Smart Electronic Systems – Facts Vs Fictions

IIIT Naya Raipur

24 July 2019

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu

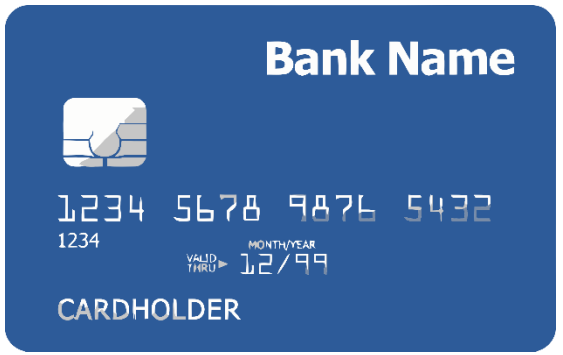
More Info: http://www.smohanty.org

Talk - Outline

- What are smart possibilities?
- Challenges in the current generation CE design
- Energy Smart CE
- Security Smart CE
- Response Smart CE
- Design Trade-offs in CE
- Conclusions and Future Directions

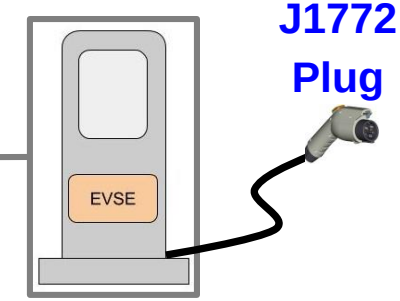
What is Common Among These?

Does Smart Mean Electronic?

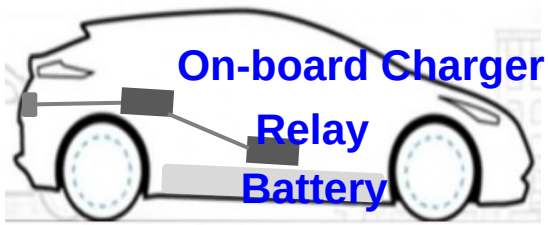


Does Smart Mean Electric?

Grid



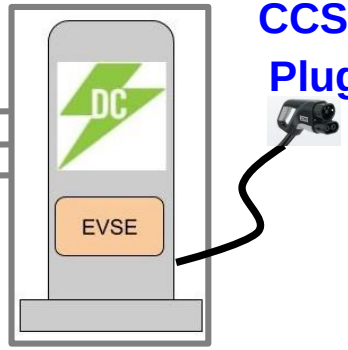
J1772 Plug



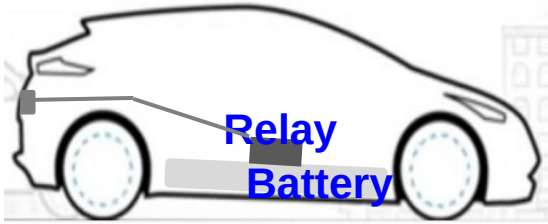
AC charging station

- Monitoring function
- Communication and safety

3 phase AC supply



CCS1 Plug



DC charging station

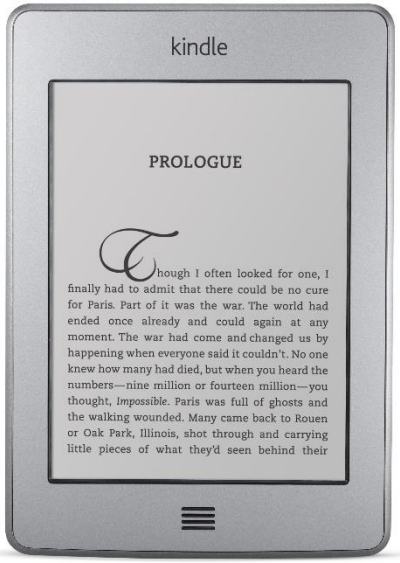
- AC-DC Off board conversion
- Monitoring Power flow
- EV to grid communication
- Safety monitoring

Electric Vehicle Supply Equipment (EVSE)

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

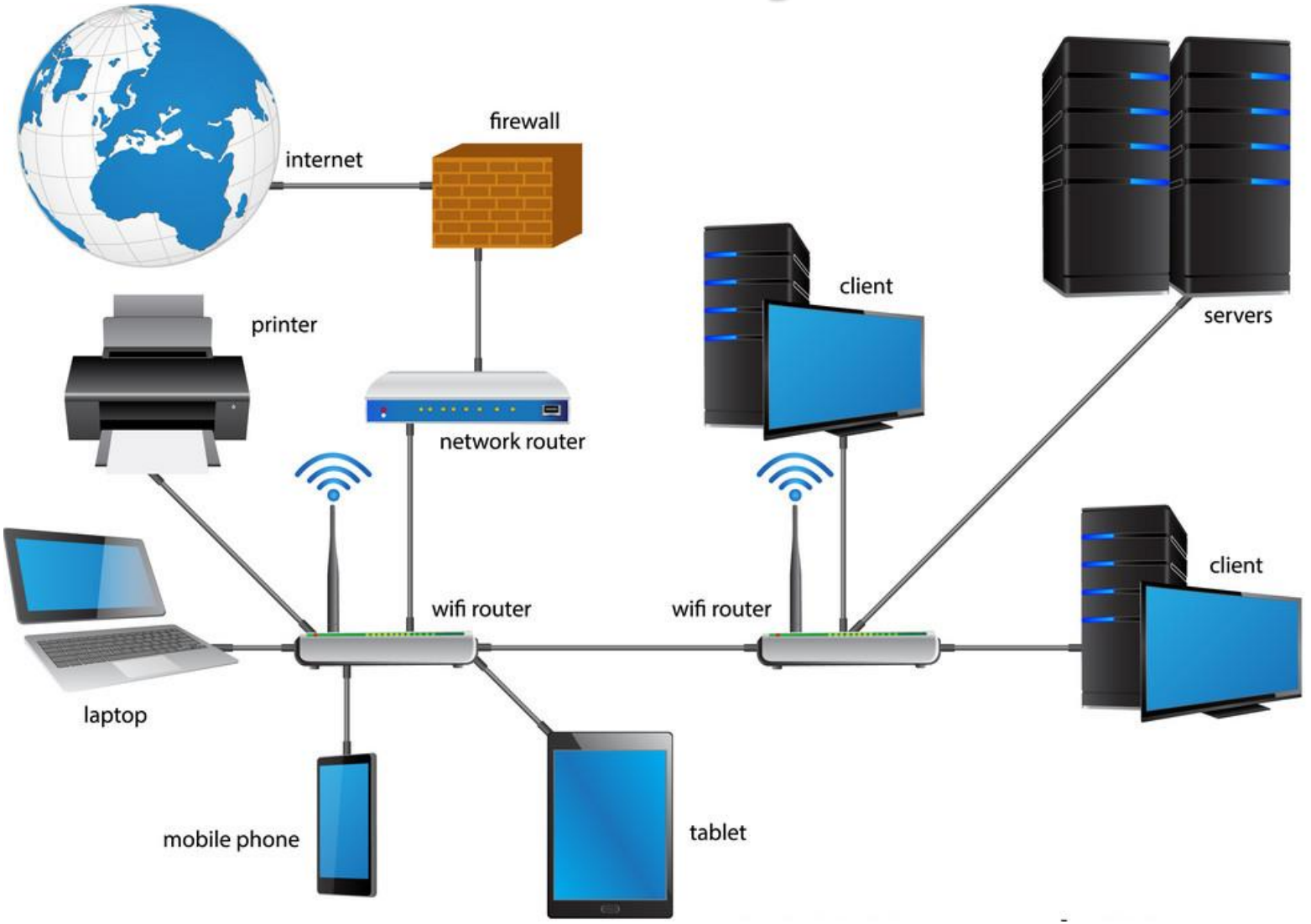
Does Smart Mean Small?

Does Smart Mean Portable?



Does Smart Mean Battery-Operated?

Does Smart Mean Cyber-Enabled?

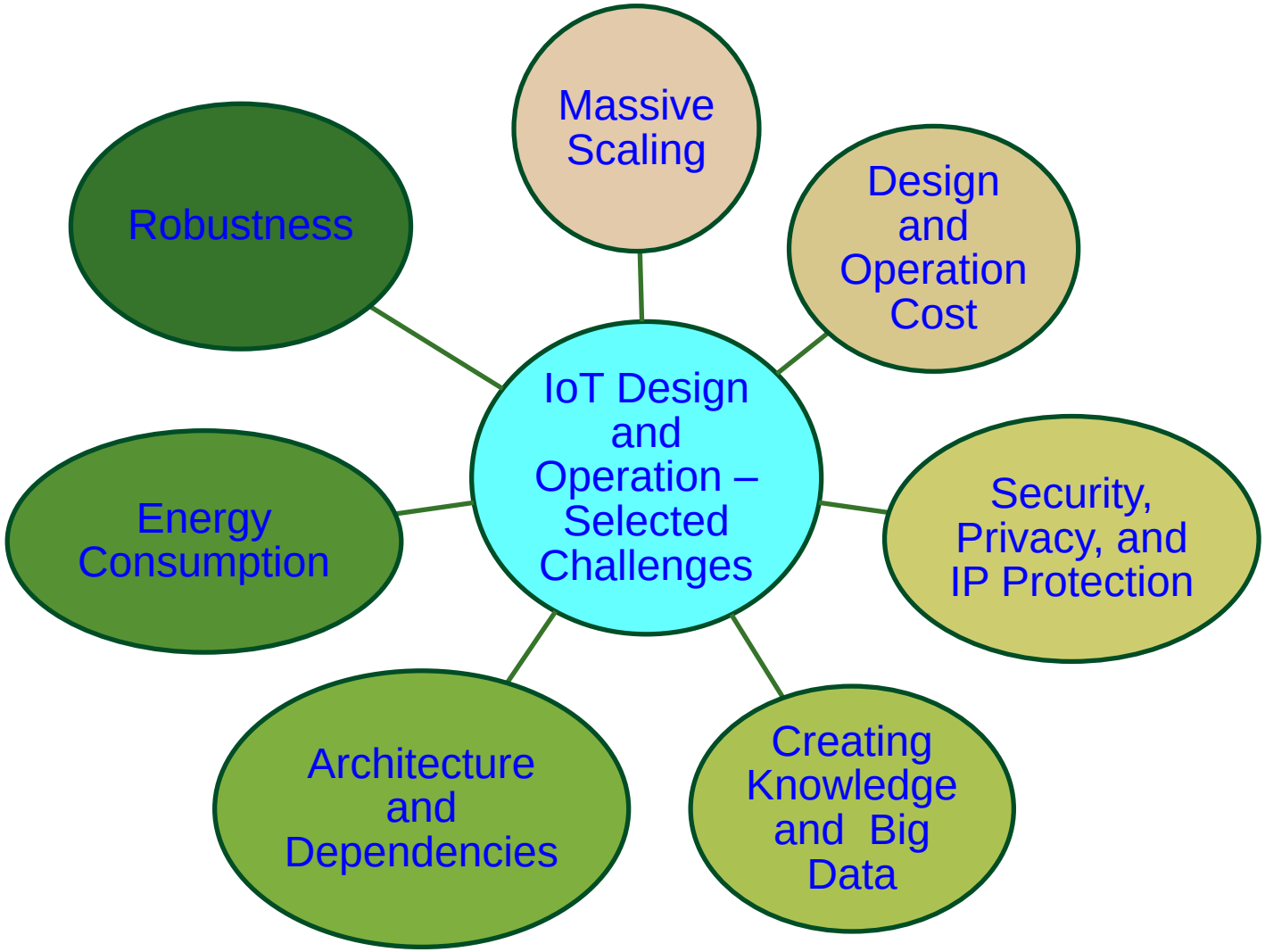


Does Smart Mean Autonomous?

Does Smart Mean AI or ML?

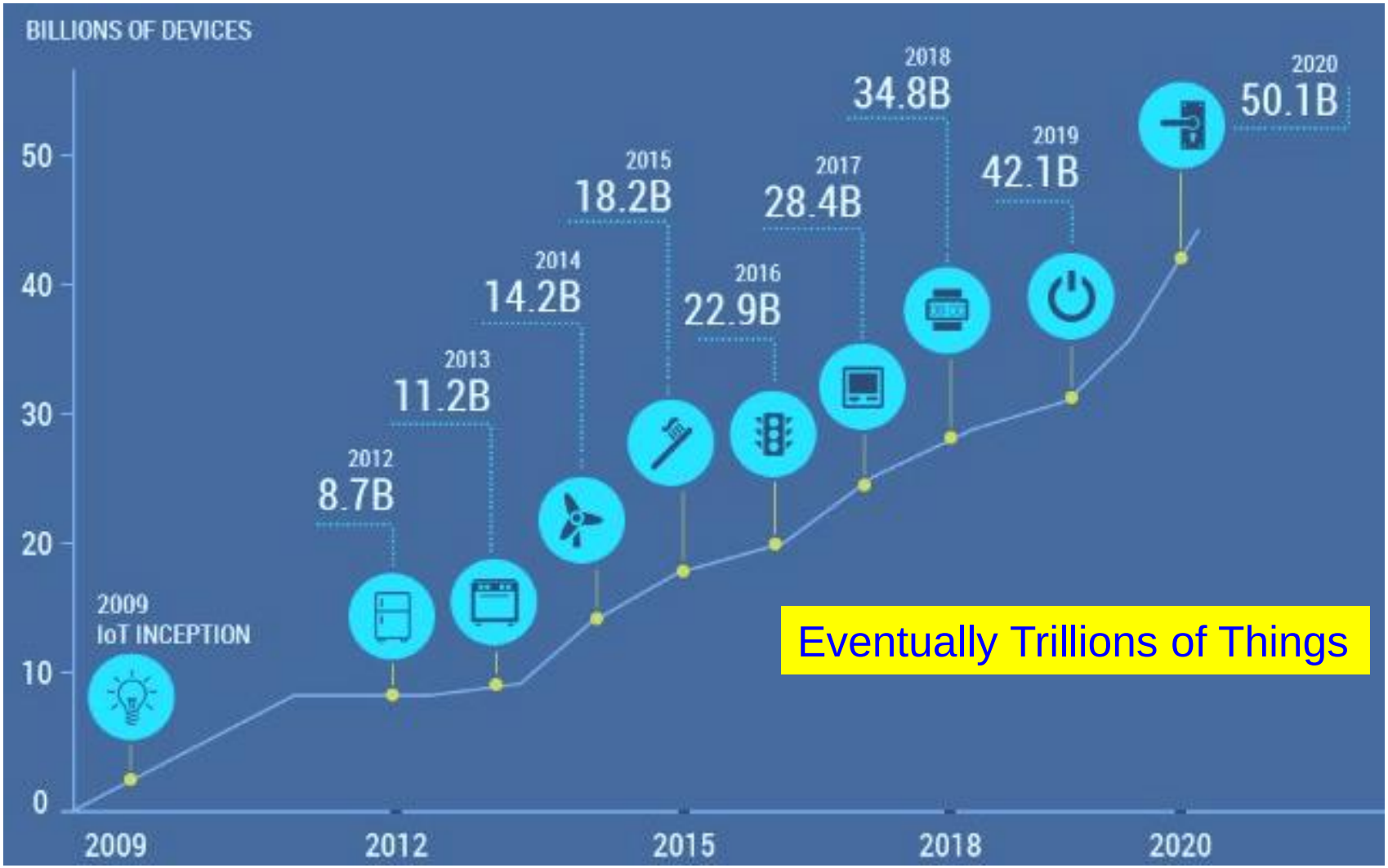
Challenges in Current Generation CE Design

IoT – 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

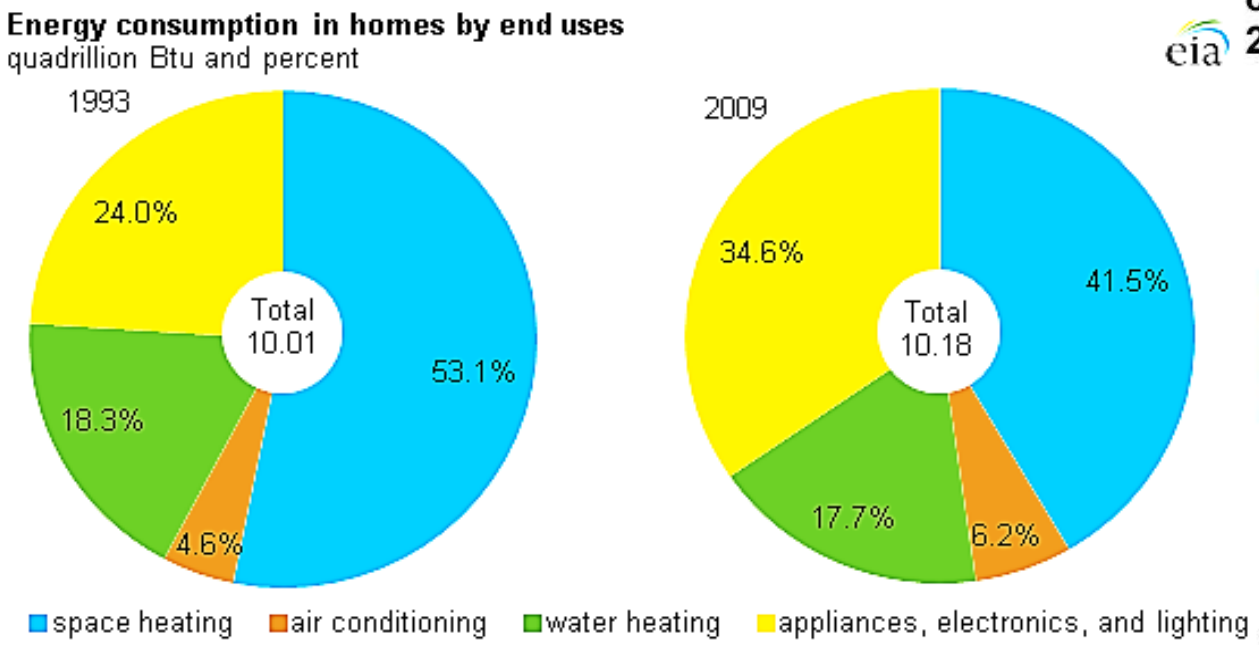
- The design cost is a one-time cost.
- Design cost needs to be small to make a smart city realization possible.

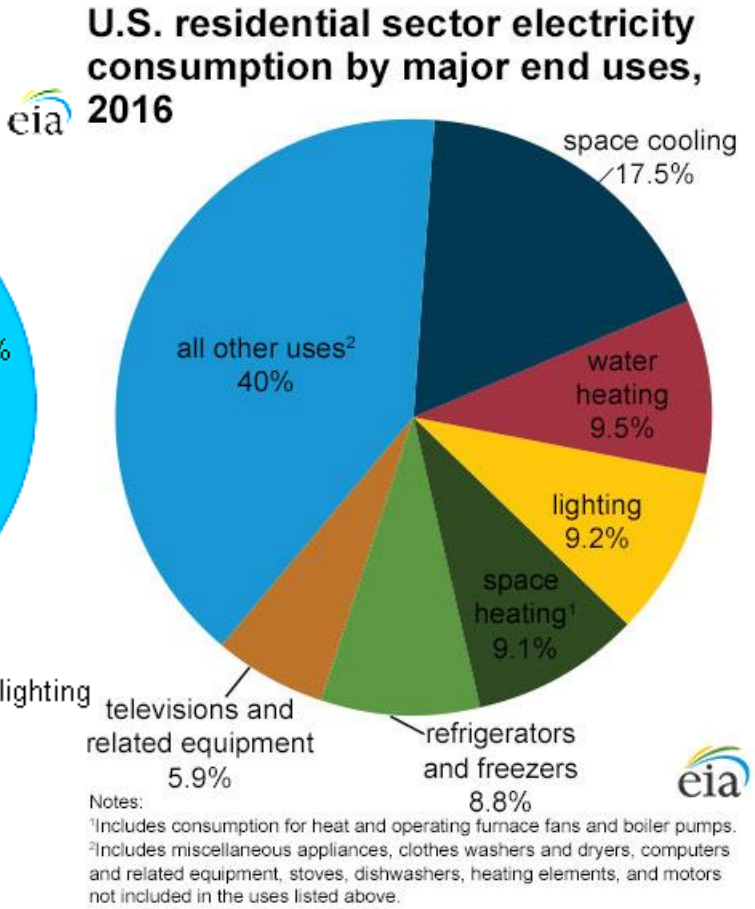
Source: http://www.industrialisation-produits-electroniques.fr

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



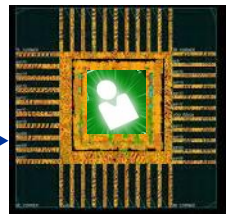


Quadrillion BTU (or quad): 1 quad = 10^{15} BTU = 1.055 Exa Joule (EJ).

Source: U.S. Energy Information Administration

Security, Privacy, and IP-Rights

Hardware Trojan

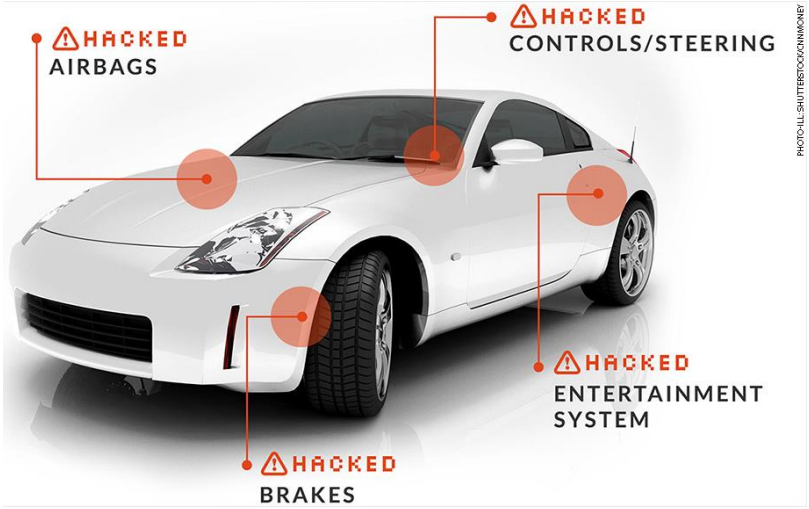


Source: Mohanty ICIT 2017 Keynote

Security - System …

Power Grid Attack

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

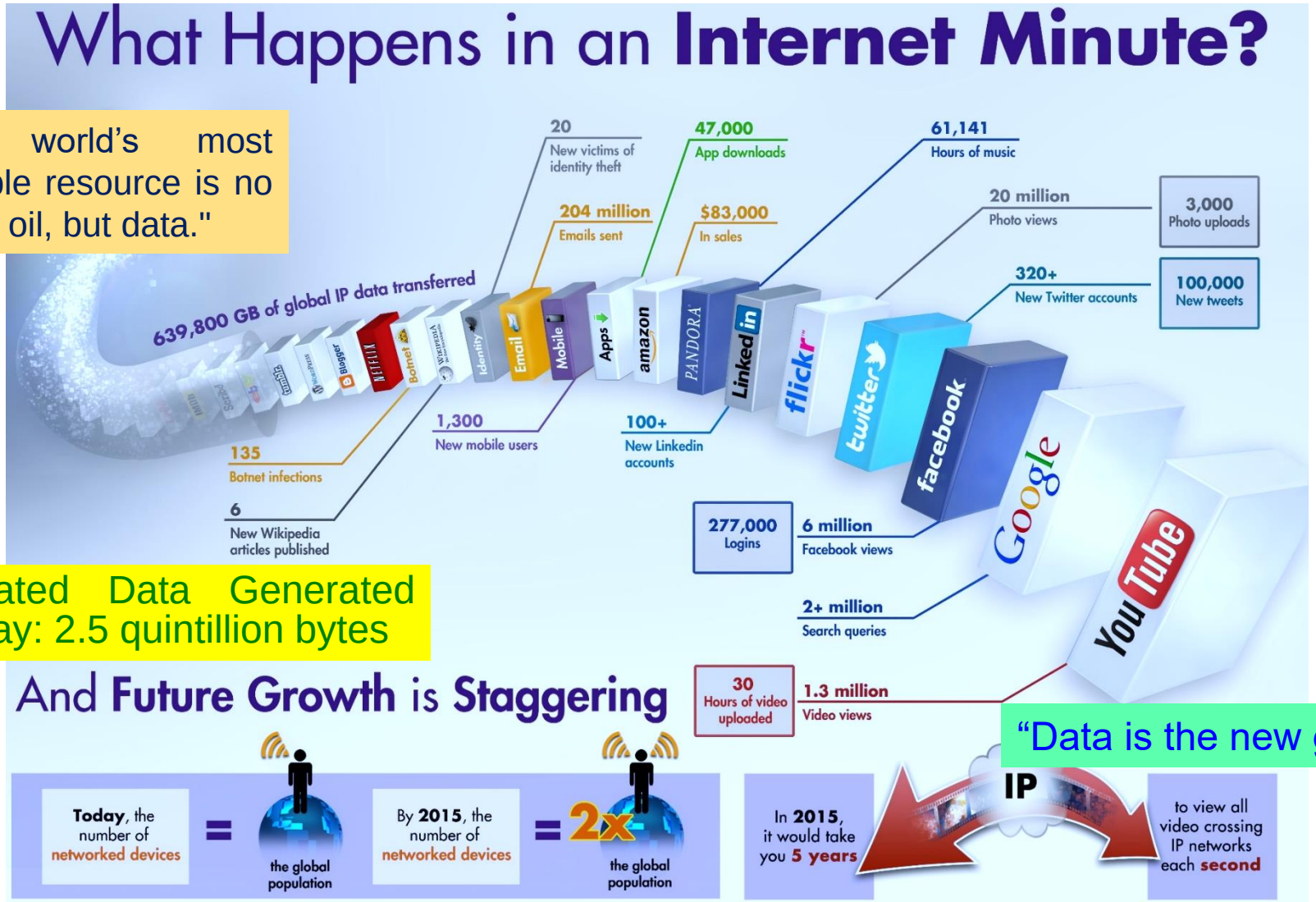


Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

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

Huge Amount of Data

"The world's most valuable resource is no longer oil, but data."



Estimated Data Generated per Day: 2.5 quintillion bytes

"Data is the new gold."

ESR-Smart in Smart City Components

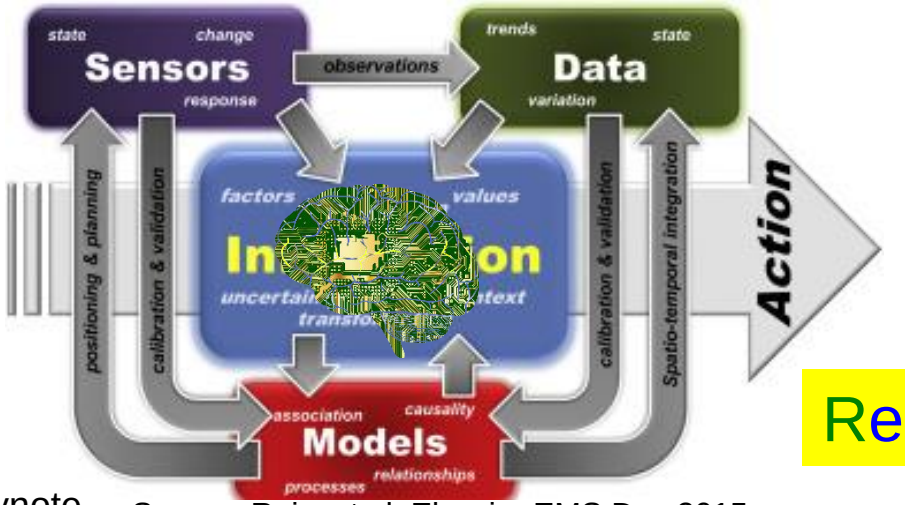
Energy Smart

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

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

Security of systems and data.

Security Smart



Source: Mohanty iSES 2018 Keynote

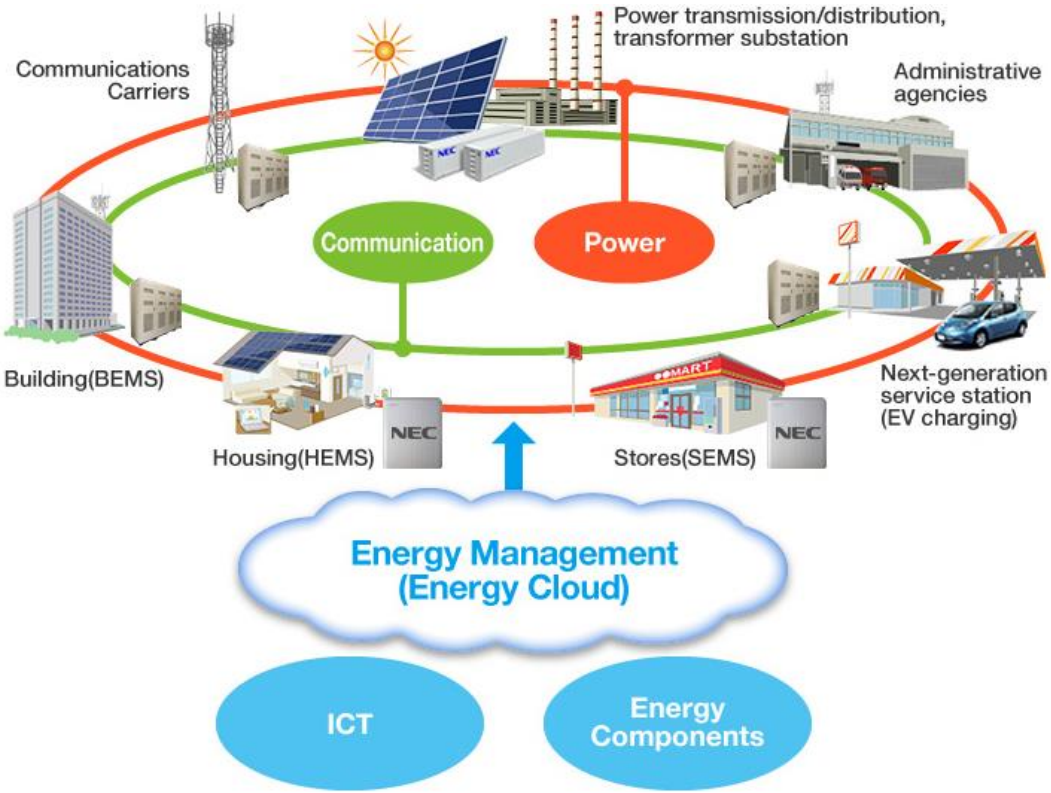
Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

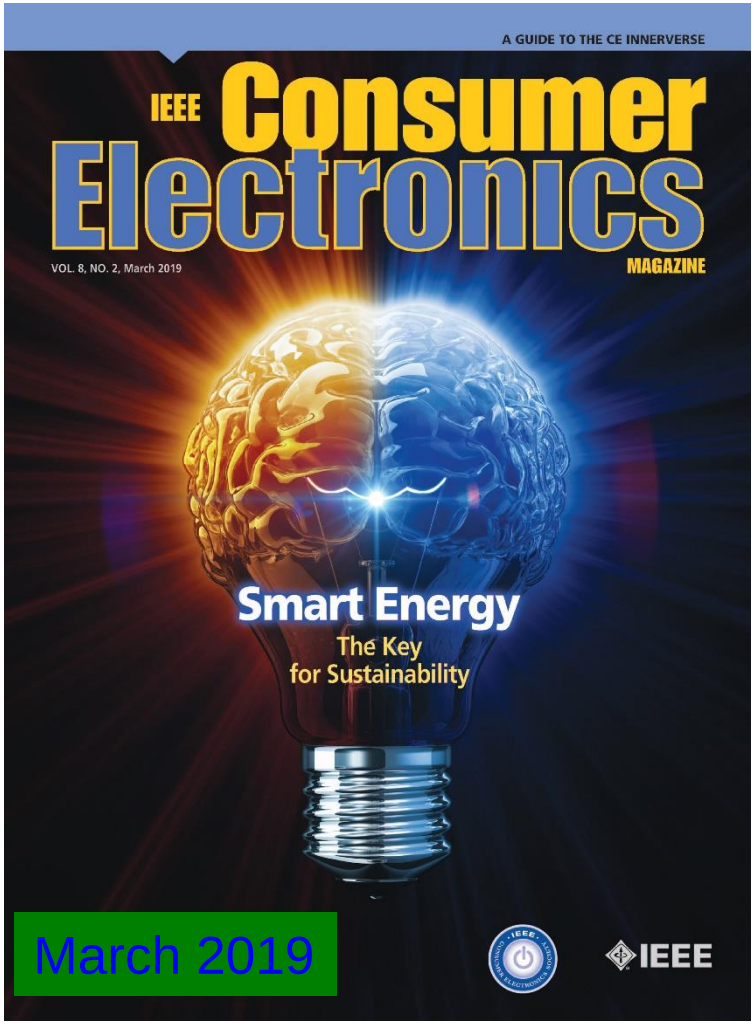
Response Smart

Energy Smart

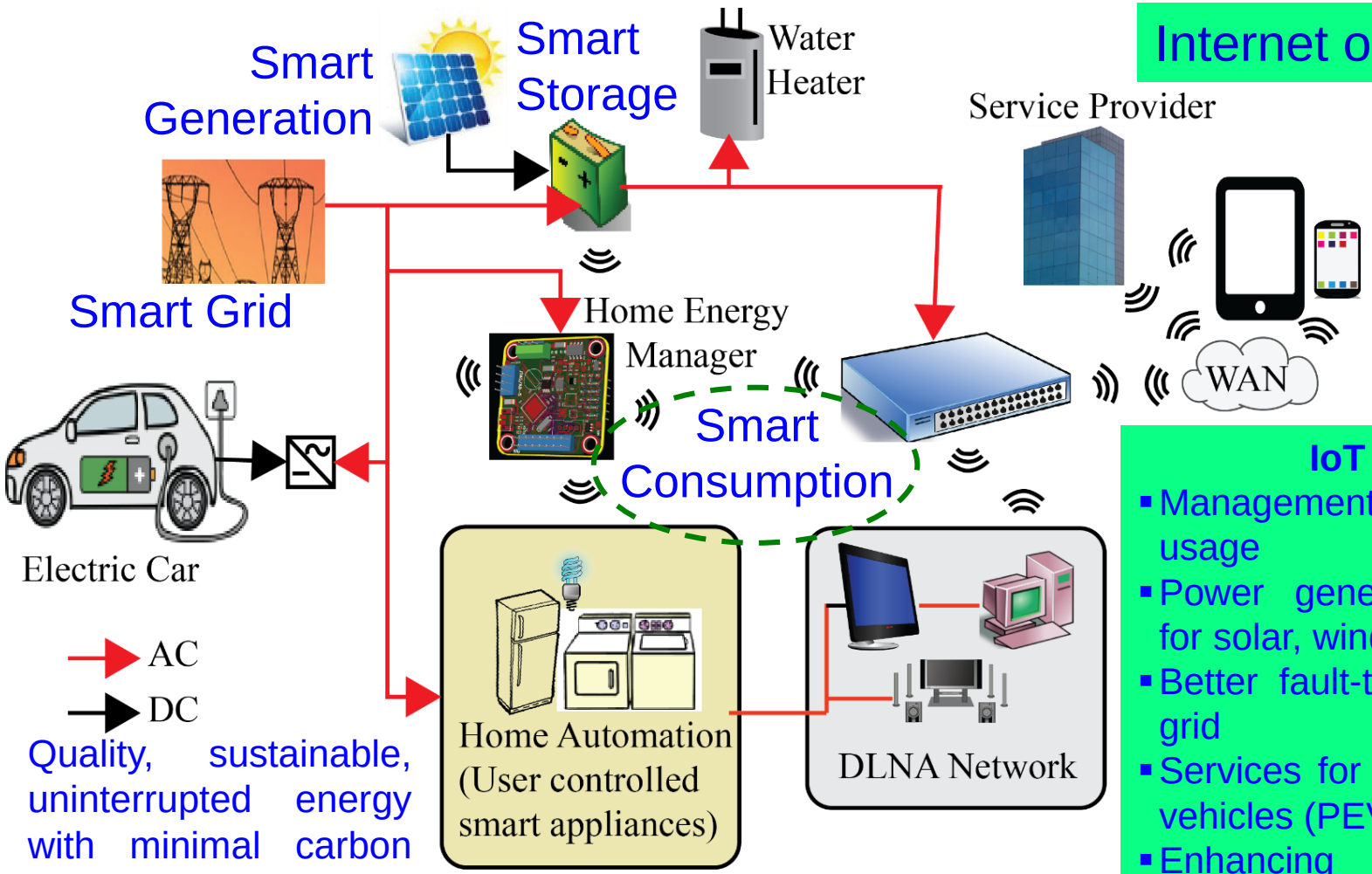
Smart Energy



Source: https://www.nec.com/en/global/solutions/energy/index.html



Smart Energy



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

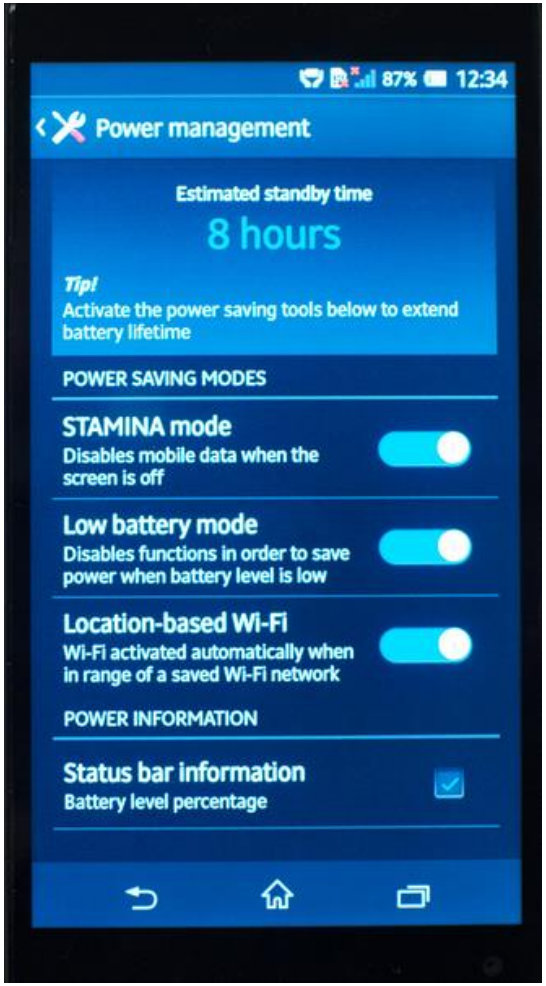
Source: Mohanty 2016, CE Magazine July 2016

