Smart Electronics

Fulbright Lecture 2023 – KL Deemed University

Guntur, India, 1-31 July 2023

Homepage

Prof./Dr. Saraju Mohanty
University of North Texas, USA.

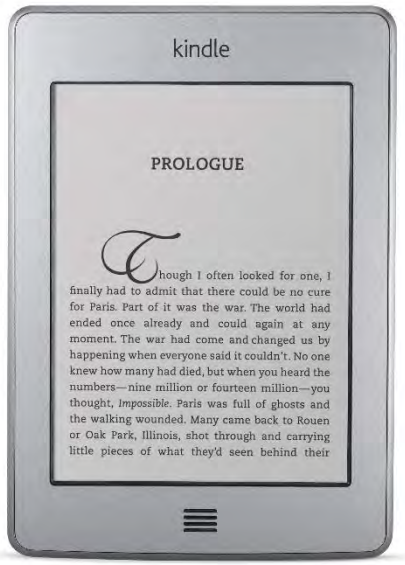
Talk - Outline

- What are Smart Possibilities?
- Challenges in the Electronic System design
- Energy Smart Electronics
- Security Smart Electronics
- Response Smart Electronics
- Design Trade-offs in Electronics
- Conclusion and Future Directions

What is Common Among These?

Does Smart Mean Small?

Does Smart Mean Portable?



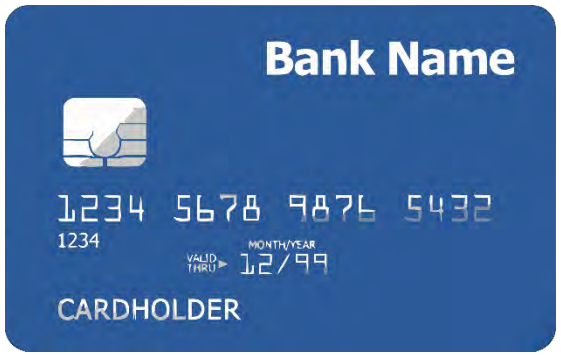
Does Smart Mean More-Features?

Does Smart Mean Low-Cost?

Does Smart Mean Efficient?

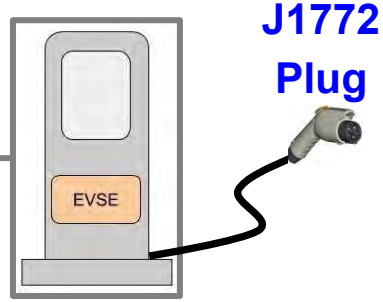
Does Smart Mean Safe?

Does Smart Mean Electronic?

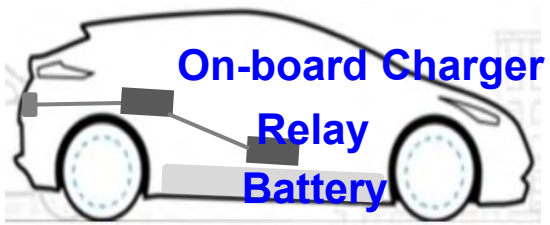


Does Smart Mean Electric?

Grid



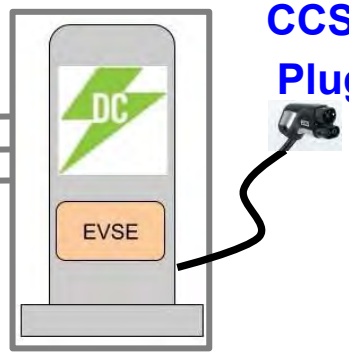
J1772 Plug



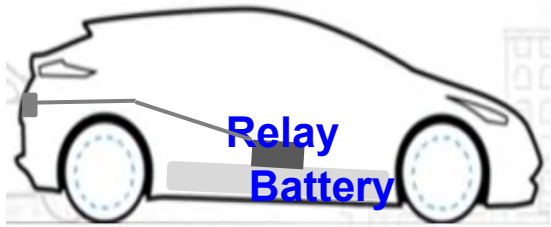
AC charging station

- Monitoring function
- Communication and safety

3 phase AC supply



CCS1 Plug



DC charging station

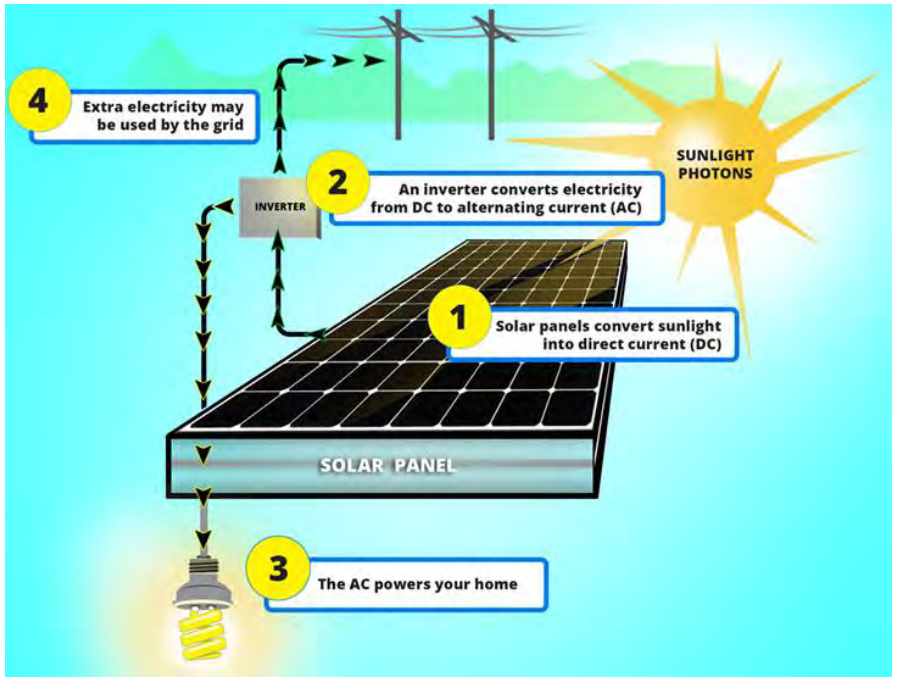
- AC-DC Off board conversion
- Monitoring Power flow
- EV to grid communication
- Safety monitoring

Electric Vehicle Supply Equipment (EVSE)

Source: Mishra, Mohanty 2018, CE Magazine Mar 2018

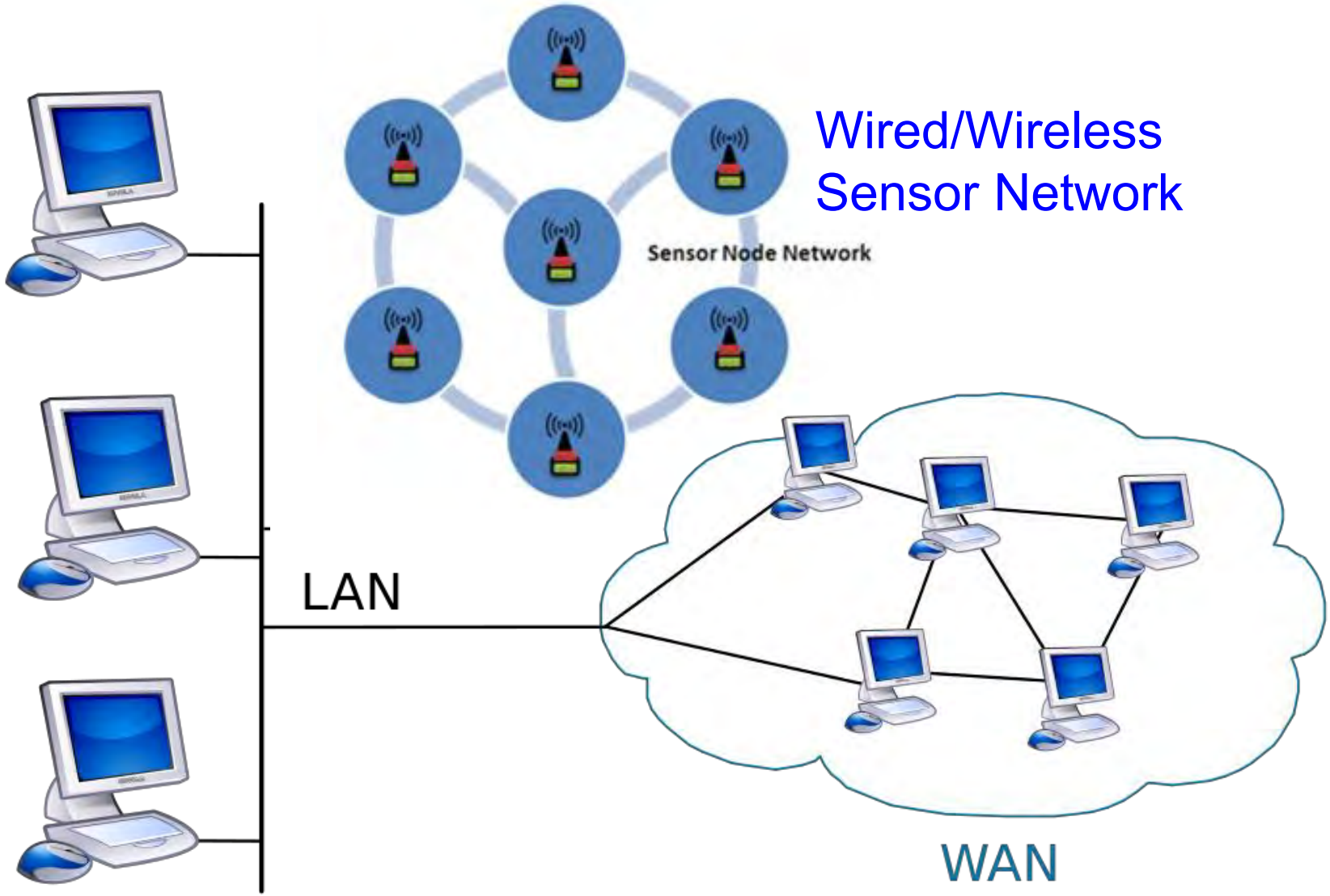
Does Smart Mean Battery-Operated?

Does Smart Mean Renewable?

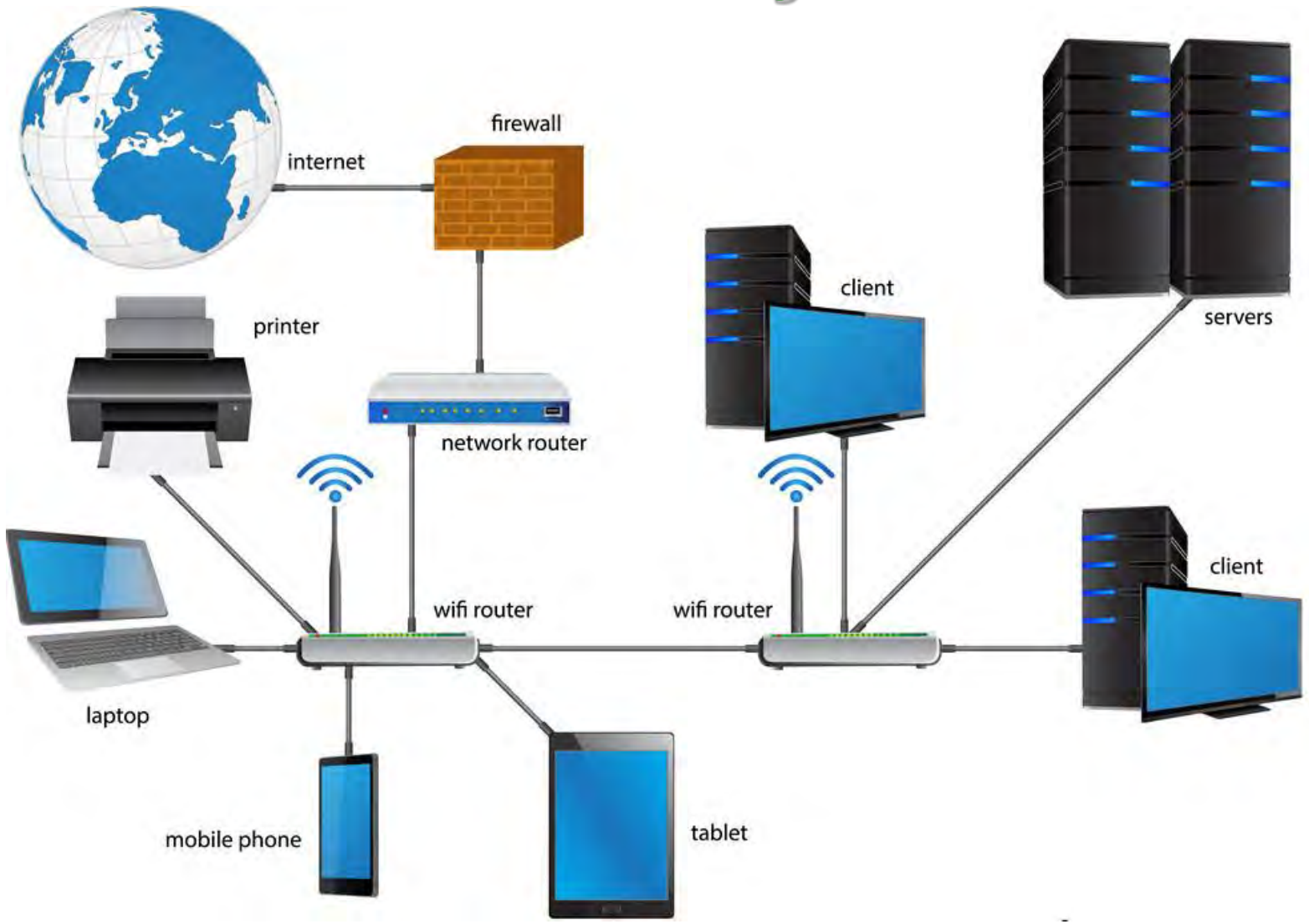


Source: https://us.sunpower.com/blog/2017/10/25/how-does-solar-energy-work/

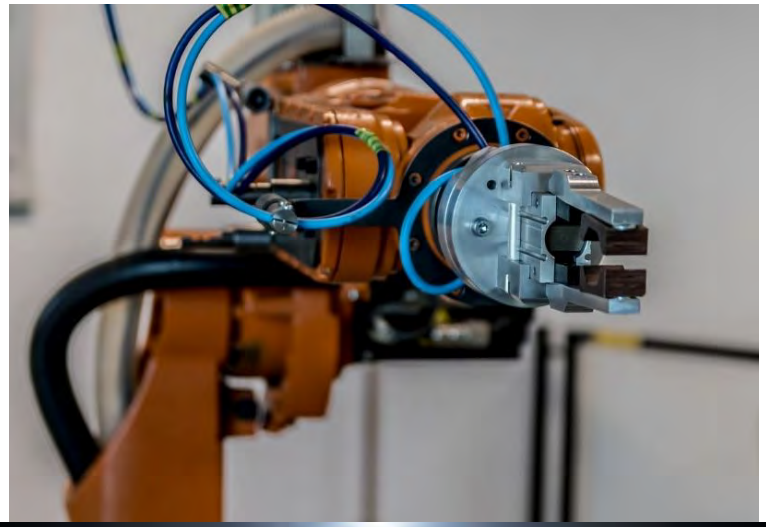
Does Smart Mean Connected?



Does Smart Mean Cyber-Enabled?

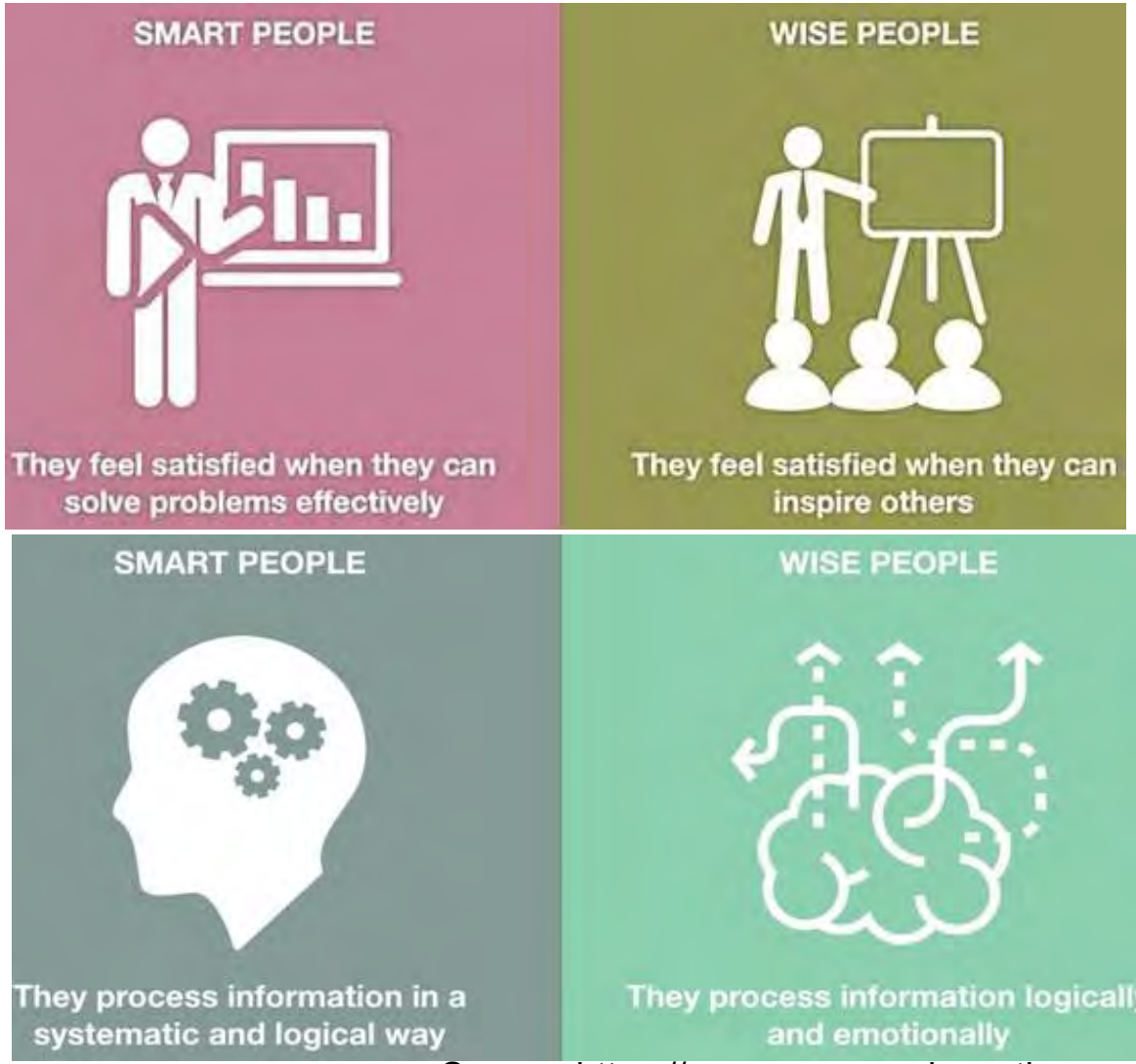


Does Smart Mean Autonomous?



Does Smart Mean Intelligence?

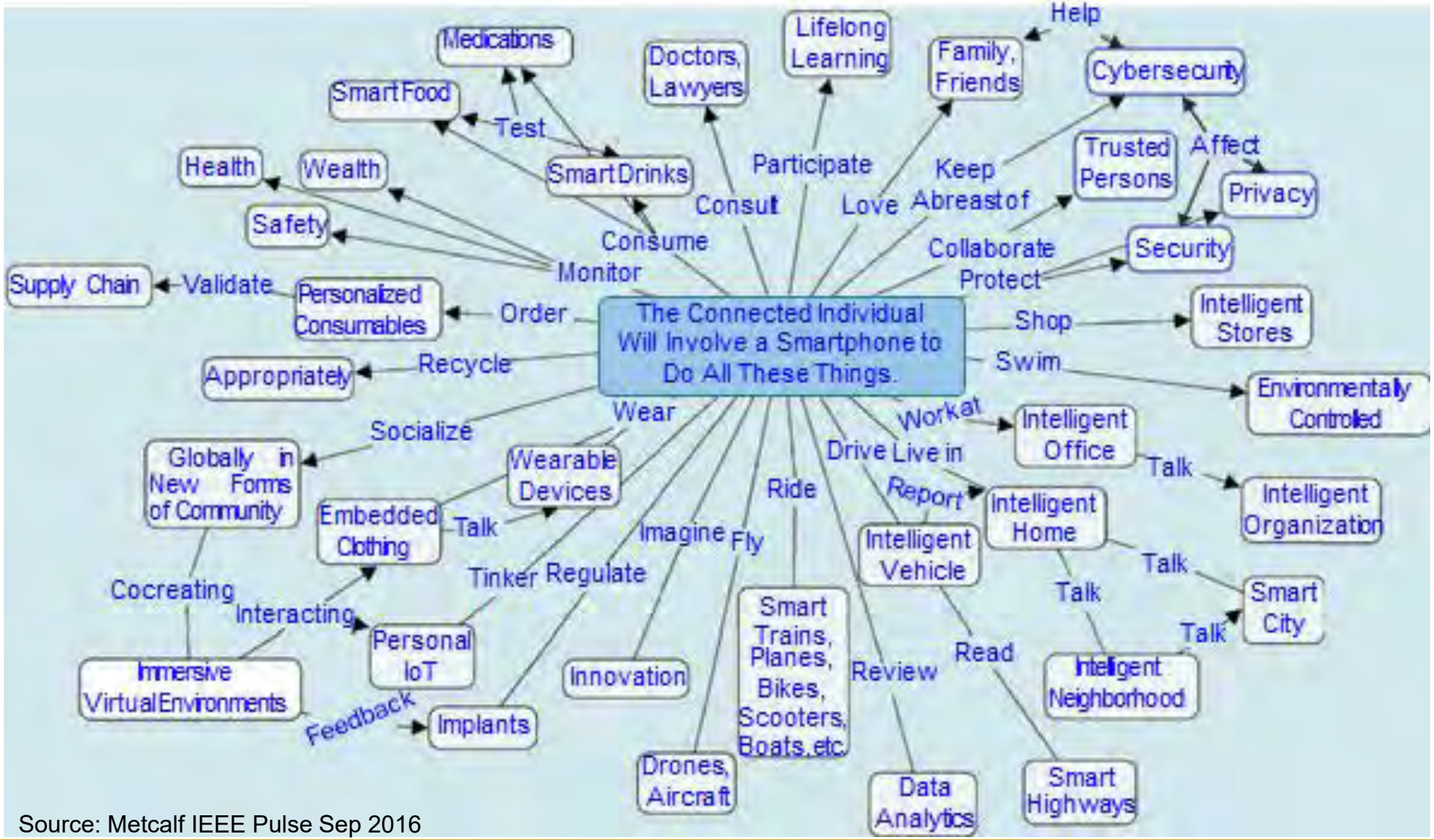
Does Smart Mean Wise?



Source: https://www.awesomeinventions.com/wise-vs-smart/

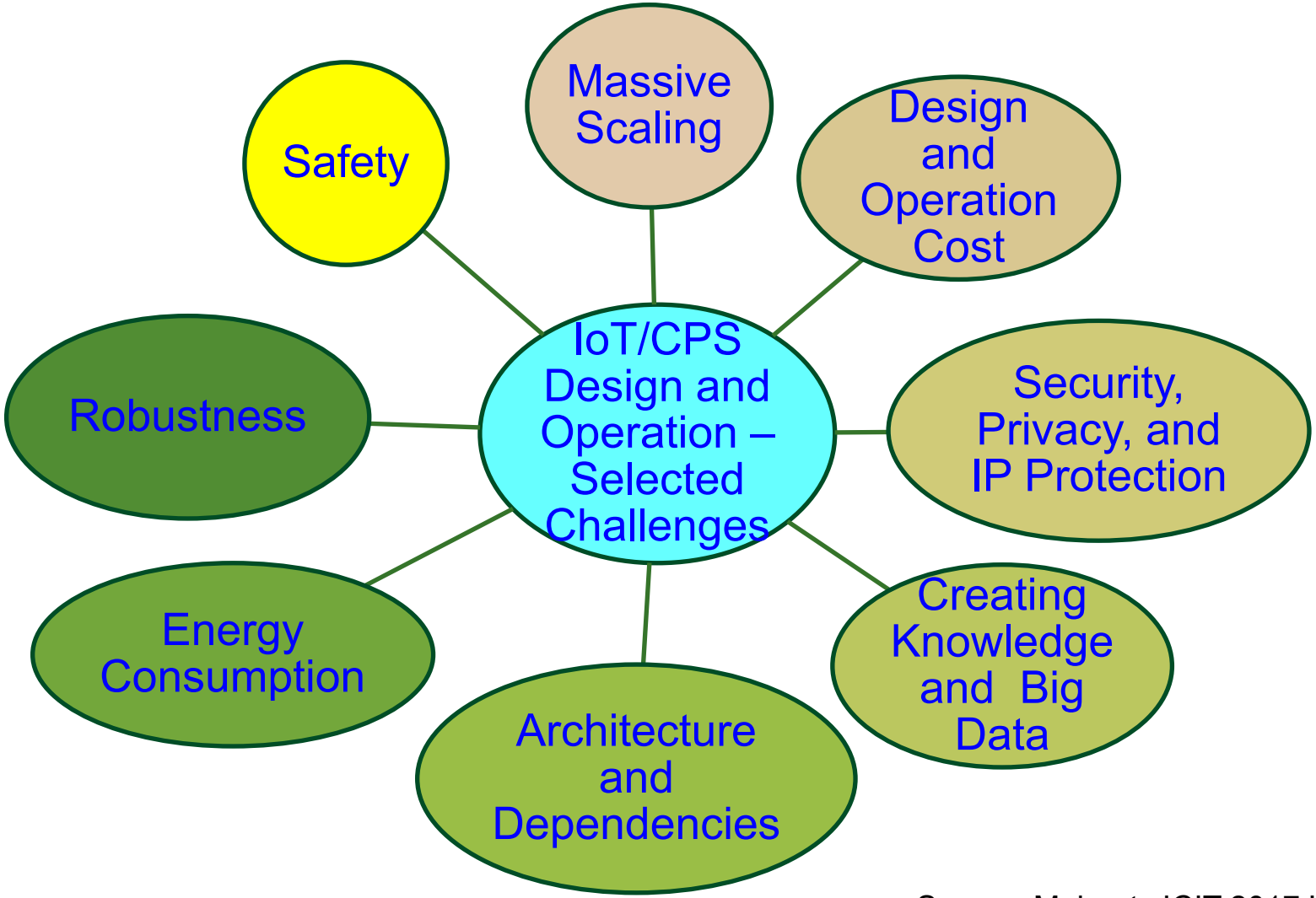
Challenges in Next Generation Electronics Design

Activities using Smart Phones



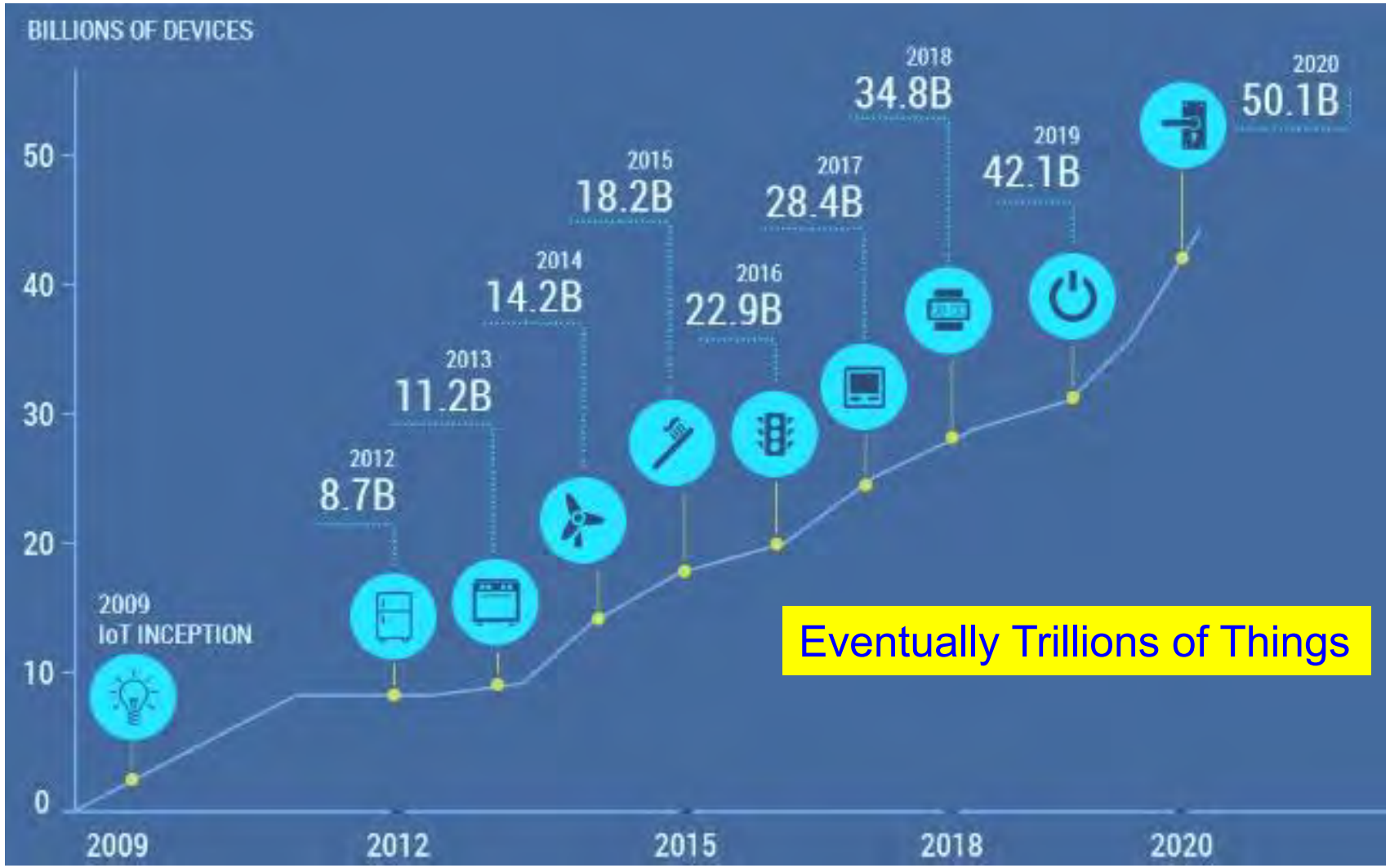
Source: Metcalf IEEE Pulse Sep 2016

IoT/CPS – Selected Challenges



Source: Mohanty ICIT 2017 Keynote

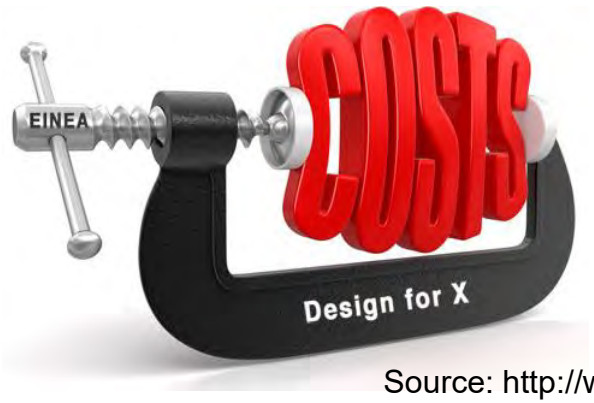
Massive Growth of Sensors/Things



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

Design Cost

- The design cost is a one-time cost.
- Design cost needs to be small to make a smart city realization possible.

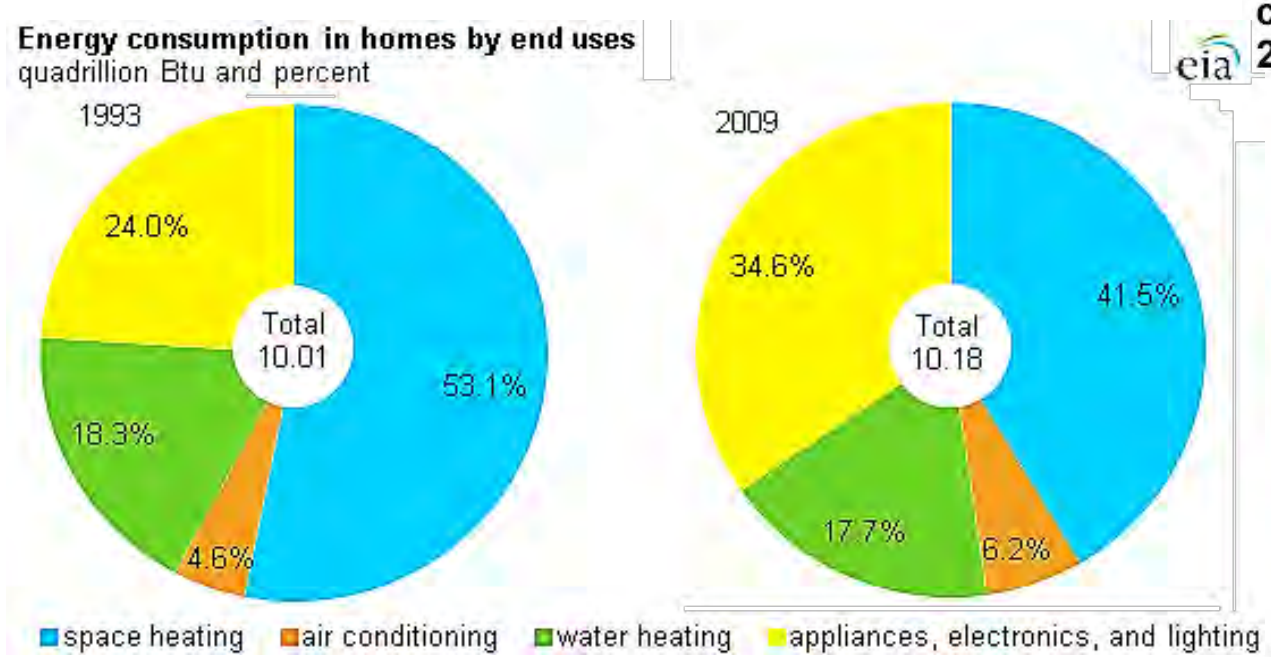


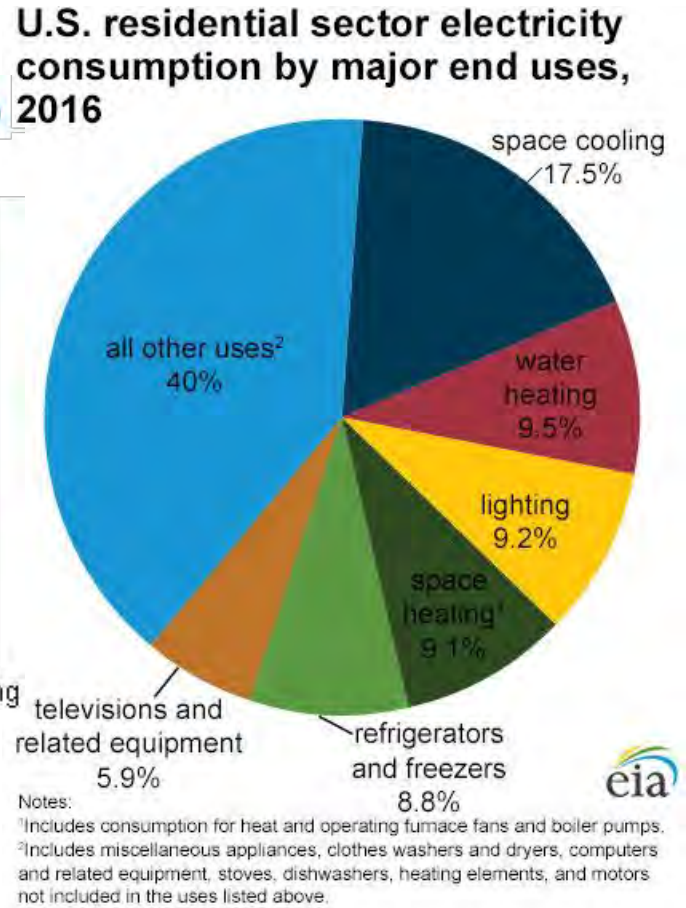
Source: http://www.industrialisation-produits-electroniques.fr

Operational Cost

- The operations cost is that required to maintain the smart city.
- A small operations cost will make it easier for cities to operate in the long run with minimal burden on the city budget.

Consumer Electronics Demand More and More Energy

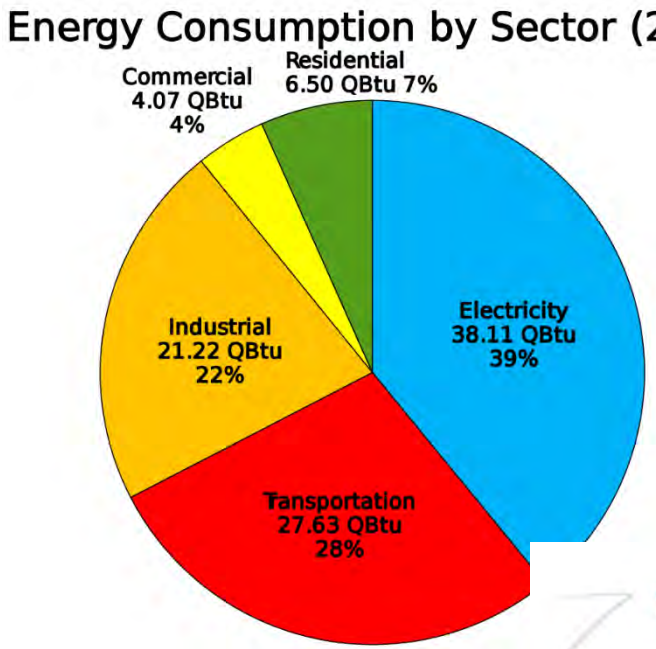


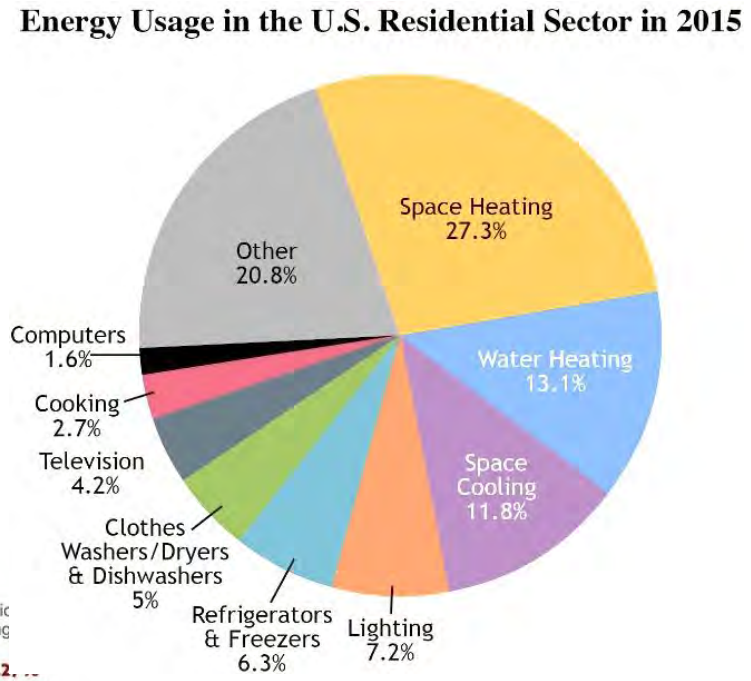


Quadrillion BTU (or quad): 1 quad = 10^{15} BTU = 1.055 Exa Joule (EJ).

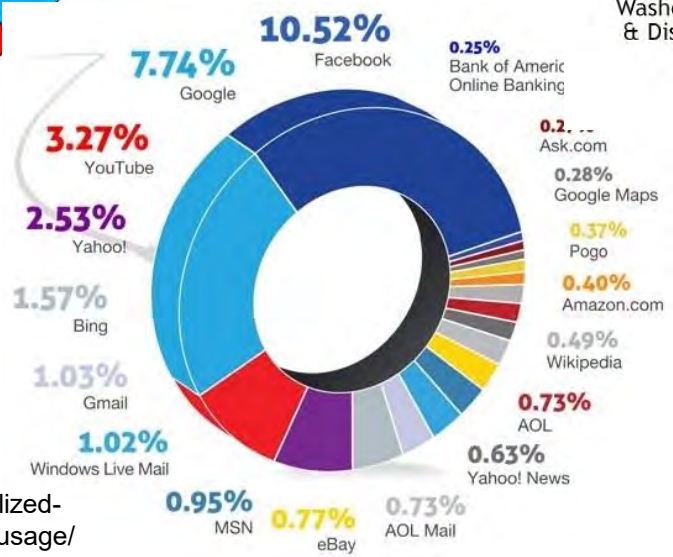
Source: U.S. Energy Information Administration

Energy Consumption





Data Center Power Usage

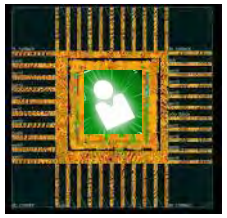


Individual Level: Imagine how often we charge our portable CE!

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

Security, Privacy, and IP Rights

Hardware Trojan



System Security

Data Security

System Privacy

Data Privacy

Counterfeit Hardware
(IP Rights Violation)

Source: Mohanty ICIT 2017 Keynote

Cyber Attacks

September 2017: Cybersecurity incident at Equifax affected 143 million U.S. consumers.

Hacked: US Department Of Justice

Who did it: Unknown

What was done: Information on 10,000 DHS and 20,000 FBI employees.

Details: The method of the attack is still a mystery and it's been said that it took a week for the DOJ to realize that the info had been stolen.

February 2016

Hacked: Yahoo #2

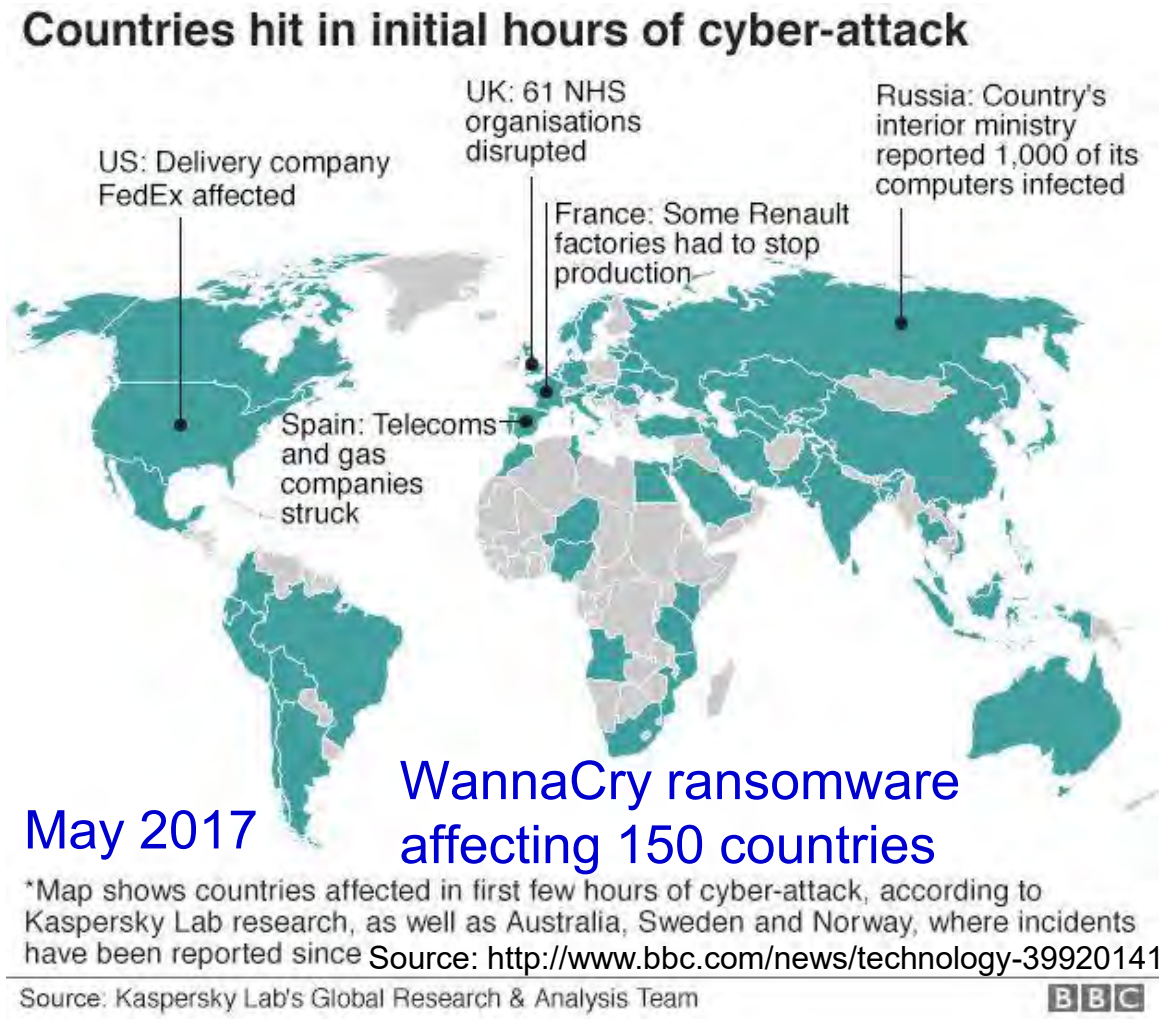
YAHOO!

Who did it: Unknown

What was done: 1 billion accounts were compromised.

Details: Users names, email addresses, date of birth, passwords, phone numbers, and security questions were all taken.

December 2016



May 2017

WannaCry ransomware affecting 150 countries

Source: http://www.bbc.com/news/technology-39920141

Source: https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/#73bb0bee48e3

Security Challenges – Information

Online Banking

Credit Card Theft

Hacked: Linkedin, Tumbler, & Myspace

LinkedIn 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

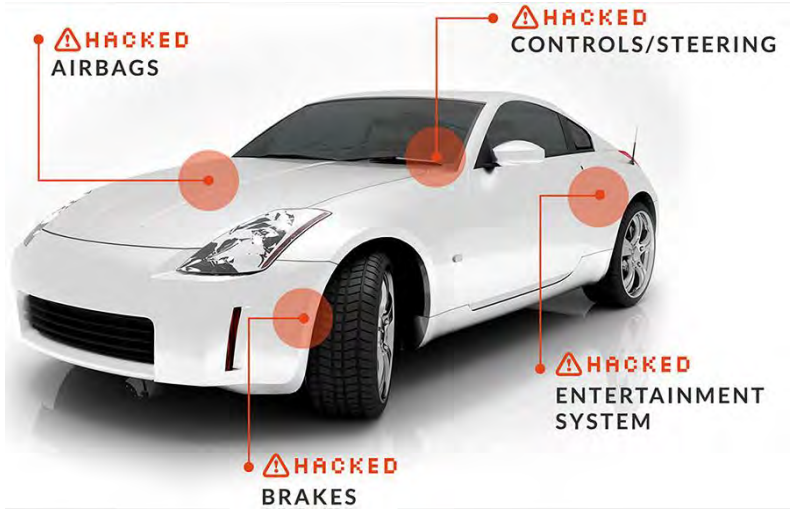
Personal Information

Credit Card/Unauthorized Shopping

Cybersecurity Challenges - System

Power Grid Attack

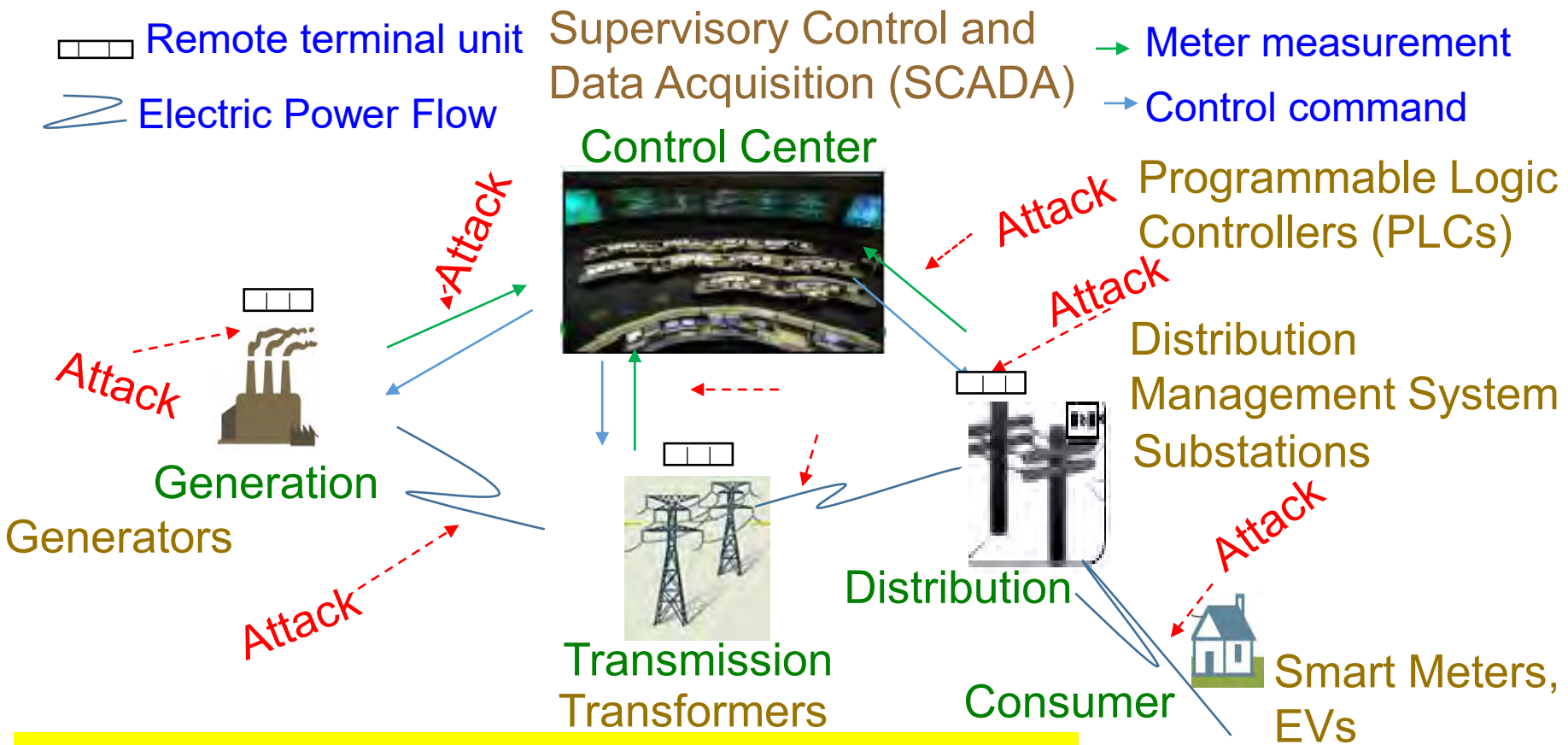
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



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

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

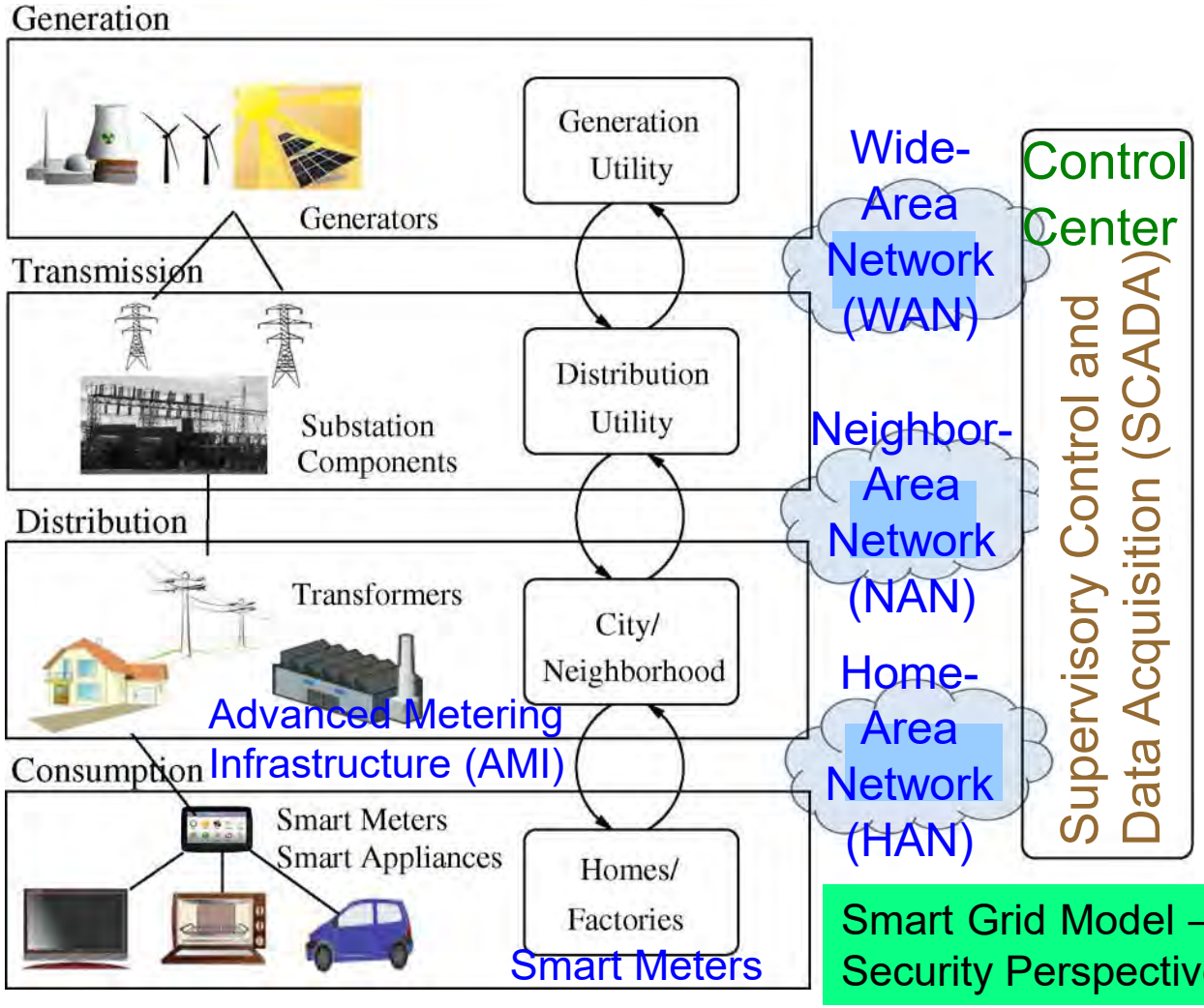
Smart Grid - Vulnerability



ICT components of smart grid is cyber vulnerable.

