Future Internet
BIG data

Dr. Panagiotis Rizomiliotis

References

- https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Taxonomy.pdf
- https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
- https://www.enisa.europa.eu/publications/big-data-security/at_download/fullReport

Big data reality

- The term big data refers to the massive amount of digital information companies and governments collect about us and our surroundings.
- Source:
  - traditional information exchange and software use via desktop computers, mobile phones
  - myriads of sensors of various types embedded in various environments
    - city streets (cameras, microphones),
    - jet engines (temperature sensors)
    - etc
  - Internet of Things, where virtually every electrical device will connect to the Internet and produce data.

How Big?

- Every day, we create 2.5 quintillion bytes of data--so much that 90% of the data in the world today has been created in the last two years alone (as of 2011)
- The amount of data generated is expected to double every two years, from 2500 exabytes (EB) in 2012 to 40,000 exabytes in 2020

- ***1 EB = 10^{18} bytes = 1000000000000000000B =***

1000 petabytes = 1 million terabytes = 1 billion gigabytes!!!!!!

A definition

- Big Data technologies is as a new generation of technologies and architectures, designed to economically extract value from very large **volumes** of a wide **variety** of data, by enabling high-**Velocity** capture, discovery, and/or analysis.
- More "V"s:
  - Veracity (i.e. validity)
  - Value: inherent wealth, economic and social, embedded in any data set;
  - Volatility: the tendency for data structures to change over time;

Main Characteristics (1/2)

- Fast data insertion. Vast amounts of data generated every second are stored and analysed.
- Distributed redundant data storage. In Big Data storage method is based on a distributed file system that gives the needed redundancy and high availability.
- Parallel task processing. Computation is performed in parallel and large volumes of unstructured data can be efficiently processed in a few minutes.
- Different types of data. Big Data technology enables concetration and analysis of unstractured data, such as conversations, videos, images, sensor data, etc.
- Scalable. Big Data systems store and distribute very large data sets across a vast number of systems that operate in parallel.
- Large scale analytics. Fast data insertion – as mentioned above - creates an enormous amount of data, which is then analysed to produce large scale analytics which contribute to a better planning or management of the area they fit (fit-of-purpose governance).

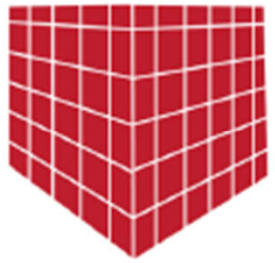
Main Characteristics (2/2)

- Hardware agnostic. Big Data processing and Big Data analytics is executed efficiently regardless the underlying infrastructure, resulting in an improved direction and decision making around hardware investments.
- Accessible. Easily access new data sources and tap into different types of data (both structured and unstructured) to generate value from that data.
- Cost effective. Big Data systems also tackle the problem of traditional relational database management systems (RDBMS). Use of databases specifically engineered for managing large volumes of data, where traditional RDBMS will be extremely expensive.

Drivers of Big Data

Decreasing cost of storage

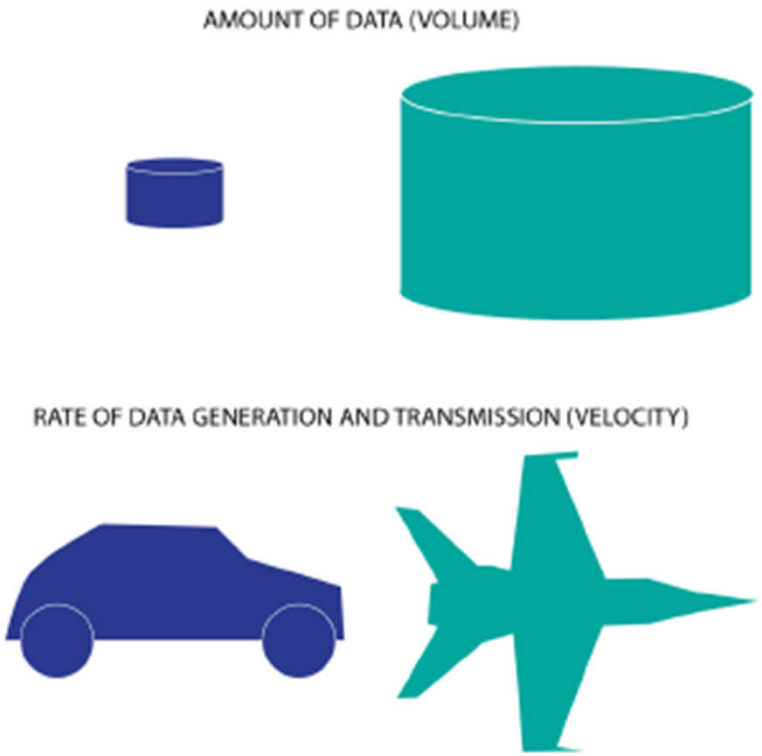
Flexibility and cost-effectiveness of datacenters and cloud computng



Development of new frameworks (such as Hadoop)

