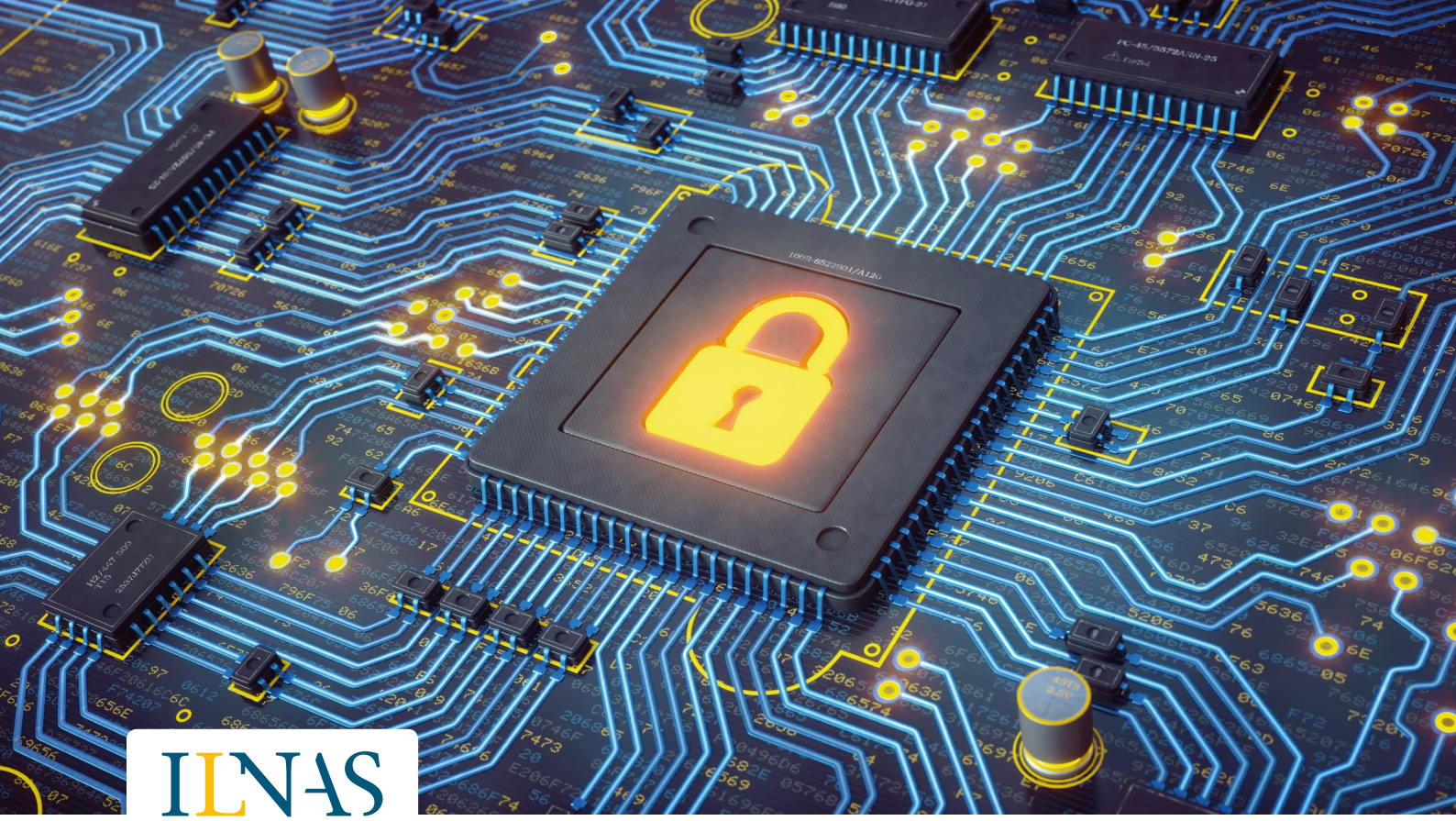


ILNAS

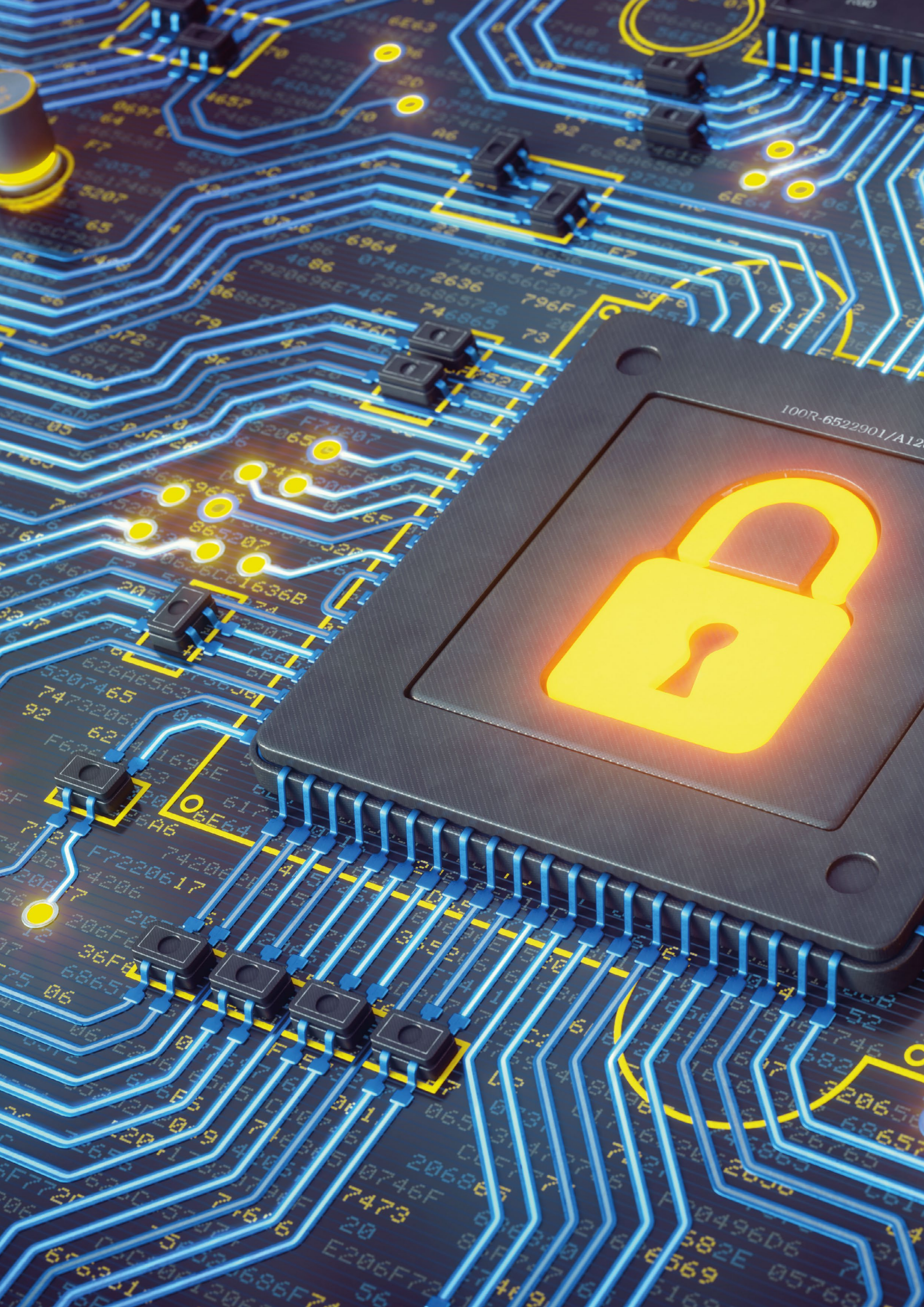
White Paper

DIGITAL TRUST FOR SMART ICT

Version 3.0 · October 2016

Avec le support de :

LE GOUVERNEMENT
DU GRAND DUCHE DE LUXEMBOURG
Ministère de l'Économie


100R-6522901/A12

White Paper

DIGITAL TRUST FOR SMART ICT

Version 3.0 · October 2016

ILNAS
Institut luxembourgeois de la normalisation,
de l'accréditation, de la sécurité et qualité
des produits et services

Avec le support de :

LE GOUVERNEMENT
DU GRAND DUCHE DE LUXEMBOURG
Ministère de l'Économie

Information and Communication Technology (ICT) is playing an increasingly important part in our everyday lives and has assumed a predominant role through the development of the economy and information society. In Luxembourg, ICT has always offered innovative products and services, allowing us to develop new and improve existing societal, market, and business activities. Furthermore, Ubiquitous Computing is increasingly becoming a reality, as more and more everyday objects and devices are equipped with sensors, actuators, computing, and communication technology. Moreover, all devices are designed to be interoperable with one another.

As a vital support sector for the economy, ICT nowadays means multiple interconnected digital media that become smarter through various technologies such as Cloud Computing, Big Data and Analytics, Internet of Things and Smart Cities, Smart Grid, Data Digitization, advanced information security technologies, etc.

In order to take the next steps in this smart world, an ad-hoc common technical language must be clearly defined. Embracing these issues, technical standardization remains a key source of knowledge, in continuous improvement, that will enable common technical convergence to be achieved. In this context, and based on strong Digital Trust principles, smart ICT currently constitutes the greatest opportunity to meet new economical, societal, and environmental challenges.

This White Paper presents the state of the art in the key area of smart ICT, its economic challenges and prospects, and notably the requirement of Digital Trust as an essential factor in performing the related development. Last but not least, in this reference document, technical standardization, which is highlighted as one of the enablers for Digital Trust for smart ICT, is fully examined with specific reference to each smart ICT area (cloud computing, big data and analytics, Internet of Things).

ILNAS, the national standards body, is tasked with implementing the national technical standardization strategy, with a strong policy regarding the ICT sector. Associated with research initiatives, this White Paper establishes the foundations on which ILNAS will develop the necessary education about ICT technical standardization at national level.

Within this framework, Luxembourg will continue to consider technical standardization as a real force multiplier for the economy, competitiveness, and the ICT sector in particular.

Etienne Schneider

Deputy Prime Minister
Minister of the Economy

TABLE OF CONTENTS

ABBREVIATIONS

2G	Second Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
4G	Fourth Generation
5G	Fifth Generation
AES	Advanced Encryption Standard
AIOTI	Alliance for Internet of Things Innovation
AMP	Alternative Mac/Phy address
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ARIB	Association of Radio Industries and Businesses
ATIS	The Alliance for Telecommunications Industry Solutions
AWI	Approved Work Item
B2B	Business-to-Business
BCDR	Business Continuity and Disaster Recovery
BDaaS	Big Data as a Service
BI	Business Intelligence
BIOS	Basic Input Output System
BLE	Bluetooth Low Energy
CAGR	Compound Annual Growth Rate
CapEx	Capital Expenses
CASB	Cloud Access Security Brokers
CCRA	Cloud Computing reference architecture
CCSA	China Communications Standards Association
CDMI	Cloud Data Management Interface
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, and Availability
CIMI	Cloud Infrastructure Management Interface
CoAP	Constrained Application Protocol
CPPS	Cyber Physical Production Systems
CPS	Cyber Physical Systems
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSC	Cloud Standards Coordination
CSP	Cloud Service Provider
DCPS	Data-Centric Publish-Subscribe
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DES	Data Encryption Standard
DLP	Data Loss Prevention
DMTF	Distributed Management Task Force
DNA	Deoxyribonucleic Acid
DRM	Digital Rights Management
DSM	Digital Single Market
DTLS	Datagram Transport Layer Security
DVA	Data Value Assessment
EaS	Education about Standardization
EDI	Electronic Data Interchange
EMEA	Europe, the Middle East and Africa
ENISA	European Union Agency for Network and Information Security
EPC	Electronic Product Code
ESOs	European Standards Organizations
ETSI	European Telecommunications Standards Institute
EU	European Union
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FTP	File Transfer Protocol
GB	Gigabytes
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HDD	Hard Disk Drive
HLA	High Level Architecture
HMAC	Keyed-Hash Message Authentication Code
HOTP	HMAC-based One-Time Password
HRM	Human Resource Management
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
ID	Identifier
IDaaS	Identity as a Service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IIoT	Industrial Internet of Things
ILCM	Information Life Cycle Management
ILNAS	*Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services*
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRQs	Interrupt Requests
ISG	Industry Specification Group
ISI	Information Security Indicators
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ISOC	Internet Society
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union (ITU) on Telecommunication Standardization Sector
JTC	Joint Technical Committee
JWG	Joint Working Group

LSP	Layered Service Provider
M2M	Machine-to-Machine
MAC	Media Access Control
MDR	Metadata Registry
MFA	Multi Factor Authentication
MITM	Man in the Middle
MQTT	Message Queuing Telemetry Transport
NaaS	Network as a Service
NBD-PWG	National Institute of Standards and Technology (NIST) Big Data Public Working Group
NetCDF	Network Common Data Form
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NP	New Project
OASIS	Organization for the Advancement of Structured Information Standards
OCC	Open Cloud Consortium
OCF	Open Connectivity Foundation
OECD	Organisation for Economic Co-operation and Development
OGF	Open Grid Forum
OLAP	Online Analytical Processing
OOB	Out of Band
OpEx	Operating/Operational Expenses
OS	Operating System
PaaS	Platform as a Service
PAP	Policy Administration Point
PC	Personal Computer
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessments
PII	Personal Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PKI	Public Key Infrastructure
PLC	Power Line Communication
PLT	Programming language theory
PMA	Protected Module Architecture
POS	Point of Sale
PSTN	Public Switched Telephone Network
PUK	PIN Unlock Key
PWG	Public Working Group
QoS	Quality of Service
R&D&I	Research and Development and Innovation
RA	Reference Architecture
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio-Frequency Identification
RIRs	Regional Internet Registries
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman (cryptosystem)
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SC	Subcommittee
SDOs	Standards Developing Organizations
SecaaS	Security as a Service
SFTP	SSH File Transfer Protocol
SG	Study Group
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMBs	Small and Medium-sized Businesses
SMEs	Small and Medium-sized Enterprises
SMS	Short Message Service
SNIA	Storage Networking Industry Association
SNRA	Sensor Network Reference Architecture
SoC	System on Chip
SPMs	Self-protecting modules
SPS	Service Policy Statements
SRG	Subgroup Rapporteur Group
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	Secure Simple Pairing
STOMP	Streaming Text Oriented Messaging Protocol
SWG	Special Working Group
TBT	Technical Barriers to Trade
TC	Technical Committee
TCB	Trusted Computing Base
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TOG	The Open Group
TOTP	Time-based One-time Password Algorithm
TPM	Trusted Platform Module
TS	Technical Specification
TSAG	Telecommunication Standardization Advisory Group
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
TTPs	Trusted Third Parties
TV	Television
UDP	User Datagram Protocol
UNCTAD	United Nations Conference on Trade and Development
UPnP	Universal Plug and Play
US	United States
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WD	Working Draft
WEP	Wired Equivalent Privacy
WG	Working Group
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks
WTO	World Trade Organization
XaaS	Everything as a Service
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

INTRODUCTION

Trust is one of the most fundamental constructs in our society [1] and involves an interaction between two parties. Trust relates to the presumption about the dependability and reliability of, and/or confidence in a person, process, system, or other entity. Mayer *et al.* [2] define trust as: "*the willingness of a party [trustor] to be vulnerable to the actions of another party [trustee] based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party*". Although its importance is widely recognized, because of its complex notion, there is still no definitive consensus in the scientific literature [3] about exactly what trust is. Nevertheless, trust comprises three fundamental elements that relate to expectations, beliefs, and the risk appetite of trustor and trustee. Huang and Nicol [4] describe it as follows: 1) expectancy – the trustor anticipates a specific behavior from the trustee; 2) belief – the trustor has confidence that the expected behavior occurs, based on the evidence of the trustee's competence, goodwill, and integrity; 3) willingness to take risk – the trustor is prepared to take a risk for that belief. The behavior of the trustee is of course beyond the control of the trustor. The trustor's belief in the trustee's expected behavior is based on the trustee's competence, goodwill, and integrity. The trustee's integrity gives the trustor confidence in the predictability of the trustee's behavior.

In the context of digital technologies, with the increased complexity and connectivity of current Information and Communication Technology (ICT) systems and the data volume and diversity involved, trust has also become a keystone, notably to ensure robustness and information security of the related systems. In this framework, this White Paper focuses on the concept of Digital Trust for Smart ICT, *i.e.* the aforementioned relationship between two parties where at least one has an activity related to a smart digital technology. ICT, also commonly referred to as Information Technology (IT), is defined by the Joint Technical Committee ISO/IEC JTC 1 as follows: "*ICT includes the specification, design and development, integration and interoperability of systems, services, tools and applications. These deal with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage, and retrieval of information, and their related accessibility, cultural, linguistic adaptability, and societal aspects*"[1].

On the whole, Smart ICT relates to any ICT technology – hardware, software, communication – collecting or using data from a significant number of devices. In some cases, these allow users to make decisions based on new information, or they allow automation and system optimization. The idea is that by using many dispersed sensors, one can create a more accurate representation of a system (whether it is the load flow in an electrical network, or people's reaction to a given message on social media) and therefore take more nuanced decisions. In this context, being smart means looking at the right parameters, and avoiding being overwhelmed by their number. For the purpose of this White Paper, Smart ICT specifically addresses technologies and applications of the Cloud, Big Data and Internet of Things (IoT).

Therefore, Digital Trust for Smart ICT indicates a positive and verifiable belief about the perceived reliability of a digital information source, product or service, leading to an intention to use [5]. Building and maintaining Digital Trust involves more aspects than in a world without electronic communications, because digital communications rely not only on human beings and their relationships, but also on digital components. In Digital Trust, not only the classical social trust concept is involved, but also technological trust from the different parties in an IT system as depicted by Giustiniano and Bolici [6] (see Figure 1).

[1] ISO/IEC JTC 1, Information technology – Strategic Business Plan 2015.

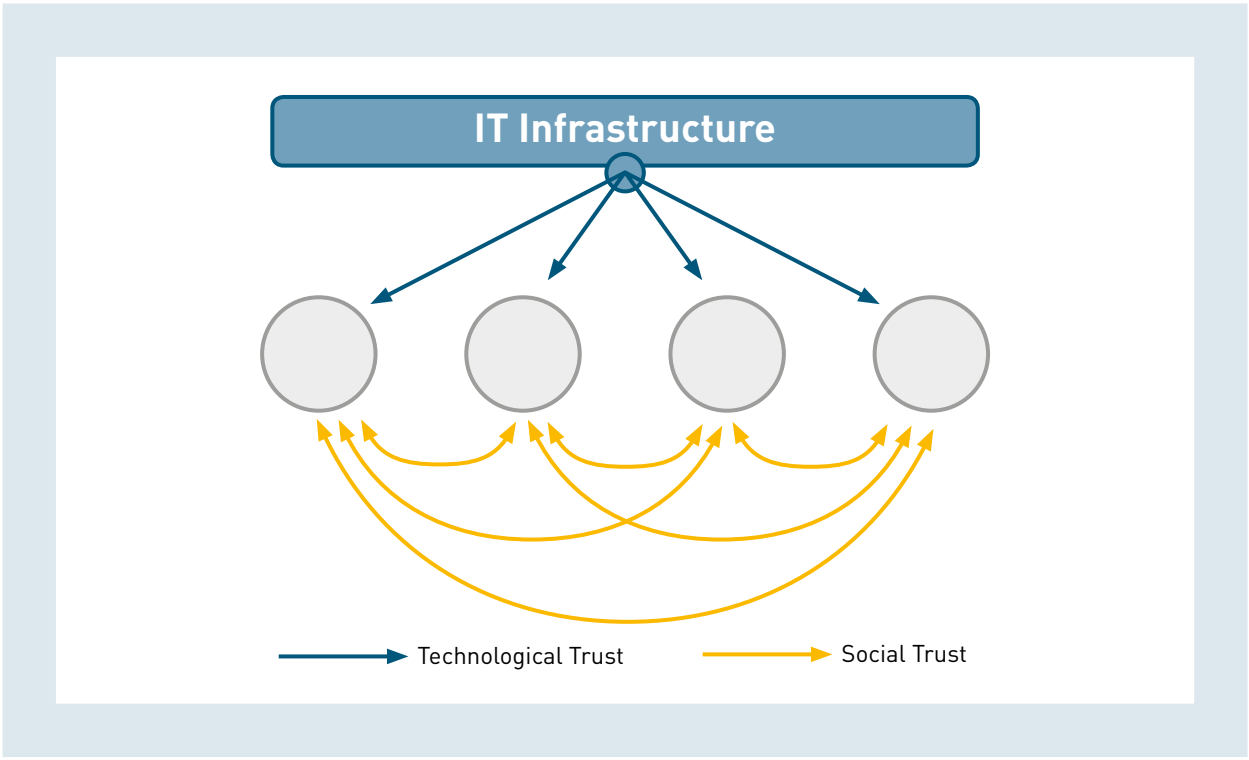


Figure 1 – Trust in the digital information age [6]

Because of that, the trust attributes *expectancy*, *belief,* and *risk willingness* are both social and technological trust components at the same time. In this case, when a trustor is willing to trust a digital service provider (the trustee), he does not have control or knowledge of the trustee IT system. The service provider serves as a proxy for the trustor regarding technological trust and thus the complexity of building and keeping trust lies in the risk of uncertainty. This uncertainty is caused by asymmetry of information, as one party has information that the other party does not [7]: is the IT infrastructure secure enough, does it prevent Personal Identifiable Information (PII) leaks, can it provide sufficient privacy guarantees?

Accenture also defines Digital Trust as "*the confidence placed in an organization to collect, store, and use the digital information of others in a manner that benefits and protects those to whom the information pertains*". They identified four key areas to Digital Trust: 1) accountability, 2) security, 3) privacy, and 4) consumer benefit and value [8], each of which must be satisfied to gain and maintain trust with a specific brand. By investing in these areas, companies can gain a competitive advantage by increased Digital Trust, as consumers believe that their personal data are adequately protected.

In this context, this White Paper has been put forward to investigate and develop knowledge in the field of Digital Trust for Smart ICT. It surveys current advances in Digital Trust from three complementary points of view: a technical analysis, a business and economic prospective analysis, and a technical standardization perspective. From the technical analysis perspective, the document reviews the basic concepts of the technology and the existing work supporting the development of Digital Trust. It presents some technical challenges related to Digital Trust. The document also proposes considerations, when implementing a Digital Trust strategy, to reap the benefits of the business and economic prospective analysis. Finally, standards and technical standardization are presented as an important tool to improve Digital Trust for smart ICT systems.

The White Paper is composed of four chapters. Chapter 1, Chapter 2 and Chapter 3 are based on research results and Chapter 4 corresponds to the work proposed by ILNAS in the standard analysis of the ICT sector[2].

Chapter 1 introduces the Internet of Things, Cloud Computing, and Big Data smart technologies. It shows how these technologies interact, places them into context, globally then individually. It explains why Digital Trust is important for their development and provides a number of suggestions on how to achieve Digital Trust.

Chapter 2 puts forward an economic analysis and forecast of Digital Trust for these smart technologies, then highlights the economic challenges of Digital Trust that need to be addressed in order for these technologies to fully develop their potential.

Chapter 3 presents an analysis of existing work and techniques that are of interest for achieving Digital Trust. First, it proposes this analysis for work that addresses several layers of Smart ICT and thus addresses the Digital Trust problem globally. Then it focuses on each of the smart technologies, to present related work that is more specific to the given technology.

Chapter 4 details the existing standards and standardization bodies enabling Digital Trust for Cloud Computing, Big Data, and IoT and how these bodies are structured and interlinked.

Finally, the conclusion summarizes the key components of Digital Trust for each of the three aforementioned smart technologies and emphasizes the importance of Digital Trust and its prospects at European and national level.

[2] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes-nationales/pub-standards-analysis-ict-v6-0/standards-analysis-ict-6-0.pdf

1 SMART ICT, A DEFINITION AND INTRODUCTION TO THE CONCEPTS

With the rapid development and the ever increasing performance and capability of Information and Communications Technology (ICT), new possibilities of interaction and integration have emerged. In recent years, the ICT field has broadened so much that it is now pervasive in every aspect of people's lives, businesses and the environment. Every market segment is now impacted directly or indirectly by these changes and today, the convergence of new digital technologies, energy and transportation systems is driving the fourth industrial revolution, which is based upon these ICT developments. This can be explained by several factors:

- Evolution of connectivity in terms of bandwidth and integration of systems and devices.
- Advent of Cloud technologies and new computing capabilities.
- Dramatic changes in hardware and software development.

These factors enable new technologies such as Internet of Things to develop and innovate through Big Data analytics, providing widely accessible and advanced services.

ICT has completely changed the way people communicate in comparison to the situation fifteen years ago. Between 2000 and 2015, Internet penetration has increased almost seven-fold from 6.5% to 43% of the global population according to the 2015 ITU report on ICT impact[3]. This evolution also made connectivity more mobile, in the sense that much of the growth in web connectivity has come from mobile devices. Also according to the 2015 ITU report, mobile broadband penetration has gone up 12-fold since 2007. In 2015, 69% of people on earth were covered by 3G broadband and as much as 89% in urban areas.

The emergence of Cloud technologies, providing on-demand usage of services and platforms, has unlocked considerable new potential and revolutionized the way business processes are addressed. It allows a switch from an on-premises, static and CapEx (Capital Expenses) model to a dynamic, elastic, and OpEx (Operating Expenses) one. The Cloud has transformed lives and businesses by allowing individuals, startups, and SMEs (Small and Medium-sized Enterprises) to access large IT infrastructures and large companies and institutions to better adapt their existing IT infrastructures according to their workflow. These large ready-to-use Cloud platforms also enable new kinds of technologies to emerge. Cloud technologies provide the power necessary to run Big Data and Analytics as well as the connectivity and management infrastructure required for the Internet of Things.

The hardware evolution driving the ever-increasing processing power of chips, along with the reduction of their size and power consumption, has led to growth in numbers and diversity of devices able to compute and communicate. The software evolution, taking advantage of the multiplicity of computation-capable machines, using parallelization algorithms and frameworks, enabled parallel systems to compute larger complex problems in a shorter timeframe.

Today, ICT has become *Smart*. Thanks to common and standard interfaces, the different components of the technology are now able to interact and collaborate to serve a common and higher goal. This starts with advances in processing techniques such as data analytics, optimization, and modeling. It continues with interaction between software systems, networked sensors, and their integration with mobile devices and new ways of gathering data, such as social media and crowdsourcing. These components are being supported by Cloud technology serving as a driver of integration, and communication protocols and infrastructures serving as the medium of their interaction.

[3] http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.VyB2DnrOjN5

If the risks associated with these disruptive Smart ICT technologies (e.g. security, privacy and compatibility among others) are carefully addressed, this will increase the potential to further transform the ICT sector and, in a more general sense, society itself; driving greater efficiency, increasing productivity, and greatly simplifying business processes. In this context, these risks will be addressed through the notion of **Digital Trust** in the technologies, in the existing platforms and in their interactions to leverage the huge potential of massive adoption of Smart ICT.

1.1 SMART TECHNOLOGY LANDSCAPE

Although the terms Cloud Computing, Internet of Things and Big Data were coined last century, the realization of these ICT concepts is recent and they became commercially available around 2004.

Google's MapReduce model and framework that is the basis of Big Data Analytics was published in 2004 [9]. The initial public beta release of the Cloud Computing platform Amazon EC2 started on August 23, 2006[4]. Just months later in November 2006, Hadoop, an Open Source implementation of the MapReduce framework, was run successfully on EC2[5], achieving a convergence of Big Data and public Cloud. In 2005, ITU published a report on Internet of Things (IoT) [10] exploring the possibilities offered by IoT for smart homes, mobility, and quality of life. At this time, they envisioned that the embedded intelligence in things themselves will enable the distribution of processing power to the edges of the network (referred to as Edge Computing), offering greater possibilities for data processing. This idea of Edge Computing comes in combination with and support of Big Data and Cloud Computing by enabling analytics and knowledge generation to occur at the source of the data itself.

All these smart technologies have now become entangled and closely linked. The Internet of Things produces both raw and pre-processed data. Big Data stores, analyses and provides mechanisms for operating and understanding the large amount of data produced. Cloud Computing supports these technologies by providing the processing power and infrastructure to allow the capture, storage, analysis of the data (see Figure 2).

[4] https://aws.amazon.com/releasenotes/Amazon-EC2/353

[5] http://glinden.blogspot.lu/2006/11/hadoop-on-amazon-ec2.html

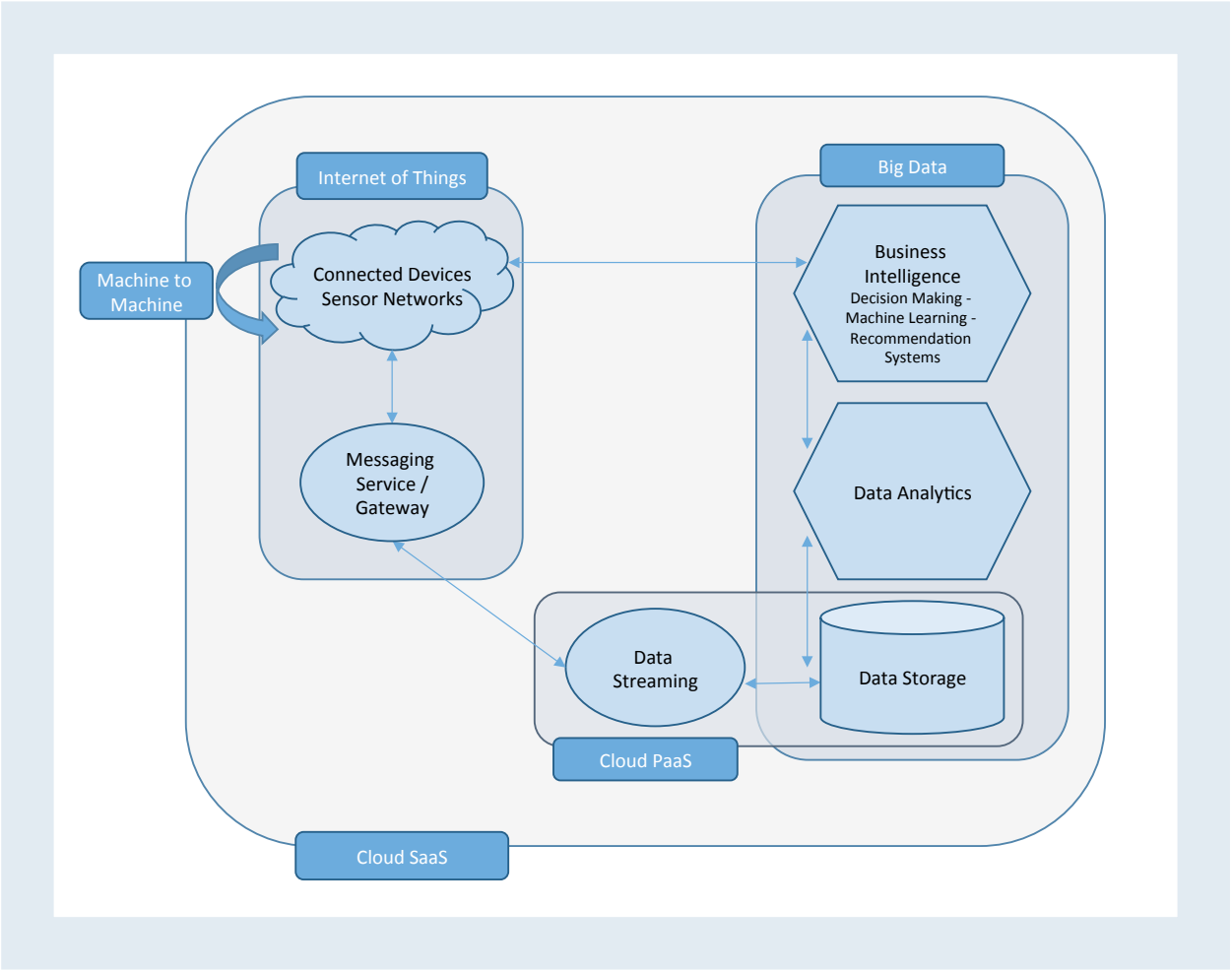


Figure 2 – Smart ICT Components and their Interactions

To better understand how these technologies work and interact together, the rest of the chapter provides an overview and the concepts of each of these three smart technologies: Internet of Things, Cloud Computing and Big Data and in particular why and how Digital Trust and its standardization are important challenges for these technologies.

1.2 INTERNET OF THINGS

The Internet of Things (IoT) has the potential to fundamentally change how individuals and businesses interact. The amount of data generated by humans and devices is exponentially growing (Box 1) and companies can capture new categories of data on an unprecedented scale. These vast amounts of data are being collected, stored, analyzed, and monitored. Businesses can aggregate these data across devices and leverage analytics to enter new markets and even create new digital ecosystems. They can monetize this to offer compelling new digital products and services and reshape consumer experiences.

Annual global IP traffic will pass the zettabyte (1000 exabytes) threshold by the end of 2016, and will reach 2 zettabytes per year by 2019. By the end of 2016, global IP traffic will reach 1.1 zettabytes per year, or 88.4 exabytes (nearly one billion gigabytes) per month, and by 2019, global IP traffic will reach 2.0 zettabytes per year, or 168 exabytes per month.

Global Internet traffic in 2019 will be equivalent to 66 times the volume of the entire global Internet in 2005. Globally, Internet traffic will reach 37 gigabytes (GB) per capita by 2019, up from 15.5 GB per capita in 2014.

Traffic from wireless and mobile devices will exceed traffic from wired devices by 2016. By the end of 2016, wired devices will account for 47% of IP traffic, and WiFi and mobile devices will account for 53% of IP traffic. In 2014, wired devices accounted for the majority of IP traffic, at 54%.

Two-thirds of all IP traffic will originate from non-PC devices by 2019. In 2014, only 40% of total IP traffic originated from non-PC devices, but by 2019 the non-PC share of total IP traffic will grow to 67%. PC-originated traffic will grow at a Compound Annual Growth Rate (CAGR) of 9%, and TVs, tablets, smartphones, and machine-to-machine (M2M) modules will have traffic growth rates of 17%, 65%, 62%, and 71% respectively.

The number of devices connected to IP networks will be more than three times the global population by 2019. There will be more than three networked devices per capita by 2019, up from nearly two networked devices per capita in 2014. Accelerated in part by the increase in devices and the capabilities of those devices, IP traffic per capita will reach 22 GB per capita by 2019, up from 8 GB per capita in 2014.

Box 1 – The amount of data being generated is unprecedented [11]

However, companies' successful engagement with the world of IoT is highly dependent on the level of Digital Trust customers have in them. Therefore, for any company to leverage the IoT business, it is imperative to gain customer confidence and thus to obtain their Digital Trust.

Before diving into the subject of IoT in more detail, it is important first to clarify what IoT is. Unfortunately, there is no unambiguous definition of IoT due to the fact that various stakeholders, including commercial businesses and scholars, have different backgrounds and are driven by specific purposes and diverse

interests [12]. Some use a broad definition of the IoT, consisting of all devices and objects connected with the Internet, whose state can be read or changed with or without the active involvement of individuals [13]. Others use a smaller scope definition, related only to smart objects and explicitly excluding person-operated/controlled devices such as laptops, routers, servers, tablets, and smartphones. This is also one interest of standardization: to provide a unified definition of a particular technology. For this chapter the (broad) definition of the ITU is used (Box 2).

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 as:

"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies".

"**thing**: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks."

Box 2 – Definition of IoT by the International Telecommunication Union [14]

However, concerning and in addition to this broad definition, the term "**Internet of Everything**" is increasingly being accepted as the best description of this phenomenon since things connected to the Internet not only link to other things, but also monitor for example health, location, and activities of people and animals, the quality of water and other elements in the natural environment [13].

1.2.1 EVOLUTION OF THE INTERNET OF THINGS

The origins of IoT can be traced back to 1999 and have been attributed to MIT's development community of Radio-Frequency Identification (RFID) technology with the aim of spreading the use of RFID in worldwide networks [15]. IoT advanced gradually in society by means of wireless communication systems such as WiFi, Bluetooth, NFC[6], WSN[7] and 4G. Today, the concept of IoT is manifold and is characterized as heterogeneous technologies and standards, which correspond to the provision of innovative products and services in various application domains [3]. These heterogeneous technologies include communication technologies, ubiquitous computing, sensing technologies, and embedded devices, which are merged in such a way that the physical and virtual worlds meet and are continuously in symbiotic interaction [12]. Logically, an IoT system consists of a set of smart devices (building blocks) that interact on a collaborative basis to fulfill a common goal.

By putting programming logic into everyday "things", these become "smart things" that collect data from the environment, compute, and integrate seamlessly with the physical world. Such a thing must be easily locatable, recognizable, addressable and controllable. Because these things are also interconnected through the Internet, an almost endless combination can be devised to create innovative products and services. The gathered "Big Data" can be shared among the different services, and as a replacement for traditional computer systems, "Cloud Computing" will offer computation, networking, communication and storage services among others. This typically illustrates the integral and intricate relationships between these three Smart ICT topics addressed in this chapter.

The evolution of IoT is supported by four technological developments: 1) Machine to Machine (M2M) communications; 2) Sensors; 3) Big Data Analytics; 4) Cloud Computing (see Figure 3).

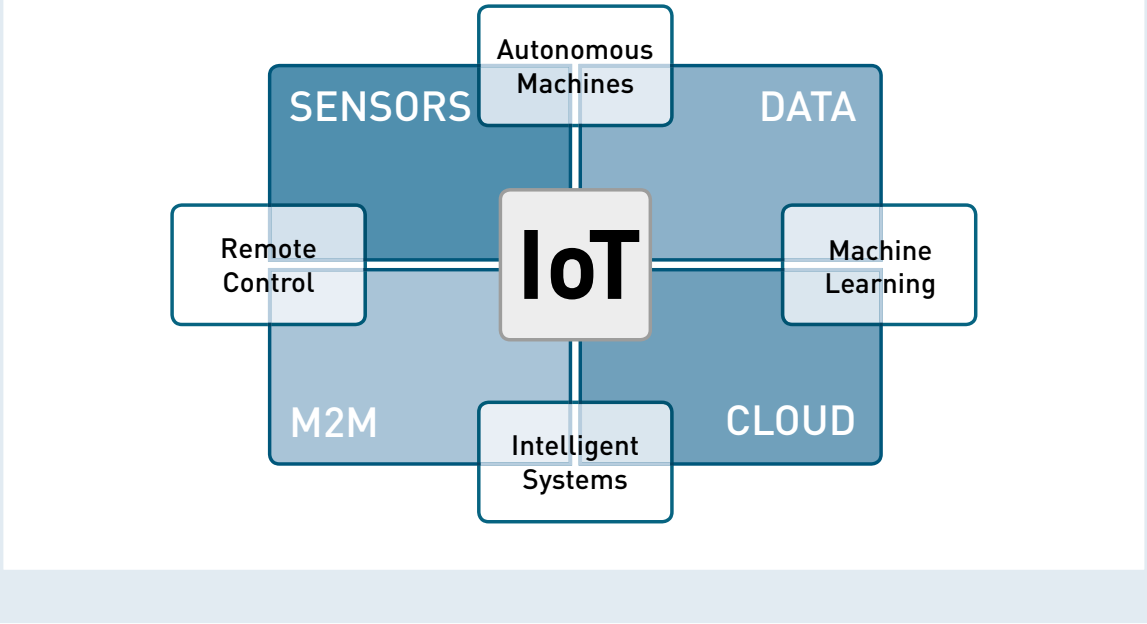


Figure 3 – Main enablers of the Internet of Things [13]

[6] https://en.wikipedia.org/wiki/Near_field_communication
[7] https://en.wikipedia.org/wiki/Wireless_sensor_network

In the remainder of this section, a brief introduction to M2M and Sensors is provided whereas Cloud Computing and Big Data will be discussed in more detail in sections 1.3 and 1.4.

Machine-to-Machine (M2M) communication previously related mainly to applications involving RFID [16], but now involves any type of electronic M2M communication (e.g. Near Field Communication (NFC), Bluetooth, WiFi, and 2G/3G/4G networks).

RFID makes use of so-called tags (a chip with antenna) that contain electronically stored data. RFID uses electromagnetic fields to allow automatic identification and tracking tags. Because these tags do not need to be within the line of sight, RFID readers are typically embedded in objects. There are two types: passive and active tags.

1. Passive tags transmit data when they collect energy from the electromagnetic fields of a nearby RFID reader.

2. Active tags contain a local power source and can operate at hundreds of meters from RFID readers.

The main issue of NFC M2M communications concerns standardization because of the unwillingness among organizations (e.g. public transport companies and retailers) to open access to their respective client base. Such NFC card infrastructures are knowingly made incompatible.

WiFi (IEEE 802.11x) is the basis for many IoT devices in home automation (i.e., for smart homes) whereas the use of mobile wireless networks is indispensable to the IoT for geographically dispersed M2M connectivity.

Sensors are electronic devices that measure physical quantities (e.g. pressure, acceleration, light and moisture) and convert these into electronic signals that can be read by other electronic devices. Sensors used in IoT include electronic sensors, biosensors, and chemical sensors and can be regarded as the interface between the physical world and the virtual world [17]. In many cases the sensor data is processed and acted upon by electronic devices called actuators that convert electrical signals into a physical phenomenon by means of a control mechanism. Examples include thermostats, carports and sun blinds. Early sensor and actuator systems discarded the generated data, but today these are increasingly transmitted to other electronic devices via a variety of means: wired and wireless, short or long range, low or high power, low or high bandwidth (see Table 1). Subsequently, these data are stored in the Cloud for further correlation and analysis. Because of the communication between these devices and control by programmed logic, machines have become aware of their surroundings (i.e., "smart") and able to act accordingly.

	GEOGRAPHICALLY FIXED	GEOGRAPHICALLY MOBILE
GEOGRAPHICALLY DISPERSED	*Application:* Smart grid, smart meter and smart city, remote monitoring. *Technology required:* Public Switched Telephone Network (PSTN), broadband, 2G/3G/4G, power line communication (PLC).	*Application:* Car automation, eHealth, logistics, portable consumer electronics. *Technology required:* 2G/3G/4G, satellite.
GEOGRAPHICALLY CONCENTRATED	*Application:* Smart home, factory automation, eHealth. *Technology required:* Wireless personal area networks (WPAN), wired networks, indoor electrical wiring, WiFi, RFID, Near Field Communication.	*Application:* On-site logistics. *Technology required:* WiFi, WPAN.

Table 1 – The different types of M2M connectivity based on geographic dispersion and geographic mobility [13]

1.2.2 DIGITAL TRUST REQUIREMENTS

Digital Trust is fundamental for ensuring the further development and success of IoT. For devices, or "things" that are permanently connected, whose purpose is the monitoring of activities and data collection and that send these data through the Internet, two major Digital Trust requirements have to be addressed: security and privacy [3]. These two broad requirements include authentication and authorization within the IoT network, data confidentiality, privacy and trust among users and things, and the enforcement of security and privacy policies. Sicari *et al.* [3] argue that conventional security measures and privacy enforcement cannot be applied to IoT technologies due to their limited computing power. In addition, the huge number of interconnected devices will cause scalability issues. Nevertheless, to guarantee Digital Trust in IoT environments, the interconnected devices have to process and handle the data in compliance with user rights and needs. Borgia [12] discusses the most significant IoT requirements that include one category specifically allocated to trust, security and privacy. Further requirements relate to efficiency, flexibility and quality, among others (see Table 2).

REQUIREMENT	REQUIREMENT DESCRIPTION
Heterogeneity	Managing the variety of devices/technologies/services/environments.
Scalability	Avoiding the explosion of resources/exchanged data/operations.
Cost minimization	Optimization of development/maintenance costs and energy consumption.
Self-*	Self-configuration, self-organization, self-adaptation, self-reaction to events and stimuli, self-discovering of entities and services, self-processing of Big Data.
Flexibility	Dynamic management/reprogramming of devices or groups of devices.
QoS	Observance of QoS guarantees (e.g. bandwidth, delay) to services/ applications.
Secure environment	Robustness to communication attacks, authentication, data transfer confidentiality, data/device integrity, privacy, trusted secure environment.

