Security and Energy Trade-Offs in Smart City Cyber-Physical Systems

IEEE Smart Cities Conference 2019 Keynote

Casablanca, 16 Oct 2019

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu

More Info: http://www.smohanty.org

Talk - Outline

- Smart City Drivers
- Smart City Components as Cyber-Physical Systems (CPS)
- Smart City Technologies
- Challenges for Smart Cities Design
- Open Questions on Technologies relevant to Smart Cities
- Conclusions and Future Directions

Smart City Drivers

Population Trend – Urban Migration

- 2025: 60% of world population will be urban
- 2050: 70% of world population will be urban

Source: http://www.urbangateway.org

Issues Challenging Sustainability

- Pollution

- Water crisis

- Energy crisis

- Traffic

The Problem

- Uncontrolled growth of urban population
- Limited natural and man-made resources

Source: https://humanitycollege.org

The Solution – Smart Cities

- Smart Cities: For effective management of limited resource to serve largest possible population to improve:
  - Livability
  - Workability
  - Sustainability

At Different Levels:
- Smart Village
- Smart State
- Smart Country

Smart Cities - Formal Definition

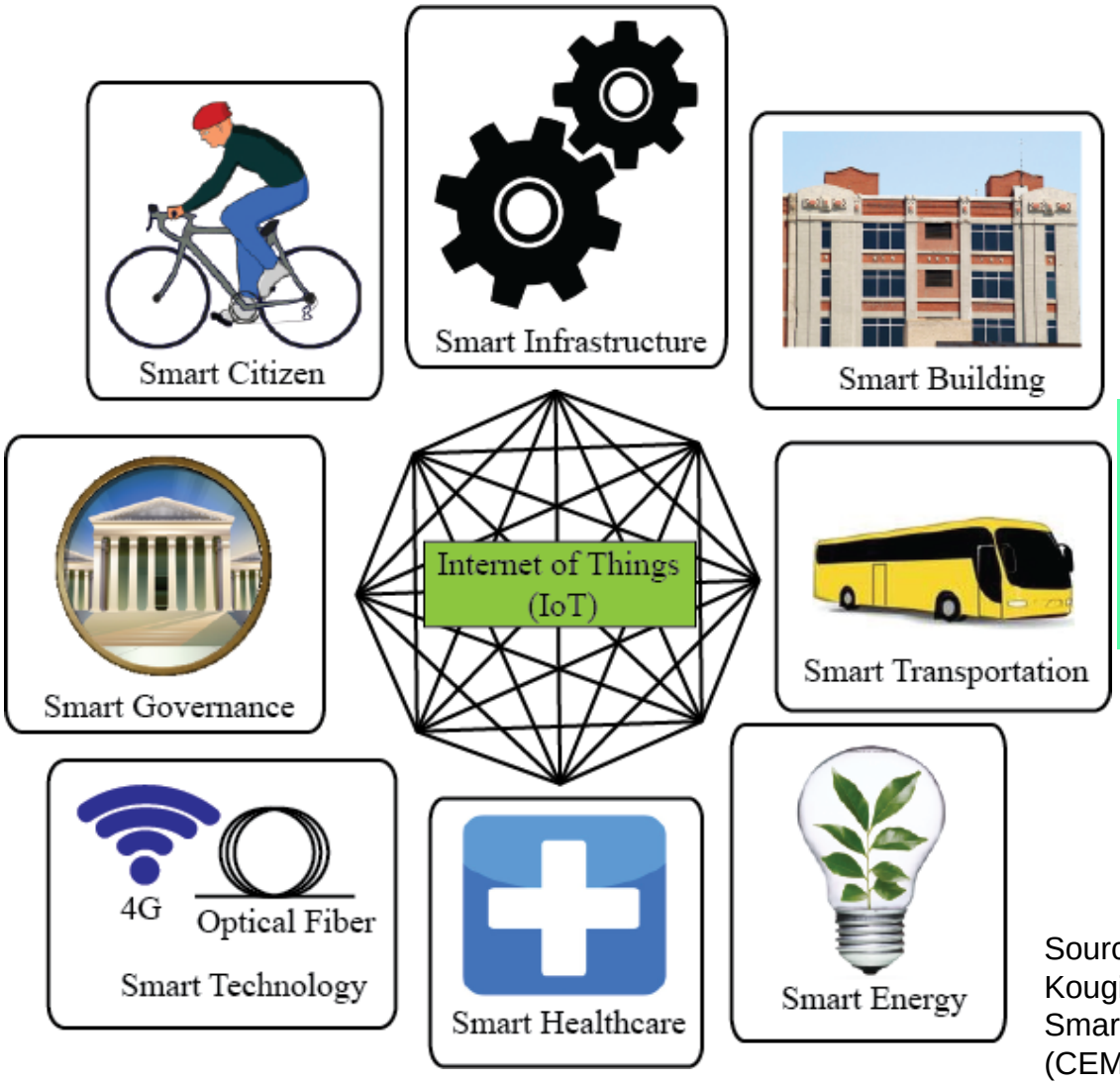
- Definition - 1: A city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city".

- Definition - 2: "A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operations and services, and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects".

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", IEEE Consumer Electronics Magazine (CEM), Volume 5, Issue 3, July 2016, pp. 60--70.

Smart City Components

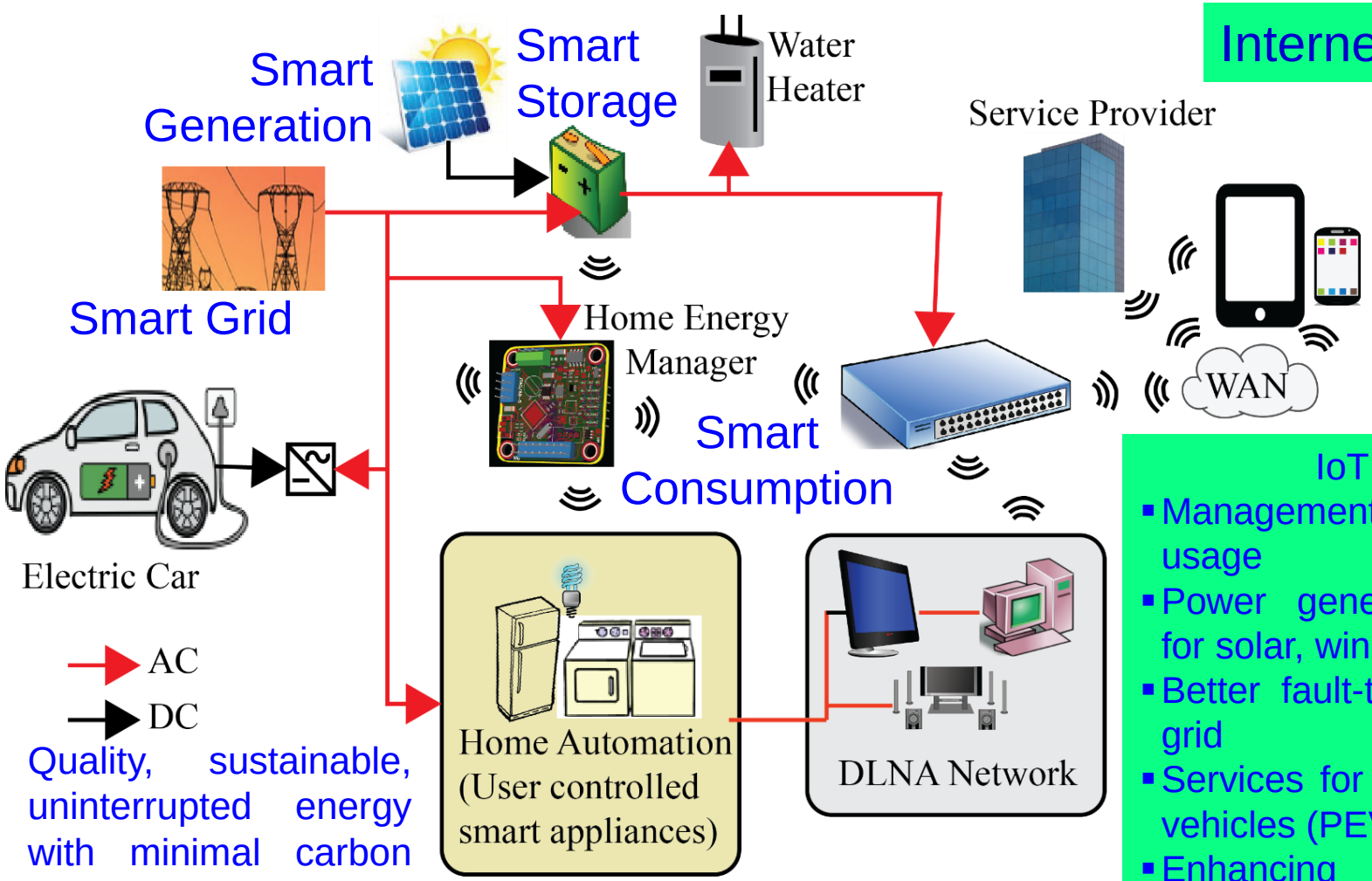
Smart Cities - Components



A smart city can have one or more of the smart components.

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", IEEE Consumer Electronics Magazine (CEM), Volume 5, Issue 3, July 2016, pp. 60--70.

Smart Energy



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

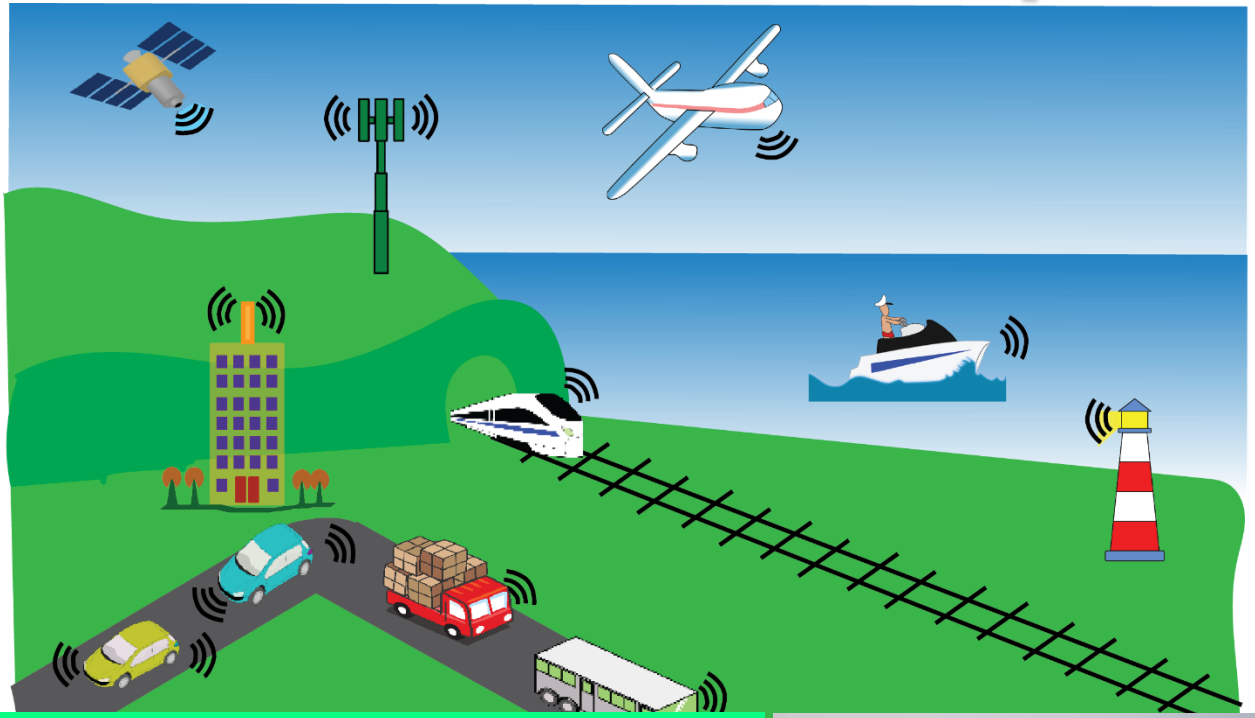
Source: Mohanty 2016, CE Magazine July 2016

Internet of Energy

IoT Role:

- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships

Smart Transportation



Smart Transportation Features:

- Autonomous driving
- Effective traffic management
- Real-time vehicle tracking
- Vehicle safety – Automatic brake
- Vehicle-to-Vehicle communication
- Better scheduling of train, aircraft
- Easy payment system

"The smart transportation system allows passengers to easily select different transportation options for lowest cost, shortest distance, or fastest route."

Source: Mohanty 2016, CE Magazine July 2016

Smart Healthcare



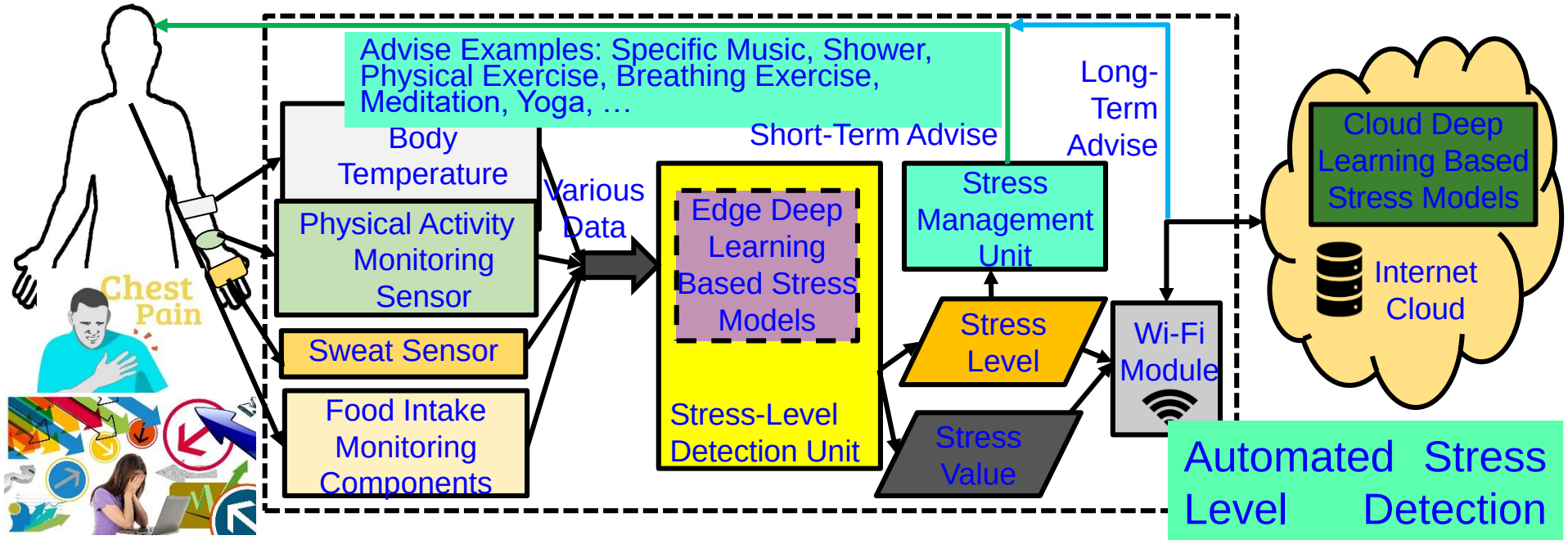
Healthy Living	Home Care	Acute care
• Fitness Tracking • Disease Prevention • Food monitoring	• Mobile health • Telemedicine • Self-management • Assisted Living	• Hospital • Specialty clinic • Nursing Home • Community Hospital

Internet of Medical Things (IoMT)

Frost and Sullivan predict smart health-care market value to reach US$348.5 billion by 2025.

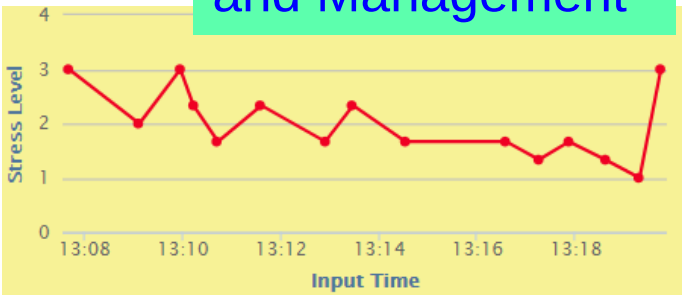
Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care", IEEE Consumer Electronics Magazine (CEM), Volume 7, Issue 1, January 2018, pp. 18-28.

Smart Healthcare - Stress Monitoring & Control



Sensor	Low Stress	Normal Stress	High Stress
Accelerometer (steps/min)	0-75	75-100	101-200
Humidity (RH%)	27-65	66-91	91-120
Temperature ℉	98-100	90-97	80-90

Automated Stress Level Detection and Management



Source: L. Rachakonda, S. P. Mohanty, E. Kougianos, and P. Sundaravadivel, "Stress-Lysis: A DNN-Integrated Edge Device for Stress Level Detection in the IoMT", IEEE Transactions on Consumer Electronics (TCE), Volume XX, Issue YY, ZZ 2019, pp. Accepted on 07 Sep 2019.

Smart Healthcare - Seizure Detection & Control

EEG Signal

Drug Injection

Seizure Detection

Yes

Drug Delivery Unit

Seizure State

Dosage Information

Wireless Transfer

Cloud Storage

Hospital

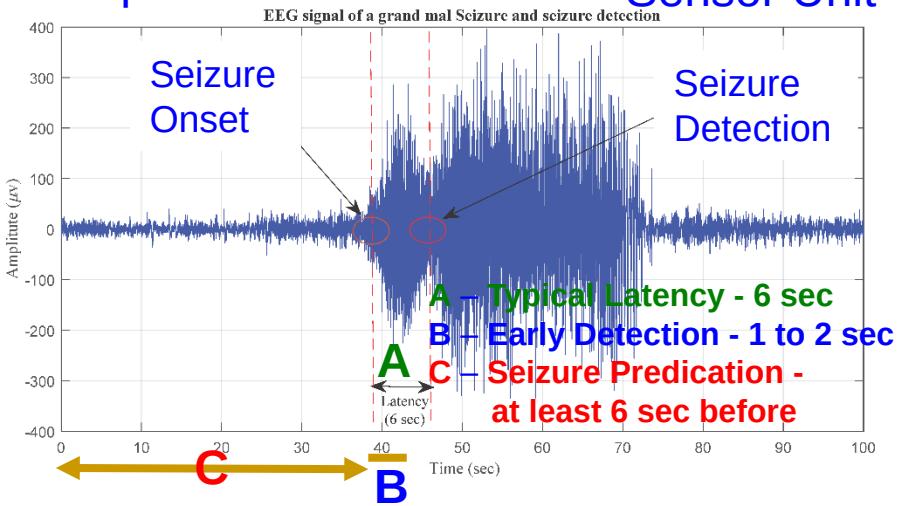
Doctor

EEG Data Acquisition

Sensor Unit

Transmission and Storage

Access Unit

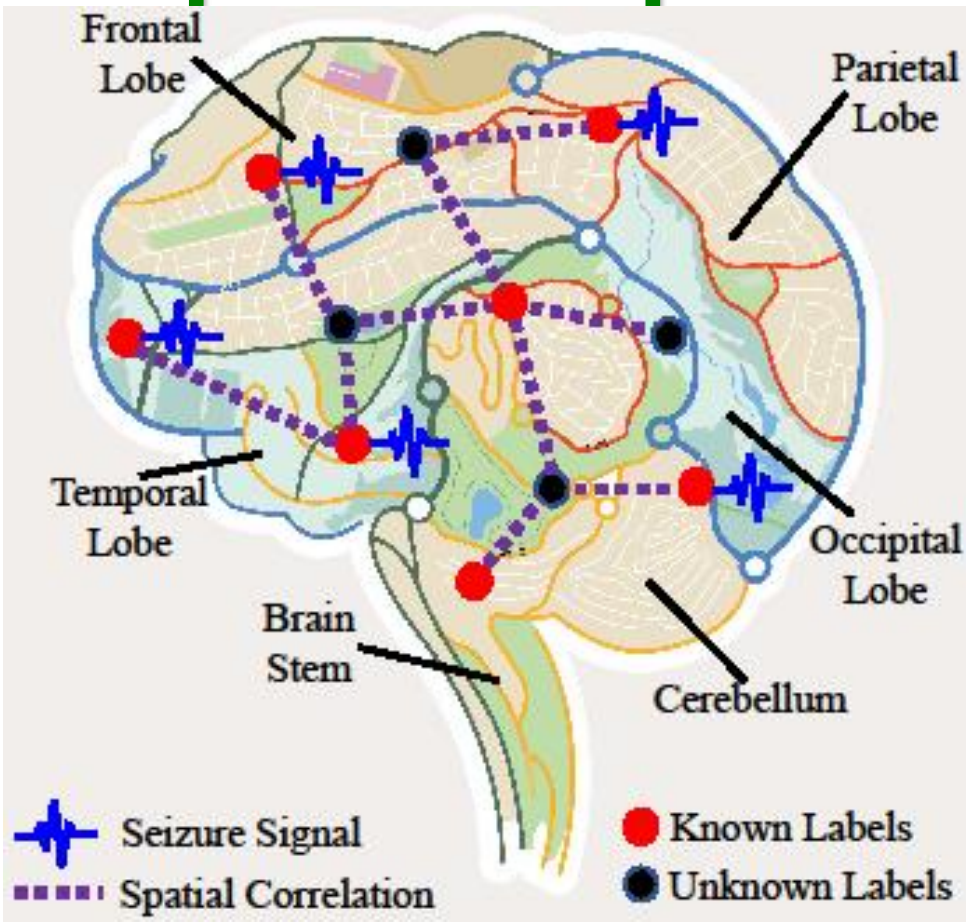


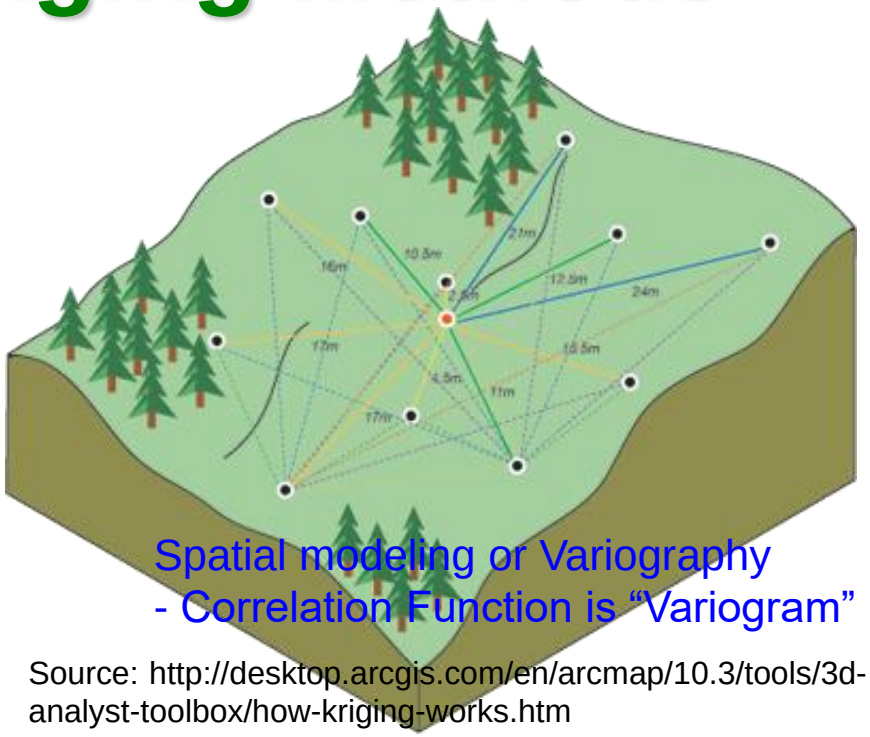
Automated Epileptic Seizure Detection and Control System

Cloud Vs Edge	Latency	Accuracy
Cloud-IoT based Detection	2.5 sec	98.65%
Edge-IoT based Detection	1.4 sec	98.65%

Source: M. A. Sayeed, S. P. Mohanty, E. Kougianos, and H. Zaveri, "Neuro-Detect: A Machine Learning Based Fast and Accurate Seizure Detection System in the IoMT", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 359--368.

Smart Healthcare – Brain as a Spatial Map → Kriging Methods





Spatial modeling or Variography
- Correlation Function is "Variogram"

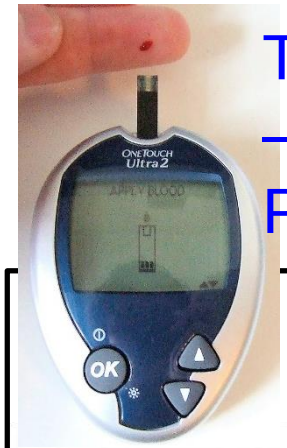
Source: http://desktop.arcgis.com/en/arcmap/10.3/tools/3d-analyst-toolbox/how-kriging-works.htm

Spatial autocorrelation principle - things that are closer are more alike than things farther

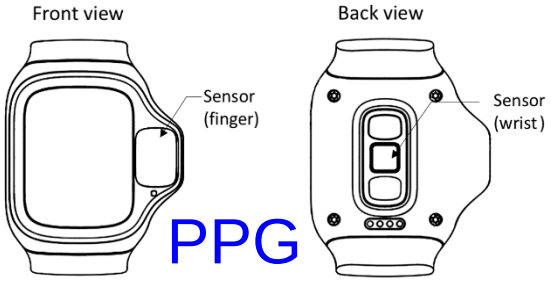
Source: I. L. Olokodana, S. P. Mohanty, and E. Kougianos, "Ordinary-Kriging Based Real-Time Seizure Detection in an Edge Computing Paradigm", in *Proceedings of the 38th IEEE International Conference on Consumer Electronics (ICCE)*, 2020, Under Review.

Smart Healthcare – iGLU –

Noninvasive, Accurate, Continuous Glucose Monitoring



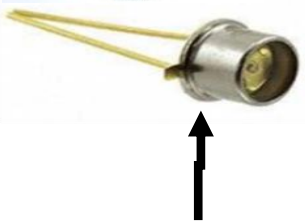
Traditional – Finger Pricking



PPG

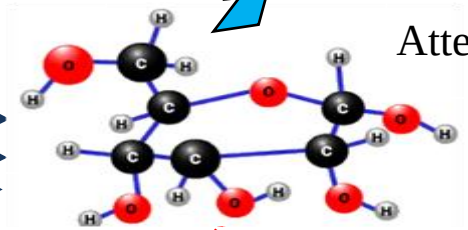
NIR

Vibrations (Stretching, Wagging, Bending)



Near Infrared (NIR) Emitters (940nm, 1300nm)

Transmitted Wave



Attenuated Wave

Infrared Detector

Analog-to-Digital Converter (ADS1115)

Infrared Detector

Clinically tested in an hospital.

Cost - US$ 20
Accuracy - 100%

Source: P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare", IEEE Consumer Electronics Magazine (MCE), Vol. 9, No. 1, January 2020, pp. To Appear.