and cheap sensors

Traditional vs Big Data



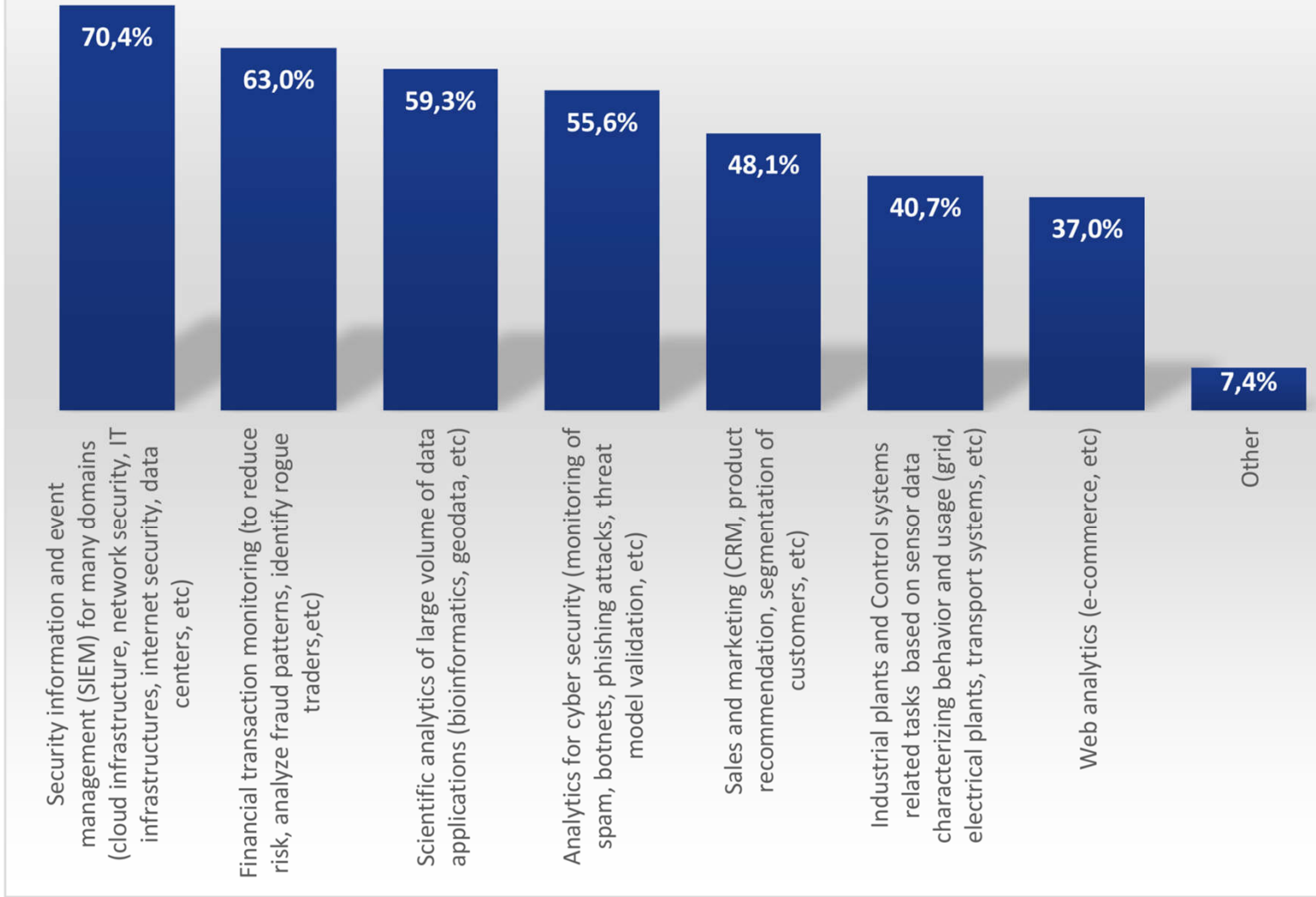
EU and Big Data

- Europe is lagging behind in the global market
  - a mere two of the top twenty companies, which use Big Data in a significant way, are in the European Union
- European Commission has formed the Big Data Value Public Private Partnership (PPP)
  - to cooperate in data-related research and innovation,
  - enhance community building around data,
  - set the grounds for a thriving data-driven economy in Europe
- ENISA was asked to support the initiative

Big data current state

- organizations see the potential of Big Data,
  - started considering Big Data solutions to add value to their business services and to optimize their internal processes.
- They are still in the research phase
- Very few that are actively exploiting the benefits of the technologies
- Most of the potential adopters are currently in the business requirements collection phase.
- Big Data systems are complex and heterogeneous,
- Architectures and platforms that would form Big Data analysis systems have not been defined yet, or are in very early stages.
- We have identified some characteristic use cases though.

Which are the most promising domains of applications for big data?



Overview

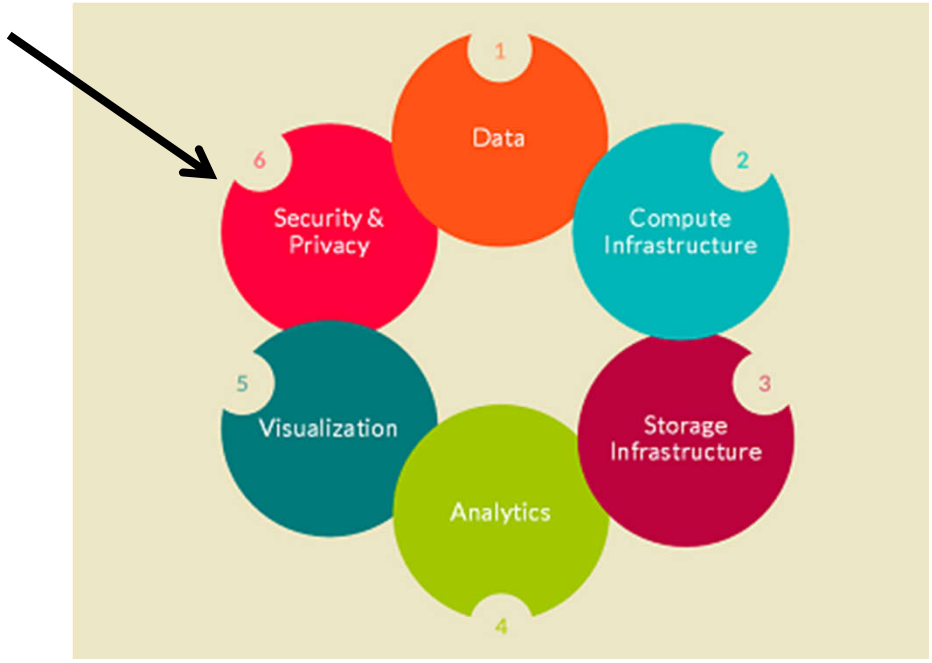
- The Big Data taxonomy
- Security Use Cases (ENISA)
- Top Ten Big Data Security and Privacy Challenges

"THAT'S your Ark for the Big Data flood? Noah, you will need a lot more storage space!"

Big data 6-D taxonomy

6 – Security & Privacy

- In details, shortly



Use Cases and recommendations

The ENISA approach

Overview

- ENISA investigates 3 use cases
- (Please refer to the deliverable for more details)

USE CASE	BIG DATA APPLICATION	CRITICALITY
Financial Sector	User of Big Data	Integrity of data and information
Power Supply (energy sector)	User of Big Data	Availability and continuity of service
Telecommunications Sector	Provider of Big Data	Secure provision of services

