ILNAS

UNIVERSITÉ DU LUXEMBOURG

Technical Reports

SMART ICT: GAP ANALYSIS BETWEEN SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION

JOINT RESEARCH PROGRAMME UNI.LU/SnT-ILNAS:
"TECHNICAL STANDARDIZATION FOR TRUSTED USE IN THE FIELD OF SMART ICT"

Version 1.0 · October 2019

ANEC

SnT
securityandtrust.lu

Technical Reports

SMART ICT: GAP ANALYSIS BETWEEN SCIENTIFIC RESEARCH AND TECHNICAL STANDARDIZATION

JOINT RESEARCH PROGRAMME UNI.LU/SnT-ILNAS:
"TECHNICAL STANDARDIZATION FOR TRUSTED USE IN THE FIELD OF SMART ICT"

Version 1.0 · October 2019

ILNAS
Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services

ANEC
Agence pour la Normalisation et l'Economie de la Connaissance

uni.lu | SnT
securityandtrust.lu

ACKNOWLEDGEMENTS

The working-group (WG) involved to prepare these technical reports is:

Name of the Contributor	Role	Institution Organization
Prof. Dr. Pascal Bouvry	Chargé de Mission auprès du Recteur	University of Luxembourg
Dr. Grégoire Danoy	Research Scientist	University of Luxembourg
Dr. Matthias R. Brust	Research Associate	University of Luxembourg
Dr. Muhammad Umer Wasim	Postdoctoral Researcher	University of Luxembourg
Ms. Saharnaz Dilmaghani	Doctoral Researcher	University of Luxembourg
Mr. Nader S. Labib	Doctoral Researcher	University of Luxembourg
Mr. Chao Liu	Doctoral Researcher	University of Luxembourg
Dr. Jean-Philippe Humbert	Deputy Director	ILNAS
Mr. Nicolas Domenjoud	Responsible ICT and Technical Standardization	ILNAS – National Standards Body
Ms. Natalia Cassagnes	Project Officer	ANEC G.I.E.
Dr. Shyam Wagle	Project Officer	ANEC G.I.E.
Dr. Jean Lancrenon	Project Officer	ANEC G.I.E.
Dr. Johnatan Pecero	Head of Standardization Department	ANEC G.I.E.

This work is funded by the joint research program "Technical Standardization for Trusted Use in the Field of Smart ICT" between ILNAS and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg.

TABLE OF CONTENTS

INTRODUCTION

The Information and Communication Technologies (ICT) sector is present in almost every aspect of society. It is strongly supporting the development of other sectors and allowing the creation of new business models contributing to the transition of the traditional economy to a digital one. Services, products and processes are being digitalized offering advanced capabilities and flexible solutions in a smart way reducing overall costs and environmental impacts. New Smart ICT platforms and technologies like Cloud Computing, Internet of Things (IoT), and Artificial Intelligence and advanced analytic contribute to this digitalization. However, the wide spread adoption of such Smart ICT platforms and technologies have resulted in a situation where the amount and variety of data that are being generated and processed are higher than ever before.

The value of data is huge, but capturing this value is complex. Data can contain personal identification information that directly concerns and compromises the private lives of individuals. Therefore, protecting this data is critical, and it is essential to ensure a high level of security and privacy in order to support the wide acceptance for, and trust in, Smart ICT. The data economy brings increasing opportunities for innovation and growth, and at the same time, many challenges and issues are open.

Researchers, as well as Standards Development Organizations (SDOs) are actively working on the development of techniques and good practices to tackle a part of these challenges and improve the trustworthiness of Smart ICT. However, gaps exist between scientific developments and technical standardization. For the benefit of society and economy, it appears essential to better link these works, which will allow, on one hand, for the research domain to take into account the last developments of the common technical language (technical standardization), and on the other hand to guarantee the integration of the latest knowledge (to disseminate valuable research results) into standards.

These technical reports provides gap analyses between research and technical standardization in three Smart ICT domains, namely Cloud Computing, Internet of Things, Artificial Intelligence and Big Data mainly on Data Privacy and Protection. This work extends the White Paper "Data Protection and Privacy in Smart ICT"[1] published in October 2018 and provides new results of the common research program "Technical Standardization for Trusted Use in the Field of Smart ICT"[2] between ILNAS and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg.

The first report focuses on Cloud Computing. It introduces state-of-the-art scientific developments and current standardization activities. In that context, it provides first an overview of recent scientific research directions on data protection and privacy in order to explore the needs from a researcher's perspective. After that, it gives a general overview of standardization efforts. Security and privacy controls in cloud, inherent properties of cloud, data storage and processing in the cloud, metering, billing and pricing aspects are the benchmarks used to carry out the gap analysis. The outcome of this study is to offer new insights and make contributions to narrow the gaps for future research and technical standardization efforts.

The second report deals with Internet of Things (IoT). The goal of this study is to first introduce the concept of trustworthiness in IoT with its main pillars, data protection, privacy and security, and then analyze developments in research and standardization for each of these. The study presents a gap analysis on data protection, privacy and security between research and standardization, throughout which the use case of Unmanned Aerial Vehicles (UAVs) is referred to, as a promising value-added service example of mobile IoT devices. The study concludes with suggestions for future research and standardization in order to address the identified gaps.

[1] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/White-Paper-Data-Protection-Privacy-Smart-ICT-october-2018.pdf

[2] https://smartict.gforge.uni.lu/

The third report concerns Artificial Intelligence. The main contributions of this study are threefold: 1) It provides a survey and analysis on data protection, privacy, and trustworthiness challenges of AI and Big Data based on the state-of-the-art research. 2) It presents a survey of standardization and the activities of SDOs for the data protection, privacy, and trustworthiness of AI. 3) It carries out a gap analysis considering both perspectives to identify and highlight the gaps such that business sectors, industries, and governments can adopt secure, and trustworthy AI.

1. Cloud Computing: Gap Analysis between Scientific Research and Technical Standardization

Technical Report on Data Protection and Privacy in Smart ICT

Abstract

Cloud computing enables end-users to access unlimited amounts of resources and services using a pay-per-use paradigm. For cloud service providers, how to protect the customers' data and privacy is a competitive and key issue which requires complex prospective considerations, including constant attention and adaptation to the market. Cloud computing involves a wide range of technical and business elements. The targets of cloud computing standardization are diverse and many standards organizations are studying cloud computing based on their expertise. This study introduces the current standardization activities and research efforts for cloud computing and conducts a systematic study to find out the current standard initiatives by different Standard Development Organizations (SDOs). This study aims at providing gap analysis between research works and technical standardization efforts for the data protection and privacy issues in cloud computing. The outcome of this study is to offer new insights and to make contributions to narrow the gaps for future research and technical standardization efforts.

1.1. Introduction

Cloud computing is a type of Internet-based computing that provides shared computer processing resources, data storage and processing facilities to users, with various capabilities to access, store and process their data in local or third-party data centers that may be located far from the user - sometimes even across the world. Cloud computing has been defined in [1] as "a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand."

The National Institute of Standards and Technology (NIST) defined framework [2] for cloud computing with its list of essential characteristics has by now evolved into the de facto standard for defining cloud computing. Based on the NIST definition, an extended version has been developed in the first international standard ISO/IEC 17788:2014/ITU-T Y.3500 (08/2014) Cloud computing - Overview and vocabulary [49] by the international subcommittee on technical standardization ISO/IEC JTC 1/SC 38 on Cloud Computing and Distributed Platforms. Over recent years, cloud computing attracted more attention due to a number of benefits mainly including cost savings, accessibility and high availability.

The most important benefit of the cloud usage model is a significant reduction in costs, primarily due to the elimination of the requirement for capital investment in infrastructure. Enterprises pay for computing and storage capacity as needed (on-demand) with no necessity for in-house equipment hosting. The users can access their data from anywhere at anytime if they have an Internet connection. The update of data on the cloud is in real-time. Compared with self-hosted IT infrastructure, cloud computing can be much more reliable with high availability guarantees (Easy Software Updates, Scalability, Manageability, Mobility, etc.) specified in the service level agreement from the service provider.

The main contributions of this study are: firstly, introducing the trust and security challenges in cloud computing aspects; secondly, summarizing the recent research directions and efforts on data protection and privacy in cloud computing in order to explore the needs from researchers' perspective. After that it gives a general overview of standardization (formal) efforts which addresses data protection and privacy in cloud computing, mainly. Finally, it presents an analysis of gaps between research and standardization, limited to the scope of this study, which aims to offer insights to narrow the gaps and build a bridge to accelerate the promotion of cloud computing business models and provide a standardized, trusted cloud environment.

The rest of this study is organized as follows: Section 1.2 describes the multiple definitions of trust and recent security challenges in cloud computing. Section 1.3 introduces the current research directions of solutions to privacy and data protection issues in cloud computing. Section 1.4 presents the overview of standardization works, which relate to cloud computing under different SDOs' perspective. Then, Section 1.5 presents a gap analysis between research and standardization. Section 1.6 explores this study with insights and recommendations based on the gap analysis in Section 1.5. Section 1.7 emphasizes the efforts put forth in Luxembourg to foster the collaboration between research and standardization. Finally, section 1.8 summarizes the study.

1.2. Trust challenges in Cloud Computing

It is critical to establish the trust relationship between the cloud service provider and users, because trust promotes successful business relationships. The definition of trust is, however, rather complex. Broadly, trust means firm belief, mutual dependency and strong confidence. Trust has been studied from different scenarios. Trust in Information Technology artifacts based on human characteristics is defined by Wang and Benbasat in [3] as "an individual's beliefs in an agent's competence, benevolence, and integrity". Knight et al. in [4] delineate trust in IT artifacts based on system characteristics as reflecting "beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible". Lee and See in [5] specify trust in automation technology as "the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability". Although cloud computing has many advantages, like on-demand self-service and ubiquitous network access for scalable computational resources, cloud users will lose control over their data, since they do not even know where it is stored. This kind of non-transparency in cloud computing brings resistance in the market and hinders the wide acceptance of cloud computing services. Based on the fundamental characteristics (on-demand self-service, broad network access, multi-tenancy and resource pooling, rapid elasticity and scalability, measured service) of cloud computing, the essential concerns from the cloud user's perspective is where their data is stored, and how to deny unauthorized users access to data. This includes 1) the protection of the data from direct data breaches, and 2) the managed but possibly unauthorized sharing to third parties. Accordingly, the involvement of trust mechanisms in cloud computing becomes a primary consideration for the potential users to choose and migrate to such a service [6], [7].

According to a recent report from the Cloud Security Alliance [8], there are 11 top threats cloud users are currently concerned about in terms of security and privacy:

1) *Data Breaches*: According to the newest report from the CSA, data breaches have become the main target of cyber attacks. Encryption technology can help for data protection, but it can also bring negative impacts on the system's performance while reducing the user-friendliness of the application.

2) *Misconfiguration and inadequate change control*: Some examples of misconfigurations include: unsafe data storage elements or containers, excessive permissions, unaltered default credentials and configuration settings, disabled standard security controls, unpatched systems, and disabled logging or monitoring, and unrestricted access to ports and services.

3) *Lack of cloud security architecture and strategy*: One of the biggest challenges for users who choose to migrate to the public cloud is to implement appropriate security measures to protect against cyber-attacks. Public cloud providers should give top priority to providing migration tools to help perform these migrations quickly and cost-effectively with security guarantees.

4) *Insufficient identity, credential, access and key management*: Insufficient authentication and credentials or poorly managed keys can lead to catastrophic damage for all parties if unauthorized data access behavior occurs.

5) *Account hijacking*: The confidentiality, integrity, and availability of services are jeopardized by hijackers.

6) *Insider threat*: An insider (such as a system administrator) with malicious intentions can ultimately access sensitive information and confidential data. Systems that rely solely on cloud service providers to provide security measures are bound to face greater security risks.

7) *Insecure interfaces and APIs*: Generally, the security and availability of cloud services depend on the API. Those interfaces must be pre-designed to prevent accidental and malicious attempts to bypass security.

8) *Weak control plane*: A weak cloud control plane means that the cloud service provider cannot fully control the security and verification of the data infrastructure. The cloud service provider does not provide sufficient security controls to meet customers' security requirements.

9) *Meta-structure and applications failures*: Meta-structures and applications are key components of cloud services. There are multiple levels of potential failures in the meta-structure and application structure models.

10) *Limited cloud usage visibility*: Limited cloud usage visibility occurs when cloud security controls fail to keep up with the fast pace of enterprises that have adopted cloud computing.

11) *Abuse and nefarious use of cloud services*: Inadequate deployment of cloud services, free cloud service trials, and fraudulent account logins through payment instrument fraud will expose cloud computing models to malicious attacks.

The security in cloud computing is not only the primary consideration for users to choose cloud services, but also the basis for cloud computing to achieve the sustainable development. Service providers and users should reach a consensus on providing and monitoring security functions to cope with the threats in cloud computing.

1.3. Current Research Directions in Cloud Computing

In this section, an overview of the research directions for data protection and privacy in cloud computing is given. To assess the status of research developments for data protection and privacy in cloud computing, we summarize the recent research efforts following the challenges [9] in cloud computing based on the benchmarks*: Security and privacy controls, inherent properties, data storage and process and billing and metering*.

1.3.1. Security and Privacy Controls in the Cloud

Based on the characteristics of *ubiquitous network access* of cloud computing, the main task of access control is to export digital identities of end users and transfer the identity attributes to different computers to guarantee a secure environment for users. Consider a specific scenario where users' data is stored and handled by a trusted service provider, it is necessary to take actions to make sure that all this data is under control and uninterrupted. Access control mechanisms are very important to reduce the risks of information leakage, no matter if intentionally or by accident, for the fact that multiple cloud users share the same cloud infrastructure for data storage and processing.

Storing user data at a cloud data center greatly relieves the storage burden of user devices and brings access convenience. Due to distrust in cloud service providers, users generally store their crucial data in encrypted form. However, in many cases, the data needs to be accessed by other entities for fulfilling an expected service, e.g., an eHealth service. How to control personal data access on the cloud is a critical issue.

Various application scenarios request flexible control on cloud data access based on data owner policies and application demands. Either data owners or some trusted third parties (cloud partners) should participate in the process for access control. However, existing work could not propose an effective and flexible solution to satisfy this demand. On the other hand, trust plays an important role in data sharing. It helps overcome uncertainty and avoid potential risks. Still, research lacks a practical solution to control cloud data access based on trust and reputation. A personal access control mechanism for cloud data access from mobile devices, which based on social trust has been proposed in [11]. In [14], the authors have explored how to achieving secure, scalable, and fine-grained data access control with highly efficient in cloud computing. In [10], a scheme to control data access in cloud computing is proposed which is based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers in a flexible manner by applying attribute-based encryption [12] and proxy re-encryption [13].

1.3.2.Inherent Properties of Cloud Computing

According to the NIST definition, and based on the ISO/IEC 17788:2014/ITU-T Y.3500 (08/2014) international standard, the cloud computing paradigm enables multi-tenancy, i.e. multiple cloud users share the virtualized resources and the physical devices. Multi-tenancy can improve the efficiency of resource utilization through resource sharing, meanwhile, how to guarantee the security among different tenants is one of the critical challenges on public clouds. For example, an attacker just needs to get the access to one virtual machine, to be able to attack all the virtual machines, which are hosted on the same physical machine. The dynamic of multi-tenancy further intensifies the complexity and brings more security challenges. In [19], the authors propose a secure multi-tenant application model which can reduce security risks and protect tenants' sensitive data for the application in Software-as-a-Service. In [20], Jouini and Rabai address security issues in cloud computing using a quantitative security risk assessment model and conducting through a generic framework which is called Multi-dimensional Mean Failure Cost (M2FC).

1.3.3.Data Storage and Processing in the Cloud

The privacy and data security issues are the important challenges for cloud applications. The main concern for security from the users' side is about that the cloud service provider has access to their sensitive data, especially for hospitals or the financial industry. In [23], Li and Keke propose a new smart approach for cryptography. In this case, the cloud service provider could not access the sensitive data directly but an intelligent cryptography approach divides users' data and stores them in distributed cloud services. Under the paradigm of cloud computing, a third party service provider is allowed to offer clients a database service on the cloud through Database-as-a-Service. Database outsourcing also bring challenges for privacy issues due to the loss of data control at the physical level from the owner of data. Searchable symmetric encryption (SSE) [24] was first proposed to guarantee and cope with sensitive privacy challenges. Researchers have made a lot of effort to develop SSE solutions [26], [25].

1.3.4.Data Protection and Privacy in Pricing

During the procedure of building a pricing strategy for a cloud service provider, a monitoring system will be typically used for collecting users' data in order to evaluate their pricing model. The third parties could have the chance to touch users' sensitive data and lead to information leakage. This concern creates a need for transparent metering indicators and billing principles.

Cloud services rely on the "pay-as-you-go" model, but most cloud services providers collect the users' history data for analyzing users' requirements to improve their revenues. During the data collection procedure, risks for users' data protection and privacy issues are involved.

In [27], the authors propose a real-time usage-based dynamic pricing (UDP) scheme, which jointly considers the privacy of customers by restricting the disclosure of individual usage. Li et al. proposed a pricing method for personal data stored in the cloud, which takes into account the potential privacy risks in [32].

The problem of large-scale resource congestion from the control and regulation point of view has been investigated in [30]. User behavior usually leads to an unfair distribution of work between nodes. A novel macro-scheduling (long-term and system-wide) mechanism with a set of mechanisms for self-regulation of resources to ensure that work is distributed in a fair and stable way, has been proposed in [30]. Pal and Hui in [31] proposed an economic model with game theory in order to fix the prices for resources.

Aspect	Top threat	Research effort
Security and Privacy Controls in the Cloud	Lack of cloud security architecture and strategy	Attribute-Based Encryption [12] Proxy Re-Encryption [13]
	Misconfiguration and inadequate change control	A scalable distributed monitoring system [15]
	Insufficient identity, credential, access and key management	Efficient credentials management [17]
	Account hijacking	Multi-factor authentication [18]
	Abuse and nefarious use of cloud services	RBAC (Role-based access control) [16]
Inherent Properties of Cloud Computing	Weak control plane	Multi-dimensional Mean Failure Cost [20]
	Metastructure and applistructure failures	Multi-dimensional Mean Failure Cost [21]
	Insecure interfaces and APIs	The Open Services Gateway Initiative service platform [22]
Data Storage and Processing in the Cloud	Data Breaches	Intelligent cryptography approach for secure distributed big data storage [23]
	Insider threat	Enabling users to define transparency policies over their data [28]
	Limited cloud usage visibility	Fuzzy authorization for Cloud storage [29]

Table 1: Top threats and corresponding research efforts

1.4. Technical Standardization

1.4.1. Overview

A standard is a kind of normative document that is approved by a recognized organization for all parties to jointly reuse, and which aims at obtaining the optimum degree of order in society and the economy within a certain range [33]. This is the common definition given by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU).

Standards are approved by recognized Standards Developing Organizations (SDOs) at different levels, mainly, in a consensus basis. Some of these SDOs are officially recognized by regulation systems as providers of standards. They publish standards when a specific societal need is identified. Recognized, official, SDOs have robust and documented process for building consensus and approving standards.

In addition to the official recognized SDOs, there are well-respected and well-known, long-existing SDOs that are not officially recognized by regulation systems, but also have well-defined and established procedures to ensure the quality of their standards. At the international level, the most recognized international standards organizations are ISO, IEC and ITU. Up to now, the three major international standards organizations have released more than 32,000 international standards, which have been widely adopted all over the world, and play an important and strategic role in fostering global economic growth and promoting scientific and technological progress. ISO/IEC JTC 1 is a joint technical committee formed between ISO and IEC on information technology issues for business and consumer applications.

At the European level, regional standards are adopted and released by regional standardization organizations. The European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) are the formal standards organizations which have been recognized by the European Union officially.

At the national level, the *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS) is the formal standards body for Luxembourg. Within ISO and IEC, each committee member has one vote. Therefore, all countries have the same decision weight.

In parallel, there are also private standards bodies - Individuals, associations, and companies (such as the Cloud Security Alliance, or CSA), Open Grid Forum (OGF), the Organization for the Advancement of Structured Information Standards (OASIS), European Computer Manufacturer's Association (ECMA). Those standardization organisms are established by industries that coordinate their efforts on specific subjects to promote, accelerate or complement the development of a standard.

Over the last few years, many companies have migrated a part of their business to the cloud. The increasing demand for transparency, coherence, and effectiveness in cloud computing domains has created a huge demand for technical standards. The standards bodies such as ITU-T, and ISO/IEC JTC 1 or the Institute of Electrical and Electronics Engineers (IEEE) started making contributions to the standardization of cloud computing in 2009.

Based on the involvement of various technologies in cloud computing, the goal of standardization in cloud computing is also diverse. Different standards bodies have different targets and focus, which makes it difficult to accurately define which issues are covered by each organization. However, in the context of this study, we broadly divide the current standardization activities in cloud computing domain into the following areas:

1) Architecture, framework development, use cases;
2) Cloud configuration management, service management, security;
3) Cloud communication, cloud API's, cloud broker.

Fig.1 shows the main relevant standardization activities under different areas in cloud computing according to this study.

1.4.2.Related committees

Within a given standards body, work is divided among Technical Committees (TCs). The TC is a technical group for a certain field that takes charge of the drafting and development of standards. There are sub-technical committees (SCs) and working groups (WGs) under TCs.

Some of the relevant SDO technical standardization and working groups are involved in the cloud computing standards development. The principal international subcommittee and major proponent developing standards on cloud computing is the ISO/IEC JTC 1/SC 38 – Cloud Computing and Distributed Platforms. Working group 3 in ISO/IEC JTC 1/SC 38 focuses on Cloud Computing Fundamentals (CCF), meanwhile working group 5 is

working on the area of data in cloud computing and related technologies. Additionally, CG 1, CG 2, and CG 3 are liaison coordination groups for JTC 1/SC 27, JTC 1/SC 41, and JTC 1/SC 42 respectively. Regarding standards dealing with security, privacy and data protection issues the ISO/IEC JTC 1/SC 27 – Information security, cybersecurity and privacy protection is one of the most important subcommittee developing standards. . For ISO/IEC JTC 1/SC 27, the most important working group dealing with part of the standardization work in the cloud computing domain is WG 4 Security controls and services.

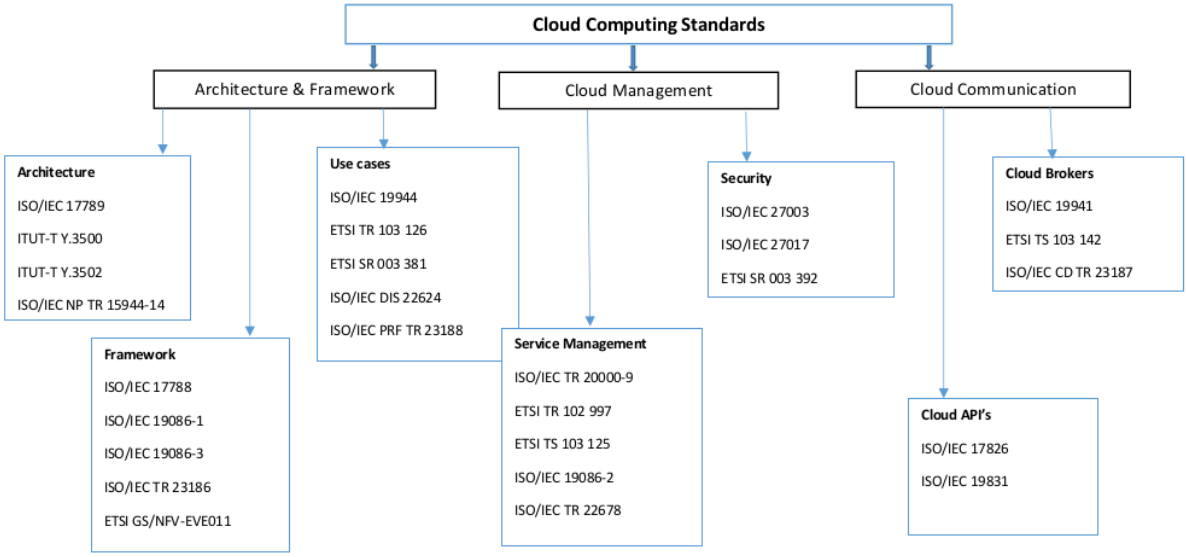

Fig. 1: Major standardization activities in cloud computing

The recently published standardization works which address data protection and privacy in cloud computing are listed in Table 2. An exhaustive list can be found in [9].