Source: (1) R. K. Kaur, L. K. Singh and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 10-15, March 2019.
(2)https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

Smart Grid - Vulnerability



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)

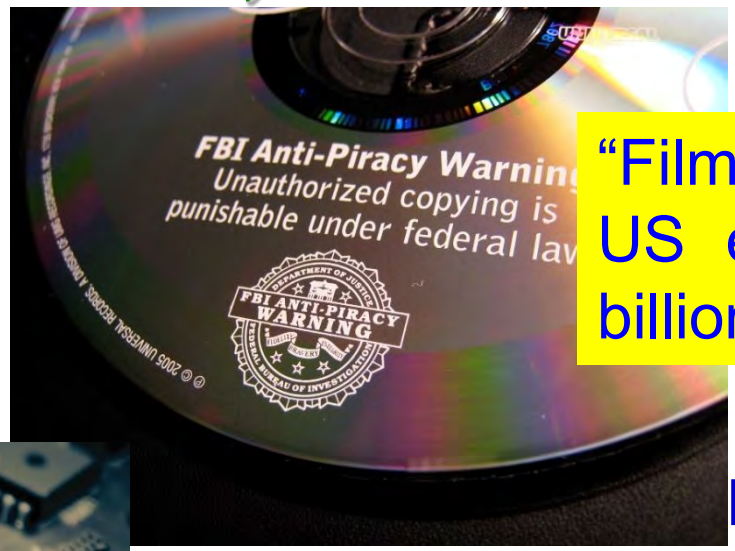
Programmable Logic Controllers (PLCs)

Smart Meters

Smart Grid Model – CPS Security Perspective

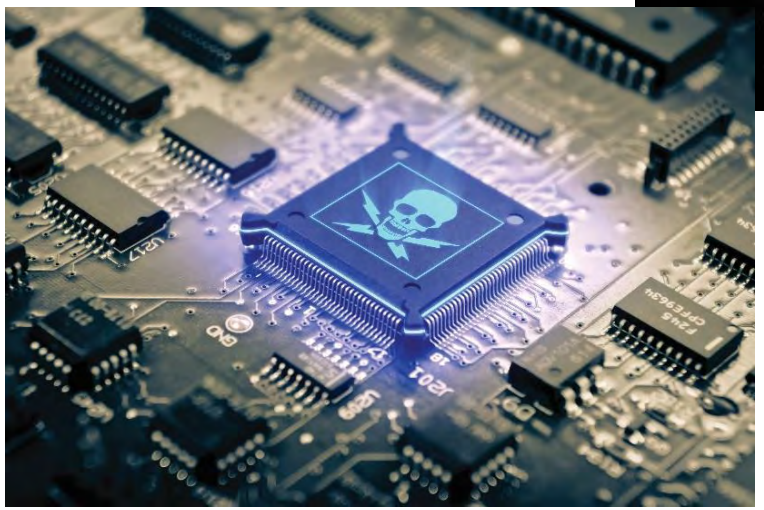
Source: Y. Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure", *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

Ownership - Media, Hardware, Software



"Film piracy cost the US economy $20.5 billion annually."

Hardware Piracy → Counterfeit Hardware



Media Piracy

Software Piracy

Top counterfeits could have impact of $300B on the semiconductor market.

IoMT Security Issue is Real & Scary

- Insulin pumps are vulnerable to hacking, FDA warns amid recall:

https://www.washingtonpost.com/health/2019/06/28/insulin-pumps-are-vulnerable-hacking-fda-warns-amid-recall/

- Software vulnerabilities in some medical devices could leave them susceptible to hackers, FDA warns:

https://www.cnn.com/2019/10/02/health/fda-medical-devices-hackers-trnd/index.html

- FDA Issues Recall For Medtronic mHealth Devices Over Hacking Concerns:

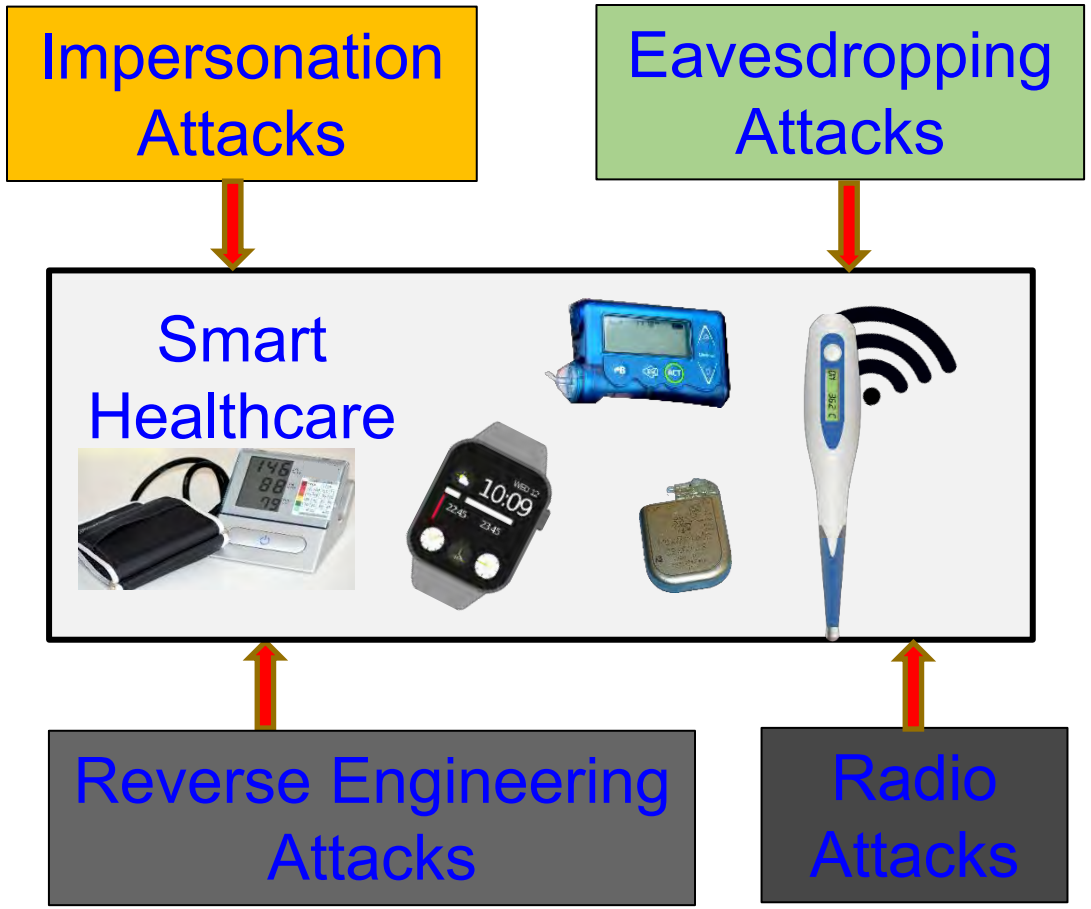
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

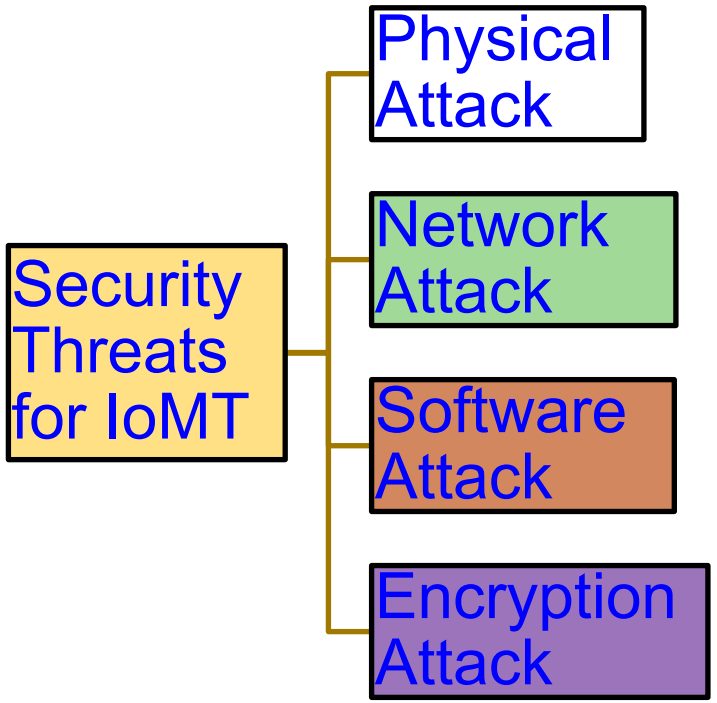
Implantable Medical Devices - Attacks

- The vulnerabilities affect implantable cardiac devices and the external equipment used to communicate with them.
- The devices emit RF signals that can be detected up to several meters from the body.
- A malicious individual nearby could conceivably hack into the signal to jam it, alter it, or snoop on it.

Source: Emily Waltz, Can "Internet-of-Body" Thwart Cyber Attacks on Implanted Medical Devices?, *IEEE Spectrum*, 28 Mar 2019, https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices.amp.html.

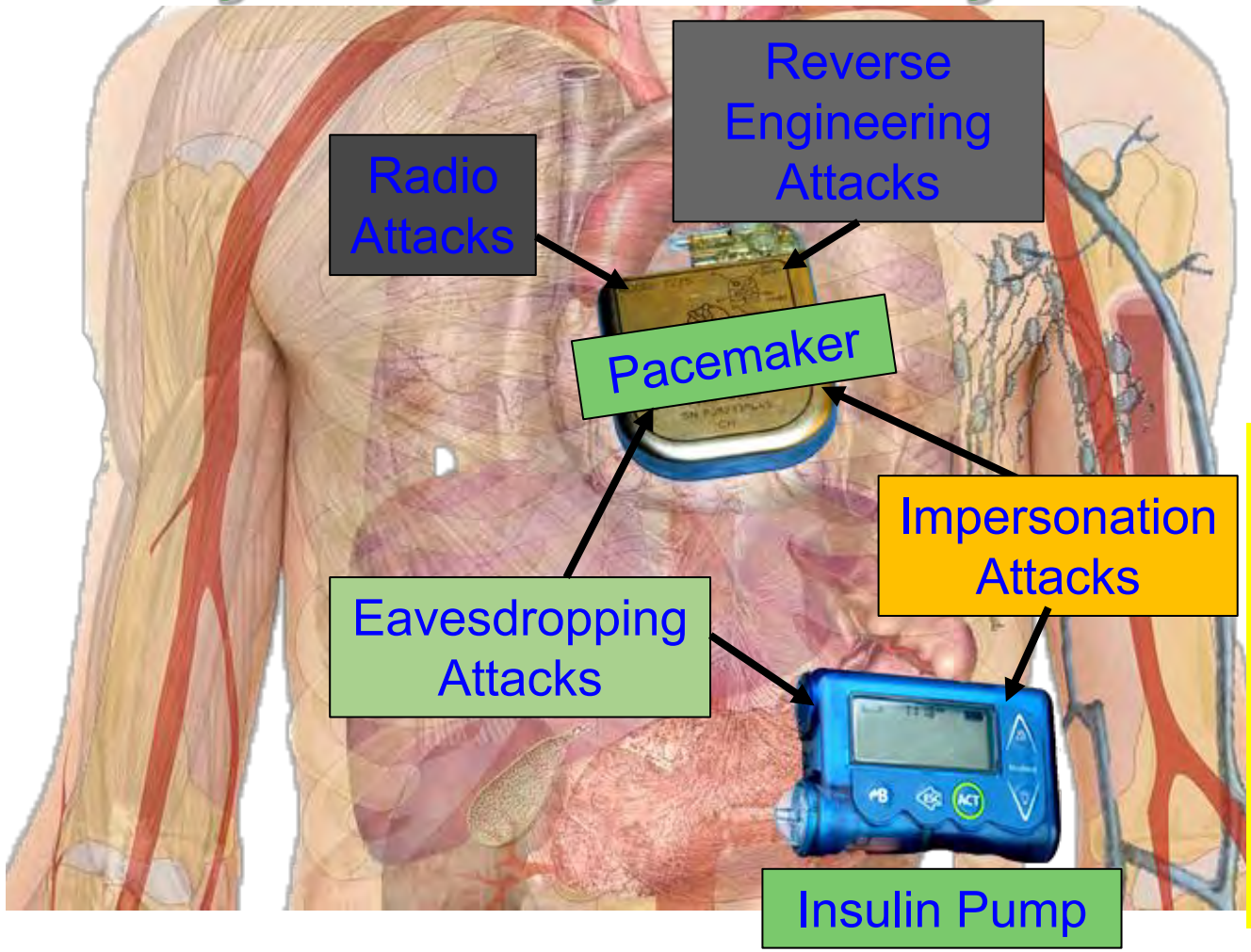
IoMT Security – Selected Attacks





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.

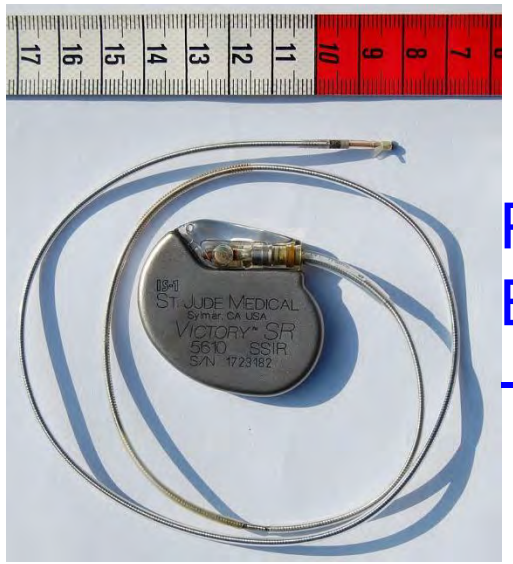
Security Measures in Healthcare Cyber-Physical Systems is Hard



Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs) -- Battery Characteristics:
→ Longer life
→ Safer
→ Smaller size
→ Smaller weight

H-CPS Security Measures is Hard - Energy Constrained



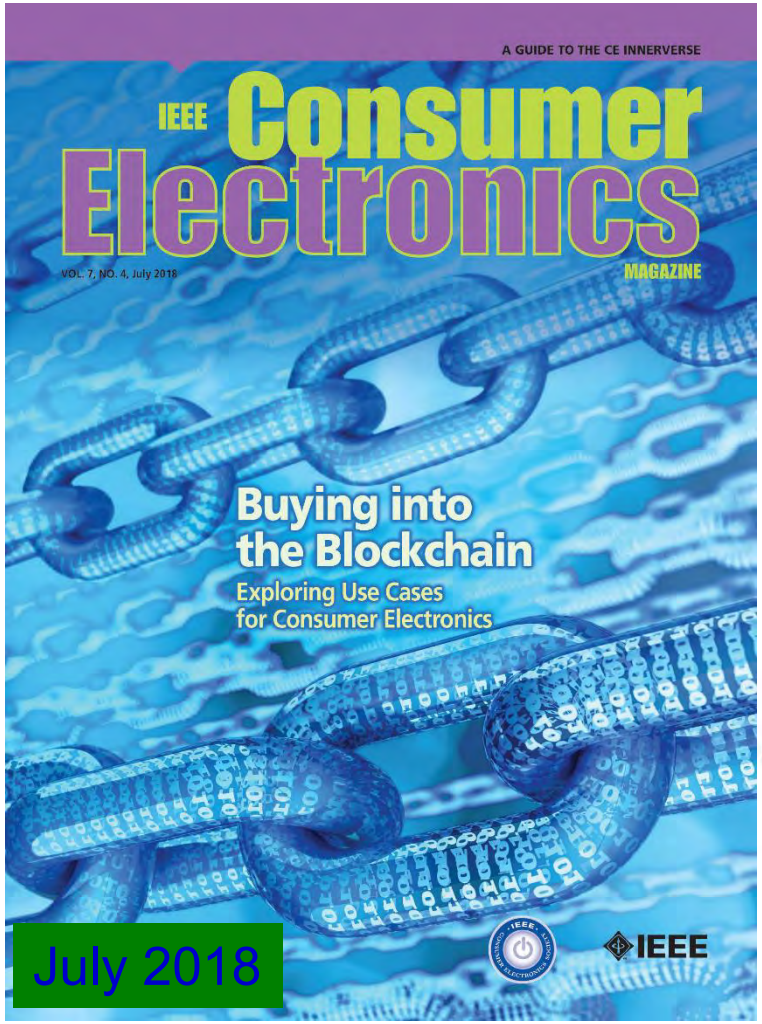
Pacemaker Battery Life - 10 years

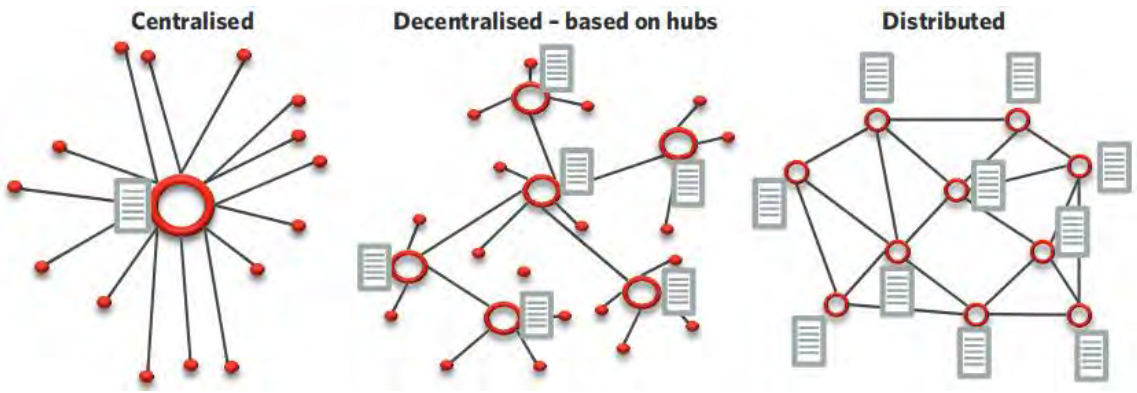
Neurostimulator Battery Life - 8 years

- 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.

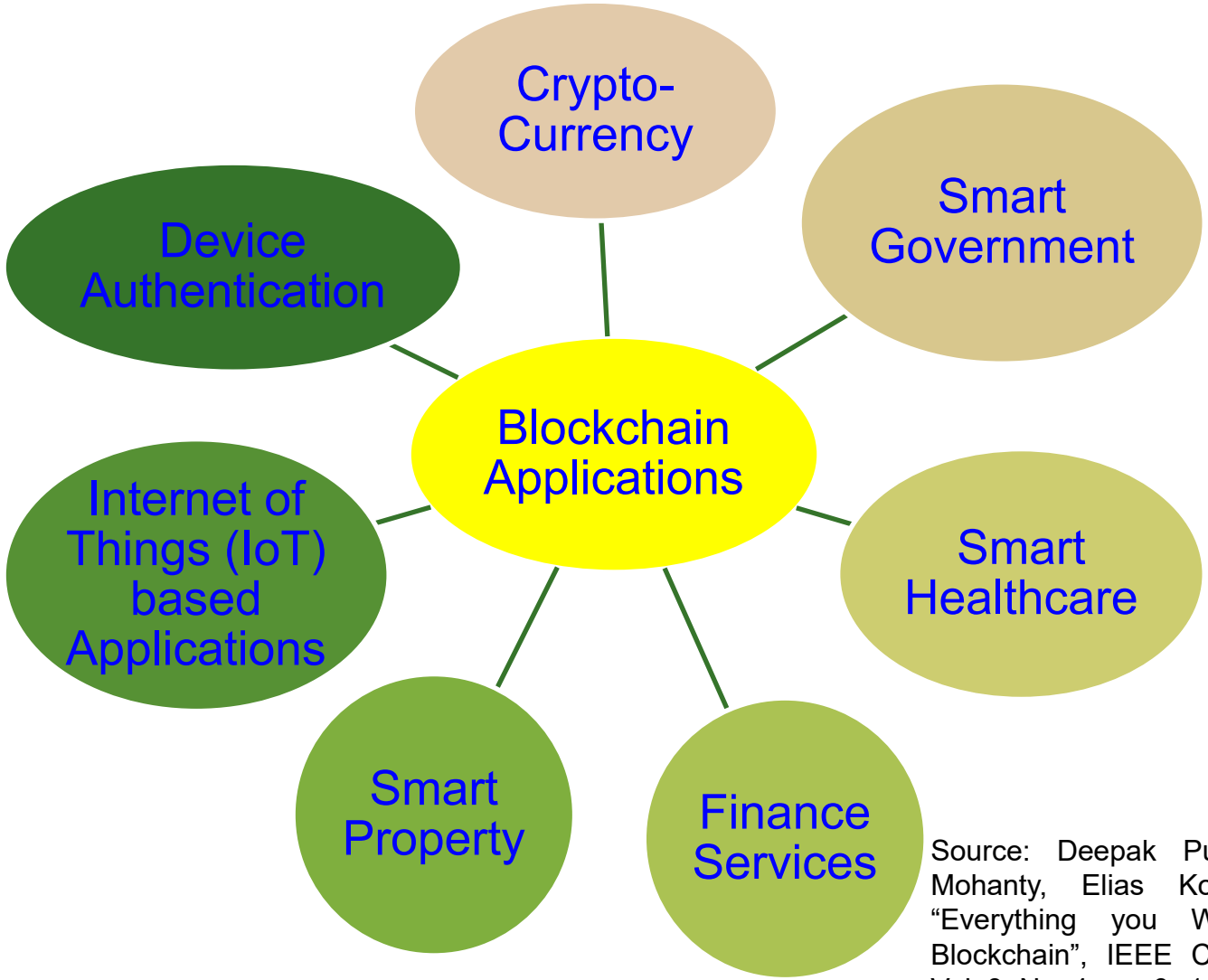
Blockchain Technology





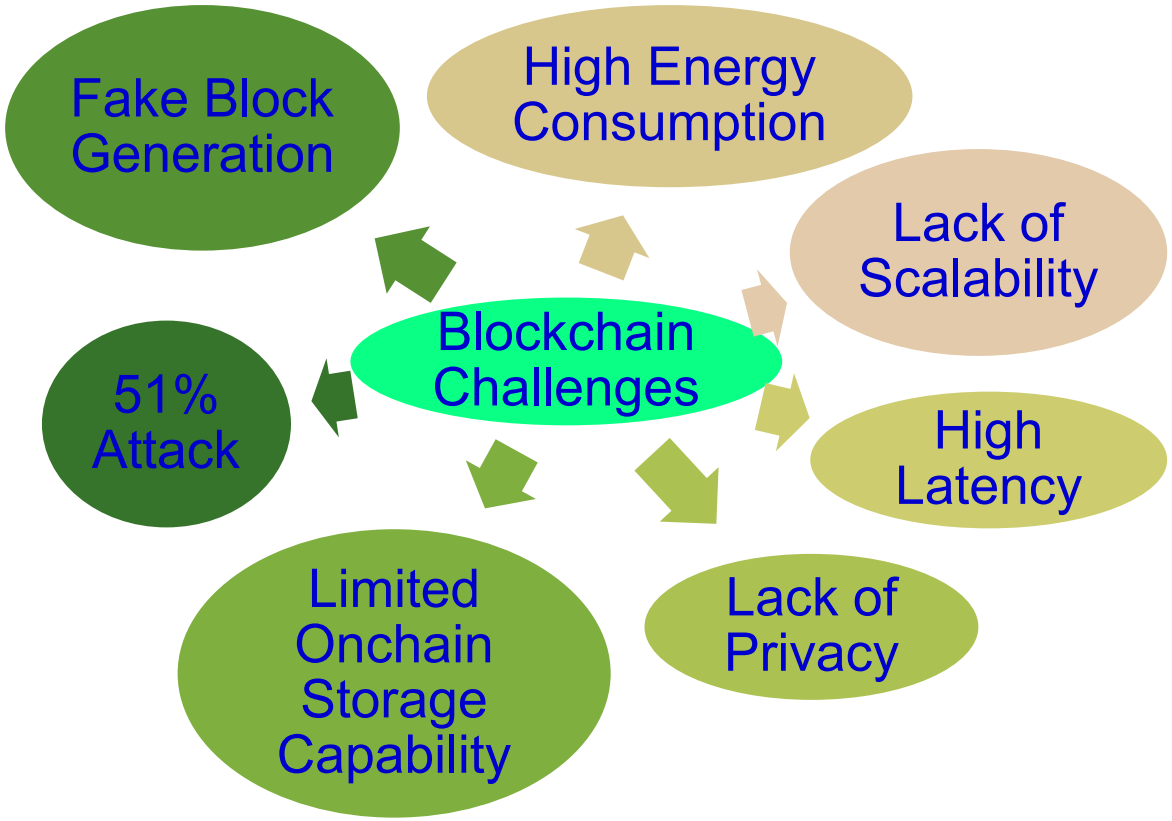
Source: https://icomalta.com/distributed-ledger-technology/

Blockchain Applications



Source: Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das, "Everything you Wanted to Know about the Blockchain", IEEE Consumer Electronics Magazine, Vol. 8, No. 4, pp. 6--14, 2018.

Blockchain has Many Challenges



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 Energy Need is Huge

Energy for mining of 1 bitcoin

=

Energy consumption 2 years of a US household

Blockchain Energy Need is Huge

Energy consumption for each bitcoin transaction

=

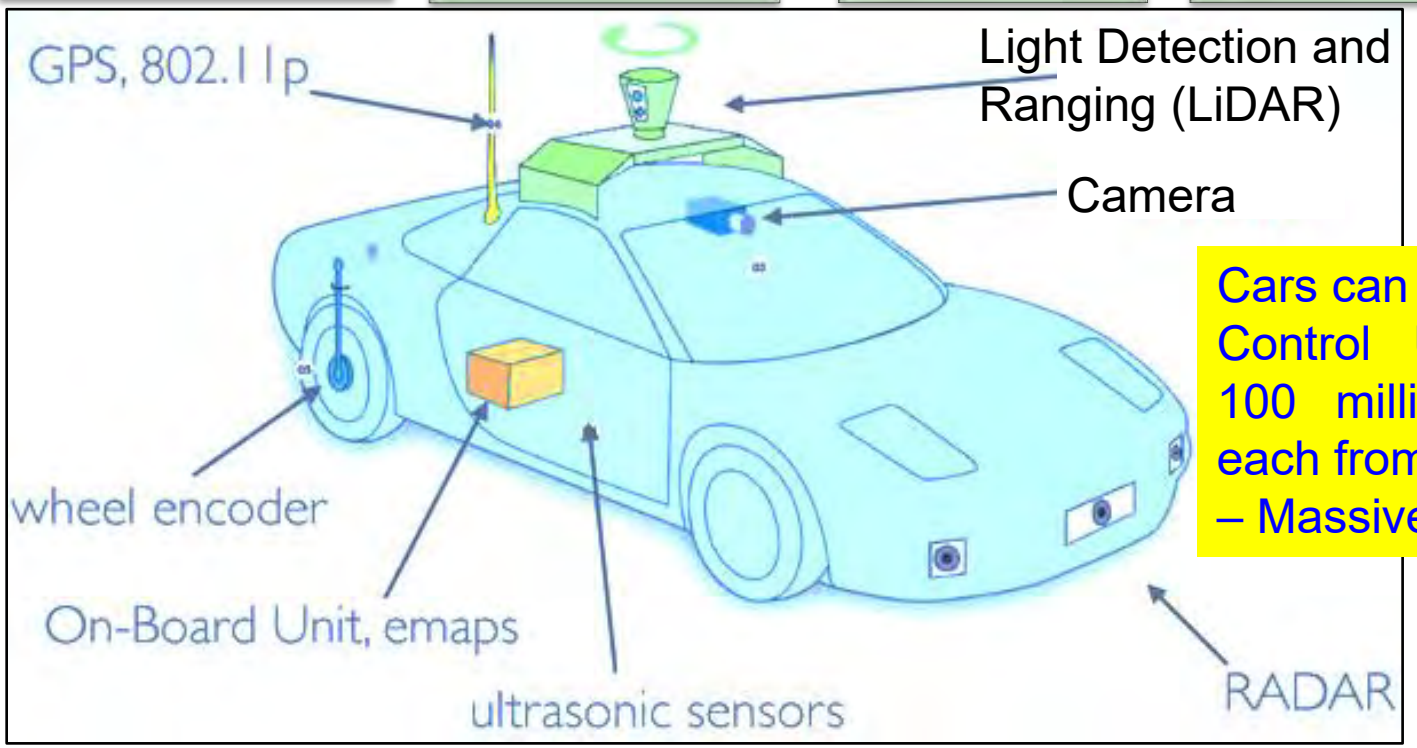
80,000X

Energy consumption of a credit card processing

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

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

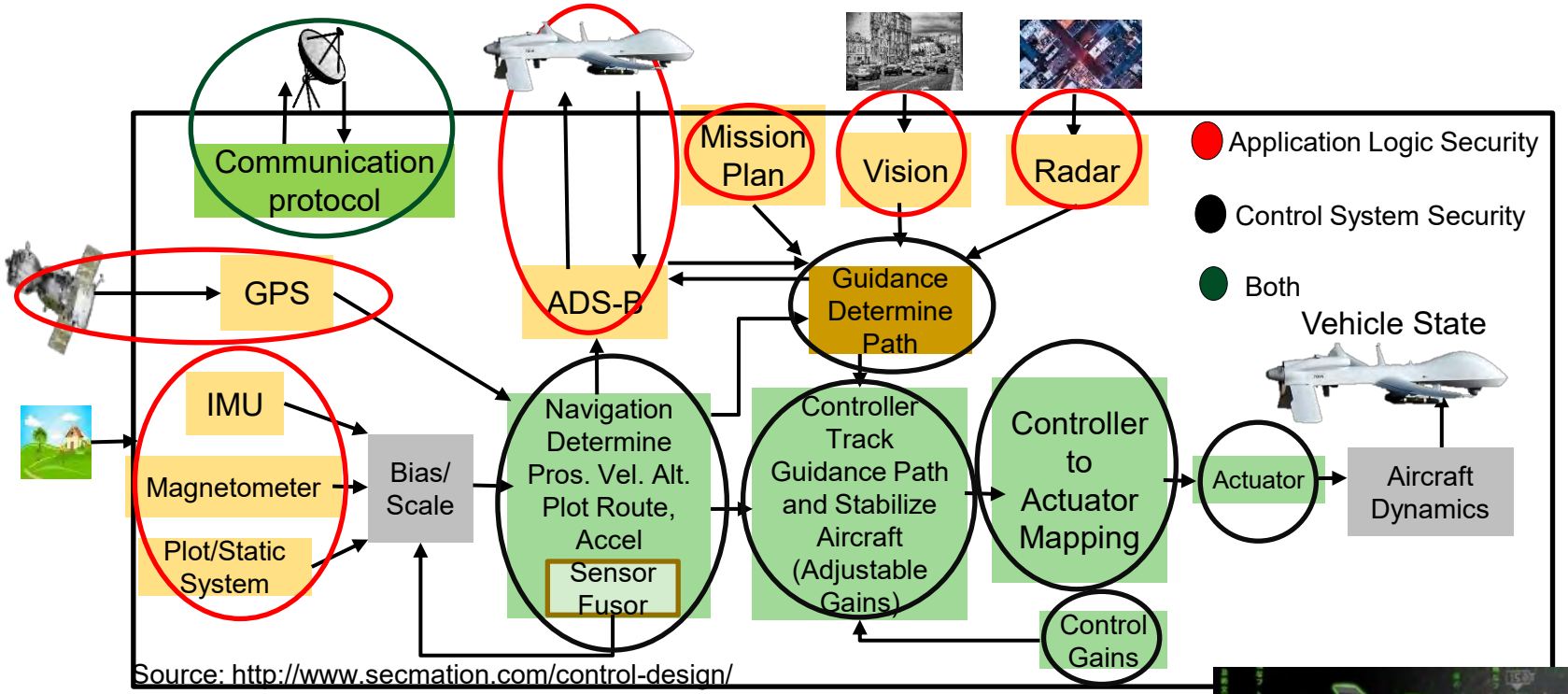
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

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



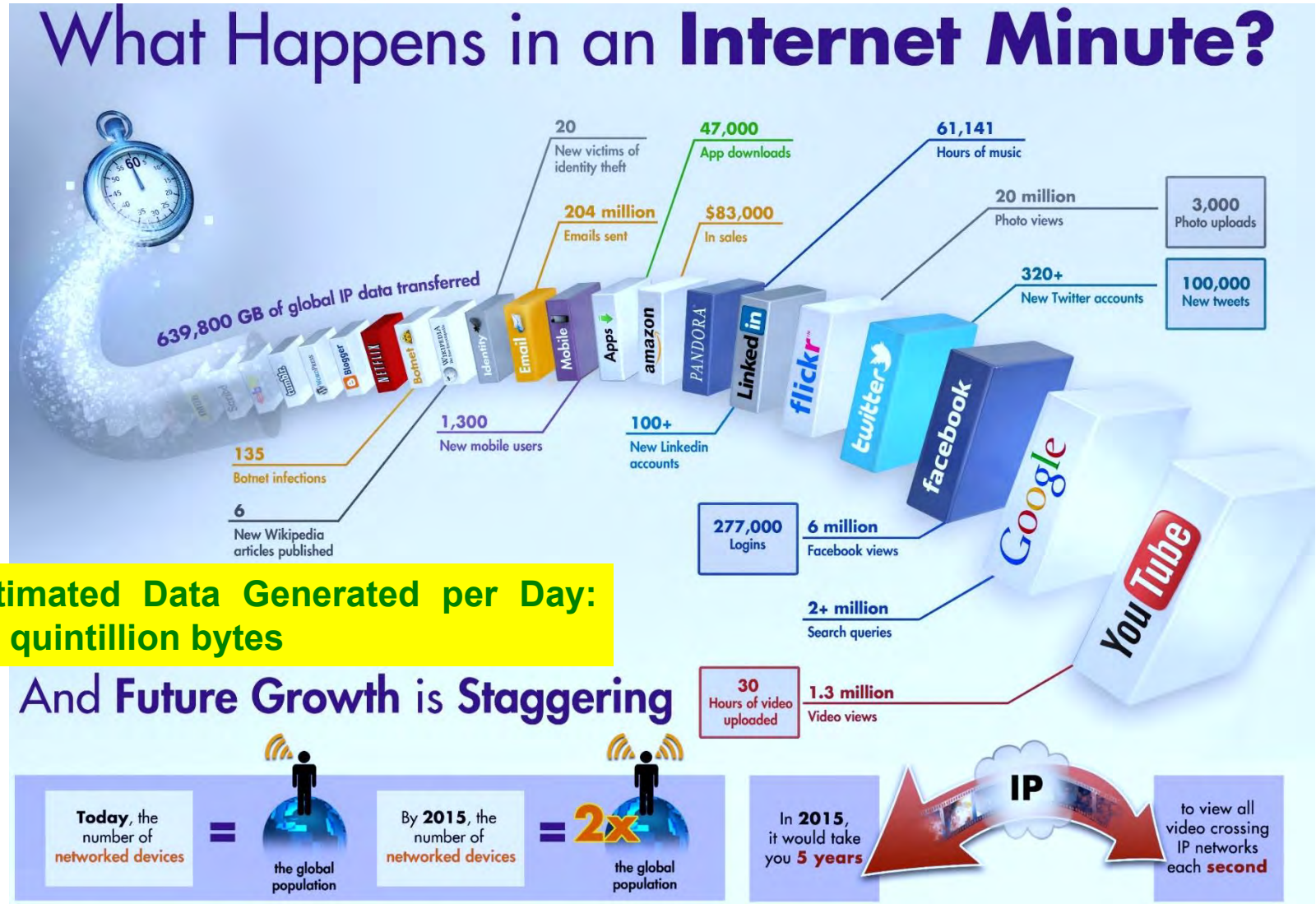
Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

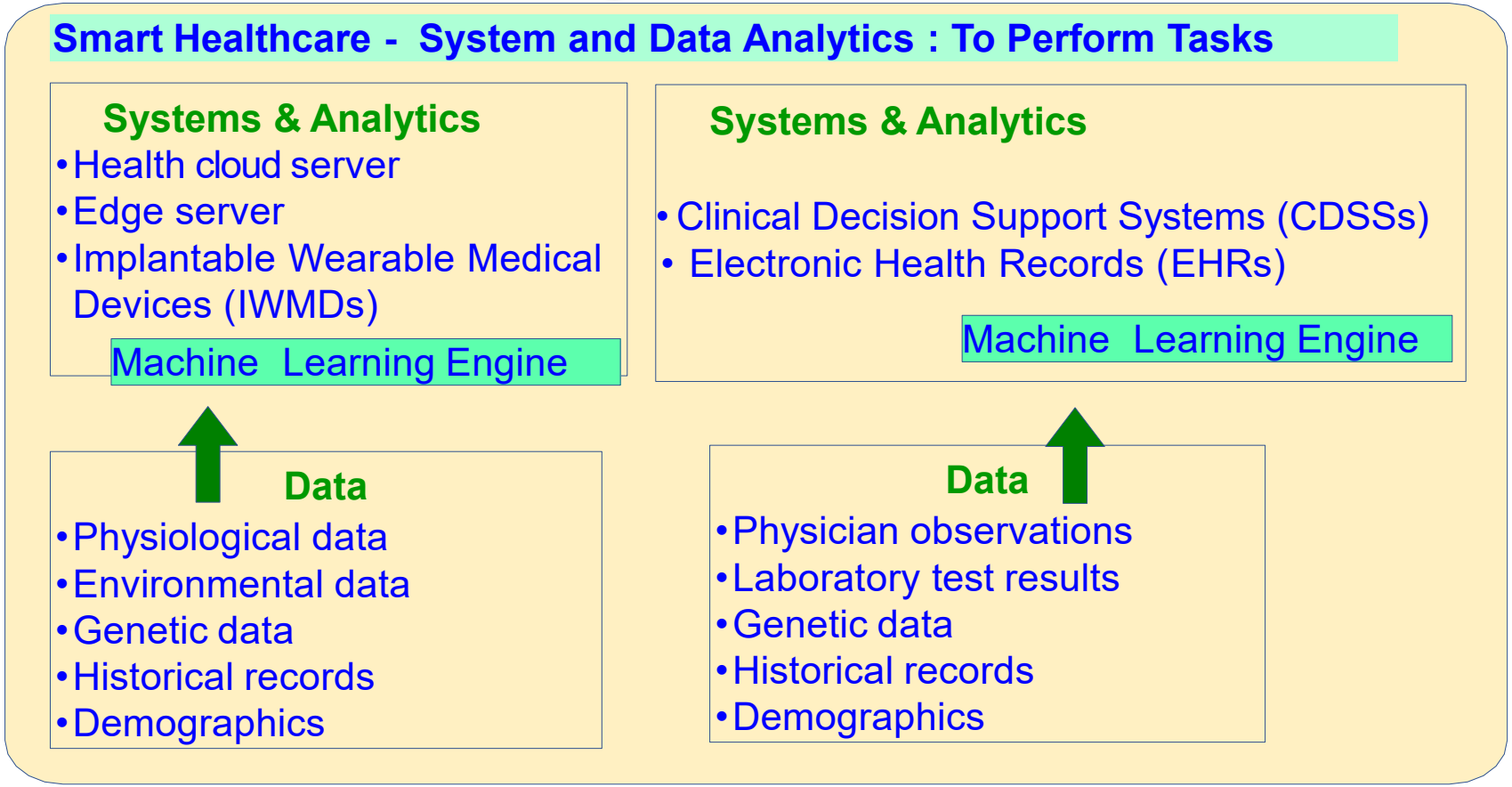
UAV Security – Energy and Latency Constraints

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

Huge Amount of Data

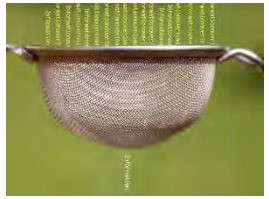


Data Holds the Key for Intelligence in CPS



Source: Hongxu Yin, Ayten Ozge Akmandor, Arsalan Mosenia and Niraj K. Jha (2018), "Smart Healthcare", *Foundations and Trends® in Electronic Design Automation*, Vol. 12: No. 4, pp 401-466. http://dx.doi.org/10.1561/1000000054

Challenges of Data in CPS are Multifold



Data Curation

Data Cost

Data Storage

Lots of Data

Data Ownership

Data Modeling

Data Quality

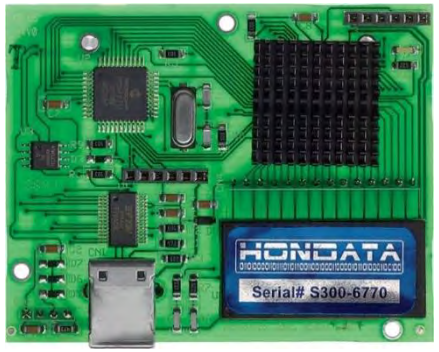
Fake Data and Fake Hardware – Both are Equally Dangerous in CPS

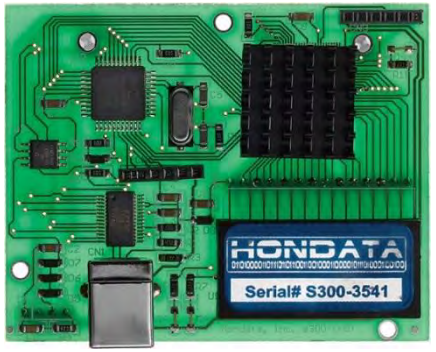
AI can be fooled by fake data

AI can create fake data (Deepfake)

Authentic Fake

An implantable medical device





Authentic Fake

A plug-in for car-engine computers

ESR Tradeoffs for Smart Electronic Systems

Security of systems and data.

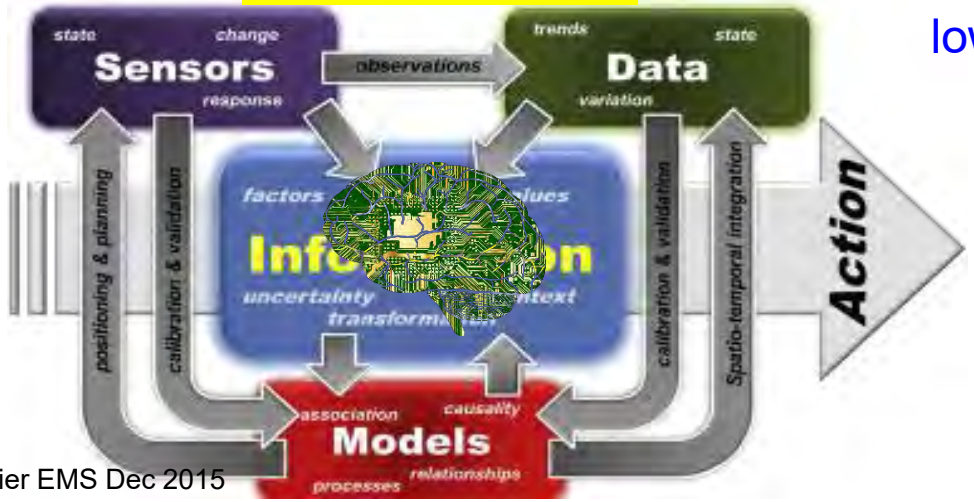
Cybersecurity

Energy

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

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

Intelligence



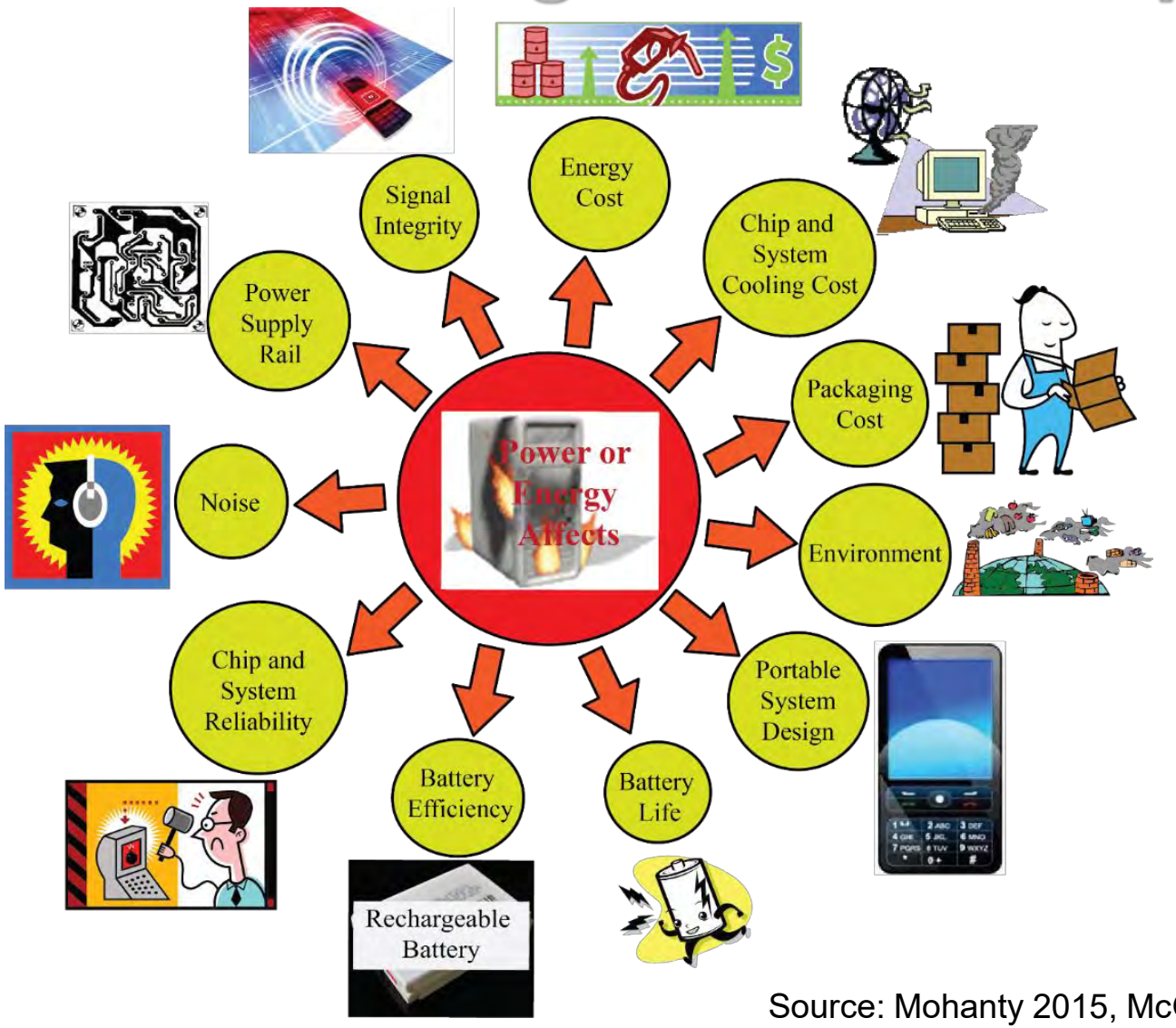
Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Source: Mohanty iSES 2018 Keynote

Energy Smart

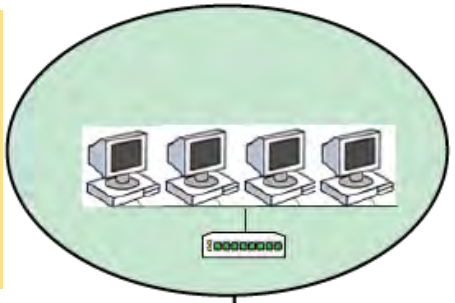
The Effects of High-Power Dissipation



Source: Mohanty 2015, McGraw-Hill 2015

Energy Consumption Challenge in IoT

Energy from Supply/Battery - Energy consumed by Workstations, PC, Software, Communications



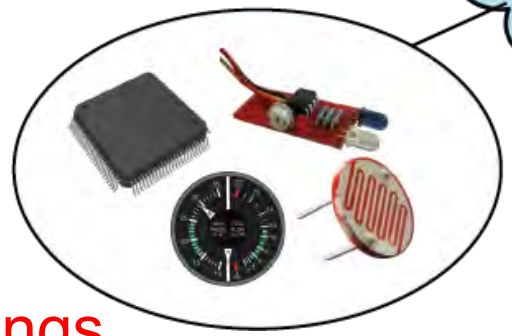
Local Area Network (LAN)

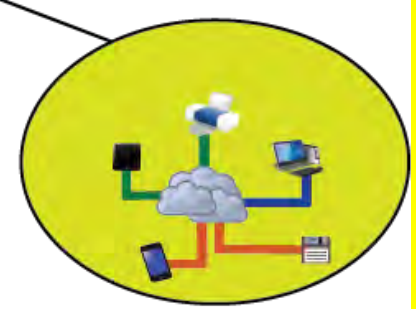
Energy from Supply/Battery - Energy consumed by Communications

Battery Operated - Energy consumed by Sensors, Actuators, Microcontrollers

Internet

The Cloud





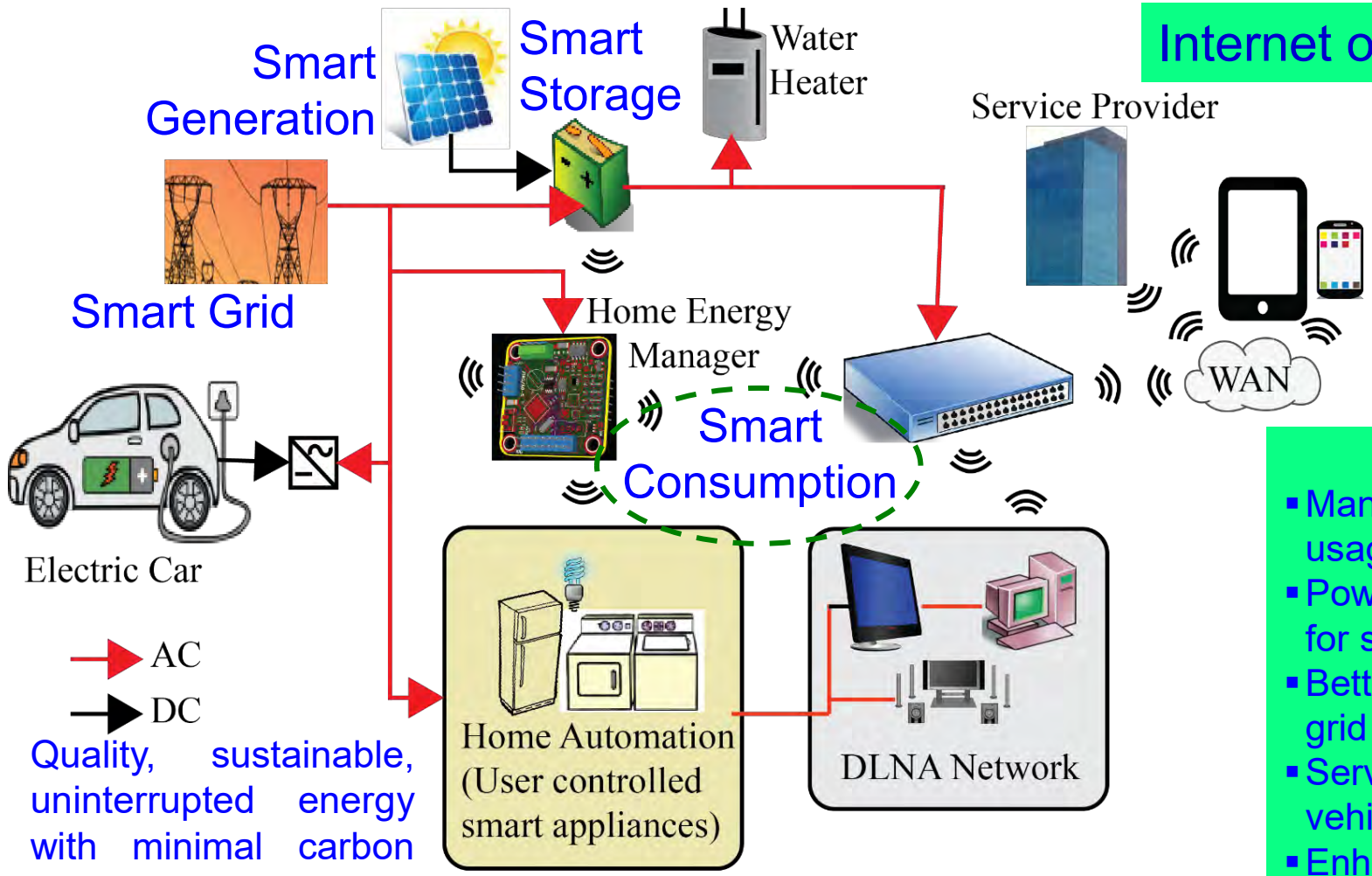
Energy from Supply - Energy consumed in Server, Storage, Software, Communications

The Things

Four Main Components of IoT.