Table 1 Criticality of Information Security for Use Cases

Challenges

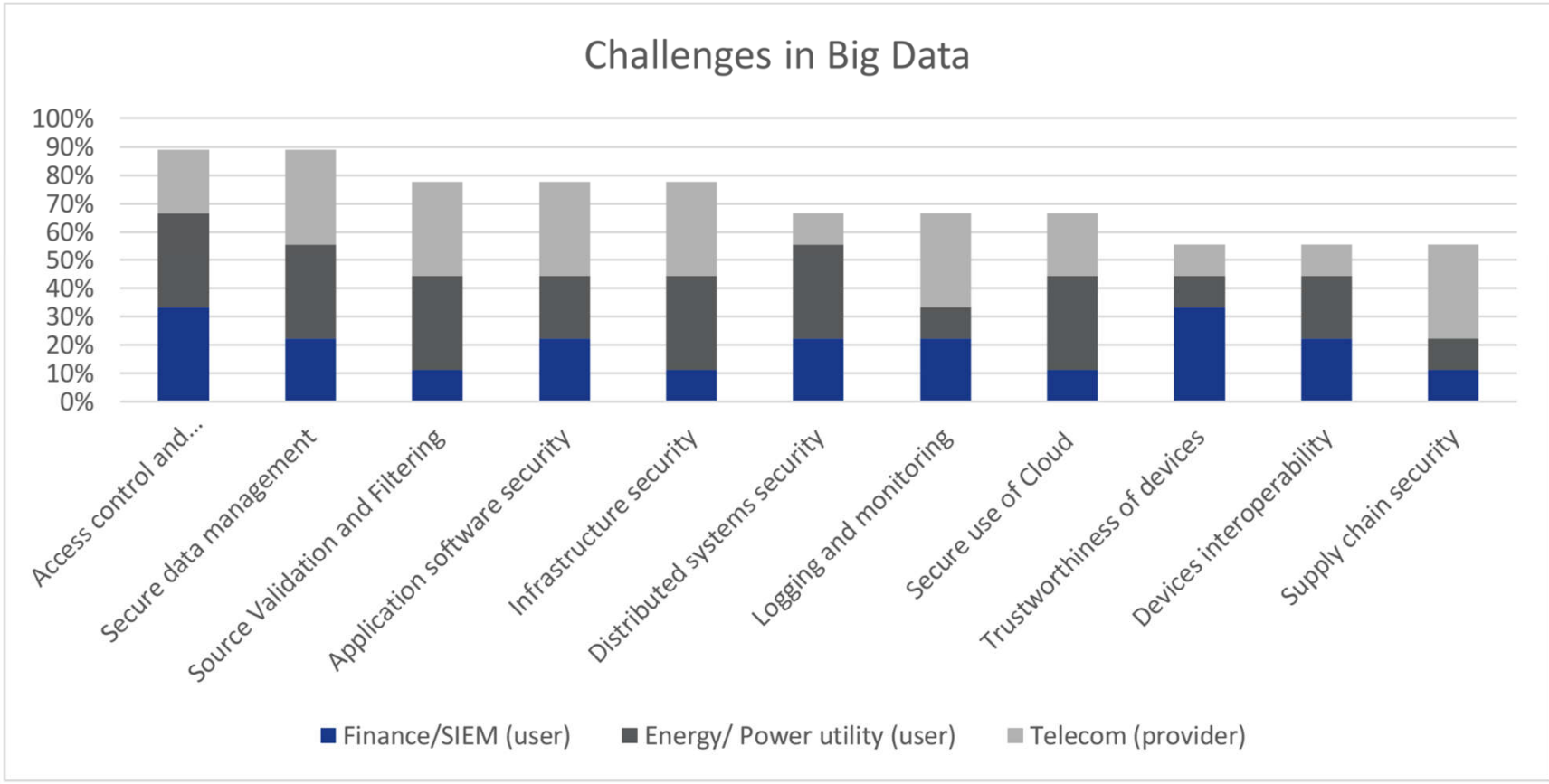


Figure 1 Big Data challenges rated by use case

Mitigations measures

- 7 good practices are proposed

Strong and scalable encryption

- Encrypt data in transit and at rest, to ensure data confidentiality and integrity.
- Ensure proper encryption key management solution, considering the vast amount of devices to cover.
- Consider the timeframe for which the data should be kept - data protection regulation might require that you dispose of some data, due to its nature after certain period of time.
- Design databases with confidentiality in mind – for example, any confidential data could be contained in separate fields, so that they can be easily filtered out and/or encrypted.

Mitigations measures

Application security

- Use regular security testing procedures to re-assure the level of security, specially after patches or functionality changes.
- Ensure tamper resistant devices to avoid misuse.
- Ensure internal security testing procedures for new and updated components are carried out regularly; if it is not possible third party evaluations, audits and certification are key elements for the confidence and trust in products and actors.
- Ensure procurement policies cover purchasing from authentic suppliers.

Mitigations measures

Standards and Certification

- Use devices which comply with desired security standards.
- Ensure obtained certification relates to the use of Big Data.

Secure use of Cloud in Big Data

- Ensure Big Data is included in the risk assessment for Cloud.
- Ensure proper Service Level Agreements have been adopted.
- Ensure proper resource isolation and exit strategies have been negotiated

Mitigations measures

Source filtering

- Use devices with authentication capabilities to ensure that validation of endpoint sources is possible
- Assign confidence levels on the endpoint sources
- Re-evaluate confidence levels of the endpoints regularly, specially after patches or changes in firmware
- If confidence in endpoint source is low, use it in combination with other higher confidence endpoint sources for taking actions

Access control and authentication

- Use authentication and authorization to ensure that Big Data queries are executed by authorized users and entities only
- Use components in the Big Data system that follow same security standards to maintain the desired level of security

Mitigations measures

Big Data monitoring and logging

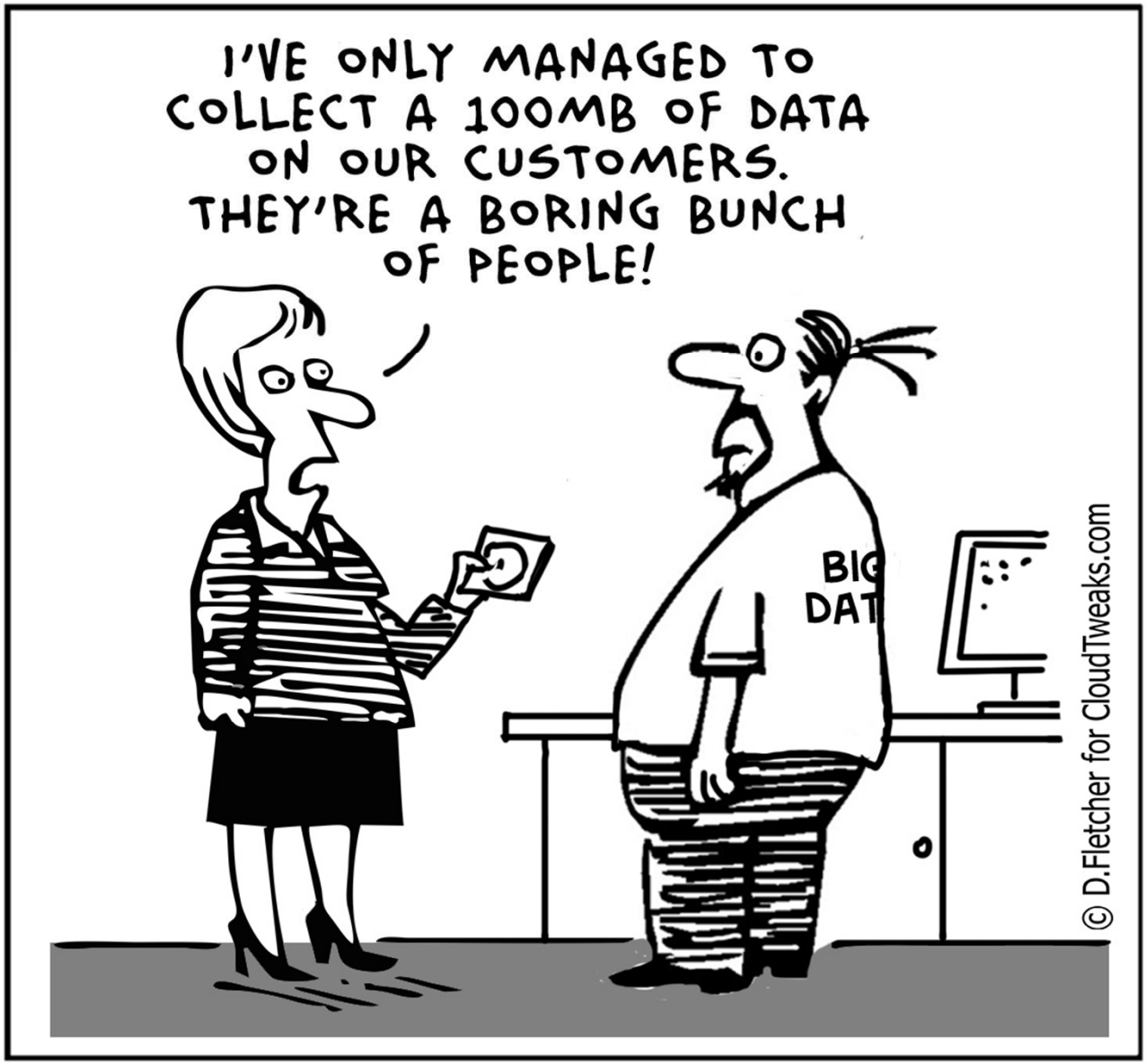
- Enable logging on nodes participating in the Big Data computation
- Enable logging on databases (relational or not) , as well as Big Data applications
- Detect and prevent modification of logs
- Regularly test the restoration of Big Data backups considering the vast amount of data being used in the system

