From Smart *Anything* to Security *Everywhere*

Andrei Tchernykh

chernykh@cicese.mx

http://usuario.cicese.mx/~chernykh/

- **Head of "Parallel Computing Laboratory" CICESE Research Center, Ensenada, Baja California, México**
- **Head of "International Laboratory of Problem-Oriented Cloud Computing" South Ural State University. Chelyabinsk, Russia**
- **Institute of System Programming of RAS, Moscow, Russia**

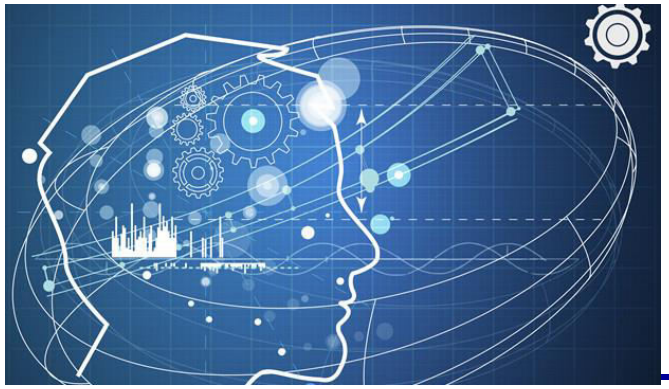
IVANNIKOV MEMORIAL WORKSHOP

RUSSIAN-ARMENIAN UNIVERSITY,

3- 4 May, 2018, Yerevan, Armenia

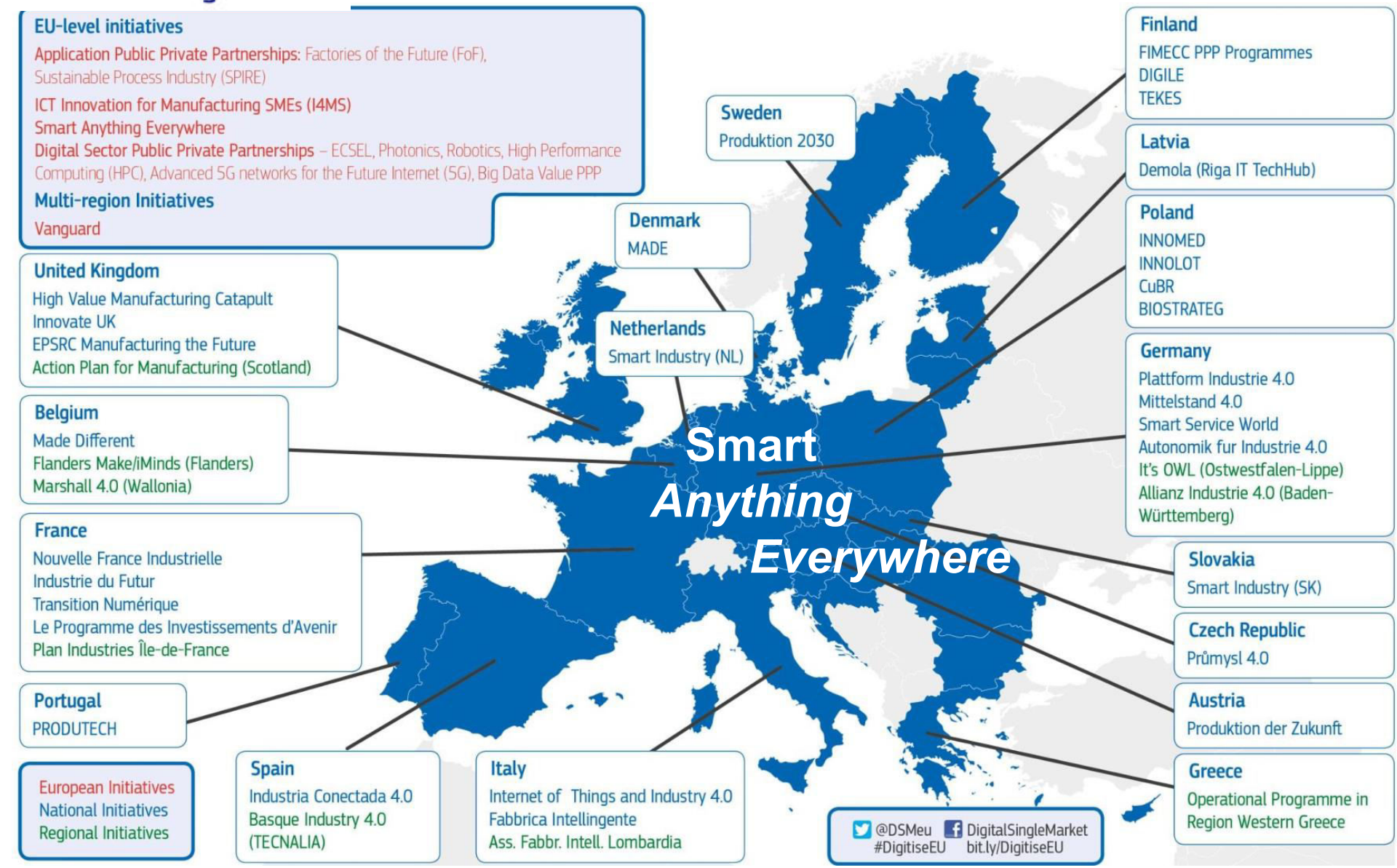
Smart Everything

- Smart Industry, Factories of the Future, Industry 4.0
- Smart City
- Smart Home
- Smart Service
- Smart Healthcare
- Smart Economy
- Smart Networking
- Smart Analytics
- Smart Security and Privacy
- Smart autonomous driving
- Smart Oil and Gas Industry
- etc.