Table 2 – IoT general requirements [12]

1.3 CLOUD COMPUTING

Cloud Computing is defined by the OECD *"as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort"* [18].

In the past decade, Cloud Computing has gained enormous popularity by many organizations all around the world as it enables *"ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [19]. It builds on the foundations of distributed computing and virtualization of resources, therefore hardware and software (processing) are in principle independent of physical structures and are no longer closely tied to a geographical location. However, the consumer may be able to specify location at a higher level such as the data center's location country or region.

The Cloud Security Alliance has specified five key characteristics of Cloud services (see Table 3), that demonstrate their relation to, and differences from, traditional computing approaches [20].

CHARACTERISTIC	DESCRIPTION
On-demand self-service	A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically without requiring human interaction with a service provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms as well as other traditional or Cloud-based software services.
Resource pooling	The provider's computing resources (e.g. storage, processing, memory, network bandwidth, and virtual machines) are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource usage by leveraging a metering of e.g. storage, processing, bandwidth, or active user accounts. It provides transparency for both the provider and consumer of the service by means of monitoring, controlling and reporting.

Table 3 – Key characteristics of Cloud Computing services [20]

1.3.1 SERVICE AND DEPLOYMENT MODELS

NIST identified a three-tiered service model Cloud stack (see Table 4), with increasing levels of service provisioning, which are referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[8].

- IaaS is the most basic Cloud-service model in which on-demand provision of infrastructure is offered, in most cases delivered with virtual machines. The subscriber maintains the operating system and software applications, while the underlying systems are managed by a service provider (including the physical computing resources, location, data partitioning, security, backup, etc.). There are many IaaS providers, including all major IT companies: Amazon Web Services, Windows Azure IaaS, Google Compute Engine, IBM SmartCloud Enterprise, and HP Enterprise Converged Infrastructure.

[8] http://dx.doi.org/10.6028/NIST.SP.800-146

- With the PaaS Cloud-service model, the subscriber gets an on-demand computing platform for development, testing, deployment and on-going maintenance of applications. It typically includes the operating system, programming-language environment, database, and web server. The subscribers (in many cases software application developers) develop and run their software solutions, without the cost of buying and managing the complexity of the underlying hardware and software. There are many PaaS providers, such as Windows Azure PaaS, Google App Engine, Red Hat OpenShift, AppFog and Engine Yard.
- SaaS is the Cloud-service model where an application is available on demand and this is the most common form of Cloud Computing delivered today. The Cloud providers manage the infrastructure and platforms that run the applications and the subscribers access the software from Cloud clients. Examples of SaaS providers are: Salesforce.com, Concur Travel, Microsoft Office 365, Gmail and MySAP.

SERVICE MODEL TYPE	CAPABILITY DESCRIPTION
Infrastructure as a Service (IaaS)	Subscriber uses processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
Platform as a Service (PaaS)	Subscriber deploys onto the Cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.
Software as a Service (SaaS)	Subscriber uses the provider's applications running on a Cloud infrastructure.

Table 4 – Cloud Computing service models [21]

Figure 4 depicts the allocation of responsibilities in the three Cloud Computing service models (i.e., IaaS, PaaS and SaaS). The figure illustrates at what level the different items of the software stack are managed compared to a traditional on-premises approach. Whereas in a traditional approach the full stack is managed by the client, in an IaaS model only the layers above (and including) Operating System are managed by the client. In a PaaS, the middleware and the lower layers are managed by the Cloud vendor and in a SaaS model, the full stack is managed by the vendor. These different models are useful for different use cases and enable Cloud providers to easily perform market segmentation and adapt their platform to their clients and their usages.

Many other Cloud-based services have been derived from the original NIST model, to take advantage of economies of scale and streamlined delivery mechanisms, such as those for Identity (IDaaS), Security (SecaaS), and Network (NaaS) as a Service. This gave rise to the term XaaS or everything as a service [22].

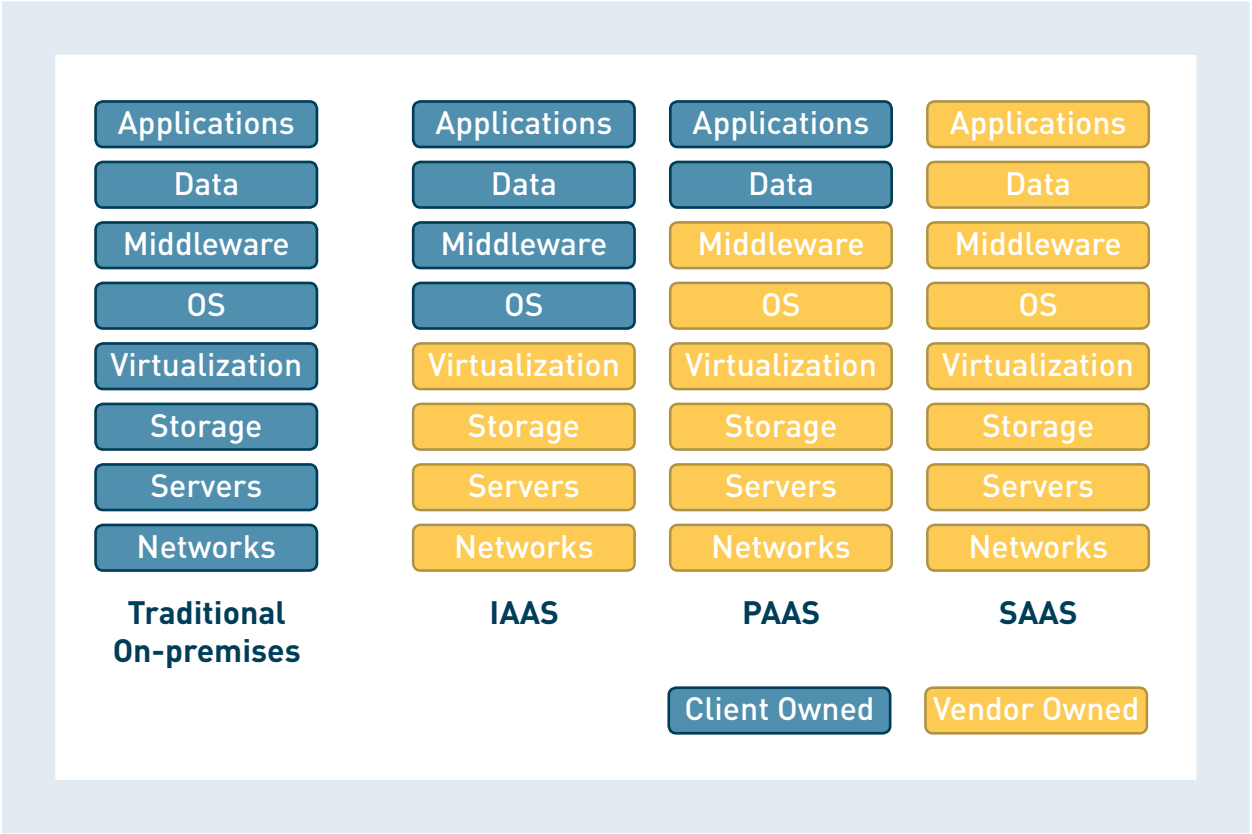


Figure 4 – Allocation of responsibilities in the Cloud Computing service models

Alongside these three service models, NIST distinguishes four deployment models of Cloud Computing[9]: private Cloud, community Cloud, public Cloud, and hybrid Cloud. Fundamentally, one can make the distinction between a private Cloud and public Cloud with the other two as derived models.

- A private Cloud is operated solely for an organization, either managed by the organization itself or a third party and can exist on-premises or off-premises.
- A community Cloud is shared by several organizations and supports a specific community that has common interests (security, compliance, jurisdiction, etc.) either managed by (one of) the organizations or a third party and can exist on- premises or off-premises.
- A public Cloud is provisioned for open use by the general public. It may be operated, managed, and owned by (a combination of) business, academic, or government organization(s) and exists on the premises of the Cloud provider.
- A hybrid Cloud is a composition of two or more Clouds (private, community, or public) that remain unique entities but are bound together to enable data and application portability.

The reasons for Cloud adoption are various, such as the intention to increase business agility by lowering the provisioning cost of new hardware and software, the lack of skilled internal staff, the need for more innovation than the organization can handle, or the desire to eliminate legacy applications and obtain equivalent services from the Cloud provider. Cloud Computing is much more scalable than traditional IT solutions, as it can follow changes in business volume requirements much more easily. Organizations struggle to adjust the risk of investing in IT, which may lead to a capacity problem or lower profits. When businesses adopt this computing paradigm, its impact resonates throughout the entire organization.

[9] http://dx.doi.org/10.6028/NIST.SP.800-145

The main benefits of Cloud Computing, as perceived by European firms, are quick and easy deployment of solutions, higher flexibility due to scaling services up or down, and a reduction in ICT-related costs [13]. Furthermore, as IT consumes a substantial amount of money, no large initial capital expenses (CapEx) in software development, hardware and software licensing are required. With Cloud Computing, a good deal of these capital costs become operational expenses (OpEx) that vary with its use (pay-per-use).

Though many of its features make Cloud Computing attractive, new security risks arise when various firms share the same group of resources [23], [24]. Security and privacy concerns become much more prominent as liabilities and damages are articulated in contracts. And due to its open nature, some authors even claim that security, privacy, and trust in the Cloud provider are the three major concerns of Cloud Computing [25]. Once a contract with a Cloud Computing provider is in place, switching providers may not be a trivial exercise, which increases the risk of vendor lock-in. So, establishing Digital Trust with Cloud service providers will require the customers' confidence, control and reliability, and the avoidance of commercial issues like lock-in [24]. Nevertheless, achieving Digital Trust in Cloud Computing would offer great advantages with a minimal, maybe even positive, impact on business risks if the Digital Trust problematics are addressed correctly.

1.3.2 DIGITAL TRUST CHALLENGES

In the field of Cloud Computing, there are still complex and important Digital Trust challenges to be tackled [26]. From the perspective of the consumer, these range from technical to commercial and strategic aspects [27]:

- Data security concerns
- Reliability of service and business continuity
- Integration and interoperability with on-premises systems
- Weak contracts, SLAs and consequences for non-performance
- Limited transparency
- Loss of control
- Immaturity of vendors
- Vendor lock-in and data portability
- Long-term costs and TCO uncertainties
- Legal and regulatory compliance

The resulting lack of trust could be a key inhibitor for further Cloud adoption in areas where confidential (sensitive to critical) information is involved. Kalluri & Rao [25] specify trust challenges of Cloud Computing from the perspective of the provider (see Table 5). If Cloud service providers succeed in tackling these security and privacy challenges, they have succeeded in achieving trustworthy services in Cloud Computing, thereby enhancing Cloud customer confidence and thus further building Digital Trust in Cloud Computing service offerings.

TRUST CHALLENGE	DESCRIPTION
Users/resources joining the Cloud dynamically	As many users and resources join and leave the Cloud dynamically, they should establish the trustful relationship with the provider and they accommodate the change which is occurring dynamically.
Different security policies	The various users and resources have diverse security policies which makes an overall suitable and consistent relationship difficult.
Continuity and provider dependency	The complexity of Cloud architectures and the lack of transparency increases security risk and centralized system management may introduce single points of failure. This could threaten the availability of Cloud users' data and computing capabilities.
Compliance with applicable regulations and best practice	The Cloud service provider has to comply with many laws and regulations such as privacy, civil and consumer protection laws.
Trust enhancement through assurance mechanisms	The Cloud Computing concept cannot guarantee full, continuous and complete control of Cloud users over their assets. Therefore, the establishment of appropriate "checks and balances" to ascertain that Cloud providers meet their obligations becomes very relevant for Cloud users. Trust models could be used to enhance trust.

Table 5 – Trust challenges of Cloud Computing [25]

Furthermore, the Cloud Security Alliance [28] has identified twelve critical issues to Cloud security, ranked in order of severity (see Table 6). This allows both consumers and providers of Cloud services to make better decisions about risk mitigation. The majority of these issues comprise a combination of human and technical problems (no's 1, 2, 5, 6, 8, 9, and 10).

CLOUD SECURITY ISSUE	DESCRIPTION
1. Data Breaches	Incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so.
2. Weak Identity, Credential and Access Management	Lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords, and certificates
3. Insecure UIs or APIs	Lack of authentication and access control or encryption and activity monitoring, in order to protect against both accidental and malicious attempts to circumvent policy.
4. System and Application Vulnerabilities	Exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations.

5. **Account Hijacking**	Attack methods such as phishing, fraud, and exploitation of software vulnerabilities
6. **Malicious Insiders**	A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems[10].
7. **Advanced Persistent Threats (APTs)**	A parasitical form of cyber-attack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property.
8. **Data Loss**	Data stored in the Cloud can be lost for a variety of reasons including software, hardware and human failures such as loss of encryption keys by consumers.
9. **Insufficient Due Diligence**	An organization that rushes to adopt Cloud technologies and choose Cloud Service Providers (CSPs) without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success.
10. **Abuse and Nefarious Use of Cloud Services**	Malicious actors may leverage Cloud Computing resources to target users, organizations, or other Cloud providers[11].
11. **Denial of Service**	Attacks meant to prevent users of a service from being able to access their data or applications.
12. **Shared Technology Issues**	Shared technology vulnerabilities can potentially be exploited in all delivery models of underlying components that comprise the infrastructure supporting Cloud service deployment. These may not have been designed to offer strong isolation properties for a multitenant architecture (IaaS), re-deployable platforms (PaaS) or multi-customer applications (SaaS).

Table 6 – Cloud Computing top threats [28]

The management of trust relationships represents a key challenge in order to meet security requirements [24] and mitigates threats, including those specified in Table 5 and Table 6. Furthermore, a number of security requirements need to be considered with respect to Cloud deployment models. Kalluri and Rao [25] provide a seven-step scheme (see Table 7), which needs to be considered from a Digital Trust perspective, when organizations want to adopt Cloud Computing solutions. This will help protect their businesses in Cloud environments.

[10] https://buildsecurityin.us-cert.gov/articles/best-practices/insider-threat

[11] Examples of misuse of Cloud service-based resources include launching DDoS attacks, e-mail spam and phishing campaigns; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting of malicious or pirated content [60].

STEP IN ADOPTING CLOUD-BASED SOLUTION	DESCRIPTION
1. **Strategically plan your Cloud security**	Considering security during the initial planning phase creates a solid foundation. Careful considerations must be taken as to how workloads will be delivered to end users.
2. **Select the Cloud provider**	Choose a Cloud provider which is able to protect sensitive and critical information. Check whether the Cloud service providers have experience in both IT and security services.
3. **Find the document about security measures provided by the Cloud provider**	Getting assurances from the Cloud provider written into the contract. The document must include applications, infrastructure, configurations, policies, rules, and regulations.
4. **Find out who will monitor your data**	Who will have access to data, why, when, and how.
5. **Have a plan for security issues**	What kind of responsibility is the Cloud provider offering, and what actions will they take during and after security issues.
6. **Verify access controls being used**	Verify access controls imposed on data to ensure that third parties cannot access the data. Define roles and responsibilities to ensure that even privileged users cannot circumvent auditing, monitoring, and testing, unless otherwise authorized.
7. **Monitoring system**	The Cloud provider must continuously monitor data, establish Cloud performance metrics and test regularly.

Table 7 – Steps in adopting a Cloud-based solution [25]

Many vendors are leveraging Cloud-based service models to deliver their solutions, including those for Security as a Service (SecaaS). The Cloud Security Alliance has categorized and described Security as a Service as part of a series of business, technical, and implementation guidance documents[12]. This allows organizations to create guidelines for implementing SecaaS offerings, facilitate SecaaS purchasing, and support those implementing or auditing SecaaS solutions. These security service categories are listed in Table 8.

[12] https://Cloudsecurityalliance.org/group/security-as-a-service/

SECAAS CATEGORY	DESCRIPTION
Network Security	Consists of security services that allocate network access, distribute, monitor, and protect network services.
Vulnerability Scanning	Scans the target infrastructure or systems for security vulnerabilities via a public network.
Web Security	Offers real-time protection of public-facing application services generally offered by proxying web traffic through the Cloud service provider.
E-Mail Security	Provides control over inbound and outbound e-mail, protecting the organization from phishing, malicious attachments, and spam, and providing business continuity options.
Identity and Access Management (IAM)	Provides identity administration, governance, and access controls. This includes authentication, identity assurance and enforcement, access intelligence, and privileged user management.
Encryption	The process of obfuscating data using cryptographic and numerical ciphers. Transforming clear-text into cipher-text to make it unreadable without the correct key.
Intrusion Management	The process of using pattern recognition to detect statistically unusual events, prevent, or detect intrusion attempts, and manage the incidents.
Data Loss Prevention (DLP)	Monitoring, protecting, and verifying the security of data at rest, in motion, and in use.
Security Information and Event Management (SIEM)	Log event information, correlation and incident data and provide real time analysis and correlation.
Business Continuity and Disaster Recovery (BCDR)	The implementation of measures designed to ensure operational resiliency in the event of any service interruptions.
Continuous Monitoring	Performs the function of continuous risk management presenting the current security posture of the organization.
Security Assessments	Third party audits of Cloud services based on industry standards.

Table 8 – Security as a Service categories [29]

When organizations procure these services and consider the requirements in these categories carefully, Digital Trust can be increased. Each security category is described, consisting of the core functionalities and technical elements, including related standards.

1.4 BIG DATA & ANALYTICS

Big Data Analytics is defined as *"technologies and techniques that a company can employ to analyze large-scale, complex data for various applications intended to augment firm performance in various dimensions"* [30].

1.4.1 BIG DATA CHARACTERISTICS

Big Data is a topic that has attracted a great deal of attention from industry, governments and academia in recent years. The term Big Data was coined in 1997 to refer to large volumes of scientific data for visualization [31]. Big Data are characterized by a collection of huge data sets (Volume), generated very rapidly (Velocity) and with a great diversity of data types (Variety). Such data is difficult to process by traditional data processing platforms, such as relational databases, and almost impossible to analyze with traditional techniques.

The three Vs (Volume, Velocity and Variety) were introduced in 2001 by Doug Laney from Metagroup. In those days, Laney did not use the term "Big Data", but he envisioned that accelerated generation of data with incompatible formats and structures as a result of e-commerce would push traditional data management principles to their limits [32]. Many others have added other Vs, but most of these do not relate to the data itself but to the result of analytics such as previewed value. IBM, has added a 4th V "Veracity" that specifically relates to the data itself [33], [34]. This additional V in combination with the original 3Vs will be used in this report to refer to the characteristics of Big Data which are depicted and described in Table 9 and Figure 5 respectively.

CHARACTERISTIC	DESCRIPTION
Volume	How much data: the amount of data that organizations try to harness to improve decision-making across the enterprise.
Velocity	How fast data is created: the speed of incoming data and how quickly it can be made available for analysis (e.g. payment data from credit cards and location data from mobile phones).
Variety	The various types of data: the different types of structured and unstructured data that an organization can collect, such as transaction-level data, text and log files and audio or video.
Veracity	How accurate the data is: the trust in the data which might be impaired by the data being uncertain, imprecise or inherently unpredictable (e.g. trustworthiness, origin, and reputation of the data source).

Table 9 – The four characteristics of Big Data

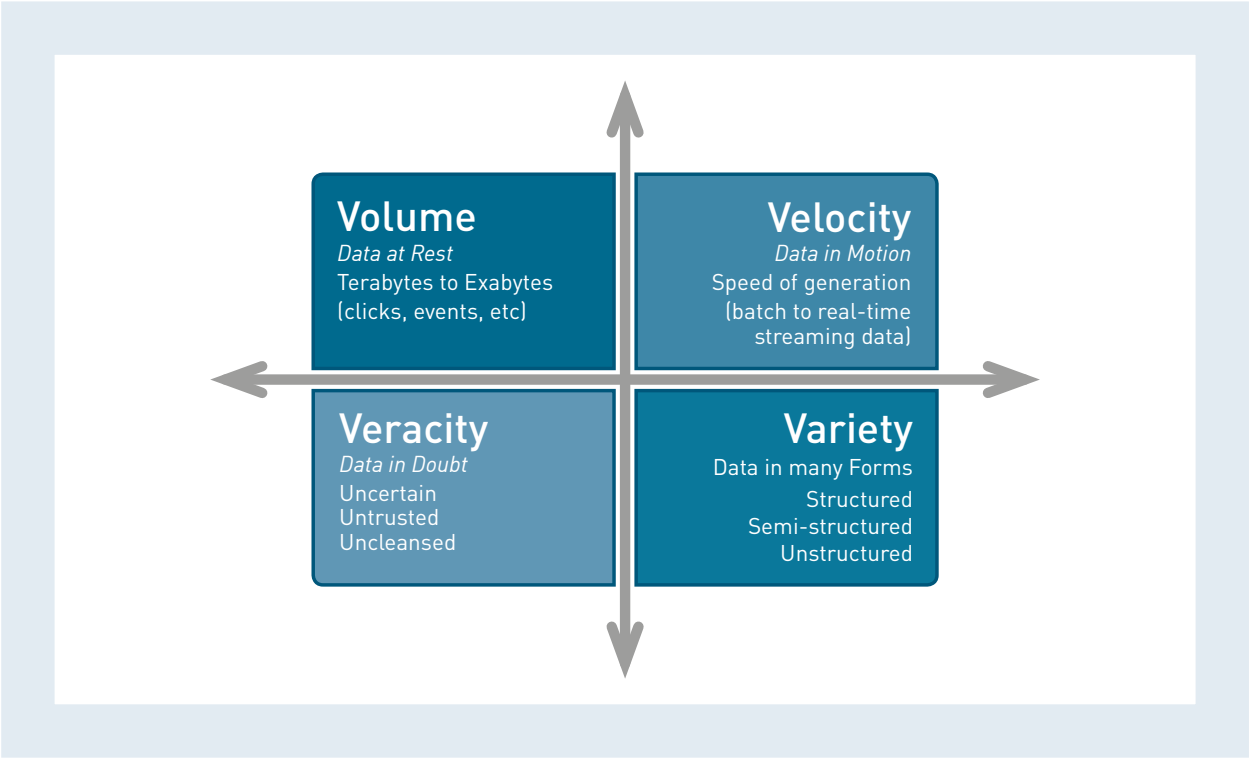


Figure 5 – The four Vs of Big Data

Big Data incorporates all kinds of data and from a content perspective one can make the distinction between structured data, semi-structured data and unstructured data [35]:

- **Structured data** – is part of a formal structure of data models associated with e.g. relational databases. It can be generated both by computer software or humans.
- **Semi-structured data** – not part of a formal structure of data models. It contains markers to separate semantic elements and enforce hierarchies of records and fields (example: XML).
- **Unstructured data** – does not belong to a pre-defined data model. Includes data from e-mails, video, social media websites, and text streams. Accounts for more than 80% of all data in organizations.

In practice mixed combinations of these three Big Data types occur which is referred to as **Poly-structured** data.

Big Data analytics, or in short Analytics, refers to techniques and technologies that are used to analyze the massive amount of data generated by both humans (e.g. in social media) and things (e.g. sensor networks), in order to acquire information from it. It is applicable to almost all areas of society, including administrative, commercial, and scientific fields, and affects individuals, business, governments, and their relationships. From the acquired information, one can provide new insights, such as "spot business trends, determine quality of research, prevent diseases, link legal citations, combat crime, and determine real-time roadway traffic conditions" [36].

Recent examples (of 2016) show the extent of data volumes generated every day in business:

- Per *second*:
  - 34,500 GB of Internet traffic
  - 53,900 Google searches
  - 121,400 YouTube videos viewed
  - 9,100 Tweets sent
  - 2,100 Skype calls
- Per *minute*: 500 hours of video uploaded to YouTube.
- Per *day*: Facebook creates 10 terabytes ($10x10^{12}$ bytes) of data; Google produces 24 terabytes of data from its search operations.

This massive increase of data can be explained by various trends in society [37], including:

- The diffusion and adoption of social network websites by individuals and businesses;
- The generation of large volumes of data by organizations to monitor user activities on websites;
- Internet of Things: billions of devices, such as sensors of mobile devices, security cameras, GPS tracking systems, etc. generate real-time streams;
- Applications in science experiments result in an increase of datasets at an exponential rate;
- Storage capacity is cheap – easier and less costly to buy storage rather than deciding what to delete;
- Analytics techniques have significantly improved, enabling acquisition of a higher degree of knowledge from data.

Some Big Data Analytics usage categories include [38]:

- Enhanced 360° customer view: extended customer views by incorporating additional internal and external information sources
- Exploration: find, visualize and understand to improve decision making
- Security/Intelligence extension: lower risk, detect fraud, and monitor cyber security in real-time
- Operations analysis: analyze a variety of machine data for improved business results
- Augmentation: integrate Big Data and traditional data for new services, e.g. augmented reality

Also the differences between traditional Business Intelligence (BI) and Analytics can be explained by the characteristics of data being generated. Where traditional BI relates to structured data from known sources with relatively small data sets used for Management Information, Big Data Analytics relates to data of all types, from often unknown sources and which has to be analyzed in real time.

More information on the subjects of Big Data and Analytics can be found in an earlier ILNAS White Paper on Big Data [39][13].

[13] http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/information-sensibilisation/white-paper-big-data/WP_BigData_v1.pdf

1.4.2 DIGITAL TRUST CHALLENGES AND SOCIETY'S DILEMMA

Today, Big Data technologies present a new set of privacy, security, ethical, and welfare concerns in diverse areas such as health, government, intelligence, and consumer data [40]. Consumers have expressed concerns about the lack of honesty among businesses and the potential misuse of personal information [41]. As Doug Laney puts it: *"Facebook's nearly one billion users have become the largest unpaid workforce in history"*[14], whereas Scott Goodson said about "free" services on the Internet that obviously also use Big Data: *"If You're Not Paying For It, You Become The Product"*[15].

Risks to privacy and anonymity through re-identification techniques arrive on the scene in areas such as social media, geo-locating of mobile devices, and medicine. Facebook "Likes" can be used to automatically and accurately predict a range of highly sensitive personal attributes such as sexual orientation, ethnicity, religious/political views, personality traits, intelligence, degree of happiness, addictive substance consumption, parental separation, age, gender, etc. [42]. Furthermore, retailers are assembling shopping profiles of individuals based on publicly available metadata from smartphones and data of social media posts. Medical data can not only reveal information regarding individuals but also information about genetics in family lines.

Kshetri [40] argues that Big Data capabilities of companies are likely to affect the welfare of technologically un-savvy consumers more negatively. This would be caused by this group of consumers lacking awareness of multiple information sources and thus being less likely to receive up-to-date and accurate information regarding multiple suppliers. He argues that social and ethical issues are pertinent due to underdeveloped regulations and regulatory infrastructure, which may result in consumer exploitation by businesses. This issue is augmented by a number of surveys that the author presents that show a large proportion of organizations lack preparedness to address security and privacy issues.

The fact that digital content is publicly available does not mean that anyone can do with it whatever they like. The monitoring of e-mail and mobile communications of numerous individuals is just another example. In other words, such issues raise significant legal and ethical problems and relate to individual privacy and the proper role of intellectual property protection [41]. This later work questions *relevance* (what counts and what does not?), *validity* (how meaningful are the findings?), *generalizability* (how far do the findings reach?), and *replicability* (can the results be reproduced?). They state that existing privacy and intellectual property laws may need to be adapted in order to accommodate Big Data practices. Therefore, governments are likely to be forced to recognize the necessity for adequate safeguards to protect the privacy of individuals and the development of higher privacy regulations [40].

There is also skepticism about the usefulness of social media data in academia. For example, data from Twitter is limited in terms of scale (spatial and temporal), scope, and quality. Boyd and Crawford [43] state: *"Twitter does not represent 'all people', and it is an error to assume 'people' and 'Twitter users' are synonymous: they are a very particular sub-set"*. The same goes for the Facebook community, which is still only a specific subset that tends to post only positive messages contributing to a biased view of society. And some even argue that given the enormous quantities of data, one will find statistically significant results based on data patterns that don't represent anything real in the general population [41].

[14] http://blogs.wsj.com/cio/2012/05/03/to-facebook-youre-worth-80-95/

[15] http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/#6599ba22b445

The Big Challenge with Big Data is to find a way of integrating these new methods and technologies into people's everyday lives, without making them more and more hesitant of using digital channels because some stakeholders are conducting mass-surveillance of private data. Big Data can be used for a vast range of commercial, public administration, and scientific purposes, but equally for highly dubious ends. As with all things, for every positive example there is also a worrying but equally realistic negative scenario [44].

1.5 LEADS FOR LEVERAGING DIGITAL TRUST

As Digital Trust is central to the customer relationship and directly linked to personal sentiment, consumers want to know their data resides in safe hands. Companies that will gain the highest consumer trust are best positioned to capitalize on business opportunities. Consequently, Digital Trust is a key building block to enable many new digital products and services. The concepts of trust and Digital Trust were investigated in detail in an earlier ILNAS White Paper [45][16] and, therefore, the reader is referred to Chapter 1 of that document for further information.

According to an Accenture survey of 24,000 consumers in 24 countries, a majority (54%) of those consumers are not confident in the security of their personal data being held by third parties. These consumers prefer to trust established brands in financial services, telecommunications, and consumer electronics such as smartphone and PC manufacturers [46]. No matter what, customers want and have to be constantly aware about how and where they share their personal data and thus companies have to take these wishes and this behavior into account to enable Digital Trust from them. Once a company has achieved Digital Trust with its consumers, they will provide the company more data. From that data, the company is able to create even more services, which establishes more loyalty and leads to even more Digital Trust as in a virtuous circle.

Although there are various ways to achieve Digital Trust, the latest ideas in industry [8], [46], [47] show a convergence of ideas that include information security, privacy, and risk management. Accenture [46] focuses on four key areas to build and maintain Digital Trust: accountability, security, privacy, and consumer benefit and value. To build Digital Trust, consumers need confidence in each of these areas.

1. **Accountability**: At all times, companies must be accountable for the protection of consumers' digital information. Companies should establish a transparent model that specifies what and how data is sourced and from whom. Monitoring what data is accessed, when and by whom is a critical aspect of maintaining trust. Furthermore, companies are accountable for misuse of and incorrect information about customers and they must promptly take corrective actions. Selecting the right business partners that enhance consumer trust is another vital ingredient to further increase customers' Digital Trust.
2. **Security**: Access control mechanisms should be more sophisticated and no longer be based on a username / password combination as more user-friendly and secure technologies are necessary to improve the user experience. Examples are biometric authentication methods using human finger prints, irises, and voice recognition to replace the numerous PIN or password-protected sources.
3. **Privacy:** User confidence in the security of personal information must be enhanced. Transparency and control are crucial elements to meet consumer privacy needs. They require the ability to opt in (instead of to opt out) for activities related to sharing information, ads, recommendations and offers based on location. If consumers do not recall giving their permission, they will probably consider this as a privacy violation. For companies to build Digital Trust, they have to create guidelines on data used to administer these activities and communicate this to consumers. This allows users to have at least some control over who uses their personal information and how.

[16] http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/information-sensibilisation/white-paper-green-computing/white-paper-green-computing.pdf

4 **Consumer benefit and value**: Two-thirds of all consumers worldwide are willing to share their personal information in exchange for some perceived value, such as discounts or services that they value. However, companies must offer real value in exchange for personal information that the consumers provide and the data in question are clearly necessary to the services that are provided. At the same time, both consumers and companies must treat the exchange of consumers' personal information as a monetary transaction. This will ease the struggle between privacy on the one hand, and providing tailored services for each consumer's specific interest on the other.

PWC [47] takes a more technical approach and focuses on five key areas for building and maintaining Digital Trust.

1 **Security**: Organizations must have confidence that their information systems are properly secured to ensure the protection of customer data and that identity and privacy issues are dealt with. This requires a good understanding of the organization's risk profile and real-time monitoring of the risks the organization is exposed to.

2 **Data quality**: Adequate data management is vital to have confidence in organizations' data, and is fundamental to creating Digital Trust with both customers and suppliers.

3 **Information systems**: These systems are properly configured and monitored to ensure they do exactly what they are supposed to do. This holds true for in-house systems as well as Cloud-based services. Activities that underpin Digital Trust relate to process adherence, performance management and compliance.

4 **Risk management**: Technological risks are well-managed and information systems are available when required by proactive identification, assessment, and monitoring. In case of incidents, the organization is able to respond quickly to mitigate high impact events.

5 **Technology-driven transformation programs**: Besides ensuring that such programs deliver the expected benefits on time and to budget, the organizations' stakeholders (including the clients) recognize the organization's commitment to innovating its business. There must be confidence that such endeavors maximize the value from investments in Digital Trust.

Of course the above activities are necessary for any development in the digital age, but more particularly for the advanced smart technologies that are discussed in this chapter: Internet of Things, Cloud Computing and Big Data & Analytics, as their implications go beyond of that of traditional IT technologies.

Digital Trust is thus a requirement for the global adoption of any Smart technology. To better understand **why** Digital Trust is necessary for the development of Smart technologies, Chapter 2 will detail the challenges and prospects of Digital Trust from an economic point of view. Then in Chapter 3 and Chapter 4, technical approaches and current standardization work will be examined to show **how** Digital Trust can be attained to support these Smart technologies.

2 DIGITAL TRUST FOR SMART ICT: ECONOMIC CHALLENGES AND PROSPECTS

This chapter first presents the economic analysis and prospects of Digital Trust, then the economic challenges of Digital Trust, in particular for the three following smart technologies: IoT, Cloud Computing and Big Data and Analytics.

2.1 ECONOMIC ANALYSIS AND PROSPECTS

The availability of new digital technologies and techniques and the ever-growing amount of data being generated 24/7 creates new opportunities for individuals and compelling economic prospects for businesses. In addition, a combination of the recognition of organizations of the need to treat data as an asset and the urge to monetize these opportunities, signifies a change towards a data-centric socio-economic model [13].

2.1.1 INTERNET OF THINGS

There are not many studies that address the IoT's wider (economic, social and political) impacts [48] and the economic implications of IoT warrants future research [13]. Two governmental studies deal with imminent challenges. In 2013, the European Commission published a study [49] focusing on IoT governance mechanisms. This report identified many issues for IoT governance related to security, privacy, ethics, and competition. In 2015, the US Federal Trade Commission also published a report [50] that acknowledges the many risks related to the deployment of IoT-based applications, again with issues related to security and privacy.

Many developments of IoT relate directly to the security and privacy rights of individuals:

1. Smartphones with their many sensors (capturing whereabouts and activity);
2. Wearables (technological gadgets such as sports gear and navigation tools);
3. Automotive (register drivers' behaviors and whereabouts);
4. Domotics (home automation, such as smart meters and security cameras);
5. Quantified self (recording aspects of a person's everyday life, e.g. food and mood).

Smartphones in particular provide an easy, ever-present interface through which people can interact with other connected devices and objects and these devices can be seen as the hub to the Internet of Things [13]. Services are offered in numerous mobile applications such as online maps, navigation, and recommendations for pubs or local businesses. Figure 6 shows the percentage of smartphone users who use the Internet in a number of European countries. Although smartphones are currently the most important source of data, data are increasingly being generated by other smart devices as part of Machine-to-Machine communication (M2M). Additional value can be created when consumer IoT systems are linked to business-to-business (B2B) systems. It is even claimed that IoT use in B2B applications will have greater economic potential than its consumer equivalent [51].

All this data from the IoT allow certain organizations to perform unprecedented analysis of individuals. In addition to privacy risks, physical security risks can also be identified. For instance, attackers may find vulnerabilities enabling them to undermine traffic control that is being managed in smart cities or even manipulate patients' medical devices or the automatic supply of doses of medicine. Attacks on IoT devices

may thus lead to physical damage or even threaten human life [52], in particular in industrial applications or cyber-physical systems.

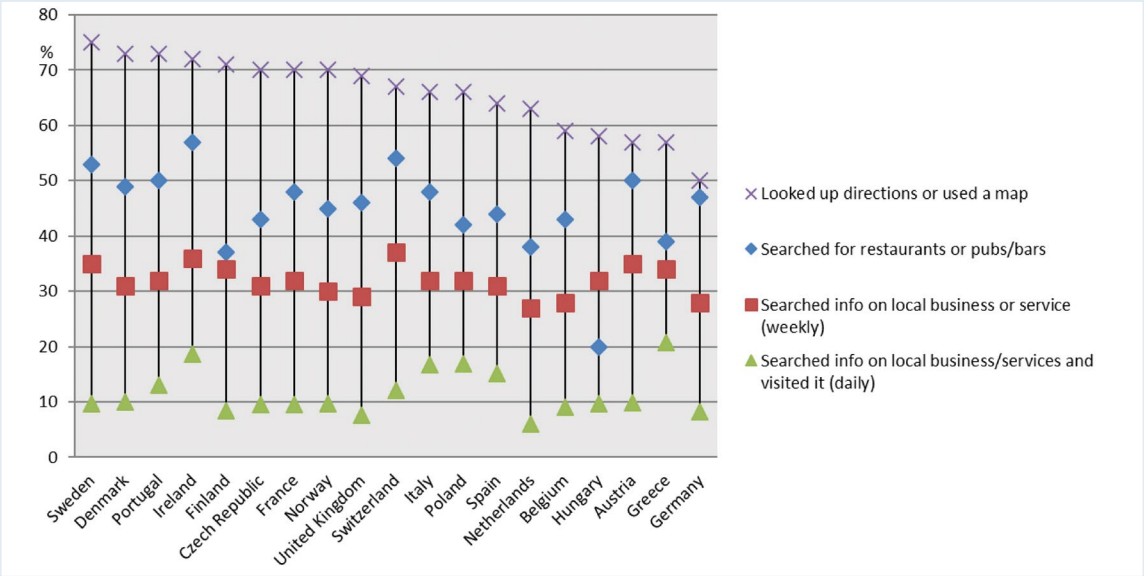


Figure 6 – Use of location-based services on smartphones [13]

One way of measuring the penetration of IoT in our society is to look at the number of SIM cards allocated to M2M communication devices on mobile networks, which is depicted in Figure 7 for a number of European countries.

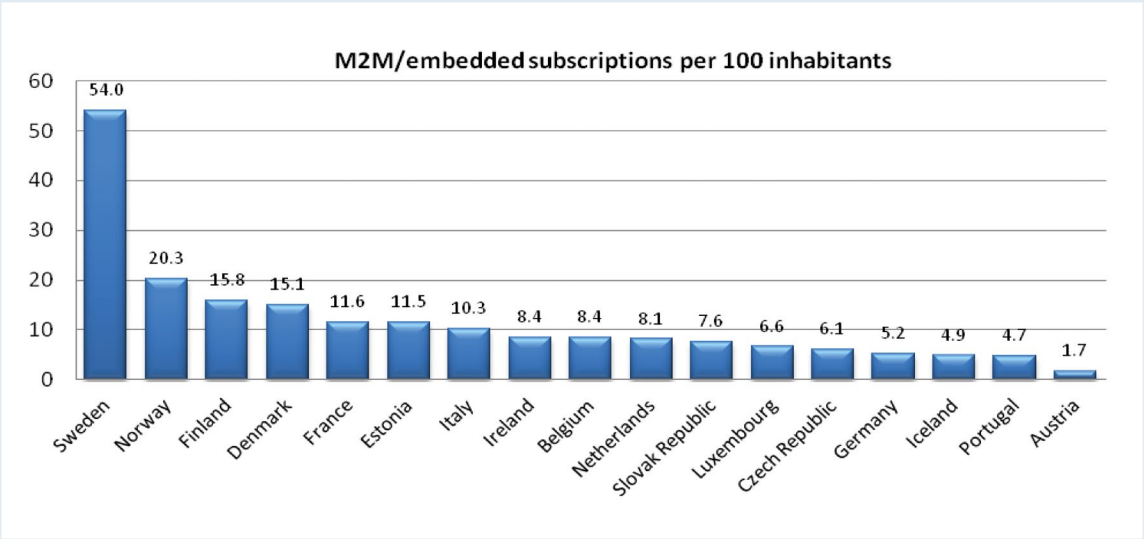


Figure 7 – Number of M2M/embedded mobile cellular subscriptions [13][17].

[17] Although Sweden leads based on number of devices, it is possible that not all these devices are located in Sweden.

The rapid developments in IoT, and the combination of this technology with Cloud and Big Data lead to various "smart" applications. Examples include: remote patient monitoring, energy consumption control, traffic control, smart parking systems, inventory management, production chain, customization of supermarket shopping, civil protection, etc. [3]. Many of these IoT applications will be concentrated in cities and will be useful for urban life, governance, and the management of municipal services and urban infrastructures.

These various IoT applications can be grouped into three major areas: 1) Smart City, 2) Industry, and 3) Healthcare and Well-being [12]. The overall objective of these applications is to enhance the quality of our everyday life, and this will have a profound impact on the economy and society as a whole. The current trend is for industry to focus its efforts on the area of Smart Cities. In the following section, the latest developments in these three areas are analyzed.

2.1.1.1 SMART CITIES

The IoT is envisioned to be instrumental in increasing the environmental sustainability of our cities and to enhance people's quality of life. A smart city is an urban development vision that integrates ICT in general and IoT in particular to manage the resources of urban environments and provide customer friendly services. Resources include energy, gas, and water whereas the main services relate to commercial and private buildings, transportation, public safety, and health but also the environment in general.

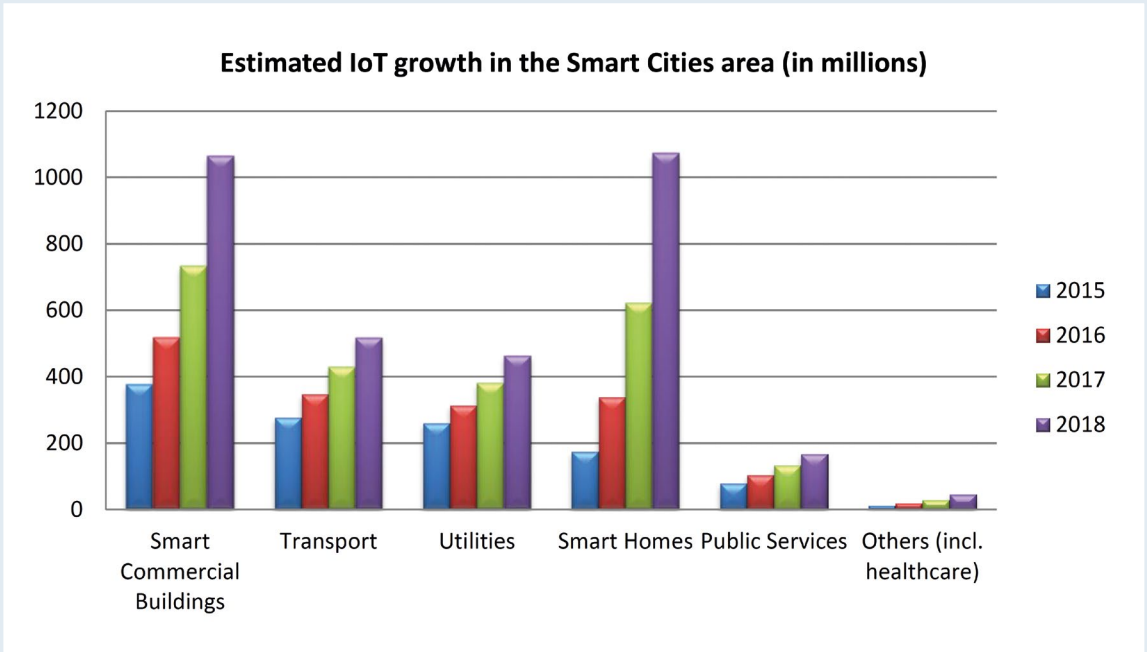


Figure 8 – Connected Things installed base within the area of Smart Cities [53]

Gartner [53] estimates that 1.6 billion connected things will be used by smart cities in 2016, an increase from 2015 of 39% (see Figure 8). These devices will be particularly useful and involved in the following smart city areas and services:

- **Smart commercial buildings** are buildings that provide services to ensure occupant productivity at the lowest cost and environmental impact over the building lifecycle. This includes, but is not limited to air quality (e.g. illumination, thermal comfort, physical security, and sanitation).
- **Transport** includes IoT-based systems for managing traffic flow (automated adaptive traffic control) and self-driving cars.
- **Utilities** relate to smart resource management of electricity, gas, water, and sewerage.
- **Smart homes** are residences equipped with IoT technology to enable occupants to control or program an array of automated home electronic devices and services (for heating, water, security, etc.) anywhere, anytime.
- **Public services** relate predominantly to health and safety and include environmental monitoring. Examples are air and water quality improvements that should increase wellness and reduce illness among citizens.