Mitigations measures

CHALLENGES/ MITIGATION MEASURES	ENCRYPTION	SECURITY TESTING AND CODE AUDITING	CERTIFICATION STANDARDS	RISK ASSESSEMENT	SOURCE FILTERING	ACCESS CONTROL AND AUTHENTICATION	MONITORING AND LOGGING
Source validation and Filtering	Yes	Yes		Yes	Yes	Yes	Yes
Secure computation	Yes	Yes	Yes		Yes	Yes	Yes
Access control and authentication	Yes	Yes	Yes			Yes	Yes
Secure Data Management	Yes	Yes				Yes	Yes
Infrastructure security		Yes	Yes		Yes	Yes	Yes
Supply chain security		Yes	Yes	Yes			
Application software security		Yes	Yes			Yes	
Trustworthiness of devices		Yes	Yes			Yes	
Interoperability of applications		Yes	Yes			Yes	
Secure Use of Cloud computing	Yes	Yes	Yes	Yes		Yes	Yes
Distributed Denial of Service Attacks		Yes			Yes		Yes

ENISA Recommendations

- Recommendation 1: Policy makers should focus on providing guidance for secure use of Big Data systems in the critical sectors.
- Recommendation 2: Big Data providers or vendors should invest in compliance with security standards for their products (devices, services, cloud etc).
- Recommendation 3: The competent authorities of the critical sectors should encourage vendors to offer security authentication mechanisms and protocols in their products.
- Recommendation 4: The standardisation bodies should adapt existing or create new security standards for Big Data.
- Recommendations 5: Industry players and vendors should invest more into enhancing technical security skills of the staff on Big Data through trainings and certifications.


I'VE ONLY MANAGED TO COLLECT A 100MB OF DATA ON OUR CUSTOMERS. THEY'RE A BORING BUNCH OF PEOPLE!
BIG DAT
© D.Fletcher for CloudTweaks.com