SDO	Reference	Title
ITU-T	ITU-T Y.3500 (08/2014) [1]	Information technology Cloud computing Overview and vocabulary
ITU-T	ITU-T Y.3502 (08/2014) [50]	Information technology Cloud computing Reference architecture
ISO/IEC JTC 1	ISO/IEC 19086-1:2016 [51]	Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts
ISO/IEC JTC 1	ISO/IEC 19086-2:2018 [52]	Cloud computing – Service level agreement (SLA) framework – Part 2: Metric mode
ISO/IEC JTC 1	ISO/IEC 19086-3:2017 [53]	Cloud computing – Service level agreement (SLA) framework – Part 3: Core conformance requirements
ISO/IEC JTC 1	ISO/IEC 19086-4:2019 [54]	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
ISO/IEC JTC 1	ISO/IEC 17788:2014 [49]	Cloud computing –Overview and vocabulary
ISO/IEC JTC 1	ISO/IEC 19941:2017 [55]	Cloud computing – Interoperability and portability
ISO/IEC JTC 1	ISO/IEC 19944:2017 [56]	Cloud computing – Cloud services and devices: Data flow, data categories and data use

SDO	Reference	Title
ISO/IEC JTC 1	ISO/IEC 27018:2019 [57]	Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC JTC 1	ISO/IEC 27036-4:2016 [58]	Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services
ETSI	ETSI TR 102 997 V1.1.1 (04/2010) [59]	CLOUD; Initial analysis of standardisation requirements for Cloud services
ETSI	ETSI TS 103 125 V1.1.1 (11/2012) [60]	CLOUD; SLAs for Cloud services
ETSI	ETSI SR 003 381 V2.1.1 (02/2016) [61]	Cloud Standards Coordination Phase 2; Identification of Cloud user needs
ETSI	ETSI SR 003 391 V2.1.1(02/2016) [62]	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing

Table 2: Published standards in cloud computing

1.4.3.Published and Under-Development Standards

In this section, some published standards by the recognized SDOs regarding cloud computing are listed. An exhaustive list can be found in [9]. ISO/IEC JTC 1/SC 38 has published 15 standards, ITU-T released 3 fundamental standards for cloud computing, and ETSI already published 7 standards. Currently, there are 9 standardization projects under development under the responsibility of ISO/IEC JTC 1/SC 38. Table 2 shows the main part of the published standards which are related to cloud computing and Table 3 shows the ongoing standardization projects under ISO/IEC JTC 1/SC 38.

Technical Committee	Standard Reference	Title
ISO/IEC JTC 1 SC 38	PDTS 23167 [63]	Information Technology – Cloud Computing – Common Technologies and Techniques
ISO/IEC JTC 1 SC 38	NP TR 23187 [64]	Information technology – Cloud computing – Interacting with cloud service partners
ISO/IEC JTC 1 SC 38	PTDR 23188 [65]	Information technology – Cloud computing – Edge computing landscape
ISO/IEC JTC 1 SC 38	NP TR 23951 [66]	Cloud computing – Best practices for cloud SLA metrics
ISO/IEC JTC 1 SC 38	19944:2017/PD AM 1 [67]	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – Amendment 1
ISO/IEC JTC 1 SC 38	DIS 22624 [68]	Information technology – Cloud Computing – Taxonomy based data handling for cloud services
ISO/IEC JTC 1 SC 38	AWI 23751 [69]	Information technology – Cloud computing – Data sharing agreement (DSA) framework
ISO/IEC JTC 1 SC 38	CD 22123 [70]	Information technology – Cloud computing – Concepts and terminology
ISO/IEC JTC 1 SC 38	PTDR 23613 [71]	Information technology -Cloud service metering and billing elements

Table 3: Cloud computing under development standards

1.5. Gap Analysis

In this section, a gap analysis between cloud computing research and technical standardization developments which addresses data protection and privacy in cloud computing is discussed following the content of Sections 1.3 and 1.4. The main purpose of this gap analysis is to assess the current gaps between research and technical standardization efforts then provide recommendations that contribute to narrow the gaps between the theoretical work and the requirements from the market.

To evaluate the current state-of-the-art of research and technical standardization for data protection and privacy in cloud computing, security and privacy controls in the Cloud, inherent properties of cloud computing, data stored and processed in the Cloud, and metering and billing for cloud service were chosen as the basic aspects for comparison.

1.5.1. Security and Privacy Controls in the Cloud

Security and privacy controls in the cloud include access control and policy management. The main challenges in security and privacy control are how to guarantee that access is offered only for authorized customers, data leakage prevention, auditing and proof of compliance.

Current research efforts which address cloud security and privacy have still been unable to provide a practical solution to control cloud data access based on trust and reputation. To cope with the above challenge, a scheme to control data access in cloud computing based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers has been proposed in [10]. Establishing trust mechanisms is one of the main objectives for standardization efforts. In [34], [35], [36], [37], [38], researchers have already made contributions to build the trust mechanisms between service provider and users, and among different service providers. Jincui and Liqun et al. in [37], [38] proposed an integrated trust mechanism to guarantee the security of data sharing. Meanwhile, trust is also a key component for technical standards. For cloud service providers, if their trust mechanisms can be certified by international standards that will increase the attractiveness and bring more confidence for users to trust the service. The security of cloud service providers can be certified by ISO/IEC 27001 – Information security management [72]. ISO/IEC 27018:2019 provides guidance aimed at ensuring that cloud service providers offer suitable information security controls to protect the privacy of their customers' clients by securing Personally Identifiable Information entrusted to them. The standard sets "commonly accepted control objectives, controls and guidelines for implementing measures" to protect PII information, and any "information that can be used to establish a link between the information and the natural person to whom such information relates". Furthermore, ISO/IEC 27017:2015 provides cloud-specific guidance on security controls based on ISO/IEC 27002. ISO/IEC 19086-4:2019 refer to the Security and Protection of PII components. This standard complements the work on Service Level Agreement related to the security and privacy metrics. ISO/IEC TR 23186:2018 Information technology – Cloud computing – Framework of trust for processing of multi-sourced data [73], mainly describes the trust framework for handling multi-source data including data usage obligations and controls, can be used for building the information security mechanism of cloud service providers.

Related Under-development Standardization: ongoing efforts related to trust in cloud computing in SC 38 or in SC 27 have been identified. This is particularly true for more sophisticated forms of cryptography (e.g. attribute-based encryption [12], Proxy re-encryption [13], etc). Proxy re-encryption is a kind of cryptographic technique allowing third parties to re-encrypt a ciphertext. The current proxy re-encryption schemes sometimes do not guarantee the property of being non-transferable. Proxy re-encryption has specific needs for data dissemination control. A major technical committee working group that works on cryptography is ISO/IEC JTC 1/SC 27/WG 2 "Cryptography and security mechanisms".

1.5.2.Inherent Properties of Cloud Computing

Due to the inherent multi-tenancy and virtualization properties of cloud computing, data protection and privacy challenges arise in virtualization (in multi-tenancy an attacker having access to a virtual machine deployed on a given physical machine could compromise other VMs hosted on the same physical machine), secure service provisioning and composition (service providers and integrators need to collaborate for newly composed services).

For cloud computing users, in the case they would like to switch cloud service providers, they need to transfer their application to a new cloud service provider. During such a procedure, the interoperability among cloud service providers should be managed. Without technical standards to address the interoperability, the movement between different cloud service providers will be limited.

Technical standards are making contributions on identity sharing among different cloud providers. The international standard ISO/IEC 19941 Information technology – Cloud computing – Interoperability and portability has been published in 2017 which aims to facilitate interoperability by establishing standardized terminology. The recent research work mainly focused on the solution for interoperability in order to solve the current fact that there are no standardized communication interfaces, protocols, etc. All this work contributes to ensuring a secure environment for interoperation.

Research and standardization efforts are both focused on communication, which aims at providing secure interoperability in the cloud. The research efforts in [39], [40], [41], [42] address the implementation of interoperation under the policy management framework. Furthermore, international standard ISO/IEC 19941 offers guidance to facilitate interoperability and portability under a standardized terminology.

Related Under-development Standardization: ISO/IEC CD TR 23187 Information technology – Cloud computing – Interacting with cloud service partners [64]. In the cloud service environment, cloud service customers, cloud service providers and cloud service partners (e.g., cloud service brokers, cloud service developers and cloud auditors) are three key roles. The interactions between cloud service customers and cloud service providers have been introduced in detail in ISO/IEC 17789:2014, and the ISO/IEC 19086-x series. The interactions among cloud service partners, cloud service customers, cloud service providers have not been explored and described in detail. The main objective of CD TR 23187 [64] is to (1) describe the interactions between cloud service partners and cloud service customers, (2) describe the interactions between cloud service partners and cloud service providers, and (3) provide guidance on how to use cloud service agreements and cloud service level agreements to build more clarity for cloud service partners interactions.

1.5.3.Data Storage and Processing in the Cloud

In the procedure of data stored and processed in the cloud, there are three main aspects related to data protection and privacy: (1) sensitivity of information, (2) confidentiality, integrity and availability of data, and (3) data storage and transfer locations. For sensitive information, the main challenge is the lack of user control over cloud resources while users' data is stored and processed in cloud.

For confidentiality, integrity and availability of data, the main challenges are security and privacy of data and the frequent outages reported on well-known cloud service providers [43]. For data storage and transfer locations, the challenge is coping with the high distribution of cloud infrastructures and the limitation of certain data protection and privacy laws that apply in specific jurisdictions [44].

In fact, there is much legal uncertainty about privacy rights in the cloud and it is hard to predict what will happen when existing laws are applied in cloud environments. It is difficult to keep track of what resources are used and in which country. Furthermore, it is not clear which party is responsible for ensuring that legal requirements for personal information are observed, or appropriate data handling standards are set and followed.

Governments in the countries where the data is processed or stored may even have legal rights to view the data under certain circumstances, and consumers may not be notified if this happens. The General Data Protection Regulation (GDPR) applies in specific jurisdictions which aims primarily to give control to EU citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. All these facts create the need for global regulations and standards on data protection and privacy.

ISO/IEC 19944:2017 provides a description of the ecosystem of devices and cloud services and the related flows of data between cloud services, cloud service customers, cloud service users and their devices. That is, the objective with this standard is to provide guidance "about how data is used on the devices in the context of the cloud computing ecosystem and the associated location and identity issues that emerge from such use" providing transparency to all stakeholders. The standard "proposes a scheme for the structure of data use statements to understand and protect the privacy and confidentiality of data". ISO/IEC TR 23186:2018 describes a framework of trust for the processing of multiple-sourced data that includes data use obligations and controls, data provenance, chain of custody, security and immutable proof of compliance as elements of the framework. For an organization processing the data, one of the major elements of trust concerns the provenance of the data that they use: how was the data put together, how reliable is the information it contain, how complete is the data it contains, does the data contain PII or confidential information of any kind. Processing of multi-sourced data will be essential to artificial intelligence applications along with machine learning on financial, transportation, energy, manufacturing, agriculture and government data. Processing of multi-sourced data requires a multi-lateral agreement between the cloud service customers and the cloud service provider(s) on the specific security technologies, techniques and standards that will be used during a given project. Secure multi-party computation (MPC) is an area of research that is beginning to be commercialized that may be useful for processing multi-sourced data. Secure MPC can be used to derive mutual outputs from independent, encrypted data sets where the data rights holders only know what is in their own data.

Related Under-development Standardization: (1) ISO/IEC 19944:2017/PDAM 1 Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – Amendment 1 [67] – Amendment to ISO/IEC 19944 [56] concerning non-personal data. ISO/IEC 19944:2017 Cloud services and devices: Data flow, data categories and data use has given a description of the ecosystem of devices and cloud services and the related flows of data between cloud services, service users. In the amendment version, a classification regarding non-personal data has been added. (2) ISO/IEC AWI 23751 Information technology – Cloud computing – Data sharing agreement (DSA) framework [69] strives to offer a standardized terminology of data sharing along with common building blocks which can be used to create data sharing agreements. The main objective of this work is to reduce the time and cost required to initiate data sharing projects. (3) ISO/IEC PRF 23188 Information technology – Cloud computing – Edge computing landscape [65] The development of techniques creates a need for integrated work across different SCs. More and more tasks from standards view need to be done through collaborations with multiple committees. Both of SC 38 and SC 41 make contributions for ISO/IEC PDTR 23188 [65]. The main scope of the work on this standard is to investigate the architecture, concept and implementation of edge computing, all while exploring the relationship among edge computing, cloud computing and IoT.

1.5.4.Metering and Billing for Cloud Service

On-demand scaling and pay-as-you-use help users to scale their resources as required and pay for what they use. However, while the cloud has traditionally been seen as a cost saving investment, evolving business demands and more and more complex IT environments are making it harder to gain full advantage and visibility into billing. Each cloud provider uses its own model for billing and metering. This makes it difficult for cloud consumers to compare billing of different providers, and once a service is taken by organizations it is also complicated to monitor their spend efficiently, resulting in unnecessary and unpredictable costs. A standard should be developed for billing and metering with mutual verifiability among cloud providers.

From researchers' perspective, usually, cloud providers design the pricing strategy to maximize their revenue following a metering indicator and billing principle proposed by themselves. There is no common standardized metering indicator and billing principle. Even the markets do not need standard offers, but standardized metrics for cloud services can help to reduce the dimensions of metering indicators. Introducing standardization in cloud pricing, would allow billing to become more prevalent and transparent and contributing to build, strength trust on cloud service providers. If standardization efforts can address the metering and billing problem, it will make it easy for users to compare different service providers and helping to monitor and control costs. The standardization community has already realized the necessity of standardized metering and billing. ISO/IEC JTC 1/SC 38 is working on the technical report PDTR 23613 Information technology -Cloud service metering and billing elements [71] which aims to narrow the gaps between market requirements and current industry practices for cloud metering and billing.

Related Under-development Standardization: (1) ISO/IEC NP TR 23951 Cloud computing – Best practices for cloud SLA metrics [66]. This project is working on describing a practical method for using the ISO/IEC 19086-2 metric model [52]. The scope of this work is to provide examples on how the metrics model can be used to compose the calculation of a cloud service performance measure in order to compare against a service quality objective. (2) ISO/IEC DIS 22624 Information technology – Cloud Computing - Taxonomy based data handling for cloud services [68].This standard focuses on the description of the framework for the structured expression of data-related policies and practices in the cloud computing environment based on the data taxonomy in ISO/IEC 19944 [56].

1.5.5.General Requirements

Cloud computing is a mature technology, however users are sometimes confused with the different terminologies. New innovative services are coming out without a standardized and uniform terminology and common description of cloud services. Furthermore, in the literature [30] [31], Pal and Hui emphasize the need for having a common reference architecture for cloud computing. The international standard ISO/IEC 19086 [53] has been updated in 2017 that contributes on unifying the common terminologies in the domain of cloud computing. Currently, the standard project ISO/IEC CD 22123 Concepts and terminology [70] is still under development. The service level agreement, a pivotal piece of any cloud or managed services relationship, consists of many terms, responsibilities, and procedures between the vendor (or service provider) and the customer. While completely necessary, SLAs often are inconsistent, lacking in governance and creating pain points during cloud procurement. To address the challenges that many organizations face in cloud procurement, the International Organization for Standardization (ISO) is in the process of establishing a standard designed to simplify SLAs.

A standard for cloud compliance agreements and SLA frameworks and technology has been established in September 2016. ISO/IEC 19086 series: Service level agreement (SLA) framework. ISO/IEC 19086-1 [51] standard offers much needed structure and guidance to cloud contracts that will help inform CSPs and buyers alike.

ISO/IEC 19086 looks to build upon ISO/IEC 17788 [49] and ISO 17789 [74], and the goal of the document is to establish common terminology, and provide building blocks for cloud SLAs, digging into the following: an overview of cloud SLAs, an identification of the relationship between the cloud service agreement and the cloud SLA, concepts that can be used to build cloud SLAs, and terms commonly used in cloud SLAs. ISO/IEC 19086-1:2016 [51] is for the benefit and use of both cloud service providers and cloud service customers. Cloud service agreements and their associated cloud SLAs vary between cloud service providers, and in some cases different cloud service customers can negotiate different contract terms with the same cloud service provider for the same cloud service. This document aims to assist cloud service customers when they compare cloud services from different cloud service providers. Additionally, parts 2, 3, and 4 go into the metrics model, requirements, and security and privacy measures that need to be in place under the new standard, respectively.

1.6. Discussions and Insights

Standardization is an efficient and economical tool offering the possibility of pursuing various objectives such as: improving efficiency, security and reliability, etc. The gaps analysis in this study shows that standardization for cloud computing still needs more effort to cover all market needs. Some new standards, which are under development, lack of maturity. Most of the standardization is focused on security and interoperability with a technology-driven approach. There are needs for standardized structures, reference architectures, protocols and interfaces.

The main interplay between the legal framework and standardization in cloud computing is in the field of data protection and privacy. Recently, SDOs established the dedicated working groups to cope with the challenges in data protection and privacy aspects. ISO/IEC JTC 1/SC 38 Cloud computing and Distributed Platforms is in charge of the development of standards to support distributed computing paradigms (Cloud Computing), ISO/IEC JTC 1/SC 27 Information Technology Security Techniques is in charge of the development of standards for the protection of information and ICT.

With the development of ICT technologies, the combination of cloud computing, Internet of Things and artificial intelligence is getting closer and closer. Researchers have begun to work on the next generation of cloud computing technology. New concepts like edge computing, fog computing and blockchain attract more and more attention. New working groups or joint working groups should be established to cope with the rapid updating of emerging technologies. ISO/IEC JTC 1/SC 38 Cloud Computing and ISO/IEC JTC 1/SC 41 IoT have a liaison coordination group in order to exchange about and coordinate the efforts on the standardization project which is related to edge computing.

Among the many challenges to be addressed, standardized interoperability is the most pressing problem. ISO/IEC 19941:2017 offers guidance to facilitate interoperability and portability under a standardized terminology. However, cloud standardization efforts should focus on the scenario of user authentication, workload migration, data migration, and workload management. Moreover, cloud management, multi-cloud, cloud audit are some of the open issues at the standardization level.

1.7. The National Example for linking Cloud Communities of Research and Standardization

In Luxembourg, ILNAS, the Luxembourg Institute of standardization, Accreditation, Safety and Quality of Products and Services –Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, is the National Standards Body, which allows and encourages the participation of the national market in the standardization process. Initiatives are in place to foster collaborations with different stakeholders such as researchers, entrepreneurs, companies and individual experts. A specific national policy for ICT technical standardization [45] aims at developing market interest and involvement, promoting and reinforcing market participation, as well as supporting and strengthening the education about standardization and related research activities.

In line with the first objective - to develop market interest and involvement ILNAS has developed a Standards Analysis [46], which allows to identify easily standardization activities of different SDOs in the Smart Secure ICT area, including cloud computing. This document is a practical tool helping ILNAS to promote technical standardization in the cloud computing area and to raise awareness among national stakeholders.

Similarly, conforming to the second project - promoting and reinforcing market participation- ILNAS is actively involved in the development of standards as a P-member of ISO/IEC JTC 1/SC 38 and it follows closely the developments of standards of different technical committees. Actually, 15 national-based experts are participating actively, in a national mirror committee (NMC), on the standardization process and defending

national interest by voting and commenting on current standardization projects. P-Membership allows ILNAS to participate at the ISO/IEC JTC 1/SC 38 Plenary Meetings. The Plenary Meetings allow contributing on the definition of priorities and objectives, and the strategic orientations concerning the development of standards. The participation in ISO/IEC JTC 1/SC 38 and monitoring of the standards developed by other SDOs, such as ETSI, allows ILNAS to actively transfer relevant information to the market and encourage its involvement in the standards development process. NMC meetings are organized to allow interested national stakeholders to strengthen their commitment into the process of technical standardization.

Finally, to meet the third project of the policy - supporting and strengthening the education about standardization and related research activities - ILNAS has undertaken different initiatives, including the development of a White Paper on Smart ICT, in collaboration with the Ministry of the Economy, with the goal of providing a comprehensive analysis of technological, economic, as well as technical standardization perspectives. Moreover, ILNAS works in collaboration with the University of Luxembourg (UL) and the Interdisciplinary centre of Security Reliability and Trust (SnT) on three ICT tracks to link research and standardization funding a unique doctorate program on linking research and standardization in Internet of Things, Artificial Intelligence (AI) and Cloud Computing. One first result of this research program was the publication in October 2018 of a White Paper Data Protection and Privacy in Smart ICT [9], which is extended with this technical report for the cloud computing domain. In parallel, in 2016, the UL/SnT-ILNAS collaboration launched the professional degree certificate Smart ICT for business innovation [47], to be extended to a complete professional Master program by 2020.

1.8. Summary

Cloud computing enables end-users to access unlimited amounts of resources and services using a pay-per-use paradigm. Cloud computing is maturing and growing and still gaining considerable attention due to the advantages such as flexibility and low cost to meet the ever-increasing data traffic demands. For a cloud service provider, guaranteeing users' data security and privacy is a key issue and requires complex prospective considerations, including constant attention and adaptation to the market. This study aimed at providing the gap analysis for the above-mentioned issues from the jointly perspective of research and standardization. The main task for building trust mechanisms in cloud computing is to establish the architecture for sensitive data with encryption mechanism. Under the trust mechanism, trust will be built in the minds of their users, and as a result, customers will be encouraged to choose cloud services. Innovative business models in cloud computing allow a wide range of interactions and collaborations across multiple service providers. Despite researcher and standardization already making contributions for establishing trust among customers and cloud service providers, sustained attention and efforts are needed as the trust relationship among users and service providers has huge market importance. The potential contributions of this study in matters of industry impact are numerous with new insights in the gap analysis of data protection and privacy in cloud computing under the joint consideration of research and technical standardization efforts.

List of Acronyms and abbreviations

SDO	Standard Development Organization
NIST	National Institute of Standards and Technology
IT	Information Technology
M2FC	Multi-dimensional Mean Failure Cost
WTO	World Trade Organization
TBT	Technical Barriers to Trade
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ITU	International Telecommunication Union
ILNAS	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
UL	University of Luxembourg
WG	Working Group
SC	Sub Committee
CCF	Cloud Computing Fundamentals
TCESI	Technical Committee on Electronic Signature Infrastructure
TR	Technical Report
CG	Coordination Group
GDPR	General Data Protection Regulation
DSA	Data Sharing Agreement
SLA	Service Level Agreement
CC	Cloud Computing
IoT	Internet of Things
AI	Artificial Intelligence

References

[1] ITU-T Y.3500, ISO/IEC, Information technology Cloud computing Overview and vocabulary

[2] P. Mell, The NIST definition of cloud computing. 2011.

[3] Wang, W., and Benbasat, I. (2005). Trust in and Adoption of Online Recommendation Agents. Journal of the Association for Information Systems, Vol. 6, No. 3: pp. 72101.

[4] McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. (2011). Trust in a Specific Technology: An Investigation of Its Components and Measures, ACM Transactions on Management Information Systems, Vol. 2, No. 2: pp.125

[5] Lee, J. D., and See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. Human Factors, Vol. 46, No. 1: pp. 5080.

[6] Li X, Du J (2013) Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing. IET Inf Secur 7:3950. https://doi.org/10.1049/iet-ifs.2012.0232.

[7] Kanwal A, Masood R, Ghazia UE, ShibliMA, Abbasi AG (2013) Assessment criteria for trust models in cloud computing. In: IEEE International Conference on Green Computing, Beijing, China, pp 254261.

[8] The Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven", 2019.

[9] ILNAS, White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical standardization, ILNAS, ANEC G.I.E, University of Luxembourg, Tech. Rep., 2018.

[10] Z Yan, X Li, M Wang, Flexible data access control based on trust and reputation in cloud computing.

[11] Zheng, Y., Wangyang, S., CloudFile: A cloud data access control system based on mobile social trust, Journal of Network and Computer Applications, Volume 86, 15 May 2017, Pages 46-58.

[12] Vipul Goyal, et. al, Attribute-based encryption for fine-grained access control of encrypted data. In CCS '06 Proceedings of the 13th ACM conference on Computer and communications security, Pages 89-98, 2006.

[13] Blaze, M., Bleumer, G., and Strauss, M. 1998. Divertible protocols and atomic proxy cryptography. In Proceedings of Eurocrypt '98. Vol. 1403. 127–144.

