Κυβερνοασφάλεια και ιδιωτικότητα στις έξυπνες πόλεις

ΚΩΝΣΤΑΝΤΙΝΟΣ ΡΑΝΤΟΣ
ΑΝΑΠΛΗΡΩΤΗΣ ΚΑΘΗΓΗΤΗΣ
WEB SERVICES AND INFORMATION SECURITY LAB
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ – ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

"In a few decades' time, computers will be interwoven into almost every industrial product"

Karl Steinbuch, 1966

Internet of Things

A vision…

Interconnect all “things” (industrial products)

Heterogeneous technologies

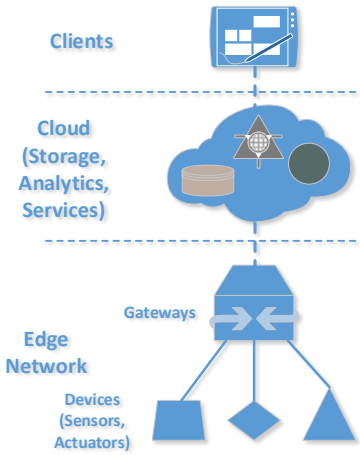
Intelligent and Innovative Services

Interact with the physical world

IT IS WHERE THE INTERNET MEETS THE PHYSICAL WORLD

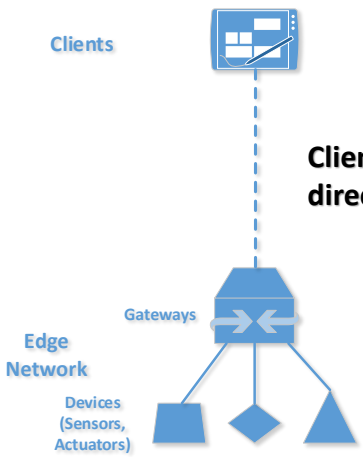
Almost EVERYTHING connected

IoT architecture



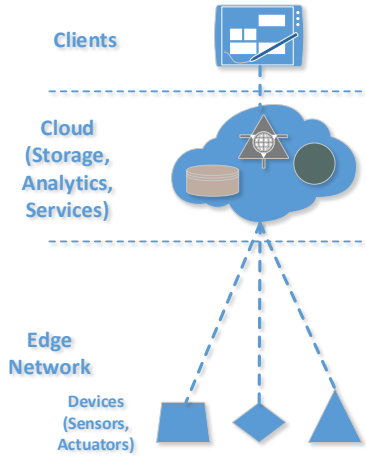
Cyber-physical systems

IoT architecture



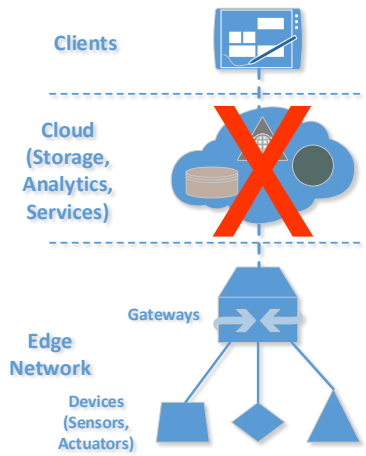
Clients can talk directly to gateways

IoT architecture



3G/4G/LTE/5G devices can talk directly to clouds

IoT architecture

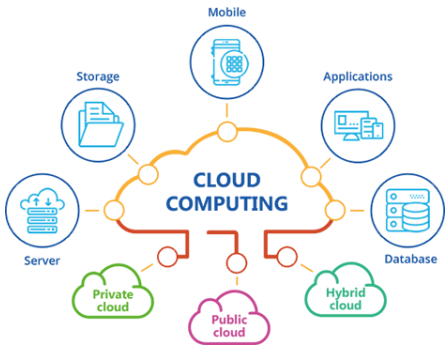


Cloud is not always necessary

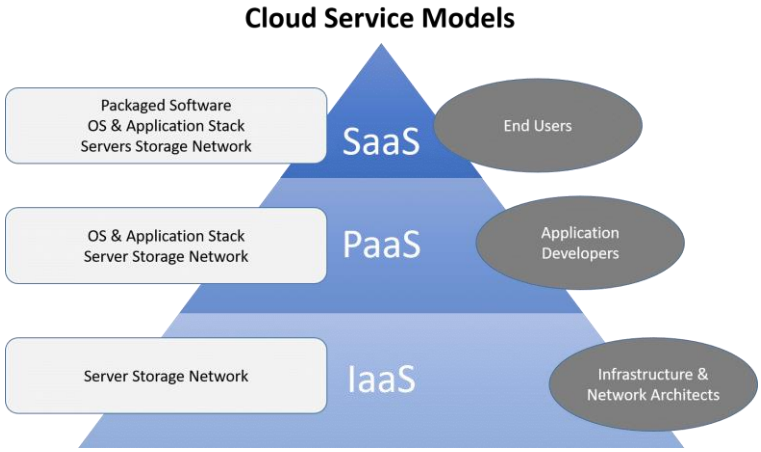
micro-datacenters in 5G cell towers

Cloud Computing

Enables worldwide **network access** to a **shared** set of **configurable IT resources** (e.g. networks, servers, storage, applications and services) that can be provided quickly
with minimal management
effort or service interaction



Cloud Computing – Main Service Models



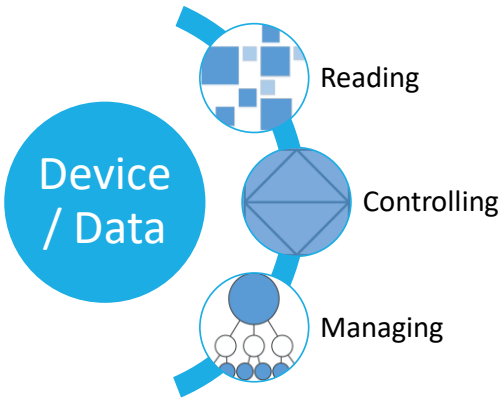
Cloud Computing – Main Service Models

Software as a Service (SaaS): Users can use the provider's apps running on a cloud infrastructure

