MOBILE BIG DATA AND IOT-BASED APPLICATIONS

TENDENCIES IN

PANELISTS

- Ustijana Rechkoska-Shikoska,
  - *University for Information Science & Technology "St. Paul the Apostle", Republic of Macedonia*
- Michael Massoth,
  - *Hochschule Darmstadt - University of Applied Sciences, Germany*
- Subhasish Mazumdar,
  - *New Mexico Tech, USA [moderator]*

INTERNET & THINGS

- Internet connected things: fridge, vacuum cleaners, thermostats, ...
- Cyber-physical infrastructure
  - static things: sensors in buildings, roads, bridges, …

SENSORS ON HUMANS AND ROBOTS

- Humans with sensor-laden wearables:
  - clothing
  - glasses
  - hearing aids
  - body diagnostic sensors
- Robots with sensors: Roomba, …

SENSORS ON MOBILE DEVICES

- Cell 'phone' containing sensors for light, image, sound, acceleration, orientation, altitude, proximity, location, + Internet + LAN, …
- How many mobile devices have we connected? 25 billion ?
  - How many sensors?
- How many Internet-connected cars are we producing ?
  - How many sensors?

CHANGE

- Cyber-physical infrastructure
  - *static* things: in buildings, roads, bridges, …
  - *mobile* things: cars, humans, animals, robots, drones, …
- Consequence: exponentially larger scale of data from all the above connected *things*

CAN WE DESIGN

- an appropriately ***smart*** environment?
  - *nervous system* of all those sensors + a software *brain* ?
- a *smart* city?
  - a smart village?
- a *smart* enterprise? (*Business Intelligence)*
- a *smart* individualized network? Network of individuals with only their chosen peers?
- a *smart* school?

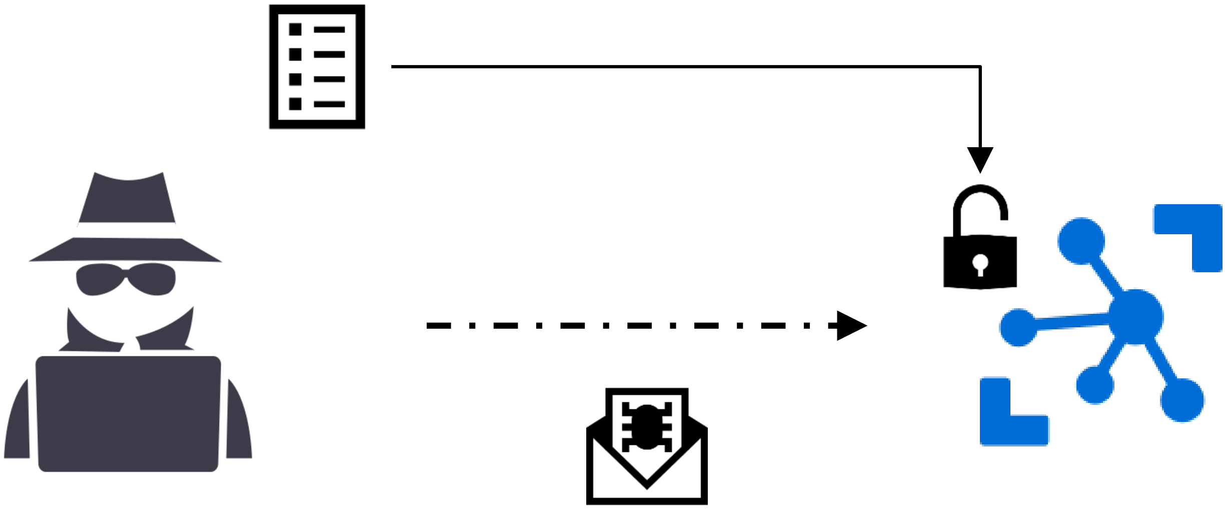
CHALLENGES

- Integrity, Privacy, (Economics?), Authentication, Confidentiality
- Weaknesses of mobile devices (energy, connectivity) and sensors
- Incorrect location
- Interoperability of sensor systems
- Is continuous sensing possible with mobile devices?
- Ethics: novel opportunities for harassment
- Is it a good idea? How should we proceed?

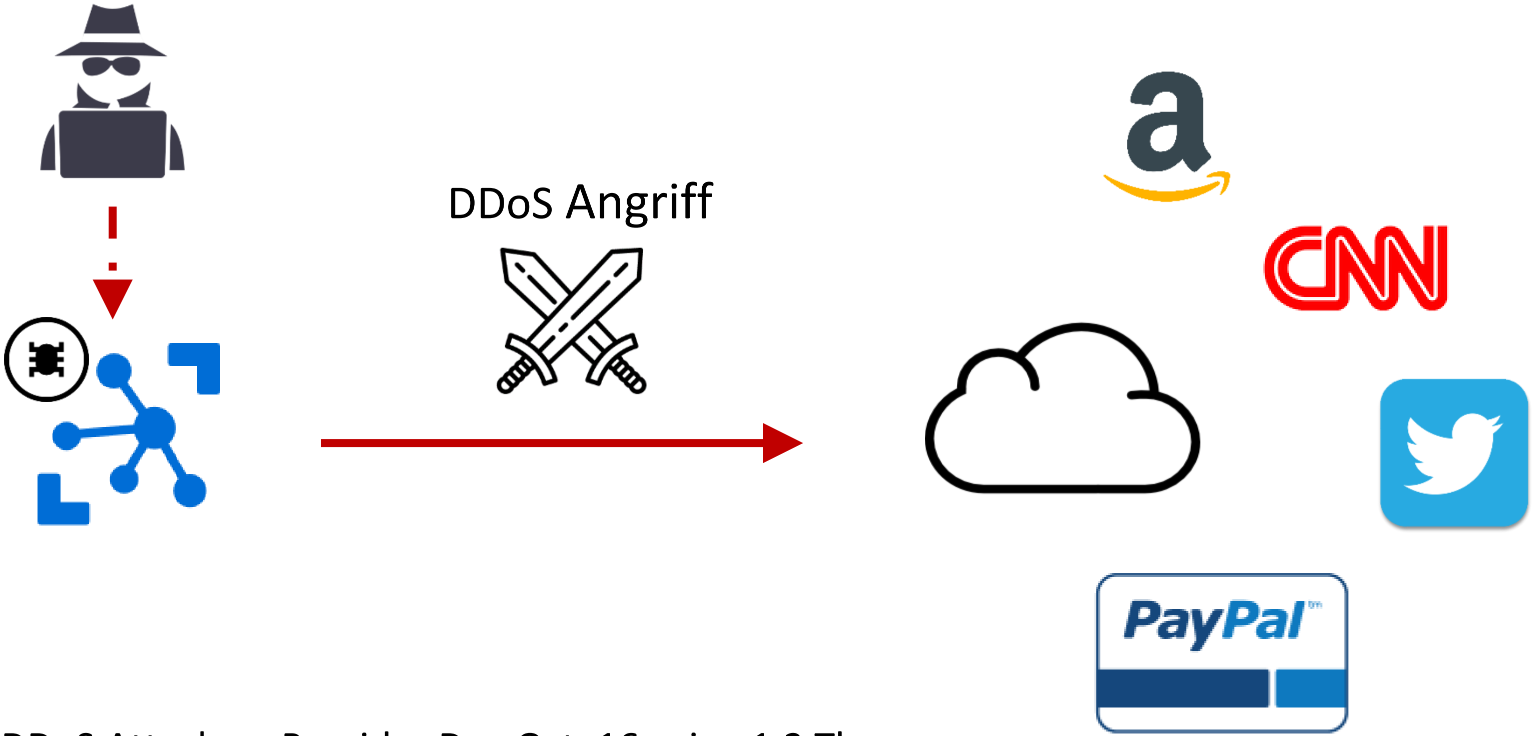
Cascading Three Step Approach for Anomaly Detection in Unsupervised Communication Meta Data of IP-based Internet of Things Devices

Andreas Schäfer (M.Sc.) and
Prof. Dr. Michael Massoth
University of Applied Science Darmstadt