Smart commercial real estate will probably account for most IoT use until 2017, after which smart homes will take over with around 1 billion connected things in 2018.

SMART COMMERCIAL BUILDINGS

The objective of smart (commercial) buildings is to make commercial real estate more energy-efficient by means of improved control of power consumption and innovative technologies to produce energy and reduce resource consumption. With IoT technologies, this will result in automated buildings where all services are connected and managed through the Internet (e.g. access control, elevators, fire detection, heating, ventilation, and air conditioning).

Smart commercial buildings are offices in which facilities are made available to easily accommodate mobile staff, e.g. augmented reality for teleconferencing. Another example are retail premises such as stores, restaurants, and banks, that are equipped with inventory optimization and advanced self-service facilities (personalized in-store offers, shopping route optimization and automated checkout).

Commercial buildings will benefit from IoT applications as they allow a unified view of facilities management and service operations to be generated through the collection of data and insights from a multitude of sensors. This includes increased energy efficiency and user-centric service environments such as security cameras. *"Especially in large sites such as industrial zones, office parks, shopping malls, airports or seaports, IoT can help reduce the cost of energy, spatial management, and building maintenance by up to 30%"* [53].

Smart commercial buildings are also important from a social responsibility perspective. 96% of staff within the 18-45 age range value sustainability and demand green workplaces. They expect their employer and workplaces to be environmentally friendly or at least environmentally aware [54].

TRANSPORT

The objective of Smart mobility (transport) is to increase the environmental sustainability of cities and citizens' quality of life by controlling and optimizing traffic on roads and public transport. IoT-enabled smart mobility can help everyone reach their destinations faster, more cheaply and more safely, and includes real-time information on traffic conditions, intelligent lighting, and other IT-enabled solutions.

It is facilitated through an intelligent infrastructure, mobile sensors directly attached to vehicles, and location-based apps on car drivers' smartphones. It makes transport more sustainable and efficient, for example by minimizing traffic signal stops, finding optimal routes to avoid traffic jams, and advising on the optimal driving speed to avoid congestion. In addition, it contributes to safety through e.g. forward collision alert and lane-departure warning systems. Smart parking systems guide drivers to the nearest available car park based on drivers' preferences and location. In public transport, delays and alternate routes are available in real-time to minimize the commuting time in public transport services, which should increase public transport attractiveness.

Important ingredients of the intelligent infrastructure are road toll collection systems and public transport/ticket payment systems that are installed in many countries based on RFID technology. These systems are activated when users drive through a toll gate or swipe their RFID-based public transport cards in front of a reader that is connected with the Internet. The drawbacks of these systems are their inflexibility, whereas systems that use wireless networks and GPS operate in any location and do not require physical infrastructure. However, implementation of these more advanced technologies has proven to be more challenging than expected in the countries that have tried [13]. The main reasons are issues relating to technology, costs, and more particularly to privacy. Thus, in the context of smart cities, Digital Trust is an essential condition of securing wider acceptance of smart mobility among consumers. In the future, more advanced applications are expected that provide innovative services relating to the integration of different modes of transport and traffic management of automated vehicles.

UTILITIES

IoT and public utilities relate to smart resource management of electricity, gas, water, and sewerage. Currently, most development work is being carried out and investment made in the Smart Grid, which is a modernized version of utility electricity delivery that gathers and acts automatically on information flows. It is defined by Ancillotti *et al.* in [55] as *"an intelligent electrical distribution system that delivers energy flows from producers to consumers in a bidirectional way"*. The data relates to energy production and consumption behavior of both producers and consumers. It involves a variety of technologies such as smart meters, smart appliances, renewable energy resources, and energy efficiency resources. In a Smart Grid the producers can also be the final customers.

It is also aimed at improving the efficiency, reliability, and sustainability of the production and distribution of electricity by load balancing and peak load management. In addition, it allows more efficient use of existing infrastructures for electrical generation, transmission, and distribution. Because of improved grid flexibility, it permits greater penetration of variable renewable energy sources such as solar power and wind power, even without the addition of energy storage. It makes use of real-time two-way digital communication between devices connected to the grid. By using Smart Meters, smart control devices and smart appliances, the expected energy demands can be predicted. As a result, peak loads can be smoothed, minimizing the possibilities of blackouts.

In addition, Smart Meters will increase consumers' awareness of their energy consumption, which gives them the opportunity to reduce it. A Smart Meter records resource consumption (electricity, gas, etc.) and sends data to the public utility, for e.g. monitoring and billing purposes, or to provide information about resource consumption. It is also a necessary component in setting real-time energy, gas, and water prices for consumers. But here too, the privacy issue is highlighted, and Digital Trust in these devices and services is paramount. Therefore, the collection, analysis, and sharing of consumer data on resource usage must balance their privacy and security considerations. Furthermore, data from Smart Meters can be leaked and reveal customer habits, e.g. their working hours and times when no one is at home. In future, the Smart Grid

will run by itself by collecting data with smart devices, seamlessly handling alternative electricity sources, integrating electric vehicles into the grid, conducting Big Data Analytics, and acting on a continuous stream of these data.

Similar to energy, the cost-efficient production and distribution of clean water in urban areas is a continuing challenge. IoT devices, such as Smart Meters and smart sensors, can be tapped for smarter water management and the role of such devices in water management is highlighted in Table 10.

Mapping of Water Resources and Weather Forecasting • Remote sensing from satellites • In-situ terrestrial sensing systems • Geographical Information Systems • Sensor networks and Internet	**Asset Management for the Water Distribution Network** • Buried asset identification and electronic tagging • Smart pipes • Just in time repairs • Real time risk assessment
Setting up Early Warning Systems and Meeting Water Demand in Cities of the Future • Rain/Storm water harvesting • Flood management • Managed aquifer recharge • Smart metering • Process Knowledge Systems	**Just in Time Irrigation in Agriculture and Landscaping** • Geographical Information Systems • Sensor networks and Internet

Table 10 – Major areas for IoT in Water Management [56]

SMART HOMES

Smart homes are residences integrated with an eco-system of devices, household appliances, and sub-systems[18] all interconnected and interacting, which can be controlled remotely via web applications. This integration gives rise to a wide range of applications in and around the home. Based on an analysis of various information flows, the smart home system can calculate the time when a person will arrive home, hence unlocking the garage door, turning up the heat, switching on the radio and making a cappuccino.

Modeling behavior of inhabitants by tracking their mobile phones and other location-aware devices, may be beneficial for lower energy usage in the home [57]. However, these technologies raise the same issues as regards privacy and security.

The other main challenge today is to facilitate communication between the myriad of heterogeneous devices and applications running on them. However, as these devices evolve, consumers in smart homes will benefit from IoT applications by means of a maturing ecosystem (through e.g. interface standardization) of home appliances, infotainment, and home sensors, including kitchen appliances, gardening systems, and home security systems.

[18] Smart devices: e.g. broadband gateways, mobiles, phones, laptops, PCs, smart TVs and set-top boxes, speakers, appliances, plugs, surveillance cameras, lights, window shades, thermostats, and meters; household appliances: e.g. refrigerators, espresso machines, washing machines, dryers, dishwashers, and self-guiding vacuum cleaners.

PUBLIC SAFETY AND ENVIRONMENTAL MONITORING

Public safety objectives include the protection of citizens, safeguarding of public and private properties, maintenance of public order, and management of natural or man-made disasters. Data collected by fixed cameras located within commercial and residential areas and on highways can be used for advanced video surveillance. Dedicated sensors, smart cameras, GPS, and wireless technologies can provide real-time localization and tracking. For example, they can be used to get a complete picture of a rally attended by around 1,000,000 people and establish a dynamic emergency plan, pinpoint riots, or coordinate rescue operations. In environmental monitoring, connected smart sensors aid in detecting forest fires, measuring toxic emissions from factories, or oil spills on shores. Another example is a smart city system to reduce the amount of water lost through leakage in a large town [58].

2.1.1.2 INDUSTRY

The industrial aspect of IoT application relates to a number of appliances, notably industrial processes, logistics and supply chain management, and agriculture and breeding [12]. These appliances are also known as Smart Manufacturing, Smart Logistics and Smart Agriculture.

SMART MANUFACTURING

Smart Manufacturing in industrial processes creates a number of advantages. A key ingredient is real-time diagnostics. Process and product improvements can be achieved based on such data. Data is analyzed in real time and results are fed back into the manufacturing process. Products and processes are inextricably linked to "their" data. But there is more, as Bosch's CEO describes: *"The next big step will be to think through the interdependencies among the machine, the production components, the manufacturing environment, and the IT that connects it all, so that the production technology controlling the machines merges with the technical data of the components. This requires a high degree of standardization so that the machine knows what it needs to do to any given component, and the components can confirm that the machine has done it. Such IT linkage goes far beyond current manufacturing systems."*[19]

Smart Manufacturing can also be applied to increase the sustainability of product manufacturing. For example, industrial processes based on IoT technologies allow monitoring of high-risk industries (e.g. chemical plants) to minimize emissions of toxic gasses. Sustainable manufacturing is defined by the US Department of Commerce as *"the creation of manufactured products that use processes that minimize negative environmental impacts, conserve energy and natural resources, are safe for employees, communities, and consumers and are economically sound"*. The application of IoT to conventional industrial processes makes them:

1. more flexible and resource-efficient;
2. more responsive to individual customer needs;
3. fully optimized in the use of direct material inputs as well as energy and water use.

Applying IoT in manufacturing creates competitive advantage, especially for start-ups and small and medium-sized enterprises (SMEs). Such companies have more flexible business models and are less reliant on established ways of working [54].

[19] Heinz Derenbach, CEO of Bosch Software Innovations GmbH, in Löffler and Tschiesner (2013).

There are important financial and reputational advantages of applying Smart Manufacturing. Retailers are increasingly demanding that their suppliers respond to their customers' wishes regarding the environment and sustainability. And an environmentally friendly reputation increases companies' financial value as those companies with a visible reputation for environmental responsibility are rated higher than others. And in the same way, poor performance can be a serious risk [54].

SMART LOGISTICS

The aim of Smart Logistics is to make transport more efficient and effective by means of IoT technology, thus lowering costs and improving profit margins for manufacturers, logistic service providers, and retailers. It includes simplifying warehouse and retail inventory by providing accurate knowledge of current inventory, while reducing inventory inaccuracies and tracking and tracing objects throughout their entire lifecycle. With route optimization systems, logistics service companies can increase their operational efficiency and planning whilst reducing redundancies, empty runs and outages. With Big Data Analytics, Telematics and sensor technology this allows logistics service providers to increase both the flexibility and the efficiency of intermodal freight (road, rail, air, marine, and inland waterways). By connecting vehicles, products and load units, improving route and load optimization, and reducing the amount of waste in the system, logistics also becomes more sustainable. In other words, the freight industry is optimized, resulting in shorter distances covered in transportation, better capacity management and lower fuel consumption.

Typical IoT applications in this area are RFID chips that are attached to objects and used to identify materials and goods. With these chips, it is possible to transmit and record physical (supply chain) event data concerning "what, where, when and why" such as received or shipped times, picked & packed locations, condition of goods during shipment, and availability of goods at specific locations. This enables tracking and tracing of items' location and status to be easily supported, even allowing for individual rerouting during a particular journey.

In the near future, IoT-enabled solutions will further optimize logistics through supply chain visibility[20]. As a result of this development, the role of Trusted Third Parties (TTPs) in supply chain management is becoming more and more relevant. A TTP allows the pooling of logistic flows of various logistic service providers and executes the distribution mechanism of costs and revenues. Such a party is essential to gain Digital Trust and developments in this area are in their initial stages. The EU Core project[21] touches on this area but primarily focuses on controlled global visibility of supply chain security risks.

SMART AGRICULTURE

Smart Agriculture makes farming more efficient through techniques such as geographic mapping, sensors, machine-to-machine connectivity, data analytics and other smart information platforms. With IoT applied to agriculture, food production will be more efficient by saving energy and water, using fewer resources (e.g. fermentation and manure management) and reducing waste. And the productivity of the farmer and crop yield will increase due to more efficient use of agricultural measures, such as, rice cultivation and fertilizers.

[20] Supply chain visibility is the ability to provide decision-makers in the supply chain with the required information, for example the what, when, where, and why of assets in the supply chain.

[21] http://www.coreproject.eu/

An extensive range of applications are available including:

- controlling agricultural production and feed with drones;
- identification of infected crops or animals to avoid the spread of contagious diseases through exact traceability;
- globally accessible data on animals such as demographics, the record of descent of an animal (pedigree), vaccines performed, veterinary checks and contracted diseases;
- real-time transmission of data about the animal's health (e.g. body temperatures for optimal breeding).

Important requirements for further developments in this area are comprehensive access to high-speed Internet on a global scale and affordable smart devices for everyone.

2.1.1.3 HEALTHCARE AND WELL-BEING

IoT can also play an essential role in the development of products and services in the area of healthcare and well-being, such as remote health monitoring of chronically ill people or improving people's social engagement.

In the field of healthcare, high expectations are made of devices, either attached to or inside the human body, that allow remote monitoring of patients at home or work. These include interconnected devices (wearable and ingestible) that allow medical staff to constantly monitor patients at home for diagnosis and control of patients' health. These devices monitor the patients' vital signs in real time[22] [59]. For patients with chronic conditions such as diabetes, these devices can improve subjects' compliance with prescribed therapies and avoid hospitalizations or post-hospitalization complications. Other applications relate to the identification of medical instrumentation and materials that keep track of objects in order to prevent such tools being left inside a patient after an operation [12]. Unfortunately, only few such devices are certified, which appears to be related to difficulties in implementation [13].

In the field of well-being, IoT may also provide benefits for improving people's quality of life. Examples are devices connected with apps running on smartphones that provide lifestyle improvement suggestions. These tools capture peoples' habits and provide them with current figures such as the number of kilometers walked, the corresponding calories burned and the recommended calories. Other applications allow specific categories of people such as elderly or disabled people to live independently. By monitoring real-time data for these people and accompanying optional remote medical consultations, this allows them to stay healthier and more active in society [12].

2.1.2 CLOUD COMPUTING

In terms of an economic analysis, Cloud Computing is disrupting not only the traditional hardware and software vendors but also many other industries. It is rapidly becoming the back-end for many forms of computing, including Big Data Analytics, Internet of Things and mobile applications. Diffusion of Cloud Computing among firms has accelerated in recent years. In 2014, over 22% of businesses used Cloud Computing services. In most countries, adoption is higher among large businesses (nearly 40%) compared to medium-sized or small firms (around 27% and 21%, respectively) (see Figure 9).

[22] Body temperature, blood pressure, heart rate, oxygen saturation, and respiratory rate

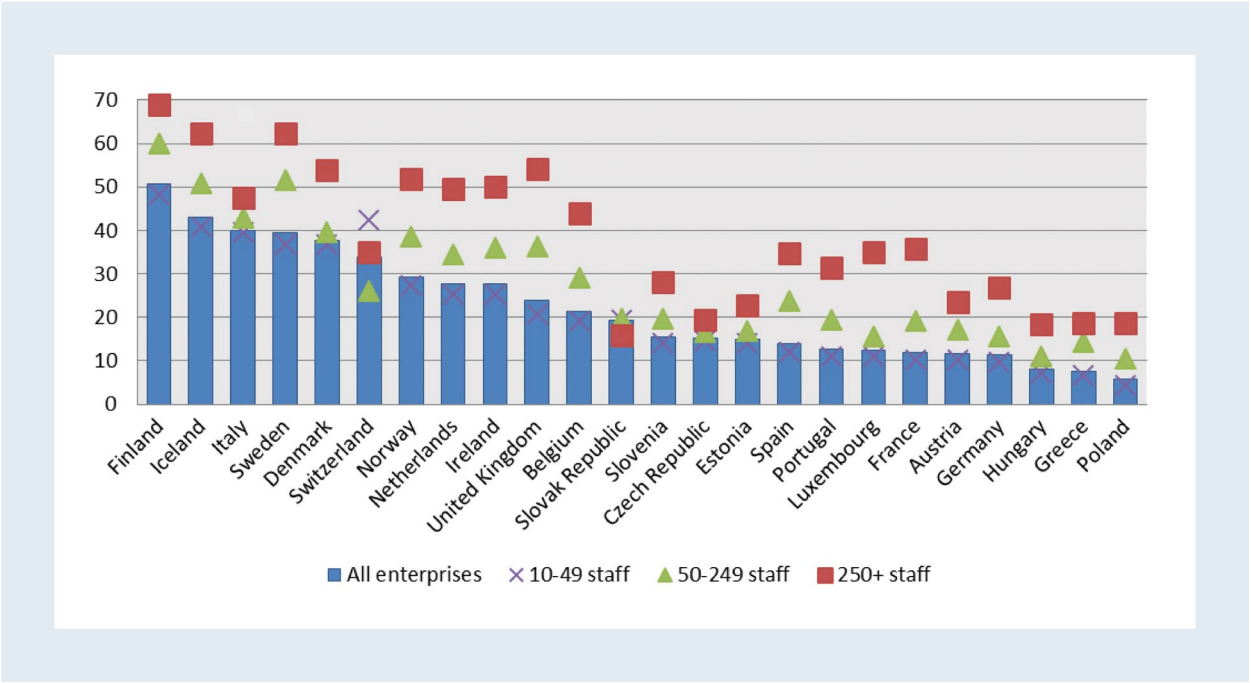


Figure 9 – Enterprises using Cloud Computing services by size [13]

Businesses have recently tended to invest more frequently in Cloud Computing services with a higher level of sophistication such as Customer Relationship Management (CRM) software, Human Resource Management (HRM) and accounting/finance software, than less sophisticated services such as office software, e-mails, or file storage. Furthermore, [13] also noted that in Austria, Iceland, the Netherlands and Norway, a large majority of businesses buying Cloud Computing services did not recognize a significant drop in IT costs. Factors preventing businesses from adopting Cloud Computing services relate primarily to the perceived risk of security breaches. Typically, large firms are doubtful about the location of the data centers, while small firms point to a lack of sufficient Cloud Computing knowledge [13].

There has also been a major increase in the use of Cloud Computing services among Internet users, such as file storage for documents, pictures, music, and videos. This facilitates ease of access and sharing with others, irrespective of location, time or device [13]. In 2014, growth of Cloud Computing adoption among Internet users in European countries ranged from 13% in Poland to 46% in Denmark. Furthermore, the uptake of computing services is much higher among young people (see Figure 10).

Nevertheless, as businesses, consumers and governments are adopting Cloud Computing at an increasing pace, the stakes could not be higher in terms of gaining and retaining Digital Trust as soon as possible. Indeed, Cloud Computing still represents a relative small proportion of overall IT spending [60]. Failure to address the Digital Trust challenge in Cloud Computing will probably result in less than optimal utilization of both economic and sustainability potential.

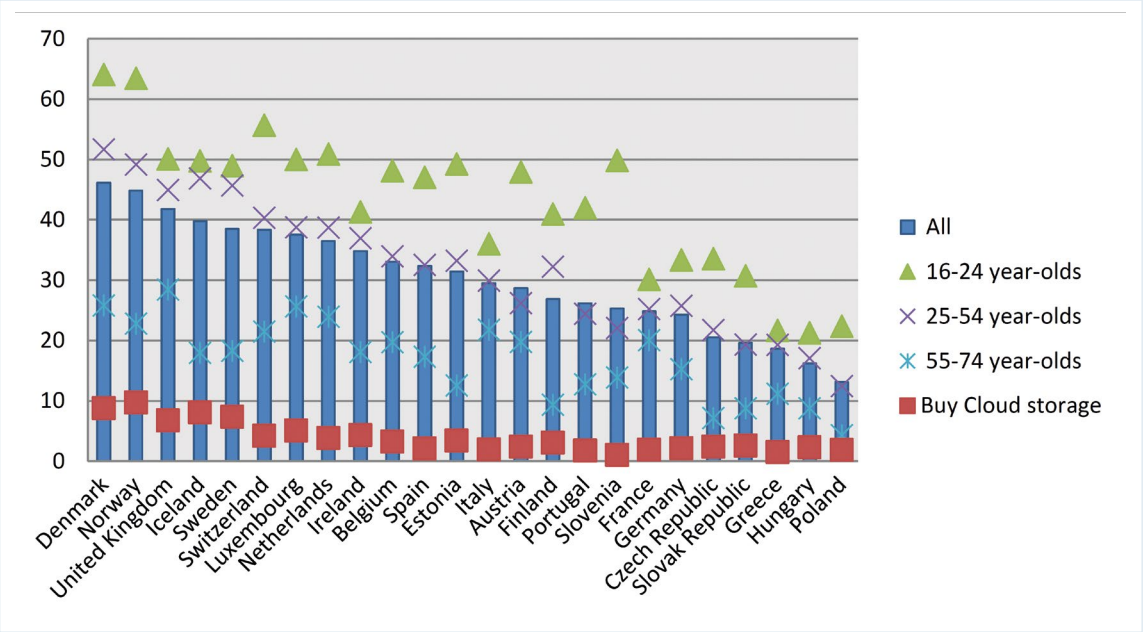


Figure 10 – Use of Cloud Computing by individuals by age class [13]

The Public Cloud adoption figures for 2016 are shown in Figure 11. Compared to the previous year, public Cloud adoption expanded across all Clouds [61]. Amazon Web Services still leads in the public Cloud adoption arena, with the largest percentage of reported running applications. However, Microsoft Azure has gained further ground with the largest percentage of organizations experimenting with its public Cloud infrastructure (IaaS and PaaS). It should be noted that because most organizations are using more than one Cloud service provider, totals add up to more than 100%.

Looking at IaaS and PaaS implementations, differentiated by company size, a similar picture emerges (see Table 11). The top 3 is the same for Enterprises and SMBs, with Amazon Web services in first place across both segments, followed by Azure IaaS and Azure PaaS. The remaining rankings, however, show significant differences. In Enterprises, VMware vCloud Air is ranked 4th and IBM SoftLayer is in fifth place. In the SMB segment, Google AppEngine is 4th followed by DigitalOcean in fifth place.

Also private Cloud adoption grows across all providers [61]. For all sizes of organization, 44% use vSphere environments as private Clouds (see Figure 12). Comparing enterprises and SMBs, VMware vSphere/vCenter is in the top position for both segments (see Table 11). VMware vCloud Suite and Microsoft System Center are placed 2nd and 3rd in the next ranking for enterprises, while OpenStack and Bare-Metal Clouds take the same positions for SMBs. Because most organizations run more than one Private Cloud implementation, totals also add up to more than 100% in this graph.

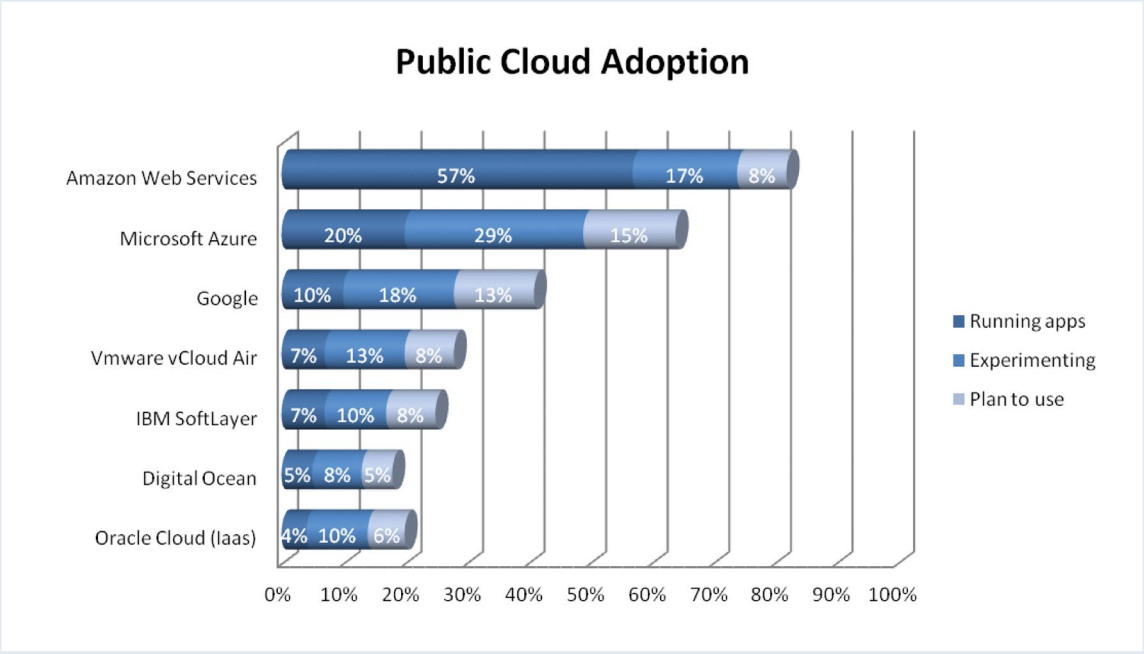


Figure 11 – Adoption of Public Clouds [61]

NO.	ENTERPRISE (1000+ EMPLOYEES)	SMB (LESS THAN 1000 EMPLOYEES)
1	Amazon Web Services	Amazon Web Services
2	Microsoft Azure IaaS	Microsoft Azure IaaS
3	Microsoft Azure PaaS	Microsoft Azure PaaS
4	Vmware vCloud Air	Google App Engine (PaaS)
5	IBM SoftLayer	DigitalOcean
6	Google App Engine (PaaS)	IBM SoftLayer
7	Oracle Cloud (IaaS)	Google IaaS
8	Google IaaS	Vmware vCloud Air
9	DigitalOcean	Oracle Cloud (IaaS)

Table 11 – Top Public Clouds Used [61]

Enterprise workloads are increasingly shifting to Cloud, especially private Cloud. 17% of enterprises have more than 1,000 Virtual Machines in the public Cloud (up from 13% in 2015). And private Cloud showed even stronger growth with 31% of enterprises running more than 1,000 Virtual Machines (up from 22% in 2015).

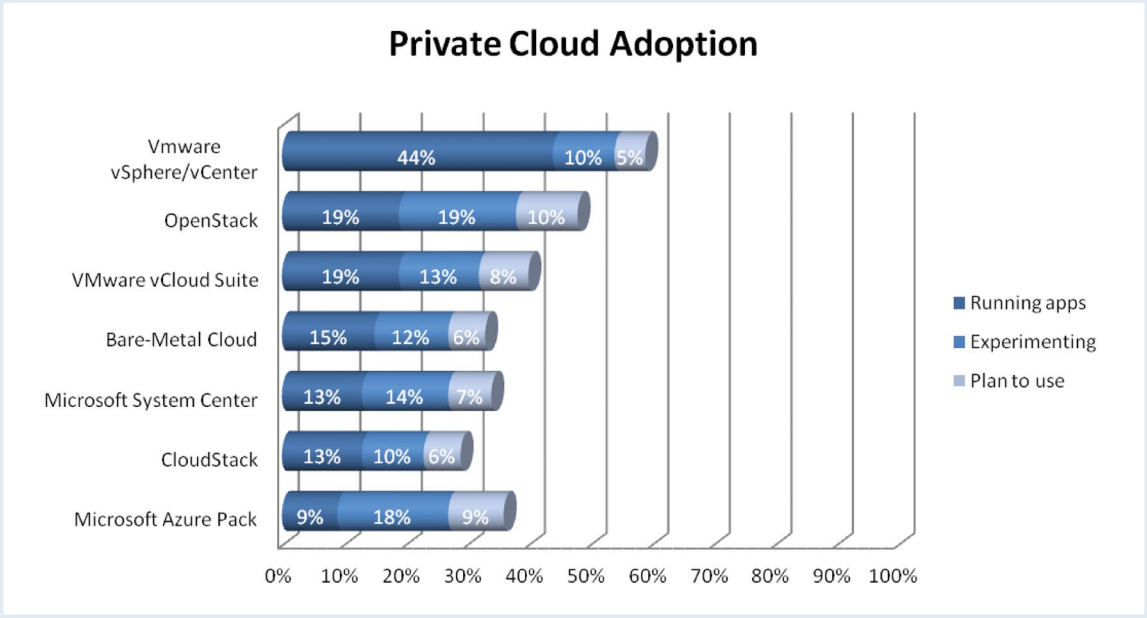


Figure 12 – Adoption of Private Clouds [61]

NO.	ENTERPRISE (1000+ EMPLOYEES)	SMB (LESS THAN 1000 EMPLOYEES)
1	Vmware vSphere/vCenter	Vmware vSphere/vCenter
2	VMware vCloud Suite	OpenStack
3	Microsoft System Center	Bare-Metal Cloud
4	OpenStack	CloudStack
5	Bare-Metal Cloud	VMware vCloud Suite
6	Microsoft Azure Pack	Microsoft System Center
7	CloudStack	Microsoft Azure Pack

Table 12 – Top Private Clouds used [61]

Several studies show there could be one million unfilled cyber security jobs in the near future[23]. A lack of qualified applicants is the primary reason for this gap. Or, as the Cloud Security Alliance put it: *"We need to focus on generating more qualified professionals in the information security field and improving the skillsets of the existing professionals in particular around Cloud technologies"* [60]. Since Cloud Computing is maturing, so has the role of staff involved in the technical architectures for Cloud Computing (see Figure 13). The role of Cloud architect has emerged as indicated by 40 percent of respondents who identify themselves as Cloud architects [61].

[23] http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#12ebde147d27

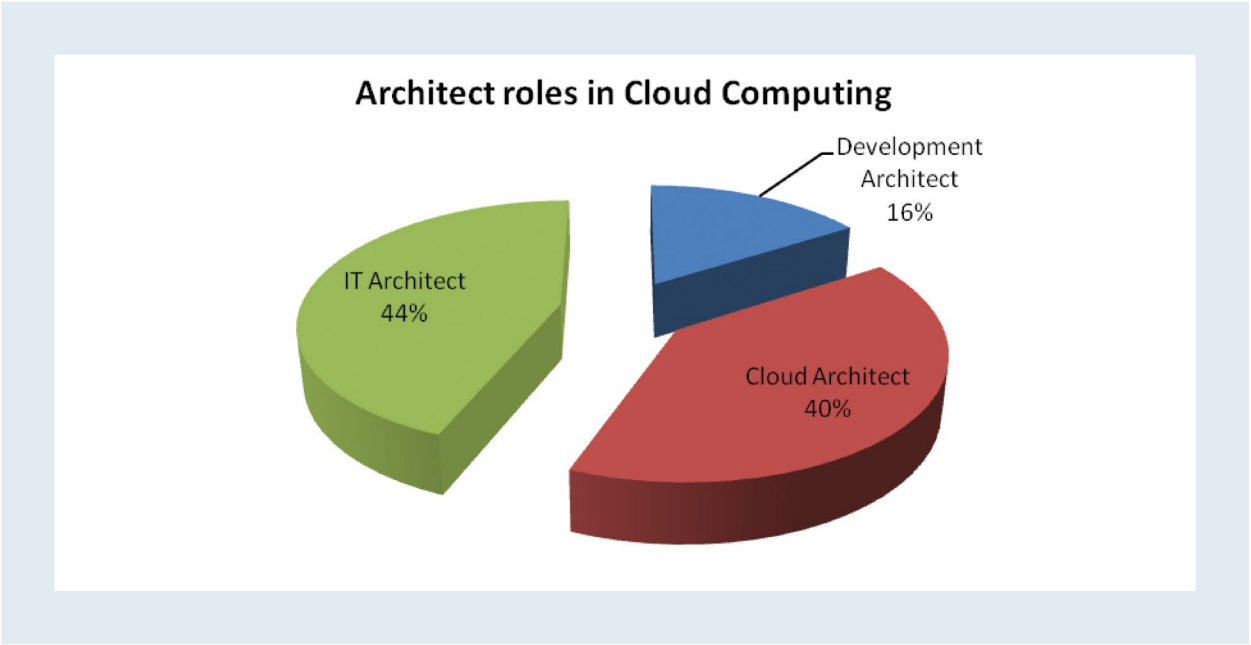


Figure 13 – Role of architects in Cloud Computing [61]

Compliance with applicable regulations and best practice is one of the challenges facing Cloud Computing in terms of trust. An important new regulatory scheme concerns the new European Personal Data Protection Regulation approved by the European Parliament[24] on April 14th, 2016 [62], that introduces comprehensive requirements for organizations doing business in Europe or storing data about European Union residents. Therefore, it is interesting to see that worldwide, only 14% of the companies that took part in a recent Cloud Security Survey [63] are fully prepared to meet these requirements. Basically, only a third of companies are prepared for the requirements in Europe, the Middle East and Africa (EMEA) and two thirds of companies in the Americas are completely unaware of them. Awareness of this new law and preparedness is highest in the EMEA region and lowest in the Americas, with only 7% of these companies currently being prepared to cope with this regulation (see Figure 14).

[24] http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era

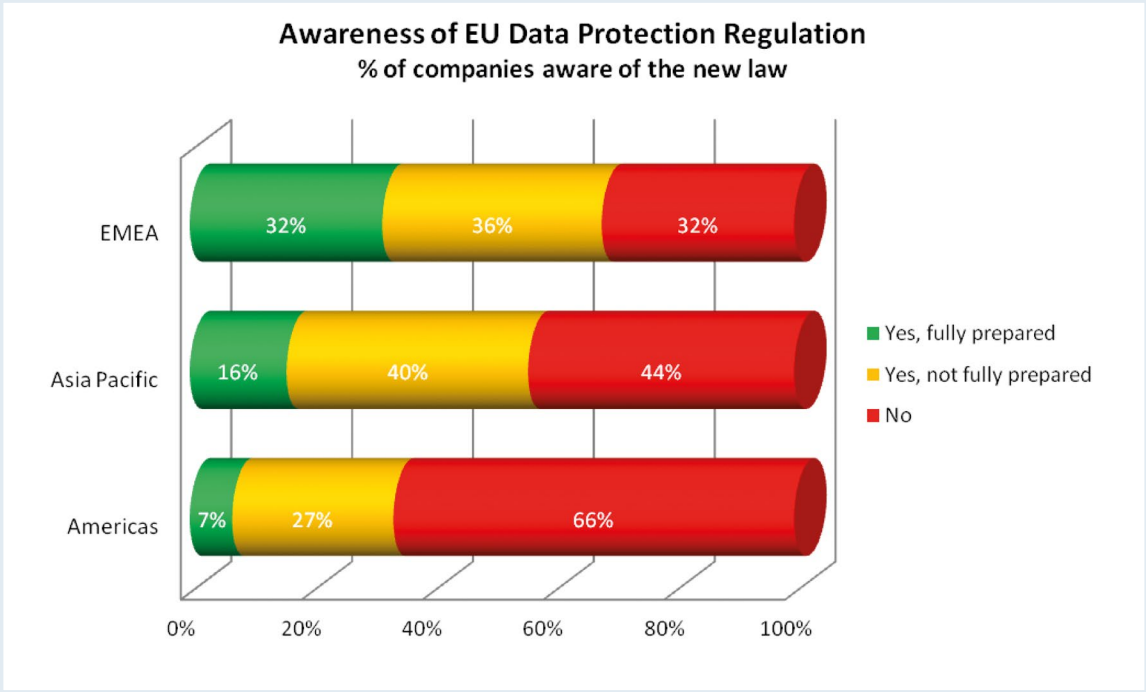


Figure 14 – EU Data Protection regulation awareness [63]

2.1.3 BIG DATA & ANALYTICS

This section presents market developments and applications related to the economic prospects of Big Data and Analytics.

2.1.3.1 MARKET DEVELOPMENTS

The link between Cloud Computing and Big Data Analytics can be easily made as many companies in the latter field take advantage of the virtual storage capabilities, identity and access management and other IaaS and PaaS that Cloud Computing offers. From an economic perspective, an important development is that many of the Big Data Analytics technologies are based on open source software, which reduces the market power of proprietary Big Data vendors. Examples include the "Hadoop" ecosystem, the engine for Big Data processing "Spark", the statistical programming language "R" through the "RHadoop" package, the general-purpose programming language "Python", and the distributed database management system "Cassandra".

The Big Data Analytics market continues to mature with increased adoption of technologies and tools by large enterprises across vertical markets [64]. Wikibon expects the Analytics market in 2026 to be worth around $85 billion, representing 17% annual growth rate over a 15-year period (see Figure 15). After an initial period of intense growth, the Big Data market is expected to slow down as of 2020, which represents a common pattern for disruptive technology markets as they mature.

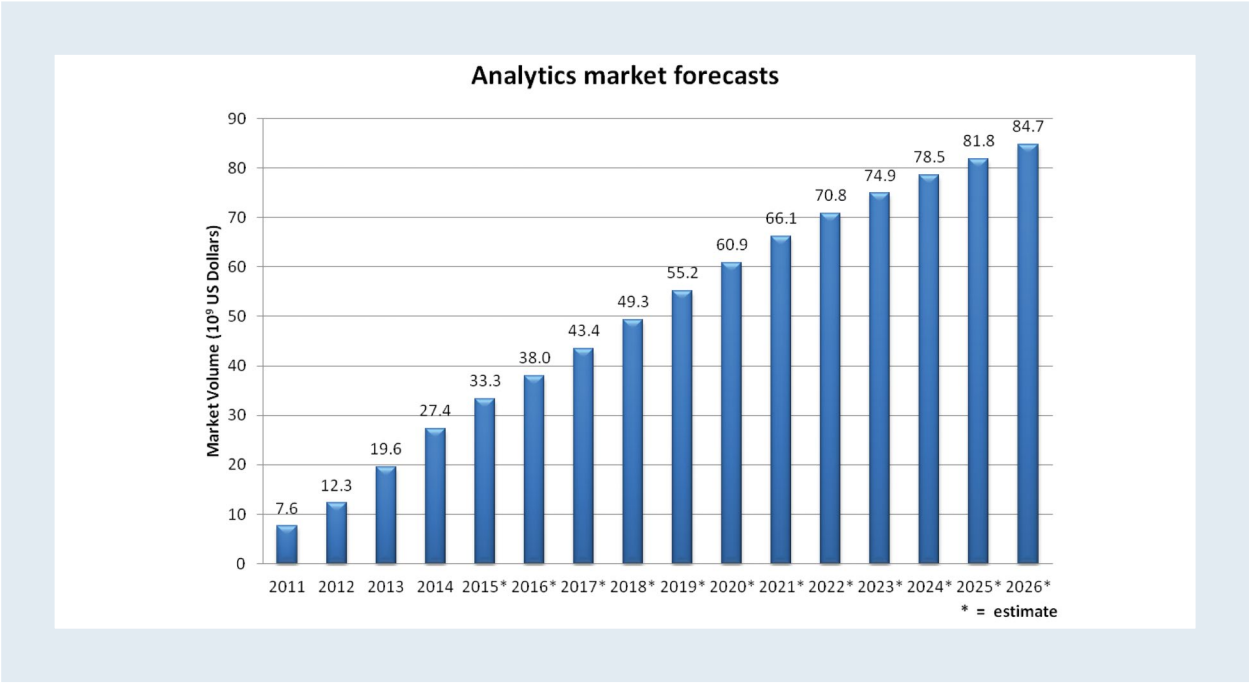


Figure 15 – Big Data Analytics market forecasts [64]

A number of factors are driving continued growth of the Big Data market [64]:

1. The maturation of data warehouses as the initial Big Data use case, applicable across vertical markets.
2. The maturation of Big Data products and services, especially the open source versions.
3. The establishment of Big Data-driven strategic decision-making, particularly in the financial services, retail, healthcare, and telecommunications industries.

NO.	VENDOR	MARKET %	BIG DATA REVENUE	TOTAL REVENUE	BIG DATA REVENUE AS % OF TOTAL REVENUE	% BIG DATA SOFTWARE REVENUE	TOTAL REVENUE	% BIG DATA SERVICES REVENUE
1	IBM	**7.4%**	1368	$99,751	1%	31%	27%	42%
2	HP	4.7%	869	$114,100	1%	42%	14%	44%
3	DELL	3.5%	652	$54,550	1%	**85%**	0%	15%
4	SAP	2.9%	545	$22,900	2%	0%	**76%**	24%
5	TERADATA	2.8%	518	$2,665	19%	36%	30%	34%
6	ORACLE	2.6%	491	$37,552	1%	28%	37%	36%
7	SAS INSTITUTE	2.6%	480	$3,020	16%	0%	68%	32%
8	PALANTIR	2.2%	418	$418	**100%**	0%	50%	50%
9	ACCENTURE	2.2%	415	$30,606	1%	0%	0%	**100%**
10	PWC	1.7%	312	$32,580	1%	0%	0%	**100%**
	TOTAL		**18607**	**n/a**	**n/a**	**38%**	**22%**	**40%**

Table 13 – Top 10 Worldwide Big Data Analytics revenue by vendor in $US millions [65]

The Big Data Market is currently dominated by well-known players (see Table 13). A number of vendors provide hardware, software, and consulting services (IBM, HP, Teradata and Oracle), whereas others have specialized in hardware (Dell), software (SAP, SAS) or services (Accenture, PWC). The overall market leader is IBM, although its Big Data revenue is just above 1% of its towtal revenue.

2.1.3.2 APPLICATIONS

A number of important applications can be identified for society as a whole, and relate to energy, agriculture and healthcare [66]. In the smart grid, balancing energy demand and supply can be better achieved with the use of Analytics. The real-time data from smart devices in the grid helps utility companies to anticipate power demand, supply, costs, and avert power outages. The use of these energy technologies must be balanced with the related privacy implications for households and their usage patterns. Household energy data, such as those consumed by household appliances, can reveal important information for those with malicious intent. UNCTAD is pressing for organizational and regulatory standards to be set on how such data is collected, processed, stored, and shared.

Analytics also provides useful tools for increasing food productivity and safety, as detailed in Section 2.1.1. Major improvement can potentially be achieved on healthcare – for example, when treatments are personalized and development of a disease is monitored to proactively treat individual patients. At the same time, such data can be analyzed to find trends and correlations with data from other patients and groups of patients. However, there must also be a balance between privacy and confidentiality of individual patients and benefits at large in the healthcare sector. If health records are disclosed to third parties, this could possibly impact insurance rates or even employment prospects. Therefore, these Digital Trust issues must also be addressed.

The staggering potential of Big Data Analytics is exemplified by the book with the declining cost of data storage, processing, and analysis (see Figure 16). Moore's Law, which assumes that processing power doubles about every 18 months relative to cost or size was applicable to the costs of DNA gene sequencing between 2001 and 2007. However, other trends besides Moore's Law have by and large contributed to the very rapid decrease in costs after 2007. Improvements in Analytics algorithms have played a significant role alongside on-demand Cloud Computing resources [67].

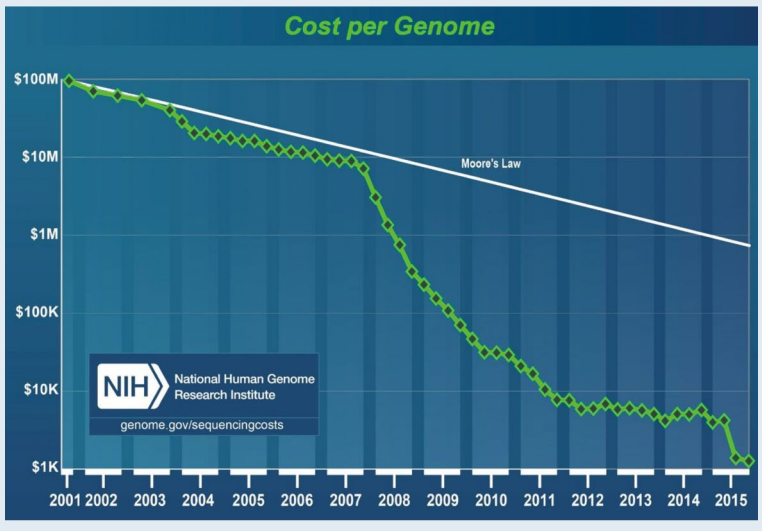


Figure 16 – Cost of genome sequencing [67]

2.2 ECONOMIC CHALLENGES OF TRUST

This section presents the economic challenges of Digital Trust to be tackled for the Internet of Things, Cloud Computing and Big Data and Analytics smart technologies.

