Smart Electronic Systems - Myths and Realities

Keynote – iSES 2018

17th December 2018

Hyderabad, India

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu

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

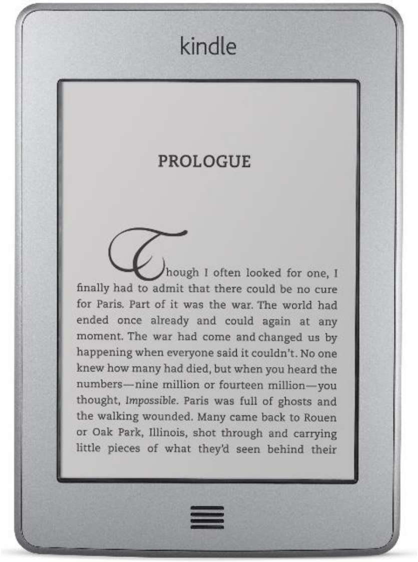
Talk - Outline

- 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 Small?

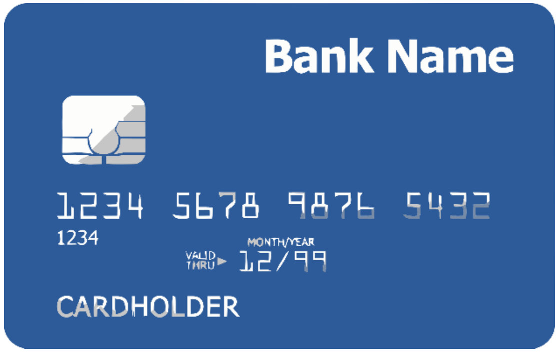
Does Smart Mean Portable?



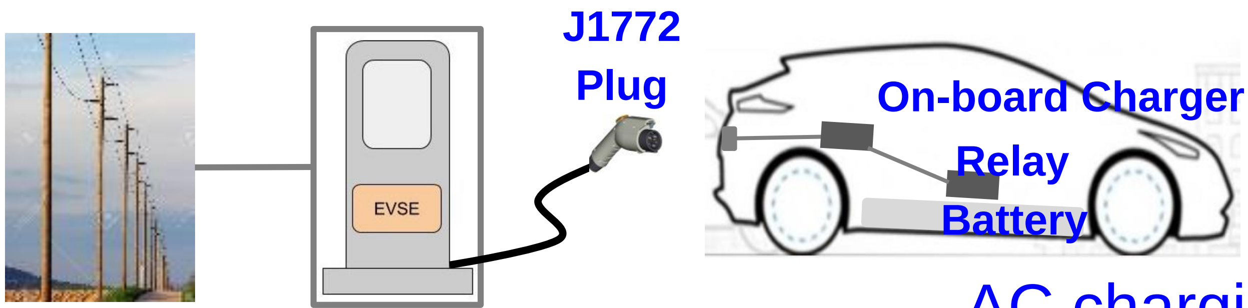
Does Smart Mean Efficient?

Does Smart Mean More-Features?

Does Smart Mean Electronic?



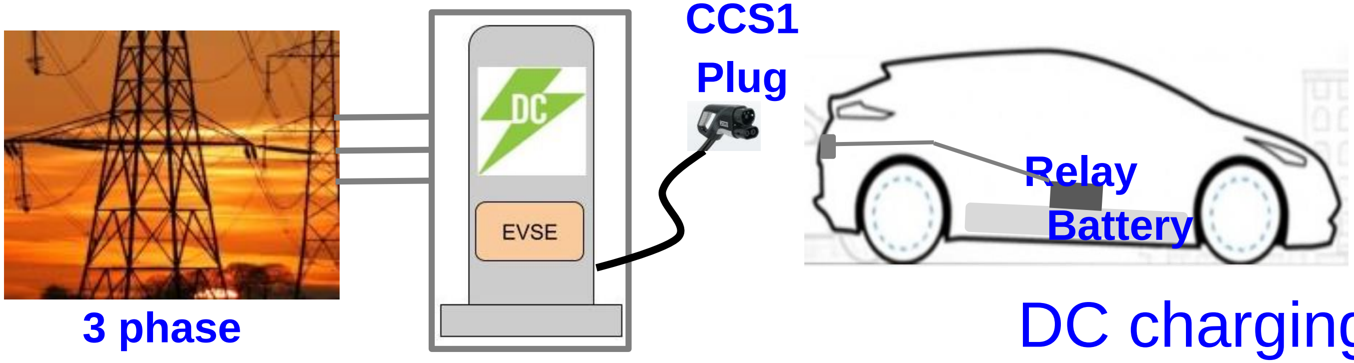
Does Smart Mean Electric?



Grid

AC charging station

- Monitoring function
- Communication and safety



3 phase AC supply

DC charging station

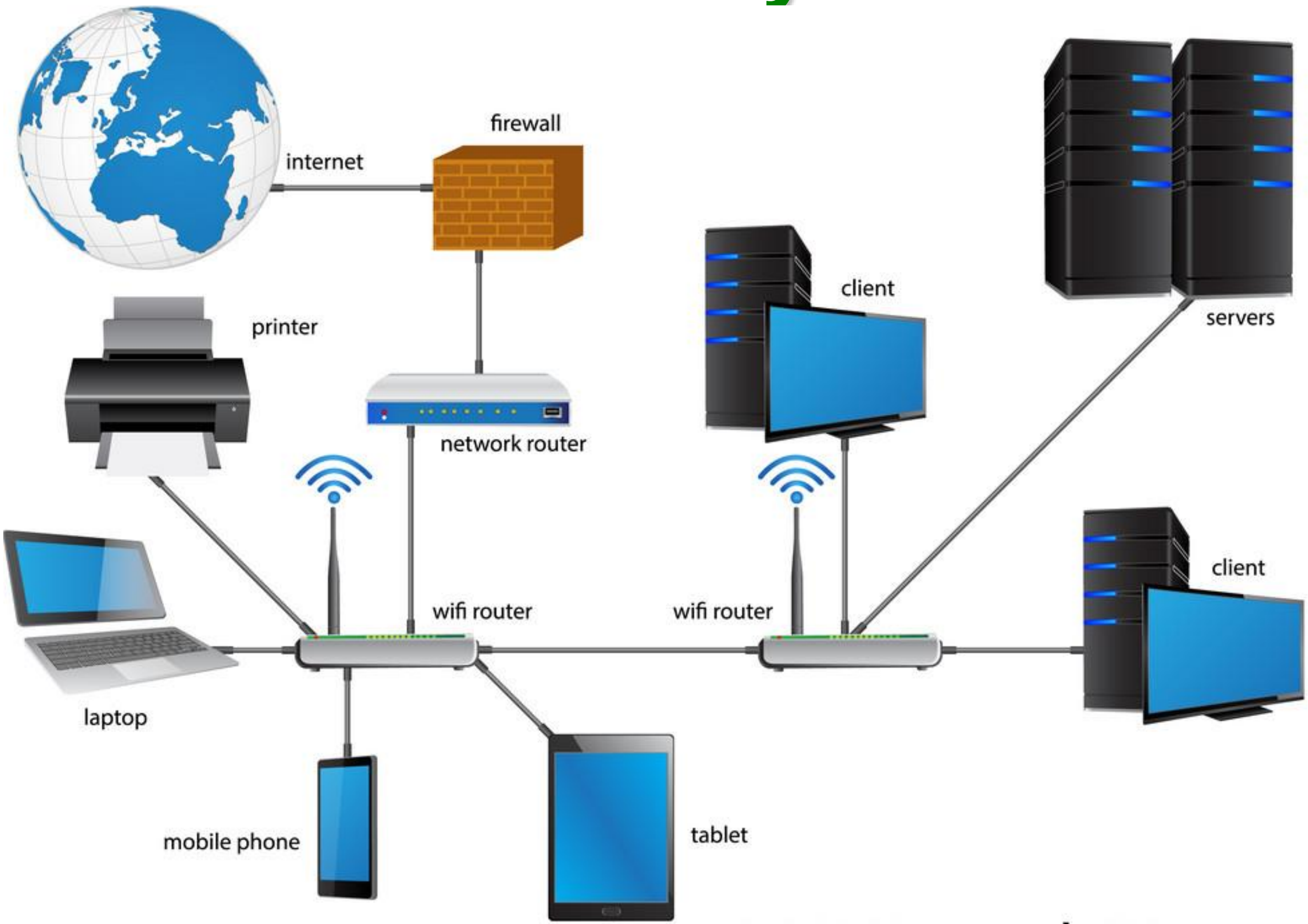
- AC-DC Off board conversion
- Monitoring Power flow
- EV to grid communication
- Safety monitoring

Electric Vehicle Supply Equipment (EVSE)

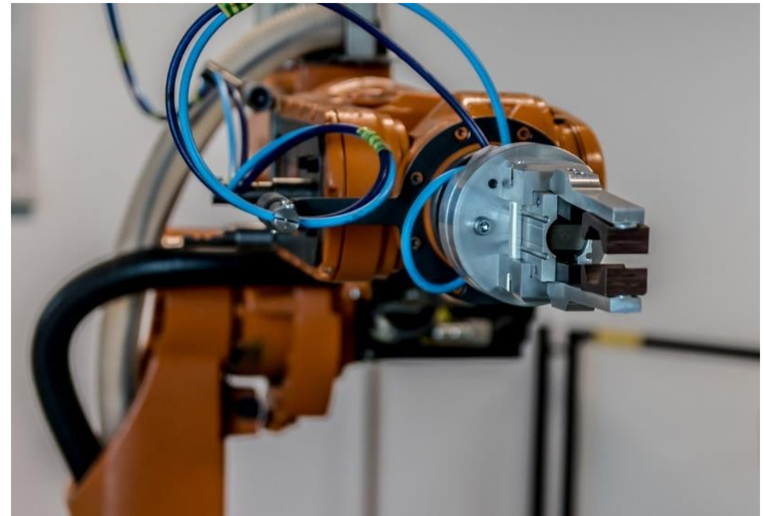
Source: Mishra, Mohanty 2018, CE Magazine Mar 2018

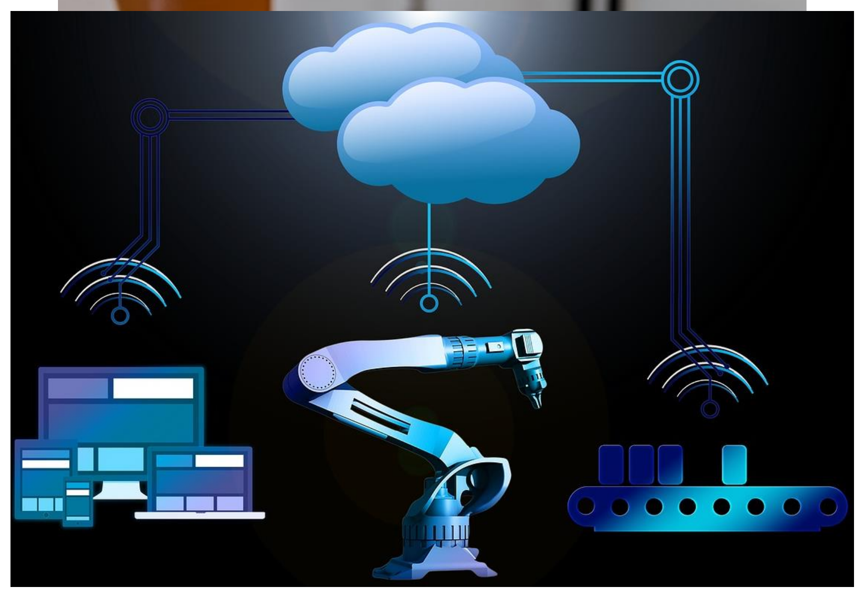
Does Smart Mean Battery-Operated?

Does Smart Mean Cyber-Enabled?



Does Smart Mean Autonomous?

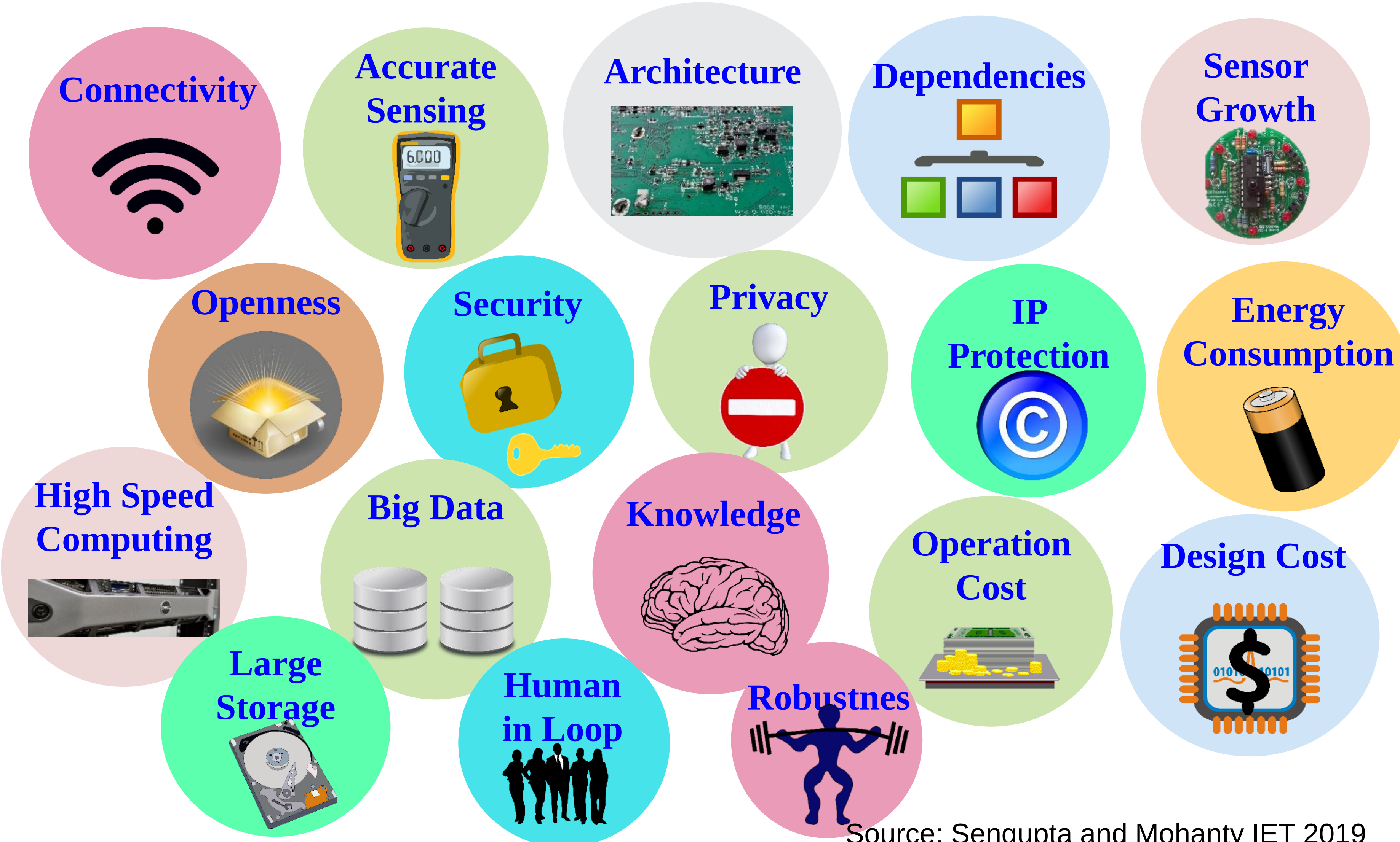




Does Smart Mean Intelligence?

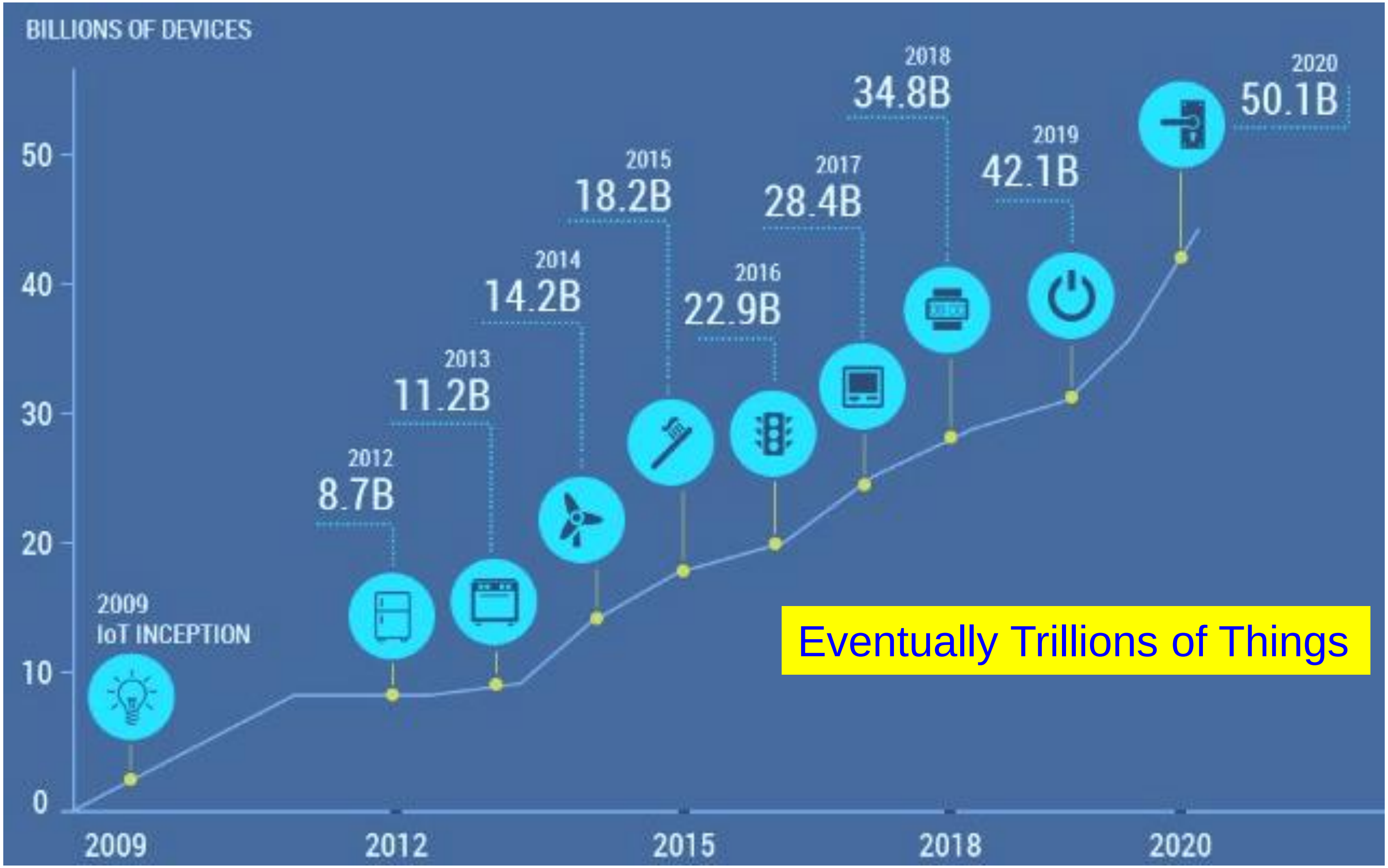
Challenges in Current Generation CE Design

CE/IoT – Selected Challenges



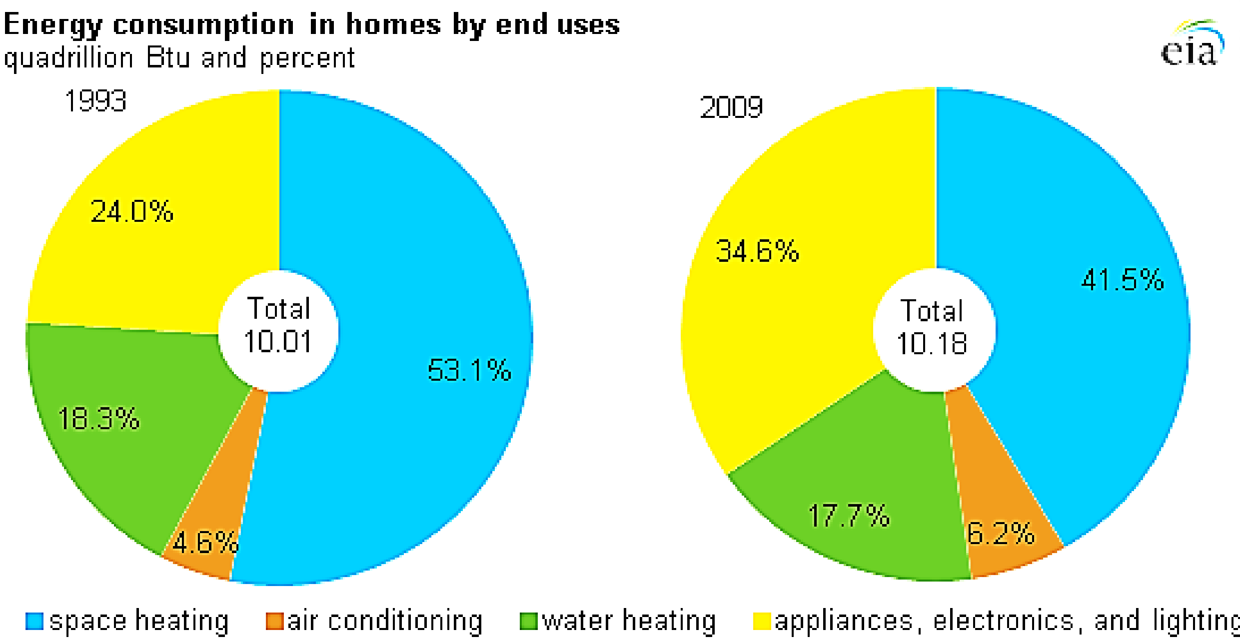
Source: Sengupta and Mohanty IET 2019

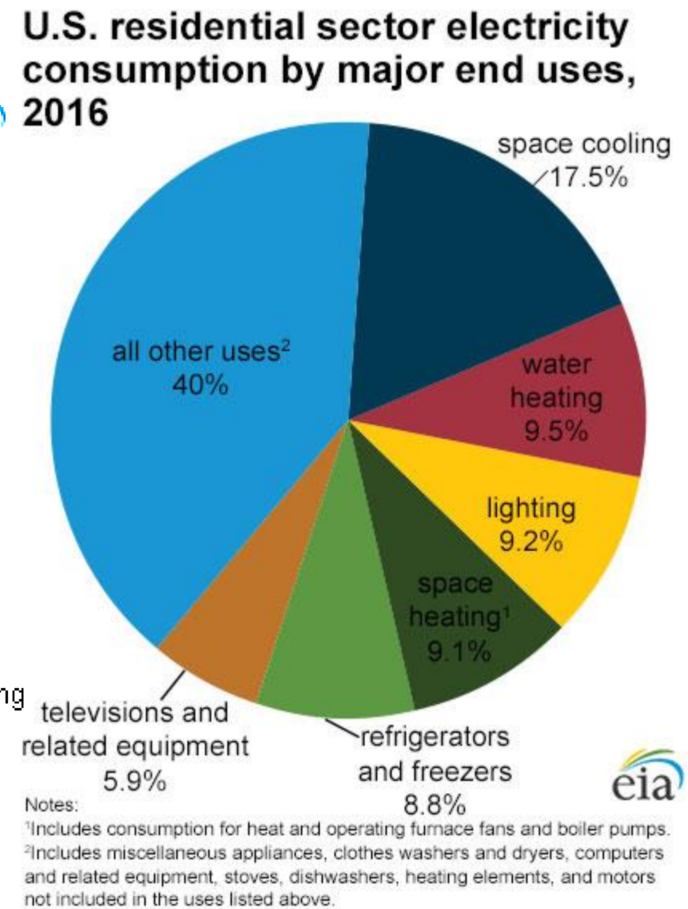
Massive Growth of Sensors/Things



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

Consumer Electronics Demand More and More Energy

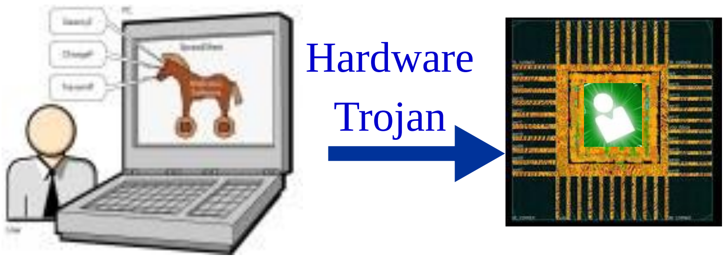




Source: U.S. Energy Information Administration

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

Security, Privacy, and IP-Rights

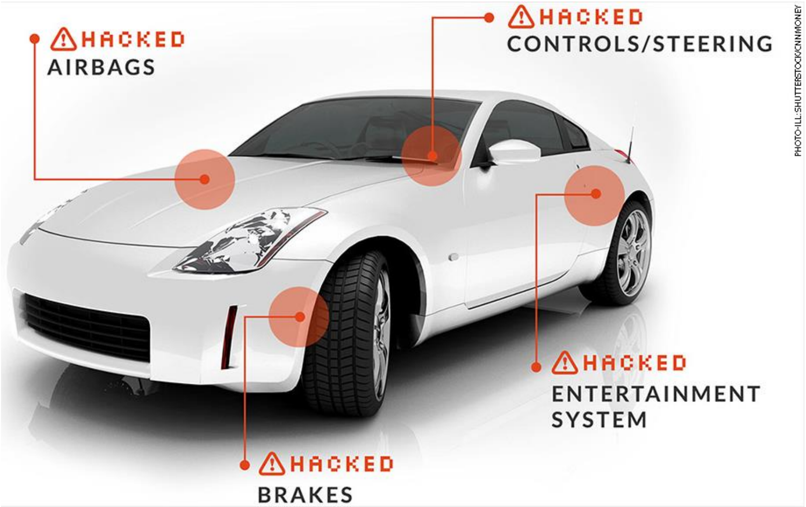


Source: Mohanty ICIT 2017 Keynote

Security - System …

Power Grid Attack

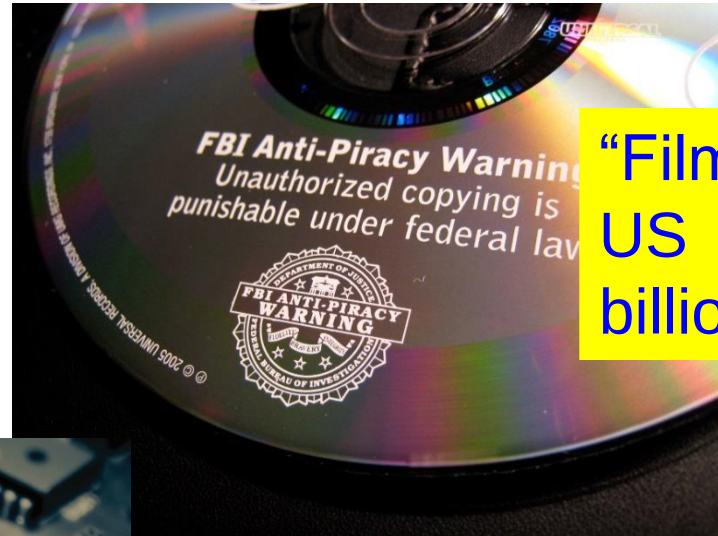
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