[14] Shucheng, Y., Cong, W., Kui, R., Wenjing, L., Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, 2010 Proceedings IEEE INFOCOM.

[15] A. Brinkmann, C. Fiehe, A. Litvina, I. Lck, L. Nagel, K. Narayanan, F. Ostermair and W. Thronicke, Scalable monitoring system for Clouds, in UCC.

[16] I. Saenko and I. Kotenko, Using Genetic Algorithms for Design and Reconfiguration of RBAC Schemes, in Proceedings of the 1st International Workshop on AI for Privacy and Security - PrAISe 16, 2016.

[17] N. M. Gonzalez, M. A. T. Rojas, M. V. M. Silva, F. Redigolo, T. C. M. Brito Carvalho, C. C. Miers, M. Naslund and A. S. Ahmed, A Framework for Authentication and Authorization Credentials in Cloud Computing, in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[18] R. Banyal, P. Jain and V. Jain, Multi-factor authentication framework for Cloud Computing, in CIMSim.

[19] M. D. Samrajesh1, and N. P. Gopalan, Secure Multi-tenant Application in Software as a Service, ERCICA2013

[20] M Jouini, LBA Rabai, A security framework for secure cloud computing environments.

[21] Gordon, Blair., Complex Distributed Systems: The Need for Fresh Perspectives, 2018 ICDCS.

[22] H. Kuijs, C. Reich, M. Knahl and N. Clarke, A Scalable Architecture for Distributed OSGi in the Cloud, in Proceedings of the 6th International Conference on Cloud Computing and Services Science, 2016.

[23] Li.Y, Keke. G, Intelligent cryptography approach for secure distributed big data storage in cloud computing, Information Sciences Volume 387, May 2017, Pages 103-115.

[24] D. X. Song, D. Wagner, and A. Perrig, Practical techniques for searches on encrypted data, in Proc. of SP00. IEEE, 2000, pp. 4455.

[25] Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, Searchable encryption over feature-rich data, IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 11, DOI:10.1109/TDSC.2016.2 593 444, 2016

[26] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, An efficient public auditing protocol with novel dynamic structure for cloud data, IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 24022415, 2017.

[27] X. Liang, X. Li, R. Lu, X. Lin, X. Shen, UDP: Usage-Based Dynamic Pricing With Privacy, Preservation for Smart Grid, IEEE TRANSACTIONS ON SMART GRID, VOL. 4, NO. 1, MARCH 2013.

[28] S. Fischer-Hbner, J. Angulo and T. Pulls, How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?, in IFIP Advances in Information and Communication Technology, 2014, pp. 77-92.

[29] S. Zhu and G. Gong, Fuzzy authorization for Cloud storage, in IEEE Transactions on Cloud Computing (TCC), 2014.

[30] Future Generation Computer Systems — Vol 26, Issue 4, Pages 531

[31] Pal, R. and Hui, P., Economic models for cloud service markets: Pricing and Capacity planning.

[32] C. Li, D. Li, G. Miklau, D. Suciu, A Theory of Pricing Private Data, ACM Transactions on Database Systems, Vol. 39, No. 4, Article 34, Publication date: December 2014.

[33] ISO/IEC Guide-2:2004Standardization and related activities General vocabulary

[34] M. Stihler, A. O. Santin, A. L. Marcon and J. Silva Fraga, "Integral Federated Identity Management for Cloud Computing," in 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), 2012.

[35] B. Keltoum and B. Samia, "A dynamic federated identity management approach for cloud-based environments," in Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing - ICC '17, 2017.

[36] K. Bendiab, S. Shiaeles and S. Boucherkha, "A New Dynamic Trust Model for "On Cloud" Federated Identity Management," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[37] C. Jincui and J. Liqun, "Role-Based Access Control Model of Cloud Computing," Energy Procedia, vol. 13, pp. 1056-1061, 2011.

[38] I. Saenko and I. Kotenko, "Using Genetic Algorithms for Design and Reconfiguration of RBAC Schemes," in Proceedings of the 1st International Workshop on AI for Privacy and Security - PrAISe '16, 2016.

[39] F. Jaidi, F. L. Ayachi and A. Bouhoula, "A Comprehensive Formal Solution for Access Control Policies Management: Defect Detection, Analysis and Risk Assessment".

[40] A. Ben Fadhel, D. Bianculli and L. Briand, "A comprehensive modeling framework for role-based access control policies," J. Syst. Softw., vol. 107, pp. 110-126, 2015.

[41] J. Sendor, Y. Lehmann, G. Serme and A. S. Oliveira, "Platform level support for authorization in Cloud services with oauth 2," in IC2E IEEE, 2014.

[42] A. Gholami and E. Laure, "Big data security and privacy issues in the Cloud," International Journal of Network Security and its Applications (IJNSA), vol. 8, no. 1, 2016.

[43] J. R. Raphael, The worst Cloud outages of 2013 (so far), 2013.

[44] L. Ojomoko, Y. Yanovich,et al, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," in Oncotarget, 2018 Jan 19; 9(5): 56655690. doi: 10.18632/oncotarget.22345

[45] ILNAS, Policy on ICT technical standardization (2015-2020), https://portail-qualite.public.lu/dam-assets/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf, accessed: 2019-09-17.

[46] ILNAS, Standards Analysis: Smart Secure ICT, ILNAS ANEC G.I.E, Tech. Rep., 2018

[47] Smart ICT Certificate for Business Innovation, https://wwwen.uni.lu/studies/fstc/certificate smart ict for business innovation, accessed: 2019-07-18
[48] JK Liu, MH Au, X Huang, Fine-grained two-factor access control for web-based cloud computing services
[49] ISO/IEC 17788:2014/ITU-T Y.3500 (08/2014), Cloud computing –Overview and vocabulary
[50] ITU-T Y.3502, Information technology-Cloud computing Reference architecture
[51] ISO/IEC 19086-1:2016 Information technology - Cloud computing - Service level agreement (SLA) framework - Part 1: Overview and concepts
[52] ISO/IEC 19086-2:2018 Cloud computing - Service level agreement (SLA) framework - Part 2: Metric mode
[53] ISO/IEC 19086-3:2017 Cloud computing -Service level agreement (SLA) framework - Part 3: Core conformance requirements
[54] ISO/IEC 19086-4:2019 Cloud computing - Service level agreement (SLA) framework - Part 4: Components of security and of protection of PII
[55] ISO/IEC 19941:2017, Cloud computing - Interoperability and portability
[56] ISO/IEC 19944:2017, Cloud computing - Cloud services and devices: Data flow, data categories and data use
[57] ISO/IEC 27018:2019, Security techniques - Code of practice for protection of personally identifiable information (PII)
[58] ISO/IEC 27036-4:2016, Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services
[59] ETSI TR 102 997 V1.1.1 (04/2010) CLOUD; Initial analysis of standardization requirements for Cloud services
[60] ETSI TS 103 125 V1.1.1 (11/2012) CLOUD; SLAs for Cloud services
[61] ETSI SR 003 381 V2.1.1 (02/2016) Cloud Standards Coordination Phase 2; Identification of Cloud user needs
[62] ETSI SR 003 391 V2.1.1(02/2016) Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing
[63] ISO/IEC TS 23167, Information Technology - Cloud Computing - Common Technologies and Techniques
[64] ISO/IEC NP TR 23187, Information technology - Cloud computing - Interacting with cloud service partners
[65] ISO/IEC PDTR 23188, Information technology - Cloud computing - Edge computing landscape
[66] ISO/IEC NP TR 23951, Cloud computing - Best practices for cloud SLA metrics
[67] ISO/IEC 19944:2017/ PDAM 1, Information technology - Cloud computing - Cloud services and devices: Data flow, data categories and data use - Amendment 1
[68] ISO/IEC DIS 22624, Information technology - Cloud Computing - Taxonomy based data handling for cloud services
[69] ISO/IEC AWI 23751, Information technology - Cloud computing - Data sharing agreement (DSA) framework
[70] ISO/IEC CD 22123, Information technology - Cloud computing - Concepts and terminology
[71] ISO/IEC PDTR 23613, Information technology - Cloud service metering and billing elements
[72] ISO/IEC 27001, Information security management
[73] ISO/IEC TR 23186: 2018, Information technology - Cloud computing - Framework of trust for processing of multi-sourced data
[74] ISO/IEC 17789: 2014, Information technology - Cloud computing - Reference architecture

2. Internet of Things: Gap Analysis between Scientific Research and Technical Standardization

Technical Report on Data Protection and Privacy in Smart ICT

Abstract

With the emergence of new digital trends like the Internet of Things (IoT), more industry actors and technical committees pursue research in utilizing such technologies as they promise better and optimized management, improved energy efficiency and better quality living by facilitating a magnitude of value-added services. However, as communication, sensing and actuation become increasingly sophisticated, such promising data-driven IoT systems generate, process, and exchange larger amounts of data, some of which is privacy-sensitive and security-critical. The sustained increase in number of connected devices, catalyzed by IoT, affirms the importance of addressing data protection, privacy and security challenges, as indices of trust, to achieve market acceptance. This consequently, emphasizes the need of a solid technical and regulatory foundation to ensure trustworthiness within the IoT ecosystem. The goal of this study is to first introduce the concept of trustworthiness in IoT with its main pillars, data protection, privacy and security, and then analyze developments in research and standardization for each of these. The study presents a gap analysis on data protection, privacy and security between research and standardization, throughout which the use case of Unmanned Aerial Vehicles (UAVs) is referred to, as a promising value-added service example of mobile IoT devices. The study concludes with suggestions for future research and standardization in order to address the identified gaps.

2.1. Introduction

Today, the much-discussed technologies of the Internet of Things (IoT) provide the essential tools allowing the development of new devices that collect data and produce unprecedented amounts of information about everything around us [1]. Broadly, IoT refers to a network of uniquely addressable, interconnected objects, built on standard communication protocols whose point of convergence is the Internet, hence enabling a wide array of services that were otherwise unfeasible to be realized [2]. IoT, nevertheless, has a distinct vision that extends interconnectivity between both physical and virtual devices by envisioning an interconnected world of things capable of providing services over the Internet. In turn, these technologies have accelerated the growth of data-driven applications and unleashed numerous opportunities for businesses, individuals and society at large [3].

The economic impact of IoT is undeniable [3], however, beyond the buzzword and notion of connected things, IoT is a complex technological paradigm. To fully exploit the potential of such technology and to establish trustworthiness, many challenges need to be addressed with data protection, privacy and security at their core. This starts with an efficient assessment and quantification of risks, which, for a complex and heterogeneous technologies like IoT, is not a trivial task [4].

In recent years, the research and standardization communities have independently worked towards solving some of the problems in IoT, exposing inconsistencies and gaps in existing solutions [5]. To that extent, the goal of this study is to analyze and explore some of such predominant gaps between IoT scientific research and technical standardization focusing on data protection, privacy and security as main pillars of achieving trustworthiness.

Throughout this study we illustrate our argument by referring to a promising category of devices that recently found its way into IoT, Unmanned Aerial Vehicles (UAVs). UAVs not only offer a new means of efficiently collecting and transmitting data, but also promise a pragmatic solution to IoT terrestrial infrastructure limitations [6]. UAVs in turn shed light on a vast array of IoT applications, encouraged by the uprising of value-added IoT services.

The contributions of this study are, firstly, introducing the concepts of trust and trustworthiness in IoT, secondly, analyzing the state-of-the-art in research and standardization. This study then presents an analysis of the identified gaps between standards and research, followed by a discussion and suggestions for future research directions and standardization roadmaps.

The remainder of this study is organized as follows. Section 2.2 describes the concept of trust in digital technologies followed by a state-of-the-art analysis in IoT research in Section 2.3. Section 2.4 presents a detailed study of standardization developments. Section 2.5 analyzes the gaps between research and standardization followed by remarks in Section 2.6. Section 2.7 emphasizes the efforts put forth in Luxembourg to foster the collaboration between research and standardization. Finally, Section 2.8 summarizes the work.

2.2. Trust and Trustworthiness

The concepts of trust and trustworthiness are complex and have been a subject of considerable scholarly interest across different disciplines [7] [8]. However, when it comes to emerging digital technologies, and IoT in particular, trust, better referred to as digital trust, and trustworthiness still need to be defined more precisely. As with the unprecedented number of connected devices and exponentially increasing data being collected within large-scale open distributed systems within the IoT ecosystem, they form the essential foundations, upon which ensuring the success and further development of the technology becomes possible [9].

Broadly, digital trust [8], adopted from the philosophical term of trust, consists of three main components, a trusting entity, a trusted entity and a desired level of performance or deliverable [7]; while trustworthiness refers to the property of a system offering a reliably constant level of confidentiality, integrity, availability, and reliability. Hence, with focus on IoT, for the remainder of this study we define trustworthiness in the IoT ecosystem as: "*The affirmative confidence of an entity in the integrity of an IoT system, the sureness of the honesty and accuracy of devices and the reliability and confidentiality of digital information and networks on both levels of interaction; user-and-machine as well as machine-to-machine; where an entity could be a human user, digital device, IoT subsystem or software agent.*" [1]

According to [10], "a market's perception of trustworthiness depends on the indices of data protection measures and regulations, privacy and security". Hence, to achieve an acceptable level of trustworthiness, data protection, privacy and security are major requirements to be addressed. Security is typically defined as the protection against unauthorized access, while data protection and privacy refer to a system's ability to protect sensitive personally identifiable information (PII) [11].

To this end, Figure 1 adapts the illustration from [1] to summarize the above by illustrating how the term "trust" has been transformed, by the emerging digital technologies, from its initial philosophical meaning described in [7] to digital trust, defined above. The figure then shows how the indices of data protection, privacy and security contribute to the property of a system being reliable, offering a constant level of integrity, availability and accuracy; hence, trustworthy. In other words, within IoT, "trusting" and "trusted persons" in [7] have been transformed into "trusting" and "trusted entities", respectively.

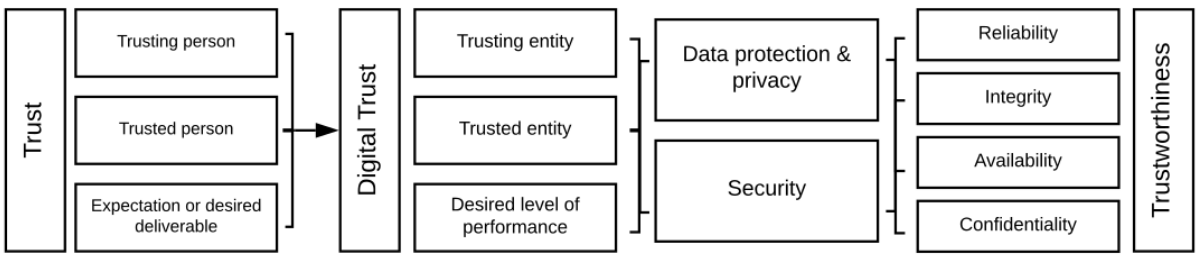

Fig.1: From trust to digital trust and trustworthiness in the IoT ecosystem

These entities could be human users, digital devices, IoT subsystems or software agents. The figure then illustrates that through an acceptable level of data protection, privacy and security measures, trustworthiness could be achieved.

2.3. Research Developments

To achieve market acceptance, an acceptable level of trustworthiness has to be met and hence, addressing data protection, privacy and security needs becomes critical. This section explores research developments and state-of-the-art in IoT data protection, privacy and security.

The IoT concept evolved rapidly over the past few years to become an umbrella-term for interconnected technologies, devices, objects as well as services. However, due to this exponential boom and rapid market adoption, there is still no clear and common definition of the concept, even after several attempts by the research community. A. Bassi et al. [13] emphasize the need of establishing a common ground for quickly emerging technologies. Nevertheless, the authors argue that it is not a trivial task and for being effective, it has to capture as many applicable vantage points as possible.

A thorough analysis of the most commonly used IoT concepts and IoT platforms can be found in [14]. Ibrar Yaqoob et al. in [12] devise an IoT taxonomy based on parameters such as applications, enabling technologies, business objectives, architectural requirements, IoT platform architecture types, and network topologies as illustrated in Fig. 2.

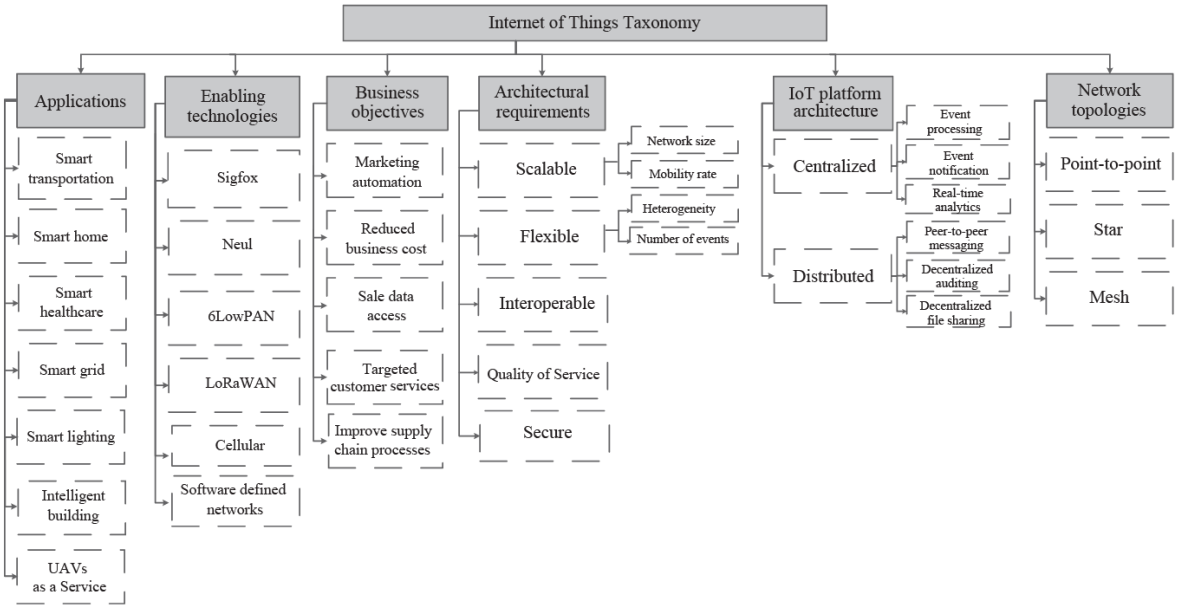

Fig. 2: IoT taxonomy based on applications, enabling technologies, business objectives, architectural requirements, IoT platform architecture types, and network topologies, adapted from [12]

From this taxonomy it can be derived that IoT is a system of systems with multiple enabling technologies and different communication protocols, adopted by different IoT entities for a wide range of application, hence making *interoperability* in IoT is an enormous challenge. One viable solution to address interoperability challenges, concerned with data protection, privacy and security, is having a common *reference architecture*. This is further supported in [15] where Ivor D. Addo et al. emphasize that an IoT general reference architecture is essential to support the security and privacy of the network. The literature provides several viable IoT architectures that could be used as a reference general model [16], [17] ranging between 3–layer to 5–layer architectures [14], [2]. However, regardless of the number of layers or how they are divided, all proposed architectures are composed of a *sensing and actuation component*, a *transmission and communication*

component, a *processing and data storage component*, and an *application and interface component* [2]. In [12], Ibrar Yaqoob et al. provide an illustration of what any future IoT architecture should achieve as shown in Fig. 3. The authors additionally argue that a reference architecture would not only support overcoming interoperability challenges, but also help achieve market acceptance.

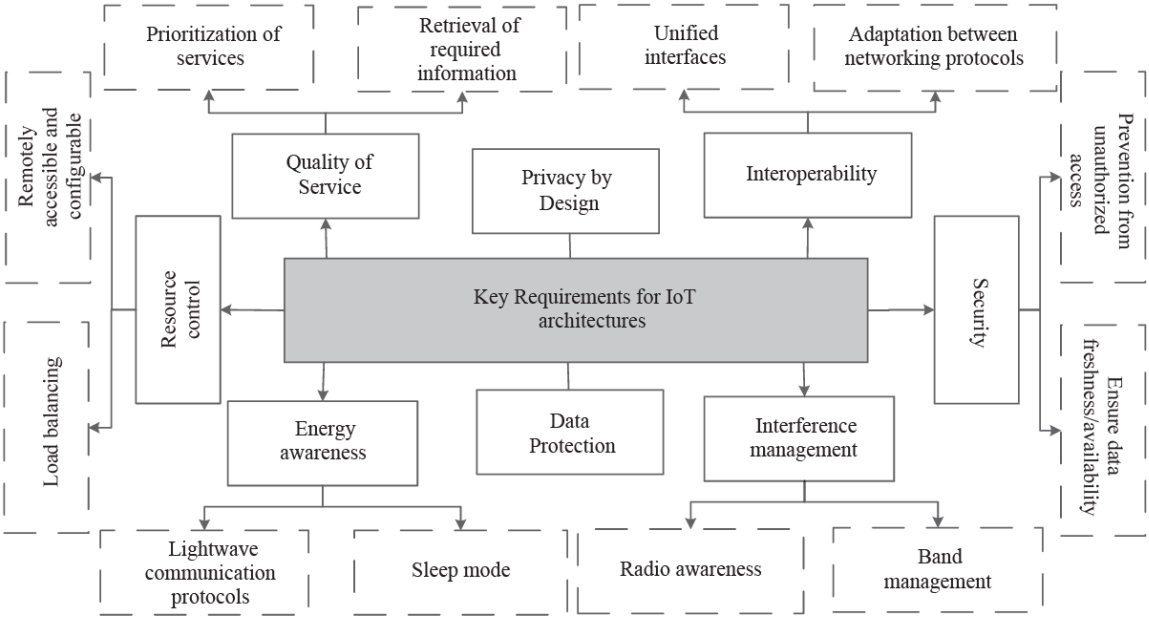

Fig. 3: IoT architecture requirements adapted from [12]

As Section 2.2 explained the link between market acceptance and data protection, privacy and security, the following subsections aim to explore the aforementioned pillars and how they hinder establishing *trustworthiness* within the IoT ecosystem.

2.3.1. Data Protection and Privacy

IoT is a rapidly expanding network of connected physical and virtual objects and hence in contrast to conventional scenarios where users' actions are the main cause of privacy vulnerabilities, within the IoT ecosystem, devices or network nodes continuously collect individuals' data without their acknowledgement or consent [18]. Therefore, ensuring privacy within the magnitude and variety of deployed IoT devices autonomously sensing and gathering private information is a pressing concern [2]. From physical and behavioral privacy, to location, information and communication privacy, most challenges fall within the transportation and data handling layers in IoT [2]. One source of challenges highlighted in the literature is due to the interoperability within IoT systems. As one system interacts with other systems, each having their own privacy policies, inconsistencies arise. This in turn emphasizes the importance of standardization addressing IoT interoperability, data structure and exchange (e.g., ISO/IEC 21823-1:2019 [19], which will be further discussed in Section 2.4.). The literature provides some mechanisms and approaches to avoid inconsistencies and preserve privacy. One approach to address this is explained in [20], where Stankovic et al. propose online consistency checking, notification and resolution schemes. Additionally, M. Conti et al. in [21] argue that mechanisms currently in use provide user-centric privacy, content-oriented privacy or context-oriented privacy. However, as mentioned above, within IoT networks, devices collect information autonomously and therefore, there is a real need for new protocols. Moreover, the recently entered-into-force privacy regulation [22] mandate that users are always informed about how their data is managed and that no data should be collected without their consent. This in turn makes it crucial to develop new methods to identify nodes or devices that passively collect or have access to passively collected user identifiable information, which M. Henze et al. in [23]

explains is a huge challenge in heterogeneous IoT networks. Table 1 shows the main privacy threats, current solutions in the literature, potential challenges and future research directions categorized under user-oriented privacy, content-oriented privacy, context-oriented privacy and others as devised in [18].