2.2.1 INTERNET OF THINGS

It is estimated that the number of connected devices in OECD countries will increase from over 1 billion in 2015 to 14 billion by 2022 [13][25]. By 2020 it is estimated that nearly half of all consumers will own a connected IoT device (25 billion worldwide), such as Smart Meters, wearable fitness monitors, e-health monitors, weight scales, smart light bulbs, home surveillance and automation sensors and pay-as-you-drive devices [13], [46].

However, the volume and severity of data breaches is also expected to increase because of this growth in connected devices and growing data traffic. Due to improvements in public awareness, commercial enterprises, governments, and consumers are becoming more concerned about these increasing security threats. At the same time, Digital Trust is fundamental to enhancing user experience and addressing legal challenges such as privacy [13]. So, the sooner companies gain Digital Trust, the better they can leverage IoT technology and business opportunities. If such companies offer real value in exchange for personal information, they further increase customer loyalty and are subsequently allowed to access even more consumer data. By using analytics to unlock value from that data, they can offer even more relevant, revenue-generating digital products and services.

IoT has profound implications and can bring tangible benefits to individuals, businesses, and society as a whole [12]. It can be applied in many different fields, including commercial and industrial processes, consumer services, public services, energy and transport systems, security, and health care, while ensuring the protection and privacy of exchanged information and content [3]. Data can be gathered in buildings, factories, and natural ecosystems with applications in urban planning, manufacturing, and environmental monitoring [13].

From a business perspective, much additional value from IoT can be captured, since most of the IoT data collected today are not used, or data that are used are not fully exploited [51]. With more sophisticated IoT applications and by using more data, improvements can potentially be achieved in terms of efficiency and effectiveness. Examples include analyzing industrial process streams to optimize operating efficiencies and using performance data from engines for predictive maintenance. In combination with the Cloud and Big Data Analytics, numerous IoT business applications can be created.

A secure environment is fundamental in IoT and this relates to technological as well as ethical and privacy concerns. Without security, there can be no Digital Trust. However, security and privacy are among the most challenging topics that companies face in the further development of online services and e-commerce in general. As regards potential priority areas for the digital economy, governments also identified security as the second and privacy as third highest priority area, with broadband technologies in first place [13].

Borgia [12] defined a set of security requirements and discusses possible solutions in order to meet them (see Table 14).

[25] UNCTAD [66]: from 15 billion in 2015 to 50 billion by 2020, with a third of them being computers, smartphones, TVs and mobile devices.

SECURITY REQUIREMENT	POSSIBLE SOLUTION DIRECTION
Authentication and authorization	SIM cards, deal efficiently with security concerns. Features include securing the identity of communicating devices, performing secure data storage, and guaranteeing secure authentication and authorization (e.g. PIN, PUK, and PKI).
Bootstrapping of objects and transmission of data	Operations required before the network becomes active and available. These include installing and configuring credentials, keys, and certificates on the devices. Solutions have to (1) entail low computational load to work on small constrained devices, (2) entail few data overheads and (3) allow dynamic configurations.
Security of IoT data	Guarantee confidentiality and integrity of sensitive data stored in the Cloud. Possible solutions may use on-chip ROM memory, on-chip One-Time-Programmable technology, and off-chip flash memory.
Access to data by authorized persons	Guarantee that only authorized users can access data, defining which operations each single user or group of users are allowed to perform on the data. Data could be protected by passwords or more advanced mechanisms such as attribute-based access control.

Table 14 – Fundamental security requirements to meet digital Trust in IoT [12]

Failure to meet IoT security requirements may even result in physical harm as a result of three likely forms of attack [13]:

- Interception of data could reveal information about infrastructure operation, such as commands to start and stop machinery;
- Injecting fake data could result in disruption of control processes, or could be used to mask physical attacks;
- Incorrect commands could be used to trigger unplanned events or send physical resources (water, oil, electricity, etc.) to dangerous destinations.

A key privacy issue relates to the possible continued use of data outside initial terms of agreement with consumers. Therefore, consumers in the IoT must in some way retain control of their data, otherwise they will avoid the IoT due to a lack of trust. Therefore, Wolf and Polonetsky [68] argue that it is imperative to focus on how personal data is used for the Internet of Things (underlining as per authors' wording):

- Use anonymized data when practical.
- Respect the context in which Personally Identifiable Information is collected.
- Be transparent about data use.
- Automate accountability mechanisms.
- Develop Codes of Conduct.
- Provide individuals with reasonable access to Personally Identifiable Information.

2.2.2 CLOUD COMPUTING

As Cloud Computing continues to gain popularity both among private and business users, every potential user of Cloud services should consider whether to trust the providers and their service offerings. General adoption of Cloud Computing without Digital Trust is very unlikely, especially when the computing services are delivered over a network that is open for public use (i.e. public Cloud). Depending on the deployment model, Digital Trust-related issues may differ [69]:

- In a private Cloud model, trust management does not represent a major concern if the organization does not rely on a third-party service provider.
- In a community Cloud, if there is a third party involved, the same issues may occur as in the private Cloud model. Otherwise trust management is limited to the relationships agreed between community subjects.
- In a public Cloud model, many potential risks exist regarding security, privacy, and loss of control over data.
- In the hybrid Cloud model, if a private Cloud is involved in the deployment model besides a public one, trust management issues related to the public model relate to the hybrid one as well.

RightScale, a Cloud management company, conducted a survey about the adoption of Cloud Computing among 1,060 respondents from a comprehensive sample of industries and organizations of varying sizes[26] [61]. The organizations included 433 Enterprise respondents (1,000+ employees) and 627 respondents from Small and Medium-sized Businesses (SMB) with less than 1,000 employees. The respondents ranged from technical executives to managers and practitioners. Four maturity levels were defined in this survey:

- Cloud Watchers develop plans and evaluate available Cloud options to determine which applications to possibly implement in the Cloud.
- Cloud Beginners are involved in proof-of-concepts or initial Cloud projects in order to gain experience and determine future projects.
- Cloud Explorers have applications deployed in the Cloud and/or multiple projects in flight and want to improve and expand the use of Cloud resources.
- Cloud Experts are experienced in intensive use of Cloud services and are looking to optimize Cloud operations as well as Cloud costs.

Figure 17 and Table 15 depict the maturity of the originations and their corresponding initiatives. More than half of the Enterprises (59%) and SMBs (51%) are either intensive Cloud users or have implemented a number of cloud services for their organizations. Of the total survey population, a minority has no plans whatsoever, or is only performing initial investigations (15% for Enterprises and 24% for SMBs). The priorities differ based on Cloud maturity. Cloud beginners and Cloud explorers are both interested in moving more workloads to the Cloud, whereas Cloud experts are primarily concerned with optimizing existing Cloud usage and achieving cost savings. Cloud beginners are experimenting with both public as well as private Cloud implementations, whereas Cloud explorers and Cloud experts are focusing on public Cloud implementations. For the latter category, continuous integration and deployment in the Cloud is also an important activity.

[26] https://www.rightscale.com/lp/state-of-the-Cloud

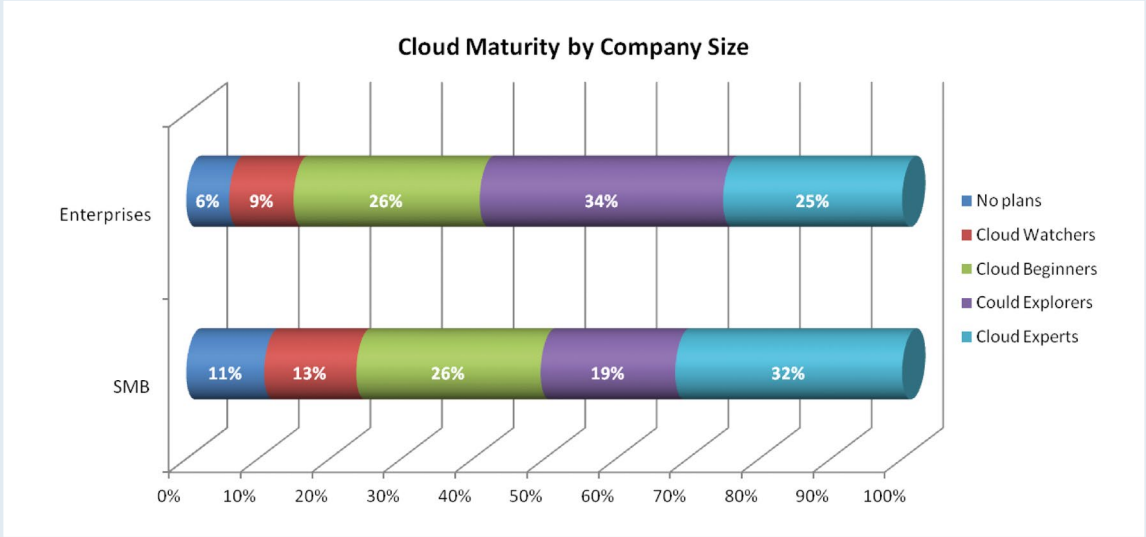


Figure 17 – Cloud maturity vs. company size [61]

NO.	CLOUD BEGINNERS	CLOUD EXPLORERS	CLOUD EXPERTS
1	Move more workloads to Cloud (43%)	Move more workloads to Cloud (63%)	Optimizing existing Cloud use / cost savings (62%)
2	Implement a Cloud first strategy (40%)	Optimizing existing Cloud use / cost savings (53%)	Continuous Integration and Deployment in the Cloud (52%)
3	Expand the public Clouds we use (37%)	Expand the public Clouds we use (51%)	Expand the public Clouds we use (50%)
4	Expand the private Clouds we use (36%)	Continuous Integration and Deployment in the Cloud (46%)	Expand use of containers (48%)
5	Optimizing existing Cloud use / cost savings (34%)	Expand use of containers (41%)	Move more workloads to Cloud (44%)

Table 15 – Top 2016 initiatives depending on Cloud maturity

The top 3 initiatives for Enterprises as well as SMBs are moving more workloads to Cloud, optimizing existing Cloud use, and expanding the public Clouds used (see Figure 18). SMBs have optimizing existing Cloud use to gain cost savings as their number 1 Cloud initiative, whereas enterprises are primarily focused on moving more of their workloads to the Cloud. Of the perceived Cloud benefits (see Figure 19), faster access to infrastructure, greater scalability and higher availability are valid for all Cloud customers, including Cloud beginners. It is also interesting to note that cost savings are not particularly considered as a major benefit by these organizations.

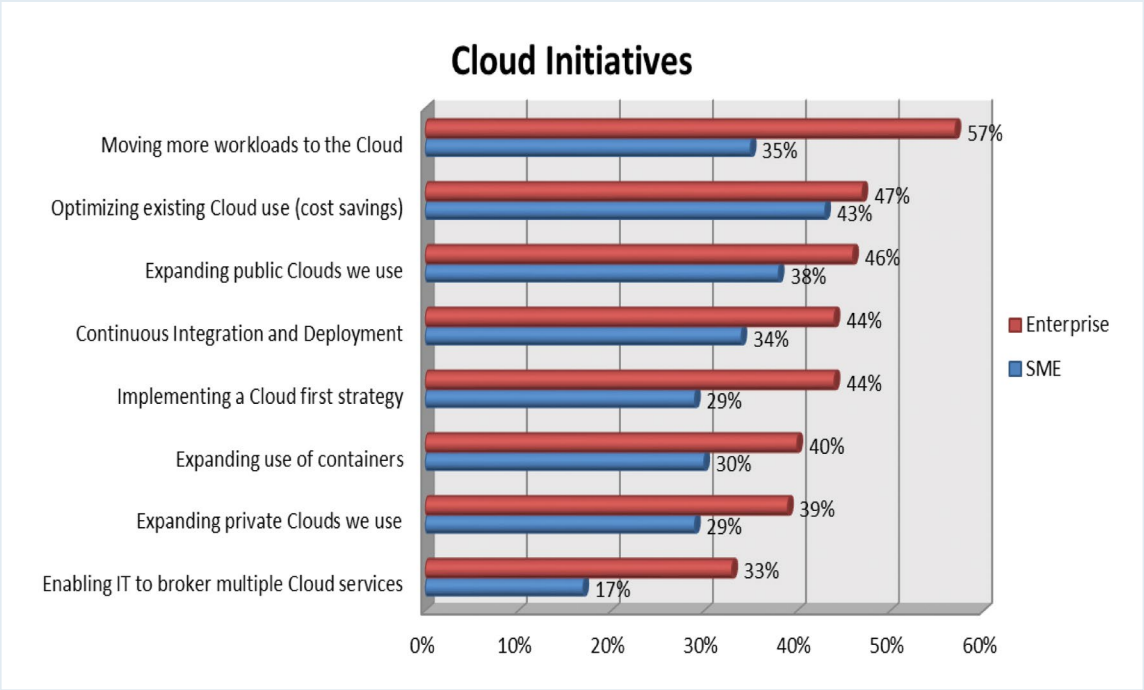


Figure 18 – Cloud initiatives in 2016 [61]

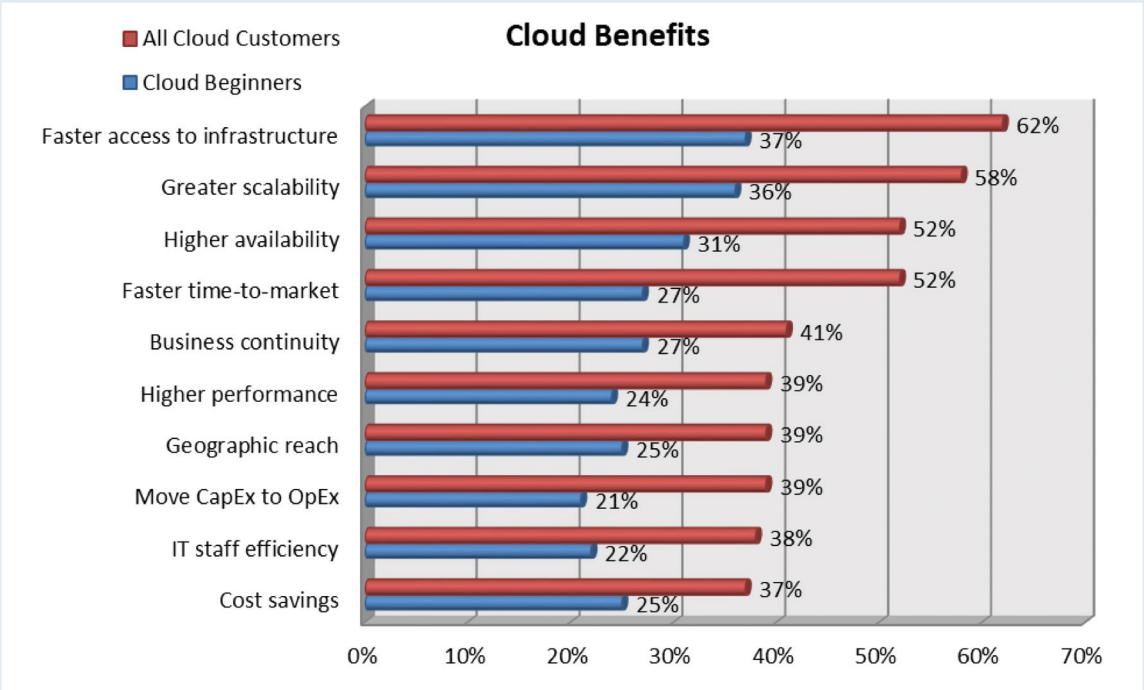


Figure 19 – Perceived Cloud benefits in 2016 [61]

Concerning Cloud usage and deployment, the percentage of enterprises that have a strategy to use multiple Clouds is above 80% (see Figure 20). Enterprises typically opt for a hybrid Cloud strategy, which consists of an integrated Cloud service utilizing both private and public Clouds. A recent growth in hybrid Cloud adoption is observed as public Cloud users add private Cloud resource pools. Furthermore, [61] noted a slight increase in the number of enterprises planning for multiple public Clouds and an equal decrease in those planning for multiple private Clouds.

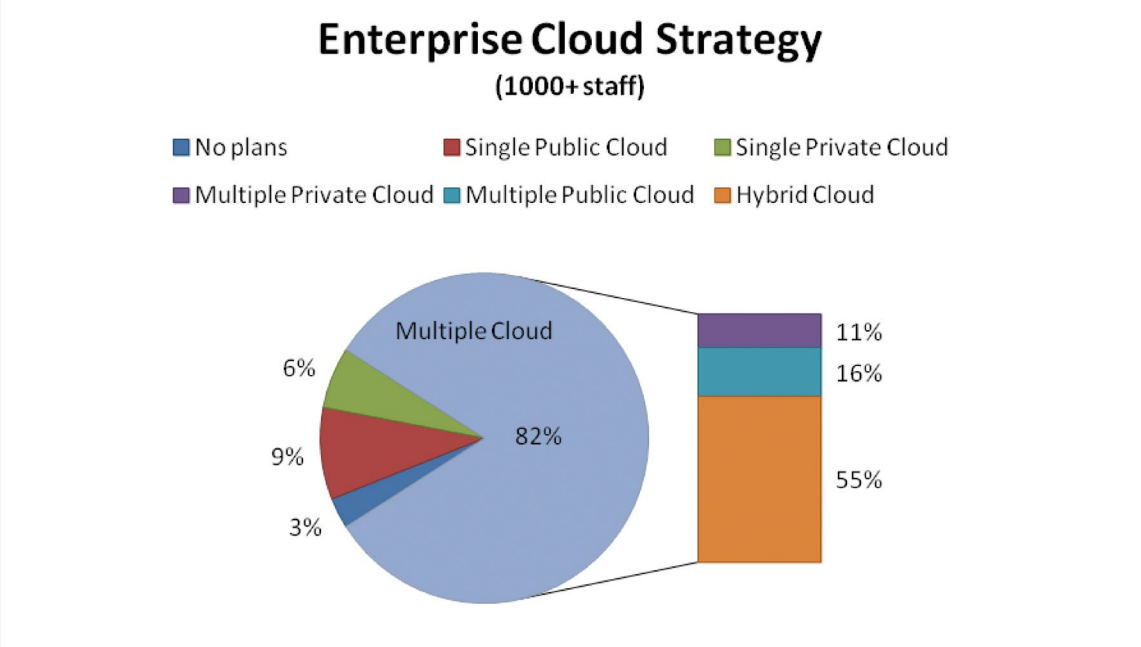


Figure 20 – Enterprise Cloud Strategy [61]

Organizations are also looking toward extending Cloud benefits to their systems of record[27] (see Figure 21). Customer relationship management (CRM) solutions currently constitute the most common system of record available as a Cloud-based service. The second largest Cloud-based services are IT service management solutions and human resources management (HRM) solutions are in third place. Applications for Accounting/Finance and Supply Chain are lagging behind. Between roughly 20 and 30% of the organizations are also planning to use Cloud-based systems of record.

[27] A system of record is an information storage system that is the authoritative data source for a given data element or piece of information.

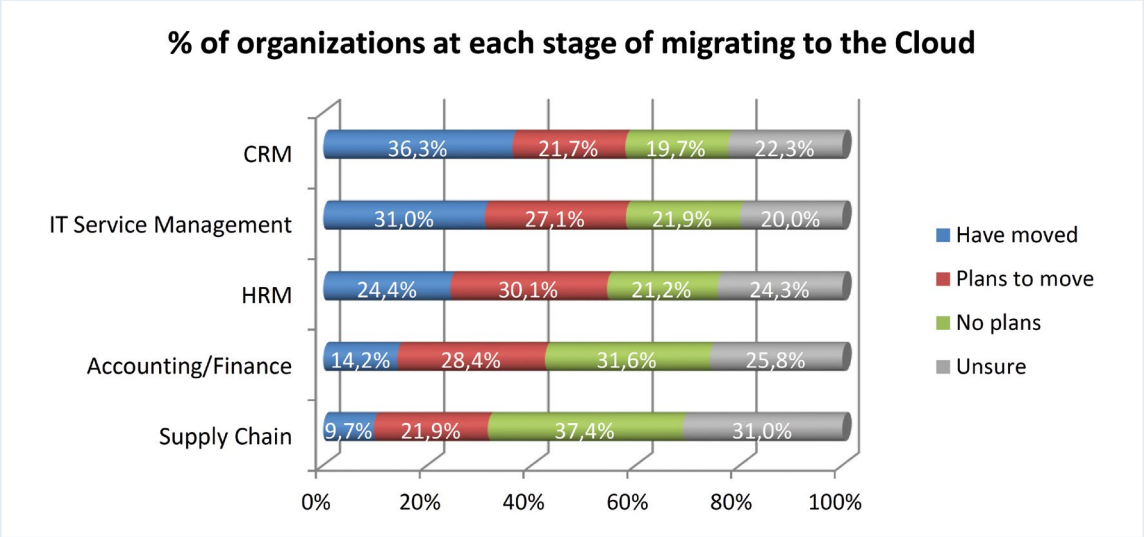


Figure 21 – Percentage of organizations at each stage of migrating to the Cloud [63]

In this survey, an interesting change was noted, as "Lack of resources/expertise" has replaced "Security" as the No.1 Cloud challenge (see Figure 22), which was consistently cited as the top challenge in Cloud. The need for Cloud expertise has obviously increased, since organizations are progressively sending additional workloads to the Cloud. A similar trend regarding Cloud security has been observed by the Cloud Security Alliance. The organization found that in the past 18 months, surveys are showing consumers are actually adopting Cloud Computing to gain better security capabilities. Nevertheless, the security of Cloud providers varies widely, with the top-tier Cloud providers having robust information security while, some Cloud providers entering the market have no recognizable security program whatsoever [60].

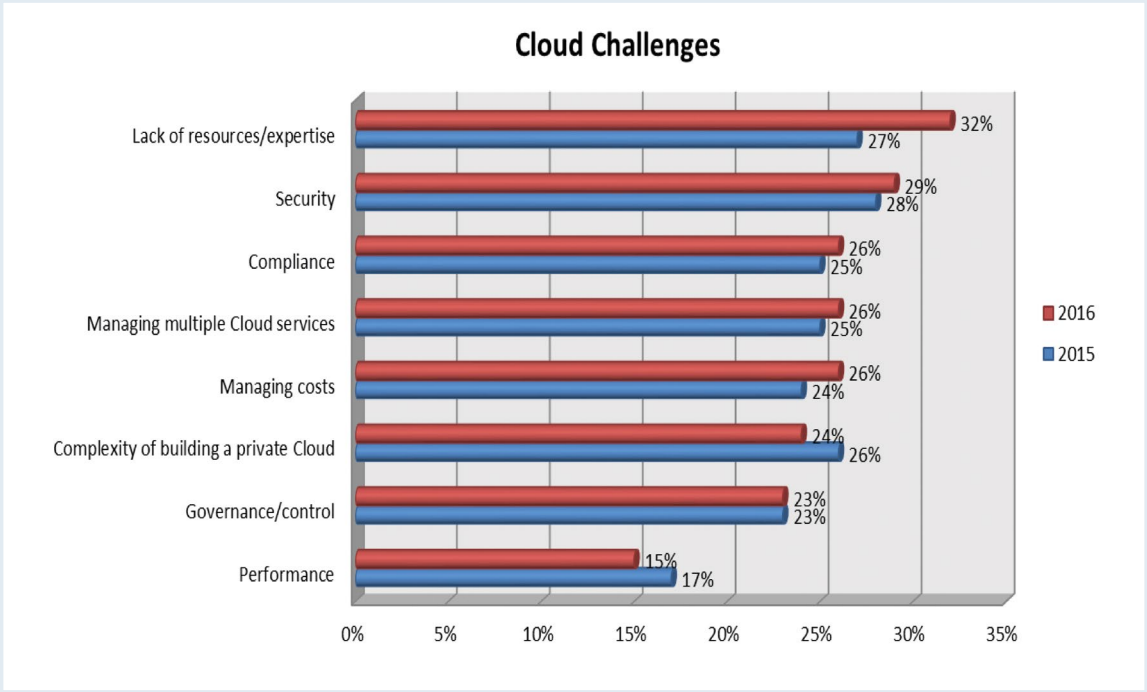


Figure 22 – Cloud challenges 2016 vs. 2015 [61]

NO.	CLOUD BEGINNERS	CLOUD EXPLORERS	CLOUD EXPERTS
1	Lack of resources/expertise (38%)	Lack of resources/expertise (34%)	Lack of resources/expertise (26%)
2	Security (35%)	Compliance (32%)	Building a private Cloud (19%)
3	Compliance (34%)	Managing Costs (30%)	Managing Costs (18%)
4	Managing multiple Cloud services (30%)	Security (28%)	Managing multiple Cloud services (18%)
5	Governance/control (29%)	Managing multiple Cloud services (26%)	Security (17%)

Table 16 – Top 5 challenges and Cloud maturity [61]

However, Cloud Computing service customers' top challenges change with their maturity (see Table 16). Although "Lack of resources/expertise" is the most important issue for all customers, security challenges decrease as customers gain further Cloud experience: "Security" is only ranked fifth by Cloud Experts. RightScale [61] found that security is not the top challenge among any subgroup, except for the Cloud Watchers. Cloud Experts do not report compliance with regulatory requirements as one of their top challenges and Cloud Beginners seem to be struggling with governance and control. Enterprises' central

IT teams have reported security as a significant challenge. However, there has been a gradual decline in security concerns among this group in recent years (see Figure 23). And almost two thirds of the IT leaders in organizations perceive security in the Cloud as at least equivalent to that of security on their own premises (see Figure 24).

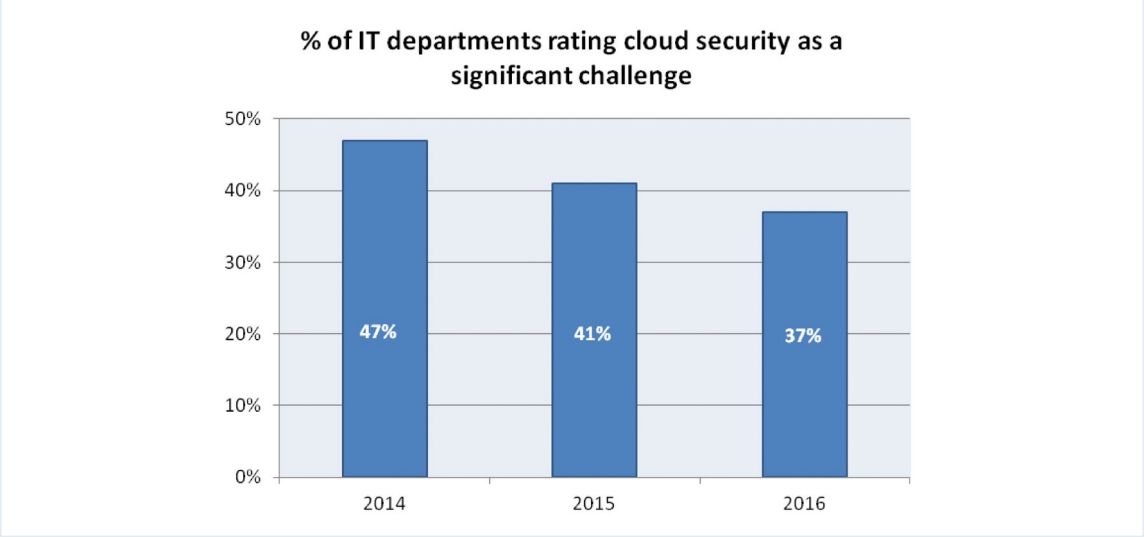


Figure 23 – Cloud security perceived as a challenge by Enterprise central IT teams [61]

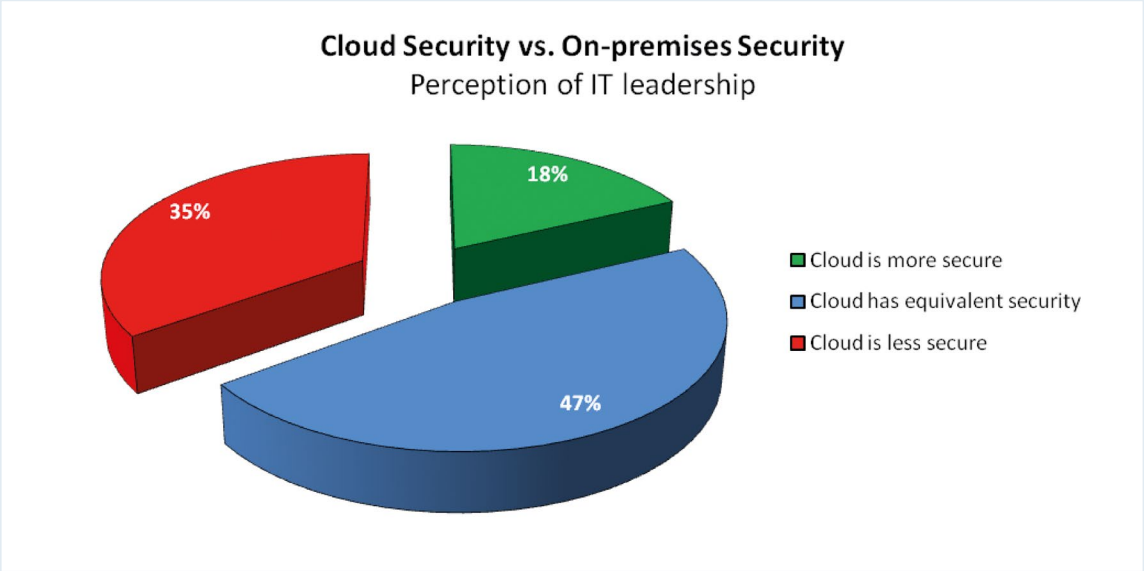


Figure 24 – Perception of Cloud Security by IT leaders [63]

On the other hand, Cloud cost challenges increase, which is especially the case for Cloud Explorers and Cloud Experts. 26% of respondents identify Cloud cost management as a significant challenge in 2016 with a gradual increase in recent years (see Figure 25). It has also been demonstrated that managing and even forecasting Cloud costs on a real workflow is difficult and that the interest of the Cloud might not be on the cost-saving aspect but on the elasticity offered by the Cloud when it comes to computing intensive workloads [70], [71]. To optimize Cloud costs, it is necessary to monitor utilization of instances and assess whether their performance is a good fit with the actual workflow. As the costs associated with the most powerful Cloud instances are significantly higher than for the less powerful ones, wasting computational power with instances that are not adapted can induce a large and unnecessary charge. Data transfer and storage also has to be considered as a potential major cost and the Cloud workflow has to take this into account to avoid unpredicted costs (for example by minimizing data retrieval from outside the Cloud or by setting up a shared file system within the Cloud itself for all instances in the same workflow).

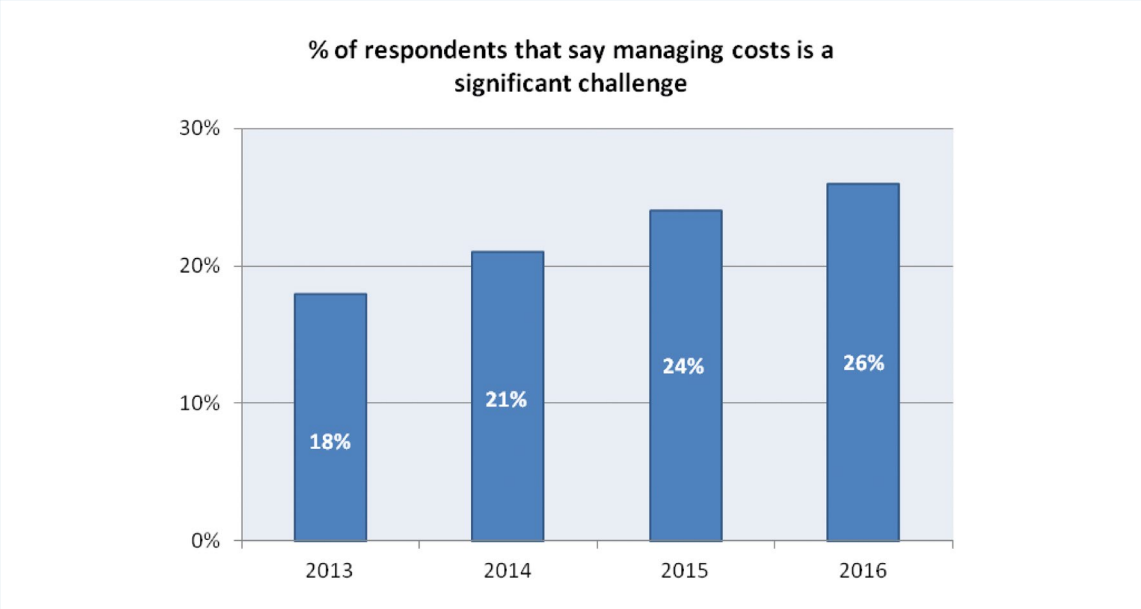


Figure 25 – Cloud cost challenges [61]

2.2.3 BIG DATA & ANALYTICS

Unfortunately, very little research is conducted on the combined subject of Digital Trust and Big Data regarding business aspects. However, trust can be approached by the value that data can create when it is exploited by a company. To correctly exploit data and enable the development of Big Data and Analytics businesses, it is necessary to actually collect the data and thus for companies to create the trustable environment required for users and clients to share that data. In fact, the best way to leverage Digital Trust for Big Data is for companies to truly understand the potential of Analytics and thus act wisely regarding the information they collect and analyze. This gives rise to three key areas of Digital Trust: data monetization, value assessment and a set of best practices.

2.2.3.1 DATA MONETIZATION

Companies can pursue three approaches to gain value from Big Data and Analytics:

- Selling: data and information-related, ranging from reports and analytics to self-service.
- Bartering: gaining new tools, services, or special deals in exchange for their raw data.
- Wrapping: generating financial impact by packaging "free" information products and services with core offerings.

These approaches are all considered as data monetization, which is defined as *"the act of exchanging information-based products and services for legal tender or something of perceived equivalent value"* [72]. Each choice has its specific characteristics, such as what one gets in exchange for the data (see Table 17).

	SELLING	BARTERING	WRAPPING
What do you get in exchange for your data?	Money	Products or services	Increased revenue from core products and services
Who should govern?	Dedicated organizational structure or business unit	Shared services group	Product Management
What are the key challenges?	Complying with legal, regulatory, and contractual constraints; Setting the right price; Leveraging advanced technology and data science; Sustaining competitive advantage	Identifying and coordinating bartering across the enterprise; Complying with legal, regulatory, and contractual constraints; Preserving value during the bartering exchange process	Avoiding merely "raising the bar" of core offerings; Meeting promised or expected service levels to avoid damage to important stakeholder relationships
Example	A retailer exchanges Point of Sale (POS) data with a data aggregator for money	A retailer provides POS data to a supplier in exchange for a software tool that helps the retailer analyze and improve sales of vendors' products	A supplier provides product reporting to a retailer at no charge, and over time receives increased sales by that vendor

Table 17 – Three data monetization choices [72]

Wixom *et al.* [73] illustrate data valuation possibilities with the analytics company comScore that sells marketing data and analytics. It measures:

- Digital consumer behavior about unique website visitors, web traffic patterns, and device choice.
- User demographics, attitudes, lifestyles, and offline behavior.
- Comparative consumer website and mobile behavior across competitors.

The data originates from four primary and trusted sources:

1. *Panel data*, from two million users, that grant comScore permission to confidentially capture measurement of user behavior and demographics.
2. *Census data*, gathered from sensors on approximately 90% of the Top 100 US digital media companies.
3. *Perceptual data* collected from panel members using proprietary surveys.
4. Data obtained *from strategic partners*, e.g. loyalty cards.

The company creates value from Big Data and achieves Digital Trust via three key assets: 1) a cost-efficient, scalable platform; 2) an analytics-savvy workforce; and 3) a deep understanding of its clients.

Therefore, it is important to understand that not only adequate technology is a prerequisite, but equally important is a skilled workforce which has profound knowledge of its customers.

Other companies exchange their raw data for tools, services, or special deals, or wrap information products and services around their core offerings. For example, UPS declared years ago that information about a package was as valuable as the package itself. To do this effectively, companies must understand their markets, partnerships and what information offerings their users value. However, the benefits of wrapping information products and services around core offerings may be short-lived. At a certain moment in time it may simply raise the bar of customer expectations.

Businesses that monetize data have six sources of value, each of which is either directly or indirectly related to Digital Trust. Organizations should focus first on one or two of these sources of value, however, all six areas are important to develop and sustain competitive advantage [72]:

- *Source of Value #1: Data* – organizations accumulate and manage unique data that has significant value in the marketplace e.g. in terms of one or more of the 4 Vs:
  - volume;
  - velocity: speed of ingestion;
  - variety: diversity of sources;
  - veracity: accuracy and comprehensiveness;
  - accessibility and processing requirements.

  Businesses must overcome issues regarding one or more of these characteristics in order to meet the needs of customers that cannot or will not provide the data themselves.
- *Source of Value #2: Data Architecture* – by leveraging open source technologies, custom programs, innovative thinking, and thoughtful designs, organizations can perform data management at low costs.

- *Source of Value #3: Data Science* – organizations should attract, develop, and retain data scientists and promote a data science culture, by investing in:
  - internal training programs to establish a common data science language;
  - knowledge management platforms to disseminate best practice;
  - university partnerships.
- *Source of Value #4: Sector Leadership* – organizations understand the business sector areas better than their clients. With deep sector expertise, it is possible to identify the most pressing business problems and determine how to effectively solve them. A variety of practices that foster deep sector expertise should be employed:
  - hire employees that have worked in client organizations;
  - partner with clients to develop solutions;
  - offer professional services to learn best practice across clients;
  - engage in your industry to benefit companies' public relations;
  - representatives speak at conferences;
  - serve on standards boards;
  - publish in trade magazines and journals.
- *Source of Value #5: Commitment to Client Action* – organizations have to recognize that clients must act upon sellers' information products and services. They have to create a sense of urgency in driving client action based on the information offerings, otherwise, the information sellers' business model is not sustainable. Typically, companies may offer:
  - extensive customer support and training;
  - client usage tracking of products and services;
  - intuitive toolsets;
  - client value generation measurements;
  - value-sharing to encourage clients to use their solutions.
- *Source of Value #6: Process Mastery* – Information sellers become masters of the business processes that their offerings inform. Information sellers often execute processes on behalf of clients, through outsourcing or by automating a client business process. Organizations cited honors, including industry or association awards, high rankings in industry lists, etc.

2.2.3.2 DATA VALUE ASSESSMENT

When competing as an Information Business by leveraging the discussed sources of value in a business model, information offerings that are rare, hard to replicate, and difficult to substitute are produced. To maximize value from Big Data and Analytics, companies can conduct a so-called Data Value Assessment (DVA), which is defined as a holistic, enterprise-level analysis of data costs, benefits, and risks [74] (see Figure 26).

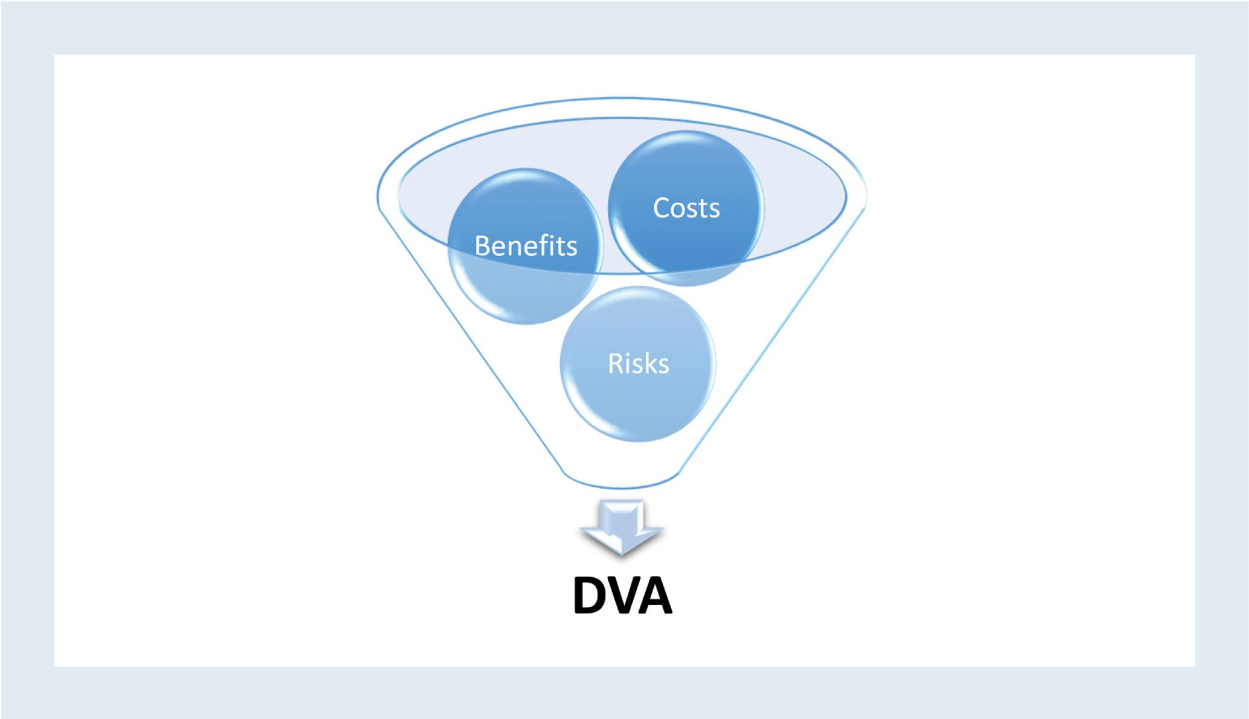


Figure 26 – Data Value Assessment [74]

A DVA is an approach generating value through Digital Trust by countering fears related to potential security breaches, privacy violations, and regulatory constraints. It can be executed either as a one-time diagnostic or as part of a comprehensive ongoing process of data governance. To provide a comprehensive and holistic understanding of data, representatives from disparate parts of the organization have to participate, such as:

- Data costs insight: IT, data management, operations.
- Data benefits advocacy: marketing, finance, analytics.
- Data risk awareness: security, privacy, risk, compliance.

Wixom and Markus [74] describe a case study in which an organization selected representative projects to determine benefits (strategic projects, products, and services) and risk (different levels of data compromised based on complexity and impact) to the company. The DVA project was split into four categories based upon the kind of data that was used: 1) basic transaction data; 2) operational data; 3) competitive information, and 4) predictive analysis and models. The project's findings included insights on reaping value from data and reducing the risks of stored data. It contributed to greater focus being placed on data management through the establishment of an enterprise data management team and helped to evolve the company's data governance practices, data risk approaches, and data classification policies. The company's approach offers *five best practices* to overcome structural and cultural challenges regarding an enterprise view of data:

1. *Take an enterprise view of data*, even if your organization does not manage data that way. Organizations must understand and govern data as a corporate asset, even when data management remains distributed.
2. *Cross-functional teams help to ensure data is evaluated in an enterprise manner.* Participation from across key organizational areas is a necessity and includes participants that describe the benefits, risks, and costs of data. Participants are typically located in silos across the organization (IT, Risk Management, Compliance, and other functional areas).

3 *Do not do DVA for its own sake,* but focus on what matters to the organization. One should not only offer a comprehensive analysis, but also create an enterprise-wide understanding of data. Although this is not necessarily an ongoing process, revisiting the data value assessments will help to keep on track.

4 *Ensure that the DVA initiative is promoted on the corporate agenda.* Typically, a leadership team communicates the importance of data as an enterprise asset, draws attention to the management board and elicits commitment for change. Briefings help to convince executives to invest more in analytics, and enterprise data governance (including security and privacy aspects).

5 *Keep the assessment real.* Since many executives are alarmed about data breaches, realistic figures regarding the cost of data breaches and data protection should be provided. Use figures from similar companies to increase credibility and convince management to take appropriate action.

By performing DVAs, companies will become savvier about resource considerations, accountability requirements, buy-in, and cultural changes. This should result in a better understanding of what it means to treat data as a strategic asset, which contributes to an improvement of customers' Digital Trust in the organization.