Problem: Many IoT devices are easy to compromise

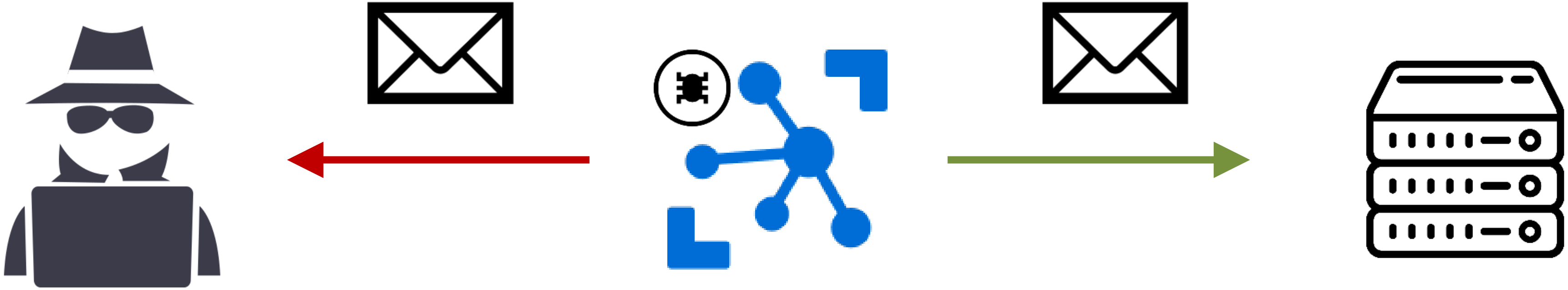


Attack vector: Compromised through botnet



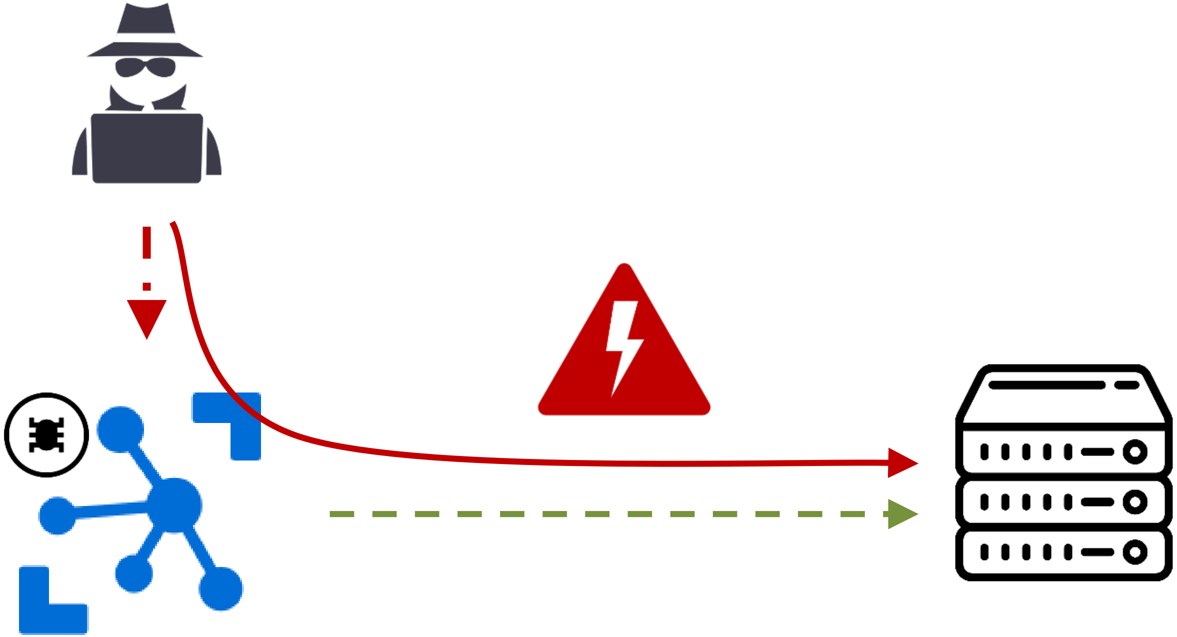
Example: DDoS Attack on Provider Dyn Oct. 16 using 1.2 Tbps

Attack vector: Espionage



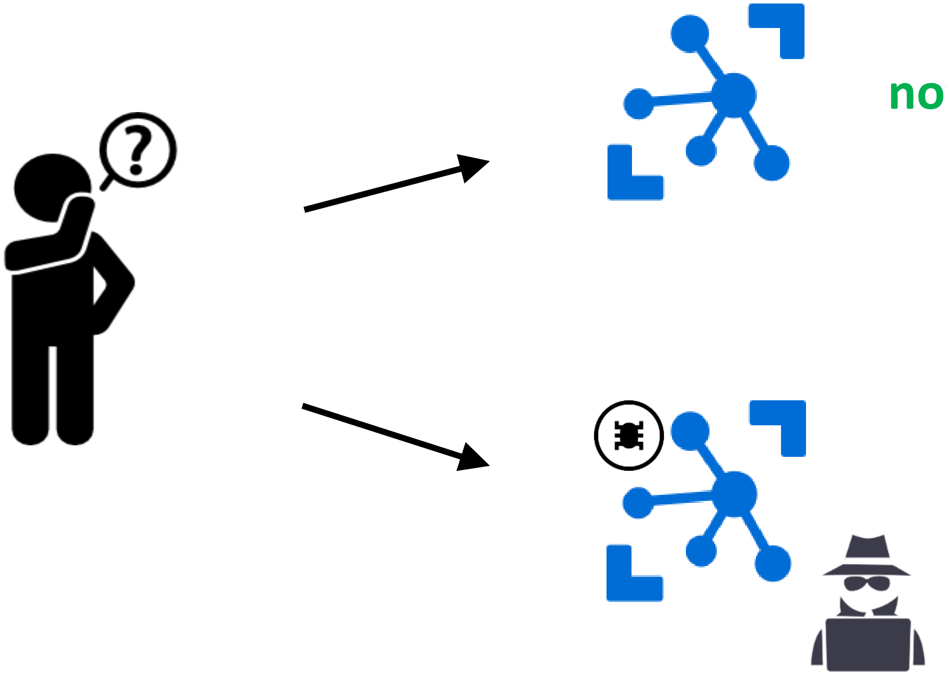
Tab data (camera stream, microphones)

Attack vector: Sabotage

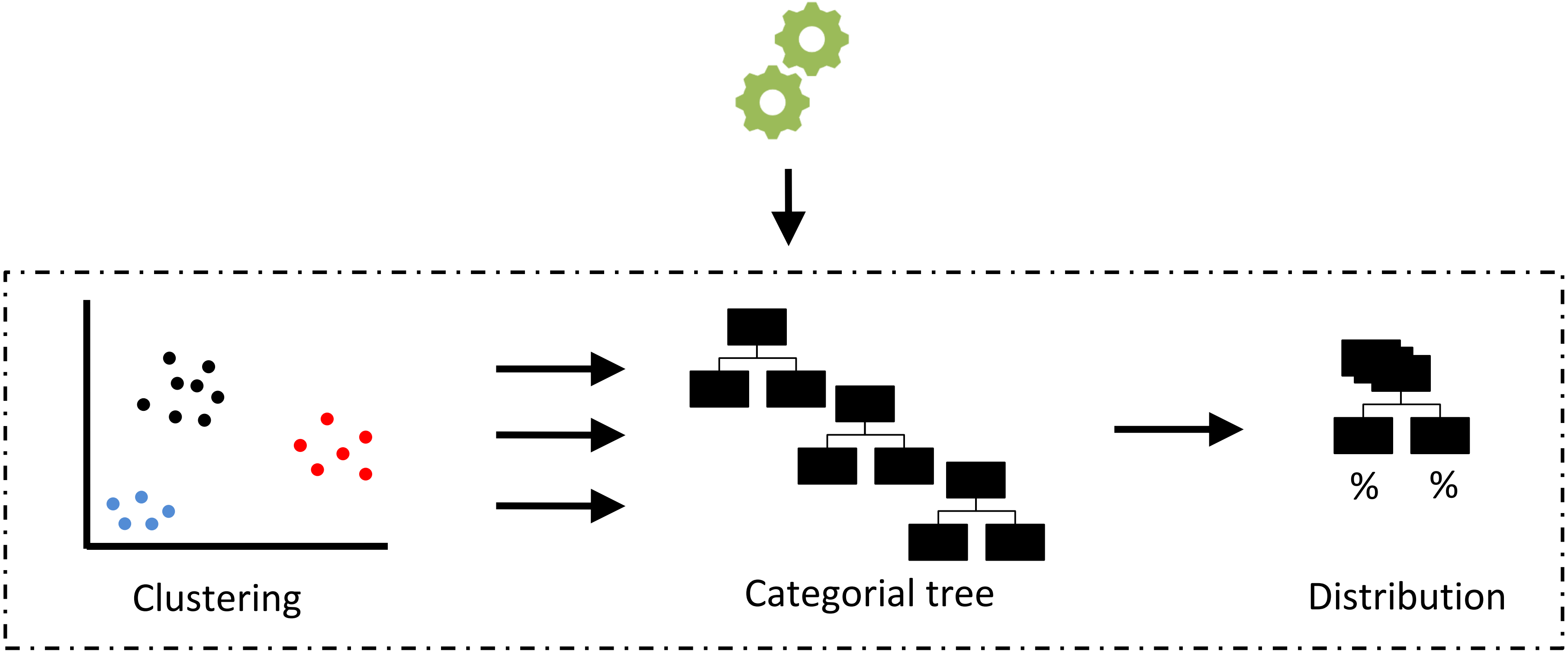


Sabotage on infastructure (Utility companies)
or using the IoT device as jumpstation

