in dimensional metrology and optical surface metrology, imaging technologies that generate enormous amounts of data that must be analyzed are becoming more common. In other cases, only difficult simulation computations can be used to determine the effects of uncertainty in these sectors. In most cases, dimensionality reduction is required to make data management easier. Similar methodologies are increasingly being used in the realm of manufacturing, where optical measurement technologies, for example, are being deployed. This necessitates the development of methodologies that allow for statements about the measurement uncertainty's quality while applying dimension reducing approaches. As a result, generic processes must always be established in conjunction with the development of the measuring procedure, and on the basis of real applications. Adapted measuring methodologies can even result in a sufficient dimensionality reduction if the measurement spots are properly selected.

Machine learning and AI, for example, have resulted in an increase in the number of publications in the subject of big data analysis. "Deep learning" is a term used to describe these techniques. "Deep learning" methods are becoming more relevant in a growing range of industries as specialized hardware, open-source software, and very huge volumes of data become more widely available [55]. The feature of the results' reliability is extremely important from the perspective of quality infrastructure – and especially from the perspective of metrology. However, such data processing processes have yet to be addressed from a metrology standpoint. Examining the dependability of data analysis and establishing procedures for quantitative assessment of the quality of the results are topics which are now being researched outside of metrology, for example at the Fraunhofer Institute for Telecommunications (HHI) in Berlin. In general, however, the improvement of procedures for determining uncertainty and making quality statements in "deep learning" is still in its infancy [55]. In the next section, we conclude what is expected to occur in the field of metrology over the following 10 years according to the impact of the different IT fields that have been presented recently.

3 Next-Generation Metrology

3.1 Digital Calibration Certificate (DCC)

The traceability of measurement data supplied by multiple equipment to the same measurement standard of the specified physical quantity is required for data comparability. Traceability is defined in metrology as the property of a measurement result that allows it to be linked to its reference by a documented, unbroken chain of calibrations, each one contributes to measurement uncertainty. [56]. Because ageing and wear can have harmful impacts on measurement instruments, scheduled calibration is essential to ensure that they work within the permissible margin of error.

Individual instrument calibrations should be documented with CCs, according to calibration necessities. The requirements for calibration intervals and permissible measurement uncertainty limits vary depending on the laws and regulations of various nations and industries. CCs are currently papers or PDF files that contain the data required by relevant standards, such as ISO 17025 or other industry-specific standards. Mutual agreements, like the International Committee on Weights and Measures' (CIPM) and Mutual Recognition Agreement (MRA), are used to ensure that calibration certificates are accepted worldwide. There are accredited calibration facilities that offer standardized calibration services in addition to NMIs. There is an opportunity to modernize these certifications in order to better fulfil the demands of calibrators, standards organizations, and data users [2]. In human cultures, measurement devices and instruments serve a critical function. The importance of measurements in facilitating the creation and trade of items and goods cannot be overstated. As a result, regular calibrations are essential for preserving the accuracy of measurement devices. Every year, millions of paper-based calibration certificates with information on calibration traceability and measurement uncertainty are issued. While paper-based calibration certificates (PCC) are currently the cheapest and safest form of CC, new technologies and uses that demand automated formation, processing, and upgrading have made them obsolete. Traditional calibration certificate administration systems, as well as the paper format of the CC, pose a challenge manual inventory management system are frequently used, which are slow and complex to manage and process. Verifying traceability history in older systems is complicated and time-consuming. Furthermore, manual systems use numerous centralized storage designs, making them vulnerable to hackers and creating a single point of failure. For numerous causes, for examples: (1) measurement instruments become more connected, (2) the increasing use of IoT systems with many measurement sensors, (3) various measurement-intensive applications/instruments, such as self-driving autos, self-driving robots, and remote surgical operations, etc., developing new types of calibration certificates is becoming more important. All of these new applications include an incorporated measurement component that necessitates calibration and automated calibration data processing. PTB was the first to present Digital Calibration Certificates [43]. They developed an XML framework for delivering metrological data that would support existing standards and meet recommendations. A DCC can be used to convey administrative data and measurement results from current CCs for a machine in a format that can be read by a computer protected by a digital signature. The concept is being developed further in the EU Horizon 2020-funded EMPIR project "SmartCom." DCCs were initially implemented in XML, but they may also be done in JSON or other forms with lower overhead and better human readability. A DCC, in our proposal, communicates an IoT device's measurement uncertainty and serves as a link to its certified traceability chain. A measurement's metadata can include a link to the DCC. The development of system-level digital metrology for IoT is enabled by DCCs, which are rooted in NMIs [2]. Obviously, relying on human intervention to assess and validate the contents of calibration certificates places major constraints on such new uses [57]. So we have many recent papers today which discuss the DCC and present many useful contributions. The authors in [57] present a survey of relevant research activity on the DCC. As a result, peer researchers were able to detect trends, pertinent concepts, and future study objectives. The other main contributions presented in [57] are as follows.

- Analyzing both of the calibration process and the CC thoroughly. As a result, calibration procedure's model, CC life-cycle, and calibration use-cases is being developed.
- Considering the benefits and drawbacks of various DCC formats.

Several projects have been initiated in the last decade which could have a substantial influence on the format and use of DCCs, For example:

European Metrology Cloud: This intends to create a coordinated IT structure for legal metrology across Europe. To stimulate the digital transformation in legal metrology, the metrology cloud supports activities such as conformity evaluation, market surveillance, reference architecture creation, new technology, and services based on data [58].

SmartCom: It is a combined research project within the European Metrology Research Program EMPIR on "Communication and Validation of Smart Data in IoT-networks." Its main goal is to define the standards for a standardized, clear, and secure measurement data and metrological data interchange format in an IoT network. (2) the progression of DCC (3) the creation of a dependable, simple to use, validated, and secure online compliance valuation approach for legal metrology cloud scheme applications [59].

GEMIMeG: A collaboration between industrialized and educational partners in Germany to develop safe and reliable calibrated measurement solutions for DT. As a result, a national quality infrastructure (QI) must be established, in which the quality of the gathered data - including data from sensors and actuators - as well as the trustworthiness of the assertions and deductions drawn from it are ensured [60].

Met4FoF: The European Metrology Research Program EMPIR is hosting a cooperative research project called "Metrology for the Factory of the Future." Its goal is to create a metrological framework and structure for the entire life-cycle of measured data in manufacturing applications, from individual sensor calibration with digital pre-processed output to uncertainty quantification in industrial sensor networks using machine learning (ML). The desired outcome is the creation of realistic test-beds that validate applied applicability and serve as models for future industry adoption [61].

IoT data is currently underutilized, owing to the difficulty in determining its source. Data marketplaces are stifled by a lack of trustworthy information on data provenance, accuracy, and timestamping. To promote data portability and (re)usability, we recommend incorporating the DCC and accompanying quantifiable data quality metadata. Provenance metadata, which includes information about time and device identity, describes the data from an exact measurement equipment in minute detail, allowing it to be used in applications where input quality is crucial (e.g., healthcare, utilities, manufacturing, automated driving, and so on) [2].