2.2.3.3 BEST PRACTICE

Wixom and Beath [75] describe how companies can effectively establish an analytics platform and tackle common obstacles. Organizations have to deal with a wide range of concerns, such as data *quality* issues (e.g. inaccurate/missing data), data *integration* challenges (e.g. lack of unique identifiers, inaccessible source systems), company *politics, meeting laws* and *regulations.* Causes for these concerns range from missing or broken business processes, or business users who cannot or will not engage with data analysis. This may relate to a lack of analytics skills and tools, a lack of time to build trust in the analysis process, or they just do not understand the data. Also lack of leadership or commitment for change, lack of vision of what insights are possible, or lack of a compelling business reason, may severely hinder the creation of a useful analytics platform.

They have identified three sets of practices to overcome obstacles preventing organizations from deriving value from their Big Data and analytics initiatives and contributing to Digital Trust. These are:

1 Employ user-centric development with the objective of actively engaging users in the development of tools and services.

2 Allocate hybrids of staff in order to develop business-savvy IT people and IT-savvy business people in order to pinpoint the right data and identify insights that matter.

3 Carry out internal marketing for the initiative and prioritize, track, and sell the value from Big Data and Analytics through company videos, knowledge-sharing events, newsletters, etc.

Organizations that initiate analytics initiatives get the best results if they solve specific, important business problems and build capabilities incrementally [75].

Digital Trust is thus necessary for business development of the three Smart technologies: Internet of Things, Cloud Computing and Big Data. In the next chapter, several technical approaches will be presented as different means of leveraging Digital Trust.

3 DIGITAL TRUST FOR SMART ICT: TECHNICAL APPROACHES

This chapter presents and reviews the existing technical approaches to Digital Trust. It first presents the means of addressing Digital Trust for Smart ICT in general, then focuses on each of the following smart technologies: Cloud Computing, Big Data and Internet of Things.

3.1 TRUST IN SMART ICT

Trust in Information and Communications Technology (ICT) systems can be explained as a computational construct whose value depends on the context and is likely to change over time [76]. Whereas trust itself is fragile, distrust is robust. In other words, trust can be lost very quickly by users, in particular through extensive media coverage of incidents and once the transition point to massive distrust is attained, it is very difficult to restore the initial state. Thus, building and maintaining trust is essential and requires a constant effort from the ICT service provider.

As the scope of this White Paper is to focus on Digital Trust aspects, this chapter will refer to Trust or Digital Trust indistinctly.

Apart from the general technical challenges of developing interconnected smart technologies related to Cloud Computing, Internet of Things and Big Data, Digital Trust is steadily becoming an increasingly significant challenge that must be addressed. Trust is essential in ICT and is no longer merely a matter of **security alone** but is transversal to ICT in almost any aspect of hardware and software ranging from consumer devices and equipment to service providers and data centers. Trust in ICT has to deal not only with purely technical problems, but also with social aspects and constraints that have to be addressed in a technical manner.

This chapter will first provide the common Trust problematics related to the Smart ICT technologies presented in this White Paper. Then, for each of these technologies, more specific details are given.

As Cloud Computing, Big Data, and IoT technologies are closely linked, this chapter will first present Trust concerns relating to Cloud Computing, then Trust for Big Data aspects that were not covered in the Cloud Computing section and finally the IoT aspects that were not covered in the Cloud Computing and Big Data sections as depicted in Figure 27.

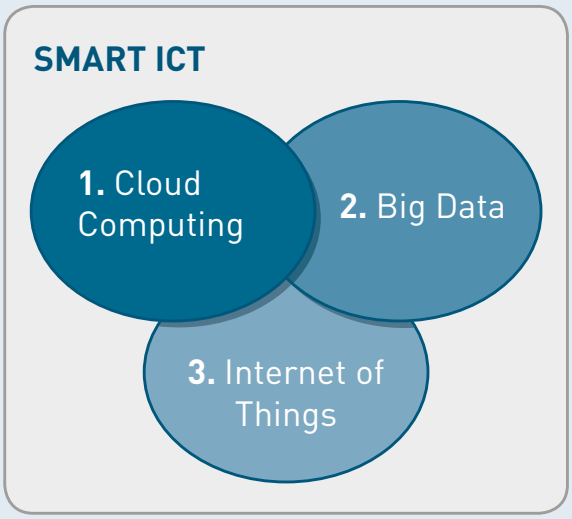


Figure 27 – Chapter organization

Digital Trust is necessary to the broad adoption of any new technology. However, owing to the actual complexity and connectivity of current systems and the data volume involved, this leads to greater vulnerability[28]. This section presents the basic components of Digital Trust that are involved in any ICT system: Privacy, Data, and Information Security and Interoperability.

3.1.1 PRIVACY

With the technological development and advent of the ICT era entailing massive and almost invisible sharing and collection of data, privacy is more than ever a central issue. Although privacy norms greatly differ across cultures, the objective of privacy is a universal and fundamental social requirement [77]. In a study about privacy behaviors regarding information technology, Acquisti *et al.* [78] characterized privacy based on three key concepts. Privacy is **uncertain**, meaning that individuals rarely have clear knowledge of what information about them is available to others and how this information can be used and with what consequences. Thus, decision-making on what information to share is often the result of a cost-benefit calculation, which is not always made taking all factors into account. Privacy is **context-dependent**, meaning that individuals' consent to disclose Personally Identifiable Information is dependent on where (e.g. which platform) they share the information[29] and if other individuals have already agreed to share the information[30]. Privacy is **malleable**, meaning that the acceptable level of privacy is often determined by a *construction* instead of a *reflection*. Acquisti *et al.* also showed the influence of default settings in the acceptance of privacy policies in ICT and highlight that the confusion induced by these policies is often deliberate. They state that, if U.S. consumers actually read the privacy policies of the website they visit, the aggregate opportunity cost would be $781 billion/year.

[28] Vulnerability of hyper-connected and complex systems as viewed by the ITU-T Focus Group on Smart Sustainable Cities – Cybersecurity, data protection and cyber resilience in smart sustainable cities.

[29] Surprisingly it was found that the more casual the information collecting source was, the more individuals agreed to share secrets, although all collecting sources had the same privacy level.

[30] It was also found that individuals trust the collecting source more if it is already well-known.

Privacy in ICT takes many forms such as anonymization of data collected [79] or location privacy [80] or even the "right to be forgotten" [81], leading to holistic approaches such as Privacy by Design [82]. Privacy by Design is a system design philosophy that aims to consider privacy as a core component of the system itself with the help of Privacy Impact Assessments (PIA) [83] at each step of the design.

With this approach, the problem of privacy in a software application or system is technically addressed at the design stage with an eight-step design strategy: MINIMIZE, HIDE, SEPARATE, AGGREGATE, INFORM, CONTROL, ENFORCE and DEMONSTRATE [84].

- MINIMIZE: restrict the amount of personal data collected to the minimum to limit the impact on privacy. This ensures that no or no unnecessary data are collected to fulfill the system's objective.
- HIDE: personal data and interrelationships are hidden from plain view from anybody. In the past, many systems have been designed using innocuous identifiers that later turned out to be privacy nightmares. Examples of such identifiers are identifiers on RFID tags, wireless network identifiers, and even IP addresses. The HIDE strategy is important and forces us to rethink the use of identifiers to prevent unwanted correlation of data.
- SEPARATE: distribute data processing and/or storage to prevent a central component having the global view of data for an individual.
- AGGREGATE: aggregation guarantees anonymity since sufficiently coarse-grained aggregation ensures that no information can be attributed to a single individual.
- INFORM: improves Trust by transparently informing subjects whenever personal data is processed, in particular by third parties.
- CONTROL: is the counterpart to the INFORM strategy that allows users to edit their personal information.
- ENFORCE: ensures compatibility with legal requirements.
- DEMONSTRATE: compliance with the privacy policy and legal requirements.

The Privacy by Design model is particularly well-suited (but not restricted) to social applications [85], location services, and IoT [86], Cloud Computing [87] or Big Data [88].

3.1.2 DATA AND INFORMATION SECURITY

In recent decades, the ICT landscape has changed considerably, in particular through the ever-increasing availability of Information Systems and their information exchange, in each of the ICT sub-sectors. The massive amount of data involved and the level of detail in the information contained in data make systems managing that data critical. Their disruption, malfunction or compromise can seriously affect our societal and individual well-being.

System security generally involves a trade-off between the complexity of breaching and implementing this security. Limited lifetime (number of uses) of the keys and audit, recovery procedures are generally implemented to reduce the implementation complexity and thus the cost incurred. However, with regards to financial loss and the negative image generated by security breaches, security is a real concern.

Authentication and encryption are core concepts in data and information security. Identity and Access Management (IAM) ensures that users accessing systems and data have the rights to do so, while encryption makes data unreadable without the correct "key". Interested readers are referred to the previous versions of this White Paper [45], [89] for further details of these two techniques. Multi Factor Authentication (MFA) is also gaining importance in respect to IAM techniques. The principle is that access to a resource (service, software, data or system) is authenticated in several steps. The first step is generally the good old credential

system with an ID and password prompt. Then, instead of granting access to the resource immediately, one or more other authentication methods are required (generally two at the time of the writing, in this case it is referred as a *two-step verification*). This can be a code embedded in an SMS received on the user mobile or a temporary and unique key generated by an application on the user mobile. For example, with the *Google Authenticator* application, it is possible to link a smartphone to a resource access and provide event-based or temporal-based access. For that purpose, *Google Authenticator* implements TOTP and HOTP security tokens, described in RFC 6238[31]. By these means, the mobile is becoming in itself an authentication method. According to Gartner, in 2016 phone-based authentication is actually dominating the market and security is becoming software-defined, increasing systems' flexibility and facilitating their management.

When it comes to Data and Information Systems, security is an abyssal topic and it is out of scope of this paper to deal with the whole stack of existing security systems and techniques. Thus, this section aims at providing a set of the most important aspects in data and information security along with some best practice.

When it comes to Data and Information Systems, security is an abyssal topic and it is out of scope of this paper to deal with the whole stack of existing security systems and techniques. Thus, this section aims at providing a set of the most important aspects in data and information security along with some best practice.

The original triad of **Confidentiality, Integrity,** and **Availability** (CIA) in Information Security has long been the basis of numerous studies in ICT. However, the evolution of Information Systems and the complexity of their interrelationships with regard to data might suggest that the CIA model has become outdated. Following this definition in 2002, the OECD's Guidelines for the Security of Information Systems and Networks [90] proposed nine components of security: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. In 2004, NIST proposed more than 30 principles and best practices for securing Information Systems [91]. Among the many principles proposed, the following should be noted:

- Security Foundation: Treat security as an integral part of overall system design.
- Risk-Based: Protect information while being processed, in transit, and in storage.
- Ease of Use: Base security on open standards for portability and interoperability.
- Increase Resilience: Isolate public access systems from mission critical resources.
- Reduce Vulnerabilities: Do not implement unnecessary security mechanisms.
- Design with Network in Mind: Use unique identities to ensure accountability.

The original IEC definition of security [92] is as follows: *"The extent to which the system can be relied upon to perform exclusively and correctly the system task(s) under defined operational and environmental conditions over a defined period of time, or at a given instant of time"*. On the other hand, the original ISO definition [93] is more centered on its factors: *"The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance"*.

Later, in the ISO/IEC consensual definition [94], authenticity, accountability, non-repudiation, and reliability are added to the CIA triad definition of Information Security.

[31] https://tools.ietf.org/html/rfc6238

In [95], Avižienis *et al.* propose an alternative definition that encompasses the aforementioned ones. Thus is a consensus-based extended definition of what dependability and security in ICT are. According to their definition, **dependability** is the ability of a system to avoid service failures that are most frequent and more severe than acceptable. This concept leads to that of **Trust** that, in this vision can be defined as *accepted dependence*. Dependability is also characterized by its attributes:

- **availability**: readiness for correct service;
- **reliability**: continuity of correct service;
- **safety**: absence of catastrophic consequences for user(s) and the environment;
- **integrity**: absence of improper system alterations;
- **maintainability**: ability to undergo modifications and repairs.

In their definition, **security** is actually a composite of some of the attributes of dependability: integrity and availability, with the confidentiality aspect added in.

This is in agreement with the usual definitions of security [96], that view it as a composite notion, namely, *"the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information"*.

This unified definition of security can therefore be summarized as the absence of unauthorized access to, or handling of, system state.

In addition to this definition, Avižienis *et al.* also add secondary attributes which are especially relevant for security:

- **accountability**: availability and integrity of the identity of the person who performed an operation;
- **authenticity**: integrity of message content and origin, and possibly of some other information, such as the time of emission;
- **nonrepudiability**: availability and integrity of the identity of the sender of a message (nonrepudiation of the origin), or of the receiver (nonrepudiation of reception).

In summary, the dependability and security specifications of a system describe what is acceptable in terms of requirements for the aforementioned attributes to enable Digital Trust.

The means to achieve these requirements are classified into four fault management categories:

- Fault **prevention**: means to prevent the occurrence or introduction of faults.
- Fault **tolerance**: means to avoid service failures in the presence of faults.
- Fault **removal**: means to reduce the number and severity of faults.
- Fault **forecasting**: means to estimate the present number, the future incidence, and the likely consequences of faults.

Fault prevention and fault tolerance aim to provide the ability to deliver a service that can be trusted, while fault removal and fault forecasting aim to achieve confidence in that ability, i.e. that specifications are adequate to the system. For that purpose, the existing technical standards that describe the implementation issues on security and how to address them [97] will be presented later on this White Paper, in Chapter 4.

The Secure by Design approach and associated framework [98] aim to tackle these Security problematics at the design stage of the system in a similar way to the Privacy by Design approach for Privacy. The Secure by Design approach defines different goals depending on the target system. For example, for telecommunication

networks it focuses on identifying entry points and necessary redundancies. For hardware it focuses on topographic properties, physical properties (e.g. no correlation can be made between the processing and energy consumption), functional properties (fault resistance) and algorithmic properties. In a Secure by Design system, security requirements are captured before design and thus are integral part of it. Risk assessment is continuously and iteratively implemented and updated during the system life cycle. Last but not least, the security level is continuously monitored and assessed to enable autonomous and adaptive security.

Data access abstraction is also aimed at improving data security. In this model, there is a separation between the applications that need access to data and data itself. In scientific applications, one of the widely used data abstraction models is NetCDF [99] which serves two purposes: data access and representation abstractions. For data access abstraction, instead of directly accessing data, the applications request APIs that can ensure the consistency of the access request. If coupled with an IAM tool, access to data is therefore securely controlled and dynamically checked for consistency (as no direct modification of the data structure is allowed) at the same time.

3.1.3 INTEROPERABILITY

Interoperability of systems is also an important aspect of Digital Trust. Although there are no studies that globally address the interoperability of every smart technology, several research projects and standards exist for a particular technology and provide different definitions of interoperability [100]. These projects and standards will be reviewed later in this chapter, in the smart technologies sections 3.2, 3.3 and 3.4 and in Chapter 4. However, in its various definitions, system interoperability is mainly composed of two criteria:

- Compatibility: a system is compatible with other systems if they can communicate and work together to serve a common purpose.
- Interchangeability: a system is interchangeable with other systems if their purpose, functionalities and offered services are the same. Moreover, interchangeability adds the constraint that the system must also allow this transition from one to another. E.g. a Cloud storage provider that prevents (or makes it difficult) to migrate stored data from its Cloud to a competitor cannot claim to be interchangeable and thus is not considered as interoperable.

Depending on the specific usage scenario, all aspects may need to be taken into account for successful deployment of a system that is compliant with state-of-the-art practices and standards.

3.2 TRUST IN CLOUD COMPUTING

When assessing Trust in relation to Cloud Computing, one must distinguish between sociological and technological means of providing Trust [101], [102]. Furthermore, in [102], Trust is also characterized with a temporal dimension, in particular for Cloud systems. This dimension is described as *Persistent Trust* for the long-term underlying properties of an infrastructure and *Dynamic Trust* for specific states and contexts, whether social or technological. This signifies that the concept of Trust itself evolves over time and matures with the advances of the underlying technology.

Moreover, a distinction must be made within the concept of Trust for Cloud Computing, depending on whether it is related to a public, hybrid or private Cloud. Indeed, the same model does not apply to all these cases. Private Clouds, generally company Clouds, are managed internally by the company and therefore access to data and authentication of resources are under control. For hybrid Clouds, the problem is slightly different because it combines the use of a private and a public Cloud but generally Personally Identifiable Information data or confidential data are treated internally. The main problem when it comes to Trust in Cloud Computing is the way data are treated and managed in **public Clouds**. In a public Cloud model, everyone may gain access to data because the Cloud resources are shared between people and the underlying security model is managed by the Cloud provider. For that reason, this chapter will focus more specifically on how to make data management trustable for the users in a shared Cloud environment.

The following of this section will revise evolutions of Trust concepts and some of the existing technical methodologies Cloud providers adopt to satisfy their users' requirements in terms of Trust.

3.2.1 TRUST AS A HUMAN CONCERN

According to a 2010 survey [103] conducted by Fujitsu, 88% of users worldwide are worried about their Personally Identifiable Information (PII) data stored online in Cloud services. The main concerns were regarding who has access to the data and where they are physically stored.

In 2010, Sato *et al.* [104] highlight that, at that time, 70% of potential Cloud users considered security as a major threat to Cloud adoption. They qualified this problem as being relevant to social security (as opposed to technical security) and classified it based on three key areas.

- The problem of multiple stakeholders, meaning that in the Cloud there are at least three parties involved (the organization using the Cloud, the Cloud provider itself and the third parties that include competitors and stakeholders in business). They highlighted that in this model, if the data is in the Cloud, the authentication process to access it is pulled back to the Cloud provider.
- Open space security, meaning that in contrast to a conventional scheme in which control of data is operated where data is stored, in the Cloud users cannot specify where their data is placed, which increases the perception of a threat regarding access to data. They suggest promoting the benefits of encryption and key management instead of traditional data placement strategy to cope with this problem.
- Mission-critical data handling, meaning that when using public Cloud services, the keystone to consent for storing PII data by Cloud users lies in the understanding and involvement of the Cloud provider in this mission. This is necessary to build the client's Trust.

More recently, in 2015, another survey [105] was conducted to explore the issues of consumer Trust in Cloud Computing. Through the participants' responses, the authors discovered that, although everyone is sharing PII data consciously or unconsciously:

- Users do not trust current systems. More than 93% are concerned about who has access to their PII data and 80% do not know where the data are stored. Moreover, 73% of users believe that security is the biggest issue preventing adoption of Cloud storage. However, most of them do not know how their data is protected.
- Users mostly (74%) do not believe their government is able to protect their rights in case of a felony offense between two parties in different countries. Instead, users want upfront protection before a crime occurs.
- Education is key to Trust. 88% of users are willing to change their habits and learn about online security.
- Trust cannot be purchased. Most users are not willing to pay more for more secure storage. Instead, they believe that it is the duty of the Cloud provider to secure data.

3.2.2 TRUST MODELS

Several approaches exist for classifying Cloud Computing Trust models. However, the literature remains inconsistent with a number of definitions and solutions to the problem of Trust and Trust management in Cloud Computing [106].

Abbadi and Martin [107] built their Cloud Trust model based on Cloud providers' operational trustworthiness. In this aforementioned work, they introduce the following properties: adaptability, scalability, resilience, availability, and reliability. A similar Trust management model was proposed in [26] based on credential attributes such as availability, reliability, turnaround efficiency, and data integrity. One of the more sophisticated models to date is that proposed by Huang and Nicol in [108]. They built their Trust model based on five existing Trust mechanisms in the Cloud:

1. Reputation-based (aggregated opinion of a community).
2. Service Level Agreement (SLA) verification-based (agreements on service provisioning).
3. Cloud transparency-based (how Cloud service providers operate).
4. Trust as a service-based (third-party delegation of Cloud Trust management).
5. Accreditation, audit, and standards-based (formal assessment by certified third parties).

Kanwal *et al.* [106] have proposed another classification that partly overlaps with that of Huang and Nicol [108] (the first two points).

1. Feedback-based (Response time-based model, Trust as a service model, PLT-based model).
2. Agreement-based (SLA-based model, Trust model for security aware Cloud).
3. Area-based (Collaborative model, Security & interoperability-based model).
4. Certificate/secret keys-based (Ticket-based model, Certificate-based model).
5. Subjective Trust (Novel weighted model, Fuzzy logic-based model).

And Firdhous *et al.* [109] approach the classification based on models used in distributed computing, that also partly overlap with the two other classifications.

1. If SLAs are part of the model.
2. If an identity management and/or authentication system is involved.
3. If data security is explicitly mentioned.
4. The Cloud deployment layers that are involved.
5. If support across multiple heterogeneous Clouds is included.

Because of this fragmented landscape of Cloud Trust mechanisms, [106] makes a case that a holistic Trust model is needed to address the requirements of Cloud consumers. Huang and Nicol [108] argue that current Trust mechanisms for Cloud Computing are, by and large, based on the perceptions of reputations, and self-assessments by Cloud service providers. Examples are Trust based on reputation and Service Level Agreement (SLA) verifications that merely focus on the "visible" elements of Cloud service performance. Third party audits are only in place in a small number of cases. Therefore, they propose a framework that integrates several Trust mechanisms based on evidence, certification and validation. This model was discussed in an earlier ILNAS White Paper[32].

Corradini *et al.* [24] propose a simplified classification to reduce the complexity of the topic and improve high-level analysis. They organize Cloud Computing Trust models into three categories: 1) policy-based; 2) recommendation-based; 3) reputation- and feedback-based. The *policy-based* models relate to contracts and agreements signed by Cloud service providers for the delivery of their services to customers. Examples of documents that provide the basis for Trust are SLAs and service policy statements (SPS). In the *recommendation-based* models, the consumer (trustor) and provider (trustee) have no previous working relationship. Such Trust relationships are usually initiated by a third-party auditor who provides a baseline to evaluate services or providers. In *reputation-based* Trust models, the trustee helps the trustor to choose Cloud services based on e.g. feedback and opinions from other consumers who have evaluated Trust with respect to services and providers.

Huang and Nicol [108] have two recommendations to further professionalize Cloud service provisioning that are beneficial to users and providers of Cloud services. Firstly, to initiate a *policy-based* approach to Trust relations, by which Cloud Trust is derived from official third party audits that prove the Cloud entity and its services are compliant with trusted policies. Secondly, facilitated by standards[33], to commence an *attribute-based* approach to Trust relations, by which attributes of the Cloud service provider and its provided services are used as evidence for Trust judgments.

Alabool and Mahmood [110] propose a further Trust level evaluation framework that is specifically applied to Digital Trust evaluation of IaaS. They applied it to IaaS Cloud providers and showed several Trust gaps that required improvement actions. Their proposed Trust model consists of nine evaluation criteria and can be used by both vendors and buyers of IaaS when implemented by an authoritative or certified third-party.

[32] http://www.portail-qualite.public.lu/fr/publications/confiance-numerique/etudes-nationales/white-paper-digital-Trust-june-2014/index.html (see pages 21-23).

[33] e.g. ISO/IEC 17788 Information technology — Cloud Computing — Overview and vocabulary

TRUST CRITERION	DESCRIPTION
Integrity	Integrity implies that all assets of IaaS, such as (hardware, software, and data) can be accessed or modified only by authorized parties.
Benevolence	The willingness and motivation of a service provider to add value, at the users request, and without expecting any reward.
Security	The ability to protect the most valuable assets and control the situation of these assets.
Competence and Ability	Competence is defined as a level of knowledge and skills that helps to differentiate between better and poorer services. Ability is how to demonstrate the competencies and expertise of the trusted party i.e. the user's perception of a trustee's ability to meet the user's specific needs.
Privacy	A fundamental human right that guarantees the prevention of unauthorized parties from gaining important information and/or using this information in unenforceable ways.
Predictability	The user's expectations regarding what the object of Trust will do. This refers to the consistency of actions and job performance which reduce uncertainty and risk.
Reputation	The value of the end user's perception based on observations or past experiences and the explored future behavior in the context of what others are achieving in the marketplace.
Accountability	The auditing of the identity of an object which helps users determine with whom it is interacting and determine legal, operational, and technical responsibility with respect to that object.
Assurance	Providing a sense of comfort or ensuring that the service has been designed, developed, and maintained based on formalized and rigorous controls and standards.

Table 18 – Trust evaluation criteria for IaaS providers [110]

3.2.3 TRUST AS A TECHNICAL CHALLENGE

In [111], Khan *et al.* characterize Trust in Cloud Computing with 4 issues: Control, Ownership, Prevention and Security. In their approach, data is the keystone of the problem and the main challenges that Cloud providers have to address are diminishing control over data and lack of transparency. They mention that it is in the interests of Cloud providers to tackle these problematics in order to keep building their client base and thus expand their business. They also insist that because of the opaque property of how Clouds are managed and because of the lack of convergence between Cloud provider assurances, provider certification is necessary. They propose the creation of an independent certification body that will assess how the security provided by Cloud offerings match up with what is advertised and what is recommended. In this scope, technical standardization can provide the tools, techniques, guidelines and assessment grid necessary to produce such a quality stamp. Finally, they conclude that auditing and certifying will work as a Trust model to boost consumers' confidence in Cloud.

3.2.3.1 ACCESS TO DATA

Encryption of data is the basis of security for data at rest. One approach for retaining control of data entails requiring the encryption of all personal data in the Cloud. The problem is that encryption limits data use. In particular, searching and indexing the data becomes problematic. For example, if data is stored in clear-text, one can efficiently search for a document by specifying a keyword. This is difficult to achieve with traditional, randomized encryption schemes. Moreover, it makes processing more complex and computationally expensive if data to process is encrypted in the Cloud [102]. Recently, a lot of work has been carried out on tackling this difficulty in order to efficiently process encrypted data. Algorithmic techniques such as [112] process ranked searches of multiple keywords in encrypted data in an efficient manner. Policy-based techniques such as [113] obfuscate data while specifying in a data-sharing policy who can obtain the data and how much of the data is available to them. Decentralized and multi-authority based approaches such as [114], [115] eliminate the burden of heavy communication and the delay of computation to improve scalability and allow more efficient storage while processing encrypted data.

In [116], these various techniques are combined and the computational complexity involved in accessing encrypted data is reduced through the use of reputation assessment of Cloud Computing entities. In this later approach, data is not always encrypted on the trustable Cloud sources and they apply re-encryption if the data owner is not available online.

3.2.3.2 USE OF DATA

In addition to data access control, control over the data lifecycle is necessary [102]. One problem linked to data lifecycle management is data proliferation and unauthorized secondary usage. Once data has been accessed, it is necessary to prevent it from being copied or re-used. The problem is similar for ensuring that deleted data is actually deleted along with its various copies and backups created through data replication [117]. The risk is even more significant for PaaS or IaaS that most often use Virtual Machine (VM)-based resources. Besides the security issues one may encounter on virtual machines such as cross-VM side-channel attacks enabling extraction of information from VMs on the same host, it is also necessary to guarantee that disks that are re-used are wiped correctly to prevent access to data from older machine instances [118].

Among the existing techniques for managing the data lifecycle, Data Coloring [119] and Watermarking [120], provide an interesting approach to data security. Instead of relying purely on encryption or isolation of sensitive data, these techniques limit the impact of a data breach by integrating a security measure within the data itself. Data coloring is a technique that embeds information or color within data without modifying its content and adds data entropy. Digital watermarking is based on data coloring. It is a copyright protection technology, which embeds copyright information in digital production to prevent it from being tampered with or illegally copied. The main idea of watermarking is to introduce small images or patterns into the data to be watermarked without affecting the data subject to normal use. If an illegal copy occurs, the owner of the data can therefore get watermarks from the illegal data to verify his ownership of the data, and even eventually who disclosed the data.

3.2.3.3 ACCOUNTABILITY

Trust in Cloud Computing is also a matter of accountability and auditability. In [121], the authors propose a detective approach to accountability. In their approach, data movements are tracked on three levels: Operating System, File System and Cloud internal network. This enables monitoring of data provenance and ensures data consistency by recording transaction logs.

Accountability is central to a trustworthy Cloud. Without accountability, Cloud consumers will lack confidence to put personal and/or confidential data in the Cloud. Switching to the Cloud model involves changes in control, in Trust and security boundaries and, potentially also in legal regulatory requirements. In [122], accountability is defined by the following attributes:

- Observability is a property of an object, process, or system which describes how well the internal actions of the system can be described by observing the external outputs of the system.
- Verifiability is a property of an object, process, or system that its behavior can be verified against a requirement or set of requirements.
- Attributability is a property of an observation that discloses or can be assigned to actions of a particular actor (or system element).
- Transparency is the property of an accountable system that it is capable of "giving account" of, or providing visibility of, how it conforms to its governing rules and commitments.
- Responsibility is defined as the state of being assigned to take action to ensure compliance with a particular set of policies or rules.
- Liability is the state of being liable (legally responsible).
- Remediability is the state of being able to be remedied.

The authors also mention that an accountable organization has to define governance to responsibly comply with internal and external criteria, particularly relating to treatment of personal data and/or confidential data.

3.2.3.4 EXISTING TOOLS AND RESEARCH PROJECTS

Numerous tools exist that aim to improve security and Trust in Cloud Computing. This section provides a list of some of the latest existing tools and research projects. However, as this is an extremely active topic, it should be considered as a sample of what is currently available or of research directions and definitely not an exhaustive list.

CertiCloud [123] is a method enabling users to certify in a reliable and secure way that the environment they have deployed (typically a Virtual Machine, VM) has not been corrupted, whether by malicious acts or other interferences. This method uses hardware component capabilities and well-known security protocols (Trusted Platform Module and RSA) to offer a secure and reassuring environment. Trusted Platform Module (TPM) is a small tamperproof hardware chip embedded in most recent motherboards that has become a de facto standard component. The basic idea behind TPM is the creation of a chain of trust between all software elements in the computing system, starting from the most basic ones i.e. the BIOS. With TPM, a trusted application runs exclusively on top of trusted and pre-approved supporting software and hardware. The implementation of this method within CertiCloud enables the user to assert the integrity of a remote resource and manage accesses through exchange of a private symmetric key. It also allows users to detect trustfully and on demand any attempt to tamper with the VM they are running. As this approach covers the full deployment and running process it tackles both problematics of access and use of data, at least on the VM side.

Cryptonite [124] is a secure Cloud storage repository that addresses the security and privacy issues of Cloud-hosted data due to the shared infrastructure model and an implicit Trust in the service providers. In this approach, the persistence and availability of Cloud storage is conserved and security is improved while maintaining a good level of performance. Client-controlled security and encryption low key management overhead incurs minimal performance costs. This approach, which supplements CertiCloud, tackles the issues of access and use of data on the storage side.

In [125], Bouvry *et al.* propose a dynamic and flexible signature scheme to verify at runtime the execution of a distributed program and to protect it against flow faults that alter the structure of the application run. This solution encompasses most of the effects of malicious code execution on distributed platforms, such as Clouds. The benefit of this solution is that, when coupled with the aforementioned ones, it enforces security at many levels of the Cloud stack: VM, data and code execution.

In [126], Naqvi *et al.* focus on the study of security assessment in federated Clouds, which is different from a public Cloud in the sense that there are no common security policies and techniques between the machines composing this Cloud. They describe a large set of tools used in their assessment and although it is beyond the scope of this paper to present them all, this approach may be useful as federated Cloud is a type of infrastructure that may be particularly relevant to SMEs.

In [127], Anisetti *et al.* propose a new Trust model grounded on a security certification scheme for the Cloud. This model is based on a multiple signature process including dynamic delegation mechanisms. It aims to support autonomic Cloud Computing systems in the management of dynamic content in security certificates and thus establish a trustworthy Cloud environment. Taking this further, in [128], Ardagna et al. present a detailed list of numerous security tools and techniques available for Clouds for each of the components of Trust.

Finally, according to Gartner, since 2015 Identity as a Service (IDaaS) and Cloud Access Security Brokers (CASB) are rapidly emerging trends. IDaaS and CASB enable IAM to be externalized to the Cloud in the same way that access and use of software is externalized in a SaaS model. With the complexity of dealing

with compliance, data security, threat prevention, and protection and mobility, this model is appealing for many organizations. Still according to Gartner, by 2017-2020, full-featured IDaaS expansion will reach the inflexion point and grow further due to increasing IoT usage and support.

3.2.4 TRUST AS A LEGAL PUZZLE

The dynamic expansion or shrinkage of a Cloud makes it difficult to keep track of what resources are used and in which country. This makes compliance with regulations related to data handling difficult to achieve. Furthermore, it is not clear which party is responsible (statutorily or contractually) for ensuring that legal requirements for personal information are observed, or appropriate data handling standards are set and followed [20]. 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 [129], [130]. Nevertheless, legal constraints exist regarding the treatment of users' private data by Cloud Computing providers. Although privacy laws vary according to jurisdiction, EU countries generally only allow Personally Identifiable Information to be processed if the data subject is aware of the processing and its purpose, and place special restrictions on the processing of sensitive data (for example, health or financial data), whereby the explicit consent of the data owner is part of sufficient justification for such processing [131]. They generally adhere to the concept of data minimization, that is, they require that Personally Identifiable Information is not collected or processed unless that information is necessary to meet the stated purposes. In Europe, data subjects can refuse to allow their Personally Identifiable data to be used for marketing purposes.

Furthermore, it is difficult to determine the exposure of data that is being transferred, because information passing through some countries can be accessed by law enforcement agencies. Not knowing which routes data in transit are taking and the heterogeneity of data regulations across the countries make it very difficult to understand the particular laws which apply. 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.

3.3 TRUST IN BIG DATA

Big Data is a general term that encompasses numerous tasks and subjects ranging from gathering to mining, processing, storing, analyzing, and visualizing data. Implementing a Big Data project involves the application and employment of numerous building blocks and techniques. Many of these coincide with those discussed in previous sections about general ICT and Cloud Computing Digital Trust concepts. A few concepts and challenges related to Trust and security are unique and/or more specific to Big Data which will subsequently be discussed.

Although many powerful technologies exist that were designed to address Big Data issues, there are still many challenges related to data structuring and exploitation that lie in areas such as data accessibility, storage, analysis and security [132]–[134]. If those challenges are not effectively addressed, Trust in Big Data technology cannot be attained.

3.3.1 DATA ACCESSIBILITY

Adequate accessibility of Big Data is essential for Analytics and knowledge discovery. But how can the ever-increasing Big Data Vs (volume, velocity, variety and veracity of data) be handled, especially when the data are poly-structured? Moreover, how can streaming data from multiple sources be aggregated and correlated? Transforming and cleaning such data before loading it into databases for analysis constitute further challenging tasks. New protocols and interfaces are necessary to manage heterogeneous data (structured, unstructured, semi-structured) and sources.

In addition, projections suggest that the growth of data will outpace[34] foreseeable improvements in costs and density of storage technologies, the available computational power for processing it, and the associated energy footprint [35]. Current storage technologies (typically hard disk drives, or HDDs) cannot maintain the same high level of performance for both sequential and random I/O operations simultaneously. This requires a rethink of how storage subsystems for Big Data processing systems should be designed. So, how can large volumes of data be stored to enable timely retrieval? New developments such as solid-state drives replacing HDDs and phase-change memory[35] could improve performance but are probably far from sufficient. In addition, current Cloud technologies do not provide the necessary high performance.

Furthermore, an integral part of any secured IT system is a functioning periodic backup and restoration procedure to assure that data can be restored in case of corruption or other various processing and storage errors. In the case of Big Data, the challenge is greater due to the growing mass of data on physically separated centers, possibly connected with limited bandwidth. The storage platform to handle the heterogeneity and volume of a Big Data backup must itself fulfill similar performance requirements as the processing platform. As a result of the backups themselves, another threat to the conservation of confidentiality arises and the backup must be protected even though it is growing continuously. An initial step toward countering these issues may be to perform a selective backup of the most important data and keep a limited historical record depending on the data type. Also, some data can be efficiently aggregated to save space or anonymized to reduce its value to a possible attacker. A simple but efficient solution could be to limit or cut the backup storage platform's connection to the Internet when it is not needed.

[34] Data traffic grew 56-fold between 2002 and 2009, compared to a corresponding 16-fold increase in computing power.

[35] A type of non-volatile random-access memory that is 500 to 1,000 times faster than conventional (flash) memory and also uses up to half the power.

3.3.2 DATA PROVENANCE AND REPRODUCIBILITY

Provenance with respect to data refers to aspects of storing data origin and operations on data with a view to tracing their history. This has been an important topic in documentation and database systems, enabling us to determine who generated and modified an item or what query and source data were used to extract it [135]. In contrast, provenance is used in scientific research to store the experimental settings, environment and input used to conduct the experiment that created the data. The overall goal being to enable reproducibility of the experiments.

Ram and Liu [136] propose an ontological model of data provenance aimed at meeting the requirements of all areas. They call it the W7 model of *"what", "when", "where", "how", "who", "which"* and *"why"* which can be related to ontological terms (known from psychology) such as event, time, space, action, agents, and things.

The Open Provenance Model[36] [137], [138] provides a framework and a specification that were established through collaborative work, workshops, and community efforts. It seeks to define a general-purpose but also precise provenance model capable of describing the provenance of digital or physical data on different levels. It is based on five types of causal dependencies (relationships) between artifacts, processes and agents as well as roles.

The W3C provides a more complete definition from the PROV[37] working group [139] that borrows similar ideas, such as entities, activities, usage, generation, agents, roles, etc. It defines both textual and graphical representations and can handle almost any possible requirement from representing simple provenance, such as origin and from versioning to querying, reasoning, provenance of provenance and collections.

The ideal representation would allow interoperability of different systems sharing the same representation of provenance. The ISO/IEC 11179-6 standard[38] provides instructions on how a registration applicant may register a data construct and for the assignment of unique identifiers for each data construct. Maintenance of administered items already registered is also specified in this document. Registration mainly addresses identification, quality, and provenance of metadata in a Metadata Registry (MDR).

Furthermore, in some use case scenarios, it is crucial to be able to fetch old data, the most prominent being the case in which Big Data analytics are used for scientific research. Be it biological sequenced DNA, experimental logs or questionnaires of individuals, a researcher must be able to at least repeat the findings at a later time in the future. Research that cannot be repeated or reproduced is of little use and it hampers the possibility of verifying findings and of extending experiments when new data becomes available. A more detailed discussion and definition of repeatability, replicability, reproducibility of scientific experiments is given by Feitelson in [140].

Another case in which data must be reproducible or remain available is when conducting analyses and trending on historical data. To get the full historical picture and most accurate trend models, a larger time window is generally preferable.

In contrast, in cases where real-time data is stream-processed to get an immediate signal or feedback, it is generally not necessary to restore old data.

[36] http://openprovenance.org/

[37] https://www.w3.org/TR/prov-overview/

[38] Information Technology – Metadata registries (MDR) – Registration

Finally, constant efforts are required to assure the confidentiality, integrity and availability of parked data over time. A periodic backup integrity-check and occasional migration of data to new and updated hardware must obviously be performed. In a world of dynamically changing and evolving access policies, managing and maintaining access to and locating old and migrating data has become increasingly challenging.

3.3.3 PRIVACY CONCERNS IN BIG DATA

Privacy is a very important component of Trust for Big Data and Analytics. The ISO/IEC AWI 20547-4[39] standard distinguishes two types of Big Data: open and closed data. While open data relates to Big Data which is publicly available, closed data describes Big Data which is under the control of a single organization or a group of organizations e.g. government or enterprise.

Wu *et al.* [141] clearly make the distinction between shareable and non-shareable data. For example, depending on different specialist applications, the data privacy and information sharing mechanisms between data producers and data consumers can be significantly different. Sharing sensor network data for applications like water quality monitoring may not be problematic and is valuable, whereas releasing and sharing mobile users' location information is clearly not acceptable for privacy concerns.

Moreover, once large amounts of data have been acquired, organizations are subject to compliance issues if it is not managed securely, whether it is open or closed data [62]. The nature of Big Data sources needs to be assessed in order to determine how much they can be trusted. For example, incorporating a source that includes sensitive PII could put an organization's reputation and its customers at risk. Masking private information when performing analyses on terabytes of data is typically disregarded at the outset, although this must be done to meet privacy requirements. One way of achieving privacy without breaking the data value is through anonymization. This can support statistical trending and analysis but support individual privacy when required as proposed in [142].

The outcome of Analytics may in fact itself become corporate intellectual property e.g. it may take the form of essential information for determining the next best action in a new product strategy or revealing company strengths and weaknesses. Either way, such information has to be secured to the same extent as the source in order to avoid putting the organization at risk.

When running deep analytics on individual data that may not seem to invade privacy, conclusions and information can be deducted and extracted that an individual may not have expected. For that purpose, Wu *et al.* [141] state that for privacy concerns, when data is shared, noise and errors can be introduced into the data to produce altered data copies (see Data Sharing section 3.3.4.1).

[39] Information technology – Big data reference architecture – Part 4: Security and privacy fabric. Standard under development.

3.3.4 INFORMATION AND DATA SECURITY

Security challenges relate to the confidentiality, integrity, and availability of Big Data. Once Big Data environments are outsourced to Cloud service providers, several threats and issues become even more severe, such as intellectual property protection, privacy protection, commercial secrets, and financial information protection. At the very least, Cloud vendors must ensure that all service level information security agreements are met. And with Cloud data storage becoming more and more popular, the network bandwidth capacity is the main bottleneck in Cloud and distributed systems that affects the availability of the Big Data environment. Furthermore, in [143], the most prominent Big Data security challenges highlighted are: access control and authentication, secure data management, source validation and filtering, and software and infrastructure security.

When terabytes and even petabytes of data are continuously accumulated, the general information or data security concerns, confidentiality, integrity, availability, authenticity etc. become an even greater challenge than in most Cloud storage cases. There will be times when data needs to migrate to new infrastructures or to be split between more providers while maintaining the mentioned security aspects.

When companies start with Big Data Analytics, they often fail to maintain the same level of data security as in traditional data management environments [144]. The acquired Big Data must therefore be securely stored and checked against intrusion. Some of the data are probably not required and should be properly disposed of. In addition, some of the data sources may come from third parties that require licenses. In order to make sure the organization does not violate rules and regulations, it must check whether and how it is allowed to use the data in the first place and if analytic outputs may be published. Data and Information security awareness is essential to ensuring that everyone in the organization has an understanding of their roles and responsibilities with regard to security. Many international standards provide guidance in this matter. The ISO/IEC 27000-series[40] consisting of various information security standards are a good reference in this context.

3.3.4.1 DATA SHARING

The sharing of data among groups or individuals is another topic which must often be addressed in combination with Big Data solutions and raises questions in terms of security and Trust. An example is a research team that wants to provide partial access to members of another research team. This could be access to data, but also to computation capabilities and tools. Another possible example is external contractors or executives who must only have access to the relevant data.

In addition to obtaining access rights, it must be ascertained whether an individual with access is allowed to grant access to a third individual or group. In [141] Wu *et al.* discuss the problem of data sharing in data mining with Big Data and its impact on privacy if there is a public disclosure of an individual's locations/ movements over time. In their view, in order to protect privacy, two common approaches are to 1) restrict access to the data, such as adding certification or access control to the data entries, so sensitive information is only accessible to a limited group of users, and therefore no sensitive information can be misconducted by unauthorized individuals and 2) anonymize data fields such that sensitive information cannot be pinpointed to an individual record [145] through use suppression, generalization, perturbation, and permutation to generate an altered version of the data.

[40] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435

In another approach [146], Dong *et al.* propose a framework for secure sensitive data sharing on a Big Data platform. This framework secures the whole data processing chain: data delivery, storage, usage, and destruction. It ensures the secure submission and storage of sensitive data based on proxy re-encryption, and guarantees secure use of clear text in the Cloud platform by the use of private space of user processes in virtual machines that can be encrypted. This approach also ensures that data owners have complete control over their data.

In [79], Perera *et al.* also state that one major privacy challenge linked to Big Data and IoT is to develop technologies that request enlightened consent from users sharing the data in an efficient and effective manner. As users have limited time and technical knowledge to engage in understanding the conditions of their consent to sharing their data, this is a particularly challenging goal to achieve. They also stress the importance of users' full control and freedom of choice regarding their data, especially with regard to providing the ability to withdraw or change previous user consents.

3.3.4.2 BIG DATA PROCESSING CHAIN

In addition to the framework proposed by Dong *et al.* in [146], the Big Data processing chain proposed by Pääkkönen and Pakkala [147], depicted in Figure 28 and detailed in Table 19, ensures provenance and security for data from collection through processing to visualization. Each processing step and intermediate storage state as well as transmission needs to comply with security standards to guarantee information security. For further details, a more complete presentation of this Big Data processing chain is provided in [39].