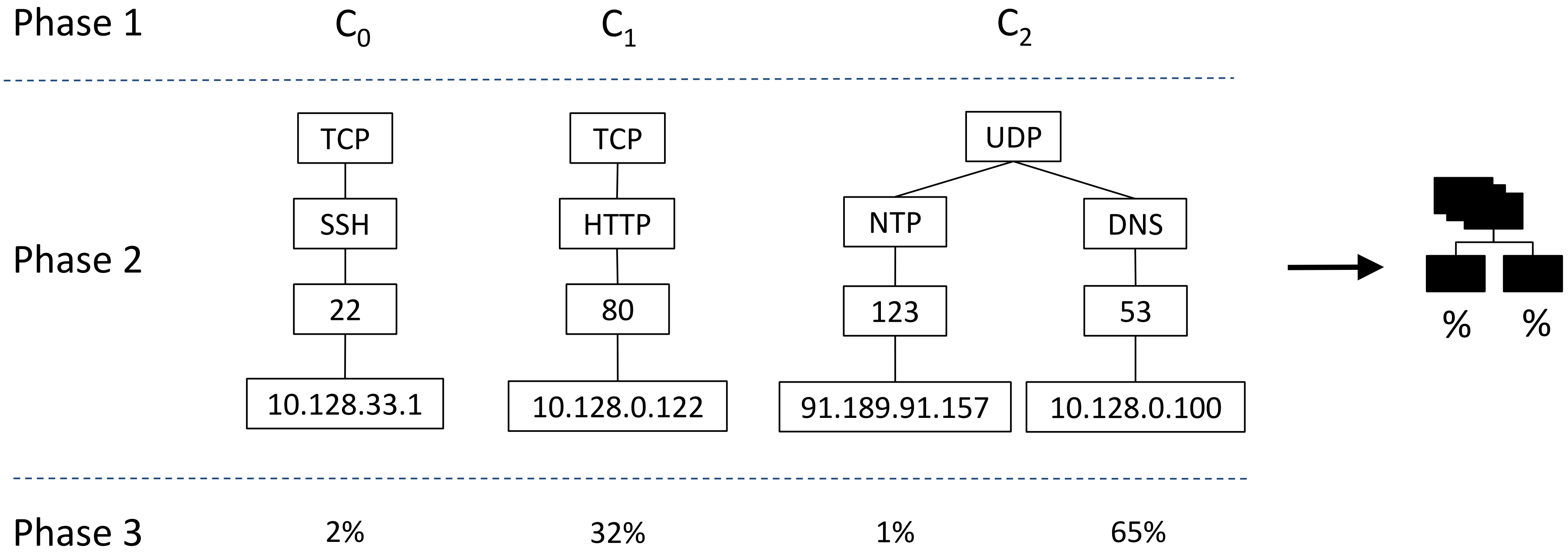
Problem: How to identify a compromised IoT device



Analyzing connection metadata



Final communication model



Phase 1: C_0 C_1 C_2

Phase 2:

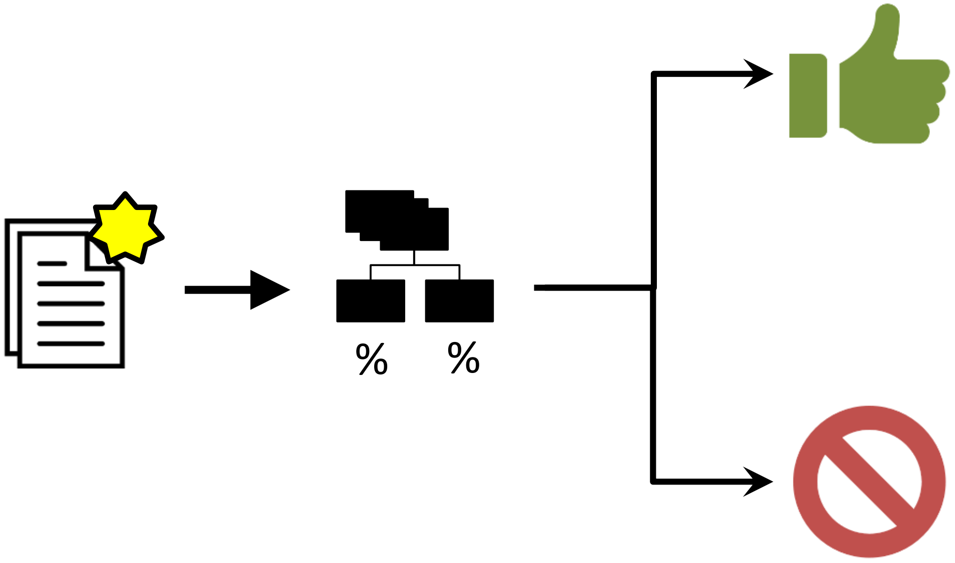
C_0: TCP – SSH – 22 – 10.128.33.1

C_1: TCP – HTTP – 80 – 10.128.0.122

C_2: UDP – NTP – 123 – 91.189.91.157; UDP – DNS – 53 – 10.128.0.100

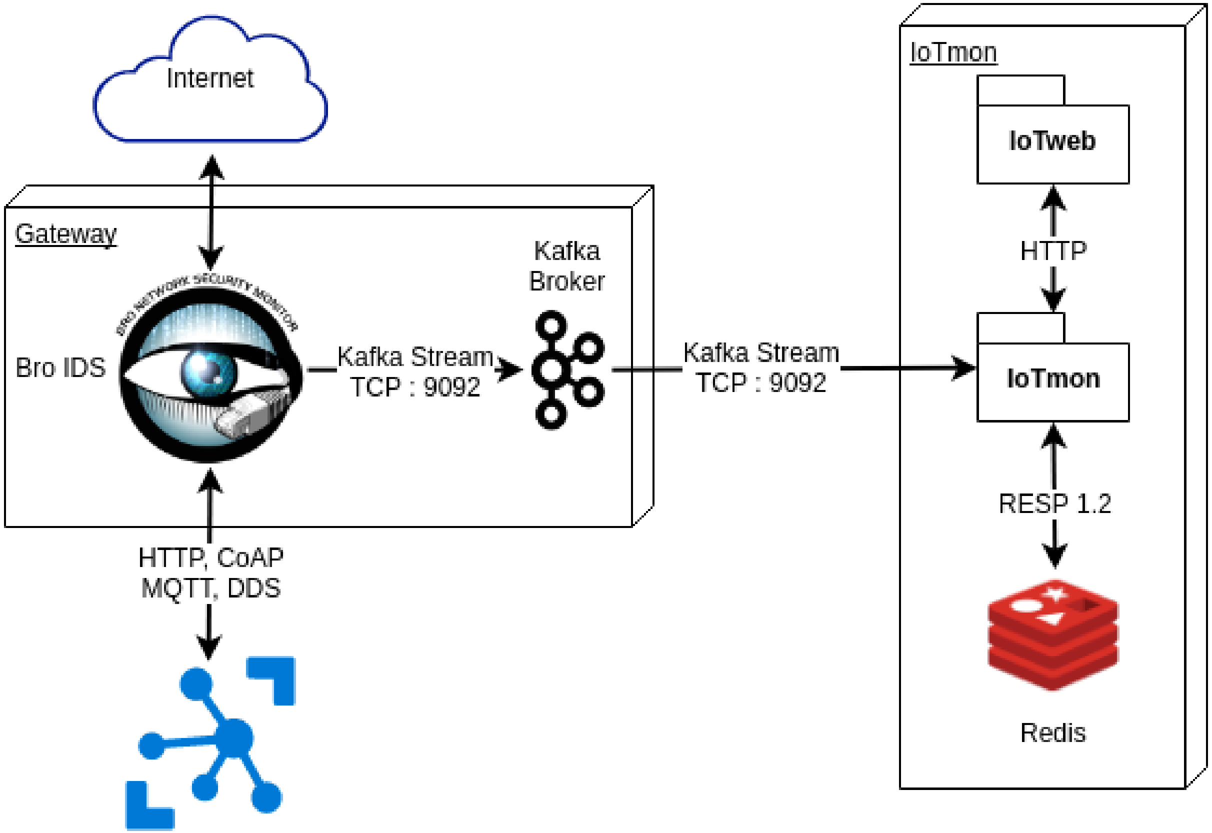
Phase 3: 2% 32% 1% 65%

Categorizing connection metadata



Step 3
Apply the communication model to **new connection metadata** and monitor the distribution onto the categories.