Source: Mohanty iSES 2018 Keynote

Smart Energy



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

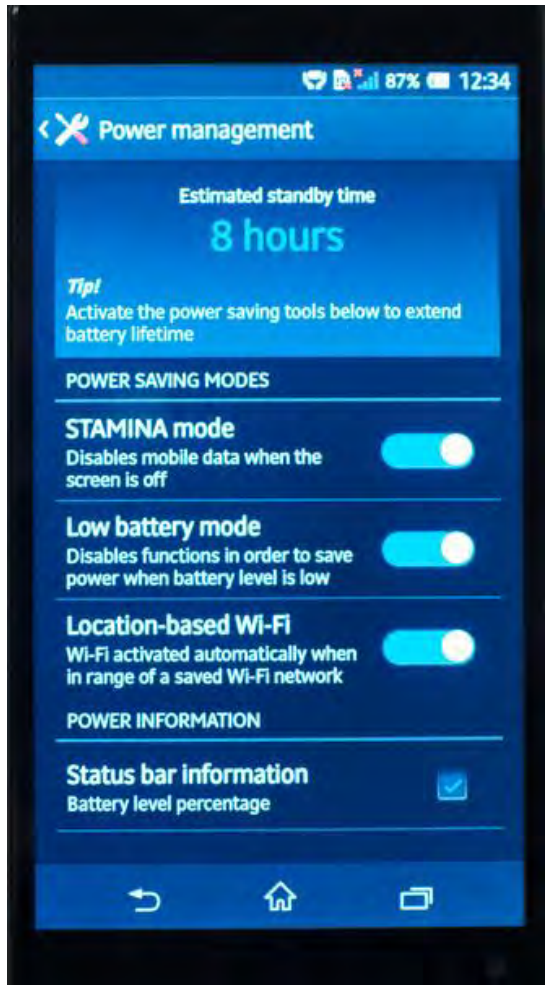
Source: Mohanty 2016, CE Magazine July 2016

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

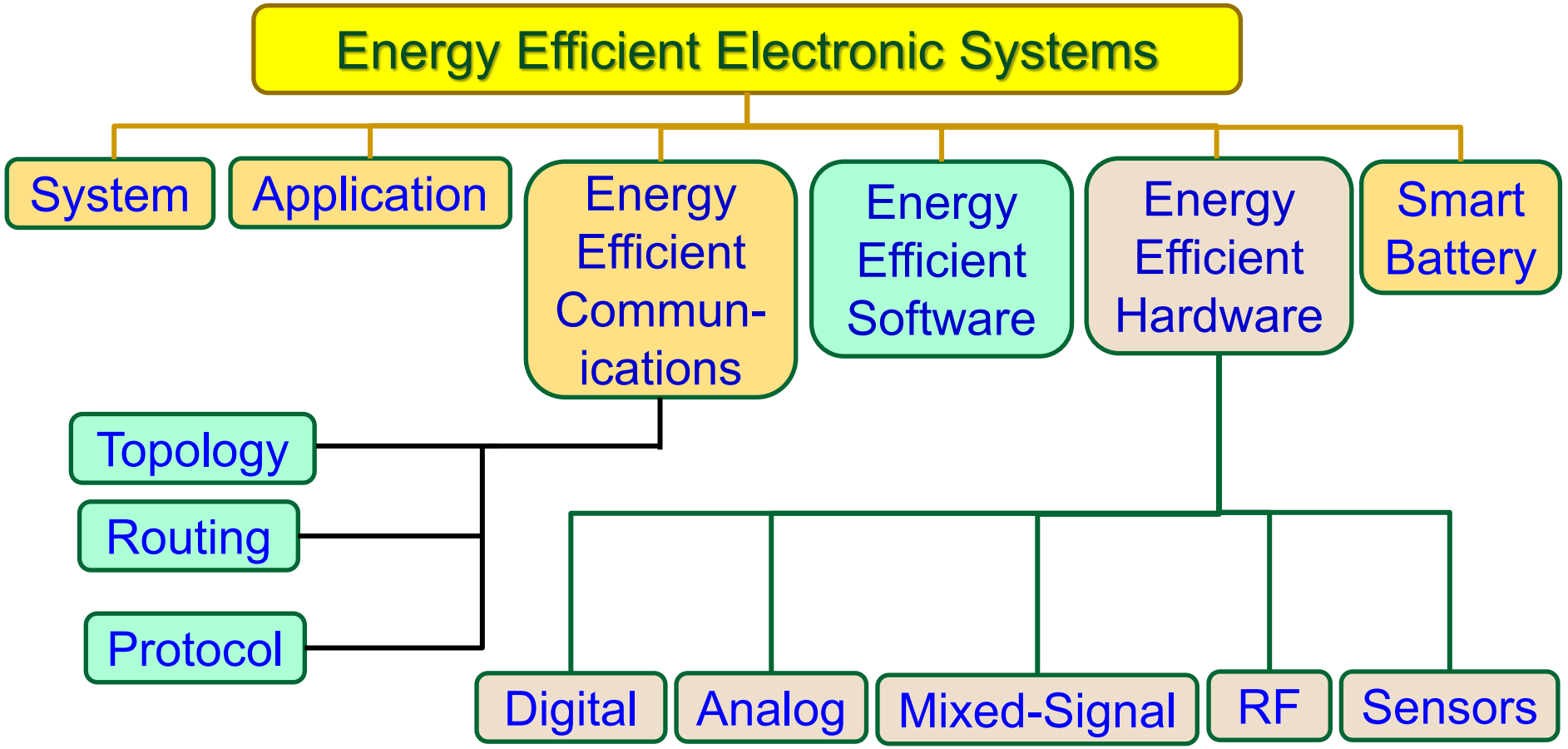
Smart Energy – Smart Consumption



Battery Saver

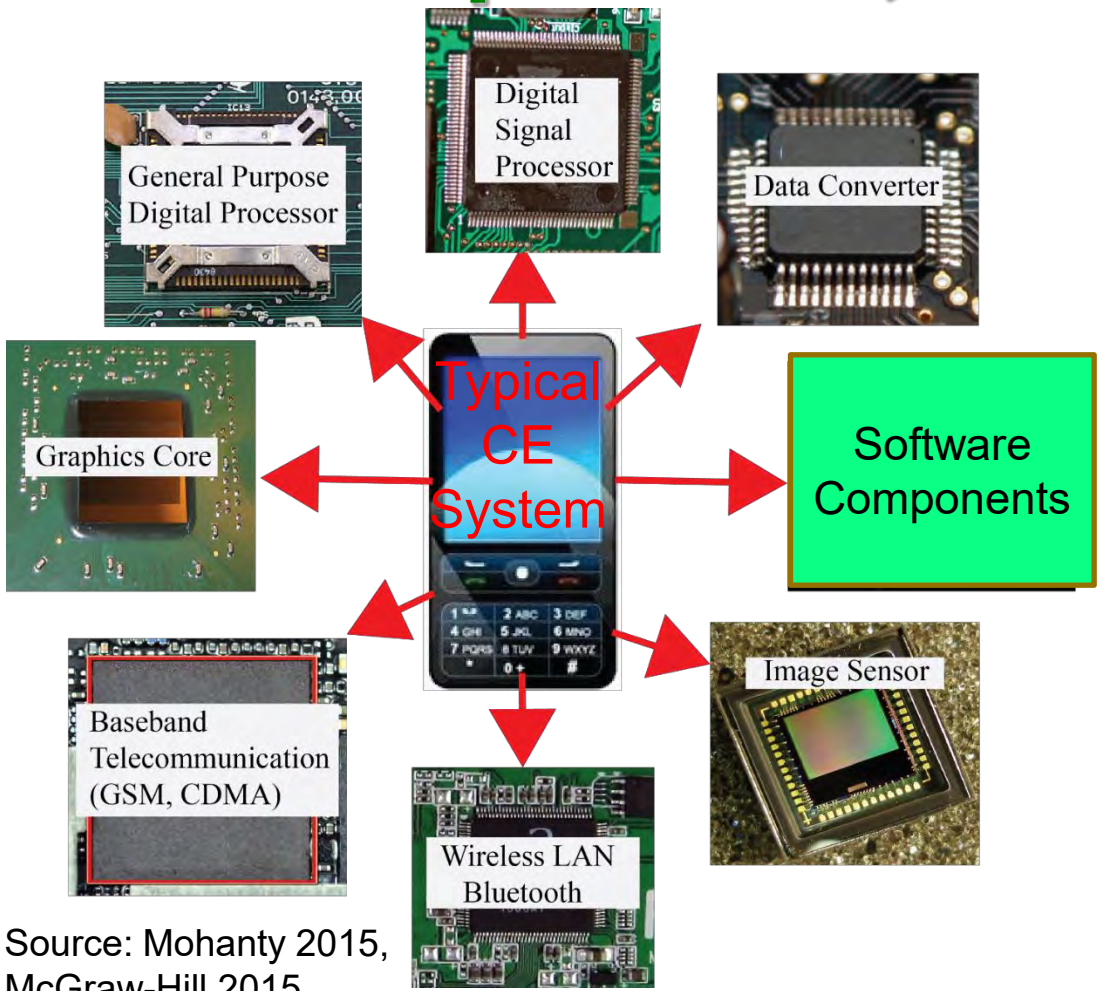
Smart Home

Energy Efficient Electronics: Possible Solution Fronts

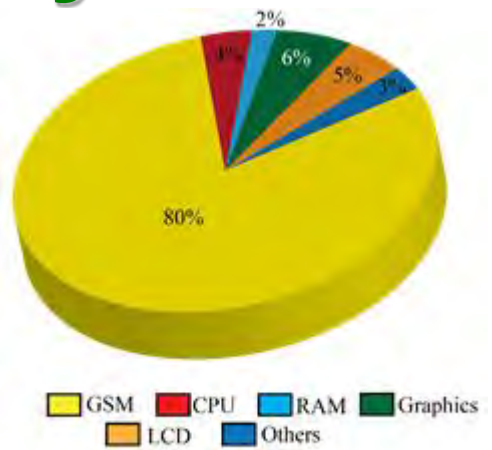


Source: Mohanty ZINC 2018 Keynote

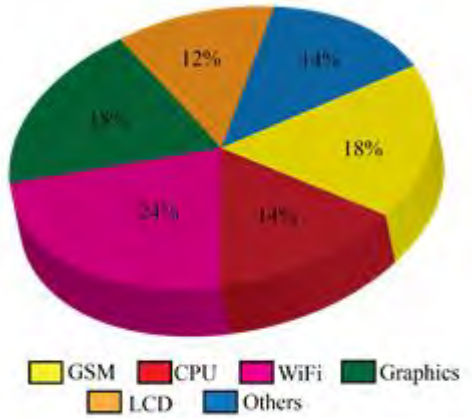
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015

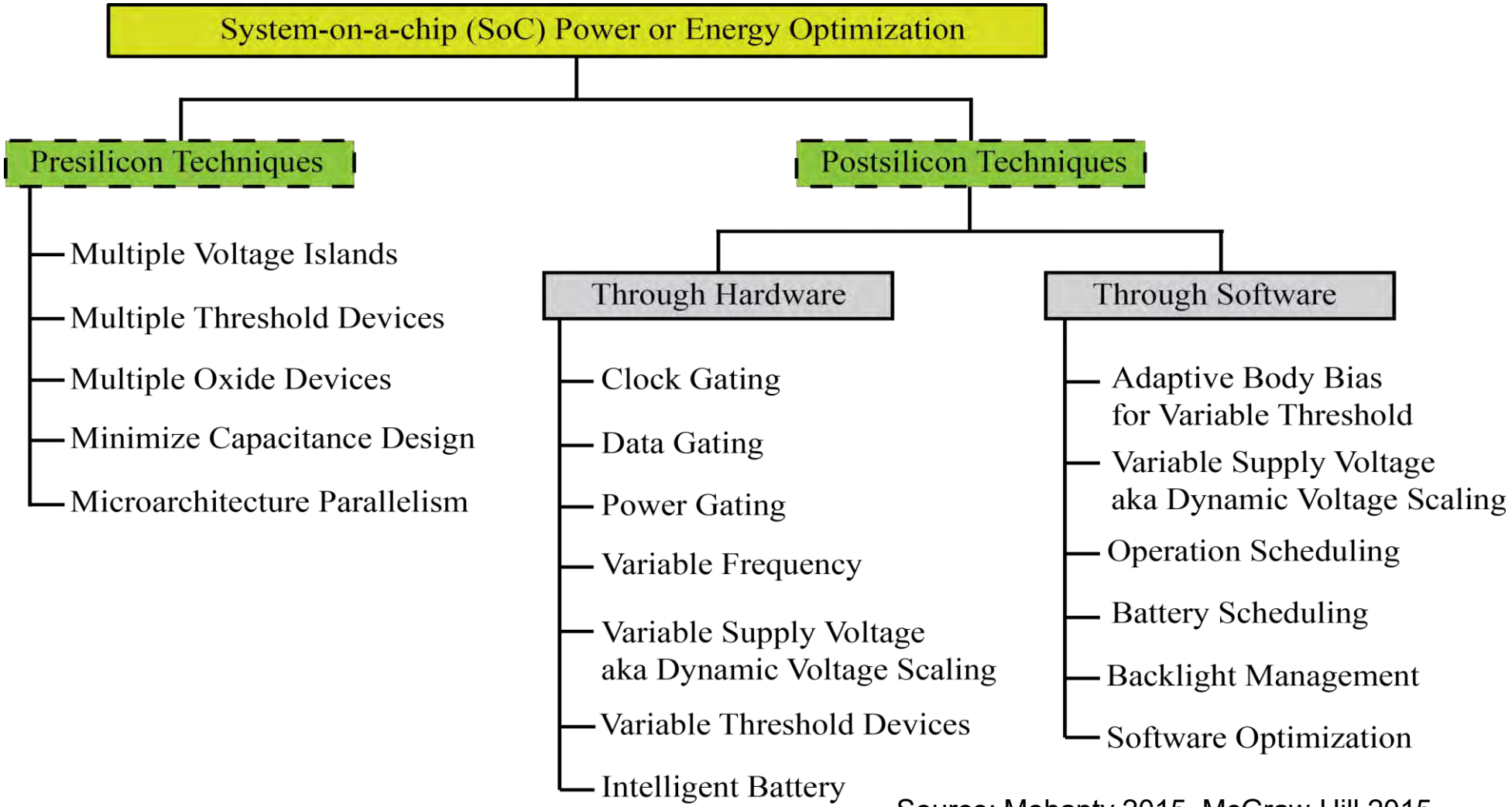


During GSM Communications



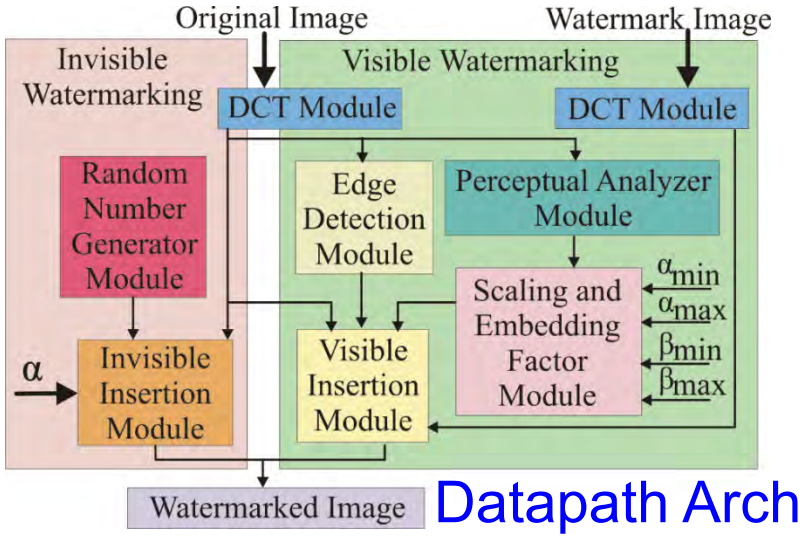
During WiFi Communications

Energy Reduction in CE Hardware

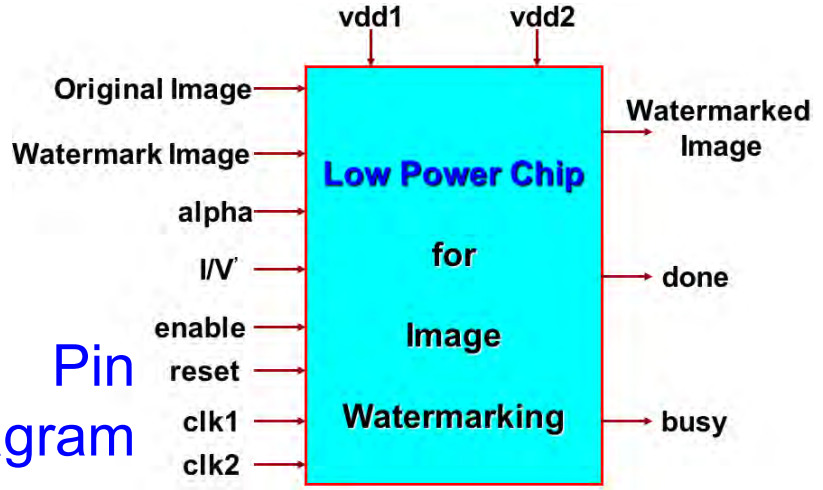


Source: Mohanty 2015, McGraw-Hill 2015

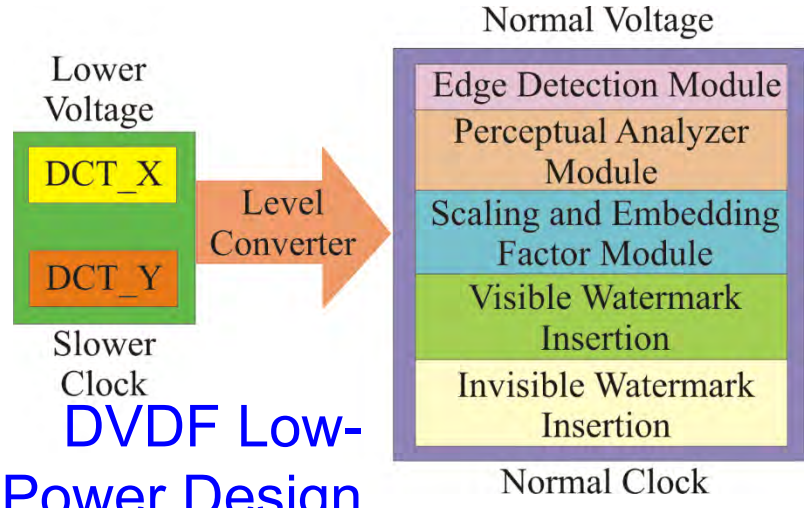
Energy-Efficient Hardware - Dual-Voltage



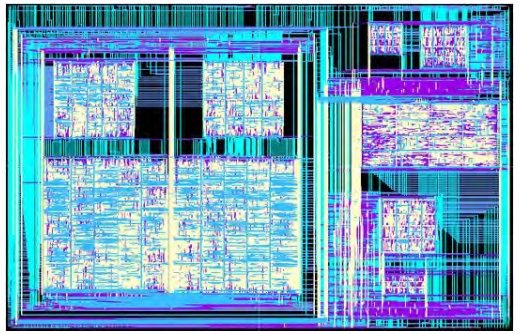
Datapath Architecture



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: Mohanty 2006, TCASII May 2006

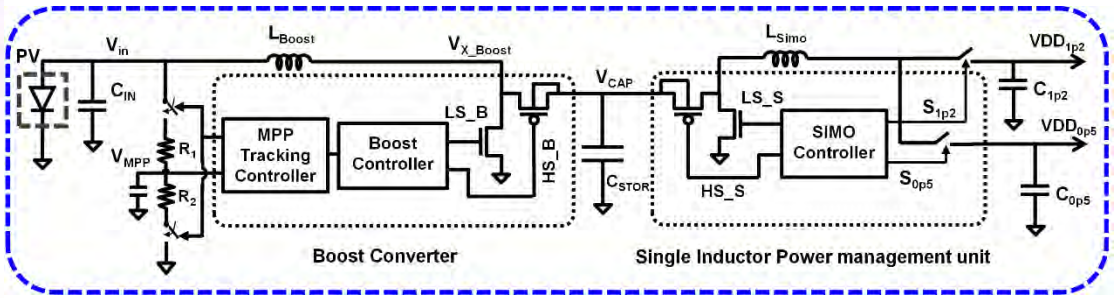
Battery-Less IoT

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/

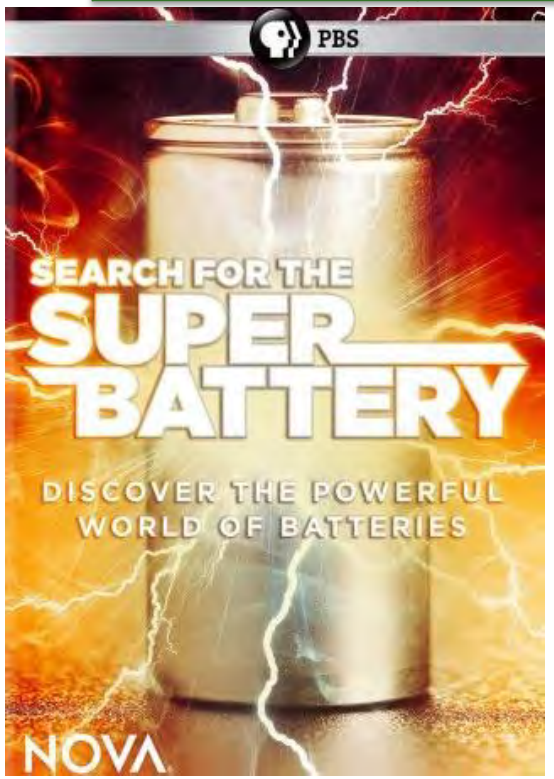


Energy Harvesting and Power Management

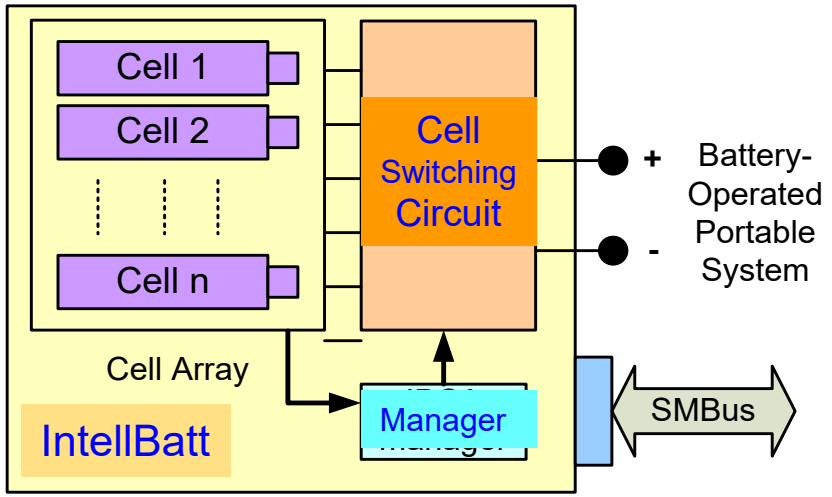
Source: http://rlpvlsi.ece.virginia.edu/node/368

Energy Storage - High Capacity and Efficiency Needed

Battery	Conversion Efficiency
Li-ion	80% - 90%
Lead-Acid	50% - 92%
NiMH	66%



Intelligent Battery



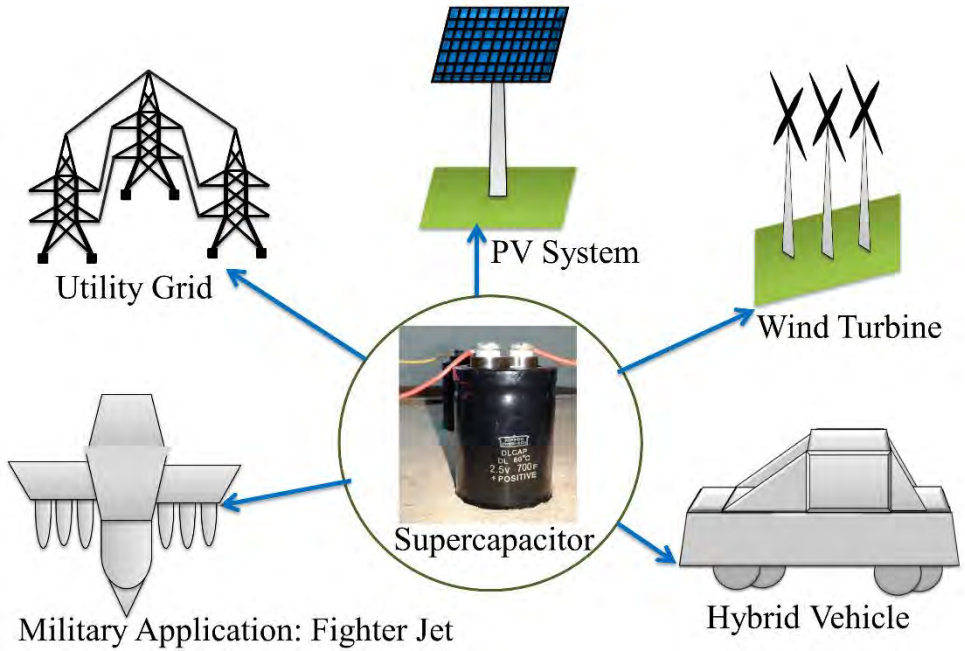
Mohanty 2010: IEEE Computer, March 2010
Mohanty 2018: ICCE 2018

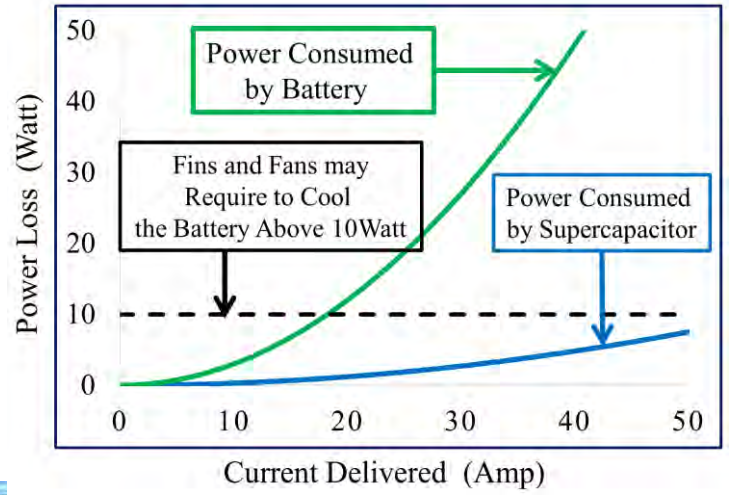
Lithium Polymer Battery

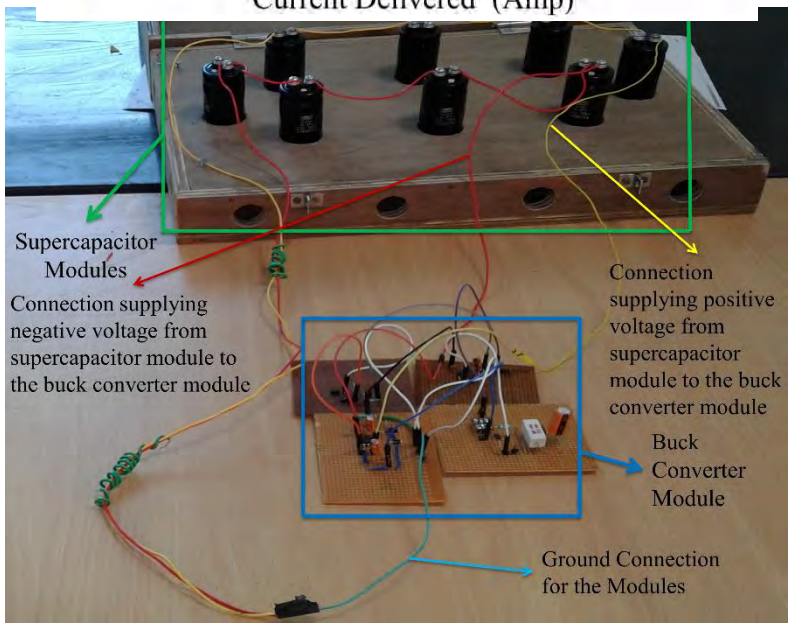
Supercapacitor

Source: Mohanty MAMI 2017 Keynote

Supercapacitor based Power for CE





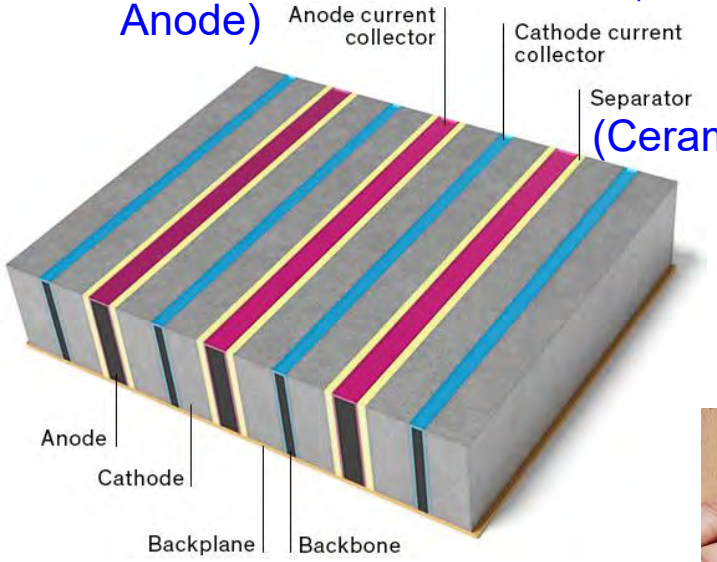


Source: Mohanty 2018, CEM Sep 2018

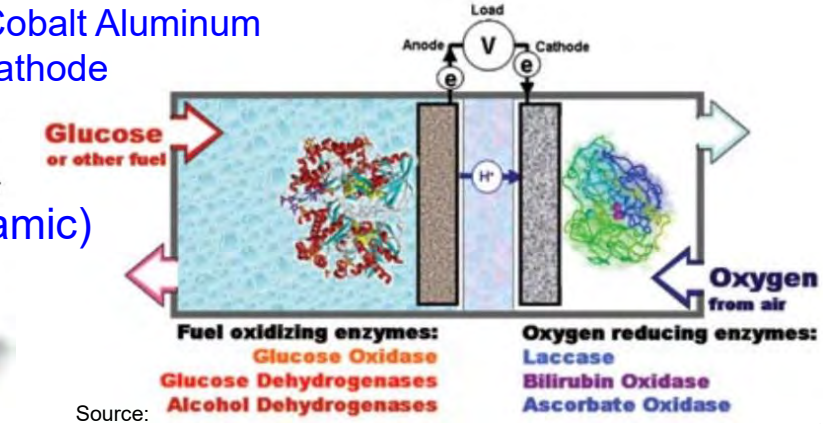
Energy Storage - High Capacity and Safer Needed

(Silicon Anode)

(Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode

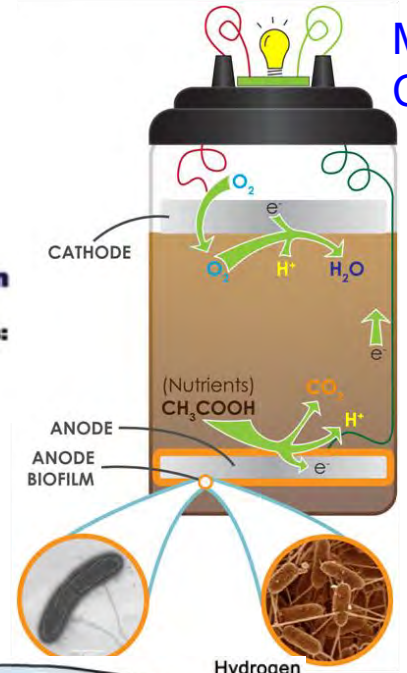


Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery

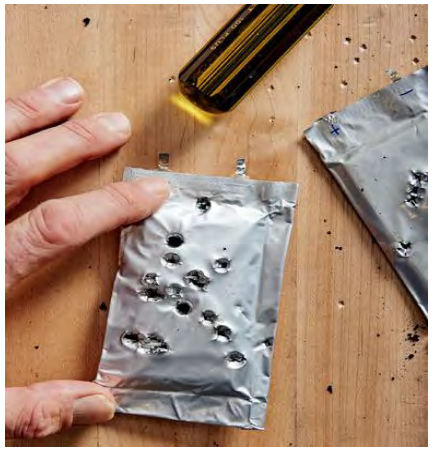


Source: https://www.electrochem.org/dl/interface/sum/sum07/su07_p28_31.pdf

Enzymatic Biofuel Cell



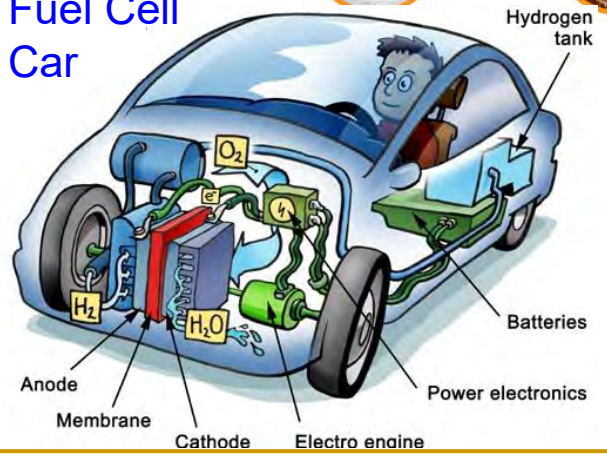
Microbial Fuel Cell (MFC)



Solid Polymer Lithium Metal Battery

Source: https://www.nytimes.com/2016/12/11/technology/designing-a-safer-battery-for-smartphones-that-wont-catch-fire.html

Fuel Cell Car



Energy Storage Efficiency and Safety

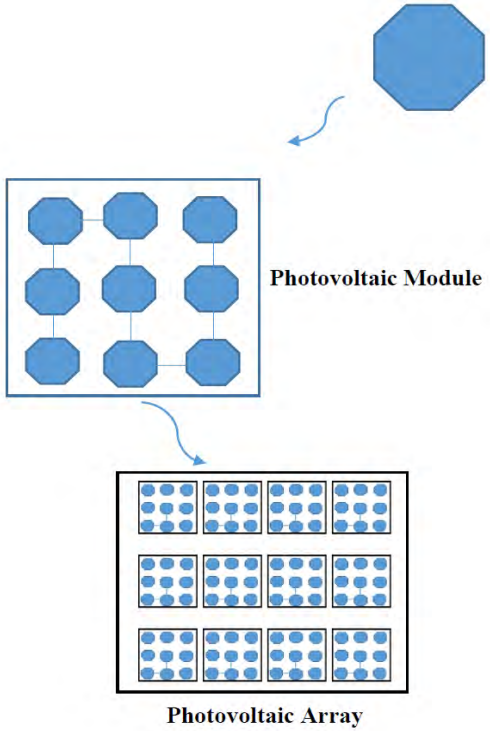
One 787 Battery: 12 Cells / 32 V DC

Source: http://www.newairplane.com

- Boeing 787's across the globe were grounded.

Smartphone Battery

Energy Conversion Efficiency

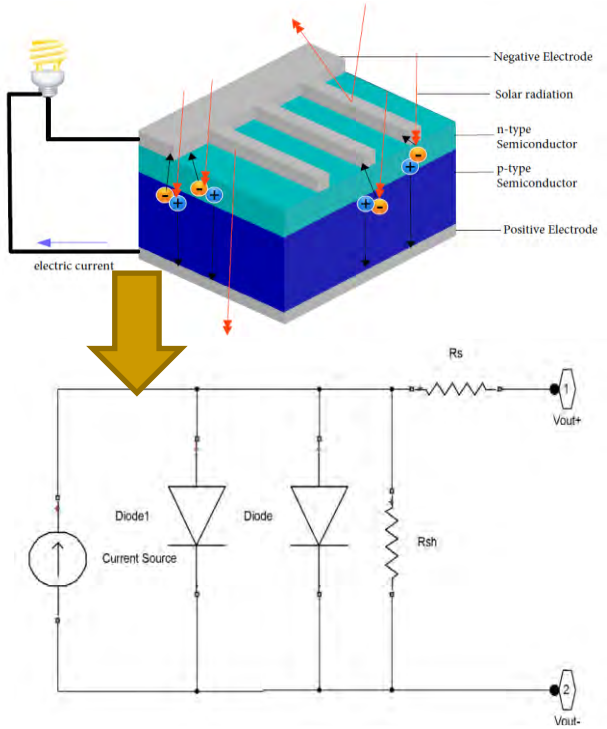


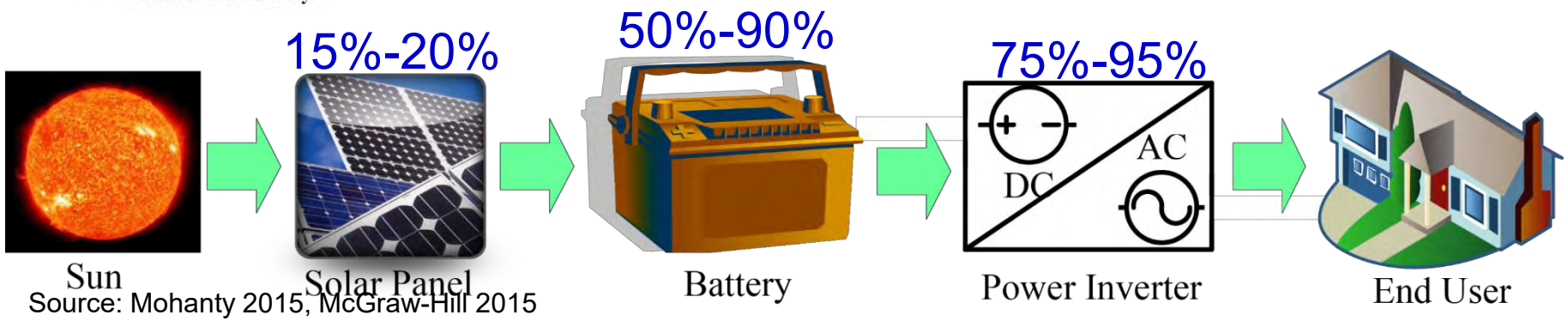
Small solar cells in CE systems to big solar panels in smart grids.

Solar Cell Efficiency:

Research stage: 46%

Commercial: 18%





Source: Mohanty 2015, McGraw-Hill 2015

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

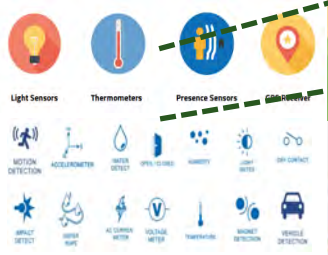
Solar Cell

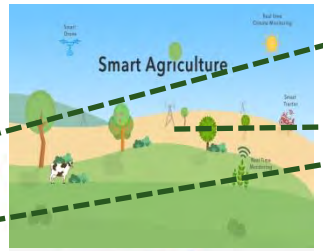
Harvesting System with Physically Unclonable Function (PUF)

Sensors

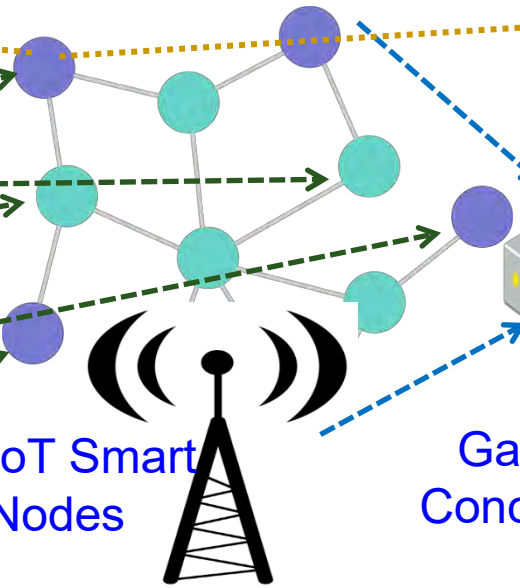
System-on-Chip (SoC)

Trans-receiver

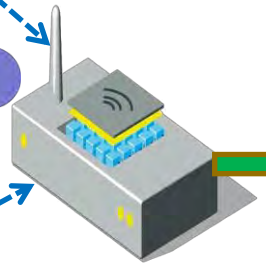




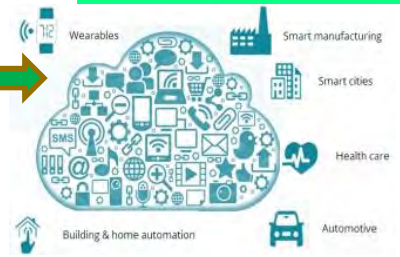
Edge Devices and their deployment



IoT Smart Nodes



Gateways/ Concentrators

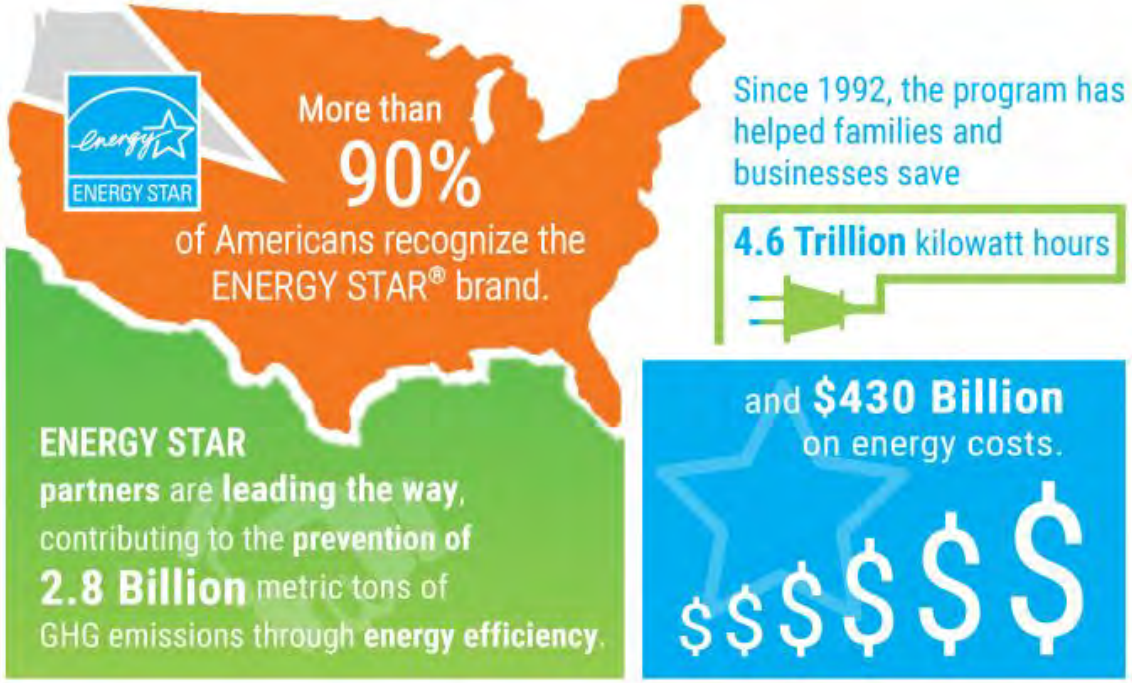


IoT-Cloud

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

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 2021, pp. doi: 10.1109/TSUSC.2020.2987616.

Energy Star Ratings



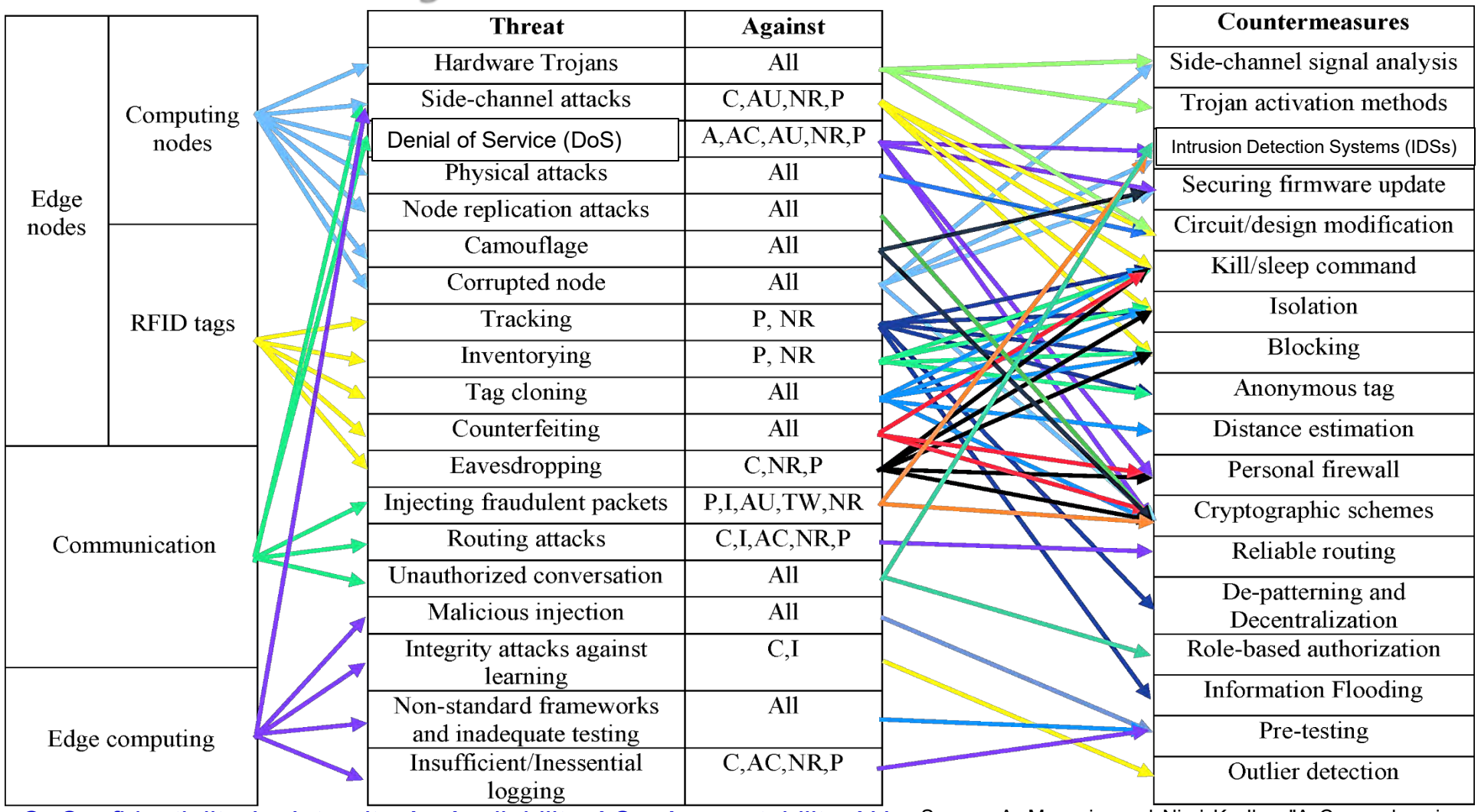
Source: https://www.energystar.gov/about/2017_energy_star_award_winners

Source: https://www.breeam.com/

Source: https://new.usgbc.org/leed

(Cyber)Security Smart

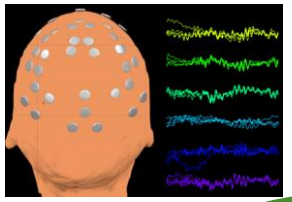
IoT Security - Attacks and Countermeasures

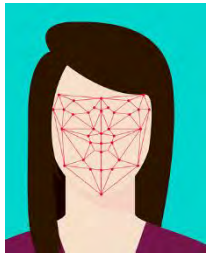


C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

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

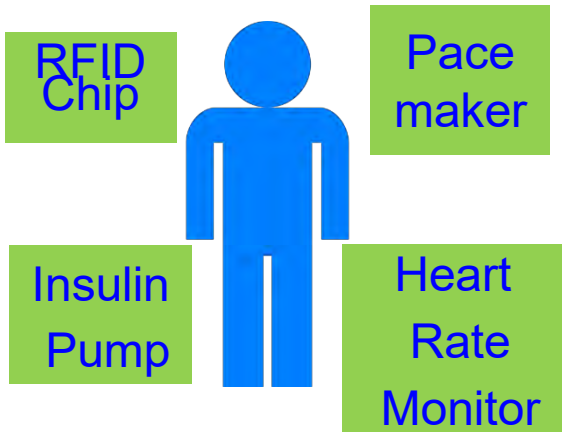
Online Signature

Touch-Screen Pattern

Source: Mohanty ISCT 2019 Keynote

CE Systems – Diverse Security/ Privacy/ Ownership Needs

Medical Devices

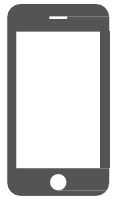


Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices



Smart Phones/ Tablets

Wearable Devices

Smart Clothing

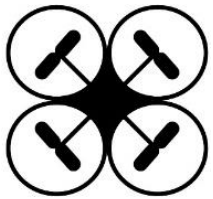
Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

Entertainment Devices



Drones /UAVs

Video Games

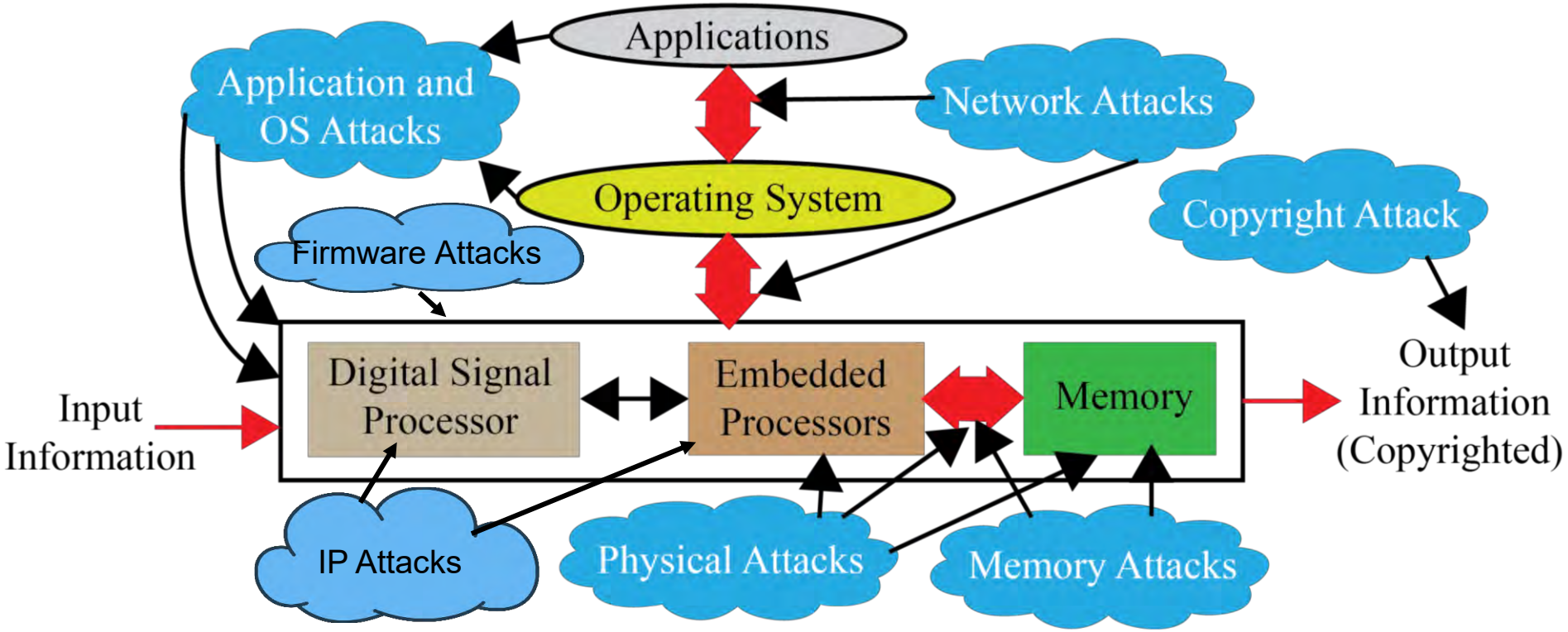
Transportation Devices

Smart Vehicles/ Autonomous Vehicles

Smart Traffic Controllers

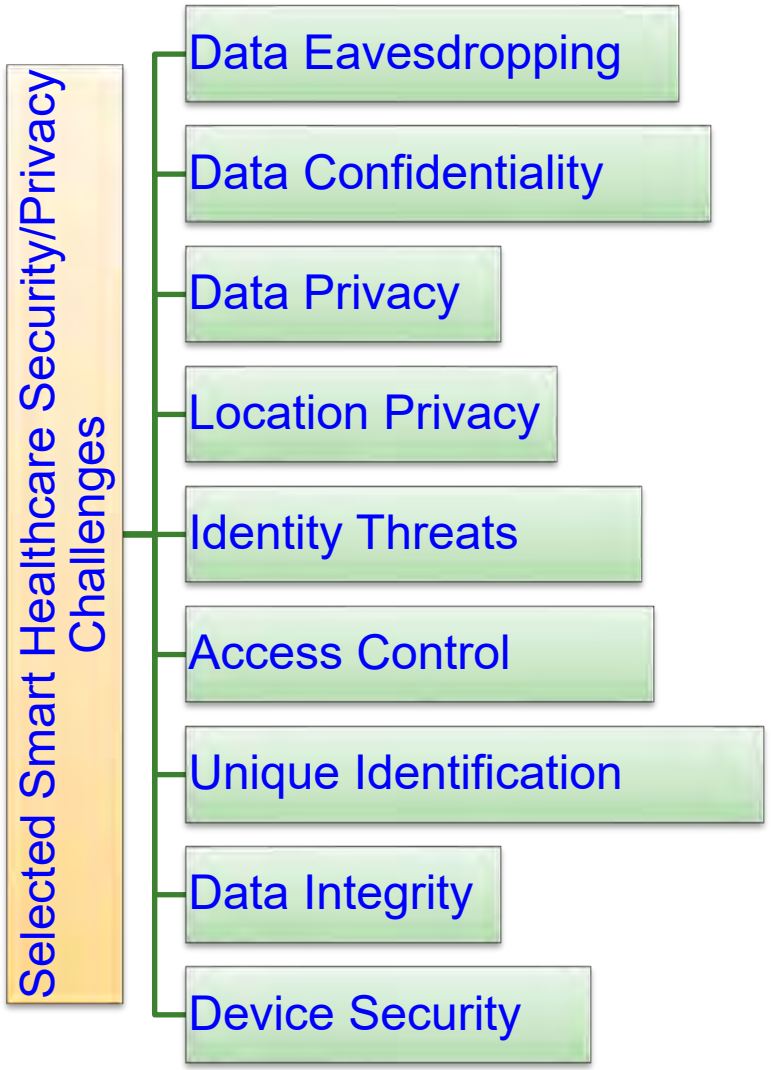
Source: Munir and Mohanty 2019, CE Magazine Jan 2019