By establishing trusted processing environments, it is possible to partially address information security issues in the Big Data processing chain. These must ensure that data processing takes place in a secure environment, server and network, e.g. by running data analysis on Virtual Machines behind virtual firewalls. Another technique is homomorphic encryption, which is a form of encryption that allows for computations to take place directly on encrypted content (see Section 3.2.3 Technical Challenge for Cloud Computing).

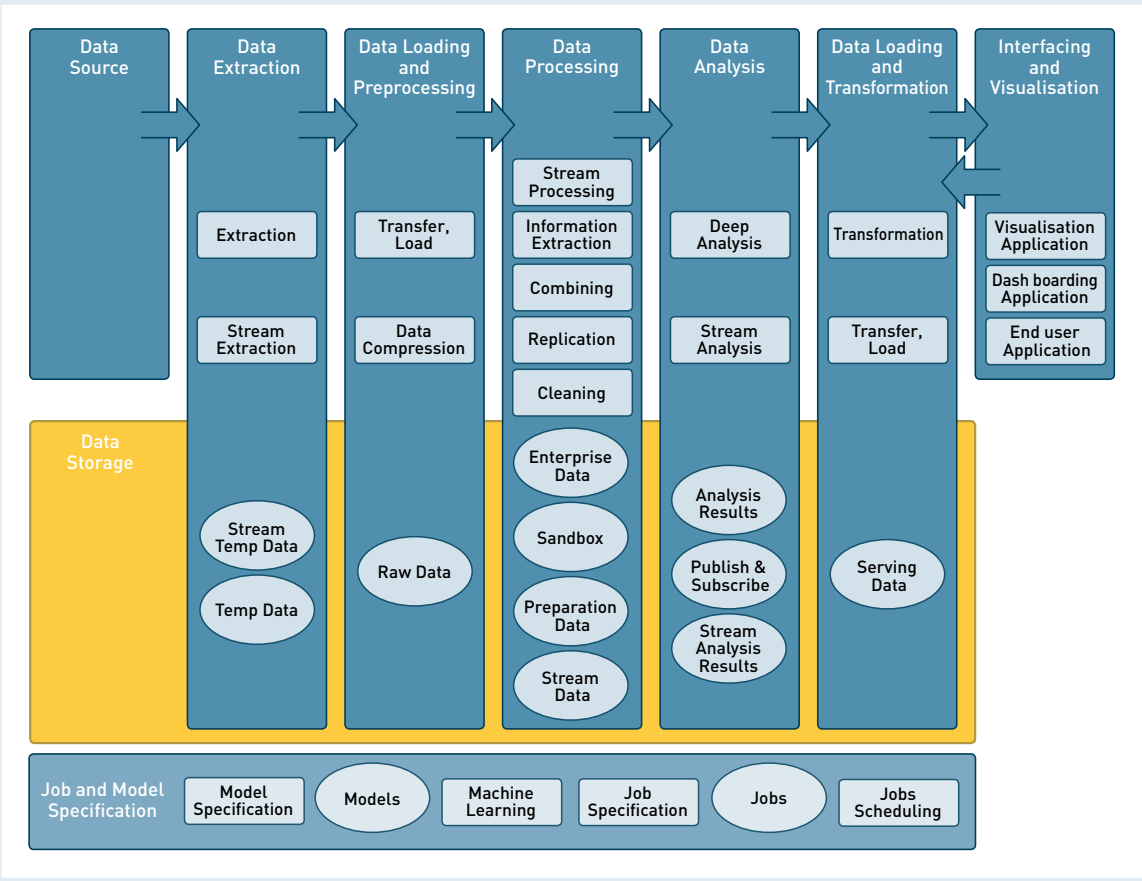


Figure 28 – A technology-independent Big Data Analytics reference architecture [147]

STAGE	DESCRIPTION
1. **Data extraction**	Data extracted from data sources may be stored temporarily in a temporary data store or directly transferred and loaded into a raw data store. Streaming data may also be extracted and stored temporarily.
2. **Data loading and pre-processing**	Data are transferred, loaded, and processed e.g. data compression. The raw data store contains unprocessed data.
3. **Data processing**	Data from the raw data store may be cleaned or combined, and saved into a new preparation data store, which temporarily holds processed data. Cleaning and combining refer to quality improvement of the raw unprocessed data. Raw and prepared data may be replicated between data stores. Also, new information may be extracted from the raw data store for Deep Analytics. Information extraction refers to storing of raw data in a structured format. The Enterprise data store is used for holding cleaned and processed data. The sandbox store is used to contain data for experimental data analysis purposes.

4. Data analysis	Deep Analytics refers to execution of batch-processing jobs for in situ data. Results of the analysis may be stored back in the original data stores, in a separate analysis results store, or in a publish & subscribe store. The publish & subscribe store enables storage and retrieval of analysis results indirectly between subscribers and publishers in the system. Stream processing refers to processing of extracted streaming data, which may be saved temporarily before analysis. Stream analysis refers to analysis of streaming data, to be saved as stream analysis results.
5. Data loading and transformation	Results of the data analysis may also be transformed into a serving data store, which serves interfacing and visualization applications. A typical application for a transformation and serving data store is servicing of Online Analytical Processing (OLAP) queries.
6. Interfacing and visualization	Analyzed data may be visualized in several ways. A dashboarding application refers to a simple UI, where key information is typically visualized without user control. Visualization application provides detailed visualization and control functions, and is realized with a Business Intelligence tool in the commercial sector. An end-user application has a limited set of control functions and may be realized as a mobile application for end users.
7. Job and model specification	Batch-processing jobs may be specified in the user interface. The jobs may be saved and scheduled with job scheduling tools. Models/ algorithms may also be specified in the user interface (model specification). Machine learning tools may be utilized for training of the models based on new extracted data.

Table 19 – Functional areas of a Big Data Analytics infrastructure [147]

Generally, encryption is used to achieve security objectives, both for data in-rest and in-move. In the case of Big Data, it is even more important to set up an authentication framework that functions across all platforms involved in the processing chain.

3.3.5 ACCESS AND POLICY MANAGEMENT TECHNIQUES

In addition to the existing IAM techniques presented earlier in this chapter in Section 3.2 on Cloud Computing, the eXtensible Access Control Markup Language[41] (XACML) is of interest for the context of Trust in Big Data [148]. This is an OASIS standard designed as a common policy expression language allowing enterprises to manage the enforcement of all the elements of their security policy in all the components of their information systems. XACML describes a declarative fine-grained, attribute-based access control policy and encourages the separation of the access decision from the point of use.

The major actors in the XACML dataflow are shown in Figure 29.

[41] https://www.oasis-open.org/committees/xacml

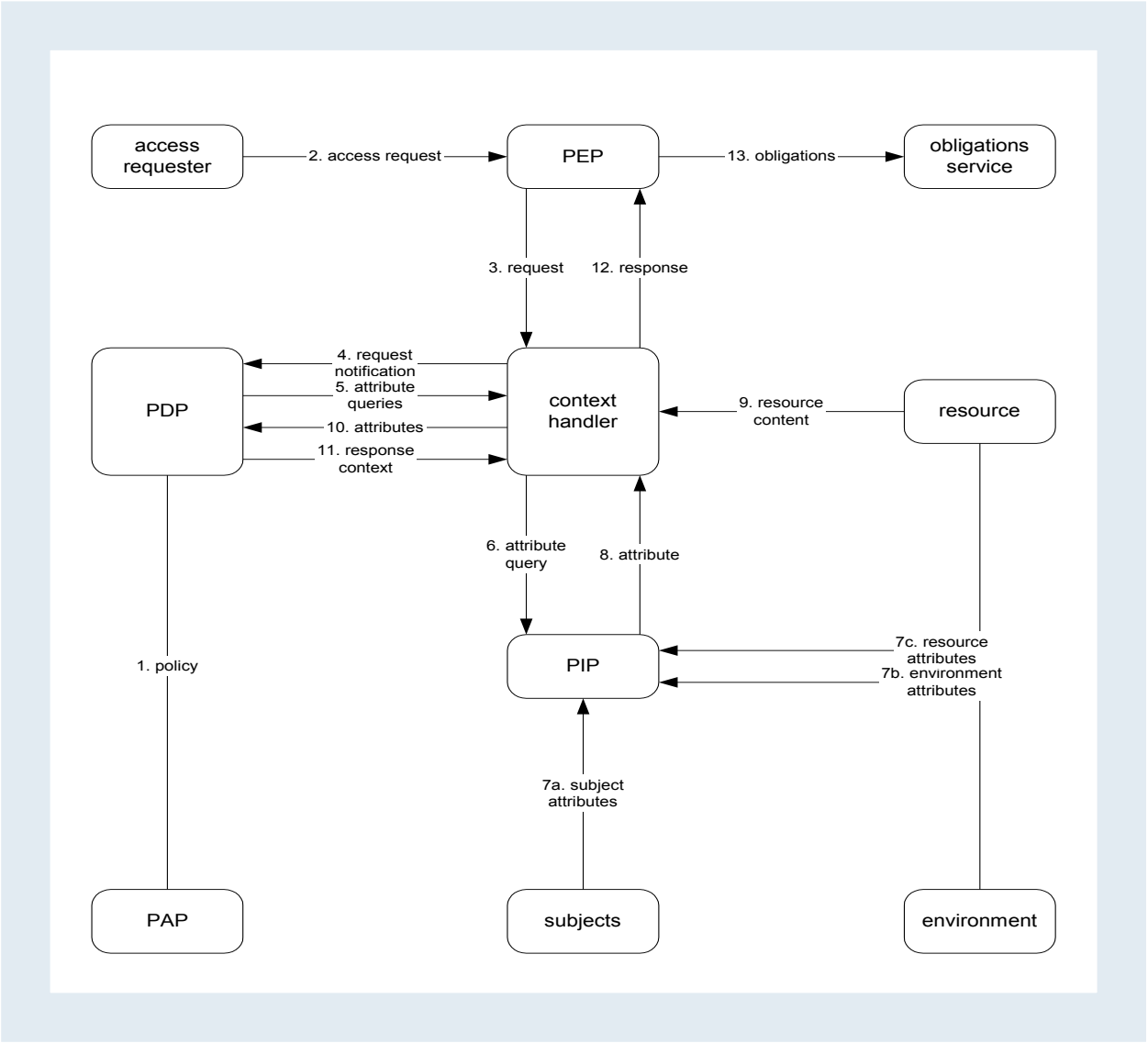


Figure 29 – XACML Dataflow [148]

Among the different actors present in this XACML Dataflow Figure, the acronyms are defined as follows:

- PAP: Policy Administration Point
- PDP: Policy Decision Point
- PEP: Policy Enforcement Point
- PIP: Policy Information Point

XACML is structured into three levels of elements: policy sets, policies, and rules. A policy set can contain any number of policy elements and policy set elements and policies are themselves defined by one or more rules that can be exchanged and applied according to predefined algorithms. Rules consist of the following components: a target, an effect, a condition, obligation expressions, and advice expressions. The following is an XACML Dataflow:

1. A user sends a request which is intercepted by the Policy Enforcement Point (PEP).
2. The PEP converts the request into an XACML authorization request.
3. The PEP forwards the authorization request to the Policy Decision Point (PDP).
4. The PDP evaluates the authorization request against the policies it is configured with. If needed it also retrieves attribute values from underlying Policy Information Points (PIP).
5. The PDP reaches a decision (Permit / Deny / NotApplicable / Indeterminate) and returns it to the PEP.

XACML can be interoperated with the Security Assertion Markup Language (SAML), an OASIS data format for exchanging authentication and authorization data between an identity and a service provider and also with OAuth, an authentication standard for interfacing different systems without using credentials.

Finally, the large amount of data involved also raises the question of scalability when dealing with Big Data analysis. The selection of an appropriate model for large-scale data analysis is critical. Furthermore, although the Big Data Vs are increasing at an exponential rate, the improvement of information processing methods is relatively slower. For real-time Big Data applications such as financial marks, social networks, traffic navigation, and transport systems, timeliness is a top priority. The need to process continually increasing amounts of disparate data is one of the key factors driving the adoption of Cloud services.

3.4 TRUST IN INTERNET OF THINGS

Many new challenges have emerged with respect to Trust as a result of an increasingly connected world. A lot of these challenges are related or similar to the challenges of Cloud Computing and Big Data and the ones that are more specific to Trust in Internet of Things can to a large part be attributed to one of these general points:

- Ability to turn off sensors and devices to give the users definitive control over what and who is being monitored when, e.g. cameras and voice recording, etc.;
- To acquire user consent and present privacy policies per use case and per access;
- Guarantee anonymity of users, their IDs, and more challengingly, the anonymity and consent of non-users;
- Communication security on the simpler devices that may not have enough power or processing capabilities to ensure costly encryption for all connections;
- New threats: physical tampering with devices and a new set of attack surfaces.

Additional security challenges identified by Cisco[42] that are also important to mention are:

- Secure remote management during and after device onboarding (i.e. connection and inclusion in a network);
- Crypto Resilience – Embedded devices may outlive algorithm lifetime;
- Tamper Detection techniques and design.

Further threats identified by Cisco include:

- Common worms jumping from ICT to IoT: Worms generally limited to running on consumer OS (Windows, Linux, iOS, Android) could harm IoT infrastructure and devices;
- "Script kiddies" or others targeting residential IoT: Unprotected webcams, stealing content, breaking into home control systems;
- Organized crime: Access to intellectual property, sabotage, and espionage;
- Cyber terrorism: Nuclear plants (with e.g. Stuxnet virus), traffic monitoring, railways, critical infrastructure.

An in-depth analysis of threats, impact and mitigation related to the continued operation of an IoT system can be found in the ETSI report "Threat analysis and counter-measures to M2M service layer"[43]. The remainder of this section will take a more detailed look at the different issues related to Trust in the Internet of Things and proposed countermeasures.

3.4.1 PRIVACY, ANONYMITY AND CONSENT

It is apparent that the topics of Privacy, Anonymity and Consent in IoT share many of the same problematics as discussed in the context of Big Data. Whether the personal data is generated by the users themselves through their interactions with systems and services or if they originate from sensors and things used by the users, it poses many of the same security issues. Once personally identifiable data have entered the data processing pipeline, many of the possibilities and risks are the same. Taking the broader definition in Box 2 into account, most data can be attributed with an IoT origin making the overlap even more pronounced.

[42] http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
[43] http://www.etsi.org/deliver/etsi_tr/103100_103199/103167/01.01.01_60/tr_103167v010101p.pdf

Minch [80] discusses privacy issues in a connected world, most prominently related to location and identification. In Table 20 the different phases of information flow are listed and Table 21 shows proposed or implemented measures to counter the unwanted information flow.

PHASE OF INFORMATION FLOW	EXAMPLE COMPONENTS/METHODS
Sensing	Triangulation Scene analysis Proximity Indirect inference
Identification	Unique identifier detection Facial recognition Vehicle license plate recognition
Storage	Object data Meta data
Processing	Self-contained inferencing Communication and matching Advanced pattern recognition and data analytics
Sharing	Intentional Unintentional
Use	Intentional Unintentional

Table 20 – Internet of Things information flow [79]

PHASE OF INFORMATION FLOW	EXAMPLE TECHNICAL PRIVACY CONTROL	EXAMPLE SOCIAL PRIVACY CONTROL	EXAMPLE LEGAL PRIVACY CONTROL
Sensing	RF blocking wallets RFID blocker tags	Socially acceptable uses for Google Glass	Prohibition of cell phone and camera use at customs
Identification	MAC address randomization in Apple iOS 8	Anonymous letters to newspaper editors or postings to online discussion forums	"Secret" ballots for voting
Storage	No physical storage Encryption Ephemeral storage	User social media privacy settings	Formal limits on amount and duration of stored data

Processing	Privacy-enhancing technologies: Anonymizing, etc.	Vendor-customer terms of service	Restrictions of database matching
Sharing	Restriction or non-provision of communication facilities	User and application sharing settings	The "right to be forgotten" Data broker restrictions
Use	No provision for input into applications	Accepted business practices and standards such as EPC guidelines	Prohibition of discriminatory use

Table 21 – Internet of Things example privacy measures [79]

Almeida *et al.* [48] argue that in order to protect individuals' personal data and to build their Digital Trust in the IoT infrastructure, legal data protection frameworks must be amended. Measures should relate to at least:

- Data caps – limits must be set on the amount and nature of the personal data collected. Not all data that can be collected must be collected.
- Notice and choice – increase individuals' awareness of data collection processes. Preferable, a statement and a menu with choices is presented to decide how the collected data will be handled, if any.
- Privacy by design – companies that manufacture IoT devices must build adequate security and privacy elements into the devices, including authentication and authorization procedures, validity checks, and data verification.
- Accountability – personal data monitored by IoT devices must be accessible at all times to the owner of the data so s/he can exercise the right to update or delete it.
- IoT ecosystem – clear indications regarding responsibility for data treatment in the IoT ecosystem. One possibility may be to introduce trusted third parties (ideally located outside an IoT ecosystem).

The authors also suggest that in addition to security and privacy issues, several other IoT problems (such as the lack of standard interoperability protocols) could be tackled through the implementation of IoT-related governance mechanisms, as already occurs with the Internet in general. This involves multi-stakeholder groups of the existing Internet governance ecosystem (IETF, ICANN, RIRs, ISOC, IEEE, IGF, and W3C). All steps should be taken to design IoT with people in mind, as privacy and ethics are not natural aspects to be considered in technology agendas. If this focus is not accomplished, it will be very hard to achieve the required Digital Trust in an IoT ecosystem.

Regulations would also be a prerequisite as it is impossible for a user to control, or even be aware of what secondary information can be extracted from his primary information. If, for example, a user charges his/her credit card every weekend in the same type of places, one would be able to deduct his/her leisure activities, and correlated with other card operations, find out with whom. If his/her location changes regularly from inside to outside, the user might be a smoker. If he/she spends time near a place of worship or is active during a particular religious holiday, it is possible to deduct the user's religious orientation.

This may seem harmless, but such information used with the wrong intentions may pose serious threats to quality of life. It could be used by a bank or by an insurance company to assess whether or not to engage in a contract with the person and under what terms. Or by malicious groups for creating black lists, etc. Efficient protection of users from secondary uses of personally identifiable data is a major challenge to be addressed on all levels, from hardware to standards and legislation. User consent in this context goes further than simply allowing access to personal data or not, and must address items such as a timeframe, context and the type of analytic result to be extracted.

3.4.2 ATTACK SURFACES AND THREATS

In [52], an industrial production environment perspective is depicted with a focus on threats in Cyber Physical Systems (CPS) and Cyber Physical Production Systems (CPPS). To a large degree, a CPS system can be regarded as analog to IoT, though the term specifically implies that software-controlled physical activity is involved. Typically, CPS is mentioned in the context of Industry 4.0 and smart factories (i.e. intelligent IoT and Big Data-assisted industrial production environments).

As these smart factories increasingly depend on devices in the production chain that are interconnected and centrally managed, numerous new attack surfaces may emerge and be identified. This is due to the security and safety-critical functionality as well as privacy-sensitive information transmitted by the connected devices or "things" (see Figure 30).

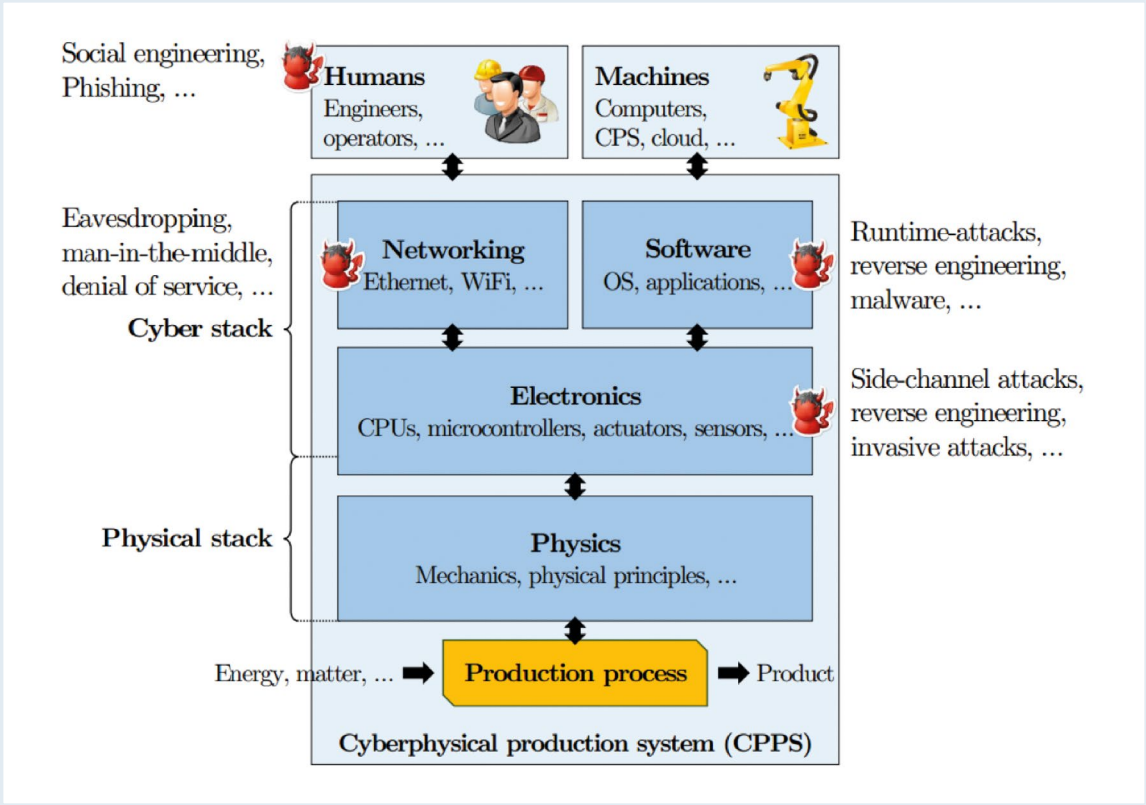


Figure 30 – Cyber Physical Production System (CPPS) architecture and attack surfaces [52]

As for many IoT systems, thorough security architectures can be too complex to handle the embedded devices. One method of building Trust and building a secure network is through Integrity Verification of so called prover devices by verifier devices through attestation. Here, achieving swarm verification of large self-organizing heterogeneous networks of devices is identified as an open research problem. The authors further argue that low latency processing may be required to enable seamless device pairing without user interaction by sampling and correlating environmental characteristics. This, on the other hand, poses privacy concerns and technical difficulties if such processing takes place in a Cloud environment, hence local analytics seem to be a better solution, though processing and storage power and capacity may then become a limitation.

3.4.3 SMART HOME SECURITY

The threat landscape of a smart home is thoroughly elaborated by the ENISA report [149]. An overview of the threat landscape in the report is shown in Figure 31. It shares the attack vectors of a CPS and extends with only a few issues mainly related to the home inhabitants, such as: DRM issues, hoaxes and abuse of personal data.

ENISA discussed several issues that can be attributed to smart homes in particular:

- Smart Homes rely on assets, such as smartphones, tablets, removable storage media, and computers which are more susceptible to voluntary and unintentional damage or even theft.
- Administration of a complex system with multiple devices and technologies may lead to erroneous use or poor integration of devices and sloppy security configurations.
- Inadequate design and planning are key issues for smart homes as they involve a continuously evolving patchwork of devices from third party providers.

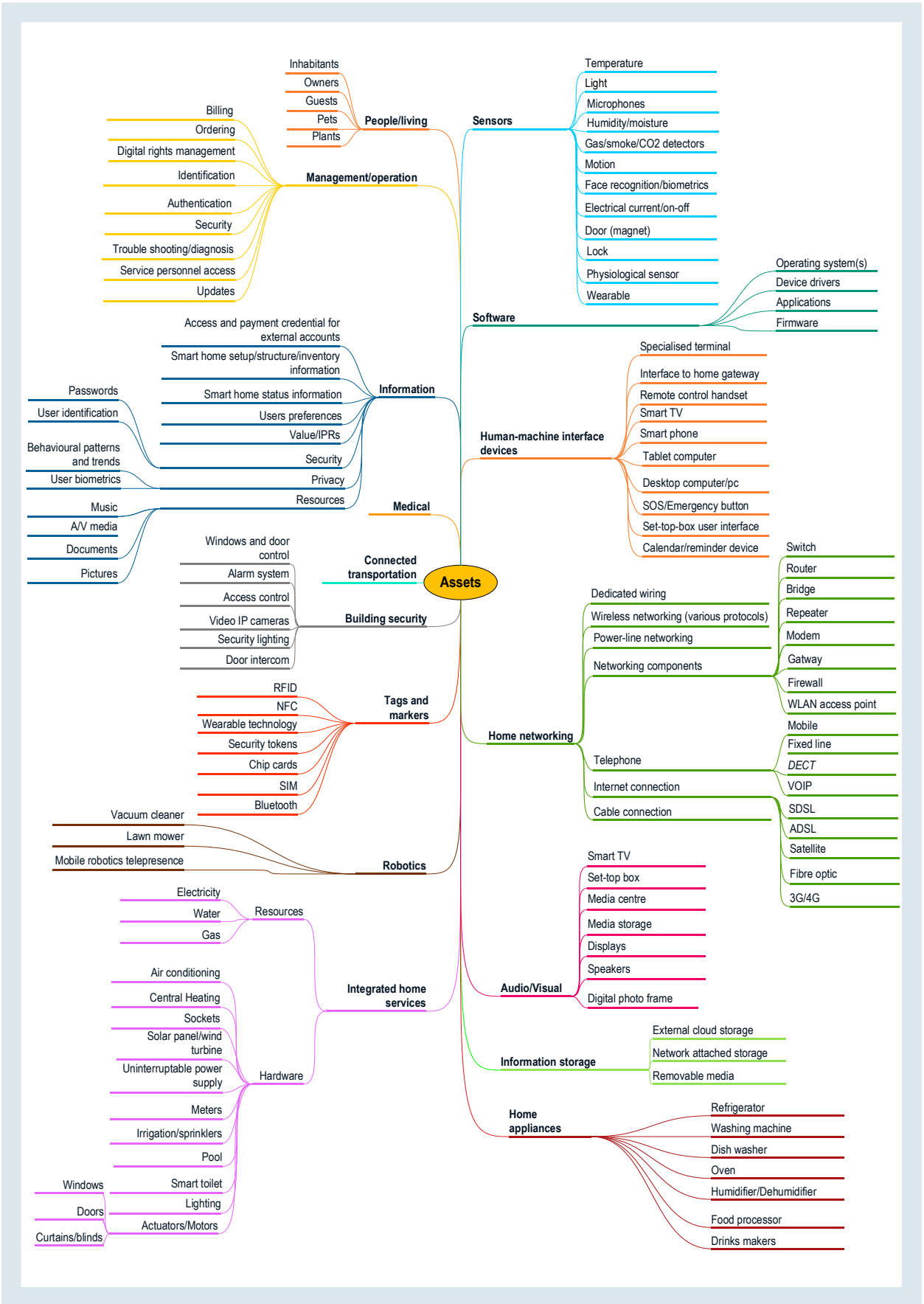


Figure 31 – Overview of Threats Assumed for Smart Home Assets [149]

Another threat highlighted specifically for smart homes, but also smart buildings in general is the absence of personnel. In most cases, the administration of a building or the advanced use of features is limited to a few people. This may pose a severe limitation and maybe even a safety risk for other building users if this key-person is absent in combination with unexpected needs or system failures. The consequences may be harmless, such as an inability to start the video entertainment system or get the car out of the garage, but may be as severe as a climate control malfunction or being trapped inside parts of the building.

In such cases, or if the building administrator loses system access, manual overwrite or reset is required. The implementation of such a mechanism will inevitably itself become a new attack surface for the system and much attention must be paid to incorporating security into the design from the beginning.

3.4.4 SECURITY IN EMBEDDED DEVICES AND REAL-TIME PROCESSING

Most tiny embedded devices which are found anywhere from home devices to industrial and production equipment include a microcontroller and an embedded real-time Operating System (OS). With the advancement of Industrial IoT (IIoT), Industry 4.0 and IoT in general, these devices are becoming increasingly connected, which adds an extra dimension to the security challenge. They are becoming more important and crucial for production, safety and well-being, and at the same time they become subject to attacks whose severity magnifies with the importance of the devices.

To address this issue, several works propose frameworks that both provide a Trusted Computing Base (TCB) for secure processing and computations on the device, while simultaneously maintaining real-time guarantees. The latter is typically of immense importance in all control applications where a response to a physical system state must be immediate and the unguaranteed millisecond range delay of operating systems is not sufficient. Real-time processing and timing can also be of importance when reading a sensor whose readings vary over time and need to be correlated with other readings without dropouts, for example for triangulation or diagnostics.

Existing TCB implementations typically produce a processing overhead that may limit the real-time characteristics of the resulting system. Self-protecting modules (SPMs) are proposed in [150] and require minimal hardware support for memory access control to be implemented. Trusted subsystems can then share the same processor and memory space, while still maintaining solid security properties. This includes strong isolation guarantees between subsystems, and high assurance on the confidentiality of subsystems' private data.

The SPM framework as proposed, however cannot protect against malicious modules that flood the network or overload the CPU to reduce other modules' availability nor guarantees that the execution within the SPM is never interrupted.

TyTAN [151] is a low-end embedded system that provides (1) a hardware-assisted dynamic root of Trust, allowing secure task loading at runtime; (2) secure Inter-Process Communication (IPC); (3) local and remote attestation; and (4) real-time guarantees.

In the TrustLite framework [152], an Intel-backed System on Chip (SoC) solution enforces access control for all memory operations. TrustLite enables features like remote device management, authentication, secure Over the Air (OTA) updates, and remote attestation to embedded devices, regardless of OS and application.

In [153], the authors report on their work-in-progress towards extending a Protected Module Architecture (PMA) for small microprocessors with availability and real-time guarantees even on a partially compromised

embedded system. By making SPMs interruptible, they are able to serve individual Interrupt Requests (IRQs) to react immediately to outside events. In addition, the SPMs can also be executed interleaved by the scheduler to allow strict timed real-time processing in parallel executed modules.

3.4.5 TRANSMISSION ENCRYPTION AND SECURITY

To encrypt the communication between IoT devices and IoT gateways, a broad range of mature technologies are available that are not necessarily related to IoT. It is beyond the scope of this White Paper to go into detail and therefore only a brief introduction is provided.

3.4.5.1 ENCRYPTION METHODS

The most widespread symmetric key methods for actual encryption of data and communication (i.e. server and client obliged to share a common key) are Data Encryption Standard (DES)[44], Triple DES (3DES)[45] and Advanced Encryption Standard (AES)[46] in 128-, 192-, and 256-bit versions.

To share and exchange the common key, a posterior handshake and identity validation procedure typically takes place relying on an asymmetric or public-key encryption and certification scheme, such as the well-known RSA algorithm and the IETF X.509[47] standard.

3.4.5.2 CRYPTOGRAPHIC NETWORKING PROTOCOLS

This section will briefly list and describe a number of key cryptographic networking protocols. These are then organized into the four abstraction layers of the TCP/IP model[48] where they operate: application layer, transport layer, Internet layer and link layer.

1 APPLICATION LAYER SECURITY

In the upper-most application layer, the most widely used protocol is Transport Layer Security (TLS)[49], the successor of Secure Sockets Layer (SSL). TLS encryption is symmetric, based on initial asymmetric (with a certificate) encryption using a handshake to exchange a shared secret. DTLS denotes an analog specification dealing with the particularities of running TLS over UDP.

Other well-known examples of encryption protocols that can be assigned to this abstraction level are protocols such as SSH or FTP over SSH (SFTP) as well as FTP and HTTP over SSL/TLS (FTPS and HTTPS).

This layer is also where most of the messaging protocols discussed below in Section 3.4.6 reside.

[44] https://en.wikipedia.org/wiki/Data_Encryption_Standard
[45] https://en.wikipedia.org/wiki/Triple_DES
[46] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[47] https://tools.ietf.org/html/rfc5280
[48] https://tools.ietf.org/html/rfc1122#page-8
[49] https://tools.ietf.org/html/rfc5246

2 TRANSPORT LAYER

For the sake of completeness, this layer comprises TCP and UDP protocols, though these do not contain any security measures.

3 INTERNET LAYER SECURITY

IPsec offers end-to-end encryption operating in the layer below TCP and UDP among IPv4, IPv6 and ICMP protocols. It supports the transport mode, as well as a network tunneling mode. While the latter encrypts the entire package and is often used for VPN tunnels, the former only encrypts the payload. IPsec supports encryption with standard AES and 3DES.

4 LINK LAYER SECURITY

Link-layer security is an approach where data encryption and decryption occurs in the link hardware when transmitting between two points within a network. The main advantage is that encryption occurs automatically without the application's intervention. However, communication is decrypted at each link, which poses security issues when a link (e.g. a router) cannot be trusted. Examples of security protocols on the WiFi-link layer include WEP, WPA and WPA2.

3.4.6 SECURITY IN IOT FRIENDLY MESSAGING PROTOCOLS

Many protocols exist with different features and different purposes. A number of these are more suitable for IoT purposes and some were specifically designed with IoT use cases in mind. Typical challenges in IoT environments are:

- Limited device capabilities in terms of processing and storage.
- Remote networks with many hops, packet loss and low bandwidth.
- Device discovery and ad-hoc networking.
- Broadcasting or multi-cast capabilities.

These points hinder security measures rather than aiding them, especially the first. In addition to the protocols presented below, these message-passing protocols are not discussed further: XMPP, AMQP and STOMP.

3.4.6.1 MQTT

The Message Queuing Telemetry Transport (MQTT)[50] protocol in version 3.1.1 is described by the standard ISO/IEC 20922. It is a lightweight, open, simple and easy-to-implement protocol based on a Client/Server publish/subscribe mechanism allowing one-to-many message distribution. It can run on top of the TCP/IP protocol or other protocols fulfilling the requirements of ordered, lossless and bi-directional network communication.

It is designed for connections with remote locations where a "small code footprint" is required or the network bandwidth is limited and is hence less suitable for high-throughput real-time applications.

[50] https://www.oasis-open.org/committees/mqtt/

MQTT supports two encryption modes which can each be either asymmetric or symmetric:

- End-to-End (E2E) where only the packet meta-data is readable by untrusted parties.
- Client-to-Broker lets a broker decrypt the package and publish it to subscribers, in which case TLS is strongly recommended.

3.4.6.2 COAP

Defined in RFC7252, the Constrained Application Protocol (CoAP)[51] is a specialized web transfer protocol for use with constrained nodes and constrained (e.g. low-power, lossy) networks using UDP as the transport protocol. CoAP provides a request/response interaction model between application endpoints, supports built-in secure discovery of services and resources, and includes key Web concepts such as URIs, multicast and Internet media types.

CoAP supports the following DTLS-enabled security modes: *PreSharedKey, RawPublicKey* and *Certificate*. If a device does not use DTLS, then *NoSec*, a **token** included in the header is used to match request and response. The token is randomly generated by the client and must be re-transmitted unmodified with a response.

3.4.6.3 M3DA

The *Mihini* agent in the M3DA protocol is a software component that acts as a mediator between an M2M server and the applications running on an embedded gateway. M3DA[52] is a protocol optimized for the transport of binary M2M data enabling device and asset management by easing the manipulation and synchronization of a device's data model, and allowing user applications to exchange typed data/commands back and forth with an M2M server.

Each client/server couple defines a common password that is transformed by a hash function (such as MD5) to a server and client key. A keyed-hash message authentication code (HMAC) is generated and included with the message for authentication. This authenticates the communication, but the payload of the messages themselves is not encrypted unless the protocol is run on top of a secured transport protocol like TLS.

3.4.6.4 DDS

Data Distribution Service (DDS)[53] describes a Data-Centric Publish-Subscribe (DCPS) model for distributed application communication using typed interfaces, rather than raw text or binary data that needs to be interpreted. The target is real-time applications with minimal resource overhead and DDS communication can be efficiently secured by means of authentication, access control and cryptographic plugins. The framework offers great flexibility in the sense that many types of authentication are supported (handshake, shared secret, etc.).

[51] https://tools.ietf.org/html/rfc7252
[52] https://wiki.eclipse.org/Mihini/M3DA_Specification
[53] http://portals.omg.org/dds/

3.4.7 AUTHENTICATION / SECURE PAIRING

This topic is partially related to identity and policy management discussed in Section , but in the context of IoT, authentication extends to the right to access and reconfigure devices or change device states. The challenge is to ensure that no compromised devices are accepted into the network, ensuring that any device integrated in the system is the correct one. Traditional existing IT solutions for security pairing, based e.g. on passwords, trusted certification authorities, or physical connection, are not feasible when devices have no interfaces for inputting passwords or secrets keys. Thus, for such cases the pairing of IoT devices must be achieved differently.

As stated by Sato *et al.* in [154], IoT devices generally communicate by using simple wireless communications such as Bluetooth and NFC whereby very basic pairing occurs and device authentication and registration are often performed by a device-id. Therefore, the connection protocols must adopt a higher security scheme than this basic registration method. Furthermore, the aforementioned method is tedious for a large amount of devices and actually poses a security risk if someone interferes during the pairing process (e.g. with a Man in the Middle attack type, MITM).

More secure authentication and pairing can be achieved with the conjunction of smartphones serving as mediators to establish security associations [155] between several IoT devices, by entering a pairing mode by pressing a physical button and scanning for such devices, or by local wireless channel such as Bluetooth Low Energy (BLE) to pair the IoT device with a base station or a smartphone [156].

In [157], NIST proposes a set of guidelines for securing Bluetooth connections, authentication and pairing. Secure pairing must be achieved by generating a secret symmetric key, called the "link key". Depending on the security level chosen in the Bluetooth protocol, the link key can be initiated with a PIN number, Secure Simple Pairing (SSP), or AMP Link Key Derivation.

The PIN number is the simplest pairing method where a digital key (at least 16 bytes) must be entered in one or both devices being paired, depending on the device type.

SSP provides four association models:

- *Numeric Comparison* which is similar to PIN pairing. However, in this model the PIN itself is not used as a key. Instead, the link key is generated with this PIN and the device ID. Therefore, an eavesdropper who is able to view or capture the key value could not use it to determine the resulting link or encryption key.
- *Passkey Entry* is similar to numeric comparison but for the case where only one device has input capabilities and the other one has display capabilities. As for Numeric Comparison, no MITM attack is possible because of the independence between the PIN and the link key.
- *Just Works* simply asks one device to accept the pairing and thus provides no MITM protection.
- *Out of Band* (OOB) was designed for devices that support a common additional wireless/wired technology (e.g. Near Field Communication or NFC) for the purposes of device discovery and cryptographic value exchange. In the case of NFC, the OOB model allows devices to pair by simply "tapping" one device against the other, followed by the user accepting the pairing via a single button push. It is important to note that to keep the pairing process as secure as possible, the OOB technology should be designed and configured to mitigate for eavesdropping and MITM attacks.

AMP link key derivation is a security model which uses AMP (Alternative Mac/Phy address). AMP describes the ability of Bluetooth devices to have two physical addresses: one for device discovery, initial connection and profile configuration and one for data transport. This model uses these two addresses to generate the link key.

Once pairing is completed, authentication is also achieved using the link key. This secret key is derived during pairing and should never be disclosed outside the Bluetooth device or transmitted over wireless links. However, the link key is passed in the clear from the host to the controller (e.g. PC to USB adapter) and the reverse when the host is used for key storage, which might lead to a security threat if one of the devices is corrupted.

Digital Trust is a complex but necessary goal to attain. In order to provide guidance to meet this challenge, the next chapter presents the standardization work and organizations related to Digital Trust for smart technologies. In the jungle of research projects and existing tools, only standardization built on a consensus between experts in the field can provide the proper guidance that will enable this challenge to be leveraged.

4 STANDARDIZATION TO LEVERAGE DIGITAL TRUST

In this White Paper, Digital Trust for Smart ICT is mainly focused on the appropriate utilization (including accountability, security, privacy, reliability) of private digital data to benefit and protect those to whom the digital information pertains. Standards and Technical standardization can help establish and maintain Digital Trust in relation to current and future Smart ICT technologies for example by setting up appropriate information security management systems, a transparent model that specifies what and how data is sourced and from whom, data governance and management, providing common communication protocols allowing the interoperability between the different applications and technologies, preventing vendor lock-in, etc.

On the basis of the principles of transparency, openness, impartiality and consensus, and effectiveness and relevance, technical standardization and standards can provide the tools, techniques, guidelines, and assessment grid necessary to build and nurture the relationship between trustor and trustee. This is necessary for defining a framework providing not only the confidence in the expectations and responsibilities around Digital Trust, but also for providing the mechanism for assessing the validity of commitments, what is advertised as a service and what is recommended. One example pertaining to Cloud Computing is the international standard *ISO/IEC 27018:2014*[54] that focuses on protection of privacy of personal data in the Cloud. This standard should reassure Cloud users that their service provider is well placed to keep data private and secure and help foster transparency in cloud provider privacy practices, while advancing stronger protections for customer data in the Cloud. Another example relating to Cloud Computing is ISO/IEC 27017:2015 that will strengthen the relationship between customers and service providers by helping service providers to reach a common understanding with their customers regarding adequate security controls and guidance on their implementation.

Standardization is an efficient and economical tool offering the possibility of pursuing various objectives such as: mutual understanding, satisfying customers' expectations and requirements, reducing costs, eliminating waste and improving efficiency, compatibility, security, performance, quality and reliability, convenience of use, trade, economic performance, accessing the latest knowledge and state-of-the-art solutions, providing positive perception and reputation of business.

Standards are established by consensus and approved by recognized Standards Developing Organizations (SDOs) consisting of:

- Formal standards bodies that are organizations benefiting from a broad recognition and meeting the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Committee agreement *Code of Good Practice for the preparation, adoption and application of standards.* Their primary activities are to develop, coordinate, promulgate, and produce *de jure* (formal) standards. On a European level, there are three formal standards organizations: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). These are officially recognized by the European Union. All three have cooperation arrangements in place with their broadly recognized counterparts: the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). In addition, there are several formal standards bodies working at national level. In this context, ILNAS[55] is recognized as the national standardization organism for Luxembourg.

[54] http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[55] http://www.iso.org/iso/about/iso_members/iso_member_body.htm?member_id=1776

- Private standards bodies, commonly referred to as *"consortia"* or *"fora"* for the ICT sector. In the context of standardization, these are organizations that include individuals, companies, associations, or governments with the common objective of participating in the creation of technical specifications or *de facto* standards, meaning these standards are widely recognized in the market. The main difference with formal standards is that these organizations are not necessarily seeking to engage with all interested parties and the specifications they produce are not systematically made available for public enquiry. In many cases, these private standards bodies set out to address or resolve only a limited number of specific issues. Examples of very well-established consortia include the Institute of Electrical and Electronics Engineers (IEEE), oneM2M, the Cloud Security Alliance (CSA), and the Organization for the Advancement of Structured Information Standards (OASIS).

When building standards, SDOs generally ensure that several conditions are met. Firstly, a standard must be based on a consensus among a group of designated experts. Then, if the scope of the standard under development has a potential impact or interest to other expert groups or standardization organisms, a *liaison* is made to prevent overlapping and contradiction. Finally, in the interest of all, standards highlight major requirements and guidelines and do not impose a particular constraint or technology. In that sense, standardization provides the most impartial and technically sound vision available on a particular subject. Thus, for professionals or researchers seeking guidance, standardization is a powerful support that must not be neglected.

This chapter will thus present how standardization bodies and committees are organized and interlinked. As ISO/IEC is the main standardization body for Smart ICT topics, this chapter focuses specifically on ISO/IEC. However, where relevant, the work of other technical standardization bodies will also be presented.