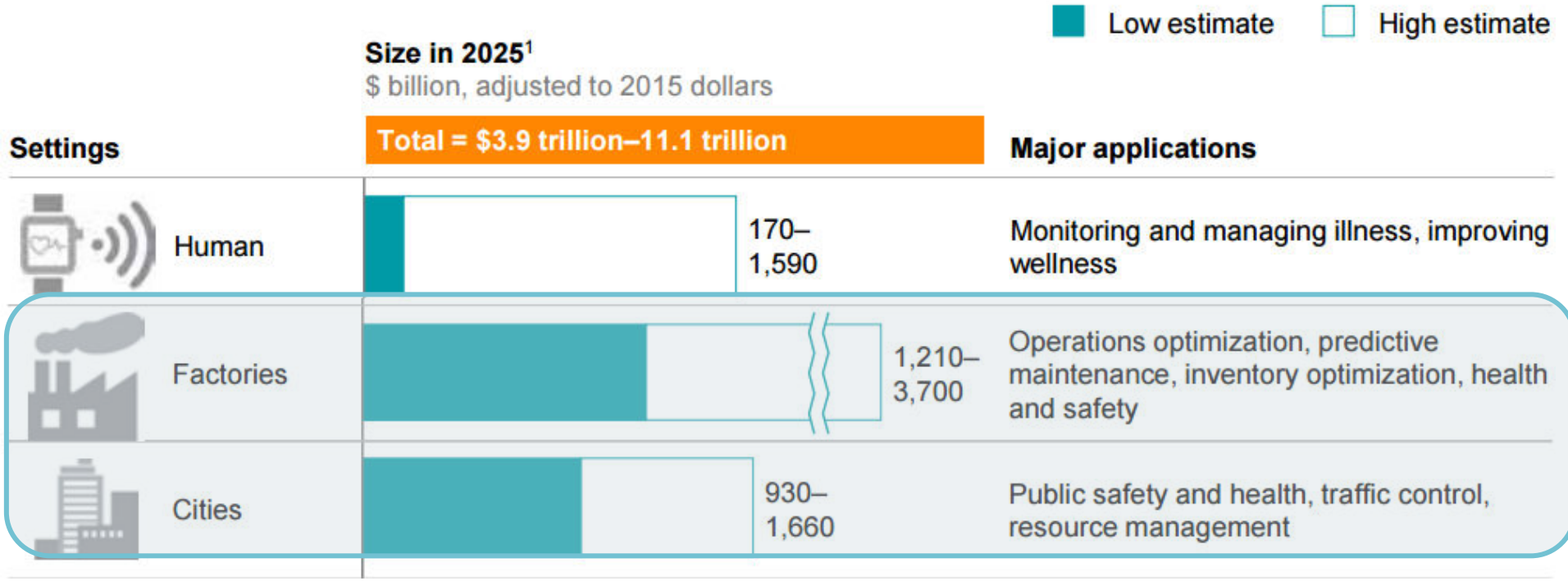
European initiatives

Horizon 2020 Programme



Smart manufacturing and the EU's 'Digitizing Industry' initiative // European Commission, 2016

Smart Things



- Fundamentally new approaches to digital design based on complete mathematical modeling and optimization technologies;
- Virtual tests, which significantly reduce the amount of expensive field tests;
- Advanced technologies and digital smart production

THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE // McKinsey Global Institute (MGI), 2015.

Smart Industry

Merging of the virtual and physical worlds

- through cyber-physical systems

Fusion of

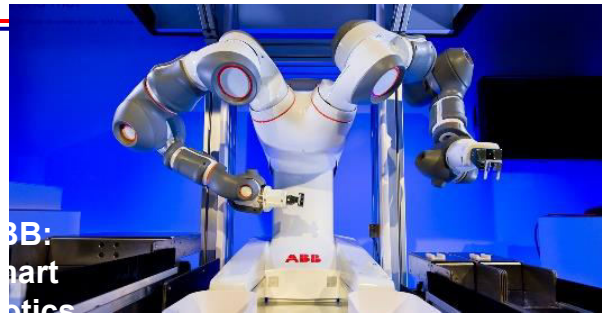
- technical processes
- intelligent sensor network
- computational models, digital twins

"Industrial Internet of Things" (IIOT) - driving operational efficiencies through

- Automation
- Connectivity
- Analytics

Data mining
Storage
Monitoring and forecasting
Identification of the critical state

- prevent accidents
- optimization



Smart City

Cities are 2 % of earth surface

- 54% population
- 75% of energy consumption

100+ new cities of 1 million+ people in next 10 years

Smart City

Smart Governance
- Participation
- Transparency and information accessibility
- Public and social service
- Multi-level governance

Smart Economy
- Innovation
- Entrepreneurship
- Local & Global interconnectedness
- Productivity
- Flexibility of labor market

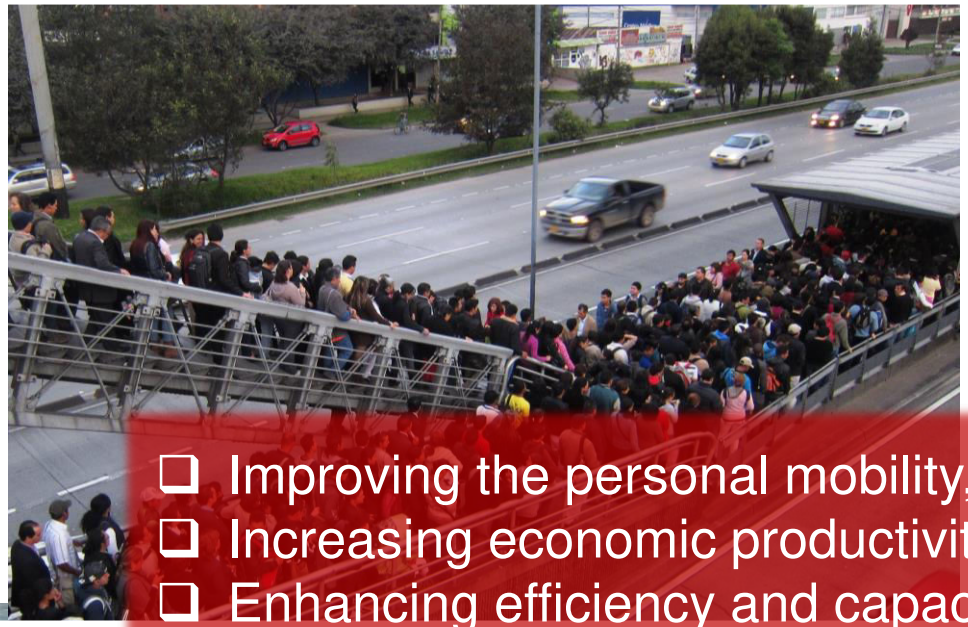
Smart Mobility
- Traffic management
- Public transport
- Logistics
- Accessibility
- Clean, non-motorized options
- Multimodality

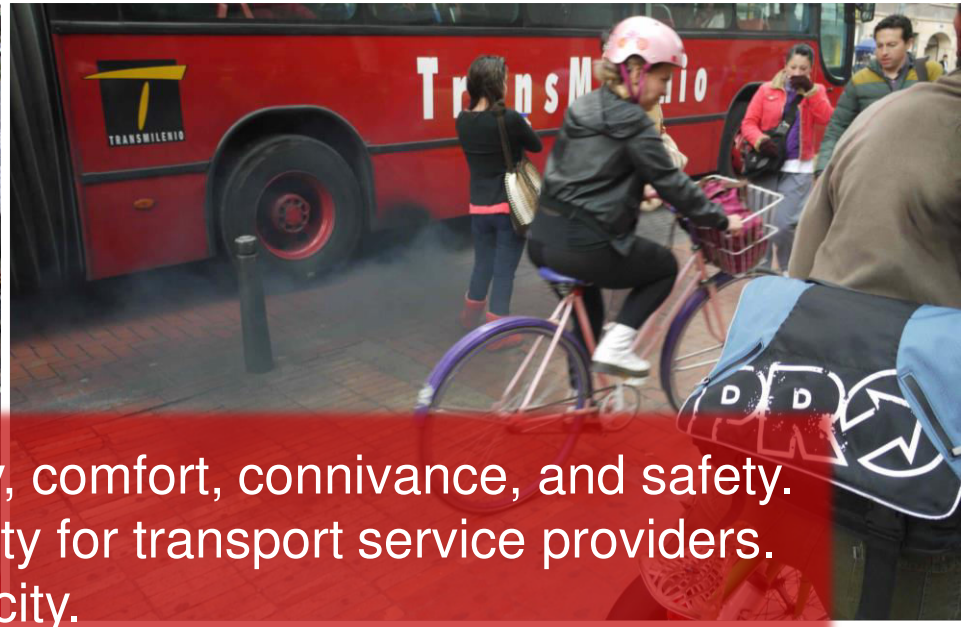
Smart Environment
- Environmental monitoring
- Energy efficiency
- Urban planning and urban refurbishment
- Smart building and smart renovation
- Resource management
- Environmental protection

Smart People
- Digital education
- Creativity
- Community building
- Urban life management

Smart Living
- Tourism
- Culture and leisure
- Healthcare
- Security
- Technology Accessibility
- Public space management