Platform as a Service (PaaS): Users can develop applications using programming languages, libraries, services, and tools supported by the provider

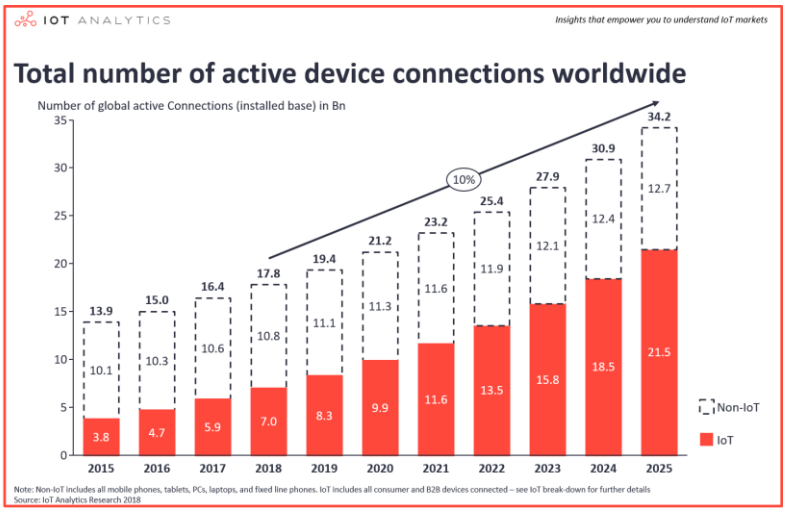
Infrastructure as a Service (IaaS): The user provides basic computing resources to develop and execute arbitrary software, which can include operating systems and applications

Smart technologies

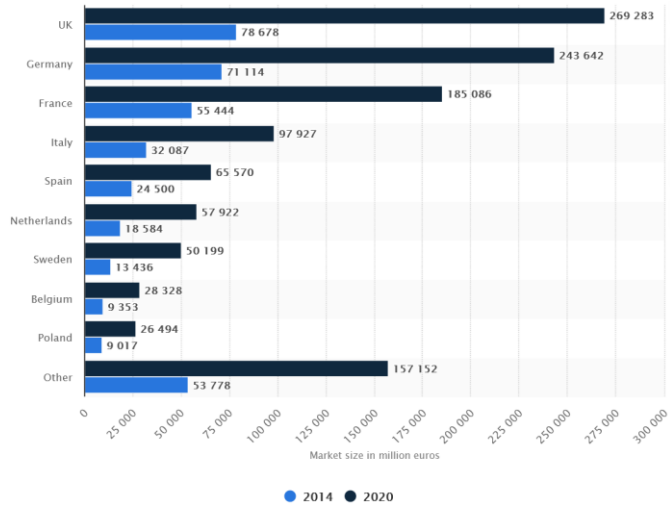


Το IoT σε αριθμούς

IoT analytics

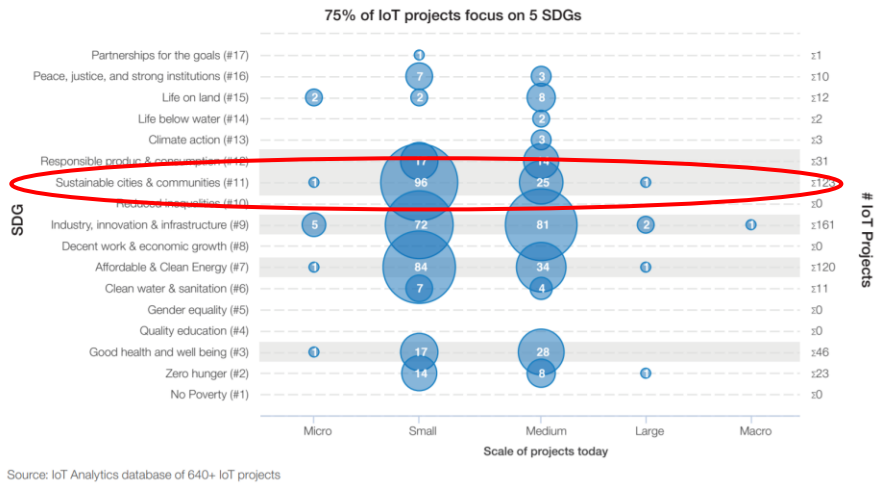


IoT market size in Europe 2014 and 2020



Source: Statista (2020)

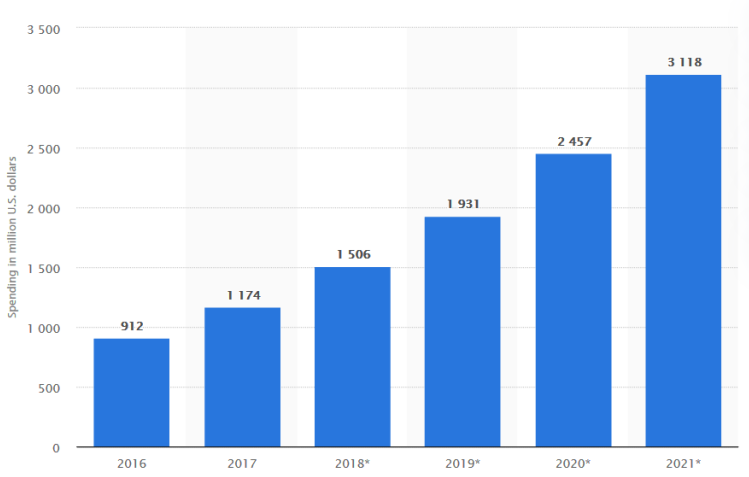
Focus of IoT projects (2018)



Source: IoT Analytics database of 640+ IoT projects

WORLD ECONOMIC FORUM

Spending on IoT security



Source: Statista (2020)

Smart cities

Smart Cities – Έξυπνες Πόλεις

Πόλεις που χρησιμοποιούν

(έξυπνες) τεχνολογίες πληροφορικής και επικοινωνιών

για να αυξήσουν την επιχειρησιακή αποτελεσματικότητα,

να μοιράζονται πληροφορίες με το κοινό και

να βελτιώσουν τόσο την ποιότητα των κυβερνητικών υπηρεσιών

όσο και την ευημερία των πολιτών.