Privacy	Threats	Current Solutions	Potential Challenges	Research Directions	References
User	Surveillance networks	• Legislation and audits • Fair Information practices	• User awareness • Seamless user interaction • Quicker legislation	• Service flexibility • Automatic negotiations	[24], [25], [26]
Content	Eavesdroppers during aggregation Infer query contents from respondents Behavior prediction from temporal patterns	• End-to-end encryption • Homomorphic encryption • Data slicing and perturbation • Flooding • Bogus queries • Data replication • Time-driven reporting • Buffering	• Dynamic topologies • Lightweight homomorphisms • Privacy revocation • Reduce overhead • Sensors-as-a-Service • User-server likability • Real-time capabilities • Conflicts w/ other mechanisms • Node capture	• Advanced crypto • Private information retrieval • Anonymous communications • Channel multiplexing • Intrusion detection mechanisms • Tamper-resistant pseudonyms	[27], [28], [29]
Context	Link messages to data sources Location leakage	• Pools of pseudonyms • Cryptographic pseudonyms • Random routing • Fake traffic	• Dynamic topologies • Network-layer pseudonyms • Identification & inventory attacks • Energy consumption • Holistic privacy • Active and internal attackers	• Agnostic identifiers • Network-wide pseudonyms • Selective response to queries • Cognitive radios • Memory obfuscation	[30], [31], [32]
Other	Data sharing Data combination	• Computation on encrypted data • Privacy-aware data mining	• Data sharing at back-end • Multi-source data combination • Invasive interfaces and display • Social smart things	• Privacy-preserving data mining • User awareness • Context-aware data presentation	[33], [31], [28]

Table 1: Privacy threats, current solutions in literature, potential challenges and future research directions based on [18]

2.3.2.Security

Security can generally be defined as protection against unauthorized access, which is emphasized by Y. Yang et al. as the root of trust and backbone of data protection in IoT [34]. It is therefore critical to extend our previous work on security challenges in IoT [2] with more recent security related challenges.

Table 2 shows some main layer-based attacks on IoT systems with their strategies as adopted from [35]. Moreover, M. Nawir et al. in [35] developed a taxonomy of IoT attacks divided under eight main categories*; including, device property, location, strategy, access level, protocol based, information damage level, host based and communication stack protocol.*

Current trends in IoT devices miniaturization come at the cost of limited computational power and energy, making most of today's security solutions unsuitable as they require heavyweight computations and large memory [34], [2]. Therefore, lightweight security solutions for IoT devices is a current pressing research challenge, given the diverse technical nature of devices. Ideally, for a quick response, given the real-time or near real-time nature of a magnitude of IoT devices, the detection, countermeasures, and repairs must run in almost real-time, as part of a run-time self-healing architecture. However, healing can require reprogramming, in particular in cases where an unanticipated attack occurs. In such scenarios, healing instructions need to be securely delivered, with authentication and attestation, to the appropriate nodes and then the nodes' running programs need to be amended by the run-time architecture. This in turn emphasizes that hardware support will be essential for providing authentication, encryption and tamper-proof keys, as explained by J. Stankovic et al. in [20] and explained in our previous work [2].

Aspect	Top threat	Research effort
Physical	Jamming Tampering	Creates radio interference and exhaustion on IoT devices. Creates compromised nodes.
Data Link	Collision Exhaustion Unfairness	Simultaneously transmit two nodes of the same frequency. By repetitive collision the nodes. Using above link layer attacks.
Network	Spoofed information Selective forwarding Sinkhole Sybil	Creates routing loops, extend or shortening sources routes. Choose what information that gathered before transmit it. Monitoring, Redundancy, Authentication. Single node duplicates its node to be in multiple locations.
Transport	Flooding De-synchronization	Repeat the request of a new connection until the IoT system reach maximum level. Disruption of an existing connection.
Application	Attacks on reliability and clone attack	Clock skewing, Selective message forwarding, Data aggregation distortion.

Table 2: Layer–based IoT attack types and strategies used adopted from [35].

2.3.2.1. Authentication

Authentication is the process of verifying the identity of a device or person. Within the IoT ecosystem, authentication is essential to allow the integration of different IoT devices that are deployed in different contexts [21]. Passwords are currently one example of commonly used IoT devices' user authentication mechanisms, however they are major source of concern due to weak passwords through which large Distributed Denial-of-Service (DDoS) attacks were recently facilitated. Another possible alternative is activity-based biometrics, however, IoT devices tend to be limited in input/output modules in turn constraining the authentication method [36], [37]. A more thorough survey on privacy can be found in [38], whereas for data protection, R. Thorburn et al. in [39] offer a detailed analysis of IoT data protection considerations.

Generally, IoT adds more challenges to existing research when it comes to authentication and efficient key deployment and management as any cryptographic key generation and exchange should not cause any major overhead on IoT network nodes as Y. Yang et al. explain in [40].

2.3.2.2. Access Control and Information Flow Control (IFC)

Access control, as explained in [2] is a security technique that can be used to regulate what or who can view or use resources in a computing environment. This is achieved by limiting connections to computer networks, system files and data [41], [42]. However, E. Fernandes et al. in [43] argue that access control is merely a gatekeeper and that it provides no further protection once code obtains access to sensitive resources. Nevertheless, complementing access control, Information Flow Control (IFC) tracks how information propagates through the program during its execution to make sure that information is handled securely. IFC techniques work by controlling how untrusted code uses access to sensitive resources. In [43], E. Fernandes et al. analyzed a set of smart home platforms and concluded that the majority of current platforms rely solely on access control. Although IFC is not a new concept, the challenge lies in applying it meaningfully to a specific domain [41], an example of that would be FlowFence. As explained in our previous work [2], FlowFence is a recent proposal for IoT frameworks that enables a data- flow-graph approach to IFC [37]. IoT, however, extends current research challenges as the deployment and management of a variety of access control and IFC mechanisms is complicated in a heterogeneous IoT network. This is due to the fact that every IoT node may only support a limited number of access verification mechanisms which could vary from other objects connected to the same network node as S. Moosavi et al. explain in [44].

2.3.2.3. Secure Architecture

As discussed at the beginning of Section 2.3 and illustrated in Figure 3, an IoT reference architecture should take into consideration such potential security vulnerabilities. However, devising an architecture that overcomes the aforementioned challenges in security is not a trivial task as emphasized by M. Conti in [21]. S. Raza et al. in [45] explain that an IoT architecture should not only address the aforementioned issues but additionally handle challenges introduced when deploying IoT devices over Software Defined Networks (SDNs) as the majority of SDNs as well as cloud environment security challenges would certainly be inherited by the underlying IoT devices. Additionally, the detection of malicious traffic over networks with different natures as well as the identification of malicious actors is extremely challenging for existing intrusion detection systems in IoT as explained by H. Pajouh et al. in [46].

2.3.3.Use Case: UAVs-as-a-Service

The main scope of the use case is to clarify the motivation behind the study of data protection, privacy, and security in IoT as well as emphasize the importance of trust. The UAV use case demonstrates the orchestration between the different IoT systems as well as highlights key challenges in UAVs as one of the promising IoT platforms. The scenario is to offer UAVs-as-a-Service for smart cities as a solution for different IoT-based data-driven smart city applications.

UAVs have rapidly found their way into IoT as both a solution to IoT terrestrial infrastructure limitations [6] and a smart device that promises new means of data collection and transmission [47], [48]. From traffic monitoring, precision agriculture, surveillance, e-Health logistics and parcel delivery, UAVs shed light on many potential applications that can be used to manage cities' assets and facilitate services. UAVs-as-a-Service allows operators and users, whether individual or organization, to enter their mission details and submit a mission request for verification. Once one or multiple UAV flight service providers, depending on the requested service, are selected, the mission is initiated. The data is then collected, analyzed and transmitted back to the user.

To consolidate this, we narrate one operational example (although the use case can lend itself to multiple other mission scenarios). This example considers a government administration request to monitor car traffic, in order to identify vehicles' lane changing patterns and find drivers who stay on the left-most traffic lane [49]. The mission requires multiple UAVs operating within the low altitude airspace, in turn introducing a number of data protection, privacy and security challenges.

2.3.3.1. Data Protection and Privacy Challenges

With the great advantages UAVs bring as agile, mobile IoT devices and aerial platforms, come several challenges directly linked to data protection. These range from the direct violation to General Data Protection Regulation (GDPR) when failing to gain consensus from large samples being monitored, to other violations related to lack of transparency and quality of collected data, profiling and data security issues [2]. Additionally, UAVs bring along multiple privacy challenges. While the majority of such challenges falls under the transmission and communication layer of IoT as mentioned in Section 2.3, UAVs introduce a set of threats to the integrity of individuals' health, behavior and location, as they can potentially invade peoples private space, and accidentally expose them by processing personal data against their will. Additionally, privacy violations can occur through the unsuspecting data collection concerning individuals without any purpose. The use of UAVs as an emerging added-value IoT service inherits the challenges of data protection and privacy outlined in Table 1. However, due to their exceptional mobility, agility and customizability of payload [47], current IoT solutions presented in the aforementioned table may not be sufficient. In [50], P. Blank et al. demonstrate some basic principles of information privacy and how they can be incorporated into existing infrastructures to build up a framework for privacy-aware UAVs. P. Blank et al. additionally propose a framework that allows UAV operators to configure UAV flight paths based on individuals' privacy configurations. S. Winkler et al. in [51] stress on the need for further regulation for the civilian and commercial use of UAVs. This is further emphasized in [52] where N. Labib et al. explain that globally harmonized regulations and technical standards are critical as UAV technology continues to be rapidly adopted by many economic sector actors.

2.3.3.2. Security Challenges

In addition to the data protection and privacy challenges that accompany UAVs deployment within the IoT ecosystem, UAVs pose several security threats linked to their safe operation and management [47]. Table 3 outlines some key security threats and models for UAVs within the context of IoT. These security threats are classified into *confidentiality, integrity, availability* threats. With the majority of threats falling under confidentiality and interception of information, security provisions of UAVs as part of IoT is a complex task requiring integrating various techniques associated with different aspects of IoT networking and UAV operation.

UAV Privacy and Security Threats				
Confidentiality	Interception of Information	Ground Control Station	Virus, Trojans, Keyloggers, Malware	
		Communication Link	Identity Spoofing, Cross Layer Attack, Hijacking Eavesdropping, Protocol Based Attacks	
		Humans/ Operator	Threats, Unintended Acts, Social Engineering	
Integrity	Modification/ Fabrication of Information	Malicious Attacks	Airborne Threats	Jamming, Distortion of Signal Retransmit Tampered Information
			Compromised Link	Malicious Code, Subroutine Exploit
Availability	Communication Interruption	Malicious Attacks	Jamming, Falsifying Command and Control Signals	
			Malicious Attacks	Spoofing, Buffer Overflow
				Flooding: UDP, SYN ICMP, Ping

Table 3: The main security threats for UAVs classified under confidentiality, integrity and availability.

In addition to the threat model mentioned in Table 3, UAVs pose physical security threats given that the majority of civil applications require UAVs to operate in low altitude airspace over populated cities. T. Lagkas et al. in [53] explain that IoT-based UAVs is a complex paradigm and that security provisions in UAVs within the IoT ecosystem is not a trivial task. The paper presents some potential IoT layer-based solution protocols to address the threats listed in Table 3, ranging from mechanisms such as Constrained Application Protocol (CoAP) and Simple Object Access Protocol (SOAP) for application layer attacks, mechanisms like IP Security (IPSec), Datagram Transport Layer Security (DTLS), firewalls, and Intrusion Protection Systems (IPS) for network layer security provisions, to hardware tamper-protection for threats at the perception and physical layer. Although, research is actively addressing potential threats accompanying the rapid adoption of IoT-based UAV application, the literature emphasizes the need for regulations and technical standardization in order to safely manage and operate the large forested number of UAVs soon to dominate the low altitude airspace over populated cities [47].

2.4. Technical Standardization

Technical standardization is globally accepted for the qualitative and technical referential of repetitive processes, products and services. Standards are developed within organizations - referred to as Standards Development Organizations (SDOs) - which bring together various stakeholders such as independent experts and representatives of organizations and governments to find consensus within a global regulatory and ethical framework [54].

The majority of used internet protocols and standards are very complex for the power and processing constrained devices in IoT. Many of these devices are designed to run proprietary protocols, creating data silos. In the short term, the vertical integration of sensors and business services will dominate IoT. The diverse communication protocols and the need for interoperability within IoT ecosystems motivate the need for establishing globally-harmonized regulations and internationally-agreed-upon technical standards to govern the technology's rapid advancements, as well as ensure a fair economy by encouraging market competition while lowering barriers to entry for newcomers [52].

This section shows the role of standardization in tackling the challenges of data protection, privacy, and security and describes current efforts of standardization committees and relevant technical standards in IoT (and UAVs).

2.4.1. Data Protection, Privacy and Security Standardization in IoT

Over the past few years, SDOs, on national, European and international levels, initiated dedicated Working Groups (WGs) in their Technical Committees (TCs) with the aim to address challenges of data protection, privacy and security within the rapidly evolving IoT ecosystem. This was further catalyzed by the new data protection regulations recently put into force, the GDPR. Some of the relevant technical standardization committees and WGs currently active in IoT standards development include ISO/IEC JTC 1/SC 41 on Internet-of-Things and related technologies, ISO/IEC JTC 1/SC 31 on automatic identification and data capture techniques, ISO/IEC JTC 1/SC 32 on data management and interchange, ISO/IEC JTC 1/SC 6 on telecommunications and information exchange between systems, ISO/IEC JTC 1/SC 27 on Information security, cybersecurity and privacy protection [55], and ETSI/TC SmartM2M on smart Machine-to-Machine communications [56]. Table 3 in [54] presents a summary of SDOs and their involvement level in IoT standardization, categorized under *terminology, interoperability, connectivity, security and privacy, trust, reliability and scalability, intelligence and others*.

With 20 published standards and 11 standards under development, ISO/IEC JTC 1/SC 41 is one of the more active technical subcommittees within IoT standardization. ISO/IEC JTC 1/SC 41 aims to stay up to date with current standardization demands by forming liaisons with other committees within the SDOs, like ITU-T and ETSI.

Out of the recently published standards, ISO/IEC 21823-1:2019 [19] Part 1 provides an overview of interoperability as it applies to IoT systems and a framework for interoperability for IoT systems. This could be considered the foundation on which the second part, ISO/IEC 21823-2 [58] on Interoperability for IoT Systems - Part 2: Transport interoperability and the third part ISO/IEC 21823-3 [59] on Interoperability for IoT Systems - Part 3: Semantic interoperability are based. Both, the second and third parts of the interoperability standard are currently under development. Table 4-A and Table 4-B mention some of the recently published and under-development standards in the IoT area; for a more exhaustive list, the reader can refer to [2], [60], [55].
The GDPR requires organizations to undertake a Data Protection Impact Assessment (DPIA) before any new application is launched to minimize or restrict data breaches. In order to comply with such a regulation, stakeholders can rely on ISO/IEC 29134:2017 [61] and ISO/IEC 27005:2018 [62] on information security risk management, which are offering guidelines for privacy impact assessments. Additionally, the standards ISO/IEC 20924:2018 on IoT terminology [63] and ISO/IEC 30141:2018 [64] on IoT reference architecture that were published at the end of 2018 are currently under revision to accommodate the rapid evolution of IoT. From an European perspective, to address and support the envisioned digital single market [65] motivated by data-driven economic strategies [3], the European Telecommunications Standards Institute (ETSI) [5] is notably focused on data protection and privacy aspects of the IoT technology. Less than one month after the General Data Protection Regulation (GDPR) came to force in May 2018, ETSI published ETSI TS 103 458 v1.1.1 on applications of attribute-based encryption for Personally Identifying Information (PII) and personal data protection on IoT devices [66]. ETSI's efforts further supported ITU-T X.1362 [67] that was published a year prior. It is worth noting that ETSI also recently published the technical specification TS 103 645 [57] on cyber security for consumer IoT, addressing basic security provisions for IoT devices.

Moreover, the standardization landscape shows consensus on the direction of their work with all of International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ETSI) and International Telecommunication Union (ITU-T) currently developing standards for trustworthiness, data exchange and interoperability (cf. Table 4). Additionally, the contributions by the delegates and National Standards Bodies (NSB) within these SDOs show the diversity of the economic actors involved. This supports the argument made in [68] where P. Wiegmann et al. conclude that as more economic actors realize the importance of data protection and privacy in achieving this desired level of trustworthiness, the more they support and encourage *multi-mode* standardization, where research organizations, industries, governments and SDOs contribute to the common challenges in securing IoT and protecting users' information. This is further highlighted in Section 2.6. Additionally, the European Union Agency for Cybersecurity (ENISA) recently published a report on IoT security and privacy standardization gaps [69], which offers the interested reader a clear overview of the recent standards in support of different category of requirements, namely, security by design, privacy by design, organizational, people and process measures, and technical measures.

2.4.2. UAVs and Technical standardization

With reference to the use case introduced in Section 2.3.3, UAVs play an important role within the IoT ecosystem, as illustrated in Fig. 4, and hence, IoT standards may apply to a majority of UAV use cases. In contrast to IoT technical standardization committees, nonetheless, UAV standardization for commercial use is relatively recent with majority of subcommittees established after 2014.

However, as industry and research continue to find more means of utilizing UAV technologies to support IoT, the interest in their standardization and regulation increases.

A. IoT Published Standards		
Technical Committee	Standard Reference	Title
ISO/IEC JTC 1	ISO/IEC 21823-1:2019	Internet of Things (IoT) – Interoperability for internet of things systems – Part 1: Framework
	ISO/IEC 27701:2019	Security techniques – Extension to 27001/27002 for Guidelines for privacy information management
	ISO/IEC 20924:2018	Information technology – Internet of Things (IoT) – Vocabulary
	ISO/IEC 30141:2018	Information technology – Internet of Things (IoT) - IoT Reference Architecture
	ISO/IEC 27005:2018	Information technology – Security techniques – Information security risk management
	ISO/IEC 29134:2017	Information technology – Security techniques – Guidelines for privacy impact assessment
	ISO/IEC TR 22417:2017	Information technology – Internet of Things (IoT) - IoT use cases
	ISO/IEC 29161:2016	Information technology – Data structure - Unique identification for the Internet of Things
ETSI	ETSI TS 103 645 V1.1.1 (02/2019)	Cyber Security for Consumer Internet of Things
	ETSI TS 103 458 v1.1.1 (06/2018)	Application of Attribute Based Encryption for PII and personal data protection on IoT devices
	ETSI TR 103 376 (10/2016)	SmartM2M; IoT LSP use cases and standards gap
ITU-T	ITU-T X.1361 (09/2018)	Security framework for the Internet of Things based on the gateway model environments
	ITU-T X.1362 (03/2017)	Simple encryption procedure for Internet of Things (IoT) environments
	ITU-T Y.4115 (04/2017)	Reference architecture for IoT device capability exposure
	ITU-T Y.4455 (10/2017)	Reference architecture for Internet of Things network service capability exposure
B. IoT Under-development Standards		
Technical Committee	Standard Reference	Title
ISO/IEC JTC 1	ISO/IEC TR 30164	Internet of Things (IoT) – Edge Computing
	ISO/IEC 21823-2	Internet of Things (IoT) - Interoperability for IoT Systems - Part 2: Transport interoperability
	ISO/IEC 21823-3	Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability
	ISO/IEC 27030	Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)
	ISO/IEC 30147	Internet of Things (IoT) Methodology for implementing and maintaining trustworthiness of IoT systems and services
	ISO/IEC 30149	Internet of Things (IoT)–Trustworthiness framework
	ISO/IEC 30161	Internet of Things (IoT)–Requirements of IoT data exchange platform for various IoT services
C. UAV Under-development Standards		
Technical Committee	Standard Reference	Title
ISO/TC 20/ SC 16	ISO 21384-3	Unmanned aircraft systems – Part 3: Operational procedures
	ISO 21384-4	Unmanned aircraft systems – Part 4: Vocabulary
	ISO 23665	Unmanned aircraft systems – Training for personnel involved in UAS operations
	ISO 21895	Categorization and classification of civil unmanned aircraft systems
	ISO 23629-7	UAS Traffic Management (UTM) – General requirements for UTM

Table 4: Overview of published and under-development technical standards for IoT and UAVs within IoT context.

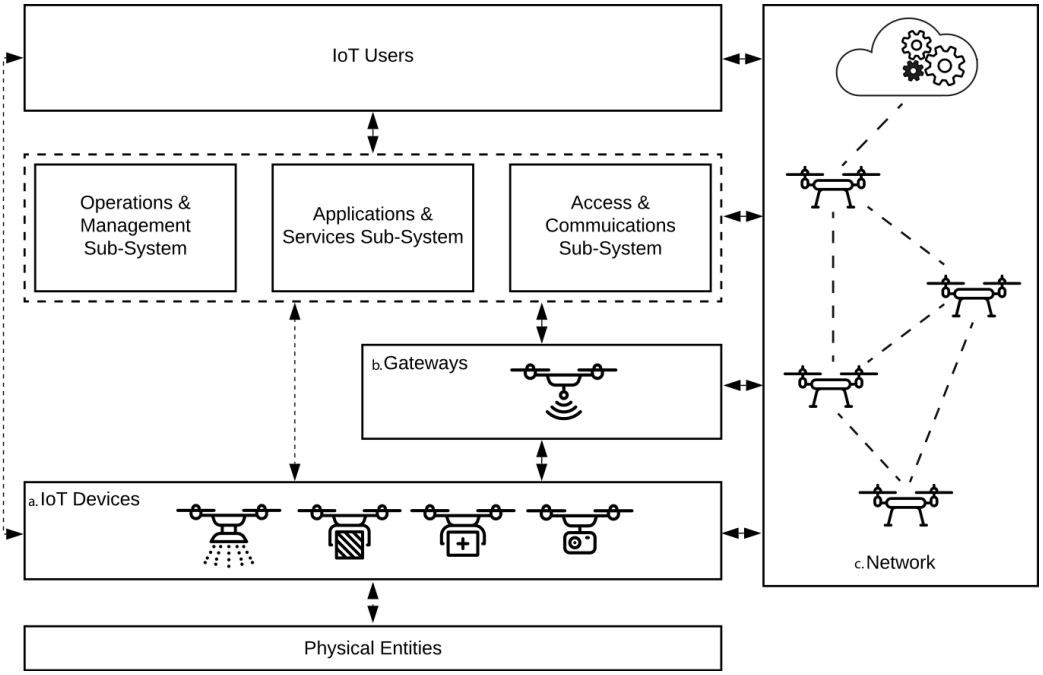

Fig. 4: Role of UAV within IoT as: a) smart terminal devices that interact with the physical world; b) aerial base stations and gateways; c) communication network connected to IoT cloud.

One of the more established international technical subcommittee is ISO/TC 20/SC 16 on Unmanned aircraft systems [70] with 17 countries participating members today but no published standards since its creation in 2014 and 6 under-development ones, five of which are highlighted in Table 4-C. The lack of published standards is again mostly because the majority of Working Groups (WG) have only been initiated recently, specifically after UAVs found their way into IoT as promising devices connected to this ubiquitous network. From EUROCAE WG 105 [71], European Union Aviation Safety Agency and SESAR Joint U-Space project [72] to ISO/TC 20/SC 16 on Unmanned Aircraft Systems, SDOs have actively started working on developing key standards for this promising IoT connected device/platform.

2.4.3. IoT Certification and Evaluation Frameworks

It is important to highlight that technical standards can be used, in certain contexts, for developing certification schemes and other standardized methods and frameworks that guide organizations' processes. Some widely known standards that can be used for certification purposes include ISO 9001 on quality management systems [73], ISO/IEC 27001 and 27002 [74] on information security management systems, or IEC 62443 cybersecurity certification. However, as mentioned in Section 2.3, most IT protocols and standards need to be adjusted to suit the new rapidly evolving IoT. Similarly, such legacy certifications and schemes of assessment do not accommodate the fast-paced development of IoT.

2.5. Gap Analysis

This section analyzes the gap between IoT research and standardization, discussed in Sections 2.3 and 2.4 respectively. To perform such an analysis, two main points are addressed: first defining a goal, and then evaluating and analyzing the current status to finally develop recommendations for a transformation roadmap in Section 2.6.

2.5.1. Defining the Goal

The goal is to enable governments, organizations, individuals and other stakeholders to utilize IoT to ideally its full potential. This can be achieved by (a) lowering barriers to entry for new market comers, (b) enabling fair

competition and (c) encouraging the introduction of new value-added services to benefit the society – without violating individuals' right of privacy and data protection.

2.5.2. Analysis

In light of the above global goal of research and standardization in IoT, technical terminology, reference architecture, interoperability and trustworthiness were selected as benchmarks for comparison as these four benchmarks form the pillars for the success of IoT as highlighted in Section 2.3 and Section 2.4.