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

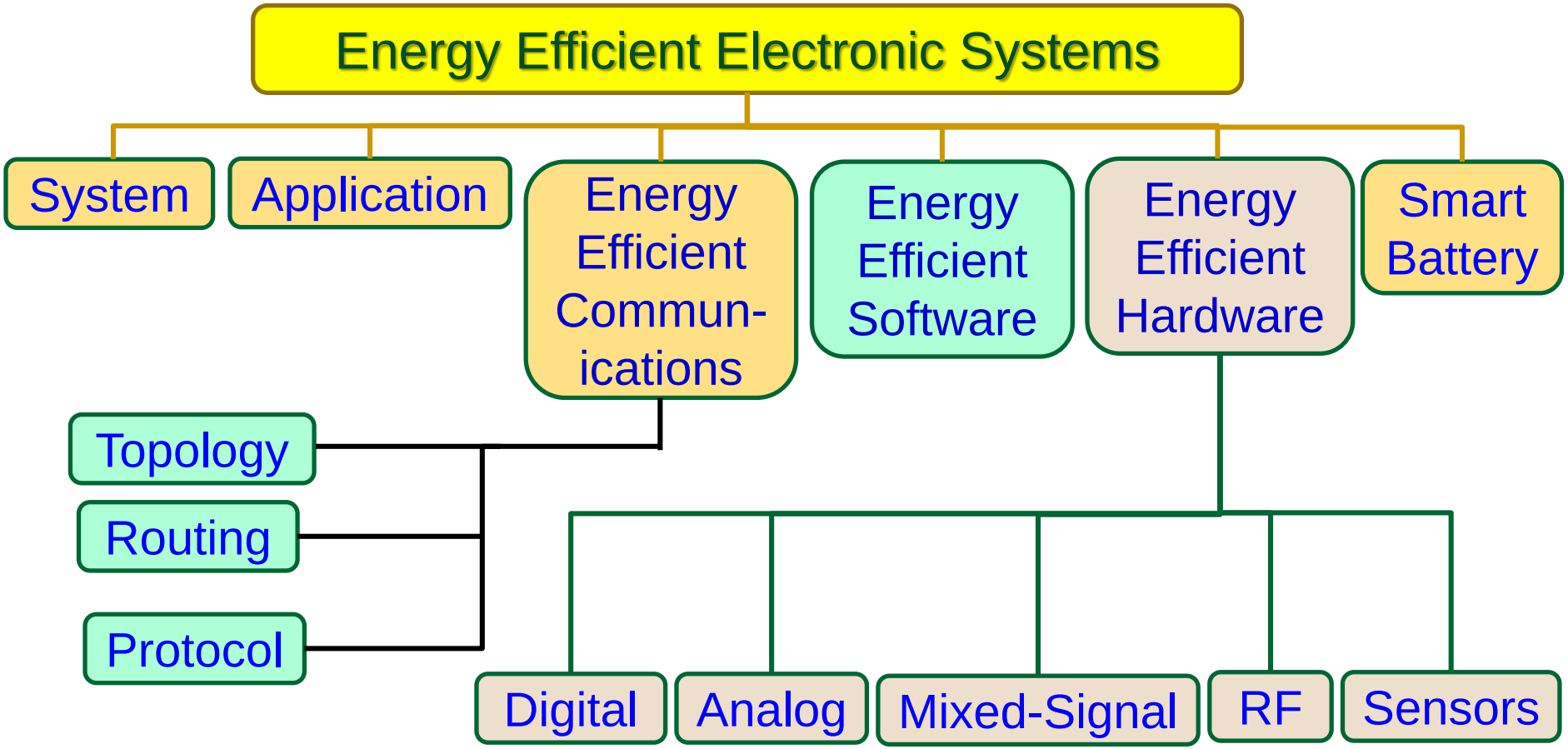
Smart Energy – Smart Consumption



Battery Saver

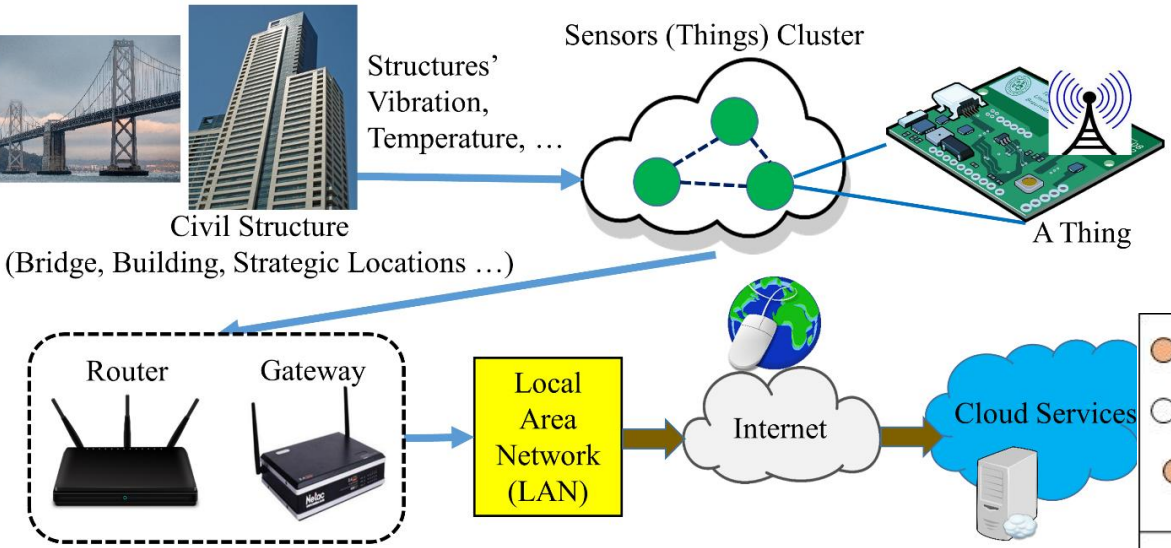
Smart Home

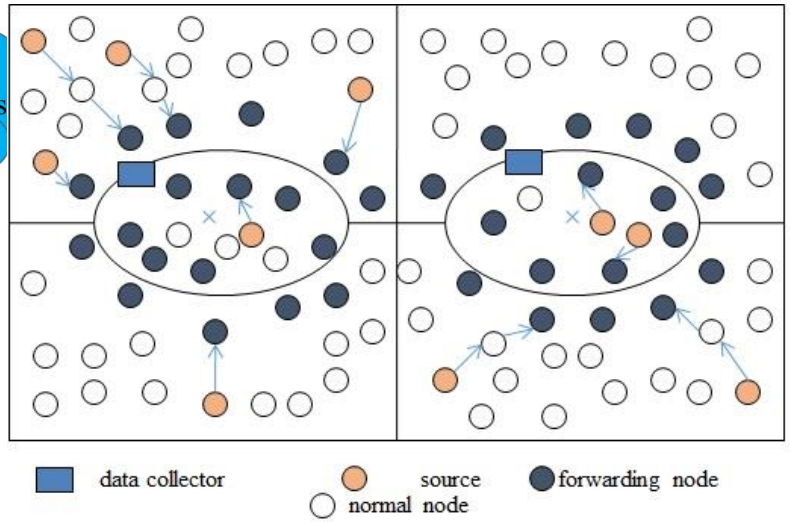
Energy Efficient Electronics: Possible Solution Fronts



Source: Mohanty ZINC 2018 Keynote

Sustainable IoT - Low-Power Sensors and Efficient Routing

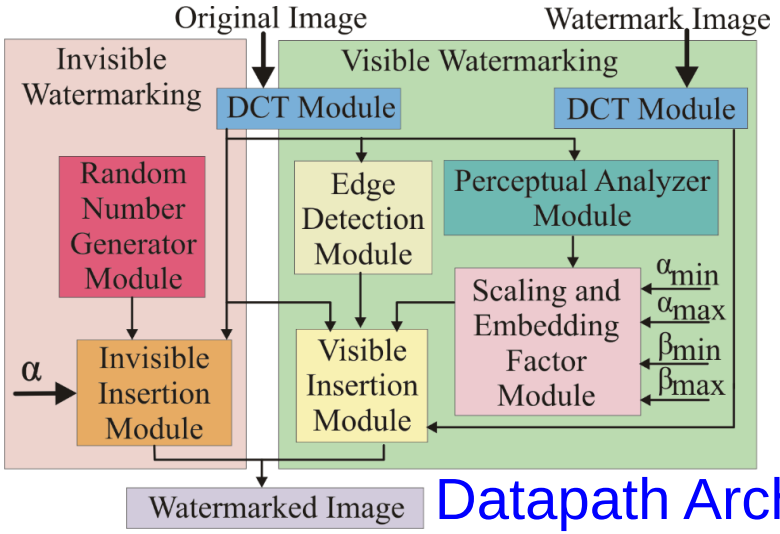




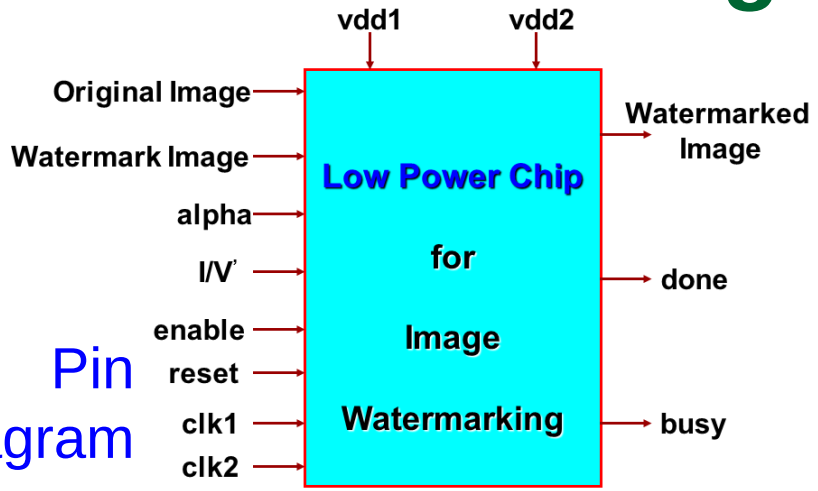
- IoT - sensors near the data collector drain energy faster than other nodes.
- Solution Idea - Mobile sink in which the network is balanced with node energy consumption.
- Solution Need: New data routing to forward data towards base station using mobile data collector, in which two data collectors follow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

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

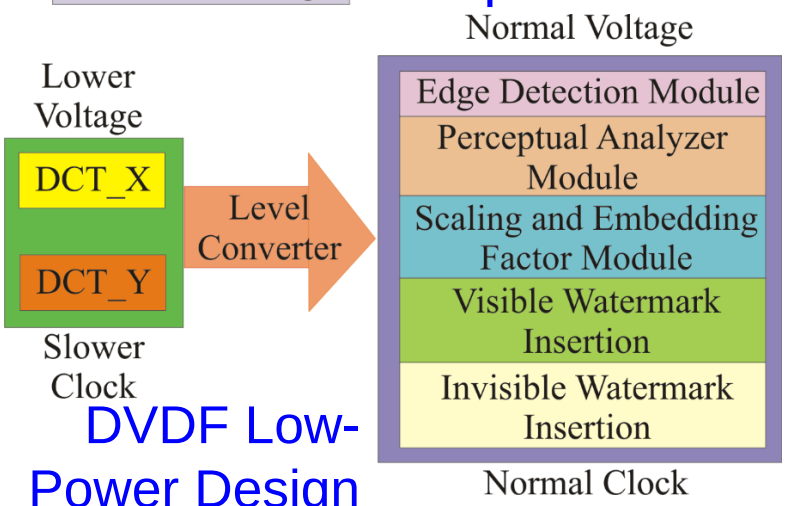
Energy-Efficient Hardware - Dual-Voltage



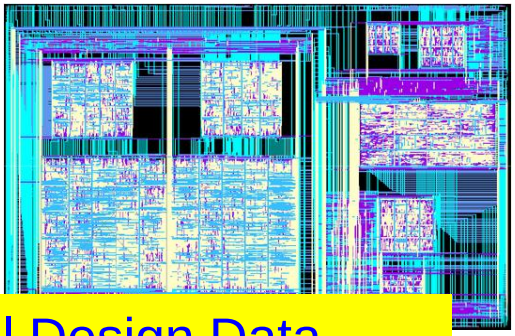
Datapath Architecture



Pin Diagram



DVDF Low-Power Design



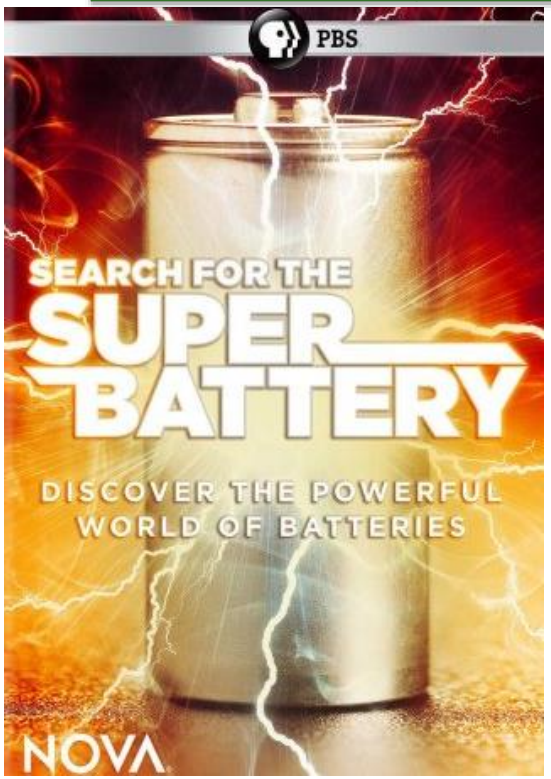
Hardware Layout

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

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

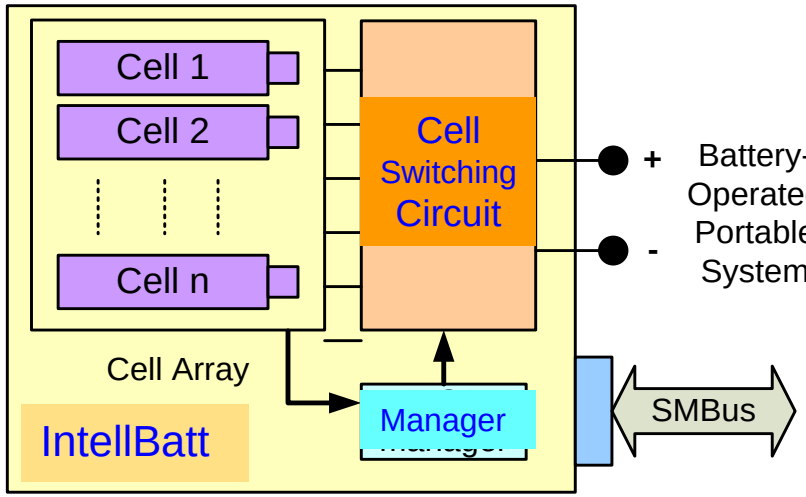
Energy Storage - High Capacity and Efficiency Needed

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



Source: Mohanty MAMI 2017 Keynote

Intelligent Battery

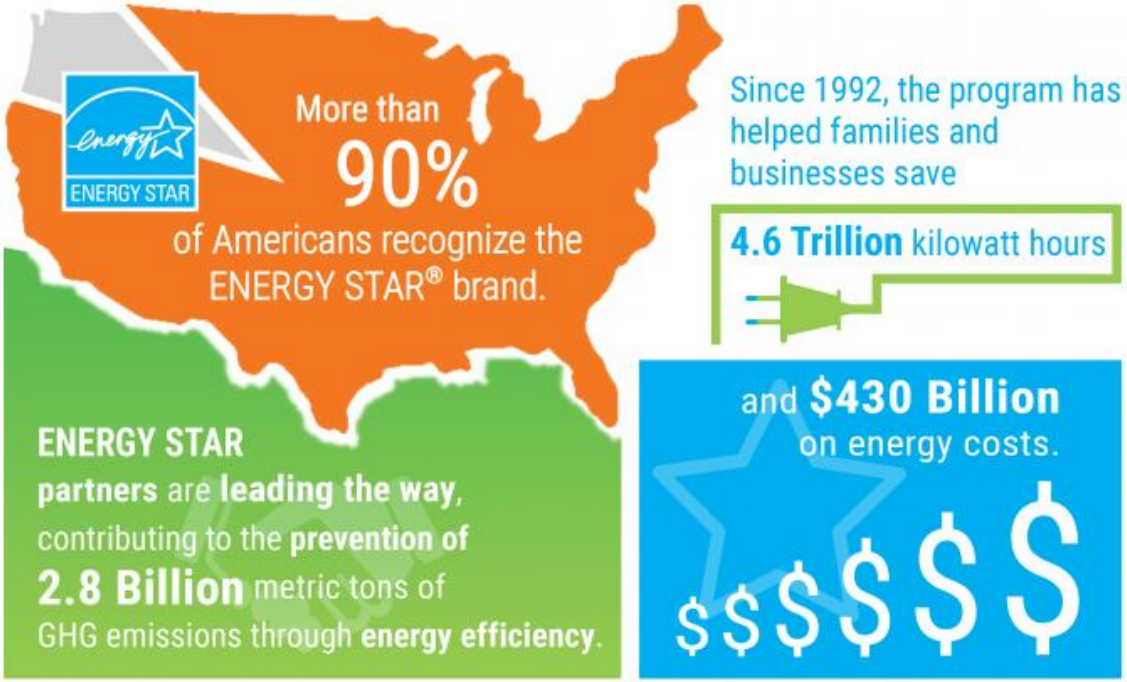


Mohanty 2010: IEEE Computer, March 2010
Mohanty 2018: ICCE 2018

Lithium Polymer Battery

Supercapacitor

Energy Star Ratings



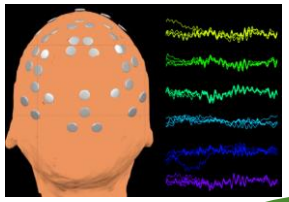
Source: https://www.energystar.gov/about/2017_energy_star_award_winners

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

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

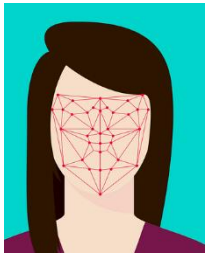
Security Smart

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

RFID Chip

Pace maker

Insulin Pump

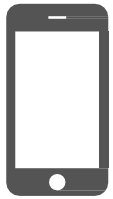
Heart Rate Monitor

Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices



Smart Phones/ Tablets

Wearable Devices

Smart Clothing

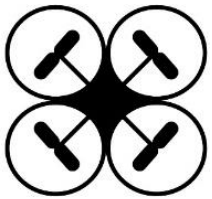
Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

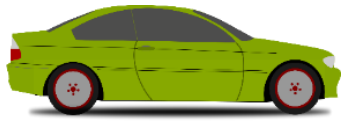
Entertainment Devices



Drones /UAVs

Video Games

Transportation Devices

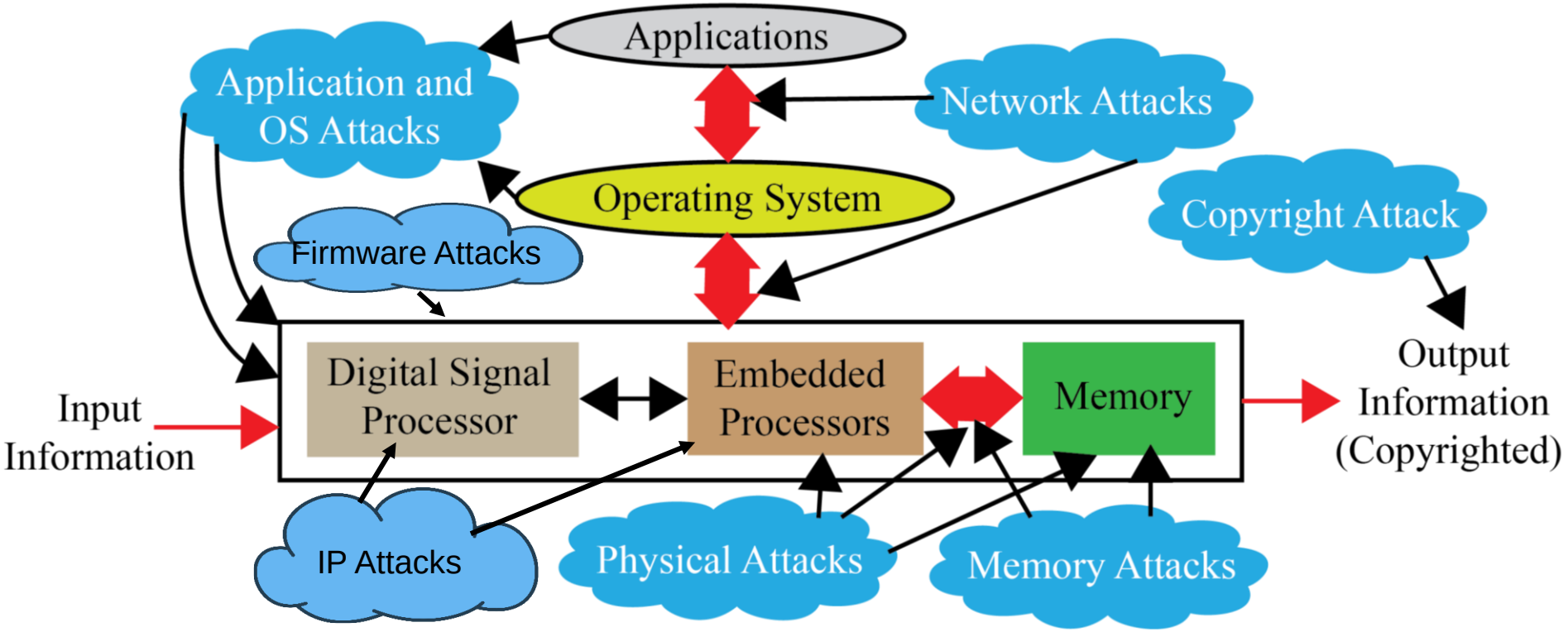


Smart Vehicles/ Autonomous Vehicles

Smart Traffic Controllers

Source: 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.

CE Security – Selected Solutions

Analysis of selected approaches to security and privacy issues in CE.

Category	Current Approaches	Advantages	Disadvantages
Confidentiality	Symmetric key cryptography	Low computation overhead	Key distribution problem
	Asymmetric key cryptography	Good for key distribution	High computation overhead
Integrity	Message authentication codes	Verification of message contents	Additional computation overhead
Availability	Signature-based authentication	Avoids unnecessary signature computations	Requires additional infrastructure and rekeying scheme
Authentication	Physically unclonable functions (PUFs)	High speed	Additional implementation challenges
	Message authentication codes	Verification of sender	Computation overhead
Nonrepudiation	Digital signatures	Link message to sender	Difficult in pseudonymous systems
Identity privacy	Pseudonym	Disguise true identity	Vulnerable to pattern analysis
	Attribute-based credentials	Restrict access to information based on shared secrets	Require shared secrets with all desired services
Information privacy	Differential privacy	Limit privacy exposure of any single data record	True user-level privacy still chal- lenging
	Public-key cryptography	Integratable with hardware	Computationally intensive
Location privacy	Location cloaking	Personalized privacy	Requires additional infrastructure
Usage privacy	Differential privacy	Limit privacy exposure of any single data record	Recurrent/time-series data challenging to keep private

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

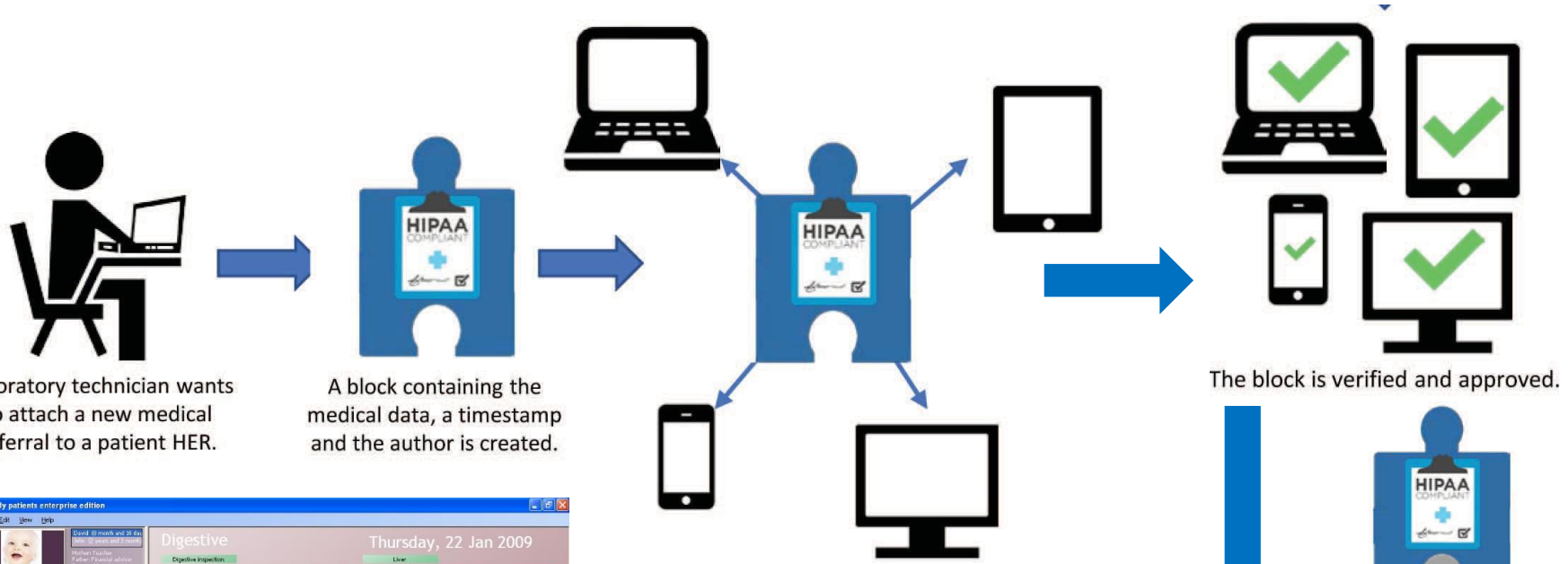
Smart Healthcare - Security and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

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

Source: Mohanty iSES 2018 Keynote

Blockchain in Smart Healthcare



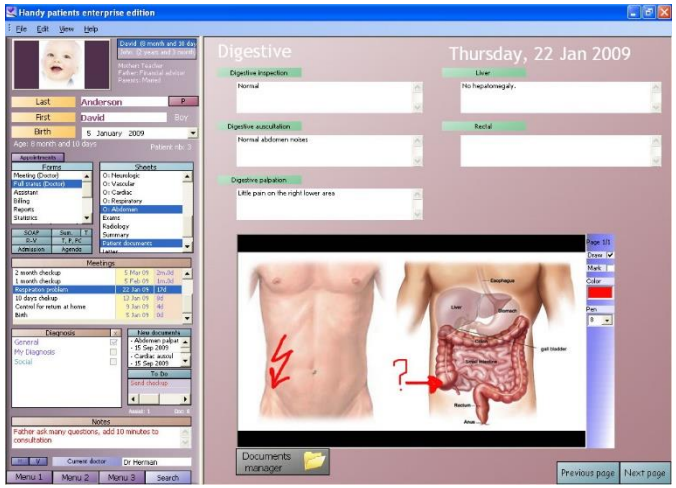
Laboratory technician wants to attach a new medical referral to a patient HER.

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

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

The block is verified and approved.

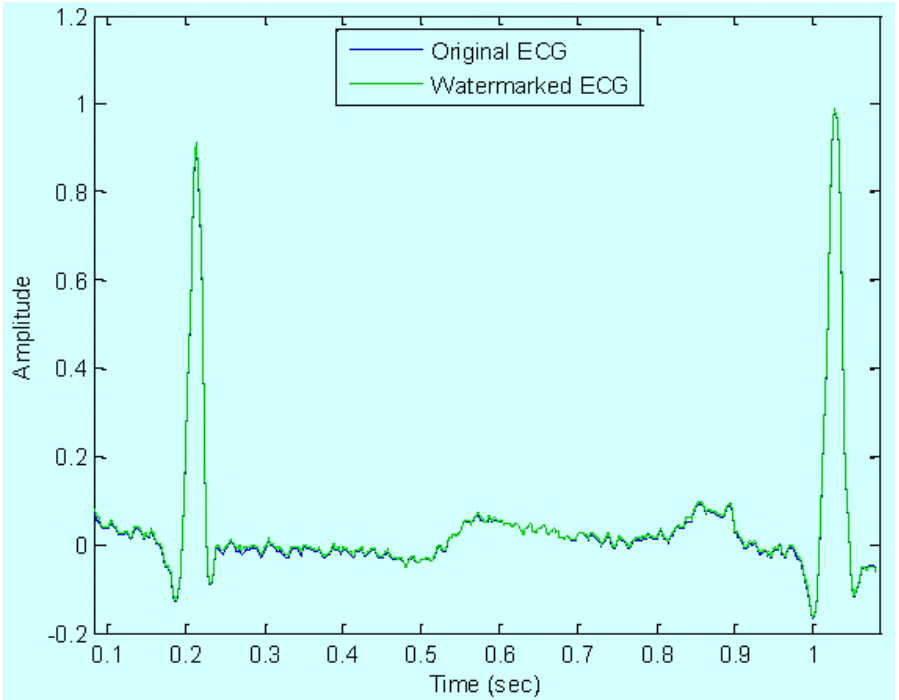
The block is inserted in the chain and linked with the previous blocks.



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

Smart 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.

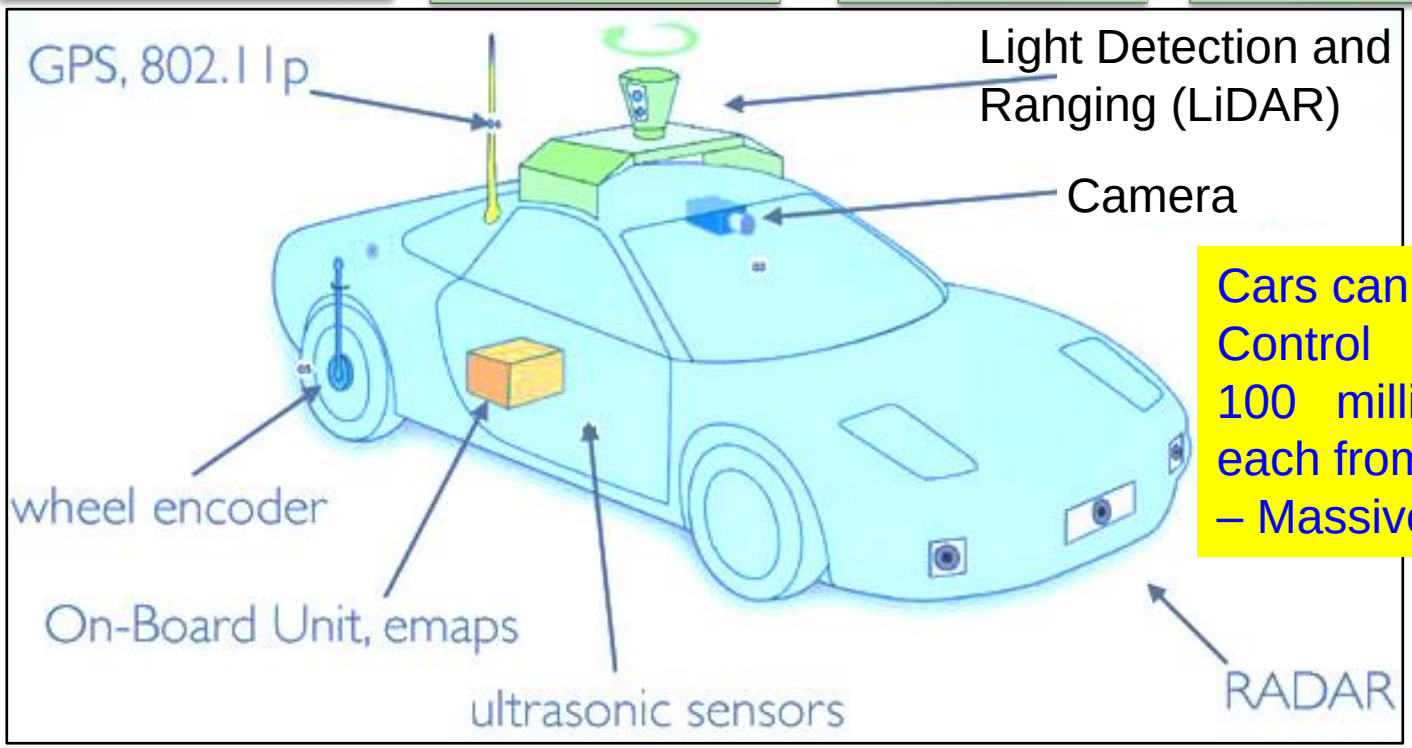


Source: Tseng 2014, Tseng Sensors Feb 2014

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.