Selected Attacks on a CE System – Security, Privacy, IP Right

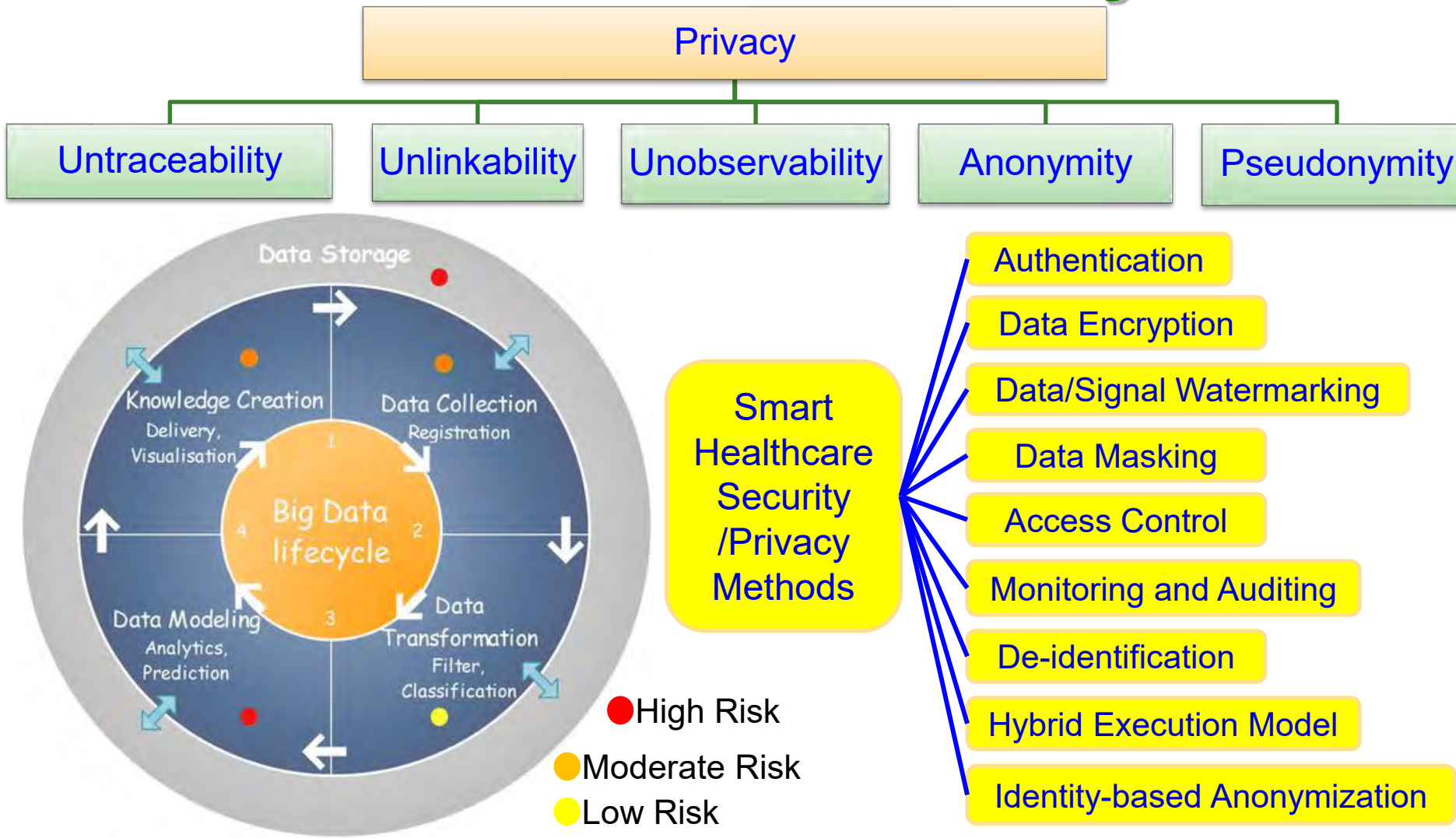


Diverse forms of Attacks, following are not the same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

Smart Healthcare - Security and Privacy Issue



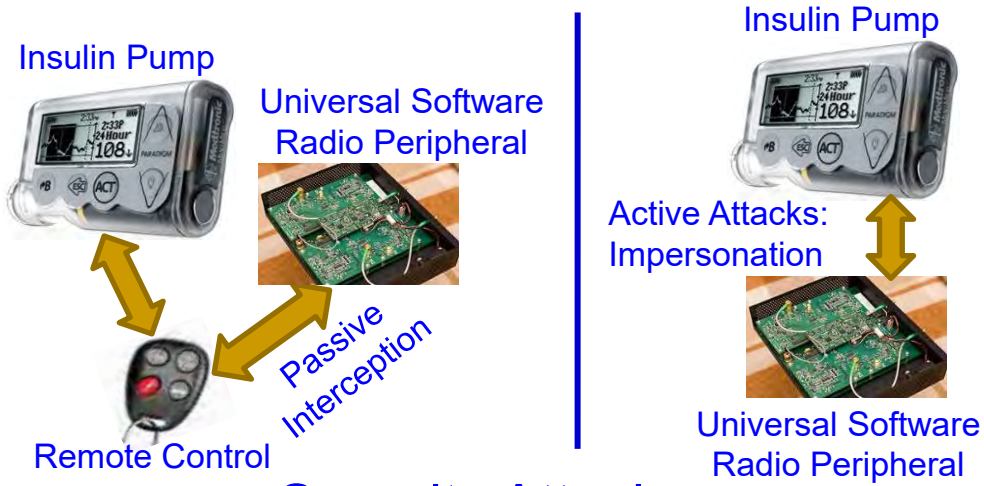
Smart Healthcare - Privacy Issue



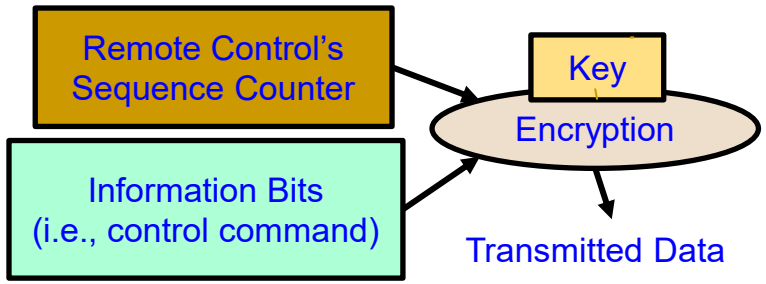
Source: Abouelmehdi et al., Springer BigData 2018 Dec

Smart Healthcare Security

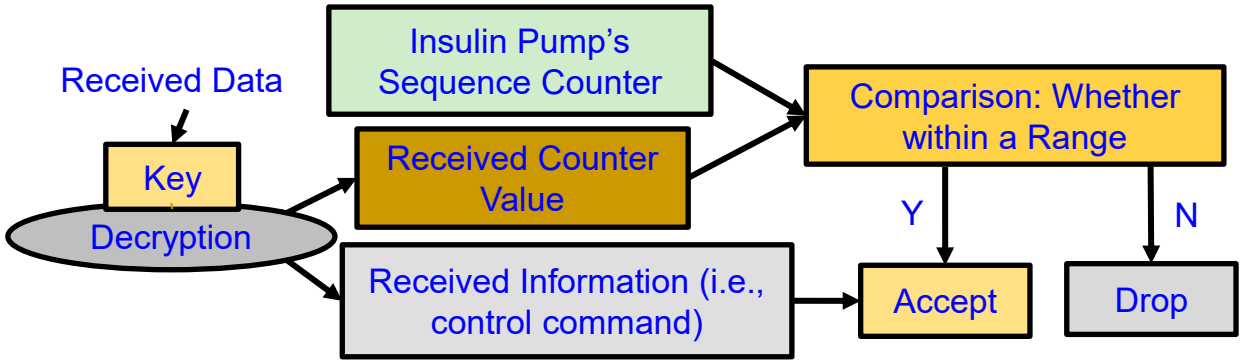
Insulin Delivery System



Security Attacks



Rolling Code Encoder in Remote Control

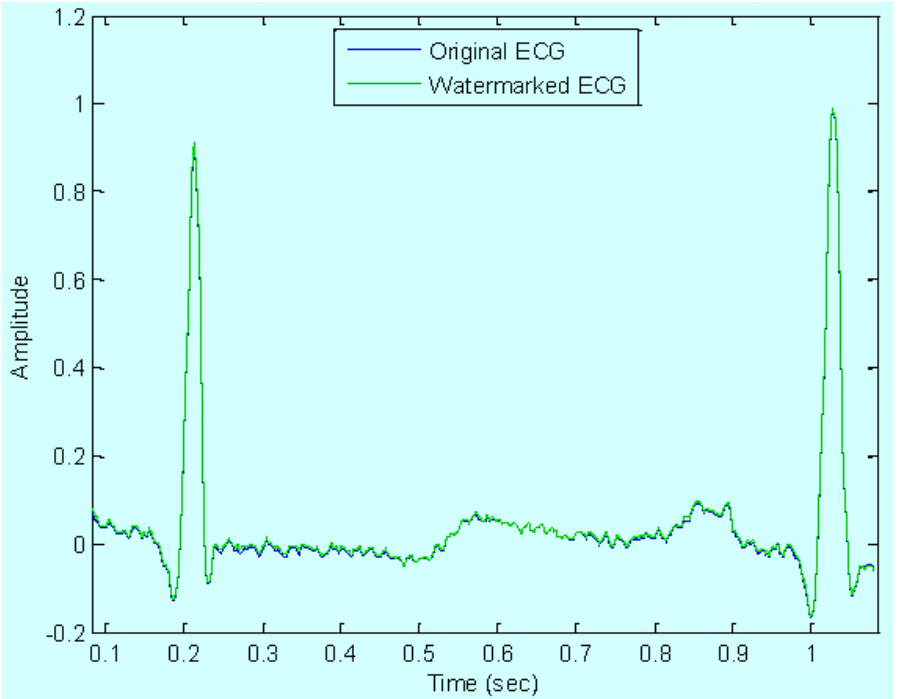


Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Smart Healthcare Security – Medical Signal Authentication

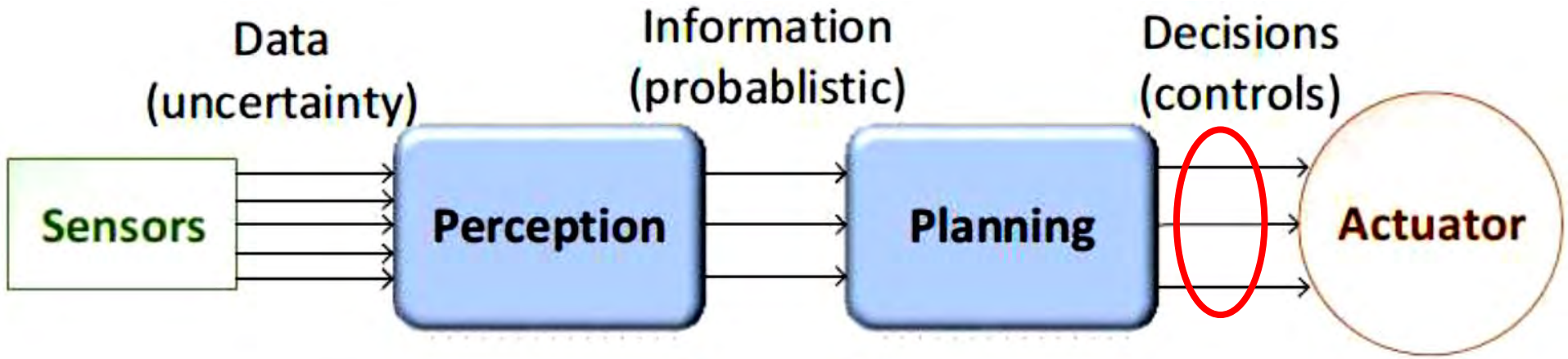
- Physiological signals like the electrocardiogram (EKG) are obtained from patients, transmitted to the cloud, and can also stored in a cloud repository.
- With increasing adoption of electronic medical records and cloud-based software-as-service (SaaS), advanced security measures are necessary.
- Protection from unauthorized access to Protected Health Information (PHI) also protects from identity theft schemes.
- From an economic stand-point, it is important to safeguard the healthcare and insurance system from fraudulent claims.



Source: Tseng 2014, Tseng Sensors Feb 2014

Smart Car – Decision Chain

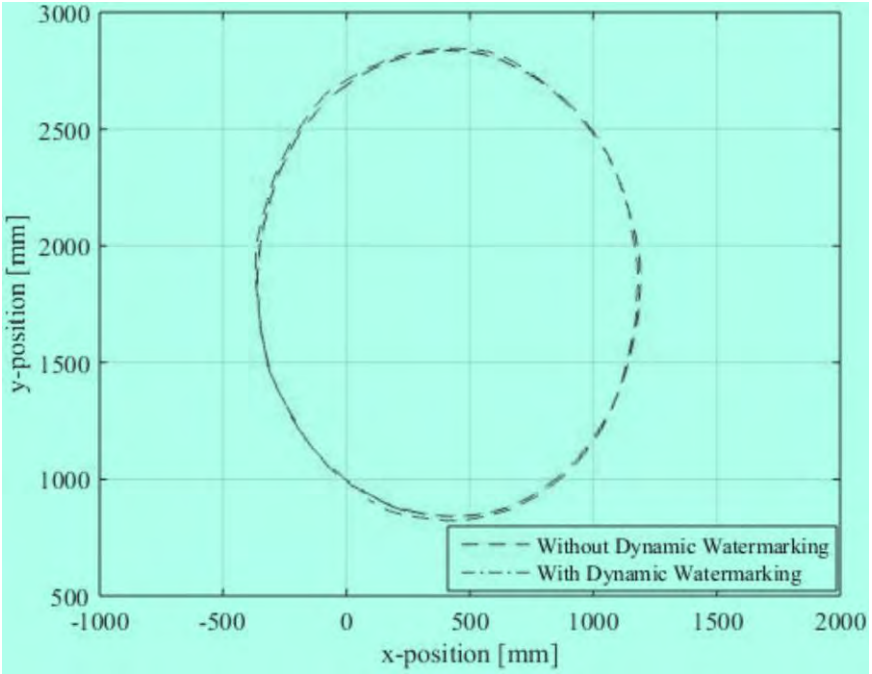
- Designing an AV requires decision chains.
- Human driven vehicles are controlled directly by a human.
- AV actuators controlled by algorithms.
- Decision chain involves sensor data, perception, planning and actuation.
- Perception transforms sensory data to useful information.
- Planning involves decision making.



Source: Plathottam 2018, COMSNETS 2018

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.

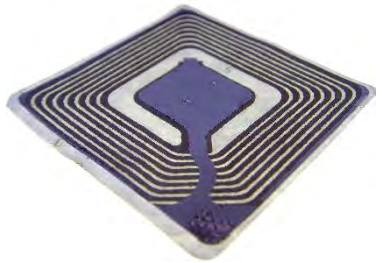


Source: Ko 2016, CPS-Sec 2016

RFID Security - Attacks

Selected RFID Attacks

- Physical RFID Threats
  - Disabling Tags
  - Tag Modification
  - Cloning Tags
  - Reverse Engineering and Physical Exploration
- RFID Channel Threats
  - Eavesdropping
  - Snooping
  - Skimming
  - Replay Attack
  - Relay Attacks
  - Electromagnetic Interference
- System Threats
  - Counterfeiting and Spoofing Attacks
  - Tracing and Tracking
  - Password Decoding
  - Denial of Service (DoS) Attacks



Numerous Applications

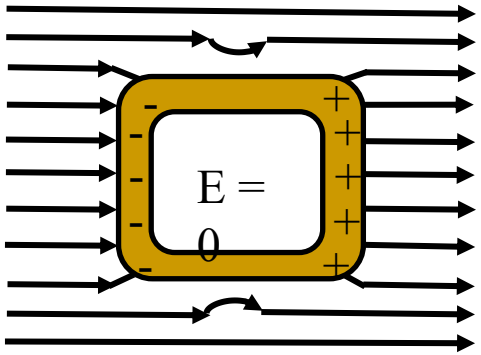
Source: Khattab 2017: Springer 2017 RFID Security

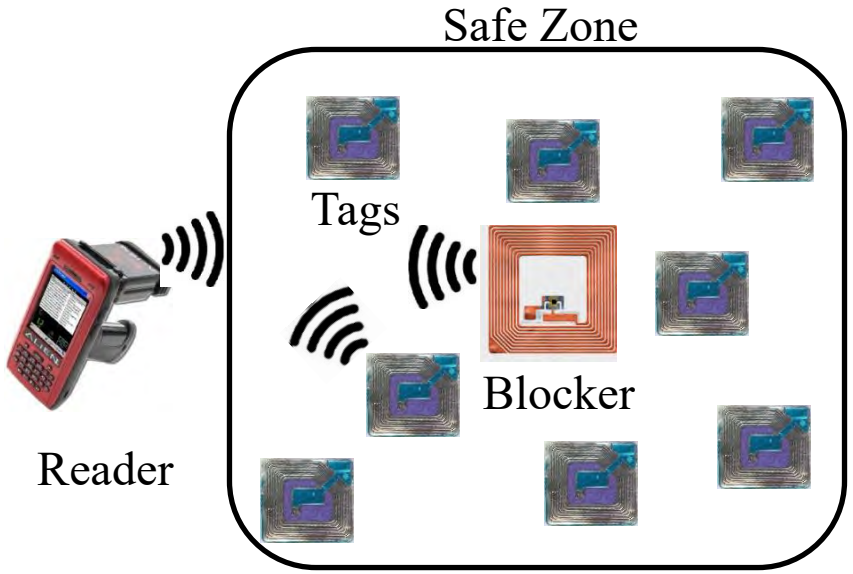
RFID Security - Solutions

Selected RFID Security Methods

- Killing Tags
- Sleeping Tags
- Faraday Cage
- Blocker Tags
- Tag Relabeling
- Minimalist Cryptography
- Proxy Privacy Devices

Faraday Cage





Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

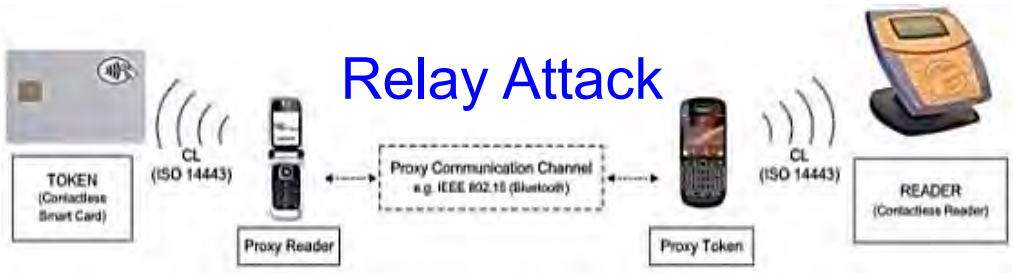
NFC Security - Attacks

- Selected NFC Attacks
  - Eavesdropping
  - Data Modification
  - Relay Attacks
  - Data Corruption
  - Spoofing
  - Interception Attacks
  - Theft

Source: http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497

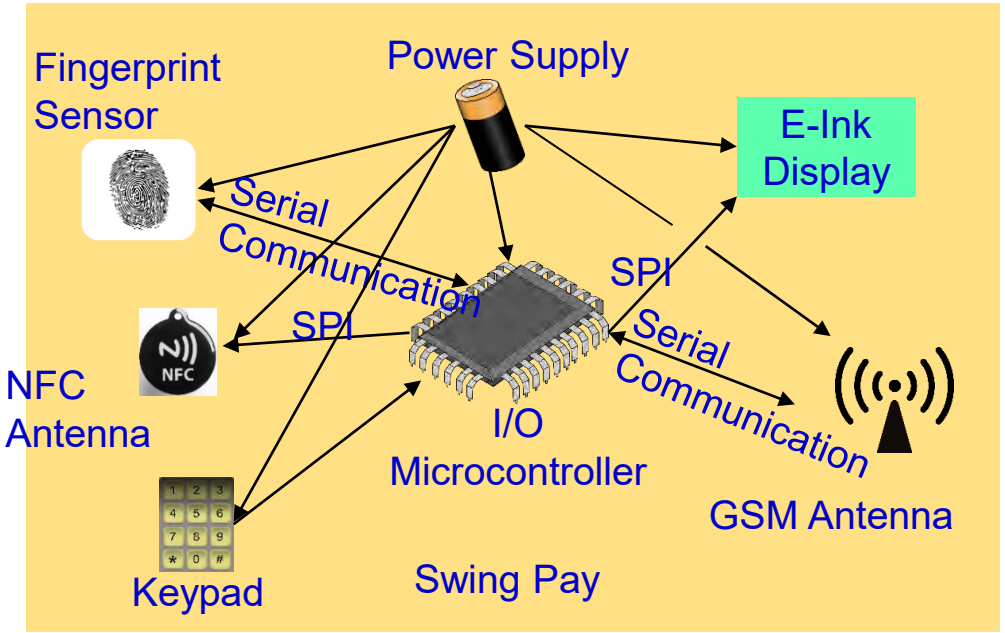
Eavesdropping

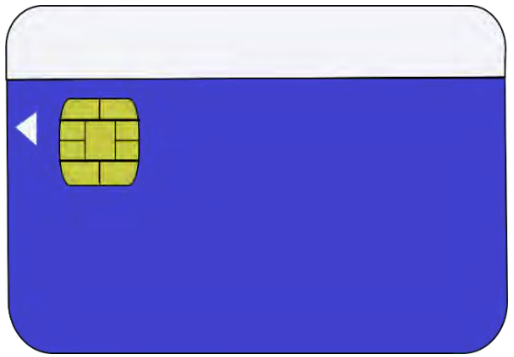
Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

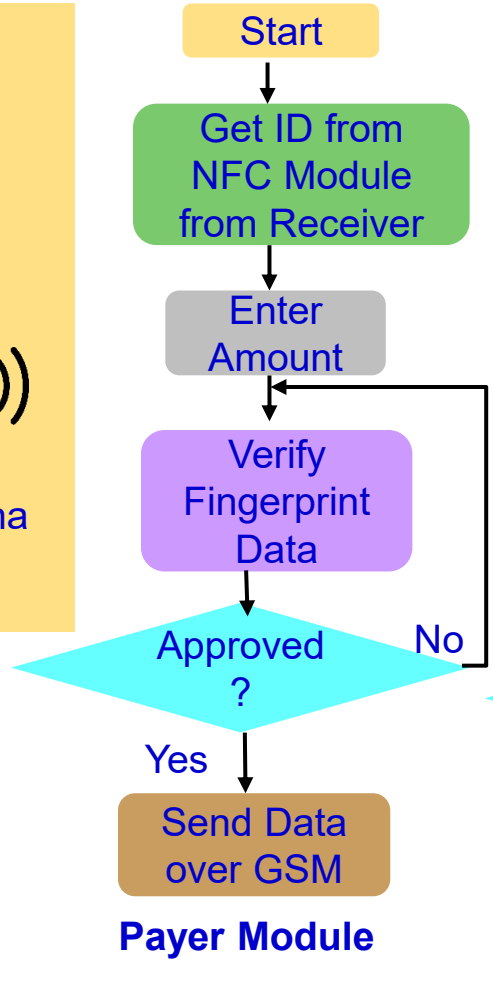


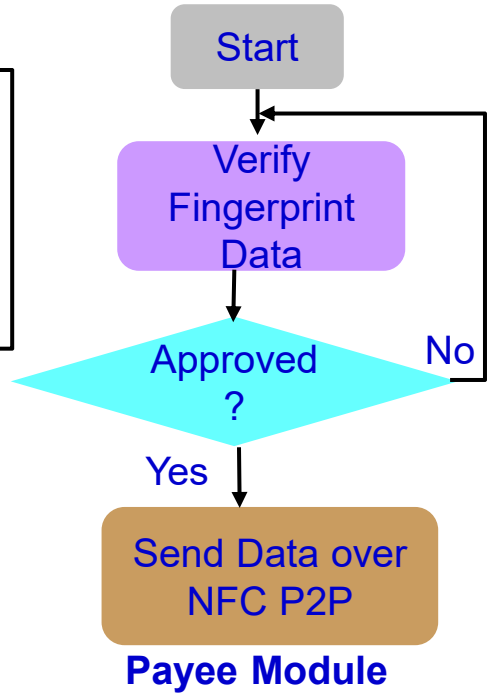
Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

NFC Security



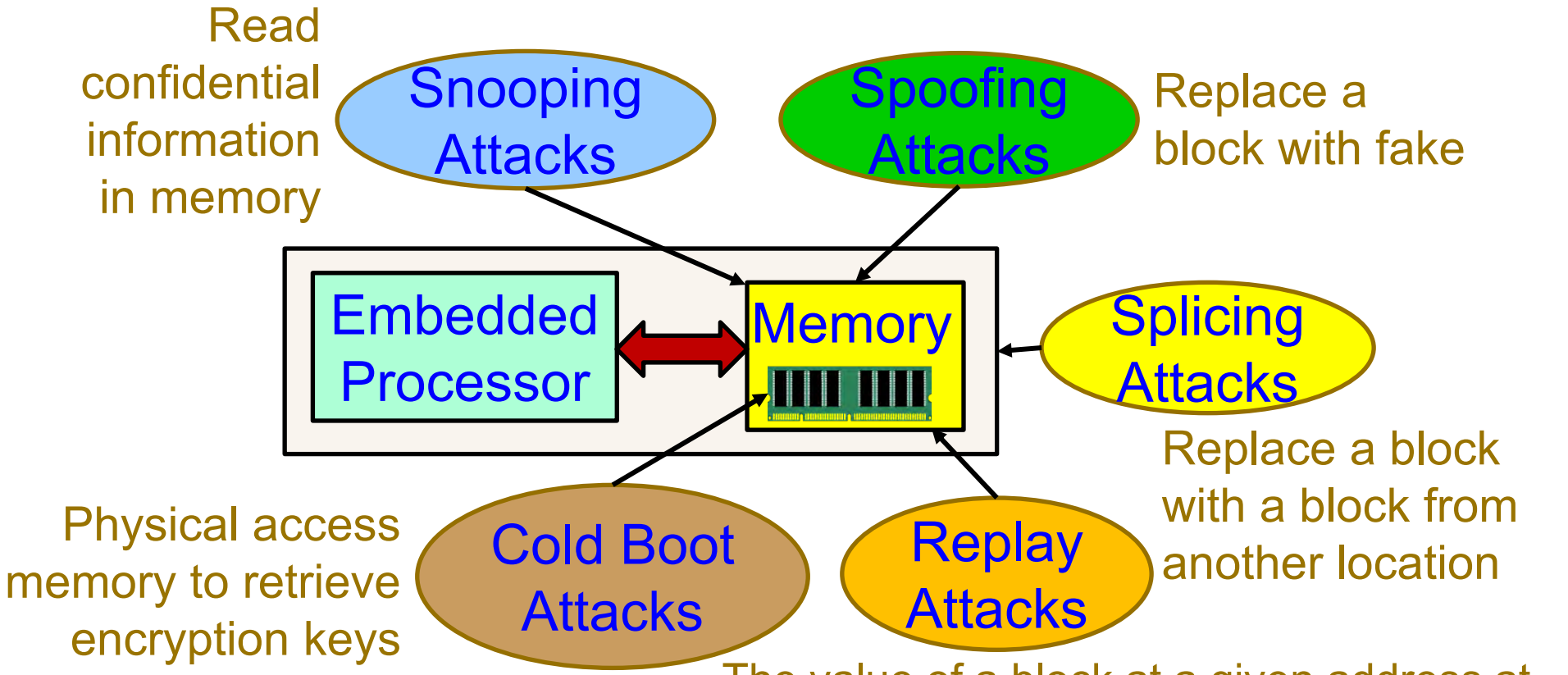






Source: Mohanty 2017, CE Magazine Jan 2017

Memory Attacks



Source: Mohanty 2013, Springer CSSP Dec 2013

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

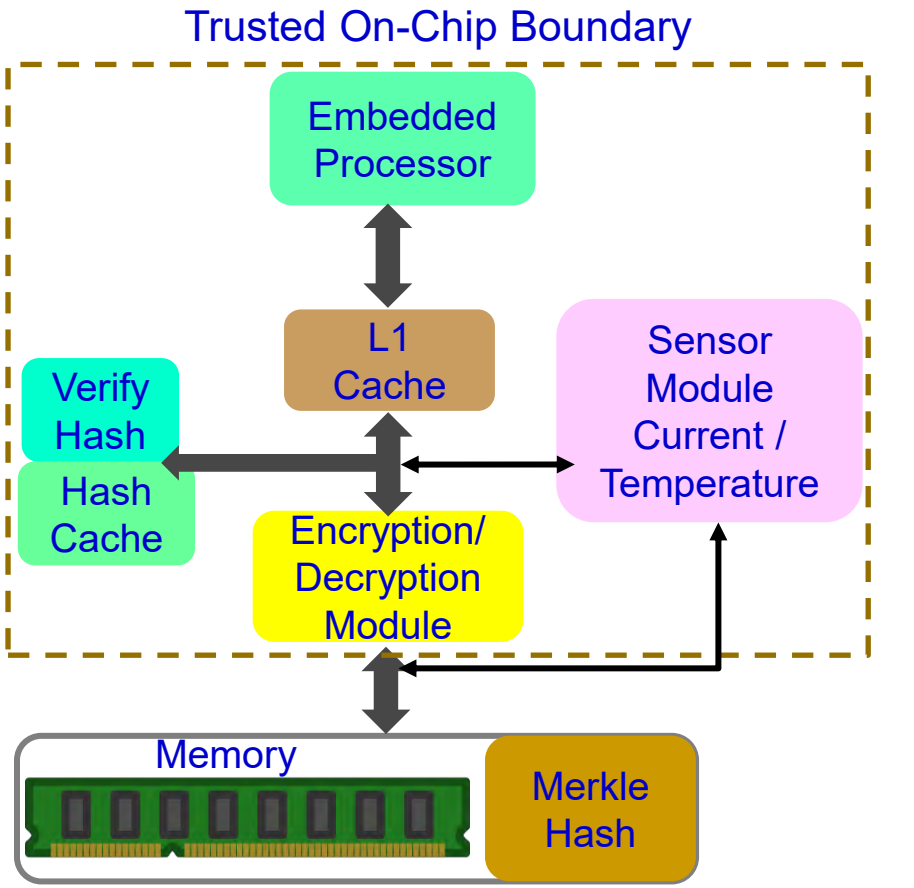
Nonvolatile / Harddrive Storage

Hardware-based encryption of data secured/protected by strong password/PIN authentication.

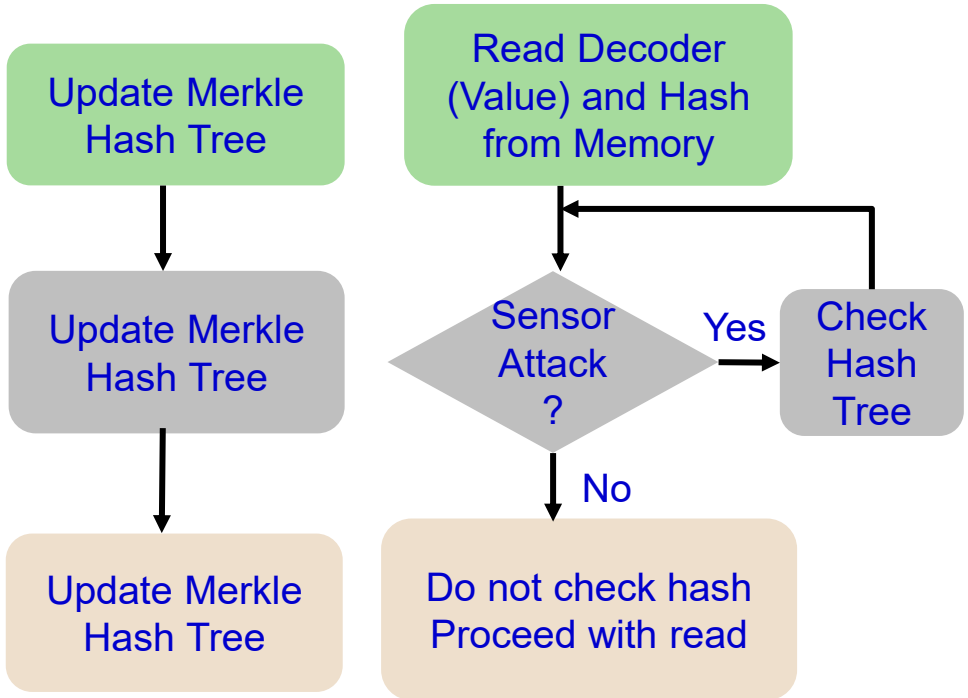
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

Embedded Memory Security



On-Chip/On-Board Memory Protection



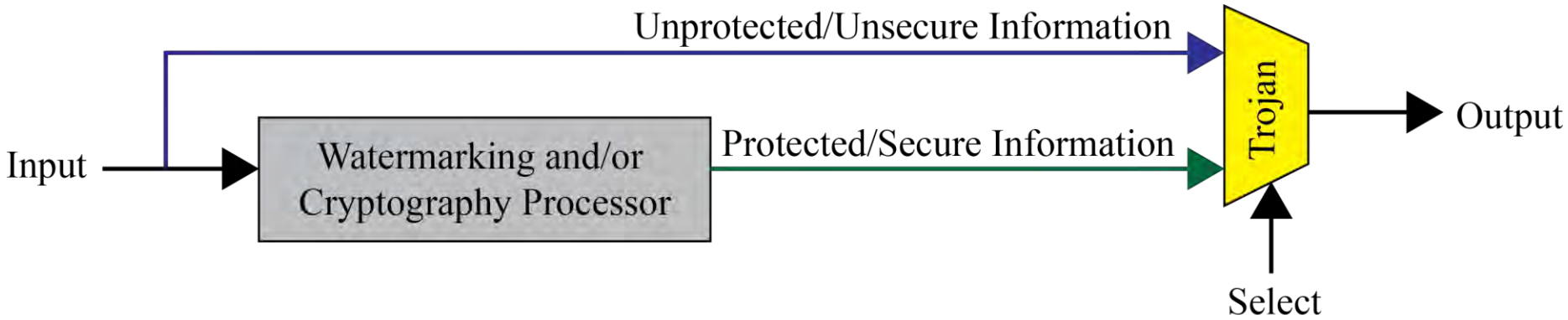
Memory integrity verification with 85% energy savings with minimal performance overhead.

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.

Malicious Design Modifications Issue

Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans

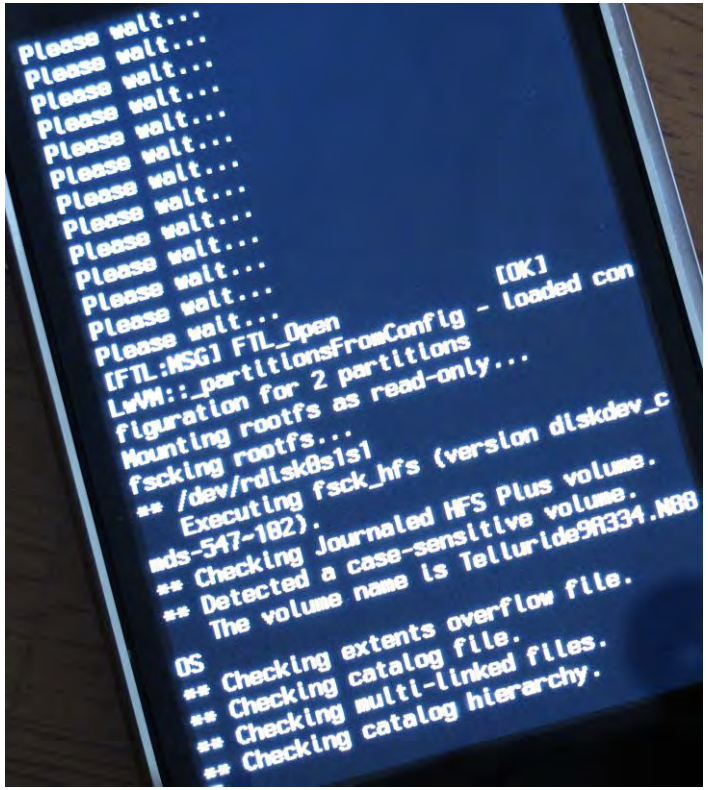


Source: Mohanty 2015, McGraw-Hill 2015

Provide backdoor to adversary.
Chip fails during critical needs.

Firmware Reverse Engineering

Extract, modify, or reprogram code

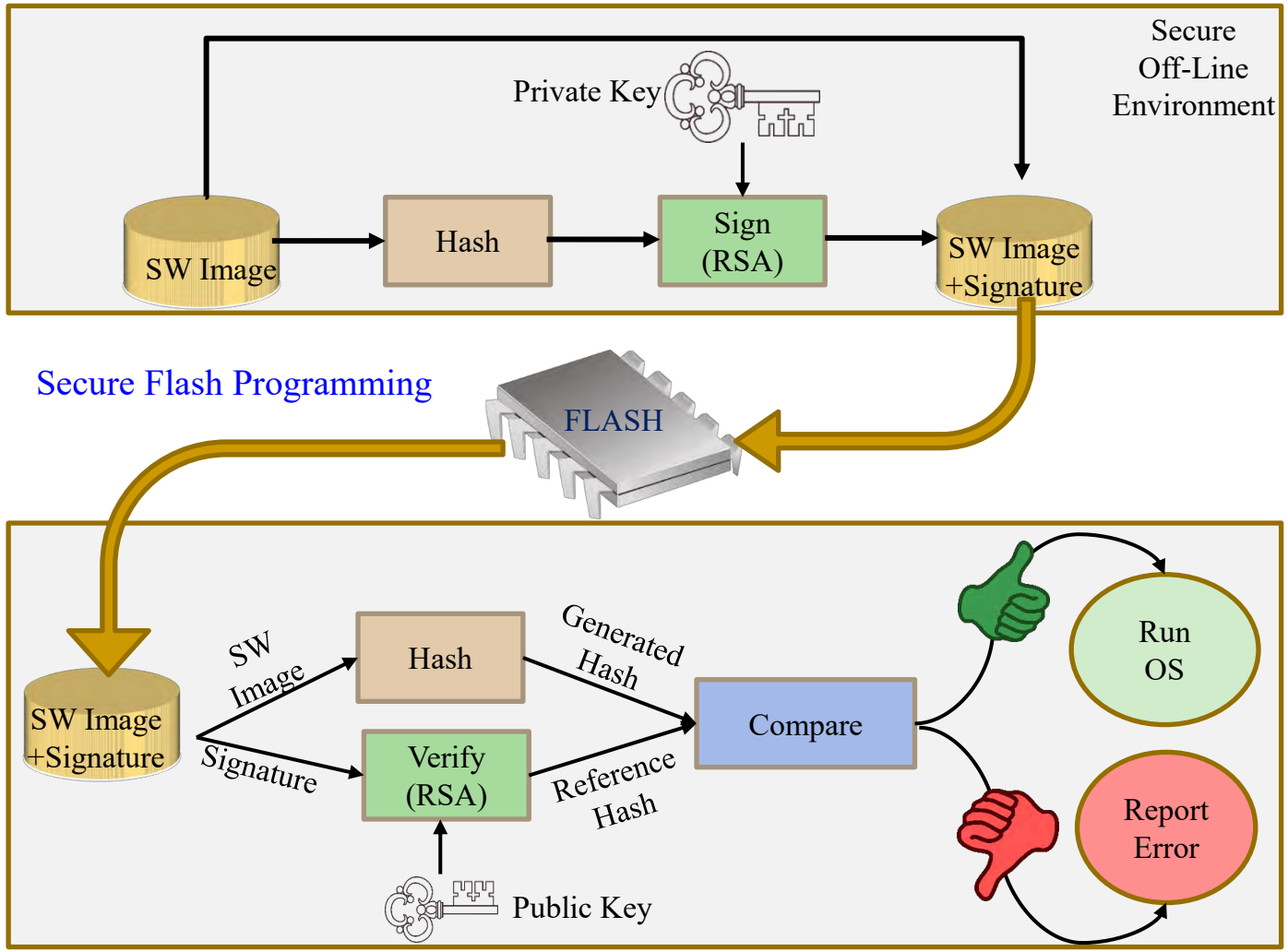


OS exploitation,
Device jailbreaking

Source: http://jcjc-dev.com/

Source: http://grandideastudio.com/wp-content/uploads/current_state_of_hh_slides.pdf

Firmware Security - Solution



Source: https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

How Secure is AES Encryption?

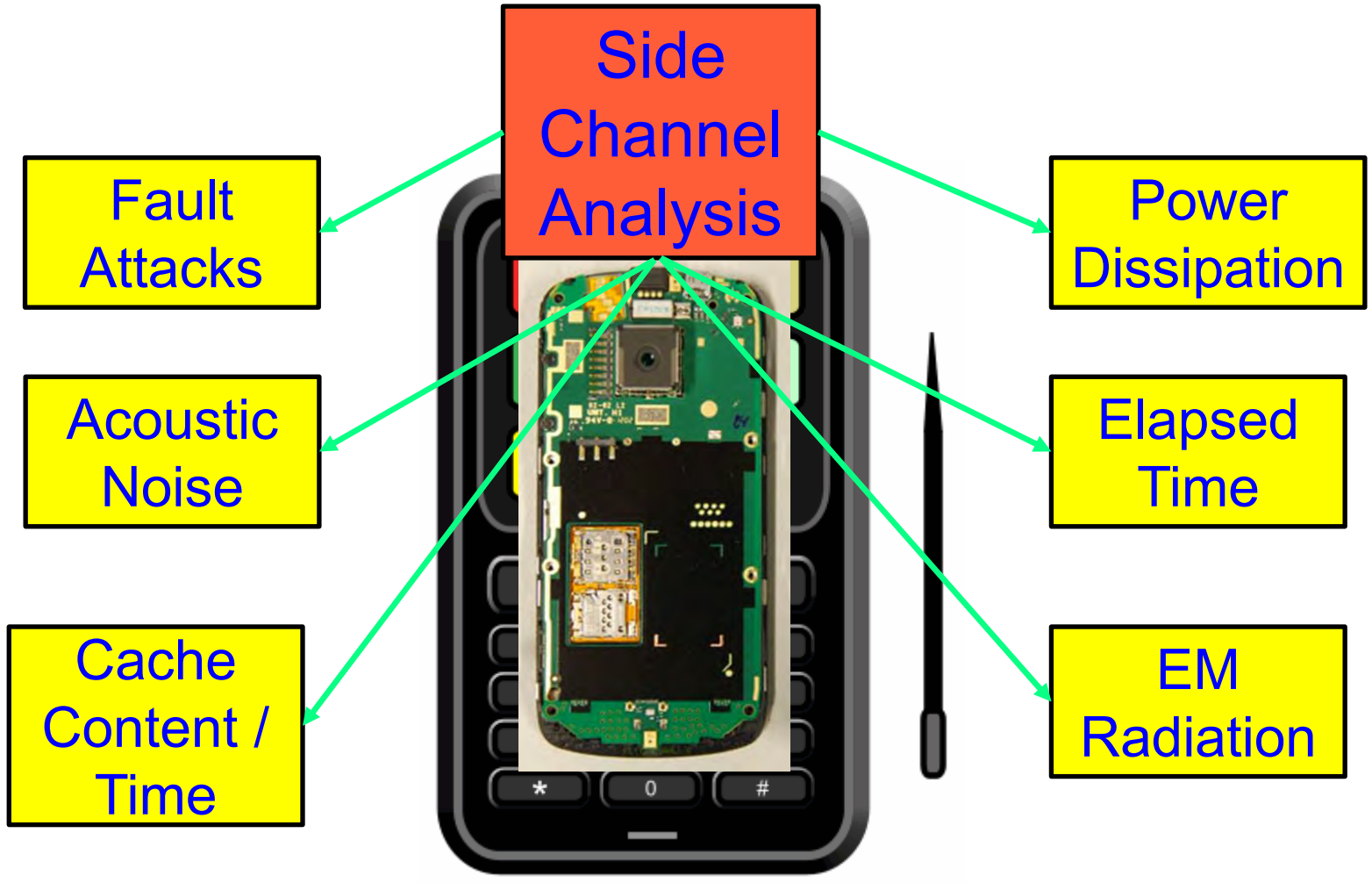
- Brute force a 128 bit key ?
- If you assume
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, you can crack the key after testing 50% of the possibilities
  - Then the earth's population can crack one 128 bit encryption key in 77,000,000,000 years (77 billion years)

Age of the Earth 4.54 ± 0.05 billion years

Age of the Universe 13.799 ± 0.021 billion years

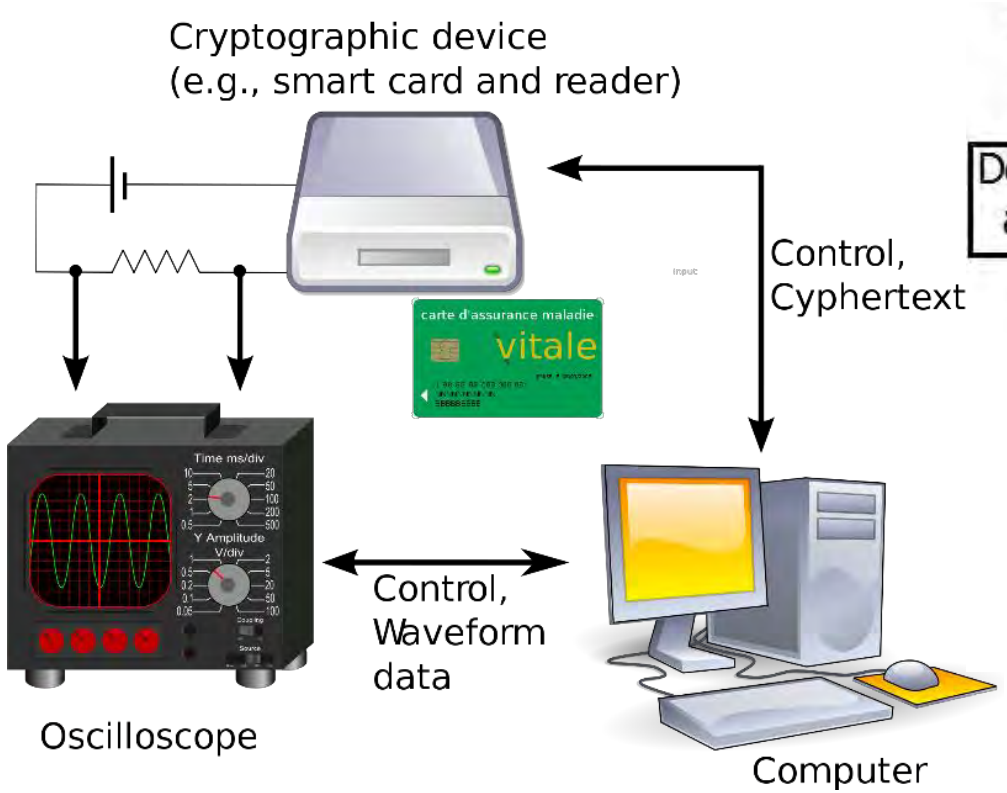
Source: Parameswaran Keynote iNIS-2017

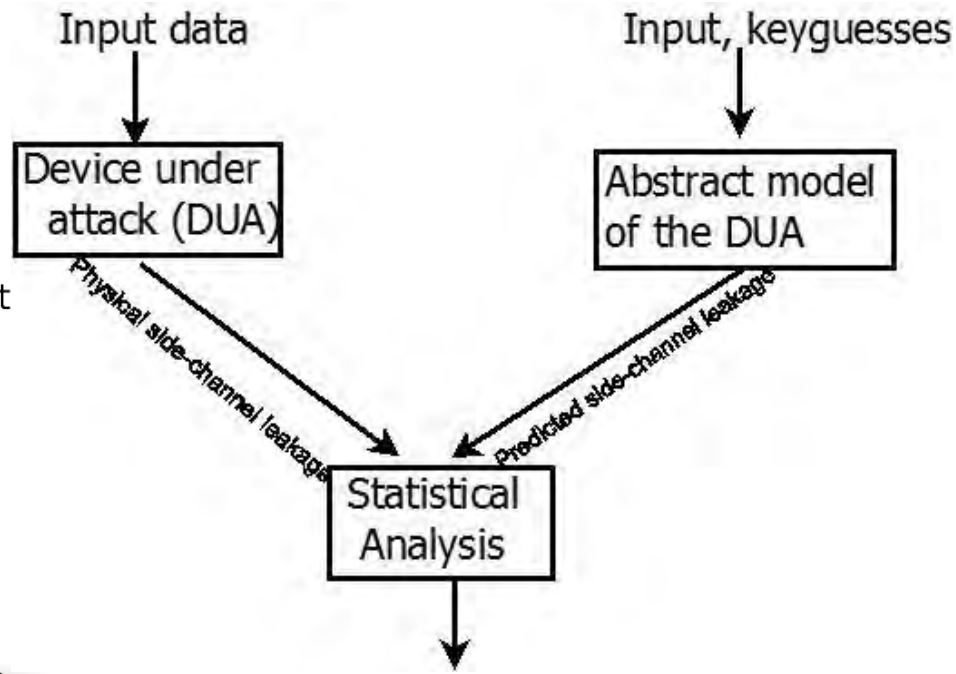
Side Channel Analysis Attacks



Source: Parameswaran Keynote iNIS-2017

Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

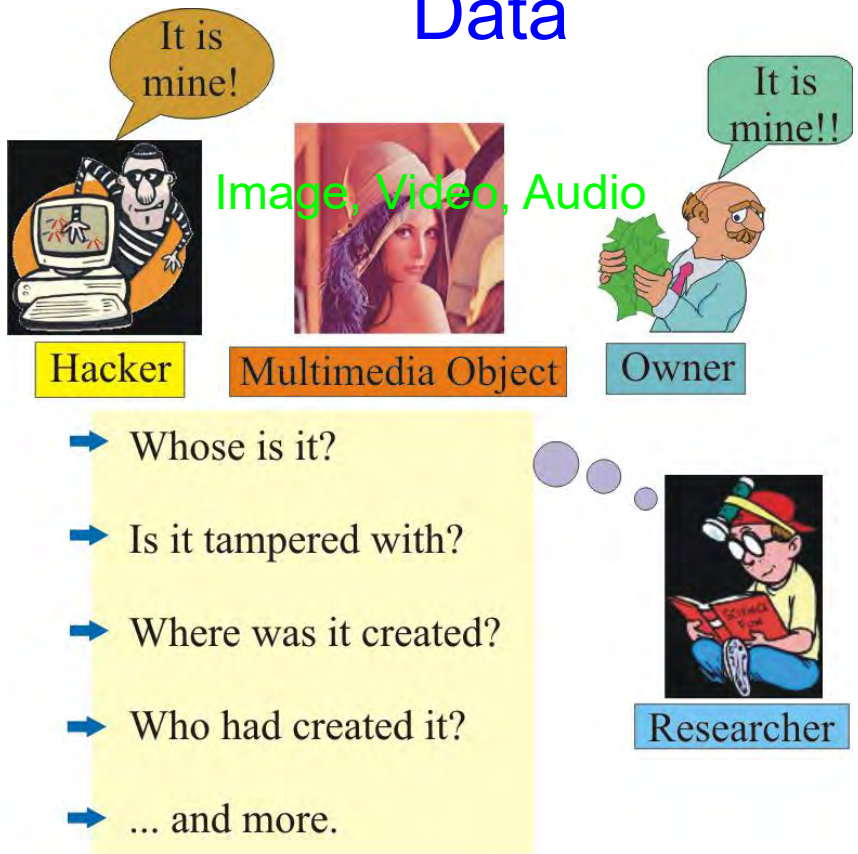




Source: Mohanty 2018, ZINC Keynote 2018

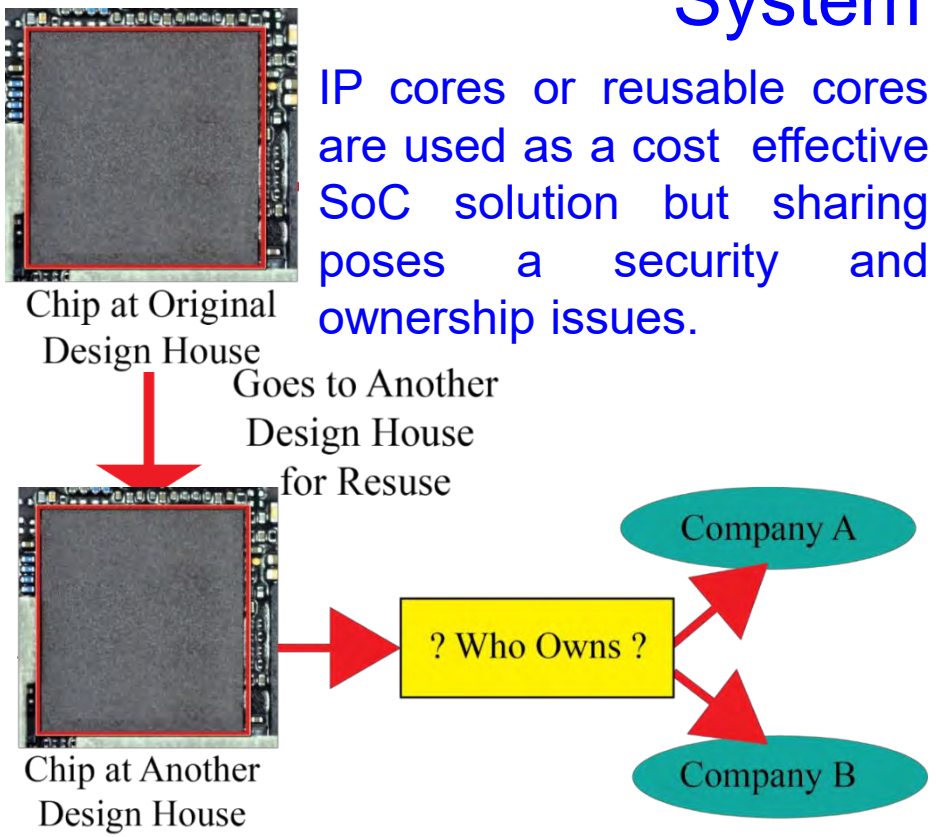
Data and System Authentication and Ownership Protection – My 20 Years of Experiences

Data



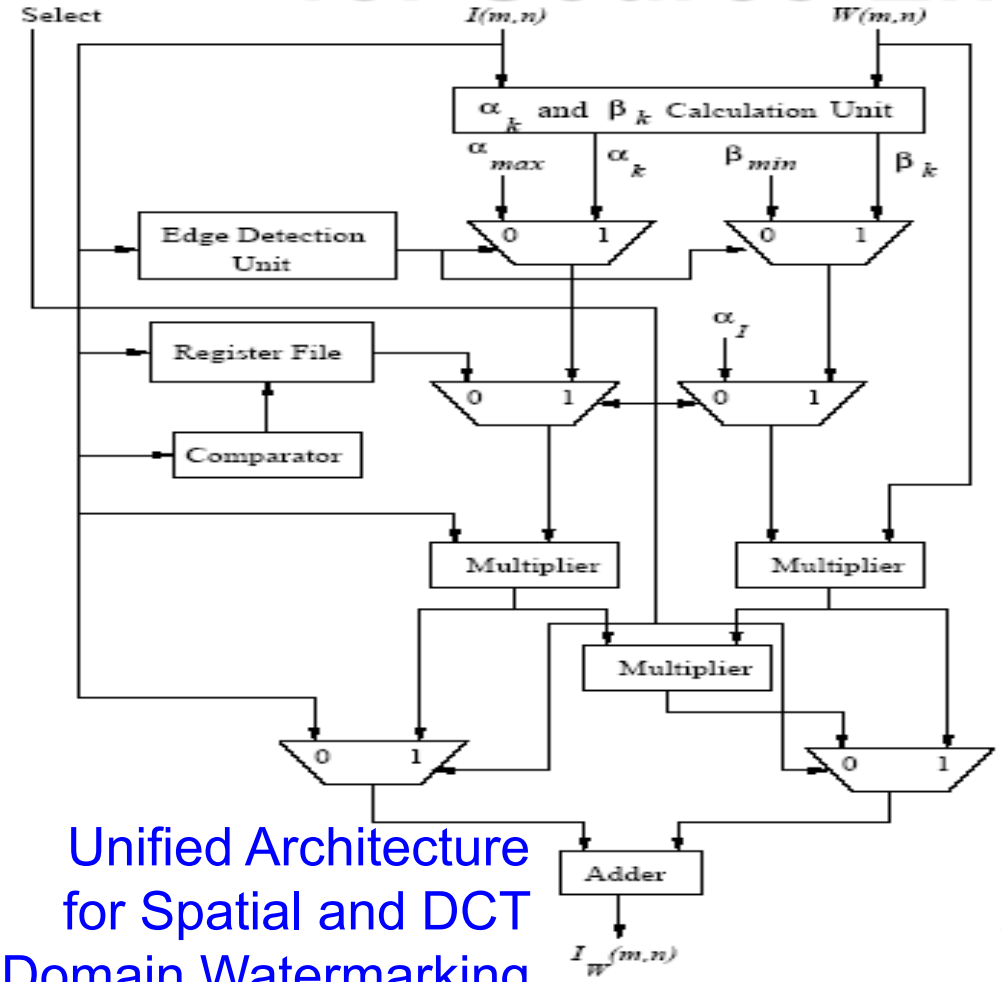
System

IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.