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

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

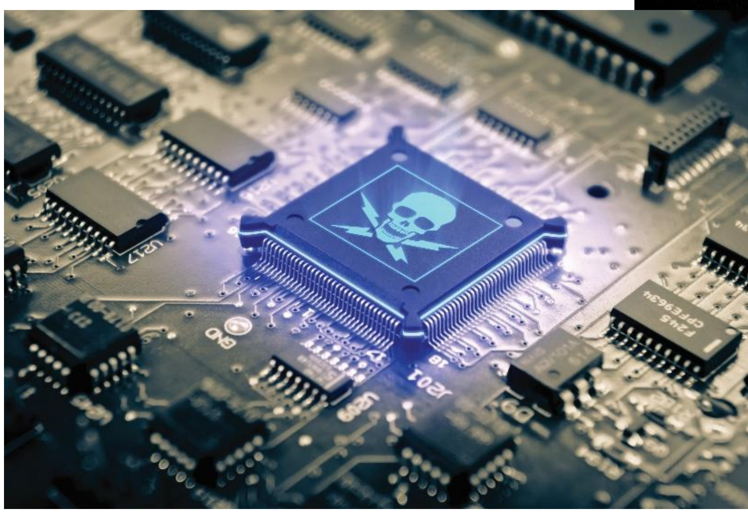
Ownership - Media, Hardware, Software



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

Media Piracy

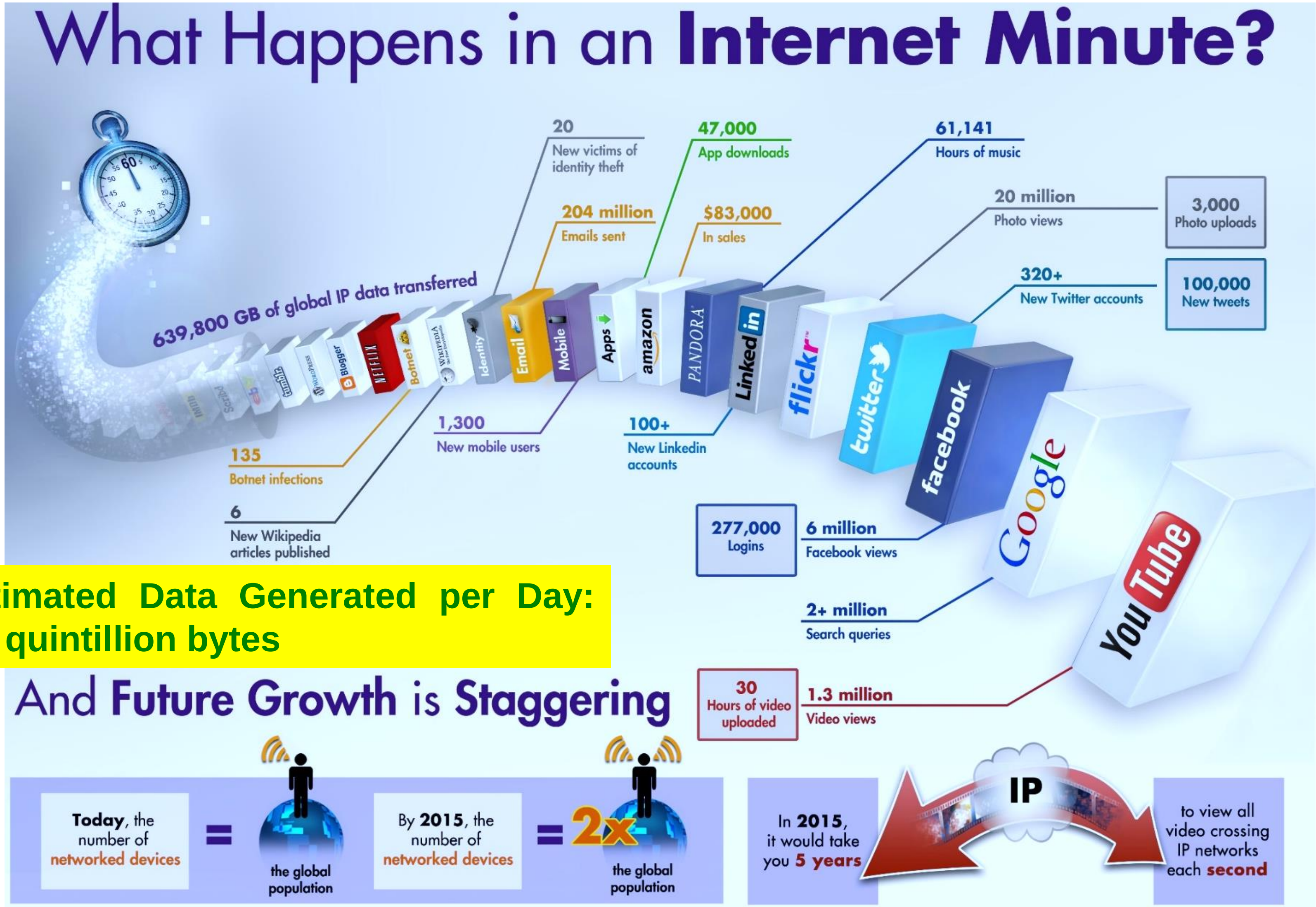
Hardware Piracy → Counterfeit Hardware



Software Piracy

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

Huge Amount of Data



Estimated Data Generated per Day: 2.5 quintillion bytes

ESR-Smart Electronics

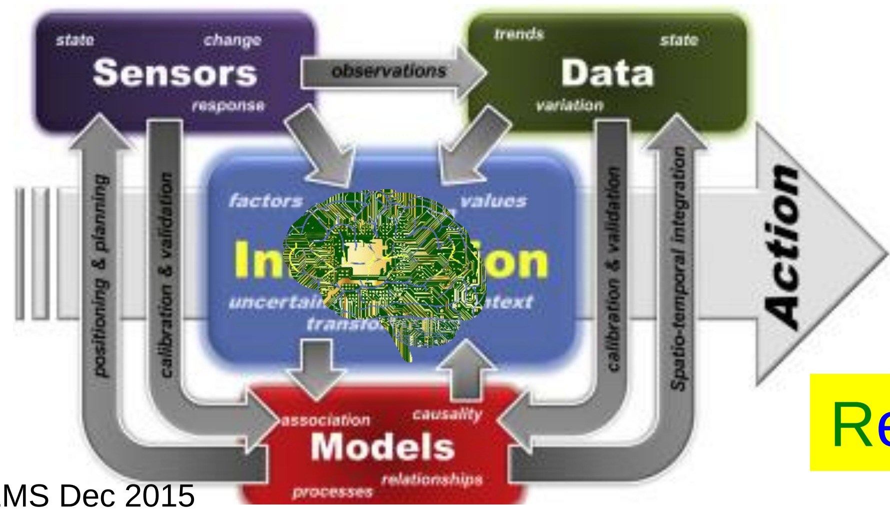
Energy Smart

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

Security of systems and data.

Security Smart

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



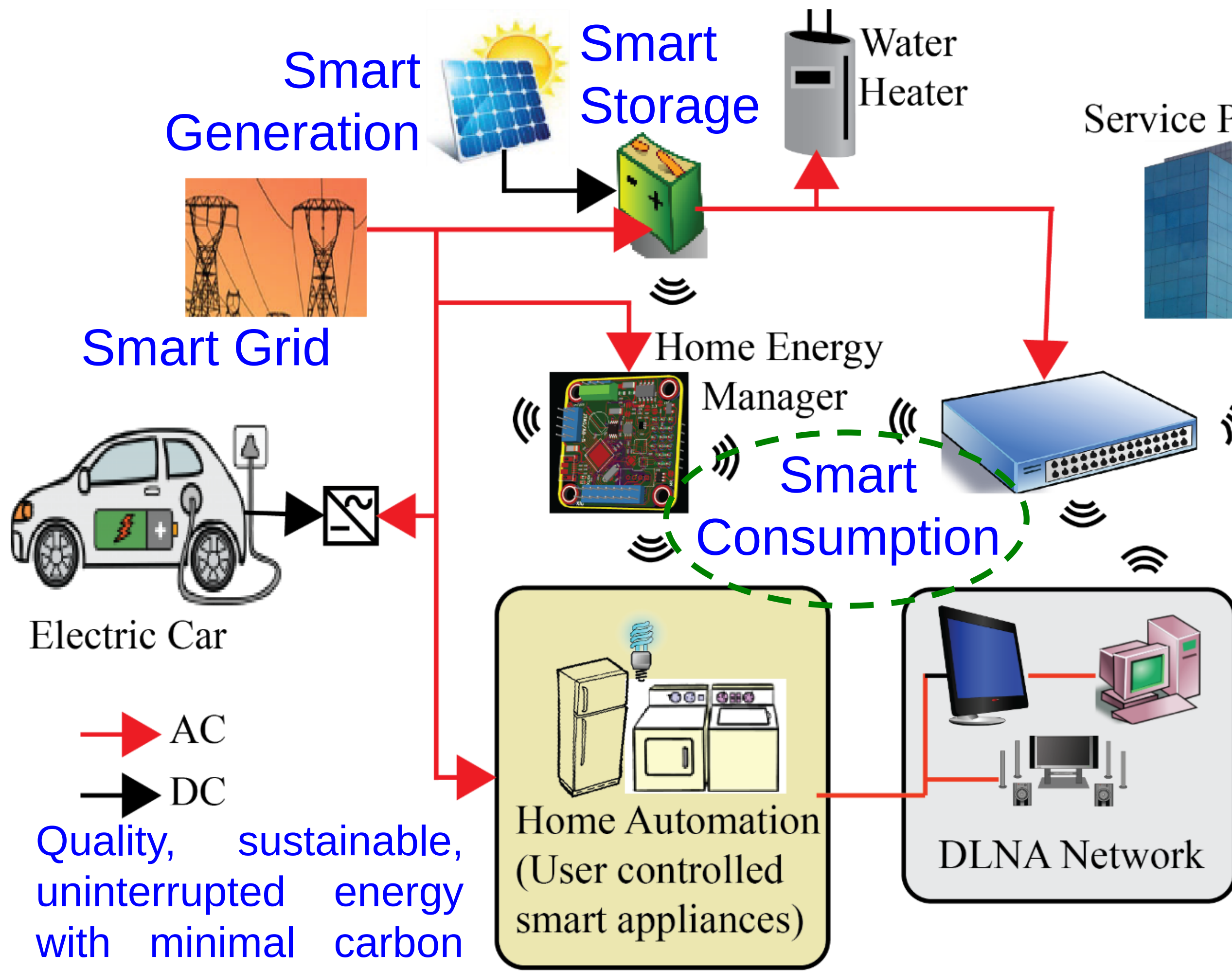
Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Response Smart

Energy Smart

Smart Energy



Source: Mohanty 2016, CE Magazine July 2016

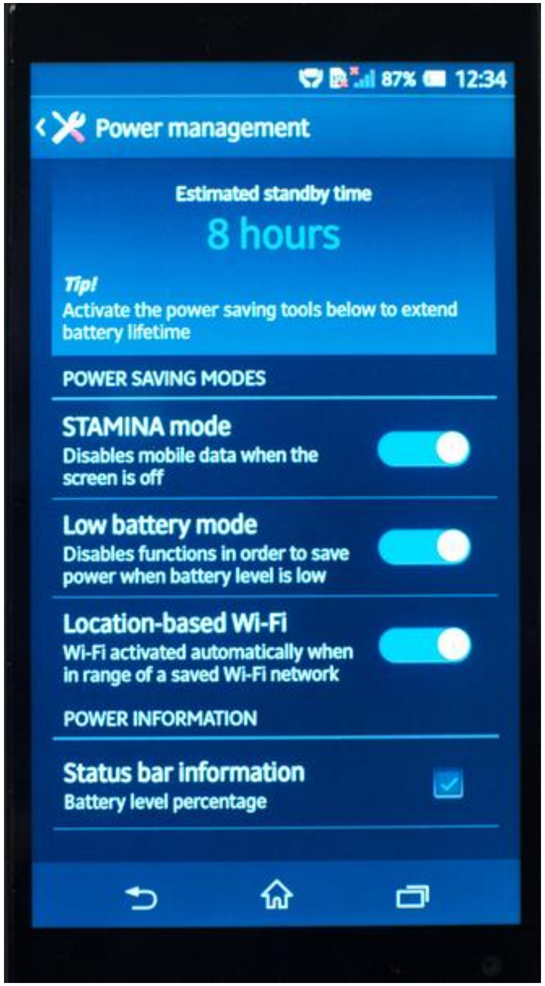
Quality, sustainable, uninterrupted energy with minimal carbon footprint.

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

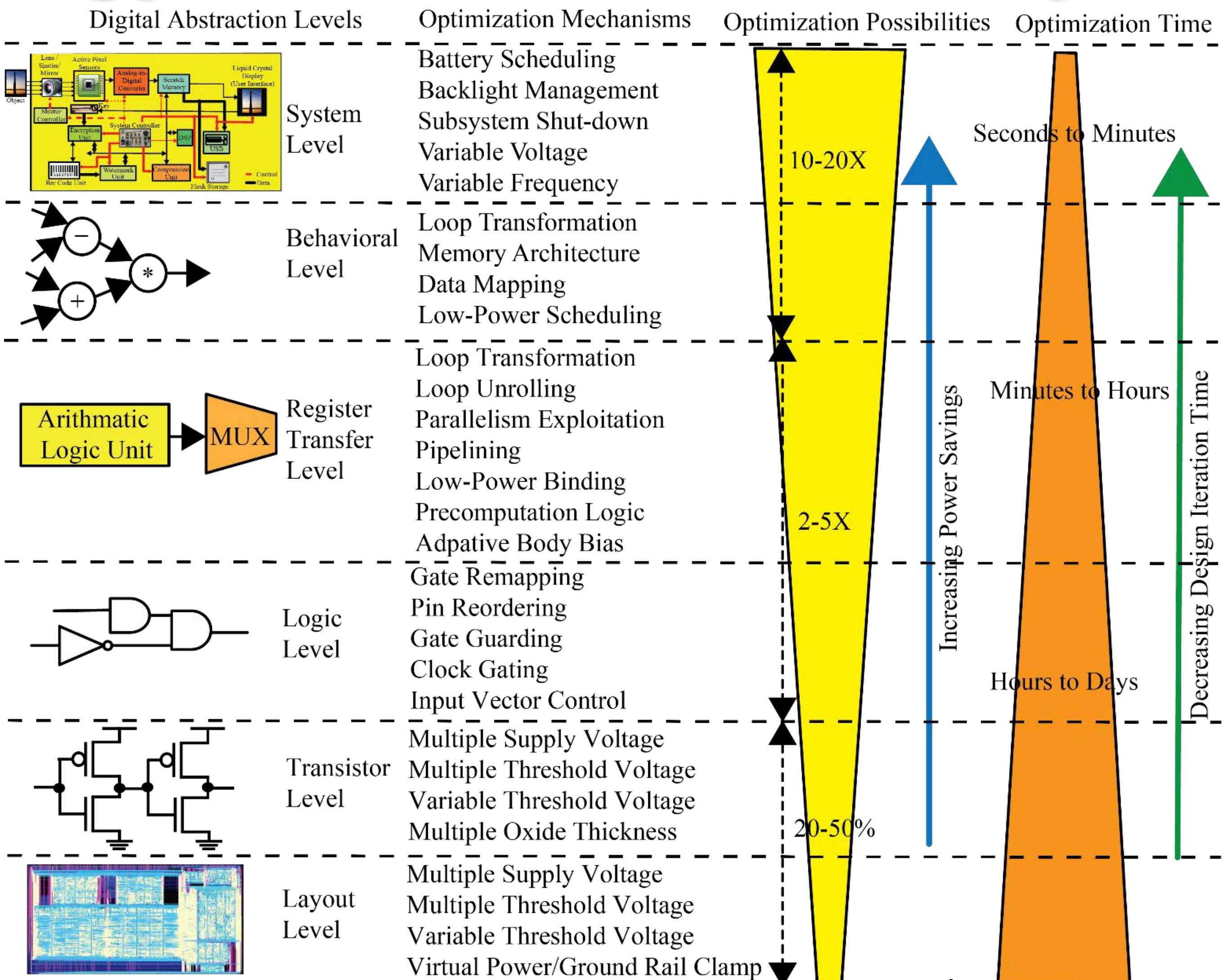
Smart Home

Energy Efficient Electronics: Possible Solution Fronts

- Energy Efficient Electronic Systems
  - System
  - Application
  - Energy Efficient Commun-ications
    - Topology
    - Routing
    - Protocol
  - Energy Efficient Software
  - Energy Efficient Hardware
    - Digital
    - Analog
    - Mixed-Signal
    - RF
    - Sensors
  - Smart Battery

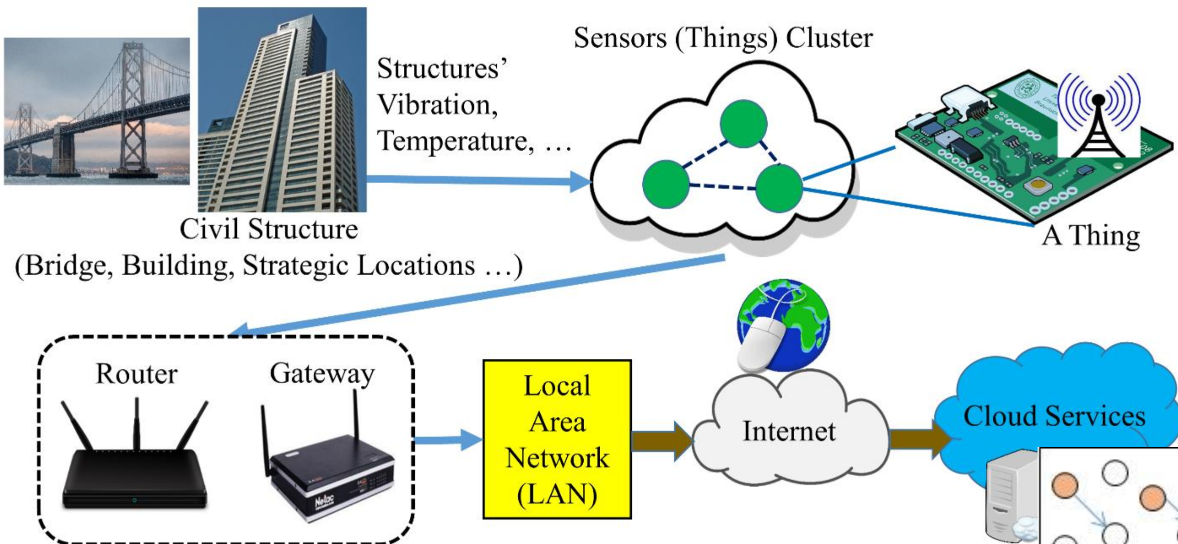
Source: Mohanty ZINC 2018 Keynote

Energy Reduction in CE Systems

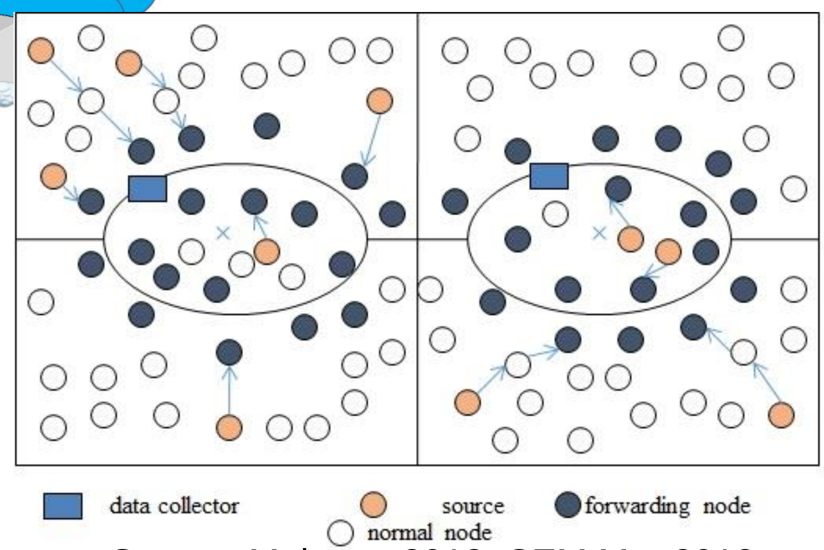


Source: Mohanty 2015, McGraw-Hill 2015

Sustainable IoT – Low-Power Sensors and Efficient Routing

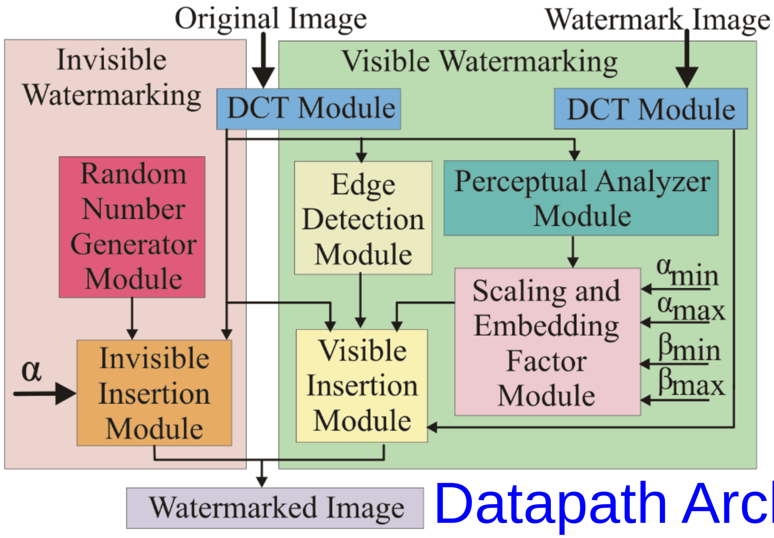


- IoT - sensors near the data collector drain energy faster than other nodes.
- Solution Idea - Mobile sink in which the network is balanced with node energy consumption.
- Solution Need: New data routing to forward data towards base station using mobile data collector, in which two data collectors follow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

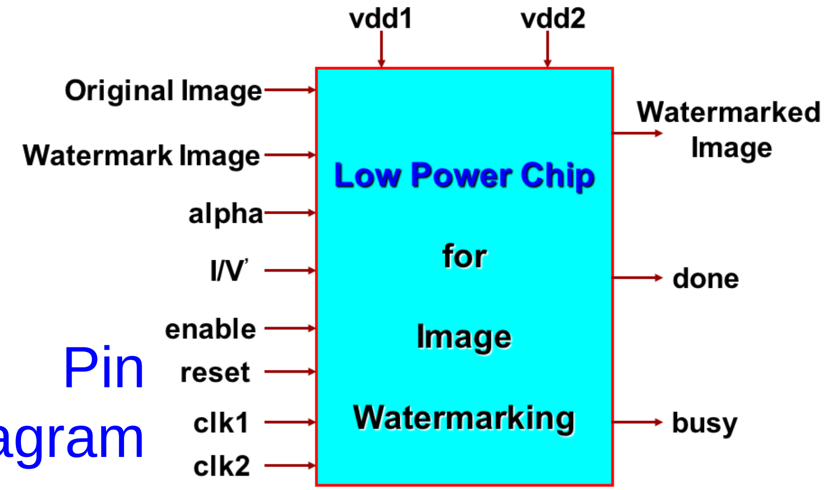


Source: Mohanty 2018, CEM Mar 2018

Energy-Efficient Hardware - Dual-Voltage

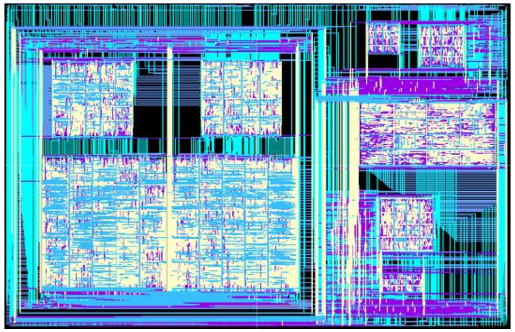


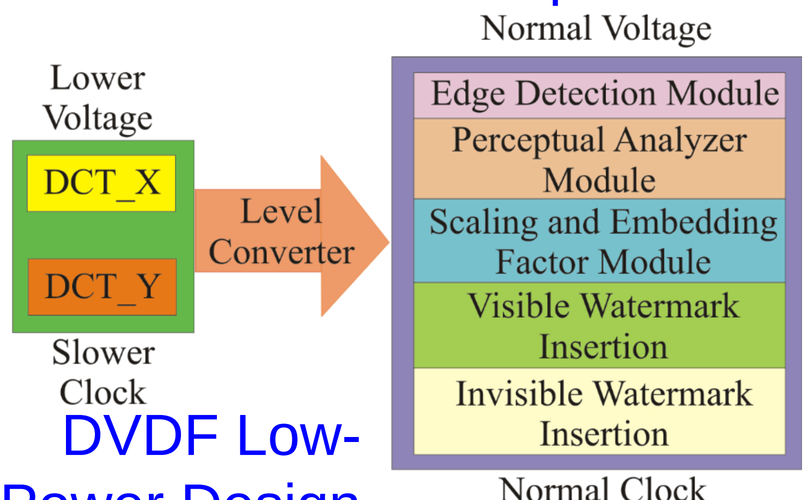
Datapath Architecture



Pin Diagram

Hardware Layout





DVDF Low-Power Design

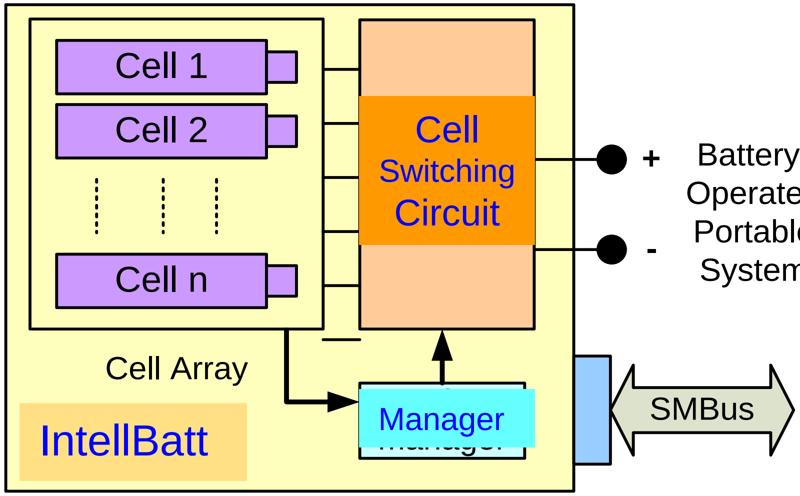
Physical Design Data
Total Area : 16.2 sq mm
No. of Transistors: 1.4 million
Power Consumption: 0.3 mW

Source: Mohanty 2006, TCASII May 2006

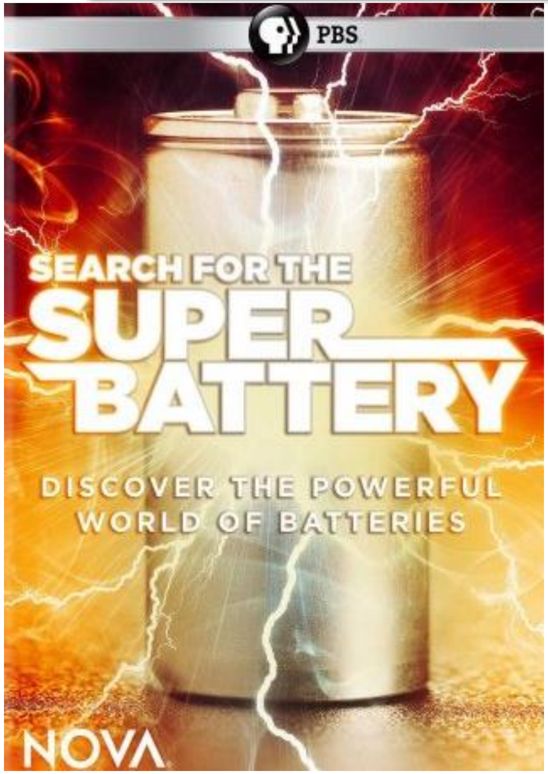
Energy Storage - High Capacity and Efficiency Needed