Implemented as proof of concept



IARIA International Academy, Research, and Industry Association

DataSys 2018
IARIA, AICT 2018

Tendencies Mobile Big Data & IoT-based Applications

Professor Ustijana Rechkoska-Shikoska, Ph.D.

Dean of Faculty for Computer Science & Engineering at

University for Information Science & Technology “St. Paul the Apostle”, Ohrid, Republic of Macedonia

USTIJANA RECHKOSKA-SHIKOSKA

ustijana@gmail.com;   ustijana.r.shikoska@uist.edu.mk ;

uist.edu.mk

Ph.D. in Computer Science and Engineering

University for Information Science and Technology “St. Paul the Apostle” - *Vice-Rector for Academic Affairs and International Cooperation*

Associate Professor in Computer Science and Informatics

Dean of Faculty for Computer Science & Engineering

Teaching & Research: Computer Engineering, Informatics, Programming, Algorithms & Data Structures, Database Systems, Wireless Sensor Networks, Cyber Security, Offensive Security, Electrical Engineering, IT in Power Engineering, Mobile computing, Image Processing, Discrete Mathematics, Digital Signal Processing

Ustijana R.S. is participating International Conferences, Congresses, International Journals with numerous publications (over 95), authoring, co-authoring.

She is also working & participating International research projects, publication of professional book, translating professional ICT books, Participating in Program & Organization Committees of International Conferences, Journals, being Publicity Chair, Reviewer, Moderator, Panelist for years.

She is Mentoring lots of BSc Graduation Thesis’ and MSc Graduation Thesis’ with her students in the ICT field

Coordinator of an International Practicum for Cyber Security and an International Observatory for Cyber Security with Norwich University, Vermont – USA.

IEEE Certificates

IARIA AICT Certificates

Certificate for Cyber Security, Norwich University, Vermont, USA,

Golden Certificate for Original Software for an active rectifier - Makinova,

Golden Certificate of an Appreciation PCO

EURO CHRIE Certificate,

IAEA Certificate,

IJEOE Editorial of a Journal

Official Reviewer of International Scientific and Research Projects by the Ministry of Education and Science of the Republic of Macedonia.

She is an active member of Lions International - LD 132, as well the Lions Club Ohrid Desareti, where she works with great enthusiasm on implementing creative ICT solutions.

Internet of Things (IoT) & Big Data, IoT analytics, IoT Security

- Integration of IoT, Cloud, Edge, Big Data, and M2M tools and technologies provide great opportunity for better services to communities for a smarter living

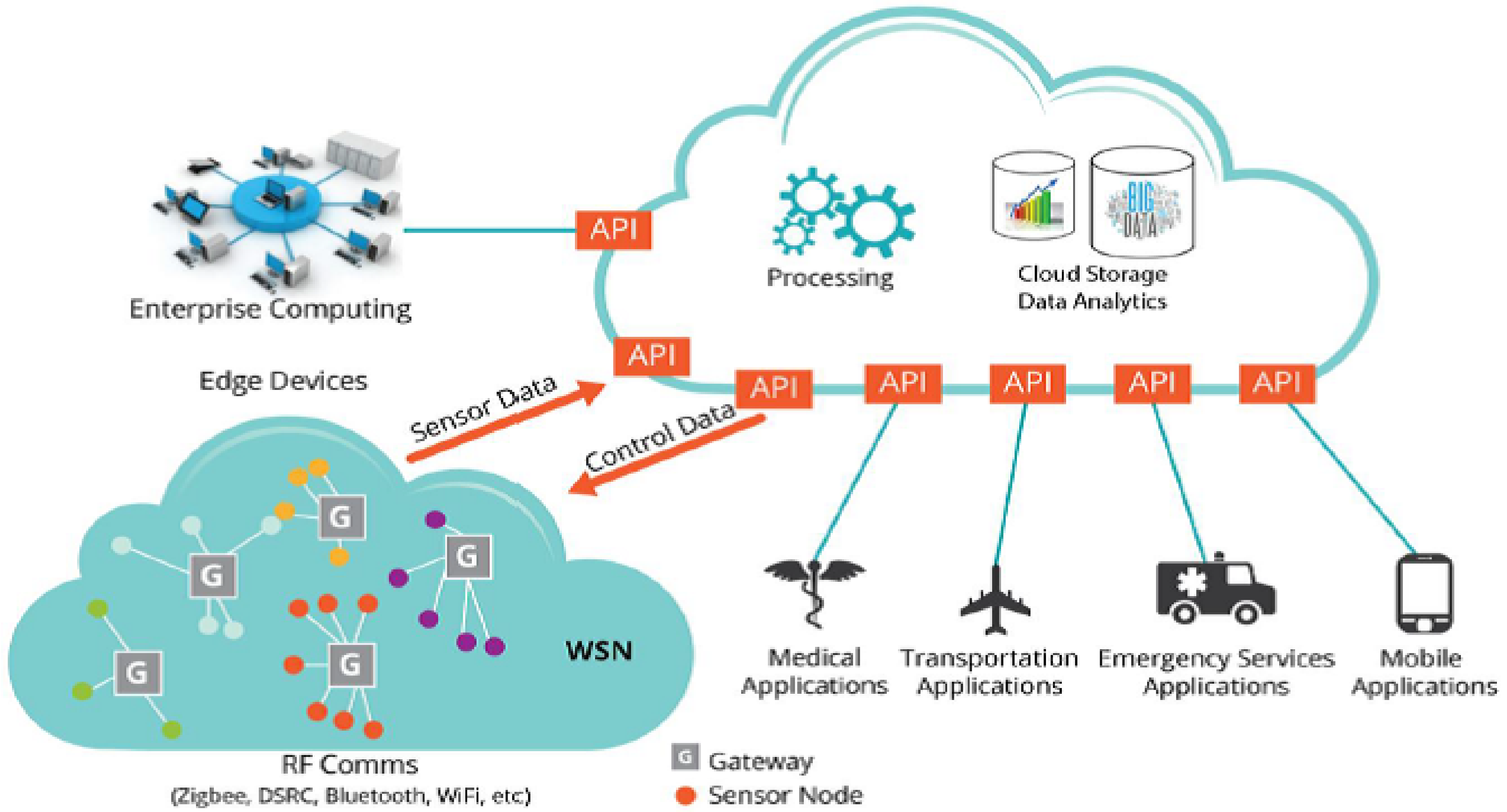
- IoT data analytics

- IoT Security

Internet of Things (IoT)

- IoT is a network of physical objects that is connected to and accessed through the Internet - connected objects contain embedded technology, such as sensors, that enable objects to sense and communicate.
- IoT changes the way decisions are made, the ones who make them, and the efficiency of making them.
- Business forecasts – by 2019 the Internet will connect 35 billion “things” like vending machines, cars, robots, thermostats, watches, servers and heavy machinery.
- By 2020, it is expected that over 40,000 exabytes of data will be generated through sensors built into physical objects connected to the Internet – that’s over 90 % of the data being generated today worldwide