As explained above, in order for organizations to place a strategic technological roadmap and to better manage data protection, privacy and security concerns they need to be able to accurately assess their current status as well as evaluate their products in the market; hence organizations typically perform regular risk assessments.

Depending on the field of work or economic sector of operation, organizations typically perform their risk management processes audits 1 to 4 times a year. Even though, this is sufficient for many technology-related fields, it remains insufficient for IoT due to the highly dynamic nature of the technology. In turn, this emphasizes the first gap in IoT standardization. To the best of our knowledge, there is currently no IoT-specific risk assessment framework developed by any SDO. P. Radanliev et al. in [75] empirically analyze gaps within different risk impact assessment approaches with the aim of identifying key elements for an IoT-specific framework. Some of the frameworks included in the study are the National Institute of Standards and Technology (NIST) framework, the Common Vulnerability Scoring System (CVSS), the Capability Maturity Model Integration (CMMI), Octave, the Transference, Avoidance, Reduction or Acceptance (TARA) framework, the Factor Analysis of Information Risk (FAIR) taxonomy, and ISO's frameworks [4]. P. Radanliev et al. then follow by extending how transformation roadmaps should adapt IoT risk assessment to the goal-oriented Approach and to the IoT Micro Mart Model further emphasizing the need for a standardized framework.

Additionally, P. Radanliev et al. in [4] outline a general taxonomic classification of cyber risk assessment requirements (cf. Fig. 5). This general classification can be extended to an IoT-specific one, in order to efficiently assess IoT security risks.

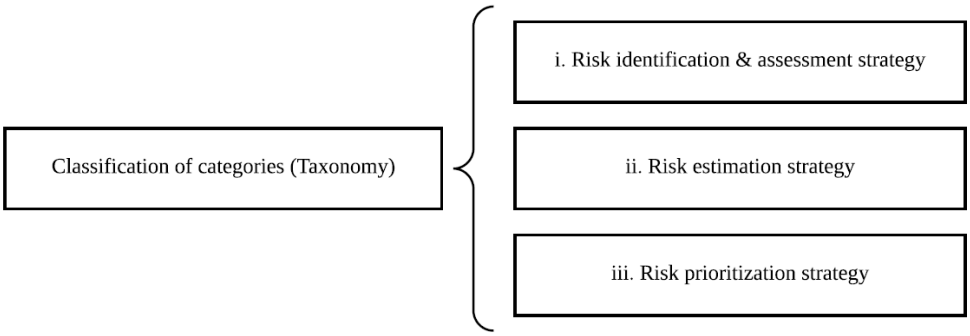

Fig. 5: Taxonomic classification of cyber risk assessment requirements [4].

Fig. 5 shows three main classifications of risk assessment strategies by P. Radanliev et al. in [4] where; i) risk identification assessment strategy covers: espionage, theft, or terrorist attacks, which in effect require electronic and physical security to anticipate and mitigate any risks.

Additionally, risk identification should be supported with forensics, prognostics, and recovery plans, for analysis of cyber-attacks and for coordination with agencies responsible to identify external cyber-attack vectors; ii) risk estimation strategy covers: information assurance, data security and protection for data in transit, from physical and electronic domains and storage facilities; and finally, iii) risk prioritization strategy which limits the access of source code to crucial personnel and provide software assurance and application security for eliminating deliberate flaws and vulnerabilities.

To prevent continuation of cyber-attacks, risk prioritization should focus on information sharing and reporting. Fast cyber-attack reporting and shared database resources should also be developed. This general classification can be adapted and extended to include more IoT-specific threats as mentioned in Table 1, Table 2 and Table 3 for UAV threats within the IoT ecosystem.

Nevertheless, SDOs have made an undeniable effort with respect to the first pillar or benchmark of comparison, technical terminology. Technical standardization committees took lead as they have published a standard on technical terminology (cf. Table 4). Additionally, considerable effort has been put into combining existing terminology and IoT concepts through multiple workshops [76]. On the other hand research lacks consistency, with multiple definitions and terminology for IoT concepts available in the literature as explained by A. Bassi et al. and J. Guth et al in [13], [14] respectively.

In [15] I. Addo et al. emphasize the importance of having a general IoT reference architecture to support the network's security and privacy. The necessity of a reference architecture for security is additionally stated in [12]. Nevertheless, the literature provides various architectures, for instance in [17] where A. Barba et al. propose architectures that could be used as reference models for a given IoT system. Moreover, Fig. 3 explains the main requirements for a general reference architecture. Clearly, devising an IoT reference architecture is an active research direction in IoT and a potential opportunity for SDOs to collaborate. Section 2.4 shows that in 2018, ISO/IEC JTC 1/SC 41 published an international standard for IoT reference architecture. However, SDOs are currently updating these standards as explained in section 2.4.1 to accommodate the dynamic and rapid evolution of IoT.

Another equally important research topic as explained in Section 2.3 is how to tackle interoperability challenges that come with the diverse communication protocols. Section 2.3 explores the challenges in data protection, privacy, and security in IoT and UAVs that can be categorized within the transmission and communication layers. Moreover, the lack of standardized systems, emphasized by current SDOs' efforts as seen in Table 4 through their under development standards, further supports this argument.

The aforementioned challenges, threats and developments lead up to the final and most critical pillar, trustworthiness, which is at the core of this work. ISO/IEC JTC 1 is putting great emphasis on defining trustworthiness within ICT and hence, study groups were established within JTC 1 subcommittees to address the matter [55]. With reference to Section 2.2 and specifically Figure 1, trustworthiness, a property of the integrity of an IoT system, depends on the indices of data protection and privacy. With regard to data protection and privacy, it was supported in [4] that research efforts are aligned with current market trends and needs. The research community is actively developing new methods and proposing new protocols and algorithms that support and further catalyze and facilitate the potential of IoT technology. However, it was realized that there was no consistency in how key terms are defined, as well as lack of collaboration between different parties working on similar challenges as A. Bassi et al. explained in [13], and as can be observed from the different proposed reference architectures [16], [17]. This in turn emphasizes the need for establishing globally-harmonized regulations to guide IoT research and help standardize definitions and concepts [52]. From the standardization point of view, data protection, privacy, and security remain among the main challenges that yet persist. SDOs have published a few standards as well as guidelines like ISO/IEC 27005:2018 [62] on information security risk management and ISO/IEC 29134:2017 [61] as a set of guidelines that can be used for privacy impact assessments required by the GDPR.

However, there is not yet any IoT-specific standards, similar to ISO/IEC27030 on guidelines for security and privacy in IoT (c.f. Table 4), that accommodate for the rapid development in the technology. This in turn shows a clear gap between research, where there is continuous work on methods and protocols for data protection and privacy, and standardization, where only a few guidelines, certifications and standards exist but merely accommodate fast-paced IoT developments. Analyzing research trends in Section 2.3 shows that work is being

intensified on finding new robust and scalable security and data protection measures for IoT. Some of these include:

- implementing better authorization mechanisms relying on the principle of least privilege [77], [78], which on the contrary is not supported by a specific standard;
- code isolation and better handling of information flow control (c.f. Table 1), however, no standardized guiding protocols exist;
- implementing new communication encryption techniques (c.f. Table 1), which again is not supported by a specific standard;
- devising robust behavior monitoring for malware detection protocols, as well as protocols to isolate any compromised IoT device (node), in an interconnected system, yet no specific standard protocol or guiding standard exists.

Nevertheless, it is important to note that the existence of multiple overlapping standards does not essentially mean that the problem is addressed as in many cases this could lead to contradicting security measures especially in a highly inter-operable system. In turn, emphasizing harmonization of existing standards and not only publishing new ones. This is supported by the ENISA report [69].

In summary, it could be referred to the two Technical Reports (TRs), ETSI TR 103 375 [79] and ETSI TR 103 376 [80] by Specialist Task Force 505 (STF) [5] which further support our analysis, summarized in Table 5. The ETSI's commissioned task, addressed two main projects, IoT Standards landscaping and IoT European Large Scale Pilots (LSP), and defined the following key next steps (from a high level perspective):

1) *"Defining a uniform IoT terminology,"*
2) *"Ensuring a high level of connectivity and interoperability between connected objects,"*
3) *"Establishing high level of security to protect connected objects from potential malicious uses or to protect data."*

Pillar	Gap Description
Terminology	Standards lack key terminology due to the rapid evolution of technology, similarly research suffers lack in harmonization.
Interoperability	Fragmentation of research landscape due to large number of heterogeneous competing communications protocols and networking technologies. Further emphasized due to incomplete or insufficient IoT-dedicated interoperability standards.
Reference Architecture	Recently published standards need updating to embrace the rapid evolution of IoT. Research provides multiple solutions however duplication require harmonization and consensus.
Trustworthiness	Research indicates that privacy and security issues are key blocking factors for users' acceptance. Additionally, only some security and privacy challenges are addressed in research on isolated application basis. Standardization landscape shows lack of IoT-specific standards while adoptable IT standards show need of harmonization.

Table 5: Summary of global IoT gap analysis findings.

Going further, with regard to the use case, even though UAV technology is evolving rapidly, certain IoT-based UAV applications cannot be further developed without a regulatory framework in place as explained by S. Pechetti et al. in [81]. A well-defined example is the use case of UAVs-as-a-Service described in Section2.3.3. The technology of UAVs is already at an advanced stage that enables many technology companies, such as DJI, Google, Amazon Prime Air and DHL, to place large investments in this market segment; however, it remains uncertain when and where commercial UAVs will be allowed to operate at a large scale within cities.

One main obstructing reason is the challenge of data protection, privacy, and security UAVs introduce. Research continuously works on addressing such pressing issues as explained in Section 2.3.3 where P. Blank et al. in [50] and N. Labib et al. in [47] address some of the critical challenges obstructing UAVs' deployment. However, S. Winkler et al. in [51] emphasize the need for a supporting regulatory framework for UAV operations. In response to this demand, various SDOs recently recognized the importance and implications of such regulations and have established dedicated working groups [70] to address these concerns.

2.6. Discussions and Insights

The analysis in Section 2.5 showed that among the many topics being studied and addressed, the lack of sufficient privacy and security protocols and supporting relevant standards is one of the main factors hindering the further development and adoption of IoT and IoT-based UAV applications. Another limiting factor that should be further investigated by SDOs and researchers is interoperability within the IoT ecosystem. As IoT is a system of systems, interoperability plays an essential role in ensuring the seamless flow of data across IoT systems within different contexts and value chains. This in turn emphasized the need for developing a standardized IoT reference architecture as explained in Section 2.3. Both research and standardization committees acknowledge the importance of having a general IoT reference architecture as well as realize its role in helping establish security, privacy and data protection within the IoT ecosystem. Moreover, regulations are needed as they form the critical foundations upon which certification mechanisms can be established as they play an important role when it comes to establishing digital trust and cultivating IoT trustworthiness within the market, technology, and end users.

To achieve an overall cross vertical IoT vision and lay down a roadmap to bridge the gaps identified in section 2.5, multi-mode standardization is encouraged. This way, governments, regulatory bodies, market leaders, SDOs, and research organizations will have aligned targets to ensure rapid development of regulations and standards to govern the fast-paced developments in IoT. This is evident in the widely adopted communication standards developed by the Institute of Electrical and Electronics Engineers (IEEE) through multi-mode standardization as explained by P. Wiegmann et al. in [68], a good example would be the widely used communication standards IEEE 802.11, 802.15.4 [82] which are commonly used within smart home IoT applications [43].

Finally, IoT research and standardization efforts show a promising momentum. In line with the analysis, collaborative workshops co-organized by SDOs, the European Commission, IoT research and innovation committees, and industry stakeholders will have an undeniable role in catalyzing and establishing consensus on IoT standards and future development. Regulations and technical standardization act as IoT technology safeguards, where standardization, encouraged by legal and regulatory affairs, help develop international digital infrastructures, which in turn help shape new regulatory models. This cycle is then completed with scientific research, which plays a critical role of continuously and systematically challenging and evaluating IoT technical standards.

2.7. The National Example for linking IoT Communities of Research and Standardization

In Luxembourg, ILNAS, the Luxembourg Institute of standardization, Accreditation, Safety and Quality of Products and Services – *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*, is the National Standards Body, which allows and encourages the participation of the national market in the standardization process. Initiatives are in place to foster collaborations with different stakeholders such as researchers, entrepreneurs, companies and individual experts. A specific national policy for ICT technical standardization [83] aims at developing market interest and involvement [56], promoting and reinforcing market participation, as well as supporting and strengthening the education about standardization and related research activities.

In line with the first objective to develop market interest and involvement, ILNAS has developed a Standards Analysis [60], which allows to identify easily standardization activities of different SDOs in the Smart Secure ICT area, including IoT. This document is a practical tool helping ILNAS to promote technical standardization in the IoT area and to raise awareness among national stakeholders.

Similarly, conforming to the second project - promoting and reinforcing market participation- ILNAS is actively involved in the development of standards as a P-member of ISO/IEC JTC 1/SC 41 and it follows closely the developments of standards of different technical committees (e.g.: ITU-T/SG 20, ETSI/TC Smart M2M). This participation in ISO/IEC JTC 1/SC 41 and monitoring of the standards developed by other SDOs, such as ETSI, allows ILNAS to actively transfer relevant information to the market and encourage its involvement in the standards development process.

Finally, to meet the third project of the policy - supporting and strengthening the education about standardization and related research activities - ILNAS has undertaken different initiatives, including the development of a White Paper on IoT, in collaboration with the Ministry of the Economy, with the goal of providing a comprehensive analysis of technological, economic, as well as technical standardization perspectives. Moreover, ILNAS works in collaboration with the University of Luxembourg (UL) and the Interdisciplinary centre of Security Reliability and Trust (SnT) on three ICT tracks to link research and standardization funding a unique doctorate program on linking research and standardization in Internet of Things, Artificial Intelligence (AI) and Cloud Computing. One first result of this research program was the publication in October 2018 of a White Paper Data Protection and Privacy in Smart ICT [2], which is extended with this technical report for the IoT domain. In parallel, in 2016, the UL/SnT-ILNAS collaboration launched the professional degree program Smart ICT for business innovation [84], to be extended to a complete professional Master program by 2020.

2.8. Summary

IoT can be considered one of the transformative technologies in the recent years as it extends the internet by envisioning a world where anything can be connected, hence creating tremendous potential of value-added applications, attracting unparalleled attention of a magnitude of stakeholders from various domains and economic sectors. However, it is important to identify and tackle the challenges that accompany such unprecedented connectivity and computing capabilities, specifically those related to security, privacy and data protection in order to achieve and maintain an acceptable level of trustworthiness.

This study presents a notion for trust and trustworthiness in IoT and emphasizes the importance of security, privacy and data protection as the main pillars of achieving IoT trustworthiness. Throughout the paper, the sections present an analysis of the current status in IoT research as well as standardization with the aid of an illustrative use case of UAVs-as-a-Service. The use case demonstrates the orchestration between different IoT systems highlighting key challenges in UAVs as an IoT device with enormous economical and societal impact. The study then presents an analysis of gaps between research and standardization followed by remarks to aid technical committees and researchers lay down their transformation roadmaps and future directions.

The analysis indicates the need of harmonization of research work and consensus between SDOs to avoid standards duplication. Additionally, the report emphasizes the need of establishing a standardized risk assessment framework dedicated for IoT, to complement existing impact assessment guidelines, in order to more accurately identify, estimate/quantify and prioritize risk strategies, as a first step in complying with GDPR but also in bridging and narrowing gaps between market needs, research and standardization.

List of Acronyms and abbreviations

CMMI	Capability Maturity Model Integration
CoAP	Constrained Application Protocol CVSS Common Vulnerability Scoring System DDoS Distributed Denial-of-Service
DPIA	Data Protection Impact Assessment
DTLS	Datagram Transport Layer Security
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FAIR	Factor Analysis of Information Risk
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers IFC Information Flow Control
ILNAS	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
IoT	Internet of Things
IPS	Intrusion Protection Systems
IPSec	IP Security
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union
LSP	Large Scale Pilots
NIST	National Institute of Standards and Technology
SC	Subcommittee
SDO	Standards Development Organization
SOAP	Simple Object Access Protocol
STF	Specialist Task Force 505
TARA	Transference, Avoidance, Reduction or Acceptance
TC	Technical Committee
TR	Technical Report
UAV	Unmanned Aerial Vehicle
WG	Working Group

References

[1] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "Trustworthiness in IoT - A Standards Gap Analysis on Security, Data Protection and Privacy–*Submitted,"* in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, Oct 2019.

[2] ILNAS, White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical standardization, ILNAS, ANEC G.I.E, University of Luxembourg, Tech. Rep., 2018.

[3] E. B. Mario Grotz, Gabriel Crean, "The data-driven innovation strategy for the development of a trusted and sustainable economy in Luxembourg," Ministry of the Economy, Luxembourg, Tech. Rep., 2019.

[4] P. Radanliev, D. C. D. Roure, R. Nicolescu, M. Huth, R. M. Montalvo, S. Cannady, and P. Burnap, "Future developments in cyber risk assessment for the internet of things," *Computers in Industry*, vol. 102, p. 1422, 2018.

[5] "Specialist Task Force 505," https://portal.etsi.org/STF/stfs/STFHomePages/STF505, accessed: 2019-07-11.

[6] M. Marchese, A. Moheddine, and F. Patrone, "Iot and uav integration in 5g hybrid terrestrial-satellite networks," Sensors, vol. 19, no. 17, p. 3704, 2019.

[7] R. Hardin, "Trust. cambridge: Polity," 2006.

[8] ILNAS, "Digital Trust for Smart ICT," Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS), White Paper.

[9] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 1, pp. 1–25, 2004.

[10] M. Nitti, R. Girau, A. Floris, and L. Atzori, "On adding the social dimension to the internet of vehicles: Friendship and middleware," in *2014 IEEE international black sea conference on communications and networking (BlackSeaCom)*. IEEE, 2014, pp. 134–138.

[11] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security "Hands-on"," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 37–46, 2016.

[12] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, "Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 10–16, June 2017.

[13] A. Bassi, M. Bauer, M. Fiedler, and R. v. Kranenburg, *Enabling things to talk*. Springer-Verlag GmbH, 2013.

[14] J. Guth, U. Breitenbu¨cher, M. Falkenthal, P. Fremantle, O. Kopp, F. Leymann, and L. Reinfurt, "A detailed analysis of IoT platform architectures: concepts, similarities, and differences," in *Internet of Everything*. Springer, 2018, pp. 81–101.

[15] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, "A Reference Architecture for Improving Security and Privacy in Internet of Things Applications," in *2014 IEEE International Conference on Mobile Services. IEEE*, 2014, pp. 108–115.

[16] M. Weyrich and C. Ebert, "Reference architectures for the Internet of Things," *IEEE Software*, no. 1, pp. 112–116, 2016.

[17] A. J. Barba and F. A. de Castro Giorno, "A Reference Architecture for the IoT Services' Adaptability-Using Agents to Make IoT Services Dynamically Reconfigurable." in *IoTBDS*, 2018, pp. 187–194.

[18] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the internet of things," *Future Generation Computer Systems*, vol. 75, pp. 46–57, 2017.

[19] ISO/IEC, "ISO/IEC 21823-1:2019 Internet of things (IoT) – Interoperability for internet of things systems – Part 1: Framework," International Organization for Standardization, Geneva, CH, Standard.

[20] J. A. Stankovic, "Research Directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[21] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," 2018.

[22] "General Data Protection Regulation (GDPR)," https://gdpr-info.eu/, accessed: 2019-07-19.

[23] M. Henze, L. Hermerschmidt, D. Kerpen, R. Ha¨ußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based internet of things," *Future Generation Computer Systems*, vol. 56, pp. 701–718, 2016.

[24] R. Rios and J. Lopez, "(un) suitability of anonymous communication systems to wsn," *IEEE Systems Journal*, vol. 7, no. 2, pp. 298–310, 2012.

[25] M. H. Behfar, E. Moradi, T. Björninen, L. Sydänheimo, and L. Ukkonen, "Design and technical evaluation of an implantable passive sensor for minimally invasive wireless intracranial pressure monitoring," in *World Congress on Medical Physics and Biomedical Engineering, June 7-12, 2015, Toronto, Canada*. Springer, 2015, pp. 1301–1304.

[26] S. Landau, "What was samsung thinking?" IEEE Security & Privacy, vol. 13, no. 3, pp. 3–4, 2015.

[27] S. B. Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and integrity for data aggregation in wsn using homomorphic encryption," *Wireless Personal Communications*, vol. 80, no. 2, pp. 867–889, 2015.

[28] S. Ozdemir, M. Peng, and Y. Xiao, "Prda: polynomial regression-based privacy-preserving data aggregation for wireless sensor networks," *Wireless communications and mobile computing*, vol. 15, no. 4, pp. 615–628, 2015.

[29] K. Hayawi, A. Mortezaei, and M. V. Tripunitara, "The limits of the trade-off between query-anonymity and communication-cost in wireless sensor networks," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*. ACM, 2015, pp. 337–348.

[30] J.-R. Jiang, J.-P. Sheu, C. Tu, J.-W. Wu et al., "An anonymous path routing (apr) protocol for wireless sensor networks." J. Inf. Sci. Eng., vol. 27, no. 2, pp. 657–680, 2011.

[31] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3769–3779, 2008.

[32] J. Chen, X. Du, and B. Fang, "An efficient anonymous communication protocol for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 12, no. 14, pp. 1302–1312, 2012.

[33] R. Rios, J. Cuellar, and J. Lopez, "Probabilistic receiver-location privacy protection in wireless sensor networks," *Information Sciences*, vol. 321, pp. 205–223, 2015.

[34] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[35] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design* (ICED), Aug 2016, pp. 321–326.

[36] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, p. 3.

[37] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "Flowfence: Practical data protection for emerging iot application frameworks," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 531–548.

[38] K. R. Sollins, "IoT Big Data Security and Privacy Versus Innovation," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1628–1635, 2019.

[39] R. Thorburn, A. Margheri, F. Paci et al., "Towards an integrated privacy protection framework for IoT: contextualising regulatory requirements with industry best practices." in *Proceedings of the 2nd Living in the Internet of Things conference*, 2019.

[40] Y. Yang, H. Cai, Z. Wei, H. Lu, and K.-K. R. Choo, "Towards lightweight anonymous entity authentication for iot applications," in *Australasian Conference on Information Security and Privacy*. Springer, 2016, pp. 265–280.

[41] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," *tech. report MSR-TR-2017-16*, 2017.

[42] A. Levy, M. P. Andersen, B. Campbell, D. Culler, P. Dutta, B. Ghena, P. Levis, and P. Pannuto, "Ownership is theft: Experiences building an embedded os in rust," in *Proceedings of the 8th Workshop on Programming Languages and Operating Systems*. ACM, 2015, pp. 21–26.

[43] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security implications of permission models in smart-home application frameworks," *IEEE Security & Privacy*, vol. 15, no. 2, pp. 24–30, 2017.

[44] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare internet of things," *Future Generation Computer Systems*, vol. 64, pp. 108–124, 2016.

[45] S. Raza, T. Helgason, P. Papadimitratos, and T. Voigt, "Securesense: End-to-end secure communication architecture for the cloud-connected internet of things," *Future Generation Computer Systems*, vol. 77, pp. 40–51, 2017.

[46] H. H. Pajouh, R. Javidan, R. Khayami, D. Ali, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks," *IEEE Transactions on Emerging Topics in Computing*, 2016.

[47] N. S. Labib, G. Danoy, J. Musial, M. R. Brust, and P. Bouvry, "A Multilayer Low-Altitude Airspace Model for UAV Traffic Management." ACM, Nov 2019.

[48] T. Lagkas, S. Bibi, V. Argyriou, and P. Sarigiannidis, "uav iot frameworks views and challenges: Towards protecting drones as "things"," 11 2018.

[49] "Data from the sky - Traffic Monitoring," http://datafromsky.com, accessed: 2019-07-18.

[50] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-aware restricted areas for unmanned aerial systems," *IEEE Security & Privacy*, vol. 16, no. 2, pp. 70–79, 2018.

[51] S. Winkler, S. Zeadally, and K. Evans, "Privacy and civilian drone use: The need for further regulation," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 72–80, 2018.

[52] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "On standardised uav localisation and tracking systems in smart cities," in *Proceedings of 17th Annual STS Conference Graz 2018 Critical Issues in Science, Technology and Society Studies*. May, 2018.