Smart Cities – Έξυπνες Πόλεις

Πόλεις που χρησιμοποιούν

- IoT αισθητήρες (sensors),
- IoT ενεργοποιητές (actuators),
- τεχνολογίες επικοινωνιών

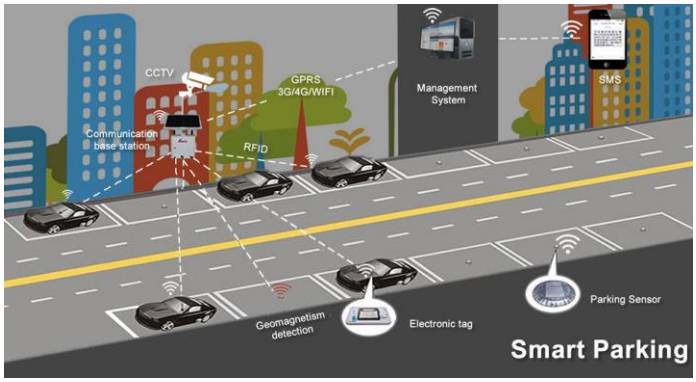
Επιτρέπουν τη διασύνδεση όλων των επιπέδων μιας πόλης:

υπέργεια – επίγεια – υπόγεια

Smart cities world

Smart Parking

Εύρεση θέσεων πάρκινγκ – Ψηφιακή πληρωμή



Smart Parking - Οφέλη

- ✓ **Βελτιστοποίηση της διαδικασίας** – εξοικονόμηση χρόνου και πόρων, και μειωμένη προσπάθεια
- ✓ **Μείωση της κίνησης** – του αριθμού των οχημάτων που χρειάζεται να κινούνται στους δρόμους
- ✓ **Μείωση της ρύπανσης του περιβάλλοντος** – λόγω της μειωμένης κίνησης.
- ✓ **Δεδομένα πραγματικού χρόνου** – αναφορικά με την κατάσταση των διαθέσιμων θέσεων.
- ✓ **Μείωση του κόστους διαχείρισης** – μέσω της αυτοματοποίησης των λειτουργιών, π.χ. πληρωμή.
- ✓ **Ποιότητα υπηρεσιών** – γρήγορη εξυπηρέτηση και άνεση

Smart Traffic Management – Έξυπνη διαχείριση της κυκλοφορίας

Παρακολούθηση και ανάλυση της ροής της κίνησης

Βελτιστοποίηση των φωτεινών σηματοδοτών – αποφυγή συμφόρησης
- Βάσει της κυκλοφορίας, των ωρών κυκλοφοριακής αιχμής, ώρα της ημέρας

Smart Traffic Management – Οφέλη

Μείωση της κυκλοφοριακής συμφόρησης
- εξομάλυνση των κυκλοφοριακών ροών
- προτεραιότητα στην κίνηση ανταποκρινόμενη στη ζήτηση σε πραγματικό χρόνο.

Μείωση της ατμοσφαιρικής ρύπανσης

Δυνατότητα να δίνεται προτεραιότητα στα λεωφορεία που προσεγγίζουν τις διασταυρώσεις

Γρηγορότερη παρέμβαση σε περίπτωση ατυχήματος

Ενεργοποίηση ελέγχου εισερχόμενης ροής.

Smart Home

Βελτίωση της ποιότητας ζωής και της ασφάλειας
- Παρακολούθηση και έλεγχο της θερμοκρασίας και υγρασίας
- Έλεγχο του φωτισμού και της έντασης αυτού
- Παρακολούθηση και φροντίδα του κήπου
- Ειδοποίηση για πλημμύρα/πυρκαγιά
- Έξυπνες κλειδαριές

Smart Home

Μέχρι το 2020, απ' όλες τις διασυνδεμένες συσκευές:
- 37%: air conditioners (186εκ μονάδες)
- 28% ψυγεία (120εκ μονάδες)
- 27% πλυντήρια (131εκ μονάδες)
- 4% πλυντήρια πιάτων (17εκ)
- 2% στεγνωτήρια
- 2% κουζίνες

IHS Markit

Πηγή: http://www.homeappliancesworld.com

Ambient Assisted Living – Αυτόνομη Διαβίωση Υποβοηθούμενη από το Περιβάλλον

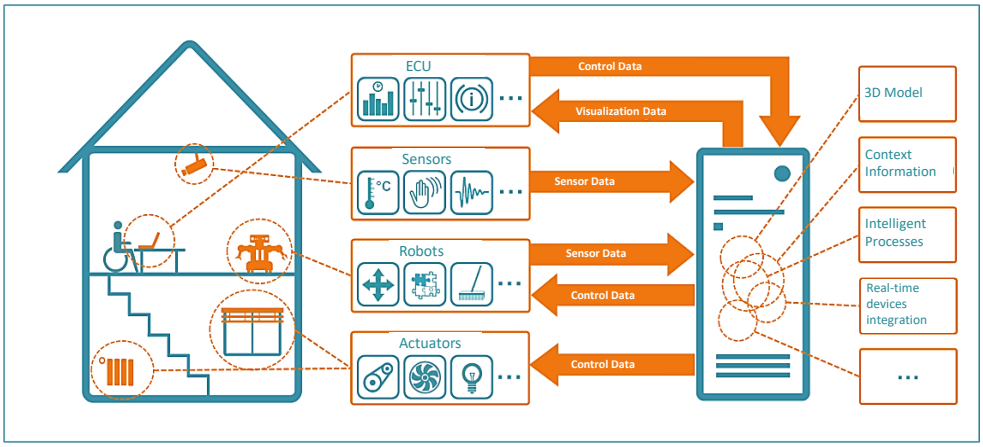
Ένα οικοσύστημα

- διαφόρων τύπων αισθητήρων,
- ηλεκτρονικών υπολογιστών,
- κινητών συσκευών,
- ασύρματων δικτύων και
- εφαρμογών λογισμικού

για την παρακολούθηση συστημάτων προσωπικής υγειονομικής περίθαλψης και τηλεϊατρικής.