3.2 Digital SI Units

As part of the SmartCom project, a new XML format was created: A Digital System of Units, to display measurement data in CCs in a machine-readable format (D-SI) [2]. All essential information includes numerical values for measurement results, units associated with the values, and measurement uncertainties, including both the value and distribution of the uncertainty. The "CIPM Task Group on the Digital SI" continues to develop D-SI [62].

The task group has developed a "Grand Vision" document as a starting step, dubbed the SI Digital Framework [63], which draws out a framework for the SI's digital transformation. The FAIR principles (Findable, Accessible, Interoperable, and Reusable data and services) are highlighted in this publication because they can considerably improve the possible for data reuse by digital systems [64]. The application of computer reasoning, machine learning (ML), and AI approaches will be facilitated by FAIR-principles-based information, for example the type of quantity, measurement accuracy, provenance of errors, and so on. Metadata can be used to ensure that physical quantity data provided by sensors is accurately understood for data analysis in increasingly networked and automated contexts, such as the IoT and cyber-physical systems. FAIR metadata underlines the requirement for independent researchers to re-examine and reproduce results of research, as well as for computer systems to automatically extract knowledge from huge and diverse sources of research information in the context of scientific research. More than just representing units of measurement in digital form is the goal of the framework. It will include a description of the system being measured as well as the methods used to collect data, and the procedures connected with the final measurement results (data, models, and software). From basic capabilities to a fully machine-actionable knowledge representation, the framework should improve machine readability. Machine-actionable data will permit automatic evaluation of dataset origin, and metrological traceability, as well as the usage of machine learning and AI techniques.

A SI Digital Framework will address the following topics in the near future:

- Quantity and SI unit data and metadata models that are interoperable;
- Digital depiction of the main metrological documents as the GUM, the VIM, and the SI Brochure;
- Establishing open, high-quality, verified-quality access to data, services, and tools, such as the Key Comparison Database (KCDB) and the Joint Committee for Traceability in Laboratory Medicine (JCTLM) database [31]; and
- Adoption of DCCs to support metrological traceability in digital systems.

The SI Digital Framework will address the following issues in the long run:

- Measurement processes, measurement workflows, analysis methods, and traceability chains are all represented digitally. Machines will be able to access and act on data having minimal or no human involvement.
- Data relating to measurement comparisons and other forms of measurement comparisons is represented digitally.

● Embedding a digital framework in many forms of cyber-physical systems, for example smart sensor networks, IoT environments, and self-contained systems, to establish traceability at the places of measurement. The SI Digital Framework is divided into three layers [31]:
An SI core representation including metadata models and interchange format implementations for fundamental quantity data elements, including values, units, and uncertainties, that has been authorized by the CIPM.

1. A services layer containing open data formats, software tools, and services that expand on the SI core representation, implemented by NMIs, the BIPM, and related organizations. Such services will increase data quality and transparency, as well as help data fit-for-purpose assessments, life-cycle analysis, and data preparation for analysis.
2. An applications layer, which has been created and deployed in the metrology community as well as in research areas that depend on the SI. This layer will include advanced analysis, AI and ML methodologies, as well as tools and services for domain-specific applications. By building on the SI core and services layers, applications will benefit from metrological traceability and hence be able to achieve high levels of reliability.

In FAIR digital data, the International System of Units (SI) is a virtual workshop that brings together prominent professionals and groups in digitalization connected to metrology and data science to discuss ideas with the first steps to take in this approach, with the goal of agreeing on basic standards for a "Digital SI" framework [65]. The International Committee for Weights and Measures (ICWM) has determined that digital representations of the International System of Units (SI) as well as related metrological principles like traceability and uncertainty must be supported. In 2019, a specialized Task Group was formed to address issue. This overview summarizes the task group's activities to date, which include an overarching "Grand Vision" statement, a sketch of a SI Digital Framework, and an international workshop titled "The SI in FAIR digital data," held on February 22nd to 26th, 2021, to involve a large number of people in a discussion about a solution.

3.3 Challenges & Opportunities

We discuss the proposed notion from both a difficulty and an opportunity standpoint. The move from present procedures to a digitized solution is a big problem from a metrological standpoint. Before DCCs can realize their full potential, the standardization of a new calibration data format will take time, needing worldwide acceptance and mutual agreements [2]. Additional metadata standards, in addition to the DCC and D-SI formats, are required to enable and advance the usability of the digital metrology structure through application fields. Traditional technologies that are not dependent on DLT solutions can be used to generate the cloud as an alternative to a DLT-based DCC cloud. With a non-DLT DCC cloud, it is necessary to find a solution that is similar to standard electronic banking systems. For example, it is necessary to have a central authority with the capacity to process all cloud contents. Malicious actors would be enticed to target such a central authority. A successful attack might bring the calibrating system to a halt. The preferred implementation is a DLT-based DCC cloud, which would require more effort to breach. Future data will be more accessible across industries with the global acceptance of this suggested model, as DCCs improve trust in the quality, accuracy, and the accuracy of measuring data. This system assumes low confidence irrespective of the system embodiment today unless a system end-to-end is controlled (the system produces the hardware, software, and installation) [2].

On the other side, we can't make key decisions based on bad data. Data quality is especially important for machine learning. Despite the fact that machine learning can successfully analyze data, such as filtering faulty measurements or timestamps, some systematic failures induced by ageing of the measurement instruments may escape unreported [2].

The addition of metrology to IoT measurements improves the data's usefulness for directed applications and third entities. Trusted information will be a driving force behind a data economy in which markets may ensure the value of sold data. As a result, the entire movement of reliable data will be improved, which will benefit all stakeholders. To make informed decisions, modern businesses rely on data. IoT sensor data that can be trusted provides a greater understanding of operations, allowing management to make more correct decisions. As a result, including metrology-based data quality measures into IoT sensors has the potential to have a greater societal impact. To make the opportunities a reality, more work is required. Validating the DCC in real-world scenarios, building a scheme to store or distribute DCCs, and safeguarding the transformation to digital traceability chain, maybe using Digital Twins, are just a few examples [2]. There is also the issue of machine learning outcomes being susceptible to manipulation by interfering with input data in critical areas. This area of study is known as "adversarial learning", and it will be useful in the new metrology world [55].

The introduction of systemic mistakes due to diminished human oversight, possible privacy violation, and increased implementation costs are all potential drawbacks of digital metrology artificially intelligence managers [22], privacy, decentralized IDs [23], and storing cryptographic fingerprints rather than data are some of the countermeasures. Measuring using digital tools requires collecting large amount of data. Also, to introduce the metrology services to customers in a digital way require collecting data about these customers which may violate their privacy rights. The presented study in [66] discloses that using security tools is positively correlated with increased risk behaviors and infections, whereas engaging in safety measures lowers the incidence of malware infections. Another important challenge is related to the developing countries. The different definitions and requirements for accurate measurement of the digital economy were devised [68]. The definition and assessments of the digital economy in the beginning focused mostly on the uptake and usage of the Internet as well as some of its effects on the economy [67]. But, as internet technologies advanced, the emphasis changed to looking at the nature of the expanding digital economy [68]. Oloyede et. al. in [68] offer future approaches to monitoring the digital economy and trends that developing nations might use. Finally, the authors in [68] recommend that the definition of the digital economy must be sufficiently flexible, the digital economy measurement toolkits are sufficiently adaptable to allow for the inclusion of developing nations, some characteristics unique to emerging nations should be accounted for in the measuring metrics, and the governments of developing nations have to act to guarantee that enough data are gathered and made accessible [68].