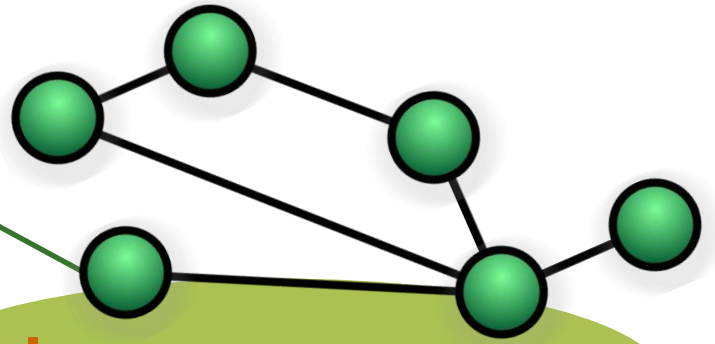
Smart City Technologies

Smart Cities - 3 Is

Instrumentation

The 3Is are provided by the Internet of Things (IoT).

Smart Cities



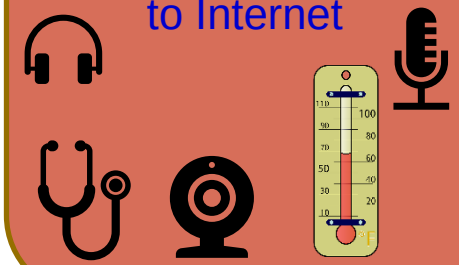
Intelligence

Interconnection

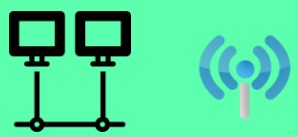
Source: Mohanty EuroSimE 2016 Keynote Presentation

Internet of Things (IoT) – Concept

Things
Sensors/actuators with IP address that can be connected to Internet



Local Network
Can be wired or wireless: LAN, Body Area Network (BAN), Personal Area Network (PAN), Controller Area Network (CAN)



Cloud Services
Data either sent to or received from cloud (e.g. machine activation, workflow, and analytics)

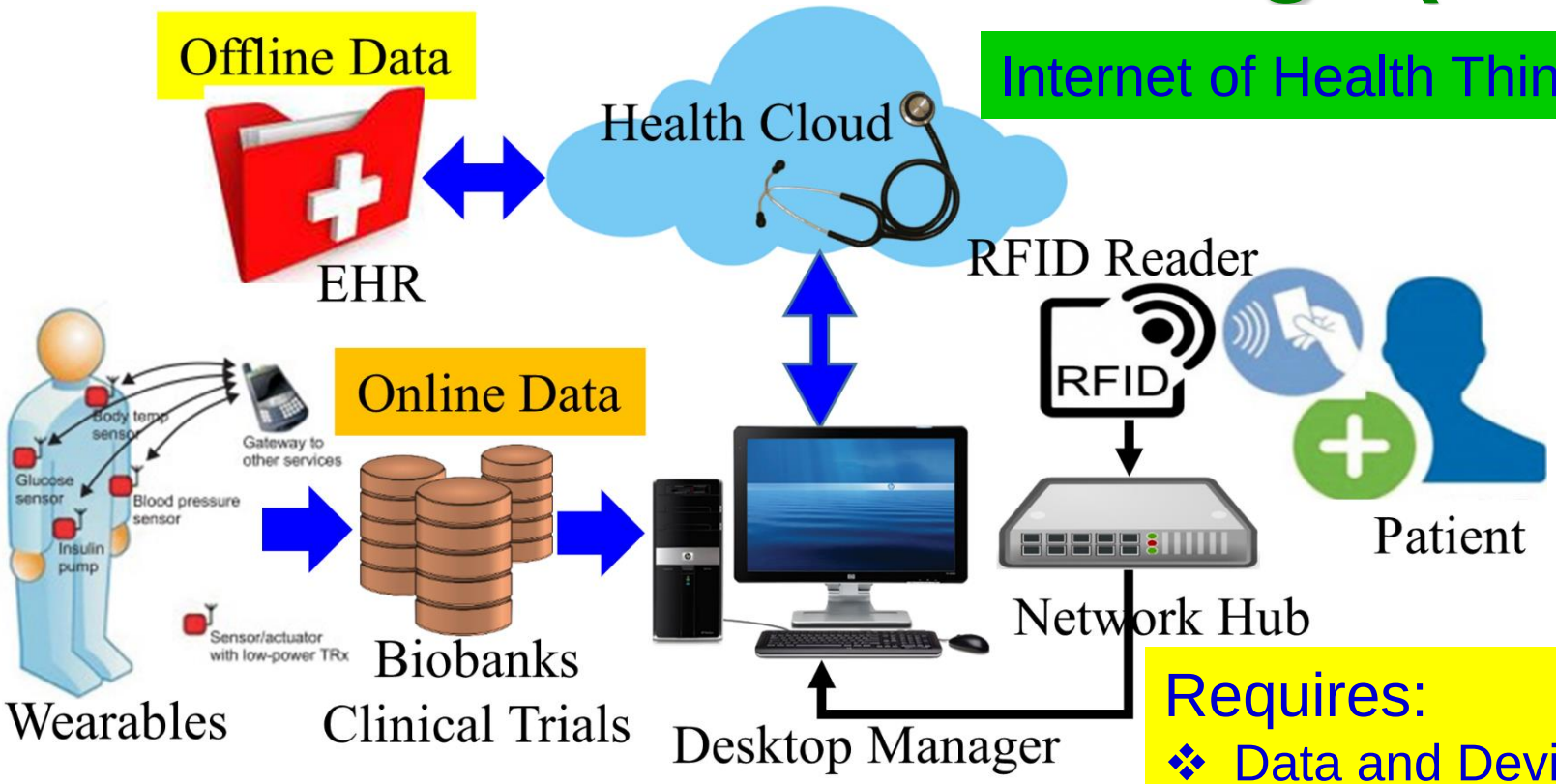
Global Network
Connecting bridge between the local network, cloud services and connected consumer devices

Connected Consumer Electronics
Smart phones, devices, cars, wearables which are connected to the Things

Overall architecture:
- A configurable dynamic global network of networks
- Systems-of-Systems

Source: Mohanty ICIT 2017 Keynote

Internet of Medical Things (IoMT)



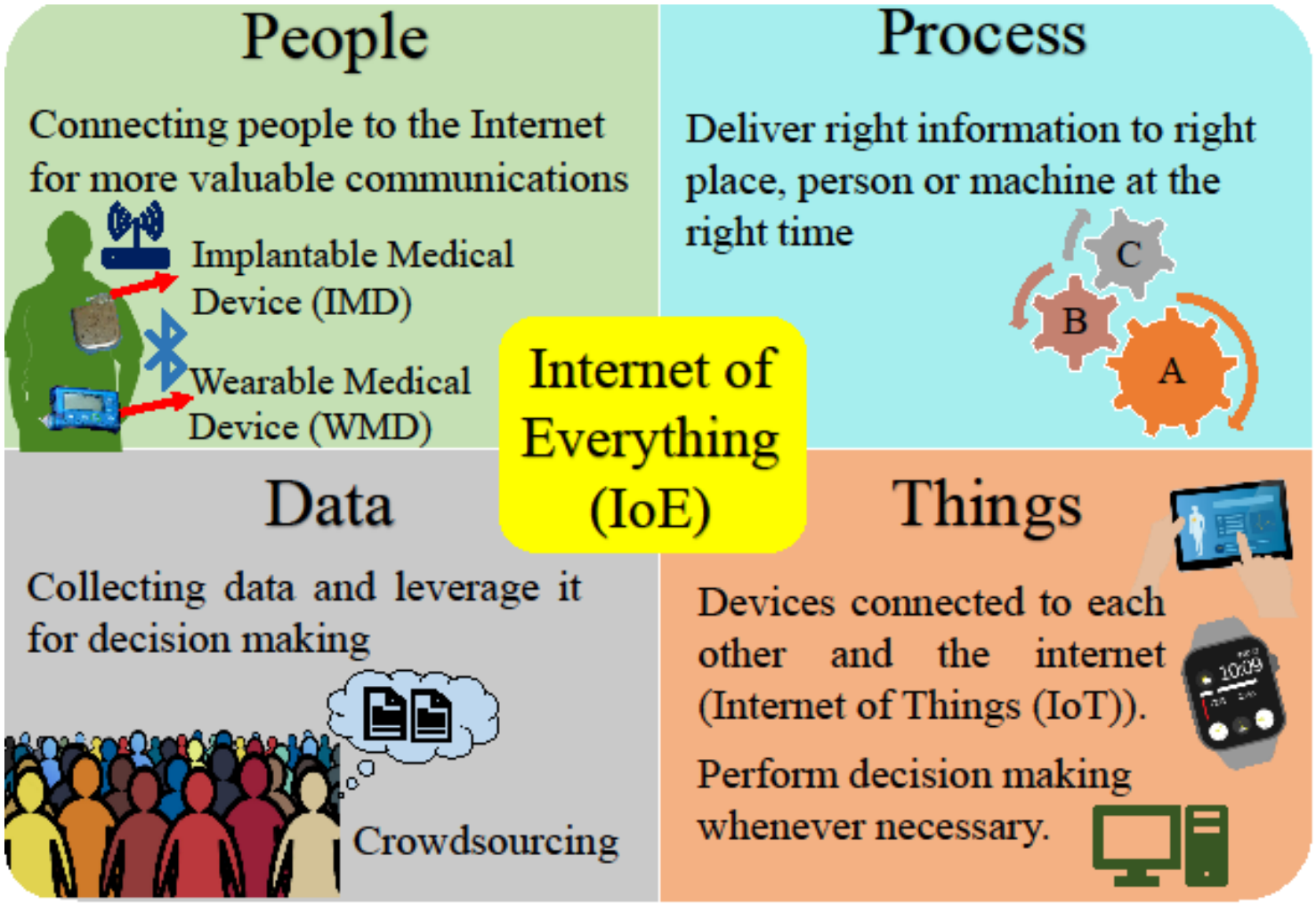
Requires:

- Data and Device Security
- Data Privacy

IoMT is a collection of medical devices and applications that connect to healthcare IT systems through Internet.

Source: http://www.icemiller.com/ice-on-fire-insights/publications/the-internet-of-health-things-privacy-and-security/
Source: http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

Internet of Every Things (IoE)

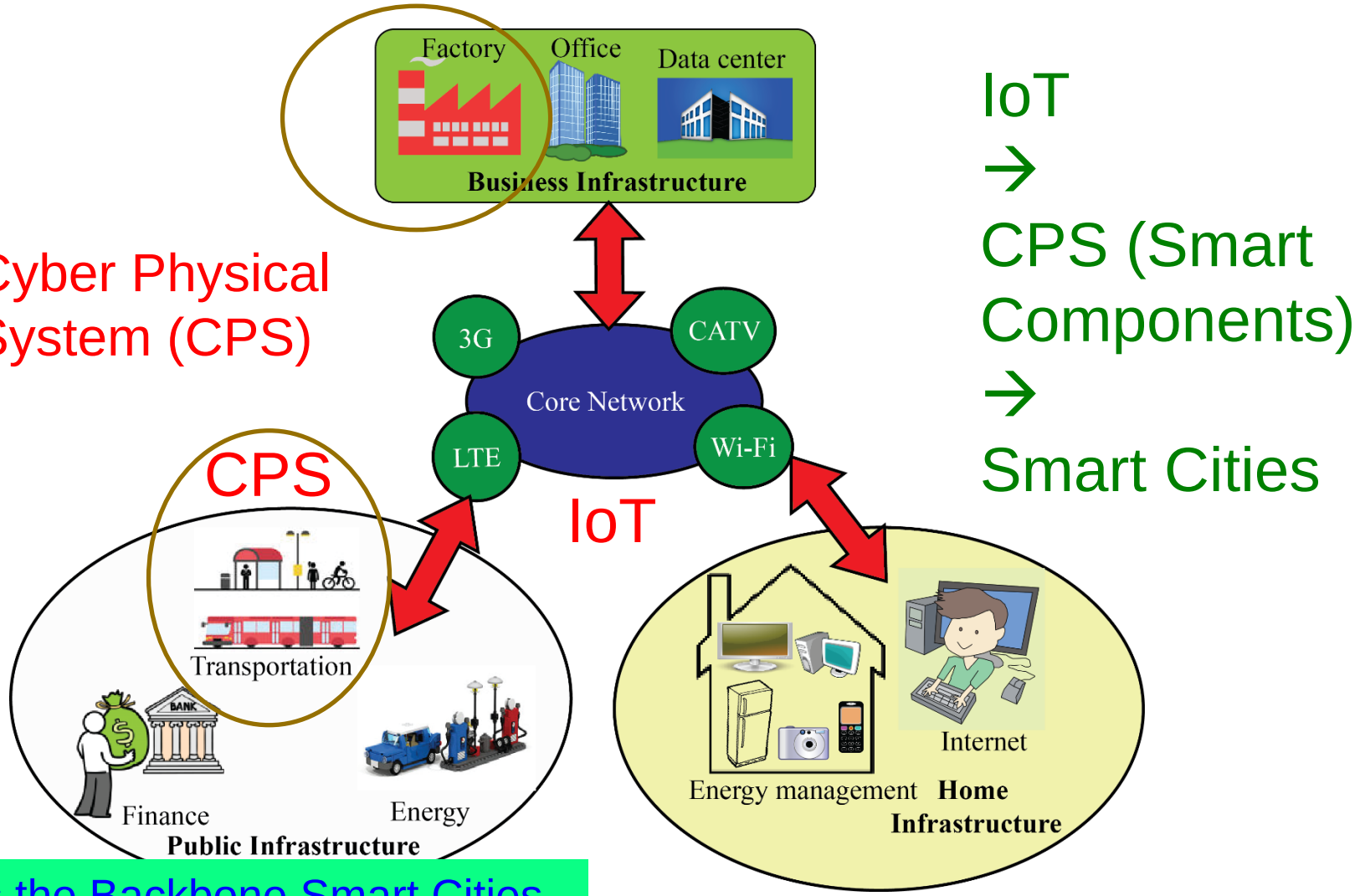


Requires:

- Data, Device, and System Security
- Data, Location, and System Privacy

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)", arXiv Computer Science, arXiv:1909.06496, September 2019, 37-pages.

IoT → CPS → Smart Cities



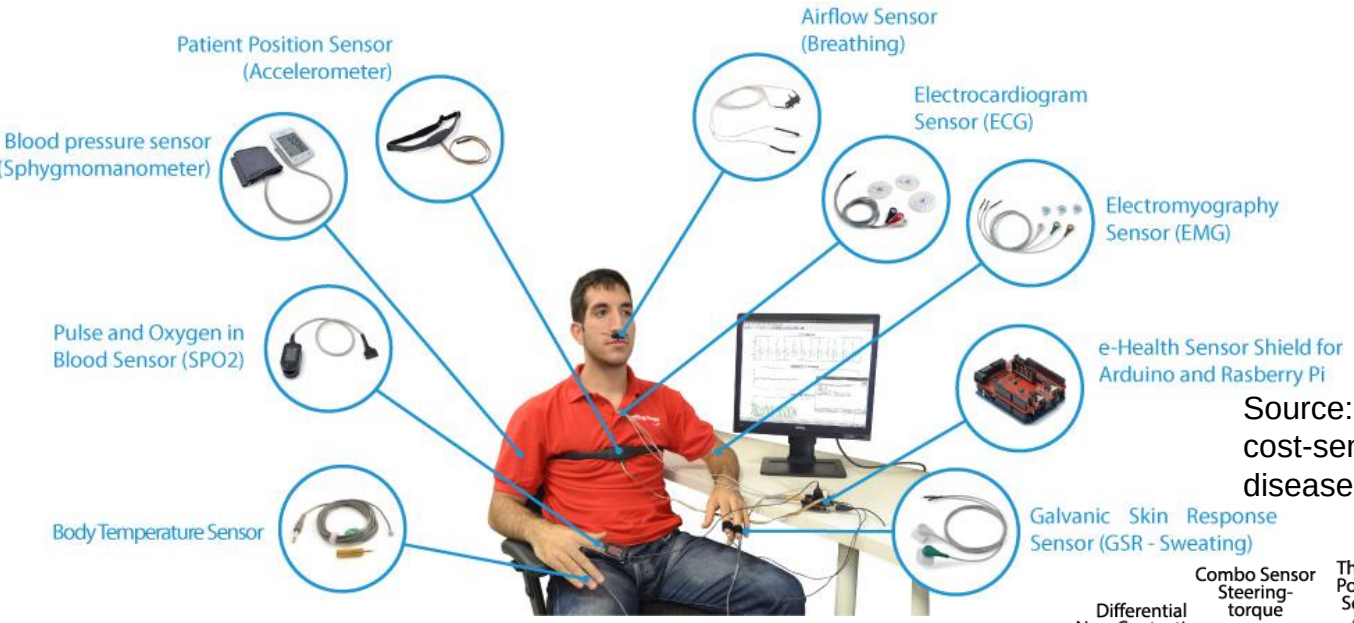
Cyber Physical System (CPS)

IoT → CPS (Smart Components) → Smart Cities

IoT is the Backbone Smart Cities.

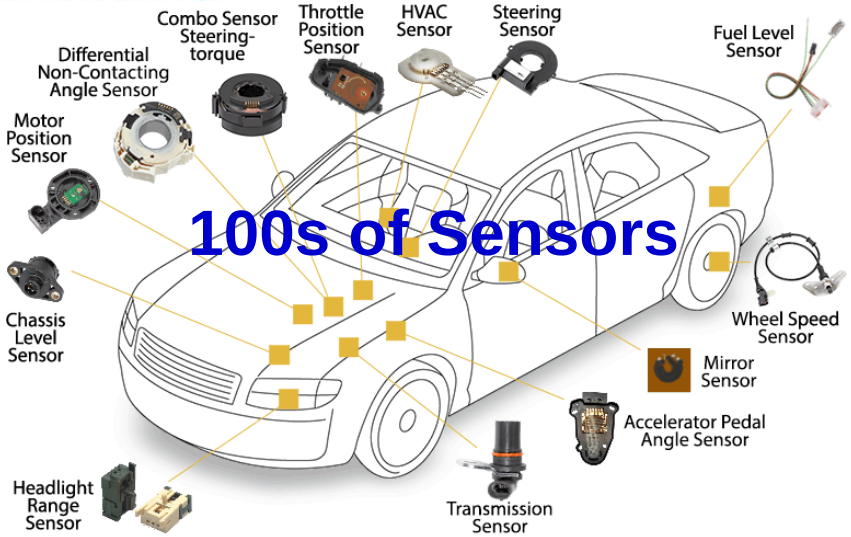
Source: Mohanty 2016, CE Magazine July 2016

Sensor Technology – Variety of Them



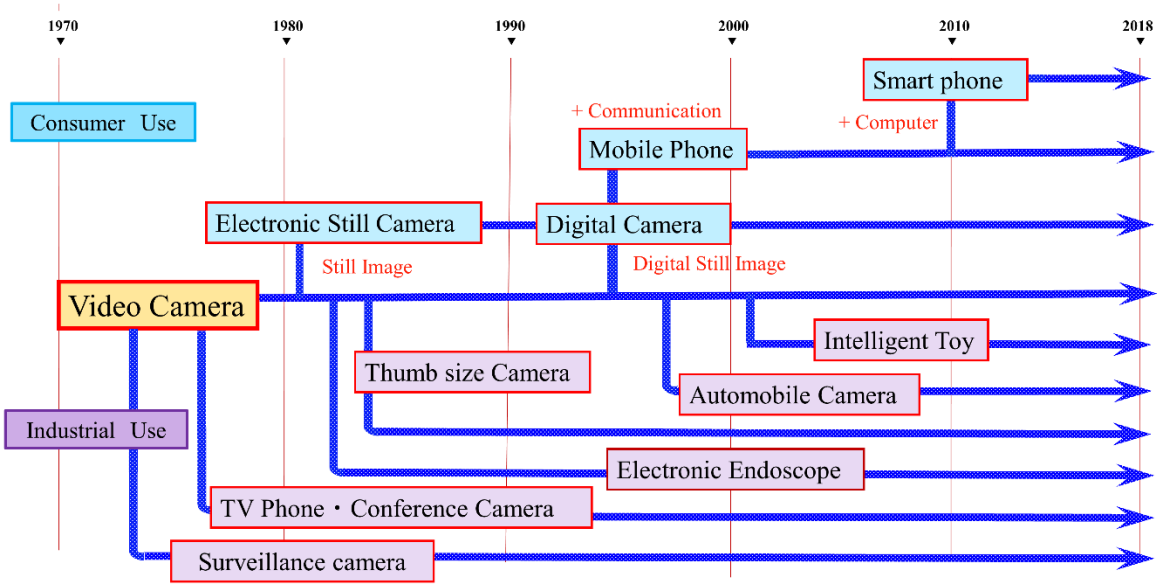
Source: http://www.libelium.com/e-health-low-cost-sensors-for-early-detection-of-childhood-disease-inspire-project-hope/

Thing ← Sensor
+ Device with its own IP address



Source: Mohanty ICCE 2019 Keynote

Cameras are Everywhere



Y. Takemura, "The Development of Video-Camera Technologies: Many Innovations Behind Video Cameras Are Used for Digital Cameras and Smartphones," IEEE Consumer Electronics Magazine, vol. 8, no. 4, pp. 10-16, July 2019.

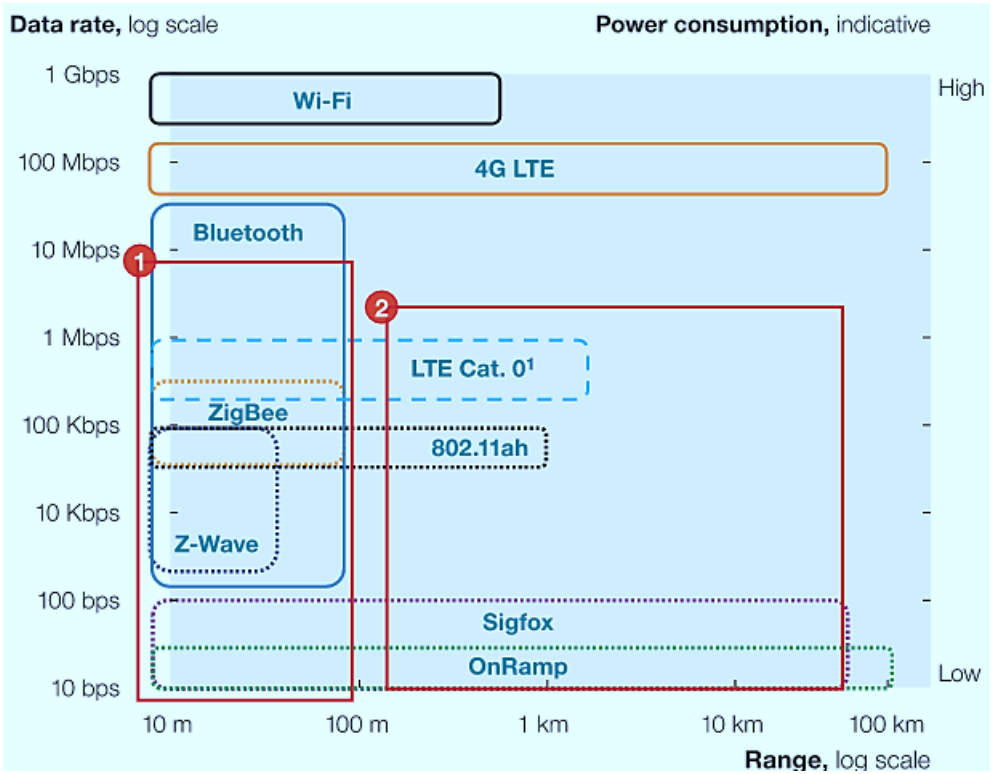
CMOS image sensors → Cameras of any size, part of any device, and placed at any location.

In 1986: 1.3 megapixels CCD sensor Kodak camera was $13,000.

IoT - Communications Technology

Selected IoT Communications Technology

- Bluetooth Low-Energy (BLE)
- Zigbee
- Z-Wave
- 6LowPAN
- Thread
- WiFi
- Cellular
- NFC
- Sigfox
- Neul
- LoRaWAN



Source: https://www.postscapes.com/internet-of-things-protocols/

Source: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

Unmanned Ariel Vehicle (UAV)

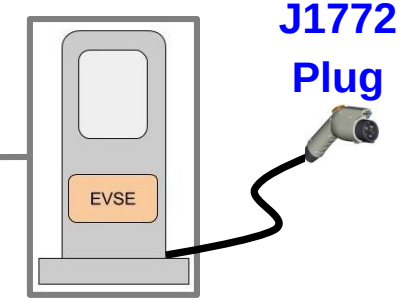
Unmanned Arial Vehicles or Remotely Piloted Vehicles is an aircraft without a human pilot on board.

- Unmanned Aerial Vehicle
- Drone - remotely piloted
- Controlled autonomously

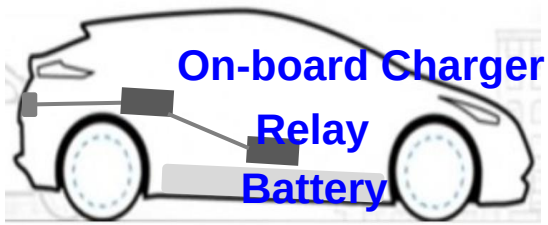
First used in Austria for military purposes during 1849.