Top Ten Big Data Security and Privacy Challenges

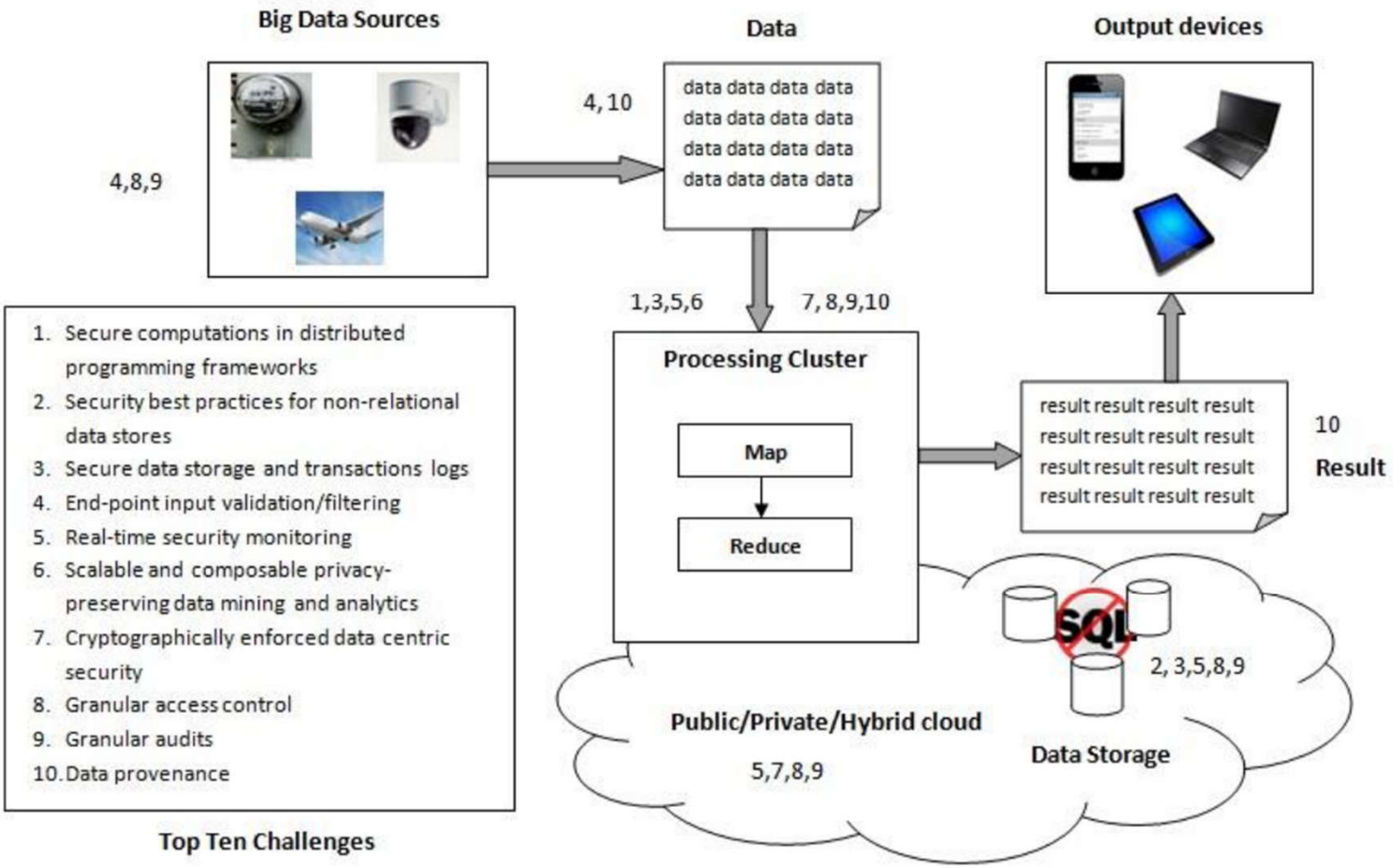
CSA approach

Criteria

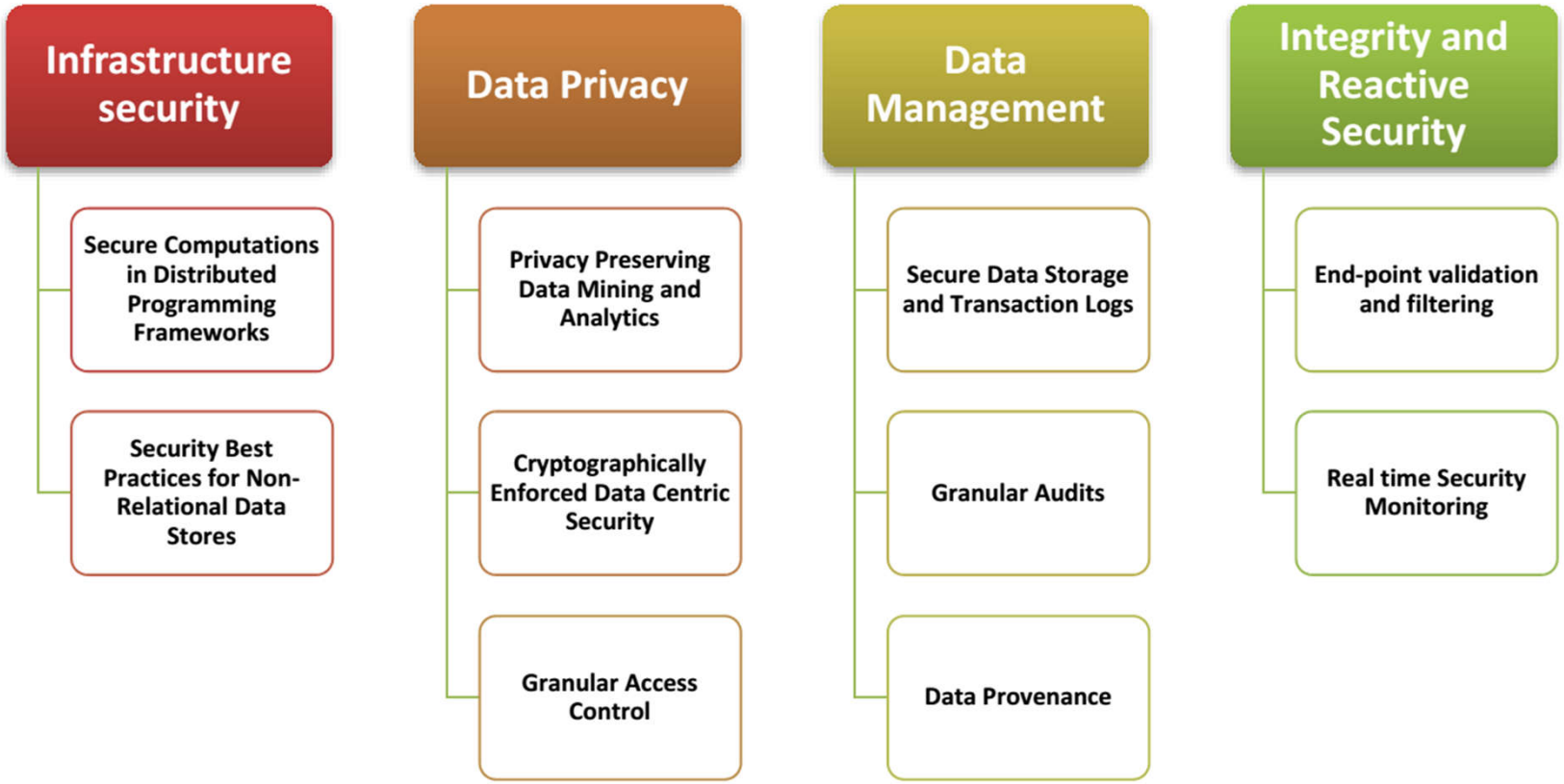
- Security-practitioners
- Published solutions.
- The proposed solution did not cover the problem scenarios.

The top ten challenges to Big Data security and privacy

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced data centric security
8. Granular access control
9. Granular audits
10. Data provenance


Big Data Sources
Data
Output devices
4,8,9
4, 10
data data data data
data data data data
data data data data
data data data data
1,3,5,6
7, 8,9,10
Processing Cluster
Map
Reduce
result result result result
result result result result
result result result result
result result result result
10
Result
SQL
2, 3,5,8,9
Public/Private/Hybrid cloud
5,7,8,9
Data Storage
1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced data centric security
8. Granular access control
9. Granular audits
10. Data provenance
Top Ten Challenges

Classification of the Top 10 Challenges



Analysis approach

1. A Use case
2. Modeling: formalizing a threat model that covers most of the cyber-attack or data-leakage scenarios
3. Analysis: finding tractable solutions based on the threat model
4. Implementation: implementing the solution in existing infrastructures

1.0 Secure Computations in Distributed Programming Frameworks

- Modeling
  1. Malfunctioning Compute Worker Nodes
  2. Infrastructure Attacks
  3. Rogue Data Nodes

- Analysis
  - trust establishment
  - Mandatory Access Control (MAC)
  - Data de-identification

  - Two problems must be tackled:
    1. Performance penalties due to imposing MAC
    2. Limitations of differential privacy in providing guarantees

2.0 Security Best Practices for Non-Relational Data Stores

- The security infrastructures of non-relational data stores popularized by NoSQL databases are still evolving
  - NoSQL injection
- NoSQL databases do not provide any support for explicitly enforcing security in the database.

3.0 Secure Data Storage and Transactions Logs

- Modeling
  1. Confidentiality and Integrity
  2. Provenance
  3. Availability
  4. Consistency
  5. Collusion Attacks
  6. Roll-Back Attacks
  7. Disputes

3.0 Secure Data Storage and Transactions Logs

- Analysis
  1. Confidentiality and integrity can be achieved with robust encryption techniques and message-digests.
  2. The exchange of signed message-digests can be used to address potential disputes
  3. Broadcast encryption
  4. Data availability can be improved through proof of retrievability (POR) or provable data possession (PDP) methods with high probability
  5. Regarding collusion attacks: policy-based encryption system (PBES)

Problems:

- There are techniques for each individual security problem in large scale auto-tier storage systems, there is no systematic approach to integrate them into a seamless, holistic solution!!
- The non-uniform security policies among different tiers pose an additional challenge to securing inter-tier data transmission.
- Balance tradeoffs among security, usability, complexity, and cost.

4.0 End-Point Input Validation/Filtering

- Modeling
  1. An adversary may tamper with a device from which data is collected, or may tamper with the data collection application running on the device to provide malicious input to a central data collection system.
  2. An adversary may perform ID cloning attacks (e.g., Sybil attacks) on a data collection system by creating multiple fake identities (e.g., spoofed iPhone IDs) and by then providing malicious input from the faked identities.
  3. A more complicated scenario involves an adversary that can manipulate the input sources of sensed data.
  4. An adversary may compromise data in transmission from a benign source to the central collection system
- Analysis

  (a) solutions that prevent an adversary from generating and sending malicious input to the central collection system, and

  (b) solutions that detect and filter malicious input at the central system if an adversary successfully inputs malicious data.

5.0 Real-Time Security Monitoring

- Modeling
  - Security monitoring requires that the Big Data infrastructure, or platform, is inherently secure
  - Common problems. For instance:
    - The security of the public cloud,
    - The security of the Hadoop cluster,
    - The security of the monitoring application itself
    - The security of the input sources

- Analysis/Implementation

  Not only technical issues. Legal restrictions

  No built-in security monitoring and analysis tools in Hadoop.

  Existing real-time monitoring, solutions and frameworks, like NIST's Security Content Automation Protocol (SCAP) are slowly entering the Big Data arena.