Επιτρέπει στους ηλικιωμένους να ζουν ανεξάρτητα όσο το δυνατόν περισσότερο και να παρακολουθούνται.

Ambient Assisted Living

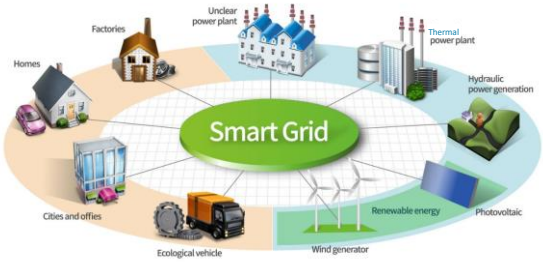


Smart Grids

Ηλεκτρικό δίκτυο που χρησιμοποιεί **πληροφορίες**, τεχνολογίες **αμφίδρομης ασφαλούς επικοινωνίας** στον κυβερνοχώρο και **υπολογιστική νοημοσύνη**, με ολοκληρωμένο τρόπο για την

- παραγωγή,
- μετάδοση,
- διανομή,
- κατανάλωση

ηλεκτρικής ενέργειας

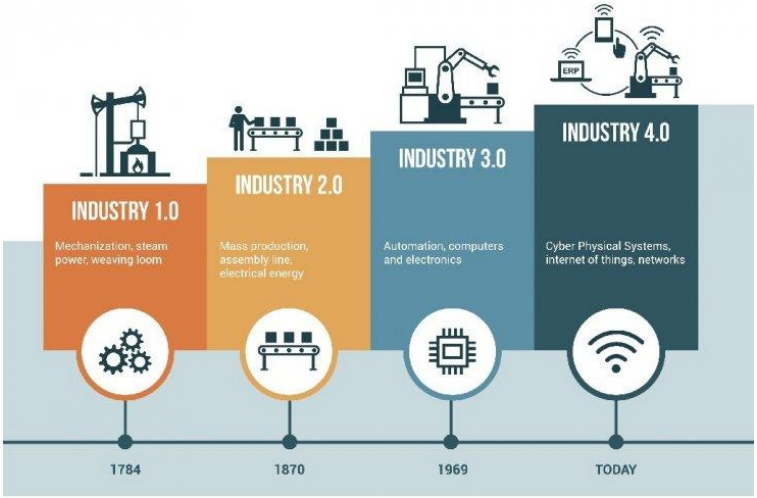


Smart Grids

Περιλαμβάνουν ποικίλα συστήματα λειτουργίας και ενέργειας:

- έξυπνους μετρητές
- έξυπνες συσκευές
- ανανεώσιμες πηγές ενέργειας
- ενεργειακά αποδοτικούς πόρους

Industrial Internet of Things



Industry 4.0 vision

*"these Cyber-Physical Systems comprise **smart machines**, **storage systems** and **production facilities** capable of **autonomously exchanging information**, **triggering actions** and **controlling each other** independently.*

This facilitates fundamental improvements to the industrial processes involved in manufacturing, engineering, material usage and supply chain and life cycle management."

Άλλοι τομείς

Παρακολούθηση των κινήσεων και της ασφάλειας επιβατών σε ΜΜΜ, ή σε οχήματα στο οδικό δίκτυο.

Απόδοση των καλλιεργειών
Βελτιστοποίηση και μείωση της χρήσης φυτοφαρμάκων / λιπασμάτων – χρήση IoT για τον εντοπισμό και την παράδοσή τους μόνο όταν χρειάζονται.

Άλλοι τομείς

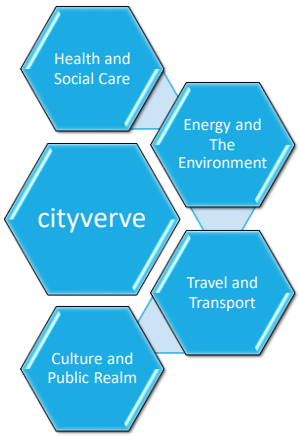
Συλλογή περιβαλλοντικών δεδομένων για τη βέλτιστη λήψη αποφάσεων και τη ρύθμιση της δημόσιας πολιτικής, ή για την προειδοποίηση για περιβαλλοντικές απειλές όπως πυρκαγιές, σεισμοί ή ηφαιστειακές διαταραχές.

Παρακολούθηση της ανθρώπινης υγείας και της φυσικής κατάστασης – π.χ. για νοσοκομειακούς ασθενείς ή αθλητές

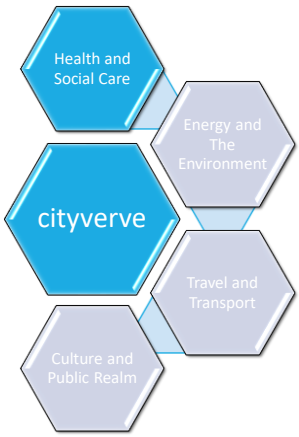
... κ.α.

CITYVERVE - Manchester

CITYVERVE - Manchester

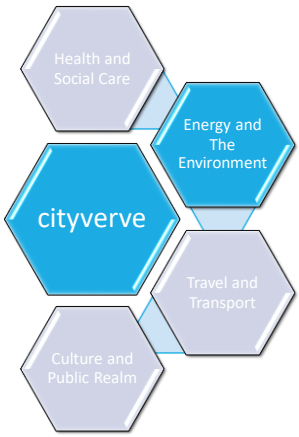


CITYVERVE



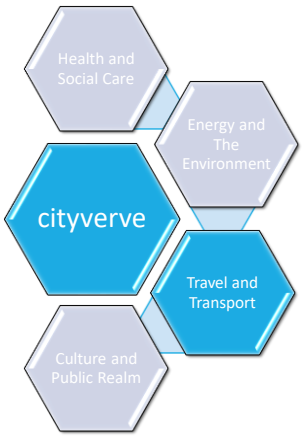
- Monitor patients at home (in-home sensors)
- Grant access to patients' homes via IoT locks managed through the cloud

