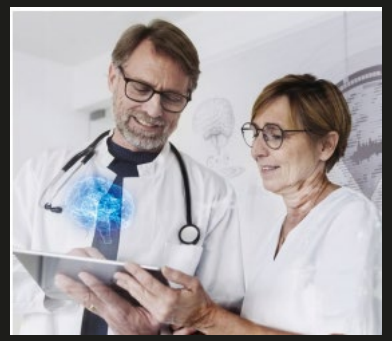
Secure AI for the Intelligent World

Ioannis Solomakos
CSO, Huawei South Balkans

HUAWEI

The Intelligent World 2030



Healthcare

Food

Home

Transport

Cities

Enterprises

Energy

Digital Trust

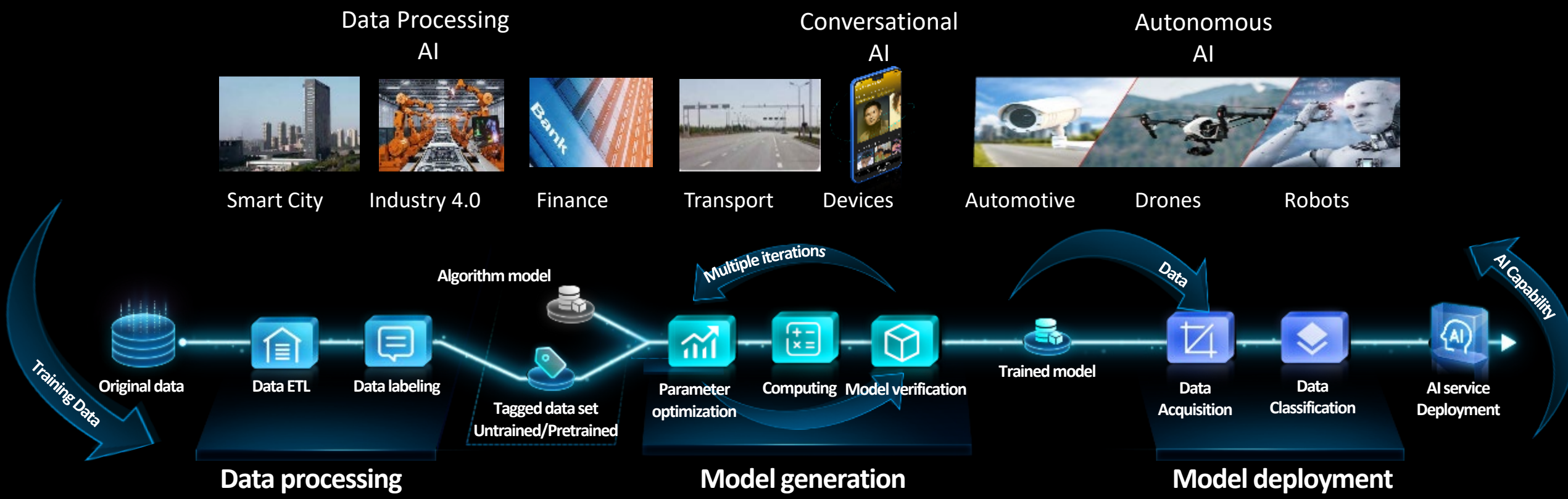
For more on the Intelligent World 2030 use cases & forecasts