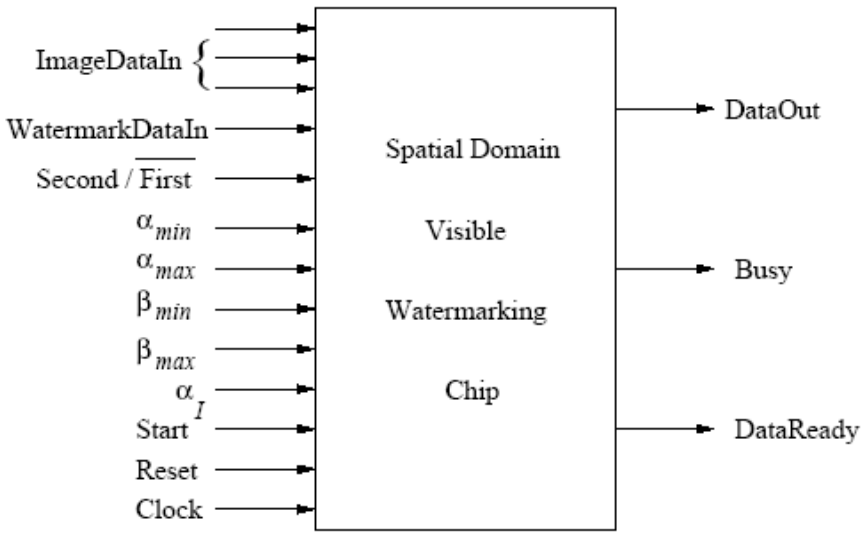


Source: S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking", *IEEE Consumer Electronics Magazine (CEM),* Volume 6, Issue 3, July 2017, pp. 83--91.

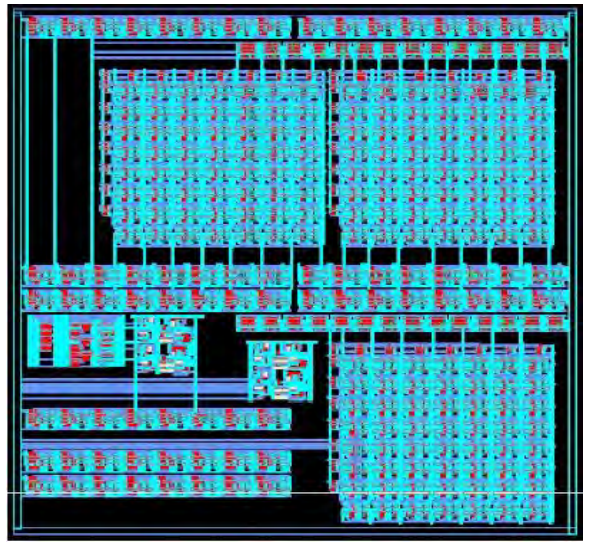
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram

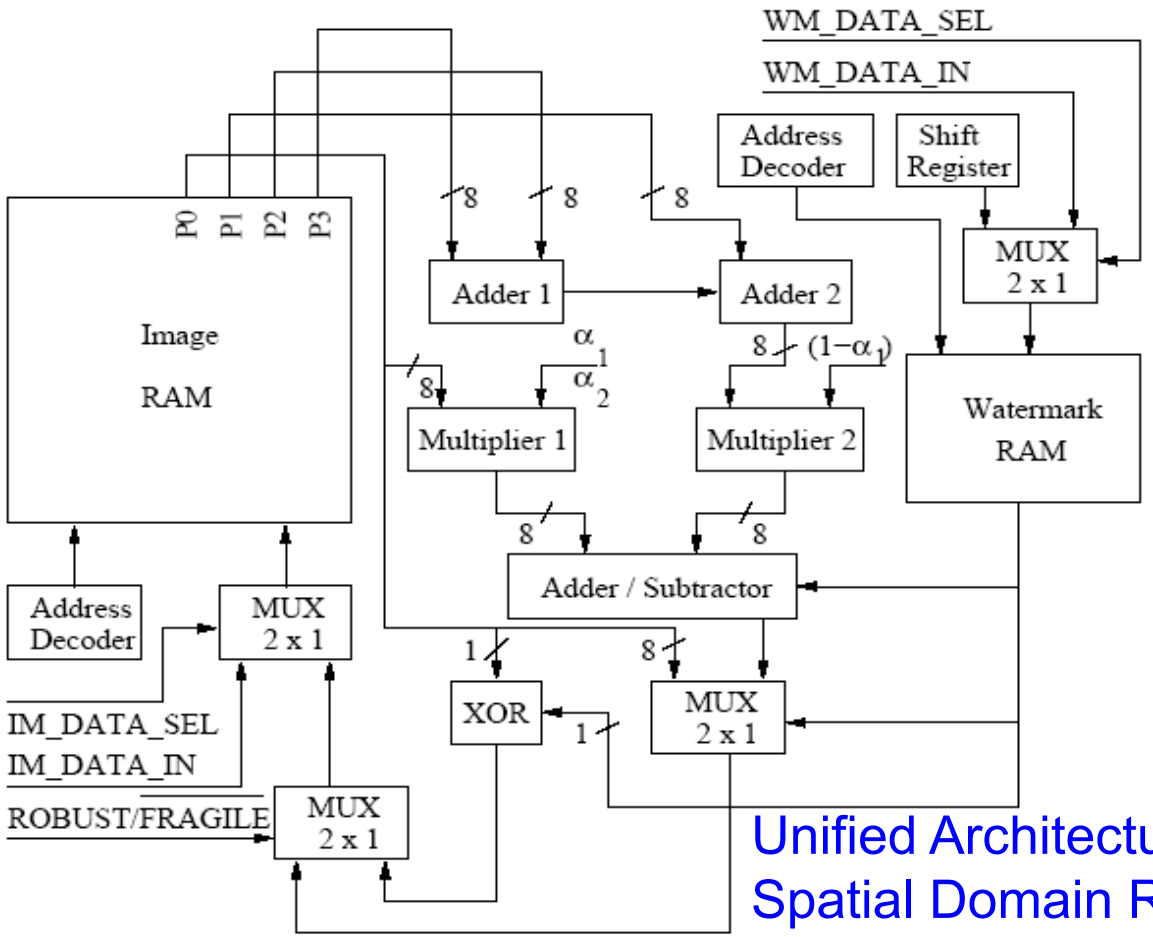


Chip Layout

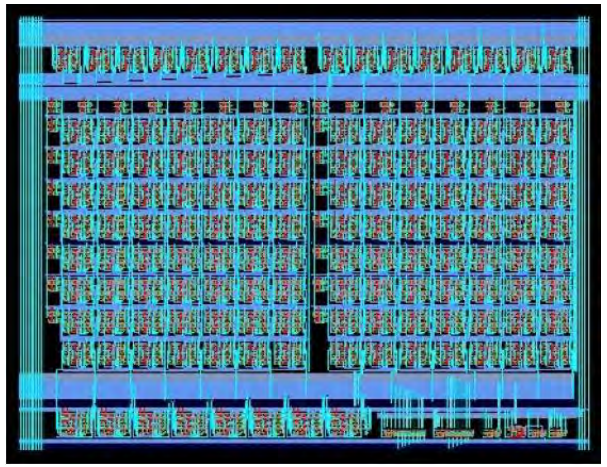
Chip Design Data
Total Area : 9.6 sq mm, No. of Gates: 28,469
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

Source: **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^2DC) Design", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 13, No. 8, August 2005, pp. 1002-1012.

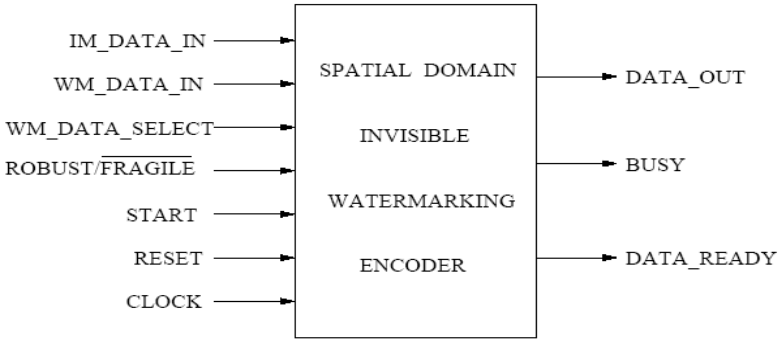
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout

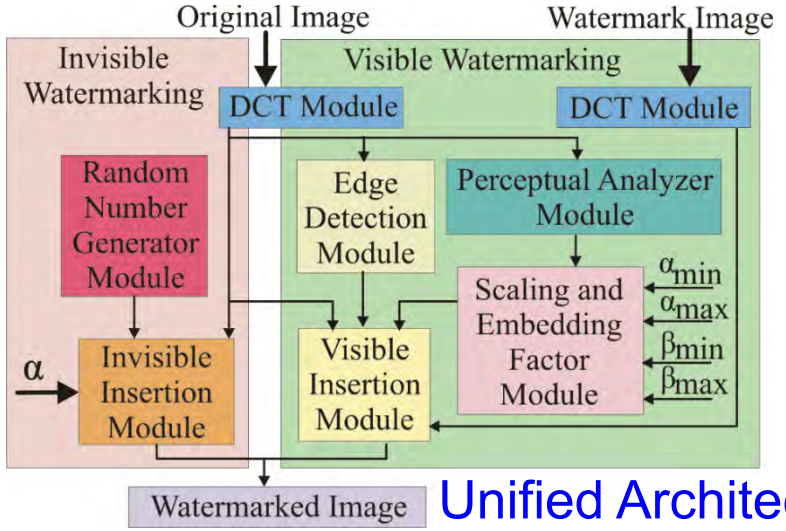


Pin Diagram

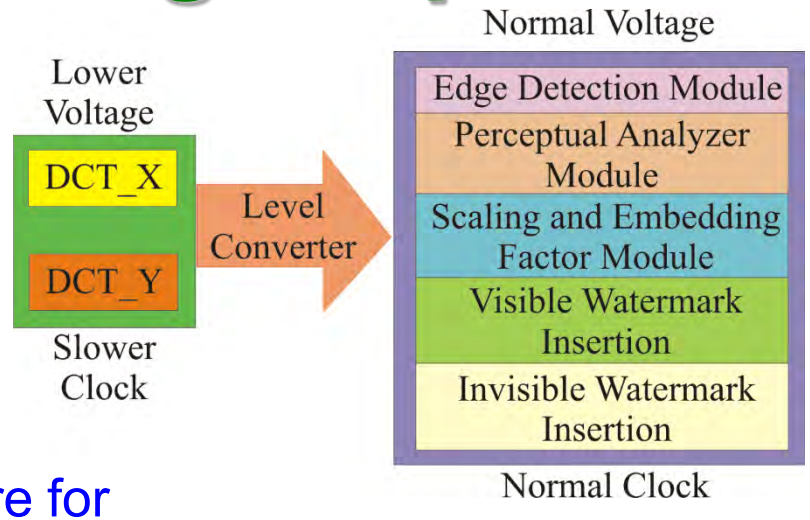
Chip Design Data
Total Area : 0.87 sq mm, No. of Gates: 4,820
Power Consumption: 2.0 mW, Frequency: 500 MHz

Source: **S. P. Mohanty**, E. Kougianos, and N. Ranganathan, "VLSI Architecture and Chip for Combined Invisible Robust and Fragile Watermarking", *IET Computers & Digital Techniques (CDT)*, September 2007, Volume 1, Issue 5, pp. 600-611.

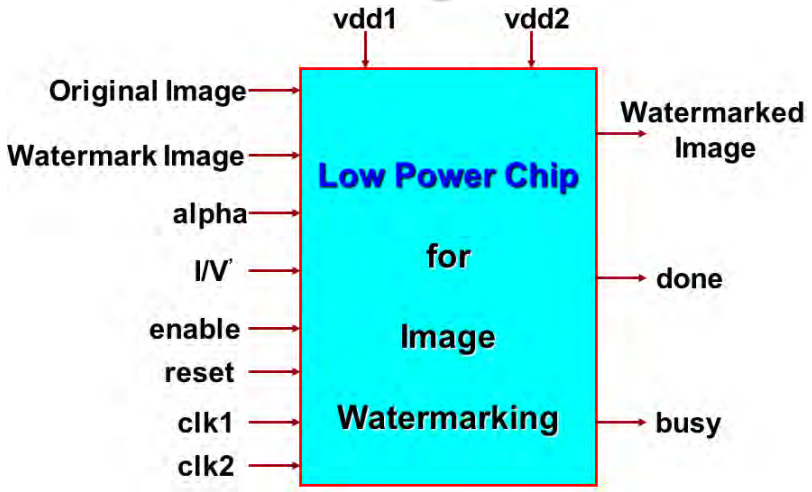
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



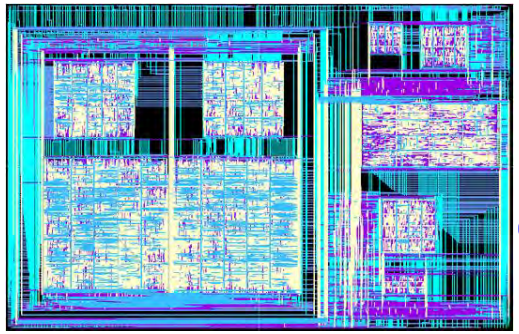
Unified Architecture for DCT Domain Watermarking



DVDF Low-Power Design



Pin Diagram

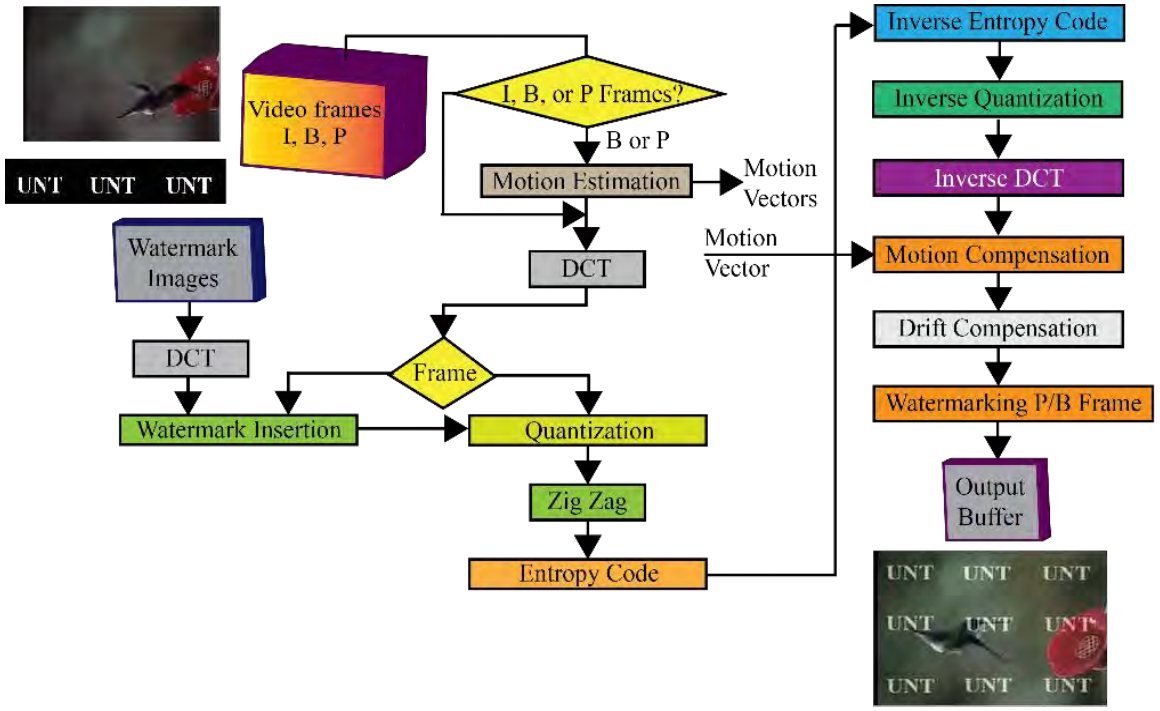


Chip Layout

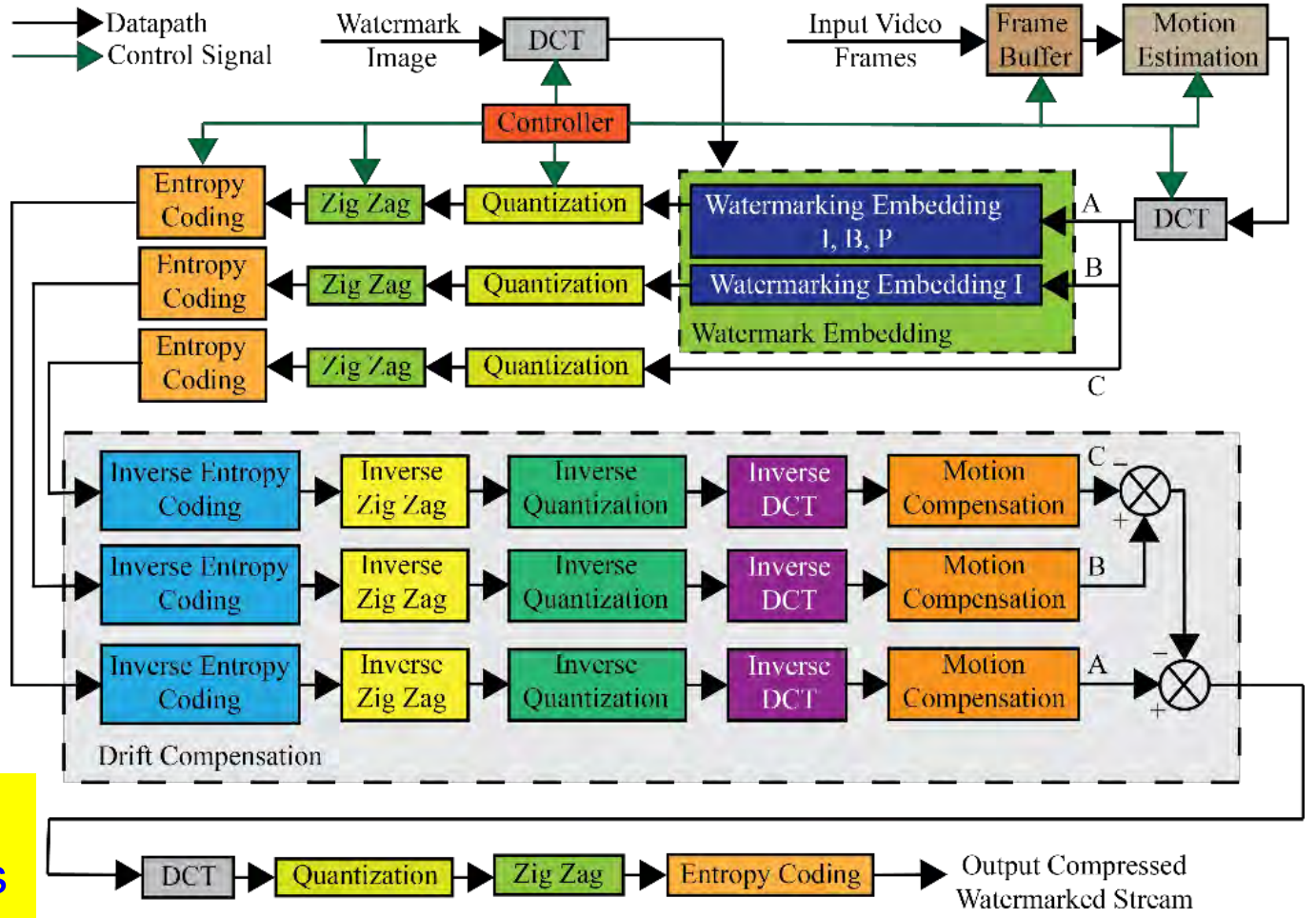
Chip Design Data
Total Area : 16.2 sq mm, No. of Transistors: 1.4 million
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

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.

Our Hardware for Real-Time Video Watermarking



(a) Video Watermarking Algorithm as a Flow Chart

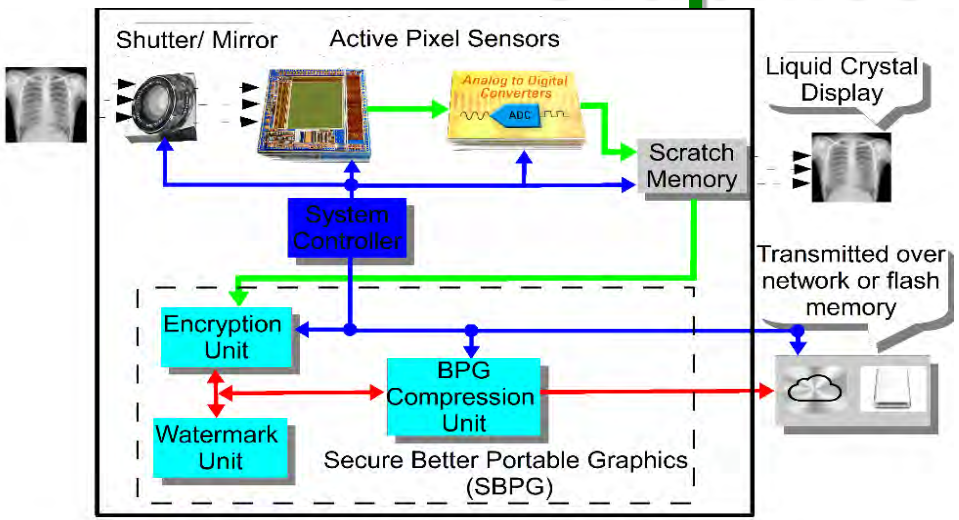


(b) Architecture of the Video Watermrking Algorithm

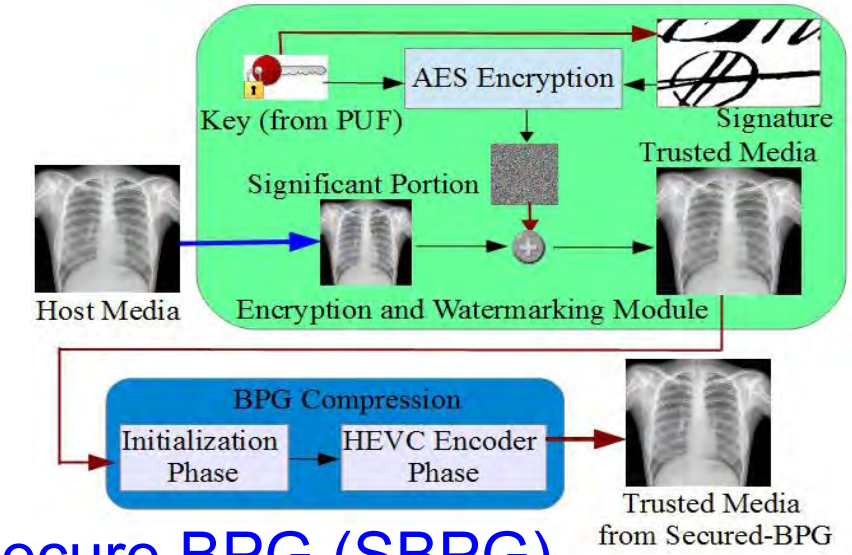
FPGA based Design Data
Resource: 28322 LE, 16532 Registers, 9 MUXes
Operating Frequency: 100 MHz
Throughput: 43 fps

Source: **S. P. Mohanty** and E. Kougianos, "Real-Time Perceptual Watermarking Architectures for Video Broadcasting", *Journal of Systems and Software*, Vol. 84, No. 5, May 2011, pp. 724--738.

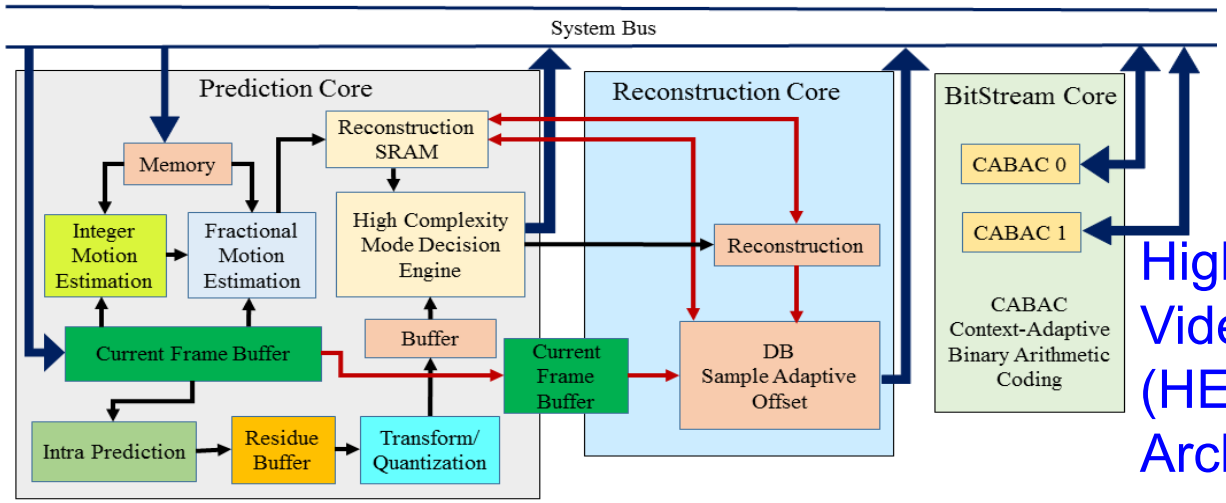
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)

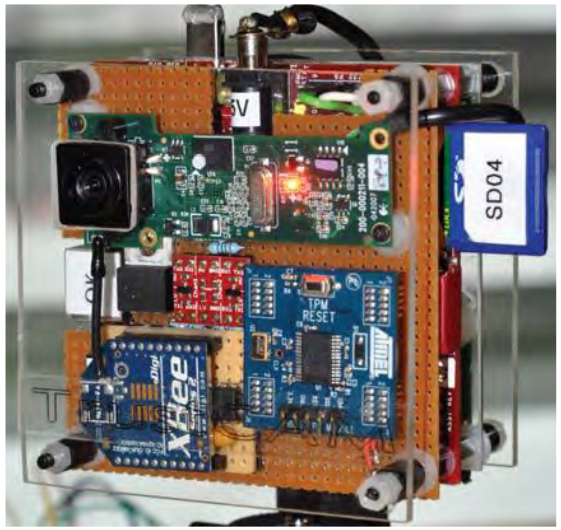


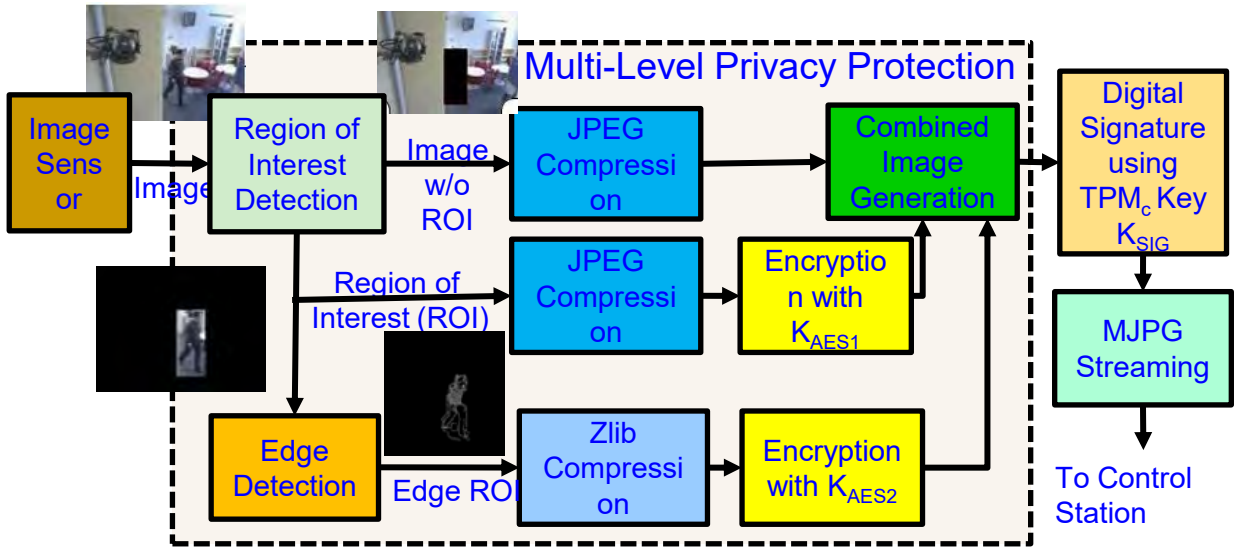
High-Efficiency Video Coding (HEVC) Architecture

Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW

Source: S. P. Mohanty, E. Kougianos, and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT (Invited Paper)", IEEE Access Journal, Volume 6, 2018, pp. 5939--5953.

My Watermarking Research Inspired - TrustCAM



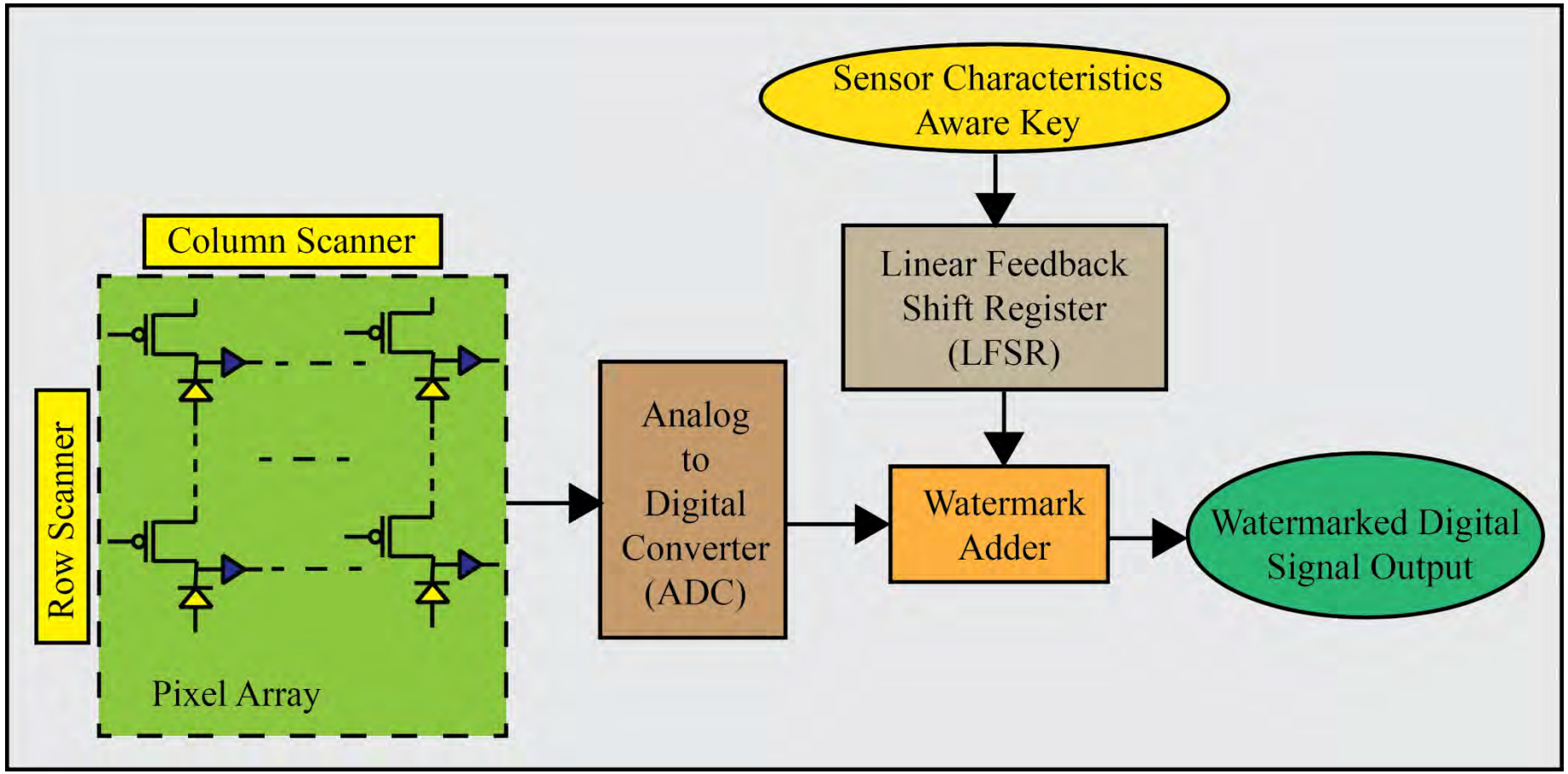


For integrity protection, authenticity and confidentiality of image data.

Source: https://pervasive.aau.at/BR/pubs/2010/Winkler_AVSS2010.pdf

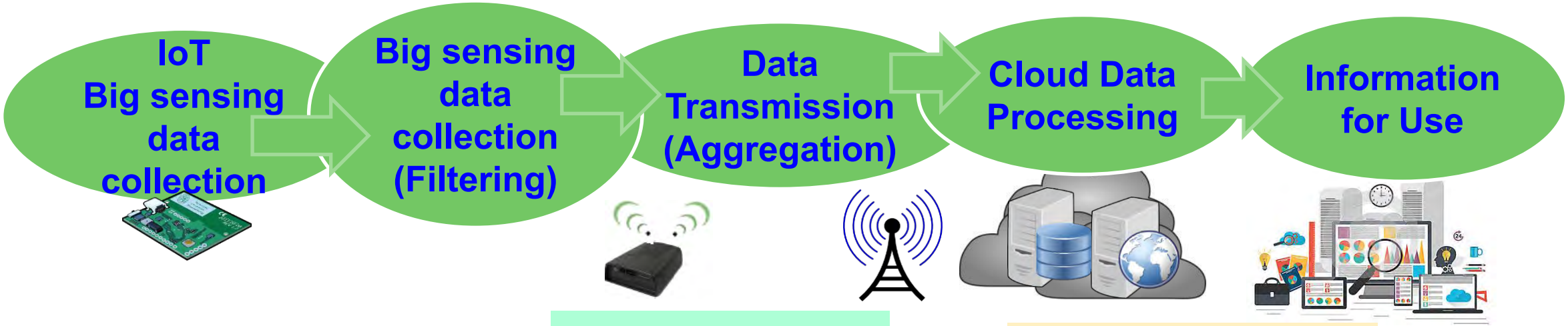
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor



Source: G. R. Nelson, G. A. Jullien, O. Yadid-Pecht, "CMOS Image Sensor With Watermarking Capabilities", in *Proc. IEEE International Symposium on Circuits and Systems* (*ISCAS*), 2005, pp. 5326–5329.

Secure Data Curation a Solution for Fake Data?



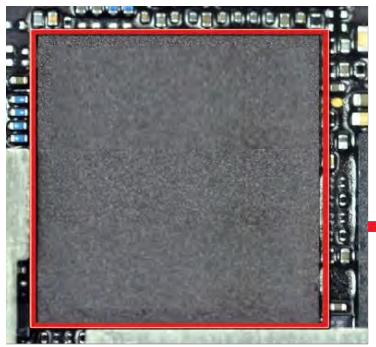
Edge Training:
- ➢ Data Signature
- ➢ Model Signature

Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

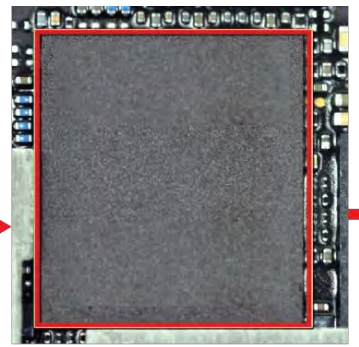
Source: C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, "Big-Sensing-Data Curation for the Cloud is Coming", *IEEE Consumer Electronics Magazine (CEM)*, Volume 6, Issue 4, October 2017, pp. 48--56.

Hardware IP Right Infringement



Chip at Original Design House

Goes to Another Design House for Resuse



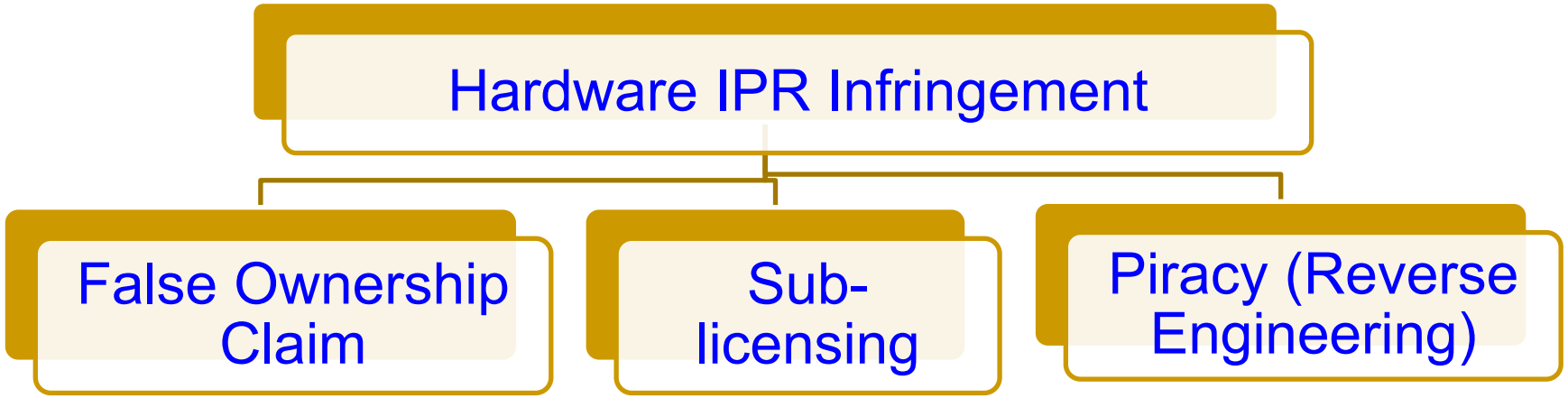
Chip at Another Design House

? Who Owns ?

Company A

Company B

Source: Mohanty 2015, McGraw-Hill 2015



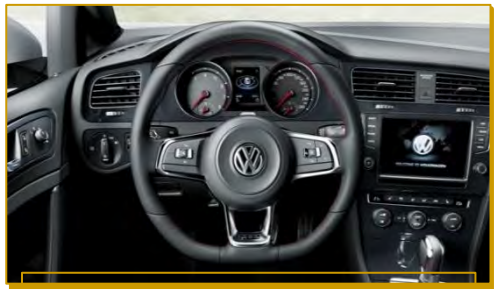
Counterfeit Hardware – IP Attacks

2014 Analog Hardware Market (Total Shipment Revenue US $)

Wireless Market
$18.9 billion (34.8%)

Consumer Electronics
$9.0 billion (16.6%)

Industrial Electronics
$8.9 billion (16.5%)



Automotive
$8.5 billion (15.7%)

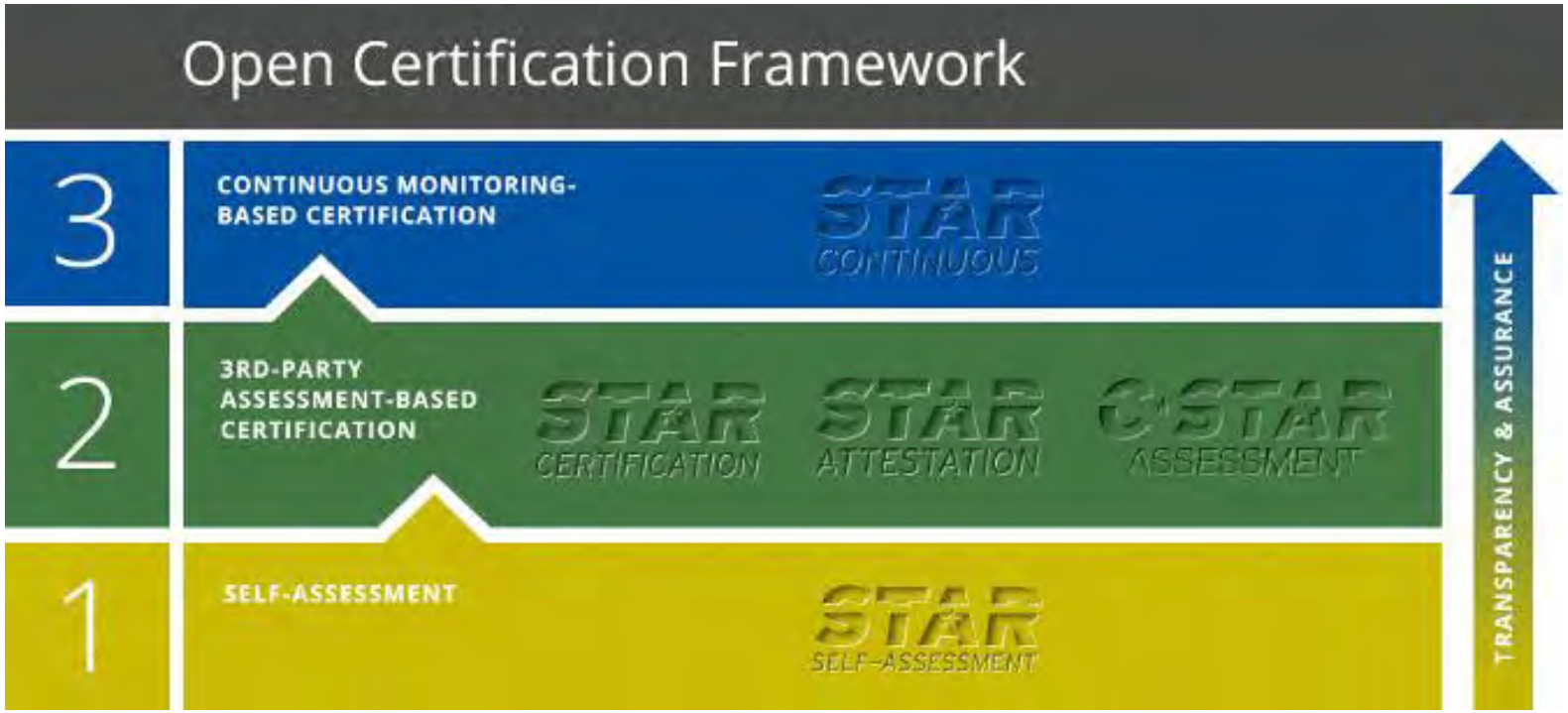
Data Processing
$6.0 billion (11%)

Wired Communications
$2.9 billion (5.4%)

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Top counterfeits could have impact of $300B on the semiconductor market.

Security Star Ratings



Source: https://cloudsecurityalliance.org/star/#_overview

Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

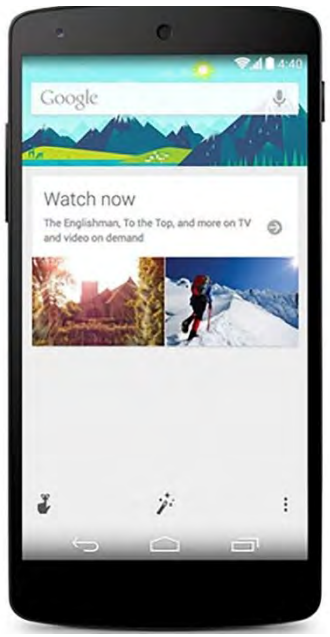
Response Smart

Systems – End Devices

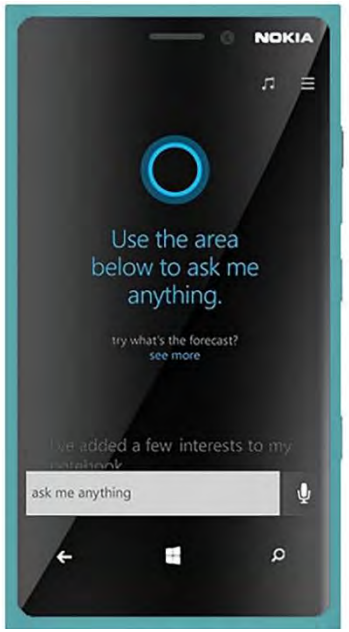
Alexa

Apple Siri

Google Now

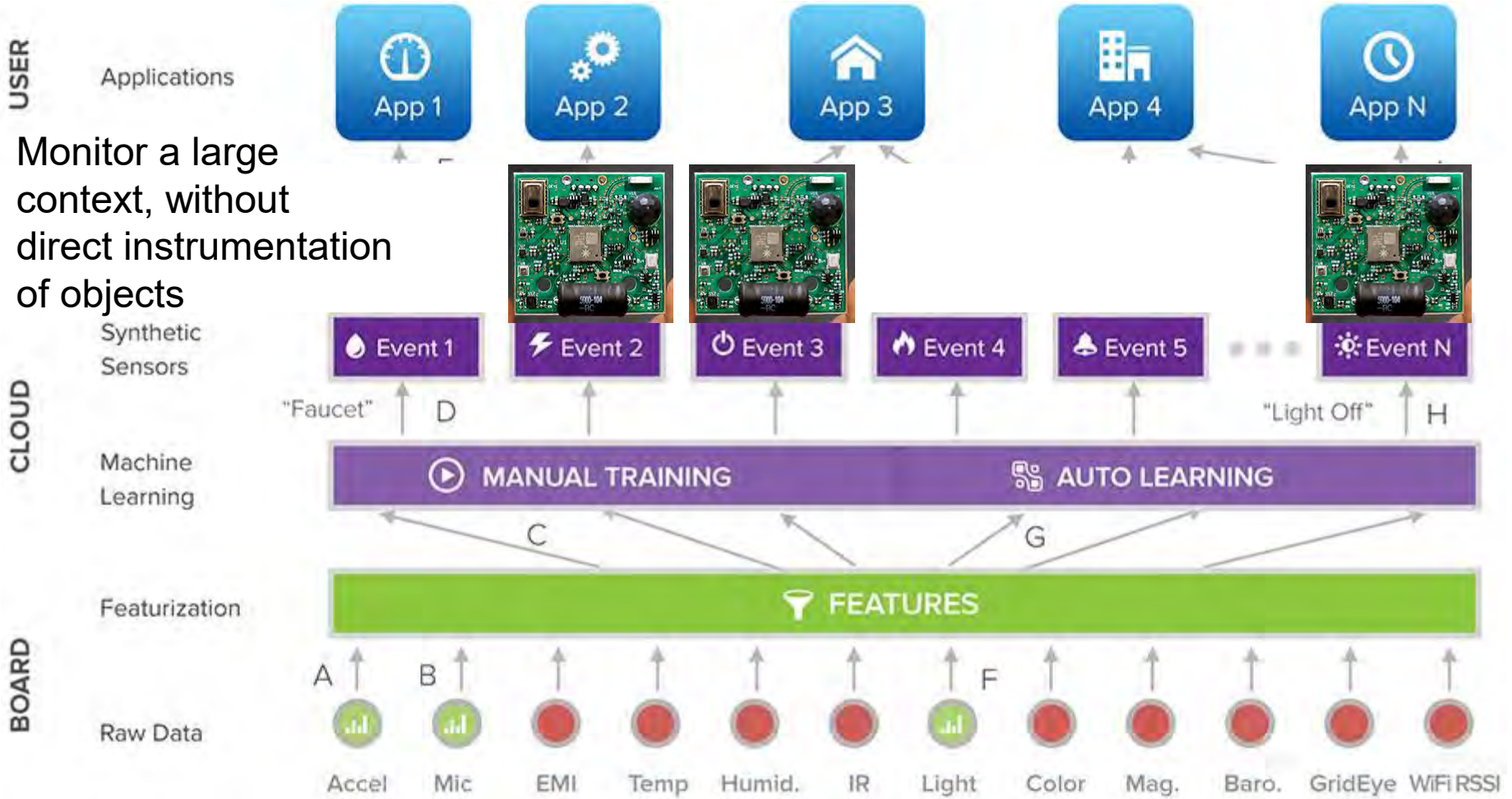


Windows Cortana



Smart Sensors - General-Purpose/ Synthetic Sensors

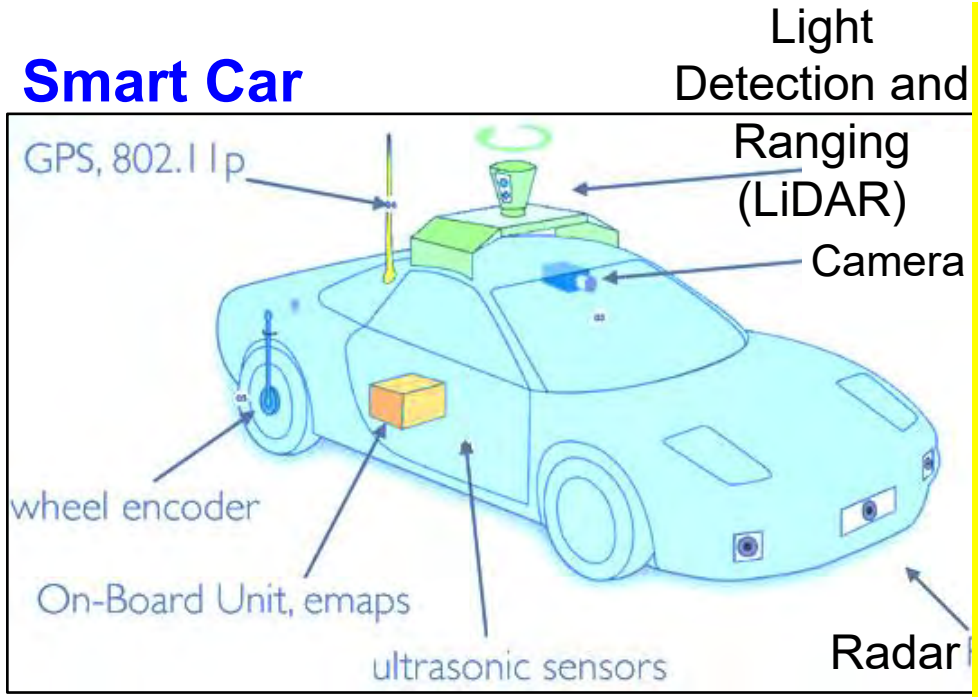
Monitor a large context, without direct instrumentation of objects



Source: Laput 2017, http://www.gierad.com/projects/supersensor/

Autonomous/Driverless/Self-Driving Car

Smart Car



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

Level 0
- Complete Driver Control

Level 1
- Most functions by driver, some functions automated.