CITYVERVE



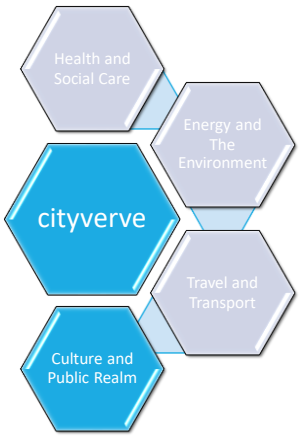
- Monitor water's quality (real-time) to prevent diseases
- Occupancy monitoring in buildings, e.g. for cleaning services
- Monitoring temperature, humidity, noise, light, and air quality – better building management and energy consumption

CITYVERVE



- Location relevant content -> People 'check-in' to bus stop -> bus operators know there are people waiting
- Integrate transportation and visitor services to allow users to make informed choices regarding the way they travel
- Real-time IoT data on the tram network, accurately measure occupancy and provide information to citizens and tourists accordingly
- Cameras linked up to the IoT network for a better understanding of the type of vehicles that are moving around the city and how congestion points can be addressed
- Smart Parking – spaces close to public transport

CITYVERVE



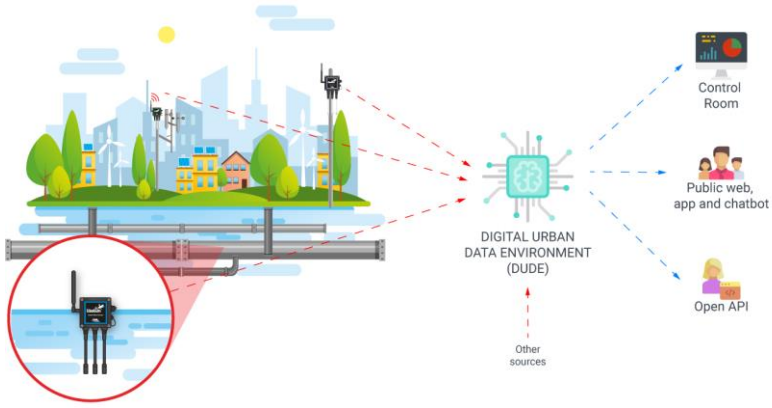
- Community Forums – introduce IoT, explore the possibilities for Manchester
- Gamification of Citizen Centric Areas - Citizens could receive rewards for certain tasks: e.g.
  - recover an eBike that had been left in a remote location,
  - receive a free bus ride if they walk half of their journey to work.

MeSM@RT - Messina

A mix of
- NB-IoT,
- Wi-Fi,
- 3G/4G and
- optical fiber

(with an experiment in 5G in the roadmap)

Messina can control almost everything that may occur in a city in real-time - increases the efficiency of urban services



Source: Libelium.com

MeSM@RT - Messina

Collect:

- Weather Station
- Air pressure
- Air temperature
- Air humidity
- Luminosity
- Noise Level Sensor
- CO
- NO2
- O3
- Particle Matter
- Water pH
- Water ORP
- Water temperature

ΣΥΓΧΡΟΝΕΣ ΑΠΕΙΛΕΣ

IoT: Critical Enablers

…or main barriers?

SECURITY

PRIVACY

INTEROPERABILITY/STANDARDS

ROI (UNCERTAIN)

LEGACY EQUIPMENT

TECHNOLOGY (IM)MATURITY

…

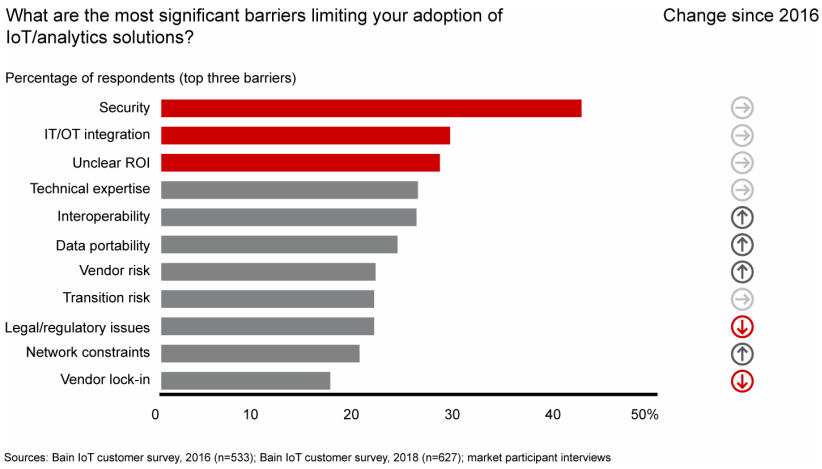
DIGITAL AGENDA FOR EUROPE
A Europe 2020 Initiative