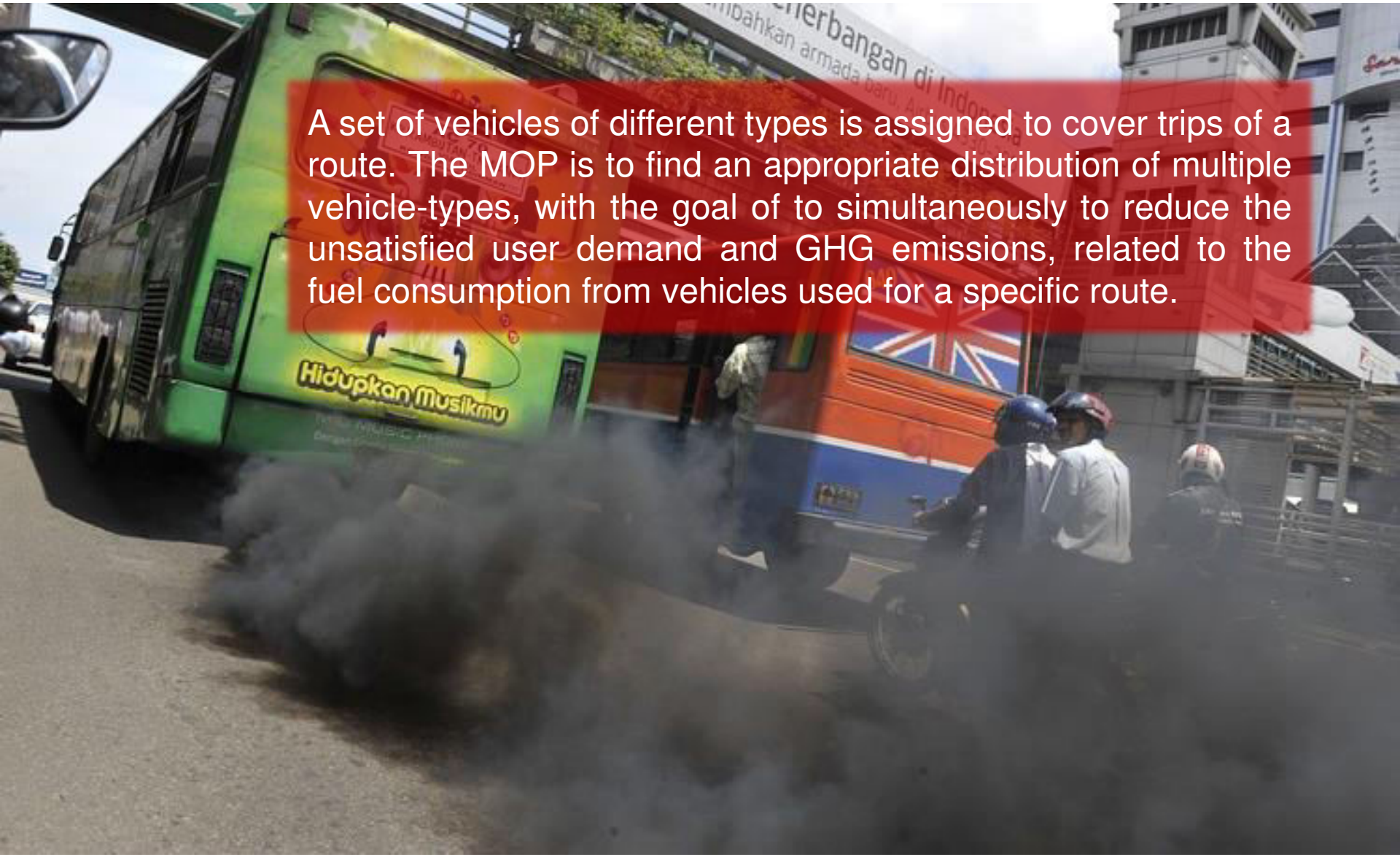
Smart Mobility





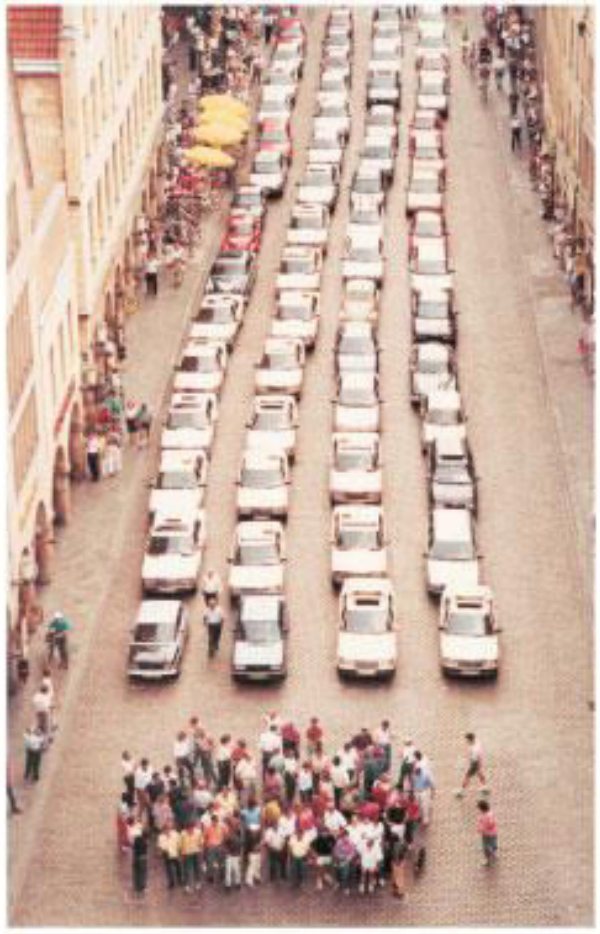
- Improving the personal mobility, comfort, connivance, and safety.
- Increasing economic productivity for transport service providers.
- Enhancing efficiency and capacity.
- Reducing gas consumption and negative environmental impact.

Environmental protection



A set of vehicles of different types is assigned to cover trips of a route. The MOP is to find an appropriate distribution of multiple vehicle-types, with the goal of to simultaneously to reduce the unsatisfied user demand and GHG emissions, related to the fuel consumption from vehicles used for a specific route.

