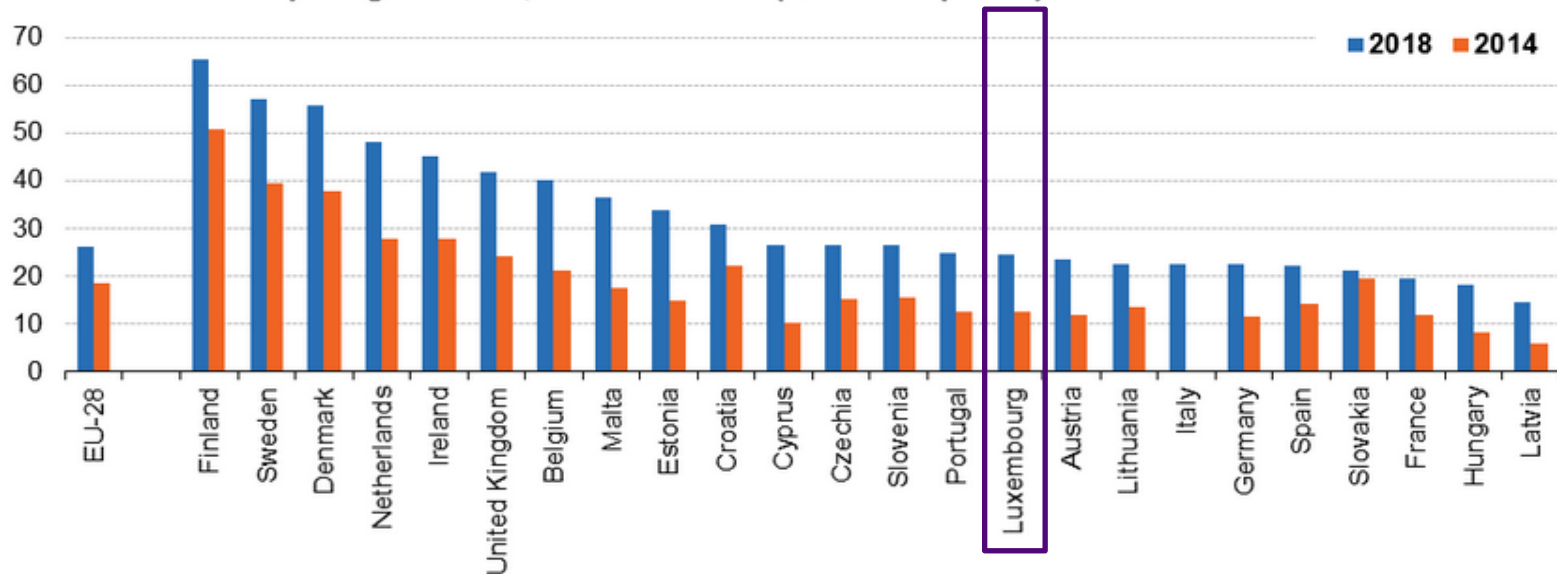- Breakfast Meeting -

Smart ICT: Gap Analysis between Scientific Research and Technical Standardization in the field of Cloud Computing