Level 2
- At least one driver-assistance system is automated.

Level 3
- Complete shift of critical safety systems to vehicle; Driver can intervene

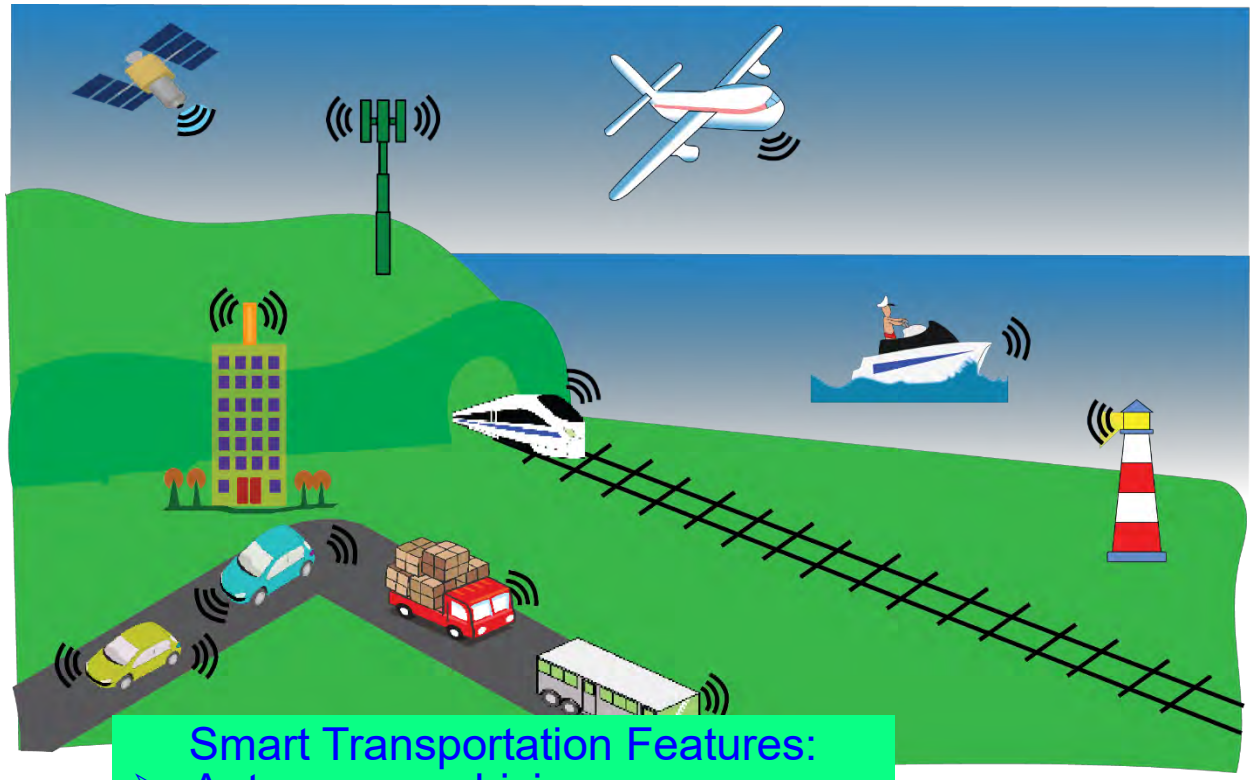
Level 4
- Perform All Safety-Critical Functions
- Limited to Operational Domain

Level 5
- All Safety-Critical Functions in All Environments and Scenarios

"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Datta 2017: CE Magazine Oct 2017

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

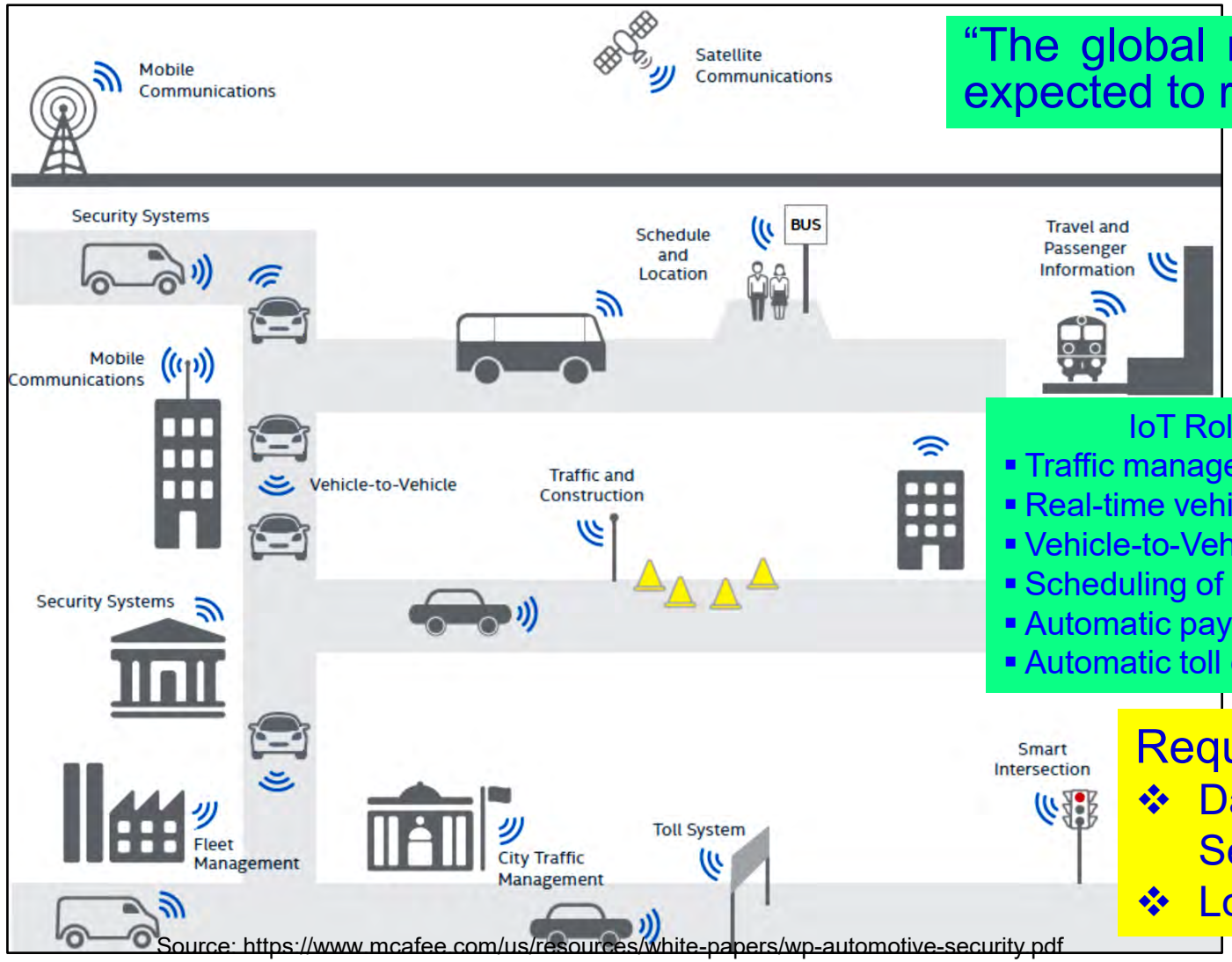
Driverless Care

Drone

"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

Transportation Cyber-Physical System (T-CPS)



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

"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Source: Datta 2017, CE Magazine Oct 2017

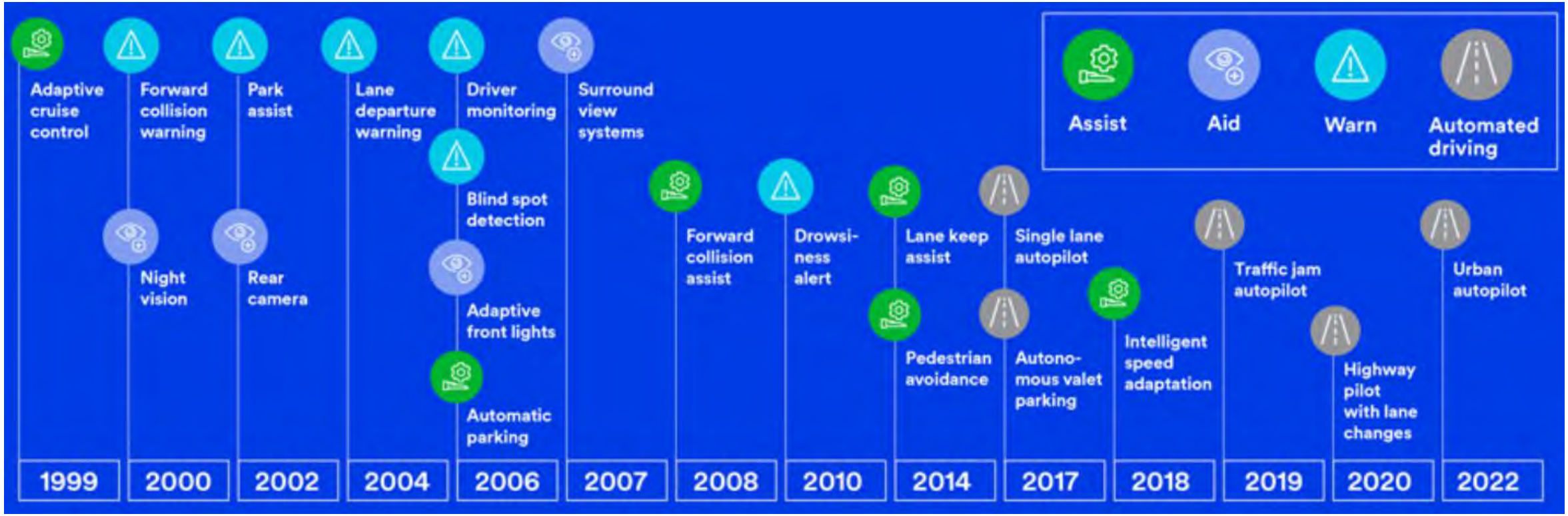
IoT Role Includes:

- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

Requires:

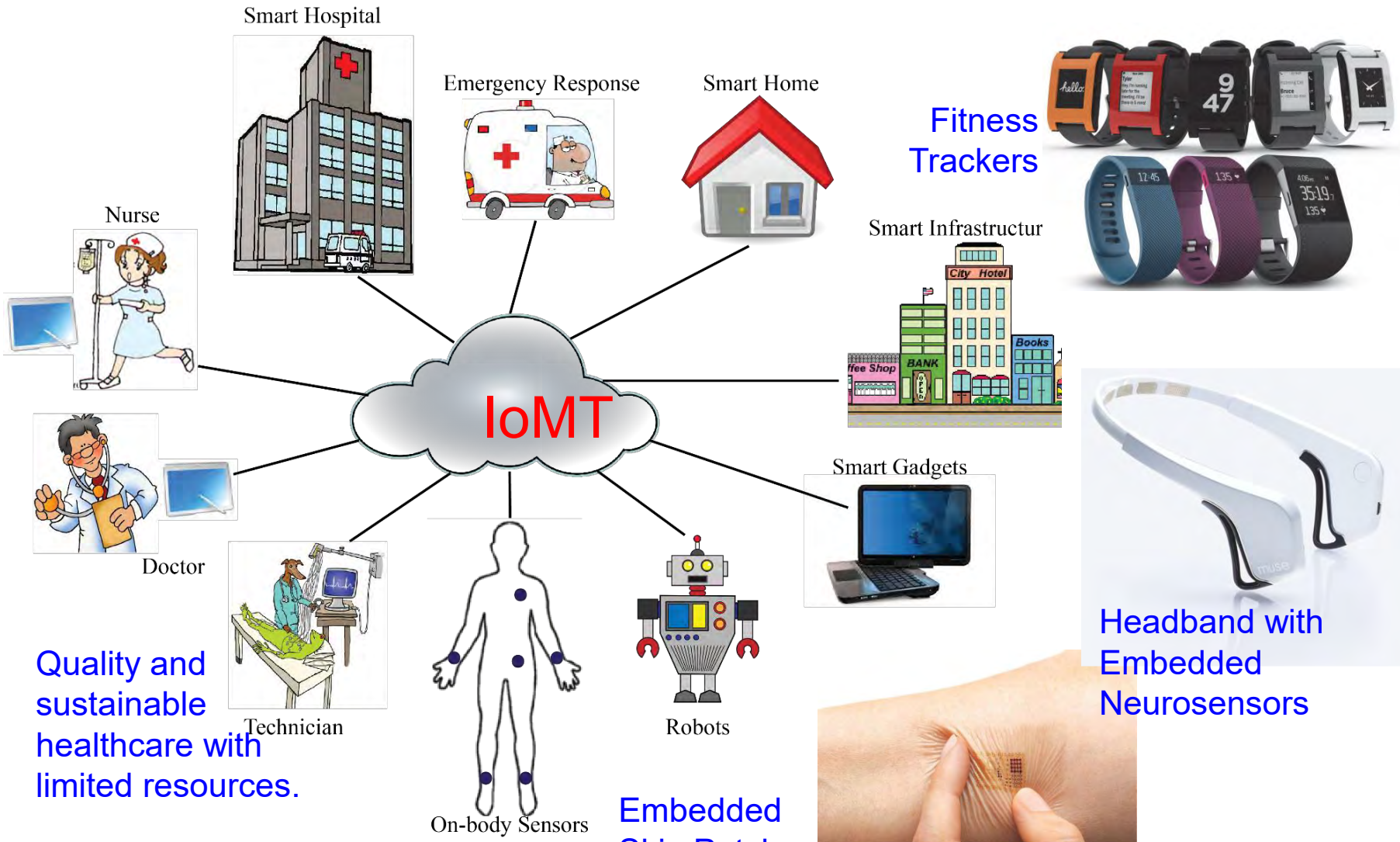
- Data and Device Security
- Location Privacy

Smart Car: Technology Roadmap



Source: https://www.3m.com/3M/en_US/particles/all-articles/article-detail/~transportation-future-of-mobility-automotive-cars/?storyid=8cea30a4-fe36-4abe-889a-37ea15134293
http://www.cargroup.org/wp-content/uploads/2018/01/Technology_Roadmap_Combined_23JAN18.pdf

Smart Healthcare



Quality and sustainable healthcare with limited resources.

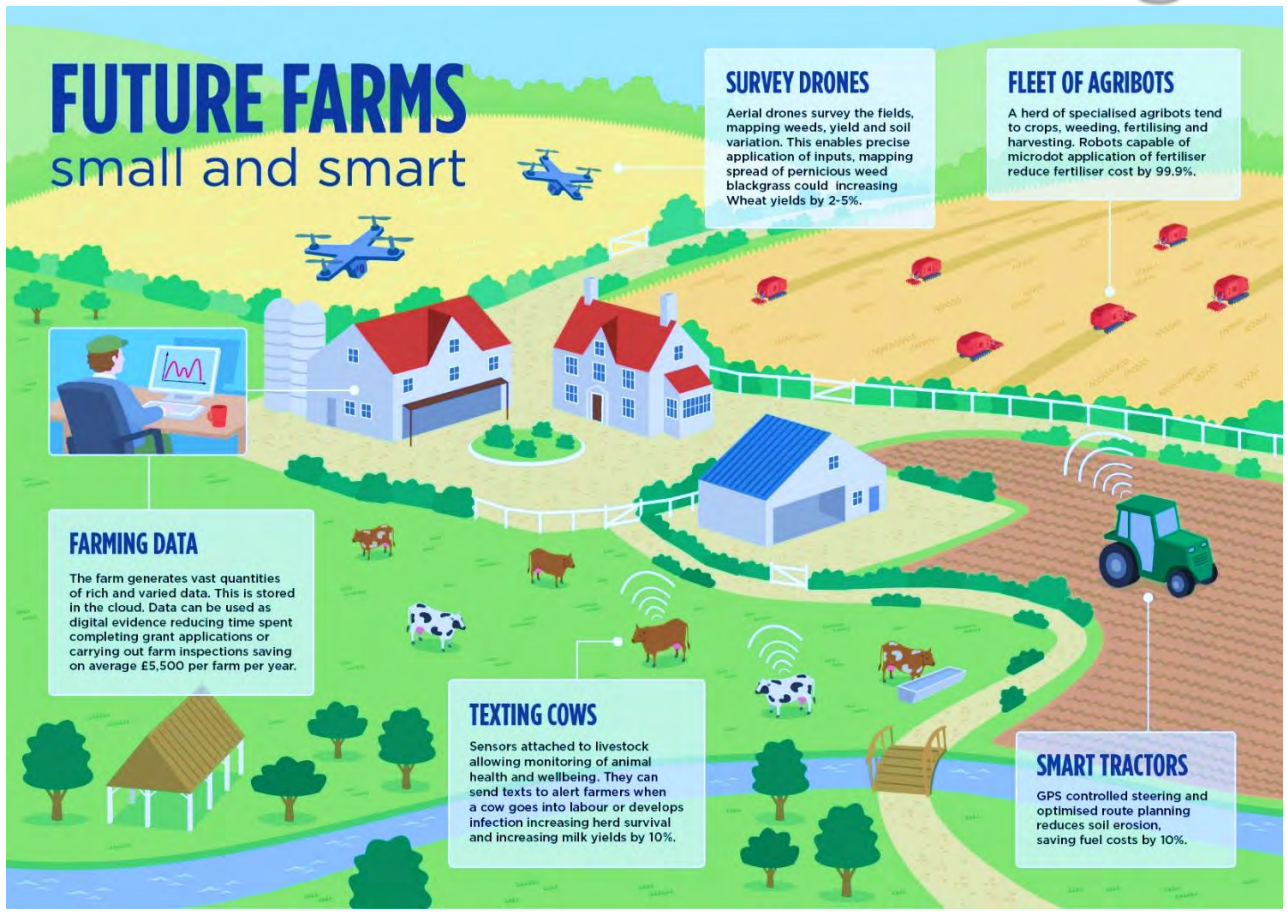
Source: Mohanty CE Magazine July 2016

Fitness Trackers

Headband with Embedded Neurosensors

Embedded Skin Patches

Smart Agriculture



Source: http://www.nesta.org.uk/blog/precision-agriculture-almost-20-increase-income-possible-smart-farming

Climate-Smart Agriculture
Objectives:
- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

http://www.fao.org

Internet-of-Agro-Things (IoAT)

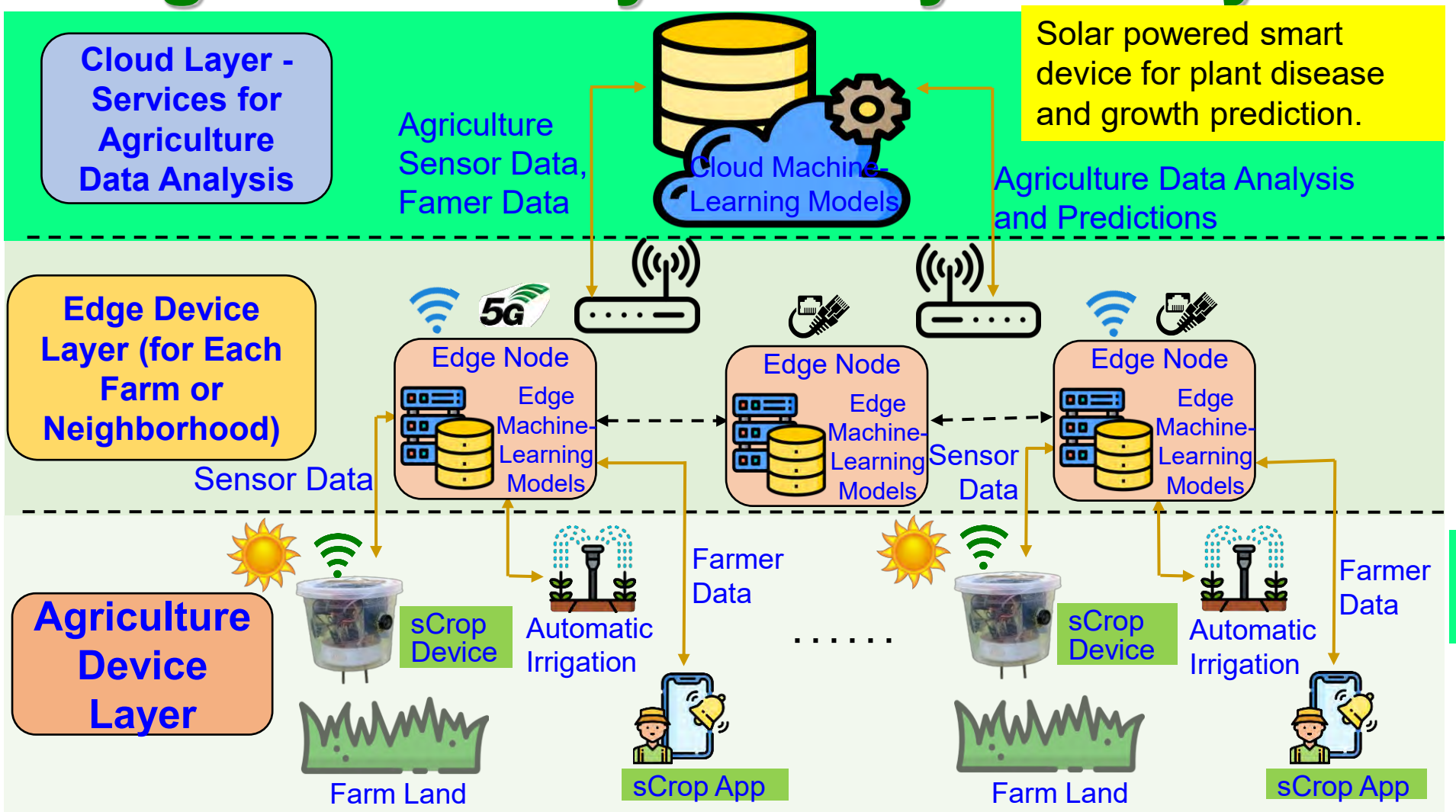
Automatic Irrigation System

Source: Maurya 2017, CE Magazine July 2017

Smart Agriculture/Farming Market Worth $18.21 Billion By 2025

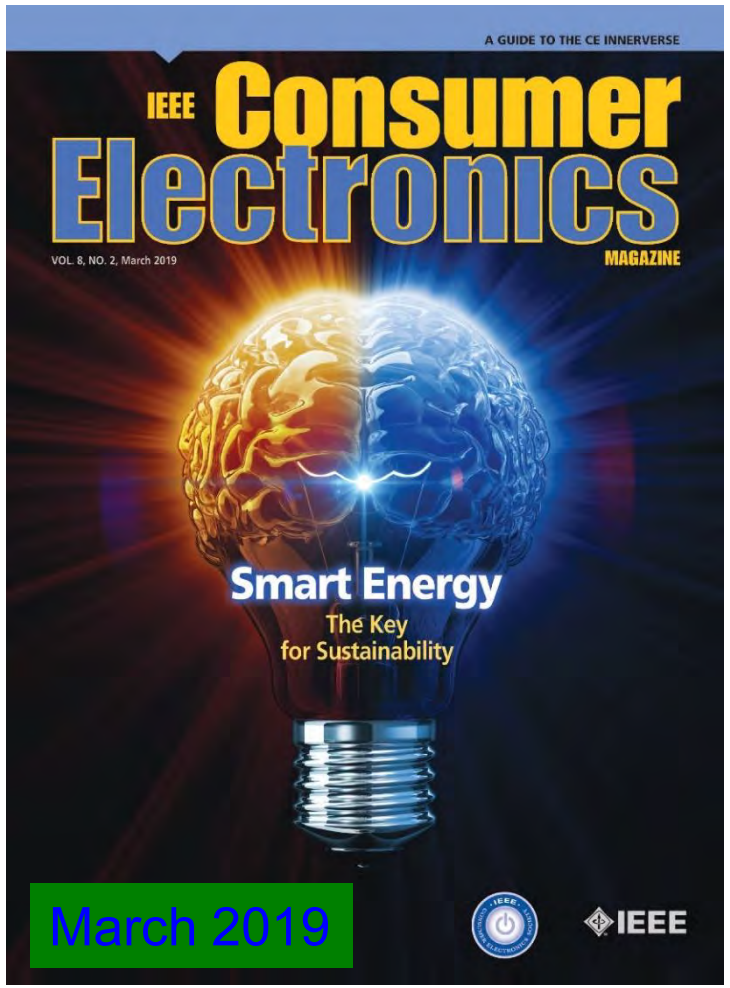
Sources: http://www.grandviewresearch.com/press-release/global-smart-agriculture-farming-market

Agriculture Cyber-Physical System (A-CPS)



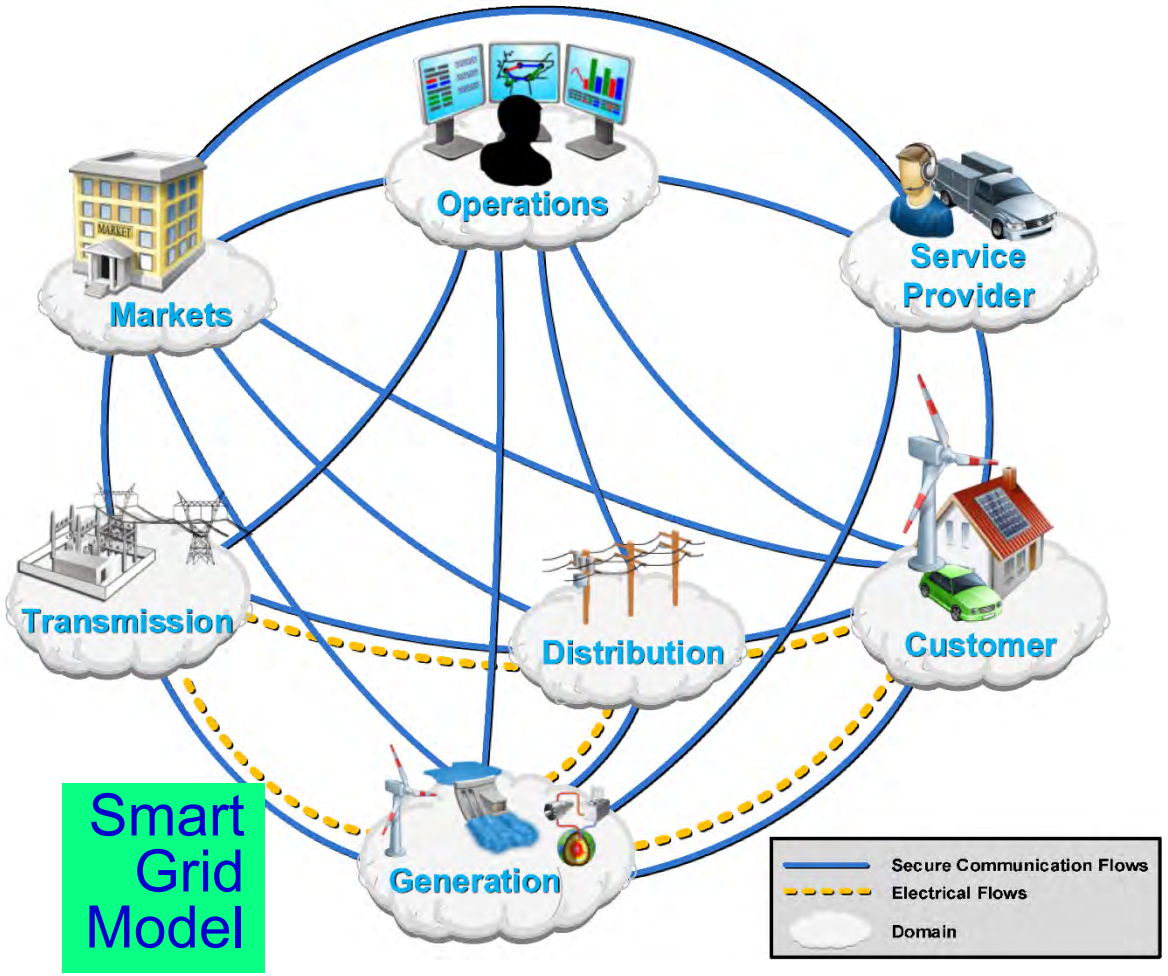
Source: V. Udutalapally, S. P. Mohanty, V. Pallagani, and V. Khandelwal, "sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture", *IEEE Sensors Journal*, Vol. XX, No. YY, ZZ 2020, pp. Accepted on 14 Oct 2020, DOI: 10.1109/JSEN.2020.3032438.

Energy Cyber-Physical Systems (E-CPS)



4 key features of smart grid:

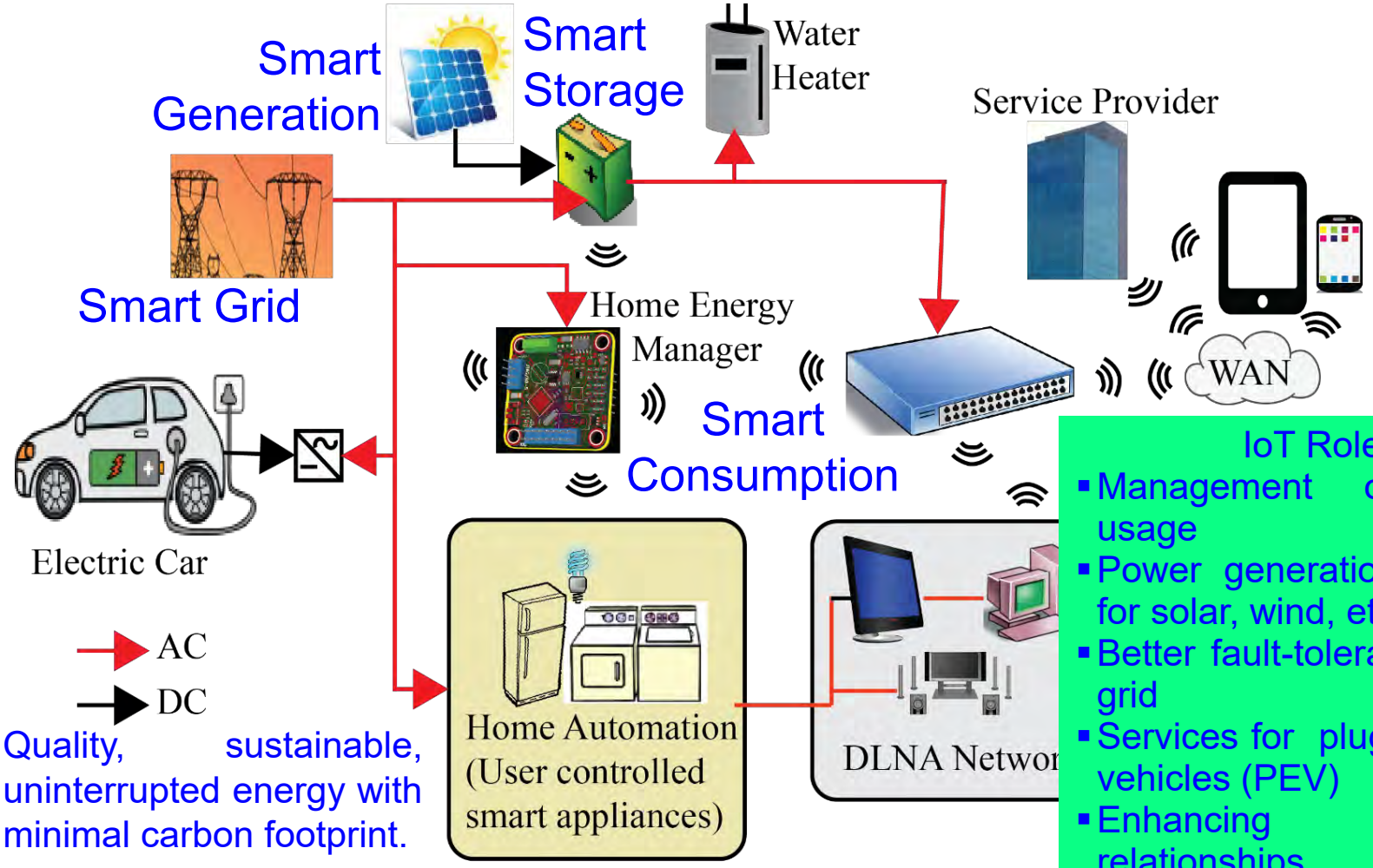
- Sensing
- Measurement
- Control
- Communications



Smart Grid Model

Source: https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30

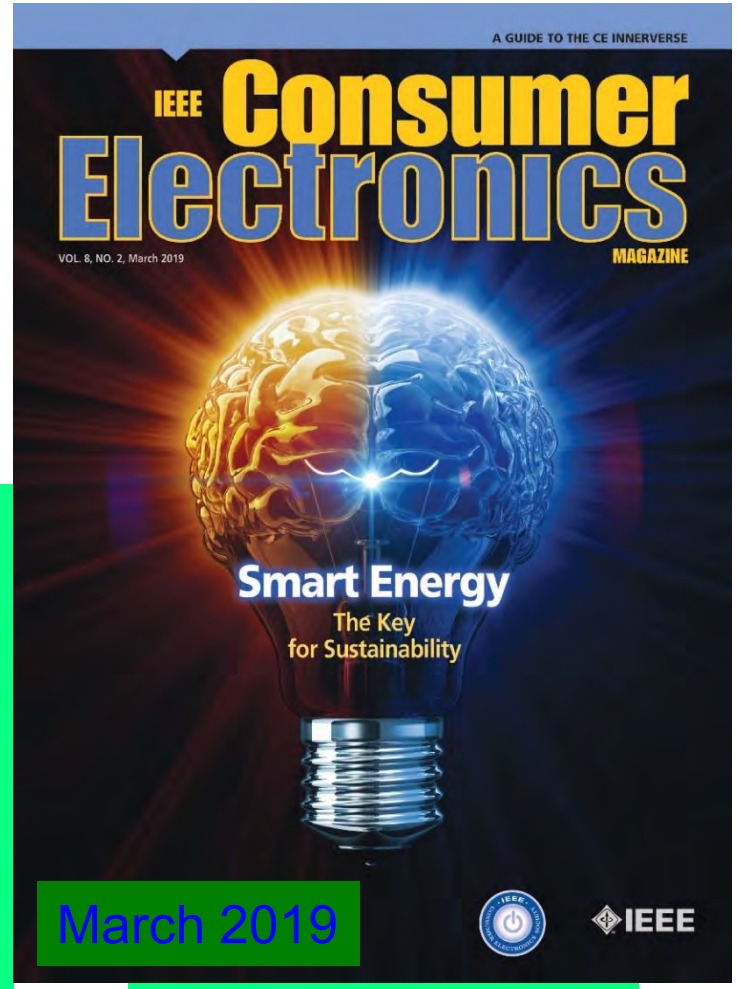
Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

IoT Role:

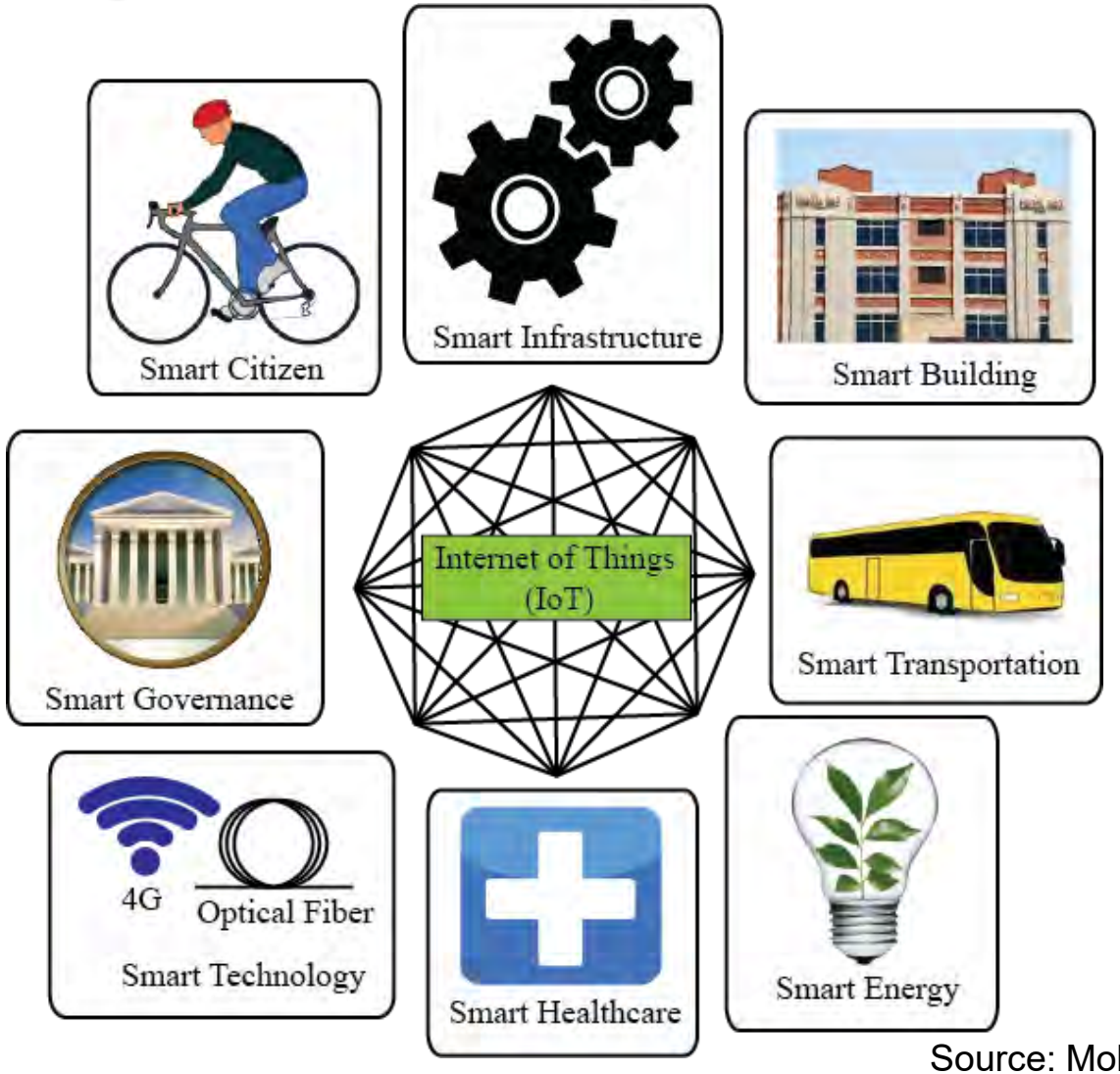
- Management of energy usage
- Power generation dispatch for solar, wind, etc.
- Better fault-tolerance of the grid
- Services for plug-in electric vehicles (PEV)
- Enhancing consumer relationships



Internet of Energy

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

System of Systems - Smart Cities



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

Source: Mohanty 2016, CE Magazine July 2016

Smart Cities Vs Smart Villages

City - An inhabited place of greater size, population, or importance than a town or village

-- Merriam-Webster

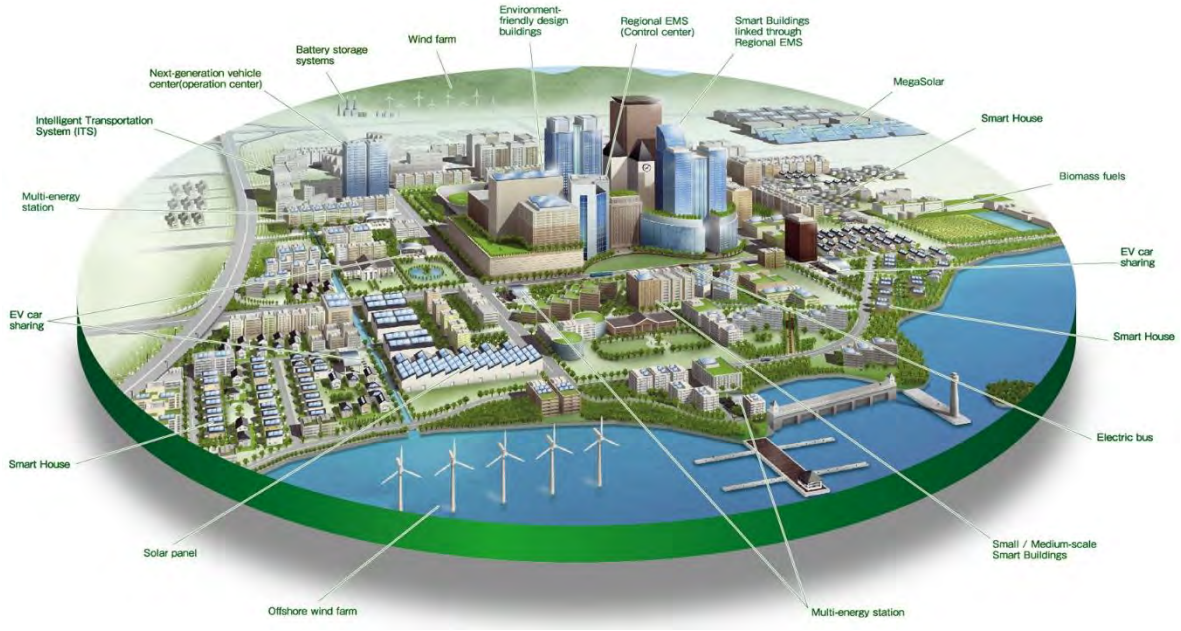
Smart City: A city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city".

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

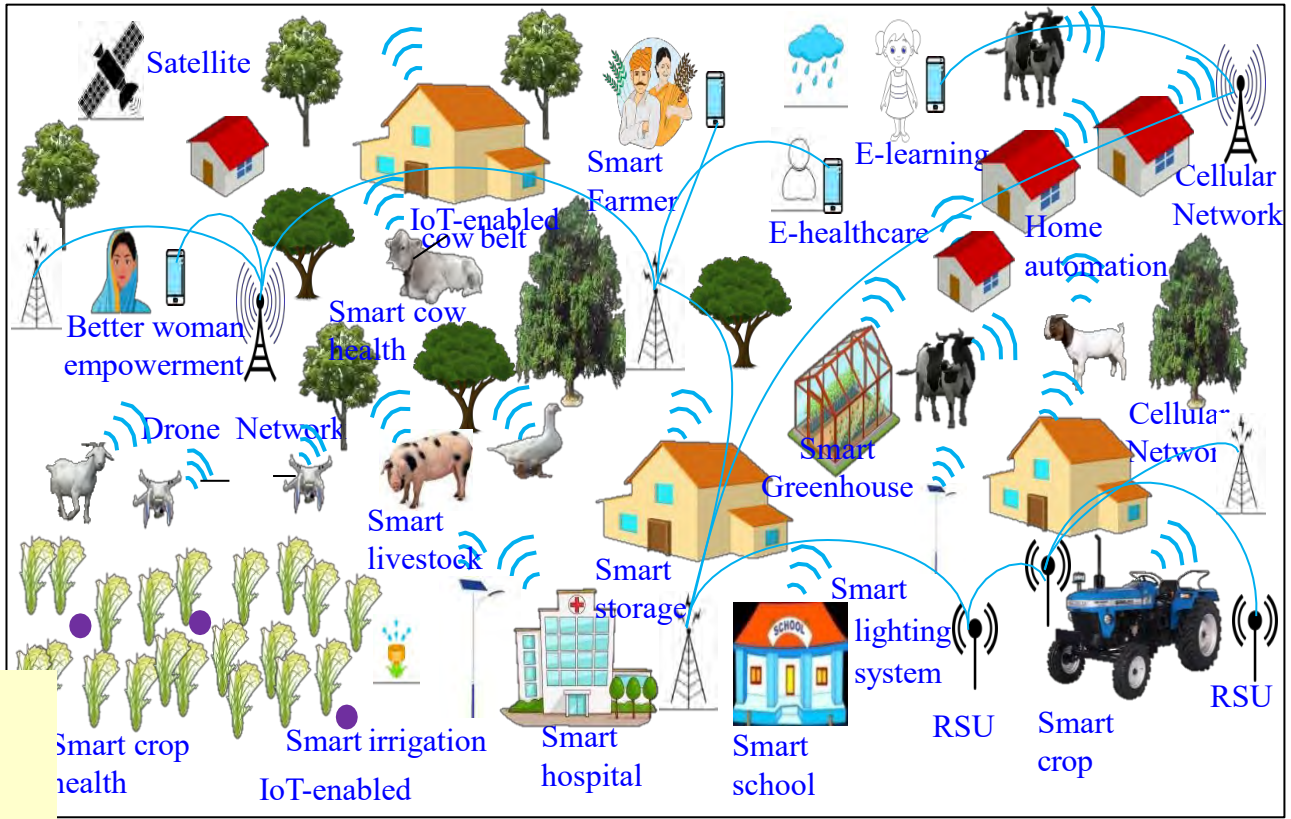
Smart Village: A village that uses information and communication technologies (ICT) for advancing economic and social development to make villages sustainable.

Source: S. K. Ram, B. B. Das, K. K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy Perspectives in IoT Driven Smart Villages and Smart Cities", *IEEE Consumer Electronics Magazine (MCE)*, Vol. XX, No. YY, ZZ 2021, DOI: 10.1109/MCE.2020.3023293.

Smart Cities Vs Smart Villages



Source: http://edwingarcia.info/2014/04/26/principal/



Smart Cities

CPS Types - More
Design Cost - High
Operation Cost – High
Energy Requirement - High

Smart Villages

CPS Types - Less
Design Cost - Low
Operation Cost – Low
Energy Requirement - Low

Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

IoT, Connected, and Smart?

"An IoT product is more valuable than a connected product or a smart product or even a smart, connected product."

However:

- Physical Component + IoT → Smart Component?
- Product + Data + AI → Smart Product?

Source: Bruce Sinclair - https://www.iot-inc.com/the-iot-product-versus-the-smart-and-connected-product-article/

Energy, Security, and Response Smart (ESR-Smart)

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
- 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

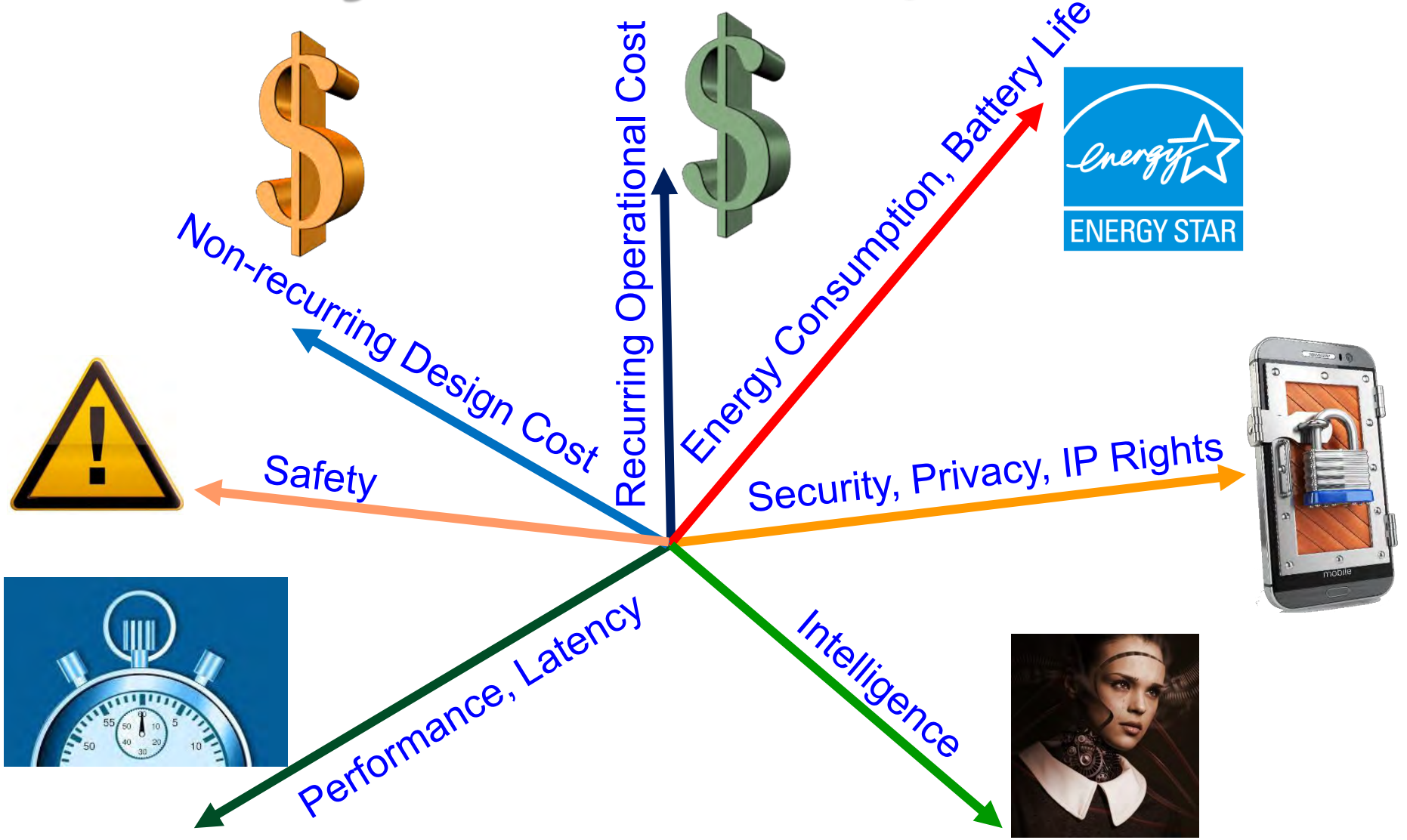
IR Hardware Security | Memory Protection | Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

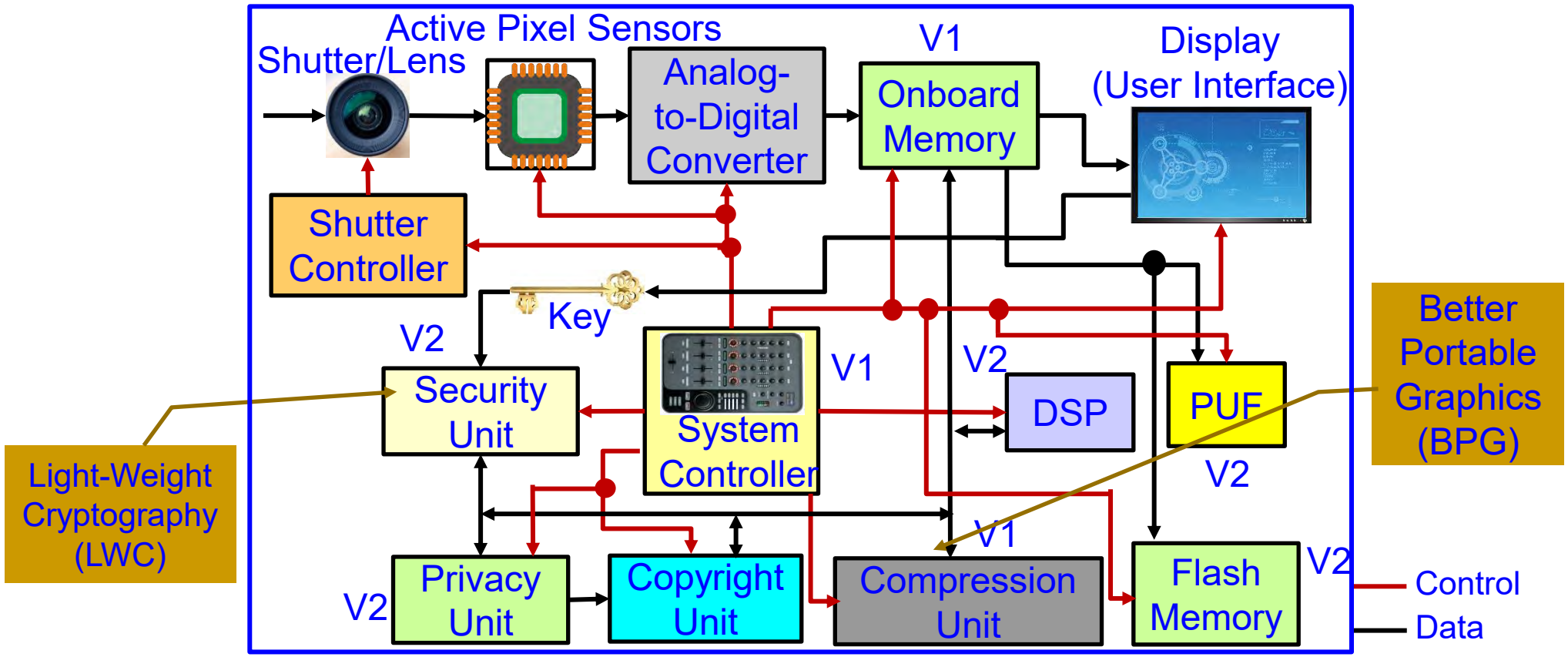
Trustworthy CE System

- A selective attributes of CE system to be trustworthy:
  - It must maintain integrity of information it is processing.
  - It must conceal any information about the computation performed through any side channels such as power analysis or timing analysis.
  - It must perform only the functionality it is designed for, nothing more and nothing less.
  - It must not malfunction during operations in critical applications.
  - It must be transparent only to its owner in terms of design details and states.
  - It must be designed using components from trusted vendors.
  - It must be built/fabricated using trusted fabs.