Three solutions: what to select



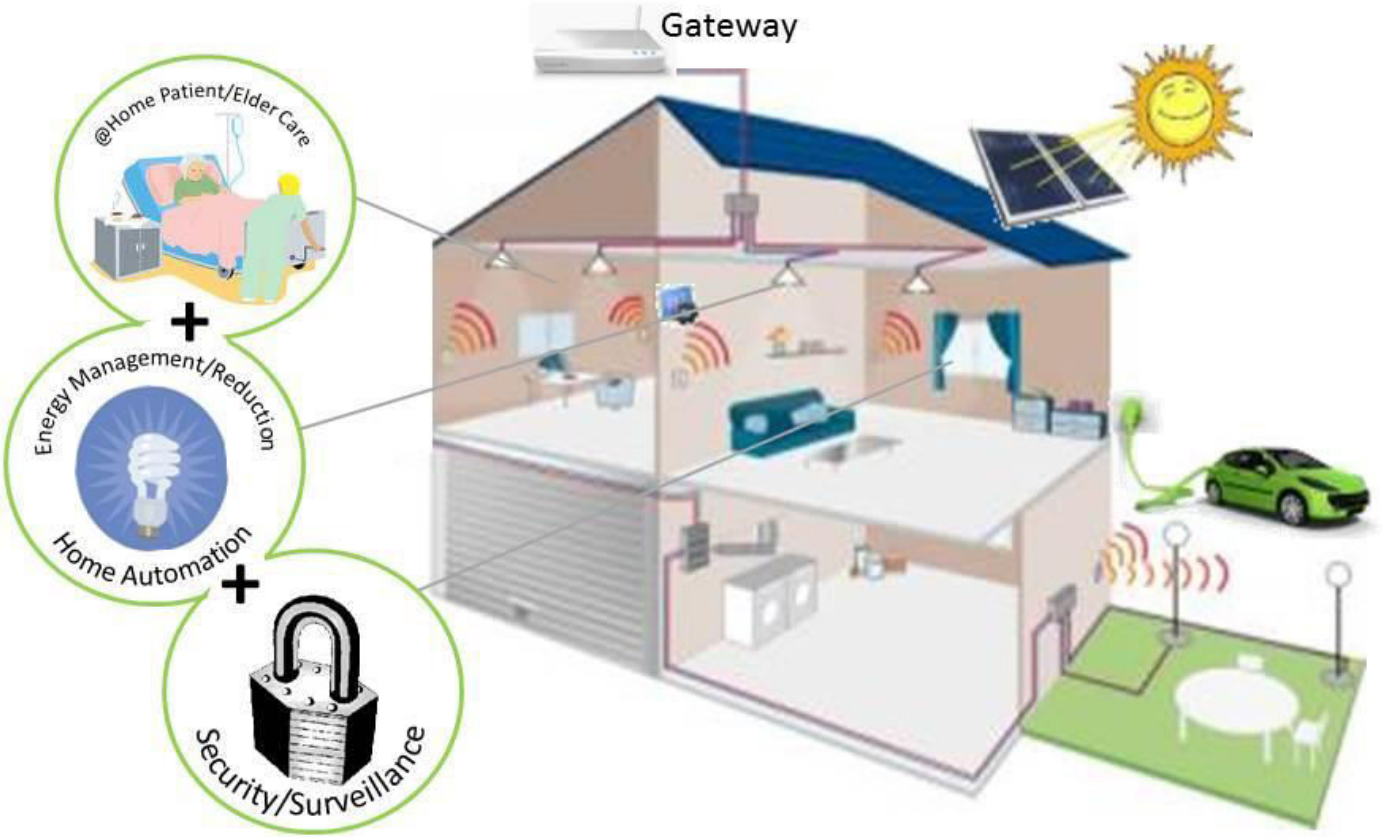
Uncertainty

- Communication failure
- Break-down of a vehicle
- Failures in the transport network
- Passenger demand
- Weather changes
- Modification of the transportation requests