3.4 Overall Solution Using IT Fields

A digital validation system that allows for effective measurement and device calibration processes is proposed in [2], bringing metrology's quantitative measurement quality metrics to IoT data. This system is based on new metrology solutions, D-SI and DCC, as well as a variety of digital security technologies, with a particular emphasis on Distributed Ledger Technologies (DLT). Fig. 3 depicts the recommended solution. The DCC of an NMI serves as the foundation of measurement trust for calibration organizations and IoT measuring equipment. The DCCs of a calibration chain are stored in the DCC-DLT cloud, with inter ledger solutions connecting several DLTs. A DCC-validated data marketplace can be created by using a measuring device's DCC to check the quality of a measurement result. DCC-DLT cloud is a hybrid of distributed ledger technology (DLT) and traditional trusted cloud solutions that provides storage and integrity for the whole traceability system, including DCC storage and measurement data validation. The DCC-DLT cloud allows the end user to (re)certify their acquired data. Devices generate DCC-validated data, which is then transferred to the end user, possibly through a data market. The DCC-validated data additionally includes metrology-based data quality metrics, which indicate the data's measurement uncertainty, as well as maybe other metadata. The DCC-DLT cloud often serves as an inactive component, storing and certifying DCCs and data. When prior calibration action needs to be revoked, the cloud can transmit alerts of the DCCs withdrawal to consumers of data and instruments in the impacted calibration chains, with the calibration removal attached to the end of the chain [2].

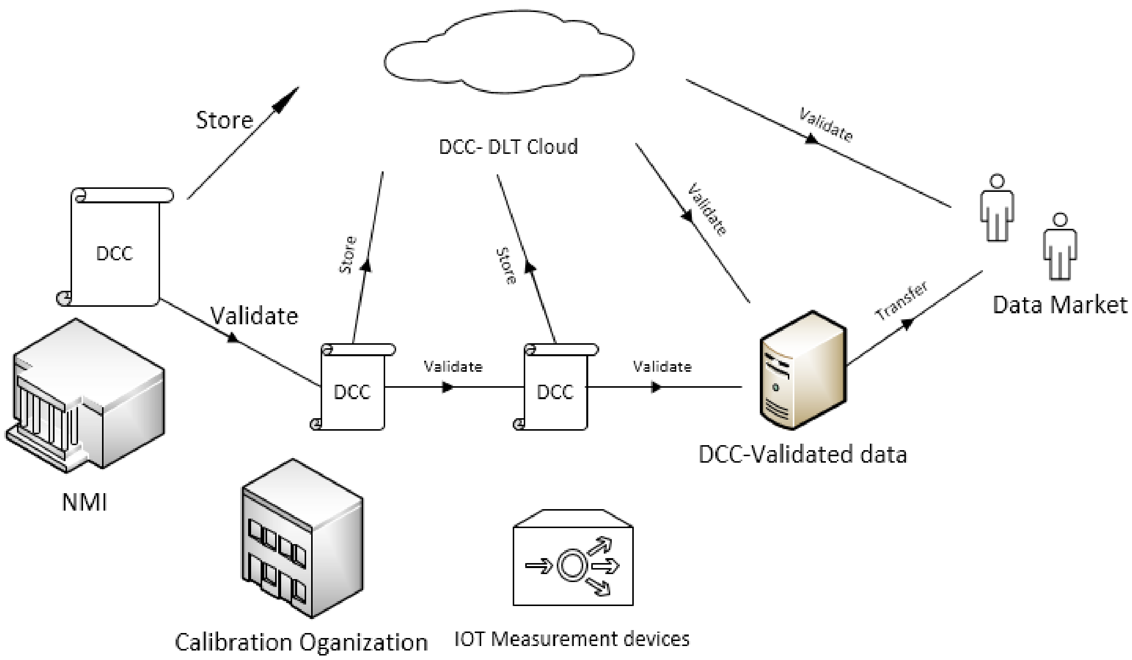

Figure 3: The proposed solution for data provenance sharing and DCCs, redrawn from [2].

We proposed an improvement to this solution by applying the blockchain technology for storing DCC. This proposal will maintain horizontal traceability which is the pervious CC for the same device up to the first manufacture CC and will maintain vertical traceability which is to trace the CC of the device to the highest-level reference standard.

4 Metrology's role in IT

As Metrology plays an important role in different sciences, commerce and industry it is also plays an important role in IT. To paraphrase Lord Kelvin's aphorism, our knowledge of anything is insufficient unless it can be measured. The obvious implication in the real world of management is that our ability to manage anything is directly proportional to our understanding of it, and thus managing something that cannot be (or is not being) assessed is difficult to impossible [69]. The discipline of metrology has significant ramifications for the science of information technology. As in other research domains, you must test, analyze, and detect. You must put in the same amount of effort in IT as you do in other science fields to meet the standards. New metrology is beneficial in addressing global concerns on software, network Security, AI and etc. In recent years, significant progress has been achieved in the field of information technology measurement, yet it is still in its infancy in certain ways [7].

Background Information for IT Metrology Researchers [70]:

IT metrology necessitates a foundation in metrology science. Perhaps, at first, this will not necessitate much metrology skills or intricate uncertainty estimates. Due to the fact that this field is still in its infancy. Understanding the objective and goal of metrology, as well as believing that metrology is the greatest tool to advance and improve the quality of any field, is adequate. It is necessary to have a reasonable experience in IT systems. It is recommended that you have some knowledge with cryptography and cryptanalysis. Networking and programming fundamentals are also essential. Then, based on the application, he'll need to gain more experience. some knowledge in electronic circuit design may be needed if something hardware will be implemented. Scientists are needed to explore, discover, and solve several research fields in security metrology. The next subsections present information about metrology's impact in the next decade for some IT fields.

4.1 Impact for software

In software, metrology is very significant. Software metrics are used to make measures in software. A software metrics are a measure used to determine the characteristics in a software program or method. Even if a metric isn't a measure (metrics are functions, but measurements are the results of metric application) [71]. Accurate measurement is required in all technical domains, and software engineering is no exception [72]. In [73], A system for evaluating the quality of software products has been established by experts. The following are some of the most common purposes for which software is evaluated [74]:

Characterization: is the practice of gathering information on some aspect of software processes and products in order to gain a better understanding of "what's going on."

Evaluation: assessing any aspect of a software either process or product, such as, using historical data from external sources or the same runtime environment.