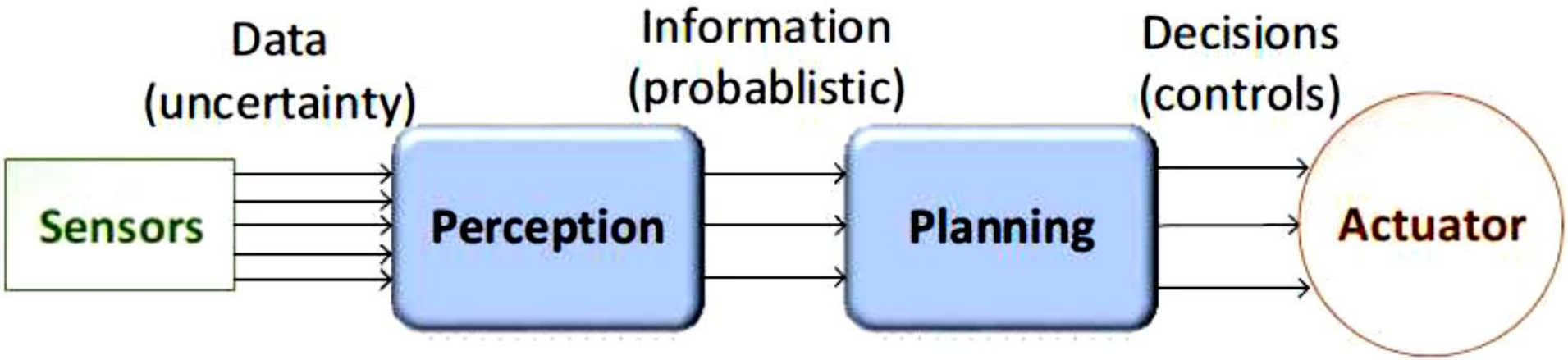
Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

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

Source: Petit 2015: IEEE-TITS Apr 2015

Smart Car – Decision Chain

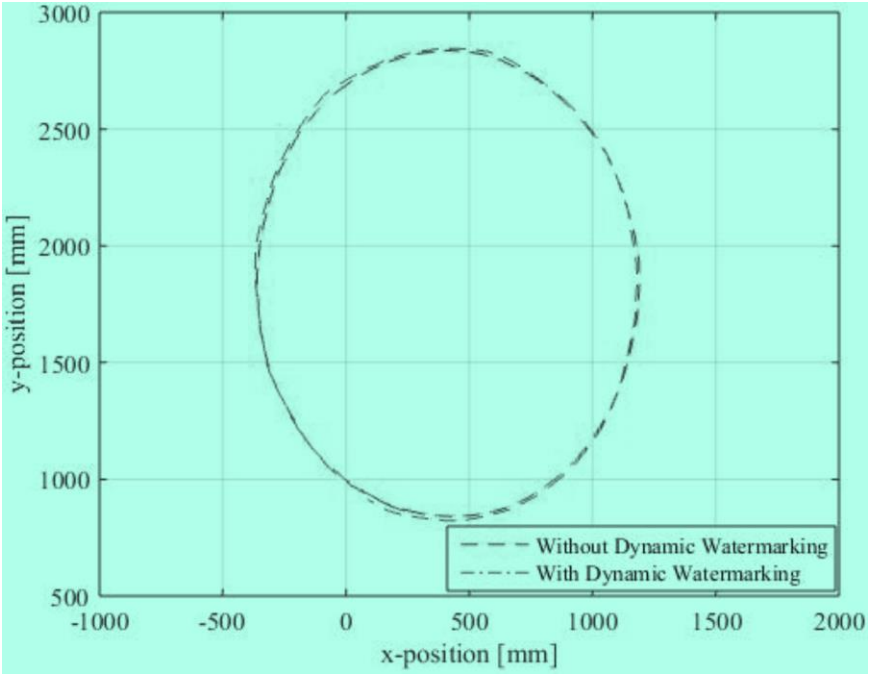
- Designing an AV requires decision chains.
- Human driven vehicles are controlled directly by a human.
- AV actuators controlled by algorithms.
- Decision chain involves sensor data, perception, planning and actuation.
- Perception transforms sensory data to useful information.
- Planning involves decision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



Source: Plathottam 2018, COMSNETS 2018

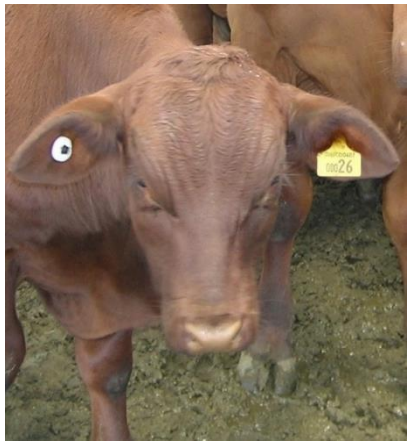
Autonomous Car Security – Collision Avoidance

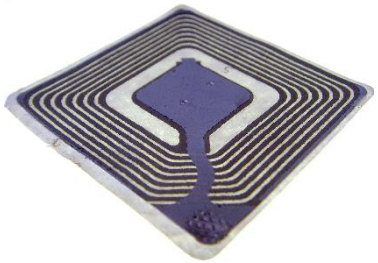
- Attack: Feeding of malicious sensor measurements to the control and the collision avoidance module. Such an attack on a position sensor can result in collisions between the vehicles.
- Solutions: "**Dynamic Watermarking**" of signals to detect and stop such attacks on cyber-physical systems.
- Idea: 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

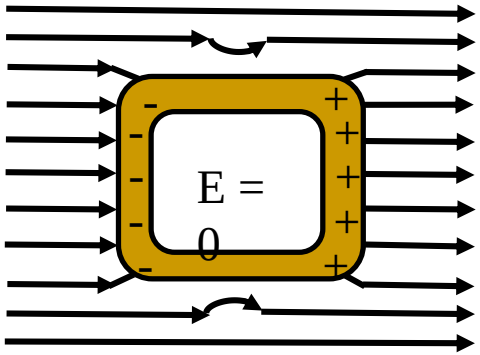
Source: Khattab 2017: Springer 2017 RFID Security

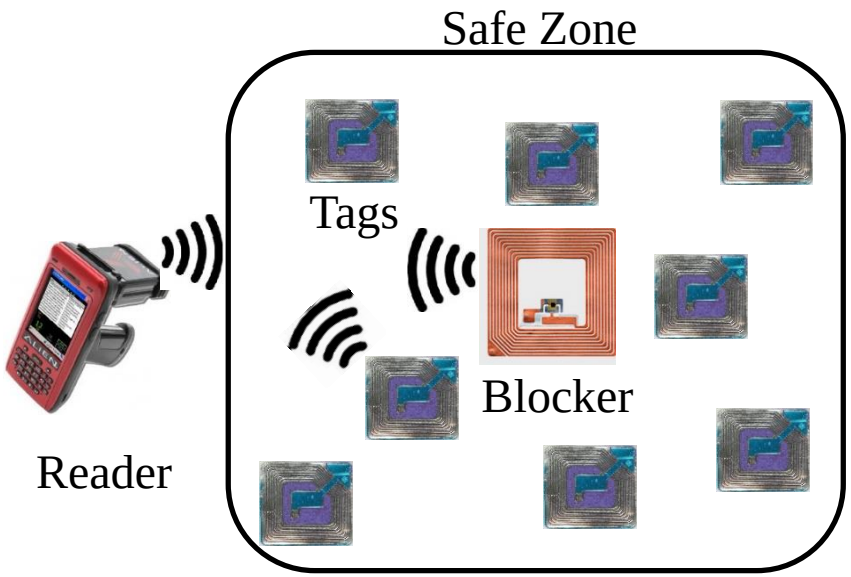
RFID Security - Solutions

Selected RFID Security Methods

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

Faraday Cage

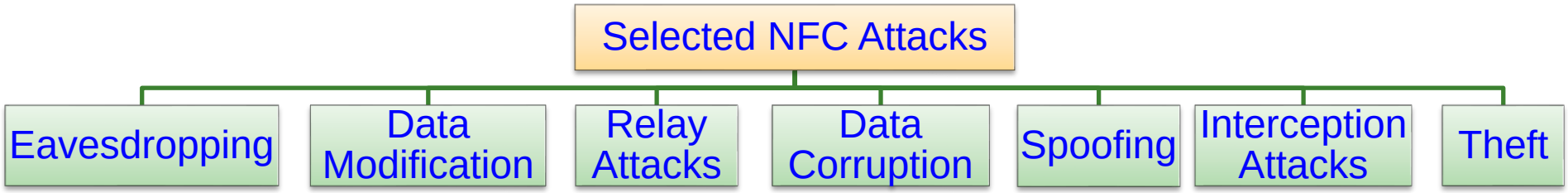




Blocker Tags

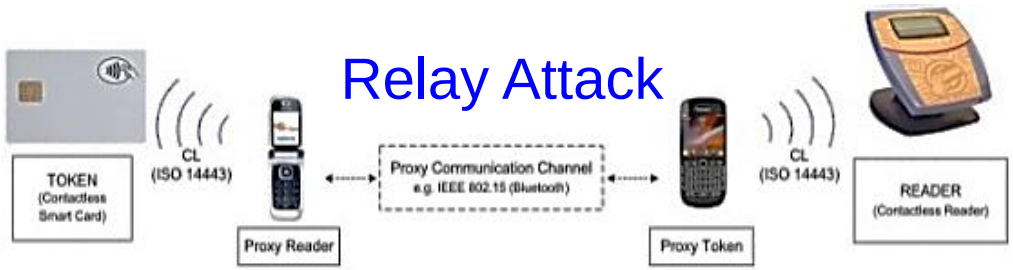
Source: Khattab 2017, Springer 2017 RFID Security

NFC Security - Attacks



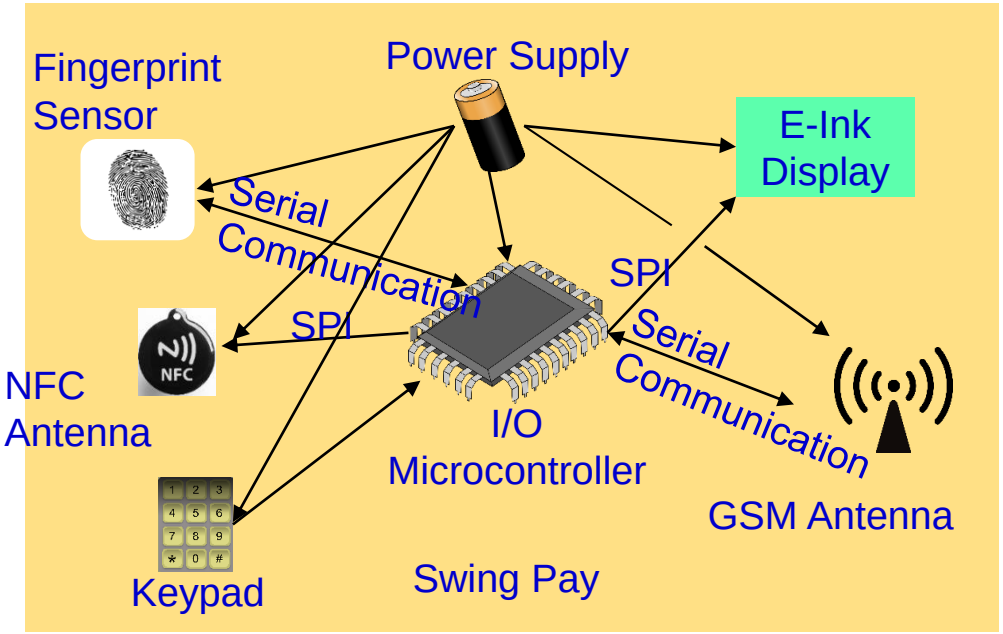
Source: http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497

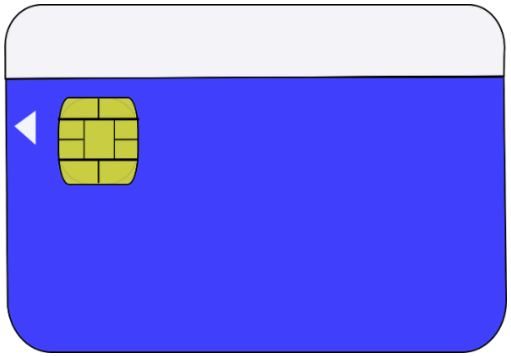
Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

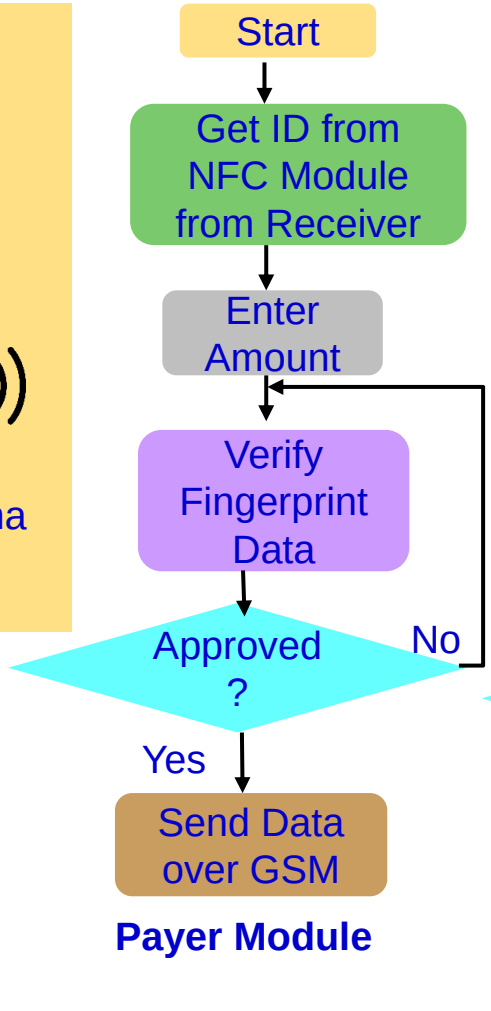


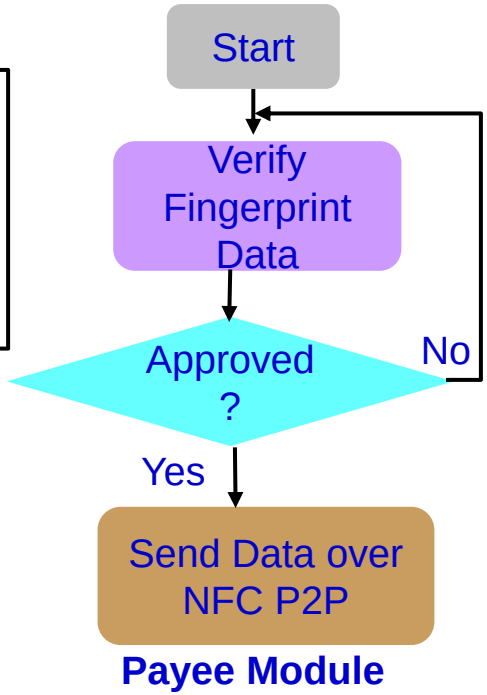
Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

NFC Security



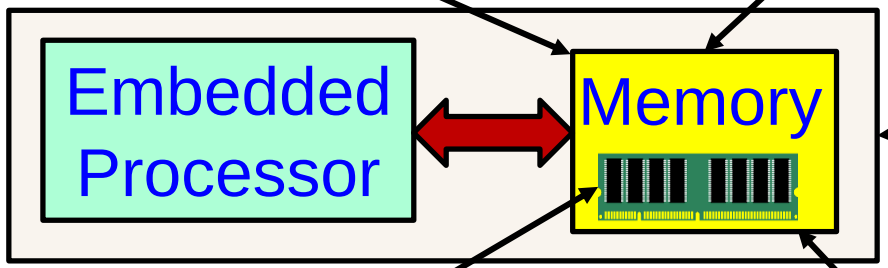






Source: Mohanty 2017, CE Magazine Jan 2017

Memory Attacks



Read confidential information in memory

Snooping Attacks

Spoofing Attacks

Replace a block with fake

Splicing Attacks

Replace a block with a block from another location

Physical access memory to retrieve encryption keys

Cold Boot Attacks

Replay Attacks

Value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, “TSV: A Novel Energy Efficient Memory Integrity Verification Scheme for Embedded Systems”, Elsevier Journal of Systems Architecture, Vol. 59, No. 7, Aug 2013, pp. 400-411.

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

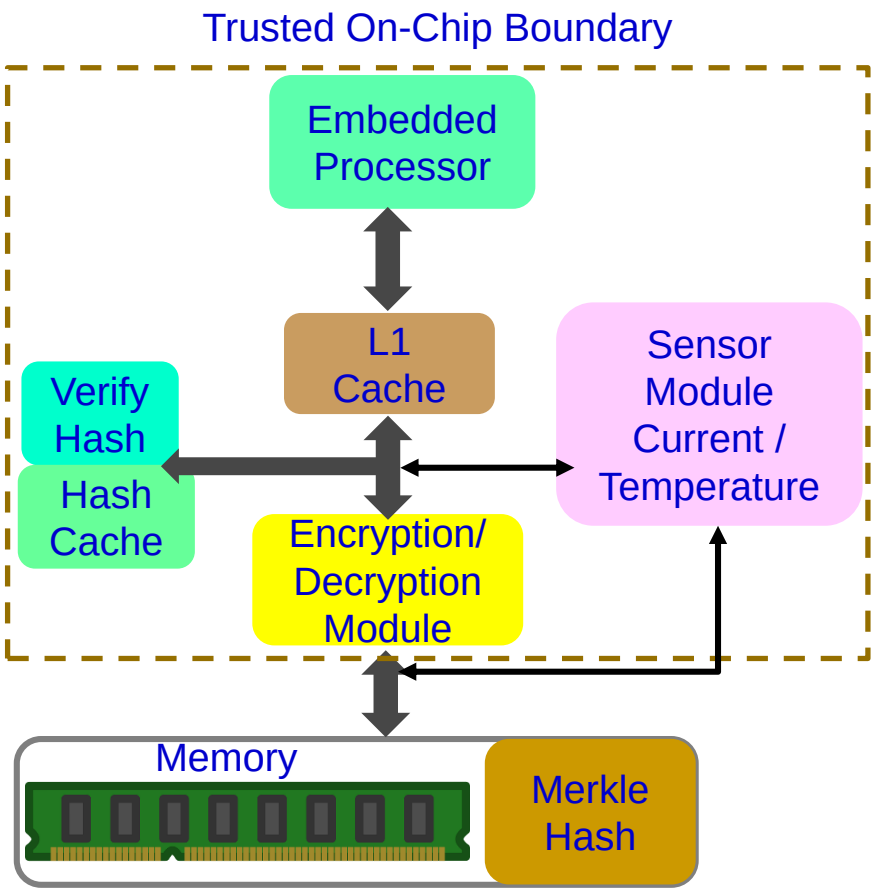
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

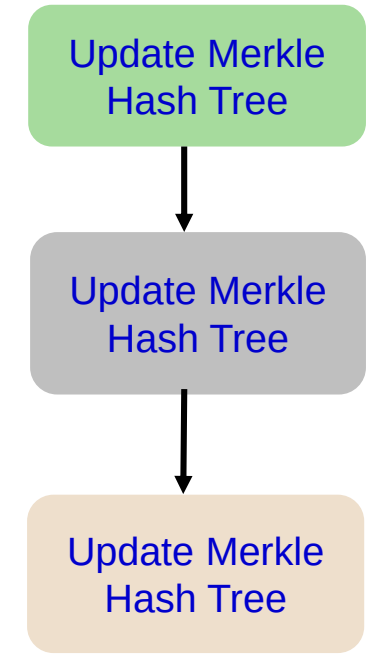
Nonvolatile / Harddrive Storage

Some performance penalty due to increase in latency!

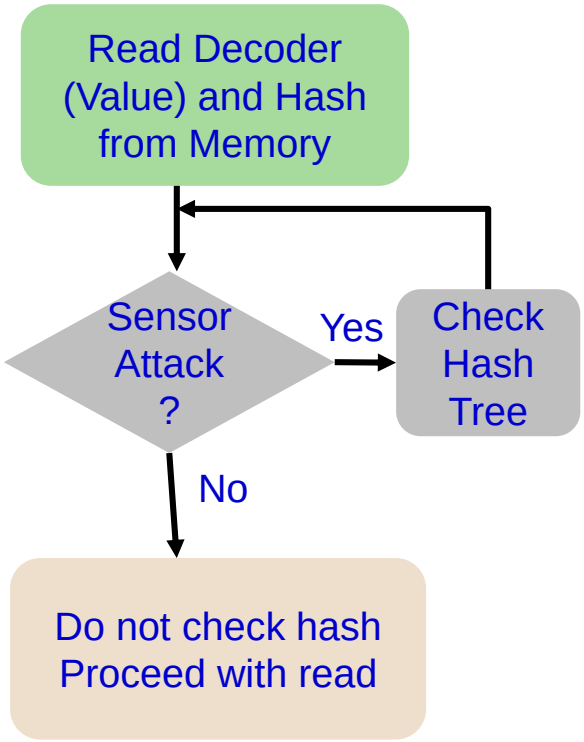
Embedded Memory Security and Protection



On-Chip/On-Board Memory Protection



Write Operation

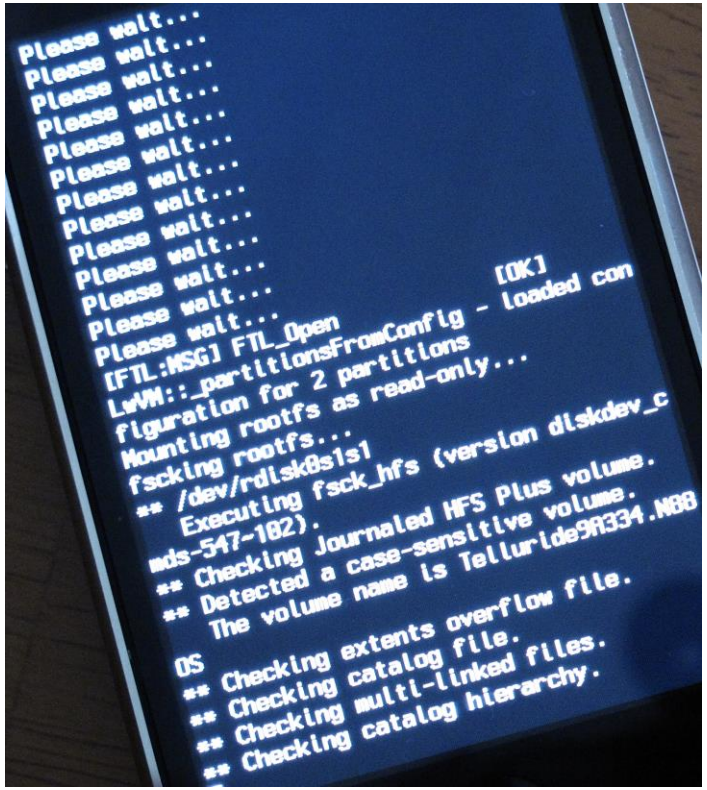


Read Operation

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.

Firmware Reverse Engineering

Extract, modify, or reprogram code

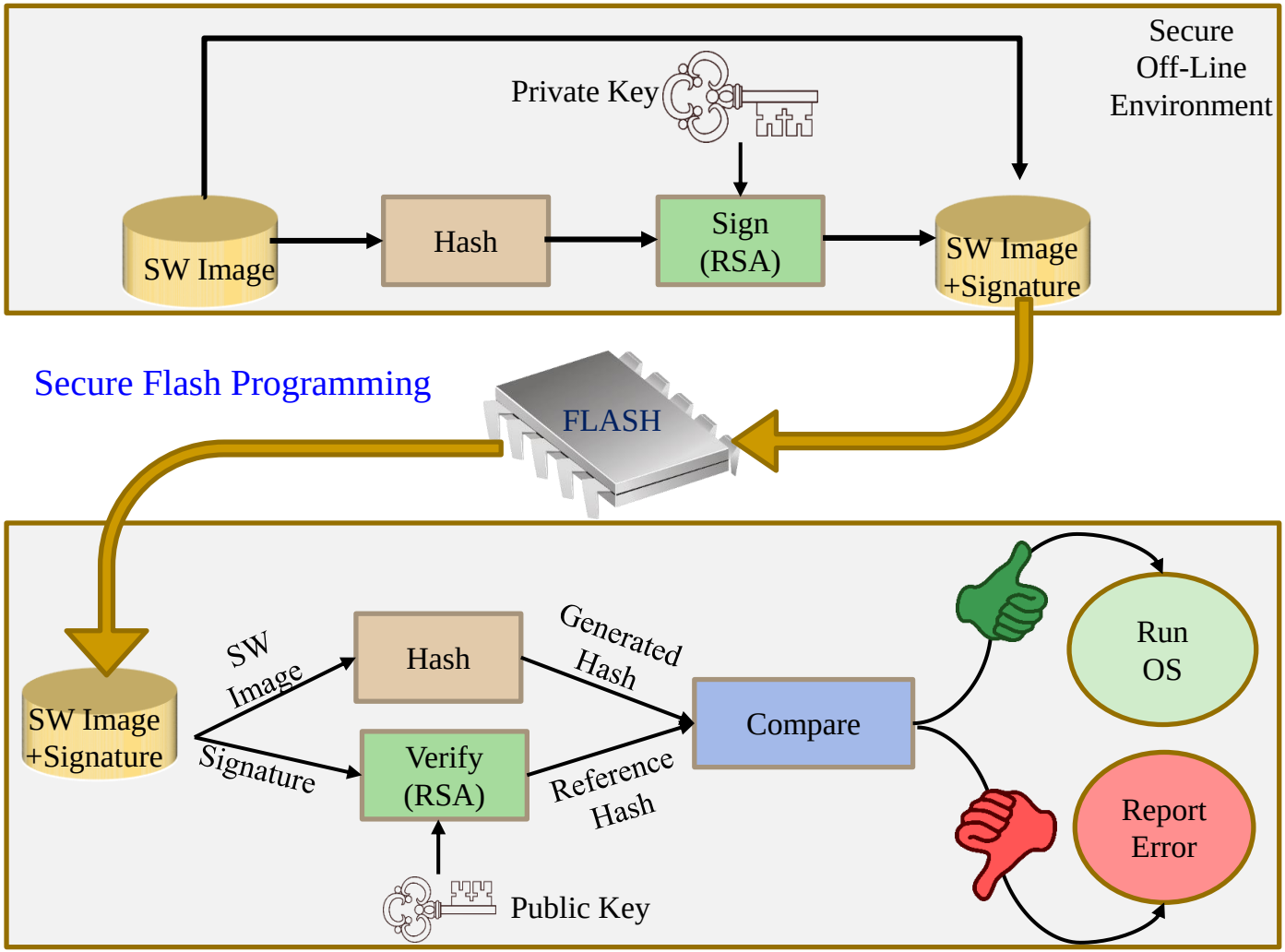


OS exploitation,
Device jailbreaking

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

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

Firmware Security



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

How Secure is AES Encryption?

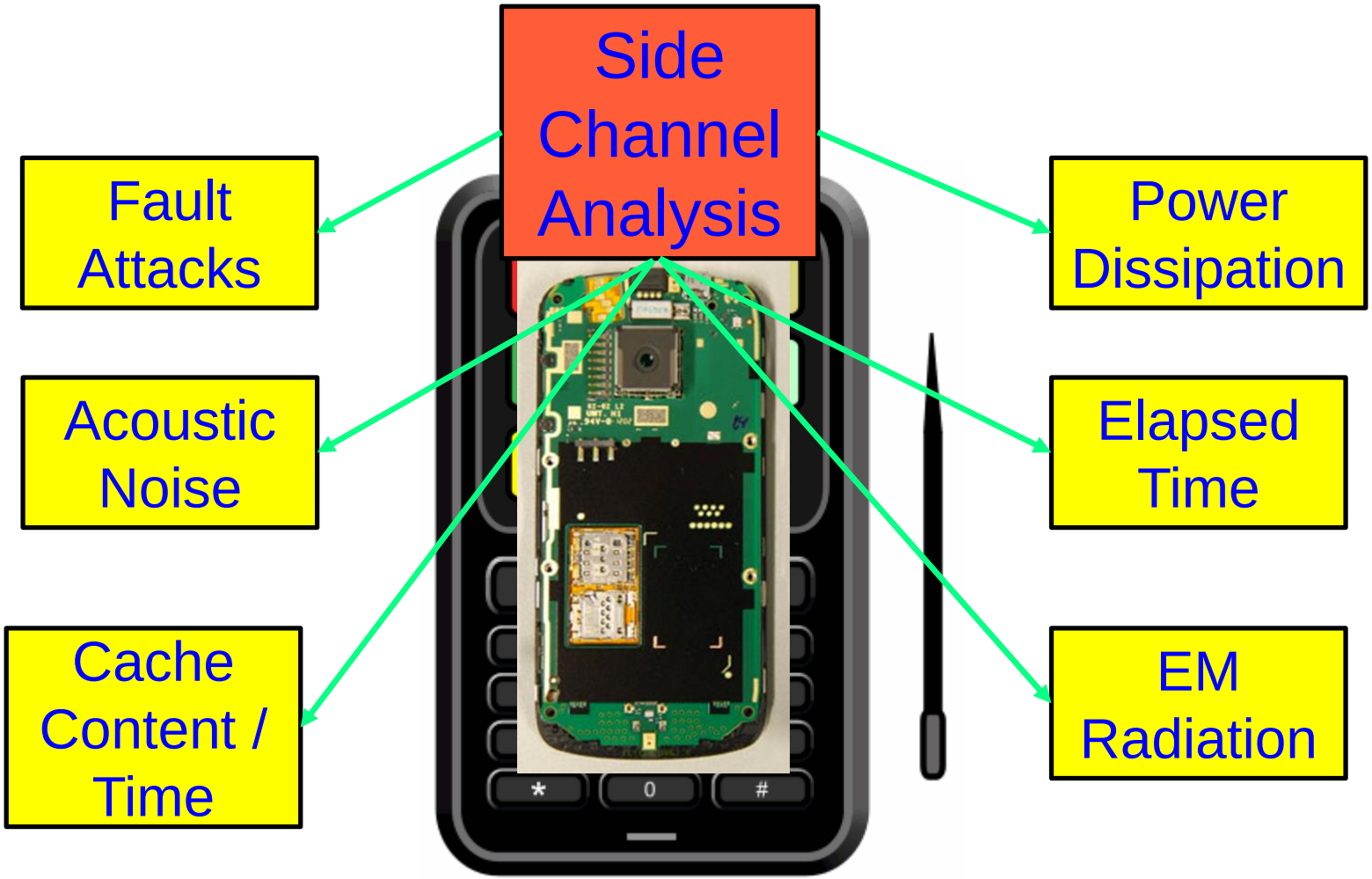
- Brute force a 128 bit key ?
- If you assume
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, you can crack the key after testing 50% of the possibilities
  - Then 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

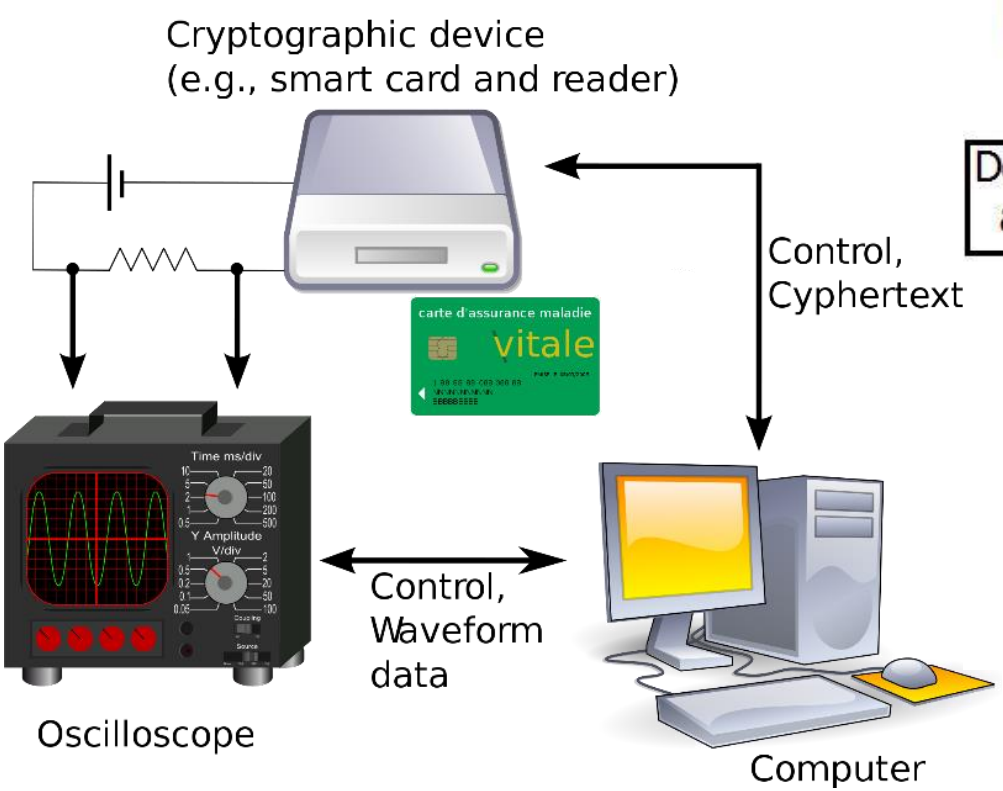
Source: Parameswaran Keynote iNIS-2017

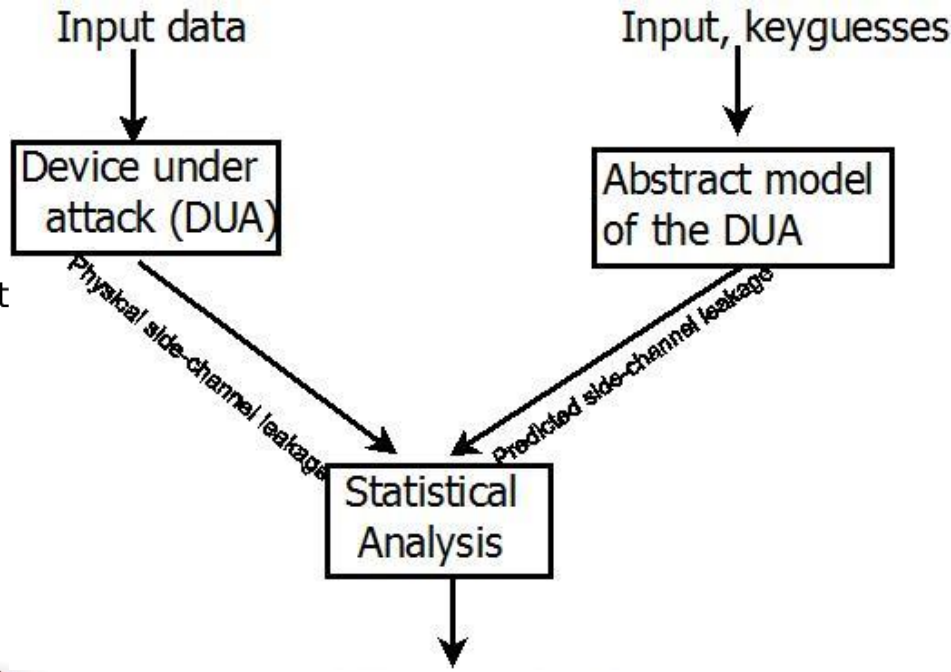
Side Channel Analysis Attacks



Source: Parameswaran Keynote iNIS-2017

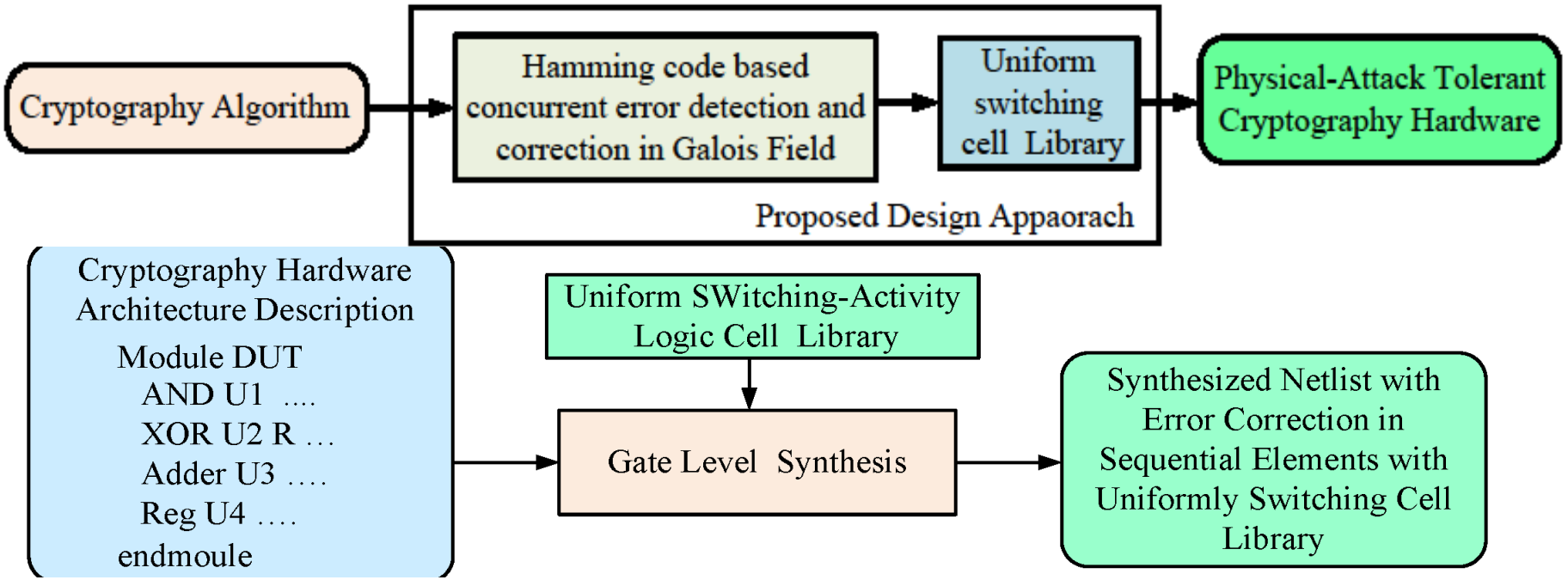
Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