EV Charging Technology

Grid



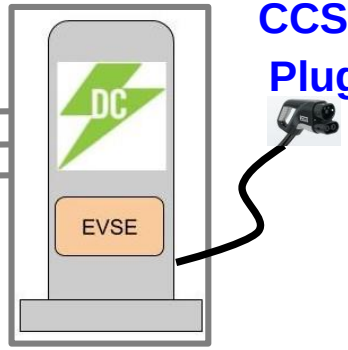
J1772 Plug



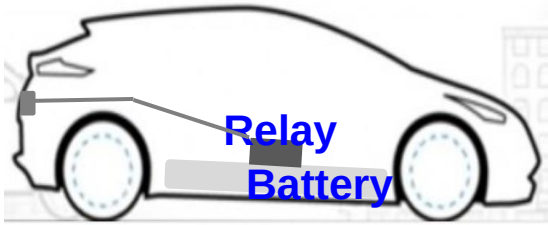
AC charging station

- Monitoring function
- Communication and safety

3 phase AC supply



CCS1 Plug



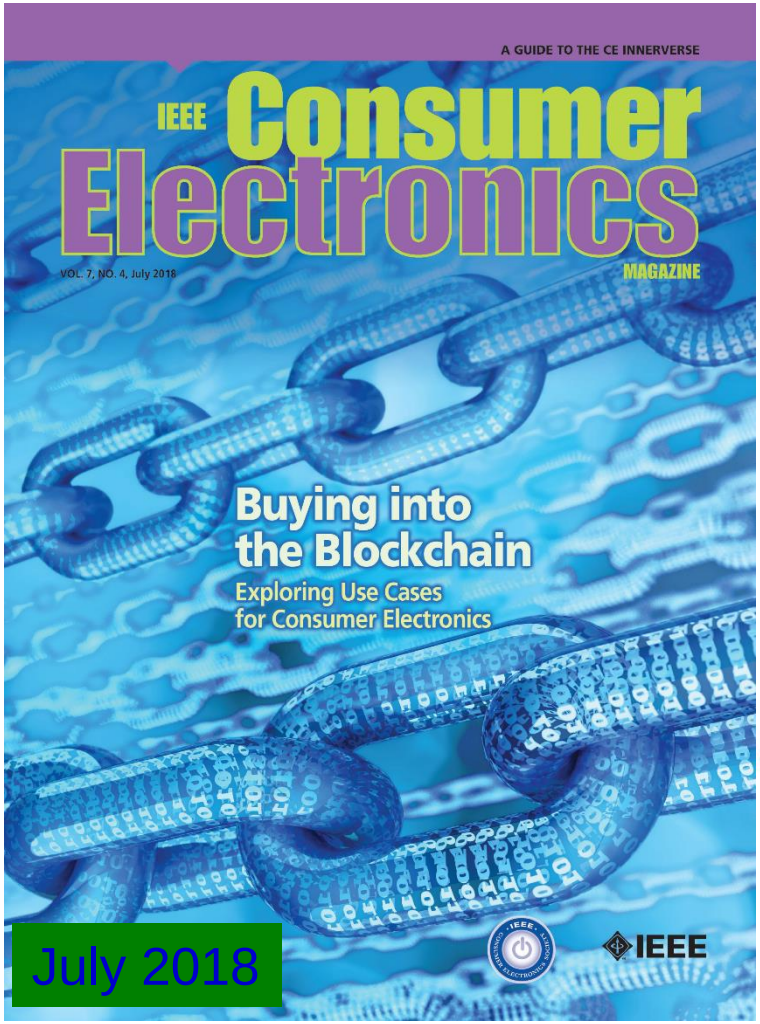
DC charging station

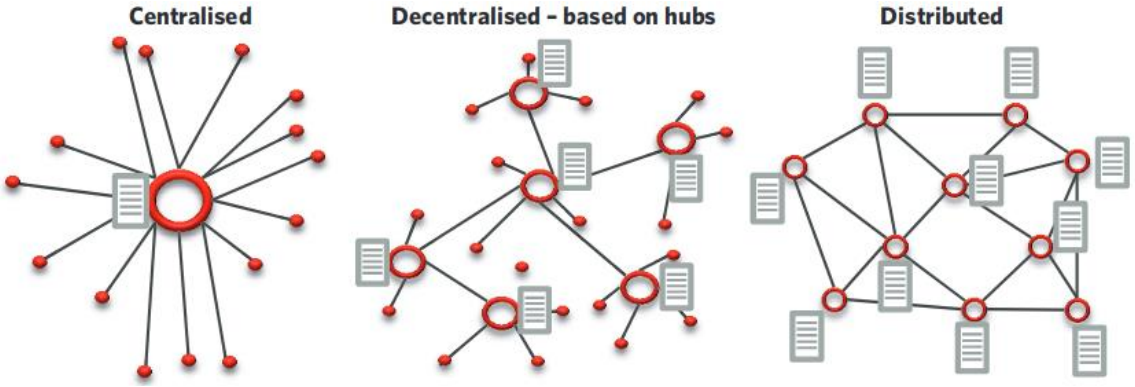
- AC-DC Off board conversion
- Monitoring Power flow
- EV to grid communication
- Safety monitoring

Electric Vehicle Supply Equipment (EVSE)

Source: S. K. Rastogi, A. Sankar, K. Manglik, S. K. Mishra, and S. P. Mohanty, "Toward the Vision of All-Electric Vehicles in a Decade", IEEE Consumer Electronics Magazine (CEM), Volume 8, Issue 2, March 2019, pp. 103--107.

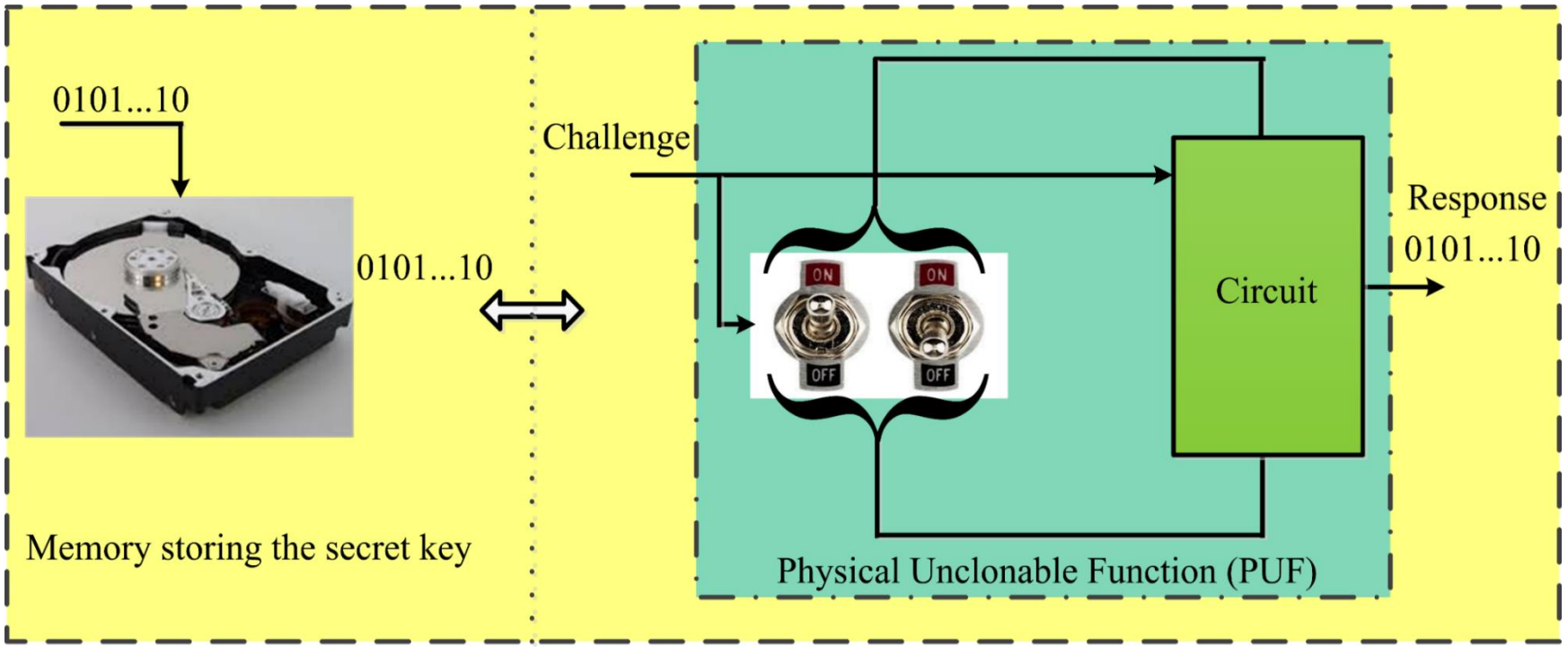
Blockchain Technology





Source: https://icomalta.com/distributed-ledger-technology/

Security Primitives - PUF



PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

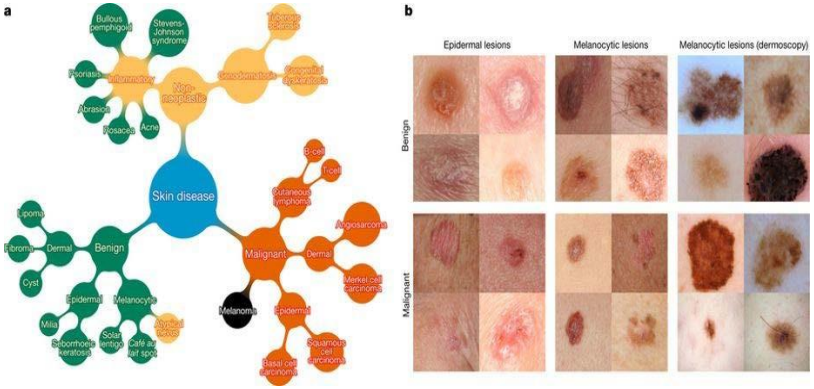
Source: S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

AI / Machine Learning is Ubiquitous

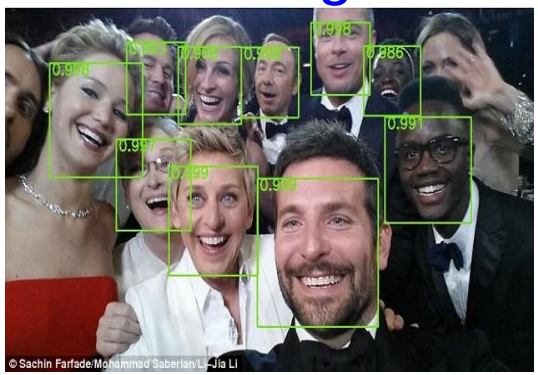
Self-driving Cars

Cybersecurity

Healthcare



Facial Recognition

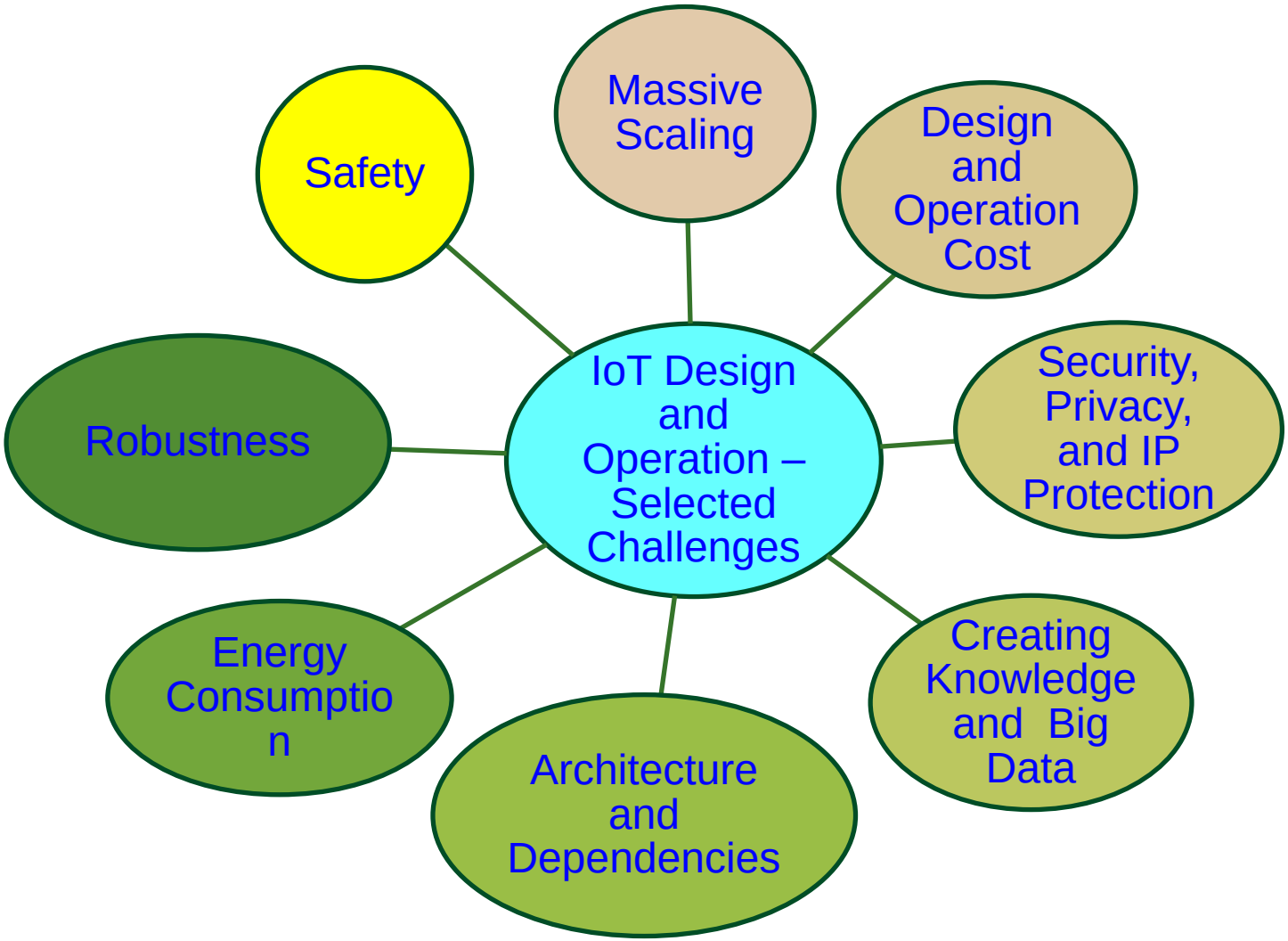


Speech Recognition

Source: Sandip Kundu ISVLSI 2019 Keynote.

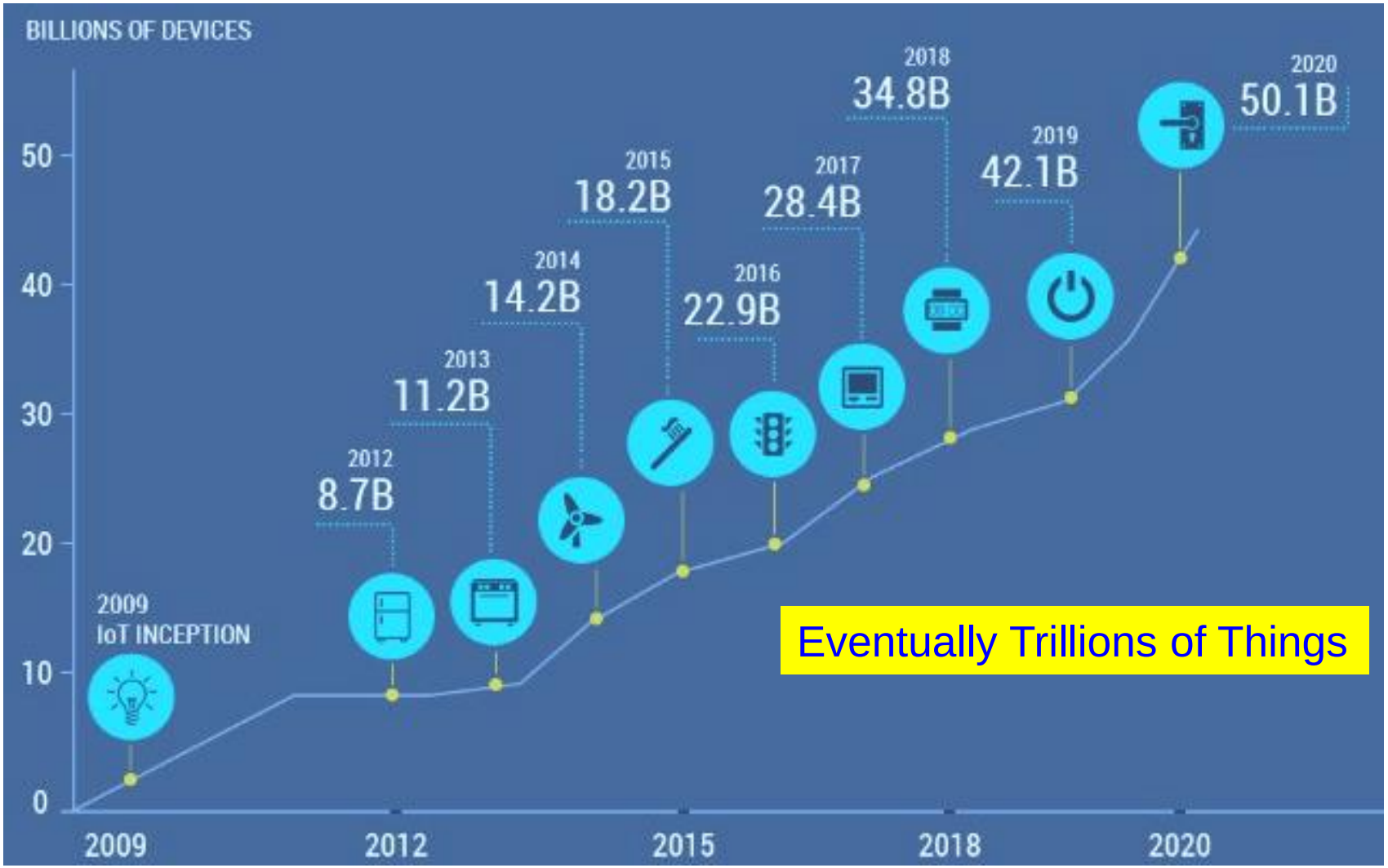
Challenges in Smart City Design

Smart City – Selected Challenges



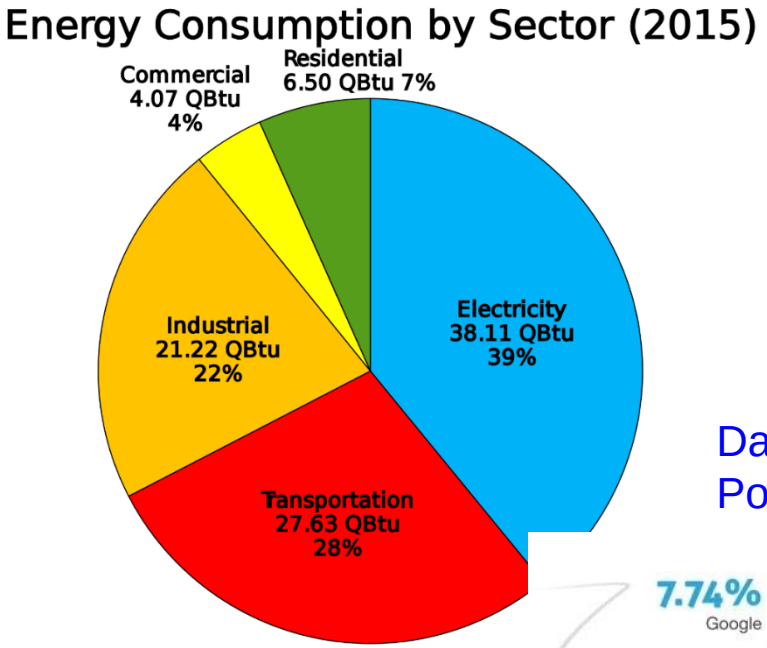
Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things

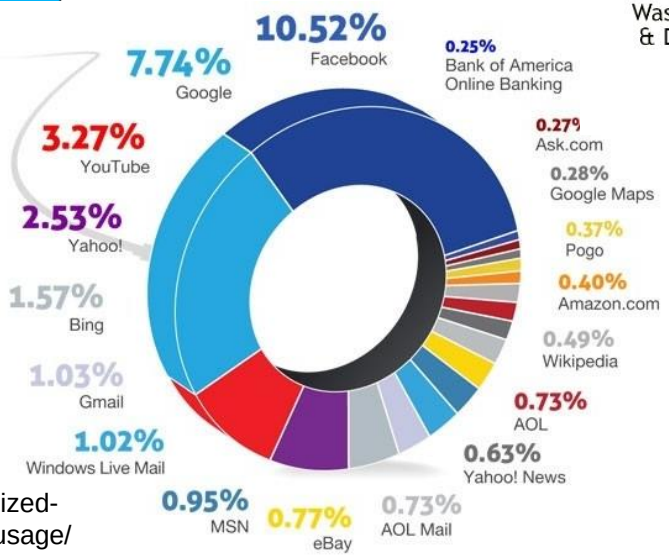


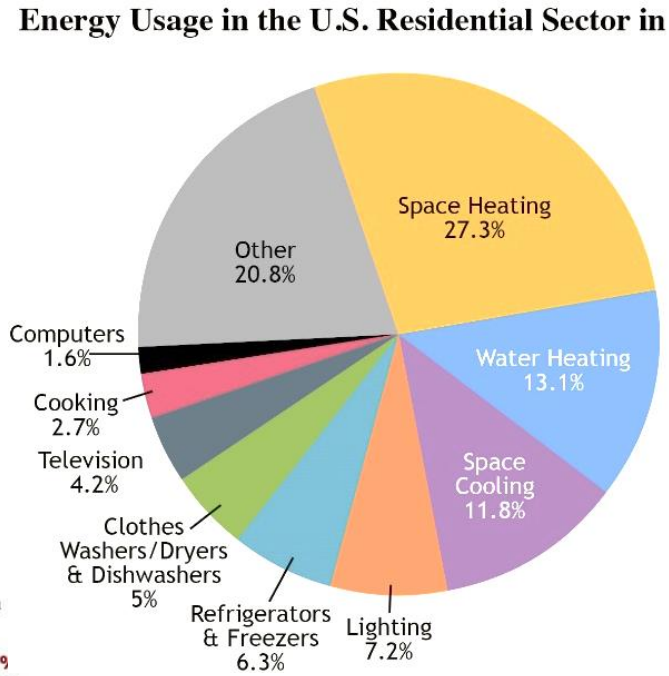
Source: https://www.linkedin.com/pulse/history-iot-industrial-internet-sensors-data-lakes-0-downtime

Energy Consumption



Data Center Power Usage





Individual Level: Imagine how often we charge our portable CE!

Source: https://www.engadget.com/2011/04/26/visualized-ring-around-the-world-of-data-center-power-usage/

CE Systems – Diverse Security/ Privacy/ Ownership Requirements

Medical Devices

RFID Chip

Pace maker

Insulin Pump

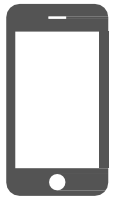
Heart Rate Monitor

Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices



Smart Phones/ Tablets

Wearable Devices

Smart Clothing

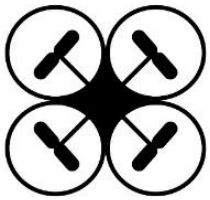
Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

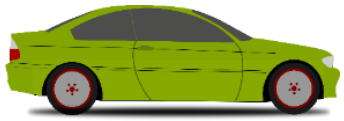
Entertainment Devices



Drones /UAVs

Video Games

Transportation Devices



Smart Vehicles/ Autonomous Vehicles

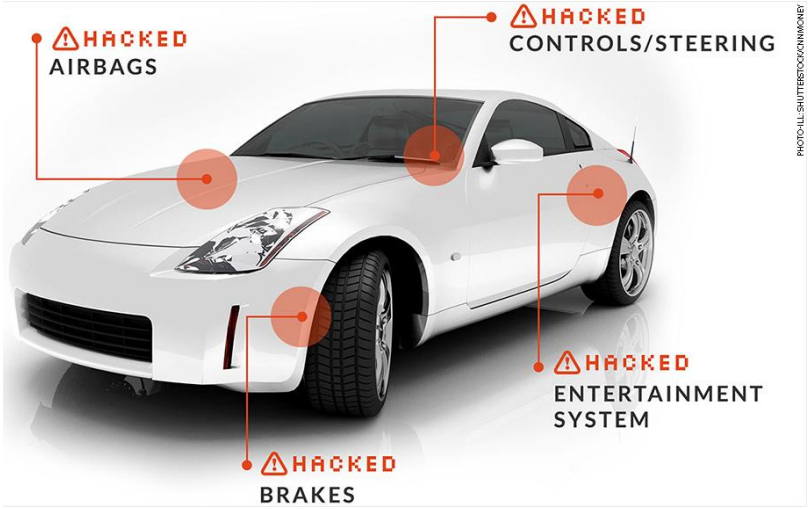
Smart Traffic Controllers

Source: D. A. Hahn, A. Munir, and S. P. Mohanty, "Security and Privacy Issues in Contemporary Consumer Electronics", IEEE Consumer Electronics Magazine (MCE), Volume 8, Issue 1, January 2019, pp. 95--99.

Security Challenge - System

Power Grid Attack

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Security Challenge – Information

Online Banking

...

Credit Card Theft

Hacked: Linkedin, Tumbler, & Myspace

Linked in

tumblr.

myspace

Who did it: A hacker going by the name Peace.

What was done: 500 million passwords were stolen.