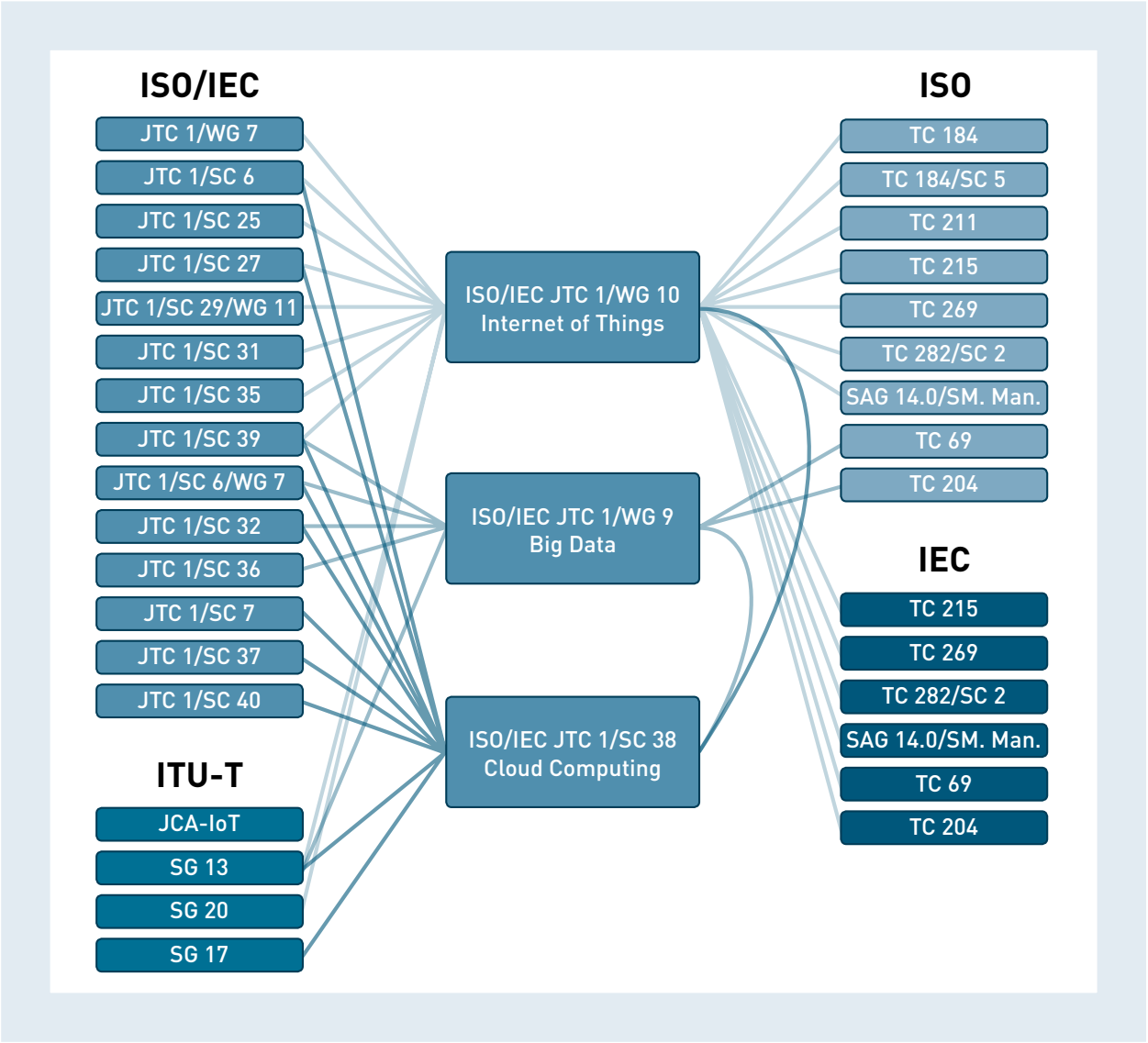


Figure 32 – Common Liaisons of WG 9, WG 10 and SC 38

The Smart ICT topics of Cloud Computing, Big Data and Internet of Things discussed in this White Paper overlap in a number of areas. Therefore, it is no surprise that the corresponding ISO/IEC JTC 1 (also referred to as JTC 1 in this document) committees and working groups, namely SC 38, WG 9 and WG 10, collaborate with each other and with many of the same standardization bodies. In Figure 32, the internal and external liaisons of WG 9, WG 10 and SC 38 are shown, omitting 1, 14 and 9 external liaisons respectively, which are not shared. The exception being The Open Group (TOG) which is a shared liaison of both WG 10 and SC 38. It is clear that the three topics are closely related and a clear separation into respective standards cannot be defined.

This chapter will provide further details of standards that are relevant to Digital Trust for Cloud Computing, Big Data and IoT, and also in a broader sense, to the Smart ICT topics discussed. Since the standards landscape is wide-ranging, only a selection of the most relevant standards is provided below. For further details, the reader is invited to refer to the standards analysis for the ICT sector in Luxembourg[56] [158].

[56] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes-nationales/pub-standards-analysis-ict-v6-0/standards-analysis-ict-6-0.pdf

4.1 CLOUD COMPUTING STANDARDIZATION TECHNICAL COMMITTEES & STANDARDS

The standards landscape for Cloud Computing is extensive, since many standards developing organizations are active in the Cloud Computing subsector and many standards and specifications have been developed. As specified by the European Commission in its European Cloud Computing Strategy[57], it is necessary to cut "through the jungle of standards" in order to identify existing solutions, market needs and, finally, to increase Cloud Computing adoption.

Rashmi *et al.* [23] argue that to achieve interoperability among Clouds and to increase stability, security, and Trust in Clouds, further cooperation is required across different organizations that develop standards. For example, customers can be locked into their current Cloud provider whose storage system may prevent them from migrating from one system to another. The authors list a large number of standards bodies with different interests, but similar to ISO/IEC JTC 1/SC 38 – Cloud Computing and Distributed Platforms:

- IEEE Cloud Computing Standard Study Group (IEEE CCSSG);
- ITU Cloud Computing Focus Group (ITU FG Cloud);
- Cloud Security Alliance (CSA);
- Distributed Management Task Force (DMTF);
- Storage Networking Industry Association (SNIA);
- Open Grid Forum (OGF);
- Open Cloud Consortium (OCC);
- Organization for the Advancement of Structured Information Standards (OASIS).

To promote further adoption of Cloud Computing, the above listed standards developing bodies must promote coordination and cooperation in this area [23]. As a minimum requirement, the authors suggest standards in the following areas, in order to increase Cloud interoperability and open up seamless data migration among Clouds:

- Network architecture;
- Data format;
- Metering and billing;
- Quality of Service;
- Resource provisioning;
- Security, identity management, and privacy.

Standards developing organizations have already analyzed the standards landscape and identified standardization gaps for Cloud Computing. This preparatory work has allowed the definition of standards development priorities. Several reports have been published with this objective:

- ISO/IEC JTC 1/SC 38 Study Group on Cloud Computing (SGCC), Study Group Report on Cloud Computing (09/2011);
- ETSI Cloud Standards Coordination Final Report (11/2013).

Standards developing organizations outlined priority topics for standardization and as a starting point developed a common set of references. This notably concerns terminology (e.g.: ISO/IEC 17788) or reference architecture (e.g.: ISO/IEC 17789). The following main topics have been identified as lacking standards and have thus been prioritized for standardization work programs:

[57] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0529&from=EN

- Service Level Agreement (SLA) is a critical topic for the Cloud and some of the main current challenges are to determine common terminology and to define metrics for measuring service level objectives. Therefore, standards organizations are currently developing a framework (e.g.: ISO/IEC FDIS 19086-1) to help avoid confusion and facilitate common understanding between Cloud service providers and Cloud service customers;
- Security and privacy standards are also essential in the context of Cloud Computing. On one hand, they will ensure the confidentiality, integrity, and availability of information and information systems (e.g.: ITU-T Draft X.1641). On the other hand, these developments are necessary for improving the confidence of Cloud consumers and facilitating the adoption of the Cloud across the world;
- Interoperability and portability standards constitute a fundamental challenge in the Cloud. Standardization organizations have launched several projects in order to unambiguously define the terminology needed (e.g.: ISO/IEC CD 19941). This will facilitate broad adoption of the Cloud by enhancing its flexibility and automation.

4.1.1 ISO & ISO/IEC

ISO/IEC JTC 1/SC 38 – CLOUD COMPUTING AND DISTRIBUTED PLATFORMS

SC 38 provides standardization in the area of Cloud Computing and Distributed Platforms. It is organized into three Working Groups (WG):

- WG 3 – Service Level Agreement;
- WG 4 – Interoperability and Portability;
- WG 5 – Data and their Flow Across Devices and Cloud Services.

ISO/IEC JTC1 REFERENCE STANDARDS ON CLOUD COMPUTING

- ISO/IEC 17788 (SC38) – Information technology – Cloud computing – Overview and vocabulary.

  ISO/IEC 17788 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, not-for-profit organizations) and provides an overview of Cloud Computing along with a set of terms and definitions. It provides the basis of terminology for Cloud Computing standards.

- ISO/IEC 17789 (SC38) – Information technology – Cloud computing – Reference architecture.

  ISO/IEC 17789 specifies the Cloud Computing reference architecture (CCRA). The reference architecture includes the Cloud Computing roles, Cloud Computing activities, and the Cloud Computing functional components and their relationships.

- ISO/IEC 17826 (SC38) – Information technology – Cloud Data Management Interface (CDMI).

  ISO/IEC 17826 specifies the interface for accessing Cloud storage and for managing the data stored therein. It is applicable to developers who implement or use Cloud storage.

- ISO/IEC 19831 (JTC1) – Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol – An Interface for Managing Cloud Infrastructure.

  ISO/IEC 19831 describes the model and protocol for management interactions between a Cloud Infrastructure as a Service (IaaS) Provider and the Consumers of an IaaS service. The basic resources of IaaS (machines, storage, and networks) are modeled with the goal of providing Consumer management

access to an implementation of IaaS and facilitating portability between Cloud implementations that support the specification. This document specifies a Representational State Transfer (REST)-style protocol using HTTP. However, the underlying model is not specific to HTTP, and it is also possible to map it to other protocols.

4.1.2 ETSI

ETSI, the European Telecommunications Standards Institute, produces globally applicable standards for ICT, including fixed, mobile, radio, converged, broadcast, and Internet technologies. ETSI is a formal standardization body that is officially recognized by the European Union as a European Standards Organization.

At the beginning of 2016, ETSI published a new set of reports in connection with Cloud Standards Coordination (CSC) Phase 2, which intends to investigate specific aspects of the Cloud Computing Standardization landscape, in particular from the point of view of users. It also offers a new "snapshot" of the state of standards. These are detailed in Table 22, which provides a summary of currently published ETSI standards related to Cloud Computing.

STANDARD NO.	STANDARD TITLE
ETSI TR 102 997 V1.1.1 (04/2010)	CLOUD; Initial analysis of standardization requirements for Cloud services
ETSI TS 103 125 V1.1.1 (11/2012)	CLOUD; SLAs for Cloud services
ETSI TR 103 126 V1.1.1 (11/2012)	CLOUD; Cloud private-sector user recommendations
ETSI TS 103 142 V1.1.1 (04/2013)	CLOUD; Test Descriptions for Cloud Interoperability
ETSI SR 003 381 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Identification of Cloud user needs
ETSI SR 003 382 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Cloud Computing Standards and Open Source; Optimizing the relationship between standards and Open Source in Cloud Computing
ETSI SR 003 391 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing
ETSI SR 003 392 V2.1.1 (02/2016)	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards
ETSI TR 103 304 V1.1.1 (07/2016)	CYBER; Personally Identifiable Information (PII); Protection in mobile and cloud services

Table 22 – ETSI Published Standards

4.1.3 ITU-T

The Study Groups of the International Telecommunication Union (ITU) on Telecommunication Standardization Sector (ITU-T) assemble experts from around the world to develop international standards known as ITU-T Recommendations which act as defining elements in the global infrastructure of ICT.

The following ITU-T groups relate to Cloud Computing:

- ITU-T/FG Cloud (currently terminated)
- ITU-T/SG 13 – Future networks
- ITU-T/SG 17 – Security

Several published ITU-T standards that are of interest to Digital Trust in Cloud Computing are also provided in Table 23.

STANDARD NO.	STANDARD TITLE
ITU-T FG Cloud TR Part 5 (02/2012)	Technical Report: Part 5: Cloud security
ITU-T Q.4040 (02/2016)	The framework and overview of Cloud Computing interoperability testing
ITU-T Y.3511 (03/2014)	Framework of inter-Cloud Computing
ITU-T X.1601 (10/2015)	Security framework for Cloud Computing (edition 2 under development)
ITU-T X.1602 (03/2016)	Security requirements for software as a service application environment
ITU-T X.1642 (03/2016)	Guidelines for the operational security of Cloud Computing
ITU-T Q Suppl. 65 (07/2014)	Draft Q Supplement 65 to Q.39xx-series Recommendations (Q.Supp-CCI) Cloud computing interoperability activities

Table 23 – ITU-T Published Standards

4.2 BIG DATA STANDARDIZATION TECHNICAL COMMITTEES & STANDARDS

Standards for Big Data technologies are essential for improving Trust in this technology, e.g. with respect to Cloud Computing, by enabling interoperability between the various applications and preventing vendor lock-in. Standards can also help to prevent over fitting in Big Data. This occurs when analytics designers tweak a model repeatedly to fit the data and begin to interpret noise or randomness as truth. Another potential benefit of standardization for Big Data is the ability to support the integration of multiple data sources. Security and Privacy are of paramount importance for both data quality and for protection. Some of the large volume of data come from social media and medical records and inherently contain private information. Analysis of such data, particularly in conjunction with its context, must protect privacy. Big Data systems should be designed with security in mind. If there is no global perspective on security, then fragmented solutions to address security may offer a partial sense of safety rather than full security. Standards will play an important role in data quality and data governance by addressing the veracity and value of data.

The remainder of this section will focus on joint efforts from ISO and IEC and on ITU, which are the most relevant standardization bodies for Big Data.

4.2.1 ISO & ISO/IEC

ISO/IEC JTC 1/WG 9 – BIG DATA

The scope of WG 9 was established in November 2014 as covering the following items:

- Serve as the focus of and proponent for JTC 1's Big Data standardization program.
- Develop foundational standards for Big Data including reference architecture and vocabulary standards for guiding Big Data efforts throughout JTC 1 upon which other standards can be developed.
- Develop other Big Data standards that build on the foundational standards when relevant JTC 1 subgroups that could address these standards do not exist or are unable to develop them.
- Identify gaps in Big Data standardization.
- Develop and maintain liaisons with all relevant JTC 1 entities as well as with any other JTC 1 subgroup that may propose work related to Big Data in the future.
- Identify JTC 1 (and other organization) entities that are developing standards and related material that contribute to Big Data, and where appropriate, investigate ongoing and potential new work that contributes to Big Data.
- Engage with the community outside of JTC 1 to grow awareness of and encourage engagement in JTC 1 Big Data standardization efforts within JTC 1, forming liaisons as required.

Projects currently under development in WG 9 are ISO/IEC 20546 on Big Data Overview and Vocabulary as well as ISO/IEC 20547 Big Data Reference Architecture (4 parts). ISO/IEC 20546 has reached 1st Working Draft status while ISO/IEC 20547 is currently at the Editors' Draft level.

The ISO/IEC 20547 standard will use the vocabulary and concepts defined in ISO/IEC 20546 and describe common features from use cases as a basis for creating a Big Data Reference Architecture with the basic modules and their relationships. It is also intended as a means of supporting the creation of specialist Big Data Architectures as a way of creating proper Big Data solutions for companies worldwide. This standard

will describe a generic high-level conceptual model that is an effective tool for discussing the requirements, structures, and operations inherent to Big Data, for example, to illustrate and understand the various Big Data components, processes, and systems, in the context of an overall Big Data conceptual model. The standard will provide a technical reference for government departments, agencies, and other consumers to understand, discuss, categorize, and compare Big Data solutions. It will also facilitate the analysis of candidate standards for interoperability, portability, reusability, and extendibility.

4.2.2 ITU-T STUDY GROUP 13

The Study Group 13 from ITU-T published the first Big Data-related standard[58]: ITU-T Y.3600 Big Data – Cloud computing based requirements and capabilities. This standard details the requirements, capabilities and use cases of Cloud-based Big Data as well as a high-level system context view and its relationships with other entities. The Big Data paradigm provides an effective, scalable solution for dealing with growing volumes of data and uncovering patterns or other information capable of making data manageable and profitable. Cloud Computing-based Big Data provides the capabilities to collect, store, analyze, visualize, and manage varieties of large volume datasets, which cannot be rapidly transferred and analyzed using traditional technologies. ITU-T Y.3600 outlines recommendations and requirements for data collection, visualization, analysis, and storage, among other areas, along with security considerations. It addresses the following subjects:

- Overview of Big Data:
  - Introduction to Big Data;
  - Big Data ecosystems and roles;
  - Relationship between Cloud Computing and Big Data;
- Cloud Computing-based Big Data system context and benefits;
- Cloud Computing-based Big Data requirements;
- Cloud Computing-based Big Data capabilities.

The recommendation describes the Big Data ecosystem through roles and sub-roles. It also defines necessary activities for roles providing and consuming Big Data services as well as relationships between roles. This Big Data ecosystem includes the data provider, Big Data service provider and Big Data service customer.

The ITU-T SG 13 study group is also developing a recommendation related to the functional architecture of Big Data as a service with the ITU-T Y.BDaaS-arch – Cloud computing – Functional architecture of Big Data as a Service. This recommendation specifies the functional components, functional architecture, and reference points of Big Data as a Service (BDaaS). The scope of this recommendation includes: overview of the functional architecture of Big Data as a Service, the functional components of Big Data as a Service, the functional architecture of Big Data as a Service, and the reference points between functional components of Big Data as a Service.

A Big Data and Internet of Things (IoT) recommendation is being developed by the SG 13 (Y.IoT-BigData-reqts). The purpose of this recommendation is to specify requirements and capabilities of the IoT for Big Data. This recommendation complements the developments on common requirements of the Internet of Things (ITU-T Y.2066) and its functional framework (ITU-T Y.2068) in terms of the specific requirements and capabilities that the IoT is expected to support in order to address challenges related to Big Data. In addition, it constitutes a basis for further standardization work concerning Big Data in conjunction with the IoT.

[58] http://www.itu.int/itu-t/recommendations/rec.aspx?rec=12584

4.2.3 NIST PUBLIC WORKING GROUP FOR BIG DATA (NBD-WG)

The focus of the National Institute of Standards and Technology Big Data Public Working Group (NBD-PWG) is to form a community of interest from industry, academia, and government, with the goal of developing consensus definitions, taxonomies, reference architectures, and technology roadmaps. The aim is to create vendor-neutral technology and infrastructure-agnostic deliverables to enable Big Data stakeholders to pick and choose the best analytics tools for their processing and visualization requirements. This must be performed on the most suitable computing platforms and clusters while allowing added value from Big Data service providers and a flow of data between stakeholders in a cohesive and secure manner. It is composed of the following subgroups:

- NIST Big Data Definitions & Taxonomies Subgroup
- NIST Big Data Use Case & Requirements Subgroup
- NIST Big Data Security & Privacy Subgroup
- NIST Big Data Reference Architecture Subgroup
- NIST Big Data Technology Roadmap Subgroup

4.3 IOT STANDARDIZATION TECHNICAL COMMITTEES & STANDARDS

Many organizations are actively involved in the standardization that is evolving around the Internet of Things and IoT standardization has proven to be difficult. It is widely acknowledged that many standardization challenges need to be addressed for further spread of IoT. Issues include, but are not limited to, security, privacy, interfaces, data structures, and architecture. Because IoT covers everything from the pure technical level up to business processes and even political decisions, there is no single standard (not even at the interface level) and as a result the world of IoT standards is completely fragmented [13]. The urgent need for standardization and necessary improvements in interoperability are critical success factors for accelerated adoption of IoT systems [51].

The following analysis will start with the ISO and IEC committees and standards, then proceed to look at other standardization bodies such as ETSI and the oneM2M group. It is clear that there is already a profound collaboration among the various organizations in an attempt to unify and reach consensus on as many aspects as possible. This is apparent from the number of liaisons which is significantly higher for the Internet of Things-related working groups (ISO/IEC JTC 1: WG 7, WG 10 and WG 11) presented below.

4.3.1 ISO & ISO/IEC

ISO/IEC JTC 1/WG 10 – INTERNET OF THINGS (IOT)

WG 10 was recently created based on the Study Report of ISO/IEC JTC 1/SWG 5 on Internet of Things (IoT) submitted to the 2014 JTC 1 Plenary. The scope of WG 10 is to develop foundational standards for IoT guiding efforts throughout JTC 1 upon which other standards can be developed covering the following:

- Developing Terms and Definitions for JTC 1 IoT Vocabulary
- Developing IoT Reference Architecture (RA) and other foundational specifications as JTC 1 standards
- Continuing the work begun in ISO/IEC JTC 1/SWG 5 on IoT standardization gaps
- Encouraging the prompt and efficient exchange of information within JTC 1 and with ISO, IEC, or other entities working on IoT, as appropriate
- Monitoring the ongoing IoT regulatory, market, business, and technology requirements
- Developing other IoT standards that build on the foundational standards when relevant JTC 1 subgroups that could address these standards do not exist or are unable to develop them.

The main focus of WG 10 is currently on defining the IoT Reference Architecture in ISO/IEC 30141, then on the definition of vocabulary in ISO/IEC 20924 and IoT use cases.

A central issue pointed out in the market requirements analysis is the importance of supporting interoperability between different levels of IoT systems in various IoT platforms based on different standards. This is due to the advances in different industries and fora on documents and standards that address needs and requirements in their own areas of expertise. To achieve a globally connected IoT landscape, the standards of WG 10 are expected to support interoperability between different IoT systems.

The following projects are being developed by WG 10:

- ISO/IEC 30141 – Internet of Things – Internet of Things Reference Architecture (IoT RA)
- ISO/IEC 20924 – Internet of Things – Definition and Vocabulary
- ISO/IEC 21823-1 – Internet of Things (IoT) – Interoperability for Internet of Things systems – Part 1: Framework

ISO/IEC JTC 1/WG 7 – SENSOR NETWORKS

WG 7 is involved in three main activities, which primarily involve standardization activities in terminology, taxonomy, and reference architectures in Sensor networks.

Secondly WG 7 explores emerging and existing technology and standardization gaps to provide approaches for using sensor networks across application areas.

Lastly WG 7 promotes communication and information-sharing among groups working in the field of Sensor networks both in and outside of JTC 1.

Related to the latter activity, WG 7 seeks liaison with a number of organizations, not limited to: relevant ISO TCs, IEC TCs and ITU-T SGs, IEEE 1451, IEEE 1588, IEEE P2030, IEEE 802.15, Open Geospatial Consortium, ZigBee Alliance, IETF 6LoWPAN, IETF ROLL WG, ETSI, IPSO Alliance, EPCglobal, ISA 100, LONMARK, KNX Association, Zwave Alliance;

WG 7 is organized as follows:

- ISO/IEC JTC1/WG 7 SRG 1 (Subgroup Rapporteur Group) on IoT standardization gaps
  - Review of IoT-related standardization activities within JTC 1 entities and outside JTC 1;
  - and identification of standardization gaps for IoT.
- ISO/IEC JTC1/WG 7 SRG 2 on network level requirements and technologies for IoT with the following scope of work:
  - Study Reference Architecture (RA) requirements;
  - Survey network-level solutions for RA requirements (both in SDOs and fora/consortia);
  - Survey related network level standards (existing and in development) in cooperation with SRG 1;
  - Identify organizations with which WG 10 should establish a liaison to share information or make proposals for joint work;
  - Identify the possible new projects in this area for WG 10;
  - Submit the study report to WG 10.

ISO/IEC JTC 1/WG 11 – SMART CITIES

The Smart Cities preliminary report of 2014[59] by the Study Group on Smart Cities, drawn up by JTC 1 in November 2013 identifies the multitude of existing work on key enabling technologies for Smart Cities. In addition, it indicates the gaps that need to be filled in order to cover all requirements with standards. Apart from requirements of a common conceptual model of the city and ensuring interoperability between different city systems and others, there is a need for the city to be able to manage issues such as privacy, security, resilience, data flows, etc. at a whole-system level.

[59] http://www.iso.org/iso/smart_cities_report-jtc1.pdf

After initial work by the study group, JTC 1/WG 11 was established in March 2016 with members from 15 countries and the preliminary scope defined as follows:

1. Serve as the focus of and proponent for JTC 1's Smart Cities standardization program.
2. Develop foundational standards for the use of ICT in Smart Cities – including the Smart City ICT Reference Framework and an Upper Level Ontology for Smart Cities – for guiding Smart City work throughout JTC 1 upon which other standards may be developed.
3. Develop a set of ICT-related indicators for Smart Cities in collaboration with ISO/TC 268.
4. Develop additional Smart Cities' standards and other deliverables that build on these foundational standards.
5. Develop and maintain liaisons with all relevant JTC 1 entities as well as with any other JTC 1 subgroup that may propose work related to Smart Cities in the future.
6. Identify JTC 1 (and other organization) entities that are developing standards and related material that contribute to Smart Cities, and where appropriate, investigate ongoing and potential new work that contributes to Smart Cities.
7. Engage with the community outside of JTC 1 to grow an awareness of and encourage engagement in JTC 1 Smart Cities standardization efforts within JTC 1, forming liaisons as required.
8. Ensure a strong relationship with ISO and IEC Smart Cities activities.

Two new work items were recently approved and assigned to WG 11:

- ISO/IEC NP 30145 – Smart city ICT reference framework – 3 parts
- ISO/IEC NP 30146 – Smart city ICT indicators

SELECTED ISO/IEC JTC1 REFERENCE STANDARDS WITH RELEVANCE TO IOT APPLICATIONS

- ISO/IEC 30141 (WG 10) – Information technology – Internet of Things – Internet of Things Reference Architecture (IoT RA)

  ISO/IEC 30141 describes the reference architecture of Internet of Things which is under development in the WD stage and will likely be split into four parts: "General Overview", "Conceptual Model", "Reference Architecture", and "Security and Privacy". Significant progress has been made with the initial work of describing Terms and Definitions and IoT Vocabulary and WG 10 has agreed on a Conceptual Model defining relations between the domain-based and entity-based reference models.

  The domains defined in the model are "User" on the top, then "Operation & Management", "Application Service", "Resource & interchange" in the next layer. In the layer below is the "Sensing and Controlling" domain, comprising the IoT gateway and devices, and the final lowest layer contains the "Physical Entity" domain.

  The reference architecture also includes references to the Confidentiality, Integrity and Availability (CIA) definitions generally known in the context of Digital Trust and from the ISO/IEC 27000 family of standards, slightly adapted to the context of IoT. In terms of security, the IoT gateways must make use of encryption in their communication and the FCAPS (Fault, Configuration, Accounting, Performance, and Security) network management model should be implemented and consider IoT-specific information models.

- ISO/IEC 20924 (WG 10) – Information technology – Internet of Things – Definition and Vocabulary

  ISO/IEC 20924 provides a definition of Internet of Things along with a set of terms and definitions. The project will help with, and provide a framework for, a deeper and better understanding of issues involving such topics so that others in the international community can address them. The work item was proposed in June to be accepted in November 2015 and is currently in the CD stage.

- ISO/IEC 21823-1 – Information technology – Internet of Things – Interoperability for Internet of Things systems – Part 1: Framework

  ISO/IEC 21823-1 provides an overview of interoperable IoT systems and a framework for interoperability to ensure information exchanges are such that the information is understood and can be efficiently processed to support peer-to-peer interoperability of IoT systems and seamless communication among IoT system entities. The work item was proposed in March to be accepted in July 2016 and is currently in the editors' draft stage.

- ISO/IEC 29182 (WG 7) – Information technology – Sensor networks: Sensor Network Reference Architecture (SNRA)

The International Standard is divided into seven parts covering terms and definitions of selected concepts relevant to the field of sensor networks, architecture views and definitions of Sensor Networks interfaces among the entity models in the reference architecture.

The architecture views include business, operational, systems, and technical views which are presented as being functional, logical, and/or physical where applicable. The seven parts are as follows:

1. General overview and requirements
2. Vocabulary and terminology
3. Reference architecture views
4. Entity models
5. Interface definitions
6. Applications
7. Interoperability guidelines

- ISO/IEC 30145 (WG 11) – Information technology – Smart City ICT Reference Framework

This standard was accepted as a new Working Item in March 2016 to be partitioned into the following three parts:

1. Smart City Business Process Framework
2. Smart City Knowledge Management Framework
3. Smart City Engineering Framework

The scope of the first part is to define a generic Business Process Framework for a smart city. This standard will thus focus on smart city-specific processes. Generic business processes common to smart cities and commercial organizations will be identified but not detailed.

- ISO/IEC 30146 (WG 11) – Information technology – Smart City ICT Indicators

  The ISO/IEC 30146 standard was also accepted as a new Working Item in March 2016 with the scope to define a comprehensive set of indicators that will enable cities to assess their progress in using ICT to enable them to become smarter.

An efficient indicator may be scientific, directive, representative, comparable, and verifiable and in this case will be consistent with the Smart City Indicators being developed by ISO TC 268.

It is beyond the scope of this White Paper to detail all organizations active in IoT standardization and the extent to which security is incorporated in the specifications. However, a few of the key organizations are listed and described below along with selected work items.

4.3.2 ETSI

The ETSI technology cluster on IoT[60] addresses various topics from M2M communications to smart devices, smart cities, smart grids, connected cars, eHealth, home automation and energy management, and remote industrial process control.

A list of standards developed by ETSI for the IoT cluster and related to Digital Trust is provided in Table 24. A number of these are related to the oneM2M group, discussed in the next section.

STANDARD NO.	STANDARD TITLE
TS 118 103	oneM2M; Security solutions (oneM2M TS-0003 version 1.4.2 Release 1)
TS 118 104	oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004 version 1.6.0 Release 1)
TS 118 108	oneM2M; CoAP Protocol Binding (oneM2M TS-0008 version 1.3.2 Release 1)
TS 118 109	oneM2M; HTTP Protocol Binding (oneM2M TS-0009 version 1.5.1 Release 1)
TS 118 110	oneM2M; MQTT Protocol Binding (oneM2M TS-0010 version 1.5.1 Release 1)
TS 118 113	oneM2M; Interoperability Testing (oneM2M TS-0013 version 1.0.0 Release 1)
TS 103 267	SmartM2M; Smart Appliances; Communication Framework
TR 103 290	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment
TS 118 103	oneM2M Security solutions
TS 118 104	oneM2M Service Layer Core Protocol Specification

Table 24 – ETSI IoT related standards

[60] http://www.etsi.org/technologies-clusters/technologies/internet-of-things

4.3.3 oneM2M

In July 2012, seven of the leading ICT Standards Development Organizations launched a new global organization, the oneM2M Partnership Project[61], with the following founding members: CCSA, TTA, ARIB, TTC, ETSI, ATIS, and TIA. There are already numerous released oneM2M standards with the general purpose of addressing the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

oneM2M TS-0003 – SECURITY SOLUTIONS

The Technical Specification 0003 is specifically oriented towards addressing security issues that may arise from the various use cases of IoT. A security architecture is described from a service point-of-view by separating it into functional and environmental layers. The specification covers numerous aspects and scenarios from security administration, authorization, and identity protection to protocol and algorithm details, leveraging on a multitude of existing standards, such as TLS/DTLS and CoAP briefly discussed in this paper.

4.3.4 ITU-T

The ITU Focus Group on Smart Sustainable Cities[62] concluded its work in May 2015 by approving 21 Technical Specifications and Reports. Among these is a report on Cyber-security, data protection, and Cyber-resilience in Smart Sustainable Cities through internal liaison with ITU-T SG 17 on security.

ITU SG 20 – IOT AND ITS APPLICATIONS INCLUDING SMART CITIES AND COMMUNITIES

Study group 20 was established in June 2015, by the Telecommunication Standardization Advisory Group (TSAG) to provide a framework and roadmaps for the harmonized and coordinated development of Internet of Things (IoT), including M2M communications, ubiquitous sensor networks and smart sustainable cities and communities.

4.3.5 NIST CYBER-PHYSICAL SYSTEMS PUBLIC WORKING GROUP (CPS PWG)

The National Institute of Standards and Technology CPS PWG, formed by NIST in 2014, brings together experts to help define and shape key aspects of CPS to accelerate its development and implementation within multiple sectors.

[61] http://www.oneM2M.org

[62] http://itu.int/en/ITU-T/focusgroups/ssc/

The Cybersecurity and Privacy Subgroup[63] is one of the five subgroups of CPS PWG and is well-aligned with the topics of this paper. The goal is to develop a cybersecurity and privacy strategy for the common elements of CPS. This includes identification, implementation, and monitoring of specific cybersecurity activities (including the identification, protection, detection, response, and recovery of CPS elements) and outcomes for CPS in the context of a risk management program. Where applicable standards, guidelines, and measurement metrics do not exist, this subgroup will identify areas for further CPS cybersecurity research and development.

4.3.6 THE ALLIANCE FOR IOT (AIOTI)

The Alliance for Internet of Things Innovation (AIOTI)[64] was initiated by the European Commission in order to develop and support dialogue and interaction among the various players involved in Internet of Things (IoT) in Europe. The structure of AIOTI consists of the Board (Steering Committee) and eleven Working Groups (WGs).

WG 3: IOT STANDARDIZATION

The "IoT Standardization" working group chaired by ETSI is involved in mapping existing IoT standards and performing an analysis of gaps as well as devising strategies and use cases for developing (semantic) interoperability.

Three main deliverables were produced in the initial phase between March 2015 and June 2016: IoT Landscape and IoT LSP Standard Framework Concepts, IoT High Level Architecture (HLA) and IoT Semantic interoperability recommendations.

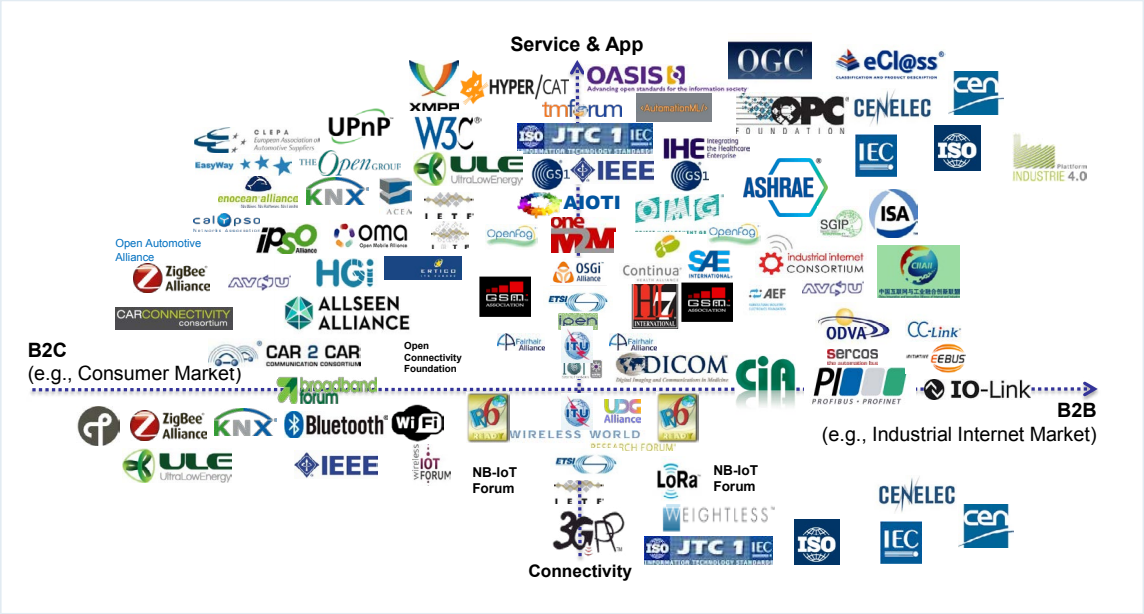


Figure 33 – IoT SDO and Alliances Landscape, AIOTI WG3 (IoT Standardization) – Release 2.5

[63] http://www.nist.gov/cps/cpswpg_security.cfm

[64] http://www.aioti.eu/

The group focuses on reference models as the basis for a reference architecture, which can be shared by industrial actors across different application domains and can help to break silos between leading vertical IoT application areas. Looking at the partner organizations (see Figure 33), it is clear that security and privacy will play an integral part in system conception and continued maintenance.

4.3.7 OPEN CONNECTIVITY FOUNDATION (OCF)

OCF acquired UPnP Forum at the end of 2015 to centralize their technologies and align efforts to standardize the two organizations. With the goal of ensuring interoperability of the billions of devices that will make up the emerging Internet of Things, the OCF will maintain the legacy UPnP specifications and certification procedures and simultaneously support new initiatives, such as UPnP+.

UPnP+ is a new certification program[65] within the UPnP ecosystem aiming to improve the reliability, security, and consistency of UPnP implementations, and to encourage the use of the latest version of UPnP specifications. These provide enhanced security and Cloud connectivity for virtualizing and enabling secure sharing of devices over the Internet as well as energy management and sustainability features.

4.3.8 IOT-A'S REFERENCE MODEL

The IoT-A reference model developed in the three years prior to November 2013[66] as a European Lighthouse Integrated Project (large scale projects, specifically designed to raise awareness and give increased visibility) is also worth mentioning. It provides an architectural reference model and defines an initial set of key building blocks. A book is also available published in Open Access.

[65] http://upnp.org/resources/whitepapers/UPnP_Plus_Whitepaper_2015.pdf

[66] http://www.iot-a.eu/public/

4.4 COMMON STANDARDIZATION TECHNICAL COMMITTEES & STANDARDS

4.4.1 ISO/IEC JTC 1/SC 27 – IT SECURITY TECHNIQUES

This committee develops standards for the protection of information and ICT. This includes generic methods, techniques and, guidelines for addressing both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls, and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity, and confidentiality of information;
- Security management support documentation including terminology, guidelines, and procedures for the registration of security components;
- Security aspects of identity management, biometrics, and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC 27 is organized as follows:

- JTC 1/SC 27/SWG-M Special Working Group on Management
- JTC 1/SC 27/SWG-T Transversal Items
- JTC 1/SC 27/WG 1 Information security management systems
- JTC 1/SC 27/WG 2 Cryptography and security mechanisms
- JTC 1/SC 27/WG 3 Security evaluation testing and specification
- JTC 1/SC 27/WG 4 Security controls and services
- JTC 1/SC 27/WG 5 Identity management and privacy technologies

The best-known standards developed by SC 27 are ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements and ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls.

4.4.1.1 ISO/IEC 27017 (SC 27) – INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS BASED ON ISO/IEC 27002 FOR CLOUD SERVICES

ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of Cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to Cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both Cloud service providers and Cloud service customers. This standard is common with the ITU-T (ITU-T X.1631).

4.4.1.2 ISO/IEC 27018 (SC 27) – INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS

ISO/IEC 27018 provides confidence in the Cloud industry based on existing information security standards, including ISO/IEC 27001 and ISO/IEC 27002. The combination of a common set of control objectives and guidelines based on ISO/IEC 27002 and additional Cloud-specific control objectives helps govern the processing of personal data in the Cloud. It also provides guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public Cloud Computing environment.

Its key objectives are to:

- Help Cloud service providers that process personally identifiable information to address applicable legal obligations as well as customer expectations.
- Enable transparency so customers can choose well-governed Cloud services.
- Facilitate the creation of contracts for Cloud services.
- Provide Cloud customers with a mechanism to ensure Cloud providers' compliance with legal and other obligations.

4.4.1.3 ISO/IEC 27036-4 – INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY FOR SUPPLIER RELATIONSHIPS – PART 4: GUIDELINES FOR SECURITY OF CLOUD SERVICES

ISO/IEC 27036-4 is part of International Standard ISO/IEC 27036 providing Cloud service customers and Cloud service providers with guidance on:

- gaining visibility of the information security risks associated with the use of Cloud services and managing these risks effectively; and
- responding to risks specific to the acquisition or provision of Cloud services that may have an information security impact on organizations using these services.

This part of ISO/IEC 27036 does not include business continuity management/resiliency issues involved in the Cloud service. ISO/IEC 27031 addresses business continuity and ISO/IEC 22301 addresses risk consolidation and management for business continuity.

This part of ISO/IEC 27036 does not provide guidance on how a Cloud service provider should implement, manage, and operate information security. Guidance can be found in ISO/IEC 27002 and ISO/IEC 27017.

The scope of this International Standard is to define guidelines supporting the implementation of Information Security Management for the use of Cloud services.

4.4.1.4 ISO/IEC 19086-4 – INFORMATION TECHNOLOGY – CLOUD COMPUTING – SERVICE LEVEL AGREEMENT (SLA) FRAMEWORK AND TECHNOLOGY – PART 4: SECURITY AND PRIVACY

ISO/IEC 190686-4 is part of International Standard ISO/IEC 19086 whose aim is to avoid confusion and facilitate common understanding between cloud service providers and cloud service customers regarding Service Level Agreements (SLAs). This part of ISO/IEC 19086 is still under development and will specify the Security and Protection of Personally Identifiable Information components of Service Level Agreements (SLA) for cloud services including requirements and guidance.

4.4.1.5 ISO/IEC 20547-4 – INFORMATION TECHNOLOGY – BIG DATA REFERENCE ARCHITECTURE – PART 4: SECURITY AND PRIVACY FABRIC

ISO/IEC 20547-4 Big Data Reference Architecture – Part 4: Security and privacy fabric is still under development in relation with ISO/IEC JTC 1/WG 9. It will specify the underlying Security and Privacy fabric that applies to all aspects of the Big Data Reference Architecture including Big Data roles, activities, and functional components. Effective standardization of security is paramount to the development of mutual trust and cooperation amongst Big Data stakeholders.

4.4.2 ISO/IEC JTC 1/SC 32 – DATA MANAGEMENT AND INTERCHANGE

This committee provides standards for data management within and among local and distributed information systems environments. SC32 enables technologies to promote harmonization of data management facilities across sector-specific areas. Specifically, SC32 standards include:

- Reference models and frameworks for the coordination of existing and emerging standards;
- Definition of data domains, data types and data structures, and their associated semantics;
- Languages, services, and protocols for persistent storage, concurrent access, concurrent update, and interchange of data;
- Methods, languages, services, and protocols for structuring, organizing, and registering metadata and other information resources associated with sharing and interoperability, including electronic commerce.

SC 32 is structured as follows:

- JTC 1/SC 32/WG 1 eBusiness
- JTC 1/SC 32/WG 2 MetaData
- JTC 1/SC 32/WG 3 Database language
- JTC 1/SC 32/WG 4 SQL/Multimedia and application packages

ISO/IEC 15944-12 Secretariat Information technology – Business Operational View – Part 12: Privacy protection requirements regarding information life cycle management (ILCM) and EDI of personal information is a Digital Trust-related standard under the direct responsibility of ISO/IEC JTC 1/SC 32. This standard is currently under development. It presents fundamental privacy protection principles and details Information Life Cycle Management (ILCM) principles in support of law and privacy protection requirements. Then it presents governance rules that ensure accountability and control of PII.

4.4.3 ISO/IEC JTC 1/SC 40 – IT SERVICE MANAGEMENT AND IT GOVERNANCE

This committee develops standards, tools, frameworks, best practice, and related documents for IT Service Management and IT Governance, including areas of IT activity such as audit, digital forensics, governance, risk management, outsourcing, service operations, and service maintenance, but excluding subject matter covered by the scope and existing work programs of JTC 1/SC 27 and JTC 1/SC 38. As part of its standardization activity, it proposed several standards that are of interest to Digital Trust, namely:

4.4.3.1 ISO/IEC 38500 – INFORMATION TECHNOLOGY – GOVERNANCE OF IT FOR THE ORGANIZATION

ISO/IEC 38500 provides guiding principles for members of governing bodies of organizations (which may comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organizations.

It also provides guidance to those advising, informing, or assisting governing bodies. They include the following: executive managers; members of groups monitoring the resources within the organization; external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies; internal and external service providers (including consultants) and auditors.

ISO/IEC 38500 applies to the governance of the organization's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organization, external service providers, or business units within the organization. This standard is applicable to all organizations, including public and private companies, government entities, and not-for-profit organizations.

4.4.3.2 ISO/IEC 38505 – INFORMATION TECHNOLOGY – GOVERNANCE OF IT

Currently under development, this standard is composed of two parts: Part 1: Applying ISO/IEC 38500 to data governance; and Part 2: Implications of 38505-1 for data management.