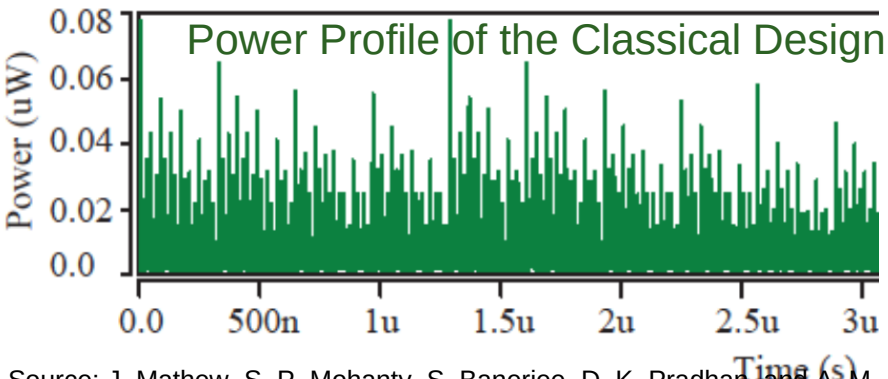


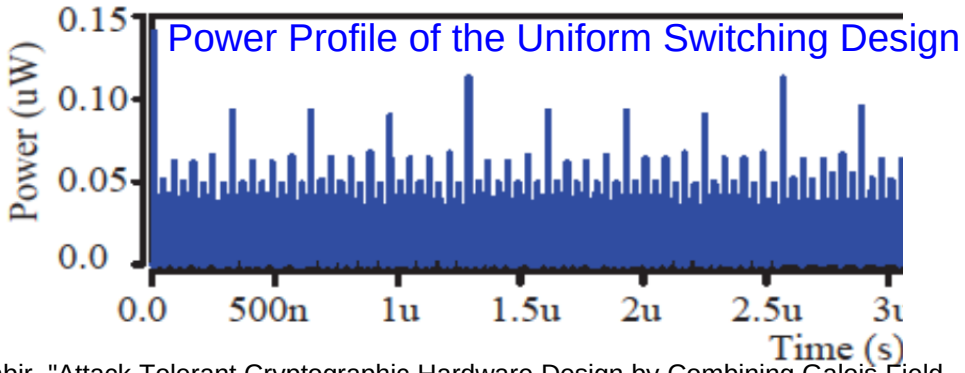


Source: Mohanty 2018, ZINC Keynote 2018

DPA Resilience Hardware: Design







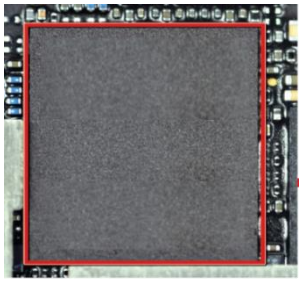
Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", Elsevier Computers and Electrical Engineering, Vol. 39, No. 4, May 2013, pp. 1077--1087.

Copyright, Intellectual Property (IP), Or Ownership Protection

Media Ownership

- Whose is it?
- Is it tampered with?
- Where was it created?
- Who had created it?
- ... and more.

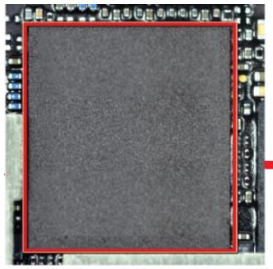
Hardware Ownership



Chip at Original Design House

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

Goes to Another Design House for Resuse



Chip at Another Design House

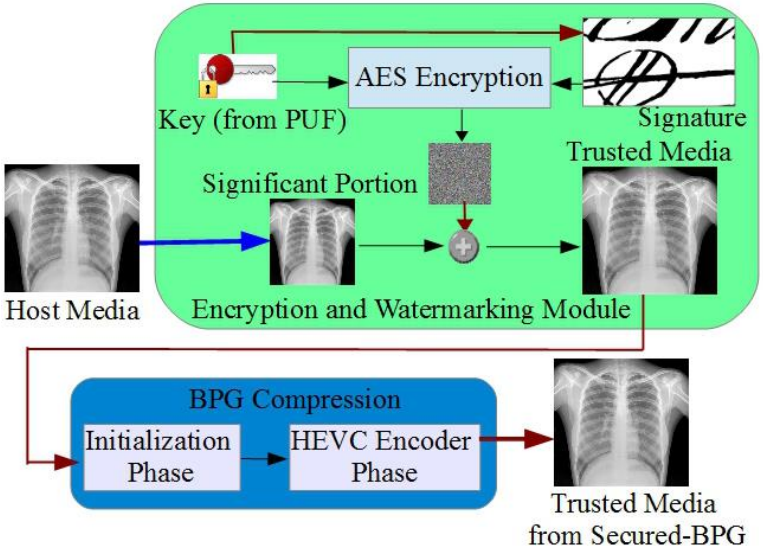
? Who Owns ?

Company A

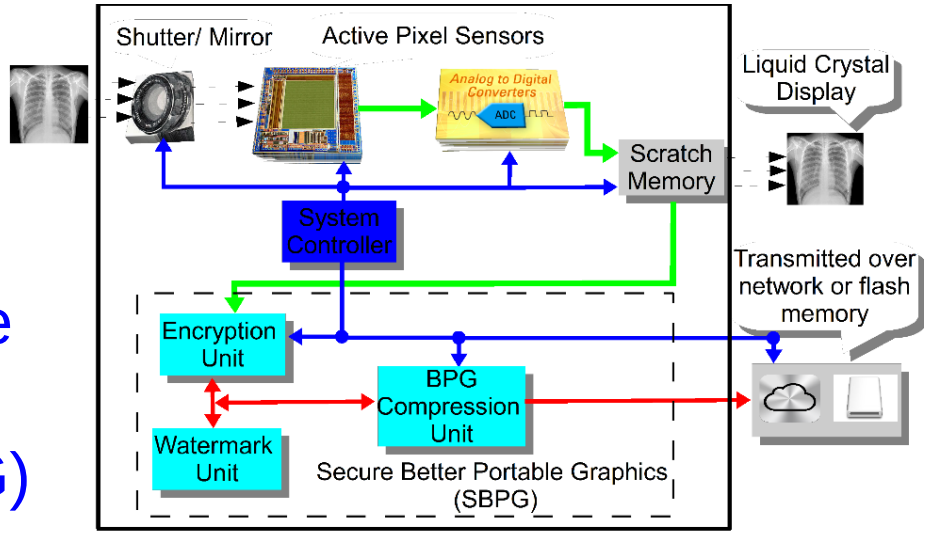
Company B

Source: Mohanty ZINC 2018 Keynote

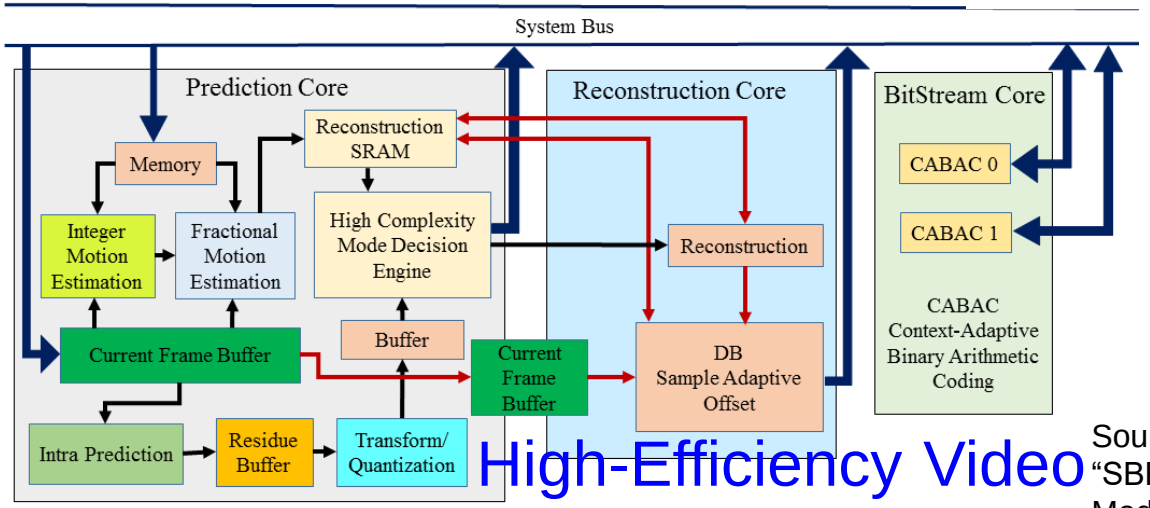
Secure Better Portable Graphics (SBPG)



Secure BPG (SBPG)



Secure Digital Camera (SDC) with SBPG

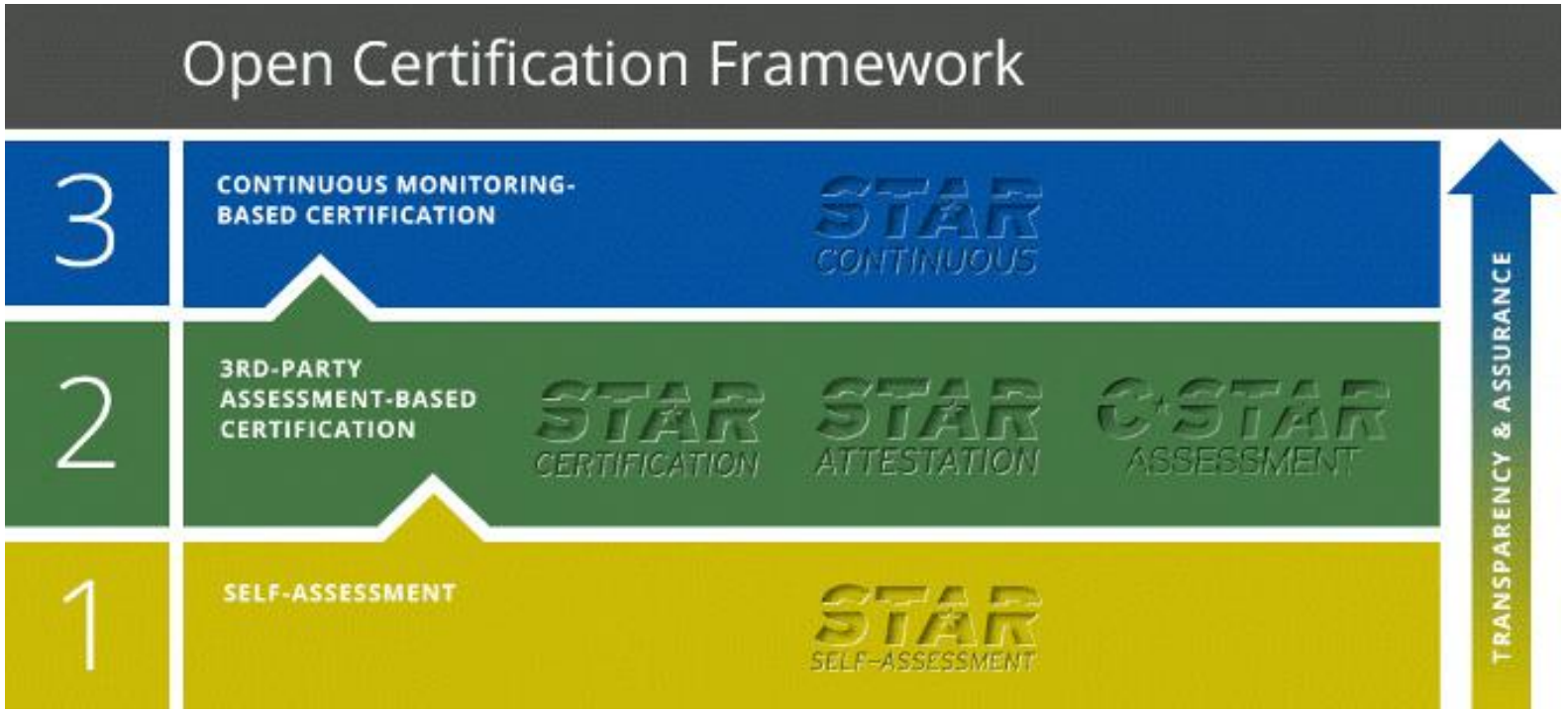


High-Efficiency Video Coding Architecture

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.

Security Star Ratings



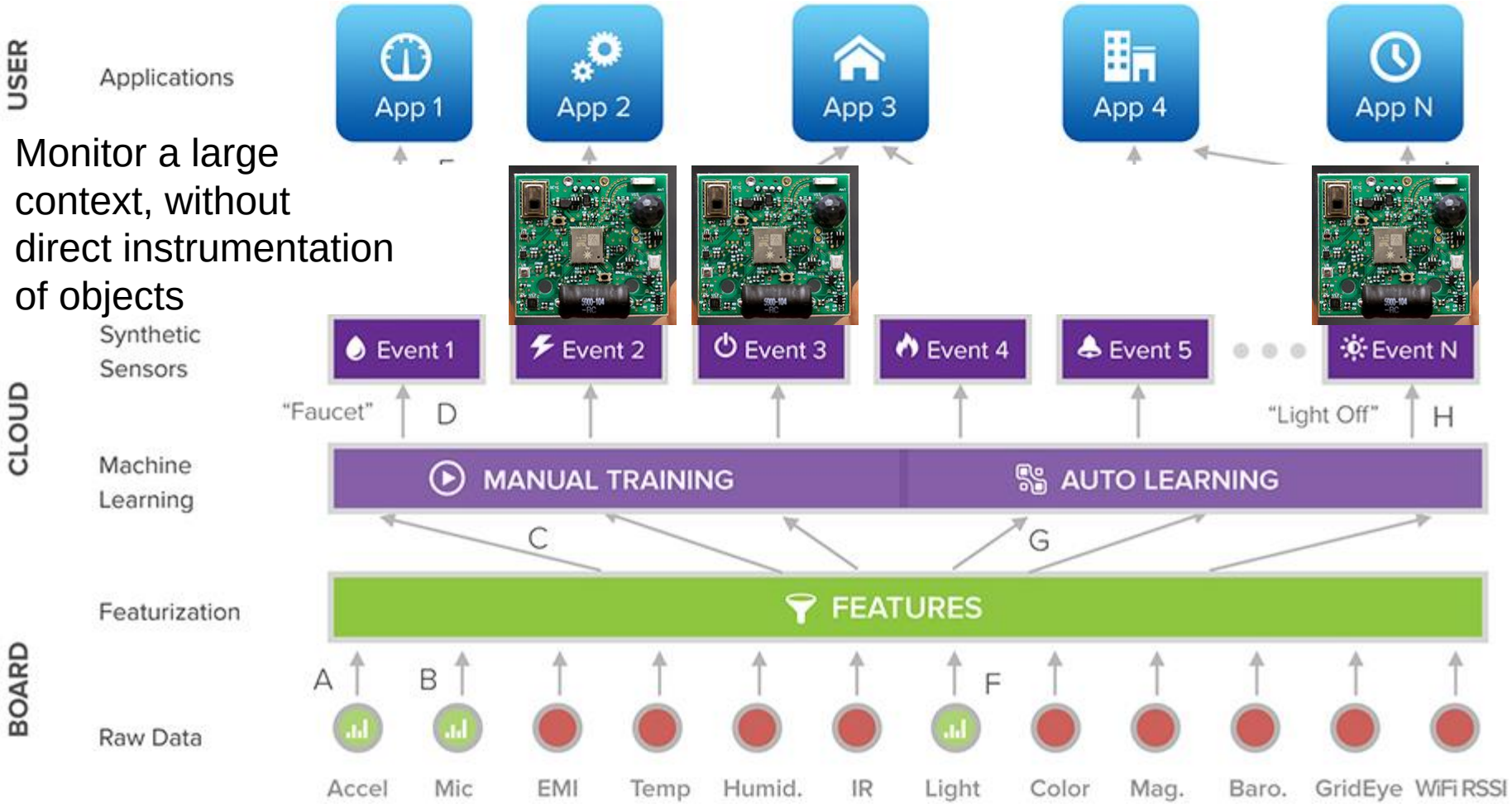
Source: https://cloudsecurityalliance.org/star/#_overview

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

Response Smart

Smart Sensors - General-Purpose/ Synthetic Sensors

Monitor a large context, without direct instrumentation of objects



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

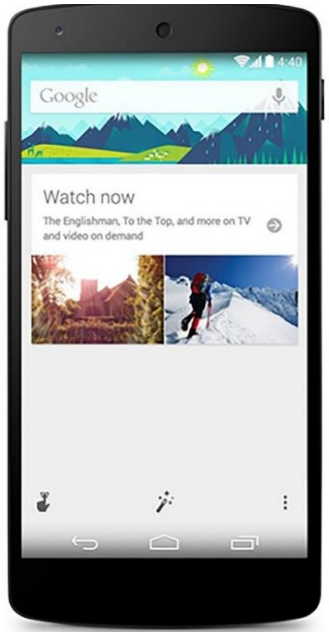
Systems – End Devices

Alexa

Google Now

Windows Cortana

Apple Siri



Smart Transportation

Autonomous/ Driverless/ Self-Driving/ Smart Care

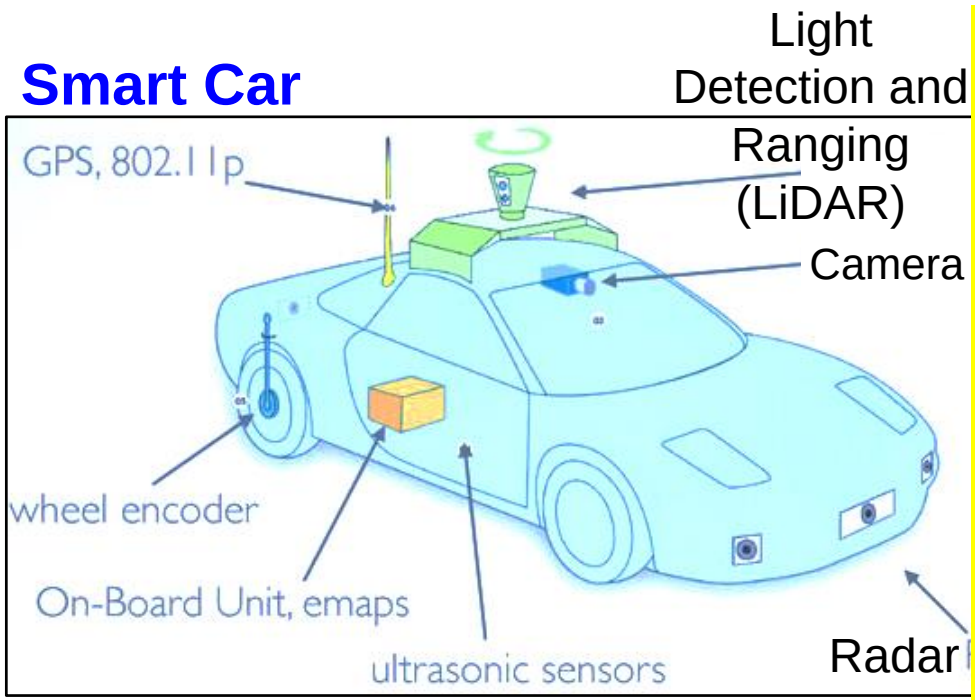
Autonomous Vehicle (AV) is capable of sensing its environment and navigating without human input.

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

Datta 2017: CE Magazine Oct 2017

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

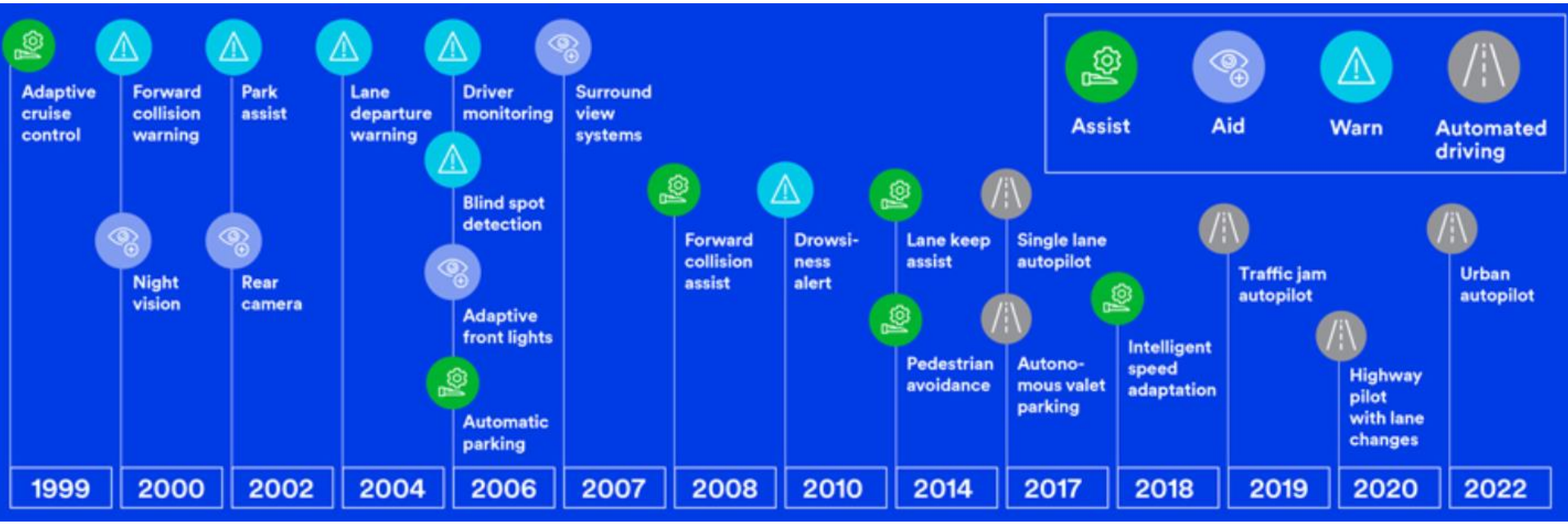
Level 4
- Perform All Safety-Critical Functions
- Limited to Operational Domain

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 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

Healthy Living

- Fitness Tracking
- Disease Prevention
- Food monitoring

Home Care

- Mobile health
- Telemedicine
- Self-management
- Assisted Living

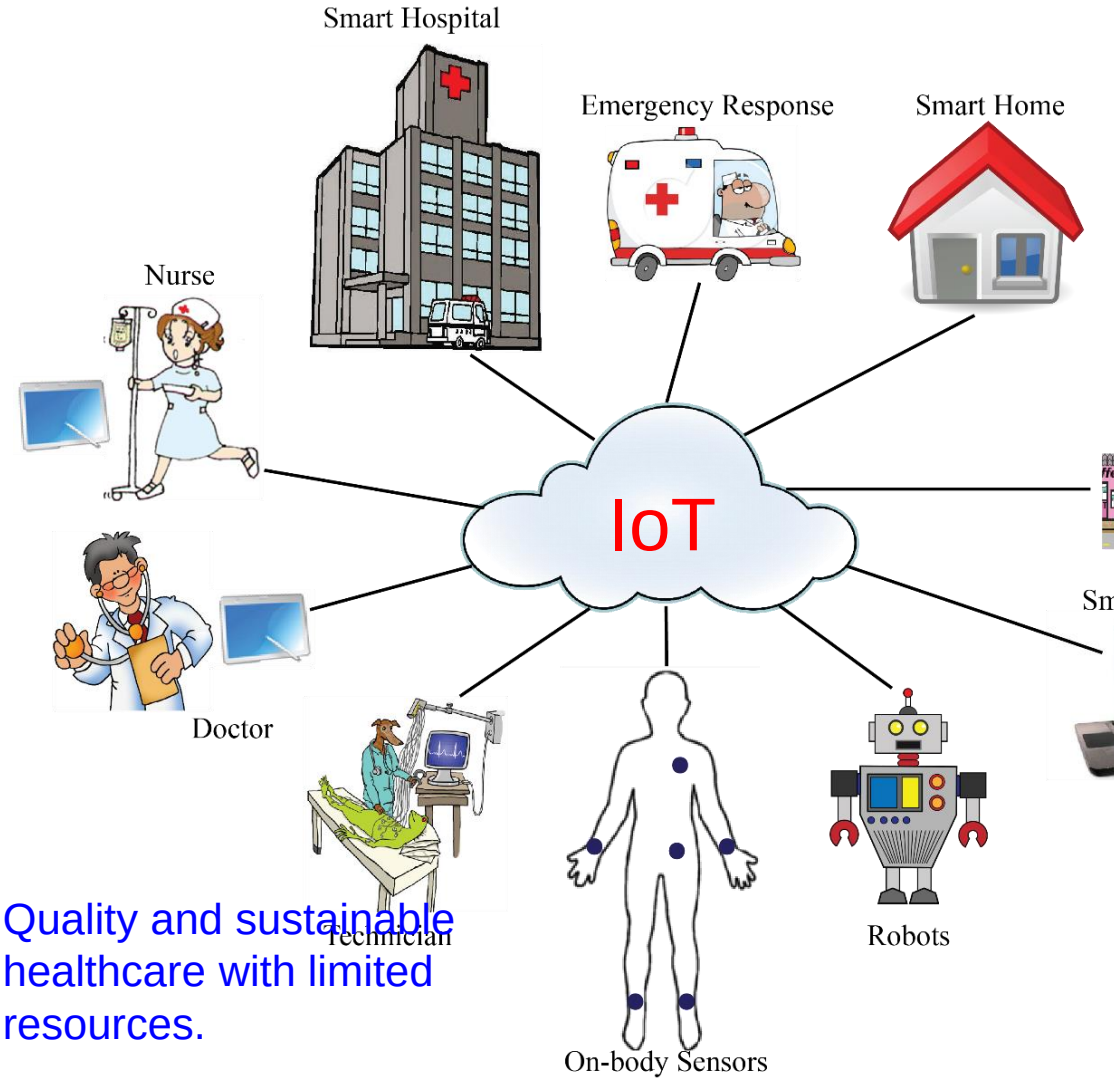
Acute care

- Hospital
- Specialty clinic
- Nursing Home
- Community Hospital

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

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

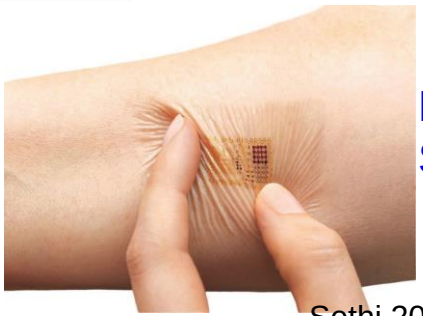
Smart Healthcare



Fitness Trackers

Headband with Embedded Neurosensors

Quality and sustainable healthcare with limited resources.

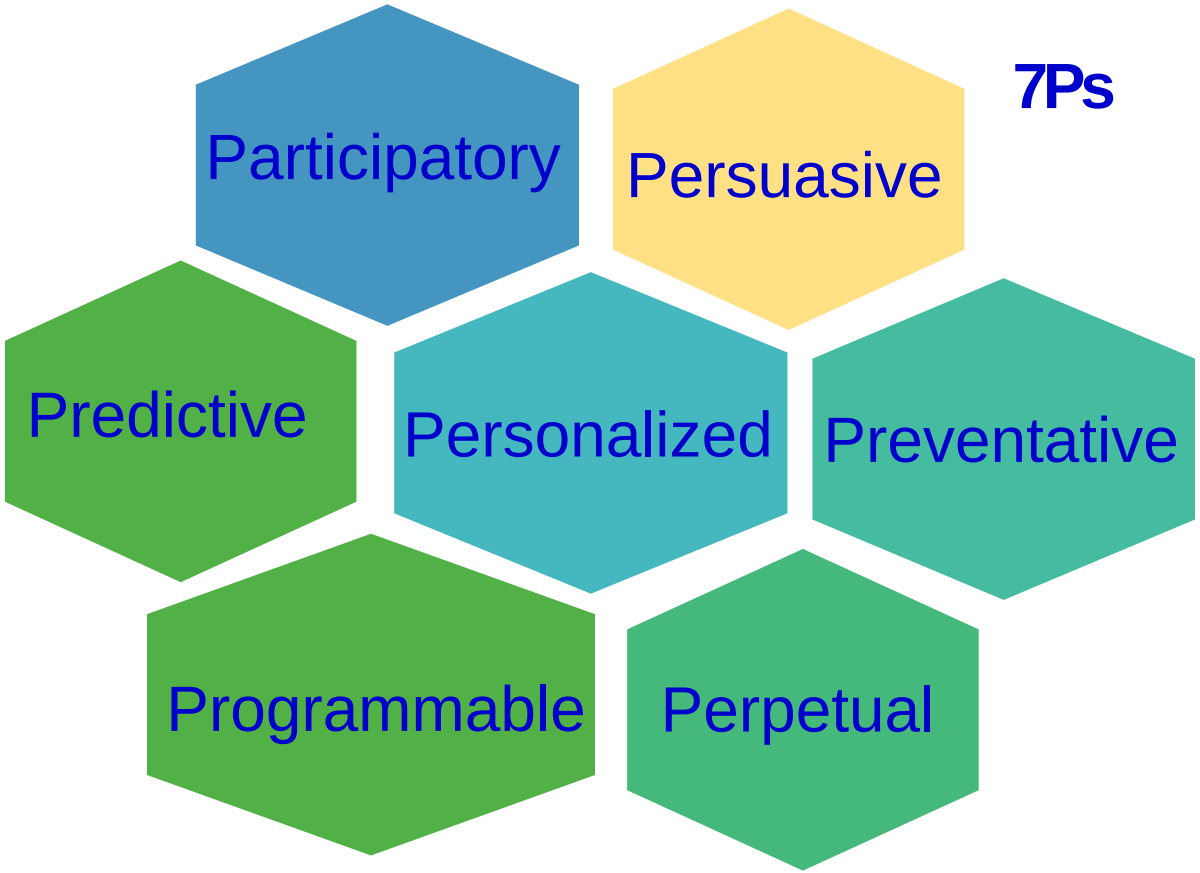


Embedded Skin Patches

Source: Mohanty 2016, CE Magazine July 2016

Sethi 2017: JECE 2017

Smart Healthcare - Characteristics - 7Ps

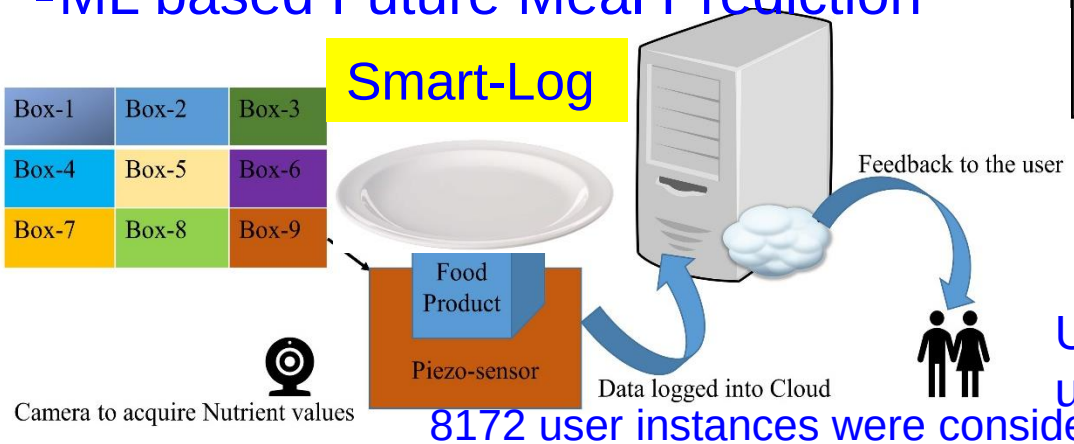


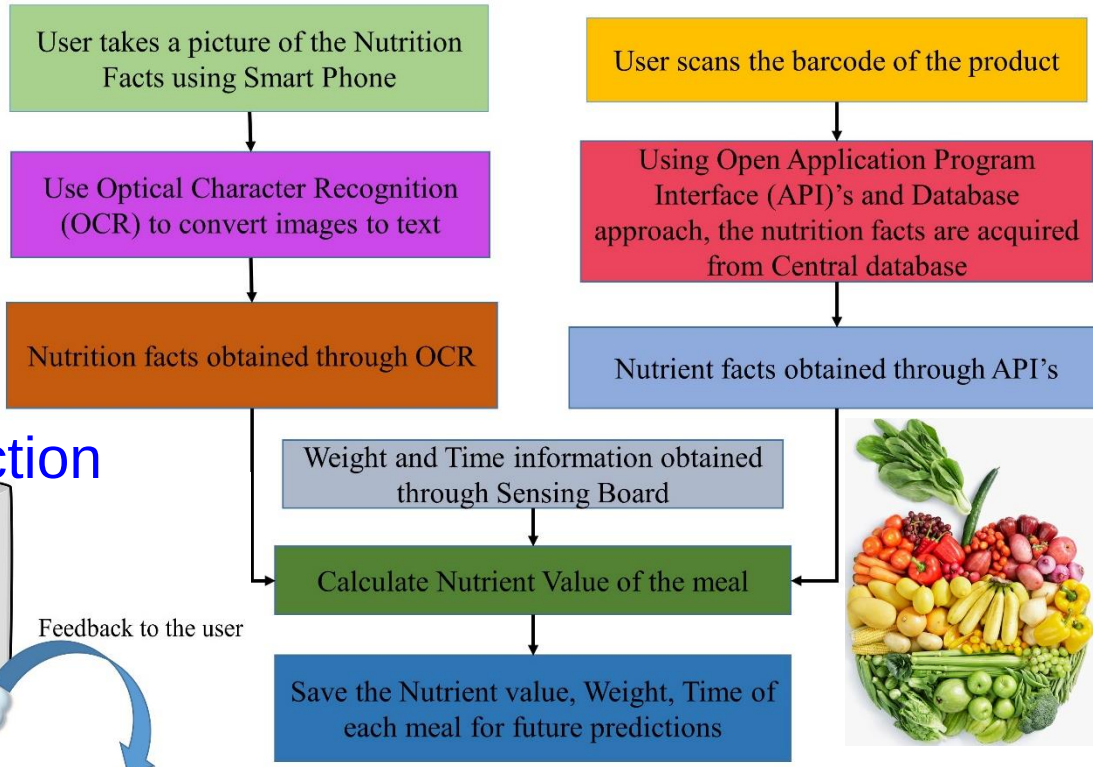
Source: H. Zhu, C. K. Wu, C. H. KOO, Y. T. Tsang, Y.Liu, H. R. Chi, and K. F. Tsang, "Smart Healthcare in the Era of Internet-of-Things", IEEE Consumer Electronics Magazine, 2019, Accepted.