AIOTI

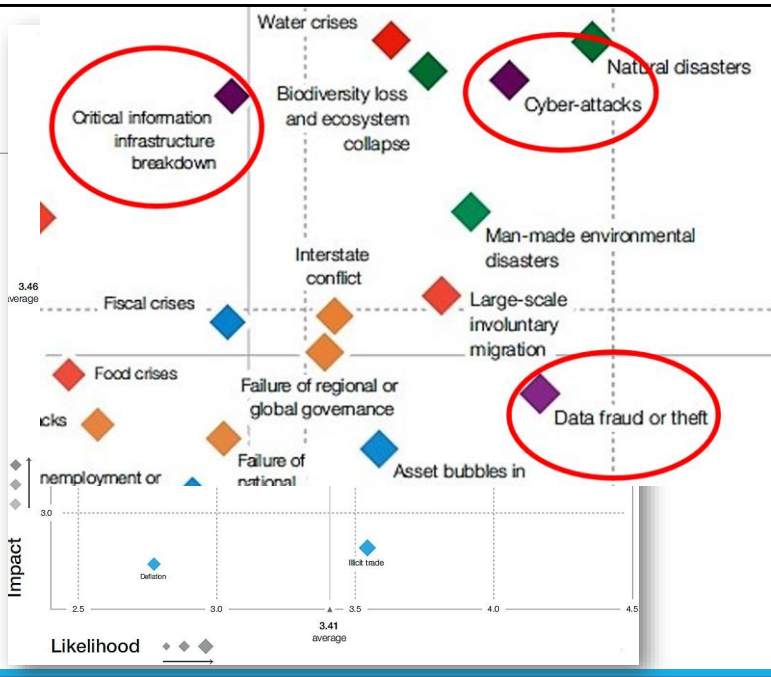
WORLD ECONOMIC FORUM

Industrial Internet Survey, 2014

Τα μεγαλύτερα εμπόδια στην ανάπτυξη του IoT

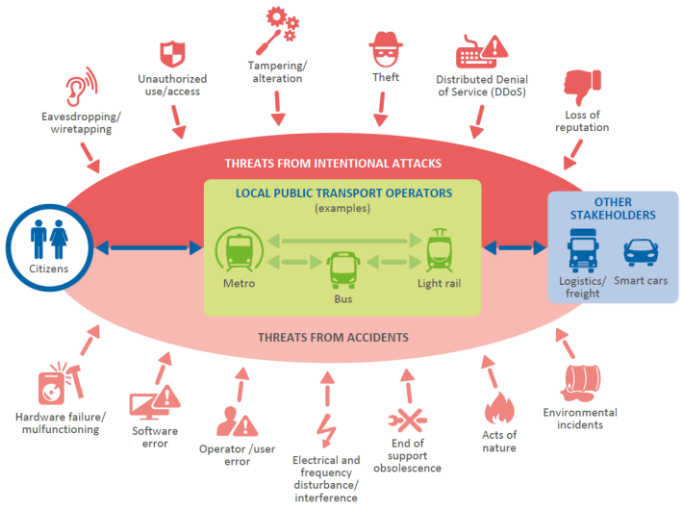


Sources: Bain IoT customer survey, 2016 (n=533); Bain IoT customer survey, 2018 (n=627); market participant interviews



Global Risks
dscape 2019

Απειλές



Πηγή: enisa.eu

Threats

Beyond contemporary cyber-threats

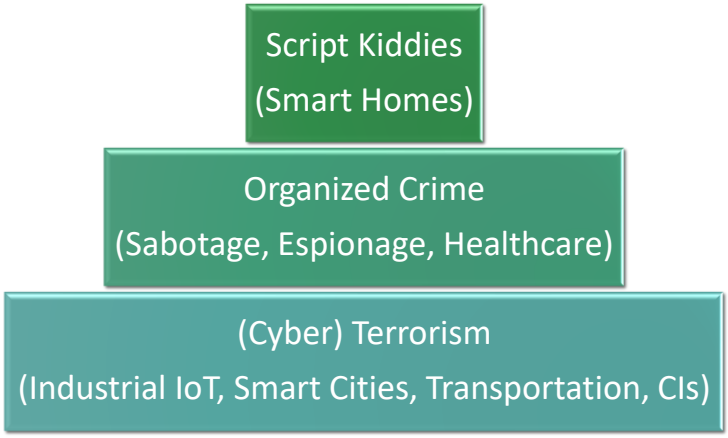
- New (yet unknown) forms of attacks
- Variety of objects – threat diversity
- New ways of interaction

Data is not the data… they are control systems

- (Industrial) Espionage
- Terrorism

MORE THAN JUST THEFT OR SERVICE DISRUPTION

Threats



Security considerations

Expanded attack surface -> more attack vectors

Closed (legacy) systems turn to IP-based

Limited resources at the edge

No physically secure (unattended) devices

Cascading effects to interconnected (Critical) Infrastructures

Wide scale of IoT

Different **remediation** needs

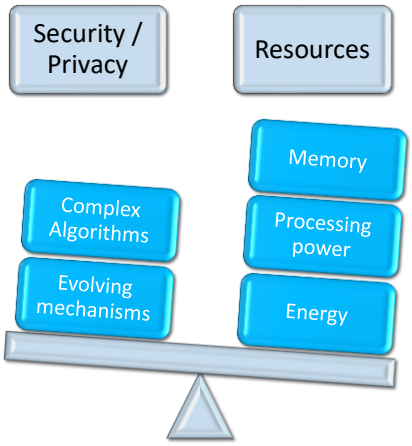
Plethora of **competitive technologies**

Heterogeneous environments

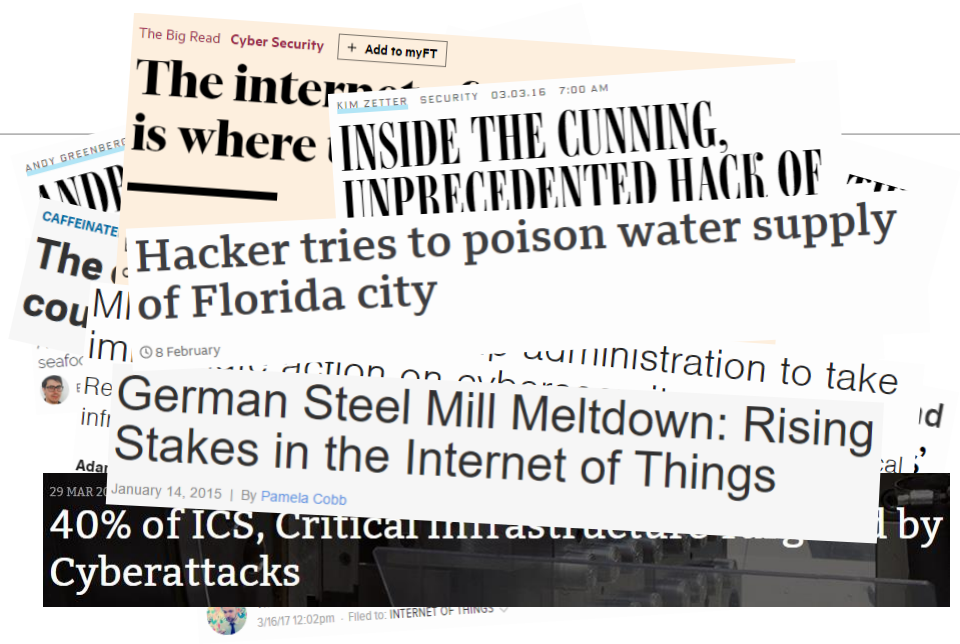
Limited Resources

- Memory
- Processing power
- Energy
- Bandwidth
- Lack of hardware crypto engines

DO THEY DOWNGRADE SECURITY?