Improvement: identifying parts of a process or product that can be altered to get positive special effects on some characteristic of interest using a cause-effect relationship, and gathering data after the modifications have been made to approve or disprove if the effect was optimistic and the magnitude of the effect

Expectation: determining a cause-and-effect relation between process attributes and product

Tracing: the gathering of data from part of software processes and products over time in order to determine if those aspects are under your command in ongoing projects.

Validation: Putting the most effective methods chosen to the test.

In measuring instruments, software is frequently integrated with hardware, which is critical for dealing with data, modifying process parameters, and driving the instrument to work. Typically, metrology characters are verified in the type approval of an instrument; however, if there are no rules or methods to carry out the check, the software check is ignored [75]. WELMEC and OIML have developed various files to instruct software check for instruments in recent years [51, 76], and it is useful for metrology institutes to develop a clear strategy to carry out software check.

4.2 Impact for Network Security

It's difficult, if not impossible, to manage something that can't be quantified, and information security is no exception [3]. ISO 27001 is a well-known need for a company information security management system (ISMS) [7]. An ISMS is a group of principles and protocols designed to assist societies in the event of a data crack. Businesses can reduce risk and maintain job continuity in the event of a staff transition by having a documented set of guidelines. For a long time, increasing bandwidth capacity, having a larger tube and quicker routers, and improving traffic flow were the main options for tackling network difficulties. Metrology has been helping to modify this mindset for about ten years, with a concentration on network administration [77]. Nowadays, metrology can give novel benefits, particularly in the area of network security. Science of metrology is a technique for detecting functional faults in networks, measuring error rates, and detecting active and passive anomalous behaviour [77]. Metrology has a variety of consequences on network security because it is so vital for improving network security quality Metrology is beneficial in a variety of methods [77]. Metrology has an impact on network security in a number of ways. Reasonable growth and improvement can be made when metrology science is applied to network security. The primary points that metrology should be applied to in order to make effective progress in network security are listed below.

A. Developing Standards, and Applying the Standards to System Implementation.
B. Metrics for Network Security.
C. Attack Effects Measuring, Detecting, and Analysing.
D. Research and development of network simulators.
E. Testing security protocols and learning how to use verification software.
F. Developing the security of the network.

4.2.1 Developing Standards, and Using the Standards to Implement a System.

Many researchers are involved in the hardware or software implementation of security systems. The system's quality and dependability will improve if the criteria are followed. You must also advance your security scheme to bring it up to par with industry requirements. A New Multicast Authentication Protocol using AES is proposed by Abouhogail in [78]. In this paper, the standard AES is used which provides various benefits to the system, including a high level of security, applicability to real-time applications, and increased confidence in the system. In addition, searching for ways to build network security standards is a popular topic in the security industry. [79] presents a new quick handover authentication strategy with privacy protection to advance the abilities of IEEE 802.16m [80], which is regarded an application to build network security schemes standards in the WiMAX field (Worldwide Interoperability for Microwave Access). WiMAX is a wireless broadband technology. Anmin Fu.et al protocol's [81] proposes a privacy-preserving quick handover authentication solution for IEEE 802.16m networks based on pseudonym. He also made a development in IEEE 802.16m [80] to reduce the required computing overhead. Arun improved the Mix-columns function of the AES algorithm in [82], resulting in higher throughput. He demonstrated two implementations on a multi-core system: One has an online key expansion option, while the other has an offline key expansion option. Dyken et al. proposed a different direction in AES algorithm optimization in [83], focusing on how to reduce the power consumption of an FPGA [84]. As a developing to IEEE802.11s network standards there are many recent researches as in [85, 86].

4.2.2 Metrics for Network Security

The subject of security metrics is concerned with the aspects that able to be measured in order to define security levels. Because of the complexity, ambiguity, non-stationarity, observability restrictions of operating systems, and attackers' malice, security cannot be quantified as a universal notion [69]. There are numerous additional causes for this. Securitymetrics.org is a community website founded in 2004 by Andrew Jaquith for (and by) information security practitioners and decision-makers, with the goal of advancing more empirical (rather than qualitative) security methods through its members' collective efforts. The website includes a news feed, a knowledge base, and a conversation and cooperation area (in the form of a members-only mailing list) [69]. Measuring security is a challenge as indicated in [87], some of the difficulties in measuring security:

- We won't be able to test all of the security criteria.
- Security is influenced by the environment, abstraction, and context.
- Security and measurement are intertwined.
- There is no such thing as a stand-alone system.
- Security is multifaceted, emergent, and dynamic irreducible.
- The antagonist alters the surroundings.
- Measuring is both an expectation and a goal for the organization.
- We're overconfident.
- We have diverse reactions to gain and loss.

4.2.3 Attack Effects Measuring, Analysing, and Discovering

Any computer network, particularly wireless networks, is vulnerable to a variety of dangers (attacks). Threats in the realm of computer networks come in a variety of shapes and impacts. Active attacks and passive attacks are the two basic types of attacks. The passive attack involves the attacker can know information from the network but cannot writing or changing it. The attacker writes, updates, or deletes something in the network's data during an active attack. Threats of any kind have an impact on the security system's objectives. To secure communication, the security system has a few objectives. The security system's most significant objectives are:

- Confidentiality: When data is kept secret from unintentional listeners, it is said to be confidential.
- Data Integrity: To maintain data integrity, the received data must match the data transmitted.
- Authentication: This refers to the fact that the person performing certain actions is the one we intended and he's been given permission to do so.

• Non-Repudiation: As soon as a system ensures data integrity, a recipient can be confident in the sender's identity and the data the sender intended to convey. However, the recipient may not be able to prove this to a third party.

• PDR stands for packet delivery ratio, which is the ratio of total data received to total data sent from sender to receiver.

Packet Dropped: The sum of packets dropped by all entities in the network is represented by this parameter.

Network Throughput: The average rate of successful messages transmitted over the communication channel is known as network throughput. Bits per second or packets per second are the units of measurement. Unreliable communication, changes in topology, restricted bandwidth, and limited power are all factors that affect this characteristic. This tendency necessitates a solid understanding of network communication in general, as well as a thorough examination of the chosen application in particular. The subsection below will assist you in selecting the appropriate network simulator to assist you in completing your mission.

4.2.4 Network Simulators: Research and Development

This division is interested in learning about various network simulators and developing in them. Many network simulators are available to test or quantify the performance parameters of any network system, including QuaLNet, NS2, NS3, OPNET, and OMNeT++ [88]. Some of them are available for purchase, while others are free to use. You can choose the simulator that is best suited to your application. [89] provides a comprehensive overview of the many types of network simulators accessible. Each simulator's benefits and drawbacks are explored in detail. Each one's programming language is specified. As a result, we may conclude that network simulators can be used to test the performance of your network. Security is one of the most essential network performance parameters, and we could put it to the test with network simulators., as described in [90]. As a result, network simulator research and development are a critical topic in the security network and metrology fields. This tendency necessitates a strong programming experience in addition to knowledge of networks and routing technologies.