6.0 Scalable and Composable Privacy-Preserving Data Mining and Analytics

- Modeling
  - An insider in the company hosting the Big Data store can abuse her level of access and violate privacy policies. An example of this scenario is the case of a Google employee who stalked teenagers by monitoring their Google chat communications.
  - If the party owning the data outsources data analytics, an untrusted partner might be able to abuse their access to the data to infer private information from users.
  - Sharing data for research is another important use. However, ensuring that the data released is fully anonymous is challenging because of re-identification.

7.0 Cryptographically Enforced Data-Centric Security

- The first approach controls the visibility of data by limiting access to the underlying system, such as the operating system or the hypervisor.
- The second approach encapsulates the data itself in a protective shell using cryptography.

- Modeling
  1. For a cryptographically-enforced access control method using encryption, the adversary should not be able to identify the corresponding plaintext data by looking at the ciphertext, even if given the choice of a correct and an incorrect plaintext.
  2. For a cryptographic protocol for searching and filtering encrypted data, the adversary should not be able to learn anything about the encrypted data beyond whether the corresponding predicate was satisfied.
  3. For a cryptographic protocol for computation on encrypted data, the adversary should not be able to identify the corresponding plaintext data by looking at the ciphertext, even if given the choice of a correct and an incorrect plaintext.
  4. The adversary should not be able to forge data that did not come from the purported source.

7.0 Cryptographically Enforced Data-Centric Security

- 7.3 – Analysis
  1. Identity and attribute based encryption methods enforce access control using cryptography. Attribute-based encryption extends this concept to attribute-based access control.
  2. Boneh and Waters construct a public key system that supports comparison queries, subset queries and arbitrary conjunction of such queries.
  3. In a breakthrough result in 2009, Gentry constructed the first fully homomorphic encryption scheme.
  4. Group signatures enable individual entities to sign their data but remain identifiable only in a group to the public. Only a trusted third party can pinpoint the identity of the individual.

8.0 Granular Access Control

- The security property that matters from the perspective of access control is secrecy – preventing access to data by people that should not have access.
- Modeling
  1. Application development expensive and complicated. The variety of applications introduces many opportunities to get granular access controls wrong.
  2. Granular access control can be decomposed into three sub-problems.
     1. Keeping track of secrecy requirements for individual data elements.
     2. Keeping track of roles and authorities for users.
- Properly implementing secrecy requirements with mandatory access control.

- Analysis
  - Reduce the complexity of the addition of granular access controls to an application.

Example: A NoSQL database that supports mature, cell-level access control. Every atomic key/value pair is tagged with an expression that describes the roles required to read that entry, and every query includes a role check.

1.

9.0 Granular Audits

- Modeling
  - Key factors for auditing comprise the following:
    - Completeness of the required audit information.
    - Timely access to audit information.
    - Integrity of the information
    - Authorized access to the audit information.

10.0 Data Provenance

- Modeling
  - Secure provenance in Big Data applications requires:
    - the provenance records to be reliable,
    - privacy-preserving,
    - access-controllable
    - provenance availability and
    - scalability
  - provenance metadata in Big Data applications can be formally modeled into three categories:
    1. Malfunctioning Infrastructure Components
    2. Infrastructure Outside Attacks
    3. Infrastructure Inside Attacks

10.0 Data Provenance

- Analysis
  - The source components that generate provenance in the infrastructure should be first authenticated.
  - periodic status updates
  - sensitive information pertaining to the data - encryption techniques are required
  - fine-grained access control of provenance is desired

  - The same (new) cryptographic solutions

Certification

The ENISA/EU approach

EU cybersecurity certification framework

- https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-ii/at_download/fullReport

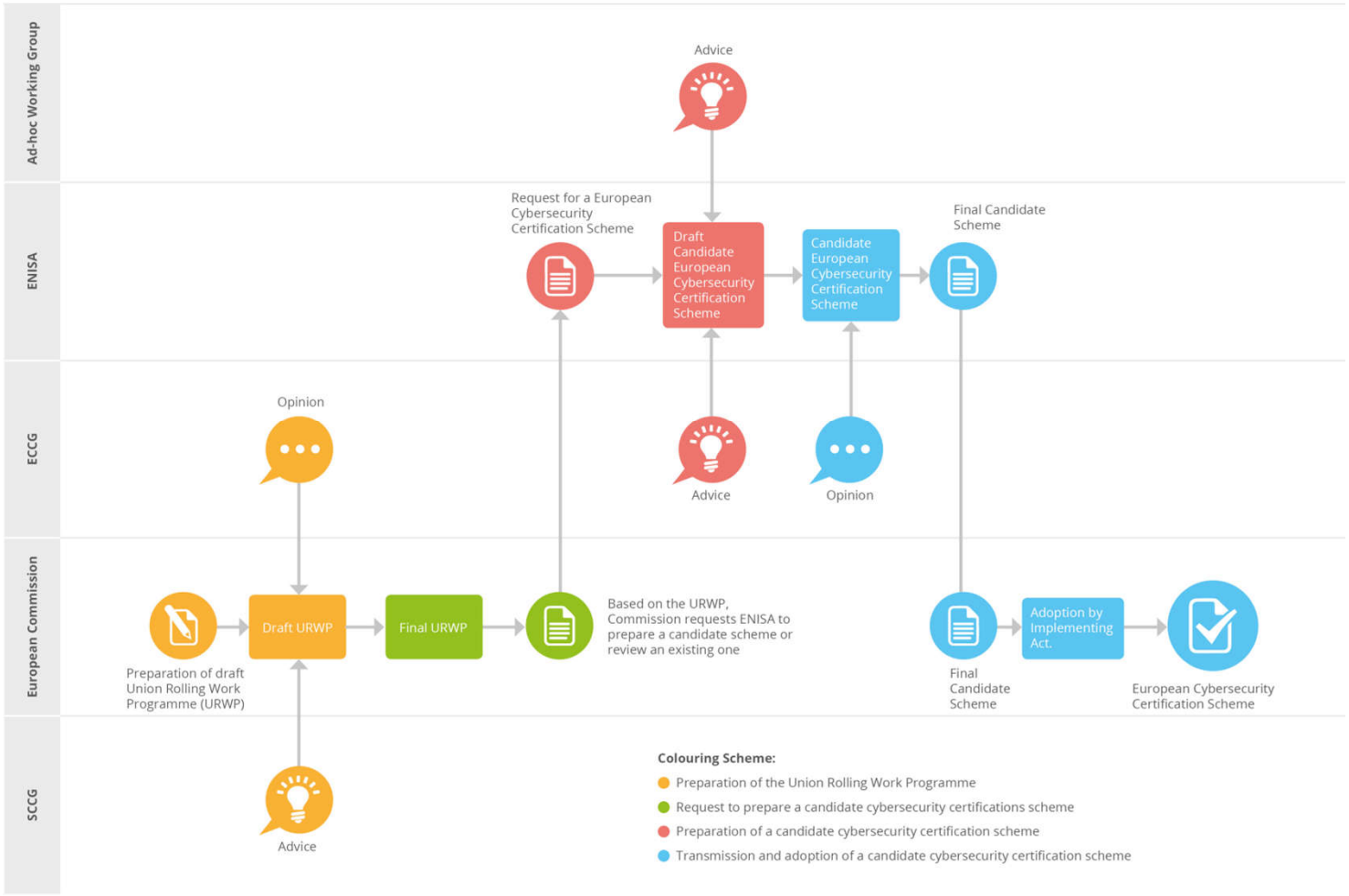
- Defines a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, processes and services comply with specified security requirements
- ENISA has a pivotal role in the design of the candidate EU cybersecurity certification schemes
- EU Cybersecurity Act (CSA), Regulation (EU) 2019/881

https://eur-lex.europa.eu/eli/reg/2019/881/oj

CSA

- The CSA provides guidelines regarding how these schemes should be designed:
  - Article 51 – Security objectives of European cybersecurity certification schemes
  - Article 52 – Assurance levels of European cybersecurity certification schemes
  - Article 54 – Elements of European cybersecurity certification schemes