Chao LIU
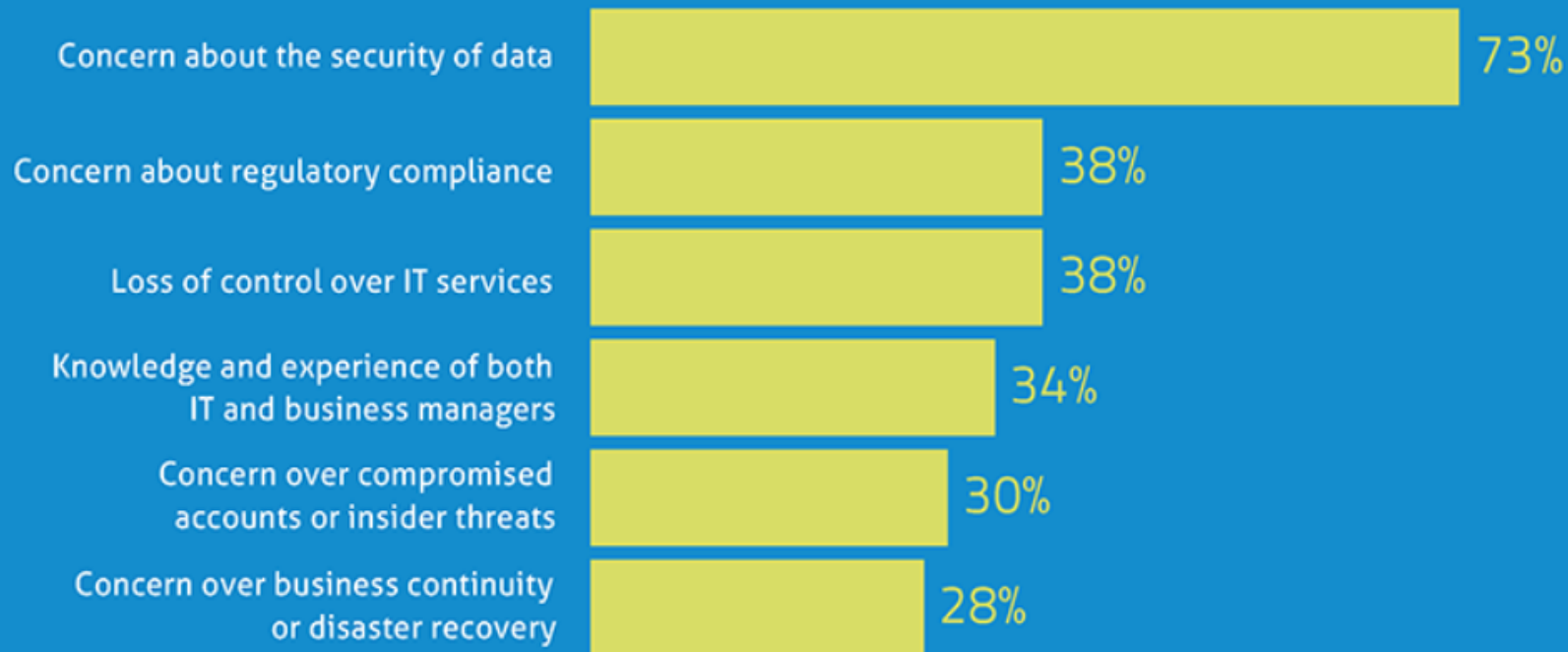
Feb 2020

Overview of the EU Cloud Market

- From 2014 to 2018, the use of Cloud Computing in the EU increased particularly in large enterprises

- Specifically, 24.5% of enterprises in Luxembourg used Cloud Computing in 2018 (26% EU-wide)

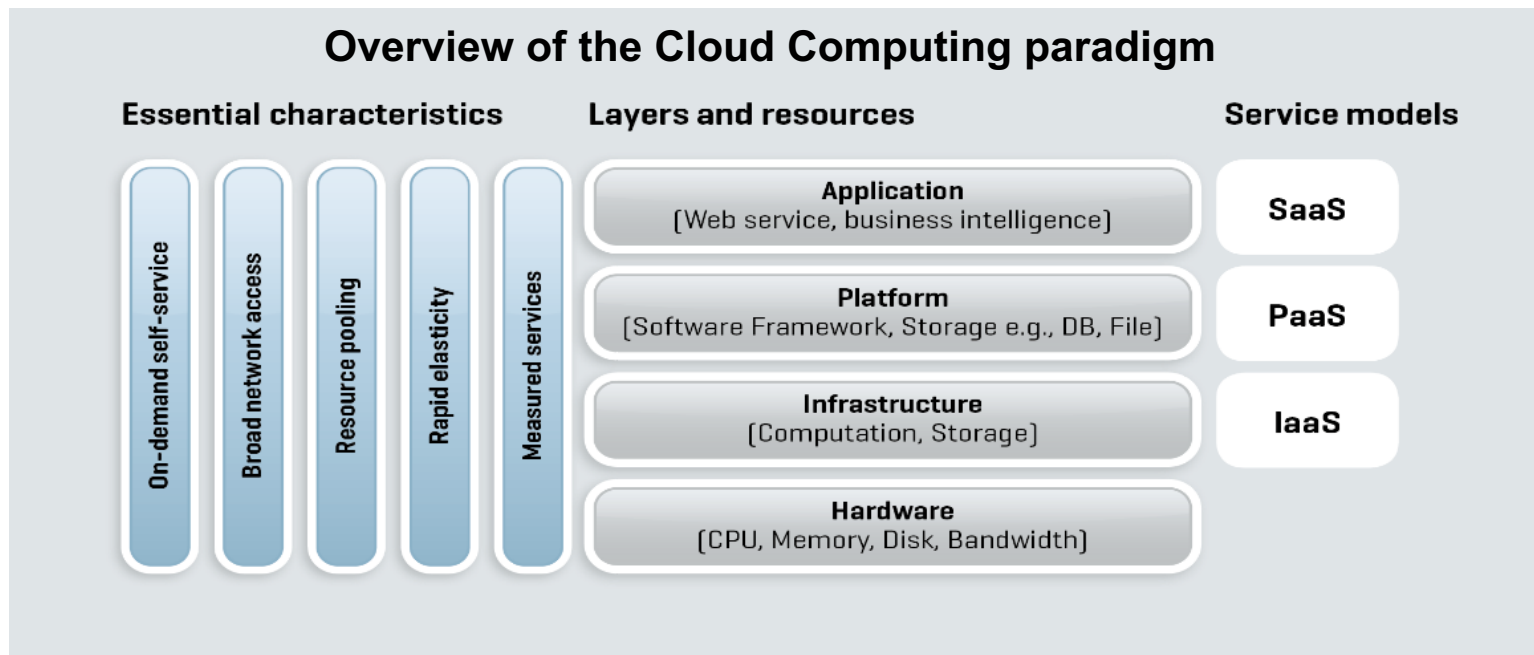**Use of cloud computing services, 2014 and 2018 (% of enterprises)**