4.2.5 Testing of Security Protocols

According to [91], a protocol is "a set of processes involving two or more persons and structured to achieve a specific goal”. As we can see from this definition, the protocol contains a number of restrictions:

1. It must follow a specific order.
2. It must have more than one component.
3. It must have a goal and carry out a mission.
4. All parties involved in the protocol must understand it and all of its procedures.
5. Participants in the protocol should accept to follow the steps.

Security protocols are computer programs that keep networks safe. The security protocols are created to meet certain security requirements. They are also an essential tool for achieving varied objectives depending on the application. Integrity, confidentiality, authentication, anonymity, non-repudiation, key distribution and so on are the basic aims of security protocols, which vary depending on the application. Intruders use a variety of tactics to thwart security goals. Failure to follow security protocols can have major implications, such as financial loss or the loss of users' trust in the program. The protocol's participants are known as agents, and they are frequently referred to as demonstrated in Fig. 4 A (for Alice) and B (for Bob). The enemy who wants to break the protocol is represented by a third party known as I (for Intruder). The server, for example, is a fourth party who judges in case of a dispute.

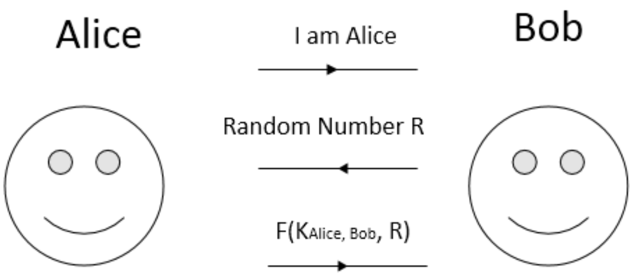

Figure 4: Example of a Simple Security Protocol.

We can test security protocols using formal and informal tools as in [92]. A reasonable enhancement can be observed in some security protocols due to applied metrology regulations as in [93-98].

4.2.6 Increasing Network Security Quality

Metrology is a branch of science concerned with enhancing the quality of any scheme. Because communication is such a crucial scheme in our daily lives, enhancing the efficiency of any communication scheme is considered a step forward in metrology. Achieving a high level of secrecy in the communication system is regarded a significant improvement in the communication system's quality. As a result, network security is becoming increasingly crucial for a wide range of applications. Bank transactions, NFC (Near Field Communication) apps [99], and e-voting are all highly significant in e-commerce. We can increase network security in a variety of ways, including the ones listed below.

1. We can cut down on the number of attacks against which the system is vulnerable.
2. Adding security functions reduces the amount of communication and processing overhead.
3. Proposing new security protocols with greater features or improving existing ones to solve difficulties.

4.3 Impact for Artificial Intelligence

The National Institute of Standards and Technology (NIST) has a long history of measuring and evaluating AI technology in a variety of fields, including biometrics, voice and language processing, computer vision, information retrieval, and robotics [100]. As the societal consequences of AI have expanded and become more apparent, certain qualities that were previously considered outside the scope of AI have been recognized as critical to assess and analyse in order to provide justified confidence in AI systems before and throughout deployment. Measuring these properties will necessitate either:

1) Formulating them in terms of mathematical objectives/constraints (which would also be useful for machine learning systems to "learn to be un-biased," for example), or
2) Devising a method to "litmus test" or otherwise explicitly specify the degree to which AI systems possess these properties. NIST's mission is to support the advancement and

deployment of measured AI technologies, and it has been charged by statute with advancing underlying research for measuring and evaluating AI technologies, such as the improvement of AI standards and finest practices, as well as AI testing methodologies and standards. To that purpose NIST will do the following [100]:

1. Design, characterize, and theoretically and empirically analyze metrics and measurement methodologies for certain aspects of AI systems, including data curation and characterization.
2. Make it easier to measure and evaluate AI technologies in terms of these properties by publishing and presenting technical reports, as well as activities like publishing software tools, hosting evaluations of externally developed systems, and publishing best practices and technical guidance documents.
3. Lead and/or participate in broad standardization efforts in support of the deployment of measured AI technologies, contributing to the development of voluntary consensus-based standards for evaluation of AI technologies.
4. Build a strong and active community around the measurement and evaluation of AI technologies.

There are numerous AI applications, each of which could be used in a variety of situations. Furthermore, there are a number of properties of an AI system that may be measured. We do not believe it is possible to construct a single and meaningful evaluation/metric/measurement approach to be utilized to measure all of AI as we presently know it for these and other reasons. Furthermore, NIST will not be able to address each potential application and configuration individually, even with significant effort. Instead, we want to do basic metrology research and produce evaluations for the applications and contexts where measurement is most important [100].

4.4 Impact for Big Data Analysis - Smart Metrology

In the industrial environment, metrology is entrusted with far greater responsibility than is normally given to it. Quality certification has largely limited industrial metrology to the legal metrology model, which appears to be severely unsuitable for industrial needs. In view of the new period that is about to begin, it is critical to reflect on and rethink the role entrusted to metrology so that it can fully participate in the coming industrial revolution [97]. As a result, we don't have a single value to choose from, but rather a range of options, some of which may be compliant and others not. This misunderstanding of the entity's true value casts doubts on its compliance, posing a risk to each choice made at any level in the above chain. The metrology service was created to address a need: reducing the danger of receiving inaccurate measurement results, which could have an influence on product quality. As a result, it is critical to comprehend this passage in order to avoid reversing the situation: "impose our metrology, because it is written in standards." Smart metrology is concerned with evaluating risks and balancing them to "only what is required." In the future, The Smart Metrologist's purpose is to improve the measured entity's knowledge by incorporating a priori information [101].

The digital revolution, which began in the early twenty-first century, saw the emergence of a new manufacturing revolution: the capability to store data in unprecedented large quantities from various sources (particularly through related items) and exploit it through increasingly high computing capabilities using AI. The enormous amount of information collected and their investigation are totally useless if untrustworthy data is retained that cannot assist in the understanding of a complicated reality in this new scenario known as "Big Data." The purpose of metrology is to assure the accuracy of measured data. Smart metrology is the application of a redesigned metrological function that is focused on reliability rather than compliance with standards: assuring measurement reliability, understanding and mastering measurement uncertainty to make informed decisions. A summary of business metrology issues can be found at [101].

5 Future Work

As a future work, we aim to benefit from the DT trend and to apply that in NIS Egypt. It can be applied gradually in three stages. After the first stage everyone can obtain the required metrology service at a high level from anywhere and at any time through an integrated, simple, and secure electronic methods. After the second stage we aim that everyone can allow to use through many electronic channels, effective metrology service in a safe, unified, and simple manner. As a third stage, we seek to achieve a complete smart system inside the different NMI's including different services with the customers and different procedures inside the labs. The future is going to become "Smart", and metrology must adapt to this change by becoming "Smart" as well. Furthermore, by directing our researches to work in setting standards for the different IT fields which are mentioned before, it will help to improve the quality and efficiency of the different IT branches.