Stakeholders' Interactions

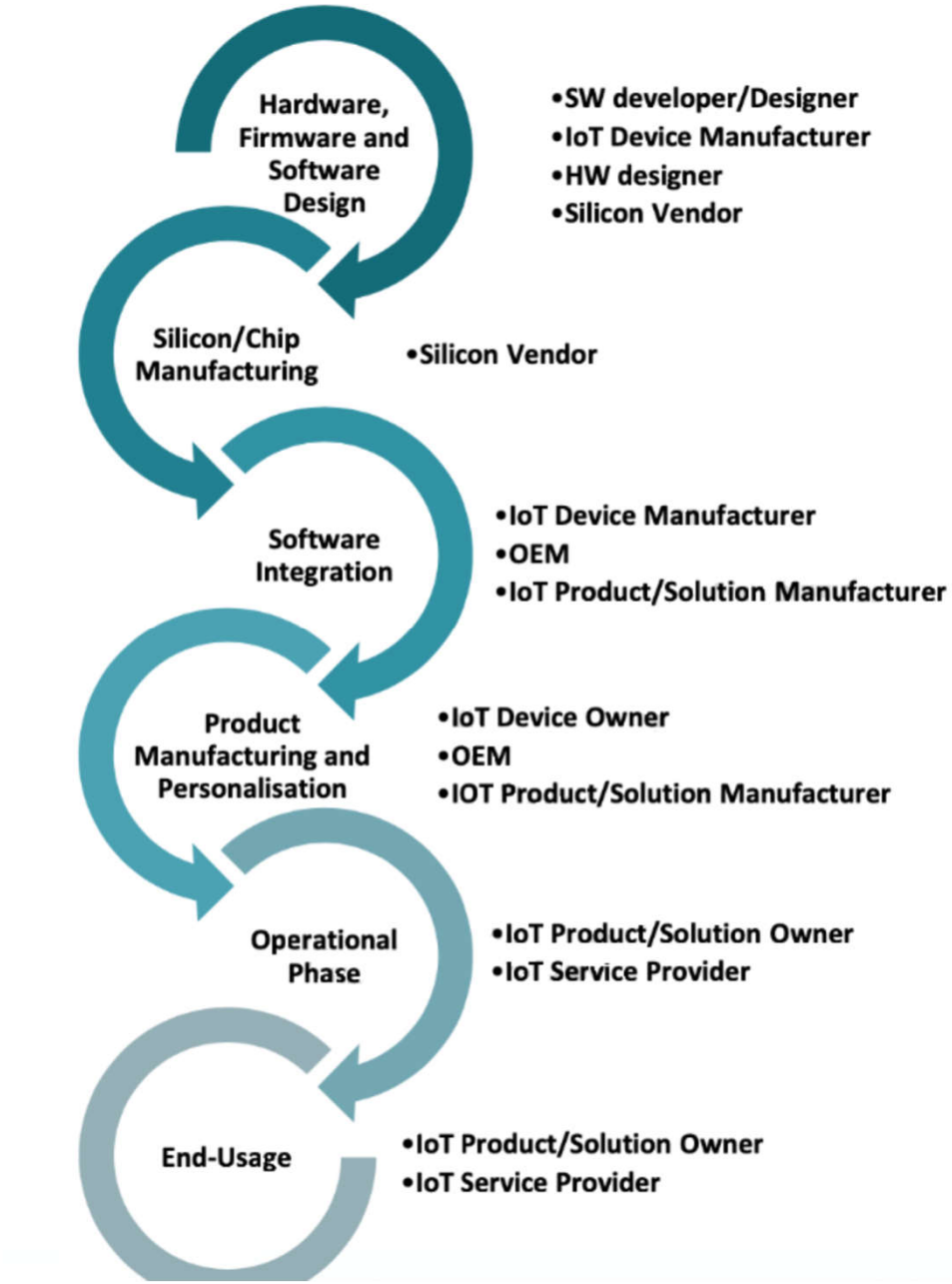


IoT certification

- Cyber security certification landscape for IoT devices in the EU
  - ETSI 303 645
  - Eurosmart IoT certification (Eurosmart, 2019)
- European standards for security evaluation models, methods, techniques and tools adapted to the IoT world are needed urgently
- There is a broad range of IoT devices and functionality
- The focus of IoT device certification regarding security lies in the area of consumer IoT devices

Eurosmart cybersecurity certification scheme for IoT

- It was developed based on the requirements of the CS Act
- The Eurosmart scheme consists of nine documents (November 2019)
- It provides the definition of Security Profiles (similarly to the Security Target in a Common Criteria (CC))
- The scheme resembles common smart card certifications schemes, like CC.
- Must be lightened for "smart home" evaluation


Hardware, Firmware and Software Design
•SW developer/Designer
•IoT Device Manufacturer
•HW designer
•Silicon Vendor
Silicon/Chip Manufacturing
•Silicon Vendor
Software Integration
•IoT Device Manufacturer
•OEM
•IoT Product/Solution Manufacturer
Product Manufacturing and Personalisation
•IoT Device Owner
•OEM
•IOT Product/Solution Manufacturer
Operational Phase
•IoT Product/Solution Owner
•IoT Service Provider
End-Usage
•IoT Product/Solution Owner
•IoT Service Provider

Eurosmart cybersecurity certification scheme for IoT

- Only experts can fully comprehend complex certification schemes which use Security Profiles.
- Consumers (like smart home device users/owners) require security principles that are simple to follow.
- A basic level of assurance that relies on self-certification should be verified by a certification body.

ETSI 303 645

- A new standard spearheaded by the UK Department for Digital, Culture, Media and Sport
- Taget: IoT devices connected to network infrastructure (such as the Internet or home network) and the connectivity to other associated services.
- It was designed as a certification standard
- Additional work is needed to create a complete certification scheme

Conclusions

- A candidate scheme must focus on consumer IoT devices (mainly used in Smart Home) and must contain the three levels:
  - **Basic security level certification:** achieved by self-assessment. It can be based on the requirements from the ETSI EN 303 645. The device must meet all mandatory requirements.
  - **Substantial security level certification:** achieved by adding defined processes in the Eurosmart scheme such as vulnerability management, policies, and mark usage. The overall scheme setup follows the same principles that derive from other EU legislation acts, such as eIDAS.
  - **High security level certification:** achieved through the Common Criteria scheme. The ETSI EN 303 645 requirements and the requirements from Eurosmart are used to create a Consumer IoT High Level Protection Profile and use the current CC infrastructure (SOG-IS22) for the certification.