Smart Healthcare – Diet Monitoring

Automated Food intake Monitoring and Diet Prediction System

- Smart plate
- Data acquisition using mobile
- ML based Future Meal Prediction





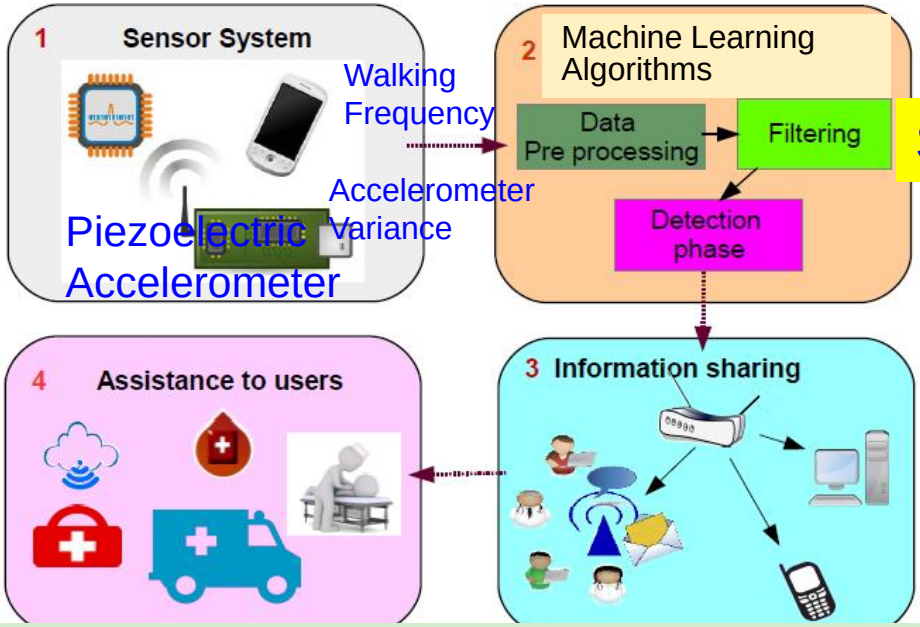
USDA National Nutrient Database used for nutrient values of 8791 items.

8172 user instances were considered

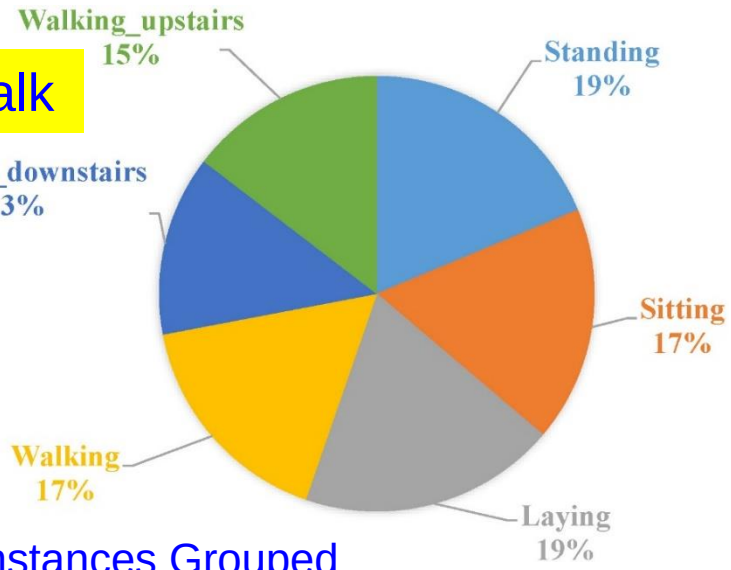
Research Works	Food Recognition Method	Efficiency (%)
This Work	Mapping nutrition facts to a database	98.4

Source: P. Sundaravadivel, K. Kesavan, L. Kesavan, S. P. Mohanty, and E. Kougianos, "Smart-Log: A Deep-Learning based Automated Nutrition Monitoring System in the IoT", IEEE Trans. on Consumer Electronics, Vol 64, No 3, Aug 2018, pp. 390-398.

Smart Healthcare - Activity Monitoring



Automated Physiological Monitoring System

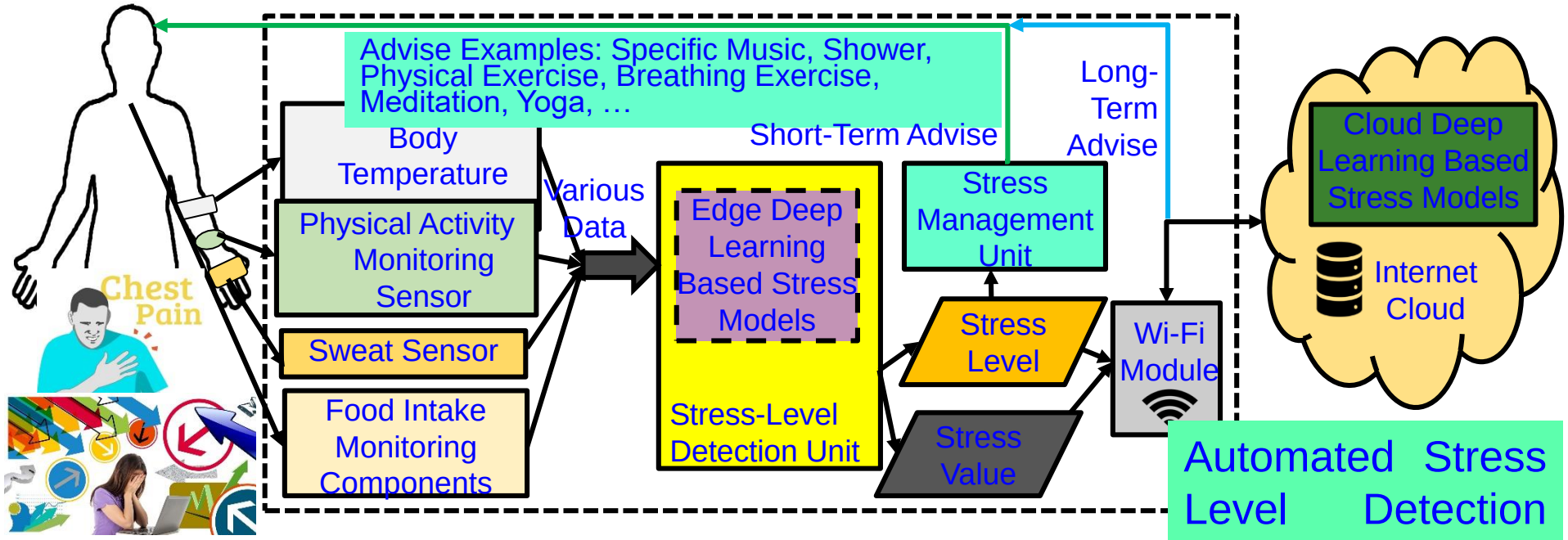


10291 Instances Grouped Under 6 Activities - Kaggle

Research Works	Method (WEKA)	Features considered	Activities	Accuracy (%)
This Work	Adaptive algorithm based on feature extraction	Step detection and Step length estimation	Walking, sitting, standing, etc.	97.9

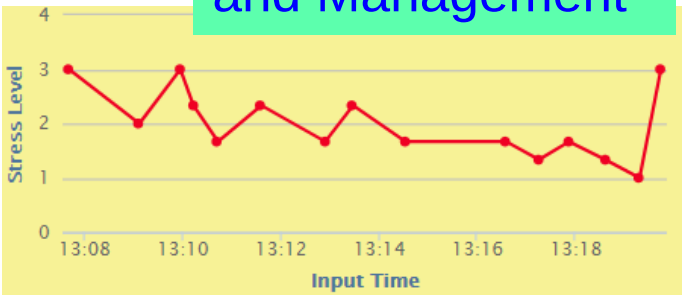
P. Sundaravadivel, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, and M. K. Ganapathiraju, "Smart-Walk: An Intelligent Physiological Monitoring System for Smart Families", in Proc. 36th IEEE International Conf. Consumer Electronics (ICCE), 2018.

Smart Healthcare - Stress Monitoring & Control



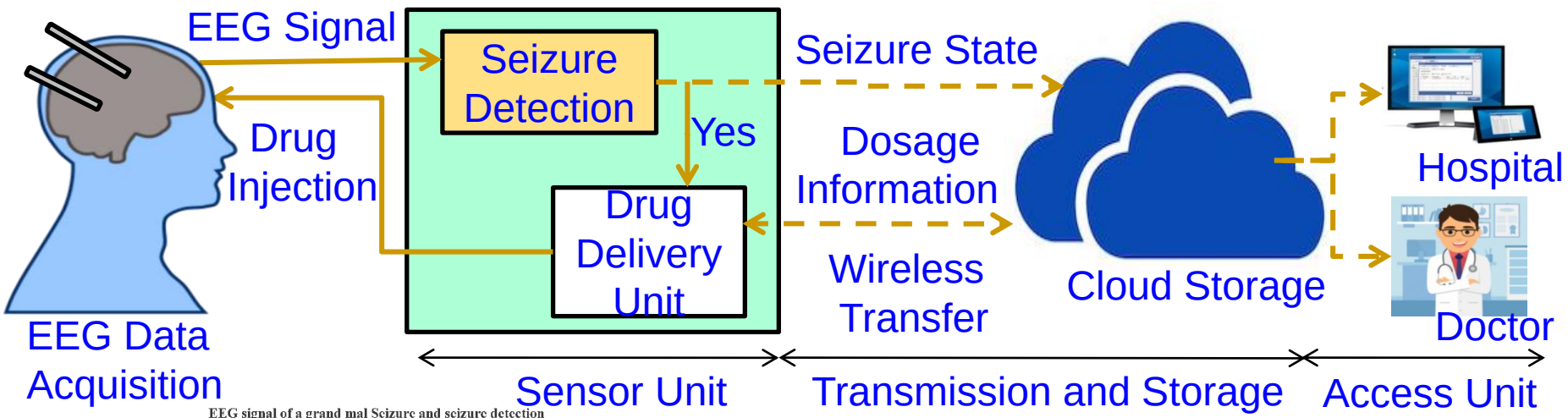
Automated Stress Level Detection and Management

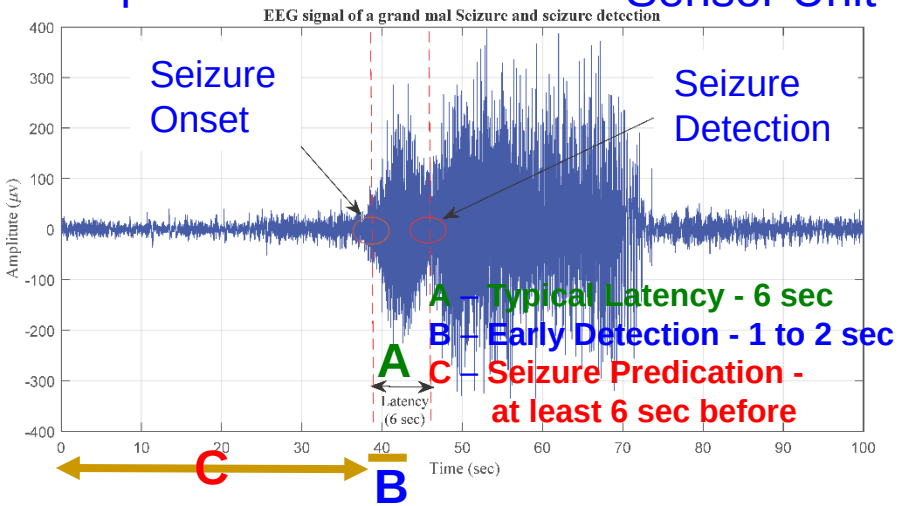
Sensor	Low Stress	Normal Stress	High Stress
Accelerometer (steps/min)	0-75	75-100	101-200
Humidity (RH%)	27-65	66-91	91-120
Temperature ℉	98-100	90-97	80-90



Source: L. Rachakonda, P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and M. Ganapathiraju, "A Smart Sensor in the IoMT for Stress Level Detection", in Proc. 4th IEEE International Symposium on Smart Electronic Systems (iSES), 2018, pp. 141--145.

Smart Healthcare - Seizure Detection & Control



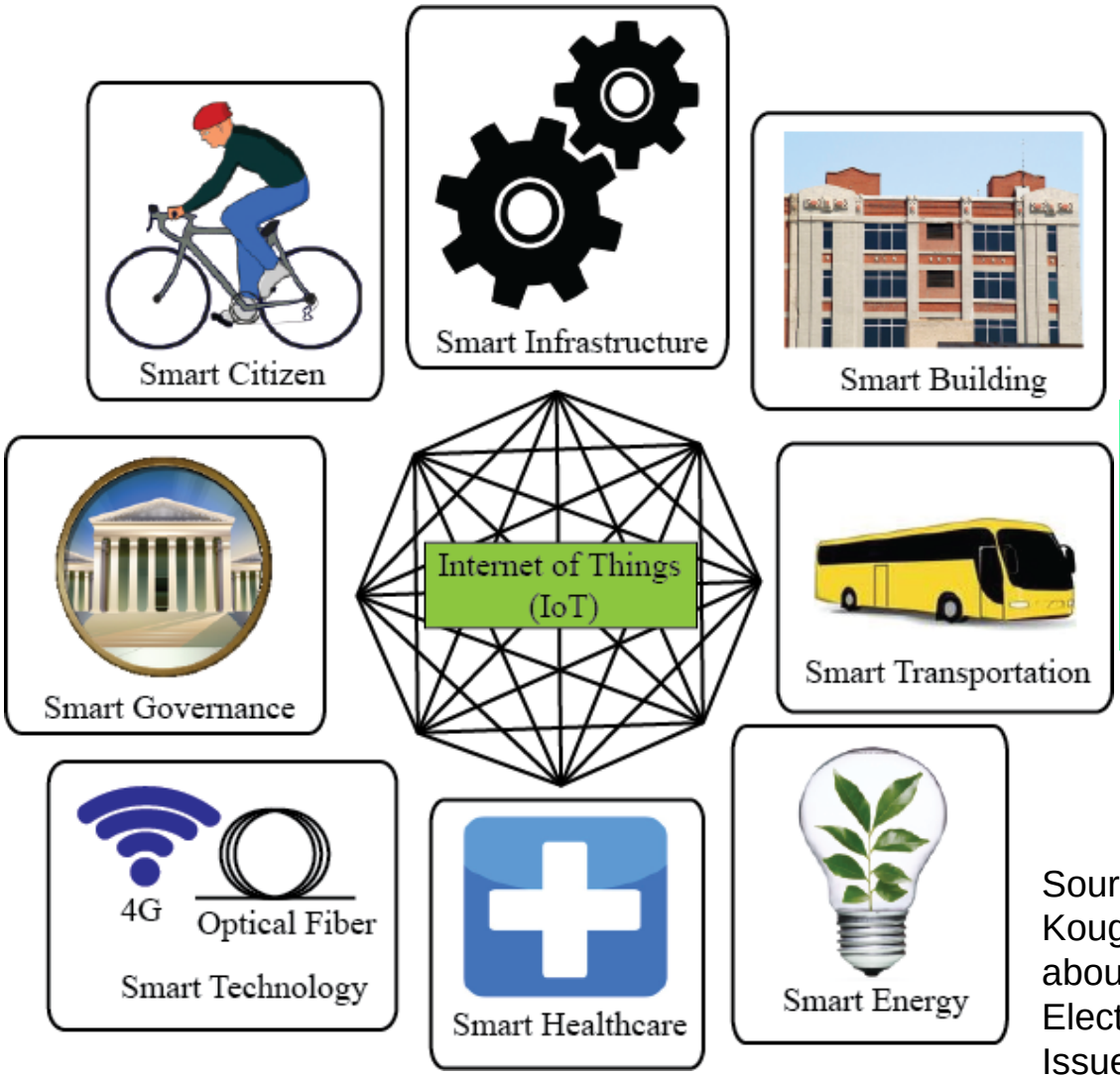


Automated Epileptic Seizure Detection and Control System

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

Source: M. A. Sayeed, S. P. Mohanty, E. Kougianos, and H. Zaveri, "Neuro-Detect: A Machine Learning Based Fast and Accurate Seizure Detection System in the IoMT", *IEEE Transactions on Consumer Electronics (TCE)*, Volume XX, Issue YY, ZZ 2019, pp. Accepted on 16 May 2019, DOI: 10.1109/TCE.2019.2917895 .

Smart Cities - Components



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

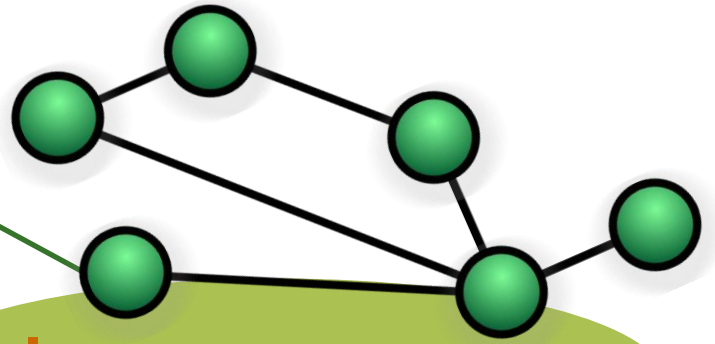
Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", IEEE Consumer Electronics Magazine (CEM), Volume 5, Issue 3, July 2016, pp. 60--70.

Smart Cities - 3 Is

Instrumentation

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

Smart Cities

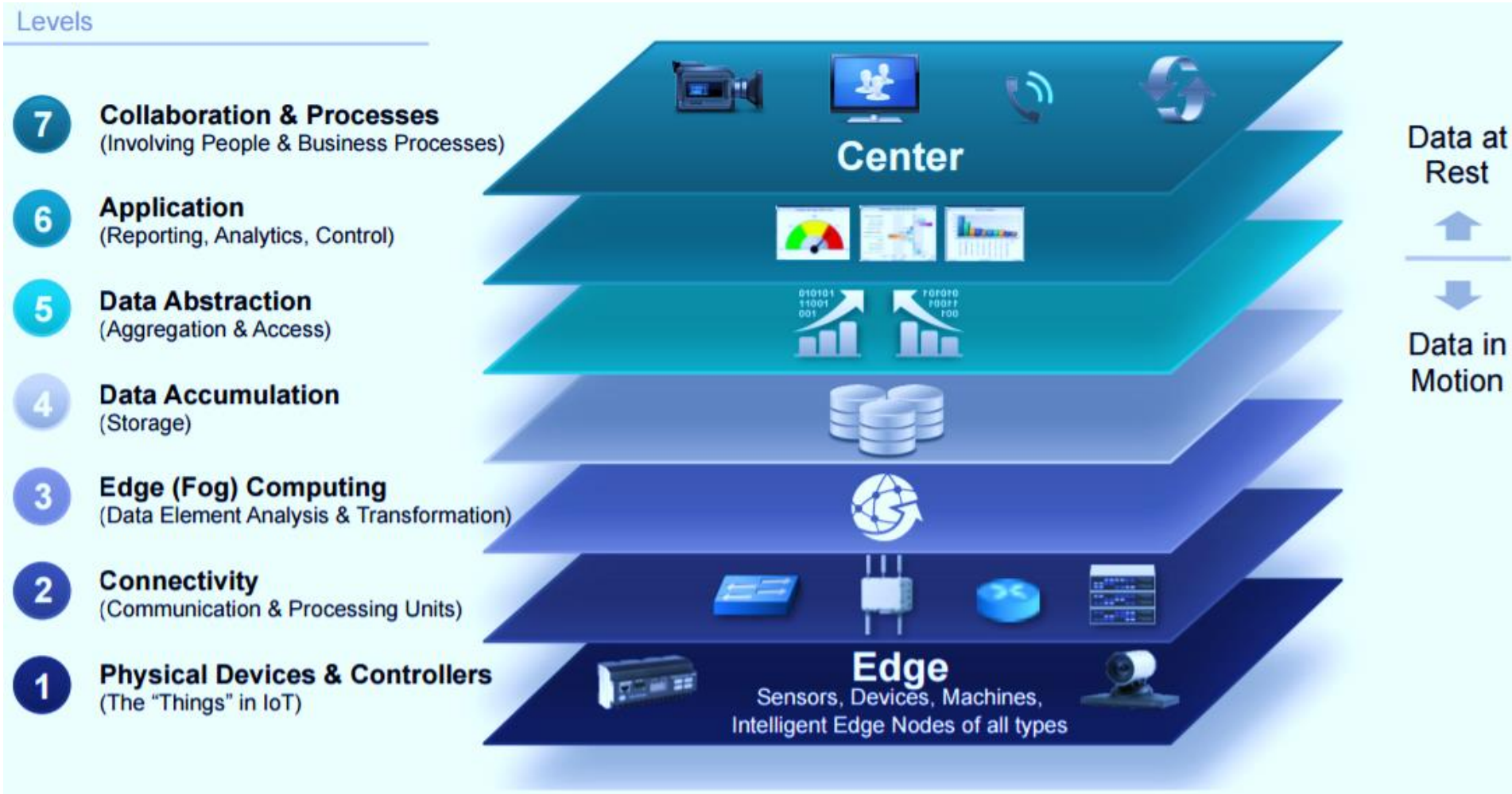


Intelligence

Interconnection

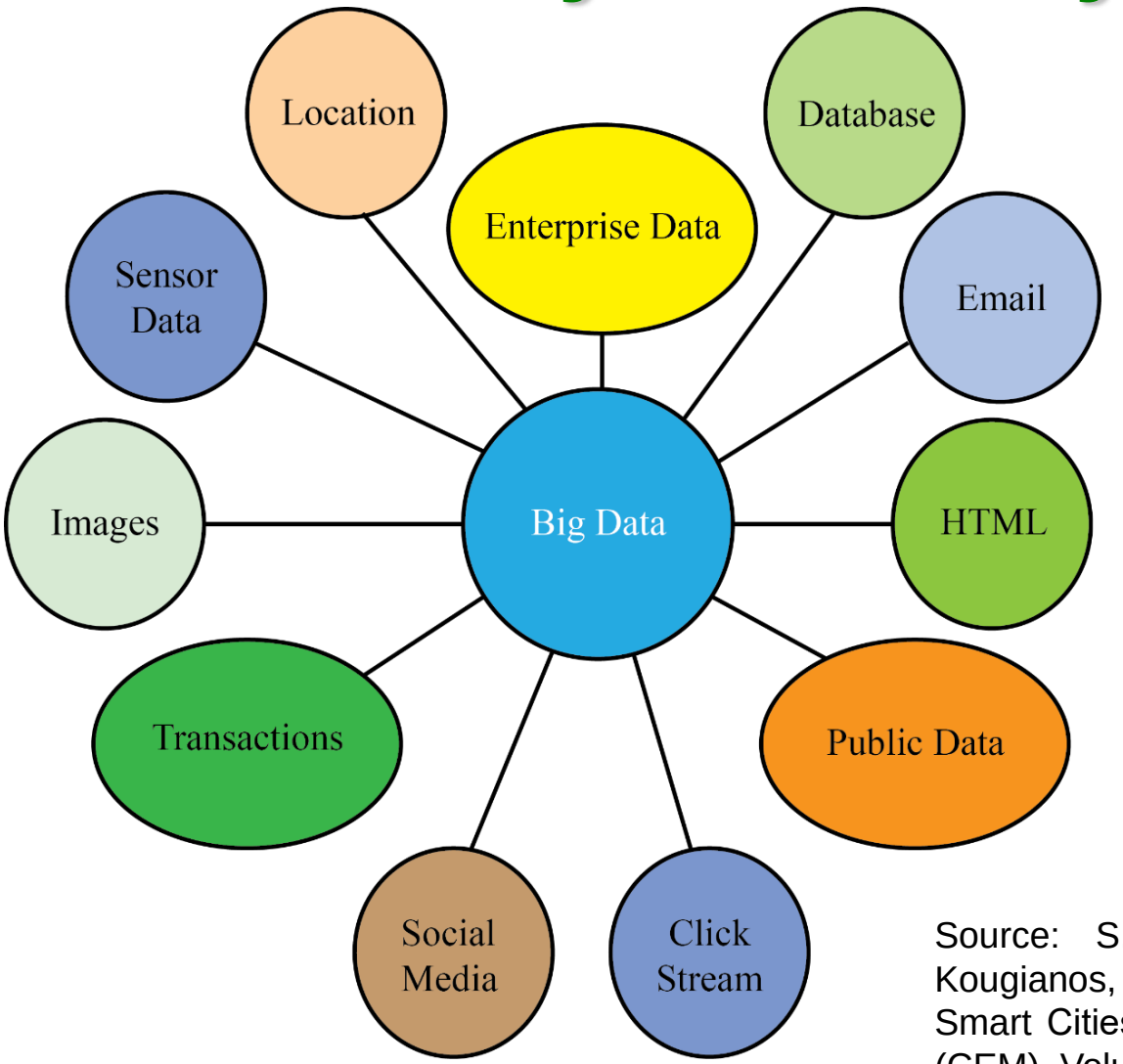
Source: Mohanty EuroSimE 2016 Keynote Presentation

IoT Architecture - 7 Level Model



Source: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

Data Analytics is Key to be Smart



Sensors, social networks, web pages, image and video applications, and mobile devices generate more than 2.5 quintillion bytes data per day.

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

Artificial Intelligence Technology

Source: http://transmitter.ieee.org/impact-aimachine-learning-iot-various-industries/

Machine Learning

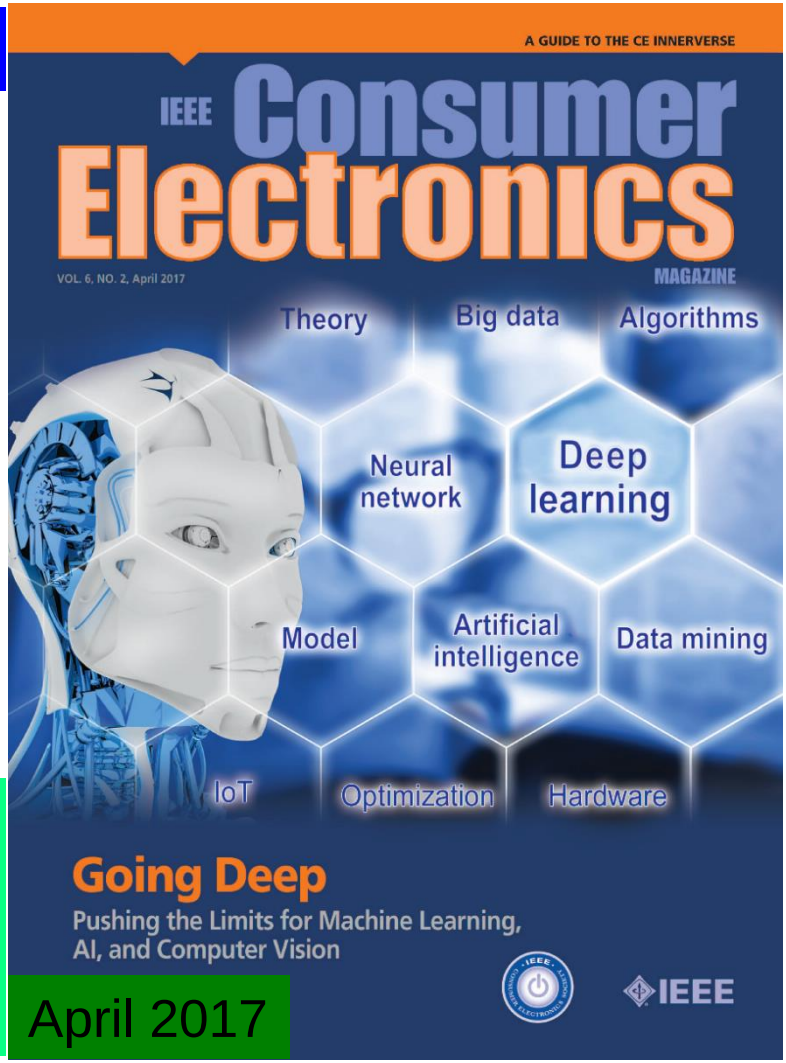
Deep Learning

Tensor Processing Unit (TPU)

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/

Smart City Use:

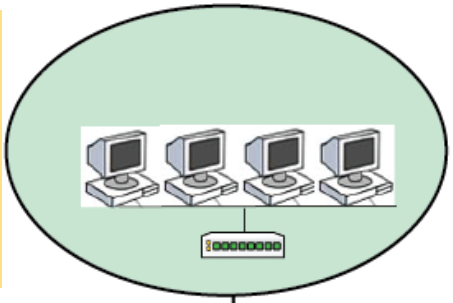
- Better analytics
- Better decision
- Faster response



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

Energy Consumption in IoT

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



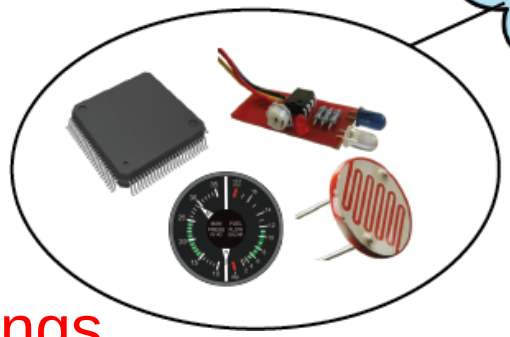
Local Area Network (LAN)

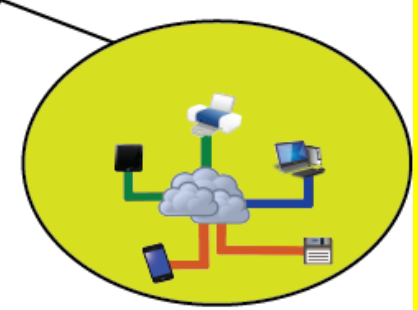
Energy from Supply/Battery - Energy consumed by Communications

Battery Operated - Energy consumed by Sensors, Actuators, Microcontrollers

Internet

The Cloud





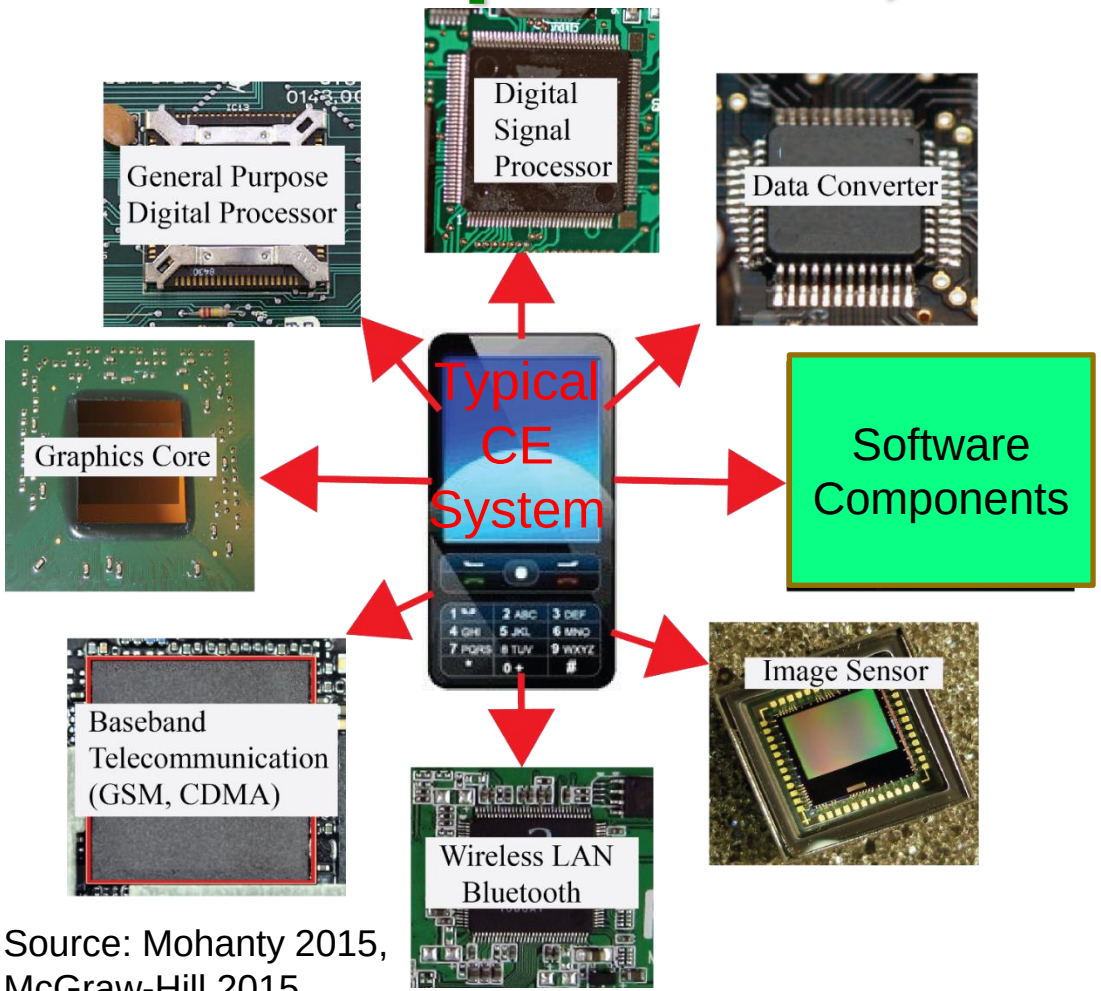
Energy from Supply - Energy consumed in Server, Storage, Software, Communications

The Things

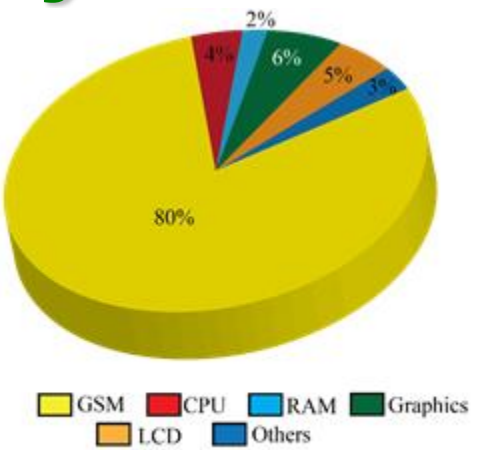
Four Main Components of IoT.