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

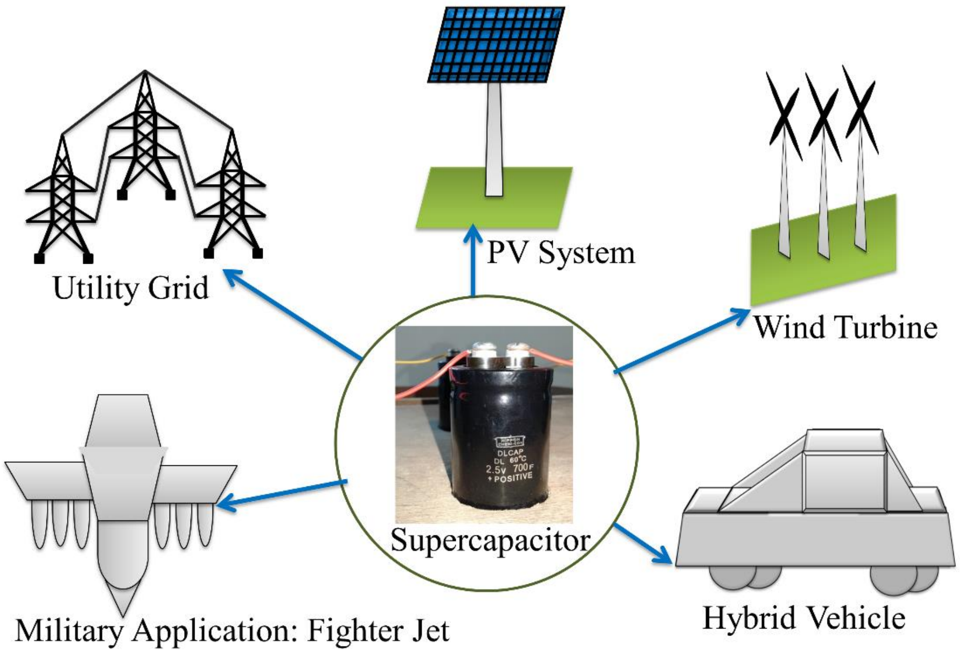


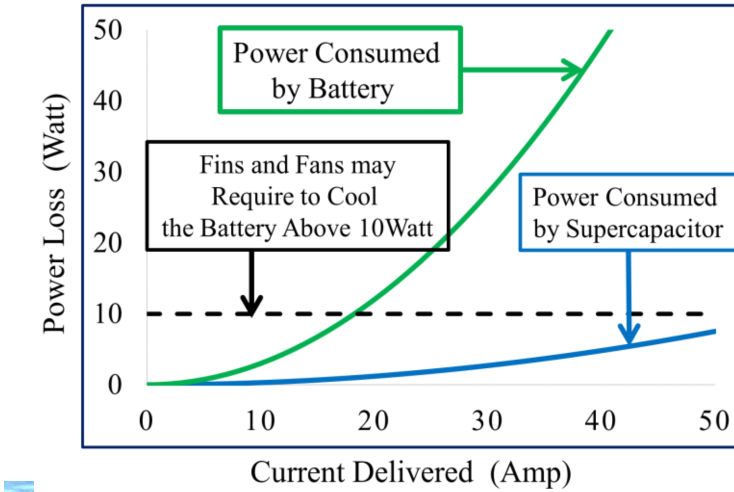
Lithium Polymer Battery

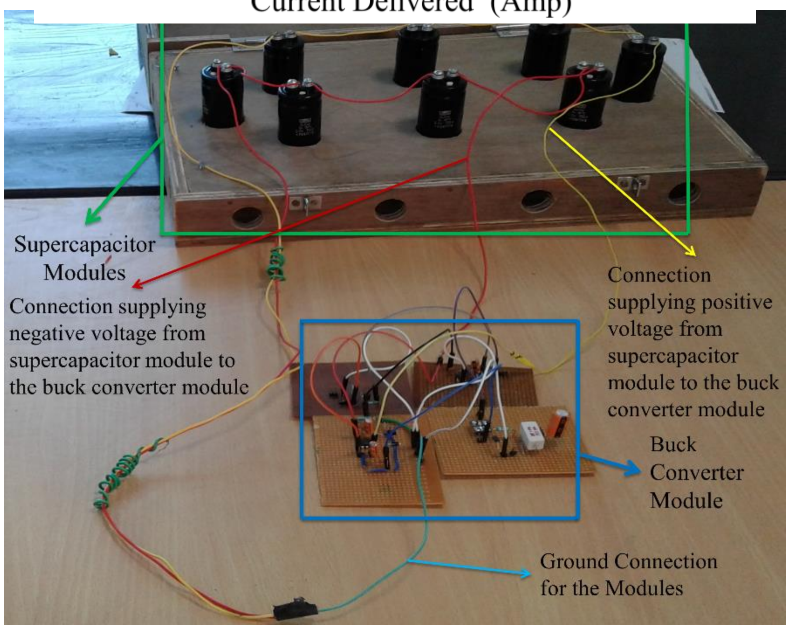
Supercapacitor

Source: Mohanty MAMI 2017 Keynote

Supercapacitor based Power for CE







Source: Mohanty 2018, CEM Sep 2018

Security Smart

CE Systems – Diverse Security/ Privacy/ Ownership Needs

Medical Devices

RFID Chip

Pace maker

Insulin Pump

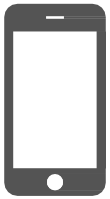
Heart Rate Monitor

Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices



Smart Phones/ Tablets

Wearable Devices

Smart Clothing

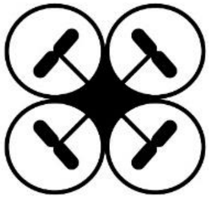
Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

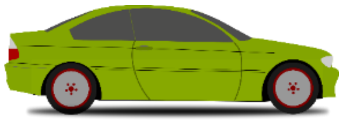
Entertainment Devices

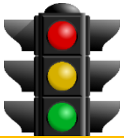


Drones /UAVs

Video Games

Transportation Devices



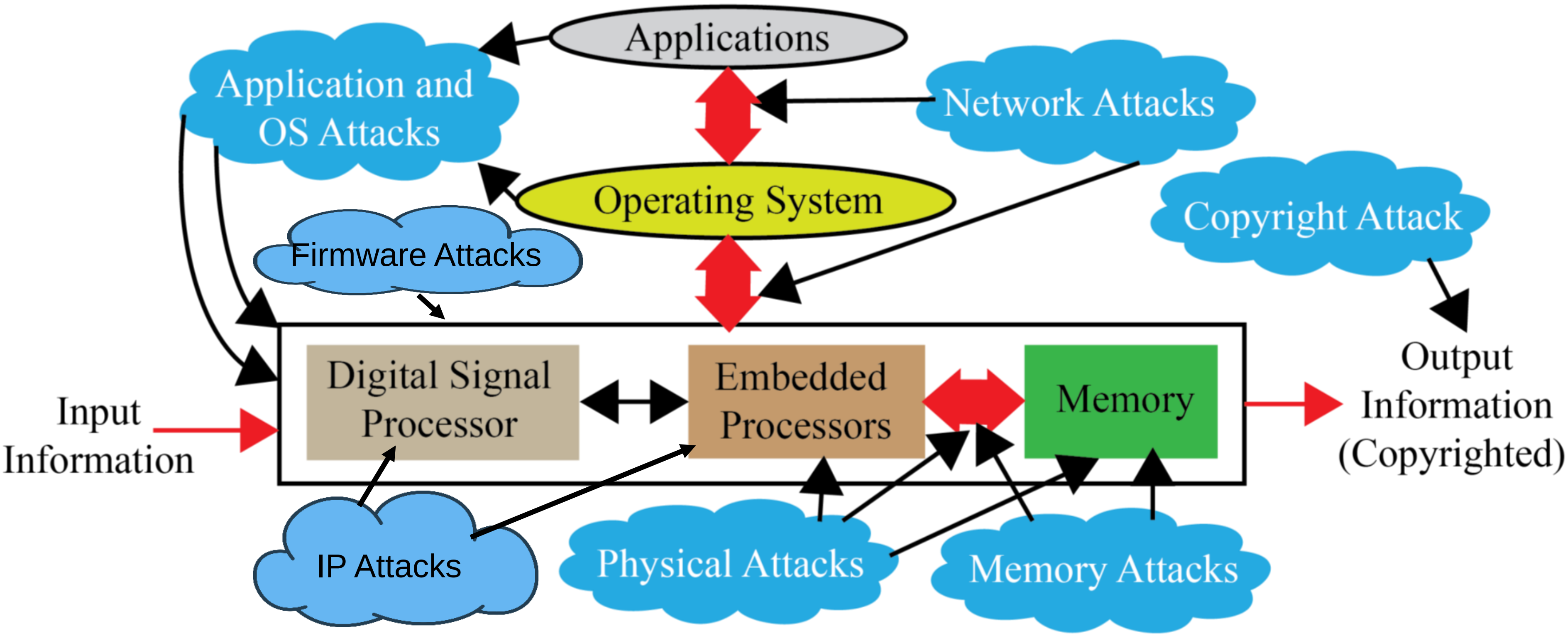


Smart Vehicles/ Autonomous Vehicles

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.

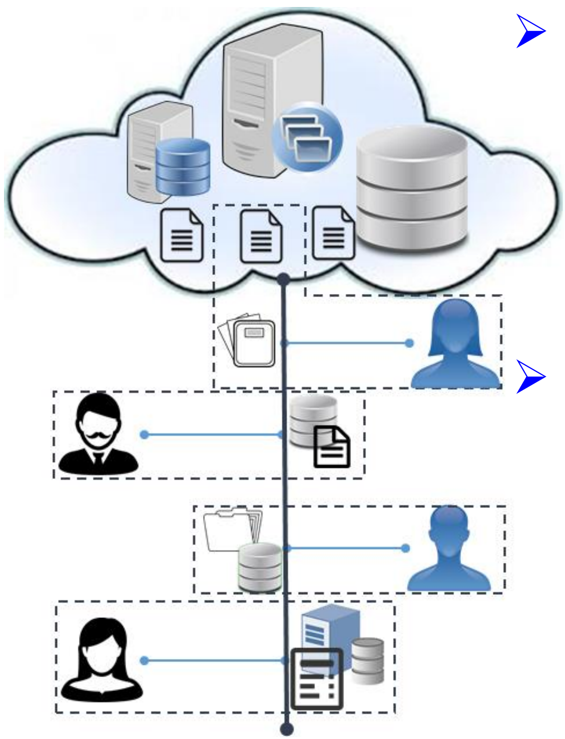
IoT Security - Software Defined Perimeter (SDP)

TCP/IP based security | Traditional

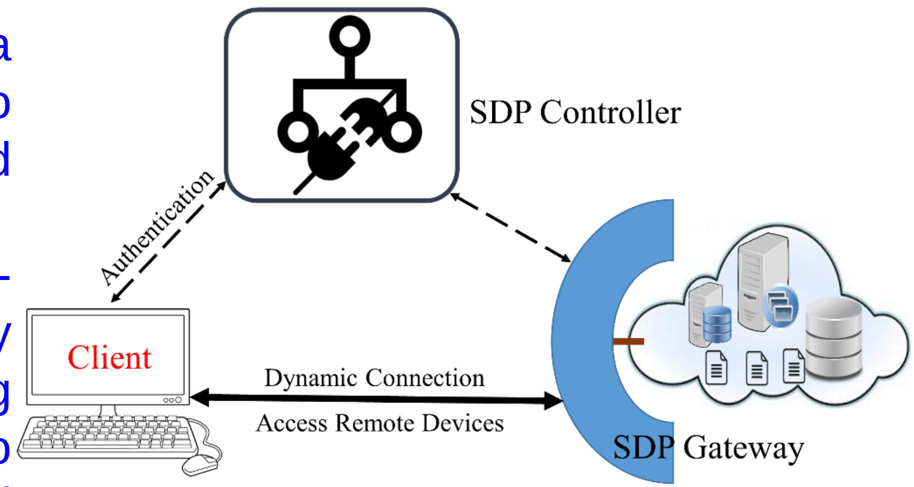
Connect First and then Authenticate

Software-Defined Perimeter | Advanced

Authenticate First and then Connect



- SDP creates a cryptographic perimeter from a source device to the edges and cloud data center.
- SDP provides user-centric security solution by creating a perimeter to enclose source and destination within the perimeter.



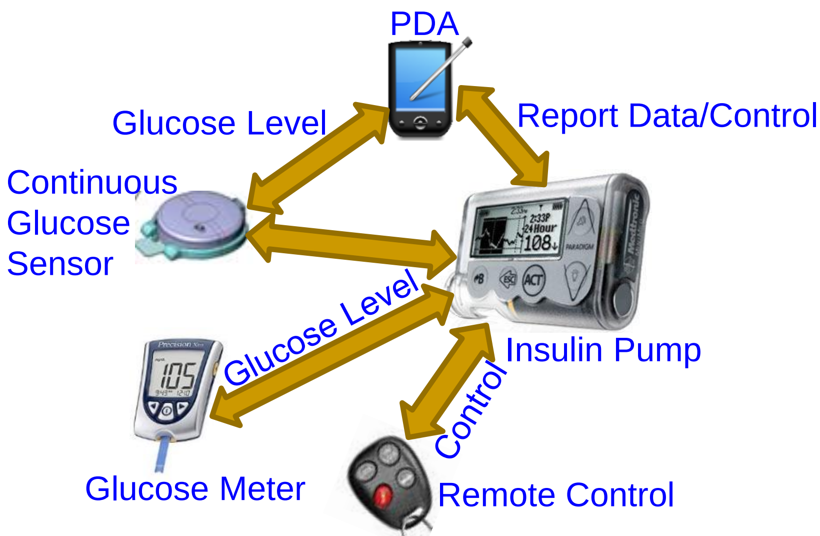
Source: Puthal and Mohanty 2017, CEM Oct 2017

Smart Healthcare - Security and Privacy Issue

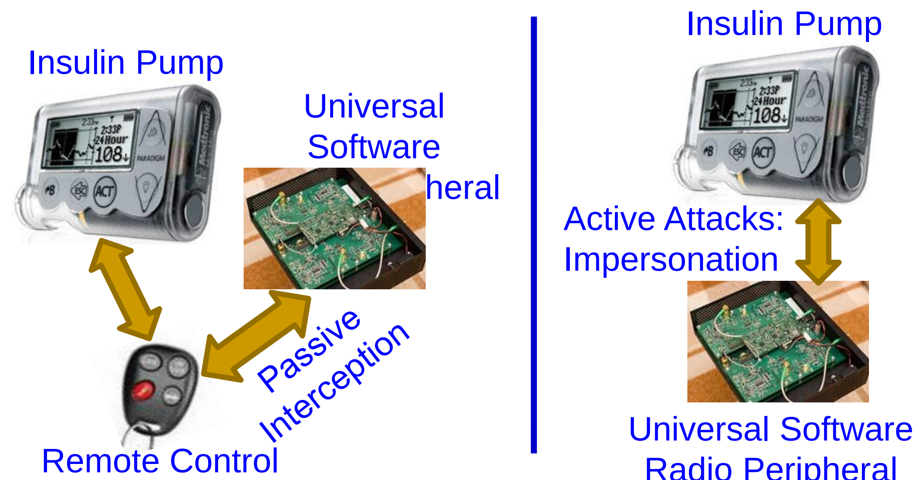
Selected Smart Healthcare Security/Privacy Challenges

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

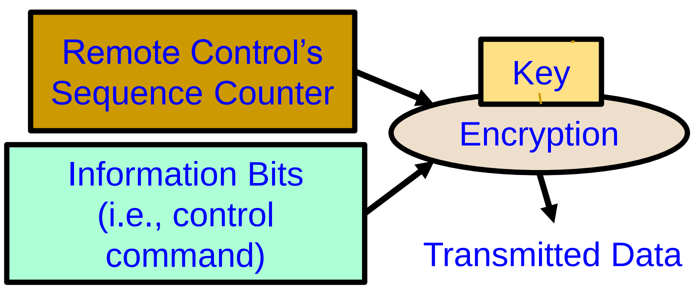
Smart Healthcare Security



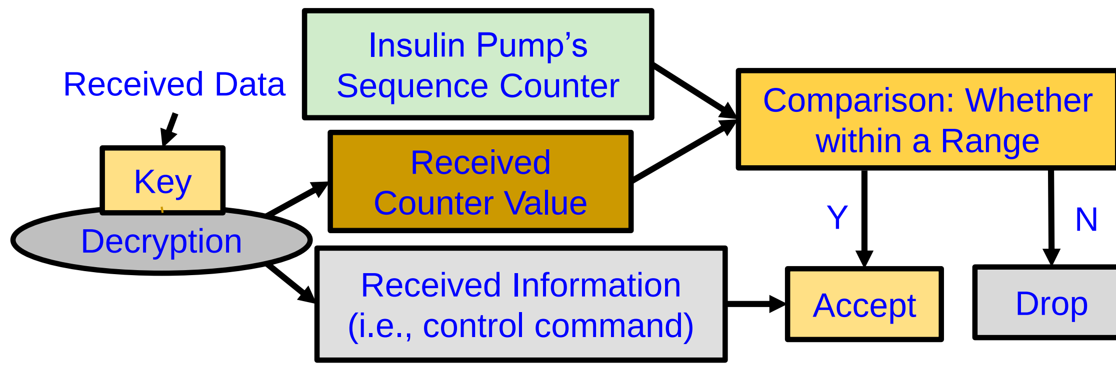
Insulin Delivery System



Security Attacks



Rolling Code Encoder in Remote Control



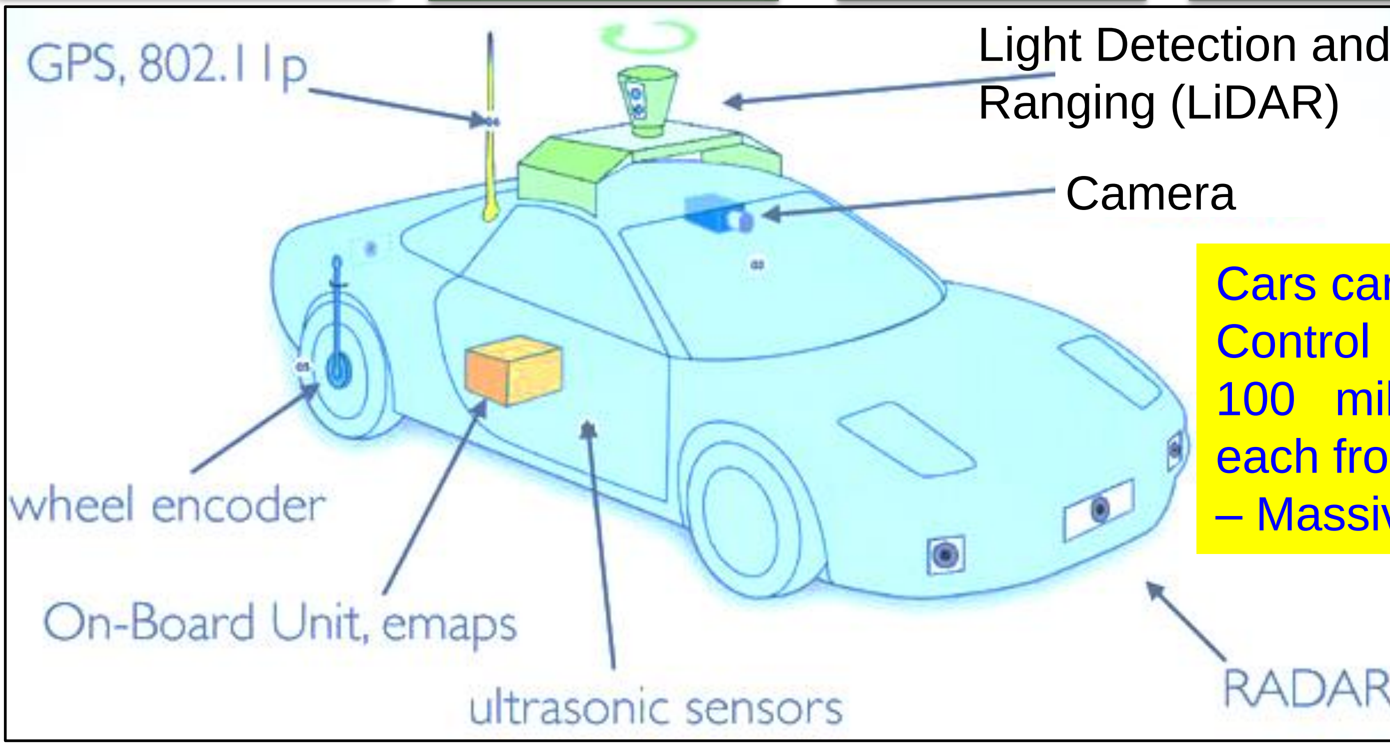
Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

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.

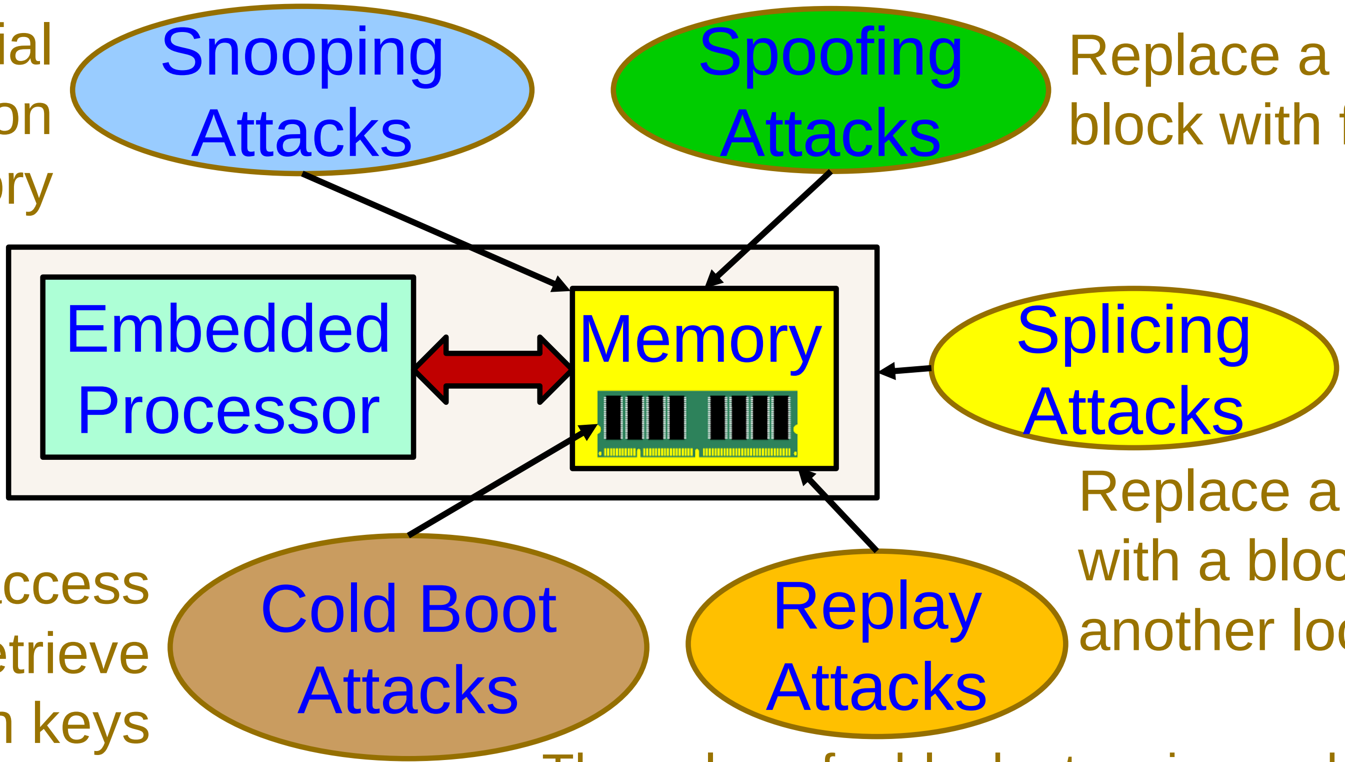
Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

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

Source: Petit 2015: IEEE-TITS Apr 2015

Memory Attacks

Read confidential information in memory



Replace a block with fake

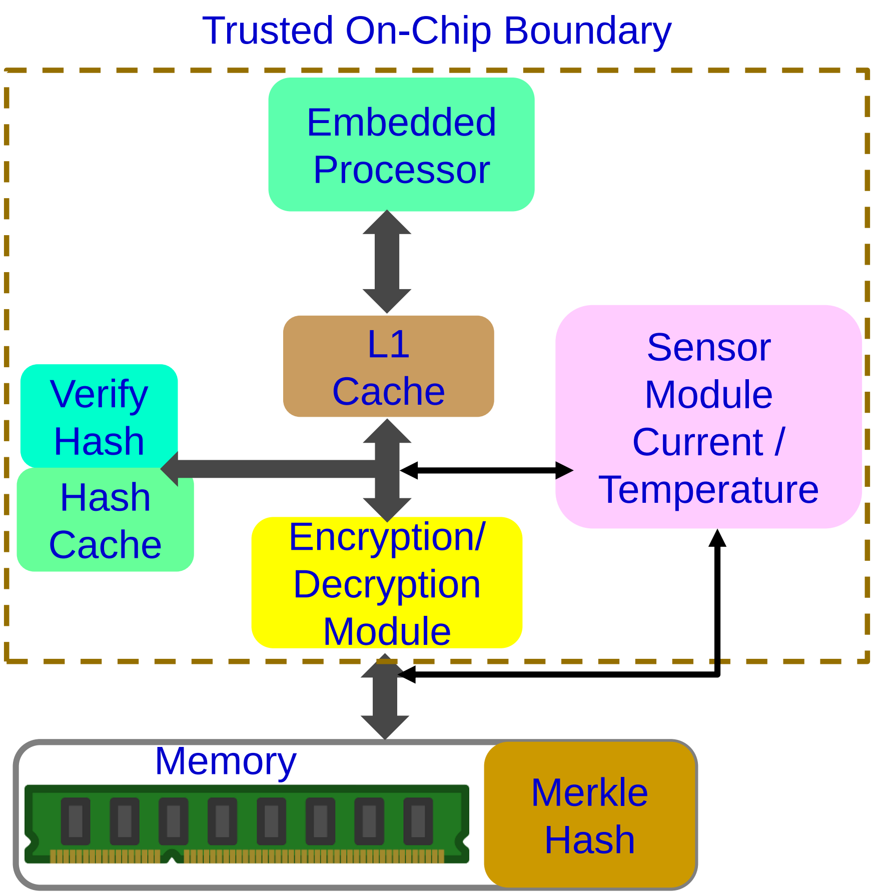
Replace a block with a block from another location

Physical access memory to retrieve encryption keys

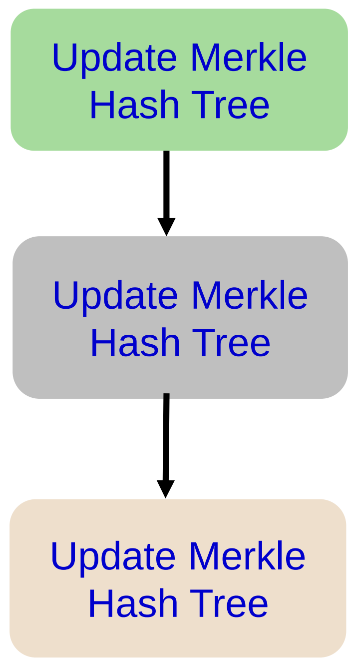
The value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

Source: Mohanty 2013, Springer CSSP Dec 2013

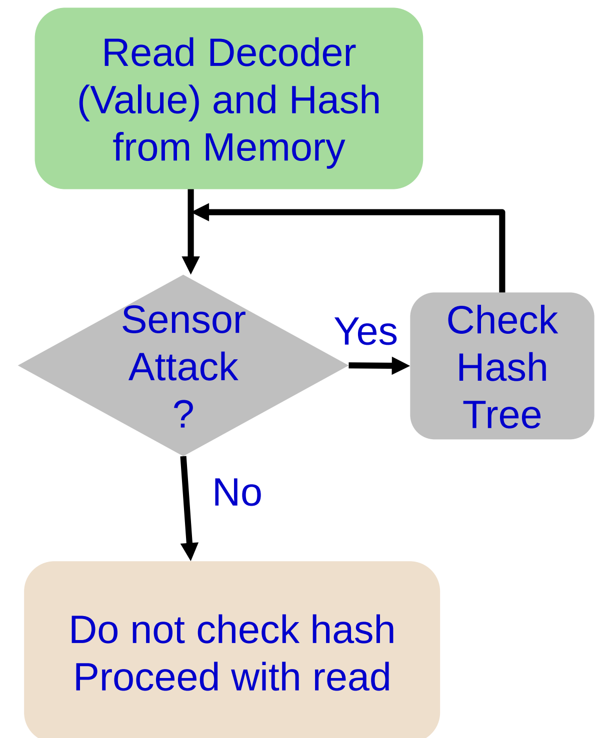
Embedded Memory Security and Protection



On-Chip/On-Board Memory Protection



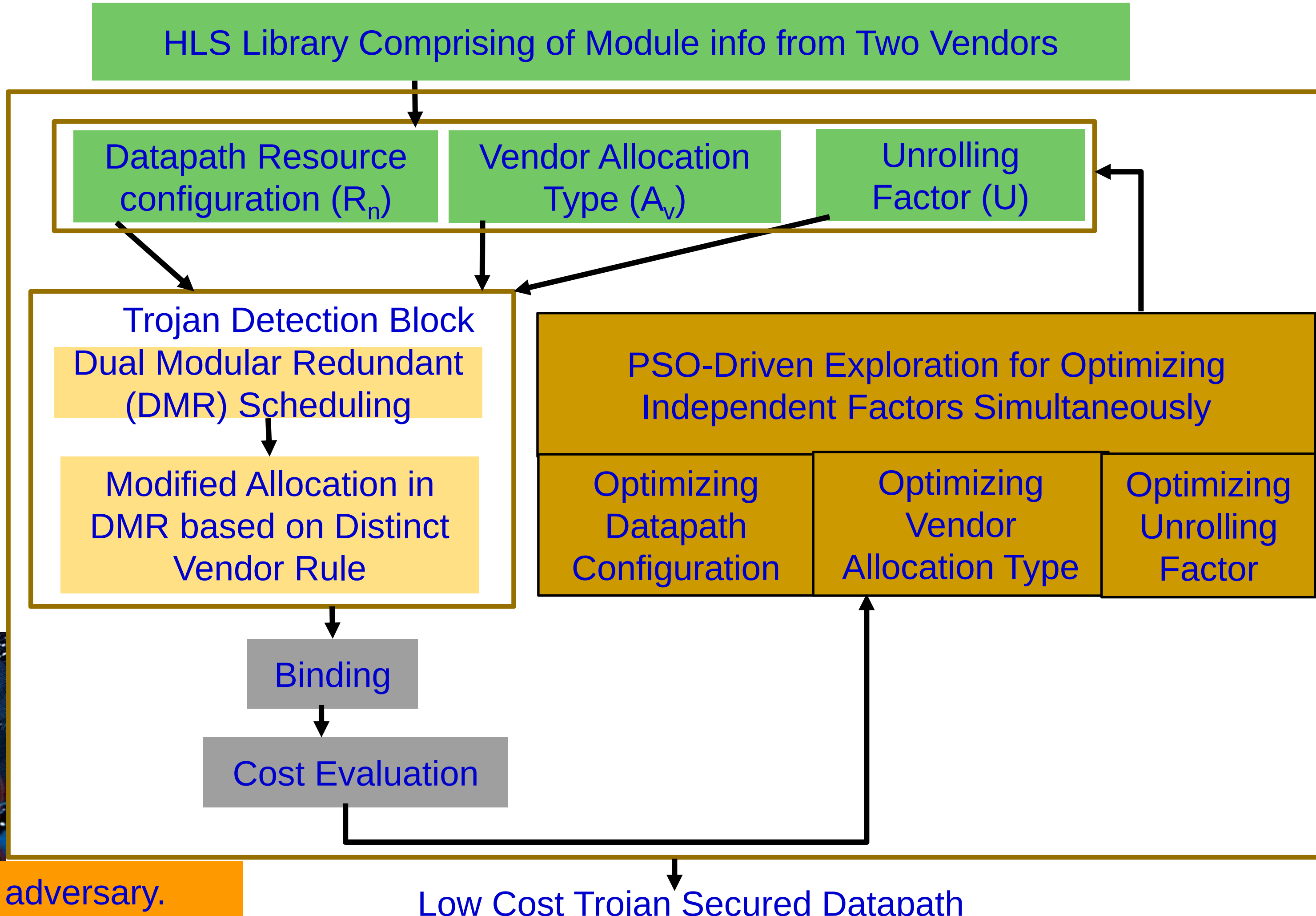
Write Operation



Read Operation

Source: Mohanty 2013, Springer CSSP Aug 2013

Trojan Secure Digital Hardware Synthesis



Provide backdoor to adversary.
Chip fails during critical needs.