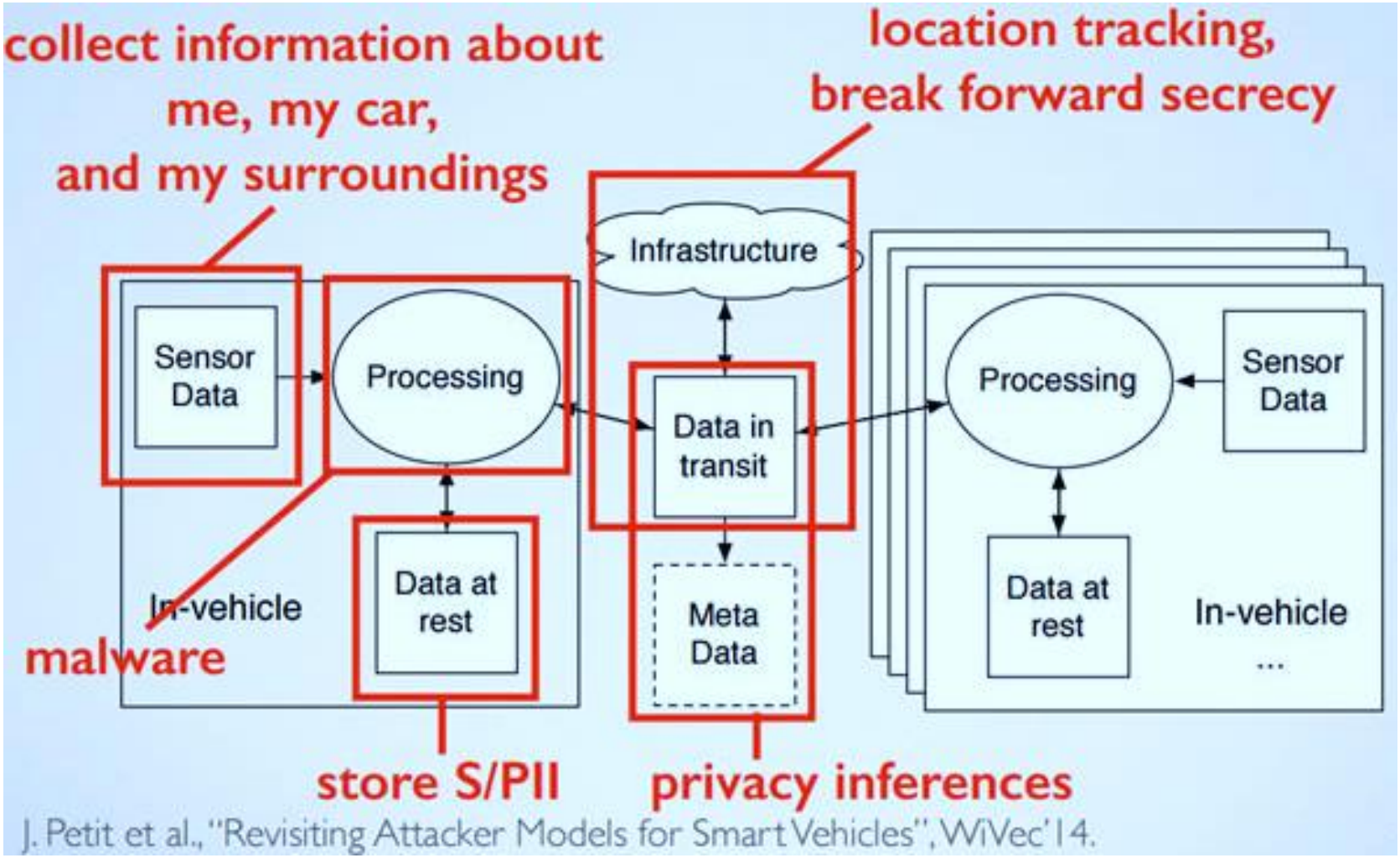
Details: Peace had the following for sale on a Dark Web Store:

- 167 million Linkedin passwords
- 360 million Myspace passwords
- 68 million Tumbler passwords
- 100 million VK.com passwords
- 71 million Twitter passwords

Personal Information

Credit Card/Unauthorized Shopping

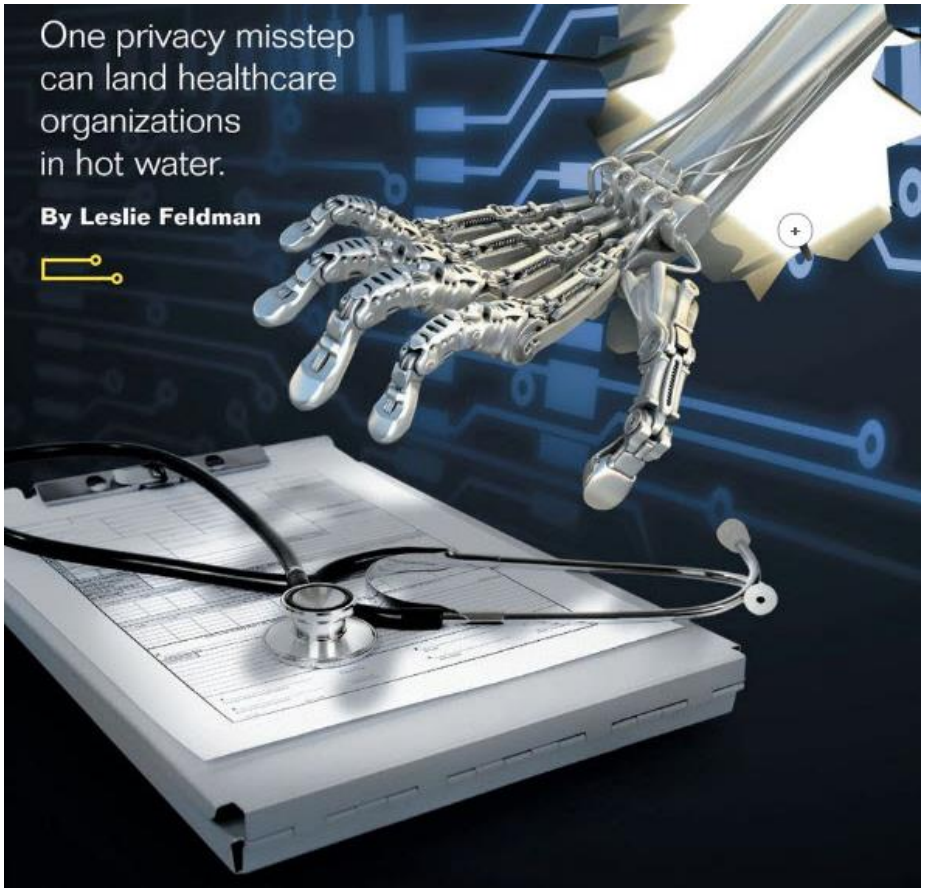
Privacy Challenge – System



Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

Privacy Challenge - Information

Source: http://ciphercloud.com/three-ways-pursue-cloud-data-privacy-medical-records/



Source: http://blog.veriphyr.com/2012/06/electronic-medical-records-security-and.html

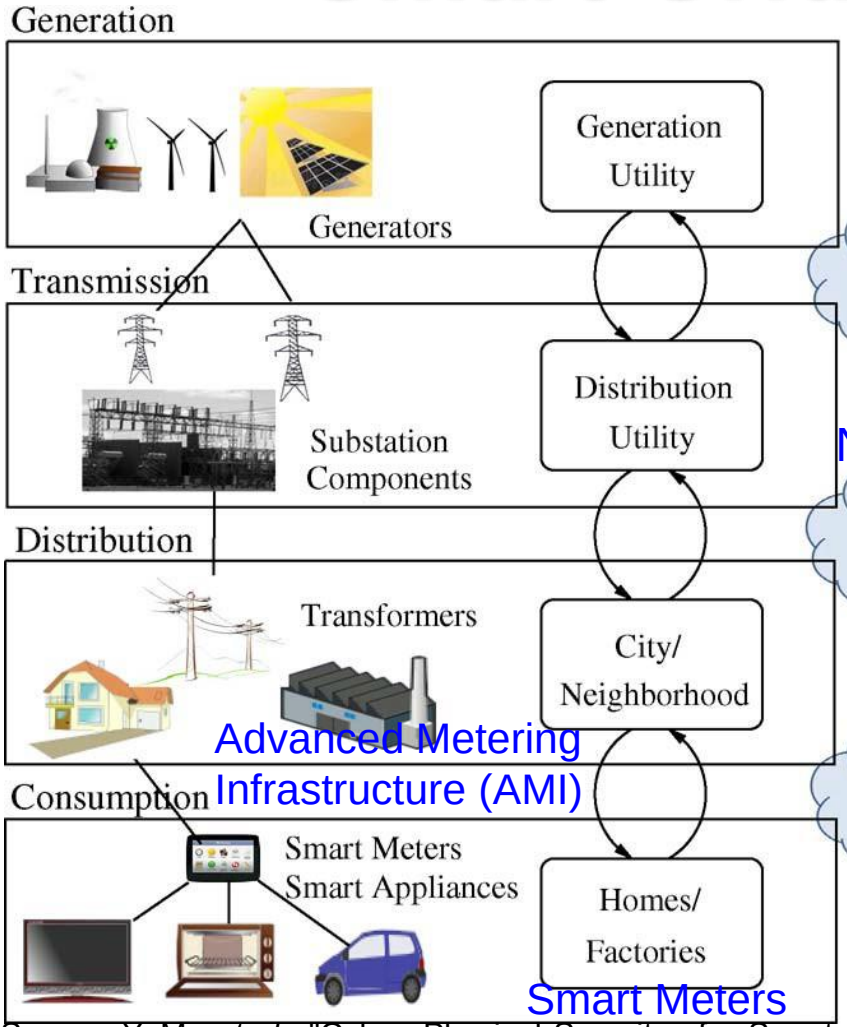
Smart Healthcare - Security and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

- Data Eavesdropping
- Data Confidentiality
- Data Privacy
- Location Privacy
- Identity Threats
- Access Control
- Unique Identification
- Data Integrity

Source: Mohanty iSES 2018 Keynote

Smart Grid - Vulnerability



Source: Y. Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure", *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

Information and Communication Technology (ICT) components of smart grid is cyber vulnerable.

Data, Application/System Software, Firmware of Embedded System are the loop holes for security/privacy.

Network/Communication Components

Phasor Measurement Units (PMU)

Phasor Data Concentrators (PDC)

Energy Storage Systems (ESS)

Programmable Logic Controllers (PLCs)

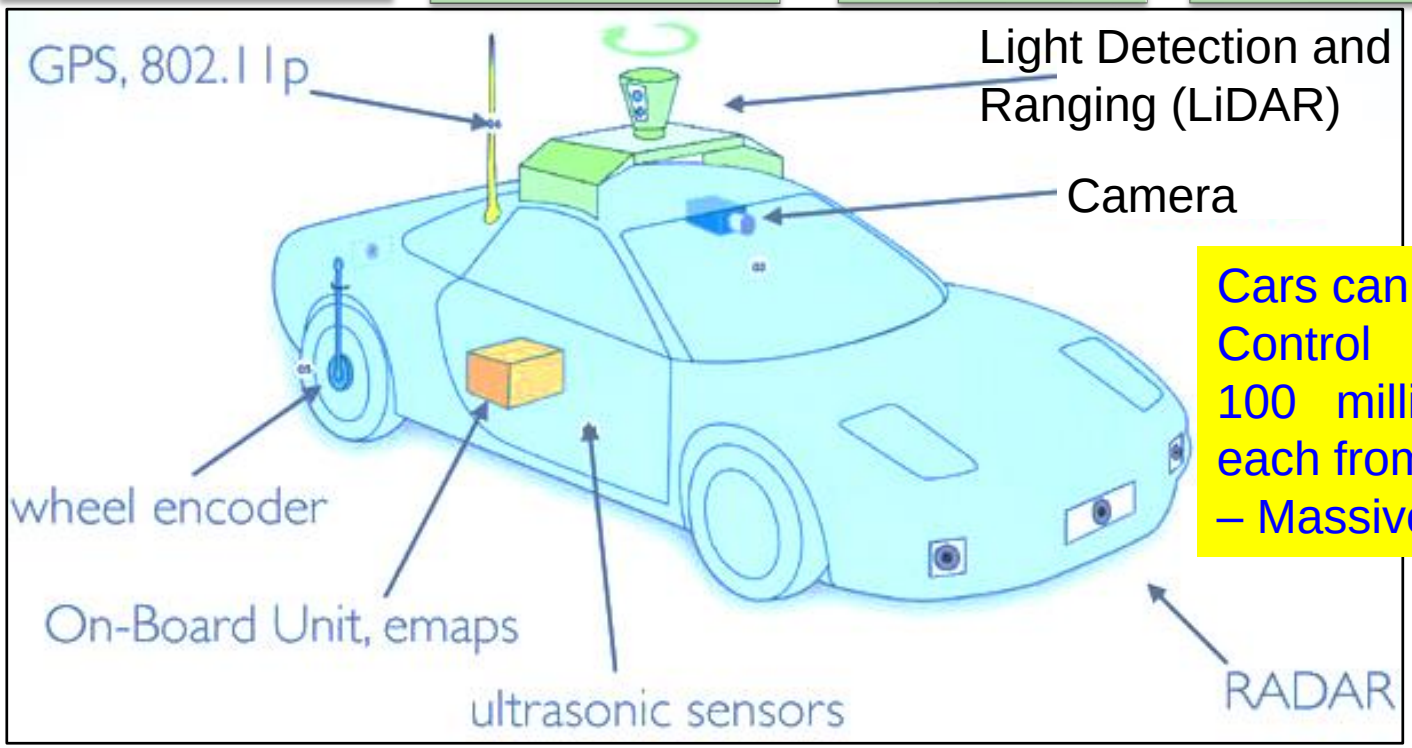
Smart Meters

Smart Grid Model - A Cyber-Physical Security (CPS) Perspective

CE System Security – Smart Car

Selected Attacks on Autonomous Cars

- Replay
- Relay
- Jamming
- Spoofing
- Tracking



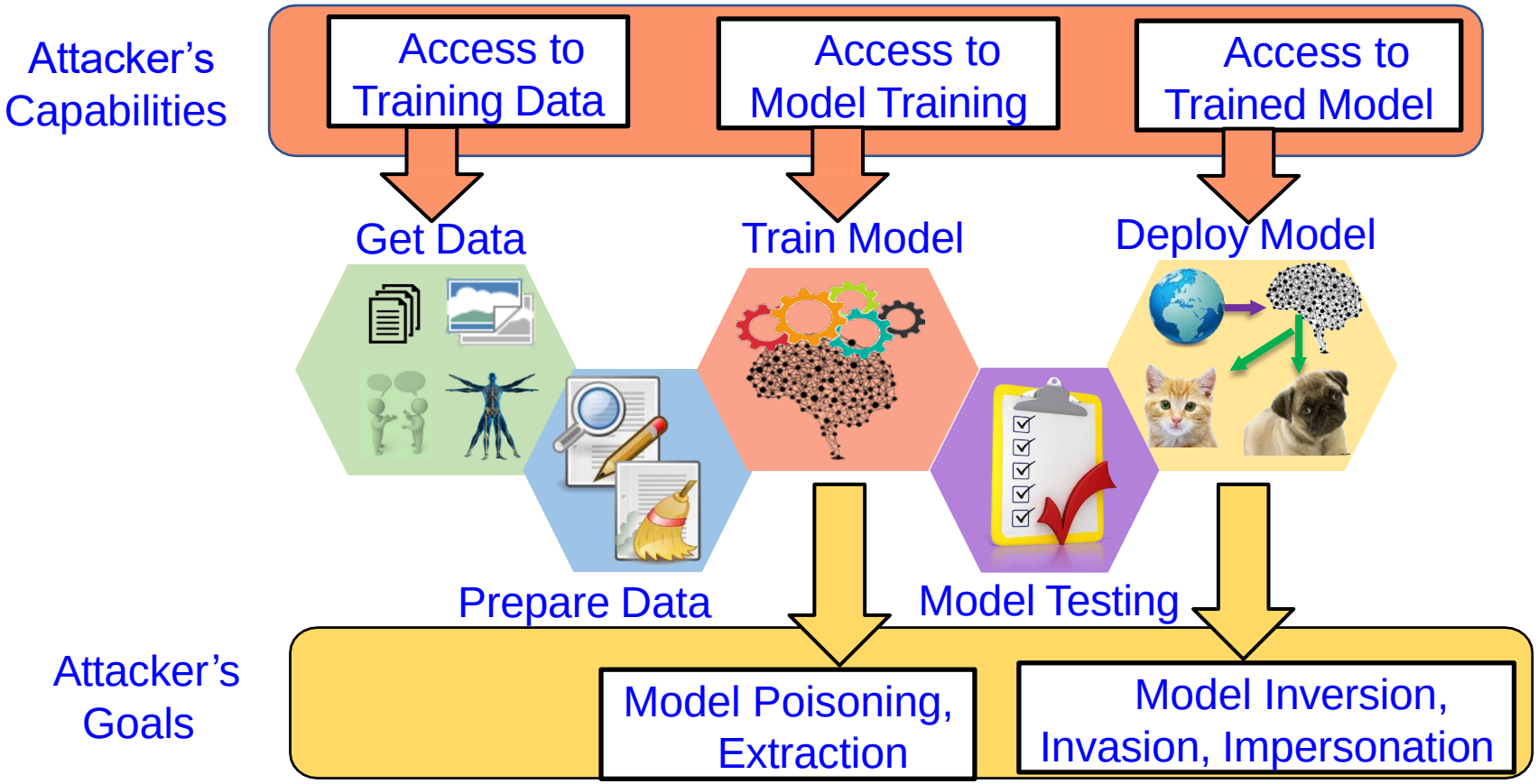
Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Source: Petit 2015: IEEE-TITS Apr 2015

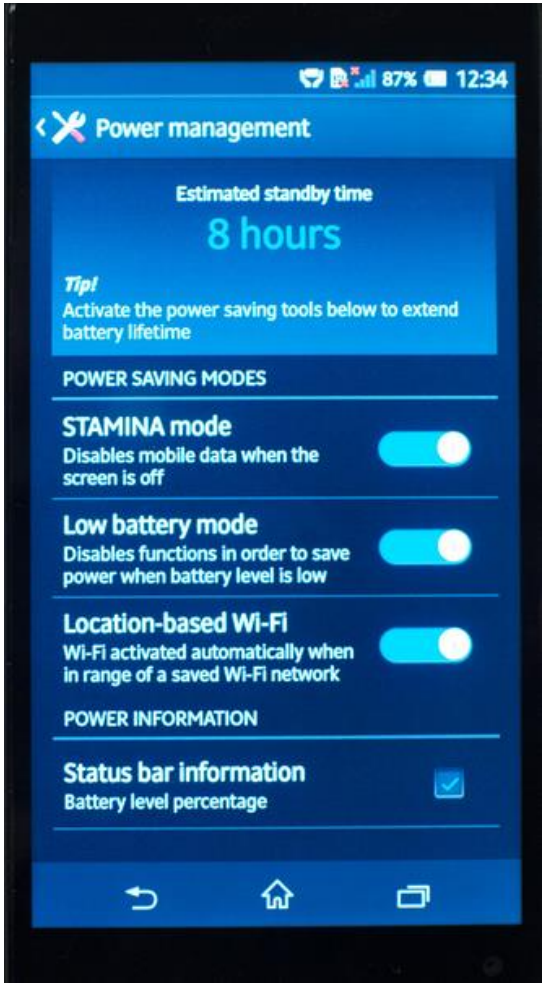
AI Security and Privacy Concerns



Source: Sandip Kundu ISVLSI 2019 Keynote.

Selected Energy Solutions

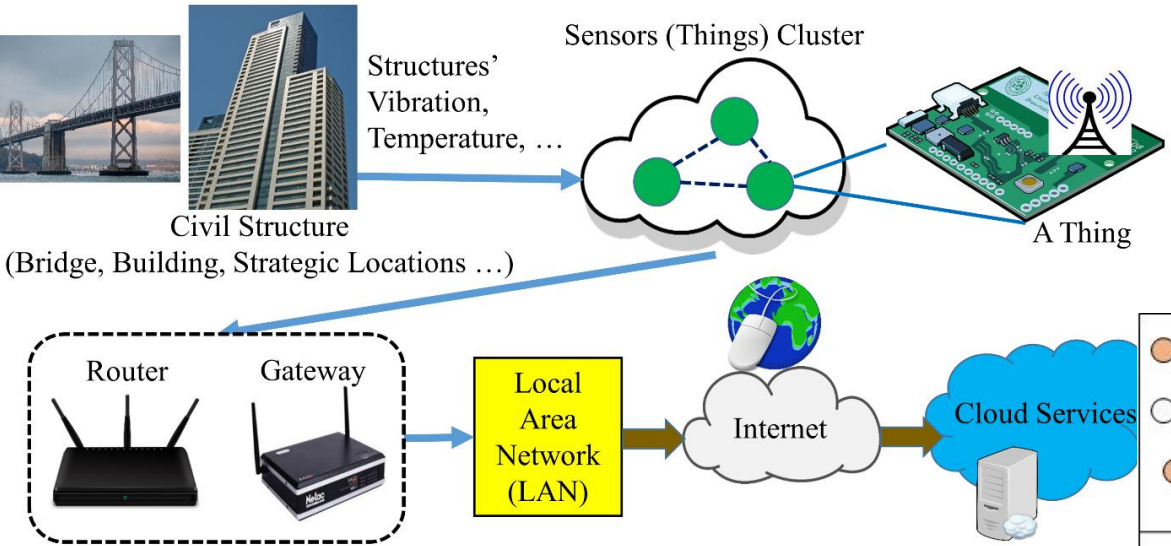
Smart Energy – Smart Consumption

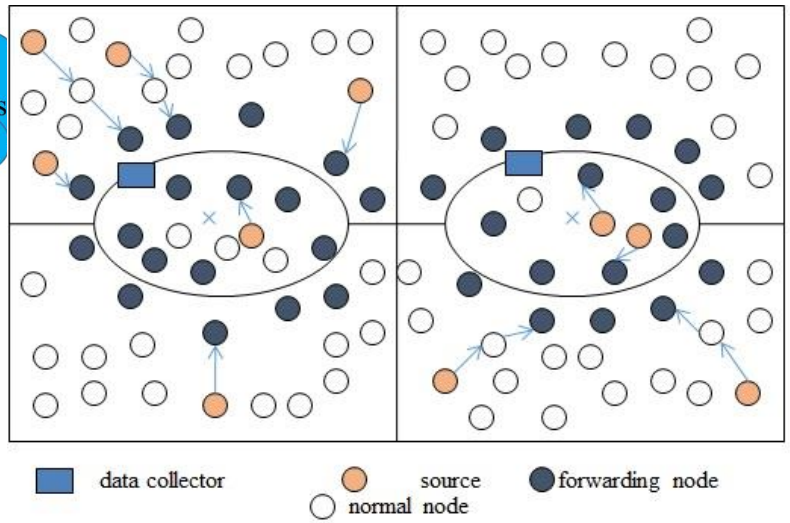


Battery Saver

Smart Home

Sustainable IoT - Low-Power Sensors and Efficient Routing

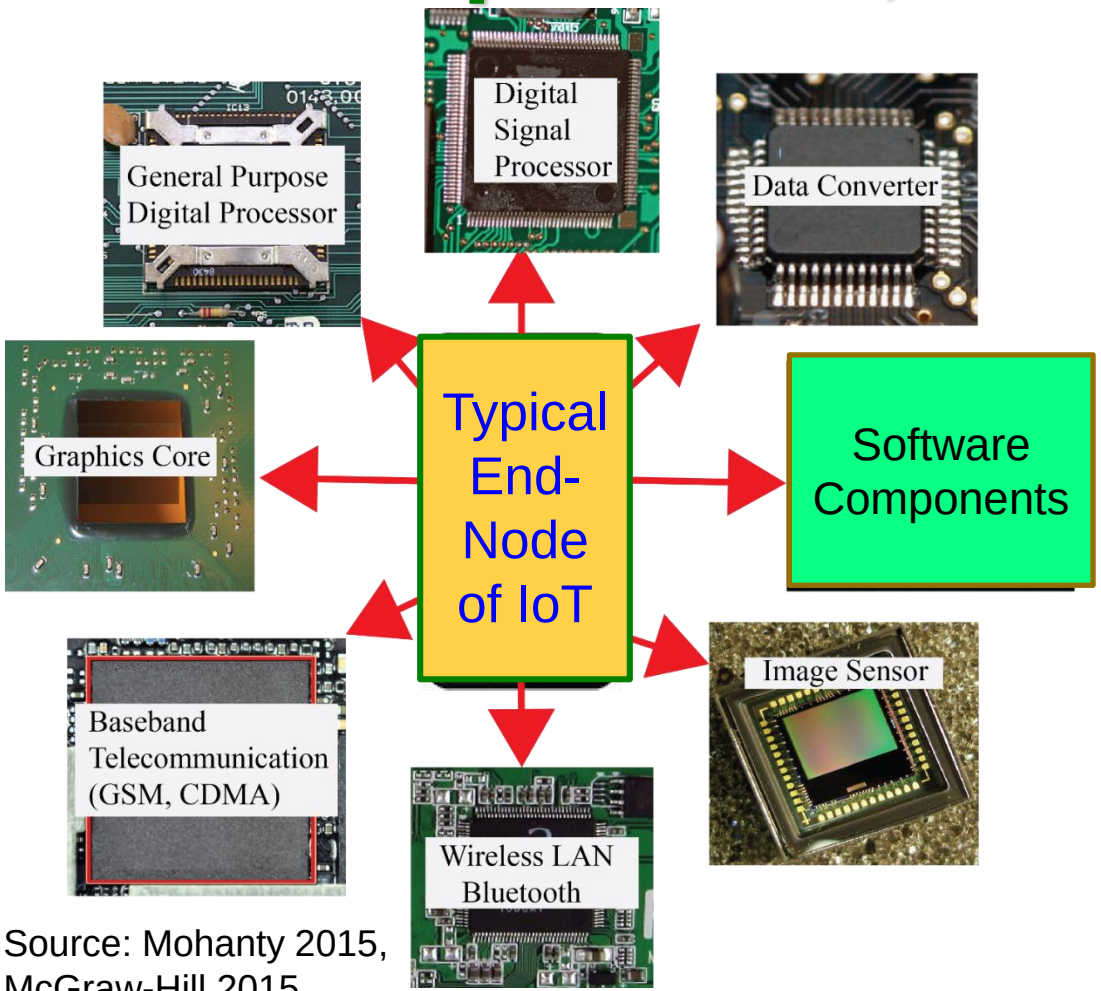




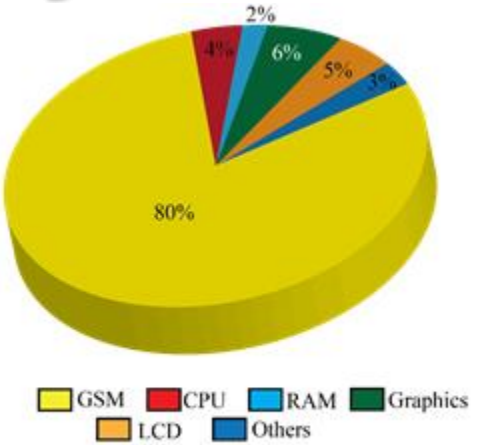
- IoT - sensors near the data collector drain energy faster than other nodes.
- Solution Idea - Mobile sink in which the network is balanced with node energy consumption.
- Solution Need: New data routing to forward data towards base station using mobile data collector, in which two data collectors follow a predefined path.

Source: S. S. Roy, D. Puthal, S. Sharma, S. P. Mohanty, and A. Y. Zomaya, "Building a Sustainable Internet of Things", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 2, March 2018, pp. 42--49.

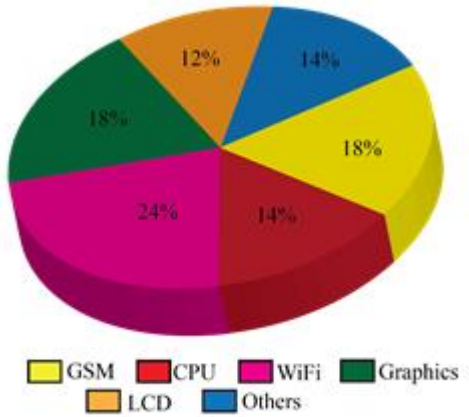
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015

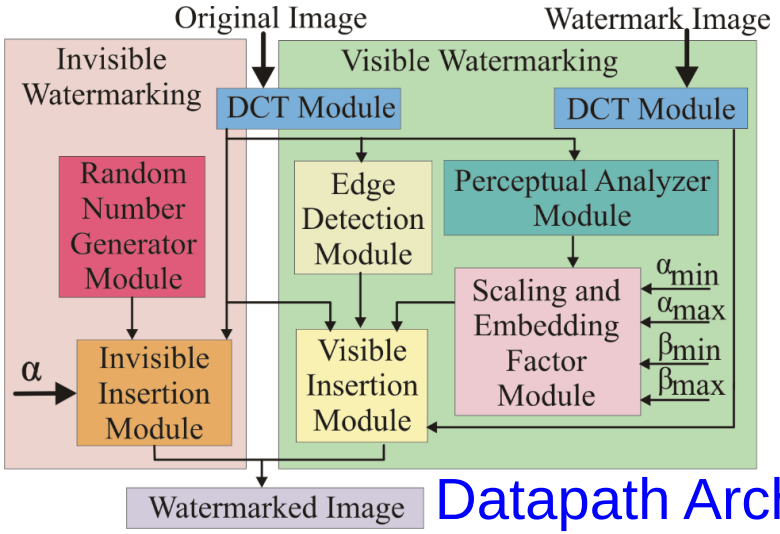


During GSM Communications

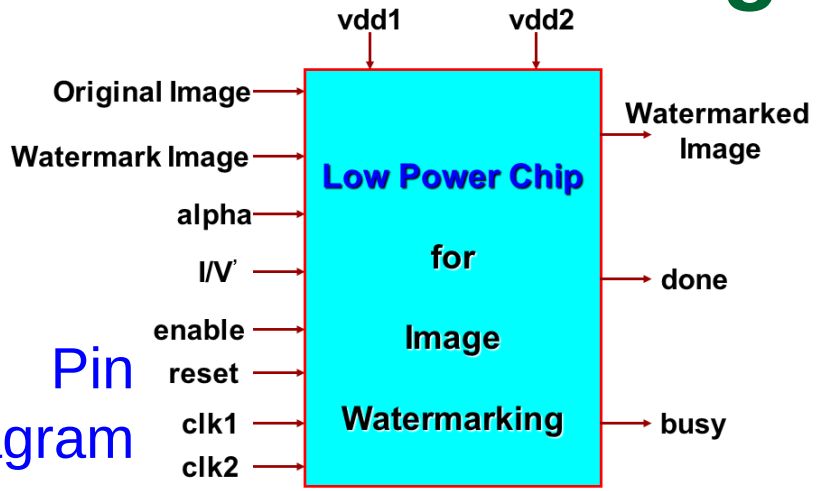


During WiFi Communications

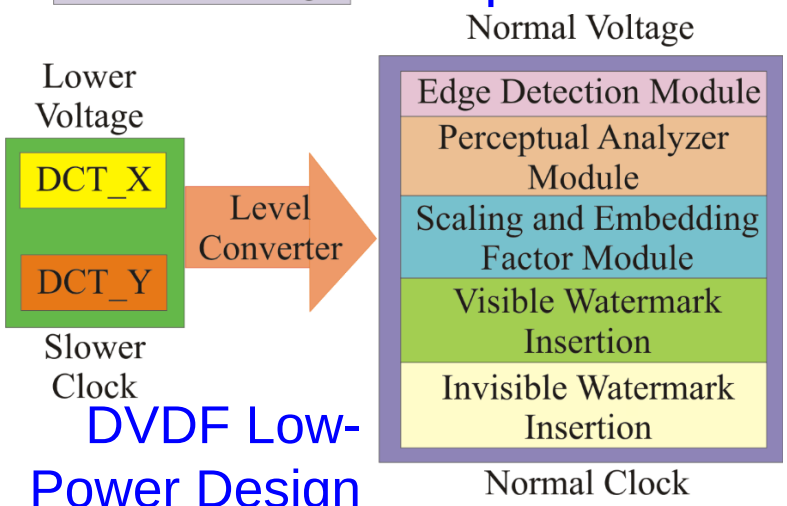
Energy-Efficient Hardware - Dual-Voltage



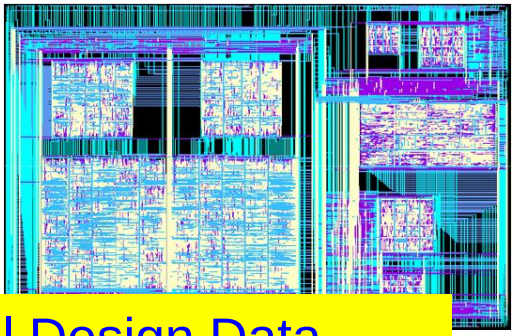
Datapath Architecture



Pin Diagram



DVDF Low-Power Design



Hardware Layout

Physical Design Data
Total Area : 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

Source: S. P. Mohanty, N. Ranganathan, and K. Balakrishnan, "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain", *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.