ΣΥΜΒΑΝΤΑ


The Big Read Cyber Security
+ Add to myFT
is where
KIM ZETTER SECURITY 03.03.16 7:00 AM
INSIDE THE CUNNING, UNPRECEDENTED HACK OF
Hacker tries to poison water supply of Florida city
8 February
German Steel Mill Meltdown: Rising Stakes in the Internet of Things
January 14, 2015 | By Pamela Cobb
40% of ICS, Critical
by Cyberattacks

US Electrical Grid

THE WALL STREET JOURNAL.

Electricity Grid in U.S. Penetrated By Spies

By Siobhan Gorman

Updated April 8, 2009 11:59 p.m. ET

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries…

Puerto Rican Electric Power Authority – 2009

Hackers used optical probes to hack the meters via the infrared maintenance port

Cost of equipment: ~$400

FBI report: “These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters,”

Cost for the utility: **$400 Million/Year**

Foscam Baby Monitor Hacked

Foscam Security Cameras Full of Security Flaws

Paul Wagenseil · Senior editor, security and privacy
Updated Jun 8, 2017

Attacker was able to control the camera and speak to the baby

Multiple incidents

Access to cameras was not password-protected or protected with the default passwords

BMW Connected Drive Vulnerable

Over a dozen vulnerabilities uncovered in BMW vehicles

Tencent's Keen Security Lab found a number of serious bugs which could be exploited by attackers to remotely attack a number of BMW models.

By Charlie Osborne for Zero Day | May 23, 2018 -- 10:10 GMT (11:10 BST) | Topic: Security

14 vulnerabilities

- 9 required physical access to the vehicle
- 5 were based on using a mobile Internet connection.

Researchers were able to imitate BMW servers and send remote unlocking instructions to vehicles

Source:
https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

Ukrainian power grid attack

Hackers compromised information systems of three energy distribution companies – temporary disruption of electricity supply to the end consumers.

30 substations were switched off

230 thousand people were left without electricity for 1 to 6 hours

NHS Ransomware attack

Wannacry Ransomware

- Delivered via email
- Locks up the files and encrypts them
- Payments made in Bitcoin

More than 30 hospitals affected

19.000 appointments cancelled

Cost for NHS: £92m

STUXNET worm

Target: Iran's Natanz nuclear plant – SCADA systems

Malware entered the network using an infected USB stick

Quickly spread through the network – looking for software that controls centrifuges (Siemens Step7) – used to separate different types of uranium

Two attacks

- centrifuges spun dangerously fast, for about 15 minutes
- a month later, it slowed the centrifuges down for around 50 minutes

Around 1000 centrifuges had to be replaced

German Still Mill

Resulted in "massive damage" to the foundry

Initial access: the attackers used

- Social engineering and
- Spear-phishing tactics

Industrial components were compromised

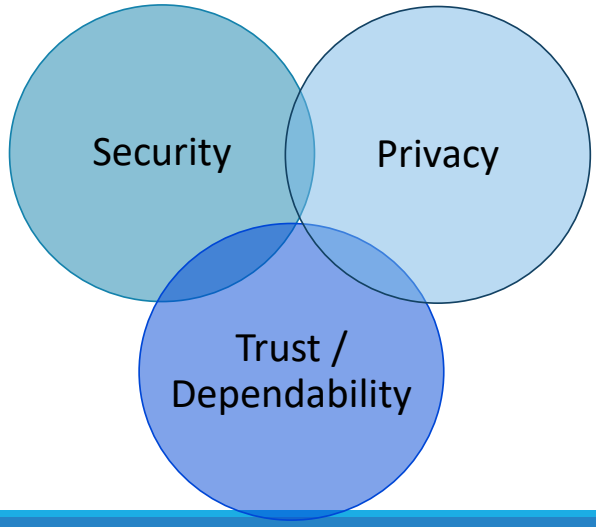
- parts of the plant failed – a blast furnace could not be shut down as normal

The anatomy of an attack

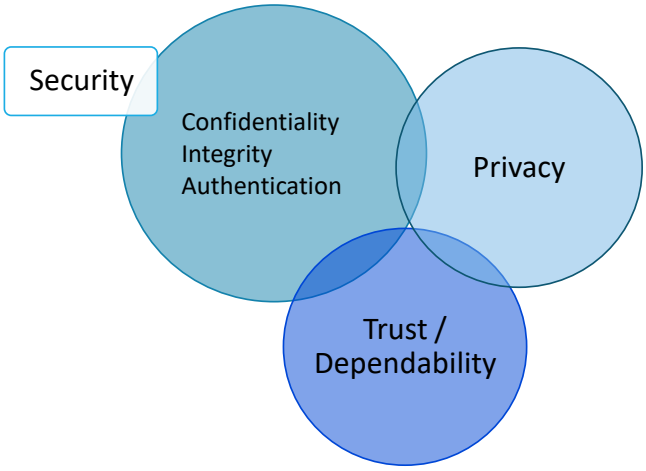
Video: https://www.youtube.com/watch?v=jK0oG-cDF4Y Script: https://drive.google.com/file/d/1uX8ALSBT86urgyQfdBjn5Wy1J5-nv6oD/view?usp=sharing