CE/IoT System - Multi-Objective Tradeoffs



Secure Digital Camera (SDC) – My Invention

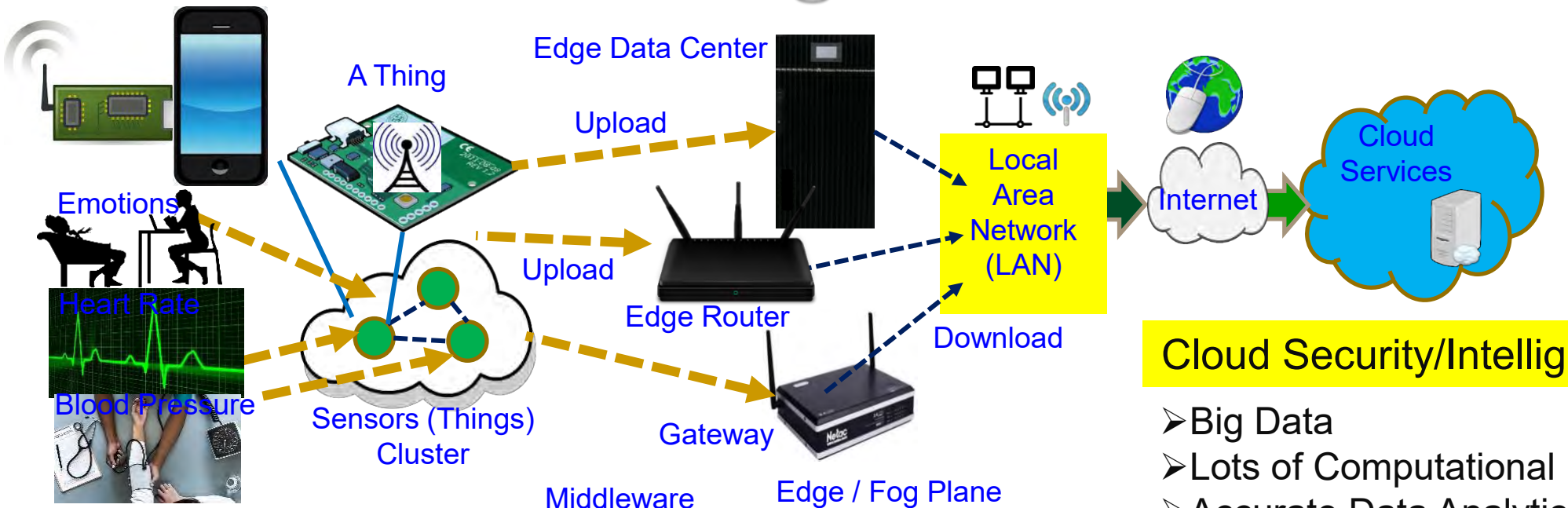


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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.

CPS – IoT-Edge Vs IoT-Cloud



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

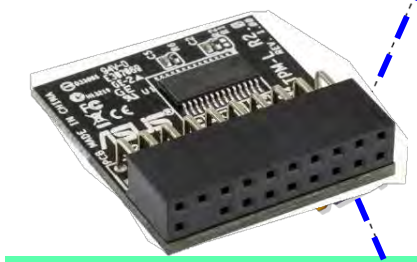
- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy overhead in Communications

TinyML at End and/or Edge is key for smart villages.

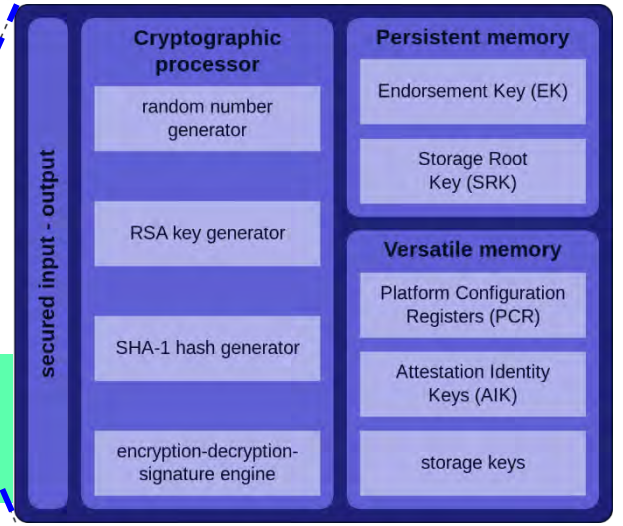
Heavy-Duty ML is more suitable for smart cities

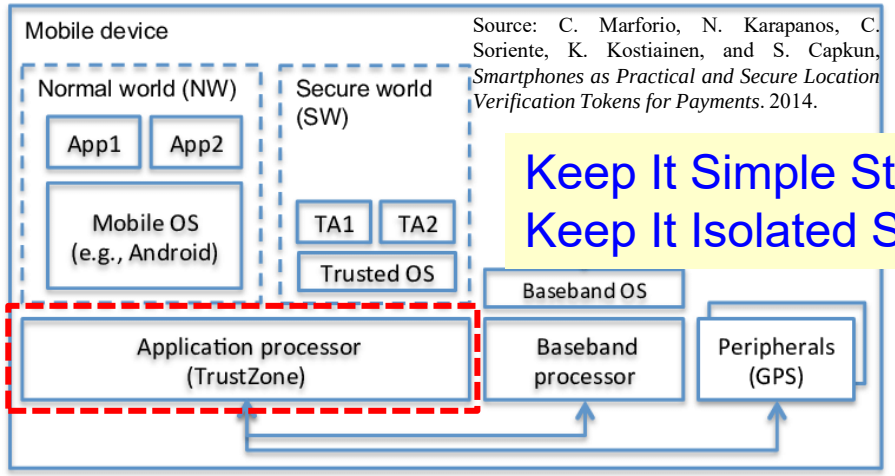
Hardware Security Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



Trusted Platform Module (TPM)





Source: C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun, *Smartphones as Practical and Secure Location Verification Tokens for Payments*. 2014.

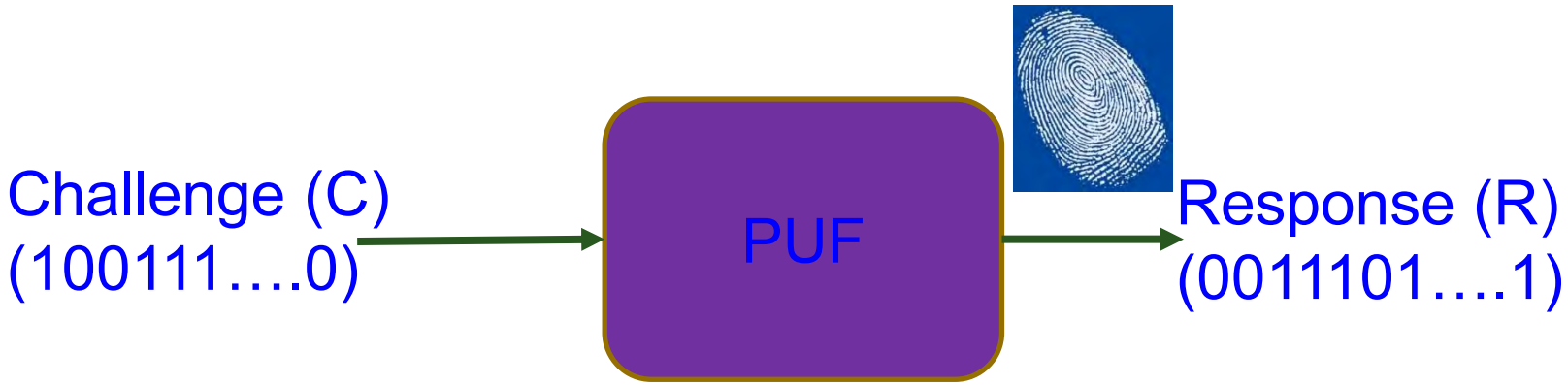
Keep It Simple Stupid (KISS) →
Keep It Isolated Stupid (KIIS)

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Physical Unclonable Functions (PUFs) - Principle

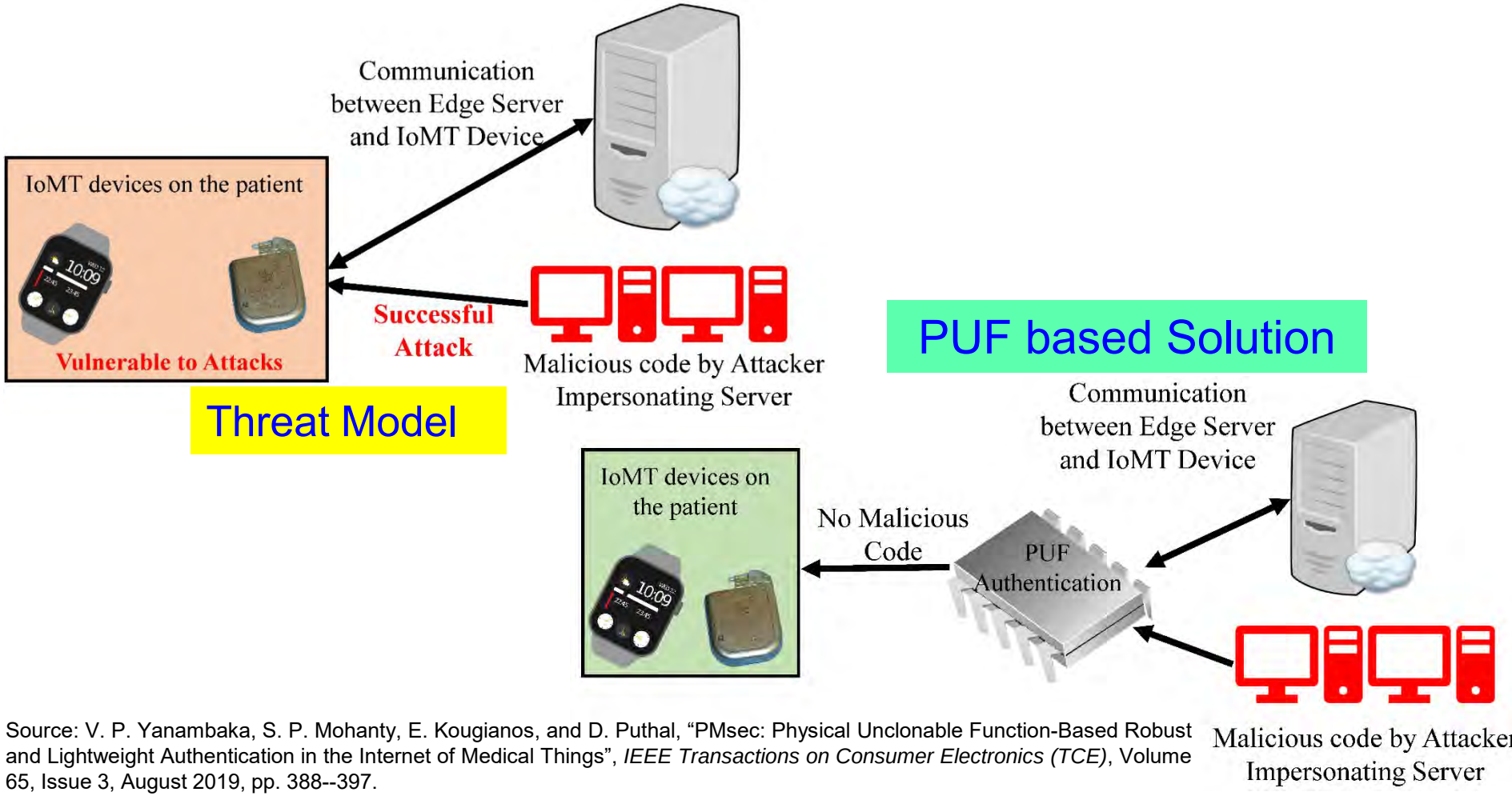
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

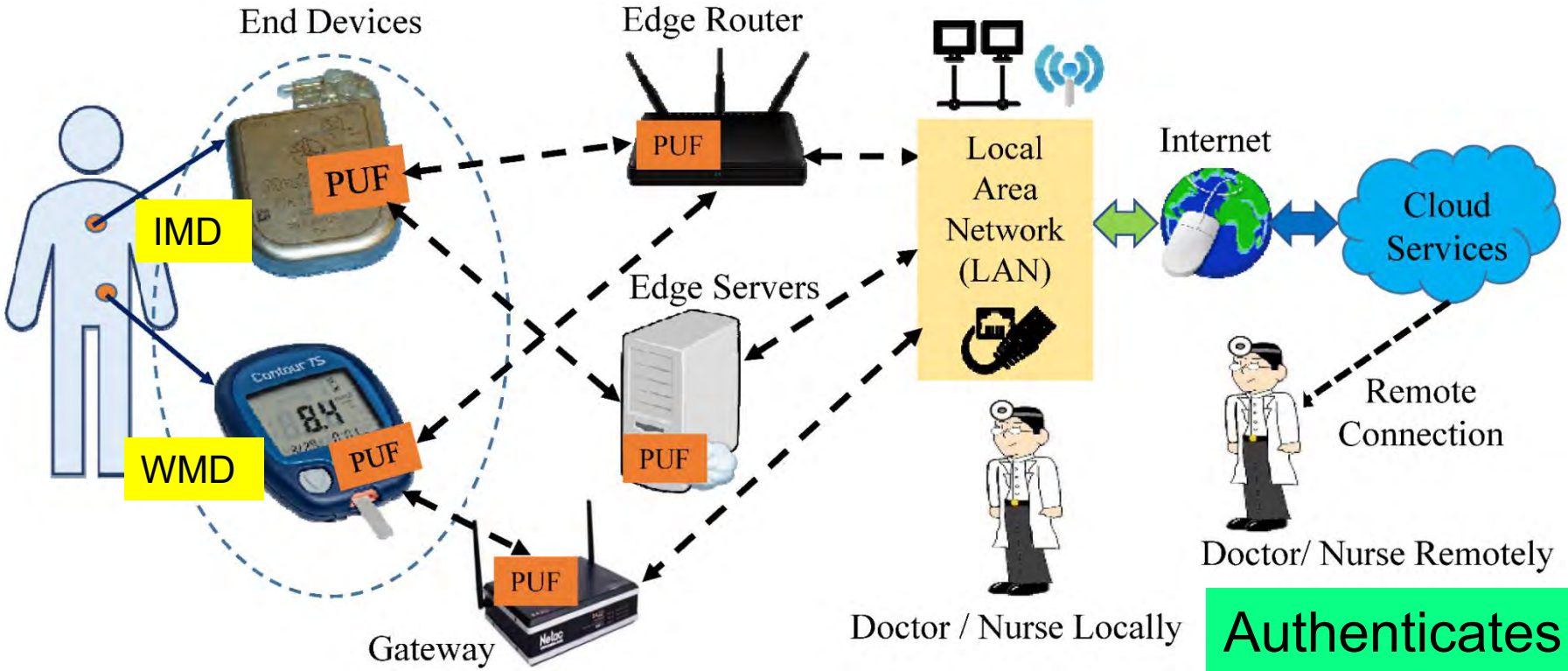
Source: S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



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.

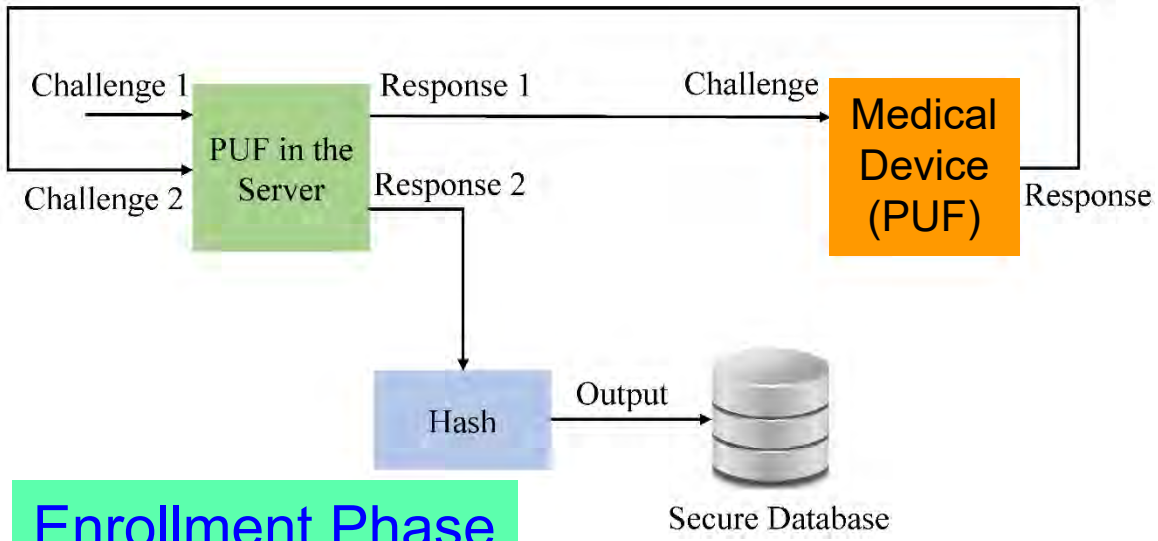
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

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 – Our Proposed PMsec

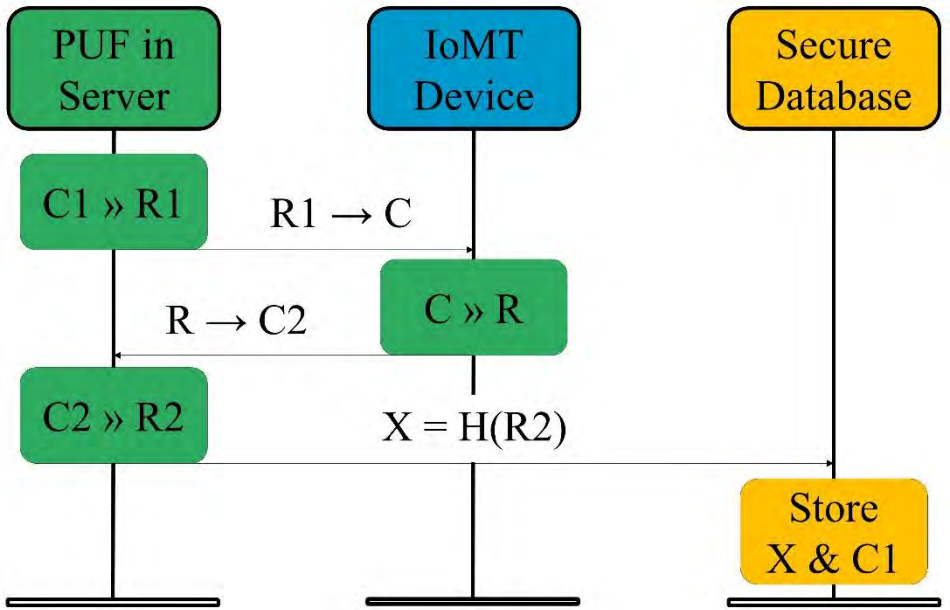


Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

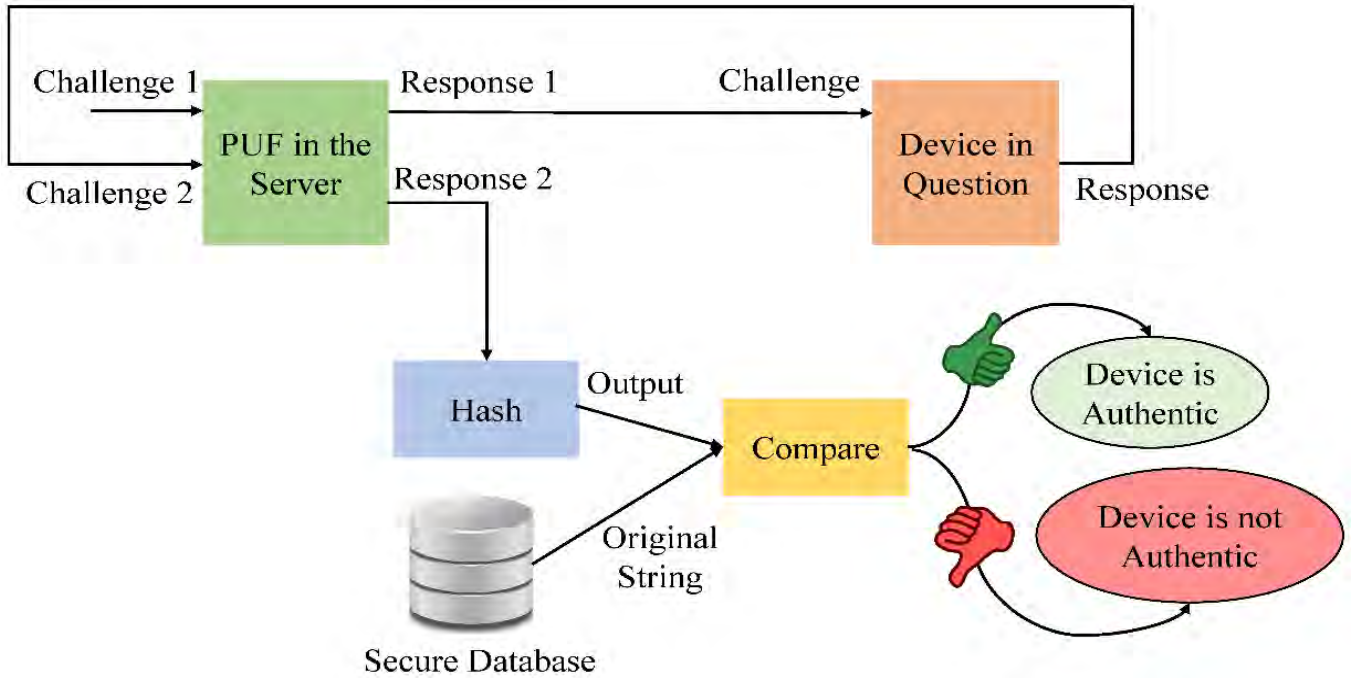


PUF Security Full Proof:

- 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 – Our Proposed PMsec

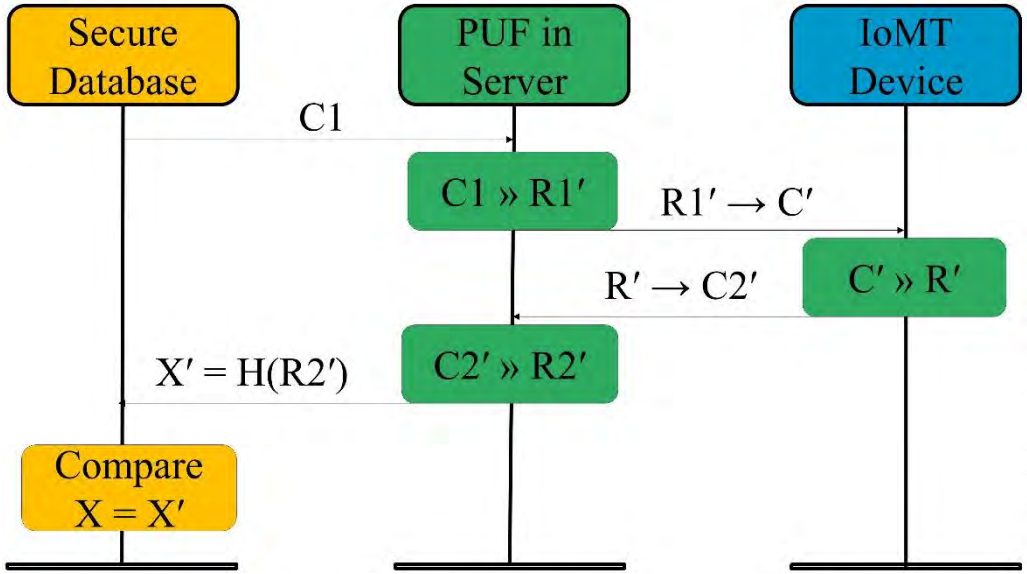


Authentication Phase

At the Doctor

- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



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 – Our PMsec in Action

```
------------Enrollment Phase------------
Generating the Keys
Sending the keys to the Client
Receiving the Keys from the client
Saving the database
>>>
```

Output from IoMT-Server during Enrollment

Output from the IoMT-Device

COM4

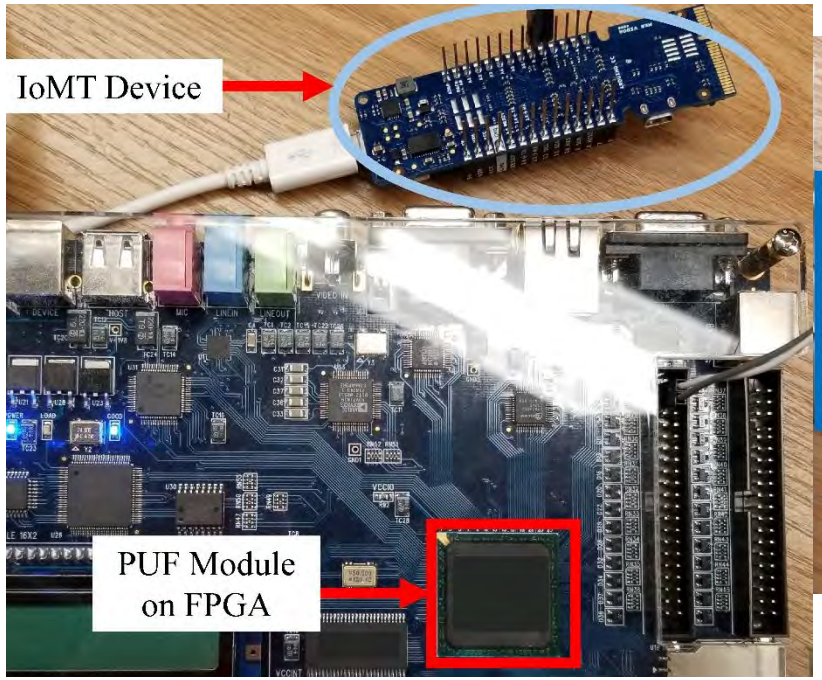
```
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 10111000010111001011110001011110001011010011011100101001010000011
Sending key for authentication
```

Output from IoMT-Server during Authentication

```
>>>
Hello
------------Authentication Phase------------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  10111000010111001011110001011110001011010011011100101001010000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>>
```

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 – Our Proposed PMsec



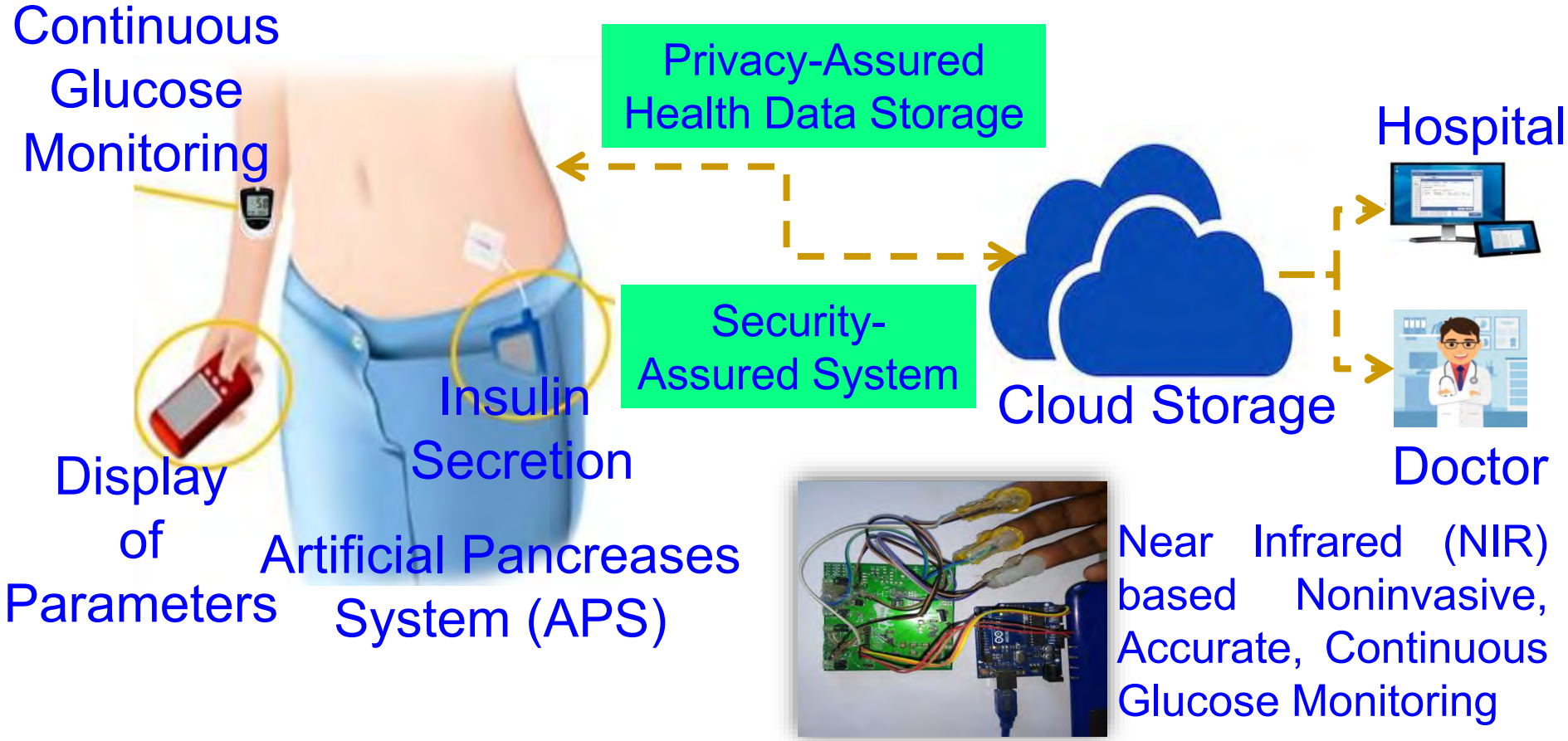
Average Power Overhead – 200 μW

Ring Oscillator PUF – 64-bit, 128-bit, …

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

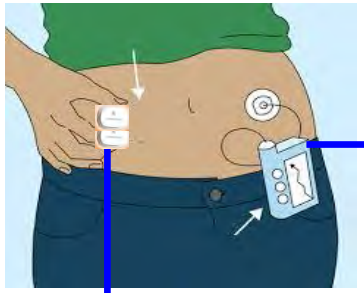
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics*, Vol 65, No 3, Aug 2019, pp. 388--397.

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery



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. 35–42.

Secure-iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery



iGLU Insulin Delivery Subsystem (PUF)

Secure-iGLU Controller (PUF)

iGLU Glucose-Level Monitoring Subsystem (PUF)

Edge Datacenter or Cloud Datacenter (CRPs from PUFs of Devices)

iGLU Device (IoMT Node)

PUF

Secure-iGLU Controller (PUF)

Arbiter PUF – 64-bit, 128-bit, 256 bit …

Challenge Response Table

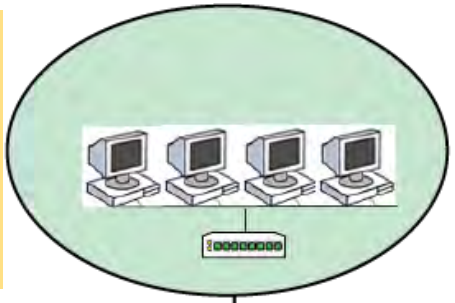
Challenges	Responses Ri
100101100	11010110
100101001	101001010
010111001	110111101

Match ?

Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020.

Energy Consumption in IoT

Energy from Supply/Battery - Energy consumed by Workstations, PC, Software, Communications



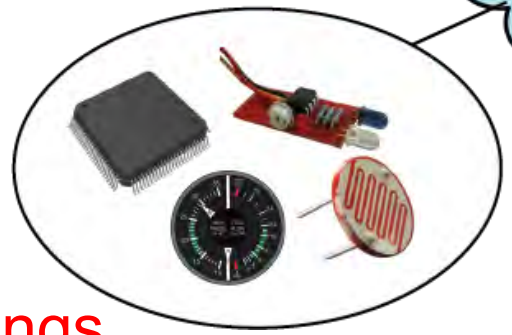
Local Area Network (LAN)

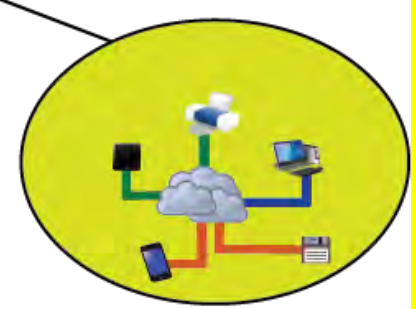
Energy from Supply/Battery - Energy consumed by Communications

Internet

Battery Operated - Energy consumed by Sensors, Actuators, Microcontrollers

The Cloud





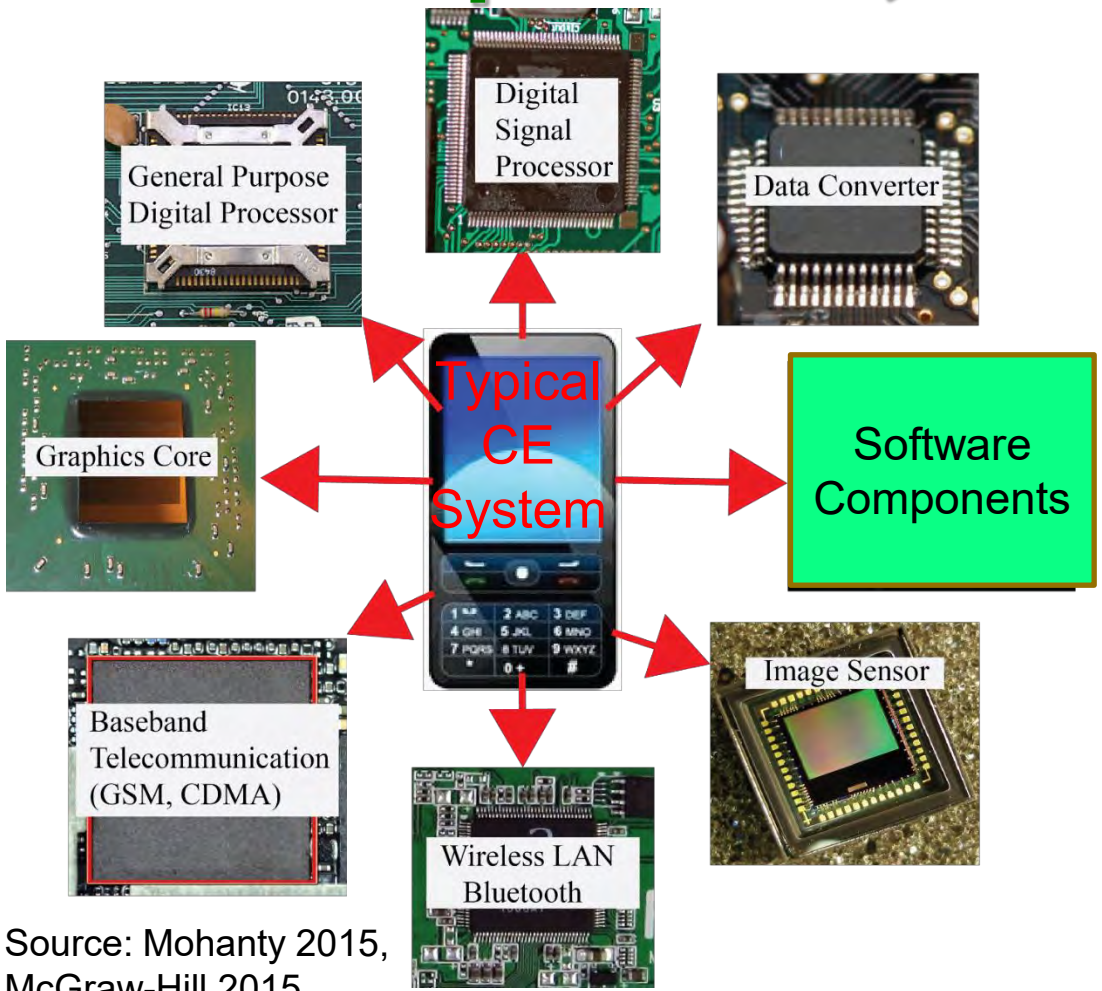
Energy from Supply - Energy consumed in Server, Storage, Software, Communications

The Things

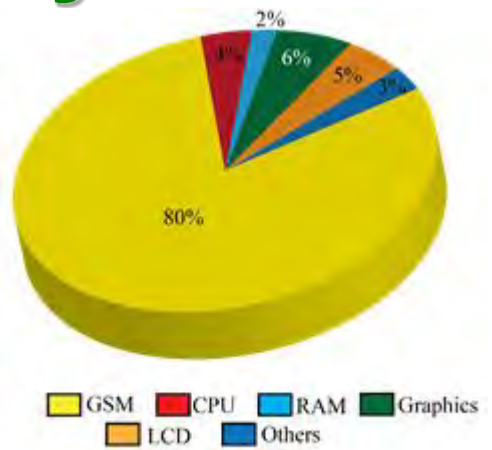
Four Main Components of IoT.

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

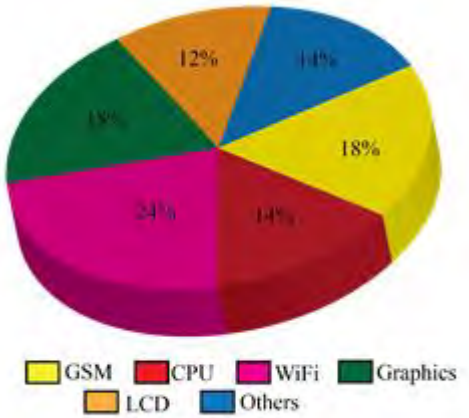
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015



During GSM Communications



During WiFi Communications

Energy Consumption and Latency in Communications

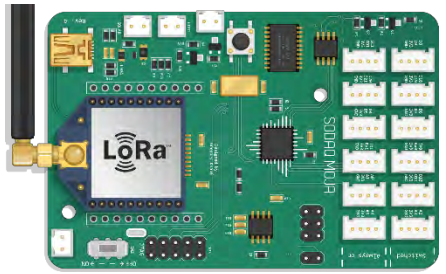
- IoT with Cloud: Sensor big data goes to cloud for storage and analytics – Consumes significant energy in communications network
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Lower power
- 5G for connected world: Enables all devices to be connected seamlessly.

Source: https://www.linkedin.com/pulse/key-technologies-connected-world-cloud-computing-ioe-balakrishnan

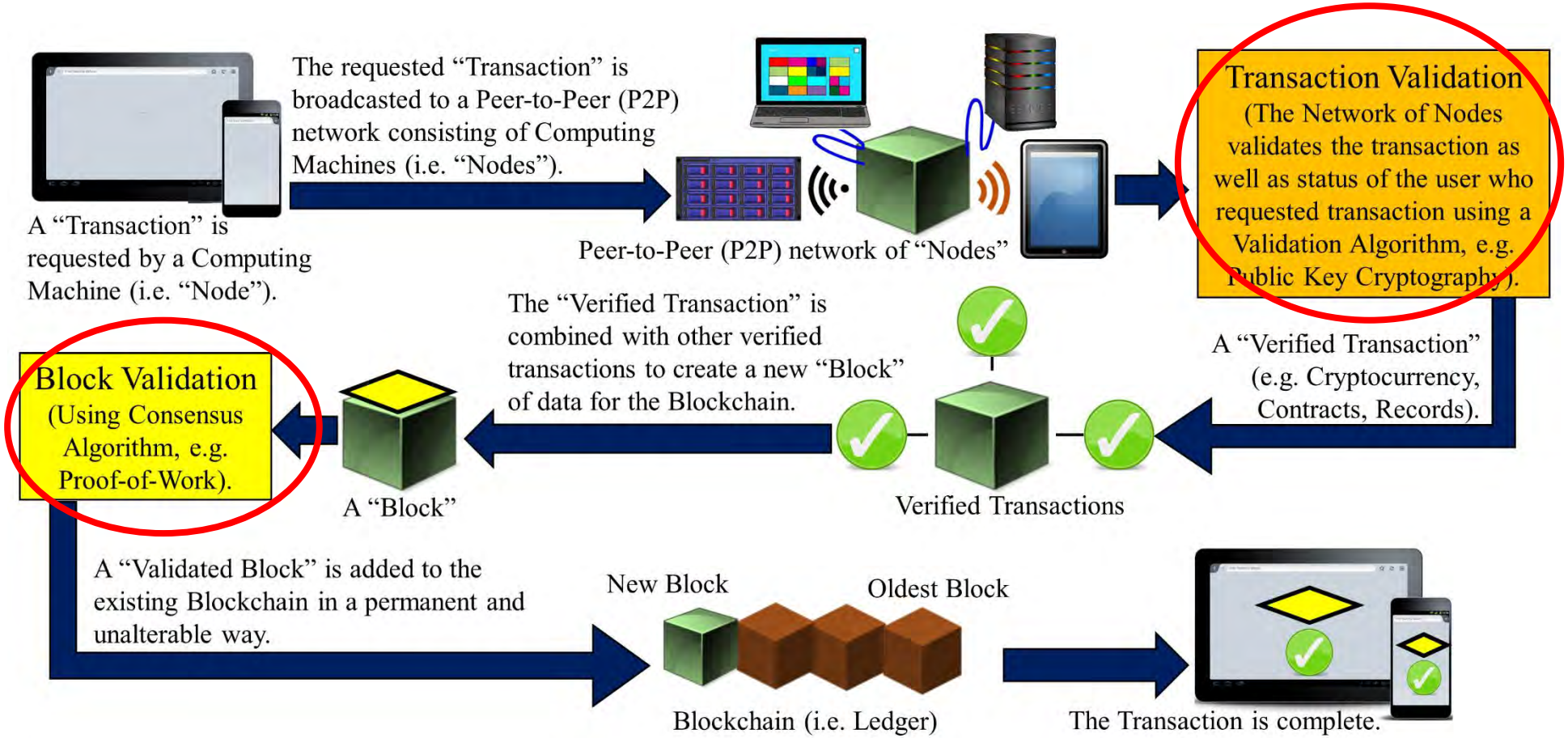
Communications – Energy and Data, Range Tradeoffs

- LoRa: Long Range, low-powered, low-bandwidth, IoT communications as compared to 5G or Bluetooth.
- SigFox: SigFox utilizes an ultra-narrowband wide-reaching signal that can pass through solid objects.

Technology	Protocol	Maximum Data Rate	Coverage Range
ZigBee	ZigBee Pro	250 kbps	1 mile
WLAN	802.11x	2-600 Mbps	0.06 mile
Cellular	5G	1 Gbps	Short - Medium
LoRa	LoRa	50 kbps	3-12 miles
SigFox	SigFox	1 kbps	6-30 miles

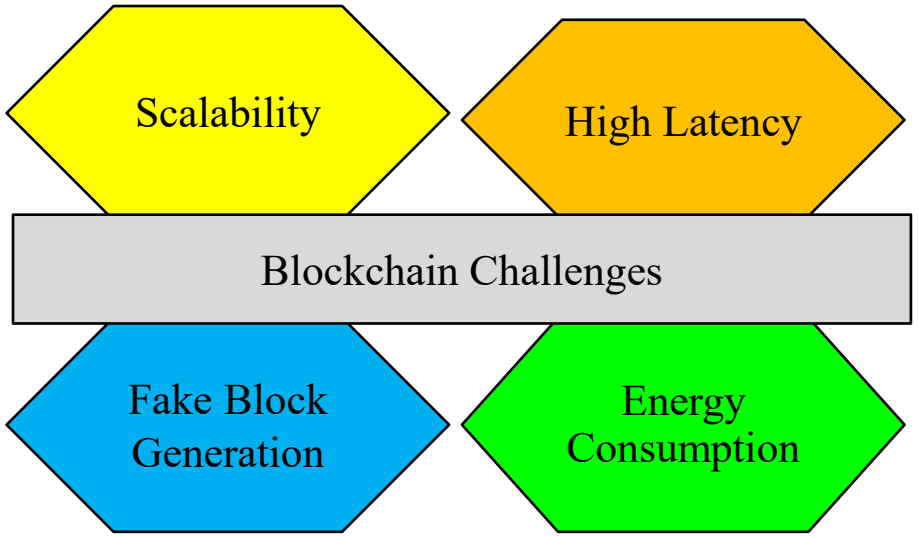


Blockchain Technology

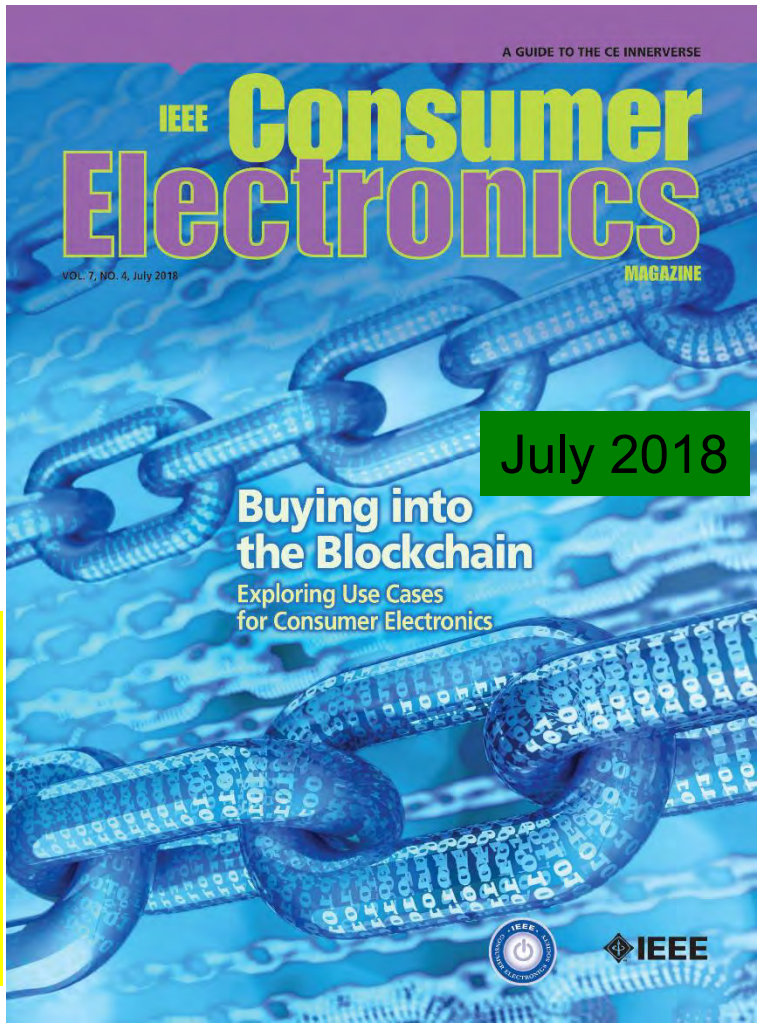


Source: Mohanty 2018, CE Magazine July 2018

Blockchain – Energy Issue



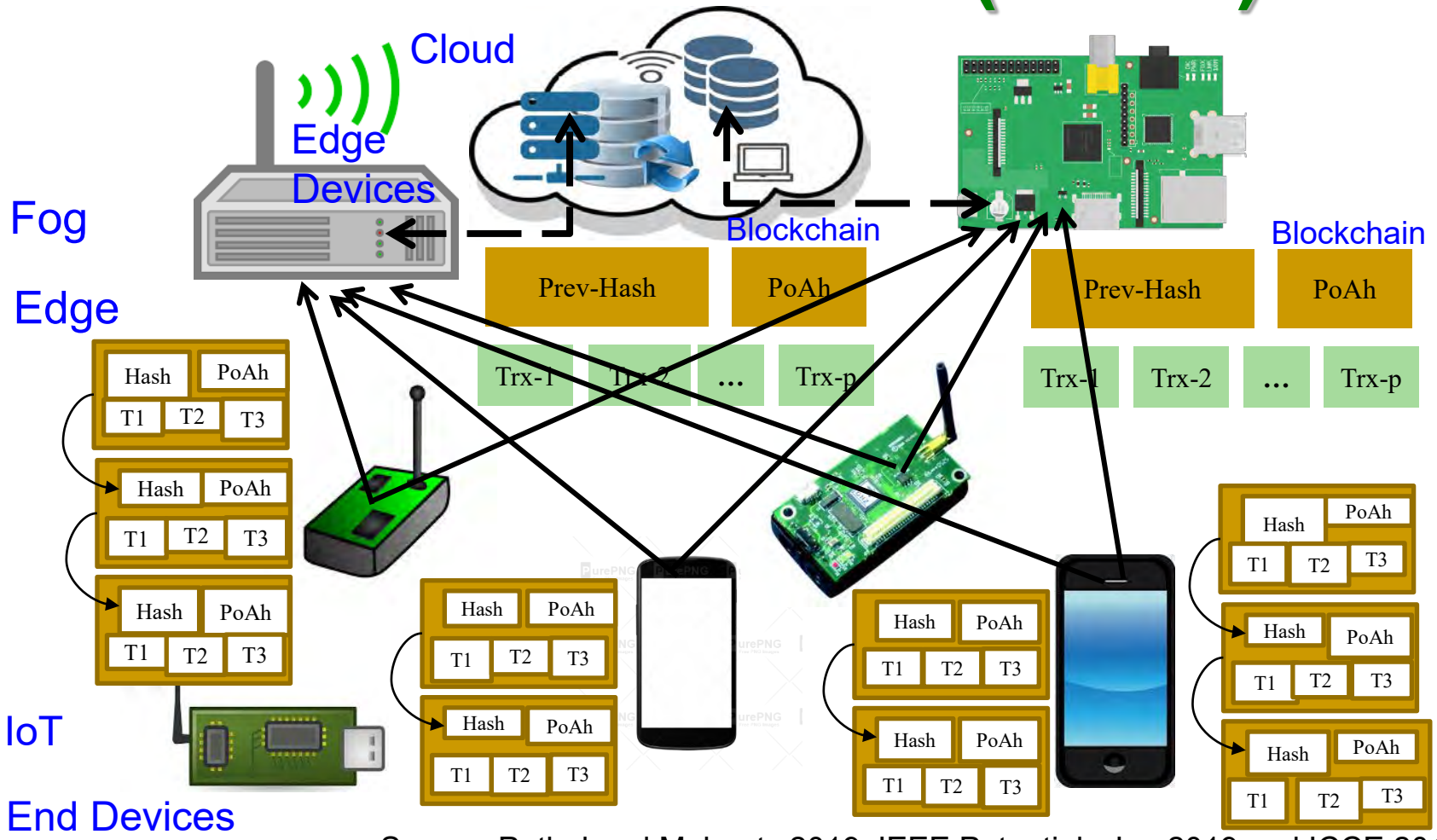
Source: Mohanty 2018, CE Magazine July 2018



- 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.