www.huawei.com/en/giv

New Digital Technologies, New Cyber Challenges

The Intelligent World

AI Development & Deployment



Intelligent World

Needs a shared understanding of Risk

AI Act

AI Liability Directive

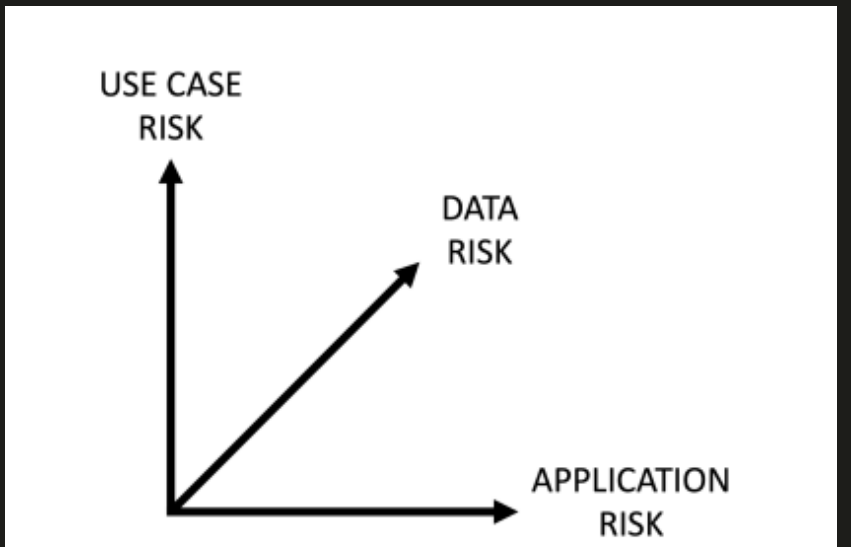
GDPR

Data Governance Act

Data Act

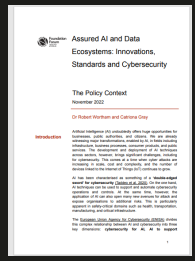
Cyber Resilience Act

Digital Services Act



Use case risks - High-risk AI systems as defined in the EU AI Act
Data risks - Provisions of GDPR, Data Act and Data Governance Act
Application risks - The AI technology stack

Need to apply a three dimensional risk approach to help understand Risk from different perspectives


Assured AI and Data Ecosystems: Innovations, Standards and Cybersecurity

The Policy Context

November 2022

Dr Robert Wortham and Catriona Gray

Introduction

Source: ForumEU 2022 - Assured AI and Data Ecosystems Policy Brief - LINK

AI Security & Privacy

A Shared Responsibility

Chief Security Officers

Data Protection Officers

ROLES	RESPONSIBILITY		
Consumers / Customers	Business Owners	Domain Experts	Domain Users
Deployers	Commercial & Privacy Assurance	Device Edge Cloud	AI Use Data Use Transparency
Data Collectors	User Authorisation	Data Subject Rights	Data Security
Solution providers	Service Providers	App / Data Engineers	Data Scientists
Technology providers	Secure Preset AI Models & TEE*, Tools	Defensive Component Technologies	Hardware Root of Trust
Law Makers	Develop Laws	Regulators	Certification

SHARED RESPONSIBILITY

DATA GOVERNANCEY

PRIVACY PROTECTION

COMPLIANCE

AI Shared Responsibility is key to all stakeholders in the industry

AI Security & Privacy

Application Risk

Chief Security Officers

Data Protection Officers

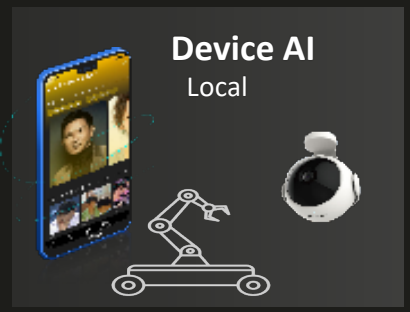
- Consumers
- Customers
- Deployers
- Data Collectors
- Solution Providers
- Full Stack AI Platform Providers
- Application Layer for Data Scientists & Application Developers
- Technology Providers
- Full Stack AI Technology Providers
- Enabling Technology Layer
- Core Technology Layer
- Law Makers

Technology Stack

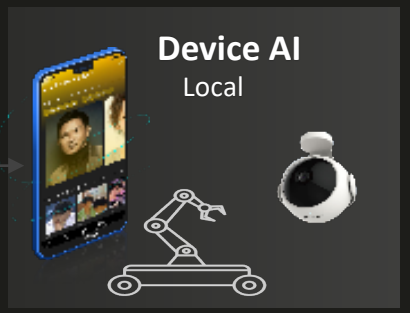
- Application Layer
- Data Layer
- Algorithm Layer
  Algorithms, API's & Data Tools
- Computing Layer
- Networking Layer