Smart Home

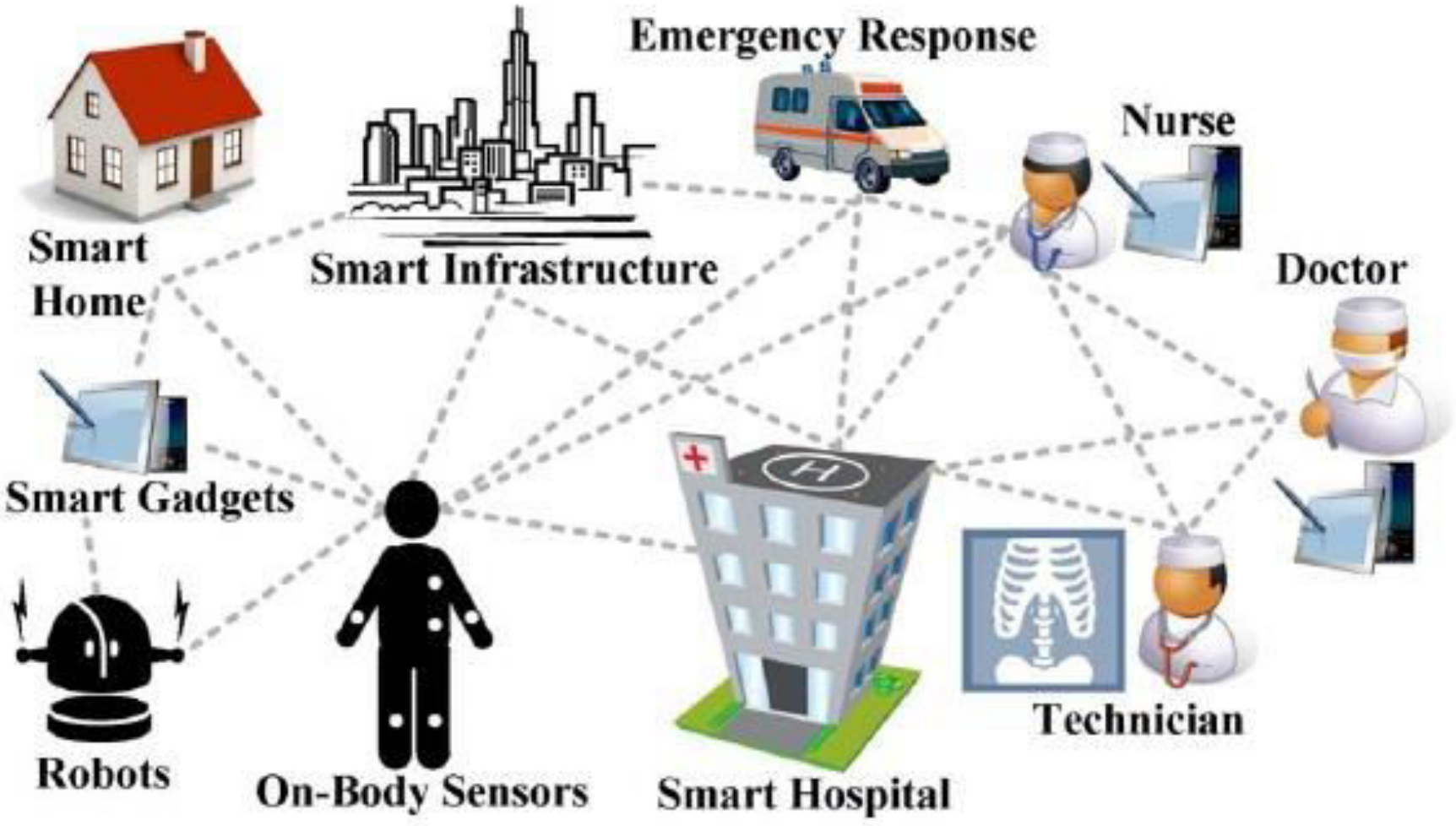
Smart Home/Business Gateway Platform

Lowers barrier to convergent smart technical and economic IoT innovation

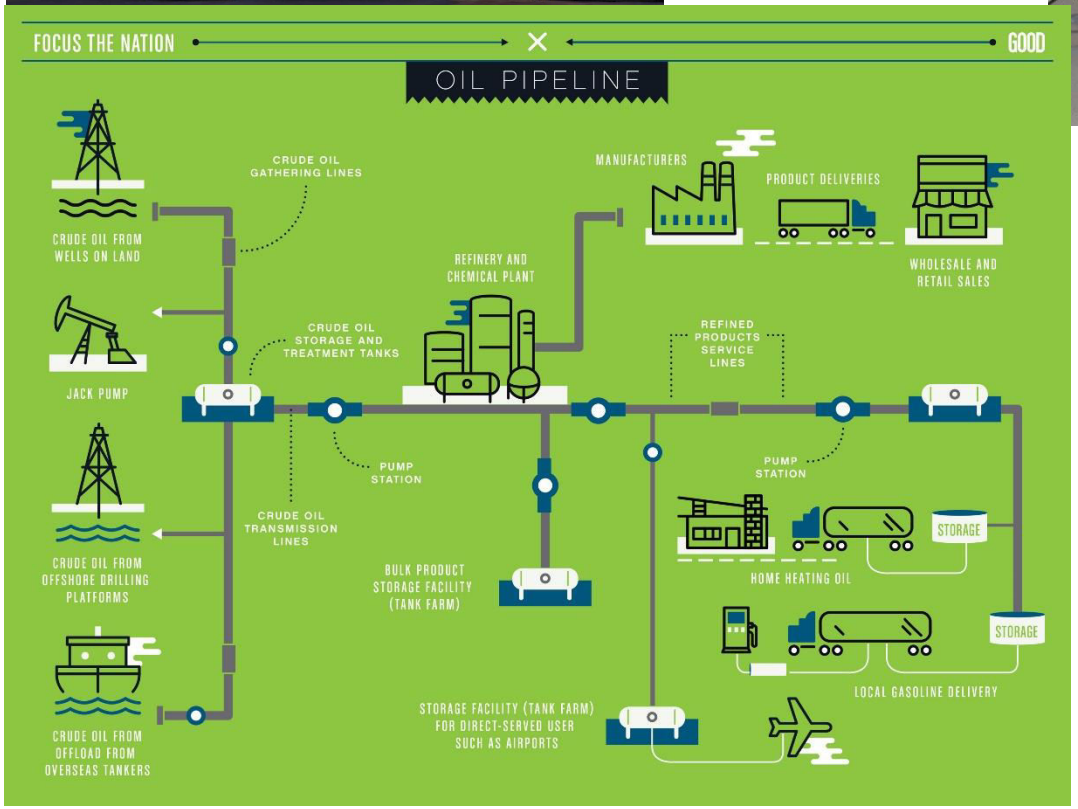


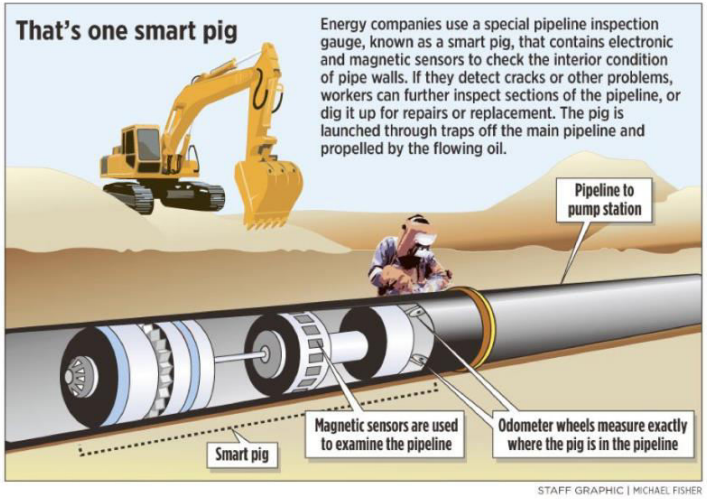
TATUNG adaptive · reliable | life.augmented | arKados | GRID2HOME SMART ENERGY SOLUTIONS | ProSyst