6 Conclusions

An IT operations automation plan can aid in the optimization of measurement procedures. Automation allows you to save time, improve quality, raise employee happiness, and lower costs across different NMIs. Our paper offers different IT branches that participate to improving the future of metrology such as, for example, IOT, AI, digital twins, and big data analysis. For example, DCCs save expenses and improve data integrity in regulated contexts by automating calibration information processing. Applications of IT in metrology could have a wide range of effects, from reduced manufacturing costs to higher production quality. Another good example is adding verification data to IoT-sourced data. For the first time, data from mega-scale distributed sensing schemes may be used properly in applications where results are essential. DCCs have the ability to revolutionize the data given by the IOT, resulting in a multi-sector revolution. Another expected feature for modern metrology is presented in this research, the D-SI. The expected challenges in the new metrology world have also been clarified. Using DLT in the DCC cloud enables validated data in metrology at a scale not possible with present systems but appropriate for the IoT's expanding extent. Using the cloud enables fast and global validity checks of DCCs, and the ramifications of implementing such a system would amplify the IoT's influence. On the other side, the science of metrology has a great influence and role in the science of IT. A rise in general belief in IoT data measurement, for example, might facilitate reliable markets for data or the usage of data in new applications that are mission-critical. Introducing digital metrology to the IoT benefits a variety of sectors and applications by permitting the usage of measures that are accurate, trustworthy, precise, and timestamped. Despite the fact that IT needs to bring Metrology closer to the production line to save a lot of time and cost, allowing for 100 percent production control, it introduces numerous sources of uncertainty into the measure. So, in the field of information technology, metrology is crucial. So, through this paper, we demonstrate the impact of metrology on software, network security, and AI. Moreover, the new term, known as smart metrology, and its impact on big data, have been clarified in the paper. As a future work a more comprehensive analysis for the new advancements and trends in metrology will be discussed. For example, the increase usage of AI as robotics in measurement developments which will lead to faster and more accurate results. Also, the growths of new measurement methods as nanotechnology and Contemporary Patterns in Modern Metrology are important topics need to be discussed.

7 Declarations

7.1. Competing Interests

No conflict of interest exists in this publication.

References

[1] Fluke Corporation, Legal Department, Everett, WA 98206-9090, " Calibration: Philosophy in Practice", Second Edition, May 1994.

[2] T. Mustapää, J. Autiosalo, P. Nikander, J. E. Siegel and R. Viitala, "Digital Metrology for the Internet of Things," 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, pp. 1-6, 2020, doi: 10.1109/GIOTS49054.2020.9119603.

[3] Torino, “INRIM Metrology towards 2030”, NRIM, 22 Dec. 2020. https://www.inrim.eu/vision

[4] https://workforce.com/news/what-exactly-is-information-technology-it. Accessed on 19 Oct. 2021.

[5] https://www.truqcapp.com/digitization-vs-digitalization-differences-definitions- and examples/. Accessed on 18 Oct. 2021.

[6] S. Rab, M. Wan, R. K. Sharma, L. Kumar, A. Zafer, K. Saeed and S. Yadav, “Digital Avatar of Metrology”, MAPAN-Journal of Metrology Society of India, 38(3), pp. 561–568, September 2023. https://doi.org/10.1007/s12647-023-00641-1

[7] https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html. Accessed on 15 Oct. 2021.

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

[9] A. Muhle, A. Gruner, 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

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

[11] 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.

[12] USAF. USAF AI Annex to DoD AI Strategy. Tech. Rep., United States Air Force (2019). https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

[13] E V Dudukalov, V D Munister, A L Zolkin, A N Losev, and A V Knishov, “The use of artificial intelligence and information technology for measurements in mechanical

engineering and in process automation systems in Industry 4.0”, Journal of Physics: Conference Series, 2021.
[14] M. Heizmann, A. Braun, M. Hüttel, C. Klüver, E. Marquardt, M. Overdick and M. Ulrich, " Artificial intelligence with neural networks in optical measurement and inspection systems", SMSI 2020 Conference – Sensor and Measurement Science International, pp. 265-266.
[15] https://www.ibm.com/eg-en/cloud/learn/neural-networks. Accessed on 17 Oct. 2021.
[16] T. M. Habib, R. A. Abouhogail, “In-Orbit Three-Axis Spacecraft Orbit Control Based on Neural Networks via Limited Thrust Budget”, International Review of Automatic Control (IREACO), Vol. 14, N. 3, May2021, pp. 144-152.
[17] T. M. Habib, R. A. Abouhogail, “Replacement of In-Orbit Spacecraft Attitude Determination Algorithms with Adaptive Neuro-Fuzzy Inference System via Subtractive Clustering”, International Review of Aerospace Engineering (IREASE), Aug.2021, pp.220-227.
[18]https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. (Accessed 1 Nov. 2021).
[19] 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, 15 May 2019.
[20] 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
[21] 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
[22] J. Siegel and S. Sarma, “A cognitive protection system for the internet of things,” IEEE Security and Privacy Magazine, vol. 17, no. 3, May 2019, pp. 40–48.
[23] A. M¨uhle, A. Gr¨uner, T. Gayvoronskaya, and C. Meinel, “A survey on essential components of a self-sovereign identity,” vol. 30, pp. 80– 86, Nov 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574013718301217
[24] Y. Lu, “Industry 4.0: A survey on technologies, applications and open research issues”, Journal of Industrial Information Integration, vol. 6, pp. 1-10, 2017.
[25] L. Barreto, A. Amaral, T. Pereira, “Industry 4.0 implications in logistics: an overview”, Procedia Manufacturing, vol. 13, pp. 1245-1252, 2017.
[26] W. MacDougall, “Industry 4.0: Smart Manufacturing for The Future”, Germany Trade and Invest; 2014.
[27] S. Fernandez-Miranda, M. Marcos, M. Peralta, F. Aguayo, “The challenge of integrating Industry 4.0 in the degree of Mechanical Engineering”, Procedia Manufacturing, vol. 13, pp. 1229-1236, 2017.
[28] R. Taymanov, K. Sapozhnikova, “Metrology challenges of Industry 4.0”, Journal of Physics, Conference Series 1065:072044, 2018, doi:10.1088/1742-6596/1065/7/072044.
[29] S. Andonov, M. Cundeva-Blajer, “Calibration for Industry 4.0 Metrology: Touchless Calibration”, Journal of Physics: Conference Series, 1065:072019, 2018.