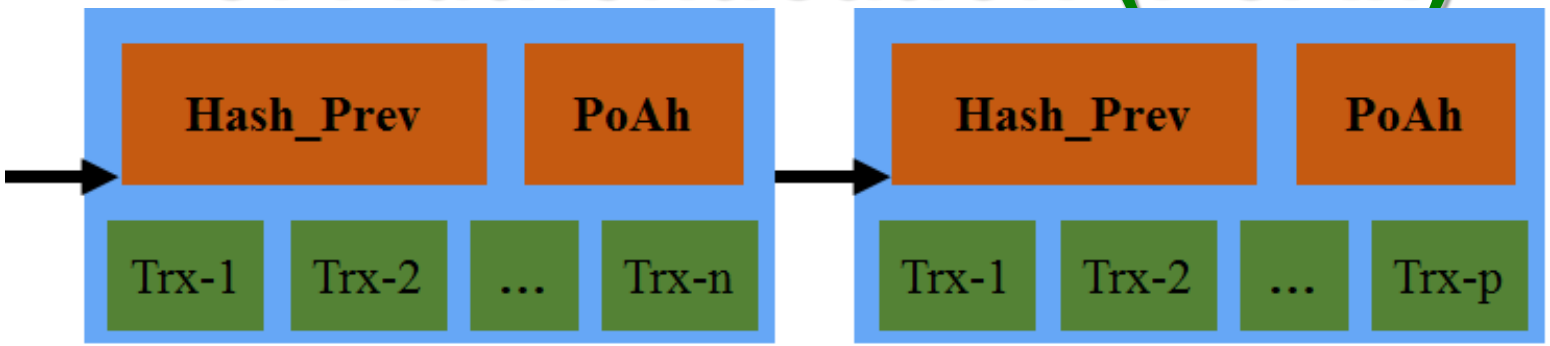
Source: N. Popper, "There is Nothing Virtual About Bitcoin's Energy Appetite", The New York Times, 21st Jan 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

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



Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

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

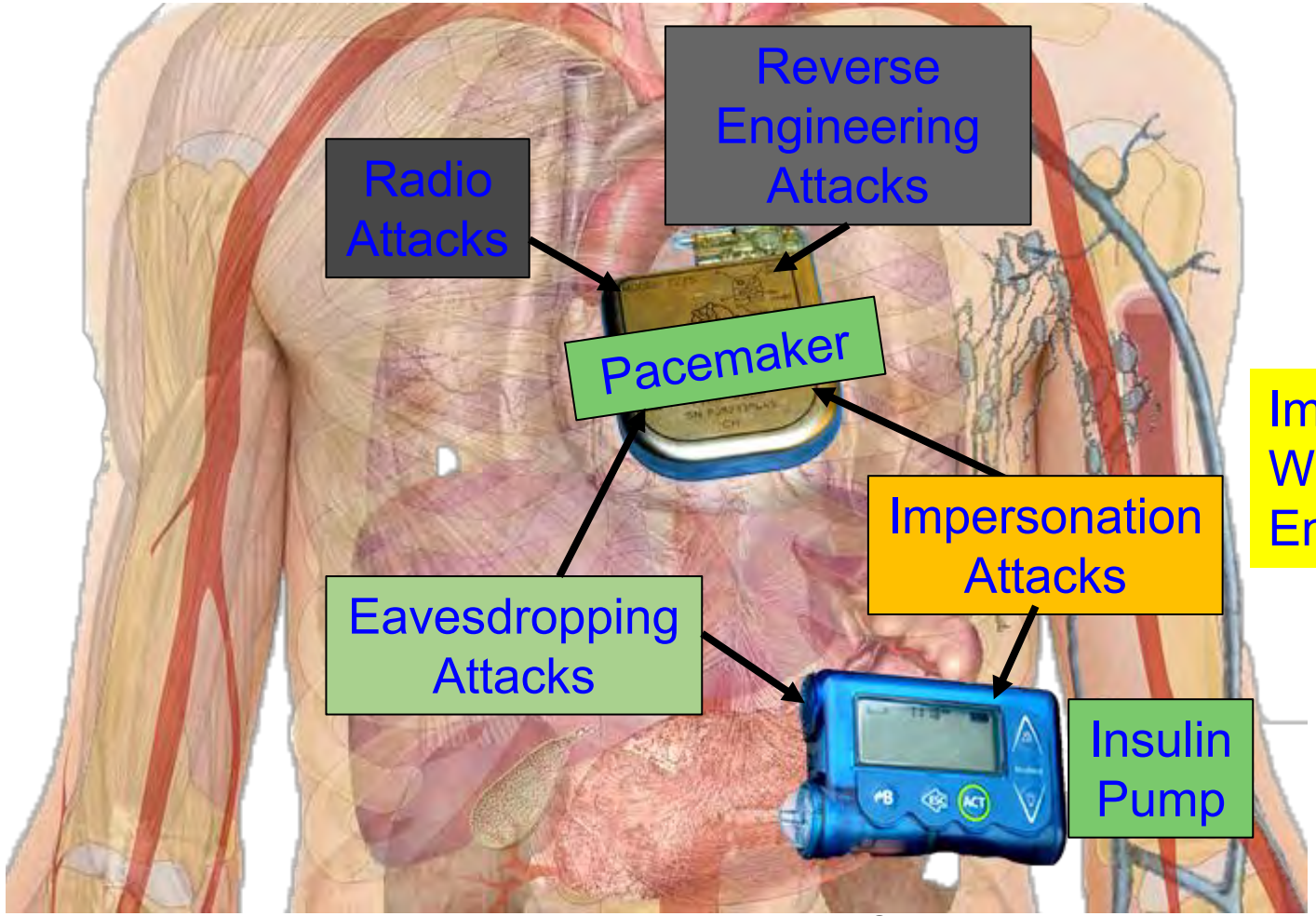


	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

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

Source: Puthal and Mohanty 2019, IEEE Potentials Jan 2019 and ICCE 2019

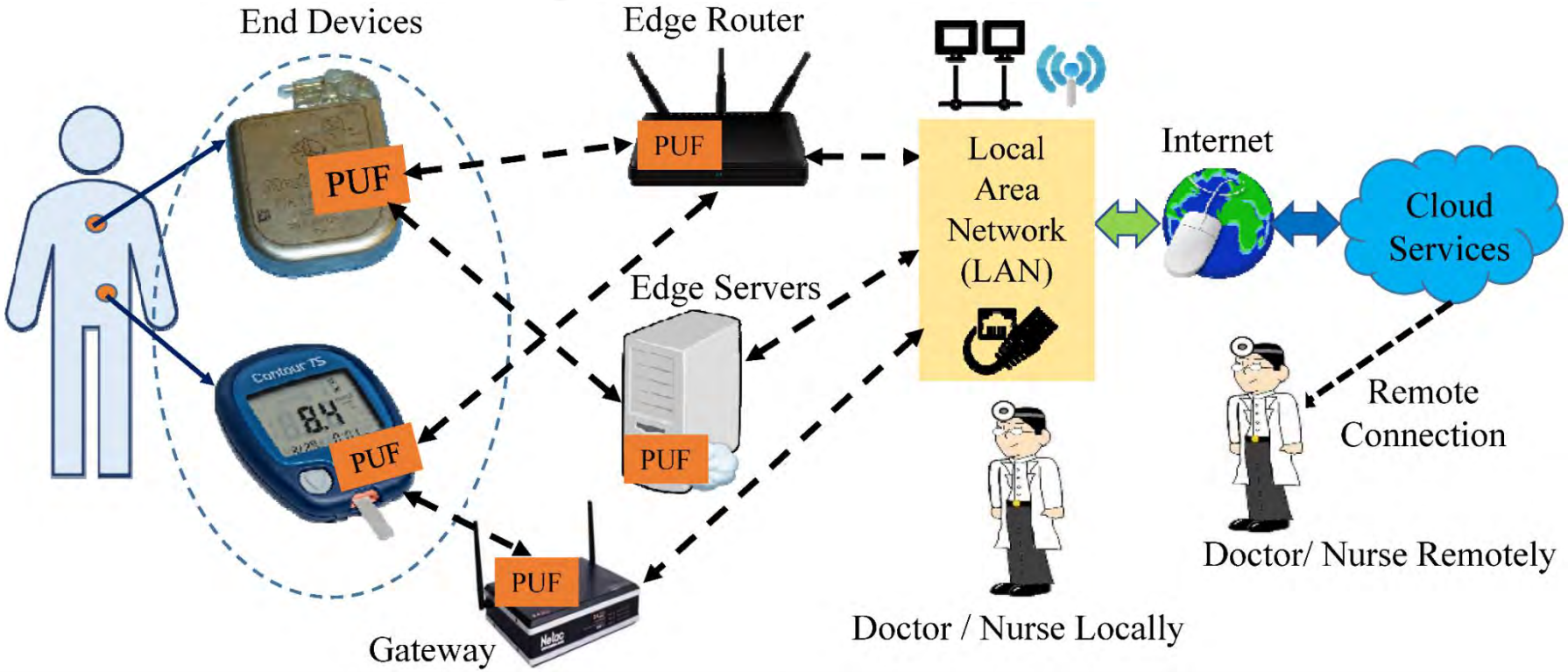
Security Measures in Smart Devices – Smart Healthcare



Implantable / Wearable Security – Energy Constraints

Source: Mohanty 2019, IEEE TCE Under Preparation

IoMT Security – A PUF a Device Authentication



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: Mohanty 2019, IEEE TCE Under Preparation

CE System Security – Smart Car

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

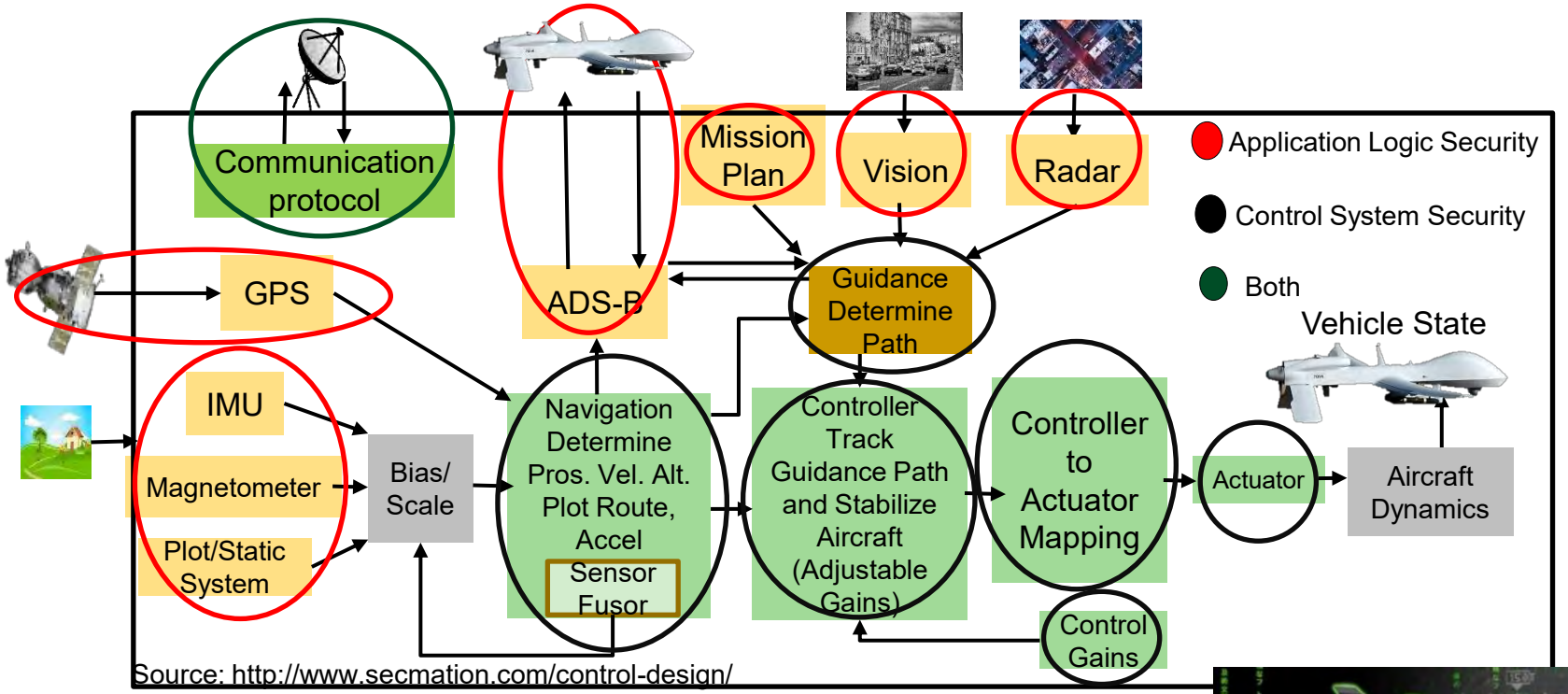
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

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

CE System Security – UAV



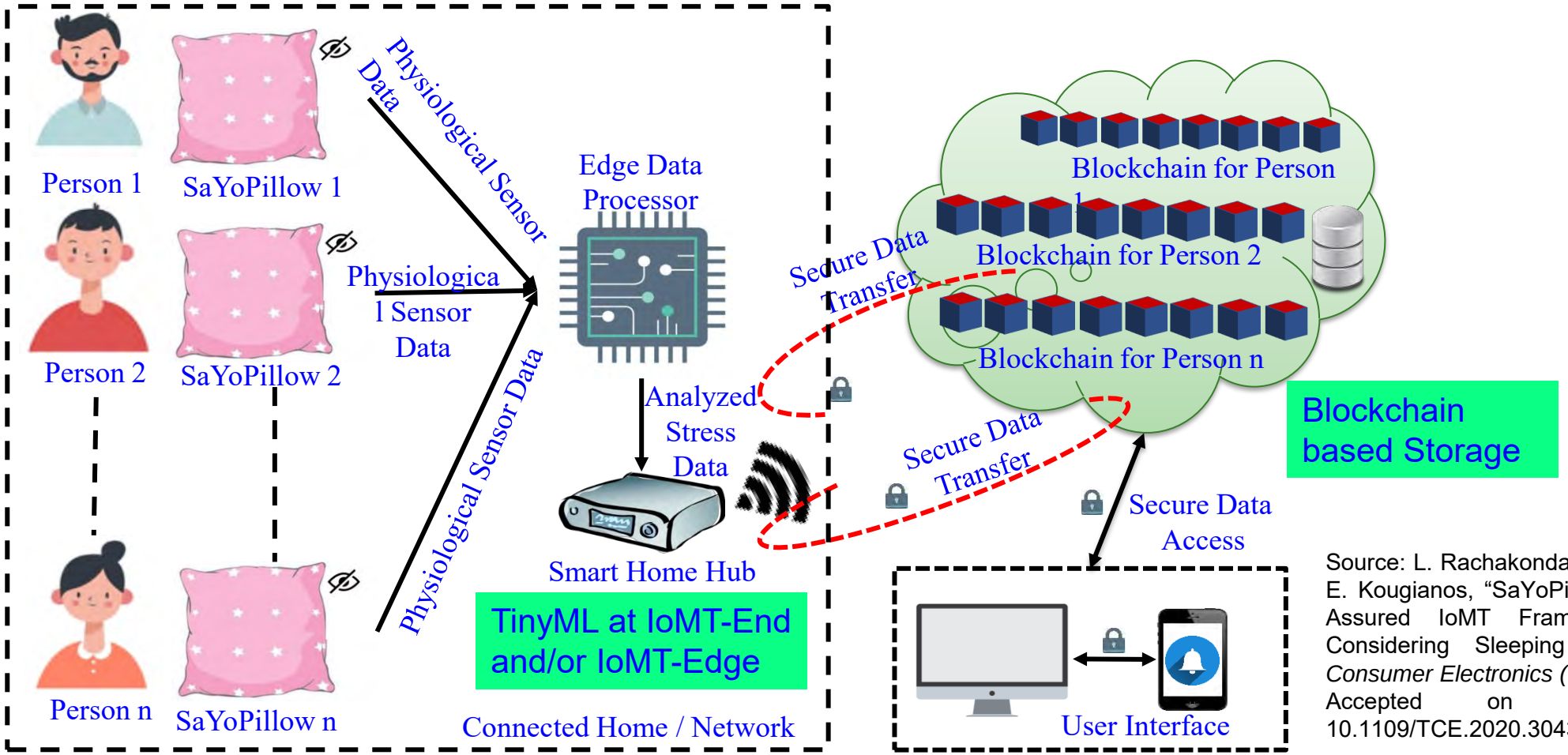
Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

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

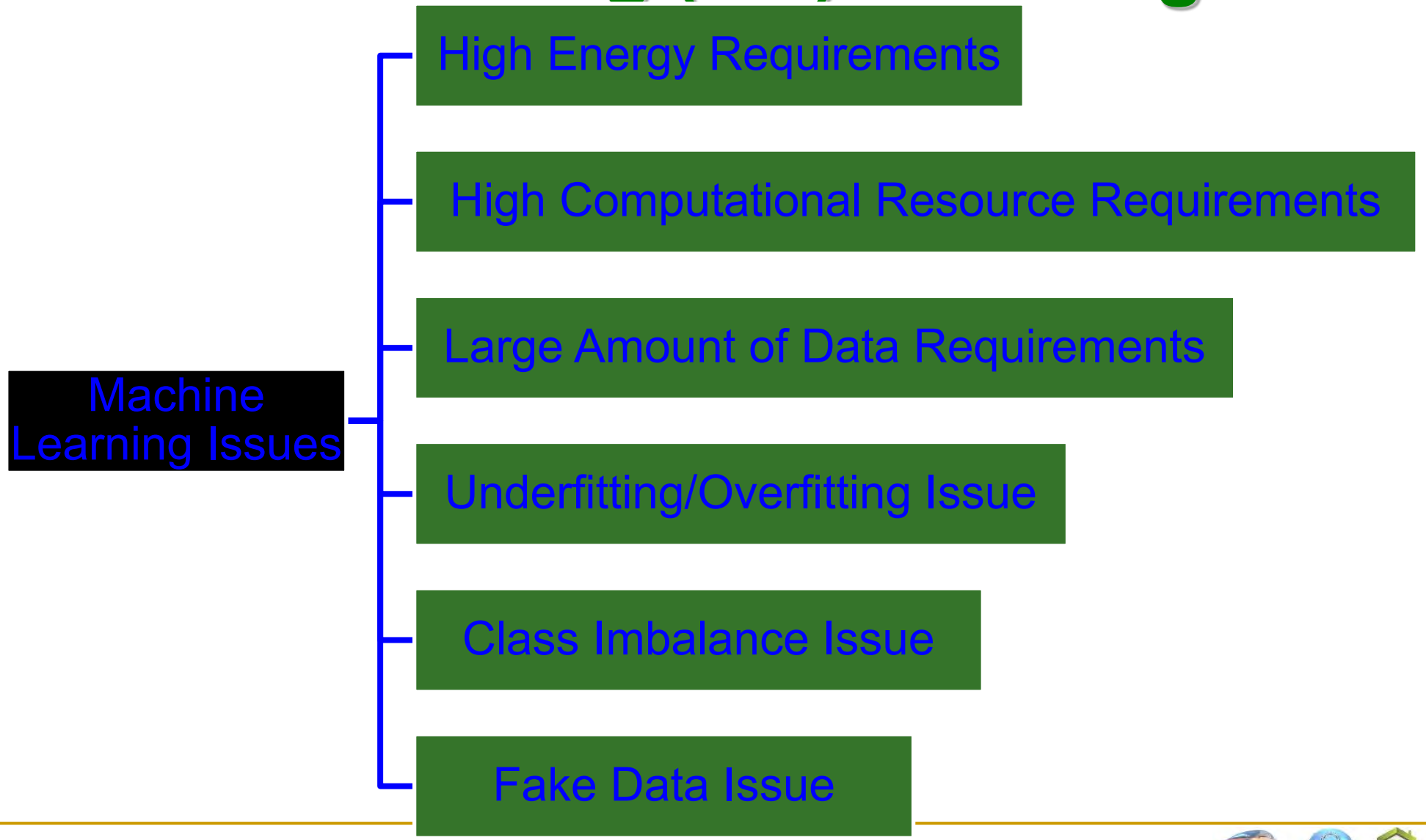
Our Smart-Yoga Pillow (SaYoPillow) with TinyML and Blockchain based Security



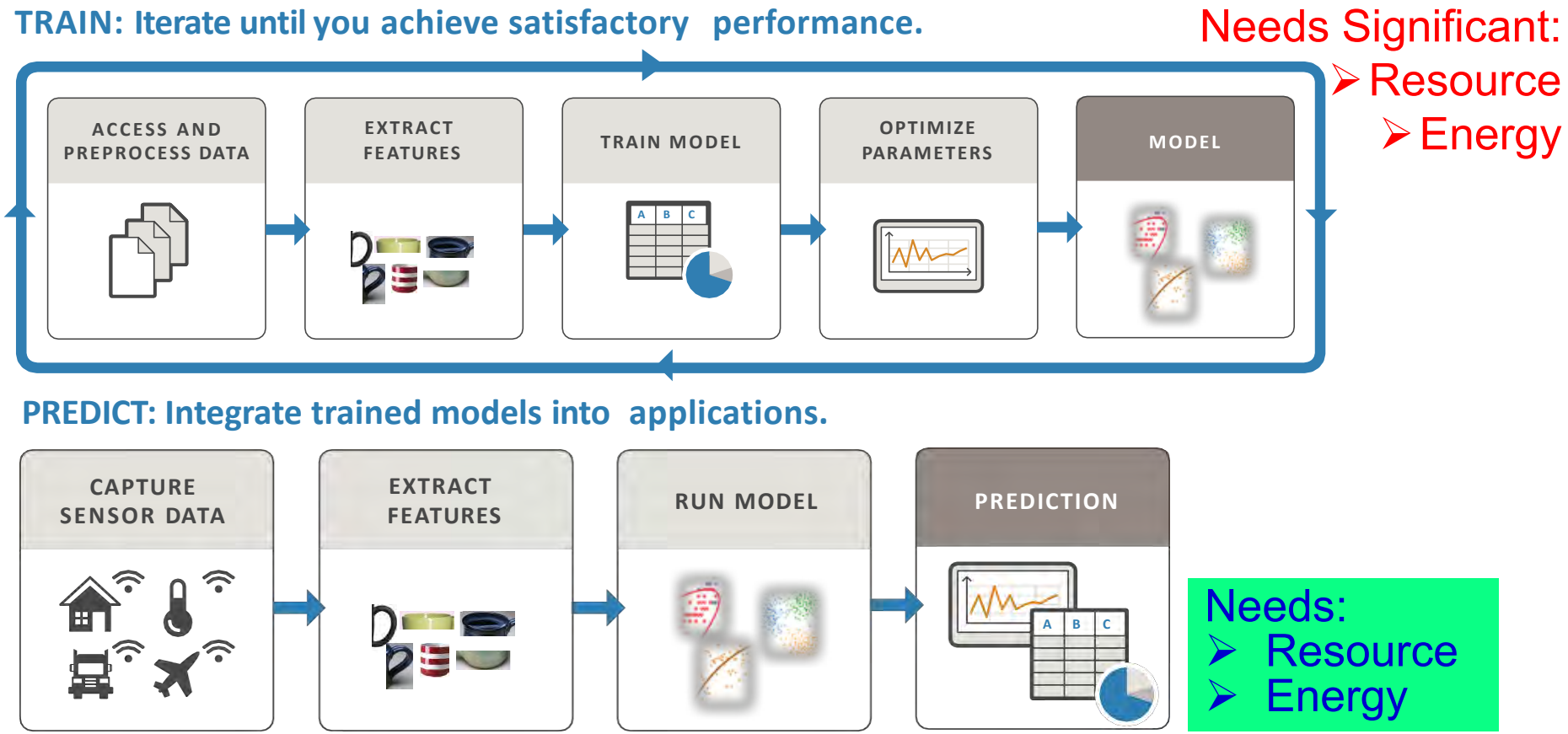
Source: L. Rachakonda, A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habit", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. XX, No. YY, ZZ 2021, pp. Accepted on 07 Dec 2020, DOI: 10.1109/TCE.2020.3043683.

Challenges in Making Smart

Machine Learning (ML) Modeling Issues



Deep Neural Network (DNN) - Resource and Energy Costs

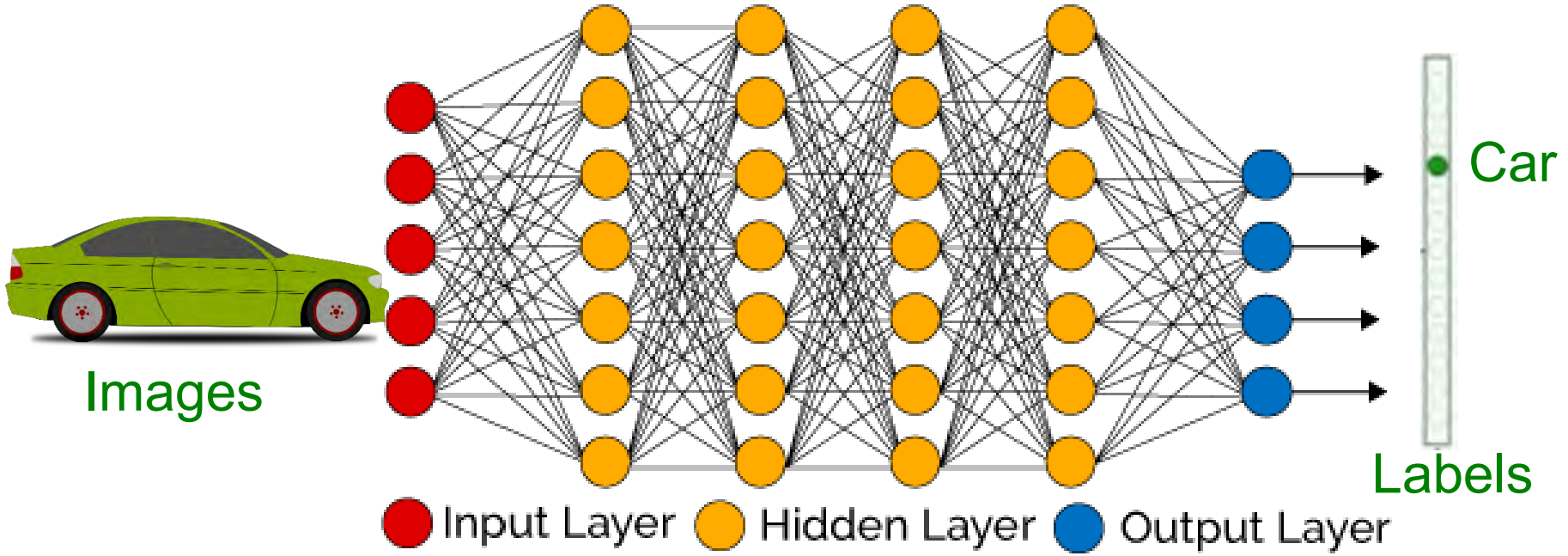


Needs Significant:
- Resource
- Energy

Needs:
- Resource
- Energy

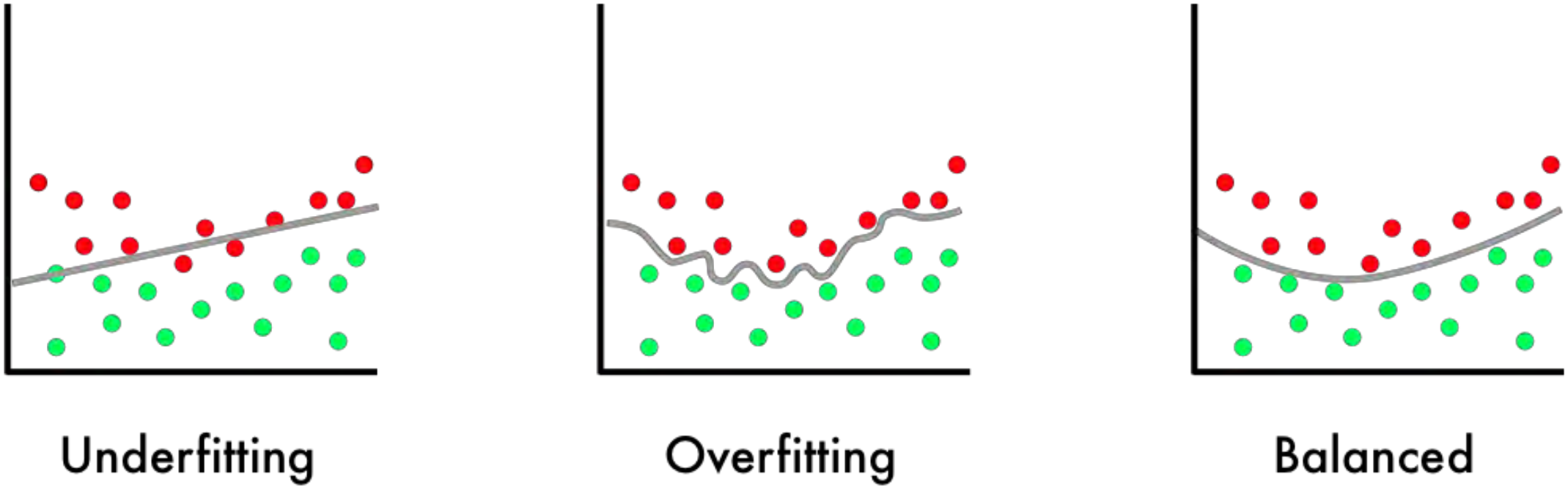
Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

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.

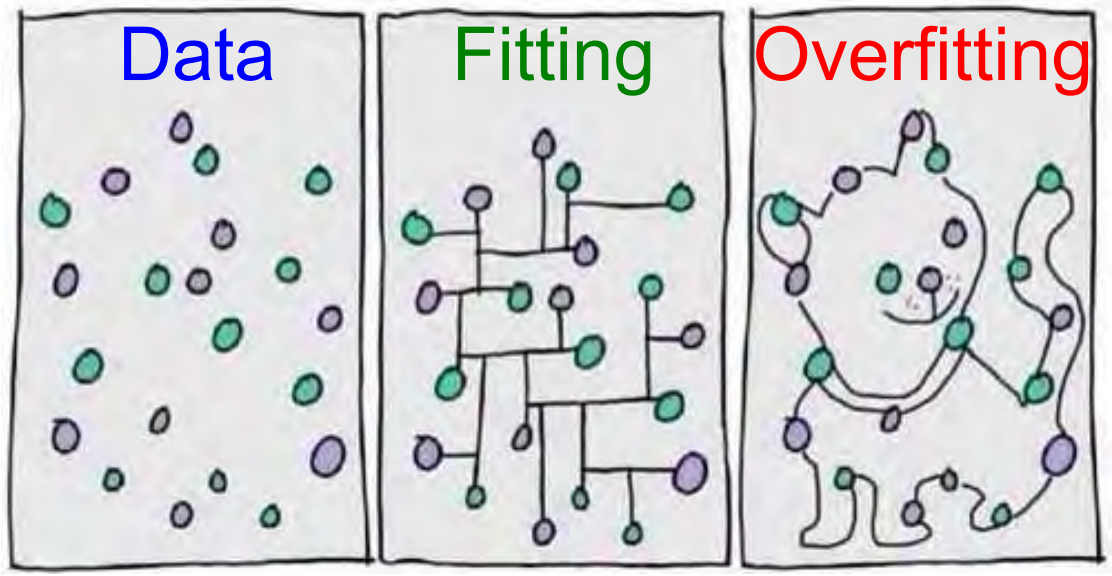
DNN: Underfitting and Overfitting Issues



Source: https://medium.freecodecamp.org/deep-learning-for-developers-tools-you-can-use-to-code-neural-networks-on-day-1-34c4435ae6b

DNN - Overfitting or Inflation Issue

- DNN is overfitted or inflated - If the accuracy of DNN model is better than the training dataset
- DNN architecture may be more complex than it is required for a specific problem.
- Solutions: Different datasets, reduce complexity



Source: www.algotrading101.com

DNN - Class Imbalance Issue

- Class imbalance is a classification problems where the classes are not represented equally.
- Solutions: Use Precision, Recall, F-measure metrics

  Not only RMSE like accuracy metrics

DNN - Class Imbalance Issue

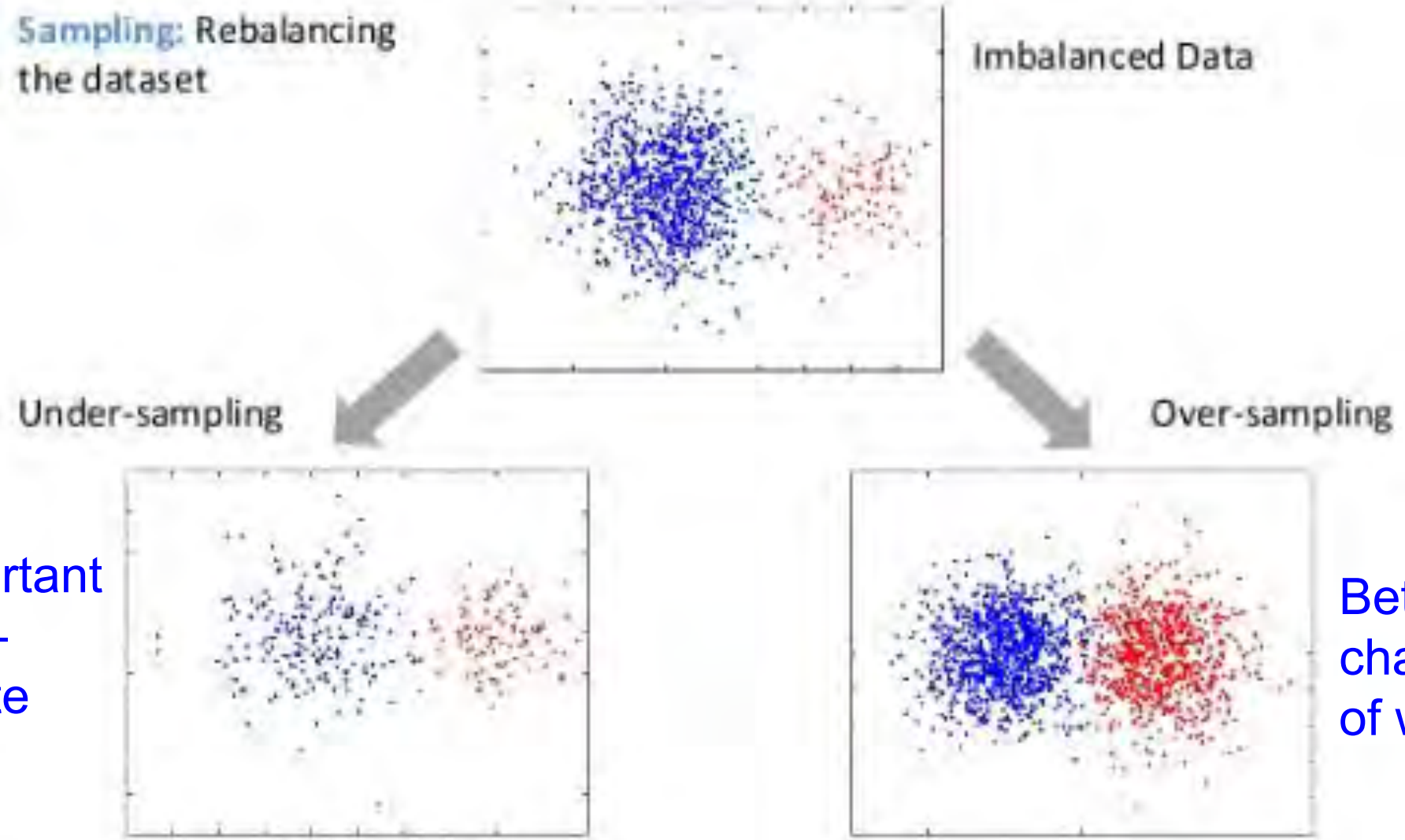
Well-known examples of imbalanced data sets:

- Fraud detection: where number of fraud cases could be much smaller than non-fraudulent transactions.
- Prediction of disputed / delayed invoices: where the problem is to predict default / disputed invoices.
- Predictive maintenance data sets.

Model won't be useful.
The cost of mis-classifying minority class could very high.

Source: https://www.datasciencecentral.com/profiles/blogs/handling-imbalanced-data-sets-in-supervised-learning-using-family

DNN - Class Imbalance Issue



Loss of important information – Less accurate

Better chances of working

Source: https://www.datasciencecentral.com/profiles/blogs/handling-imbalanced-data-sets-in-supervised-learning-using-family

DNN - Class Imbalance Issue - Solutions

Methods to handle unbalanced data sets

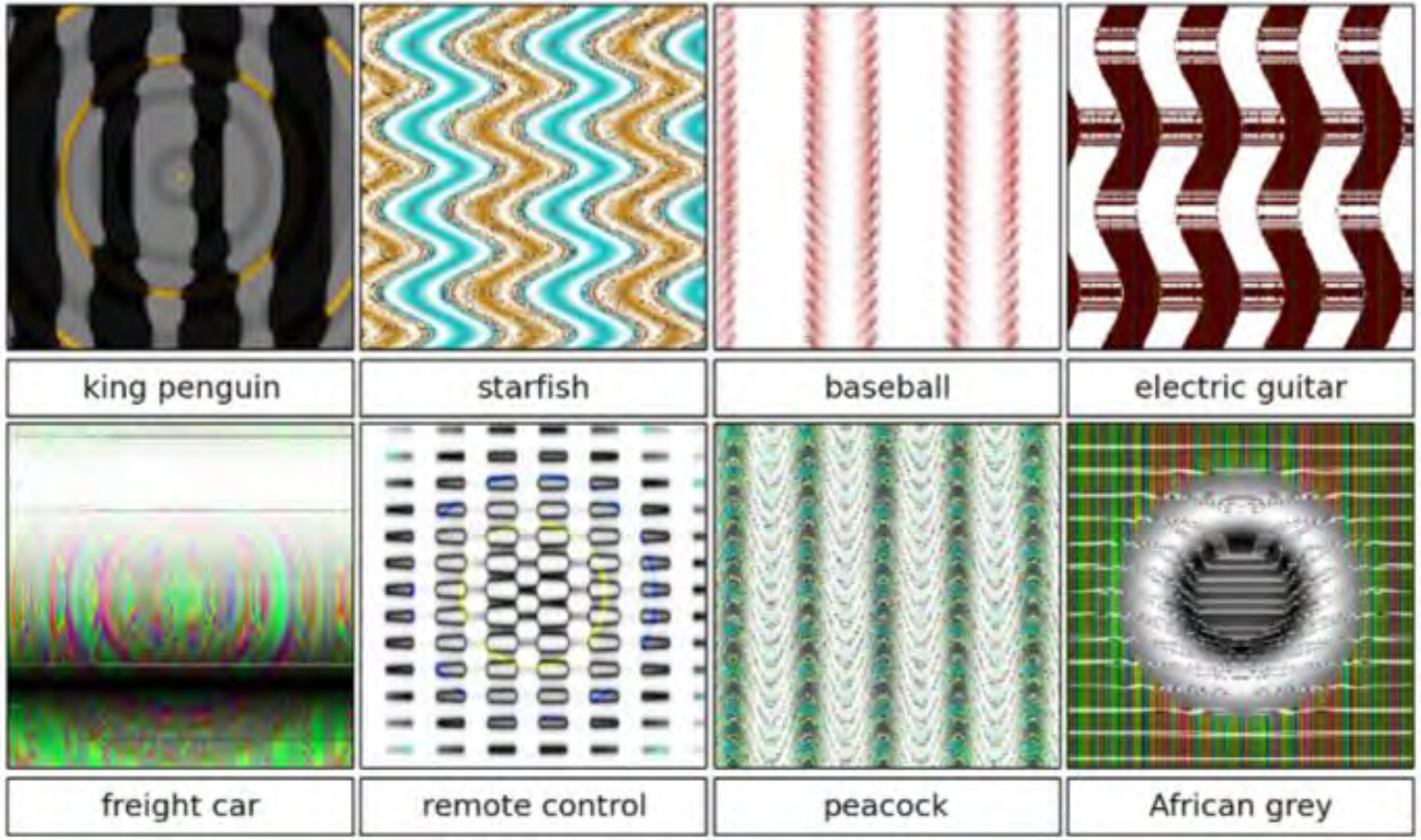
- Exploring different ML algorithms
- Collecting more data
- Modifying class weights
- Penalizing the models
- Using anomaly detection techniques
- Using oversampling techniques
- Using undersampling techniques

Source: https://www.datasciencecentral.com/profiles/blogs/handling-imbalanced-data-sets-in-supervised-learning-using-family

Machine learning: "I'm as intelligent as human beings".
Also machine learning:

DNNs are not Always Smart

DNNs are not Always Smart

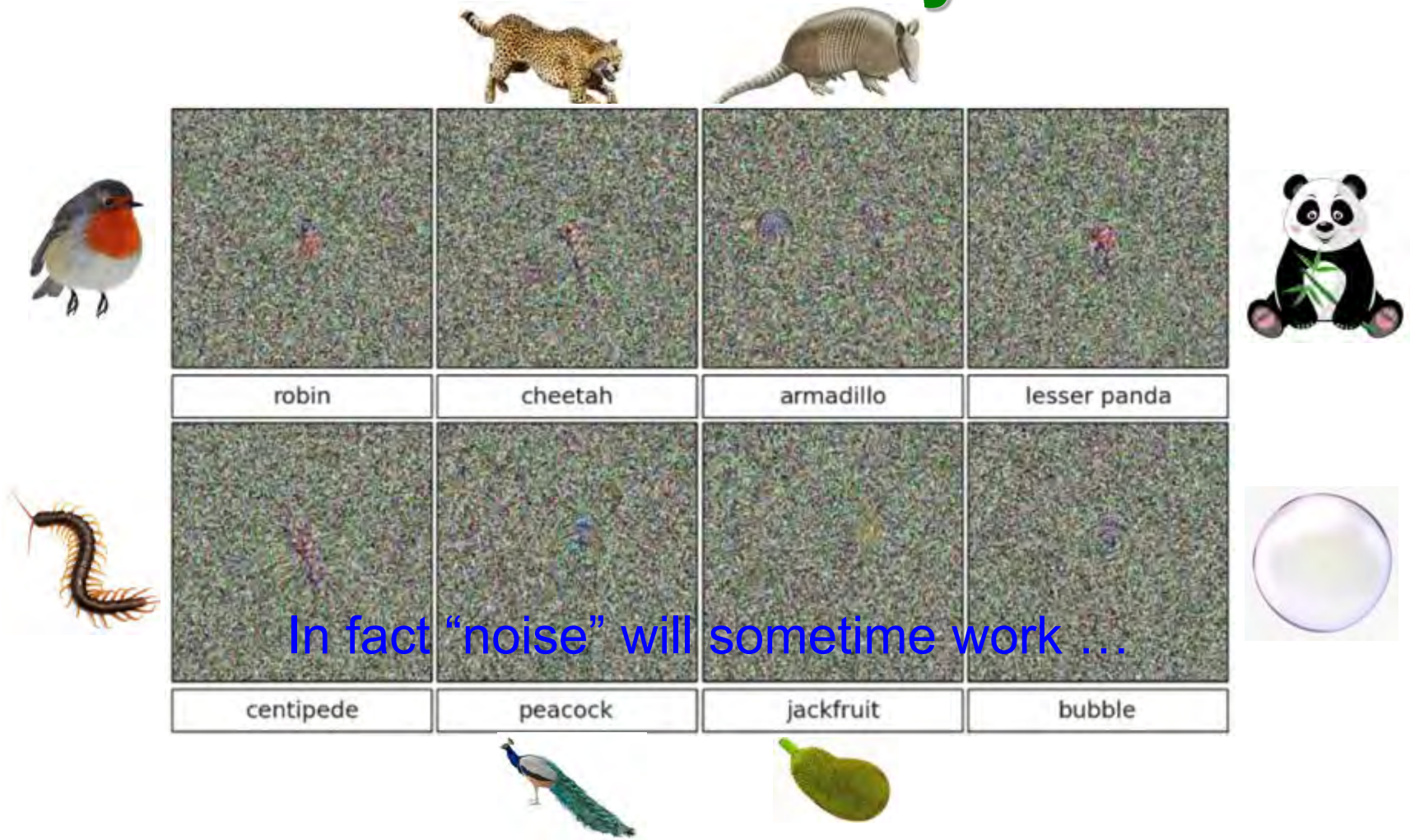


DNNs can be fooled by certain “learned” (Adversarial) patterns …

Source: Nguyen, et al. 2014 - Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

Source: Corcoran Keynote 2018

DNNs are not Always Smart

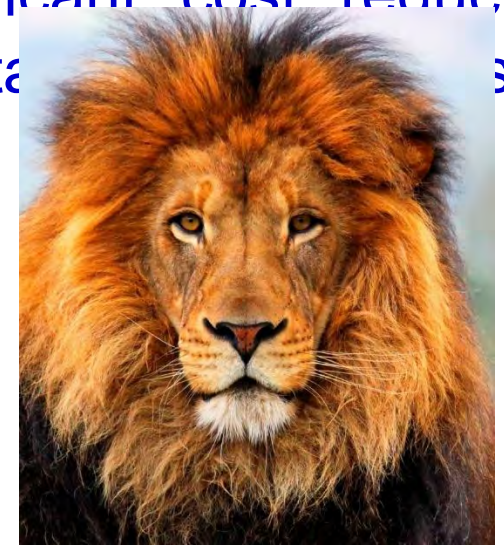


Source: Nguyen, et al. 2014 - Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

Source: Corcoran Keynote 2018

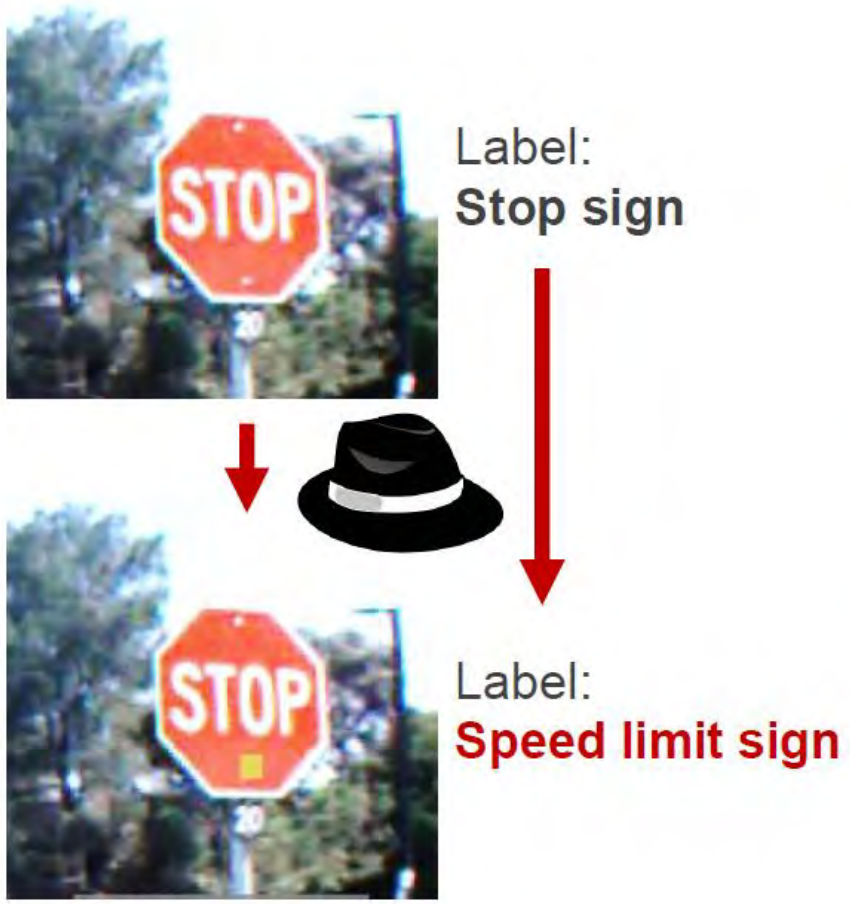
DNNs are not Always Smart

- 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 annota sets



Source: Corcoran Keynote 2018

AI Security - Trojans in Artificial Intelligence (TrojAI)



Adversaries can insert **Trojans** into AIs, leaving a trigger for bad behavior that they can activate during the AI's operations

Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

Conclusion

Smart and Intelligence – Dictionary Meaning

Smart:

1 (of a person) clean, tidy, and well dressed.

'you look very smart'

2.1 (of a device) programmed so as to be capable of some independent action.

'hi-tech smart weapons'

Intelligence:

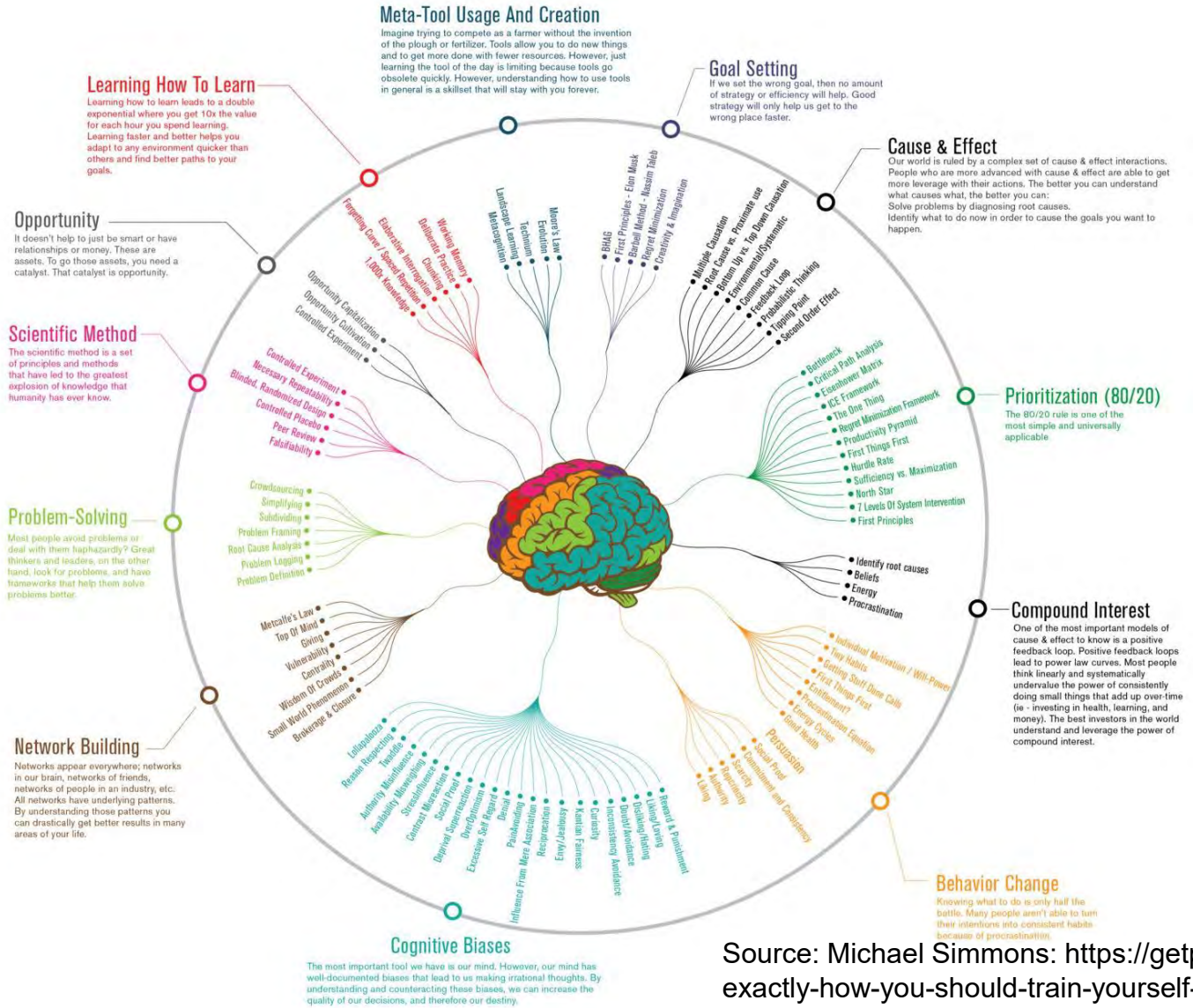
The ability to acquire and apply knowledge and skills.

Source: https://en.oxforddictionaries.com

Smartness

- Ability to take decisions based on the data, circumstances, situations?
- Analytics + Responses

How to Train Yourself To Be Smarter



Source: Michael Simmons: https://getpocket.com/explore/item/this-is-exactly-how-you-should-train-yourself-to-be-smarter

Conclusion

- “Smart” terms is used to present a variety of characteristics of CE.
- Energy smart is important for battery and energy costs point of view.
- Security smart is important for connected CE.
- Response smart is making decisions based on ML data analytics.
- ML has its own cost in terms of training and execution.
- ESR-smart is the trade-offs of energy, security, and response in the design of CE.

Future Directions

- Security, Privacy, IP Protection of Information and System need more research.
- Security of the CE systems (e.g. smart healthcare device, UAV, Smart Cars) needs research.
- Important aspect of smart CE design: trade-offs among energy, response latency, and security.
- Edge computing involving data curation, learning, and security at the edge is an important research direction.

Key References

- S. Saeedi, A. C. M. Fong, S. P. Mohanty, A. K. Gupta, and S. Carr, "Consumer Artificial Intelligence Mishaps and Mitigation Strategies", IEEE Consumer Electronics Magazine, Vol. 11, No. 3, May 2022, pp. 13--24, DOI: https://doi.org/10.1109/MCE.2021.3075329.
- D. Puthal, and S. P. Mohanty, "Cybersecurity Issues in AI", IEEE Consumer Electronics Magazine, Vol. 10, No. 4, July 2021, pp. 33--35.
- 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.