Smart Healthcare

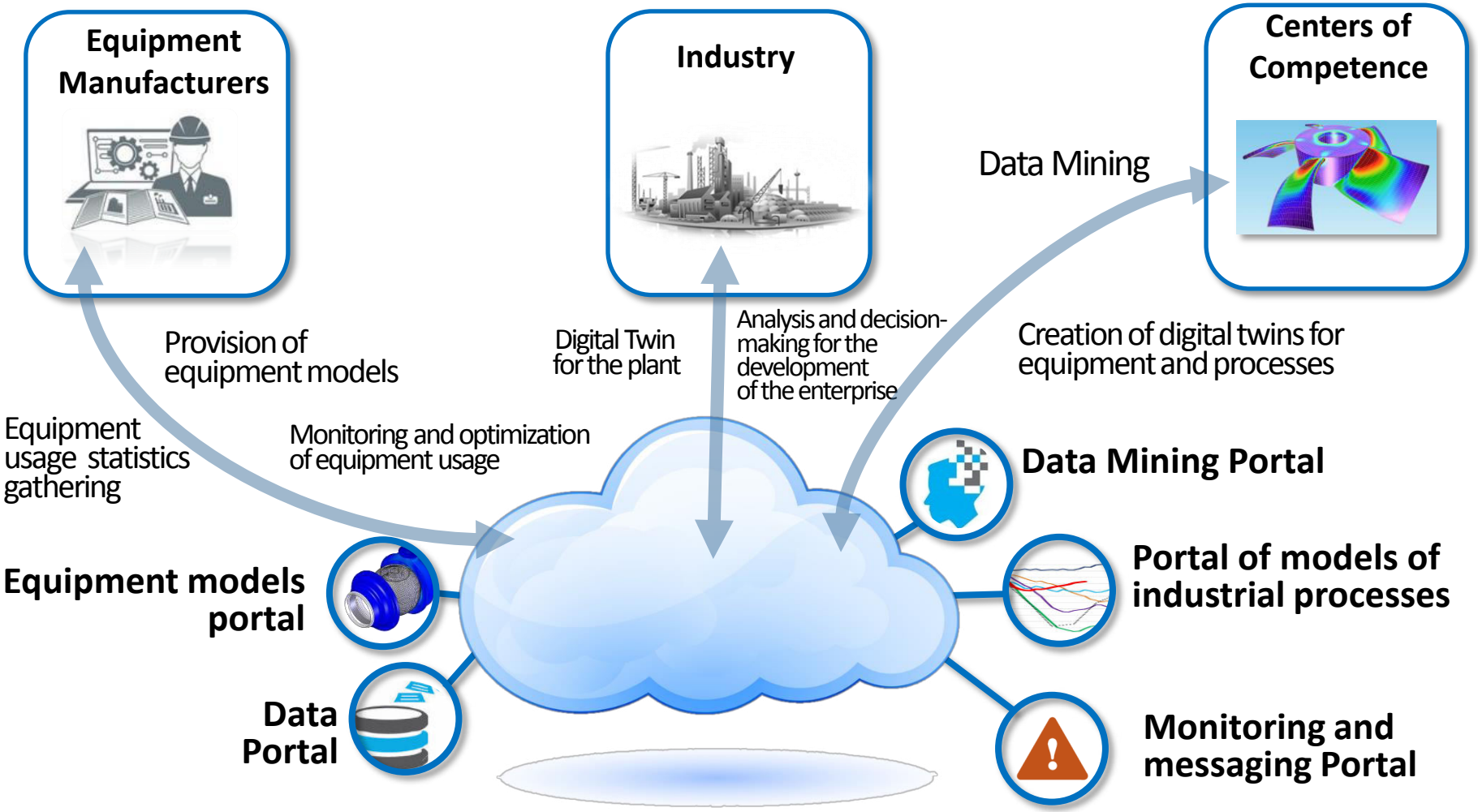


Smart oil and gas industry



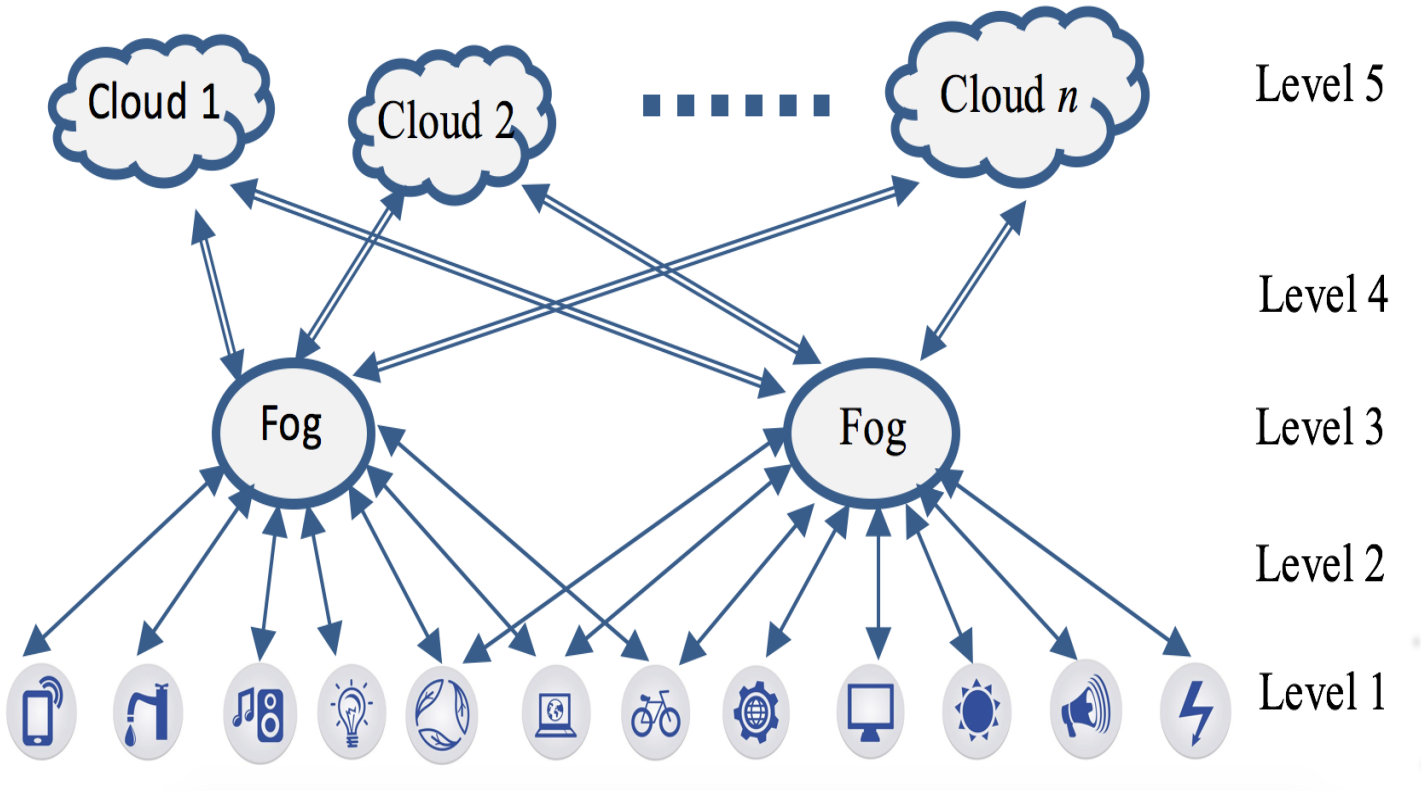


Cloud Platform



Internet of Things - Platform for Connected Smart Objects

Integrates sensing, communications, and analytics



Analytics

Storage

Computational models

Remote services

Data mining

Remote monitoring

Intelligent sensors

Edge computing

Merging of the virtual and physical worlds

- through cyber-physical systems

Security requirements

Reliability
- fault-tolerant systems, operational in case of components failures

Availability
- ensuring to access the information when needed

Confidentiality
- protecting the information from disclosure to unauthorized parties

Integrity
- whole and undivided

Privacy
- free from public attention, not observed or disturbed by other people.

Scalability
- ability to be used or produced in a range of capabilities

Надежность
- отказоустойчивые системы, работающие в случае сбоев компонентов

Доступность
- обеспечение доступа к информации при необходимости

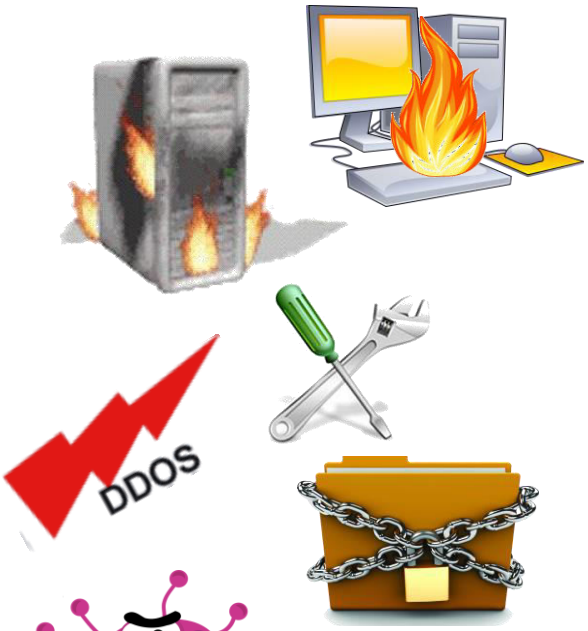
Конфиденциальность
- защита информации от неавторизованных сторон

Целостность
- цельный и неразделенный

Секретность
- без общественного внимания, не наблюдаемого или нарушенного другими людьми.

Масштабируемость
- возможность использования в средах различной размерности

Security Threats



Environmental threats

- Earthquakes, floods, fire, etc

Deliberate threats

- Interception, hacker attacks, etc.

Accidental threats

- PC errors, Virus, Spam, etc.

Экологические угрозы

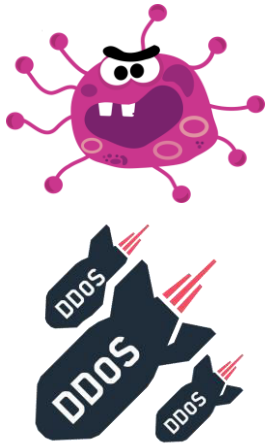
- Землетрясения, наводнения, пожары и т. д.

Преднамеренные угрозы

- Перехват, хакерские атаки ..

Случайные угрозы

- Ошибки ПК, Вирус, Спам ...



- Theft of money, personal data, corporate information;
- Espionage
- Intentional organization of accidents,
- Organization of power outages;
- Interception of control of devices and systems;
- Violation of the transport system and others.
- etc

- Кража денег, личных данных, корпоративной информации;
- шпионаж
- Преднамеренная организация аварий,
- Организация отключений электроэнергии;
- Перехват управления устройствами и системами;
- Нарушение транспортной системы.
- и т.д.

Security Threats at Levels 1, 3, 5

1. **Access Control Issues**
2. **Account Hijacking**
3. **Data Breaches**
4. **Insecure APIs**
5. **Malicious Insider**
6. **Abuse and Nefarious**
7. **Denial of Service**
8. **Data Loss**
9. **System and Application Vulnerabilities**
10. **Shared Technology Issues**

etc.