[53] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "Uav iot framework views and challenges: towards protecting drones as things," *Sensors*, vol. 18, no. 11, p. 4015, 2018.

[54] S. Wagle and J. E. Pecero, "Efforts towards iot technical standardization," *ADHOC-NOW 2019*, no. 1, pp. 1–16, 2019.

[55] "Subcommittees and working groups (IEC-ISO/IEC JTC1)," https://www.iec.ch/dyn/www/f?p=103:29:13789532098875::::FSP ORG ID,FSP LANG ID:3387,25#3, accessed: 2019-07-11.

[56] ILNAS, "White Paper: Internet of Things - Technology, Economic View and Technical Standardization," ILNAS ANEC G.I.E, Tech. Rep., 2018.

[57] ETSI, "ETSI TS 103645 V1.1.1 Cyber Security for Consumer Internet of Things (IoT)," ETSI, Technical Standard.

[58] ISO/IEC, "ISO/IEC 21823-2 ED1 Internet of Things (IoT) - Interoperability for IoT Systems - Part 2: Transport interoperability," International Organization for Standardization, Geneva, CH, Standard.

[59] ——, "ISO/IEC 21823-3 ED1 Internet of Things (IoT) - Interoperability for IoT Systems - Part 3: Semantic interoperability," International Organization for Standardization, Geneva, CH, Standard.

[60] ILNAS, "Standards Analysis: Smart Secure ICT," ILNAS ANEC G.I.E, Tech. Rep., 2018.

[61] ISO/IEC, "ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for privacy impact assessment," International Organization for Standardization, Geneva, CH, Standard.

[62] ——, "ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management," International Organization for Standardization, Geneva, CH, Standard.

[63] ——, "ISO/IEC 20924:2018 Information technology – Internet of Things (IoT) – Vocabulary," International Organization for Standardization, Geneva, CH, Standard.

[64] ——, "ISO/IEC 30141:2018 Internet of Things (IoT) – Reference Architecture," International Organization for Standardization, Geneva, CH, Standard.

[65] "European Digital Single Market," https://ec.europa.eu/commission/priorities/digital-single-market en, accessed: 2019-07-18.

[66] ETSI, "ETSI TS 103458 v1.1.1 Application of Attribute Based Encryption for PII and personal data protection on IoT devices," ETSI, Technical Standard.

[67] ITU-T, "ITU-T X.1362 Simple encryption procedure for Internet of Things (IoT) environments ," ITU-T, Technical Standard.

[68] P. M. Wiegmann, H. J. de Vries, and K. Blind, "Multi-mode standardisation: A critical review and a research agenda," *Research Policy*, vol. 46, no. 8, pp. 1370–1386, 2017.

[69] "IoT Security Standards Gap Analysis," https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis, accessed: 2019-07-19.

[70] "ISO TC 20/SC 16," https://www.iso.org/committee/5336224.html, accessed: 2019-07-11.

[71] "EUROCAE working groups," https://www.eurocae.net/about-us/working-groups/, accessed: 2019-07-11.

[72] "U-Space Project," https://www.sesarju.eu/U-space, accessed: 2019-07-11.

[73] "ISO 9001 Quality management," hhttps://www.iso.org/iso-9001-quality-management.html, accessed: 2019-07-30.

[74] "ISO 27000 family on Information Security Management Systems," https://www.iso.org/isoiec-27001-information-security.html, accessed: 2019-07-30.

[75] P. Radanliev, D. C. De Roure, J. R. C. Nurse, P. Burnap, E. Anthi, U. Ani, L. Treall Maddox, O. Santos, and R. Mantilla Montalvo, "Definition of Internet of Things (IoT) Cyber Risk Discussion on a Transformation Roadmap for Standardisation of Regulations Risk Maturity Strategy Design and Impact Assessment," *arXiv e-prints*, p. arXiv:1903.12084, Mar 2019.

[76] "Towards a Definition of the Internet of Things (IoT)," https://iot.ieee.org/definition.html, accessed: 2019-07-18.

[77] J. Sachowski, *Implementing digital forensic readiness: From reactive to proactive process*. CRC Press, 2019.

[78] J. Bacon, D. Eyers, T. F. J. . Pasquier, J. Singh, I. Papagiannis, and P. Pietzuch, "Information flow control for secure cloud computing," *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, pp. 76–89, March 2014.

[79] ETSI, "ETSI TR 103 375 v1.1.1 SmartM2M; IoT Standards landscape and future evolutions ," ETSI, Technical Report.

[80] ——, "ETSI TR 103 376 v1.1.1 SmartM2M; IoT LSP use cases and standards gaps ," ETSI, Technical Report.

[81] S. V. Pechetti, A. Jindal, and R. Bose, "Exploiting Mapping Diversity for Enhancing Security at Physical Layer in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 1, p. 532544, 2019.

[82] "IEEE Standards," https://standards.ieee.org/standard/, accessed: 2019-07-11.

[83] ILNAS, "Policy on ICT technical standardization (2015-2020)," https://portail-qualite.public.lu/dam-assets/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf, accessed: 2019-09-17.

[84] "Smart ICT Certificate for Business Innovation," https://wwwen.uni.lu/studies/fstc/certificate smart ict for business innovation, accessed: 2019-07-18.

3. Artificial Intelligence and Big Data: Gap Analysis between Scientific Research and Technical Standardization

Technical Report on Data Protection and Privacy in Smart ICT

Abstract

The emergence of Artificial Intelligence (AI) and its applications in several domains has raised debates regarding threats and vulnerabilities while adopting AI systems. Unlike traditional software systems, AI systems deal with a large amount of various data, called Big Data, which are highly correlated with individuals' privacy. In a broader perspective, AI systems are expected to deliver reasonable results even for events that were not part of their training. Therefore, trustworthiness and data protection are essential elements for such systems when being adopted by various stakeholders. Various studies in the literature have discussed the risks and challenges of data protection, privacy, and trustworthiness of AI. Companies, governments, and business sectors often rely on guidelines provided by Standards Developing Organizations (SDOs) and regulations to ensure secure and safe implementation of technology. For privacy and trustworthiness concerns to be addressed adequately while adopting AI, the knowledge gap between research, standardization and regulations should be bridged. In this study, the aim is to highlight the gaps between research and standardization by providing the surveys of activities of both fields towards privacy, data protection and trustworthiness of AI. The potential improvements towards developing guidelines based on scientific outcomes are introduced to adopt and integrate privacy-preserving and trustworthiness AI systems in related domains.

3.1. Introduction

The accumulation of enormous data along with the advanced data analysis and statistical techniques, hand in hand with the significant growth in computing power, AI systems have become ubiquitous and a powerful tool in several domains. The huge volume of data assembled by various sources, from connected devices to social media, termed as Big Data [1], is a valuable asset that has motivated governments, business sectors and companies to benefit from AI for several purposes such as to gain insights, prediction, and for decision making. Only between 2018 and 2019, the AI market has increased by 154%, reached a $14.7 billion market size in the world [2]. It is foreseen that the revenues of the world market will reach almost $37 billion by 2025 [3]. Due to the high demand from the industry, various Standards Developing Organization SDOs have set up Sub-committees (SCs) with the scope of providing standardization in the area of AI to help different sectors and companies for the adoption of AI and to address the concerns raised by this technology.

Although, the integration of Artificial Intelligence (AI) in various domains such as transportation, finance, and education [4] has greatly benefited society, it presents a variety of challenges and questions regarding the privacy and trustworthiness of the systems including the discrimination of the outcomes, system failure against false, unseen, or untrusted data, and privacy leakage. Protecting individuals' data in AI systems against these challenges is not a trivial task due to the complexity and characteristic of AI systems compared to the conventional software systems. New assets are raised by AI, it is not only the data which is a valuable property within companies that are adopting AI but also the core learning model and the extracted coefficients and parameters corresponding to that specific model, and the results as well. Therefore, the data protection, privacy, and trustworthiness have become the most challenging issues in recent years when it comes to any system that benefits from AI which is the focus of this study.

Developing solutions allowing AI systems to learn from large-scale, often sensitive datasets while preserving people's privacy is one of the main challenges. Recent studies have focused on data analysis, considering data protection, privacy, and security in the three main phases of Big Data analysis including data preparation, data

processing and data analysis [5]. However, the growth of Machine Learning (ML) and AI systems has raised new data protection, privacy, and trustworthiness concerns.

The technology has been the target of many adversarial attacks [6], [7], [8], [9] in the last couple of years within different applications such as medical systems [6], [10], face recognition [11], [12], speech recognition [13], sentiment analysis [14], image classification [15], finance and banking [16]. In a recent paper published in Science [17], the impact of adversarial attacks against AI medical systems shows that under such attacks an image of a melanocytic nevus is recognized as malignant with a high confidence score. The reported attacks and their impact on society and individuals highlight the urgency of identifying threats towards developing defense mechanisms and hence defining verified AI systems [18] by SDOs.

3.1.1.Background Information

In computer science, AI is associated with the accomplishments of tasks or problems by computers for which human intelligence is assumed to be required. AI is designed such that it acquires information from the environment as the input and takes actions to maximize success in achieving particular goals [19], [20]. One way of achieving AI is by ML techniques which are build based on the concept of "without being explicitly programmed". Indeed, without ML an AI software requires developing a million lines of complex rule-based codes. In principle, ML consists of a set of algorithms and statistical models for computer systems to efficiently perform a particular task without relying on rule-based programming or human interaction [21]. Developing the mathematical model is strongly dependent on the dataset, referred to as training data, which allows the program to gradually improve through the experiences and learning process from the data [22] for predicting, detecting or making decisions [23].

In a high-level overview there are three categories of methods functioning in various problems regarding AI and ML: **1) Supervised learning, 2) Unsupervised learning,** and **3) Reinforcement learning**. Figure 1 describes these methods and the most prominent techniques within each category, which lead to different applications and problem solving.

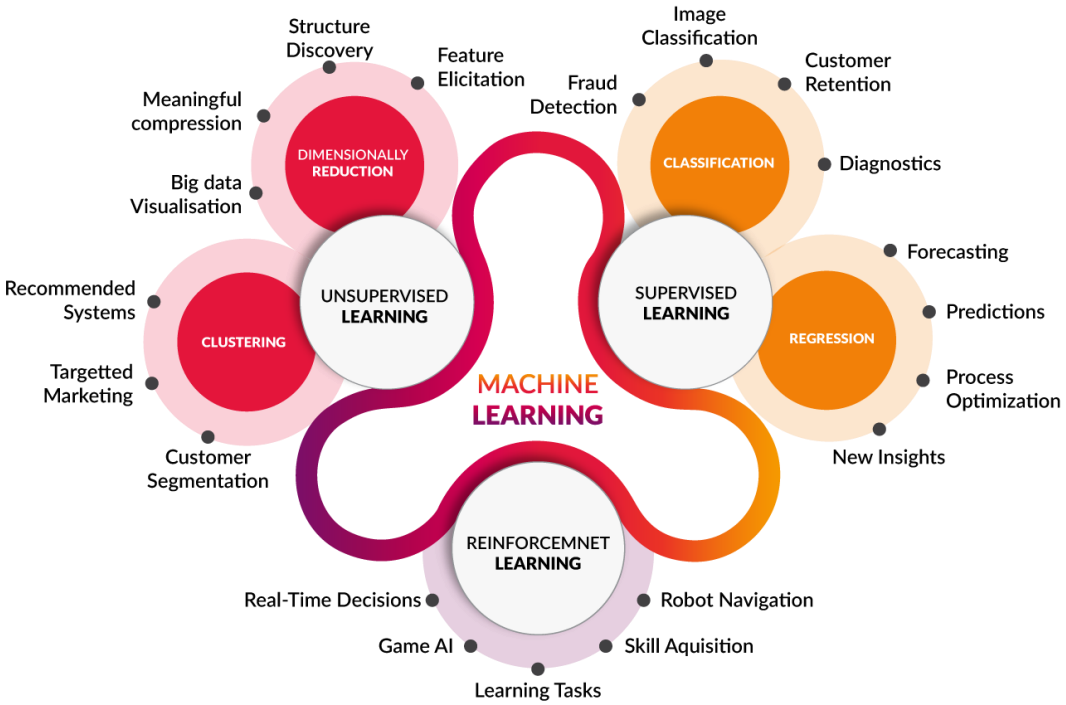

Fig. 1: Applications of different Machine Learning techniques: Unsupervised, Supervised and Reinforcement Learning [26].

As shown in Figure 1, Regression and Classification techniques are mostly used in supervised learning to predict or classify data based on the knowledge learned from the dataset which has been tagged by labels. Unsupervised learning, on the other hand, is mostly employed for extracting new information from the data and to recommend new options (e.g., marketing advertisements) by using techniques such as Clustering or Dimensional Reduction. Furthermore, reinforcement learning is about to learn depending on a sequence of previous actions to maximize a total reward for the system. An example for reinforcement learning is the machines which are beating humans in computer games [24] such as the ancient game of GO [25] that is a self-thought AI program which has yet the best response.

The main target of this study is the AI systems which are based on ML techniques. For the purpose of this study, we defined an AI life-cycle in Figure 2 that is considered as a framework to address the challenges and threats of AI.

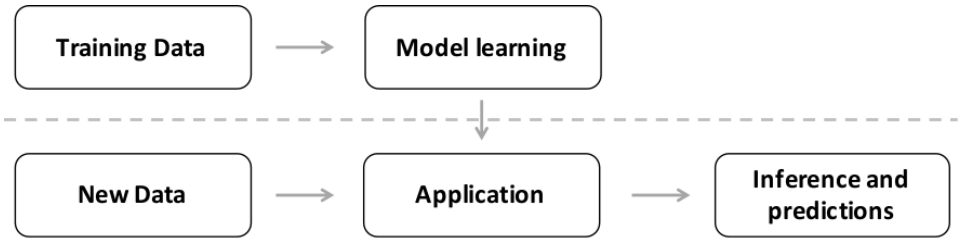

Fig. 2: AI life-cycle scheme.

3.1.2. Contribution

The main contributions of this study are threefold: 1) It provides a survey and analysis on data protection, privacy, and trustworthiness challenges of AI and Big Data based on the state-of-the-art research. 2) A survey of standardization and the activities of SDOs for the data protection, privacy, and trustworthiness of AI. 3) A gap analysis considering both perspectives to identify and highlight the gaps such that business sectors, industries, and governments can adopt secure, and trustworthiness AI.

The remainder of this study is structured as follows: Section 3.2 describes the scientific perspective on data protection, privacy, and trustworthiness considering the most recent papers and research outcomes in different AI systems. Section 3.3 presents the perspective of SDOs by describing the activities and existing projects. Next, in Section 3.4 a gap analysis is provided as a result of the two provided surveys with the purpose of analyzing the connection between research and standardization. The insights and discussion based on the gap analysis are provided in Section 3.5. Section 3.6 provides a National Example for linking AI Communities of Research and Standardization. Finally, Section 3.7 summarizes and concludes the paper.

3.2. Data Protection, Privacy, and Trustworthiness

The challenges and threats regarding data protection, privacy, and trustworthiness are classified from several perspectives in the literature [27], [28]. In this study, the life-cycle of AI systems presented in Figure 2 has been considered as the backbone to highlight threats which compromise data protection, privacy, and trustworthiness at each stage. Figure 3 describes the privacy and safety violations in different stages of an AI system life-cycle, and the details regarding these violations are provided in next subsections.

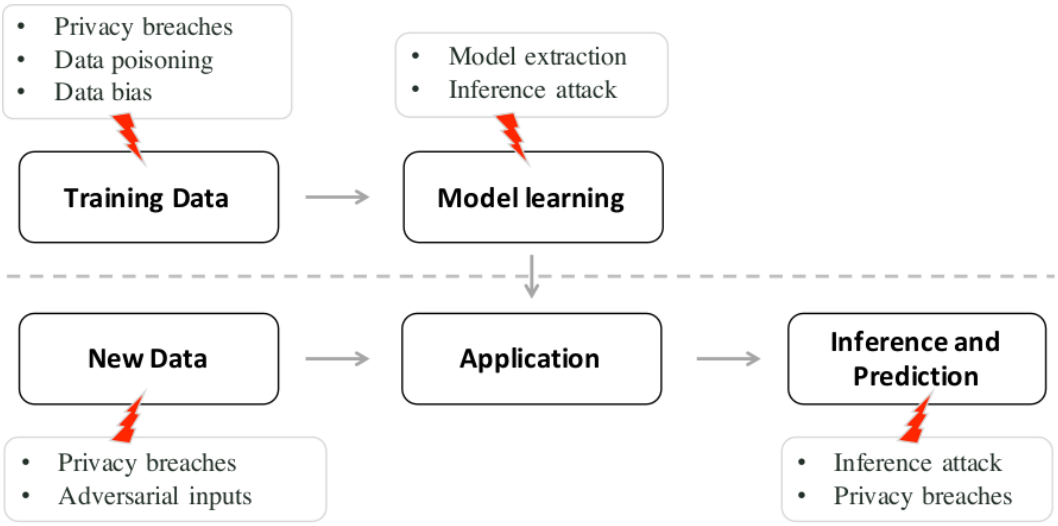

Fig. 3: Privacy violations in different stages of AI life-cycle.

3.2.1.Data Privacy Breaches

The data protection mechanisms from the literature are classified into three defense levels that have protected data over time and yet the list is evolving to more advanced mechanisms [29].

1) **Anonymization**. Data anonymization is a type of information sanitation for privacy and data protection. The process is followed by removing personal identifiers from datasets, such that they remain anonymous. The two main functions as the basic tools for unionisation are generalisation (replacing the data with less precise information [30]) and suppression (removing the identifiers from the data or replacing them with tags [31]), that are applied to data before publishing it.
2) **De-identification**. The process that is used to prevent an individual's identity from being connected with other information in a dataset [32]. The k-anonymity [33] is one popular technique of this family of de-identification.
3) **Privacy-Enhancing Techniques (PET)**. A set of methods for protecting personal data by minimising the possession of personal data without losing the functionality of an information system [34].

Figure 4 describes the defense level evolution of privacy-preserving techniques considering the significant growth of Big Data and data analysis techniques. Data protection started with the anonymization techniques for datasets consisting of low- dimensional data where only replacing clear identifier was enough solely to provide privacy and data protection. However, in an experiment, researchers were able to re-identify the medical records of the Governor by benefiting from a second dataset of the public electoral rolls of the city of Cambridge [35]. A study on mobile phone metadata revealed that unique identification of 95% of individuals from a population of 1.5 million people, requires only 4 approximate location and time data points [36]. Thus, to prevent the re-identification in such datasets, the second defense level was developed by k-anonymity [33]. The k-anonymity is a property of dataset which describes the level of anonymity within that dataset such that the identity of each individual is not distinguishable from at least k-1 other individuals. The l-diversity and t-closeness are the extensions of this method. With the evolution in the nature of data and computational approaches, the conventional de-identification methods become obsolete [37]. Big Data is generated not only in a great volume but also in high-dimensions where the sensitivity of data might not be visible in such a rich dataset. Nevertheless, AI and ML techniques might infer individuals' sensitive information through the data analysis. Hence, the third defense level of data protection mechanism deployed under PET to allow datasets to be analyzed with AI and ML algorithms in a privacy-preserving way by using a mix of access control and data protection mechanisms. Different methods of PET are described in more detail in [5].

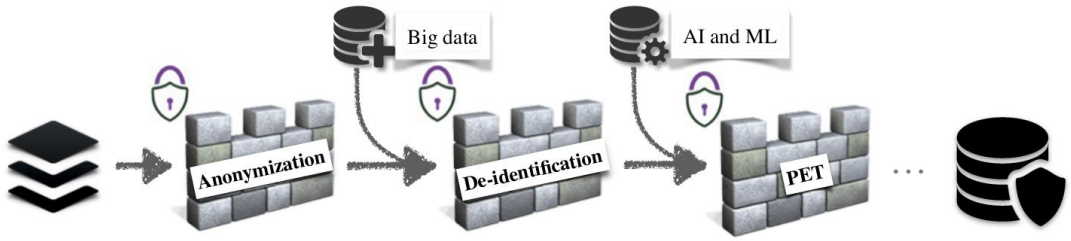

Fig. 4: A general overview of the evolution of defense techniques for AI and Big Data analysis.

Table 1 describes techniques within each defense mechanism and examples of applications for each model along with attack models.

Defense level	Techniques	Applications	Attack examples
Anonymization	Generalization Suppression	Health data [38] Web browsing	Re-identification [35]
De-identification	k-anonymity l-diversity t-closeness	Location-based services [39], [40] e-health [41] Wireless sensor networks [42]	Re-identification of behavioral datasets [43], [44] Risk of inference [45], [46]
Privacy-enhancing Technologies (PET)	Homomorphic encryption (HE) Differential privacy Federated Learning [52]	Bitcoin [47] e-health [48], [49] Recommender systems [50]	Attack on a HE scheme [51]

Table 1: The description of different techniques for each defense level.

The next generation of the privacy-preserving framework is focused on the concept of *sending the code to the data*. The OPen ALgorithms (OPAL) project [29] has combined different mechanisms such as access-control protocols, aggregation schemes to develop a platform, which allows third-parties (e.g., researchers) to submit algorithms that will be trained on data. The privacy of individuals, however, is guaranteed while data is being analyzed. Moreover, Google's DeepMind [53] has also developed a *verifiable data audit,* which ensures that any interaction with health records data is recorded and accessible to mitigate the risk of foul play.

3.2.2.Biased Data

The decisions achieved by AI systems can reinforce injustice and discrimination [54] for the purpose of shortening candidate lists for credit approval, hiring, and criminal legal system [55]. In a project by MIT [56] known as Gender shade[3], the AI gender classification products are being analyzed. They reveal the error rate of gender classification systems sold by giant technology companies (e.g., Microsoft, IBM, and Amazon) in 2018 up to 34.4% on classifying men and women with darker skin tone. Even though some of these systems have significantly improved to reduce the bias in the detection algorithm by 2019 [57], they did not eliminate it thoroughly [58].

Bias is not a deliberate feature of AI systems, but rather the result of biases presents in the input data used to train the systems [59]. However, it can target different features and attributes in decisions making including gender, race, age, national origin, etc. Overall, the most dominant types of bias that are identified in AI systems lie into the four categories: 1) Sample Bias describing an unbalanced representation of samples in the training data, 2) Algorithm Bias which refers to the systematic errors in the system, 3) Measurement Bias results from poorly measuring the outcome, and 4) Prejudicial Bias indicates the incorrect attitude upon an individual data.

[3] http://gendershades.org/

To identify different types of bias various metrics are introduced in the literature [59], [60] including difference in means, difference in residuals, equal opportunity, disparate impact, and normalized mutual information. Moreover, benefiting from the metrics, methods to mitigate AI bias are developed such as optimized preprocessing [61], reject option classification [62], learning fair representations [63], and adversarial debiasing [64]. Besides, several toolboxes are developed as well which have accumulated the identification metrics along with the mitigation methods for different ML algorithms into a framework to diagnose and remove AI bias. The available toolboxes are Lime [65], FairML [66], Google What-If and IBM Bias Assessment Toolkit [67], which is mostly used for face detection systems.

3.2.3.Data Poisoning

Data poisoning is an attack that happens in AI systems by injecting adversarial training data into the system to corrupt the model and force it to produce false results [68]. The attack works in different ways: one common adversarial model is to alter the boundaries of the classifier such that it misclassifies the categories in the favour of the attacker. This is known as the model skewing in poisoning attacks. The other type of poisoning attack happens by polluting the feedback mechanisms as a mean to misclassify the abusive and good contents. This attack is called feedback weaponization. In a particular study on injecting poisoned sample to a deep learning model [69], it is shown that only 50 polluted samples are enough to achieve a 90% attack success in the system.

An early example of poisoning attacks is the signature generation misleading against malware detection [70] in 2006. Researchers have investigated the feasibility of poisoning attacks against different ML algorithms such as Support Vector Machine (SVM) classifier. In a study [71] the effect of adversarial data manipulation on SVM has been studied. In another study [72] the authors have proposed countermeasures towards a robust SVM algorithm. Moreover, [73] has studied regression learning and defined countermeasures for data poisoning in regression learning. While these research have focused in within an offline setting, others investigated the online settings [74], [75]. In [74], authors considered an online setting and studied a data poisoning attack strategy assuming it as an optimization problem. They suggested a strategy to reduce the poisoning attack of ML algorithms in online learning. Several other studies [68], [76], and [69] have investigated on the challenges and threats posed by poisoning attack in learning models and developed frameworks and strategies to protect ML against poisoning attacks by evaluating their model on various datasets in realistic settings.