Top Challenges

TOP CHALLENGES HOLDING BACK CLOUD PROJECTS

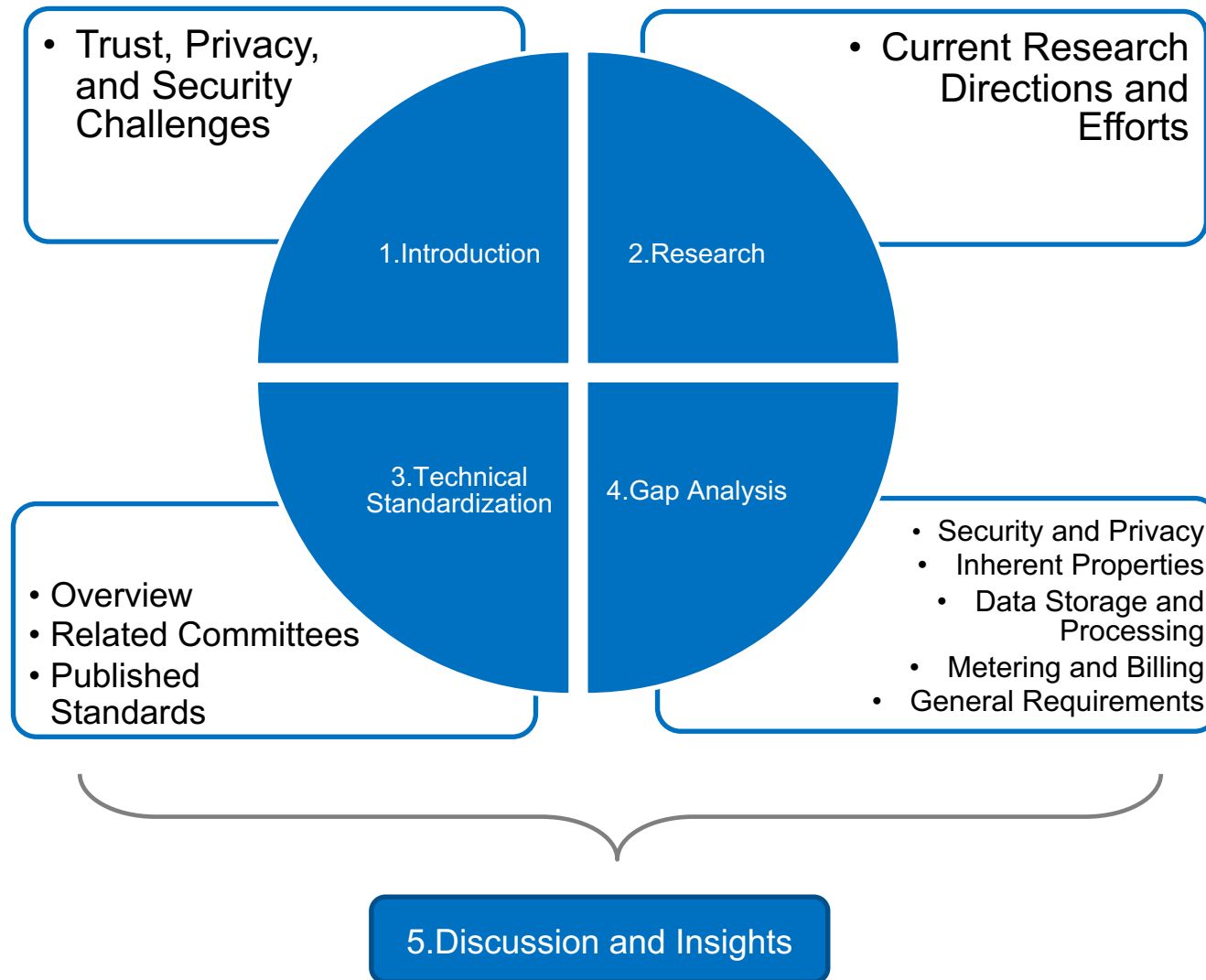| Challenge	Percentage
Concern about the security of data	73%
Concern about regulatory compliance	38%
Loss of control over IT services	38%
Knowledge and experience of both IT and business managers	34%
Concern over compromised accounts or insider threats	30%
Concern over business continuity or disaster recovery	28%