1. Проблемы с управлением доступа
2. Взлом аккаунтов
3. Нарушения данных
4. Небезопасные API
5. Злоумышленник - инсайдер
6. Злоупотребление и недобросовестность
7. Отказ в обслуживании
8. Потеря данных
9. Уязвимость систем и приложений
10. Проблемы совместных технологии

Cloud Security Alliance (2016)
12 Cloud Computing Top Threats in 2016.

Security Risks at Levels 1, 3, 5

- Stealing data
- Poor management
- Hijack user accounts
- Stolen confidential data
- To attack unsafe APIs Cloud/Fog providers
- A user who has authorized access to the network and system, but has intentionally decided to act maliciously
- Malicious users utilize resources to undertake malicious activity
- Technical failures due to technical overloads a system's
- Data is accidentally deleted from the system
- Bugs arising from software ad configuration errors
- Organization rushed the adoption, design, and implementation of any system
- Occur due to sharing infrastructures, platforms or applications

- Кража данных
- Плохое управление
- Взлом учетных записей пользователей
- Кража конфиденциальных данных
- Атаки через небезопасные API-интерфейсы к Облачным / туманным провайдерам
- Пользователь, который имеет авторизованный доступ к сети и системе, но намеренно решил действовать злонамеренно
- Вредоносные пользователи используют ресурсы для совершения злонамеренных действий
- Технические сбои из-за технических перегрузок
- Данные случайно удаляются из системы
- Ошибки, возникающие при ошибках конфигурации программного обеспечения
- Поспешность в принятии, разработки и внедрении любой системы
- Совместное использование инфраструктур, платформ или приложений

Cloud Security Alliance (2016)
12 Cloud Computing Top Threats in 2016.

Security Solutions at Levels 1, 3, 5

Cloud Security Alliance (2016)
12 Cloud Computing Top Threats in 2016.

Cryptographic	Криптография
Encryption algorithm	Алгоритмы шифрования
Data origin authentication	Аутентификация
Digital Signature Scheme	Цифровая подпись
Homomorphic encryption	Гомоморфное шифрование
Secret sharing schemes	Схемы распределения секрета
Data replication	Репликация данных
Redundant Residue Number System	Система остаточных классов
Erasure code	Коды Стирания
Regenerating code	Коды регенерации

Access to Privileged Systems

- User errors, Carelessness
  Errores de usuario, Descuido
- Falsification, Offline
  Falsificación, Desconectado
- etc.

Security Breaches (Нарушения безопасности)

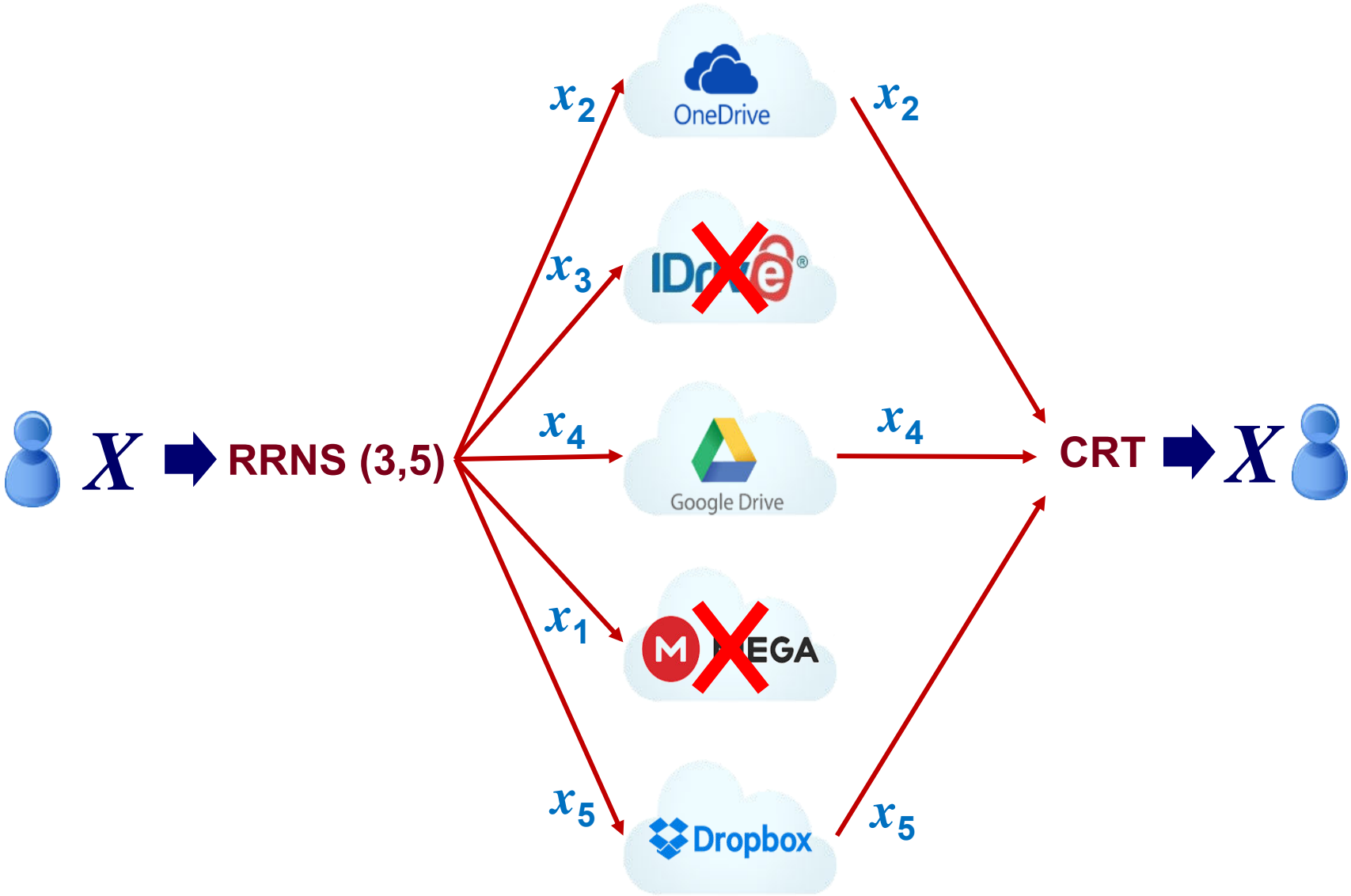
An incident during which an encrypted data is substituted or hacked, and the valuable data stored within is compromised.