The Internet of Things



IoT & Big Data

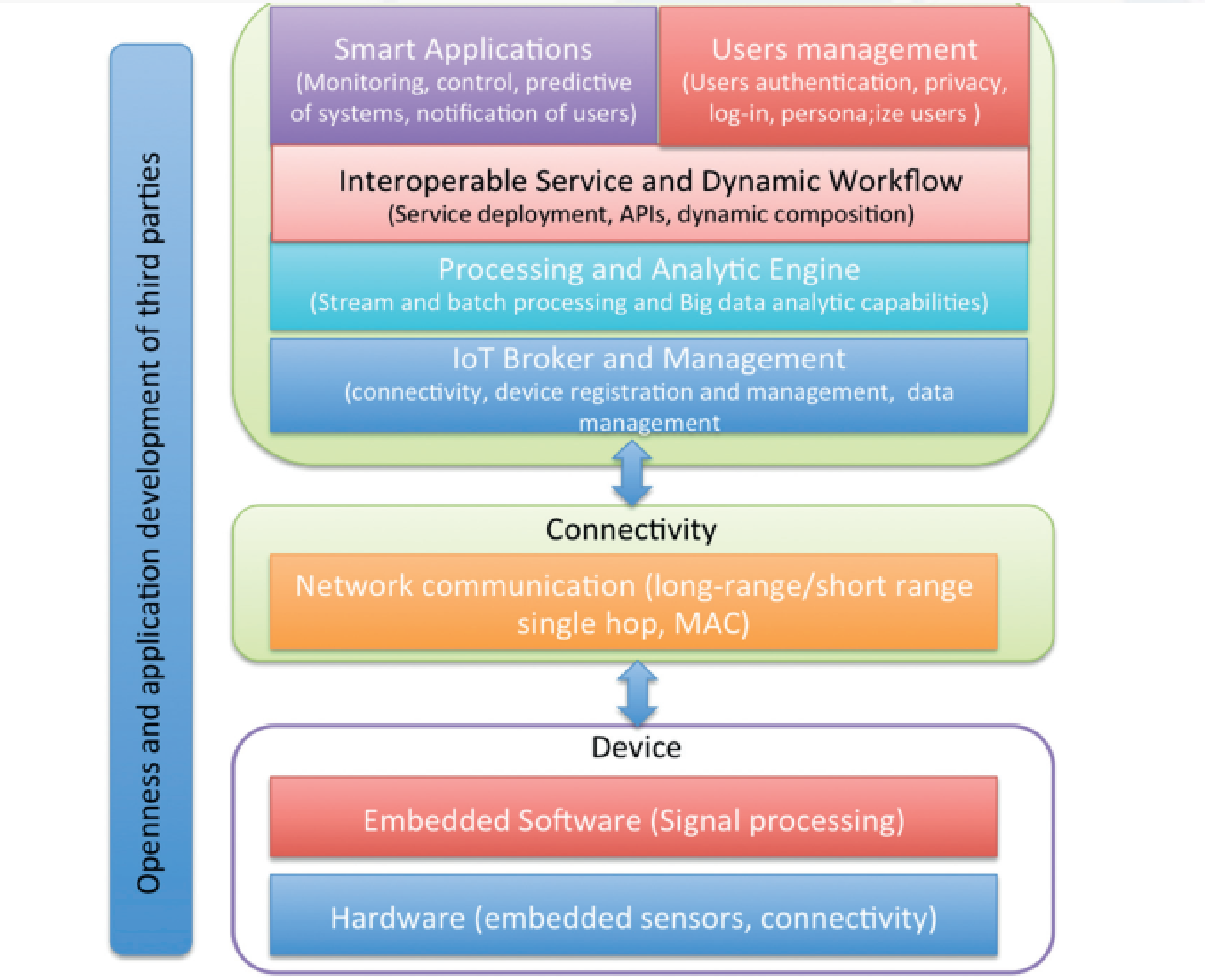
- The rise of future Internet technologies, including cloud computing and BigData analytics, enables the wider deployment and use of sophisticated IoT analytics applications.
- The integration of IoT data streams within cloud computing infrastructures enables IoT analytics applications to benefit from the capacity, performance and scalability of cloud computing infrastructures.
- IoT analytics applications are also integrated with edge computing infrastructures, which decentralize processing of IoT data streams at the very edge of the network, transferring only selected IoT data from the edge devices to the cloud.

INTERNET
OF THINGS
31
SALE

IoT, Cloud & BigData Integration for IoT analytics

- The volume and quality of the data generated by IoT devices is very different from the traditional transaction-oriented business data
- Coming from millions of sensors and sensor-enabled devices, IoT data is more dynamic, heterogeneous, imperfect, unprocessed, unstructured and real-time than typical business data
- It demands more sophisticated, IoT-specific analytics to make it useful.

Architecture of IoT and BigData platform



Openness and application development of third parties

Smart Applications
(Monitoring, control, predictive of systems, notification of users)

Users management
(Users authentication, privacy, log-in, persona;ize users)

Interoperable Service and Dynamic Workflow
(Service deployment, APIs, dynamic composition)

Processing and Analytic Engine
(Stream and batch processing and Big data analytic capabilities)

IoT Broker and Management
(connectivity, device registration and management, data management

Connectivity

Network communication (long-range/short range single hop, MAC)

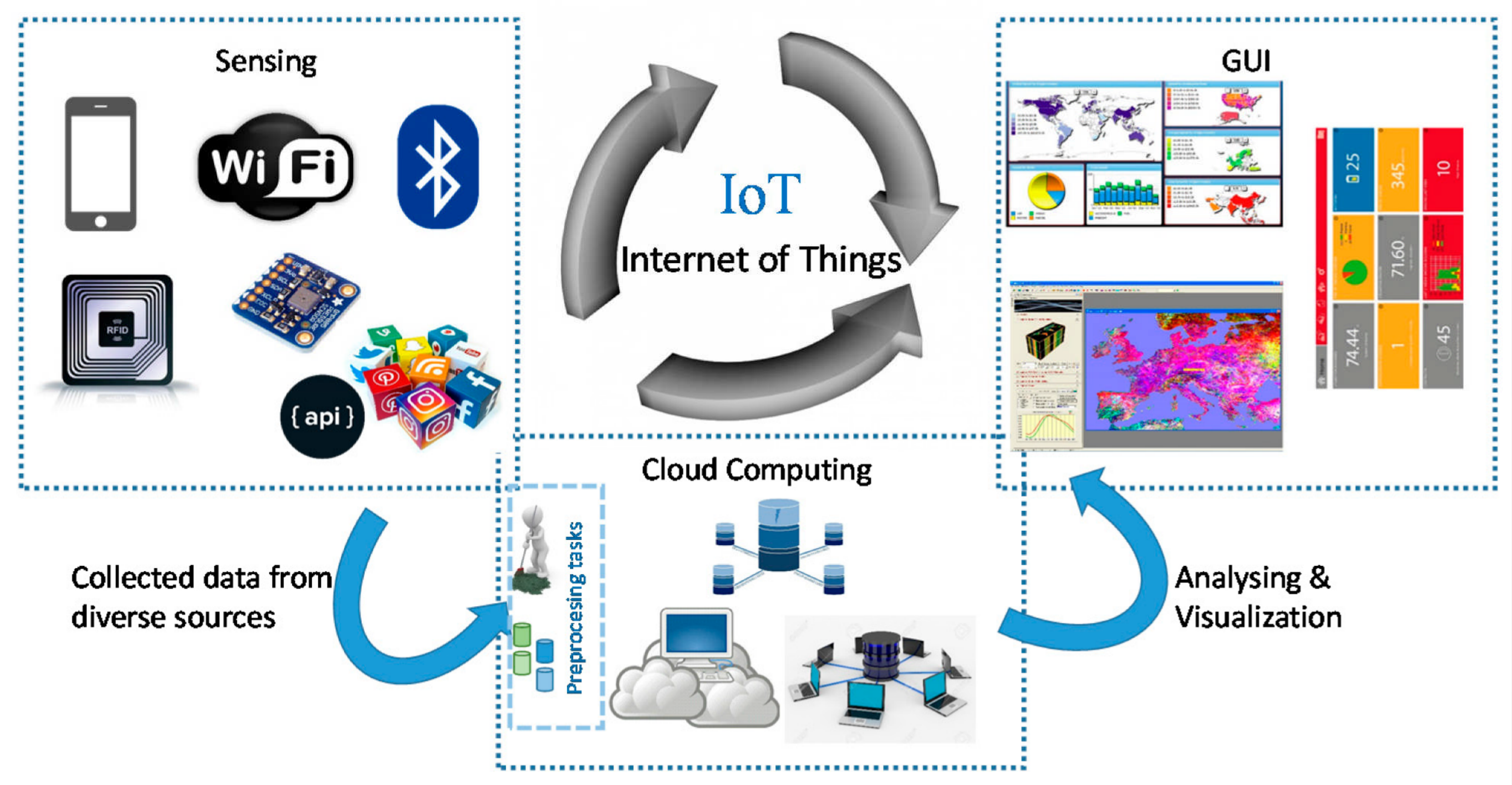
Device

Embedded Software (Signal processing)

Hardware (embedded sensors, connectivity)

IoT, M2M, Cloud Computing

- The development of the Internet of Things (IoT) paradigm has advanced the research on Machine to Machine (M2M) communications and enabled tele-monitoring architectures for E-many applications
- There is a need for converging current decentralized cloud systems, general software for processing Big Data and IoT systems
- Important is Analyzing the existing components and methods of securely integrating big data processing with cloud M2M systems and proposing a converged architectures in order to develop efficient app.