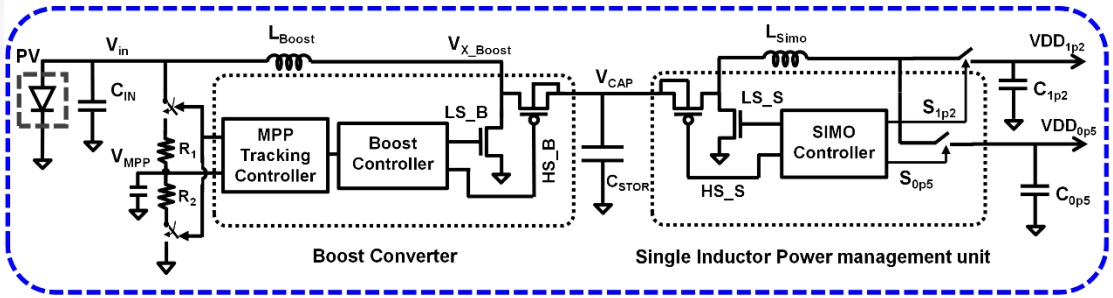
Battery-Less IoT

Battery less operations can lead to reduction of size and weight of the edge devices.

Source: http://newscenter.ti.com/2015-02-25-TI-makes-battery-less-IoT-connectivity-possible-with-the-industrys-first-multi-standard-wireless-microcontroller-platform

Batter-Less SoC

Source: https://www.technologyreview.com/s/529206/a-batteryless-sensor-chip-for-the-internet-of-things/

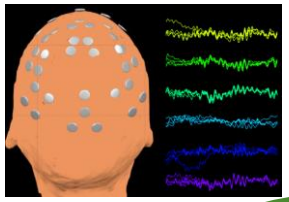


Energy Harvesting and Power Management

Source: http://rlpvlsi.ece.virginia.edu/node/368

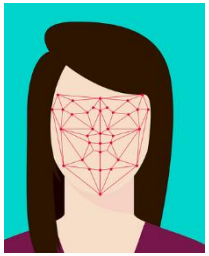
Selected Security Solutions

Security, Authentication, Access Control – Home, Facilities, ...



Finger Vein

Facial Recognition



Fingerprint

Electroence phalography (EEG)

Security Methods (Authentication)

Personal Identification Number (PIN)

Electrocar diography (ECG)

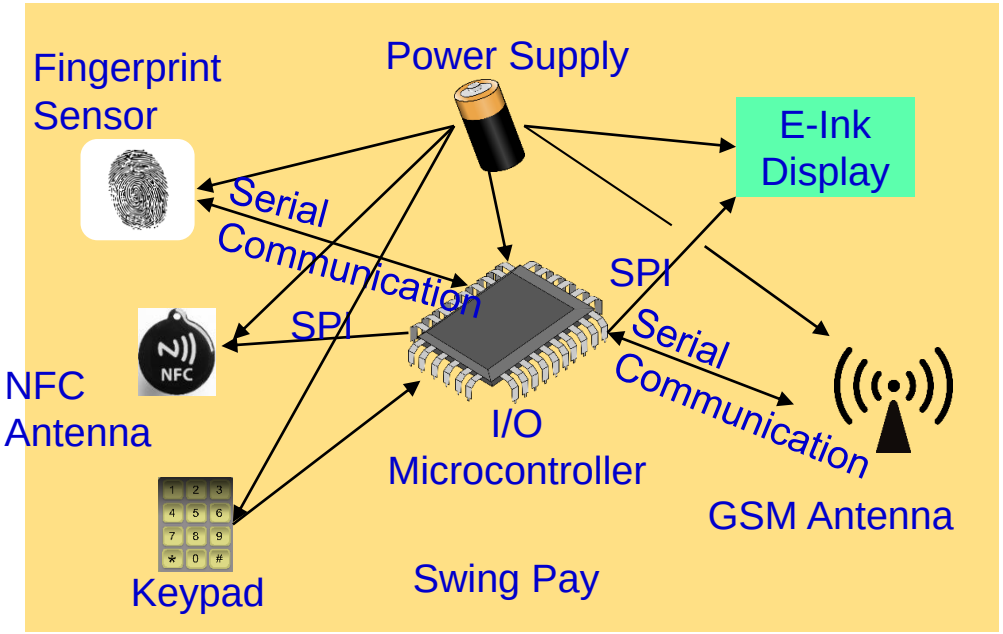
Password

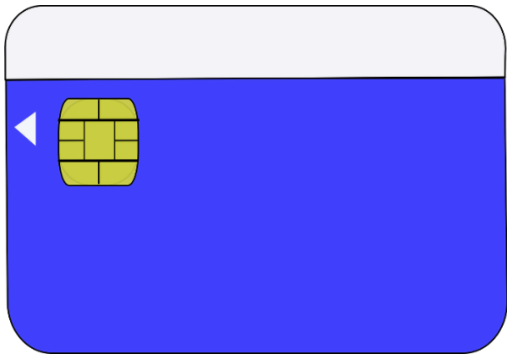
Online Signature

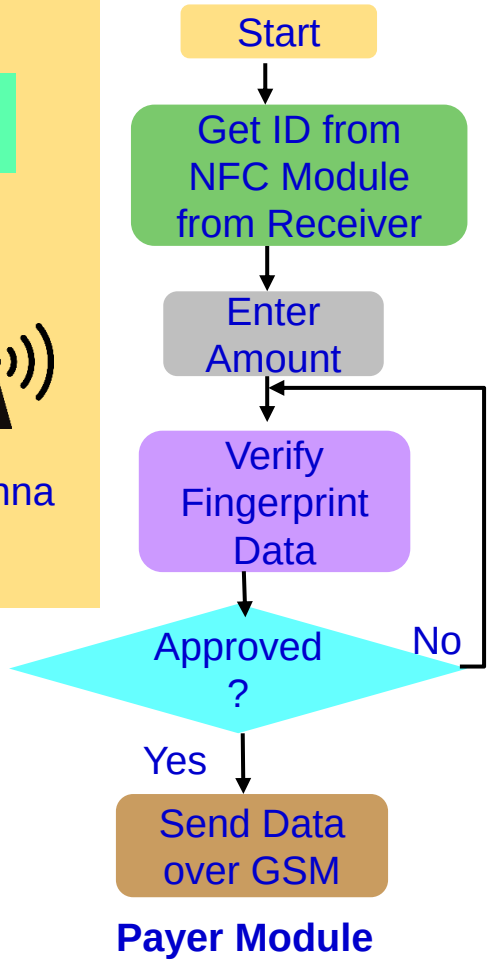
Touch-Screen Pattern

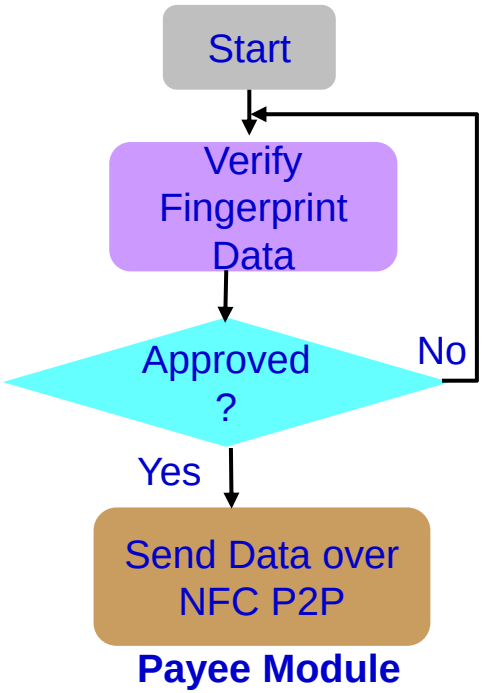
Source: Mohanty ISCT 2019 Keynote

NFC Security - Solution





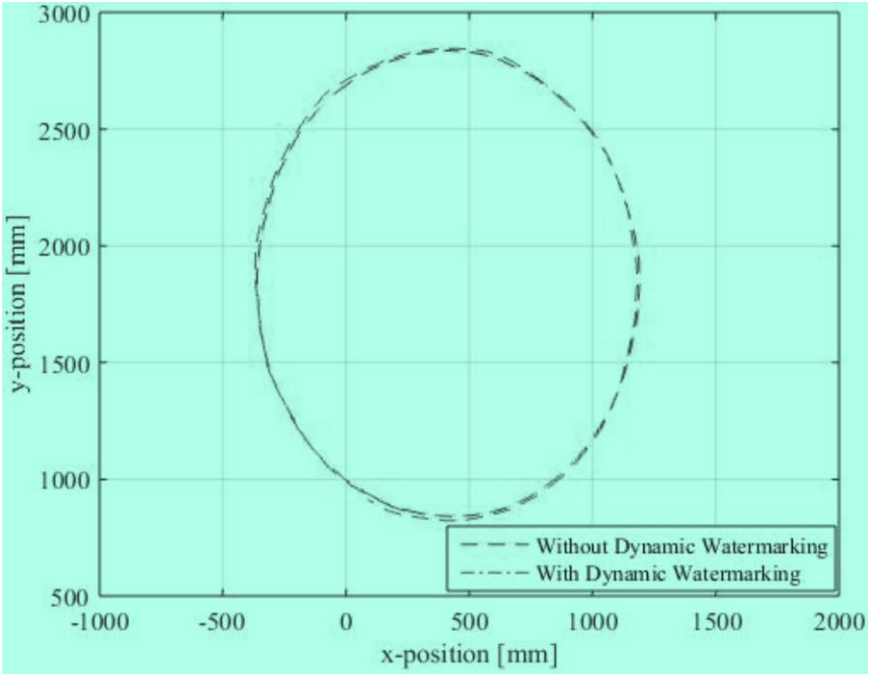




Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", IEEE Consumer Electronics Magazine (CEM), Volume 6, Issue 1, January 2017, pp. 82--93.

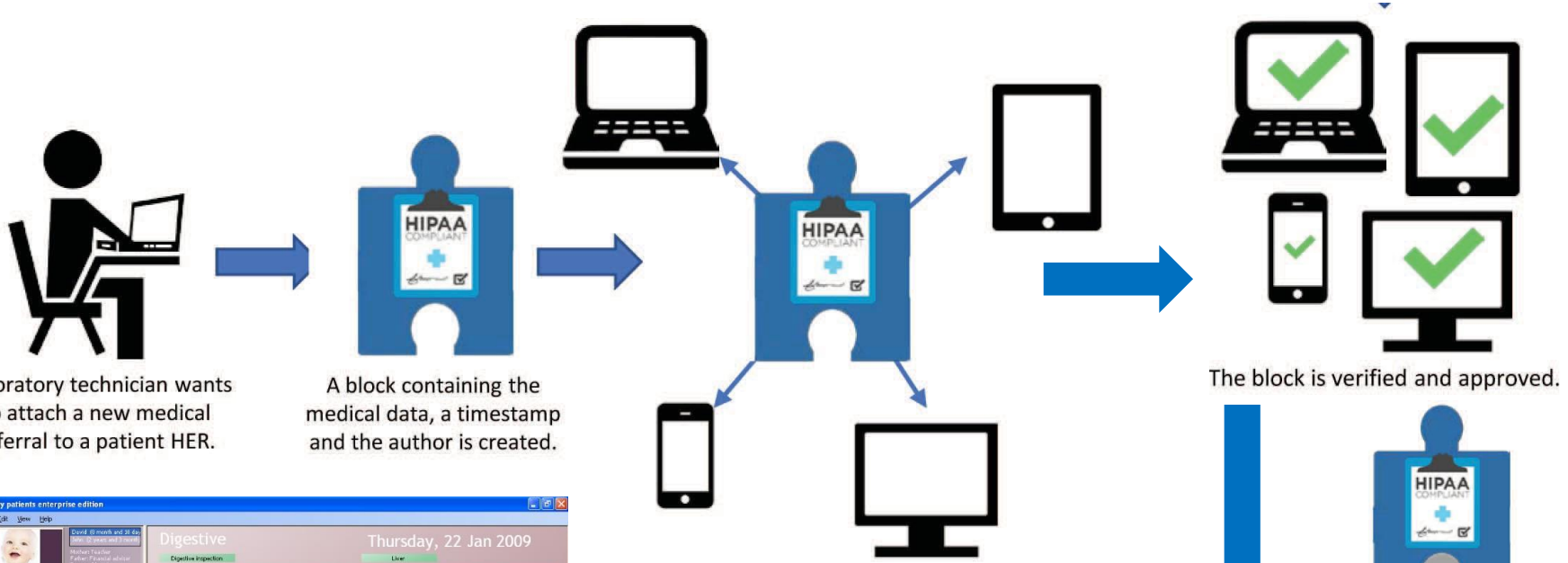
Autonomous Car Security – Collision Avoidance

- Attack: Feeding of malicious sensor measurements to the control and the collision avoidance module. Such an attack on a position sensor can result in collisions between the vehicles.
- Solutions: "**Dynamic Watermarking**" of signals to detect and stop such attacks on cyber-physical systems.
- Idea: Superimpose each actuator *i* a random signal $e_i[t]$ (watermark) on control policy-specified input.



Source: Ko 2016, CPS-Sec 2016

Smart Healthcare – Data Protection



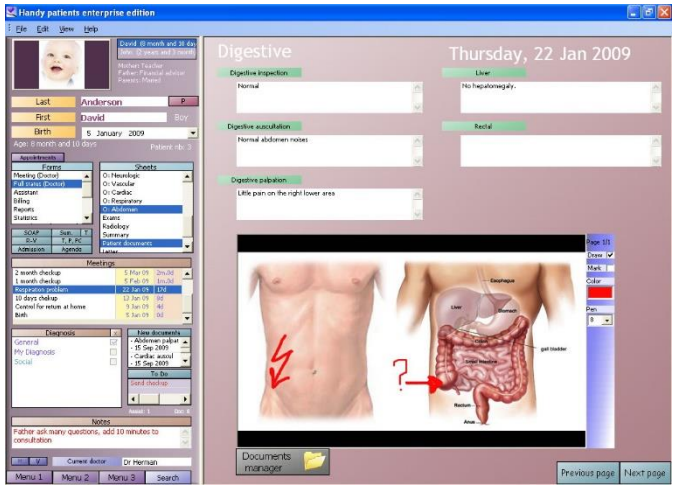
Laboratory technician wants to attach a new medical referral to a patient HER.

A block containing the medical data, a timestamp and the author is created.

The block is delivered to all the peers in the patient's network, such as the patient itself, his/her family members, and general practitioner.

The block is verified and approved.

The block is inserted in the chain and linked with the previous blocks.



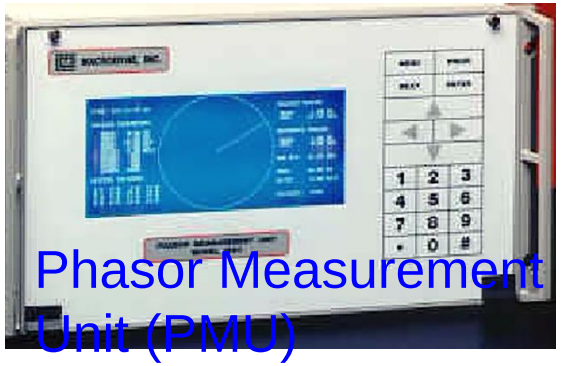
Source: C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.

Smart Grid Security - Solutions

Smart Grid – Security Solutions

- Network Security
- Data Security
- Key Management
- Network Security Protocol

Smart Meter


Phasor Measurement Unit (PMU)

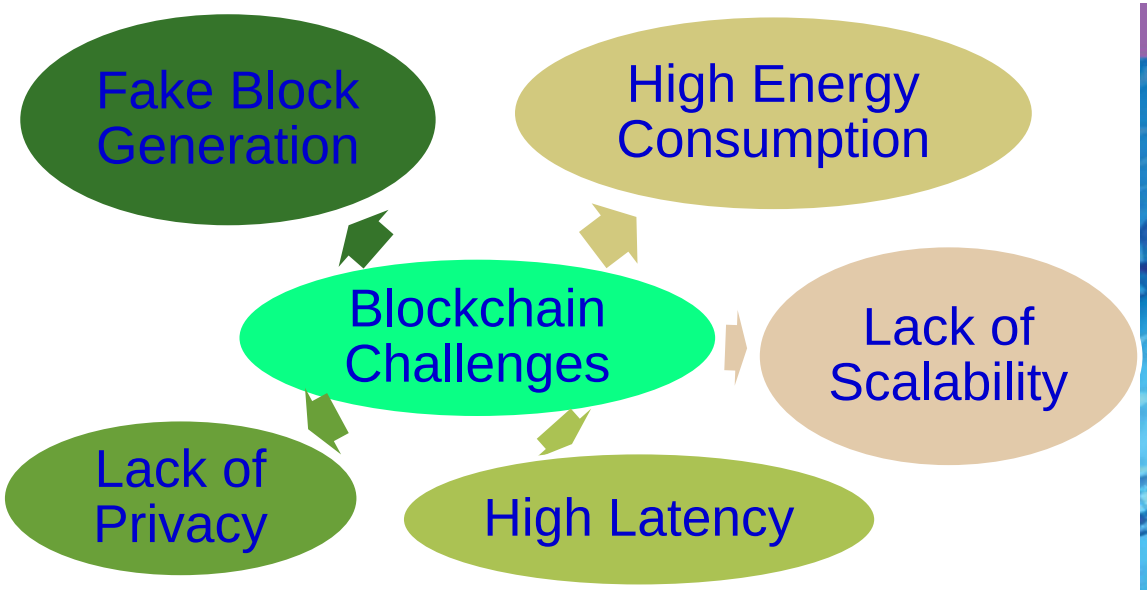
Smart Grid Cybersecurity - Strategies

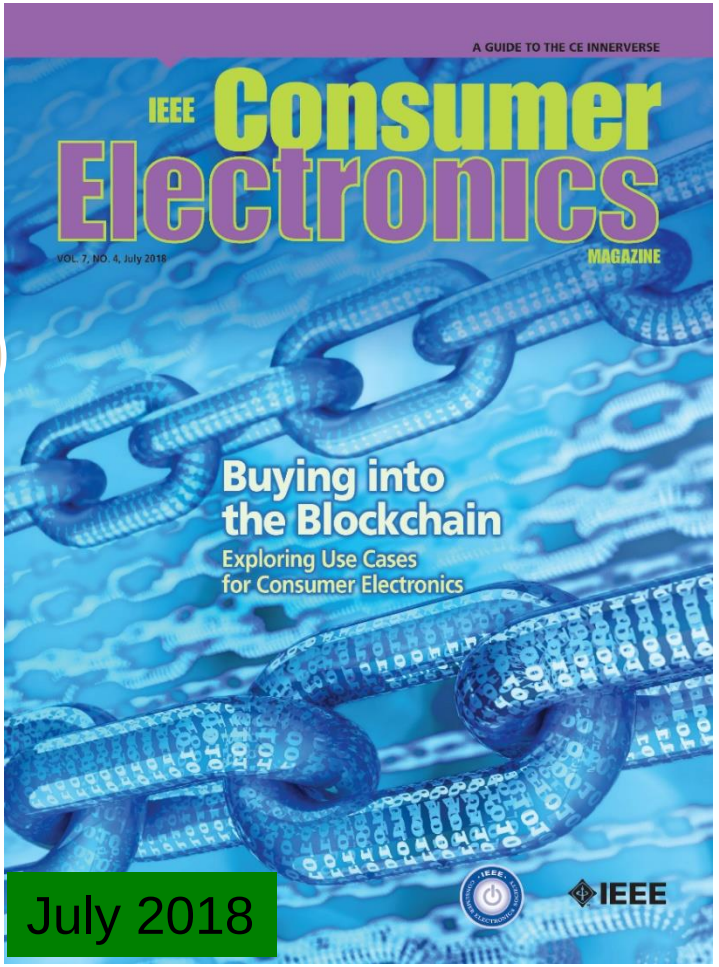
- Make Smart Grids Survivable
- Use Scalable Security Measures
- Integrate Security and Privacy by Design
- Deploy a Defense-in-Depth Approach
- Enhance Traditional Security Measures

Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids", *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

Blockchain a Solution for Everything?

Blockchain - Challenges

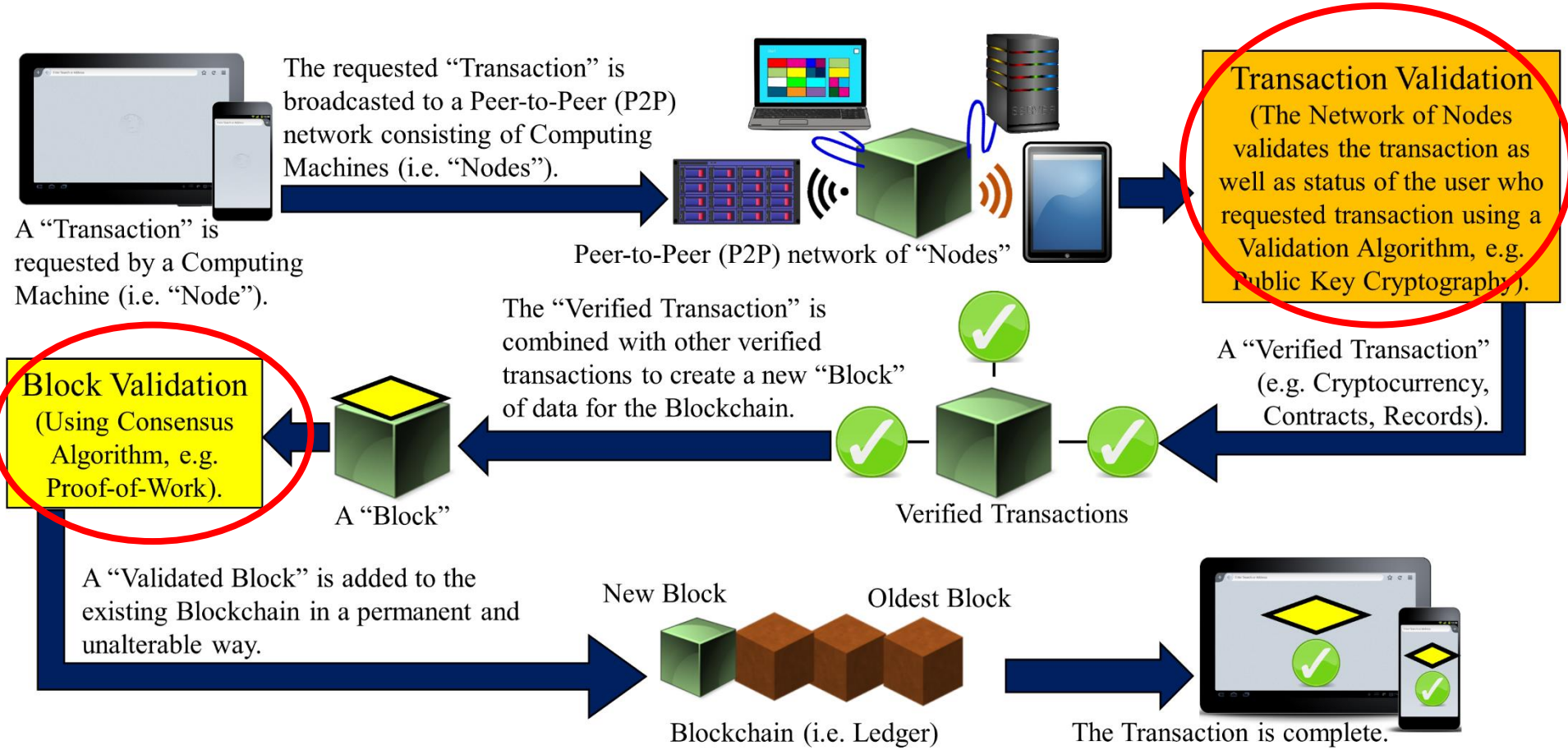




- Energy for mining of 1 bitcoin → 2 years consumption of a US household.
- Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing.