Collusion (тайный сговор)

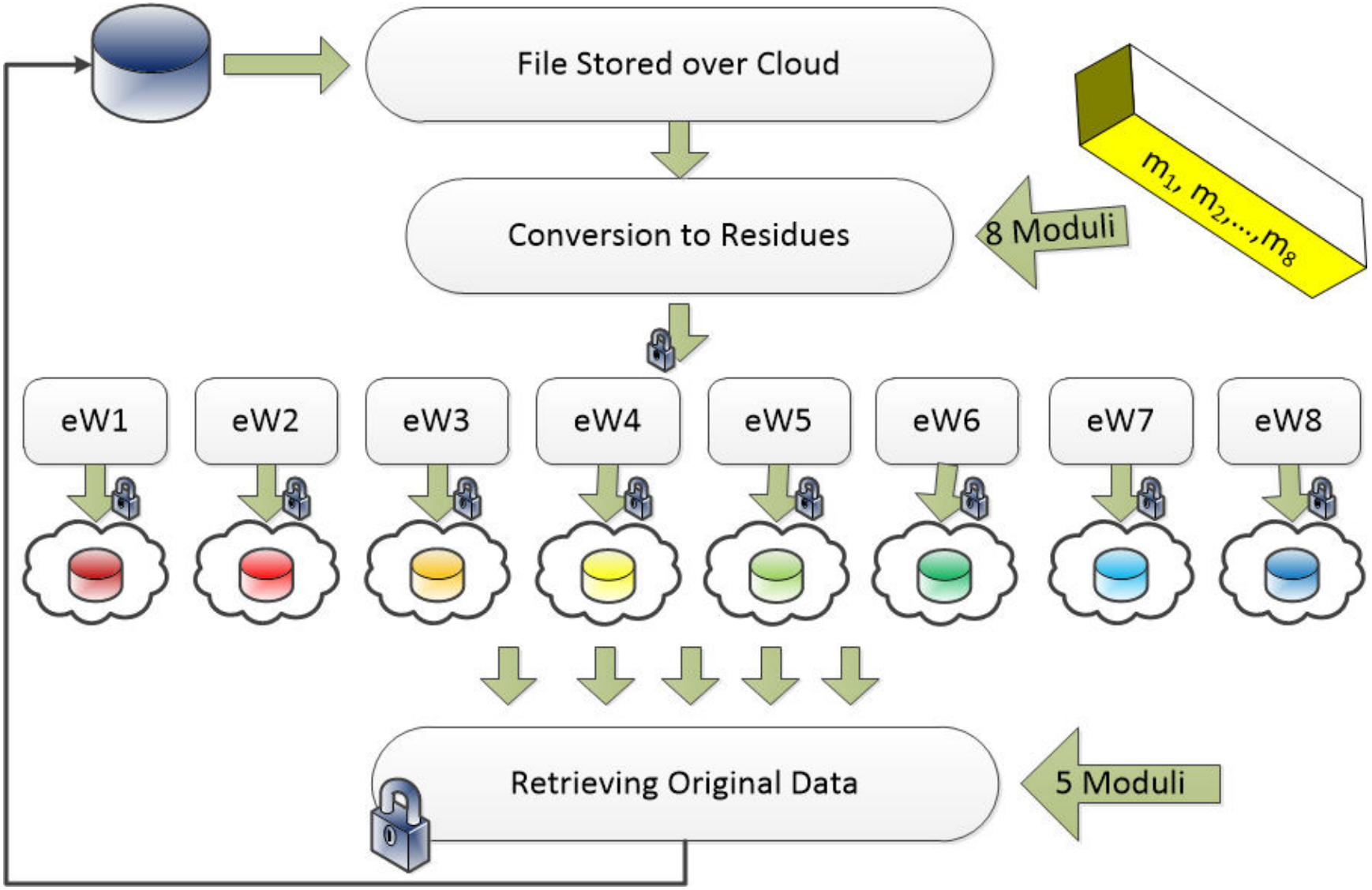
Improper secret agreement between two or more entities, to obtain unauthorized access to confidential data.

Incumplimiento de seguridad de datos. sustituyen o piratean datos encriptados y se comprometen los datos almacenados en ellos.

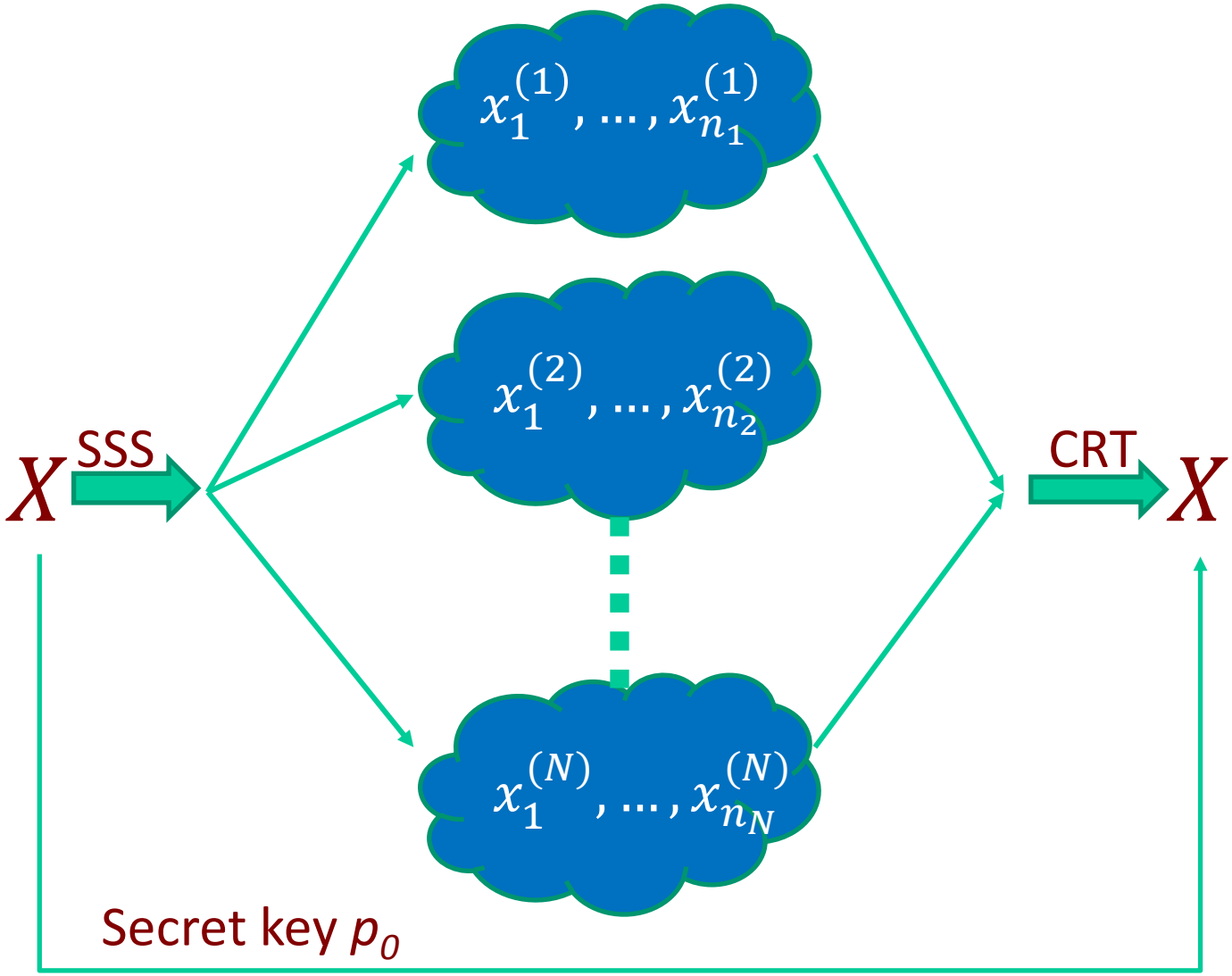
Our model


X
RRNS (3,5)
x_2
x_3
x_4
x_1
x_5
OneDrive
IDrive
Google Drive
MEGA
Dropbox
x_2
x_4
x_5
CRT
X

Storage over clouds using RNS



Our model



n_i is weight of i-th cloud

Pros

- Security
- Confidentiality
- Collusion
- Privacy
- Availability
- Reliability
- Scalability
- Homomorphic
- Small Redundancy
- Load Balancing

Cons

- Average data coding rate

Thanks for your attention!


+++ опубликовано на err404.ru +++