Sensing

IoT

Internet of Things

GUI

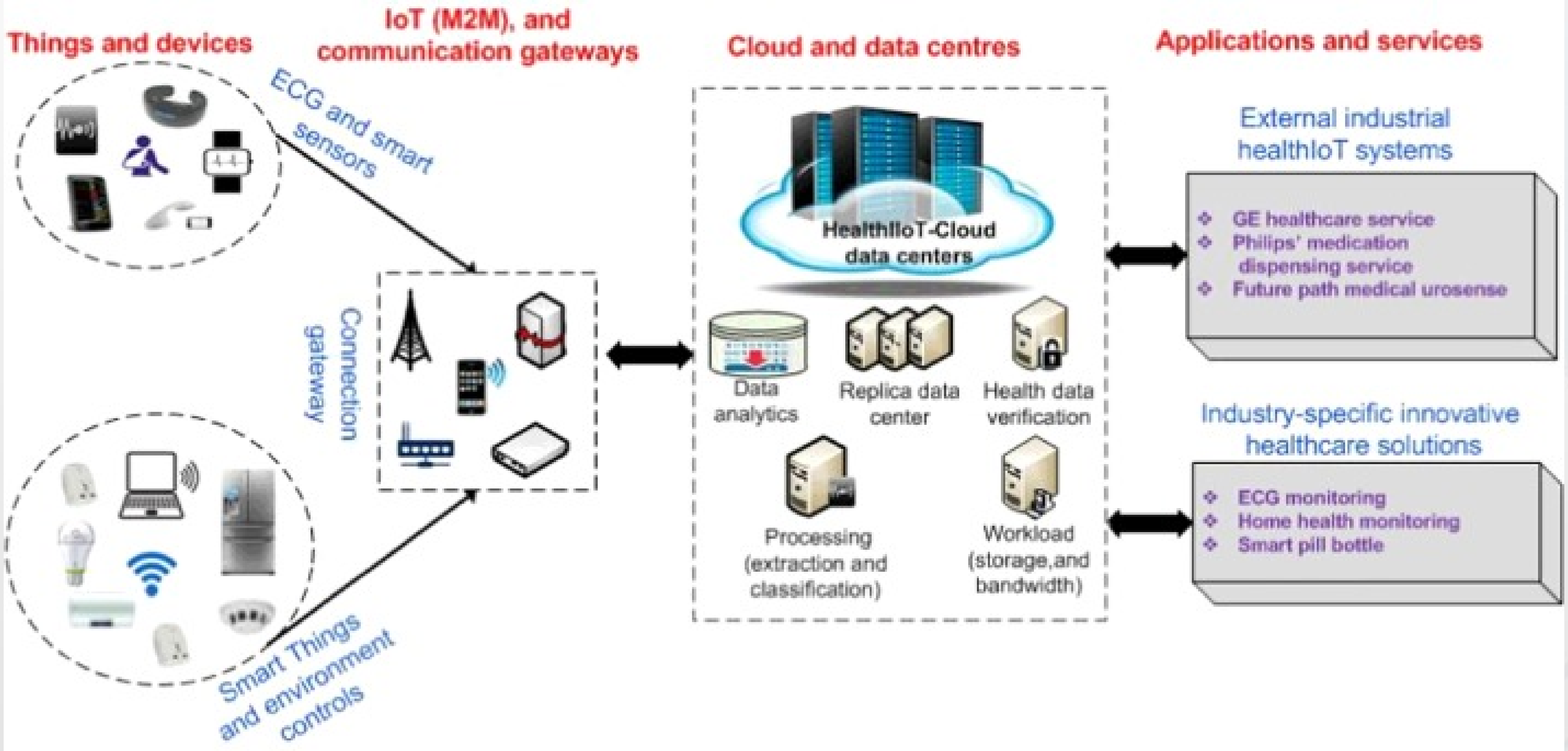
Collected data from diverse sources

Cloud Computing

Preprocesing tasks

Analysing & Visualization

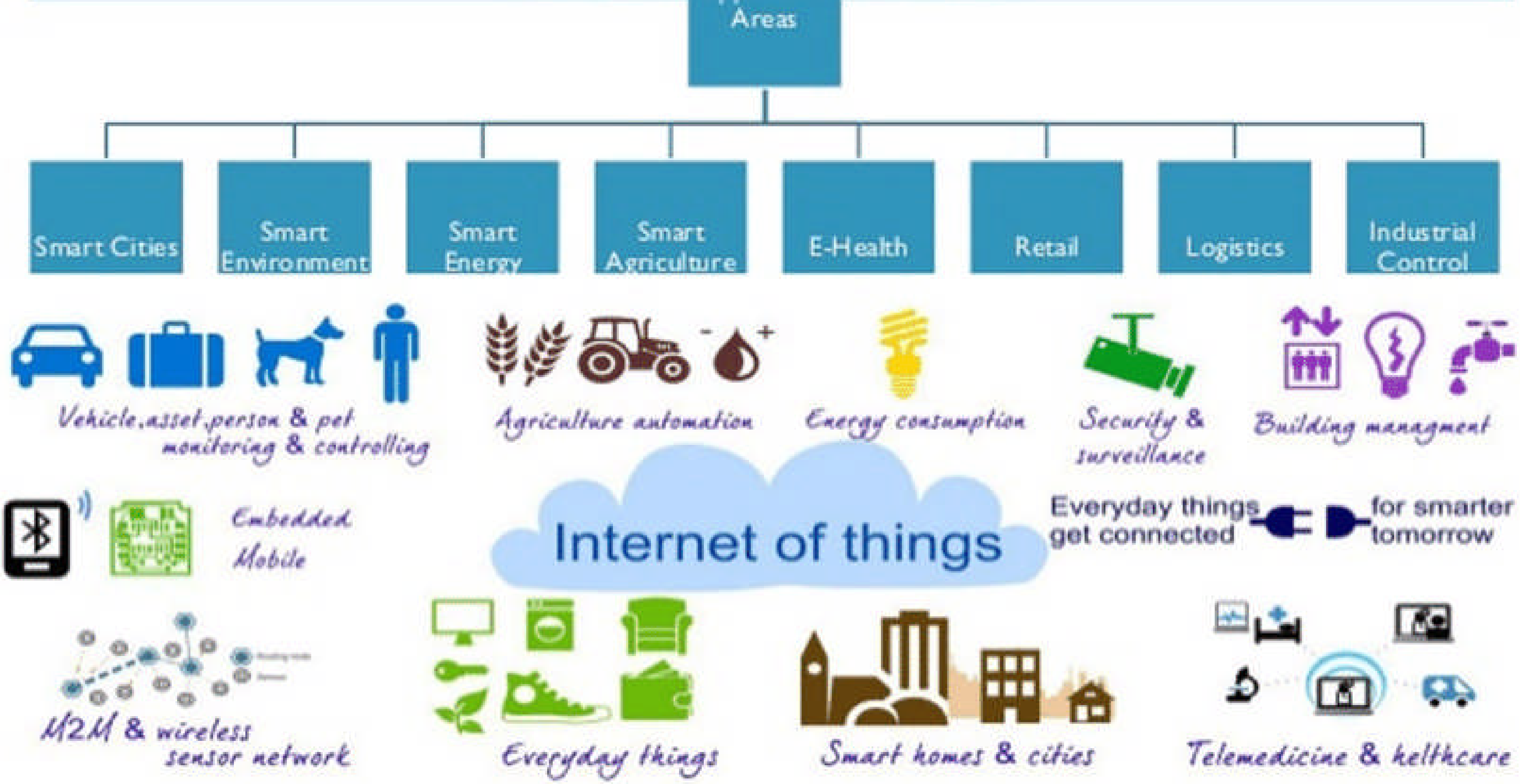
IoT, M2M, Cloud Computing, Applications & Services


Things and devices
IoT (M2M), and communication gateways
Cloud and data centres
Applications and services
ECG and smart sensors
Connection gateway
Smart Things and environment controls
HealthIoT-Cloud data centers
Data analytics
Replica data center
Health data verification
Processing (extraction and classification)
Workload (storage,and bandwidth)
External industrial healthIoT systems
GE healthcare service
Philips' medication dispensing service
Future path medical urosense
Industry-specific innovative healthcare solutions
ECG monitoring
Home health monitoring
Smart pill bottle

Integration of Cloud computing and Internet of Things

- Cloud computing and Internet of Things (IoT) are two very different technologies that are both already part of everyday’s life.
- Novel paradigms where Cloud and IoT are merged together are enablers of a large number of application scenarios.
- integration of Cloud and IoT - new CloudIoT paradigm, which involves completely new applications, challenges, and research issues.
- Thanks to the adoption of the CloudIoT paradigm a number of applications are playing a leading role the Future Internet.