White Paper: Data Protection and Privacy in Smart ICT - Research and Standardization (2018)

Key Objectives

- Overview of data protection and privacy in Cloud Computing
- Clarifying the fundamentals of Cloud Computing
- Exploring the links between research and standardization, namely: frameworks of trust, interoperability and portability, terminology

Overview of the Cloud Computing paradigm

Essential characteristics	Layers and resources	Service models
On-demand self-service / Broad network access / Resource pooling / Rapid elasticity / Measured services	Application [Web service, business intelligence]	SaaS
	Platform [Software Framework, Storage e.g., DB, File]	PaaS
	Infrastructure [Computation, Storage]	IaaS
	Hardware [CPU, Memory, Disk, Bandwidth]	

White Paper: Data Protection and Privacy in Smart ICT-Scientific Research and Technical Standardization, ILNAS-UL 2018
A similar definition of Cloud computing is also provided by the National Institute of Standards and Technologies (NIST)

4

Technical Report: Smart ICT - Gap Analysis between Research and Standardization in Cloud Computing (2019)

- Trust, Privacy, and Security Challenges

- Current Research Directions and Efforts

1.Introduction

2.Research

3.Technical Standardization

4.Gap Analysis

- Overview
- Related Committees
- Published Standards

- Security and Privacy
  - Inherent Properties
    - Data Storage and Processing
  - Metering and Billing
- General Requirements

5.Discussion and Insights

Research Directions

1. Security and Privacy Controls
- The main task of access control is to export digital identities of end users and transfer the identity attributes to different computers to guarantee a secure environment for users.
- Various application scenarios request flexible control on cloud data access based on data owner policies and application demands.

2. Inherent Properties
- Cloud computing paradigm enables multi-tenancy, multiple cloud users share the virtualized resources and the physical devices.
- The dynamic of multi-tenancy further intensifies the complexity and brings more security challenges.

3. Data Storage and Processing
- Users' data is stored in distributed cloud services
- A third party service provider is allowed to offer clients a database service on the cloud through Database-as-a-Service.