4.4.3.3 ISO/IEC 30121 – INFORMATION TECHNOLOGY – GOVERNANCE OF DIGITAL FORENSIC RISK FRAMEWORK

ISO/IEC 30121 provides a framework for governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost-effectiveness of digital evidence disclosure. This International Standard is applicable to all types and sizes of organizations.

4.4.4 ETSI/TC CYBER – CYBER SECURITY

The activities of ETSI TC CYBER include the following broad areas:

- Cyber Security
- Security of infrastructures, devices, services, and protocols
- Security advice, guidance, and operational security requirements for users, manufacturers, and network and infrastructure operators
- Security tools and techniques to ensure security
- Creation of security specifications and alignment with work done in other TCs.

4.4.5 ETSI/ISG ISI – INFORMATION SECURITY INDICATORS

The Industry Specification Group on Information Security Indicators (ISG ISI) is producing specifications which together will form a reliable and commonly-recognized reference model for the measurement of information security risks. These specifications are expected to help enforce the forthcoming European Commission critical infrastructure directive and data protection legislation (the revision of the Data Protection Directive 95/46/EC).

4.4.6 CEN-CENELEC TECHNICAL COMMITTEES

The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) are both officially recognized standardization bodies that bring together the national standards agencies of 33 countries. CEN-CENELEC works closely with the European Commission to ensure that standards correspond with any relevant EU legislation.

The following are the relevant CEN-CENELEC groups:

- CEN-CENELEC-ETSI Cybersecurity Coordination Group
- CEN/CLC/JWG 8 – Privacy management in products and services (note: M/530 – privacy by design)
- CEN/TC Project Committee 365 – Internet Filtering

CONCLUSIONS AND OUTLOOK

Trust, and specifically Digital Trust, plays a fundamental role in all interactions in our society as it reduces uncertainties and enables reliance on others. It underpins the digital economy at personal, business and institutional levels and is pre-conditional to the emergence of new business models. Three disruptive developments that resonate in social, technological, and business domains contribute to the growing importance of Digital Trust:

- **Internet of Things**: ubiquitous mobile Internet penetration of smartphones, tablets, and other smart devices generating real-time (big) data that is typically stored in the Cloud.
- **Cloud Computing**: flexible, on-demand IT technologies that enable business agility. Its stored data can be analyzed using Analytics technologies.
- **Big Data and Analytics**: software for all kinds of social and business interactions, such as social electronic networks and peer-review sites for sharing information and online ratings.

Digital Trust is of paramount importance to all our interactions in modern society due mainly to the combination of these developments. Two key elements of Digital Trust relate to security and privacy. With unprecedented levels of personal information shared by consumers regarding their habits, hobbies, and households, a breach of Trust can quickly result in serious negative business consequences such as consumer alienation and brand erosion. Therefore, companies must ensure Digital Trust across all their products and services and establish accountability for appropriate security and privacy measures. The requirement to build and maintain Digital Trust must be treated as an enterprise concern in order to underpin companies' business strategies for the digital age.

The proliferation of mobile devices (i.e. smartphones, tablets, hybrids, etc.) and a new generation of devices that is equipped with embedded software and communicating/actuating capabilities has a profound impact on multiple sectors of our society at large and the economy in particular. With many of these Things seamlessly connected, a virtual continuum of interconnected and addressable objects is created as part of a global network. This Internet of Things will change the very foundation of competition and will drive new business models including industrial automation, energy distribution, logistics, and agriculture.

Further adoption of IoT and the achievement of its full potential will depend on two key factors that need further elaboration: interoperability and security/privacy. Current technology and related standards are relatively immature and make interoperability of proposed solutions between the various Things a real challenge. Even though standardization bodies cooperate to avoid conflicting standards, the standards landscape is fragmented and some existing standards still overlap. Secondly, the various connected devices (such as medical equipment, smart meters and smartphones) may not have the required security protections implemented, resulting in the potential misuse of personal data.

The benefits of Cloud Computing are far-reaching as it delivers supporting technology to organizations more efficiently than ever before. The realized benefits of Cloud Computing continue to grow and include:

- Business agility and flexible disaster recovery capacity.
- IT investment savings, with a shift from CapEx to OpEx.
- IT budget re-allocation (from run & maintain to deploy & exploit).
- Increased responsiveness and speed of deployment.
- Improved reliability, security, and change frequency security.
- Enablement of "web native" applications (social, mobile, IoT).

Cloud Computing has transformed business and government practices. In particular, the positioning of IT departments within organizations needs to be reconsidered. Mooney [27] specified imperatives to prepare a company for the Cloud in their shift from server- to service-based thinking, towards brokering Cloud services to the entire organization:

- Re-define the IT value proposition.
- Re-structure IT governance.
- Re-document enterprise architecture.
- Re-engineer the IT organization.
- Re-allocate IT funding.

In other words, the defining implications of Cloud Computing are for:

- Corporations: a shift from "owning resources" to "using capabilities".
- IT departments: a shift from "managing IT" to "deploying services".

Cloud Computing adoption is still growing, which is particularly the case for hybrid Cloud adoption, because of the recent trend of growth in the use of private Cloud, combined with the ubiquity of public Cloud. Cloud providers are still improving their service offerings and Cloud best practice is becoming more and more established.

Despite of all these advances, new security challenges have emerged and existing vulnerabilities have been amplified. Although security and privacy can be adoption barriers because of the increasing maturity of both Cloud providers and users, a reduction in concerns about Cloud security is emerging. In fact, the shortage of trained resources/expertise has overtaken security as the top Cloud challenge [61]. Other issues relate to cost concerns, although few organizations are actively working to reduce costs and to further improve Cloud ROI. Therefore, organizations should consider moving additional workloads to Cloud, especially their systems of records, while also planning to optimize existing Cloud usage and looking for ways to reduce costs, such as adapting existing workloads to the Cloud Service Providers cost models.

Big Data is growing faster than many businesses can cope with, and is less about data that is big than it is about the Analytics capability to aggregate, search, cross-reference, and visualize large data sets. The opportunities for businesses, governments and academia are manifold. Examples include real-time customer service offerings, productivity increases and cost reductions, logistic chain optimizations, improved financial fraud detection and prevention, monitoring and dismantling terrorist networks, better scientific modeling of natural disasters and revealing hidden correlations for treating genetically inherited diseases.

Big Data Analytics is seen by many businesses as a way to gain advantage over their competitors. Therefore, many businesses are experimenting with and implementing Big Data capabilities. For an organization to get the greatest benefit from their Big Data capability, the data must be validated first to ensure that the quality of data fits its purpose. The result of Big Data analytics must be easy-to-understand, consumable information integrated with the intuitive knowledge of co-workers to create actionable information. In addition, an organization must have processes in place in order to apply actionable information gained through the process.

Big Data technologies are still in the initial stages of development and challenges include capture, curation, storage, search, sharing, transfer, analysis, and visualization [159]. Therefore, more capital investment should be made to further develop the practice and science of Big Data. New standards should be set from both a technological and privacy perspective. And as a matter of urgency, the inadequate and outdated data protection regulations need to be modernized. The new EU data protection rules for personal data

protection recently adopted by the European Parliament[67] (GDPR approved by the EU parliament on April 14th 2016 [62]) are a good example of steps taken in this direction.

IoT applications, Cloud Computing and Big Data Analytics can contribute to sustainable development at international, regional, and local levels. However, some issues still need to be resolved. Although security is no longer the top challenge for Cloud Computing, now is the time to build security and privacy by design for these three technologies to enhance Digital Trust. As regards privacy specifically, a common understanding of ownership rights to data supported by up-to-date regulations will provide transparency regarding what data are used, how data are being used, and ensure that the data are appropriately protected. Moreover, it is important to create compelling value propositions for data that is being collected and used.

Furthermore, to allow widespread adoption of IoT and enable its full value to be achieved, the cost of basic hardware must continue to fall and the ability of IoT devices to interoperate must be improved. Interoperability and portability issues also apply to Cloud Computing and to a lesser extent, Big Data Analytics. The adoption of open and international standards will play a crucial role in achieving these goals. ICT actors need to work together to better align their security and privacy requirements, architectures, and initiatives, in order to conceive state-of-the art Digital Trust in industry and accelerate adoption of these three fascinating technologies to benefit society as a whole.

In addition to being a key factor for Trust in ICT and for business development, standardization is also further promoted by the European Commission for the Digital Single Market [160]. Since standards ensure the interoperability of digital technologies, they provide the necessary foundations for achieving such a level of cooperation among EU countries by ensuring the smooth and reliable interaction of technologies, fostering research and innovation, and thus enabling economies of scale. Not only is the need for well-defined standards now recognized, but also the urgent necessity of bringing together the different standardization bodies and striking a balance between the manufacturing industry and service sectors. The increasing complexity of standard proliferation and the diversity of technical standardization technical committees that are involved, present a risk for innovation.

In that scope, the EU Commission has recently published a communication[68] establishing ICT standardization priorities for the Digital Single Market (DSM). It defines five priority areas: 5G communications, Cloud Computing, the Internet of Things, (Big) Data technologies and Cybersecurity, which are considered to be the essential building blocks of the DSM. The Commission proposes a number of actions to develop these areas:

- It intends to "support funding the development and use of the ICT standards needed to further improve the interoperability and portability of the cloud. This includes making more use of open source elements by better integrating open source communities into SDOs' standard setting processes, by the end of 2016".
- It will "foster an interoperable environment for the Internet of Things, working with ESOs and international SDOs" and "Explore options and guiding principles, including developing standards, for trust, privacy and end-to-end security, e.g. through a 'trusted IoT label'".
- It will "Increase R&D&I investment specifically for data interoperability and standards as of 2016. This will cover areas such as (i) cross-sectorial data integration (e.g. for entity identifiers, data models, multilingual data management, etc.); (ii) better interoperability of data and associated metadata. This will also be used to contribute to global standardization in the field of data."

[67] http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era

[68] COM (2016) 176: ICT Standardisation Priorities for the Digital Single Market

The EU Commission considers cybersecurity as a transversal block and "invites ESOs, other SDOs and relevant stakeholders to draw up practical guidelines covering IoT, 5G, Cloud, Big Data and smart factories. These should aim to ensure that security and seamless secure authentication are considered from the outset in the development of ICT standards. They should highlight best practices and gaps to be addressed. Based on the degree of uptake and progress, the Commission will consider adopting a Recommendation by end 2017 regarding the integration of cyber security and application of privacy and personal data protection requirements including data protection-by-design and data protection-by-default".

The actions planned by the EU Commission are also aimed at stimulating digital transformation of industry in a broader sense. For example, they should therefore enable the establishment of more effective and safer healthcare systems (especially through better data interoperability) and encourage the development of intelligent transport systems or intelligent energy systems.

The EU Commission plans to complement these priority actions with a high-level process that will complement the European Multi-stakeholders Platform[69], the ICT Rolling Plan on ICT Standardisation[70], and the Annual Union Work Programme for European Standardisation[71]. This high-level process is aimed at:

- Validating priorities and improving the efficiency of the standard-setting process in Europe;
- Regularly reviewing and monitoring progress;
- Improving EU support for ICT priority standardization;
- Ensuring fair and non-discriminatory access to ICT standardization;
- Strengthening the EU's presence in international dialogue and cooperation on ICT standards.

Through the establishment of these ICT standardization priorities for the Digital Single Market, the EU Commission aims to build an interoperable and secure environment to allow the proper development of Smart ICT through standardization.

Furthermore, at a national level, the *National Cybersecurity Strategy II* [161] aims to establish the necessary framework for meeting security-related challenges through "*norms, standards, certificates, labels, and frames of reference for requirements for the government and critical infrastructures*". These strategic priorities from Luxembourg and the EU particularly stress the importance of Digital Trust and ICT standardization for a sector that will be more crucial than ever to every country's economy in the decades to come and cross almost all economic sectors.

In order to make further progress in the area of "Digital Trust for Smart ICT", ILNAS has notably focused on developing a scheme of education about technical standardization and associated ICT research activities, providing the necessary support to strengthen technical standardization at national level and thus serve stakeholders' economic interests. Within this framework, ILNAS is conducting a national technical standardization strategy for 2014-2020[72], and, directly linked to this, "Luxembourg's Policy on ICT technical standardization for 2015-2020"[73], a strong policy regarding the ICT sector.

[69] https://ec.europa.eu/digital-single-market/european-multi-stakeholder-platform-ict-standardisation

[70] http://ec.europa.eu/DocsRoom/documents/15783/attachments/1/translations/en/renditions/native

[71] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52015DC0686

[72] http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf

[73] http://www.portail-qualite.public.lu/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-TIC-2015-2020/Policy-on-ICT-technical-standardization-_2015-2020_.pdf

Indeed, the ILNAS Policy on ICT Technical Standardization has been defined in order to foster and strengthen the national ICT sector involvement in standardization work through three leading projects: a) developing market interest and involvement, b) promoting and reinforcing market participation, and c) supporting and strengthening the Education about Standardization (EaS) and related research activities. In this way, ILNAS has been actively working on the implementation of the ICT technical standardization policy resulting in concrete developments and projects.

Firstly, ILNAS is directly involved in the main standardization organizations, ensuring Luxembourg's positioning in international development and facilitating knowledge transfer to the market. Regarding the ICT sector, ILNAS is particularly interested in leading the Joint Technical Committee ISO/IEC JTC 1, which is one of the most recognized producers of ICT International Standards. Moreover, ILNAS, through its Digital Trust department, is the national representative of the "European Multistakeholder platform on ICT Standardization", which is notably responsible for the annual development of a "Rolling Plan on ICT Standardization", defining the most important standardization initiatives and actions supporting EU policies.

Secondly, ILNAS is strengthening its relation with academic partners in order to structure standards-related education and research in Luxembourg. In this context, and within the framework of developing a national standardization culture, ILNAS has created a university certificate entitled "Smart ICT for Business Innovation" in partnership with the University of Luxembourg.

This professional training, which is considered a priority for fostering the transfer of normative knowledge through training and awareness-raising at national level, addresses Smart ICT across the technical standardization and business innovation spectrum.

Moreover, this pilot project conducted between September 2015 and September 2016 was only the first step in Education about Standardization projects run by ILNAS. The main objective is to offer a Master degree related to technical standardization. This project is directly based on the university certificate pilot project and would address Smart ICT topics in line with national priorities, providing a smart way of linking technology, standards, and business and creating an additional means of innovate at national level.

Directly linked with this Master flagship project, the development of related research activities constitutes a crucial component in generating the necessary knowledge for such a specialization. Therefore, ILNAS will set up a 4-year research program dedicated to "Digital Trust for Smart ICT". This research program aims to build a solid base of knowledge and expertise in Smart ICT taking into account aspects related to security, reliability, and standardization and considering Digital Trust as a transversal axis. The associated research activities are considered to be crucial to the development of the future Master program and consolidation of the university certificate and future activities of education about standardization.

Finally, through these developments and prospective projects, ILNAS is contributing to the creation of a Trust environment at national level by strengthening the use of recognized best practice advocating interoperability, security, quality, safety, and more importantly, standards and technical standardization.

REFERENCES

[1] G. Walsham, "Knowledge management: the benefits and limitations of computer systems," *Eur. Manag. J.*, vol. 19, no. 6, pp. 599–608, 2001.

[2] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational Trust," *Acad. Manag. Rev.*, vol. 20, no. 3, pp. 709–734, 1995.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[4] D. M. Huang, J., Nicol, "A Formal-Semantics-Based Calculus of Trust," in *IEEE Internet Computing, 14(5)*, 2010, pp. 38–46.

[5] F. Rowley, J., & Johnson, "Understanding trust formation in digital information sources: The case of Wikipedia," *J. Inf. Sci.*, 2013.

[6] F. Giustiniano, L., Bolici, "Organizational trust in a networked world: Analysis of the interplay between social factors and Information and Communication Technology," *J. Information, Commun. Ethics Soc.*, vol. 10, no. 3, pp. 187–202, 2012.

[7] W. Tan Y. H., Thoen, "A logical model of trust in e-commerce," *Electron. Mark.*, vol. 10, pp. 258–263, 2011.

[8] Accenture, "Digital Trust in the IoT Era." Accenture Consulting, 2015.

[9] D. Jeffrey and G. Sanjay, "MapReduce: Simplified Data Processing on Large Clusters," in *OSDI*, 2004.

[10] ITU Internet Reports, "The Internet of Things," 2005.

[11] Cisco, "The Zettabyte Era Trends and Analysis." 2015.

[12] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1–31, 2014.

[13] OECD, "OECD Digital Economy Outlook 2015," OECD Publishing, Paris, report, 2015.

[14] ITU-T, "Overview of the Internet of things. Recommendation ITU-T Y.2060," 2012.

[15] K. Gama, L. Touseau, and D. Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware," *Comput. Commun.*, vol. 35, no. 4, pp. 405–417, 2012.

[16] OECD, "Machine-to-machine communications: Connecting billions of devices," OECD Digital Economy Papers, OECD Publishing, Paris, report, 2012.

[17] J. S. Wilson, *Sensor technology handbook*. Elsevier, 2004.

[18] OECD, "Cloud Computing: The Concept, Impacts and the Role of Government Policy," 2013.

[19] J. Hogan, M., Liu, F., Sokol, A., Tong, "Nist cloud computing standards roadmap," 2011.

[20] CSA, "Security Guidance for critical areas of focus in cloud computing V3.0," Cloud Security Alliance, report, 2011.

[21] H. Yang and M. Tate, "A descriptive literature review and classification of cloud computing research," *Commun. Assoc. Inf. Syst.*, vol. 31, no. 2, pp. 35–60, 2012.

[22] Y. Duan, "Value Modeling and Calculation for Everything as a Service (XaaS) based on Reuse," *Softw. Eng. Artif. Intell. Netw. Parallel Distrib. Comput.*, vol. 13, pp. 162--167, 2012.

[23] R. R, S. G., M. S., V. L. Ghorade, M. S. Surendrababu, and S. B. Basapur, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions," *Int. J. Cloud Comput. Serv. Archit.*, vol. 3, no. 4, 2013.

[24] F. Corradini, D. Angelis, I. F., F., and F. Marcantoni, "A Survey of Trust Management Models for Cloud Computing," *5th Int. Conf. Cloud Comput. Serv. Sci. Lisbon*, 2015.

[25] R. K. Kalluri and C. G. Rao, "Addressing the Security, Privacy and Trust Challenges of Cloud Computing," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6094–6097, 2014.

[26] P. Manuel, "A trust model of cloud computing based on Quality of Service," *Ann. Oper. Res.*, vol. 233, no. 1, pp. 281–292, 2015.

[27] J. Mooney, *Essential Practices for Embracing the Inevitability of the Cloud*. MIT Sloan School of Management, Center for Information Systems Research, Boston, {MA}, 2012.

[28] CSA, "The Treacherous 12 - Cloud Computing Top Threats in 2016," Cloud Security Alliance, report, 2016.

[29] CSA, "Defined Categories of Security as a Service - Continuous Monitoring as a Service, Security as a Service Working Group," Cloud Security Alliance, report, 2016.

[30] O. Kwon, N. Lee, and B. Shin, "Data quality management, data usage experience and acquisition intention of big data analytics," *Int. J. Inf. Manage.*, vol. 34, no. 3, pp. 387–394, 2014.

[31] M. Cox and D. Ellsworth, "Managing big data for scientific visualization," in *ACM Siggraph*, 1997, vol. 97, p. 21.

[32] D. Laney, "3D data management: Controlling data volume, velocity and variety," *META Gr. Res. Note*, vol. 6, p. 70, 2001.

[33] M. Schroeck, R. Shockley, J. Smart, D. Romero-Morales, and P. Tufano, "Analytics: The real-world use of big data: How innovative enterprises extract value from uncertain data," *IBM Inst. Bus. Value*, 2012.

[34] P. Zikopoulos, K. Parasuraman, T. Deutsch, J. Giles, D. Corrigan, and others, *Harness the power of big data The IBM big data platform*. McGraw Hill Professional, 2012.

[35] K. Kambatla, G. Kollias, V. Kumar, and A. Grama, "Trends in big data analytics," *J. Parallel Distrib. Comput.*, vol. 74, no. 7, pp. 2561–2573, 2014.

[36] J. Girard, *Strategic Data-Based Wisdom in the Big Data Era*. IGI Global, 2015.

[37] R. Jin, "Lectures in Advanced Computing Platforms for Data Processing." 2014.

[38] Lin. C., "Lectures in Big Data Analytics." 2016.

[39] ILNAS & ANEC, "White Paper Big Data," 2016.

[40] N. Kshetri, "Big data's impact on privacy, security and consumer welfare," *Telecomm. Policy*, vol. 38, no. 11, pp. 1134–1145, 2014.

[41] H. Ekbia, M. Mattioli, I. Kouper, G. Arave, A. Ghazinejad, T. Bowman, and C. R. Sugimoto, "Big data, bigger dilemmas: a critical review," *J. Assoc. Inf. Sci. Technol.*, 2015.

[42] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behaviour," in *Proceedings of the National Academy of Sciences*, 2013, pp. 5802–5805.

[43] D. Boyd and K. Crawford, "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon," *Information, Commun. Soc.*, vol. 15, no. 5, pp. 662–679, 2012.

[44] T. F. Dapp and V. Heine, *Big data. The untamed force*. 2014.

[45] V. Wessel, T. R., F., and ILNAS, "White Paper Digital Trust, Towards Excellence in ICT," ILNAS, report, 2014.

[46] Accenture, "Accenture Digital Consumer Survey." Accenture Consulting, 2015.

[47] PWC, *Building Digital Trust. The confidence to take risks*. {PricewaterhouseCoopers} {B.V.}, The Netherlands, 2014.

[48] V. A. Almeida, D. Doneda, and M. Monteiro, "Governance Challenges for the Internet of Things," *IEEE Internet Comput.*, vol. 4, pp. 56–59, 2015.

[49] EU Commission, "Report on the Consultation on IoT Governance," 2013.

[50] Federal Trade Commission, "Internet of Things: Privacy & Security in a Connected World, FTC Staff Report," 2015.

[51] McKinsey, "The Internet of Things: mapping the value beyond the hype." McKinsey Global Institute, 2015.

[52] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, vol. 17, pp. 1–6, 2015.

[53] Gartner, "Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016." Gartner, 2015.

[54] OECD, "Sustainable Manufacturing Toolkit. Seven Steps to Environmental Excellence." {OECD} Directorate for Science, Technology and Industry ({DSTI}), {OECD} Publishing, Paris, 2011.

[55] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges," *Comput. Commun.*, vol. 36, pp. 1665–1697, 2013.

[56] ITU, "ICT as an Enabler for Smart Water Management." 2010.

[57] C. Chen, D. J. Cook, and A. S. Crandall, "The user side of sustainability: Modeling behavior and energy usage in the home," *Pervasive Mob. Comput.*, vol. 9, no. 1, pp. 161–175, 2013.

[58] IBM, "Managing Ireland's water supply with predictive analytics. Helping reduce loss and save resources." IBM Research Ireland, 2013.

[59] F. Delmastro, "Pervasive communications in healthcare," *Comput. Commun.*, vol. 35, no. 11, pp. 1284–1295, 2012.

[60] CSA, "State of Cloud Security 2016," Cloud Security Alliance, report, 2016.

[61] RightScale, "State of the Cloud Report." {RightScale} Inc, Santa Barbara CA, 2016.

[62] EU Parliament Press Service, "Data protection reform - Parliament approves new rules fit for the digital era Press release," no. 20160407, pp. 2–4, 2016.

[63] CSA, "The Cloud Balancing Act for IT: Between Promise and Peril," Cloud Security Alliance, report, 2016.

[64] Wikibon, "Executive Summary: Big Data Vendor Revenue and Market Forecast, 2011-2026." 2015.

[65] Wikibon, "Big Data Vendor Revenue and Market Forecast 2013-2017." 2014.

[66] UNCTAD, "Issues Paper On Foresight for Digital Development." 2015.

[67] K. A. Wetterstrand, "DNA Sequencing Costs: Data from the NHGRI Genome Sequencing Program (GSP)," 2016.

[68] W. C. and P. J., "An Updated Privacy Paradigm for the 'Internet of Things,'" in *Future of Privacy Forum, November 19, 2013*, 2013.

[69] V. Kumar, B. Chejerla, S. Madria, and M. Mohania, "A survey of trust and trust management in cloud computing," in *Managing Trust in Cyberspace*, T. M. S. and others, Eds. CRC Press, Taylor and Francis Group, 2013, pp. 41–69.

[70] J. Emeras, S. Varrette, and P. Bouvry, "Amazon Elastic Compute Cloud (EC2) vs. in-House HPC Platform: a Cost Analysis," in *9th IEEE International Conference on Cloud Computing (Cloud)*, 2016.

[71] X. Besseron, J. Emeras, B. Peters, S. Varrette, and P. Bouvry, "HPC or the Cloud: a cost study over an XDEM Simulation," in *7th International Supercomputing Conference in Mexico (ISUM)*, 2016.

[72] B. H. Wixom, "Cashing in on Your Data," *CISR Res. Brief.*, vol. XIV, no. 18, 2014.

[73] B. H. Wixom, J. W. Ross, C. M. Beath, and C. A. Miller, "Capturing Value From Big Data at ComScore Through Platform, People and Perception," *CISR Res. Brief.*, vol. XII, no. 11, 2013.

[74] M. M. L. Wixom B.H., "Data Value Assessment: Recognizing Data as an Enterprise Asset," *CISR Res. Brief.*, vol. XV, no. 3, 2015.

[75] B. C. M. Wixom B.H., "Winning the Data Race," *CISR Res. Brief.*, vol. XIV, no. 3, 2014.

[76] K. J. Hole, *Anti-fragile ICT Systems*, Simula Spr. Cham: Springer International Publishing, 2016.

[77] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, no. 973, pp. 647–651, 2012.

[78] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science (80-.).*, vol. 347, no. 6221, pp. 509–514, 2015.

[79] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big Data Privacy in the Internet of Things Era," *IT Prof.*, vol. 17, no. 3, pp. 32–39, 2015.

[80] R. P. Minch, "Location Privacy in the Era of the Internet of Things and Big Data Analytics," *Syst. Sci. (HICSS), 2015 48th Hawaii Int. Conf.*, pp. 1521–1530, 2015.

[81] EU Commission, "Proposal for a Regulation of the European Parliament and of the Council EUR-Lex - 52012PC0011," 2012.

[82] P. Schaar, "Privacy by Design," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 267–274, Apr. 2010.

[83] T. Antignac and D. Le M, "Privacy by Design : From Technologies to Architectures," *Priv. Technol. Policy*, pp. 1–17, 2014.

[84] J. Hoepman, "Privacy Design Strategies," *ICT Syst. Secur. Priv. Prot.*, pp. 446–459, 2014.

[85] Ben C. F. Cho and J. Tam, *Privacy by Design: Examining Two Key Aspects of Social Applications*, HCI in Bus., vol. 9191. Cham: Springer International Publishing, 2015.

[86] M. Duckham, L. Kulik, and A. Birtley, "A Spatiotemporal Model of Strategies and Counter Strategies for Location Privacy Protection," *4th Int. Conf. GIScience '06*, pp. 47–64, 2006.

[87] D. Slamanig, T. Lor, and L. Thomas, "E-Democracy – Citizen Rights in the World of the New Computing Paradigms," vol. 570, pp. 202–206, 2015.

[88] P. Michelucci, Ed., *Handbook of Human Computation*. New York, NY: Springer New York, 2013.

[89] ILNAS & TUDOR, "White Paper Digital Trust," 2012.

[90] OECD, "OECD Guidelines for the Security of Information Systems and Networks," *Organ. Econ. Co-operation Dev.*, 2002.

[91] G. Stoneburner, C. Hayden, and A. Feringa, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A," *NIST Spec. Publ. 800-27 Rev A*, p. 35, 2004.

[92] IEC Standard 61505, "Industrial-Process Measurement and Control Evaluation of System Properties for the Purpose of System Assessment, Part 5: Assessment of System Dependability, Publication 1069-5," 1992.

[93] Document ISO/TC 176/SC 1 N 93, "Quality Concepts and Terminology part 1: Generic Terms and Definitions," 1992.

[94] ISO/IEC 27000:2009, "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary," 2009.

[95] A. Avižienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secur. Comput.*, vol. 1, no. 1, pp. 11–33, 2004.

[96] ITSEC, "Information Technology Security Evaluation Criteria," 1991.

[97] ISO/IEC Standard 15408, "Common Criteria for Information Technology Security Evaluation," 1999.

[98] F. Cavenne, *ICT Systems Contributing to European Secure-by-Design Critical Infrastructures*, ISSE 2009. Wiesbaden: Vieweg+Teubner, 2009.

[99] R. Rew and G. Davis, "NetCDF: An Interface for Scientific Data Access," *IEEE Comput. Graph. Appl.*, vol. 10, no. 4, pp. 76–82, 1990.

[100] K. Kosanke, "ISO Standards for Interoperability: a Comparison," in *Interoperability of Enterprise Software and Applications*, D. Konstantas, J.-P. Bourrières, M. Léonard, and N. Boudjlida, Eds. London: Springer London, 2006, pp. 55–64.

[101] S. Pearson, M. C. Mont, and S. Crane, "Persistent and Dynamic Trust: Analysis and the Related Impact of Trusted Platforms," *Security*, vol. 3477, pp. 355–363, 2005.

[102] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci.*, pp. 693–702, 2010.

[103] Fujitsu Limited, "Personal data in the cloud: A global survey of consumer attitudes," 2010.

[104] H. Sato, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," *Proc. - 2010 10th Annu. Int. Symp. Appl. Internet, SAINT 2010*, pp. 121–124, 2010.

[105] H. I. Albert S. and A. Rajeev, "Trust in Cloud Computing," *Ieee*, pp. 01–08, 2015.

[106] A. Kanwal, R. Masood, U. E. Ghazia, M. A. Shibli, and A. G. Abbasi, "Assessment criteria for trust models in cloud computing," in *Green Computing and Communications ({GreenCom})*, I. I. C. on, P. IEEE Cyber, and S. Computing, Eds. 2013, pp. 254–261.

[107] I. M. Abbadi and A. Martin, "Trust in the Cloud," *Inf. Secur. Tech. Rep.*, vol. 16, no. 3, pp. 108–114, 2011.

[108] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 2, no. 1, pp. 1–14, 2013.

[109] M. Firdhous, O. Ghazali, and H. Suhaidi, "Trust management in cloud computing: a critical review," *Int. J. Adv. ICT Emerg. Reg.*, 2011.

[110] H. M. Alabool and A. K. Mahmood, "A novel evaluation framework for improving trust level of Infrastructure as a Service," *Cluster Comput.*, pp. 1–22, 2015.

[111] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Prof.*, vol. 12, no. 5, pp. 20–27, 2010.

[112] J. Koodi and G. Srinivasachar, "Privacy-Preserving Multi-keyword Ranked Search Over Encrypted Cloud Data Key Words," *Int. Res. J. Eng. Technol.*, vol. 2, no. 3, pp. 2280–2284, 2015.

[113] N. Chandran, M. E. Chase, K. E. Lauter, and V. Vaikuntanathan, "User-controlled data encryption with obfuscated policy." Google Patents, 2015.

[114] J. Chen and H. Ma, "Privacy-preserving decentralized access control for cloud storage systems," *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 506–513, 2014.

[115] T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," *INFOCOM, 2013 Proc. ...*, pp. 2625–2633, 2013.

[116] R. Yan, Z. Li, X. Kantola, "Controlling Cloud Data Access Based on Reputation," *Mob. Networks Appl.*, no. March, pp. 828–839, 2015.

[117] S. U. R. Malik, S. U. Khan, S. J. Ewen, N. Tziritas, J. Kolodziej, A. Y. Zomaya, S. A. Madani, N. Min-Allah, L. Wang, C.-Z. Xu, Q. M. Malluhi, J. E. Pecero, P. Balaji, A. Vishnu, R. Ranjan, S. Zeadally, and H. Li, "Performance analysis of data intensive cloud systems based on data management and replication: a survey," *Distrib. Parallel Databases*, vol. 34, no. 2, pp. 179–215, Mar. 2015.

[118] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," *Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW '09*, no. Vm, p. 91, 2009.

[119] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, 2010.

[120] Y. C. Liu, Y. T. Ma, H. S. Zhang, D. Y. Li, and G. S. Chen, "A method for trust management in cloud computing: Data coloring by cloud watermarking," *Int. J. Autom. Comput.*, vol. 8, no. 3, pp. 280–285, 2011.

[121] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A framework for accountability and trust in cloud computing," *Proc. - 2011 IEEE World Congr. Serv. Serv. 2011*, pp. 584–588, 2011.

[122] M. Felici, T. Koulouris, and S. Pearson, "Accountability for Data Governance in Cloud Ecosystems," *2013 IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, pp. 327–332, 2013.

[123] B. Bertholon, S. Varrette, and P. Bouvry, "Certicloud: A Novel TPM-based Approach to Ensure Cloud IaaS Security," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, 2011, pp. 121–130.

[124] A. Kumbhare, Y. Simmhan, and V. Prasanna, "Cryptonite: A secure and performant data repository on public clouds," *Proc. - 2012 IEEE 5th Int. Conf. Cloud Comput. CLOUD 2012*, pp. 510–517, 2012.

[125] S. Varrette, B. Bertholon, and P. Bouvry, "A Signature Scheme for Distributed Executions Based on Control Flow Analysis," in *Security and Intelligent Information Systems: International Joint Conferences, SIIS 2011, Warsaw, Poland, June 13-14, 2011, Revised Selected Papers*, P. Bouvry, M. A. Kłopotek, F. Leprévost, M. Marciniak, A. Mykowiecka, and H. Rybiński, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 85–102.

[126] S. Naqvi, A. Michot, and M. Van De Borne, "Analysing impact of scalability and heterogeneity on the performance of federated cloud security," *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 1137–1142, 2012.

[127] M. Anisetti, C. A. Ardagna, and E. Damiani, "A certification-based trust model for autonomic cloud computing systems," *Proc. - 2014 Int. Conf. Cloud Auton. Comput. ICCAC 2014*, pp. 212–219, 2015.

[128] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From Security to Assurance in the Cloud: A Survey," *ACM Comput. Surv.*, vol. 48, no. 1, p. 2:1–2:50, Jul. 2015.

[129] USA Gov., "UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED (USA PATRIOT ACT) ACT OF 2001 An Act," 2001.

[130] P. Mirfield, "Regulation of Investigatory Powers Act 2000 (2): Evidential aspects," 2001.

[131] OECD, "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)," 2013.

[132] C. L. Philip Chen and C.-Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," *Inf. Sci. (Ny).*, vol. 275, pp. 314–347, Aug. 2014.

[133] A. Fernández, S. del Río, V. López, A. Bawakid, M. J. del Jesus, J. M. Benítez, and F. Herrera, "Big Data with Cloud Computing: an insight on the computing environment, MapReduce, and programming frameworks," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 4, no. 5, pp. 380–409, Sep. 2014.

[134] I. A. T. Hashem, I. Yaqoob, N. Badrul Anuar, S. Mokhtar, A. Gani, S. Ullah Khan, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, "The rise of 'big data' on cloud computing: Review and open research issues," *Inf. Syst.*, vol. 47, pp. 98–115, Aug. 2015.

[135] P. Buneman, S. Khanna, and W. C. Tan, "Why and Where: A Characterization of Data Provenance," *Icdt*, pp. 316–330, 2001.

[136] S. Ram and J. Liu, "A new perspective on semantics of data provenance," *CEUR Workshop Proc.*, vol. 526, pp. 1–6, 2009.

[137] L. Moreau, J. Freire, J. Futrelle, R. E. McGrath, J. Myers, and P. Paulson, *The Open Provenance Model: An Overview*, Provenance., vol. 5272. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[138] L. Moreau, B. Clifford, J. Freire, J. Futrelle, Y. Gil, P. Groth, N. Kwasnikowska, S. Miles, P. Missier, J. Myers, B. Plale, Y. Simmhan, E. Stephan, and J. Van den Bussche, "The Open Provenance Model core specification (v1.1)," *Futur. Gener. Comput. Syst.*, vol. 27, no. 6, pp. 743–756, Jun. 2011.

[139] P. Groth and L. Moreau, "PROV-Overview. An Overview of the PROV Family of Documents," World Wide Web Consortium, techreport, 2013.

[140] D. G. Feitelson, "From repeatability to reproducibility and corroboration," *ACM SIGOPS Oper. Syst. Rev.*, vol. 49, no. 1, pp. 3–11, 2015.

[141] X. Wu, X. Zhu, G. Q. Wu, and W. Ding, "Data mining with big data," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 1, pp. 97–107, Jan. 2014.

[142] ISACA, "Privacy and Big Data," 2013.

[143] ENISA, "Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems," 2015.

[144] M. Hurwitz, Judith and Nugent, Alan and Halper, Fern and Kaufman, *Big data for dummies*. John Wiley & Sons, Inc., 2013.

[145] G. Cormode and D. Srivastava, "Anonymized data," in *Proceedings of the 35th SIGMOD international conference on Management of data - SIGMOD '09*, 2009, p. 1015.

[146] X. Xinhua Dong, R. Ruixuan Li, H. Heng He, W. Wanwan Zhou, Z. Zhengyuan Xue, and H. Hao Wu, "Secure sensitive data sharing on a big data platform," *Tsinghua Sci. Technol.*, vol. 20, no. 1, pp. 72–80, Feb. 2015.

[147] P. Pääkkönen and D. Pakkala, "Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems," *Big Data Res.*, vol. 2, no. 4, pp. 166–186, 2015.

[148] OASIS, "eXtensible Access Control Markup Language (XACML) version 3.0," 2013.

[149] D. Barnard-Wills, L. Marinos, and S. Portesi, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media," 2014.

[150] R. Strackx, F. Piessens, and B. Preneel, "Efficient isolation of trusted subsystems in embedded systems," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 50 LNICST, pp. 344–361, 2010.

[151] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, "TyTAN: tiny trust anchor for tiny devices," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, pp. 1–6, 2015.

[152] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan, "TrustLite: A Security Architecture for Tiny Embedded Devices," *Proc. Eur. Conf. Comput. Syst.*, pp. 1–14, 2014.

[153] J. Van Bulck, "Towards Availability and Real-Time Guarantees for Protected Module Architectures," pp. 146–151, 2016.

[154] H. Sato, A. Kanai, S. Tanimoto, and T. Kobayashi, "Establishing Trust in the Emerging Era of IoT," in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2016, pp. 398–406.

[155] J. Suomalainen, "Smartphone assisted security pairings for the Internet of Things," in *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, 2014, pp. 1–5.

[156] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, D. Wagner, K. Thomas, M. Mccoyd, F. Li, and J. Chuang, "Smart Locks: Lessons for Securing Commodity Internet of Things Devices," 2016.

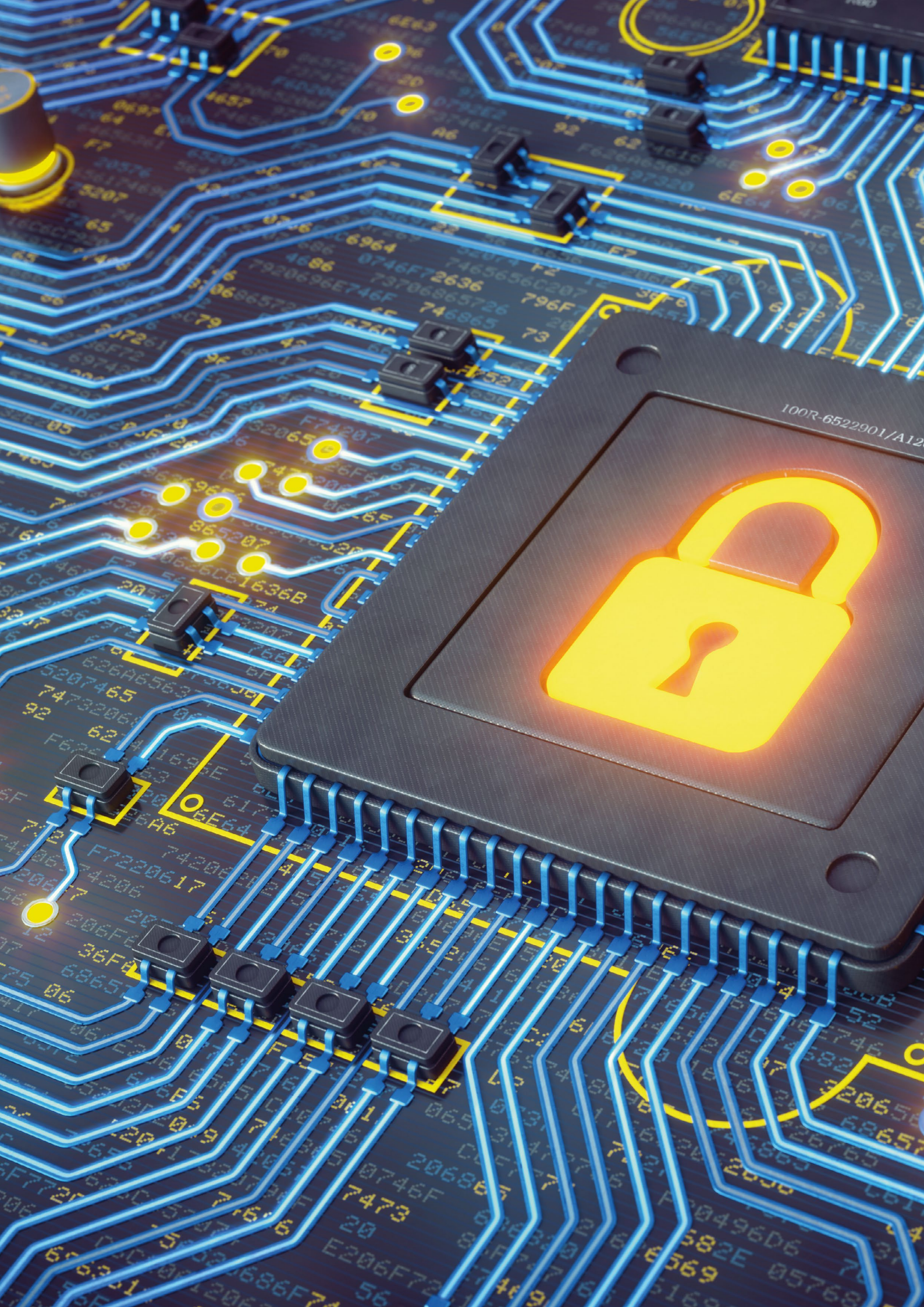
[157] NIST, "Guide to Bluetooth Security," 2012.

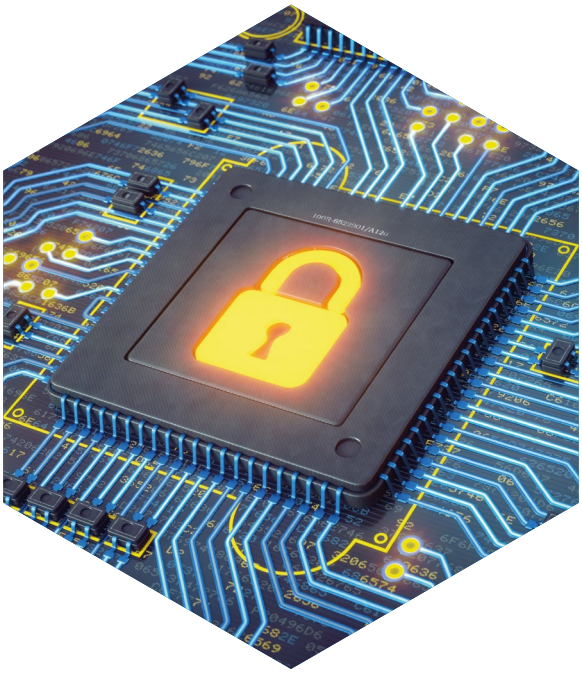
[158] ILNAS & ANEC, "Standards Analysis ICT Sector Luxembourg," 2016.

[159] Q. Huang, S. Jing, J. Yi, and W. Zhen, *Innovative Testing and Measurement Solutions for Smart Grid*. John Wiley & Sons, 2015.

[160] EU Commission, "ICT Standardisation Priorities for the Digital Single Market," 2016.

[161] Gouvernement du Grand-Duché de Luxembourg, "NATIONAL CYBERSECURITY STRATEGY II," 2015.





ILNAS

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

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