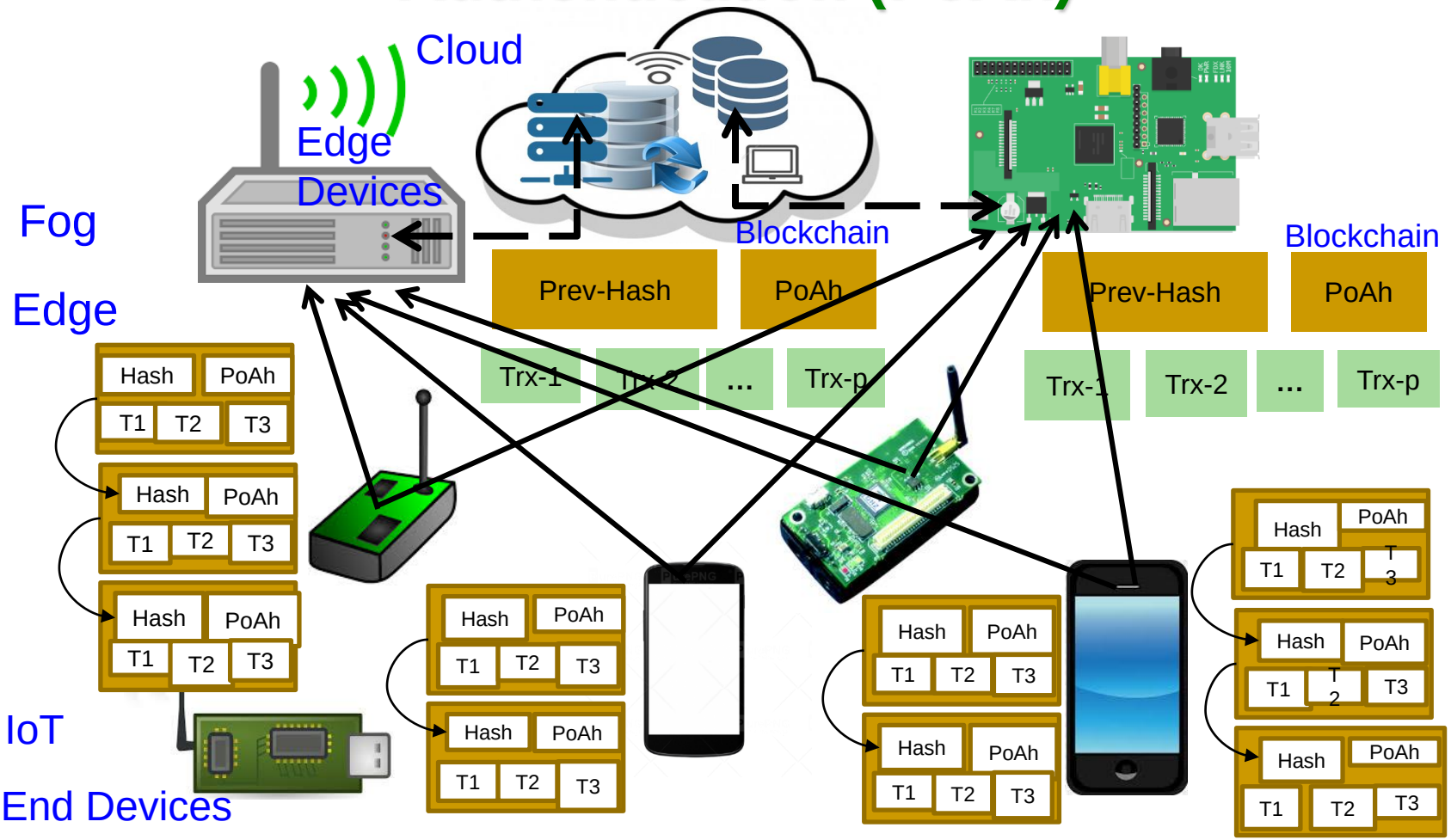
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Technology



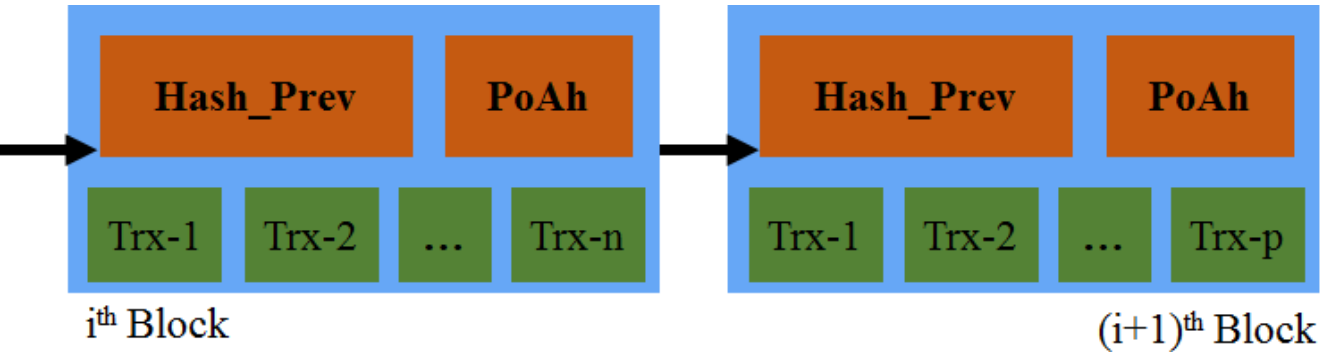
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

IoT Friendly Blockchain - Proof-of-Authentication (PoAh)



Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Volume 38, Issue 1, January 2019, pp. 26--29.

IoT Friendly Blockchain - Proof-of-Authentication (PoAh)



Eliminates cryptographic "puzzle" solving to validate blocks.

	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

PoW - 10 min in cloud | **PoAh - 3 sec in Rasperry Pi** | **PoAh - 200X faster than PoW**

Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in Proc. 37th IEEE International Conference on Consumer Electronics (ICCE), 2019.

Cryptocurrency Comparison

	Bitcoin	Dash	Monero	Verge	PIVX	Zcash
Origin	-	Bitcoin	Bytecoin	Bitcoin	Dash	Bitcoin
Release	January 2009	January 2014	April 2014	October 2014	February 2016	October 2016
Consensus Algorithm	PoW	PoW	PoW	PoW	PoS	PoW
Hardware Mineable	Yes	Yes	Yes	Yes	No	Yes
Block Time	600 sec.	150 sec.	120 sec.	30 sec.	60 sec.	150 sec.
Rich List	Yes	Yes	No	Yes	Yes	No
Master Node	No	Yes	No	No	Yes	No
Sender Address Hidden	No	Yes	Yes	No	Yes	Yes
Receiver Address Hidden	No	Yes	Yes	No	Yes	Yes
Sent Amount Hidden	No	No	Yes	No	No	Yes
IP Addresses Hidden	No	No	No	Yes	No	No
Privacy	No	No	Yes	No	No	Yes
Untraceability	No	No	Yes	No	No	Yes
Fungibility	No	No	Yes	No	No	Yes

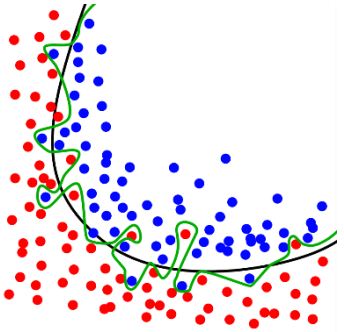
Source: J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019.

How Intelligent is Artificial Intelligence (AI)?

ML Modeling Issues

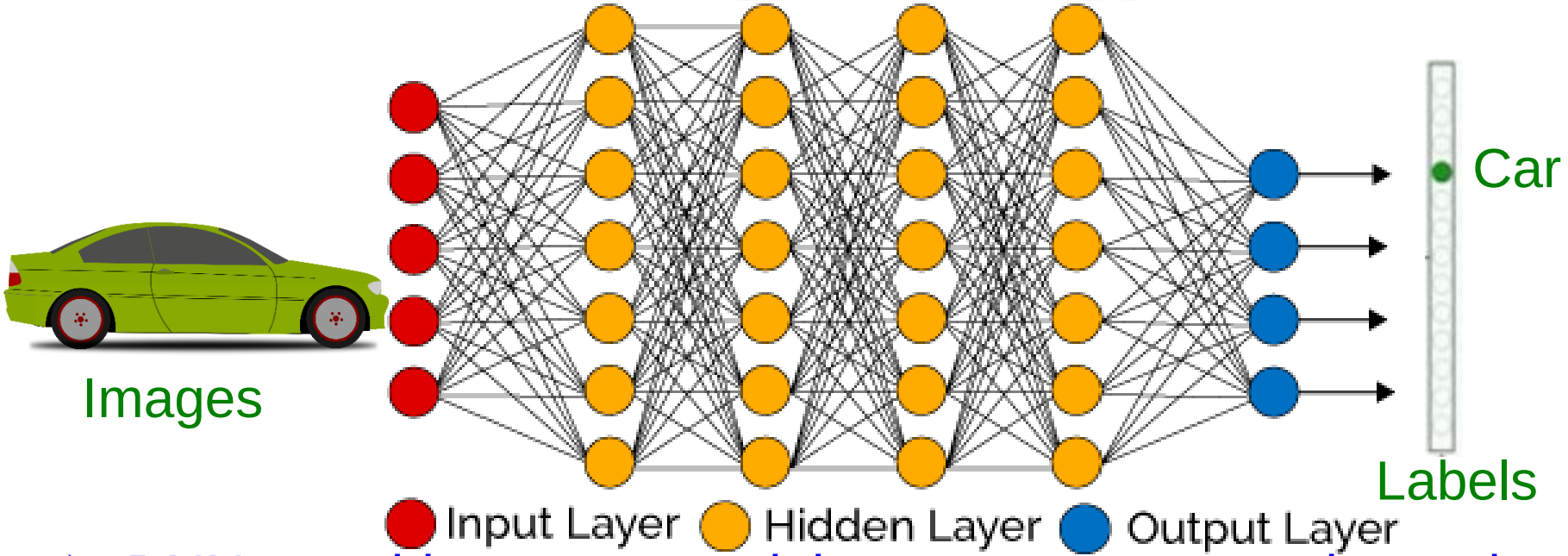
Machine Learning Issues

- High Energy Requirements
- High Computational Resource Requirements
- Large Amount of Data Requirements
- Underfitting/Overfitting Issue
- Class Imbalance Issue
- Fake Data Issue



Source: Mohanty ISCT Keynote 2019

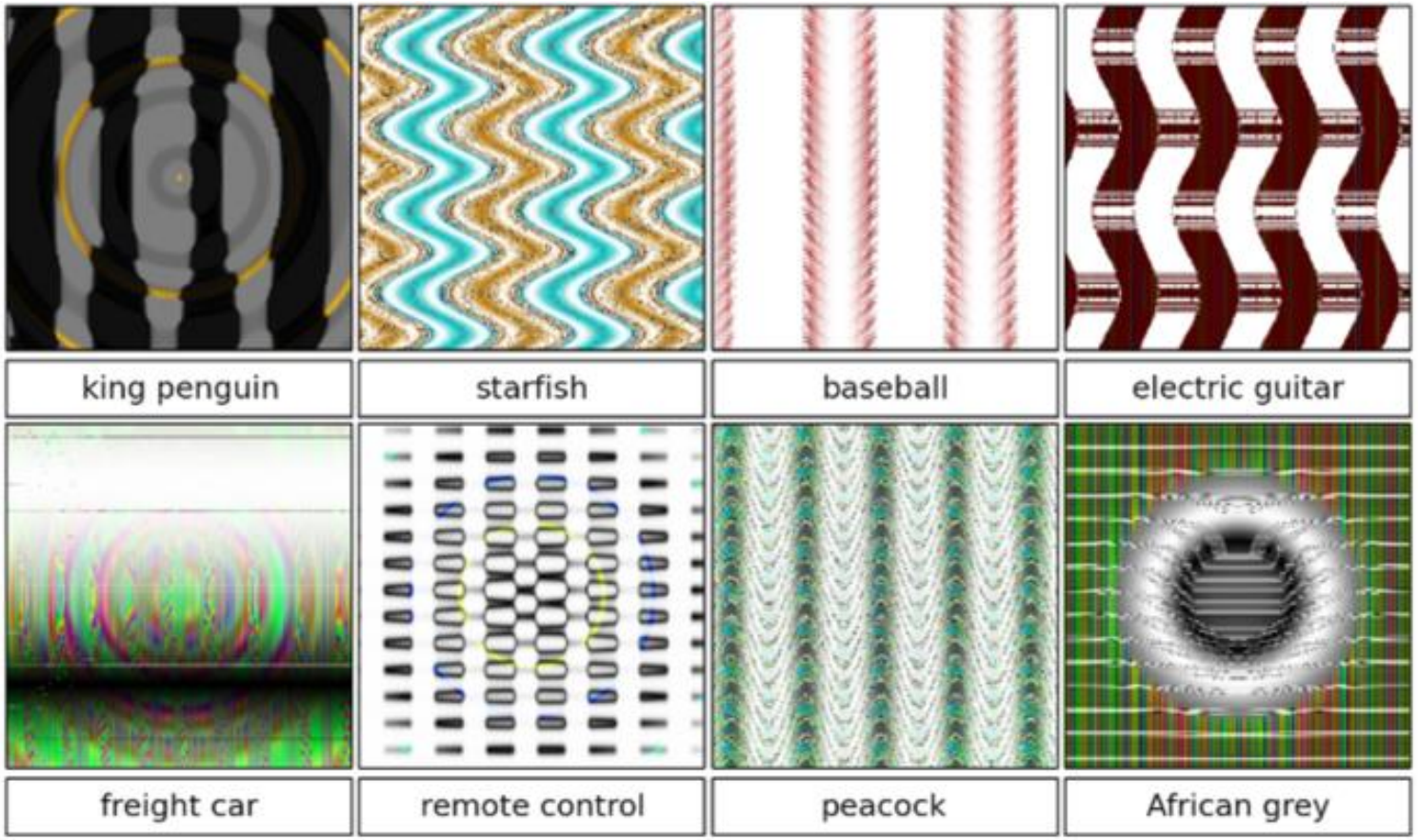
DNN Training - Energy Issue



- DNN considers many training parameters, such as the size, the learning rate, and initial weights.
- High computational resource and time: For sweeping through the parameter space for optimal parameters.
- DNN needs: Multicore processors and batch processing.
- DNN training happens mostly in cloud not at edge or fog.

Source: Mohanty iSES 2018 Keynote

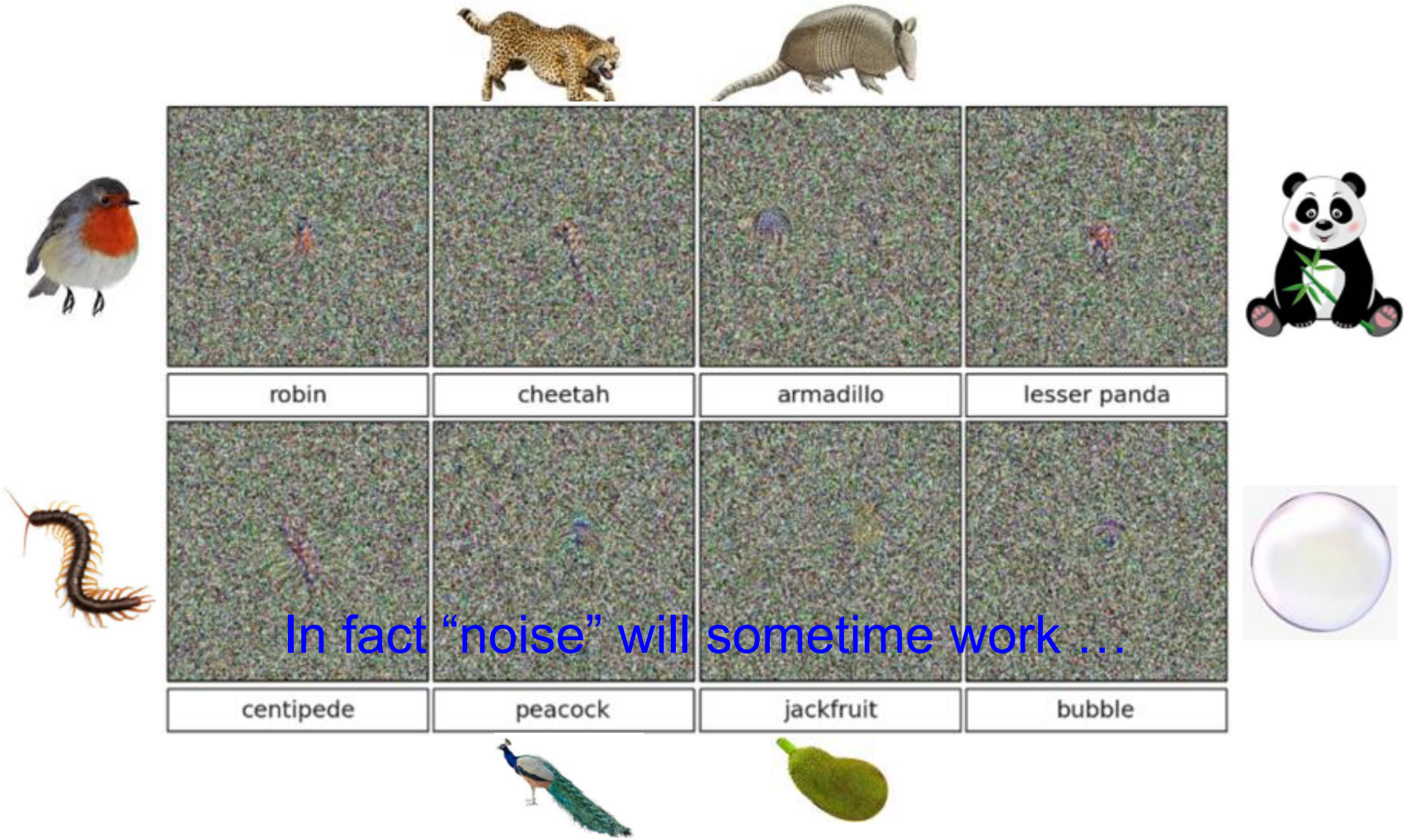
DNNs – Fooled by Learned Adversarial Patterns



DNNs can be fooled by certain “learned” (Adversarial) patterns …

Source: A. Nguyen, J. Yosinski and J. Clune, "Deep neural networks are easily fooled: High confidence predictions for unrecognizable images," in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 427-436.

DNNs – Noise can Work

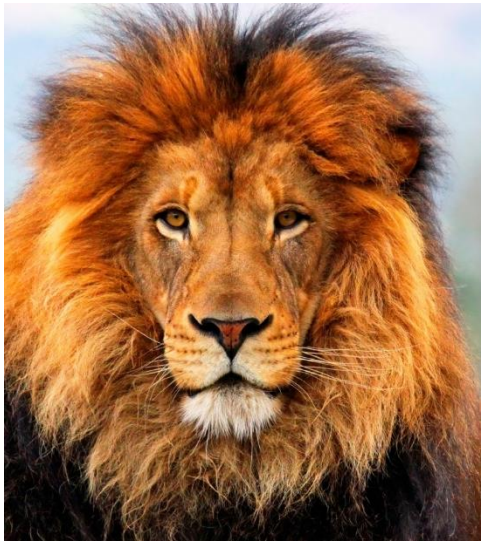


Source: A. Nguyen, J. Yosinski and J. Clune, "Deep neural networks are easily fooled: High confidence predictions for unrecognizable images," in Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 427-436.

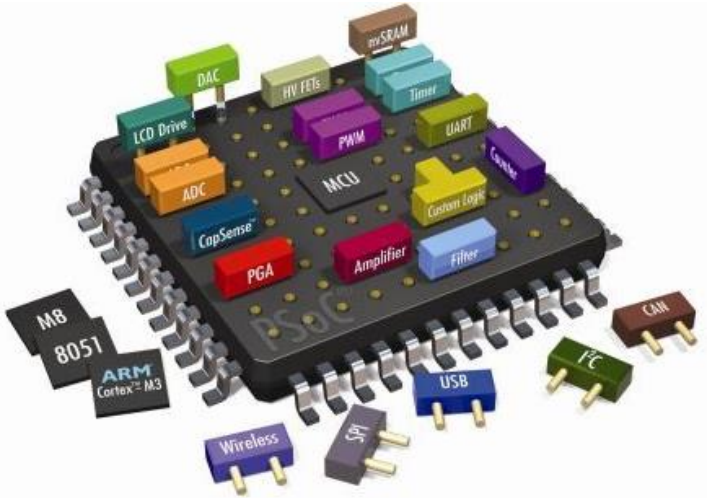
DNNs – Can be Fooled by Fake Data?

- Why not use Fake Data?
- "Fake Data" has some interesting advantages:
  - Avoids *privacy issues* and side-steps *new regulations* (e.g. General Data Protection Regulation or GDPR)
  - Significant cost reductions in data acquisition and annotation for big datasets

Source: Corcoran Keynote 2018



Software or Hardware based Solutions for Security?



Attacks - Software Vs Hardware

Software Based

- Software attacks via communication channels
- Typically from remote
- More frequent
- Selected Software based:
  - Denial-of-Service (DoS)
  - Routing Attacks
  - Malicious Injection
  - Injection of fraudulent packets
  - Snooping attack of memory
  - Spoofing attack of memory and IP address
  - Password-based attacks

Hardware Based

- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
  - Hardware backdoors (e.g. Trojan)
  - Inducing faults
  - CE system tampering/jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - CE hardware counterfeiting

Source: Mohanty ICCE Panel 2018

Security - Software Vs Hardware

Software Based

- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can't stop hardware reverse engineering

Hardware Based

- High-Speed operation
- Energy-Efficient operation
- Low-cost using ASIC and FPGA
- Tasks of encryption easy compared to software – bit permutation
- Easy integration in CE systems
- Possible security at source-end like sensors, better suitable for IoT
- Susceptible to side-channel attacks
- Can't stop software reverse engineering

Maintaining of Security of Consumer Electronics, CE Systems, IoT, CPS, etc. needs Energy and affects performance.

Hardware Assisted Security

- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
  - Software based security approaches that rely on some form of encryption can't be full proof as breaking them is just matter of time.
  - It is projected that quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security: Security/Protection provided by the hardware: for information being processed by a CE system, for hardware itself, and/or for the CE system.

Hardware Assisted Security

- Hardware-Assisted Security: Security provided by hardware for:
  - (1) information being processed,
  - (2) hardware itself,
  - (3) overall system

Privacy by Design (PbD)

Security/Secure by Design (SbD)

- Additional hardware components used for security.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

IR Hardware Security

Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

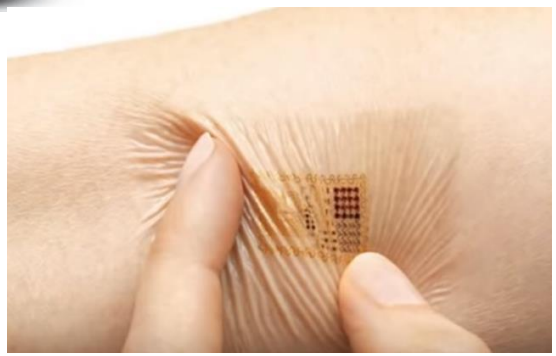
Wearable Medical Devices (WMDs)

Fitness Trackers

Headband with Embedded Neurosensors

Source: https://www.empatica.com/embrace2/

Smart watch to detect seizure



Embedded Skin Patch

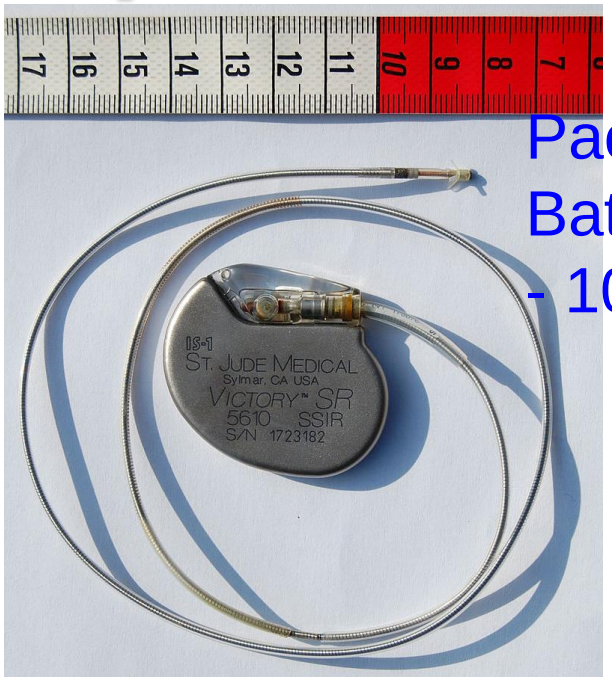
Source: http://www.sciencetimes.com/articles/8087/20160107/ces-loreals-smart-skin-patch-reveals-long-exposed-sun.htm

Wearable Medical Devices (WMDs)
→ Battery Constrained

Insulin Pump

Source: https://www.webmd.com

Implantable Medical Devices (IMDs)



Pacemaker
Battery Life
- 10 years

Neurostimulator
Battery Life
- 8 years

- Implantable Medical Devices (IMDs) have integrated battery to provide energy to all their functions → Limited Battery Life depending on functions
- Higher battery/energy usage → Lower IMD lifetime
- Battery/IMD replacement → Needs surgical risky procedures

Source: Carmen Camara, PedroPeris-Lopeza, and Juan E.Tapiadora, "Security and privacy issues in implantable medical devices: A comprehensive survey", Elsevier Journal of Biomedical Informatics, Volume 55, June 2015, Pages 272-289.