Device - Edge – Cloud Collaboration

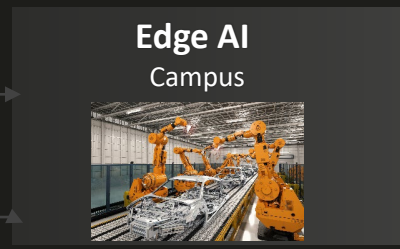
Isolated / Federated Training / Inference
Data Protection – on Device, on Edge, on Cloud
Cloud - Hybrid Cloud – Multi Cloud



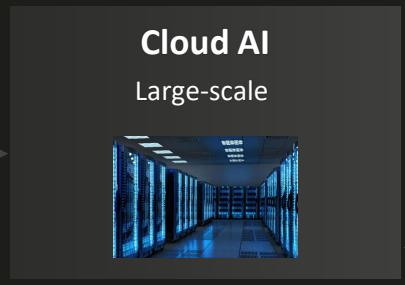
Device - Device



Device - Edge



Edge - Cloud



Device - Cloud

Cloud – Cloud

AI Deployment Models

DATA GOVERNANCEY

Identify the AI Boundary based on application and data protection requirements

AI Security & Privacy

Data Risk

Consumers

Customers

Deployers

Data Collectors

Solution Providers

Full Stack AI Platform Providers

Application Layer for Data Scientists & Application Developers

Technology Providers

Full Stack AI Technology Providers

Enabling Technology Layer

Core Technology Layer

Law Makers

Application Layer

Data Layer

Algorithm Layer
Algorithms, API's & Data Tools

Computing Layer

Networking Layer

Technology Stack

Chief Security Officers

Data Protection Officers

Data Subject

Consumer
Data Controller

Data Processor

Technology Provider

Data Protection Roles

People

Users

Customer

Solution Providers
AI Solution Providers
Application Developers
Cloud Service Providers

Technology Providers
Algorithmes & Data Tools
Computing
Networking

PRIVACY PROTECTION

Data collection must comply with data protection laws across the roles

AI Security & Privacy, a risk based approach

Application Capability

Level Definition	C1 Trustworthy & Controlled Data Sharing	C2 Result Explainability	C3 Model Self-Protection	C4 System Traceability	C5 Continuous Dynamic Self-Adaption to Environment	Exemple Scenario
L5 Full Autonomous Decision / Action	**Fully Autonomous Intelligence:** The system is autonomous, solves problems and self-healing, it protects itself from adversarial supply chain, environmental attacks					Autonomous Mobility & Robots
L4 High Automation Assisted Decision	**High Automation Intelligence**: The system is automated with data labelling, algorithm & model watermarking to protect from supply chain attack					Manufacturing, Transport & Supply Chain
L3 Conditional Predicitve Analysis	**Adversarial Intelligence**: Can defend from adversarial attack on future actions What will happen? Trusted Recommender?					Intelligence & Security Systems
L2 Diagnostic, Explainable Analysis	**Explainable Intelligence:** With explainability, transparent models, Why did it happen?					Anonymized Healthcare Diagnostic
L1 Data Analysis	**Analytical Intelligence**: What happened?					Information & Productivity