Current Scenario (Trends)



Areas

Smart Cities

Smart Environment

Smart Energy

Smart Agriculture

E-Health

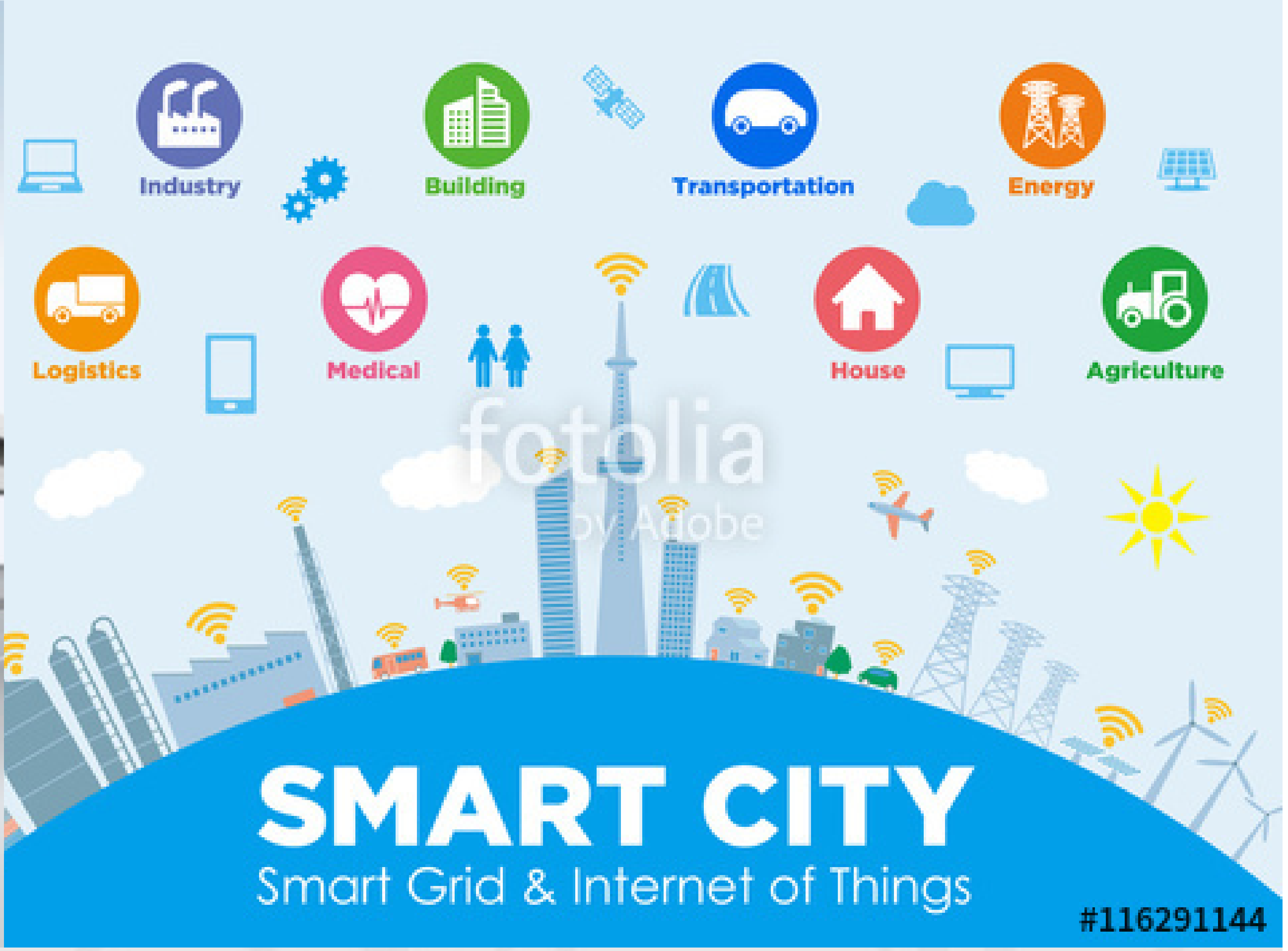
Retail

Logistics

Industrial Control

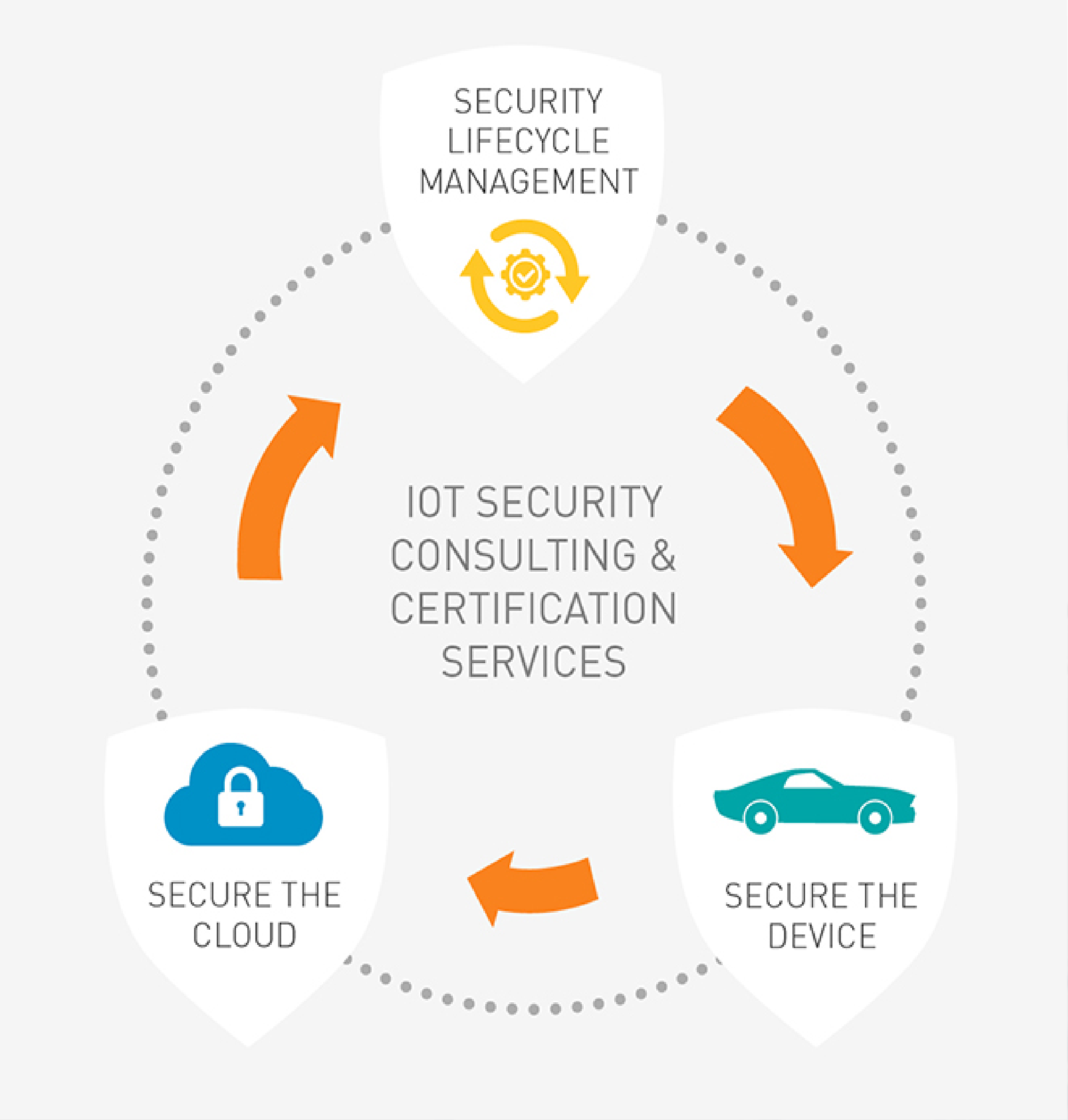
- Smart City represents one of the most promising and prominent Internet of Things (IoT) applications
- Thanks to Internet of Things (IoT) solutions, Smart cities aren’t just a dream of the future, many are already active and expanding rapidly. Municipal governments are leveraging cellular and Low Power Wide Area (LPWAN) wireless technologies to connect and improve infrastructure, efficiency, convenience and quality of life for residents and visitors.
- Today, 54% of people worldwide live in cities, a proportion that’s expected to reach 66% by 2050. Combined with the overall population growth, urbanization will add another 2.5 billion people to cities over the next three decades. Environmental, social and economic sustainability must match this rapid expansion, smart city technology is paramount to success and meeting these goals.

IoT, Big Data, Smart Cities



- Secure wireless connectivity and IoT technology is transforming traditional elements of city life - like streetlights - into next generation intelligent lighting platforms with expanded capabilities.
- This includes integrating solar power and connecting to a cloud-based central control system that connects to others assets in the ecosystem.
- Connected cameras, intelligent road systems and public safety monitoring systems can provided an added layer of protection and emergency support to aide citizens when needed.
- Protecting smart cities themselves from vulnerabilities?
- How can we defend against hacking, cyber-attacks and data theft?
- In cities where multiple participants are sharing information, how do we trust that participants are who they say they are? And how do we know the data they report is true and accurate? The answer lies in physical data vaults and strong authentication and ID management solutions.