[30] V. Alonso, A. Dacal- Nieto, L. Barreto, A. Amaral, E. Rivero, “Industry 4.0 implications in machine vision metrology: an overview”, Procedia Manufacturing 41, pp. 359–366, 2019.
[31] S.J. Chalk, D.N. Coppa, F. Flamenco, A. Forbes, B.D. Hall, R.J. Hanisch, K. Hosaka, D. Hutzschenreuter, J.S. Park, R.M. White, “International development of the SI in FAIR digital data”, Measurement: Sensors, vol. 18, 100293, 2021, https://doi.org/10.1016/j.measen.2021.100293.
[32] M. Wollschlaeger, T. Sauter, J. Jasperneite, “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0”, IEEE Industrial Electronics Magazine, 11(1), pp. 17-27, 2017.
[33] M. Bauza, J. Tenboer, M. Li, A. Lisovich, J. Zhou, D. Pratt et al, “Realization of Industry 4.0 with high speed CT in high volume production”, CIRP Journal of Manufacturing Science and Technology, 22, pp. 121-125, 2018.
[34] G. Byrne G, E. Ahearne, M. Cotterell, B. Mullany, G. O’Donnell, F. Sammler, “High Performance Cutting (HPC) in the New Era of Digital Manufacturing – A Roadmap”, Procedia CIRP, 46, pp. 1-6, 2016.
[35] C. Emmer, K. Glaesner, A. Pfouga, J. Stjepandić, “Advances in 3D Measurement Data Management for Industry 4.0”, Procedia Manufacturing.; 11, pp. 1335-1342, 2017.
[36] V. Majstorovic, S. Stojadinovic, Z. Jakovljevic, S. Zivkovic, D. Djurdjanovic, J. Kostic et al, “Cyber-Physical Manufacturing Metrology Model (CPM3) – Big Data Analytics Issue”, Procedia CIRP, 72, pp. 503-508, 2018.
[37] F. Tao and Q. Qi, “Make more digital twins”, Nature Publishing Group, vol. 573, no. 7775, pp. 490–491, 26 Sept. 2019, https://www.nature.com/articles/d41586-019-02849-1.
[38] J. Autiosalo, J. Vepsäläinen, R. Viitala and K. Tammi, "A Feature-Based Framework for Structuring Industrial Digital Twins," in IEEE Access, vol. 8, pp. 1193-1208, 2020, doi: 10.1109/ACCESS.2019.2950507.
[39] 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.
[40] J. E. Siegel, S. Kumar and S. E. Sarma, "The Future Internet of Things: Secure, Efficient, and Model-Based," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2386-2398, Aug. 2018, doi: 10.1109/JIOT.2017.2755620.
[41] 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.
[42] F. Thiel, “Digital transformation of legal metrology - the European metrology cloud”, vol. LIX, no. 1, pp. 10-21, Jan. 2018.
[43] S. Hackel, F. H¨artig, J. Hornig, and T. Wiedenh¨ofer, “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
[44] S. Nakamoto, et al., “Bitcoin: A peer-to-peer electronic cash system”, 2008.
[45] S. Zhang, J. Hyouk Lee, “Analysis of the main consensus protocols of blockchain”, ICT Express, V. 6, I. 2, June 2020, pp. 93-97.

[46] F. Longoa, Letizia Nicoletti, A. Padovano, G. d'Atri, Marco Forte, “Blockchain-enabled supply chain: An experimental study”, Computers & Industrial Engineering 136, 2019, pp. 57-69, 2019.
[47] H. R. Hasan, K. Salah, R. Jayaraman, R. W. Ahmad, I. Yaqoob, and M. Omar, “Blockchain-Based Solution for the Traceability of Spare Parts in Manufacturing,” IEEE Access, vol. 8, pp. 100308–100322, 2020, doi: 10.1109/ACCESS.2020.2998159.
[48] T. Takatsuji, H. Watanabe, Y. Yamashita, “Blockchain technology to visualize the metrological traceability”, Precision Engineering, 58, pp.1-6, 2019.
[49] Takegawa N, Furuichi N., “Traceability Management System Using Blockchain Technology and Cost Estimation in the Metrology Field, Sensors, 23(3):1673, 2023. https://doi.org/10.3390/s23031673.
[50] Miličević K, Omrčen L, Kohler M, Lukić I. “Trust Model Concept for IoT Blockchain Applications as Part of the Digital Transformation of Metrology”, Sensors, 22(13):4708, 2022 https://doi.org/10.3390/s22134708.

[51] “WELMEC 7.2 Software Guide,” WELMEC European cooperation in legal metrology, 2015.
[52] D. Peters, J. Wetzlich, F. Thiel, and J. Seifert, “Blockchain applications for legal metrology,” in 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp. 1–6, May 2018, doi: 10.1109/I2MTC.2018.8409668.
[53] https://www.ibm.com/analytics/hadoop/big-data-analytics. Accessed on 17 Oct. 2021.
[54] https://enterprisersproject.com/what-is-digital-transformation. Accessed on 18 Oct. 2021.
[55] Metrology for the Digitalization of the Economy and Society, Report of the German Council of Science and Humanities, 2017.
[56] 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.
[57] M. S. Gadelrb, R. A. Abouhogail, “Towards a New Generation of Digital Calibration Certificate: Analysis and Survey”, Measurement 181, 2021, 109611.
[58] F. Thiel, M. Esche, F.G. Toro, A. Oppermann, J. Wetzlich, D. Peters,” The European Metrology Cloud, 18th International Congress of Metrology”, pp. 09001, 2017, https://doi.org/10.1051/metrology/201709001.
[59] “SmartCom Project: Communication and validation of smart data in IoT-networks”. https://www.euramet.org/research-innovation/search-research projects/details/project/communication-and-validation-of-smart-data-in-iot-networks/?L=0&tx_earametctcp_project%5Baction%5D=show&tx_earametctcp_project%5Bcontroller%5D=Project&cHash=2341e12363c8623088e97fd7acf8872c. (Accessed Oct. 10, 2021).
[60] “GEMIMeG Project,” Feb. 27, 2019. https://www.gemimeg.ptb.de/startseite/ (Accessed Oct. 26, 2021).
[61] “Met4FoF Project: Metrology for Factory of the Future.” https://www.euramet.org/research-innovation/search-research-projects/details/project/metrology-for-the-factory-of-the-

future/?L=0&tx_eurametctcp_project%5Baction%5D=show&tx_eurametctcp_project%5Bcontroller%5D=Project&cHash=575fbce9df841dc03cd08e8cc3099fff. (Accessed Oct. 10, 2021).

[62] CIPM Task Group on the Digital SI. [Online]. Available: https://www.bipm.org/en/committees/ci/cipm/wg/cipm-tg-dsi. Accessed 2 Nov. 2021.

[63] CIPM Task Group on the Digital-SI, Draft of the grand vision: transforming the international system of units for a digital world - version 3.4.

[64] M.D. Wilkinson, M. Dumontier, I.J. Aalbersberg, G. Appleton, et al., “The FAIR Guiding Principles for scientific data management and stewardship”, Sci Data 3, 160018, 2016, https://doi.org/10.1038/sdata.2016.18

[65] https://www.bipm.org/en/bipm-workshops/digital-si. Accessed on 17 Oct. 2021.

[66] Á. Arenas, G. Ray, Antonio Hidalgo, A. Urueña, “ How to keep your information secure? Toward a better understanding of users security behaviour”, Technological Forecasting and Social Change, Volume 198, , 2024, https://doi.org/10.1016/j.techfore.2023.123028.