Source: Sengupta, Mohanty 2017: TCAD April 2017

How Secure is AES Encryption?

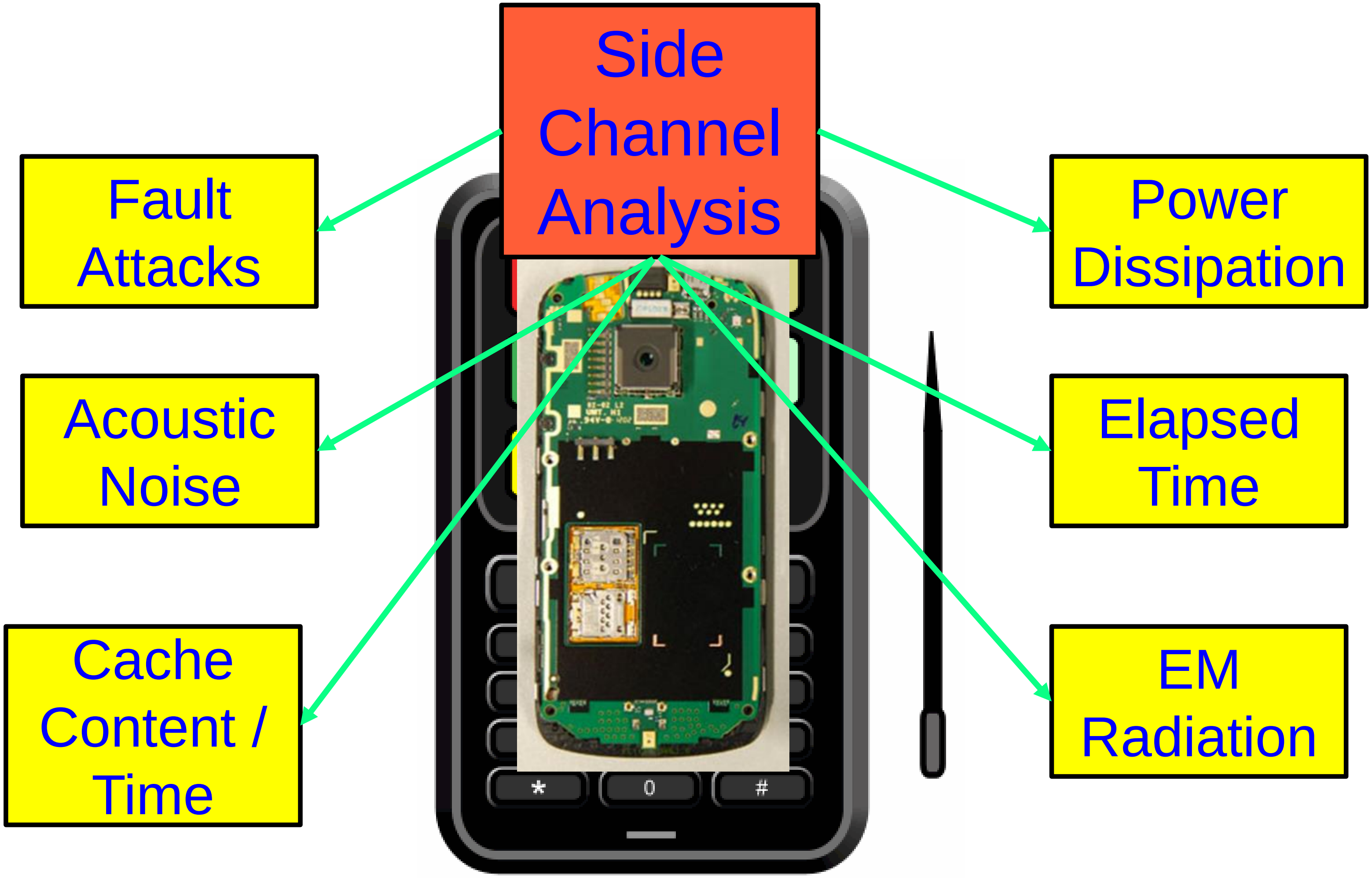
- Brute force a 128 bit key ?
- If you assume
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, you can crack the key after testing 50% of the possibilities
  - Then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

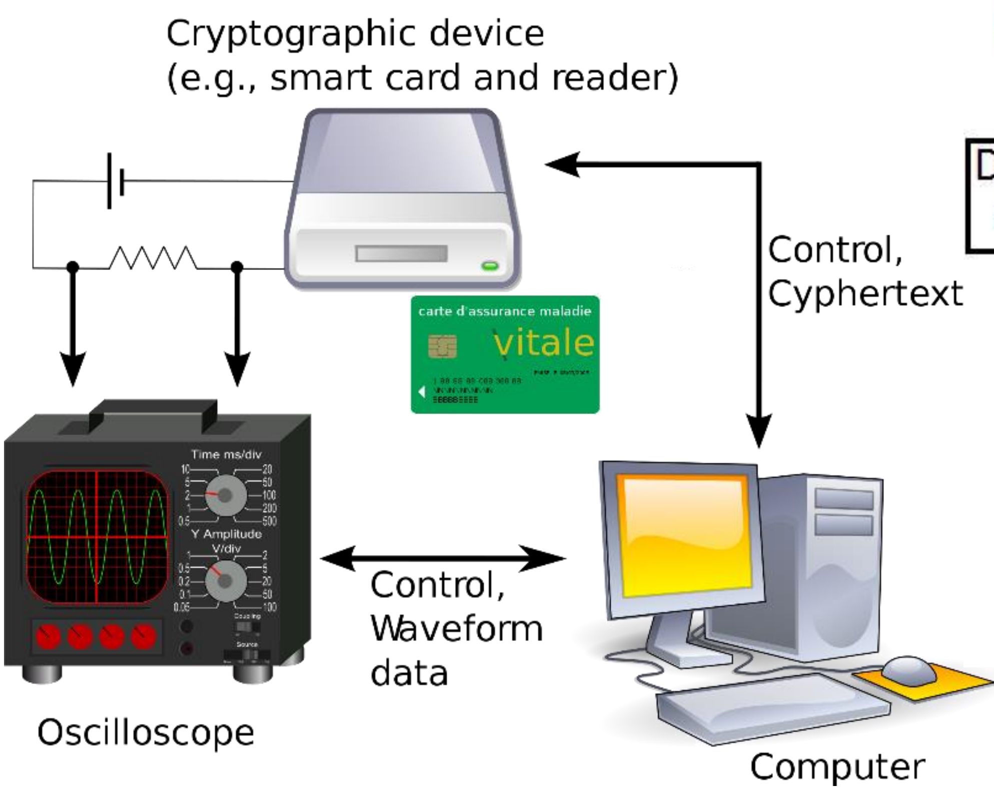
Source: Parameswaran Keynote iNIS-2017

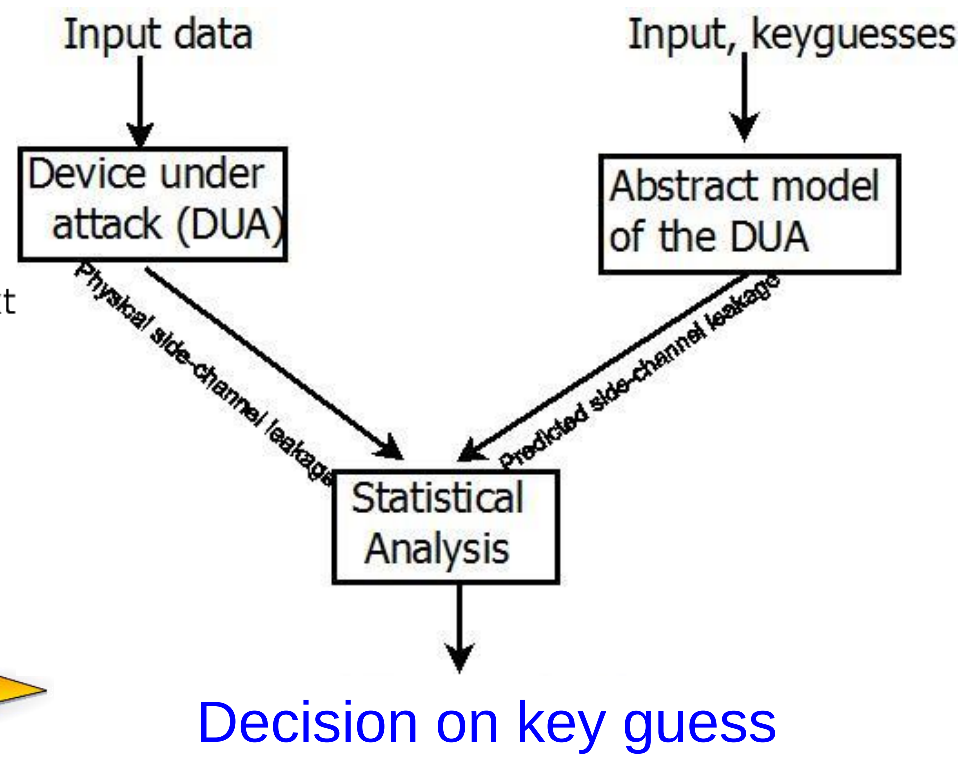
Side Channel Analysis Attacks



Source: Parameswaran Keynote iNIS-2017

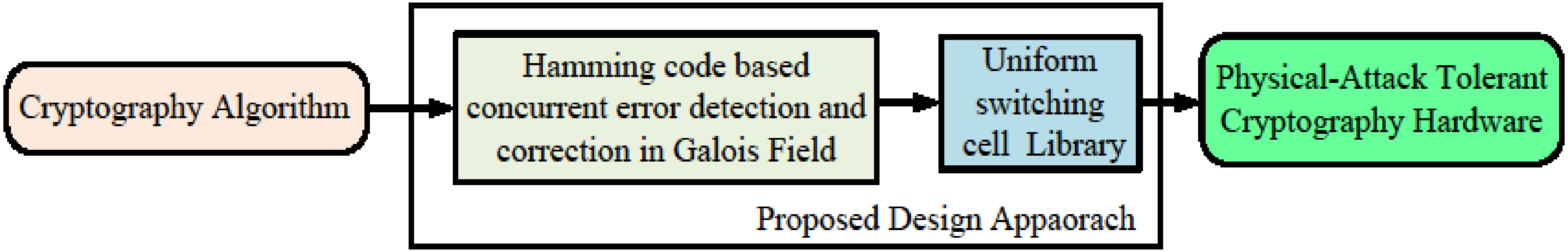
Side Channel Attacks – Differential and Correlation Power Analysis (DPA/CDA)

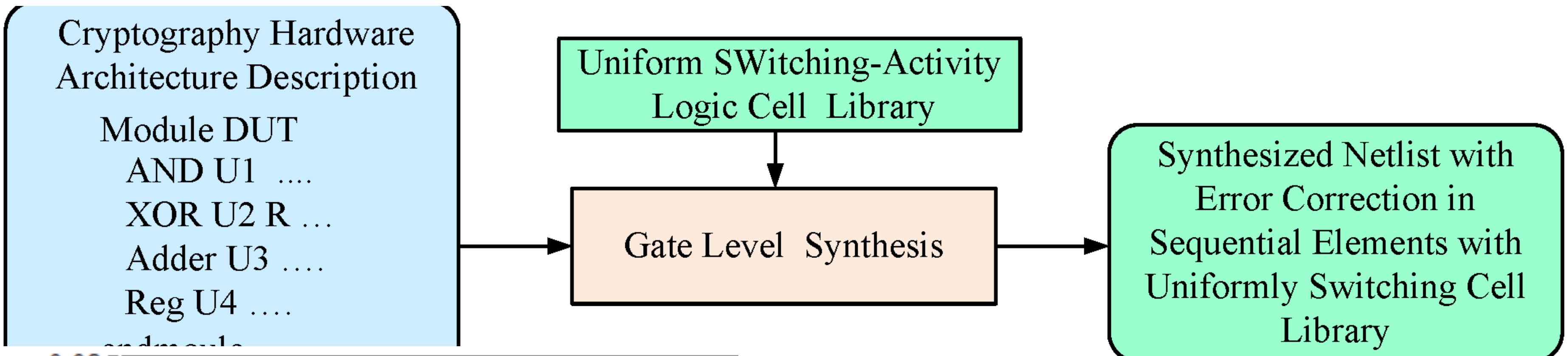


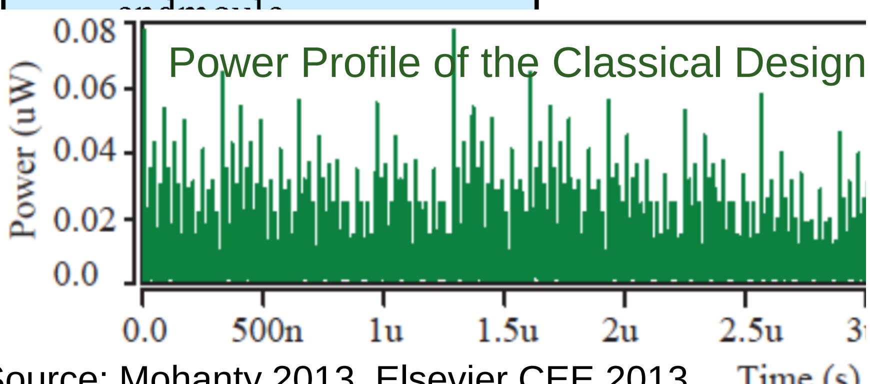


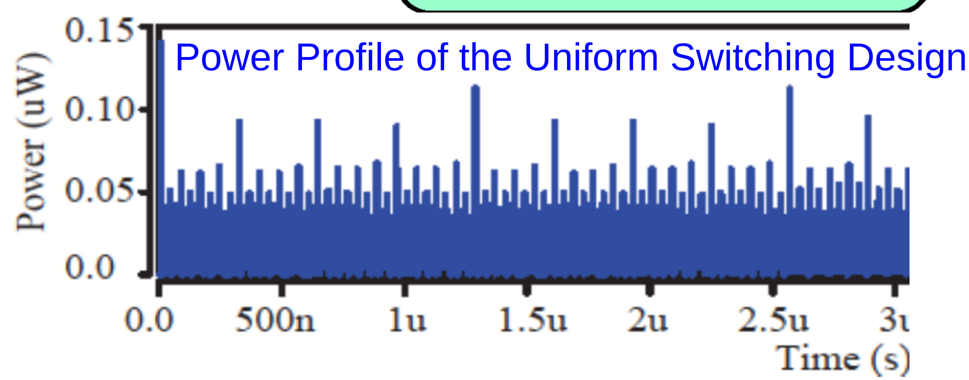
Source: Mohanty 2018, ZINC Keynote 2018

DPA Resilience Hardware: Synthesis





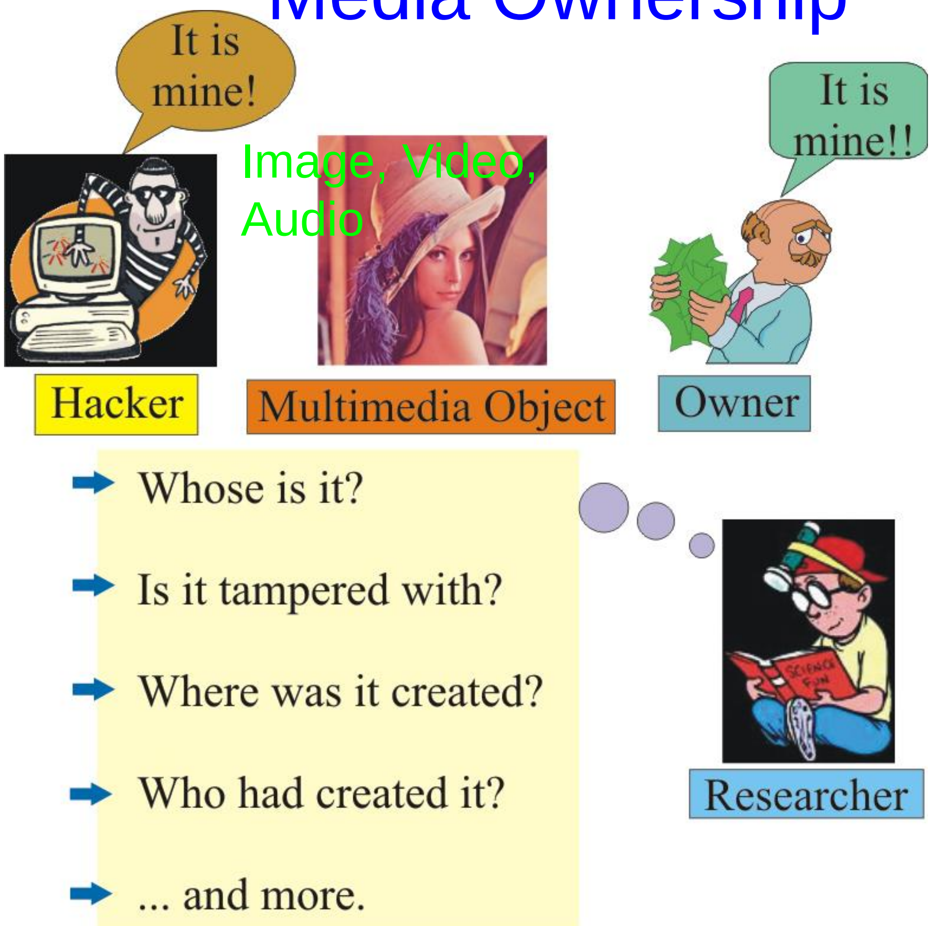




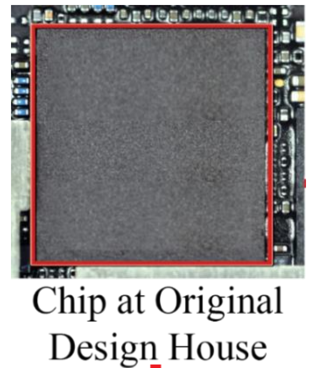
Source: Mohanty 2013, Elsevier CEE 2013.

Copyright, Intellectual Property (IP), Or Ownership Protection

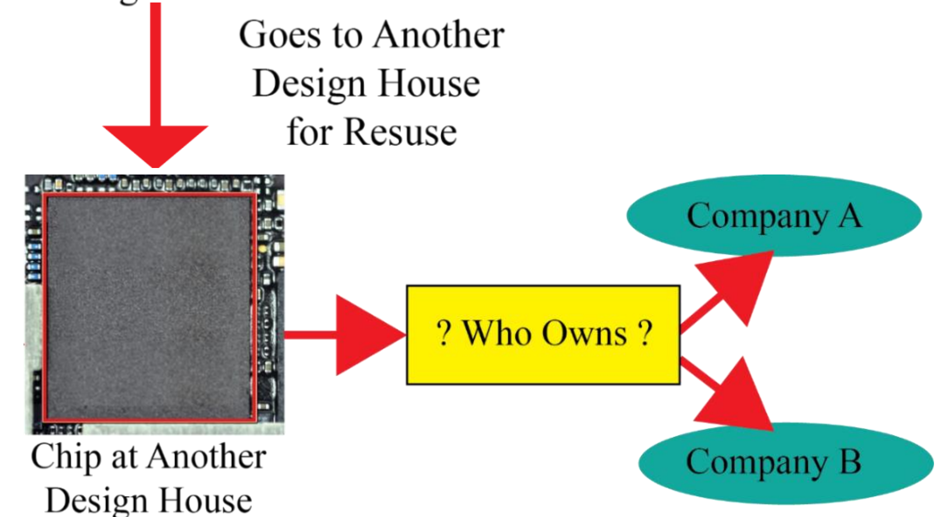
Media Ownership



Hardware Ownership

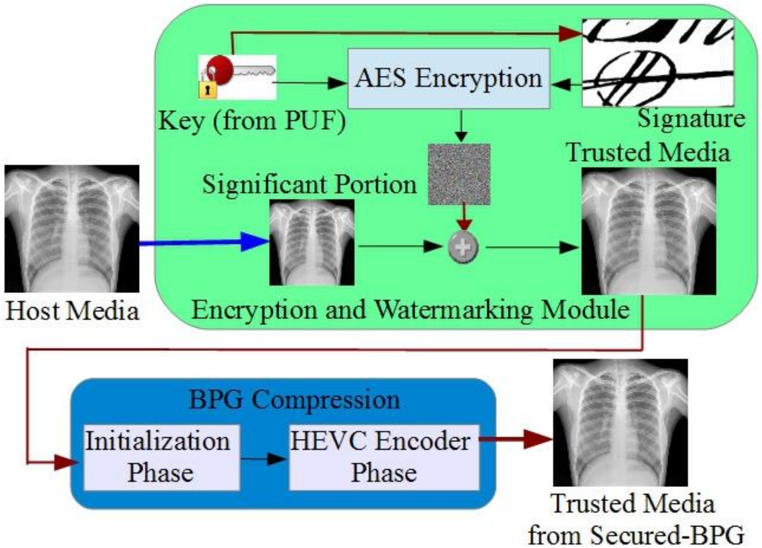


IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.