Smart Car Security - Latency Constrained

Protecting Communications
Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

Over The Air (OTA) Management
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

Protecting Each Module
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

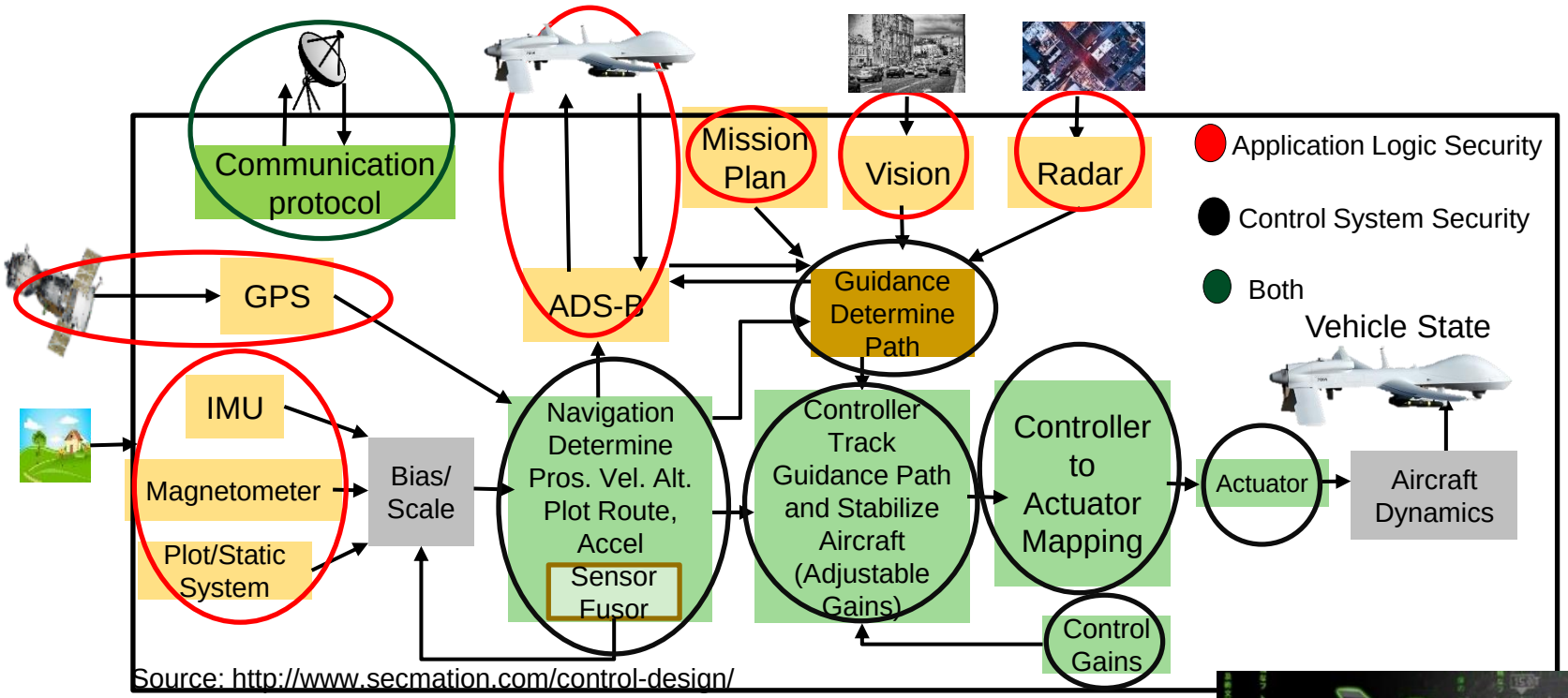
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Security – Latency Constraints

Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

UAV Security - Energy & Latency Constrained



Source: http://www.secmation.com/control-design/

Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Smart Grid Security Constraints

Smart Grid – Security Objectives

- Availability
- Integrity
- Confidentiality

Smart Grid – Security Requirements

- Identification
- Authentication
- Authorization
- Trust
- Access Control
- Privacy

Smart Grid – Security Solution Constraints

- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

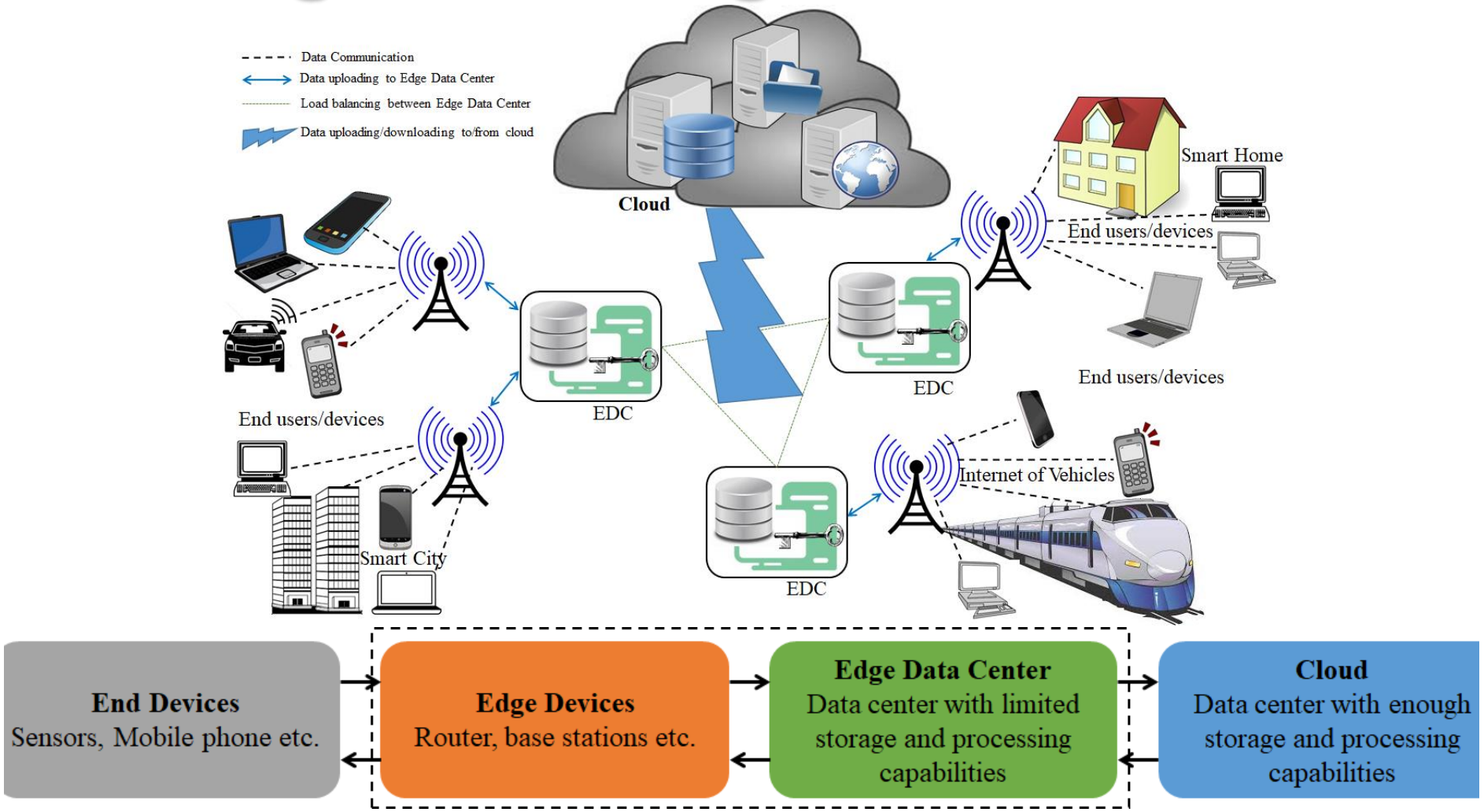
Source: R. K. Pandey and M. Misra, "Cyber security threats - Smart grid infrastructure," 2016 National Power Systems Conference (NPSC), 2016, pp. 1-6.

Where and How to Compute?

Sensor, Edge, Fog, Cloud?

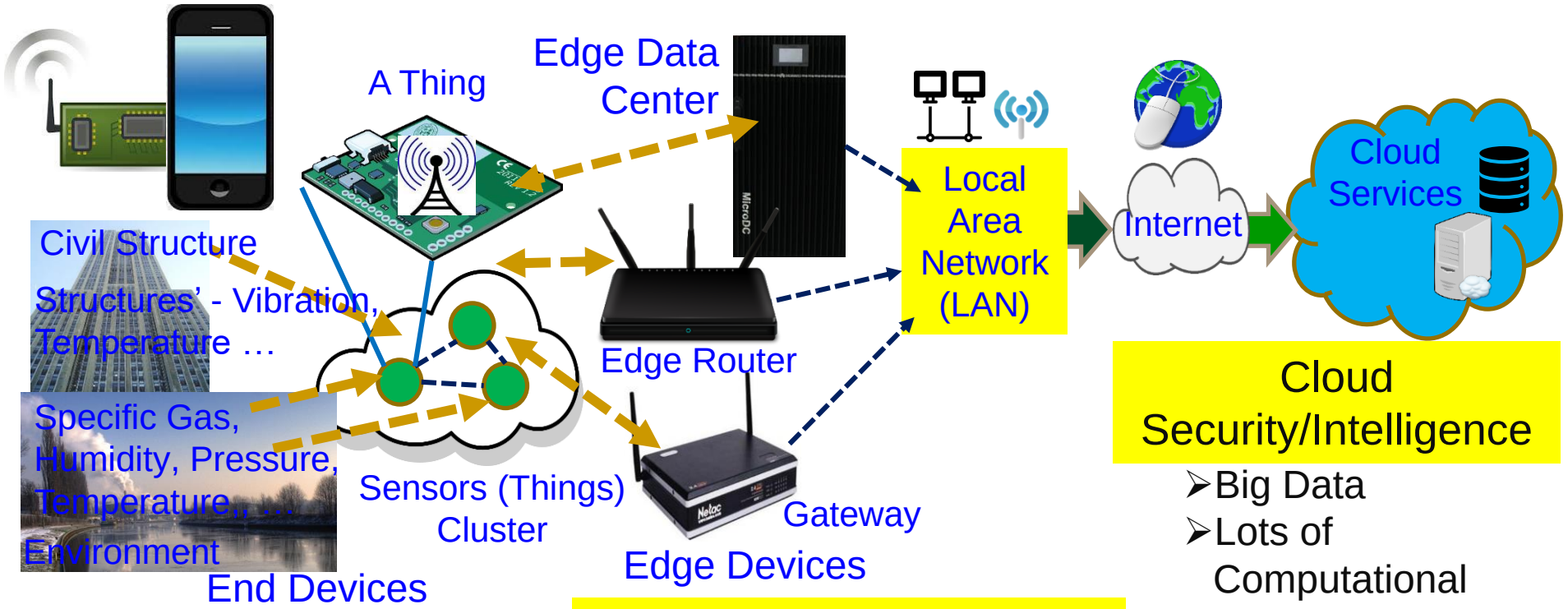
ASIC, FGPA, SoC, FP-SoC, GPU, Neuromorphic, Quantum?

Big Data - Edge Datacenter



Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing", IEEE Communications Magazine, Volume 56, Issue 5, May 2018, pp. 60--65.

End, Edge Vs Cloud Security, Intelligence …



End Security/Intelligence

- Minimal Data
- Minimal Computational Resource
- Least Accurate Data Analytics
- Very Rapid Response

Edge Security/Intelligence

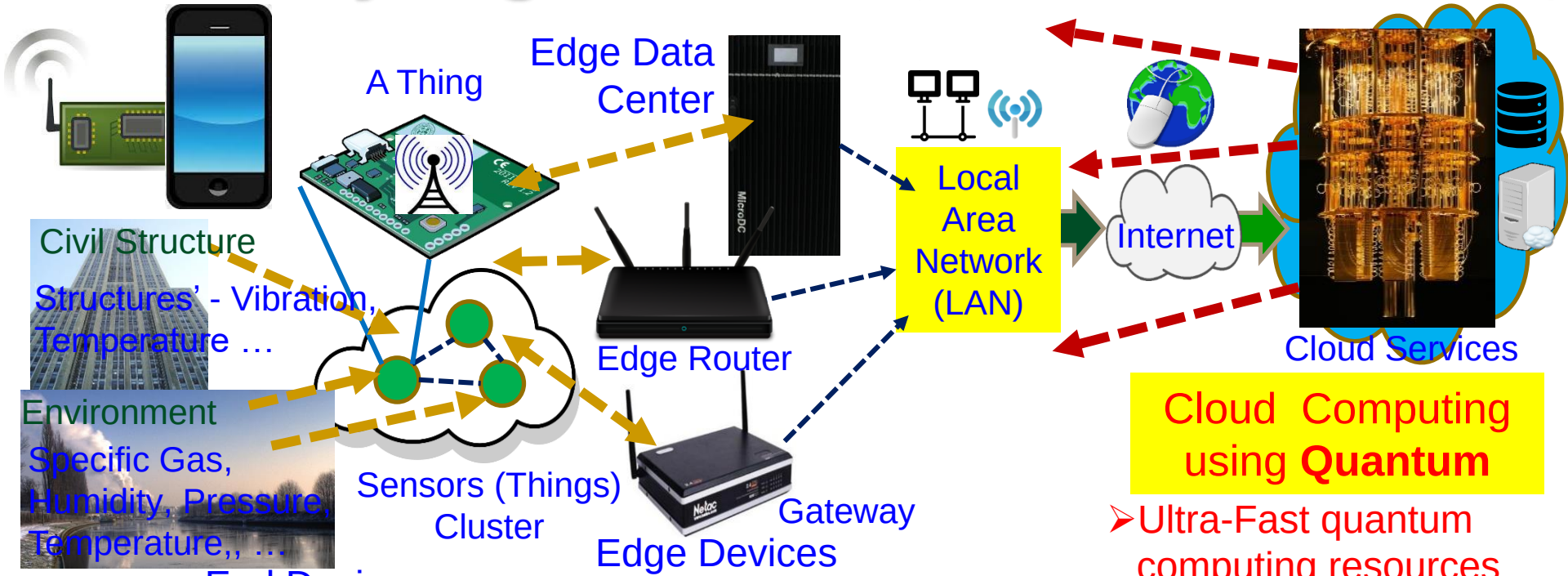
- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

Cloud Security/Intelligence

- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy overhead in Communications

Source: Mohanty iSES Keynote 2018 and ICCE 2019 Panel

A Security Nightmare - by Quantum Computing



In-Sensor/End-Device Computing

- Minimal computational resource
- Negligible latency in network
- Very lightweight security

Edge Computing

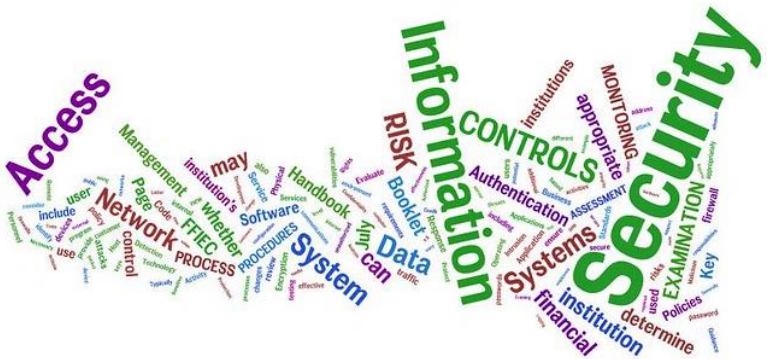
- Less computational resource
- Minimal latency in network
- Lightweight security

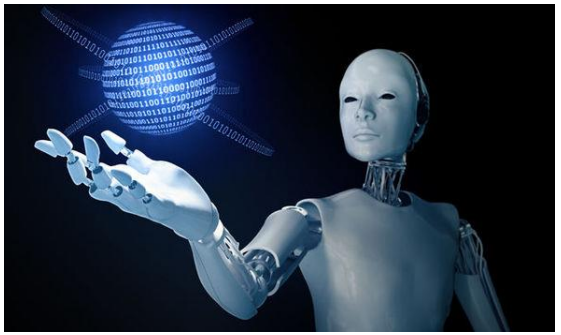
Cloud Computing using **Quantum**

- Ultra-Fast quantum computing resources
- High latency in network
- Breaks every encryption in no time

A quantum computer could break a 2048-bit RSA encryption in 8 hours.

Security, Energy-Efficiency, AI Together?





ESR-Smart Electronics

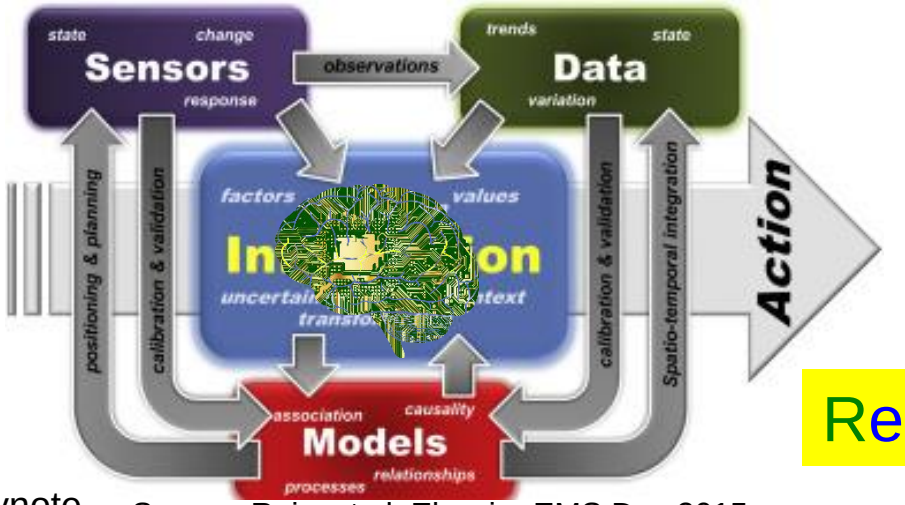
Energy Smart

Source: https://mashable.com/2012/10/05/energy-efficient-smartphone/

Energy consumption is minimal and adaptive for longer battery life and lower energy bills.

Security of systems and data.

Security Smart



Accurate sensing, analytics, and fast actuation.

Response Smart

Source: Mohanty iSES 2018 Keynote

Source: Reis, et al. Elsevier EMS Dec 2015

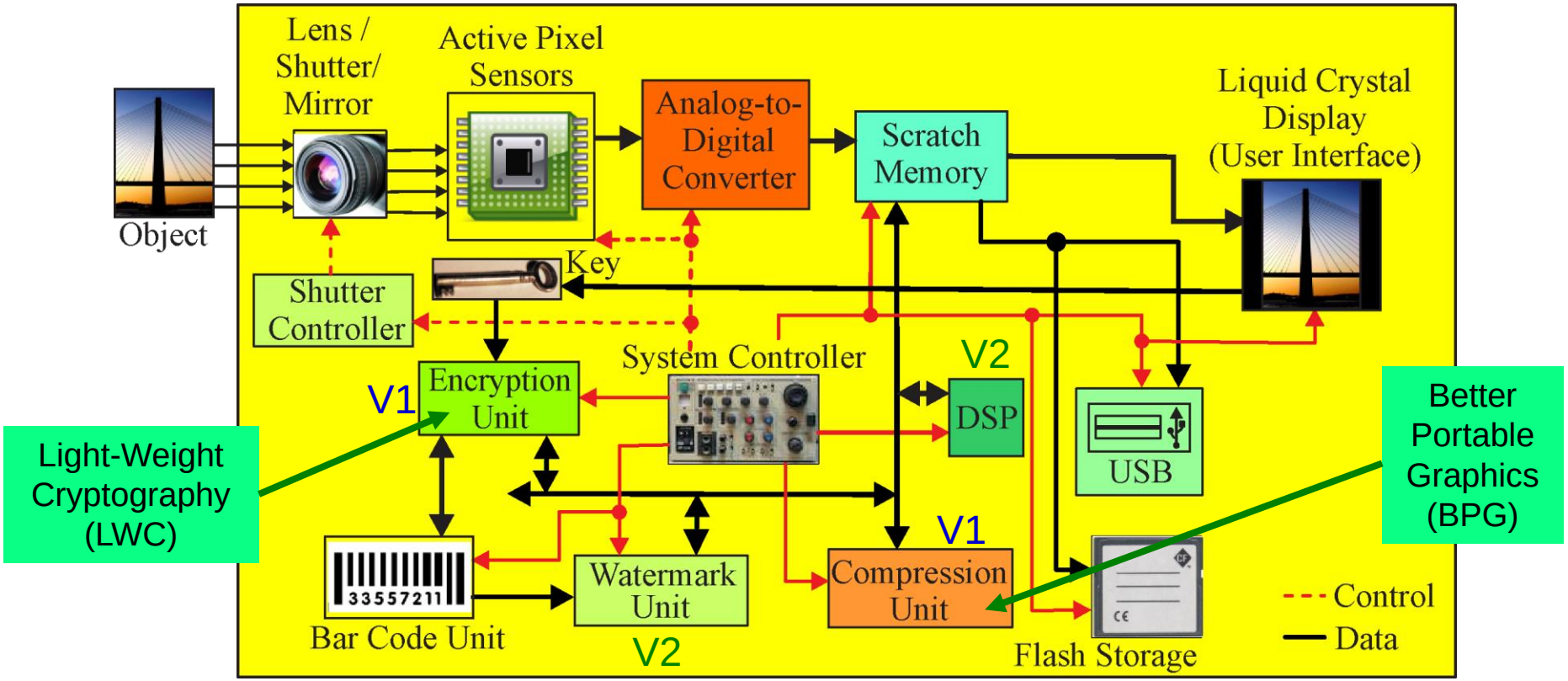
Security by Design (SbD) and/or Privacy by Design (PbD)

Embedding of security/privacy into the architecture (hardware+software) of various products, programs, or services.

Retrofitting: Difficult → Impossible!

Source: https://teachprivacy.com/tag/privacy-by-design/

ESR-Smart – End-Device Optimization



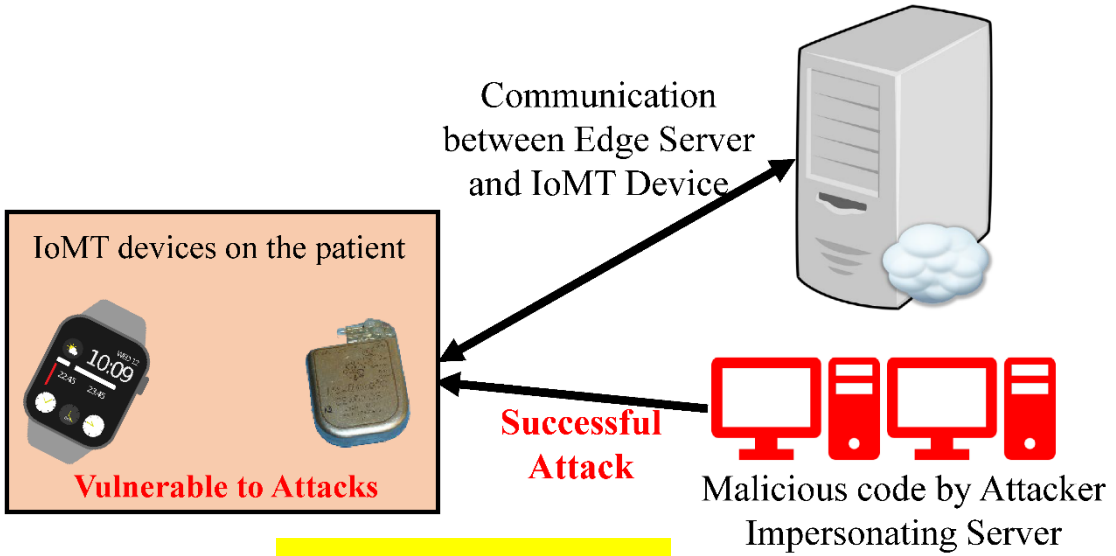
Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Security and/or Privacy by Design (SbD and/or PbD)

Source: S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", Elsevier Journal of Systems Architecture (JSA), Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

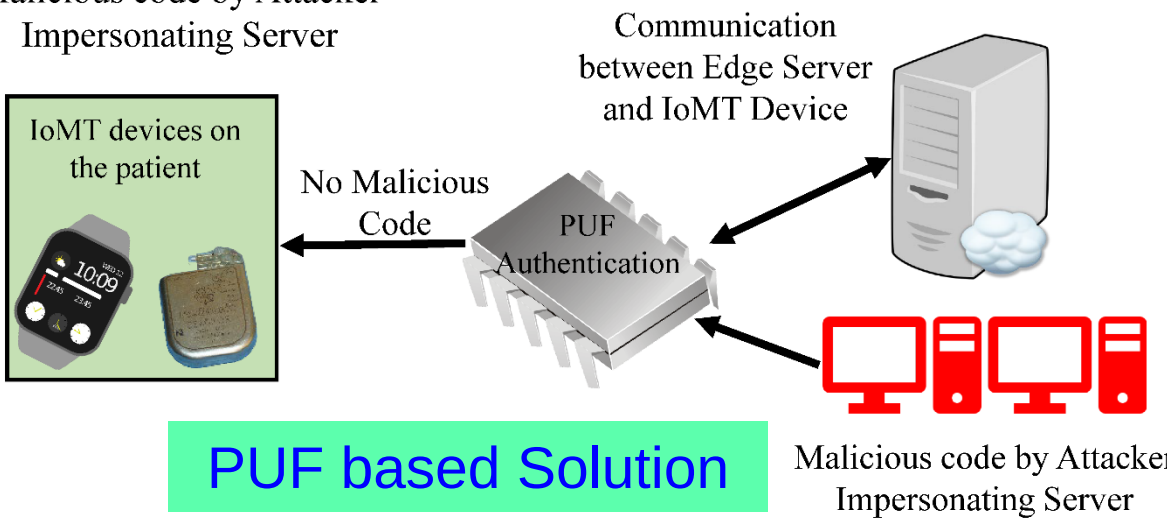
Source: Mohanty 2006, TCAS-II May 2006; Mohanty 2009, JSA Oct 2009; Mohanty 2016, Access 2016

IoMT Security - PUF based Device Authentication



Can provide: Device and System Security

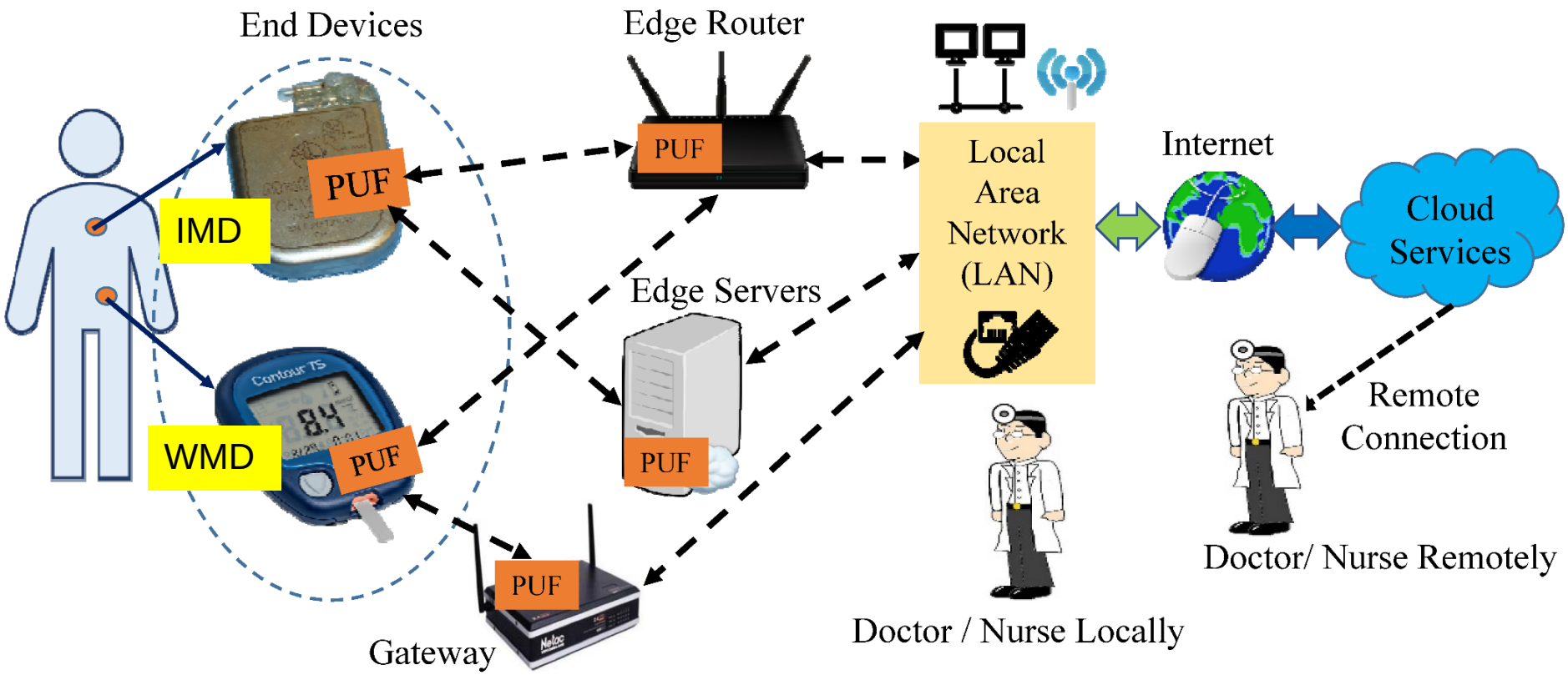
Threat Model



PUF based Solution

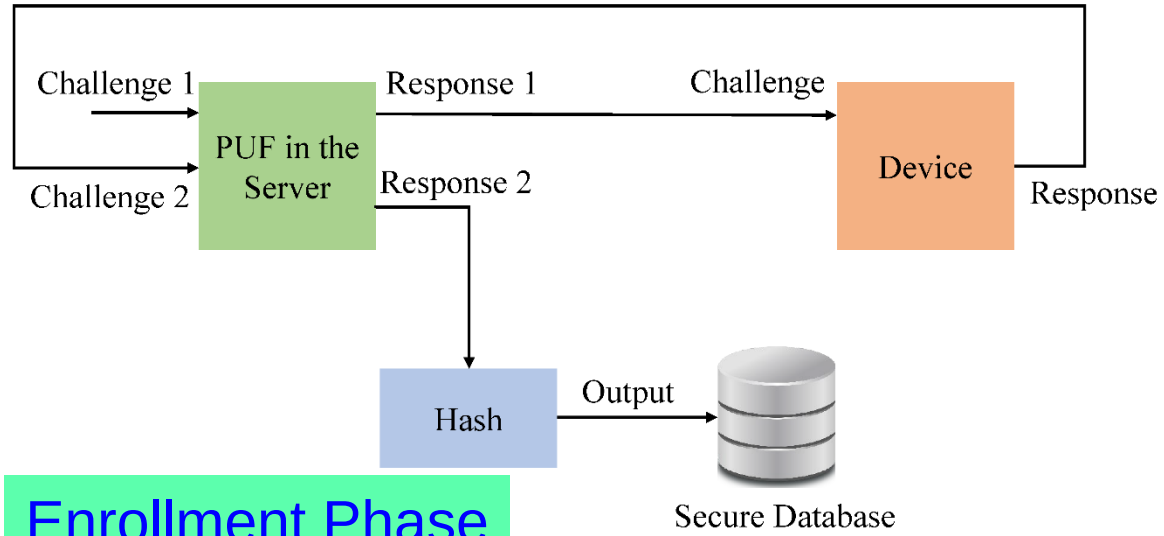
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security - PUF based Device Authentication