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

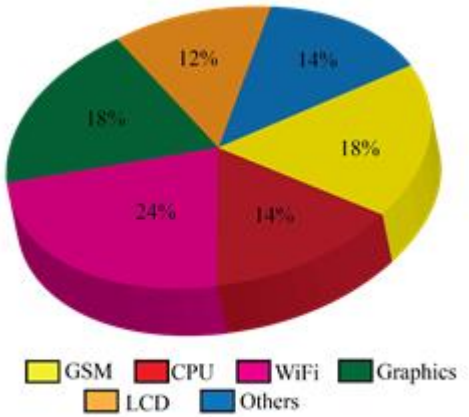
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015



During GSM Communications



During WiFi Communications

Energy Consumption and Latency in Communications

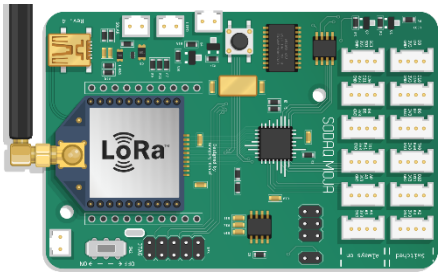
- IoT with Cloud: Sensor big data goes to cloud for storage and analytics – Consumes significant energy in communications network
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Lower power
- 5G for connected world: Enables all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

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

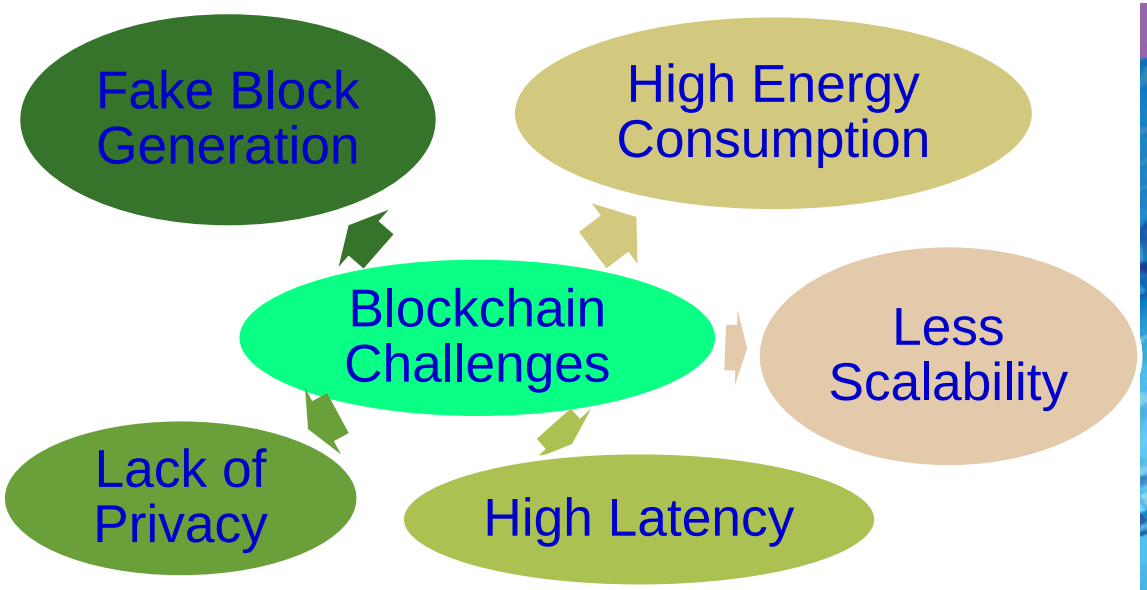
Communications – Energy and Data, Range Tradeoffs

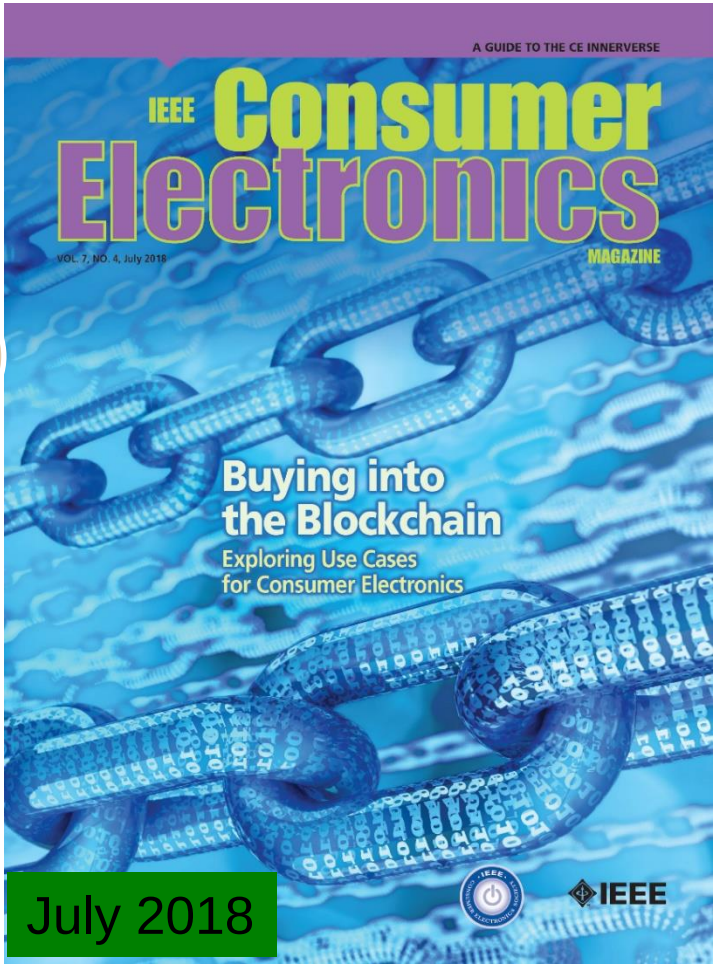
- LoRa: Long Range, low-powered, low-bandwidth, IoT communications as compared to 5G or Bluetooth.
- SigFox: SigFox utilizes an ultra-narrowband wide-reaching signal that can pass through solid objects.

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 - Challenges

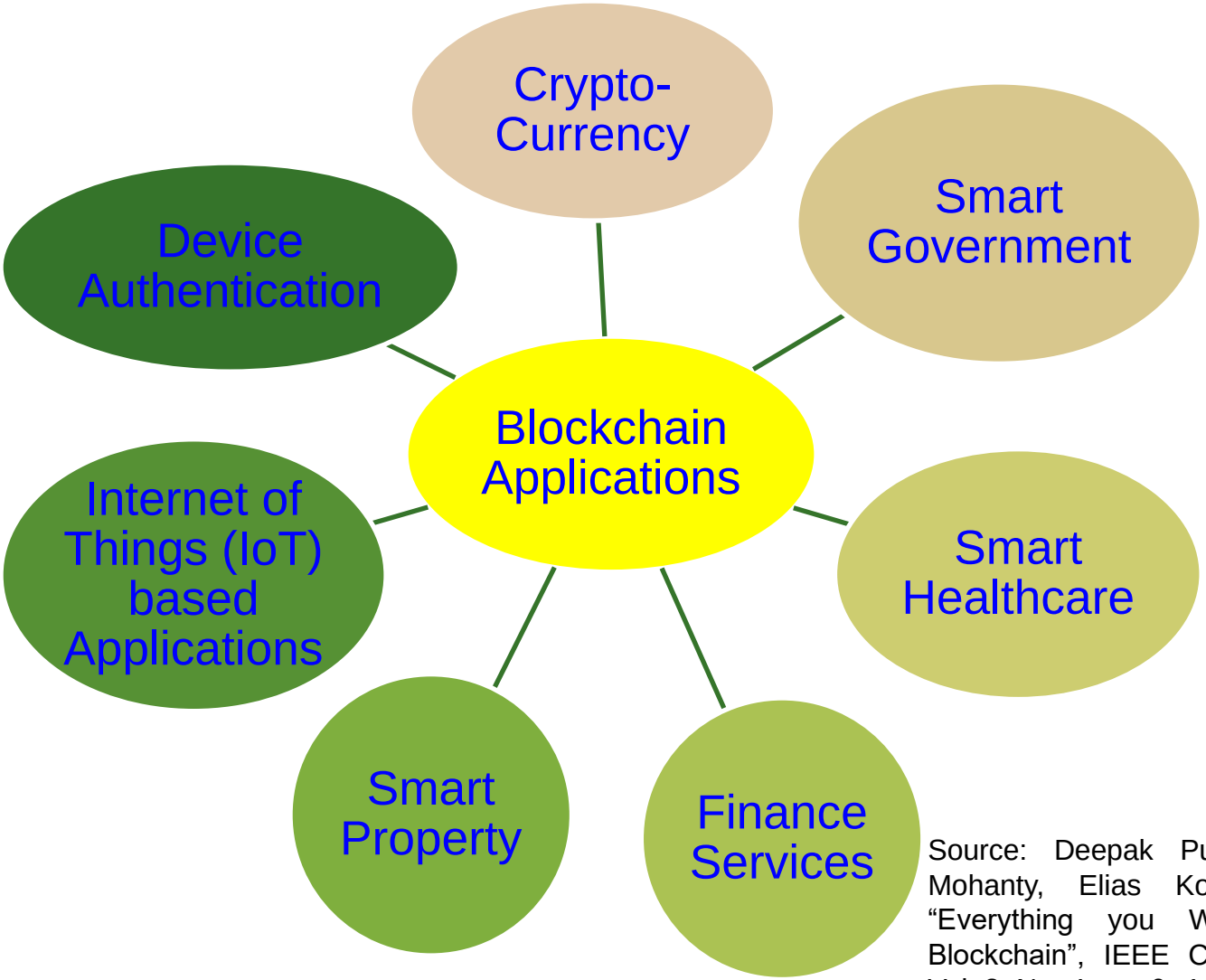




- Energy for mining of 1 bitcoin → 2 years consumption of a US household.
- Energy consumption for each bitcoin transaction → 80,000X of energy consumption of a credit card processing.

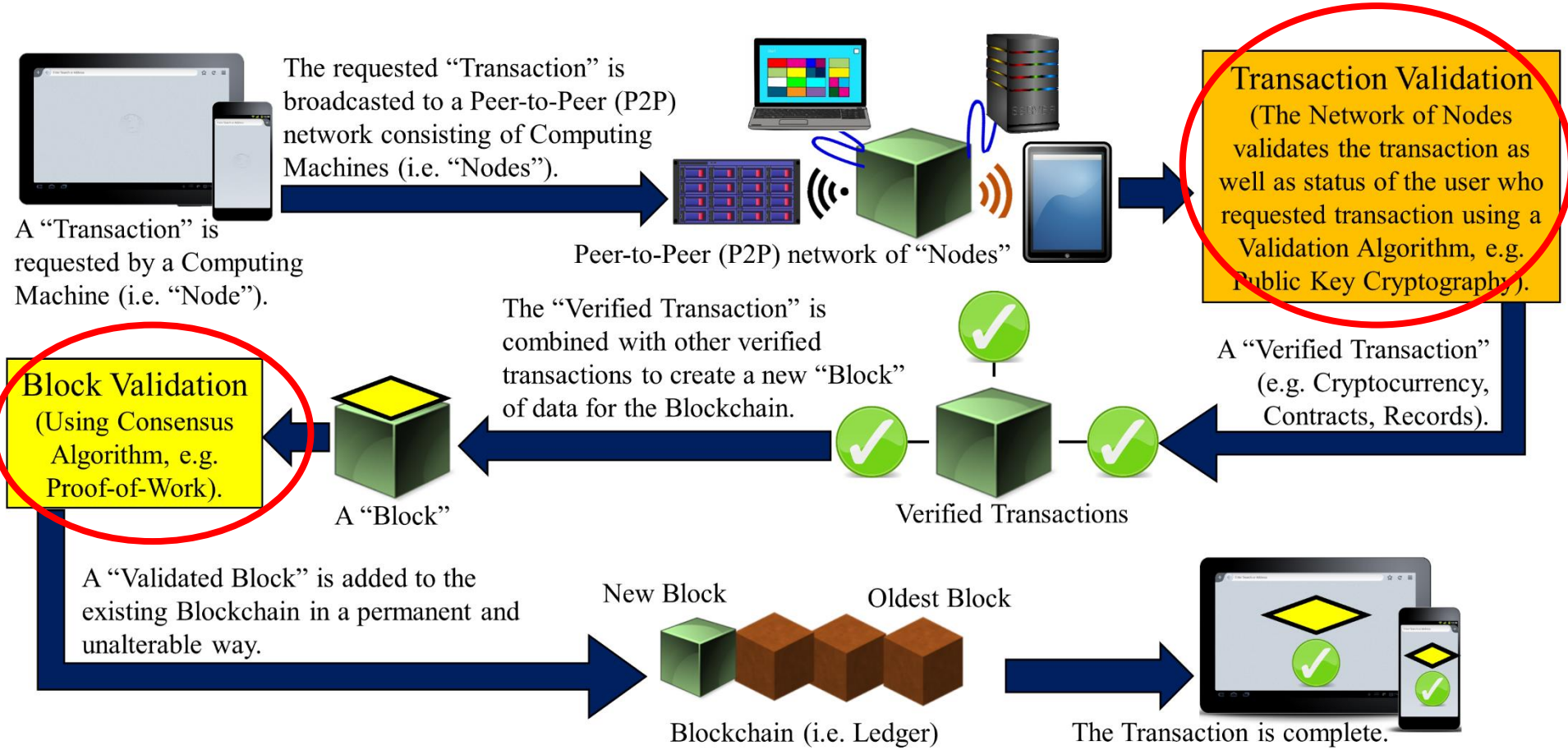
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Blockchain Applications



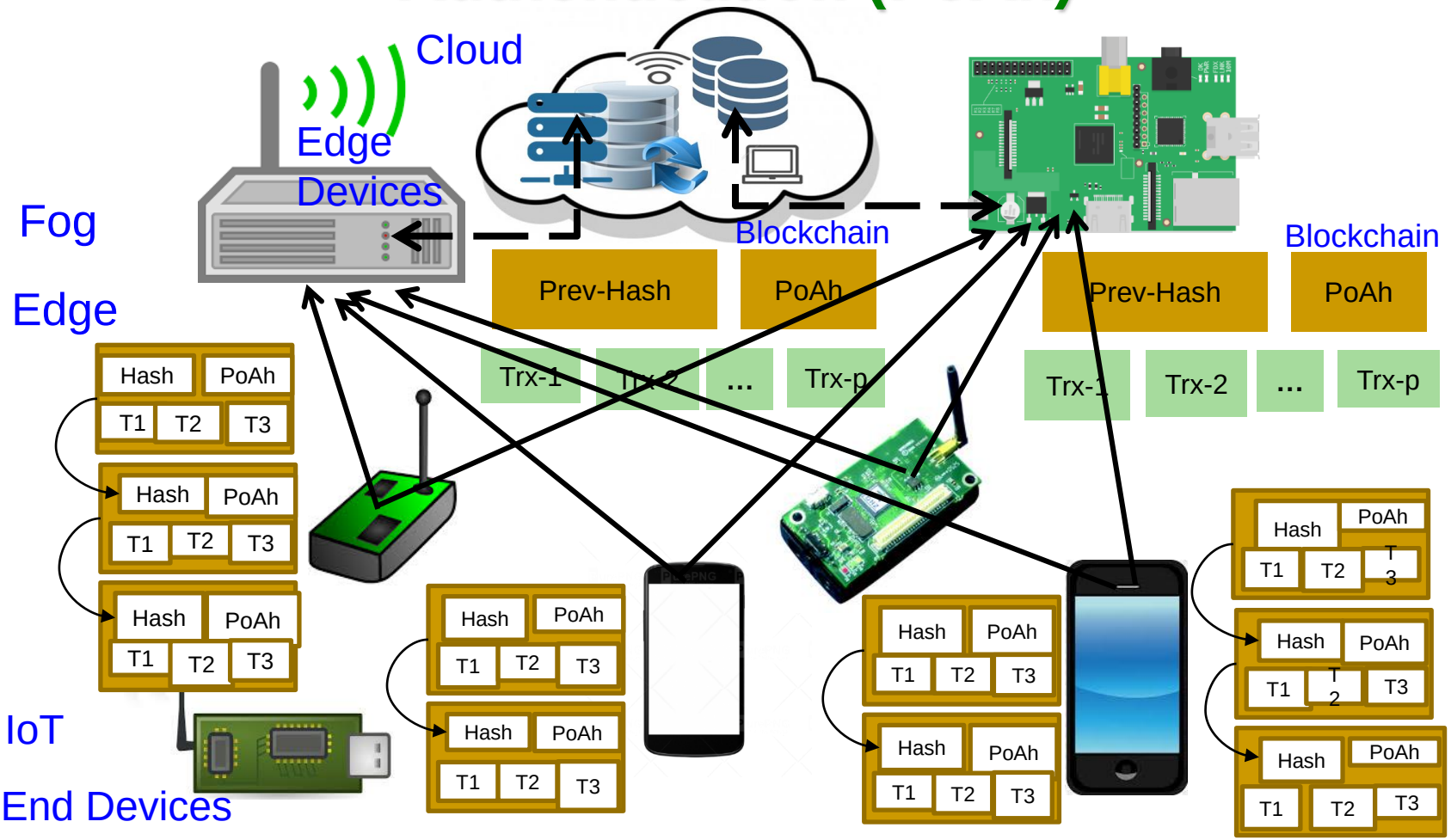
Source: Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das, "Everything you Wanted to Know about the Blockchain", IEEE Consumer Electronics Magazine, Vol. 8, No. 4, pp. 6--14, 2018.

Blockchain Technology



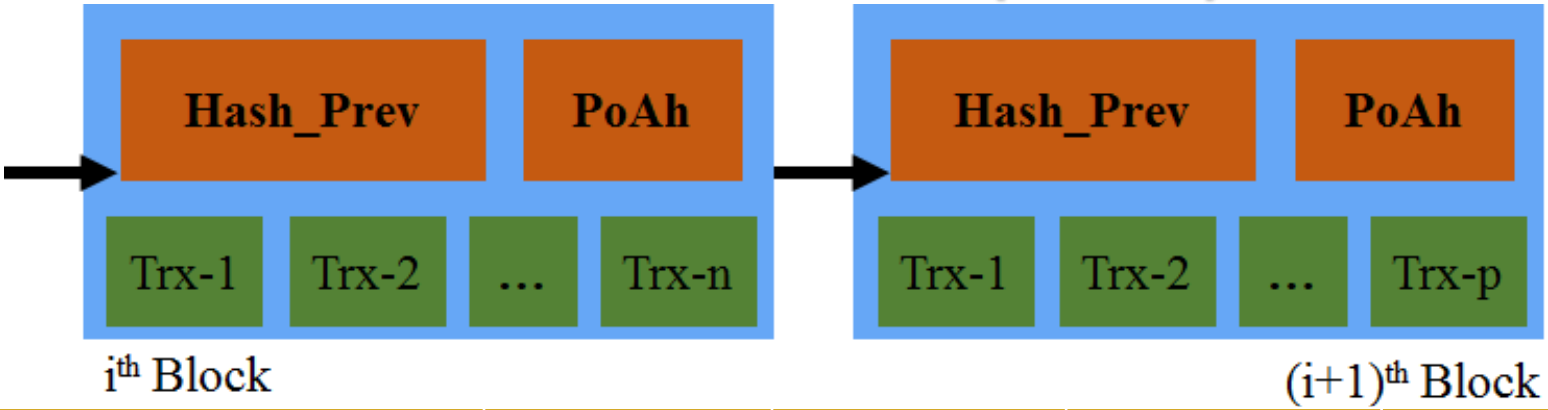
Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

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



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

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

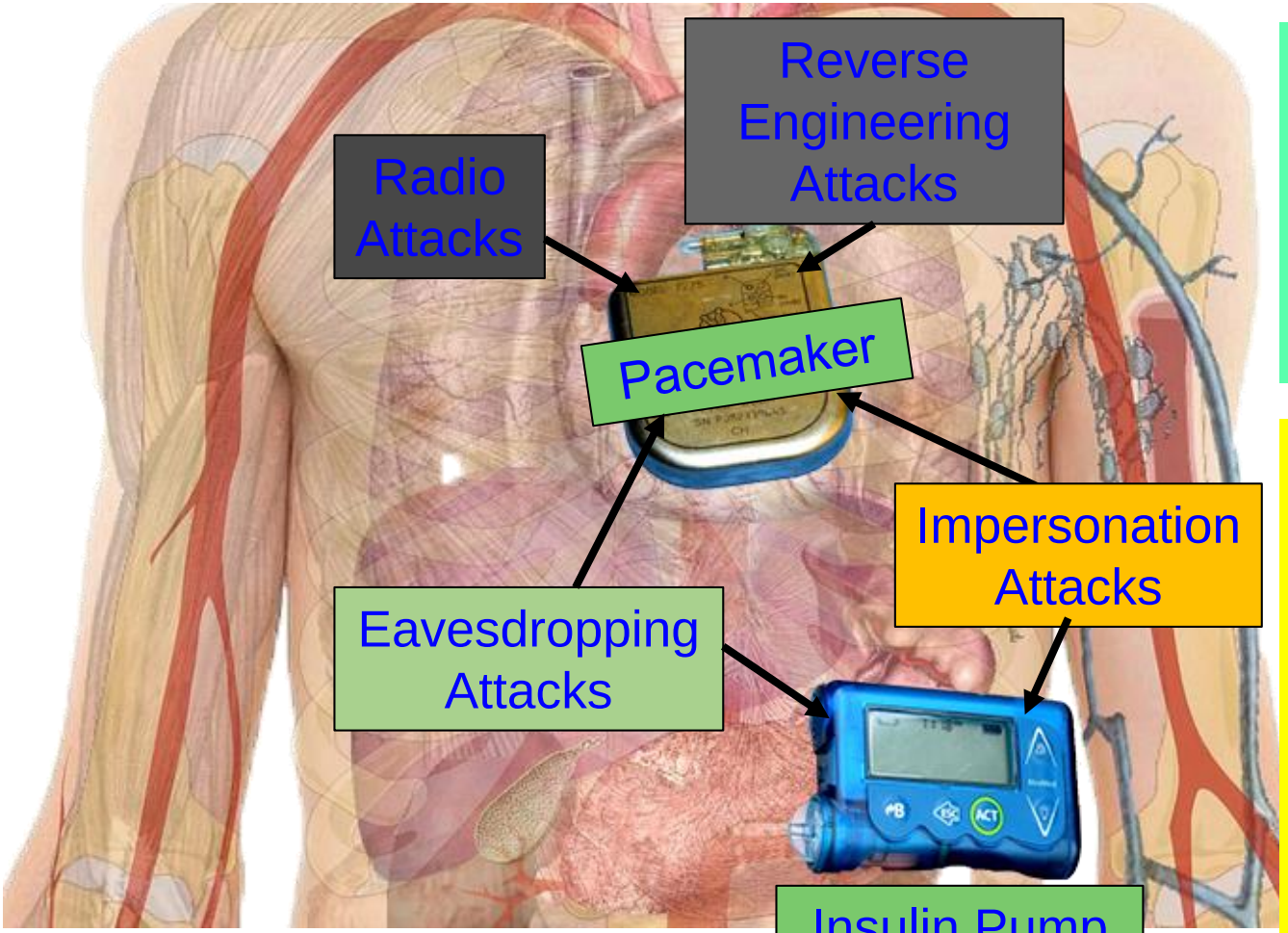


	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

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

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

Security Measures in Smart Devices – Smart Healthcare



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

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

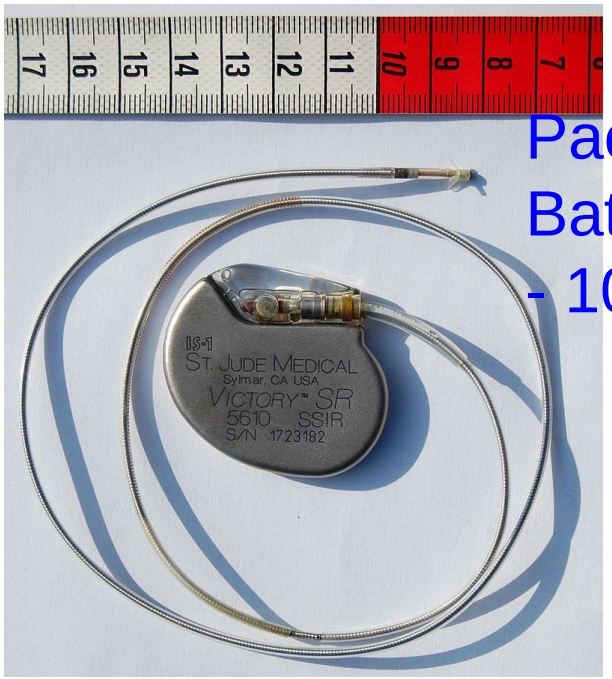
Source: Mohanty Keynote ICCE 2019

Implanted 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 - Energy Constrained



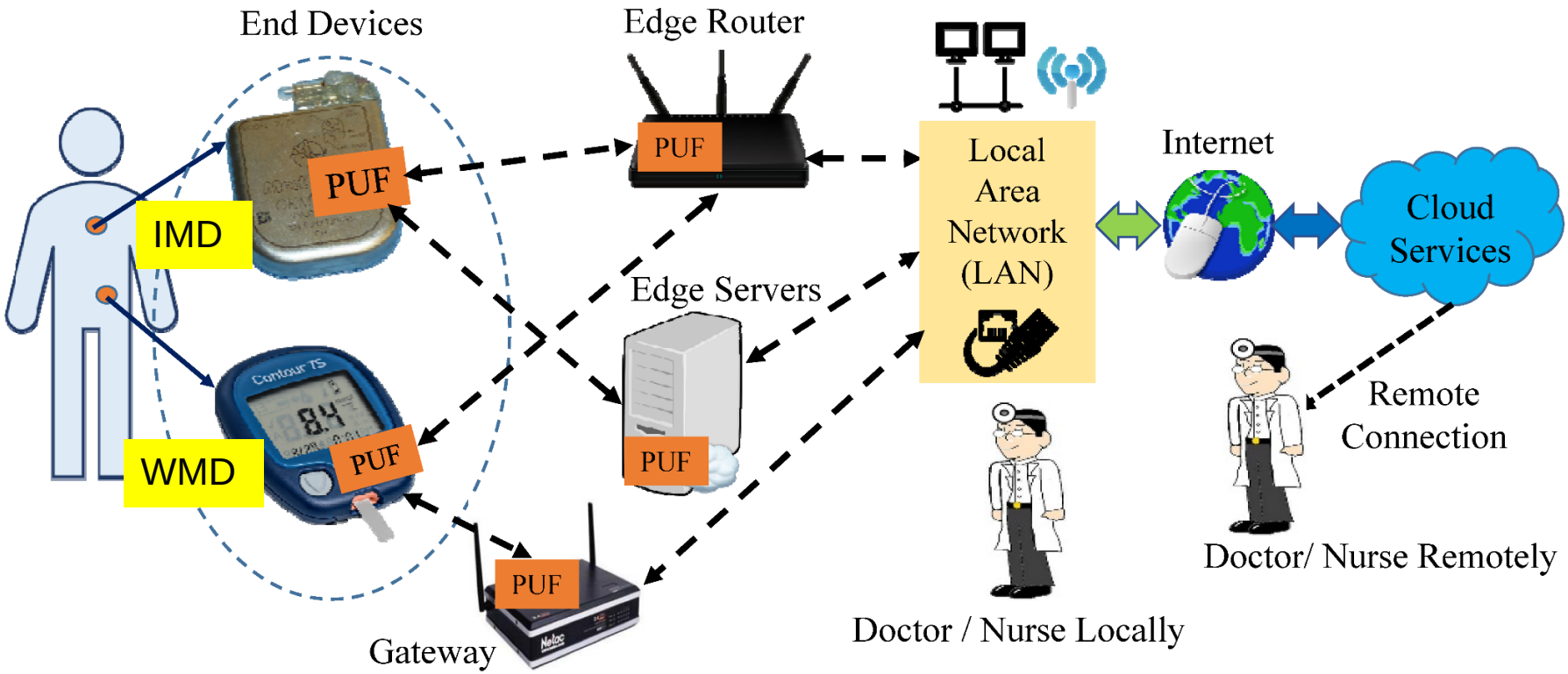
Pacemaker
Battery Life
- 10 years

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

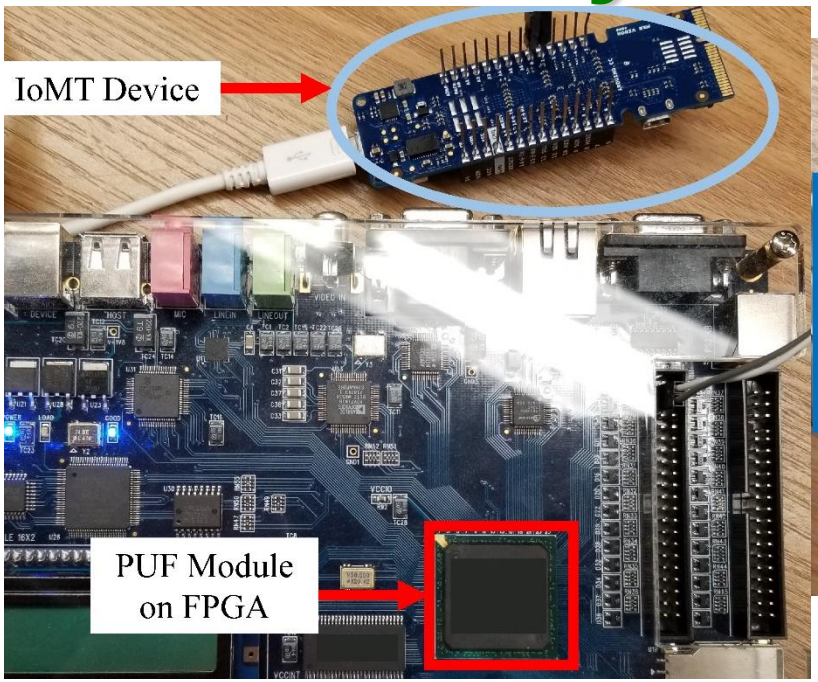
Source: Carmen Camara, PedroPeris-Lopeza, and Juan E.Tapiadora, "ecurity and privacy issues in implantable medical devices: A comprehensive survey", Elsevier Journal of Biomedical Informatics, Volume 55, June 2015, Pages 272-289.

IoMT Security - PUF based Device Authentication



Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume XX, Issue YY, ZZ 2019, pp. Accepted on 28 June 2019, DOI: 10.1109/TCE.2019.2926192.

IoMT Security - PUF based Device Authentication



Average Power Overhead – ~ 200 μW

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

Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", IEEE Transactions on Consumer Electronics (TCE), Volume XX, Issue YY, ZZ 2019, pp. Accepted on 28 June 2019, DOI: 10.1109/TCE.2019.2926192.

Smart Car Security - Latency Constrained

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

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

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

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

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

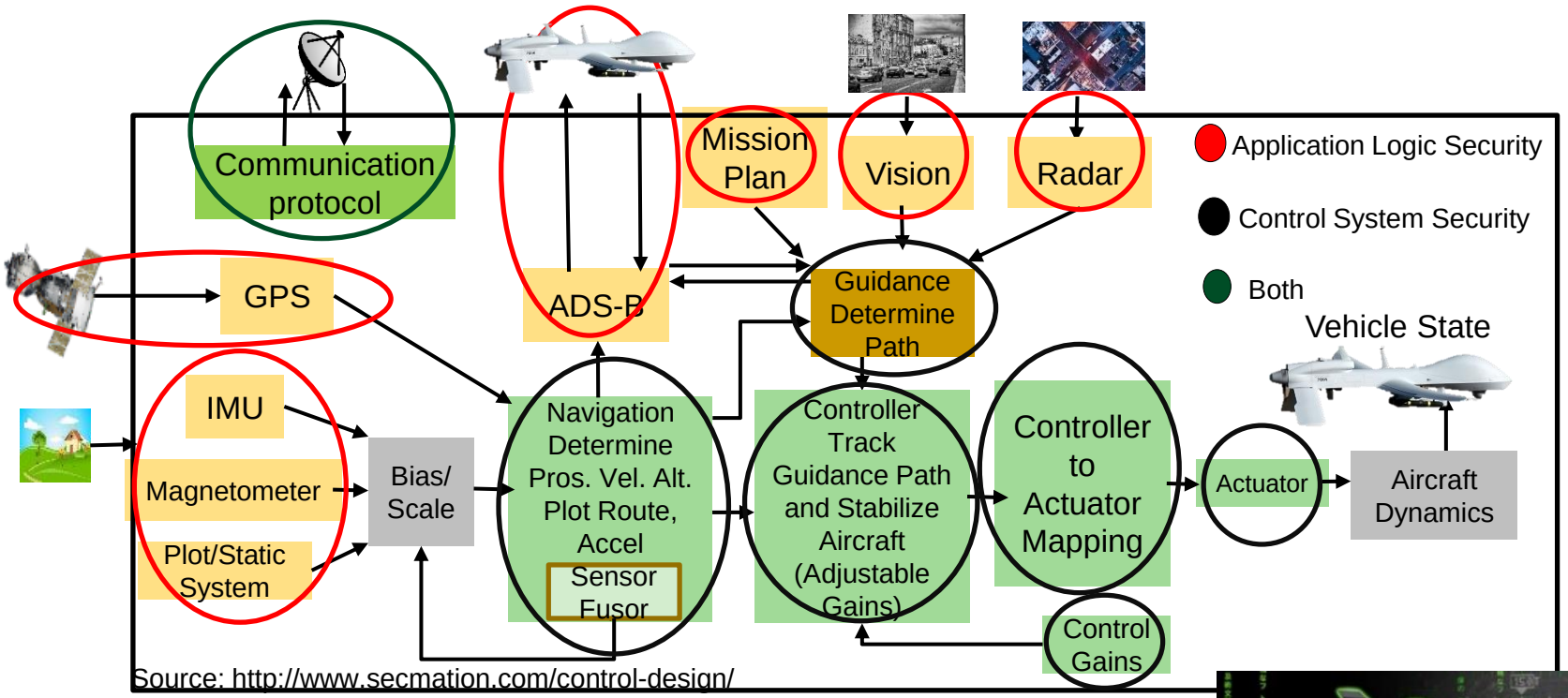
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Security – Latency Constraints

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

UAV Security - Energy & Latency Constrained



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

Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

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

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

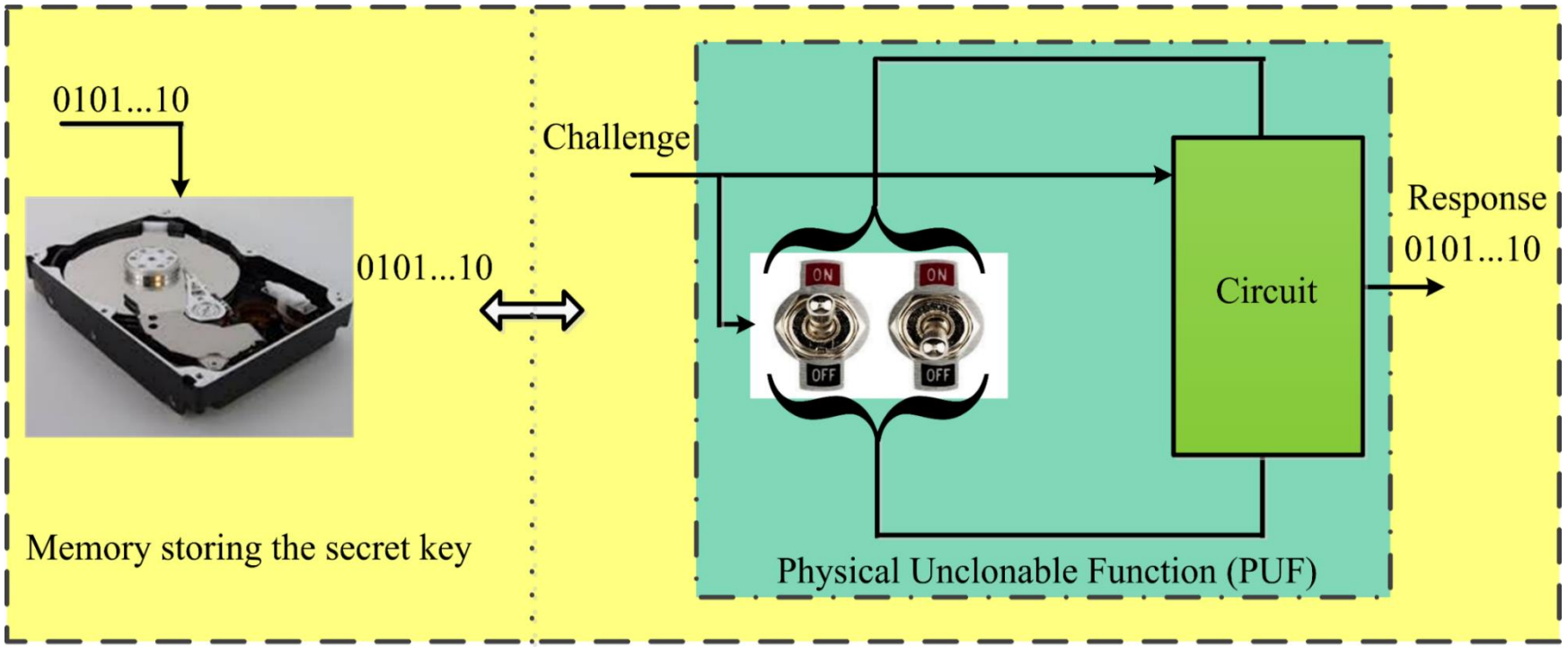
IR Hardware Security | Memory Protection | Digital Core IP Protection

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.