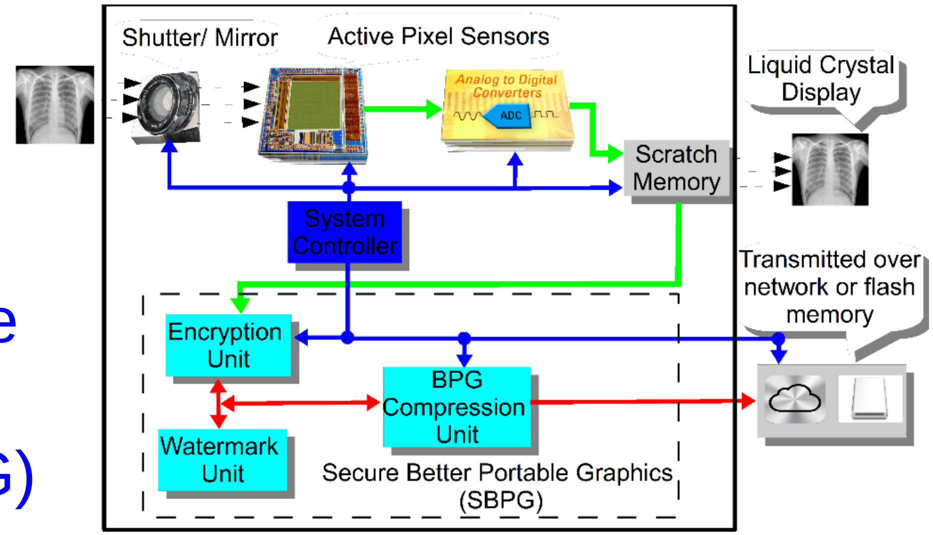


Source: Mohanty ZINC 2018 Keynote

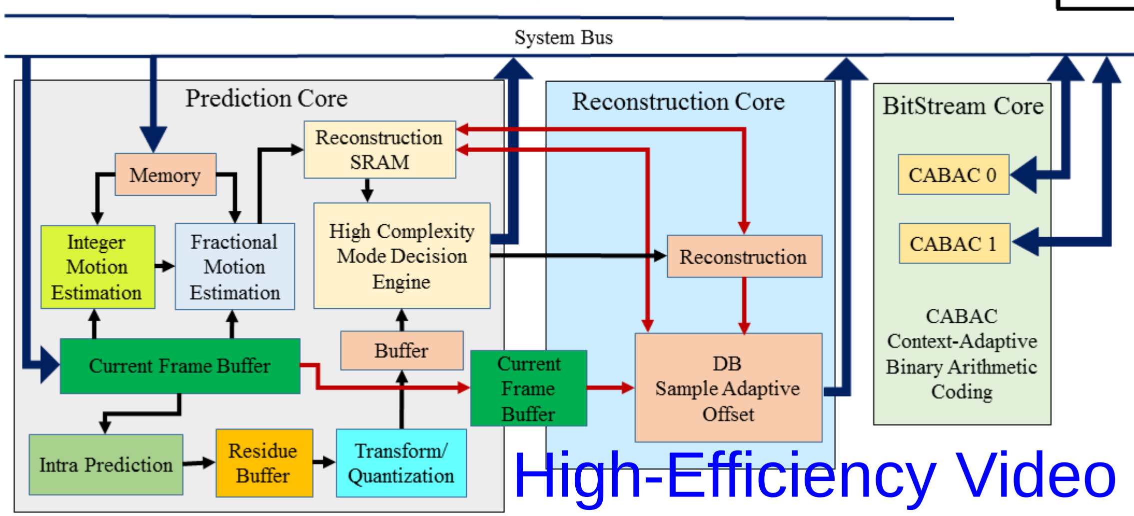
Secure Better Portable Graphics (SBPG)



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: Mohanty 2018, IEEE-Access 2018

Counterfeit Hardware – IP Attacks

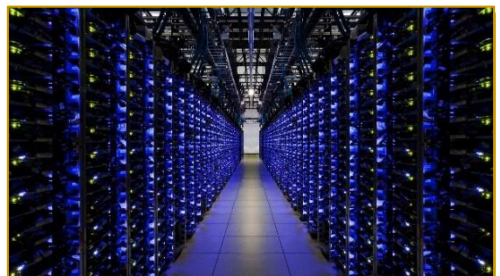
2014 Analog Hardware Market (Total Shipment Revenue US $)

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%)



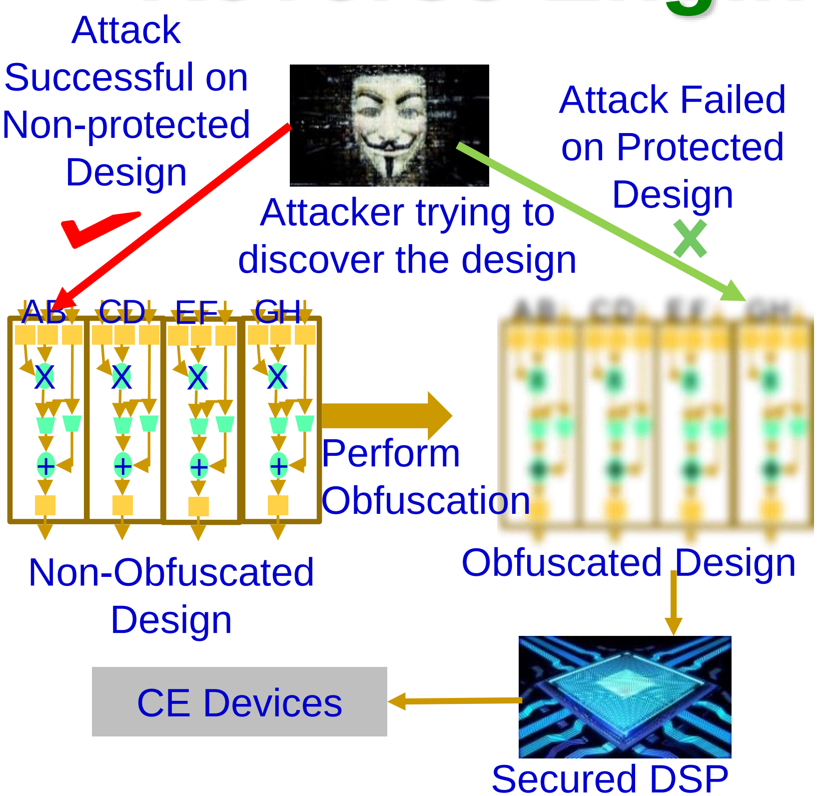
Data Processing
$6.0 billion (11%)

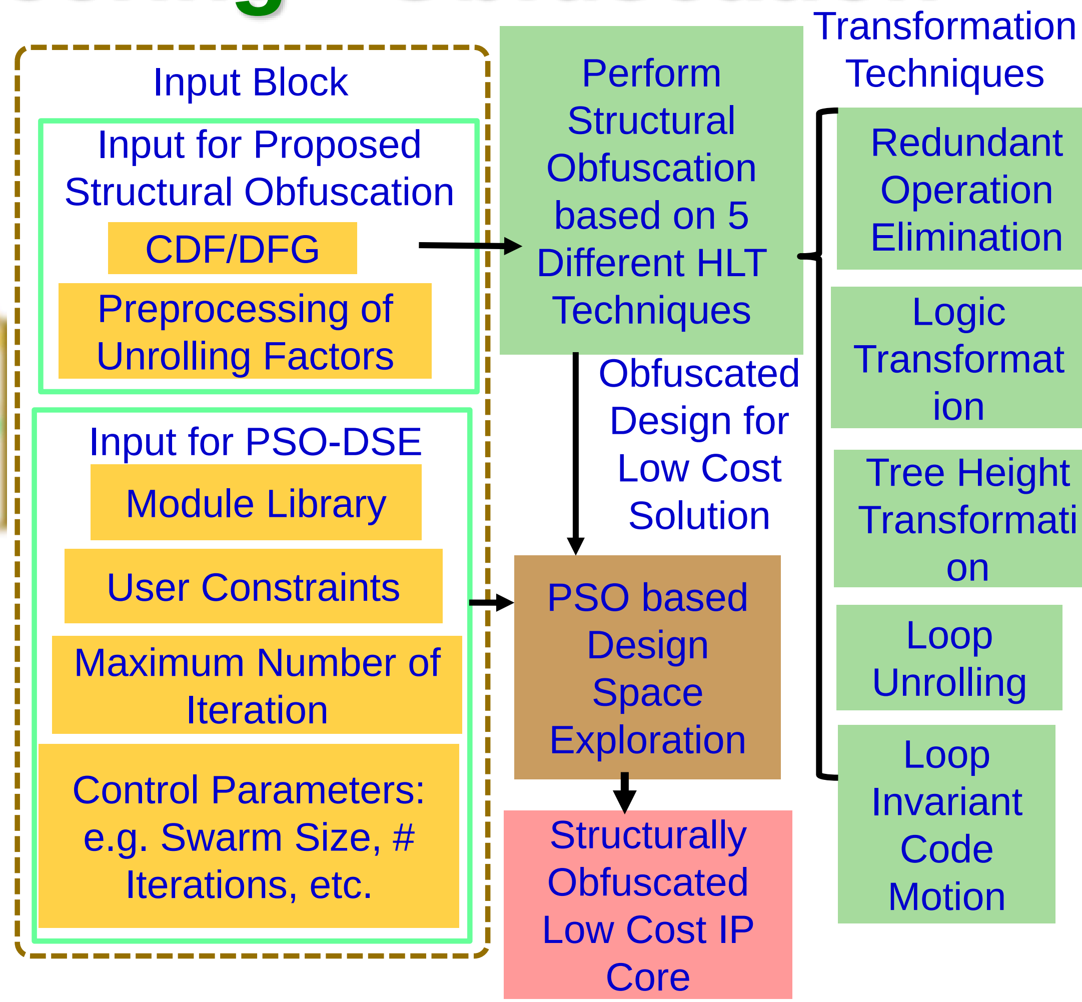
Wired Communications
$2.9 billion (5.4%)

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

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

Digital Hardware Synthesis to Prevent Reverse Engineering - Obfuscation





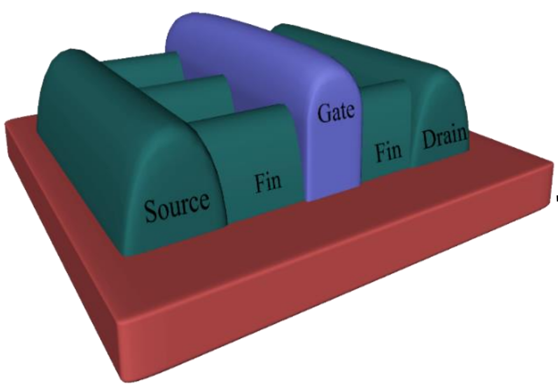
Obfuscation – Intentional modification of the description or the structure of electronic hardware to conceal its functionality for making reverse-engineering difficult.

Source: Sengupta, Mohanty 2017, TCE November 2017

PUF - Principle

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

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



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

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

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

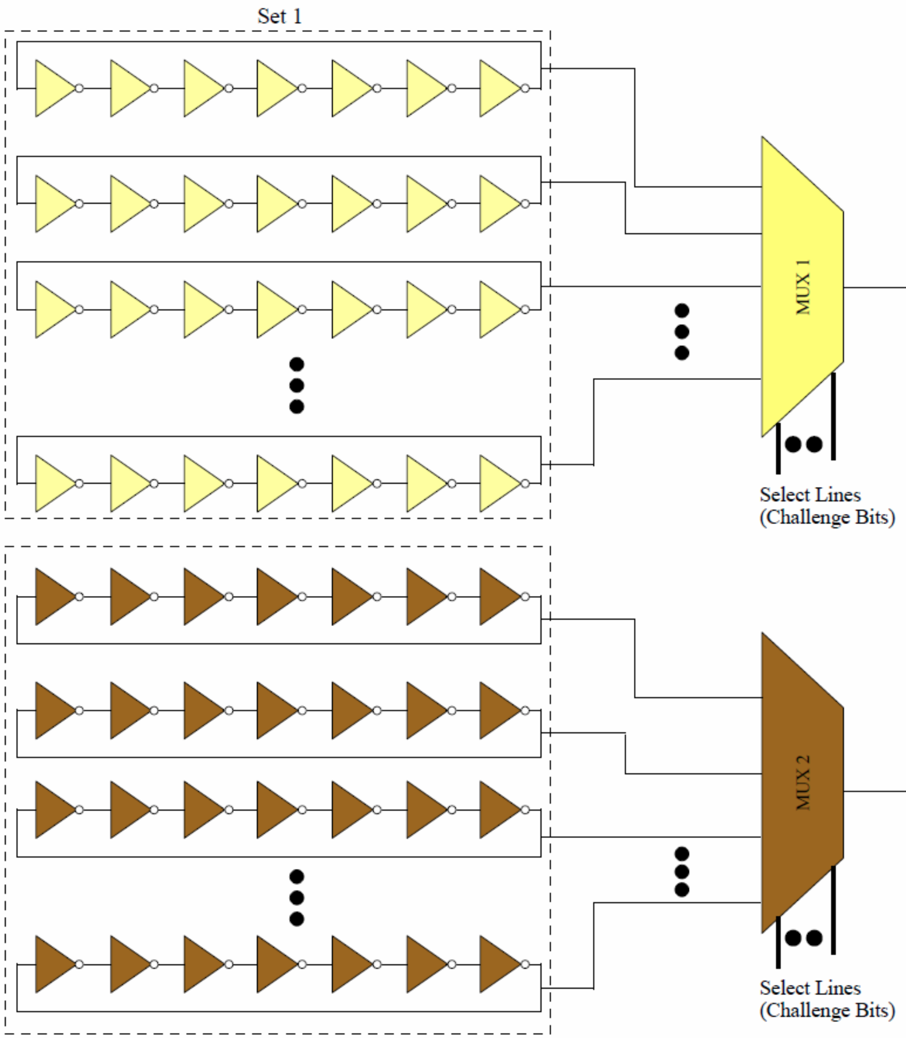
Challenge Response (Outputs from a PUF Module)

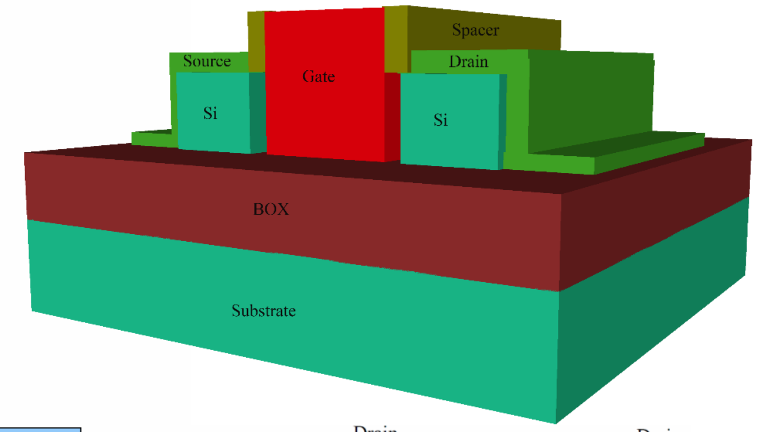
Random Binary Output 010101 …

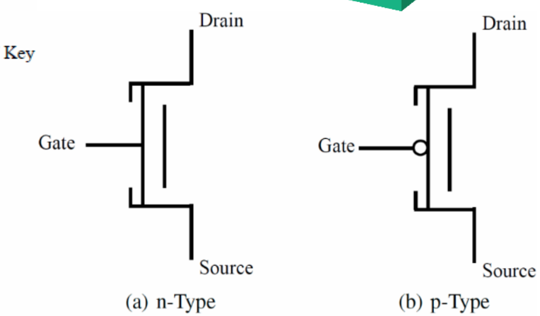
PUFs don’t store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

Source: Mohanty 2017, Springer ALOG 2017

Power Optimized Hybrid Oscillator Arbiter PUF



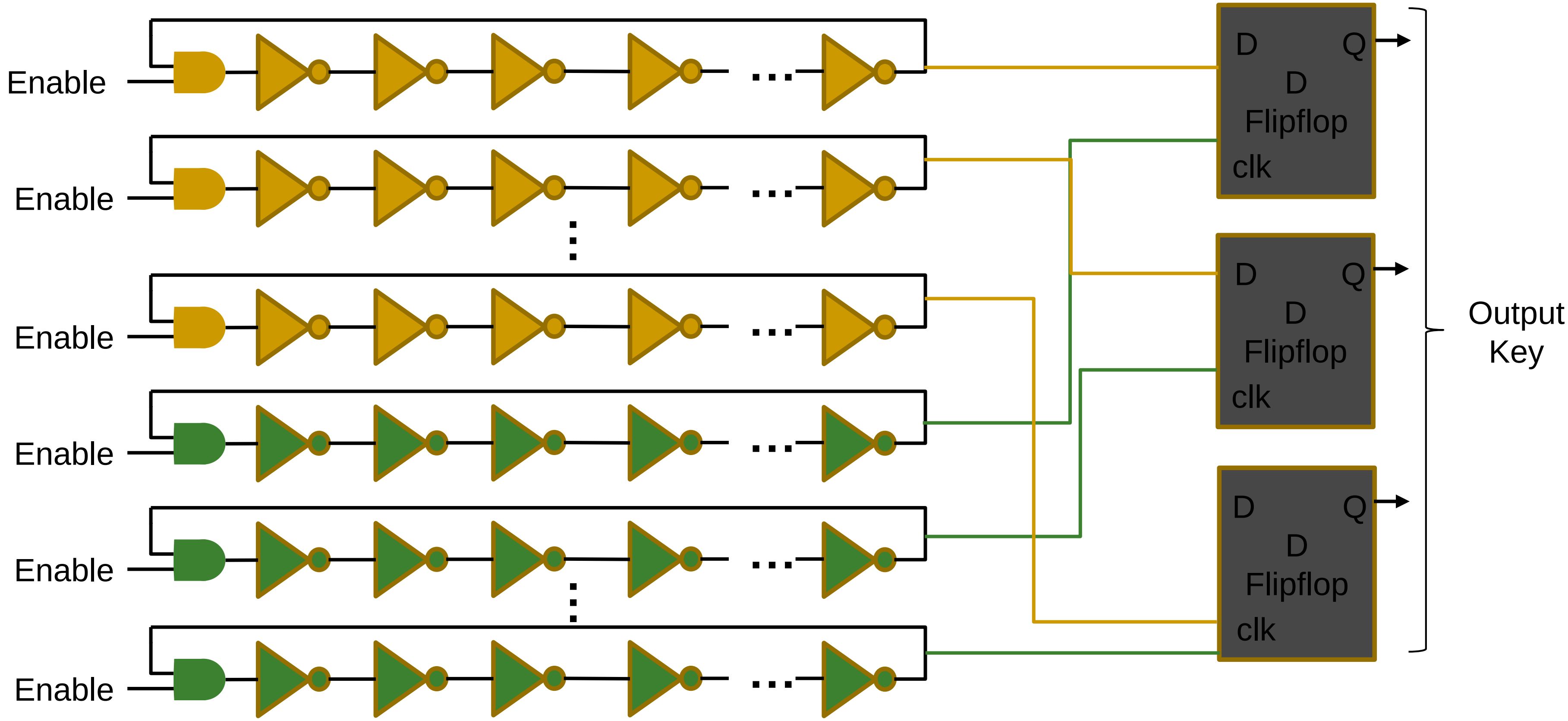




Characteristics	FinFET Technology	DLFET Technology
Average Power	219.34 μW	121.3 μW
Hamming Distance	49.3 %	48 %
Time to generate key	150 ns	150 ns

Source: Mohanty 2018, TSM May 2018
Source: Mohanty 2017, Springer ALOG 2017

Speed Optimized Hybrid Oscillator Arbiter PUF



Characteristics	FinFET Technology	DLFET Technology
Average Power	250.15 mW	151 μW
Hamming Distance	49.6 %	50 %
Time to generate key	50 ns	50 ns

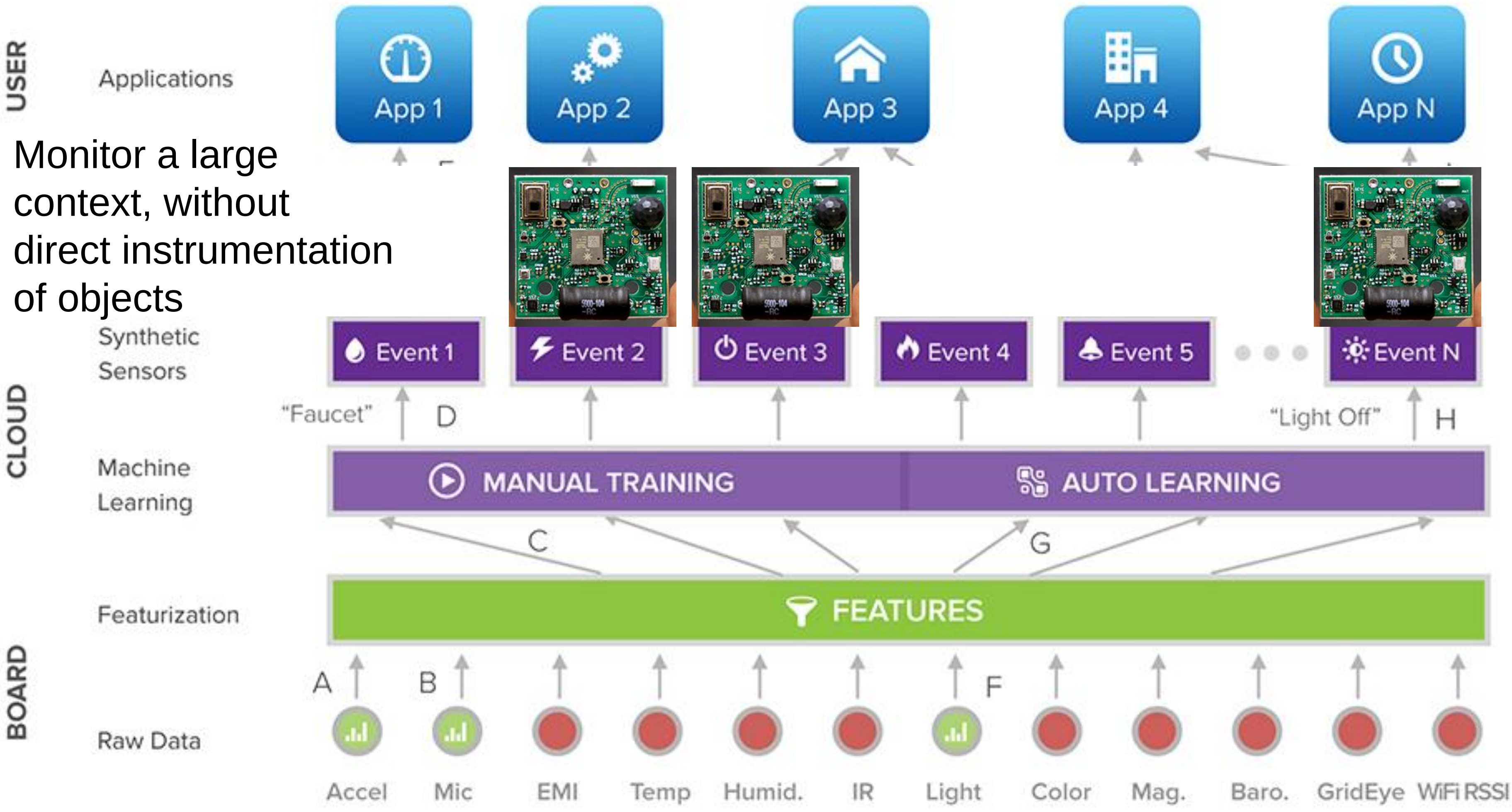
Source: Mohanty 2018, TSM May 2018

Source: Mohanty 2017, Springer ALOG 2017

Response Smart

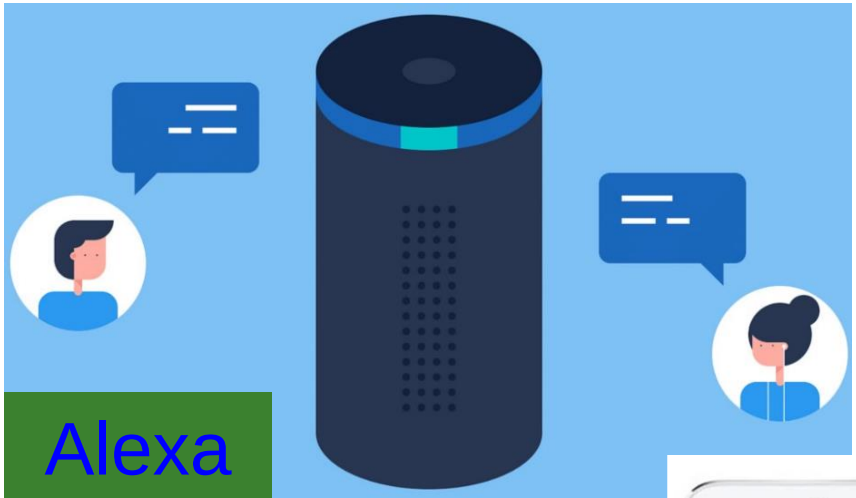
Smart Sensors - General-Purpose/ Synthetic Sensors

Monitor a large context, without direct instrumentation of objects



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

Systems – End Devices

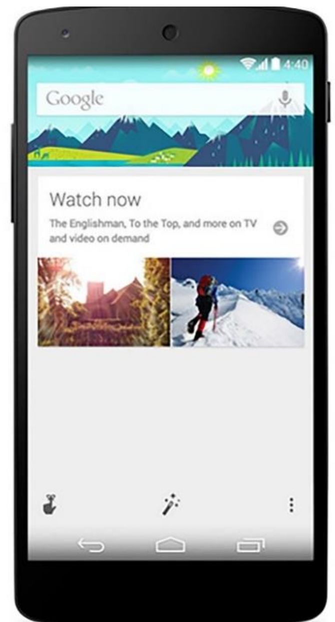


Alexa

Google Now

Windows Cortana

Apple Siri

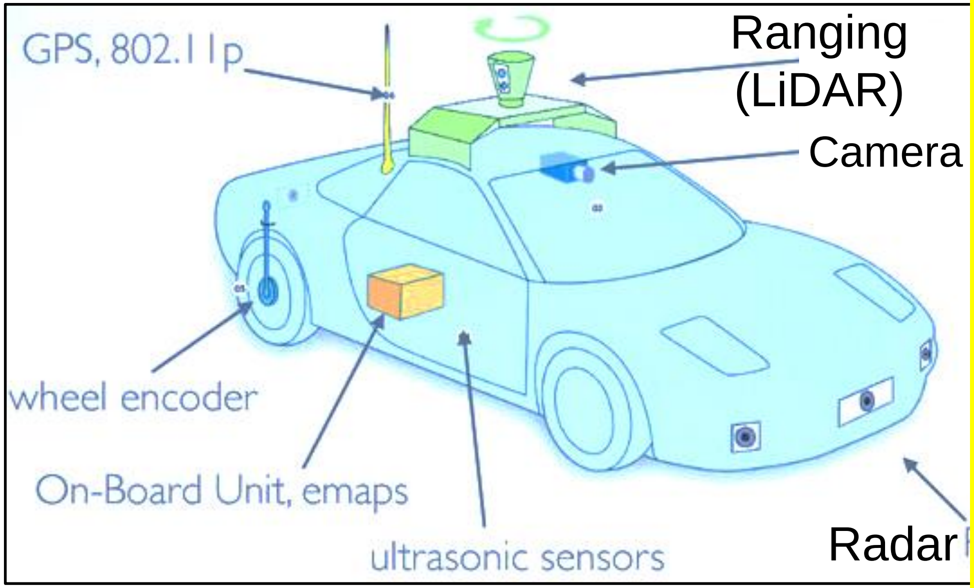


Smart Electronic Systems Laboratory (SESL)

UNT

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

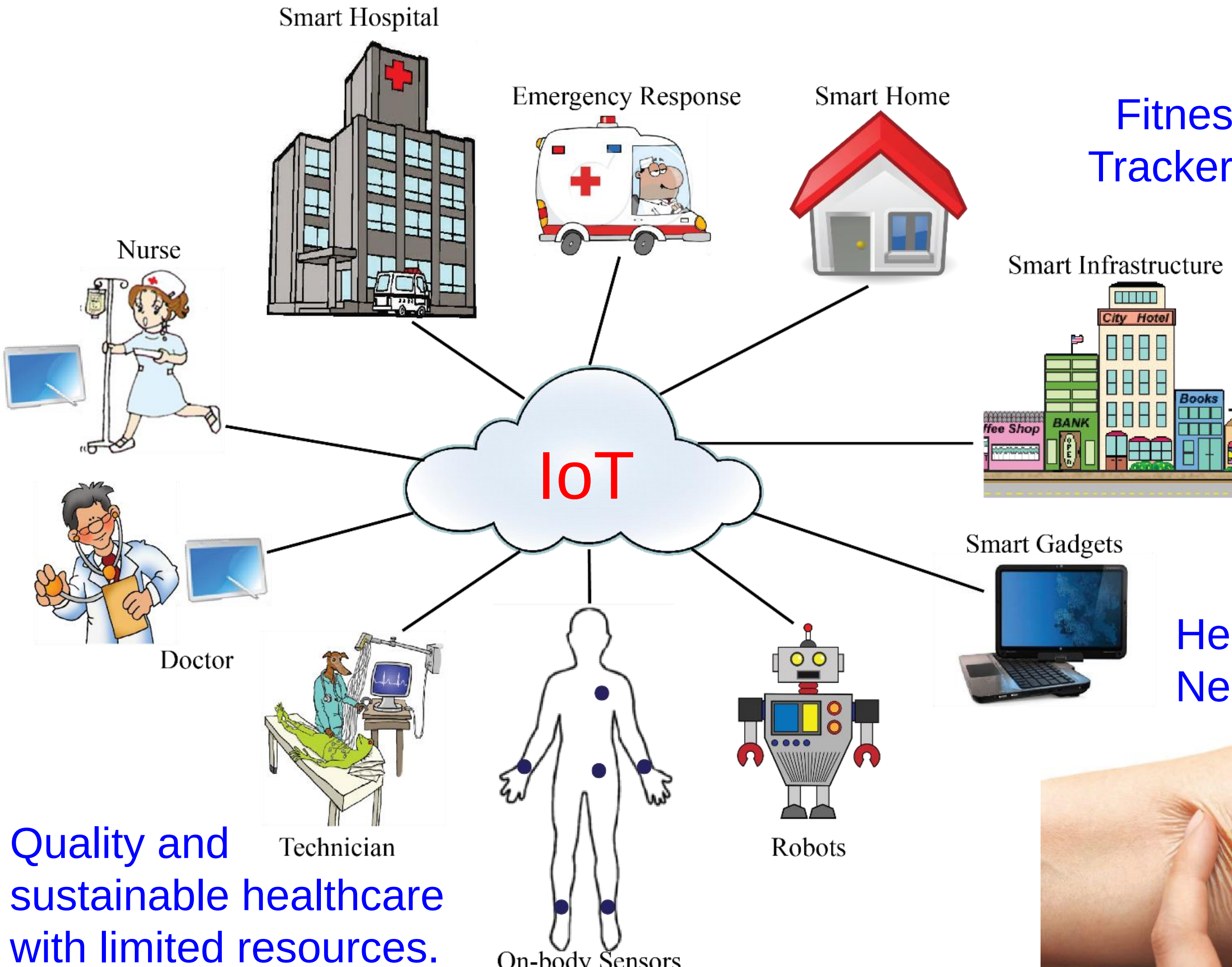
Level 5

- All Safety-Critical Functions in All Environments and Scenarios

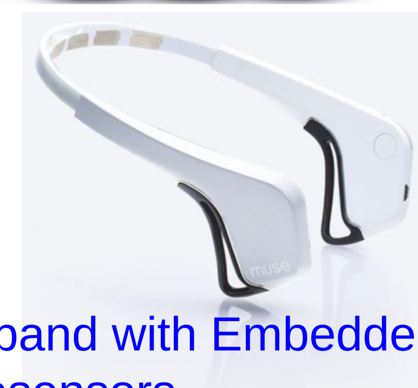
"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Datta 2017: CE Magazine Oct 2017

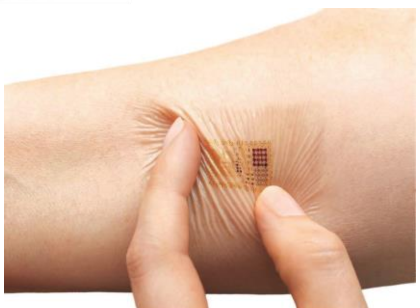
Smart Healthcare – using IoMT



Fitness Trackers



Headband with Embedded Neurosensors



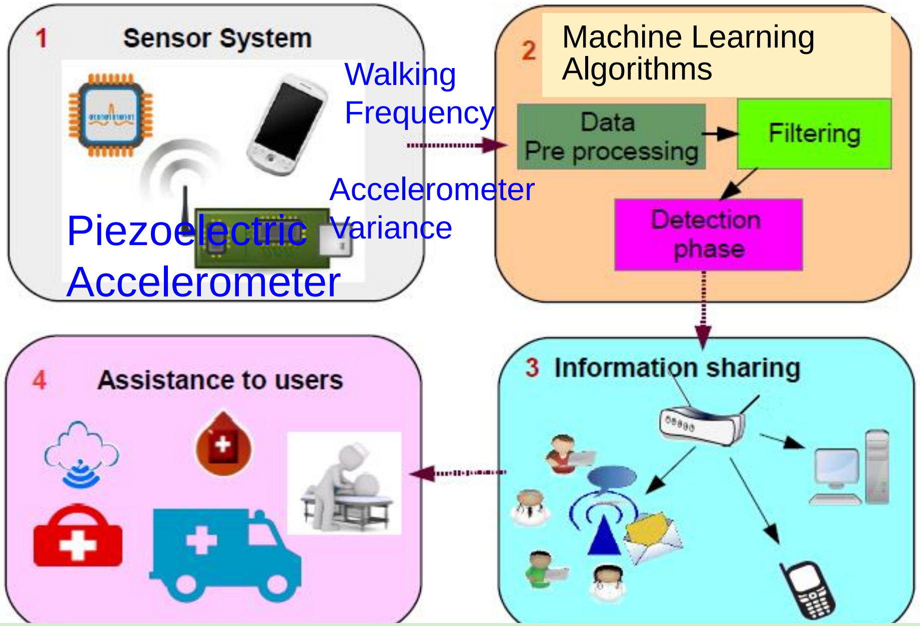
Embedded Skin Patches

Quality and sustainable healthcare with limited resources.