Ασφάλεια

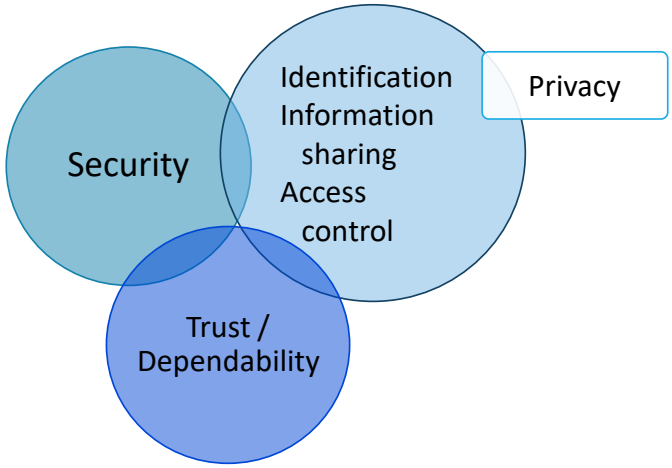
Pillars of robust IoT Ecosystem



Pillars of robust IoT Ecosystem



Pillars of robust IoT systems



Privacy concerns

Control data and flow

User awareness and valid consent

Properly propagated modified consents

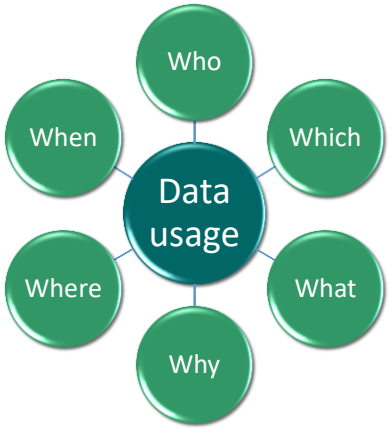
Context-aware access control

Sensor fusion

Data Aggregation

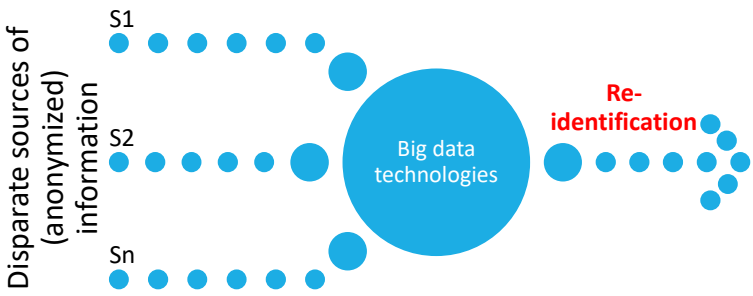
Process Repurposing

Data usage



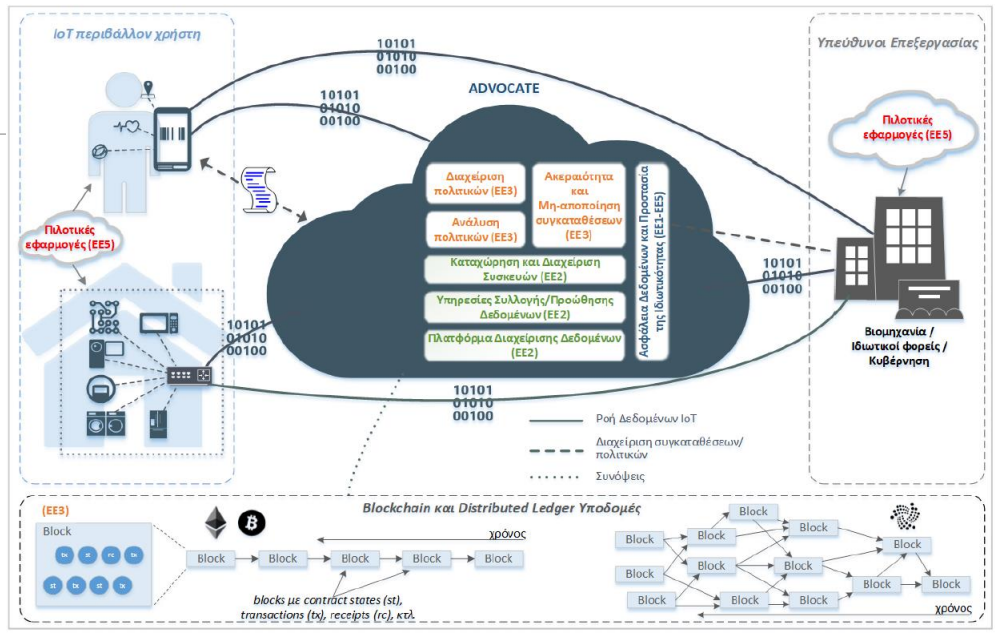
Privacy

IoT provides **access to (potentially) sensitive data**

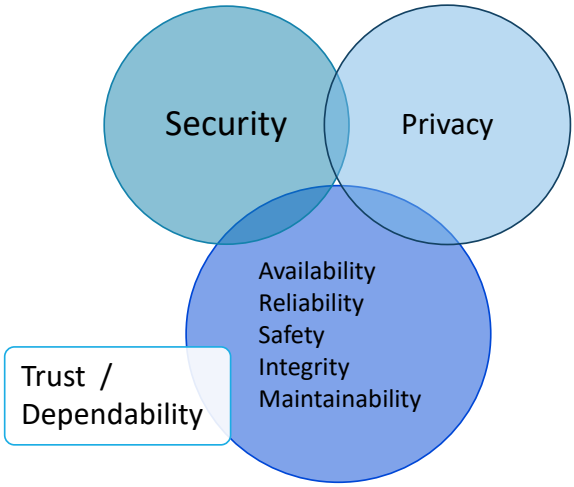


Privacy-centric nodes

ADVOCATE



Three pillars of robust IoT systems



Dependability

Security and privacy by design

- Secure deployment and configuration protection
- System wide assurance
- Resiliency
- Tamper-resistance
- Trusted Execution Environment
- Secure elements
- Software/Firmware updates

Network Security

- End-to-end security
- Intrusion Detection
- Traffic Obfuscation
- Secure routing
- Latency control

IoT Security Model

Detect anomalies
- Normal vs Abnormal
- Indicators of Compromise
- Zero-day exploits

Real-time monitoring (device, data, relationships)
- Billions of devices, services
- Analytics

Deploy countermeasures
Rapid response
Remediation strategy

Security metrics – a means for improvement

Identify appropriate ones

Examples

- Anonymity and location privacy
- Secure routing
- Network Latency

Functionality must be embedded in systems

ΣΑΣ ΕΥΧΑΡΙΣΤΩ!

ΚΩΝ/ΝΟΣ ΡΑΝΤΟΣ
krantos@cs.ihu.gr

Web Services and
Information Security Lab
wesis.cs.ihu.gr