3.2.4.Model Extraction

Trained models in AI represent valuable intellectual property assets which are trained by particular datasets such as medical records, financial transactions. They can be the target of adversaries to duplicate the model - for example a stock prediction model- to design another model against it [77]. Thus, the protection of the confidentiality of machine learning models is one of the main concerns of stakeholders. The model extraction attack is applicable to many popular ML algorithms such as logistic regression, linear classifier, support vector machine, and neural network [78], [79]. Therefore, new security measures should be developed to protect these assets.

There are two types of model extraction attacks: 1) *Model inversion attacks*, and 2) *Membership and property inference*. The former can be done by reverse-engineering given the input and output from the model [80] or more precisely sending queries and analyzing the response [77]. The authors prove that only by sending hundreds of queries to the system, they can clone the system with almost 100% of accuracy. In the second category of attacks, the adversary may reveal sensitive information of individual(s) whose information was part of the training dataset of the model [81]. In particular case studies, having access to the trained model, attackers could learn about the genomic information of individuals [10], and in another adversarial access to a facial recognition system, they could reveal almost 80% of an individual's image.

3.2.5. Adversarial Inputs

This particular attack can highly corrupt the robustness of an AI system compared to the previous mentioned attacks. The adversarial inputs are malicious samples that are designed by adding a few bytes chosen carefully to the original sample [82] with the aim of fooling the system toward misclassifying outputs [83]. Such attacks are highly compromising in the computer vision and Natural Language Processing (NLP) fields [84]. In an experiment on autonomous vehicles [15], it is shown that a couple of minor changes on the stop sign caused the learning model to misclassify the sign with a speed limit 45 sign. Even though for a human eye the modified sign is still the stop sign. DeepFool [85] is one of the popular attack models [83] regarding the adversarial samples.

As mentioned above, the adversarial inputs are crafted from the original inputs by making small perturbations which lead to a large modification in the output. Hence, one potential solution to encounter this attack is to guarantee that the output does not change significantly by a small modification of the input. Computer vision that is largely based on neural networks, is one of the main targets of this type of attacks. Deepfool [85] propose an approach to quantify the robustness of deep neural network classifiers by calculating the perturbations that fool the classifier. Several techniques [86], [83], [87] are developed in the literature to defeat the adversarial sample attack, nevertheless, the problem has not been solved completely. In particular for neural networks, a team of Google, Stanford and MIT members has developed a community-run hub for learning about robust ML [88]. Their purpose is to keep updating a state-of-the-art robustness defense and evaluation techniques against adversarial examples. Furthermore, a different perspective is published in a most recent paper [89] which demonstrates that adversarial samples can be directly attributed to the presence of non-robust features that derived from patterns in the data distribution and are highly predictive, yet brittle and incomprehensible to humans.

3.2.6. Robustness for Security and Safety

Robustness in AI is the ability of the system to cope with and correctly function while facing the input which has not been defined during the training of the system. Considering the decision making power given by AI systems, it is significant that the system continues to operate upon unforeseen events to provide a vertical layer risk-reduction and additional security and safety of the system. In a standardized terminology from IEEE [90], robustness has been defined as "*The degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions*".

A dominant issue which targets the robustness of an AI system is the training stage of ML models. In the vast majority of the cases, the training samples are not perfect enough to cover all the aspects which may result in an insufficiently robust system. Thus, it may lead to a failure in providing a correct inference in the system such as car crashing in autonomous vehicles. To summarize, when the testing distribution differs from the training distribution, machine learning systems may not only exhibit poor performance but also wrongly assume that their performance is good [91]. Several AI models have failed when they have been tested against strong adversaries, even though they reacted as a thoroughly robust system against weaker adversaries [92].

In a research by an MIT team, a method is devised to evaluate the level of robustness in neural network models [93] that are designed for different tasks. The technique is based on detecting the misclassifications of a model. Moreover, a set of metrics is developed in the literature as well to identify and measure the robustness of an AI system including CLEVER, Empirical robustness, Loss sensitivity.

A variety of approaches are identified to build robustly performing ML system while encountering unseen dataset [91]. In an intuitive solution, one could try training on multiple scenarios which are significantly different from the training data. Nevertheless, one of the substantial features of AI systems is the ability of reasonable prediction of unforeseen inputs. Hence, tackling the robustness issue is not a trivial task.

3.3. Technical Standardization

Standardization plays an essential role in the adoption of AI within the industrial ecosystem. There are different organizations in the electro-technical, telecommunications or general-purpose domains that bring all the stakeholders such as entrepreneurs, governments, industries, and researchers together at various levels: national standardization organizations, European standardization organizations and international standardization organizations. Table 2 provides an example of the standards organizations per domain and per level. All the organizations are engaged on challenges from different aspects of AI, to define the life-cycle and use cases, and highlight the issues raised by the topic with respect to the data protection, privacy, and trustworthiness of AI.

	General Standardization	Electro-Technical Standardization	Telecommunications Standardization
International level	ISO	IEC	ITU-T
European level	CEN	CENELEC	ETSI
National level	ILNAS	ILNAS	ILNAS

Table 2: Examples of standards organizations

Joint Technical Committee (JTC) as ISO/IEC JTC 1 covers multiple Sub-Committees (SCs) with respect to the smart ICT and information technology. Among the several SCs that they have established under ISO/IEC JTC 1, are SC 27 – Information Security, Cybersecurity and Privacy Protection, which focuses on the development of standards considering privacy and security of ICT technologies, and SC 42 – Artificial Intelligence that is dedicated to AI. Particularly in SC 27, there is a Working Group (WG) 5, Identity Management and Privacy Technologies, dedicated to privacy protection. It is also interesting to mention a Technical Committee (TC) ISO/TC69 – Application of statistical methods, which is under direct responsibility of ISO and works, among other things, on the application of statistical methods to data analysis, which is very relevant to ML techniques. There are various projects and publications from these SCs and TC that can be found in [5]. In this study, we only highlight the recent publications and ongoing projects presented in Table 3.

On the other hand, IEEE as an important private association producing technical specifications, has mainly focused on developing deliverables to address the legal and ethical perspectives of AI rather than the technical aspects regarding privacy and data protection. The organization has recently approved [94] various projects to address ethical aspects of AI in various domains and applications ranging from data privacy and ethical design to threats posed by AI. In addition, ITU-T has directed AI activities to communication technologies. The list of activities and ongoing projects of these organizations are described in Table 4.

At European level, CEN and CENELEC have recently announced [95] the establishment of "Focus Group Artificial Intelligence" starting from 2019, to focus on developing standards in AI considering the European requirements. Besides, ETSI has also initiated projects that even though they may not directly discuss AI, they have focused on the use cases, applications and security challenges of AI. The list of projects is provided in Table 4.

ISO/IEC JTC 1/SC 42		
Published standards		
Identifier	**Title**	**Scope**
ISO/IEC 20546	Information technology – Big Data – Overview and vocabulary	Terminological foundation for Big Data
ISO/IEC TR 20547-2	Information technology – Big Data reference architecture – Part 2: Use cases and derived requirements	Examples of Big Data use cases
ISO/IEC TR 20547-5	Information technology – Big Data reference architecture – Part 5: Standards roadmap	Describes Big Data relevant standards
ISO/IEC JTC 1/SC 42		
Under-development standards		
Identifier	**Title**	**Scope**
ISO/IEC AWI TR 20547-1	Information technology – Big Data reference architecture – Part 1: Framework and application process	The framework of Big Data reference architecture
ISO/IEC DIS 20547-3	Information technology – Big Data reference architecture – Part 3: Reference architecture	Presents user view and functional view of Big Data Reference Architecture
ISO/IEC PDTR 24028	Information technology – Artificial intelligence (AI) – Overview of trustworthiness in artificial intelligence	Topics related to trustworthiness in AI systems
ISO/IEC AWI 23894	Information technology – Artificial intelligence – Risk management	Guidelines on managing risk in AI
ISO/IEC AWI TR 24368	Information technology — Artificial intelligence — Overview of ethical and societal concerns	High-level overview of societal concerns in AI
ISO/IEC WD 22989	Information Technology – Artificial Intelligence – Artificial Intelligence Concepts and Terminology	Basic concepts for AI
ISO/IEC NP TR 24029-1	Information technology – Artificial Intelligence (AI) – Assessment of the robustness of neural networks - Part 1: Overview	Existing methods to assess the robustness of neural networks
ISO/IEC NP TR 24027	Information technology – Artificial Intelligence (AI) – Bias in AI systems and AI aided decision making	Describes sources of bias in AI systems and possible mitigation measures
ISO/IEC AWI TR 24372	Information technology – Artificial intelligence (AI) – Overview of computational approaches for AI systems	Provides an overview of computational approaches and some specialised AI systems
ISO/IEC JTC 1/SC 27		
Published standards		
Identifier	**Title**	**Scope**
ISO/IEC TS 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	Developing privacy functional requirements
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	Terminology, and classification of de-identification techniques
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework	Defines a privacy architecture framework
ISO/IEC TR 27103	Information technology – Security techniques – Cybersecurity and ISO and IEC Standards	Provides guidance to leverage existing standards in a cybersecurity framework
ISO/IEC 18033-6	IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption	Specifies mechanisms for homomorphic encryption

ISO/IEC JTC 1/SC 27		
Under-development standards		
ISO/IEC WD 27045	Information technology – Big data security and privacy – Processes	
ISO/IEC CD 20547-4	Information technology – Big data reference architecture – Part 4: Security and Privacy	Secure implementation of Big Data architecture
ISO/IEC AWI 27556	Information technology – User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	

Table 3: ISO/IEC publications and under-development documents with respect to AI and data protection and privacy.

SDO	Identifier	Working Group / Project Title
IEEE	P7000	Model Process for Addressing Ethical Concerns During System Design
	P7001	Transparency of Autonomous Systems
	P7002	Data Privacy Process
	P7003	Algorithmic Bias Consideration
	P7004	Child and Student Data Governance
	P7005	Employer Data Governance
	P7006	Personal Data AI Agent Working Group
	P7007	Ontological Standard for Ethically driven Robotics and Automation Systems
	P7008	Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems
	P7009	Fail-Safe Design of Autonomous and Semi-Autonomous Systems
	P7010	Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems
	P7011	Process of Identifying & Rating the Trustworthiness of News Sources
	P7012	Machine Readable Personal Privacy Terms
	P7013	Inclusion and Application Standards for Automated Facial Analysis Technology
	P7014	Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems
ETSI	ENI ISG	Experiential Networked Intelligence Industry Specification Group
	SAI ISG	Securing AI Industry Specification Group
	ZSM ISG	Zero touch network and Service Management Industry Specification Group
ITU-T	AI4H	Artificial intelligence for health
	ML5G	Machine Learning for Future Networks including 5G

Table 4: Other SDOs activities with respect to data protection, privacy, and trustworthiness of AI.

3.3.1. Terminology, Computational Techniques, and Use cases

Terminology and vocabulary. The vocabulary and terminology of AI have been declared in different documents starting in 1995. The purpose is to address terminologies and concepts in AI and Big Data. ISO/IEC 2382-28 [96] is the first standard concepts corresponding to information technology and general aspects regarding AI and expert systems. The document was later updated to ISO/IEC 2382 [97].

In particular, ISO/IEC 20546 [98] published by SC 42, represents an overview and terminology for Big Data-related standards. Moreover, a new document, ISO/IEC WD 22989 [99] is under development which is addressing the concepts and terminology of AI. In addition, ISO/TC 69 on applications of statistical methods is currently working on ISO/NP 3534 which focuses on the terms used in Big Data applications. The framework and life-cycle of AI systems and Big Data analytics have also been discussed in SC 42. The framework of AI systems using machine learning algorithms is discussed in ISO/IEC WD 23053 [100] which is under development. ISO/IEC AWI TR 20547-1 [101] and ISO/IEC DIS 20547-3 [102] consider the framework and architecture of Big Data.

The former document suggests the process of applying the architecture in a particular domain, while the latter specifies Big Data reference architecture including the Big Data roles, activities, and functional components and their relationships.

Computational approaches. TC 69 and SC 42 are active regarding the techniques and models for Big Data analytics. Particularly the activities in TC 69 are focused on the validation of models and results of Big Data using the statistical techniques. ISO/NP TR 23348 [103] provides guidelines to validate the results of Big Data analytics by providing quality measures. ISO/NP TR 23347 [104] describes the data science life-cycle from the data preparation stage to analytics. Furthermore, ISO/IEC AWI TR 24372 [105] is a work in progress which presents an overview of computational approaches for AI systems.

Applications and use cases. In a recently established WG by SC 42, the different applications and use cases of AI in various domains have been taken into account. Some previously collected use cases of Big Data usage are described in ISO/IEC TR 20547-2 [106]. Recently, the use cases of AI in various domains have been collected. These are being reported in ISO/IEC NP TR 24030 [107] and are expected to be published in 2020.

3.3.2. Data Protection, Privacy, and Trustworthiness

Data privacy. SC 27 is addressing various aspects of information security. Among different WGs of this committee, data protection and privacy projects are either part of WG 5, Identity management and privacy technologies or WG 2, Cryptography and security mechanisms. In an ongoing project of ISO/IEC CD 20547-4 [108], the privacy and security of Big Data is addressed to propose a guideline for secure implementation of Big Data. More specifically, ISO/IEC TR 27103 [109] has focused on de-identification (e.g., k-anonymity), ISO/IEC 20889 [110] introduces various privacy-enhanced techniques (PET), including anonymization, and ISO/IEC 18033-6 [111] discusses homomorphic encryption.

SC 42 has established a working group (i.e., WG 3 Trustworthiness) to address the challenges of trustworthiness and safety for AI systems. The Technical Report (TR) of ISO/IEC PDTR 24028 [112] is an ongoing work from WG 3 which identifies the challenges and threats to the trustworthiness of AI systems. The report is also providing general solutions and mitigation strategies to address challenges.

Biased data. ISO/IEC NP TR 24027 [113] introduces bias concerning AI systems by describing the different types of bias and measurement methods to mitigate bias in AI systems.

Data poisoning. Data poisoning attack is introduced in privacy threats of the trustworthiness report ISO/IEC PDTR 24028 [112] while the detailed information of the mitigation and possible defense methods is still missing from the standardization documents.

Model extraction. This attack is also introduced under the mentioned technical report (ISO/IEC PDTR 24028 [112]) as a threat to an AI system, however, no particular document is dedicated to this topic.

Adversarial inputs. Likewise, adversarial inputs are also only introduced in the TR of WG 3, ISO/IEC PDTR 24028 [112].

Robustness. In an ongoing item ISO/IEC NP TR 24029-1 [114], threats and challenges regarding the robustness of neural networks-based AI systems are introduced. Moreover, the scope of the document covers the metrics to verify the robustness of an AI system.

3.4. Gap Analysis

As a primary concern to integrate AI systems in society, there is a great need for auditing and regulations to hold these systems accountable. The main purpose of this section is to analyze the gaps between the research development and activities of SDOs towards providing guidelines for companies to ensure adopting safe AI. A standard definition and guideline would benefit and could enhance the collaboration between researches and business sectors by providing a standard language to communicate.

The purpose of the gap analysis, therefore, is threefold: 1) **Identification**, introducing the privacy and security threats and challenges, 2) **Metrics and Mitigation Strategies**, quantifying the degree of the vulnerability of the system and removing the threat, 3) **Secure Implementation**, developing a system with the constraints to avoid the threat and test it against attacks. The result of the gap analysis considering the research survey provided in this study and standardization is described in Table 5. Next, each phase is explained in more details.

Phase		Existing/ Under development Standards	Gaps

Identification	AI and ML systems (terminology and computational approaches)	ISO/IEC 2382
		ISO/IEC WD 22989
		ISO/NP TR 23347
		ISO/IEC AWI 24372
		ISO/NP 3534-5
		ISO/IEC WD 23053
			• Techniques:
			  ○ Deep learning
			  ○ Clustering
			  ○ Reinforcement learning
			  ○ Transfer learning

	Applications and use cases	ISO/IEC NP TR 24030
		ISO/IEC TR 20547-2
			• Use cases:
			  ○ AI-enabled chips
			  ○ Recommender systems

	Privacy and security threats	ISO/IEC PDTR 24028	• A general picture of the threats considering the AI assets
			• Missing threats/challenges:
			  ○ Evasion attacks
			  ○ Data breaches
			  ○ Inferential attack

Metrics and Mitigation Strategies	Quantifying risks	ISO/IEC PDTR 24028	• Considering data sensitivity Risks of different phase of AI life-cycle

	Measurements	ISO/IEC PDTR 24028
		ISO/IEC NP TR 24027
		ISO/IEC NP TR 24029-1
			• Data quality:
			  ○ Robustness
			  ○ Bias

	Defense strategies	ISO/IEC 20889
		ISO/IEC TR 27103
		ISO/IEC 18033-6
			• Attack models
			• Techniques:
			  ○ Differential privacy
			  ○ Federated learning

Secure Implementation	Test and evaluation	ISO/IEC CD 20547-4 ISO/IEC NP TR 24027 ISO/IEC NP TR 24029-1	• AI life-cycle ○ Risk and threats evaluation (e.g., bias, robustness, security)
	Implementation	ISO/IEC CD 20547-4	• Secure implementation of AI systems: ○ Constraints and restriction • Adversarial machine learning

Table 5: A general overview of the gap analysis as the outcome of the research and standardization survey.

3.4.1.Identification

As a preliminary step towards protecting a technology from any adversarial attack is the identification and recognition of the system itself, the assets and the vulnerabilities and threats. Even though AI systems may differ from one use case to another, the general procedure and specifications of most systems are similar. Standard terminology and framework, therefore, are the backbones to identify AI systems and therefore to develop security mechanisms. Nevertheless, there is not yet a publication from SDOs which specifically focuses on building the common language to comprise all aspects of AI systems including the basic vocabulary, computational approaches, applications and use cases, data privacy and security threats and vulnerabilities, and the defense mechanisms.

Data protection, privacy, and security of AI systems have been taken into account by ISO/IEC SC 42/WG 3 as described in Section 3.3.2. The challenges and threats (e.g., data poisoning, model extraction) of AI systems have been introduced in this study. In addition, data privacy and security techniques are mostly the targets of ISO/IEC SC 27 as described in Section 3.3.2. However, popular security methods (e.g., differential privacy, federated learning) which are engaged in many privacy-preserving ML algorithms have not been considered by SDOs yet. Therefore, one gap here is the identification of possible threats and security challenges in the life-cycle of the AI system and the pipeline of ML algorithms as described in Section 3.2 in Figure 3. The omnipresence of AI in many specific use cases (e.g., face recognition) requires bringing in the knowledge from that particular field into AI to develop a specific guideline on computational approaches and privacy threats since system's vulnerabilities are highly correlated with the application of that system. One of the most dominant use cases of AI and ML techniques is on bio-metric data. Face recognition, fingerprint and retina scanning, genomics are areas where AI helped to improve the computations. ISO SC 37 is the specific technical committee regarding bio-metric, even though the committee has not yet provided any documents regarding the data protection and AI based use cases of the domain. Likewise, for other domains such as transportation, finance, etc.

3.4.2.Metrics and Mitigation Strategies

As described in Figure 3, there are various risks which can threaten the system in each phase. Therefore, the metrics and mitigation strategies should be adapted based on the target phase. As explained in Section 3.3.2, some of security and data privacy techniques have been taken into account, however, considering the new assets of AI systems, data protection and privacy techniques in standards should be upgraded to address these concerns. Besides, the attack models corresponding to each threat (e.g., data poisoning) also is necessary to be specified and discussed in standardization documents.

Furthermore, the measurements and quality metrics are important elements to describe the level of privacy, data protection and trustworthiness of a system. Lack of robustness of an AI system could cause many privacy and security violations. As mentioned in Section 3.2, there exist several metrics to consider for this evaluation. While some of the metrics are general and suitable for most of the AI systems, others are designed to evaluate a specific factor. Even though there is a variety of domains and use cases where AI-based decision making systems are performing, a general regulation is missing when industries need to adopt such systems. Moreover, assuming different applications and use cases of AI, it is important to define specific metrics since some features such as individuals' data sensitivity may change from one use case to another. The risks and challenges, therefore, needs to be considered for each use case.

Regarding security techniques and privacy preserving methods, PETs are not fully addressed in SC 27. Particularly, techniques such as federated learning [52] which has been recently developed. Differential privacy is described in some documents, however, its application in deep learning and AI systems is not yet defined.

3.4.3. Implementation and Test

The implementation of AI systems should be completed by a standard set of tests and evaluations to ensure the privacy, security, and trustworthiness of a system. An important element in developing AI systems is the input data which is highly vulnerable and may strongly affect the result and even the purpose of the machine. As described in Figure 3, input data (training and new data) can be the target of several attacks and data protection violations. Preparing the input data, hence, is an essential stage which requires constraints and restriction to develop a sufficient quality and quantity of data and to achieve fair results. Moreover, with respect to the learning model used in the systems (Section 3.1), the size of the dataset can also affect the robustness and fairness of the model. Likewise, specifications and metrics to protect the training model are necessary as well to reduce the chance of possible risks.

To develop and employ a safe and secure AI system, the accumulation of all above-mentioned mechanisms and metrics are required which is a major gap in the standard documents and regulations. However, it could be addressed considering the outcomes of various research and case studies in the literature (Section 3.2). Furthermore, existing standards for the domains which are now benefiting from AI systems are not up-to-date with respect to AI concerns, risks and threats. For instance, ISO/IEC TR 24714-1 [115] describes the life-cycle of a bio-metric system, and ISO/IEC 24745 [116] discuss bio-metric information protection, however, the evaluations and metrics regarding potential hazards toward AI-based bio-metric systems have not been mentioned.

3.5. Discussion and Insights

In this section, some solutions with respect to the gaps mentioned in the previous section are discussed in order to benefit from the research outcomes and address the gaps in standardization. The multi-domain nature of AI has attracted the attention of both academia to develop and extend the technology and companies to investigate on them [117], [118], [119]. Nevertheless, SDOs have not yet fully addressed the topics in their standardization guidance.

Considering the TCs of ISO, one possibility is the adoption of AI into relevant TCs and SCs. The step towards filling this gap has been taken by the Liaisons. Several SCs established Liaisons with SC 42 such as ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection, ISO/IEC JTC 1/SC 37 - Biometrics, ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms, ISO/IEC JTC 1/SC 41 - Internet of Things and related technologies, ISO/TC 69 - Application of statistical methods, ISO/TC 37 - Language and terminology, ISO/TC 204 - Intelligent transport systems, etc. Besides, other SDOs such as IEEE and ITU are the organizations in liaison with SC 42. The collaboration can initiate the innovation for stakeholders such as researchers, government, businesses/companies to accelerate the adoption of AI into different business sectors. Some identified domains for future collaborations between SC 42 and its existing (ISO/TC 69, ISO/TC 204, ISO/TC 37) and potential (ISO/TC 22, ISO/TC 68, ISO/ TC 20/SC 16) Liaisons is shown in Figure 5.

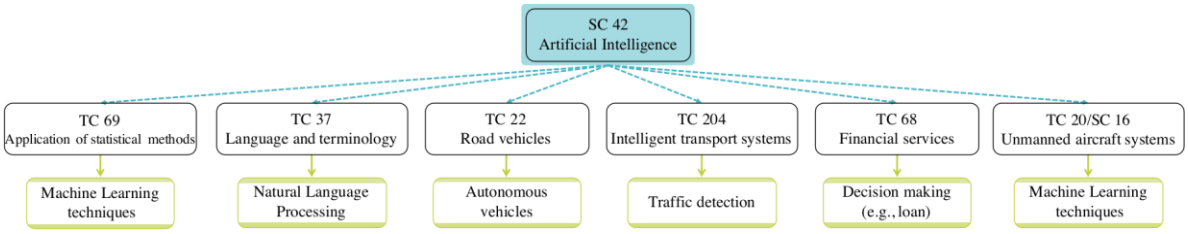

Fig. 5: Collaborations within different technical committees in ISO towards integrating AI for developing new standards.