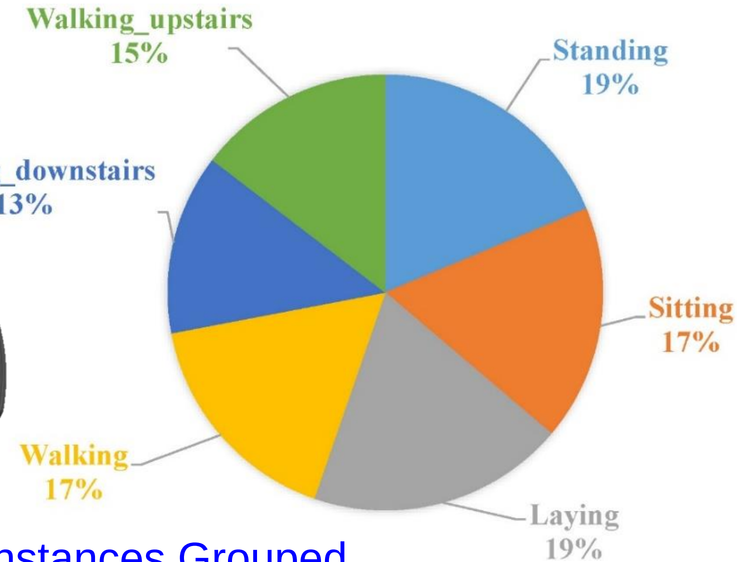
Source: Mohanty 2016, CE Magazine July 2016

Sethi 2017: JECE 2017

Smart Healthcare - Smart-Walk



Automated Physiological Monitoring System



10291 Instances Grouped Under 6 Activities - Kaggle

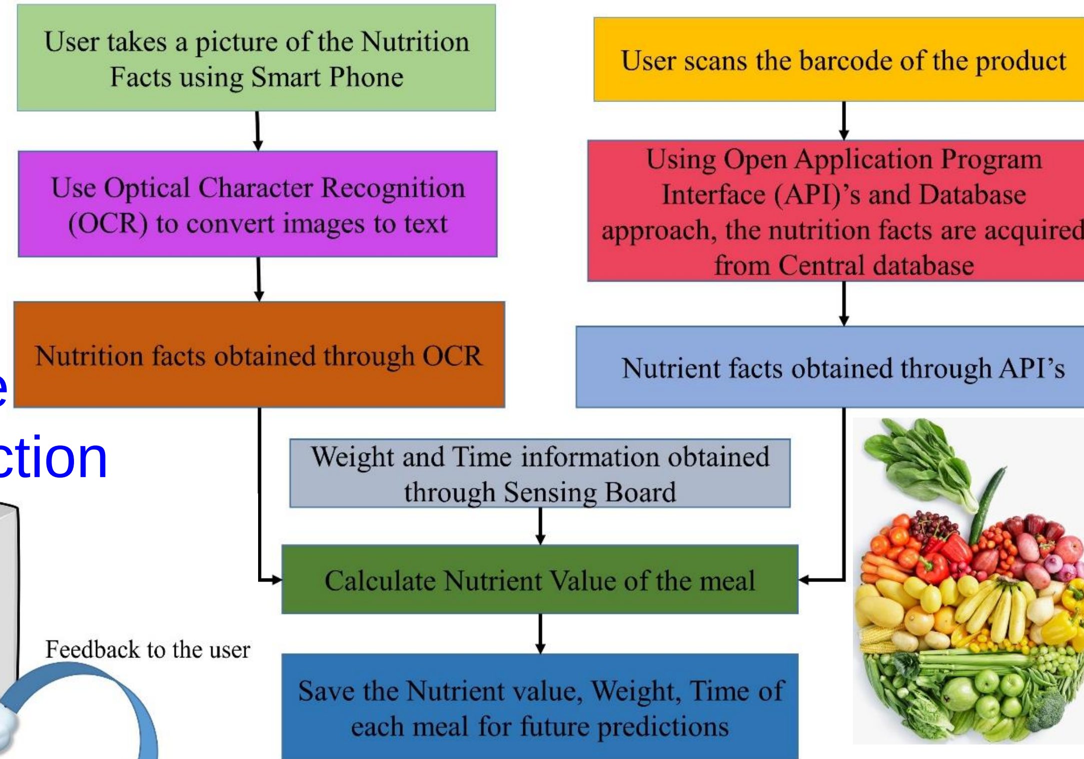
Research Works	Method	Features considered	Activities	Accuracy (%)
This Work	Adaptive algorithm based on feature extraction (WEKA)	Step detection and Step length estimation	Walking, sitting, standing, etc.	97.9

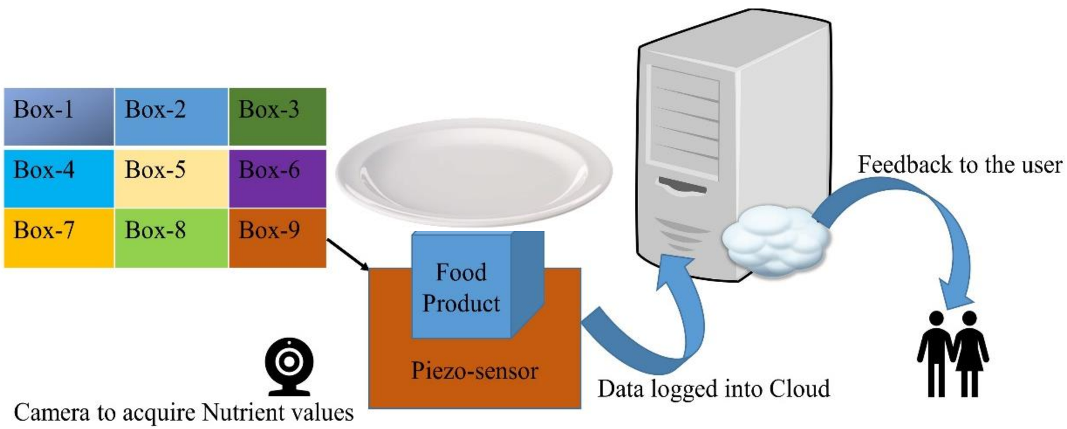
Source: Mohanty ICCE 2018

Smart Healthcare - Smart-Log

Automated Food intake Monitoring and Diet Prediction System

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





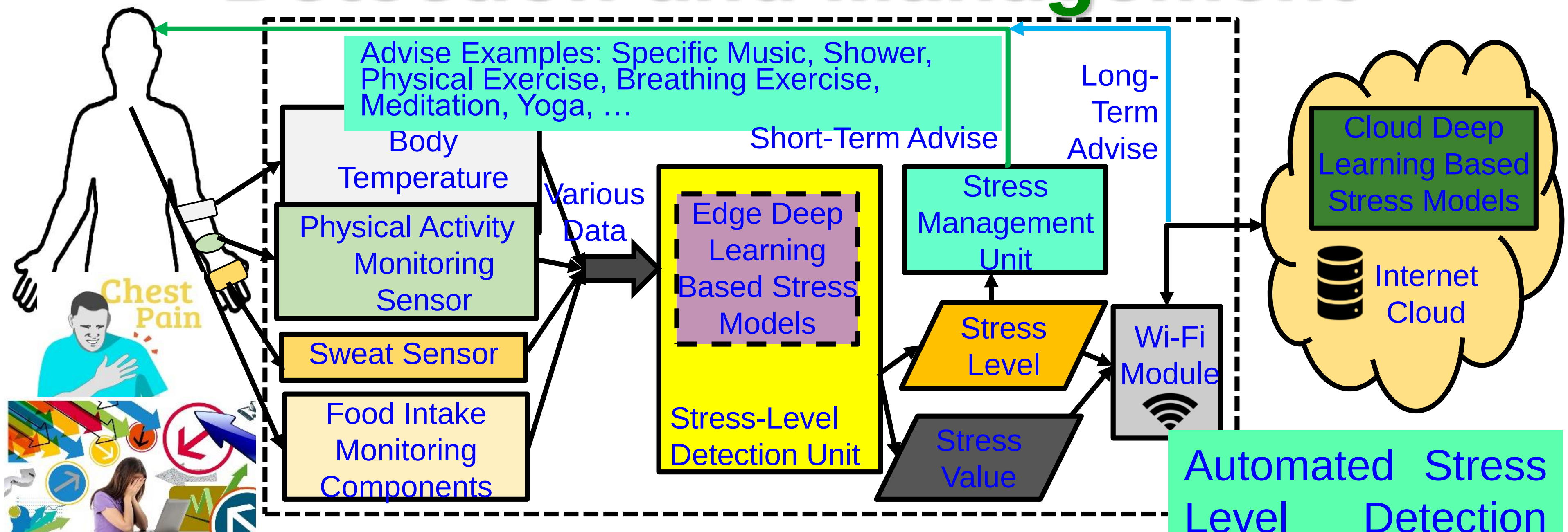
USDA National Nutrient Database for Standard Reference is used for nutrient values of 8791 items.

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

8172 user instances were considered

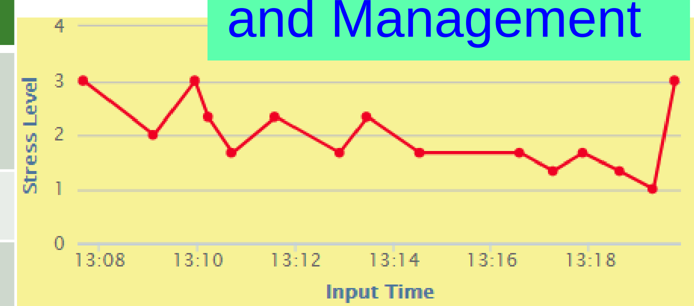
Source: Mohanty ICCE 2018

Smart Healthcare – Stress Level Detection and Management



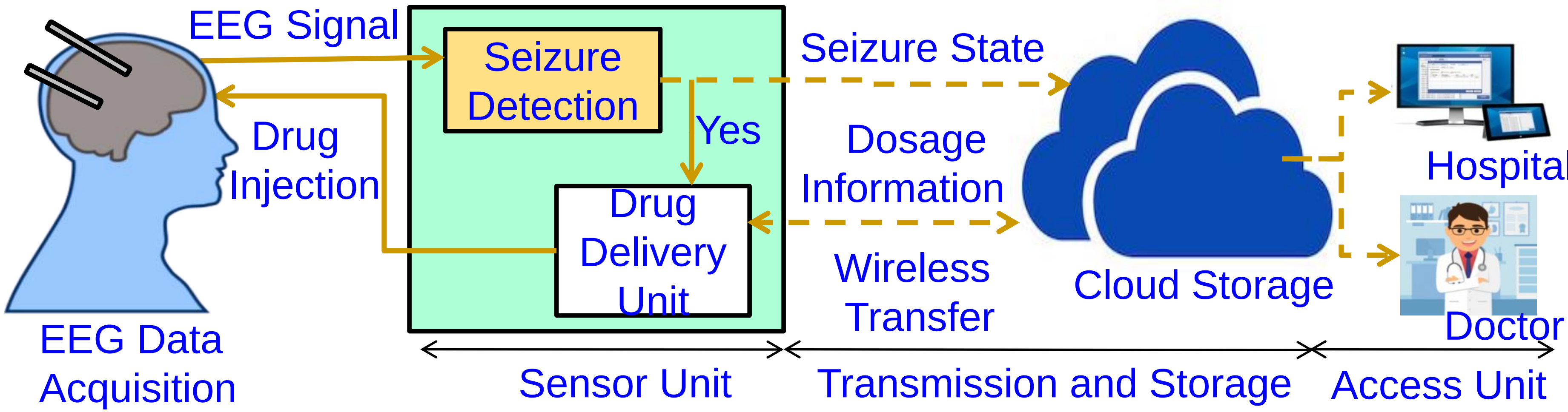
Automated Stress Level Detection and Management

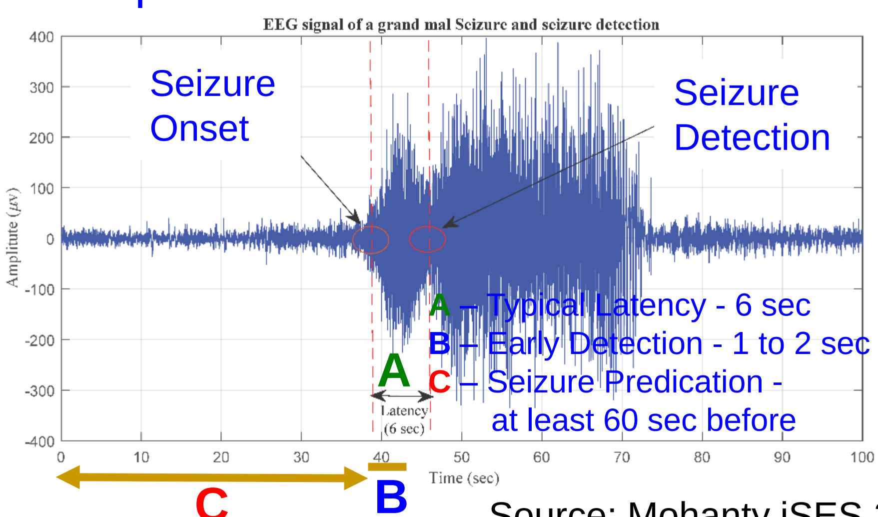
Sensor	Low Stress	Normal Stress	High Stress
Accelerometer (steps/min)	0-75	75-100	101-200
Humidity (RH%)	27-65	66-91	91-120
Temperature ℉	98-100	90-97	80-90



Source: Mohanty iSES 2018 and Mohanty ICCE 2019

Smart Healthcare – Seizure Detection and Control



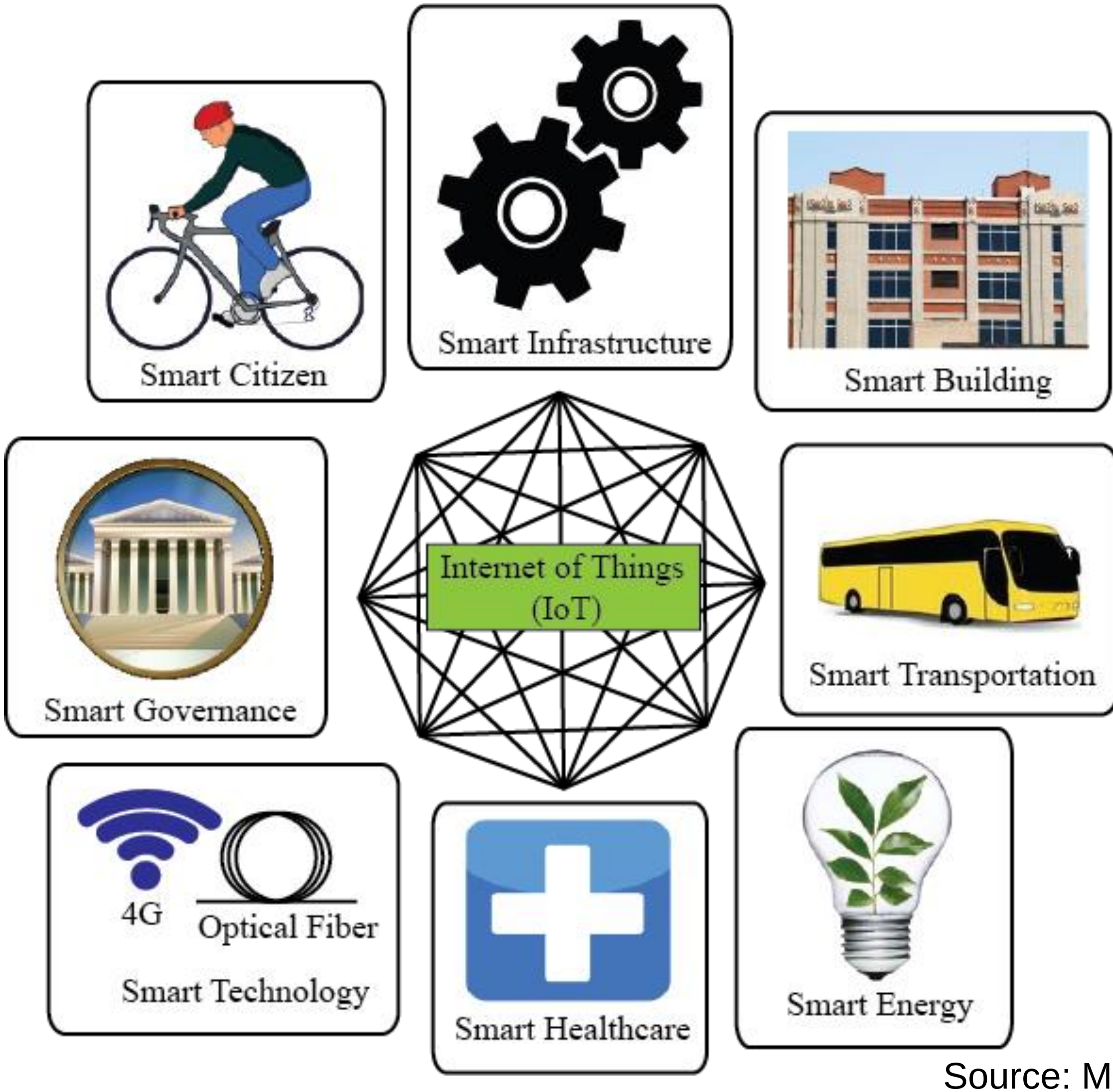


Automated Epileptic Seizure Detection and Control System

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

Source: Mohanty iSES 2018, IEEE Smart Cities 2018, and Mohanty ICCE 2019

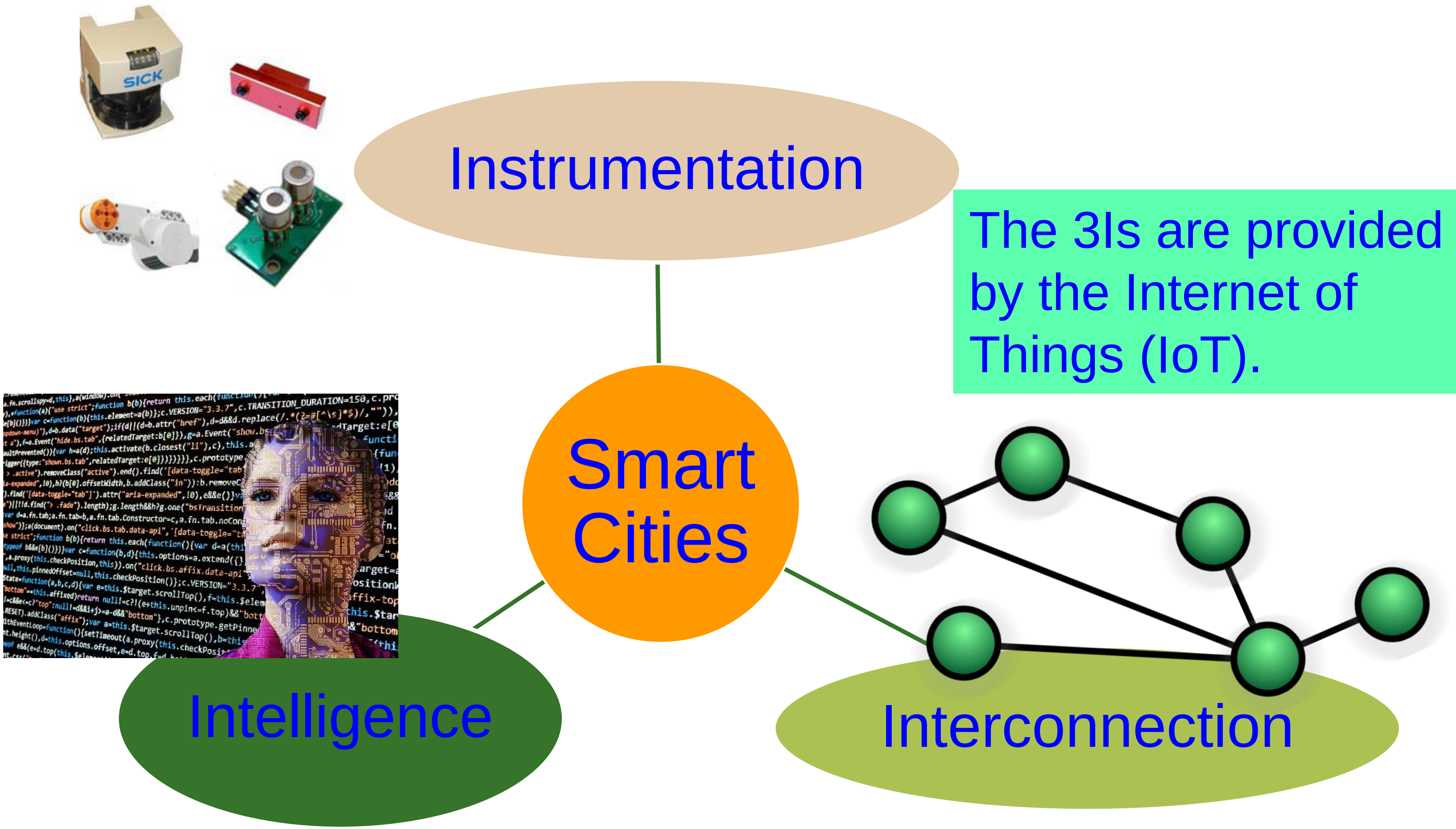
System of Systems - Smart Cities



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

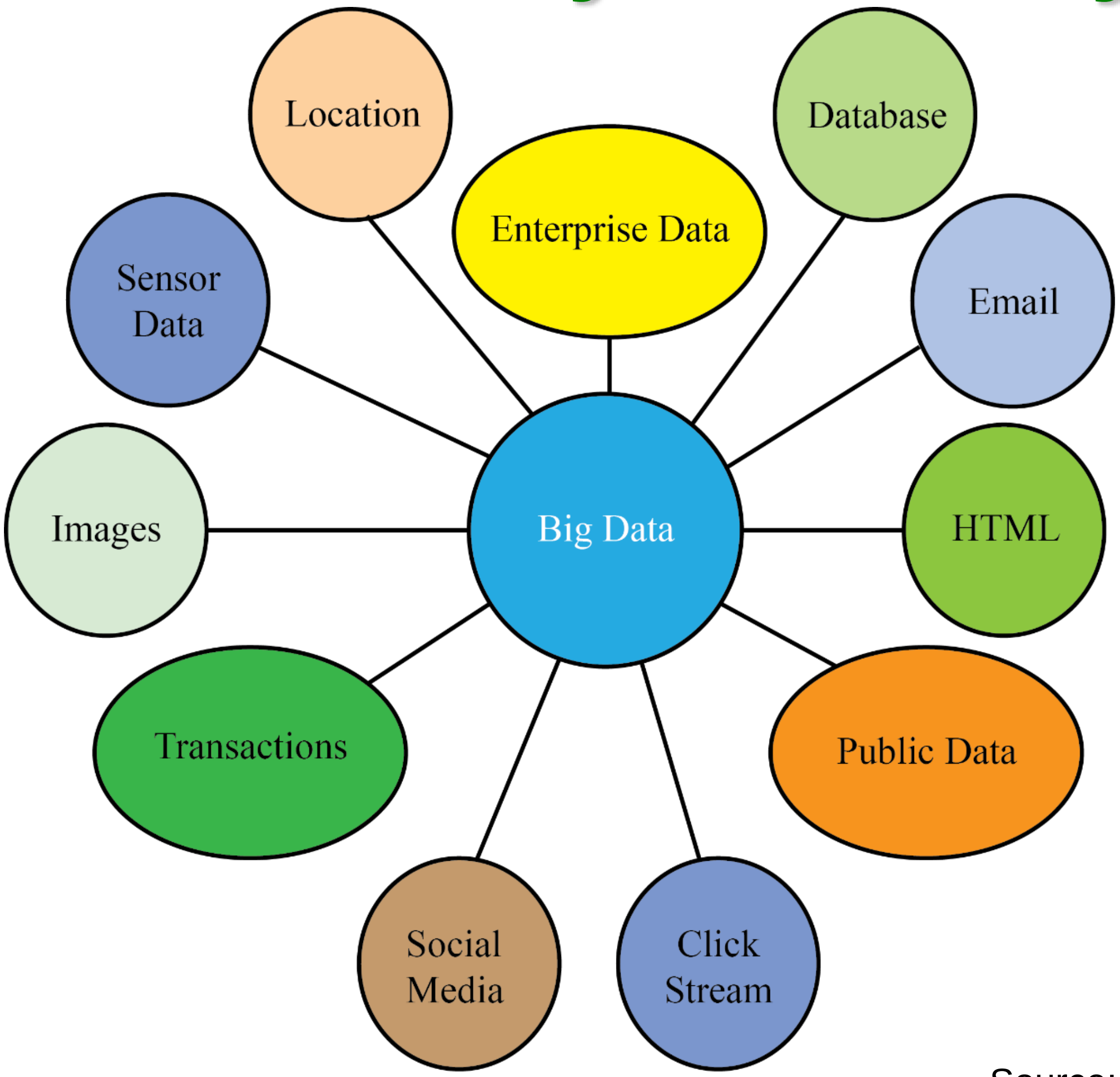
Source: Mohanty 2016, CE Magazine July 2016