Security Primitives - PUF



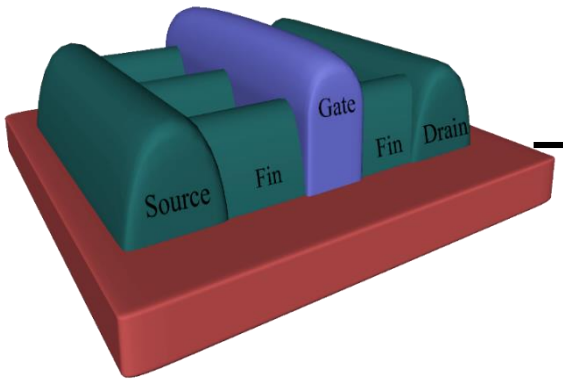
PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

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

Physical Unclonable Function (PUF) - Principle

Manufacturing Variations (e.g. Oxide Growth, Ion Implantation, Lithography)

Challenge Inputs (Inputs given to PUF Module, e.g. Select line of Multiplexer)



Parameters Affected Due to Variations (e.g. Length, Gate-Oxide Thickness, Fin Height, Fin Width)

PUF Design (e.g. Arbiter PUF, SRAM PUF, Ring Oscillator PUF)

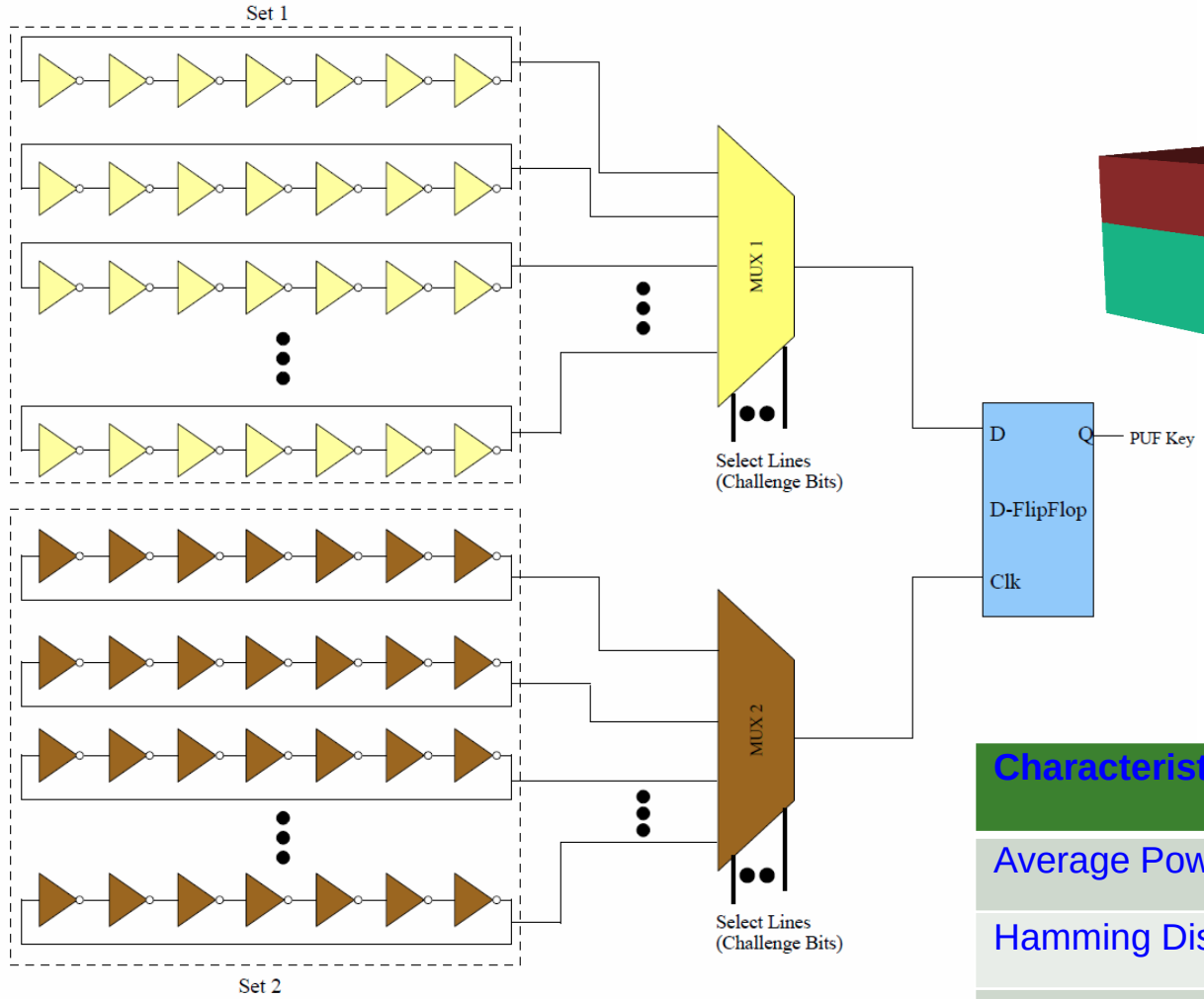
Challenge Response (Outputs from a PUF Module)

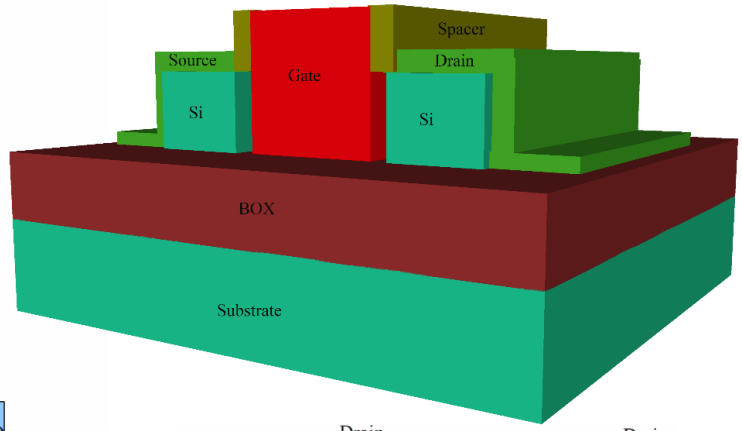
Random Binary Output 010101 …

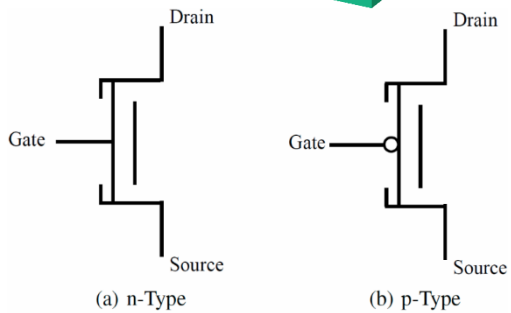
Silicon manufacturing process variations are turned into a feature rather than a problem.

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, Springer Analog Integrated Circuits and Signal Processing Journal, Volume 93, Issue 3, December 2017, pp. 429--441.

Power Optimized Hybrid Oscillator Arbiter PUF



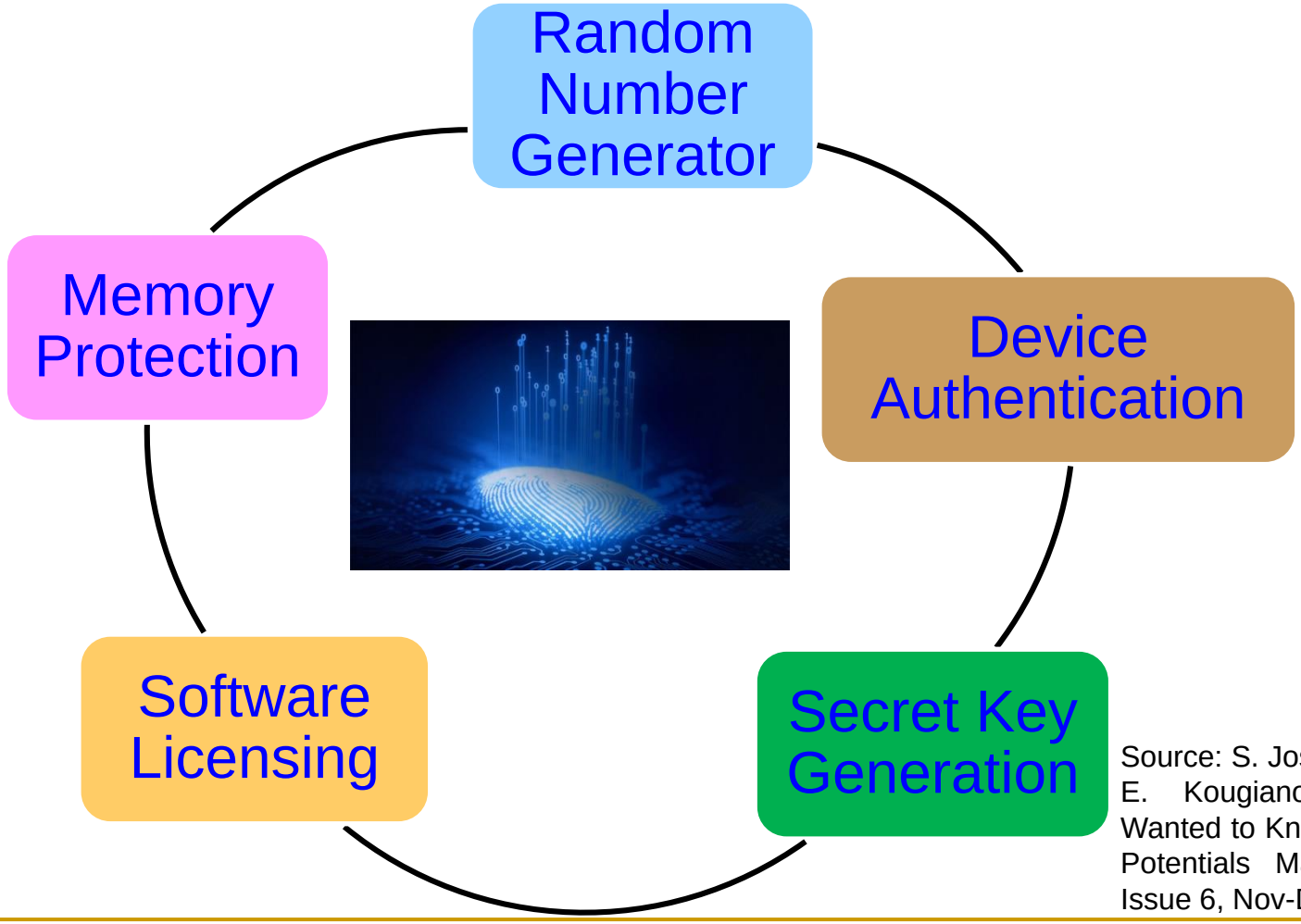




Characteristics	FinFET Technology	DLFET Technology
Average Power	219.34 μW	121.3 μW
Hamming Distance	49.3 %	48 %
Time to generate key	150 ns	150 ns

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, IEEE Transactions on Semiconductor Manufacturing (TSM), Volume 31, Issue 2, May 2018, pp. 285--294.

Physical Unclonable Functions (PUFs) - Applications



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

CE/IoT System - Multi-Objective Tradeoffs

Non-recurring Design Cost

Recurring Operational Cost

Energy Consumption, Battery Life

Safety

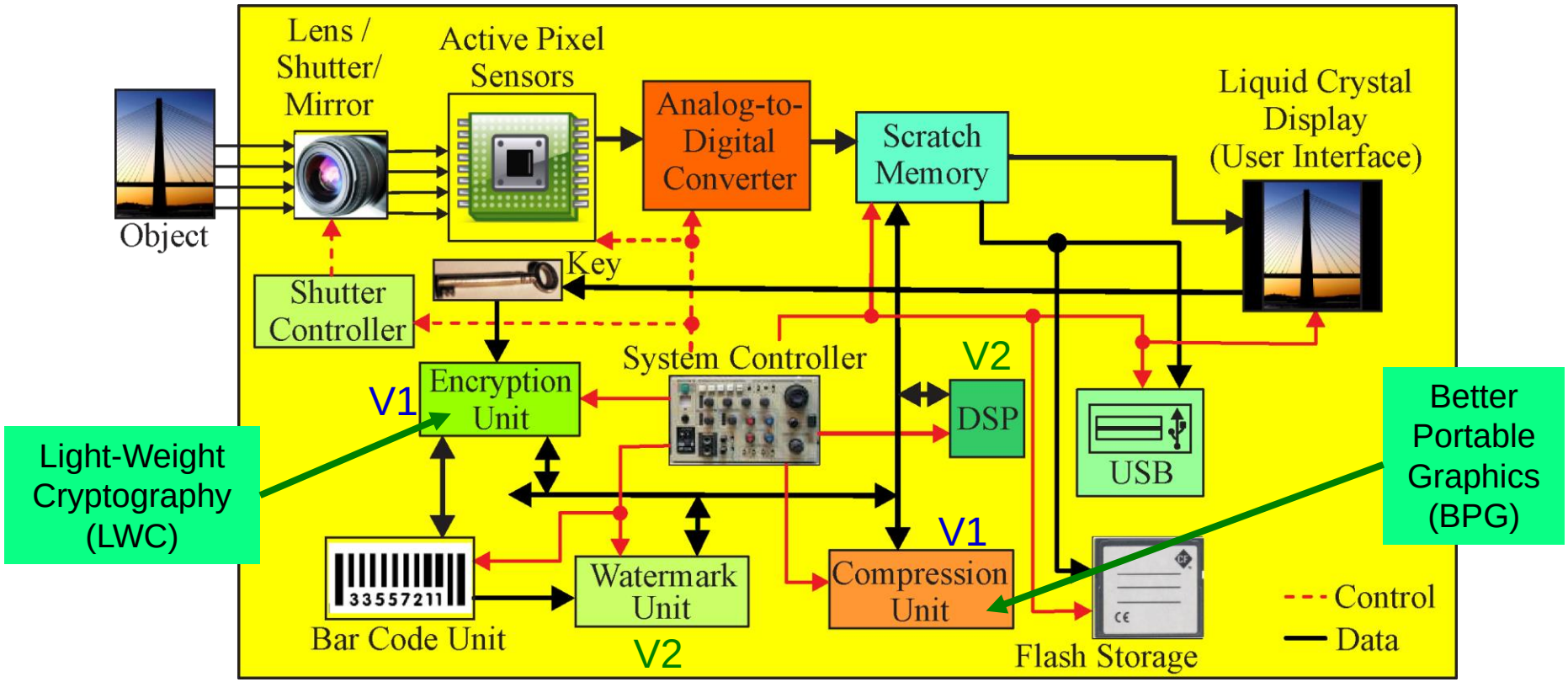
Security, Privacy, IP Rights

Performance, Latency

Intelligence

Source: Mohanty ICCE 2019 Keynote

ESR-Smart – End-Device Optimization



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

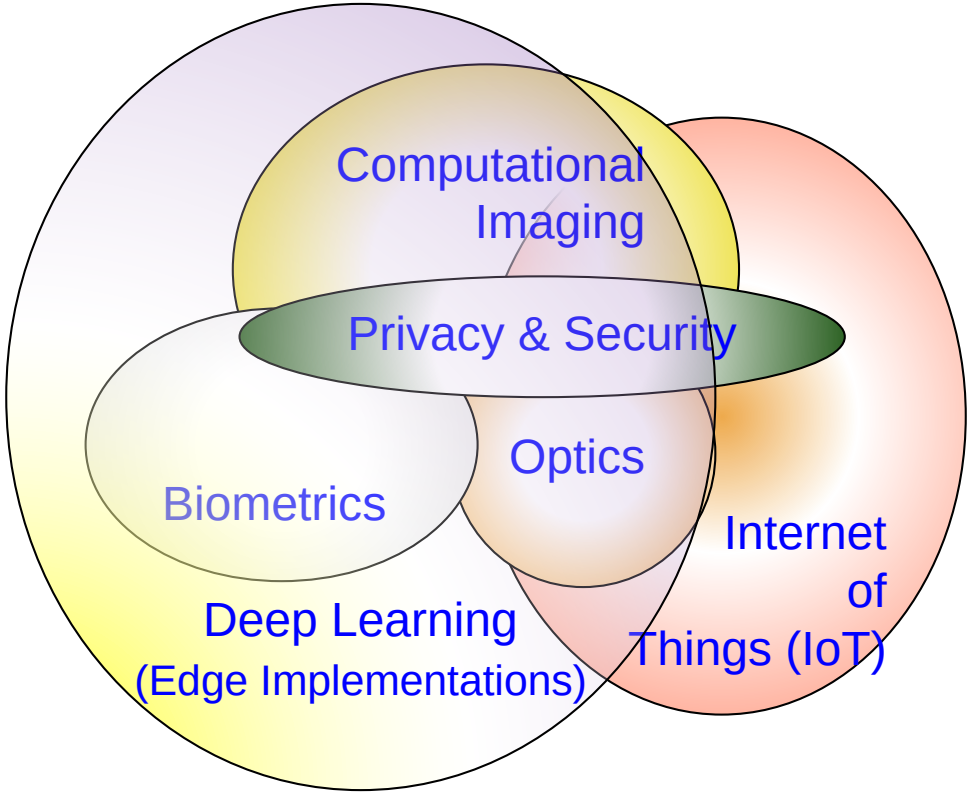
Source: S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", Elsevier Journal of Systems Architecture (JSA), Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

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

Challenges in Making Smart

Deep Learning is the Key

- "DL at the Edge" overlaps all of these research areas.
- New Foundation Technologies, enhance data curation, improved AI, and Networks accuracy.

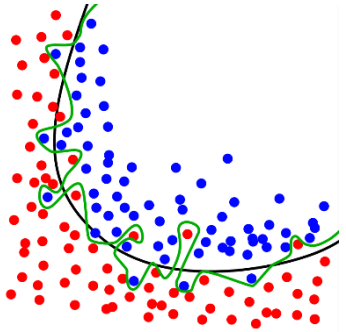


Source: Corcoran Keynote 2018

ML Modeling Issues

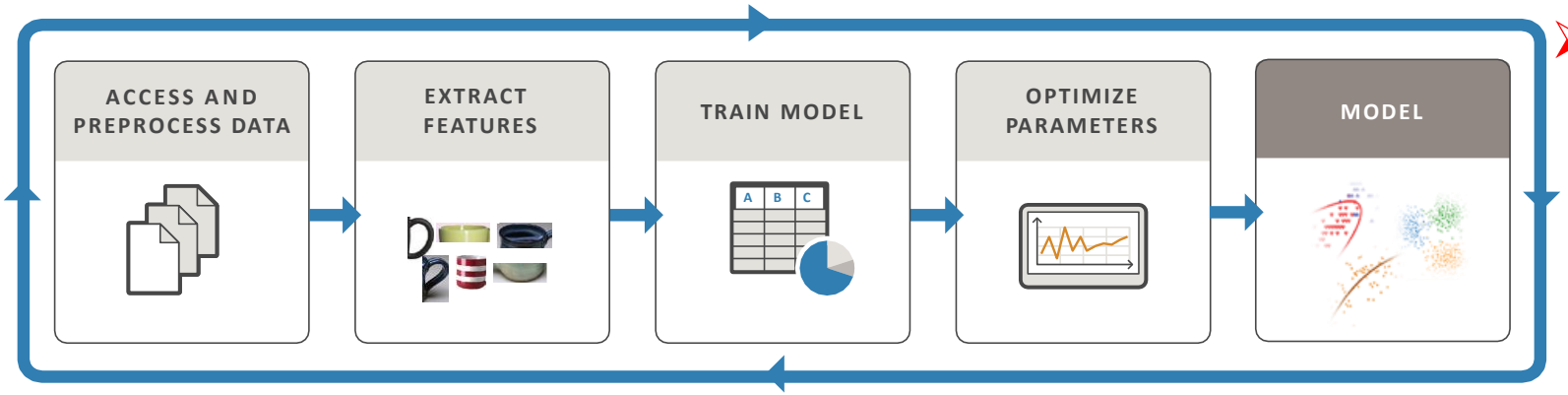
Machine Learning Issues

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



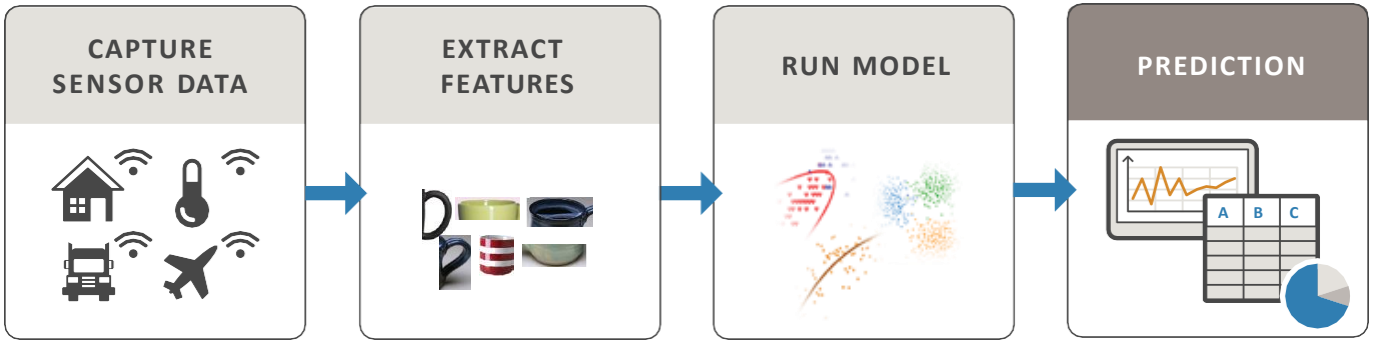
Deep Neural Network (DNN) - Resource and Energy Costs

TRAIN: Iterate until you achieve satisfactory performance.



Needs Significant:
- Resource
- Energy

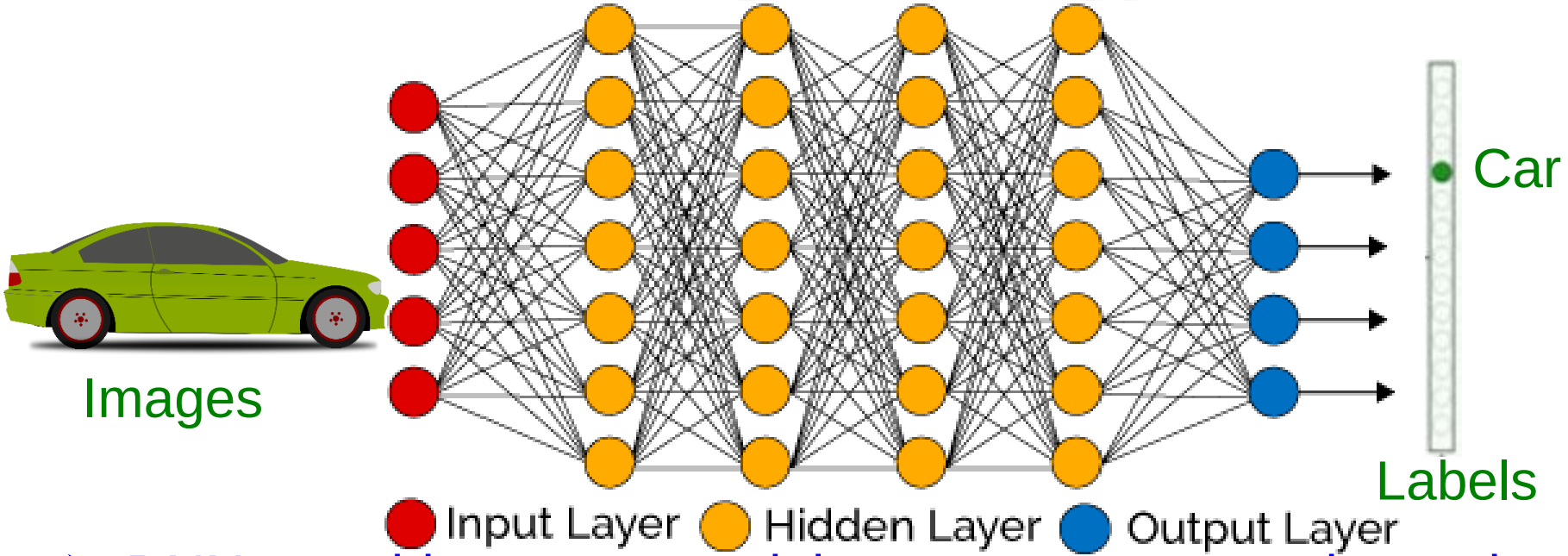
PREDICT: Integrate trained models into applications.



Needs:
- Resource
- Energy

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

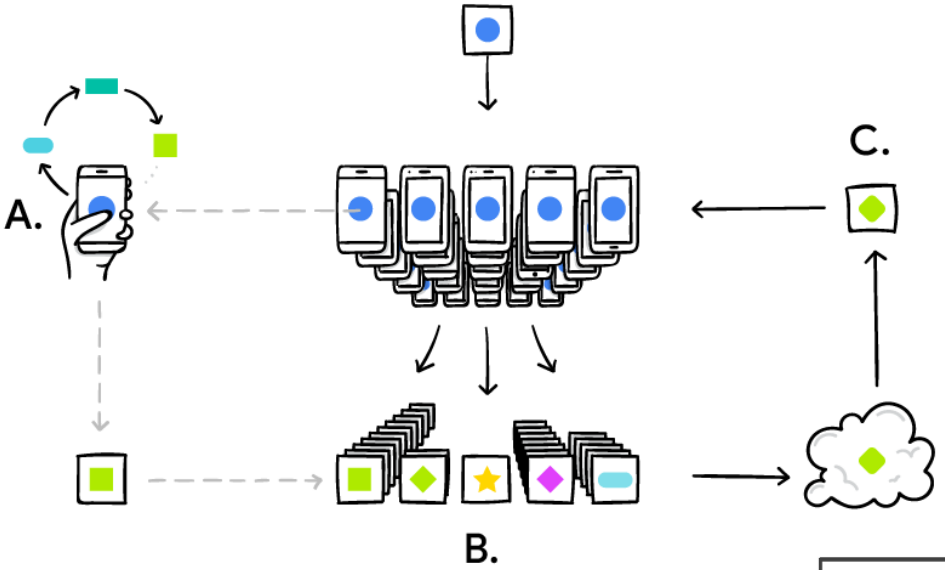
DNN Training - Energy Issue



- 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.

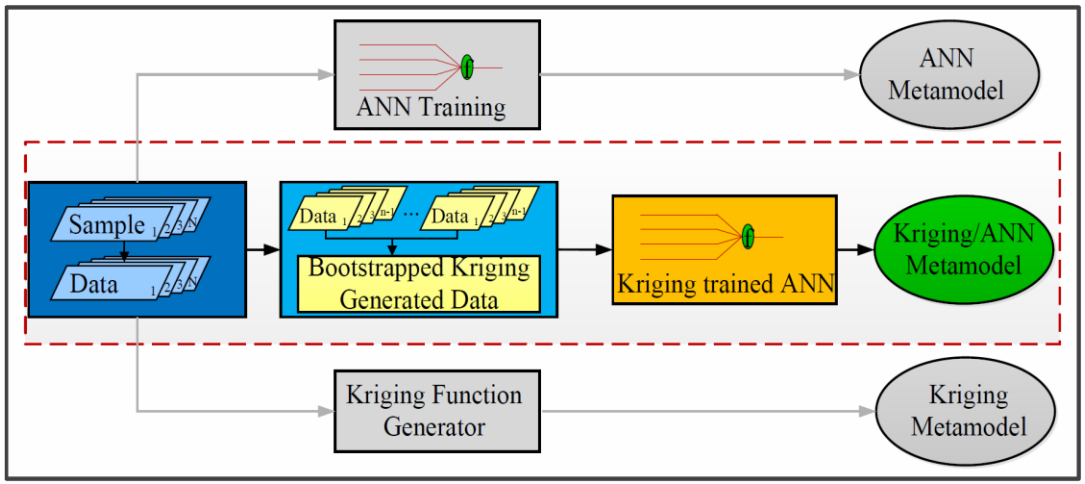
Source: Mohanty iSES 2018 Keynote

Enhancing DNN Training/Learning



Federated Learning (Google) – A type of Distributed Learning

Source: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

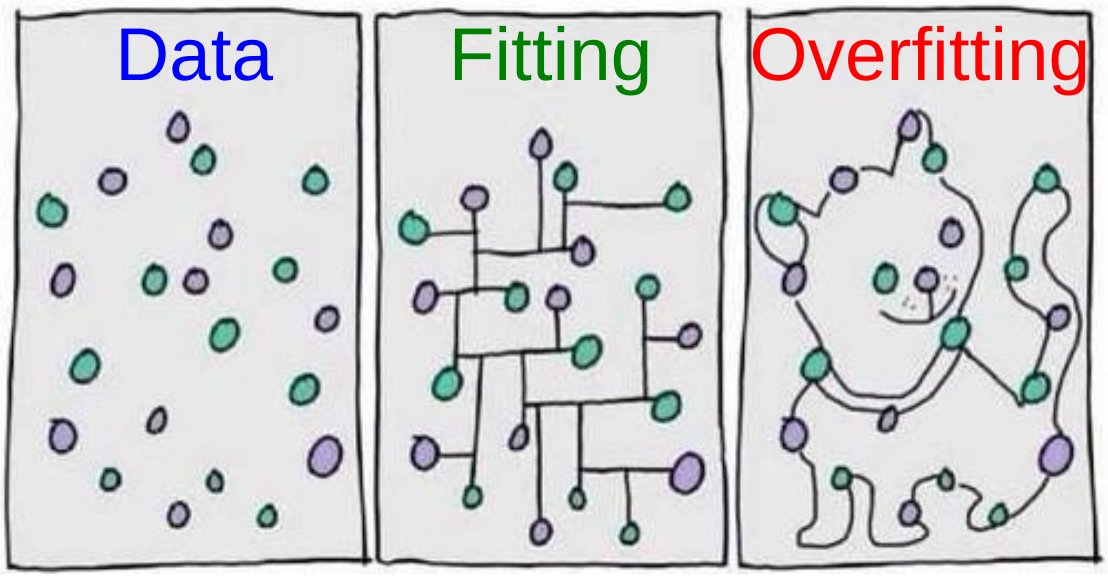


Hierarchical Learning

Source: O. Okobiah, S. P. Mohanty, and E. Kougianos, "Kriging Bootstrapped Neural Network Training for Fast and Accurate Process Variation Analysis", in Proceedings of the 15th ISQED, 2014, pp. 365--372.