4. Billing and Metering
- Cloud services rely on the "pay-as-you-go" model, but most cloud services providers, collecting users' data in order to evaluate their pricing model, risks for users' data protection and privacy issues are involved.
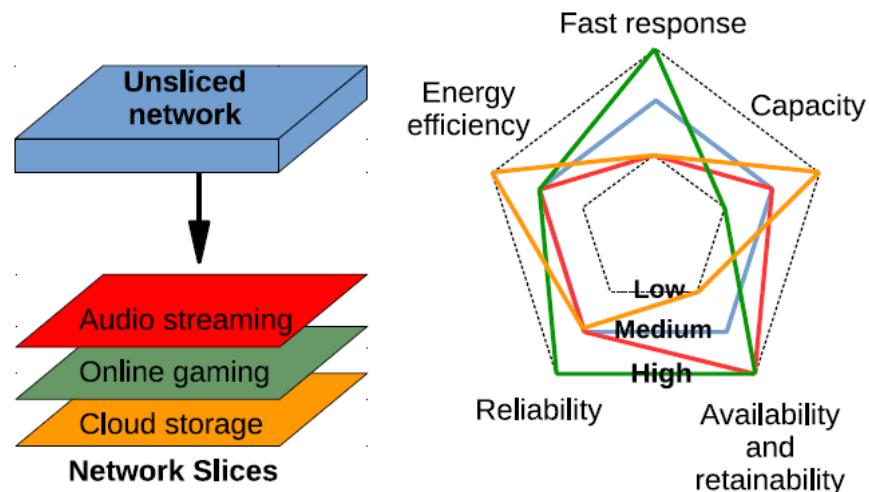
5. Network Slicing
- New scenario for the adoption of cloud computing

Data Protection and Privacy in Cloud Computing

Research Directions: IaaS in Network Slicing

- The Slice Provider (SP) owns the physical resource and multiple Slice Customers (SCs) serve their end users with various network slices which created by SP

- End-to-end network slicing has been viewed as a key enabler for 5g

Research Directions: Network Slicing in 3GPP
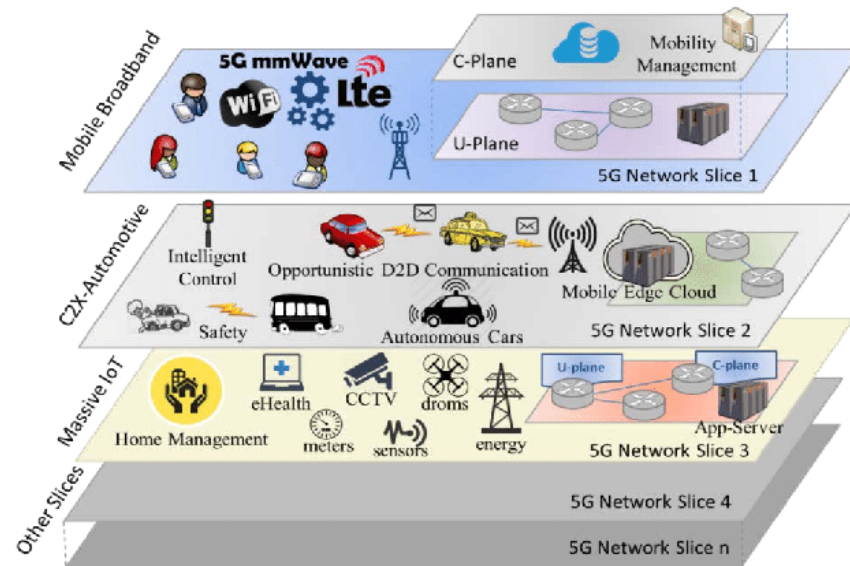
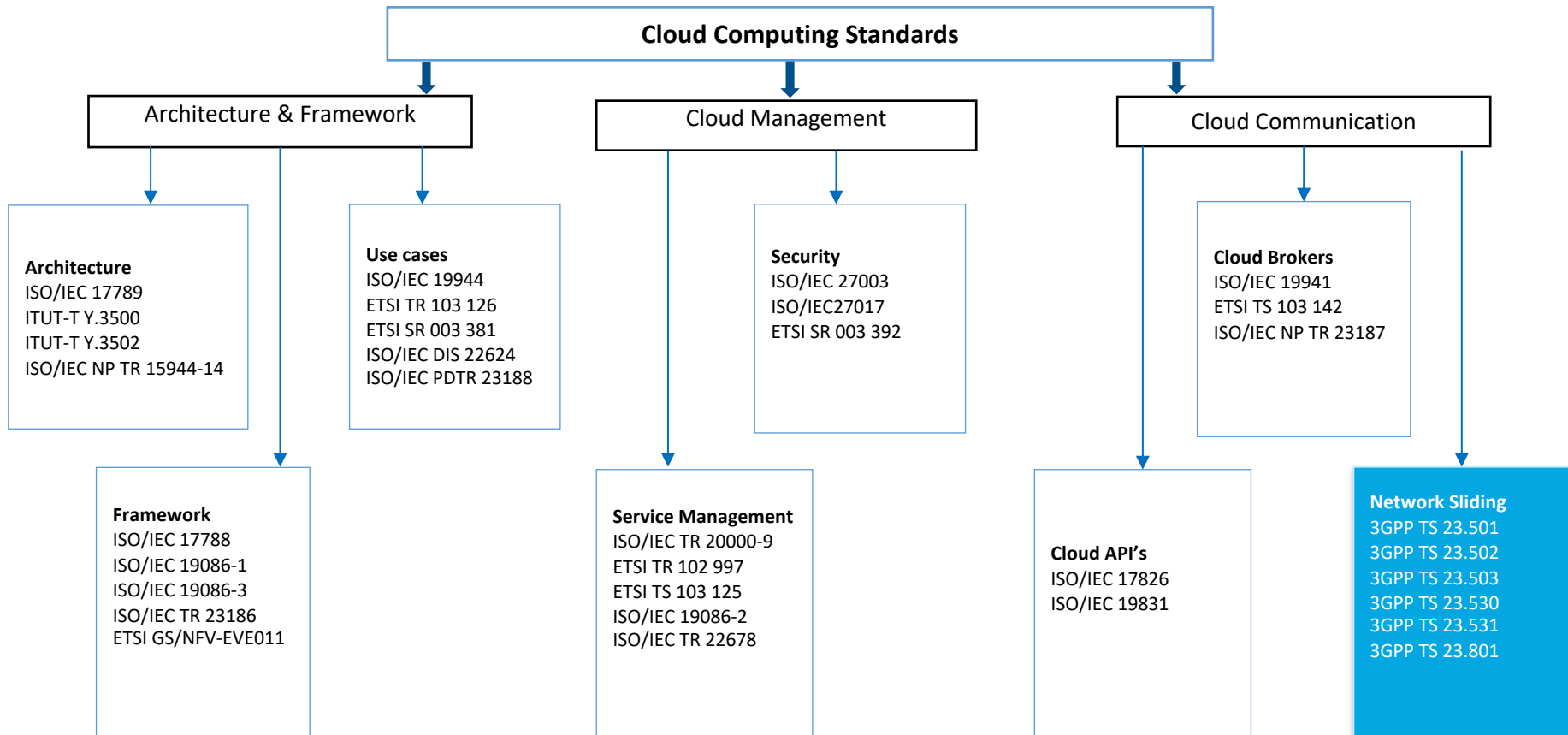| Slice/Service type	Characteristics
eMBB (enhanced Mobile Broadband)	High capacity
URLLC (ultra- Reliable Low Latency Communications)	Low latency, high reliability, high availability
MIoT (Massive IoT)	Fast response, high reliability, low latency