[67] K. Barefoot, et al., Defining and Measuring the Digital Economy, vol. 15, US Department of Commerce Bureau of Economic Analysis, Washington, DC, 2018.

[68] Abdulkarim A. Oloyede, Nasir Faruk, Nasir Noma, Ebinimi Tebepah, Augustine K. Nwaulune, Measuring the impact of the digital economy in developing countries: A systematic review and meta- analysis, Heliyon, Volume 9, Issue 7, 2023, e17654, ISSN 2405-8440, https://doi.org/10.1016/j.heliyon.2023.e17654.

[69] R. Barabanov, S. Kowalski, L. Yngström, “Information Security Metrics: State of the Art: State of the art”, DSV Report series No 11-007, 25 May 2011.

[70] R. A. Abouhogail, "Network Security and Metrology", International Journal of Security and Its Applications, Vol.9, No.11, pp. 251-270, 2015.

[71] S., Reena, and R. S. Chhillar. "Novel Approach to Software Metrics." International Journal of Soft Computing and Engg 2.3,pp. 232-236, 2012.

[72] H. Noor, Dr. B. Hayat, A. Hamid, T. Wakeel, R. Nasim, “Software Metrics: Investigating Success Factors, Challenges, Solutions And New Research Directions”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, V. 9, I. 8, AUG. 2020.

[73] A V Kopyltsov, “Selection of metrics in software quality evaluation”, 2020 J. Phys.: Conf. Ser. 1515 032018.

[74] S. U. Farooq, S. M. K. Quadri, Nesar Ahmad, “Software Measurements and Metrics: Role in Effective Software Testing”, International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 1 Jan 2011, pp. 671-680.

[75] B. Ma, Pin Lu, Xiaohui Mao, Yu Shen, “SOFTWARE CHECK OF MEASURING INSTRUMENT ACCORDING TO WELMEC AND OIML FILES”, Metrology for Green Growth, Sept. 9-14, 2012, Busan, Republic of Korea

[76] OIML D31: General requirements for software controlled measuring instruments, 2019.

[77] J-F Scariot, Be Martinet, "NetSEC: metrology-based application for network security", Future Generation Computer Systems, Vol. 19, pp.303–311, 2003.

[78] R. Abdellatif Abouhogail, “New Multicast Authentication Protocol for entrusted members using advanced encryption standard”, the Egyptian Journal of remote sensing and space sciences, 16 Dec 2011.

[79] R. Abdellatif Abouhogail, "Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks", International Journal of Security and Its Applications, of Security and Its Applications, Vol.8, No.5, pp.361 -376, 2014.
[80] IEEE 802.16 Work Group, IEEE standard 802.16m-2011, "Air interface for broadband wireless access systems amendment 3: advanced air interface", Tech. Rep. IEEE; May 2011.
[81] A. Fu, Yuqi ng Zhang, Zhenchao Zhu, Qi Jing, Jingyu Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network", Computers and Security, pp.741-749, June 2012.
[82] M.S.Arun, V.Saminathan, " Parallel AES Encryption with Modified Mix-columns For Many Core Processor Arrays", International Journal of Engineering Science and Innovative Technology (IJESIT)Vol. 3, Issue 3, May 2014.
[83] J. Van Dyken, Jose G. Delgado-Frias, "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm", Journal of Systems Architecture (JSA), Vol. 56, pp.116-123, 2010.
[84] http://www.xilinx.com/training/fpga/fpga-field-programmable-gate-array.htm.
[85] R. A. Abouhogail, " Improving the Handoff Latency of the Wireless Mesh Networks Standard", International Journal of Security and Its Applications, vol.10, 5, pp.73 -86, 2016.
[86] R. A. Abouhogail, M. S. Gadelrb, "A New Secure and Privacy Preserved Protocol for IEEE802.11s Networks", Computers & Security, 77, pp.745-755, Aug. 2018.
[87] Robert K. Cunningham, "Why Measuring Security Is Hard", IEEE Security and Privacy Magazine 8(4), pp. 46-54, July 2010.
[88] S. V. Mallapur, and Siddarama R. Patil," A Novel Approach Of Simulation Tools For Mobile Ad-Hoc Networks",IJCSC, vol. 3, 1, January-June, pp. 1-10, 2012.
[89] E. Ahmed, R. A. Abouhogail, A. Yahya, "A Comparison Study of Currently Used Network Simulators", Al-Azhar Engineering Thirteenth International Conference. Dec. ,2014.
[90] H. Singh and M. Singh, "Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs", International Journal of Advanced Trends in Computer Science and Engineering, vol. 2, 3, 2013, May-June.
[91] Bruce Schneier, Applied Cryptography, John Wiley& Sons, Inc, 1994.
[92] Reham Abdellatif Abouhogail, "A Comparative Analysis of Tools for Testing the Security Protocols", I.J. Information Technology and Computer Science, pp. 30-37, 12 Dec. 2019.
[93] R. A. Abouhogail, " Improving the Handoff Latency of the Wireless Mesh Networks Standard", International Journal of Security and Its Applications, Vol.10, 5, pp.73 -86, 2016.
[94] A. H. Ali, R. A. Abouhogail, I. F. Tarrad and M. I. Youssef, "A new design of Mobile Payment system based on NFC Technology", International Journal of Engineering & Technology IJET-IJENS vol. 17, 3, pp.7-18, June 2017.
[95] R. A. Abouhogail, M. S. Gadelrb, "A New Secure and Privacy Preserved Protocol for IEEE802.11s Networks", Computers & Security, pp.745-755, Aug. 2018.
[96] R. A. Abouhogail, "A New Secure Lightweight Authentication Protocol for NFC mobile Payment", International Journal of Communication Networks and Information Security (IJCNIS), vol. 11, 2, pp. 283-289, August 2019.
[97] R. A. Abouhogail, A. H. Ali, "Design and Development of an Advanced Authentication Protocol for Mobile Applications using NFC Technology", Journal of Computer Science, 15(12), pp. 1809-1819, Dec. 2019, DOI:10.3844/jcssp.2019.1809.1819

[98] R. A. Abouhogail, "A New Efficient Authentication Protocol for Wireless Healthcare Sensor Networks", International Journal on Engineering Applications (IREA), vol. 8, 5, pp. 277-285, Sept.2021.

[99] A. H. Ali, R. A. Abouhogail, I. F. Tarrad and M. I. Youssef "Assessment and Comparison of Commonly used Wireless Technologies from Mobile payment Systems Perspective", International Journal of Software Engineering and Its Applications, Vol.8, No.2, pp.255-266, Jan 2014.

[100] AIME Planning Team, "Artificial Intelligence Measurement and Evaluation at the National Institute of Standards and Technology", NIST, June 14, 2021.

[101] A. Lazzari, Jean-Michel Pou, C. Dubois, and L. Leblond, "Smart metrology: The importance of metrology of decisions in the big data era", IEEE Instrumentation and Measurement Magazine, pp. 22-29, Dec. 2017.