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

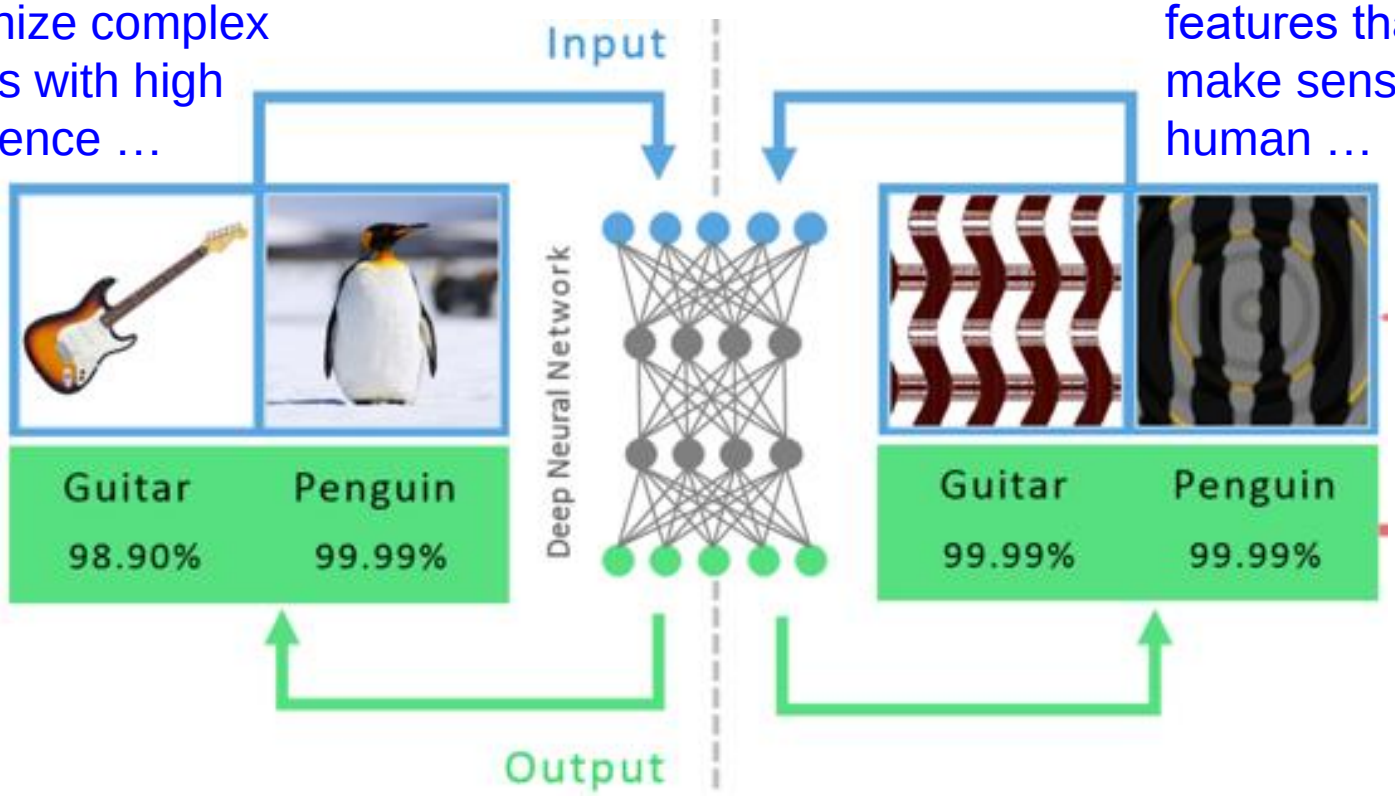
- Class imbalance is a classification problems where the classes are not represented equally.
- Solutions: Use Precision, Recall, F-measure metrics

  Not only RMSE like accuracy metrics

DNNs are not Always Smart

DNNs can learn to recognize complex objects with high confidence …

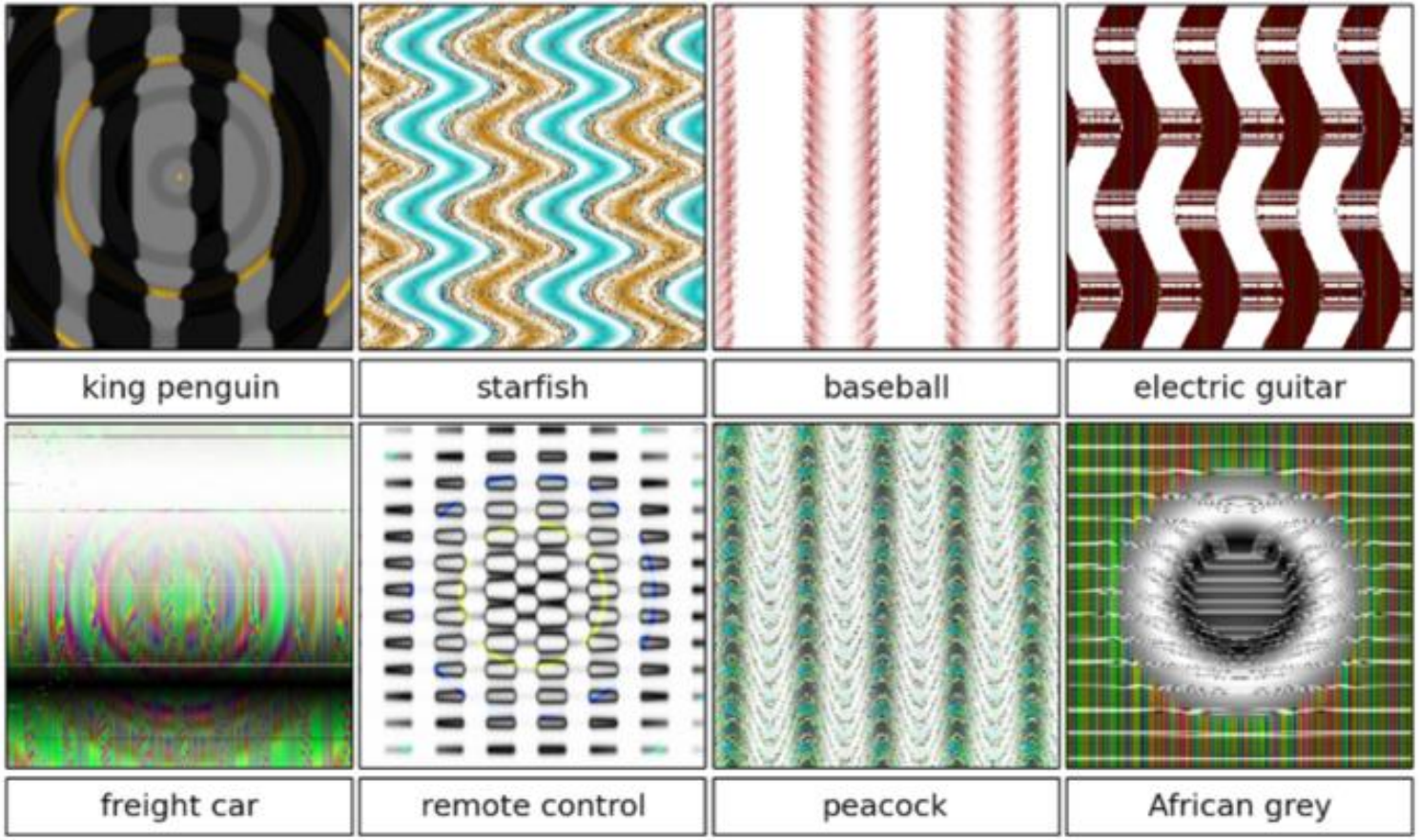
But often they learn features that don't make sense to a human …



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

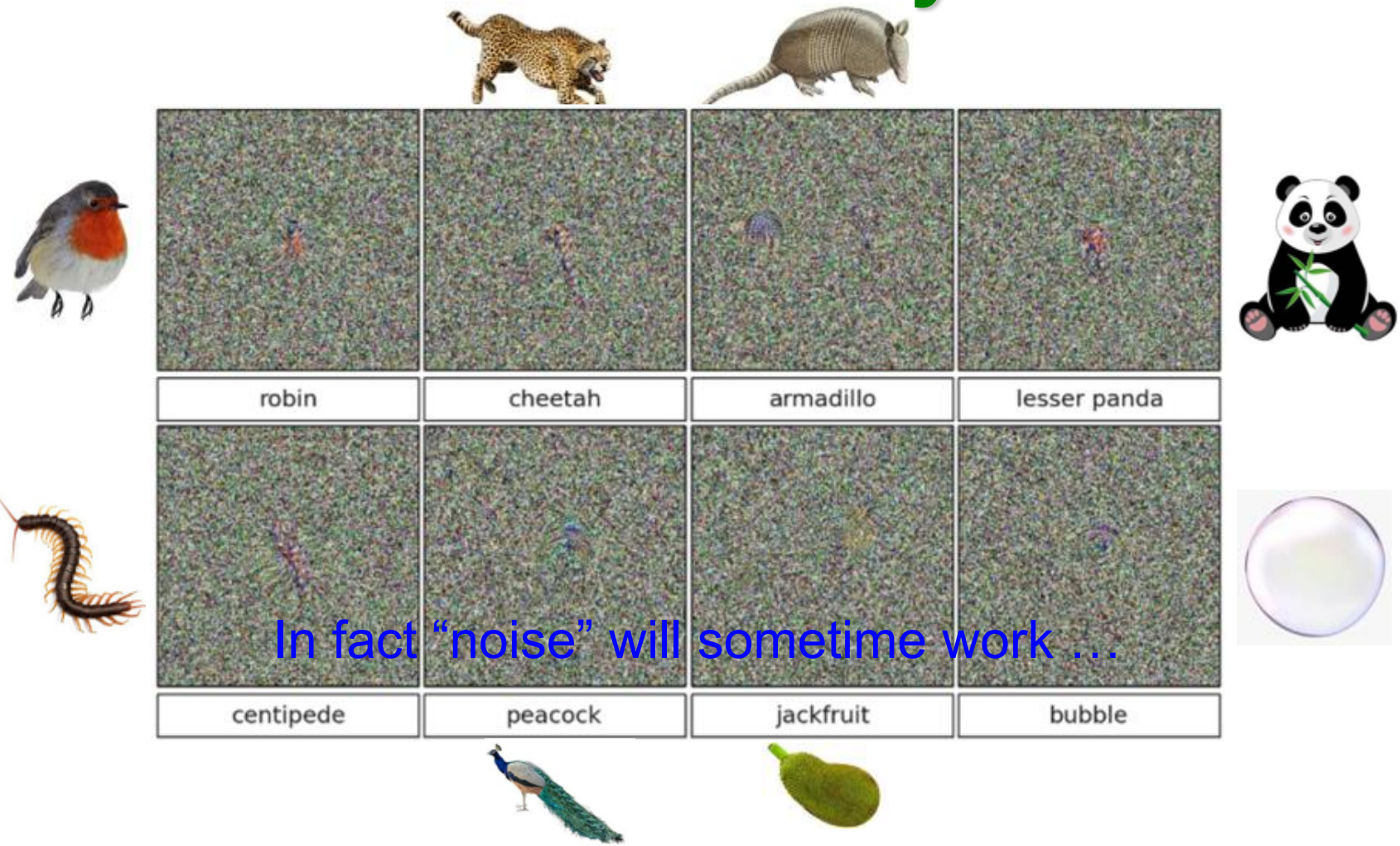


DNNs can be fooled by certain “learned” (Adversarial) patterns …

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

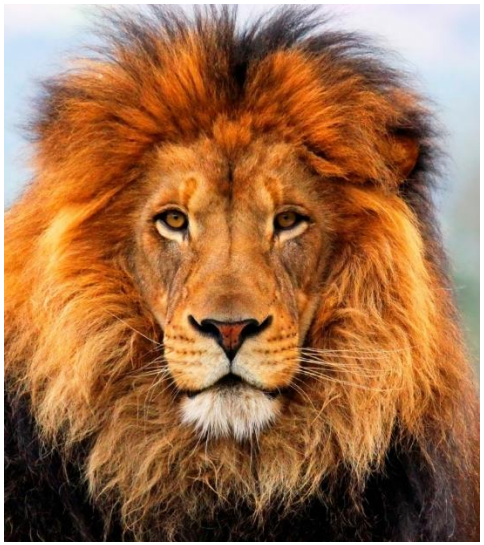


Source: Nguyen, et al. 2014 - Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

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 annotation for big datasets



Source: Corcoran Keynote 2018

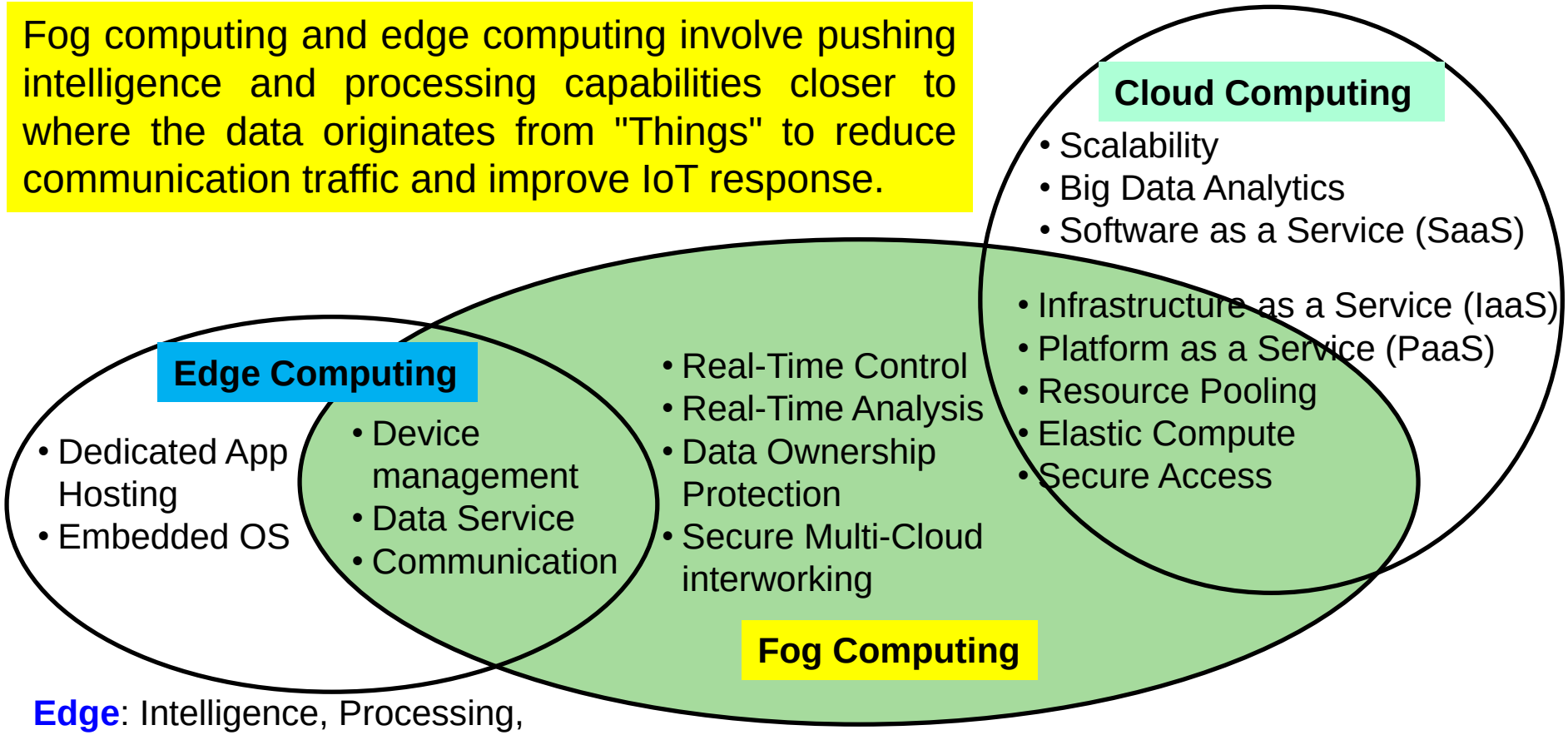
Where and How to Compute?

Sensor, Edge, Fog, Cloud?

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

Fog Vs Edge Vs Cloud Computing

Fog computing and edge computing involve pushing intelligence and processing capabilities closer to where the data originates from "Things" to reduce communication traffic and improve IoT response.



Edge: Intelligence, Processing, and Communication - Devices like Programmable Automation Controllers (PACs)

Fog: Intelligence - LAN, Processing - fog node or IoT gateway.

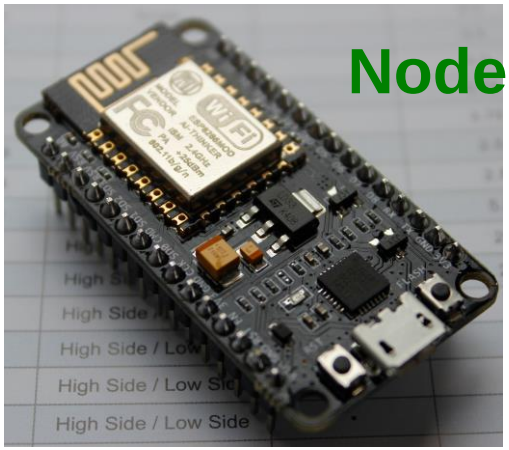
Source: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference

Source: https://www.nebbiolo.tech/wp-content/uploads/whitepaper-fog-vs-edge.pdf

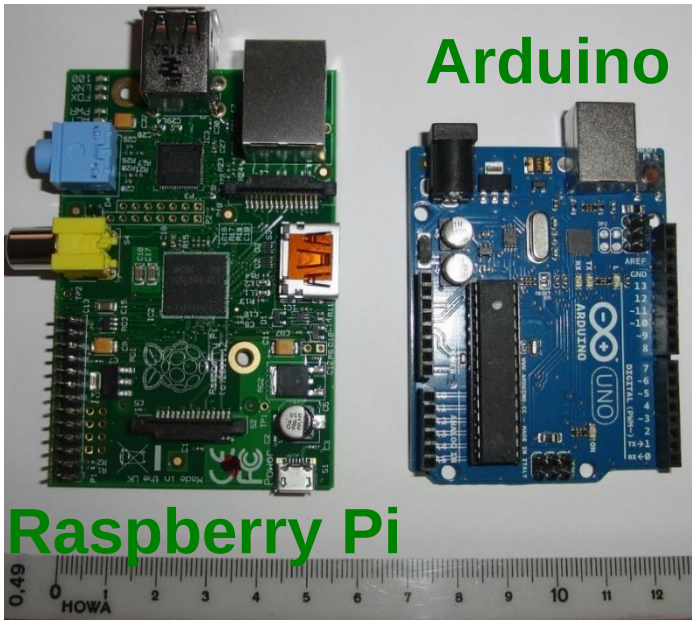
Computing Technology - IoT Platform

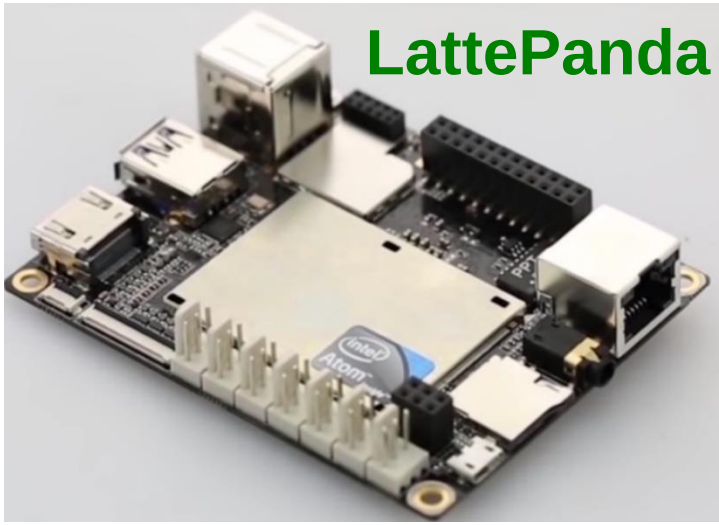
ESP8266

Source: https://www.sparkfun.com/products/13678



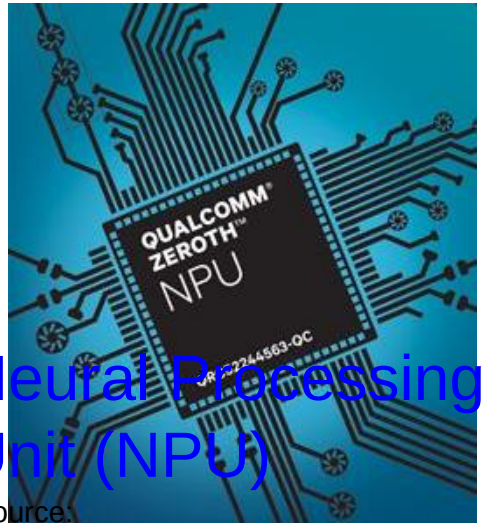
NodeMCU





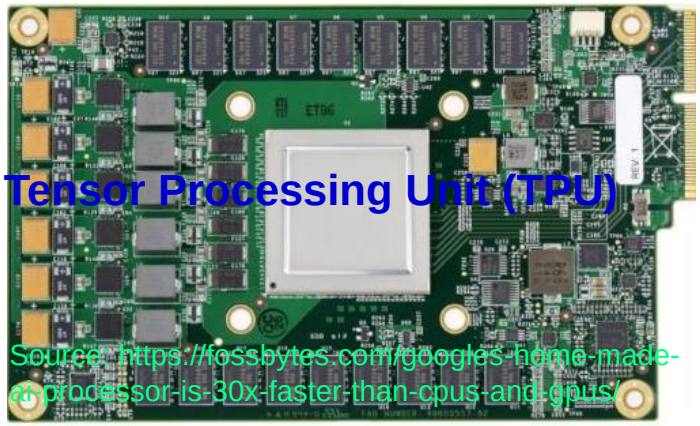
Source: http://www.lattepanda.com

Computing Technology - Current and Emerging



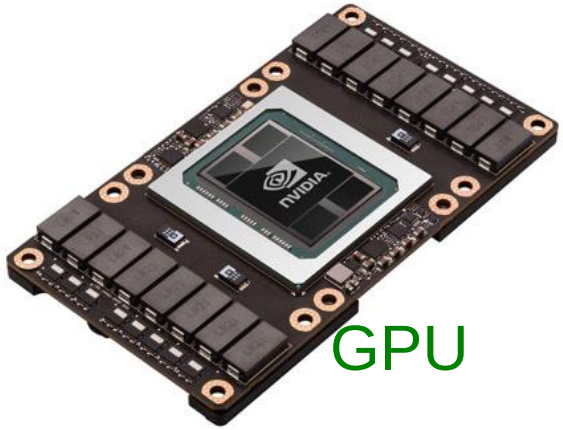
Neural Processing Unit (NPU)

Source: https://www.qualcomm.com/news/onq/2013/10/10/introducing-qualcomm-zeroth-processors-brain-inspired-computing

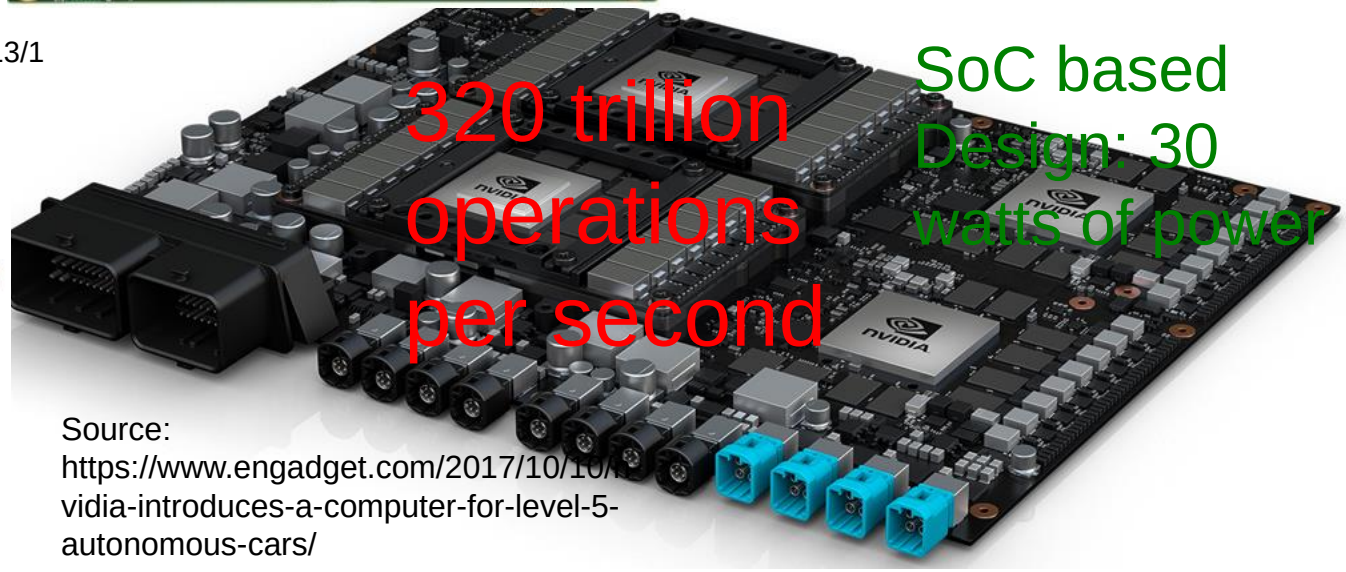


Tensor Processing Unit (TPU)

Source: https://fossbytes.com/googles-home-made-ai-processor-is-30x-faster-than-cpus-and-gpus/



GPU



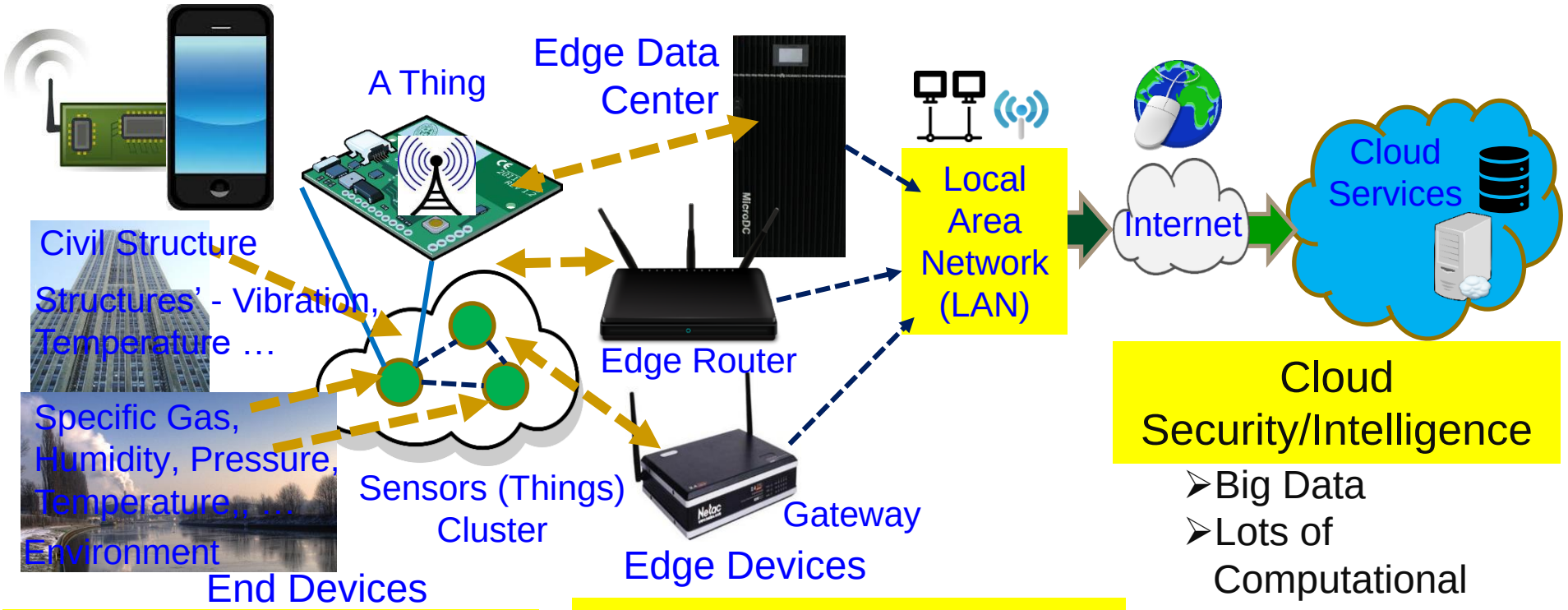
Source: https://www.engadget.com/2017/10/10/nvidia-introduces-a-computer-for-level-5-autonomous-cars/

ML Hardware – Cloud and Edge

Product	Cloud or Edge	Chip Type
Nvidia - DGX series	Cloud	GPU
Nvidia - Drive	Edge	GPU
Arm - ML Processor	Edge	CPU
NXP - i.MX processor	Edge	CPU
Xilinx - Zinq	Edge	Hybrid CPU/FPGA
Xilinx - Virtex	Cloud	FPGA
Google - TPU	Cloud	ASIC
Tesla - AI Chip	Edge	Unknown
Intel - Nervana	Cloud	CPU
Intel - Loihi	Cloud	Neuromorphic
Amazon - Echo (custom AI chip)	Edge	Unknown
Apple - A11 processor	Edge	CPU
Nokia - Reefshark	Edge	CPU
Huawei - Kirin 970	Edge	CPU
AMD - Radeon Instinct MI25	Cloud	GPU
IBM - TrueNorth	Cloud	Neuromorphic
IBM - Power9	Cloud	CPU
Alibaba - Ali-NPU	Cloud	Unknown
Qualcomm AI Engine	Edge	CPU
Mediatek - APU	Edge	CPU

Source: Presutto 2018: https://www.academia.edu/37781087/Current_Artificial_Intelligence_Trends_Hardware_and_Software_Accelerators_2018_

End, Edge Vs Cloud Security, Intelligence …



End Security/Intelligence

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

Edge Security/Intelligence

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

Cloud Security/Intelligence

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

Source: Mohanty iSES 2018 Keynote

Conclusions

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:

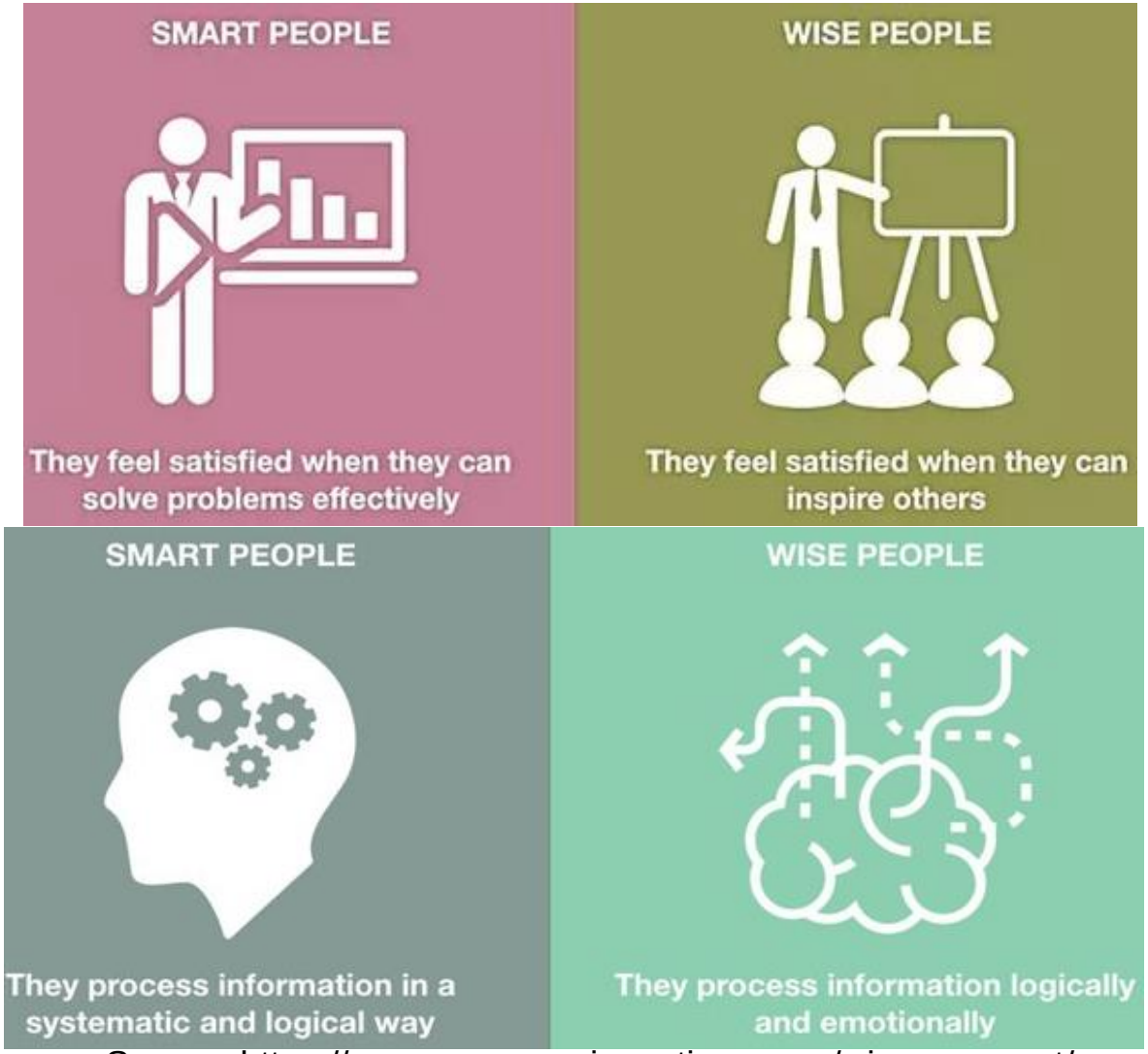
The ability to acquire and apply knowledge and skills.

Source: https://en.oxforddictionaries.com

Smartness

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

Does Smart Mean Wise?



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

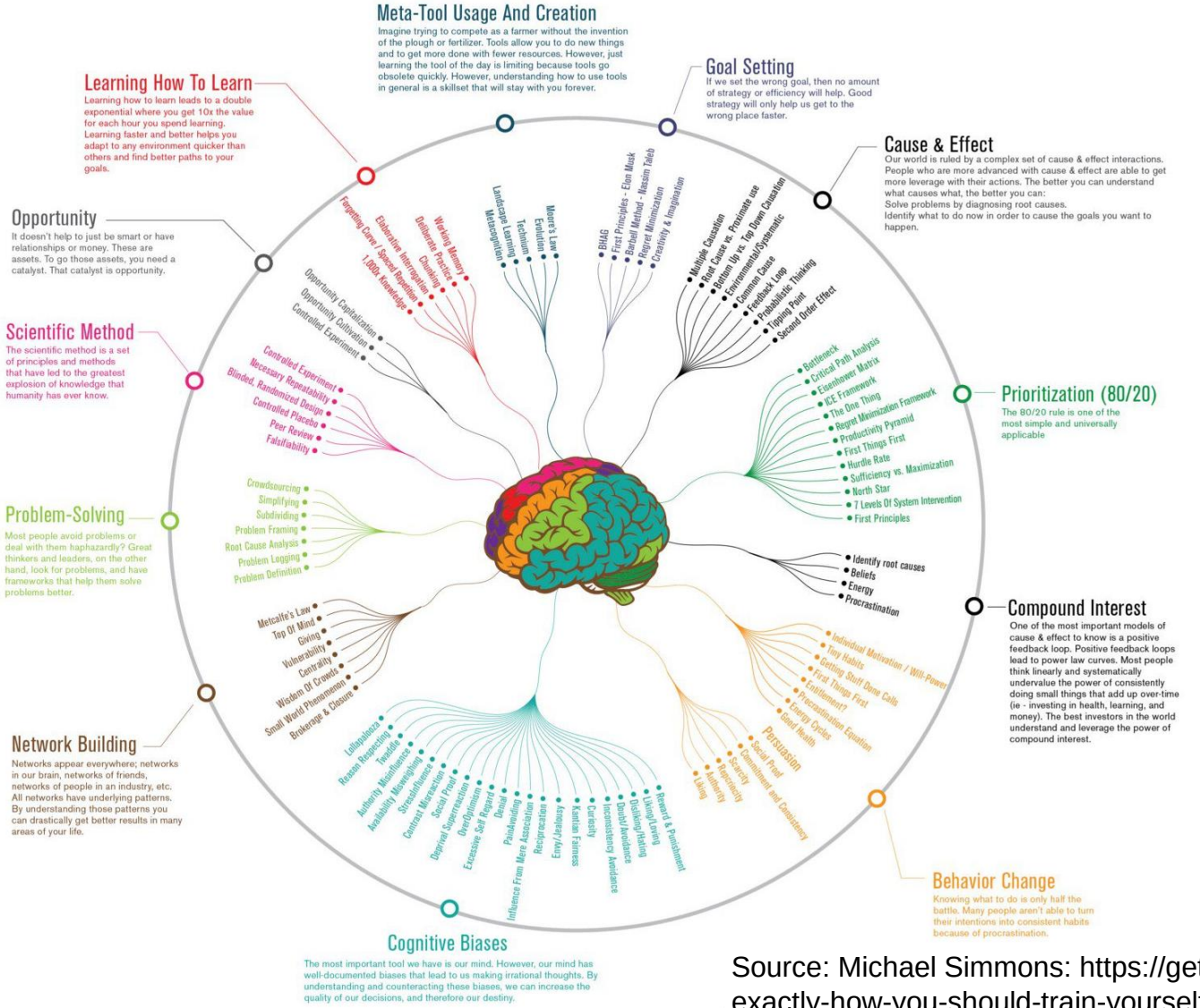
- Can Electronics be wise?

- Why not?
  - If AI is intelligence, then it should evolve to wise!

Intelligence Quotient (IQ) ?

- If Smart Electronics means Intelligence then can we measure its IQ?

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

Conclusions

- "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.

Hardwares are the drivers of the civilization, even softwares need them.

Thank You !!!

Slides Available at: http://www.smohanty.org