Top Threats and Research Efforts
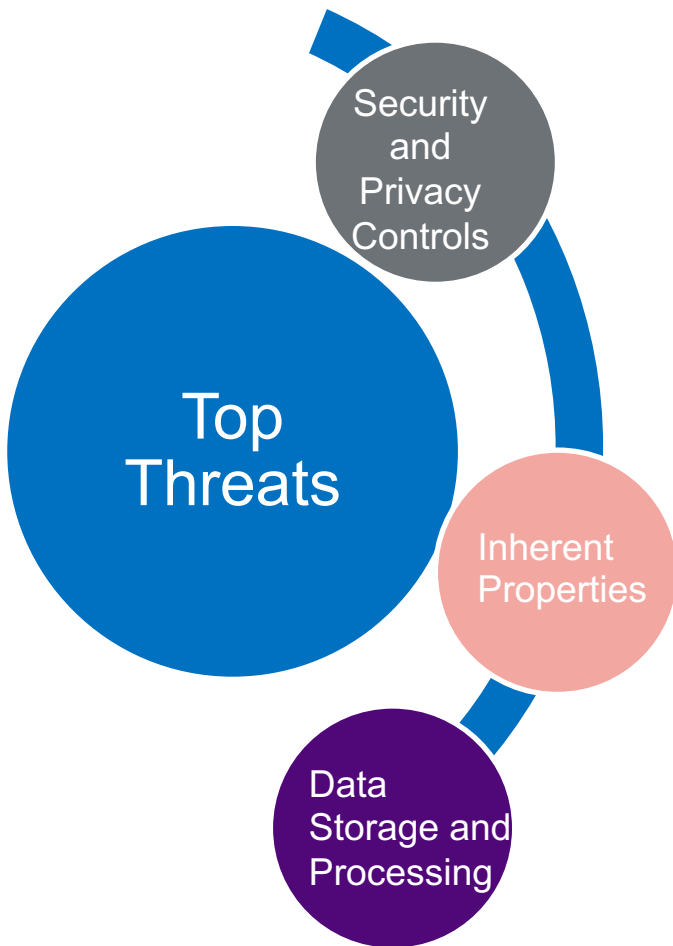
1. Lack of cloud security architecture and strategy