Furthermore, one of the critical aspects of standards is updating the existing documents due to the fast changes in the smart ICT related technologies. In particular, some of the existing documents such as ISO/IEC 24745 [116] regarding biometric information protection, and ISO/TS 12812-2 [120] about data protection for mobile financial services, represent domains which mostly integrated AI in their systems. Hence, such documents required to be updated so that they address the challenges with respect to the AI data protection and privacy as well. Besides, a general qualification of AI systems is required to be developed to ensure the quality and security of an AI system. It benefits stakeholders in different domains such that one could implement a verified AI and employ it. Likewise, ISO 9001 and ISO 27001, a guideline with a set of evaluation methods, metrics and benchmarks are required to be defined towards a certified AI system.

3.6. The National Example for linking AI Communities of Research and Standardization

In Luxembourg, ILNAS, the Luxembourg Institute of standardization, Accreditation, Safety and Quality of Products and Services – *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* - is the National Standards Body, which allows and encourages the participation of the national market in the standardization process. Initiatives are in place to foster collaborations with different stakeholders such as researchers, entrepreneurs, companies and individual experts. A specific national policy for ICT technical standardization [121] aims at developing market interest and involvement which started by publishing a white paper for Big Data [122] and currently is working on another white paper for AI.

The aim is promoting and reinforcing market participation, as well as supporting and strengthening the education about standardization and related research activities. In line with the first objective - to develop market interest and involvement ILNAS has developed a Standards Analysis [123], which allows identifying easily standardization activities of different SDOs in the Smart Secure ICT area, including Big Data and AI. This document is a practical tool helping ILNAS to promote technical standardization in Big Data and AI area and to raise awareness among national stakeholders.

Similarly, conforming to the second project - promoting and reinforcing market participation- ILNAS is actively involved in the development of standards as a P-member (participating member) of ISO/IEC JTC 1/SC 42 and it follows closely the developments of standards of different technical committees. This participation in ISO/IEC JTC 1/SC 42 and monitoring of the standards developed by other SDOs, such as ETSI, allows ILNAS to actively transfer relevant information to the market and encourage its involvement in the standards development process.

Finally, to meet the third project of the policy - supporting and strengthening the education about standardization and related research activities - ILNAS has undertaken different initiatives, including the development of White Papers on Big Data and AI, in collaboration with the Ministry of the Economy, with the goal of providing a comprehensive analysis of technological, economic, as well as technical standardization perspectives. Moreover, ILNAS works in collaboration with the University of Luxembourg (UL) and the Interdisciplinary centre of Security Reliability and Trust (SnT) on three ICT tracks to link research and standardization funding a unique doctorate program on linking research and standardization in Internet of Things, Artificial Intelligence (AI) and Cloud Computing. One first result of this research program was the publication in October 2018 of a White Paper Data Protection and Privacy in Smart ICT [5], which is extended with this technical report for the AI domain. In parallel, in 2016, the UL/SnT-ILNAS collaboration launched the professional degree program Smart ICT for business innovation [124], to be extended to a complete professional Master program by 2020.

3.7. Summary

This study is focused on challenges and threats with respect to data protection, privacy, and trustworthiness of AI systems. As threats and social contexts evolve, so too will the technology need to adapt - as well as the rules and regulations that govern the use of such technologies. The two perspectives of the research outcomes and standardization activities have been considered in this study. An AI life-cycle was defined in the paper to address the challenges and threats on the defined scheme. First, a survey on research results in the area has been described and next, another survey of standardization activities and publications has been presented through this study. As a result of the two surveys, a gap analysis is provided to address the gaps with respect to the high demands from industries regarding the safe and secure AI systems.

List of Acronyms and abbreviations

WG	Working Group
AI	Artificial Intelligence
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
ETSI	European Telecommunication Standards Institute
IEC	International Electrotechnical Commission
ILNAS	Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union (ITU) on Telecommunication Standardization Sector
JTC	Joint Technical Committee
ML	Machine Learning
NLP	Natural Language Processing
PET	Privacy-Enhancing Techniques
SC	Sub-committee
SDO	Standards Developing Organization
TC	Technical Committee
TR	Technical Report
WG	Working Group

References

[1] D. Laney, "3d data management: Controlling data volume, velocity and variety," *META group research note*, vol. 6, no. 70, p. 1, 2001.

[2] S. Feldman. (2019) Who Is investing in AI? [Online]. Available: https://www.statista.com/chart/17910/artificial-intelligence-investment-worldwide/

[3] K. Aditya and C. Wheelock, "Artificial intelligence market forecasts," Tractia, Tech. Rep., 2016. [Online]. Available: https://www.tractica.com/wp- content/uploads/2016/08/MD-AIMF-3Q16-Executive-Summary.pdf/

[4] A. K. Keith Kirkpatrick, "Artificial intelligence use cases," Tractica, Tech. Rep., 2018.

[5] ILNAS, White Paper: Data Protection and Privacy in Smart ICT - Scientific Research and Technical standardization, ILNAS, ANEC G.I.E, University of Luxembourg, Tech. Rep., 2018.

[6] S. G. Finlayson, H. W. Chung, I. S. Kohane, and A. L. Beam, "Adversarial attacks against medical deep learning systems," *arXiv preprint arXiv:1804.05296*, 2018.

[7] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," *Machine Learning*, vol. 81, no. 2, pp. 121–148, 2010.

[8] B. Biggio, G. Fumera, and F. Roli, "Security evaluation of pattern classifiers under attack," *IEEE transactions on knowledge and data engineering*, vol. 26, no. 4, pp. 984–996, 2013.

[9] ——, "Pattern recognition systems under attack: Design issues and research challenges," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 28, no. 07, p. 1460002, 2014.

[10] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart, "Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing," in 23rd USENIX *Security Symposium* (USENIX *Security* 14), 2014, pp. 17–32.

[11] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1322–1333.

[12] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition," *in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1528–1540.

[13] N. Carlini and D. Wagner, "Audio adversarial examples: Targeted attacks on speech-to-text," in 2018 *IEEE Security and Privacy Workshops* (SPW). IEEE, 2018, pp. 1–7.

[14] M. Alzantot, Y. Sharma, A. Elgohary, B.-J. Ho, M. B. Srivastava, and K.-W. Chang, "Generating natural language adversarial examples," in EMNLP, 2018.

[15] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 1625–1634.

[16] N. Carlini, C. Liu, J. Kos, U´. Erlingsson, and D. Song, "The secret sharer: Evaluating and testing unintended memorization in neural networks," 2019.

[17] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," Science, vol. 363, no. 6433, pp. 1287–1289, 2019.

[18] S. A. Seshia, D. Sadigh, and S. S. Sastry, "Towards verified artificial intelligence," *arXiv preprint arXiv:1606.08514*, 2016.

[19] D. L. Poole, A. K. Mackworth, and R. Goebel, *Computational intelligence: a logical approach*. Oxford University Press New York, 1998, vol. 1.

[20] S. J. Russell and P. Norvig, *Artificial intelligence: a modern approach*. Malaysia; Pearson Education Limited,, 2016.

[21] D. Pyle and C. San Jose, "An executives guide to machine learning," *McKinsey Quarterly*, vol. 3, pp. 44–53, 2015.

[22] J. G. Carbonell, R. S. Michalski, and T. M. Mitchell, "An overview of machine learning," in *Machine learning*. Elsevier, 1983, pp. 3–23.

[23] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[24] O. AI. Watch our AI system play against five of the worlds top Dota 2 Professionals. [Online]. Available: https://openai.com/five/

[25] D. Silver and D. Hassabis, "Alphago: Mastering the ancient game of go with machine learning," *Research Blog*, vol. 9, 2016.

[26] Argility. Some low level application of AI and machine learning. [Online]. Available: https://www.argility.com/argility-ecosystem-solutions/iot/machine- learning-deep-learning/

[27] H. Bae, J. Jang, D. Jung, H. Jang, H. Ha, and S. Yoon, "Security and privacy issues in deep learning," *arXiv preprint arXiv:1807.11655*, 2018.

[28] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," IEEE access, vol. 6, pp. 12 103–12 117, 2018.

[29] OPAL. (2017) Open Algorithms. [Online]. Available: http://www.opalproject.org/

[30] K. El Emam, L. Arbuckle, G. Koru, B. Eze, L. Gaudette, E. Neri, S. Rose, J. Howard, and J. Gluck, "De-identification methods for open health data: the case of the heritage health prize claims dataset," *Journal of medical Internet research*, vol. 14, no. 1, p. e33, 2012.

[31] K. El Emam, "Methods for the de-identification of electronic health records for genomic research," *Genome medicine*, vol. 3, no. 4, p. 25, 2011.

[32] K. Ito, J. Kogure, T. Shimoyama, and H. Tsuda, "De-identification and encryption technologies to protect personal information," *Fujitsu Scientific & Technical Journal*, vol. 52, no. 3, 2016.

[33] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," technical report, SRI International, Tech. Rep., 1998.

[34] G. Van Blarkom, J. J. Borking, and J. E. Olk, "Handbook of privacy and privacy-enhancing technologies," *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, vol. 154, pp. 24–43, 2003.

[35] L. Sweeney, "Simple demographics often identify people uniquely," *Health (San Francisco)*, vol. 671, pp. 1–34, 2000.

[36] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, p. 1376, 2013.

[37] Y.-A. de Montjoye et al., "Response to comment on unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 351, no. 6279, pp. 1274–1274, 2016.

[38] Z. Huang, E. Ayday, J. Fellay, J.-P. Hubaux, and A. Juels, "Genoguard: Protecting genomic data against brute-force attacks," in *2015 IEEE Symposium on Security and Privacy. IEEE*, 2015, pp. 447–462.

[39] F. Liu, K. A. Hua, and Y. Cai, "Query l-diversity in location-based services," in *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*. IEEE, 2009, pp. 436–442.

[40] F.-J. Wu, M. R. Brust, Y.-A. Chen, and T. Luo, "The privacy exposure problem in mobile location-based services," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–7.

[41] T. S. Gal, Z. Chen, and A. Gangopadhyay, "A privacy protection model for patient data with multiple sensitive attributes," *International Journal of Information Security and Privacy (IJISP)*, vol. 2, no. 3, pp. 28–44, 2008.

[42] M. M. Groat, W. Hey, and S. Forrest, "Kipda: k-indistinguishable privacy-preserving data aggregation in wireless sensor networks," in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 2024–2032.

[43] M. Arrington, "Aol proudly releases massive amounts of user search data," *TechCrunch News*, August, 2006.

[44] A. Narayanan and V. Shmatikov, "How to break anonymity of the netflix prize dataset," *arXiv preprint cs/0610105*, 2006.

[45] B. Felbo, P. Sundsøy, S. Lehmann, Y.-A. de Montjoye et al., "Using deep learning to predict demographics from mobile phone metadata," 2016.

[46] E. Jahani, P. Sundsøy, J. Bjelland, L. Bengtsson, Y.-A. de Montjoye et al., "Improving official statistics in emerging markets using machine learning and mobile phone data," *EPJ Data Science*, vol. 6, no. 1, p. 3, 2017.

[47] Argility. (2011) Homomorphic encryption and Bitcoin. [Online]. Available: https://www.lesswrong.com/posts/XCuwfWFuiGxCWXFtW/homomorphic- encryption-and-bitcoin

[48] E. Ayday, J. L. Raisaro, P. J. McLaren, J. Fellay, and J.-P. Hubaux, "Privacy-preserving computation of disease risk by using genomic, clinical, and environmental data," in *Presented as part of the 2013 USENIX Workshop on Health Information Technologies*, 2013.

[49] S. E. Dilmaghani, "A privacy-preserving solution for storage and processing of personal health records against brute-force attacks," Ph.D. dissertation, Bilkent University, 2017.

[50] F. McSherry and I. Mironov, "Differentially private recommender systems: Building privacy into the netflix prize contenders," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2009, pp. 627–636.

[51] Y. Hu and F. Wang, "An attack on a fully homomorphic encryption scheme." *IACR Cryptology ePrint Archive*, vol. 2012, p. 561, 2012.

[52] H. B. McMahan, E. Moore, D. Ramage, S. Hampson et al., "Communication-efficient learning of deep networks from decentralized data," arXiv preprint *arXiv:1602.05629*, 2016.

[53] L.-B. Suleyman, M., "Trust, confidence and verifiable data audit, deepmind," 2017.

[54] M. Wall. (2019) Biased and wrong? Facial recognition tech in the dock. [Online]. Available: https://www.bbc.com/news/business-48842750

[55] K. Hao. (2019) AI is sending people to jailand getting it wrong. [Online]. Available: https://www.technologyreview.com/s/612775/algorithms-criminal- justice-ai/

[56] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Conference on fairness, accountability and transparency*, 2018, pp. 77–91.

[57] I. D. Raji and J. Buolamwini, "Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial ai products," in *AAAI/ACM Conf. on AI Ethics and Society*, vol. 1, 2019.

[58] A. Amini, A. Soleimany, W. Schwarting, S. Bhatia, and D. Rus, "Uncovering and mitigating algorithmic bias through learned latent structure," 2019.

[59] J. H. Hinnefeld, P. Cooman, N. Mammo, and R. Deese, "Evaluating fairness metrics in the presence of dataset bias," *arXiv preprint arXiv:1809.09245*, 2018.

[60] T. Speicher, H. Heidari, N. Grgic-Hlaca, K. P. Gummadi, A. Singla, A. Weller, and M. B. Zafar, "A unified approach to quantifying algorithmic unfairness: Measuring individual &group unfairness via inequality indices," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, ser. KDD '18. New York, NY, USA: ACM, 2018, pp. 2239–2248. [Online]. Available: http://doi.acm.org/10.1145/3219819.3220046

[61] F. Calmon, D. Wei, B. Vinzamuri, K. N. Ramamurthy, and K. R. Varshney, "Optimized pre-processing for discrimination prevention," in *Advances in Neural Information Processing Systems*, 2017, pp. 3992–4001.

[62] F. Kamiran, A. Karim, and X. Zhang, "Decision theory for discrimination-aware classification," in *2012 IEEE 12th International Conference on Data Mining*. IEEE, 2012, pp. 924–929.

[63] R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork, "Learning fair representations," in *Proceedings of the 30th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, S. Dasgupta and D. McAllester, Eds., vol. 28, no. 3. Atlanta, Georgia, USA: PMLR, 17–19 Jun 2013, pp. 325–333.

[64] B. H. Zhang, B. Lemoine, and M. Mitchell, "Mitigating unwanted biases with adversarial learning," in Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. ACM, 2018, pp. 335–340.

[65] M. T. Ribeiro, S. Singh, and C. Guestrin, ""why should I trust you?": Explaining the predictions of any classifier," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, CA, USA, August 13-17, 2016*, 2016, pp. 1135–1144.

[66] J. A. Adebayo et al., "Fairml: Toolbox for diagnosing bias in predictive modeling," Ph.D. dissertation, Massachusetts Institute of Technology, 2016.

[67] R. K. Bellamy, K. Dey, M. Hind, S. C. Hoffman, S. Houde, K. Kannan, P. Lohia, J. Martino, S. Mehta, A. Mojsilovic et al., "Ai fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias," *arXiv preprint arXiv:1810.01943*, 2018.

[68] J. Steinhardt, P. W. W. Koh, and P. S. Liang, "Certified defenses for data poisoning attacks," in *Advances in neural information processing systems*, 2017, pp. 3517–3529.

[69] X. Chen, C. Liu, B. Li, K. Lu, and D. Song, "Targeted backdoor attacks on deep learning systems using data poisoning," *arXiv preprint arXiv:1712.05526*, 2017.

[70] J. Newsome, B. Karp, and D. Song, "Paragraph: Thwarting signature learning by training maliciously," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2006, pp. 81–105.

[71] B. Biggio, I. Corona, B. Nelson, B. I. Rubinstein, D. Maiorca, G. Fumera, G. Giacinto, and F. Roli, "Security evaluation of support vector machines in adversarial environments," in *Support Vector Machines Applications*. Springer, 2014, pp. 105–153.

[72] B. Biggio, B. Nelson, and P. Laskov, "Support vector machines under adversarial label noise," in *Asian Conference on Machine Learning*, 2011, pp. 97–112.

[73] M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru, and B. Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," *in 2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 19–35.

[74] Y. Wang and K. Chaudhuri, "Data poisoning attacks against online learning," *arXiv preprint arXiv:1808.08994*, 2018.

[75] X. Zhang and X. Zhu, "Online data poisoning attack," CoRR, vol. abs/1903.01666, 2019. [Online]. Available: http://arxiv.org/abs/1903.01666

[76] O. Suciu, R. Marginean, Y. Kaya, H. Daume III, and T. Dumitras, "When does machine learning FAIL ? generalized transferability for evasion and poisoning attacks," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1299–1316.

[77] F. Trame`r, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 601–618.

[78] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 36–52.

[79] D. Lowd and C. Meek, "Adversarial learning," *in Proceedings of the Eleventh ACM SIGKDD International Conference on Knowledge Discovery in Data Mining*, ser. KDD '05. New York, NY, USA: ACM, 2005, pp. 641–647. [Online]. Available: http://doi.acm.org/10.1145/1081870.1081950

[80] S. J. Oh, M. Augustin, B. Schiele, and M. Fritz, "Towards reverse-engineering black-box neural networks," *arXiv preprint arXiv:1711.01768*, 2017.

[81] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 3–18.

[82] B. Kolosnjaji, A. Demontis, B. Biggio, D. Maiorca, G. Giacinto, C. Eckert, and F. Roli, "Adversarial malware binaries: Evading deep learning for malware detection in executables," in *2018 26th European Signal Processing Conference (EUSIPCO)*. IEEE, 2018, pp. 533–537.

[83] J. Zhang and X. Jiang, "Adversarial examples: Opportunities and challenges," *arXiv preprint arXiv:1809.04790*, 2018.

[84] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, 2013.

[85] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: a simple and accurate method to fool deep neural networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2574–2582.

[86] M. Cisse, P. Bojanowski, E. Grave, Y. Dauphin, and N. Usunier, "Parseval networks: Improving robustness to adversarial examples," in *Proceedings of the 34th International Conference on Machine Learning-Volume 70*. JMLR. org, 2017, pp. 854–863.

[87] F. Croce, M. Andriushchenko, and M. Hein, "Provable robustness of relu networks via maximization of linear regions," *arXiv preprint arXiv:1810.07481*, 2018.

[88] RobustML. List of Published White-box Defenses to Adversarial Examples. [Online]. Available: https://https://www.robust-ml.org/defenses//

[89] A. Ilyas, S. Santurkar, D. Tsipras, L. Engstrom, B. Tran, and A. Madry, "Adversarial examples are not bugs, they are features," *arXiv preprint arXiv:1905.02175*, 2019.

[90] I. S. C. Committee et al., "Ieee standard glossary of software engineering terminology (ieee std 610.12-1990). los alamitos," CA: *IEEE Computer Society*, vol. 169, 1990.

[91] D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, and D. Mane´, "Concrete problems in ai safety," *arXiv preprint arXiv:1606.06565*, 2016.

[92] A. Athalye, N. Carlini, and D. Wagner, "Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples," *arXiv preprint arXiv:1802.00420*, 2018.

[93] V. Tjeng, K. Xiao, and R. Tedrake, "Evaluating robustness of neural networks with mixed integer programming," *arXiv preprint arXiv:1711.07356*, 2017.

[94] P. Cihon, "Standards for ai governance: International standards to enable global coordination in ai research & development," 2019.

[95] CEN-CENELEC.(2019) Artificial Intelligence, Blockchain and Distributed Ledger Technologies. [Online].Available: https://www.cencenelec.eu/standards/Topics/ArtificialIntelligence/Pages/default.aspx

[96] "ISO/IEC 2382-28: Information technology – Vocabulary – Part 28: Artificial intelligence – Basic concepts and expert systems," International Organization for Standardization, Geneva, CH, Standard, 1995.

[97] "ISO/IEC 2382: Information technology – Vocabulary," International Organization for Standardization, Geneva, CH, Standard, 2015.

[98] "ISO/IEC 20546: Information technology – Big data – Overview and vocabulary," International Organization for Standardization, Geneva, CH, Standard, 2019.

[99] "ISO/IEC WD 22989: Artificial intelligence – Concepts and terminology," International Organization for Standardization, Geneva, CH, Standard.

[100] "ISO/IEC WD 23053: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)," International Organization for Standardization, Geneva, CH, Standard.

[101] "ISO/IEC AWI TR 20547-1: Information technology – Big data reference architecture – Part 1: Framework and application process," International Organization for Standardization, Geneva, CH, Standard.

[102] "ISO/IEC DIS 20547-3: Information technology – Big data reference architecture – Part 3: Reference architecture," International Organization for Standardization, Geneva, CH, Standard.

[103] "ISO/NP TR 23348: Statistics – Big Data Analytics – Model Validation," International Organization for Standardization, Geneva, CH, Standard.

[104] "ISO/NP TR 23347: Statistics – Big Data Analytics – Data Science Life Cycle," International Organization for Standardization, Geneva, CH, Standard.

[105] "ISO/IEC AWI TR 24372: Information technology – Artificial intelligence (AI) – Overview of computational approaches for AI systems," International Organization for Standardization, Geneva, CH, Standard, 2018.

[106] "ISO/IEC TR 20547-2: Information technology – Big data reference architecture – Part 2: Use cases and derived requirements," International Organization for Standardization, Geneva, CH, Standard, 2018.
[107] "ISO/IEC NP TR 24030: Information technology – Artificial Intelligence (AI) – Use cases," International Organization for Standardization, Geneva, CH, Standard.
[108] "ISO/IEC CD 20547-4: Information technology – Big data reference architecture – Part 4: Security and Privacy," International Organization for Standardization, Geneva, CH, Standard.
[109] "Information technology – Security techniques – Cybersecurity and ISO and IEC Standards," International Organization for Standardization, Geneva, CH, Standard, 2018.
[110] "ISO/IEC 20889: Privacy enhancing data de-identification terminology and classification of techniques," International Organization for Standardization, Geneva, CH, Standard, 2018.
[111] "IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption," International Organization for Standardization, Geneva, CH, Standard, 2019.
[112] "ISO/IEC PDTR 24028: Information technology – Artificial Intelligence (AI) – Overview of trustworthiness in Artificial Intelligence," International Organization for Standardization, Geneva, CH, Standard.
[113] "ISO/IEC NP TR 24027: Information technology – Artificial Intelligence (AI) – Bias in AI systems and AI aided decision making," International Organization for Standardization, Geneva, CH, Standard.
[114] "ISO/IEC NP TR 24029-1: Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview," International Organization for Standardization, Geneva, CH, Standard.
[115] "ISO/IEC TR 24714-1: Information technology Biometrics Jurisdictional and societal considerations for commercial applications Part 1: General guidance," International Organization for Standardization, Geneva, CH, Standard, 2008.
[116] "ISO/IEC 24745: Information technology Security techniques Biometric information protection," International Organization for Standardization, Geneva, CH, Standard, 2011.
[117] P. Stone, R. Brooks, E. Brynjolfsson, R. Calo, O. Etzioni, G. Hager, J. Hirschberg, S. Kalyanakrishnan, E. Kamar, S. Kraus et al., "Artificial intelligence and life in 2030," *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, p. 52, 2016.
[118] A. Parbhakar. (2018) Hot topics in AI research. [Online]. Available: https://towardsdatascience.com/hot-topics-in-ai-research-4367bdd93564
[119] T. K. Dang. (2019) 5 Top AI Trends. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/04/25/5-top-ai-trends/17ccbc16aa02
[120] "ISO/TS 12812-2: Core banking Mobile financial services Part 2: Security and data protection for mobile financial services," International Organization for Standardization, Geneva, CH, Standard, 2017.
[121] ILNAS, Policy on ICT technical standardization (2015-2020), https://portail-qualite.public.lu/dam-assets/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf, accessed: 2019-09-17.
[122] "White Paper: Big Data," ILNAS ANEC G.I.E, Technical Report, 2018.
[123] "Standards Analysis: Smart Secure ICT," ILNAS ANEC G.I.E, Technical Report, 2018.
[124] (2018) Smart ICT Certificate for Business Innovation. [Online]. Available: https://wwwen.uni.lu/studies/fstc/certificate

October 2019 · SMART ICT: Gap analysis between scientific research and technical standardization · V1.0 · © ILNAS/UNI.LU/ANEC/SnT

ILNAS
Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

uni.lu
UNIVERSITÉ DU
LUXEMBOURG

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : info@ilnas.etat.lu

www.portail-qualite.lu