- Availability: Access to data & the way of collecting it, sharing it is critical, and security solutions must avoid negative effects on availability.
- Integrity: Smart cities depend on reliable and accurate data. Measures must be taken to ensure that data is accurate and free from manipulation.
- Confidentiality: Some of the data collected, stored and analyzed will include sensitive details about consumers themselves. Steps must be taken to prevent unauthorized disclosure of sensitive information.
- Accountability: Users of a system must be responsible for their actions. Their interactions with sensitive systems should be logged and associated with a specific user. These logs should be difficult to forge and have strong integrity protection.
- To achieve these security core objectives, strong authentication and ID management solutions need to be integrated into the ecosystem to ensure that data is shared only with authorized parties.
- The solutions also protect backend systems from intrusion and hacking.


SECURITY LIFECYCLE MANAGEMENT
IOT SECURITY CONSULTING & CERTIFICATION SERVICES
SECURE THE CLOUD
SECURE THE DEVICE

Internet of Things (IoT) Security

- Denial of Service (DDoS) attacks on providers of critical Domain Name System (DNS) services to companies like Twitter, Netflix, CNN etc. are to be discuss about.
- There are tools for hacking IoT devices, such as Samsung SmartTVs, to remotely record conversations in hotel or conference rooms.
- Privacy is also a concern with IoT devices.
- Children's Online Privacy Protection Rule (COPPA) – very important to be considered
- In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.

IoT Security

- Building security into a device can be costly, slow down development, and sometimes stand in the way of a device functioning at its ideal speed and capacity.
- The devices are directly exposed to the Web because of poor network segmentation. It can just open up a backdoor to let criminals in.
- Congress introduced the Internet of Things Cybersecurity Improvement Act, which seeks to require that any devices sold to the US government be patchable, not have any known security vulnerabilities, and allow users to change their default passwords.
- There are solutions purpose-built for securing IoT devices and networks, but there’s a long way to go before standards are established.

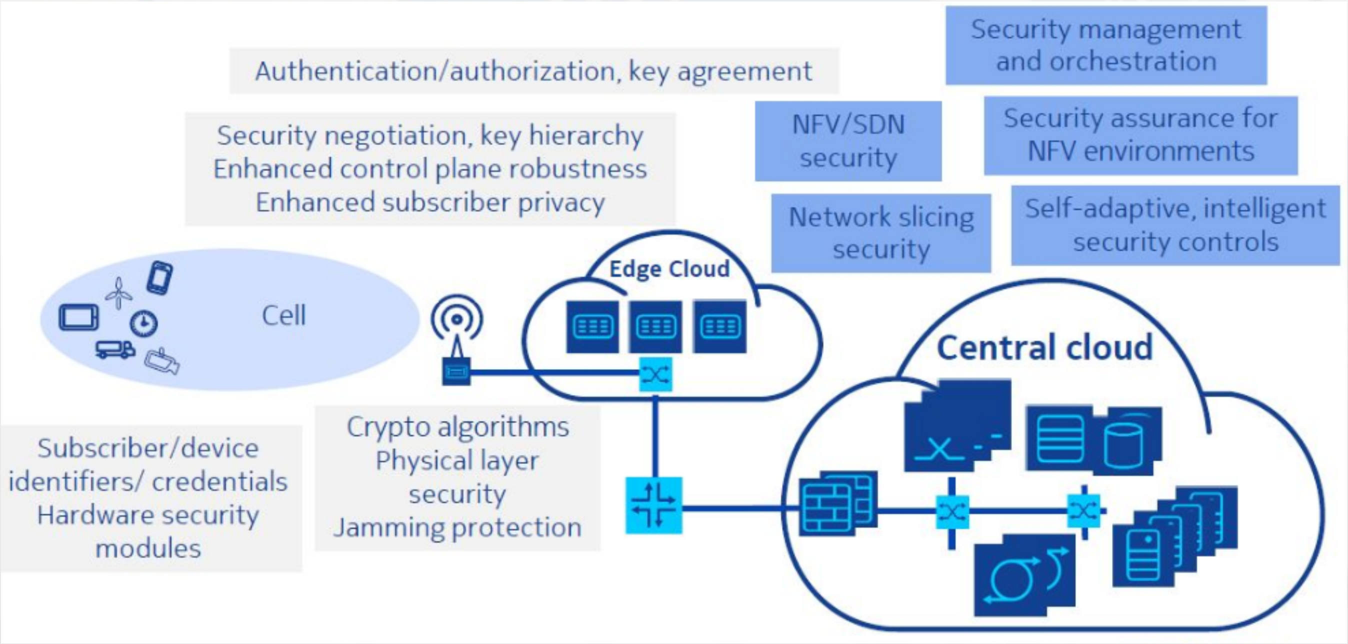
IoT Security Services

- Designing a new IoT solution or evaluating an existing connected devices, helps identify, analyze and mitigate risk by designing end-to-end security architectures that safeguard assets and data.
- Some solutions provide better security thorough penetration testing of devices, systems including reverse engineering, physical and logical manipulation.
- Modern solutions enclose data encryption and cloud security provide a secure way for enterprises and cloud assets, keeping the full potential of the cloud environment, ensuring their intellectual property, too.

IoT security to protect data

- IoT Security is key to gain and retain consumer trust on privacy and to fullfill the full potential of the IoT promise.
- There are leading edge IoT security solutions and services to protect connected objects, from the design and manufacturing stages, through their entire lifecycle, guarding data against attacks.
- To protect the devices - Evaluate if the devices into the network really need to be smart. It’s better to treat IoT tech as hostile by default instead of trusting it with someone’s personal info, or allowing it access the network.
- To Segment a network - IoT devices at homes or businesses should be separated from networks that contain sensitive information.

- A difficult password to crack, and storing it in a password manager.
- A lot of devices are built on different platforms, different operating systems, and use different programming languages.
- Developing malware attacks for every one of those devices is not so real. If businesses want to make IoT a profitable model, security will increase out of necessity.



Authentication/authorization, key agreement

Security negotiation, key hierarchy
Enhanced control plane robustness
Enhanced subscriber privacy

Subscriber/device identifiers/ credentials
Hardware security modules

Crypto algorithms
Physical layer security
Jamming protection

NFV/SDN security

Network slicing security

Security management and orchestration

Security assurance for NFV environments

Self-adaptive, intelligent security controls

- M2M-optimised SIM and embedded SIM: resistant environments represent a strong authentication token for cellular applications, they encrypt and authenticate data and securely identify devices on global mobile networks.
- Cinterion Secure Element: the hardware component, embedded in devices, provides the maximum level of protection at the edge, for the most critical IoT applications. Its tamper-proof environment works as a ´safe´ for secure storage of encryption keys and security credentials.
- SafeNet Hardware Security Modules - safeguarding the most sensitive IoT devices´ keys which are centrally stored to protect the cryptographic infrastructure of some of the most security-conscious organizations in the world.
- Trusted Key Manager: the new solution authenticates IoT devices and secures data exchanges on both cellular and non-cellular networks, preventing unauthorized devices and IoT players from joining the network. It enables strong digital security through a simple and trustful mechanism of secure key provisioning, remote credential activation and lifecycle management.
- IP Protection: protection of the intellectual property of embedded software applications and data files.

- It is challenging to consider the **security and privacy** issues in IoT analytics for **smart cities**.
- With the support of edge analytics, the IoT analytics platform is now geographically deployed with the extension further down to the edges, like mobile base stations, IoT gateways, and even some endpoint devices as well.
- It is becoming more challenging to secure the platform and IoT data.

- Some intrusion detection might be needed to detect attacks and potential threats in real time – Privacy in IoT is still great challenge, but will be an essential point for IoT adoption.

Safer IoT

- City authorities should also become aware that IoT solutions will increase dramatically the demand for broadband connections at the transition from connecting people to connecting things.
- Urban IoT platforms: Future Internet technology is a driver for new infrastructure, platforms and solutions for smart cities.
- Multimodal sensors, extended networks of sensors over all city infrastructures, embedded user interfaces, mobile devices, and M2M communication will enable location-aware services, real-time response, and eventually forecasting.
- The recommendation is for integrated solutions involving communities of citizens, IoT platforms, and services targeted at the problems of different city districts and utilities.

IARIA

International Academy, Research, and Industry Association

Thank you for your attention!

Многу Ви Блгодарам!

Muchas gracias por su atención!

Merci Beaucoup!

Grazie Mille!

Vielen Dank!