Smart Cities - 3 Is



Source: Mohanty ICIT 2017 Keynote

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: Mohanty 2016, CE Magazine July 2016

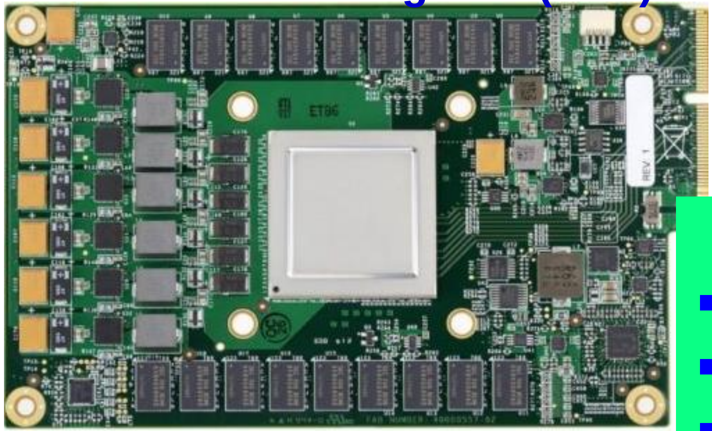
Artificial Intelligence Technology

Machine Learning

Deep Learning

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

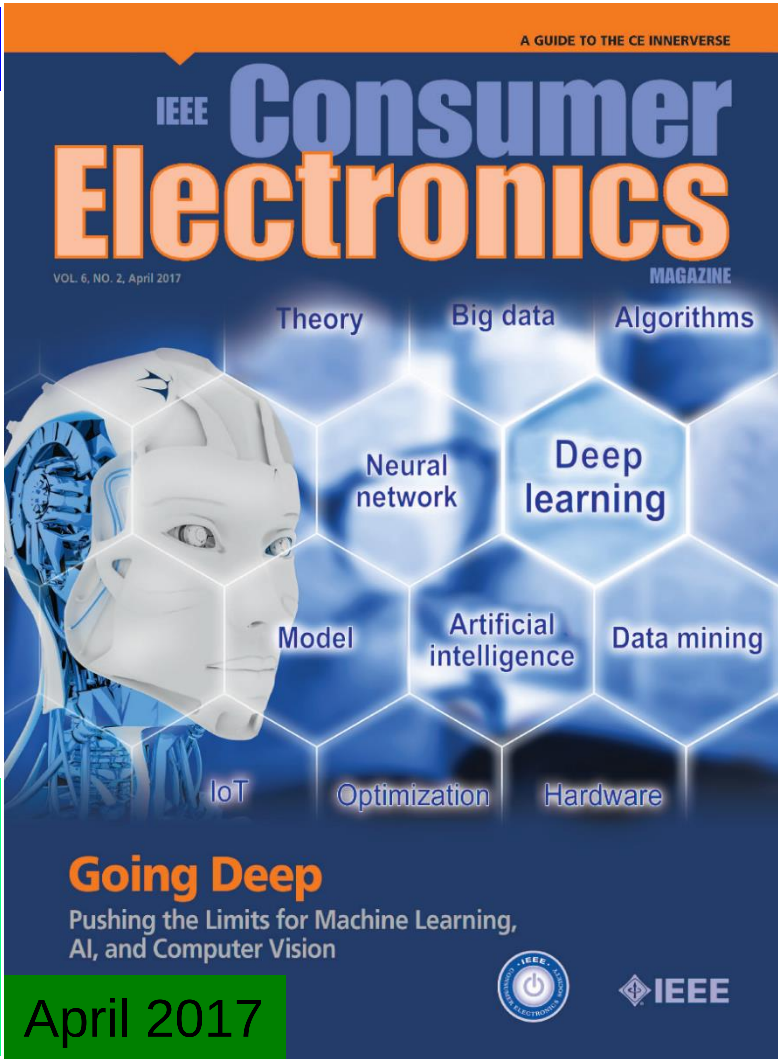
Tensor Processing Unit (TPU)



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

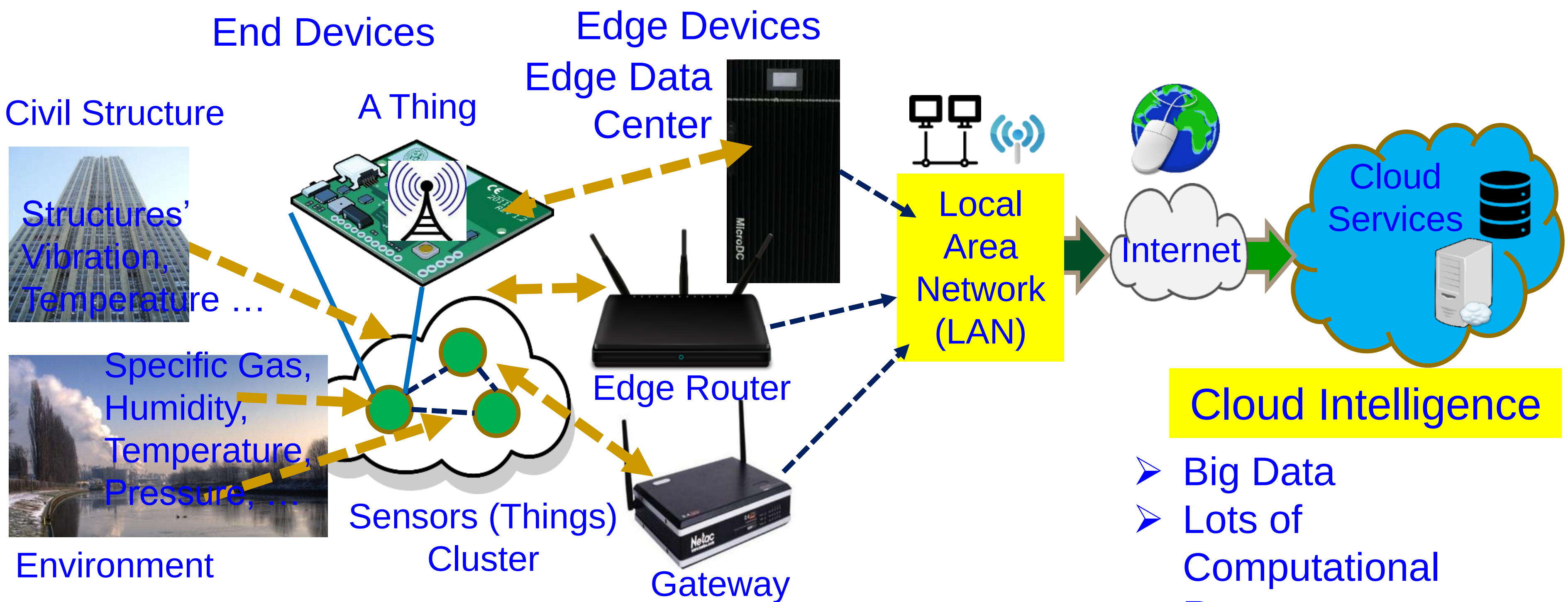
Smart City Use:

- Better analytics
- Better decision
- Faster response



April 2017

Edge Vs Cloud Intelligence



Cloud Intelligence

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

Edge Intelligence

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

Source: https://www.iec.ch/whitepaper/pdf/IEC_WP_Edge_Intelligence.pdf

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)

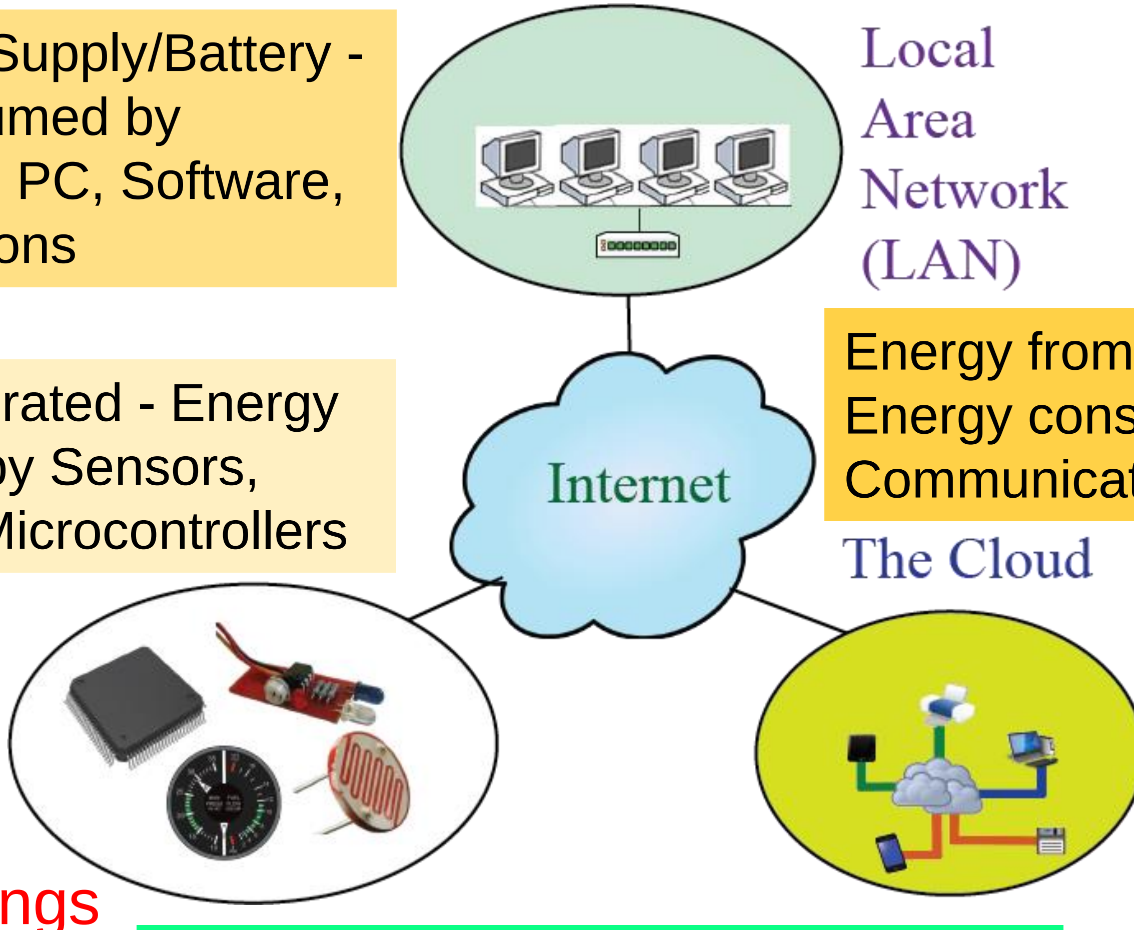
Energy Consumption in IoT

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

Battery Operated - Energy consumed by Sensors, Actuators, Microcontrollers

Energy from Supply/Battery - Energy consumed by Communications

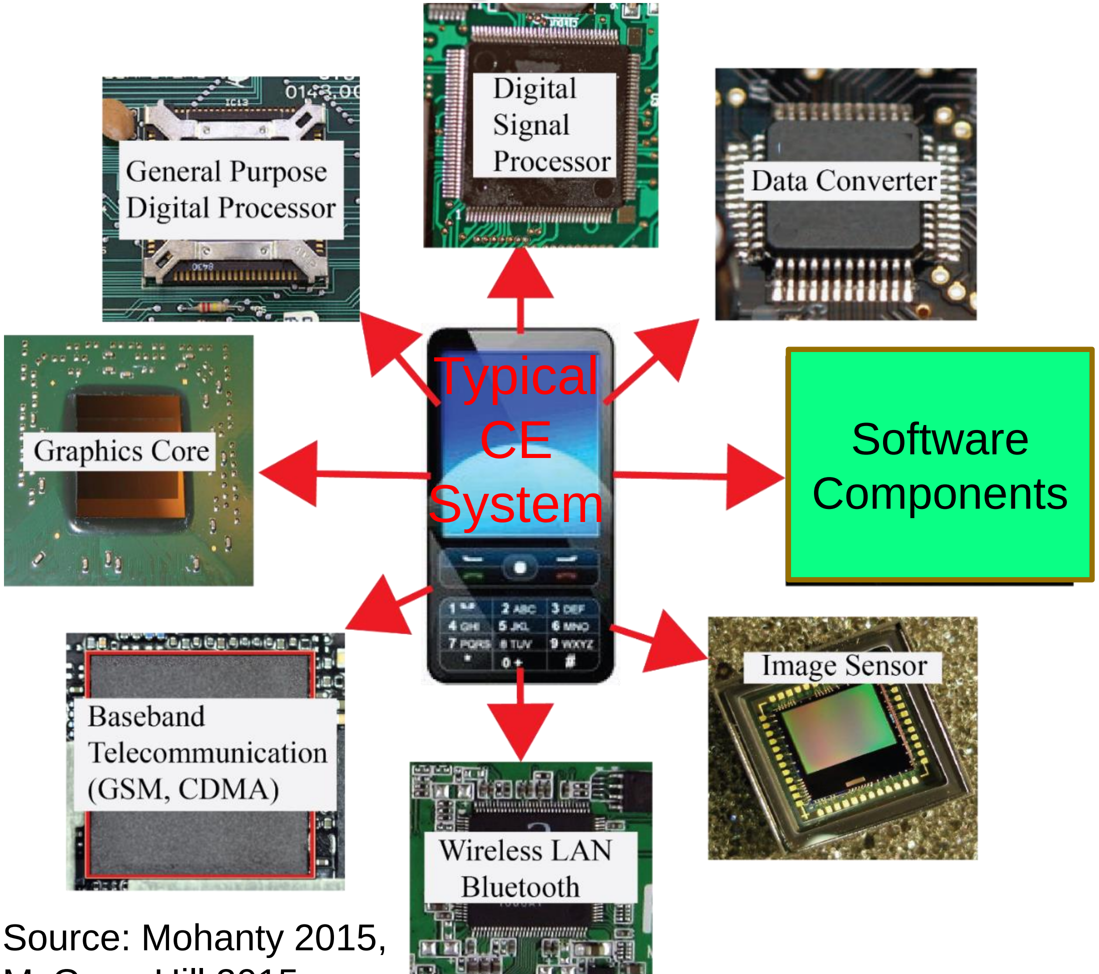
Energy from Supply - Energy consumed in Server, Storage, Software, Communications



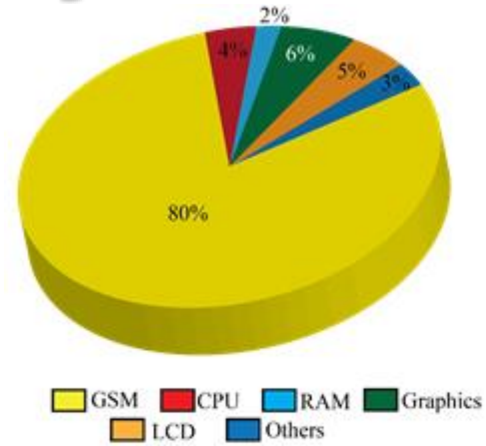
Four Main Components of IoT.

Source: Mohanty 2016, EuroSimE 2016 Keynote Presentation

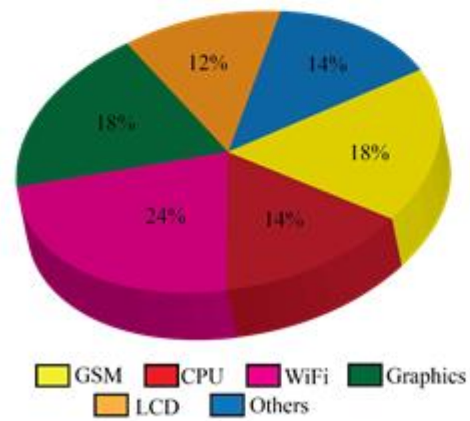
Energy Consumption of Sensors, Components, and Systems



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.

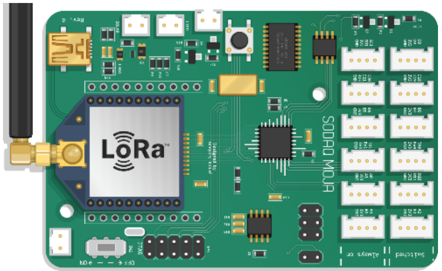
Source: https://www.linkedin.com/pulse/key-technologies-connected-world-cloud-computing-ioe-balakrishnan

Communications – Energy and Data, Range Tradeoffs

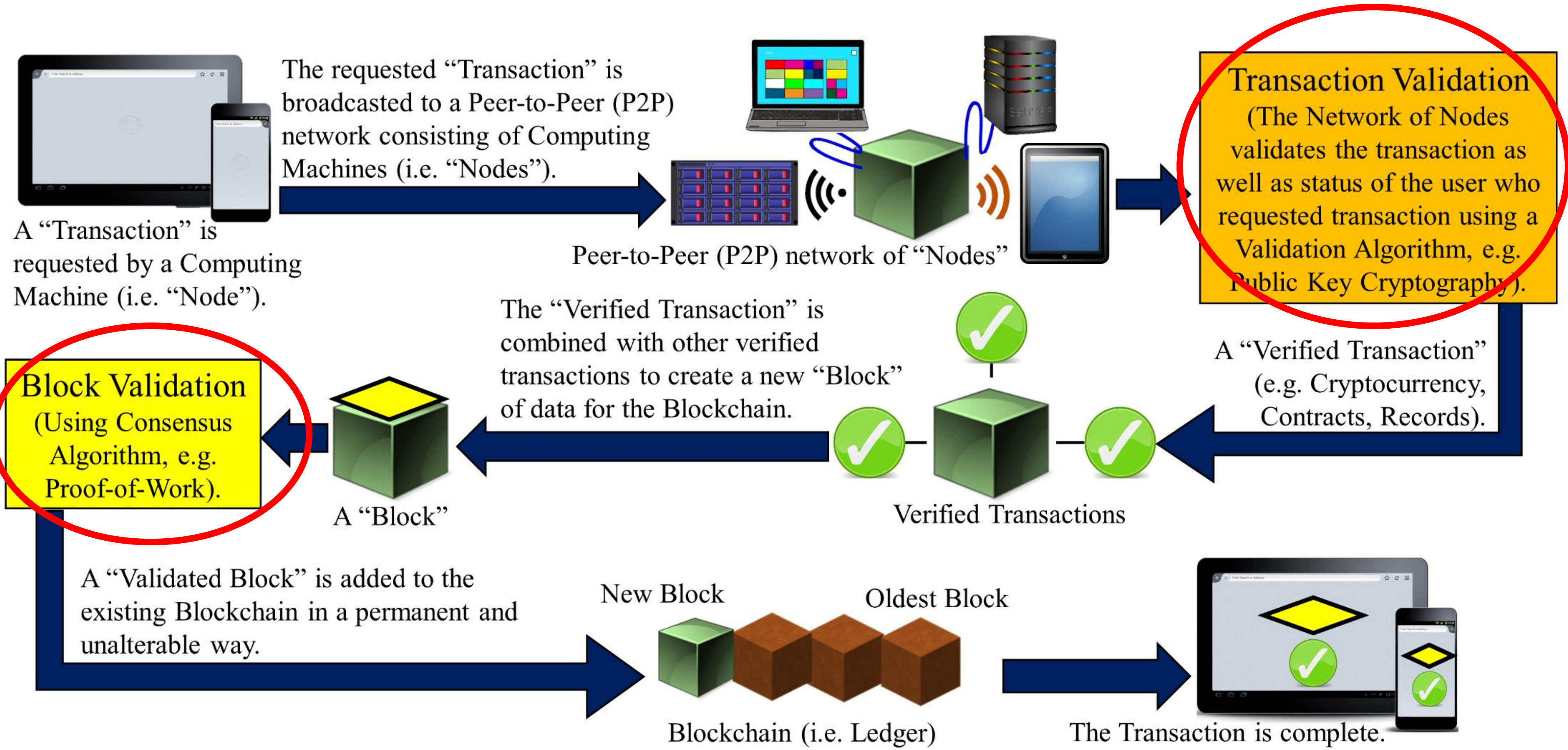
- LoRa: Long Range, low-powered, low-bandwidth, IoT communications as compared to 5G or Bluetooth.
- SigFox: SigFox utilizes an ultra-narrowband wide-reaching signal that can pass through solid objects.

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

sigfox

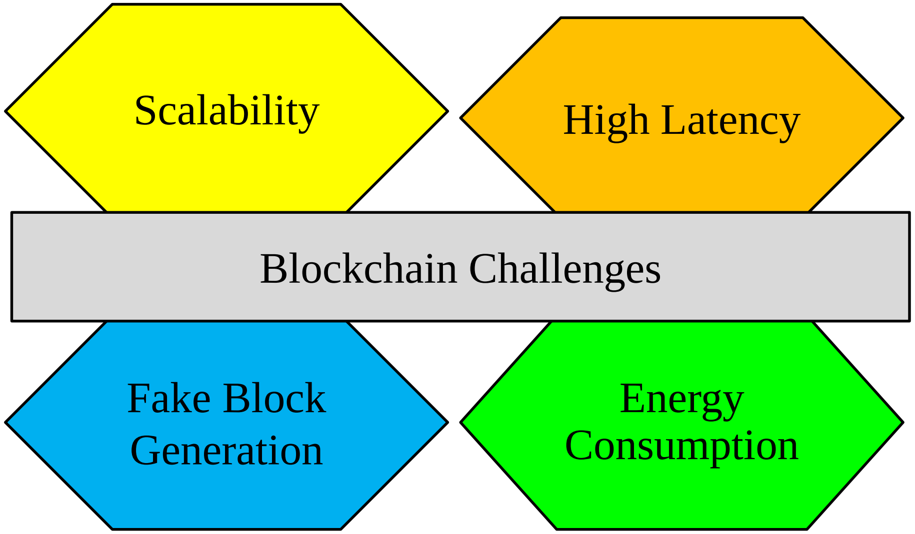


Blockchain Technology



Source: Mohanty 2018, CE Magazine July 2018

Blockchain – Energy Issue

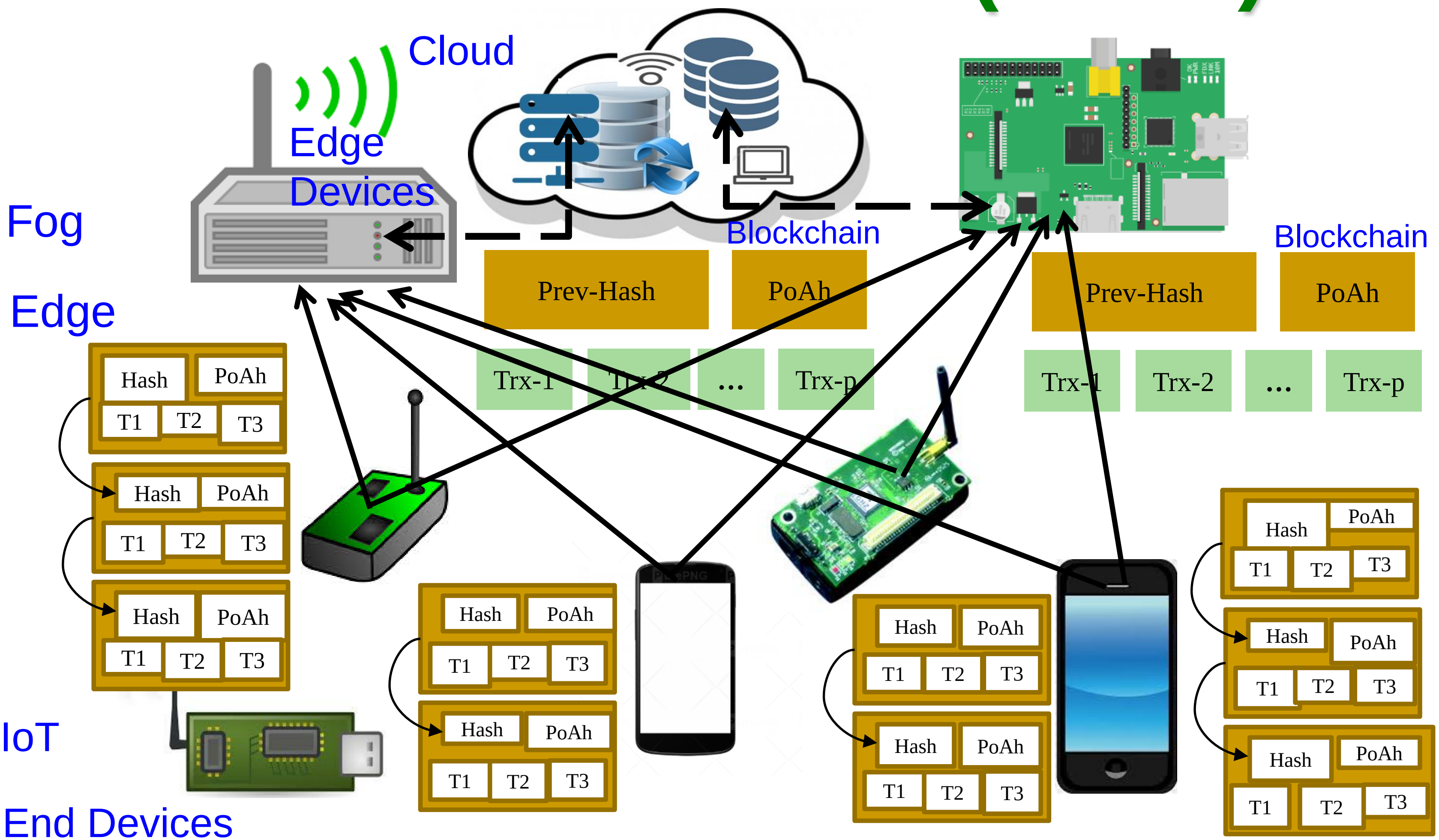


Source: Mohanty 2018, CE Magazine July 2018

- 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.