Application Risk

Technology, to enable AI Security and Privacy

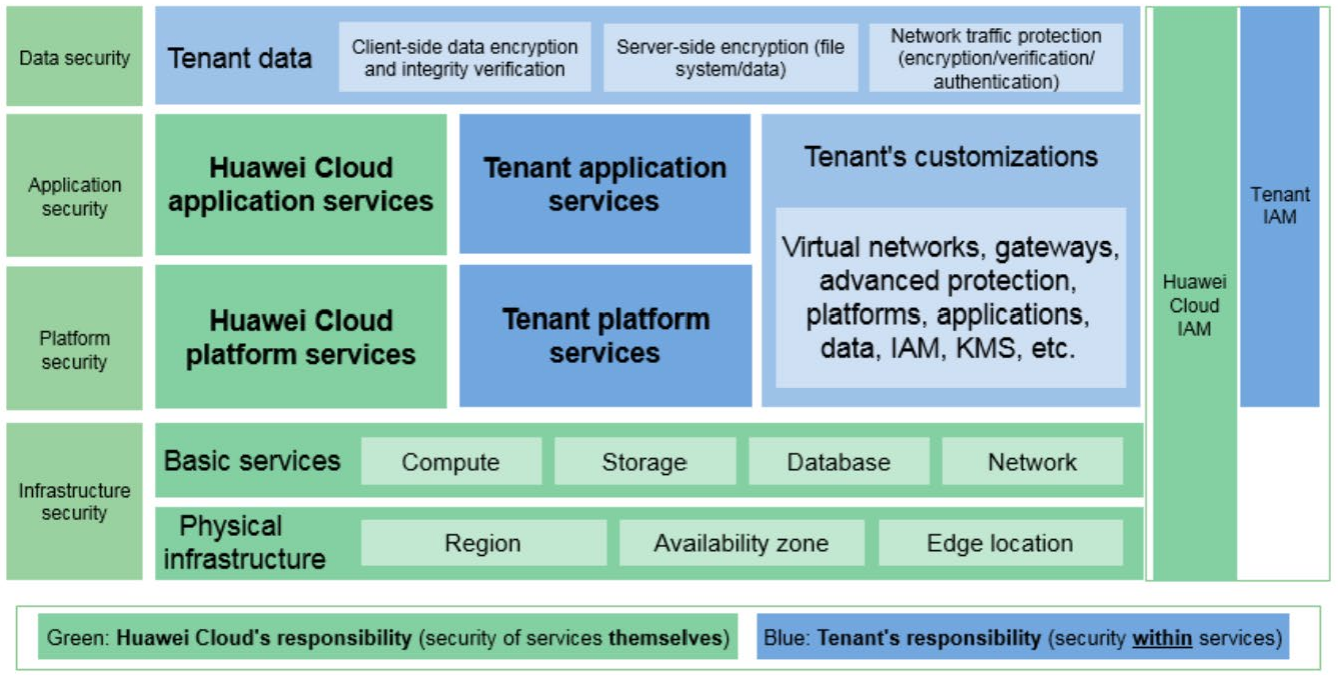
C5 Continuous, Dynamic Self Adaption to environment	Security Reinforcement Learning	Ensemble Learning Technique	Secure Fallback Mechanism	…	..
C4 System Traceability	Data Security Label	Model Signature Tracking	Model Watermark	…	…
C3 Model Self-Protection	Defence from adversarial Attack	Model Theft Prevention	Model Security Detection	Secure enclaves/ TEE	…
C2 Results Explainability	Ante-hoc Explainability	Post-hoc Explainability	…	…	…
C1 Trustworthy & Controllable Data Sharing	Edge Collaboration	Differential Privacy	Secure Federated Learning	Secure MPC/ Homomorphic encryption	Data Filtering Technology

Increase Protection capability to match the Application Risk

HUAWEI

Cloud Shared Responsibility – Cloud Provider and Tenant Application

Figure 2-1 Huawei Cloud shared responsibility model



The current cloud compliance landscape is broad and multi-dimensional.

1. Cybersecurity at a traditional data center is tasked with protecting all that data center's technology assets so that all applications and services can operate without risk of outage in a stable, secure, and high-performance manner, ranging from internal-facing data center O&M to customer-facing IaaS, PaaS, and SaaS cloud services.
2. However, Cloud security services typically support the customization of a variety of advanced security settings as per each tenant's security needs.
3. A Shared Responsibility Model provides clarity around who is responsible for the security of each element.

Artificial Intelligence Fire Detection project

EARLY DETECTION
IMMEDIATE INTERVENTION

Pilot Fire Detection Program
at Syggrou Forest

Ινστιτούτο Γεωπονικών Επιστημών

HUAWEI

NOVA

PROBOTEK

Level L1 **Analytical Intelligence**

Secure AI for an Intelligent World

Shared Responsibility takeaways:

- Needs a shared understanding of Risk: application, data & use case
- Increase Protection to match the Risk
- Bring together of Policy and Tech to develop the shared understanding

Thank you

Ioannis Solomakos - CSO, Huawei South Balkans