2. Misconfiguration and inadequate change control

3. Insufficient identity, credential, access and key management

4. Account hijacking

5. Abuse and nefarious use of cloud services

6. Weak control plane

7. Metastructure and applistructure failures

8. Insecure interfaces and APIs

9. Data Breaches

10. Insider threat

11. Limited cloud usage visibility

The Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven", 2019.
Technical Report: Gap Analysis between Scientific Research and Technical Standardization in Cloud Computing 2019

Analysis of Two Threats

Top Threat	Research Aspect	Research Effort
1. Lack of Cloud Security, Architecture and Strategy	Security and Privacy Controls	1) Attribute-Based Encryption
		2) Proxy Re-Encryption
9. Data Breaches	Data Storage and Processing	1) Intelligent Cryptography Approach
		2) Fuzzy Authorization

Major Standardization Activities

Cloud Computing Standards

Architecture & Framework

Architecture
ISO/IEC 17789
ITUT-T Y.3500
ITUT-T Y.3502
ISO/IEC NP TR 15944-14

Use cases
ISO/IEC 19944
ETSI TR 103 126
ETSI SR 003 381
ISO/IEC DIS 22624
ISO/IEC PDTR 23188

Framework
ISO/IEC 17788
ISO/IEC 19086-1
ISO/IEC 19086-3
ISO/IEC TR 23186
ETSI GS/NFV-EVE011

Cloud Management

Security
ISO/IEC 27003
ISO/IEC27017
ETSI SR 003 392

Service Management
ISO/IEC TR 20000-9
ETSI TR 102 997
ETSI TS 103 125
ISO/IEC 19086-2
ISO/IEC TR 22678

Cloud Communication

Cloud Brokers
ISO/IEC 19941
ETSI TS 103 142
ISO/IEC NP TR 23187

Cloud API's
ISO/IEC 17826
ISO/IEC 19831

Network Sliding
3GPP TS 23.501
3GPP TS 23.502
3GPP TS 23.503
3GPP TS 23.530
3GPP TS 23.531
3GPP TS 23.801

Gap Analysis

Security and Privacy Controls in the Cloud	• Lack of practical solutions to control cloud data access based on trust and reputation	ISO/IEC 27001,TR 23186:2018 ISO/IEC 17789 Under-development: Little ongoing efforts
Inherent Properties of Cloud Computing	• The interactions between different cloud service providers and cloud partners has not been explored and described in detail	ISO/IEC 19941 Under-development: TR 23187
Data stored and processed in the Cloud	• Lack of global regulations	GDPR ISO/IEC 19944:2017/PDAM 1 ISO/IEC AWI 23751 ISO/IEC PDTR 23188
Metering and Billing for Cloud Service	• Lack of standardized and transparent metering indicator and billing principle	PDTR 23613 TR 23951, DIS 22624
General	• A standardized and uniform terminology and common description of cloud services • Update reference architecture • The need for simplifying SLAs.	ISO/IEC 19086 CD 22123 ISO/IEC 19086-1
Network Slicing	• There are misinterpretations and confusing in terms of its concept, technology, applications & pricing models.	3GPP TS 23.501 3GPP TS 23.502 3GPP TS 23.503 3GPP TR28.801 3GPP TR28.530

SnT

UNIVERSITÉ DU LUXEMBOURG

Summary

- The rapid technology developments require continuous standards updating efforts

- New working groups or joint working groups should be established to cope with the above

- For CSPs, guaranteeing users' data security and privacy is a key issue and requires complex prospective considerations, including constant attention and adaptation to the market

- Sustained attention and efforts are needed as the trust relationship among users and service providers has huge market importance

- The main task for building trust mechanisms in Cloud Computing is to establish the architecture for sensitive data with encryption mechanism

Thank you for your Attention