Cloud Certifications schemes

Type of imitative	Name	Brief description
Public and European Norms	BSI C5[24] (Germany)	C5 is intended for professional CSPs. C5 defines which requirements, named as controls in the documentation, are to be complied with by the CSPs, as well as the minimum set of requirements that the CSPs have to meet. The requirements expressed in the supporting documentation have been elicited from widespread security standards and supplemented with BSI's own requirements. BSI is based on CSA CCM[25] and ISO 27001[26].
	ANSSI SecNumCloud[27] (France)	SecNumCloud[27 above] is intended for CSPs. Its controls are mostly based on ISO 27001[26] and structured in similar categories. However, it contains additional requirements that differentiate it from the existing standard and that do not induce equivalence between the two sets of rules. These supplementary requirements refer to service agreement content definition, data location French language usage, and activities to perform at the end of contract.

Cloud Certifications schemes

Type of imitative	Name	Brief description
	Esquema Nacional de Seguridad[28] (Spain)	ENS sets out the basic principles and minimum requirements as well as the protection measures to be implemented in the Administration's systems. It focuses on integral security, risk management, incident management and continuous improvement. It also establishes three levels and details the applicability of each measure in each of the three levels.
	ISO 27000 family[29]	Set of standards that define security measures for Information Service Management systems. The controls for generic ISMS are defined in 27002[30], while the cloud-specific controls are defined in 27017[31]. 27018[32] focuses on personally identifiable information.
Private	CSA STAR[33]	Designed for CSPs. The security controls upon which organizations can get certified are the ones defined in the CSA Cloud Control Matrix[34] (CCM) (Cloud Security Alliance)
	Zeker Online[35]	Zeker Online is a Dutch private, independent organization, that aims to certify providers of cloud – based services, IaaS, PaaS or SaaS. This certification has two big pillars: 1) legal requirements, covering all data-related aspects such as data portability, GDPR[36] compliance and so on; 2) infrastructure
Public – Private	Trusted Cloud[37]	Trusted Cloud focuses on SMEs, both CSPs and cloud users, and covers data security aspects, quality of service, transparency, data protection and contractual issues. Trusted Cloud is the non-profit association founded after the conclusion of the German program "Trusted Cloud" (funded by the Federal Ministry of Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie, BMWi)).

Example: OPEN CERTIFICATION FRAMEWORK

Open Certification Framework - OCF

- CSA
- Industry initiative
- 2012
- https://cloudsecurityalliance.org/research/ocf/

- Multi-layered cloud provider certification
- Based on CSA Security, Trust and Assurance Registry (STAR) specifications

OCF levels

1. CSA STAR Self Assessment: Cloud providers can submit reports to the CSA STAR Registry to indicate their compliance with CSA best practices. This is available immediately.
2. CSA STAR CERTIFICATION: third-party independent assessment.
   - leverages the requirements of the ISO/IEC 27001:2005 management systems standard together with the CSA Cloud Controls Matrix (CCM). These assessments will be conducted by approved certification bodies only.
3. STAR Certification: enhanced (in the future) by continuous monitoring-based certification.

STAR Certification

- it supports an independent third-party assessments based on the Cloud Control Matrix and ISO 27001.
- Collaboration with BSI
- Based upon the 'Plan, Do, Check, Act' (PDCA) approach

CCM

CONTROL AREAS 3.0.1	CONTROL AREAS 1.4
1. Application & Interface Security	1. Compliance
2. Audit Assurance & Compliance	2. Data Governance
3. Business Continuity Management & Operational Resilience	3. Facility Security
4. Change Control & Configuration Management	4. Human Resources
5. Data Security & Information Lifecycle Management	5. Information Security
6. Datacenter Security	6. Legal
7. Encryption & Key Management	7. Operations Management
8. Governance and Risk Management	8. Release Management
9. Human Resources	9. Resiliency
10. Identity & Access Management	10. Risk Management
11. Infrastructure & Virtualization Security	11. Security Architecture
12. Interoperability & Portability	
13. Mobile Security	
14. Security Incident Management, E-Discovery & Cloud Forensics	
15. Supply Chain Management, Transparency and Accountability	
16. Threat and Vulnerability Management	

Notation


CCM v3.0.1 DOMAINS
AIS Application & Interface Security
AAC Audit Assurance & Compliance
BCR Business Continuity Mgmt & Op Resilience
CCC Change Control & Configuration Management
DSI Data Security & Information Lifecycle Mgmt
DSC Datacenter Security
EKM Encryption & Key Management
GRM Governance & Risk Management
HRS Human Resources Security
IAM Identity & Access Management
IVS Infrastructure & Virtualization
IPY Interoperability & Portability
MOS Mobile Security
SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA Supply Chain Mgmt, Transparency & Accountability
TVM Threat & Vulnerability Management
136 CONTROLS
Cloud Controls Matrix v3.0
//
133 CONTROLS
Cloud Controls Matrix v3.0.1

STAR Certification

SCORE	DESCRIPTOR
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement-Based Approach
13-15	Optimizing Approach

STAR Certification

- Depending on the capability level the client achieves their audit report will categories there performance against the maturity model as either:
  - No Award
  - Bronze Award
  - Silver Award
  - Gold Award

STAR Certification

- The award is based on the average score received across the control areas.

Average score of less than 3	No award
Average score between 3 and 6	Bronze award
Average score between 6 and 9	Silver award
Average score greater than 9	Gold award

- If an organization is certified to ISO 27001 it is very unlikely that they would not achieve at least a bronze award.

Conclusion

Assurance level	Cloud security certification	Cloud Services
Basic	Trusted Cloud Zeker Online ENS low	IaaS, SaaS Infrastructure IaaS, SaaS
Substantial	BSI C5 CSA STAR ISO 27017 ENS medium	IaaS, SaaS IaaS, SaaS IaaS IaaS, SaaS
High	SecNumCloud ENS high	IaaS, SaaS


DATA
AI
VR
IOT
#137505501

Use case 1

TITLE	DESCRIPTION
Sector	Finance Sector
Usage of Big Data	Analytics, data driven decision making, real time services offering, risk quantification and prediction models building, fraud patterns analysis, rogue users identification
Security Challenges	• Trustworthiness of devices collecting data • Source validation and filtering of data • Application software security • Access control and authentication • Interoperability of devices • Distributed systems security (DDoS attack)

Table 2 Finance sector use case

Use case 2

TITLE	DESCRIPTION
Sector	Energy Sector
Usage of Big Data	Analytics, data driven decision making, risk quantification and prediction models building
Security Challenges	• Source validation and filtering of data • Application software security • Infrastructure Security • Distributed systems security (DDoS attack) • Access control and authentication

Table 3 Energy sector use case

Use case 3

TITLE	DESCRIPTION
Sector	Telecommunications
Usage of Big Data	Big Data provider: Increase volume for data storage, services optimisation, adaptive e-services offering, real time services offering, data analytics, prediction models offering data driven decision making, risk quantification
Security Challenges	• Source validation and filtering • Application software security • Access Control and authentication • Supply chain security • Secure data management • Infrastructure security • Secure Cloud use

Table 4 Telecoms sector use case