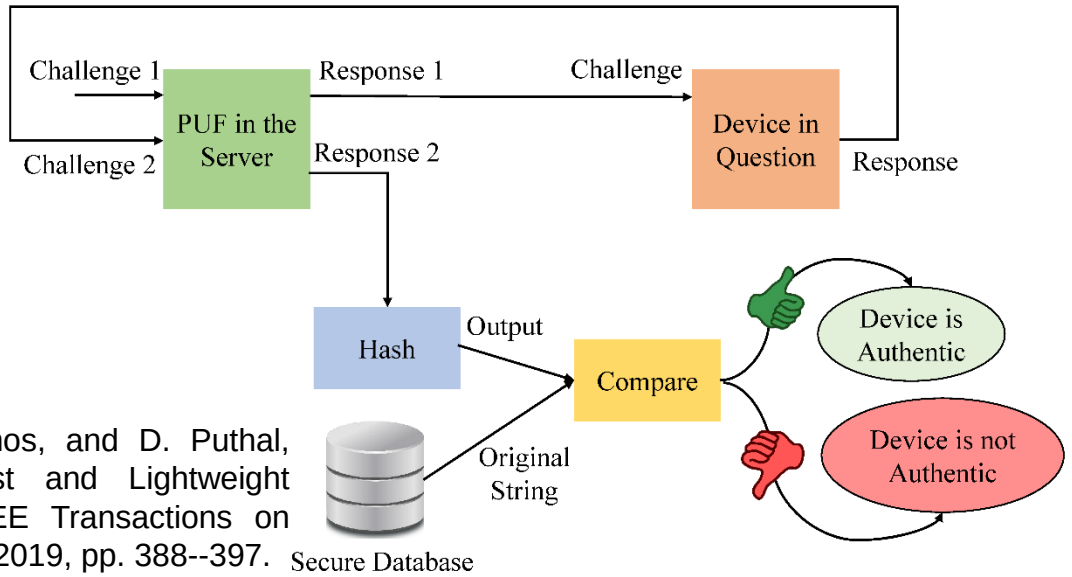
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security - PUF based Device Authentication



Enrollment Phase

Authentication Phase

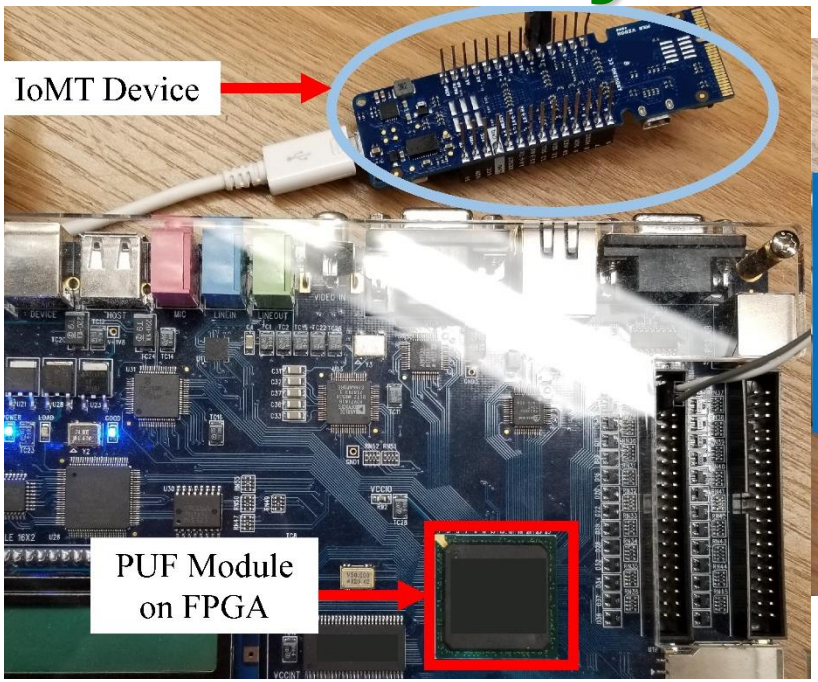


PUF Security Full Proof:

- Only server PUF Challenges are stored, not Responses
- Impossible to generate Responses without PUF

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security - PUF based Device Authentication

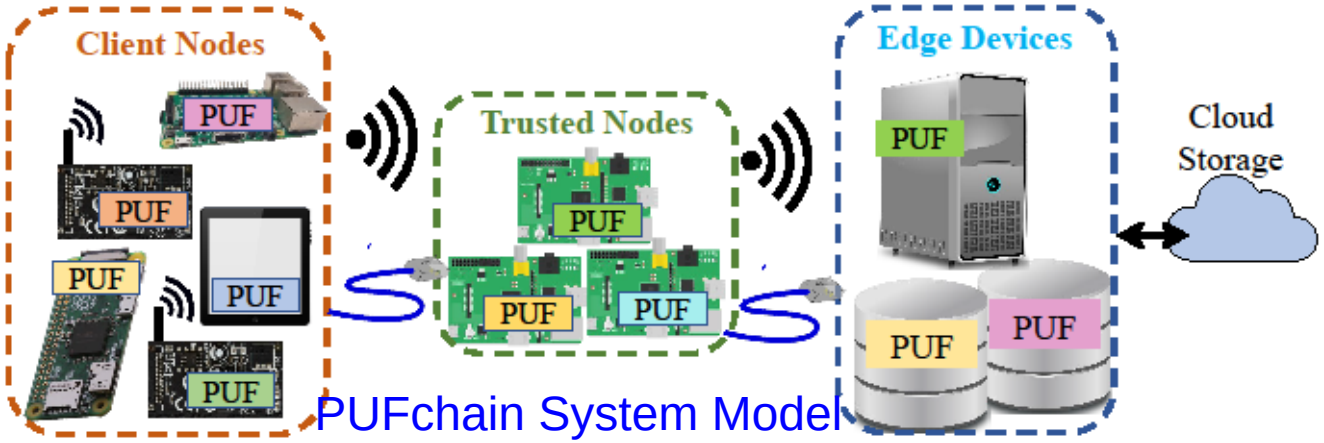


Average Power Overhead – ~ 200 μW

Proposed Approach Characteristics	Value (in a FPGA / Raspberry Pi platform)
Time to Generate the Key at Server	800 ms
Time to Generate the Key at IoMT Device	800 ms
Time to Authenticate the Device	1.2 sec - 1.5 sec

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume 65, Issue 3, August 2019, pp. 388--397.

PUFchain: Hardware-Assisted Scalable Blockchain

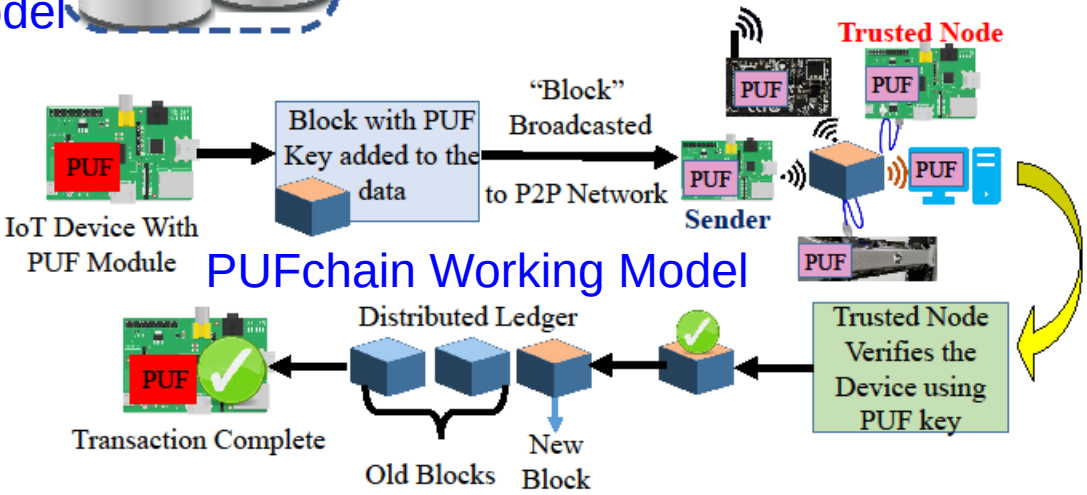


PUFchain System Model

Can provide: Device, System, and Data Security

PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode

Proof of PUF-Enabled Authentication" (PoP) is 1,000X faster than the well-established Proof-of-Work (PoW) and 5X faster than Proof-of-Authentication (PoAh).



PUFchain Working Model

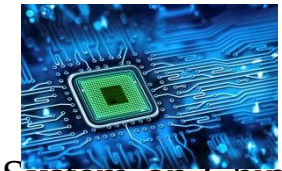
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", IEEE Consumer Electronics Magazine (MCE), Vol. XX, No. YY, ZZ 2020, pp. Accepted.

Eternal-Thing: Combines Security and Energy Harvesting at the Edge

Solar Cell

Harvesting System with Physically Unclonable Function (PUF)

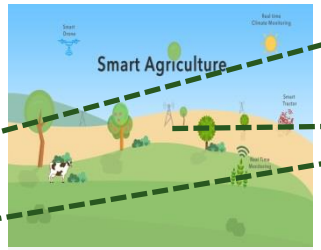
Sensors

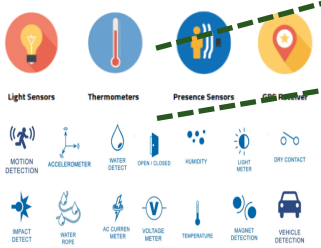


System-on-Chip (SoC)

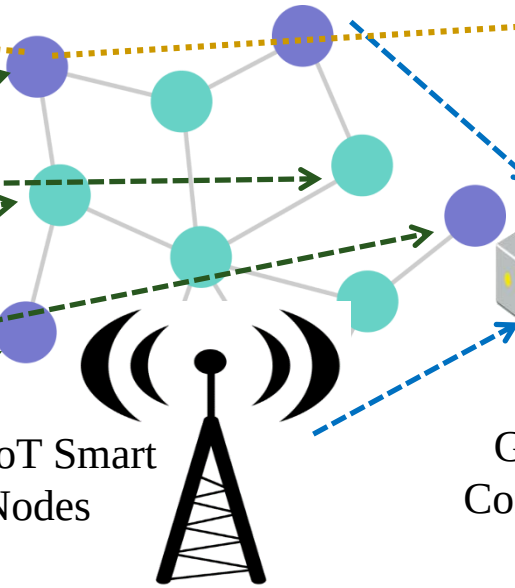
Trans-receiver

Provides security while consuming only 22μW power due to harvesting.

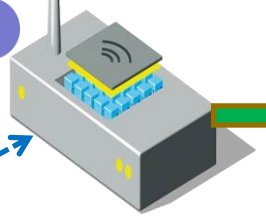




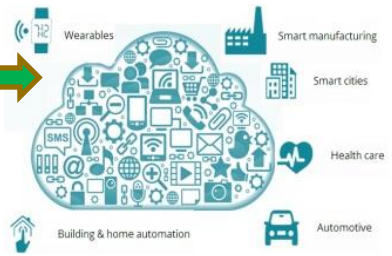
Edge Devices and their deployment



IoT Smart Nodes



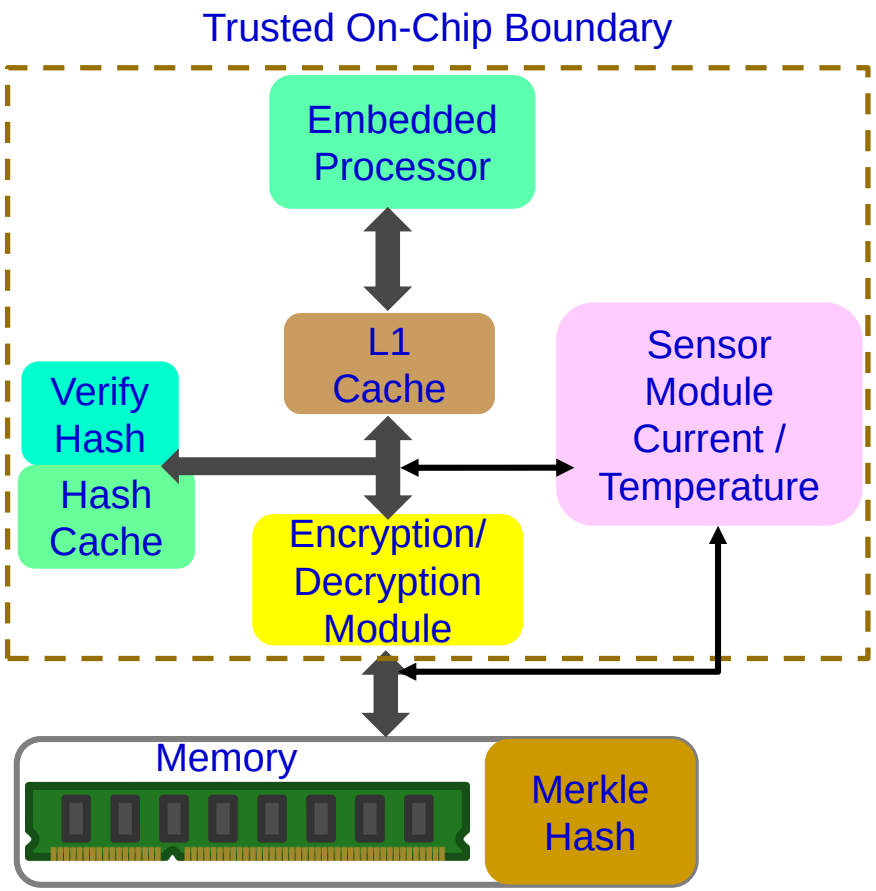
Gateways/ Concentrators



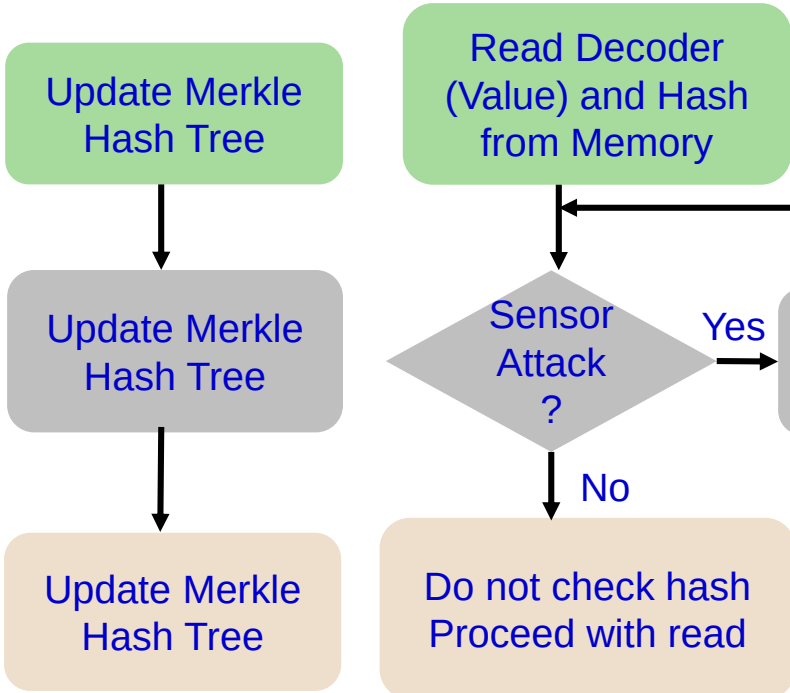
Cloud

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, "Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT", IEEE Transactions on Sustainable Computing, Vol. XX, No. YY, ZZ 1999, pp. Under Review.

Embedded Memory Security



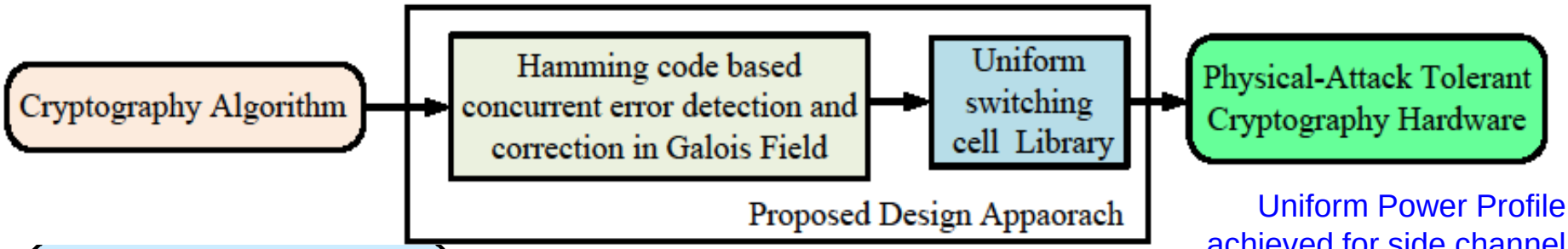
On-Chip/On-Board Memory Protection



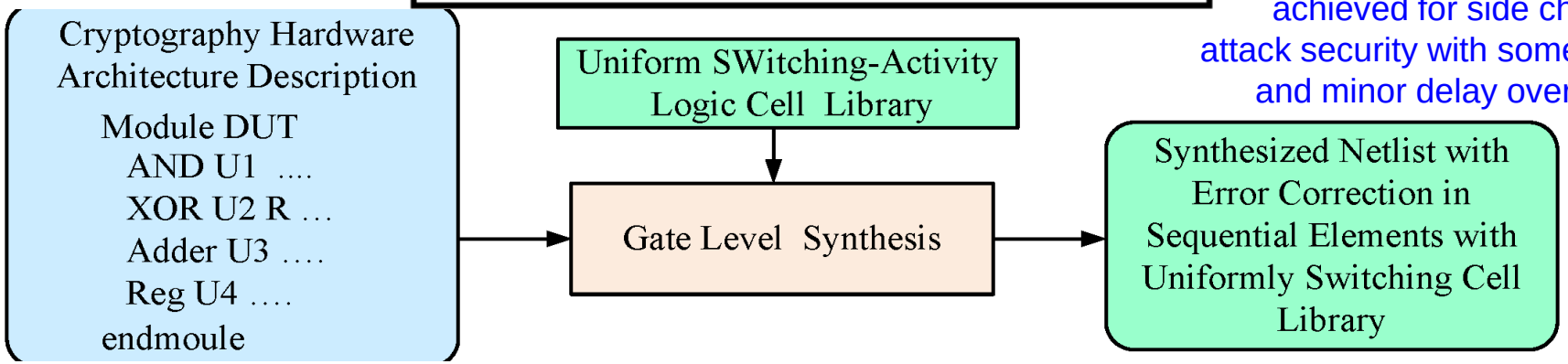
Memory integrity verification with 85% energy savings with minimal performance overhead.

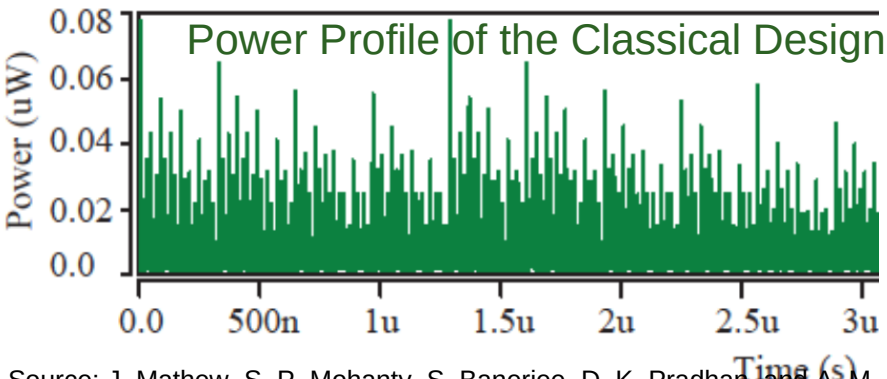
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", Springer Circuits, Systems, and Signal Processing Journal (CSSP), Volume 32, Issue 6, December 2013, pp. 2581--2604.

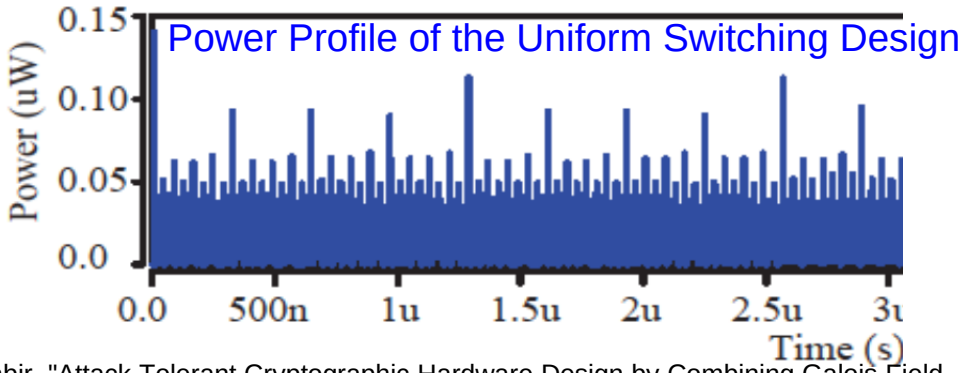
DPA Resilience Hardware Design



Uniform Power Profile achieved for side channel attack security with some area and minor delay overhead.







Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", Elsevier Computers and Electrical Engineering, Vol. 39, No. 4, May 2013, pp. 1077--1087.

Conclusions

Conclusions

- Smart Cities and their component design need to deal with multifront challenges including security, energy.
- Privacy, security, and ownership rights are important problems in CE systems.
- The various technologies and components including Data, System, AI need security; both software and hardware based solutions are possible.
- Many hardware based solutions exist for media copyright and information security. It is low-cost and low-overhead solution as compared to software only based.
- Hardware-Assisted Security (HAS): Security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system. HAS has evolved to Security by Design (SbD).

Future Directions

- Privacy and/or Security by Design (PbD or SbD) needs research.
- Security, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS) need more research.
- Security of systems (e.g. Smart Healthcare device/data, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable Smart City: needs sustainable IoT
- Internet-of-Everything (IoE) is the in which human are active parts, and thus needing research.

Call for Papers: Cybersecurity for the Smart Grid [CFP]

Computer seeks articles for an upcoming special issue.

Submission Deadline: ~~1 October 2019~~
Author notification: 10 December 2019
Publication Date: May 2020

The security and well-being of societies and economies are tied to the reliable operation of power systems. Due to the advancements of information and communication technologies, the traditional electric grid is evolving towards an intelligent smart grid. Despite the reliability and efficiency benefits, the inadequate level of security measures is leading to a greater threat landscape. Securing smart grid environments presents numerous challenges that need to be considered; smart grids are heterogeneous interconnected systems, and this heterogeneity and diversity necessitate non-static, application specific methods able to capture the complex interrelationships of various elements. Despite existing efforts, more focus is required on interoperable, cost-recovery, effective, and insurance mechanisms able to help guide further regulations and standards in this area. Such strategies need to ensure that technical solutions can “understand” interdependencies, integrate expertise from the engineering and cybersecurity communities, reduce institutional and policy barriers, and prioritize specific recommendations which can address the interoperability issues between technical, management, and policy-oriented approaches.

IEEE Consumer Electronics Magazine

The IEEE Consumer Electronics Magazine (MCE) is the flagship award-winning magazine of the consumer electronics (CE) society of IEEE. From 2018, the magazine is published on a bimonthly basis and features a range of topical content on state-of-art consumer electronics systems, services and devices, and associated technologies.

The MCE won an Apex Grand Award for excellence in writing in 2013. The MCE is the winner in the Regional 2016 STC Technical Communication Awards - Award of Excellence! The MCE is indexed in Clarivate Analytics (formerly IP Science of Thomson Reuters). The 2018 impact factor of MCE is 3.273.

Aim and Scope

- Consumer electronics magazine covers the areas or topics that are related to "consumer electronics".
- Articles should be broadly scoped – typically review and tutorial articles are well fit for a magazine flavor.
- Technical articles may be suitable but these should be of general interest to an engineering audience and of broader scope than archival technical papers.
- Topics of interest to consumer electronics: Video technology, Audio technology, White goods, Home care products, Mobile communications, Gaming, Air care products, Home medical devices, Fitness devices, Home automation and networking devices, Consumer solar technology, Home theater, Digital imaging, In-vehicle technology, Wireless technology, Cable and satellite technology, Home security, Domestic lighting, Human interface, Artificial intelligence, Home computing, Video Technology, Consumer storage technology. Studies or opinion pieces on the societal impacts of consumer electronics are also welcome.

Have questions on submissions or ideas for special issues, contact EiC at: saraju.mohanty@unt.edu

Submission Instructions

Submission should follow IEEE standard template and should consist of the following:

I. A manuscript of maximum 6-page length: A pdf of the complete manuscript layout with figures, tables placed within the text, and

II. Source files: Text should be provided separately from photos and graphics and may be in Word or LaTeX format.

- High resolution original photos and graphics are required for the final submission.
- The graphics may be provided in a PowerPoint slide deck, with one figure/graphic per slide.
- An IEEE copyright form will be required. The manuscripts need to be submitted online at the URL: http://mc.manuscriptcentral.com/cemag

Editorial Board

More Information at:
http://cesoc.ieee.org/publications/ce-magazine.html

IEEE

Smart Electronic Systems Laboratory (SESL)

Electromagnetic Pulse (EMP) Attack

- An electromagnetic pulse (EMP) is the electric wave produced by nuclear blasts which can knocking out electronics and the electrical grid as far as 1,000 miles away.
- The disruption could cause catastrophic damage and loss of life if power is not restored or backed up quickly.

Source: http://bwcentral.org/2016/06/an-electromagnetic-pulse-emp-nuclear-attack-may-end-modern-life-in-america-overnight/

Acknowledgement(s)

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.