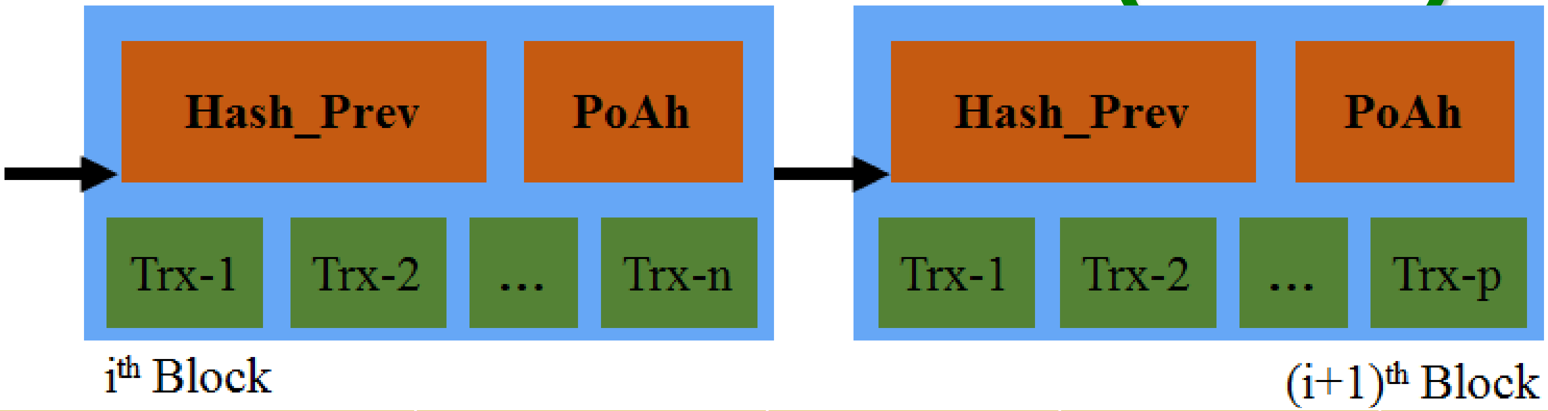
Source: N. Popper, "There is Nothing Virtual About Bitcoin's Energy Appetite", The New York Times, 21st Jan 2018, https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

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)

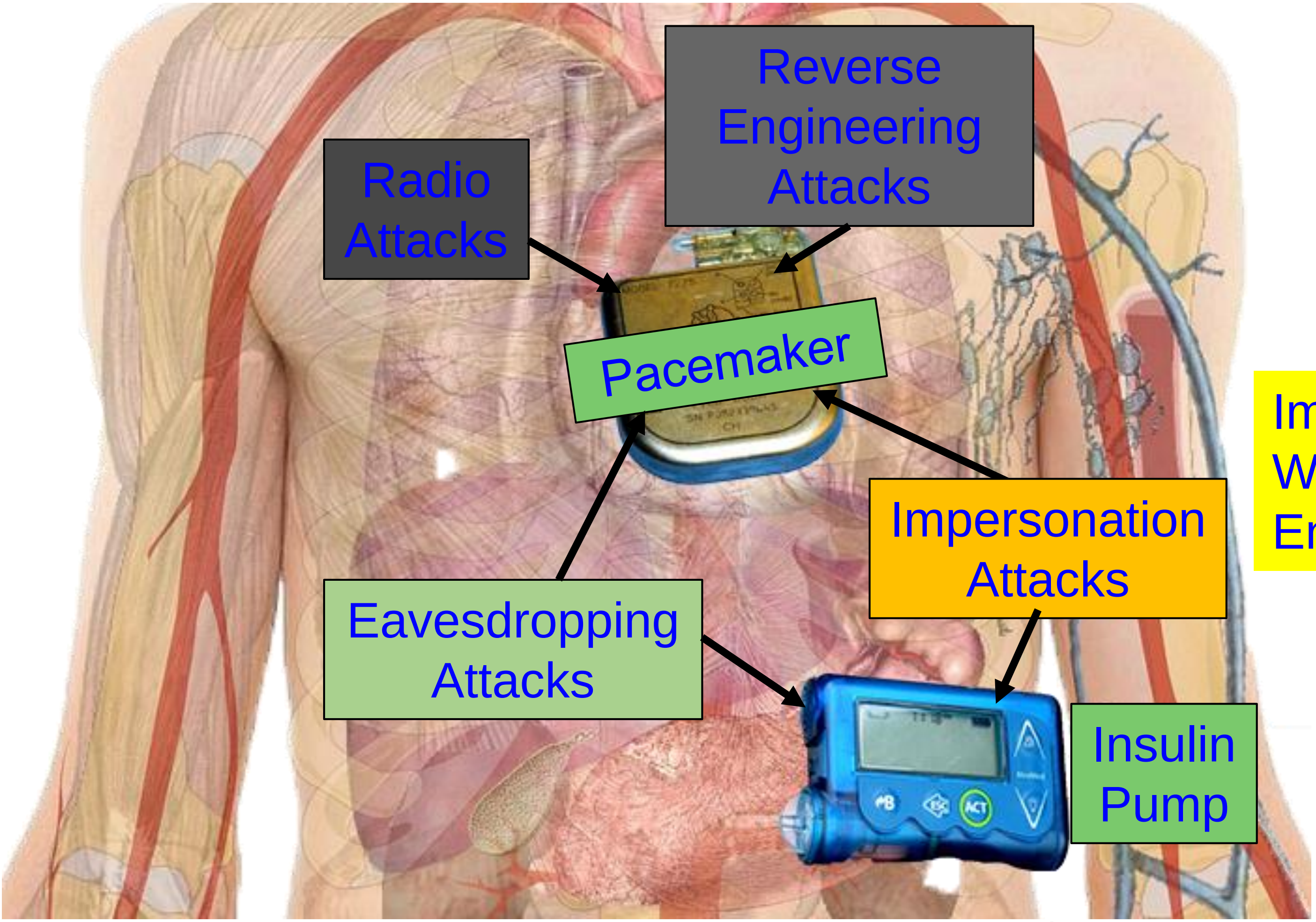


	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Activity (PoA)	Proof-of-Authentication (PoAh)
Energy consumption	High	High	High	Low
Computation requirements	High	High	High	Low
Latency	High	High	High	Low
Search space	High	Low	NA	NA

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

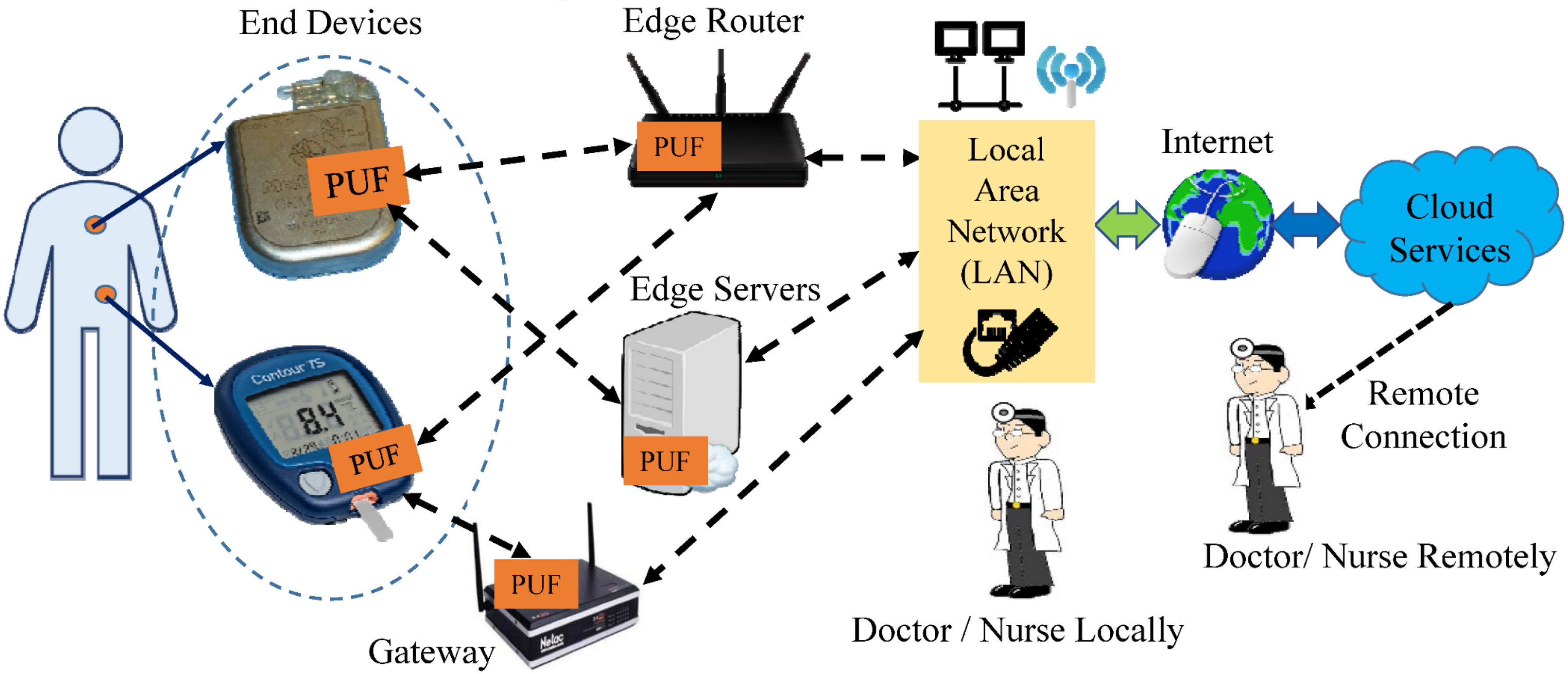
Security Measures in Smart Devices – Smart Healthcare



Implantable / Wearable Security – Energy Constraints

Source: Mohanty 2019, IEEE TCE Under Preparation

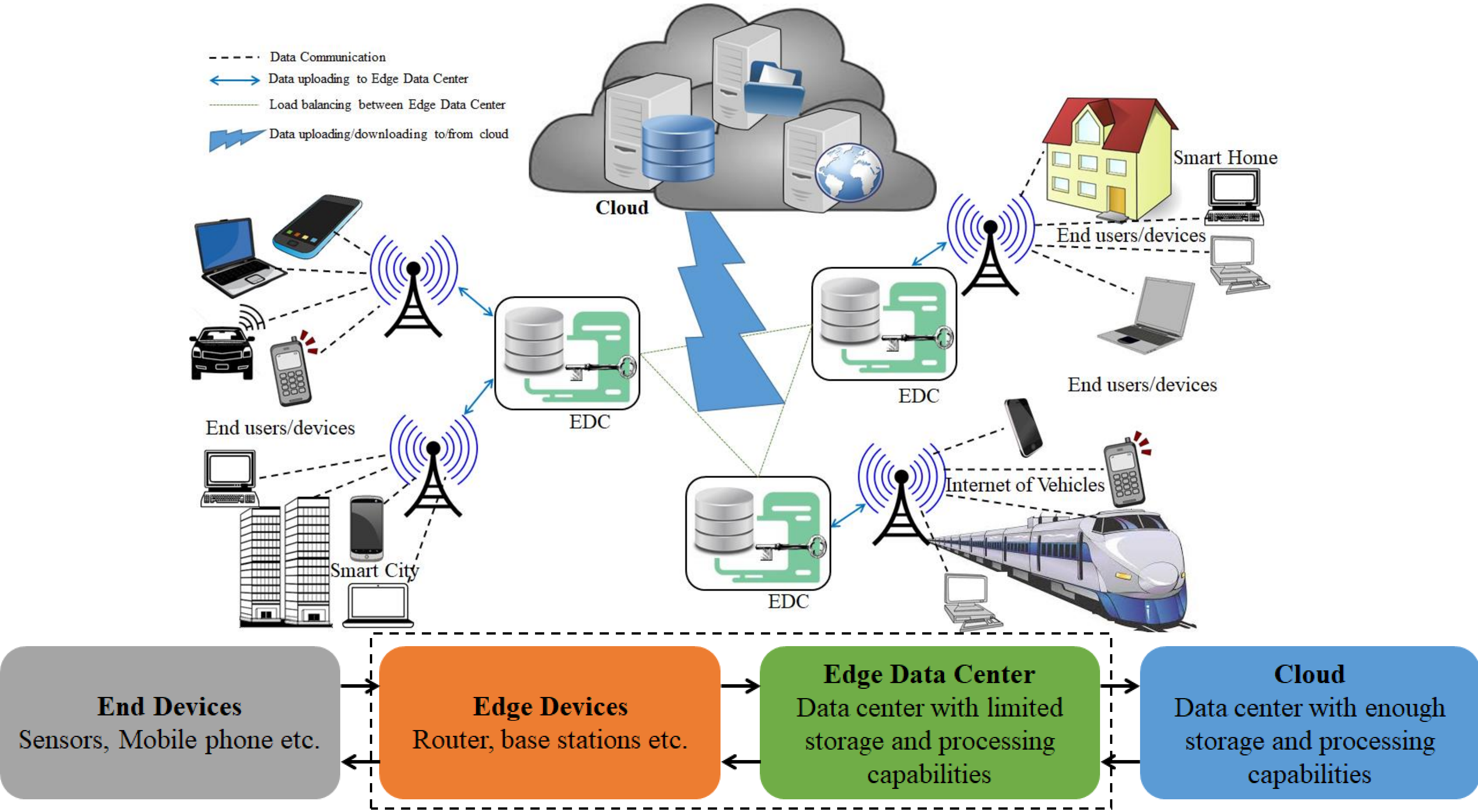
IoMT Security – A PUF a Device Authentication



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

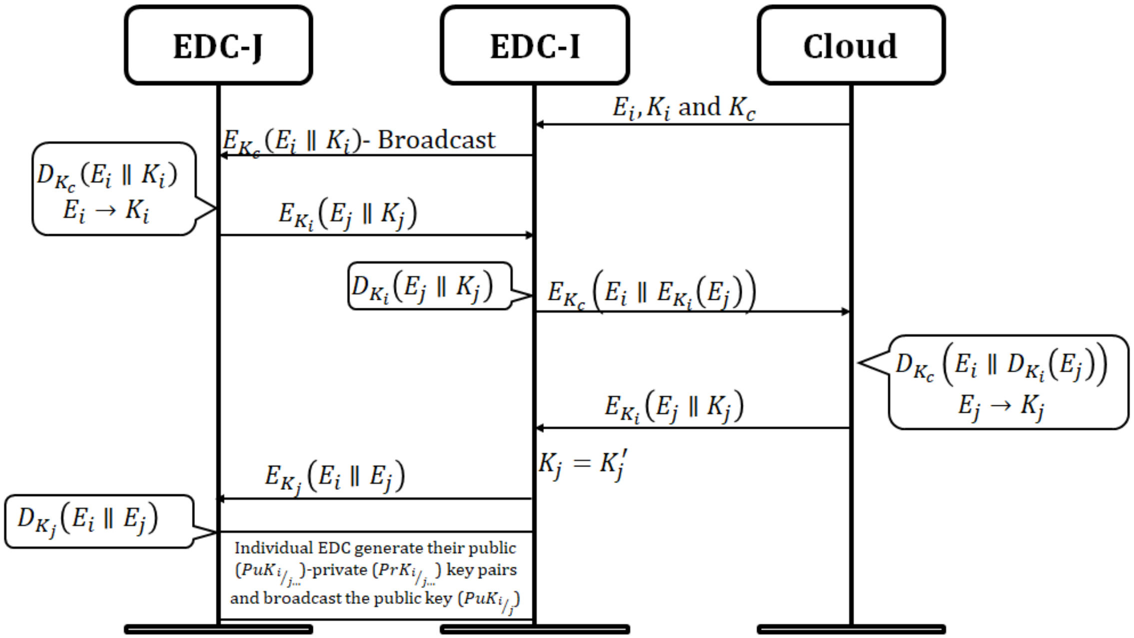
Source: Mohanty 2019, IEEE TCE Under Preparation

Secure Edge Datacenter



Source: Puthal, Mohanty 2018, IEEE Comm. Magazine May 2018

Secure Edge Datacenter



Algorithm 1. Load Balancing Technique

1. If (EDC-I is overloaded)
2. EDC-I broadcast (E_i, L_i)
3. EDC-J (neighbor EDC) verifies:
4. If (E_i is in database) & ($p \leq 0.6$ & $L_i << (n-m)$)
5. Response $E_{Kpu_i}(E_j || K_j || p)$
6. EDC-I perform $D_{Kpr_i}(E_j || K_j || p)$
7. $k_j' \leftarrow E_j$
8. If ($k_j' = k_j$)
9. EDC-I select EDC-J for load balancing.

Secure edge datacenter –

- Balances load among the EDCs
- Authenticates EDCs

Response time of the destination EDC has reduced by 20-30 % using the proposed allocation approach.

Source: Puthal, Mohanty 2018, IEEE Comm. Magazine May 2018

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

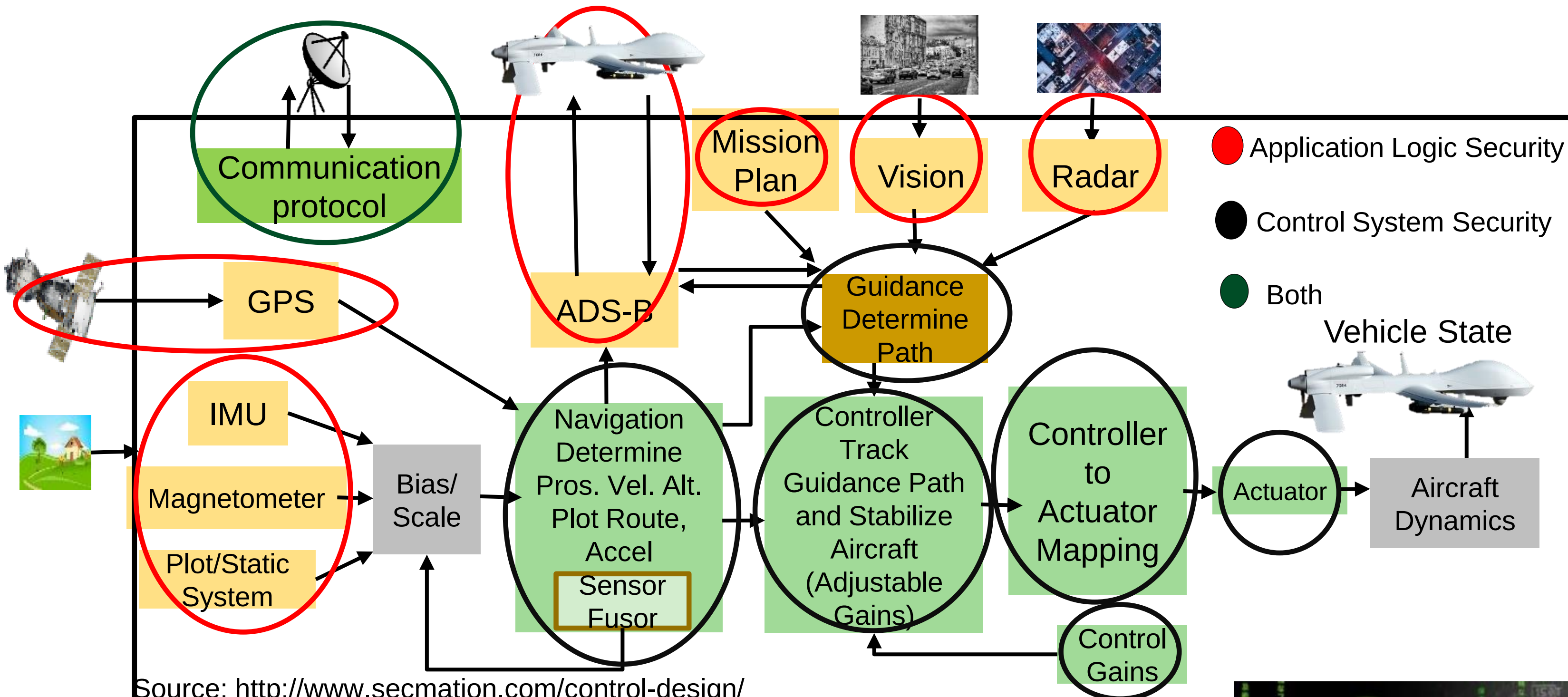
Autonomous Vehicle – Computing Need

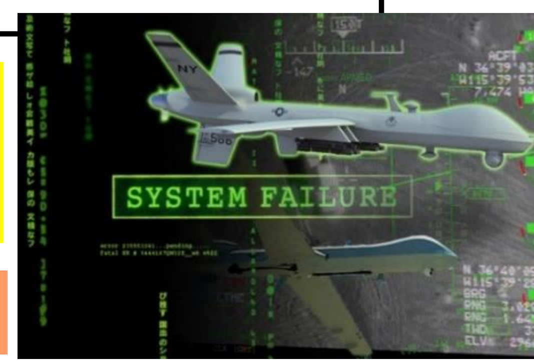
Source: https://www.engadget.com/2017/10/10/nvidia-introduces-a-computer-for-level-5-autonomous-cars/

Computing need in small server room stored in the trunk:

- ❖ AI and data-crunching
- ❖ Huge amounts of data coming from dozens of cameras, LiDAR sensors, short and long-range radar

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/

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

- 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.

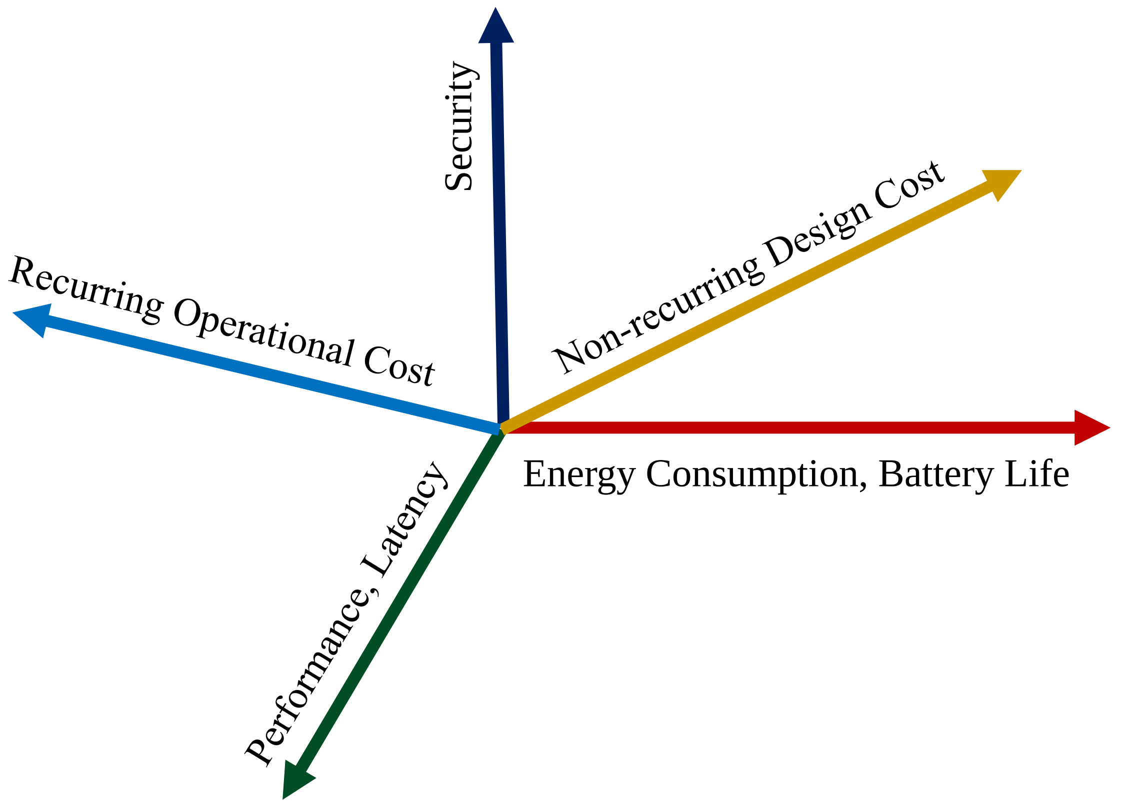
Source: Sengupta and Mohanty IET 2018

RF Hardware Security | Digital Hardware Security – Side Channel

Hardware Trojan Protection | Information Security, Privacy, Protection

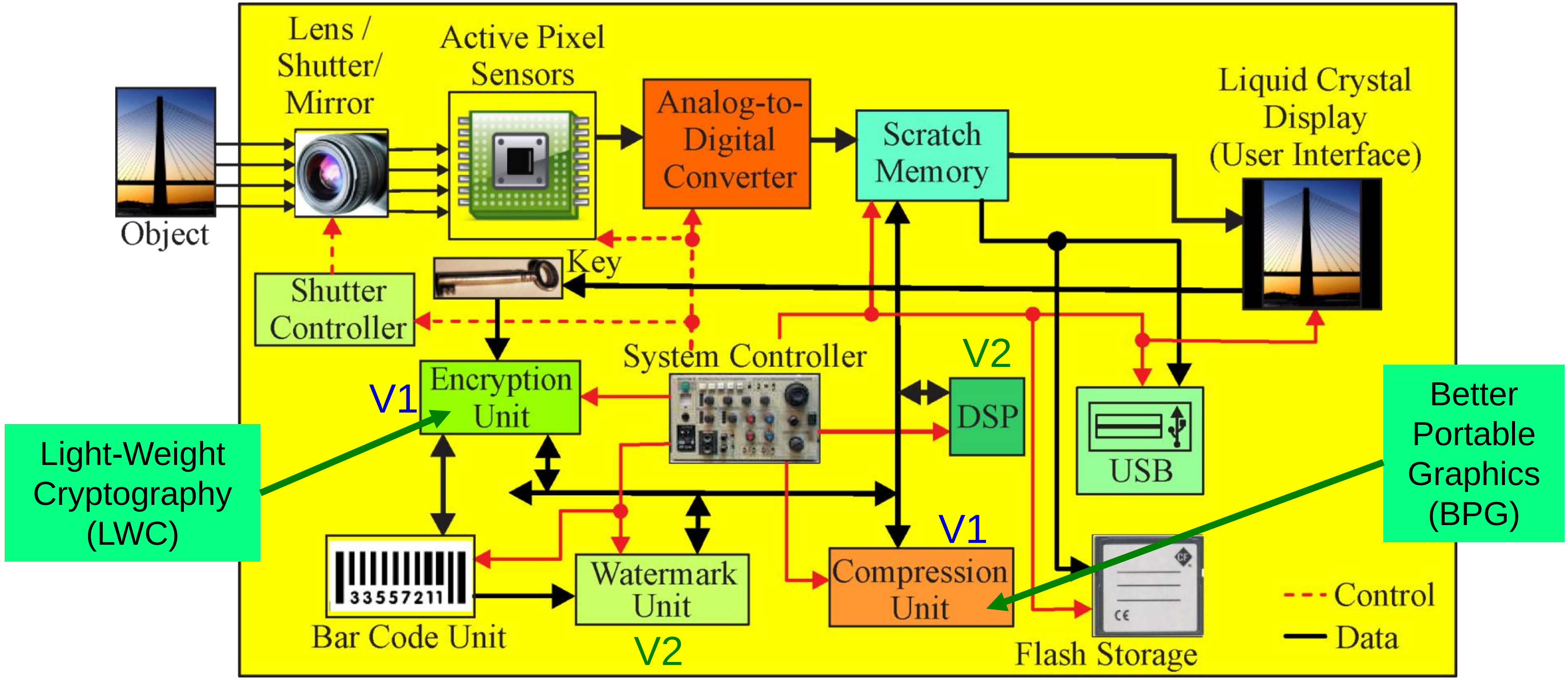
IR Hardware Security | Memory Protection | Digital Core IP Protection

CE System Design and Operation Tradeoffs



Source: Mohanty ICCE Panel 2018

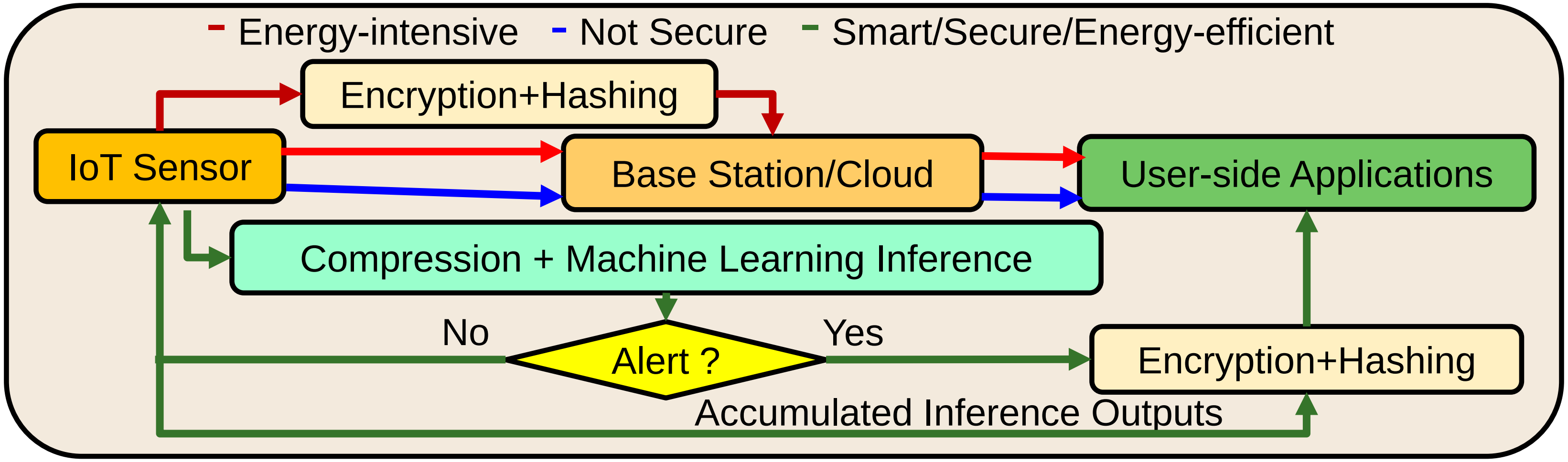
ESR-Smart – System Level



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

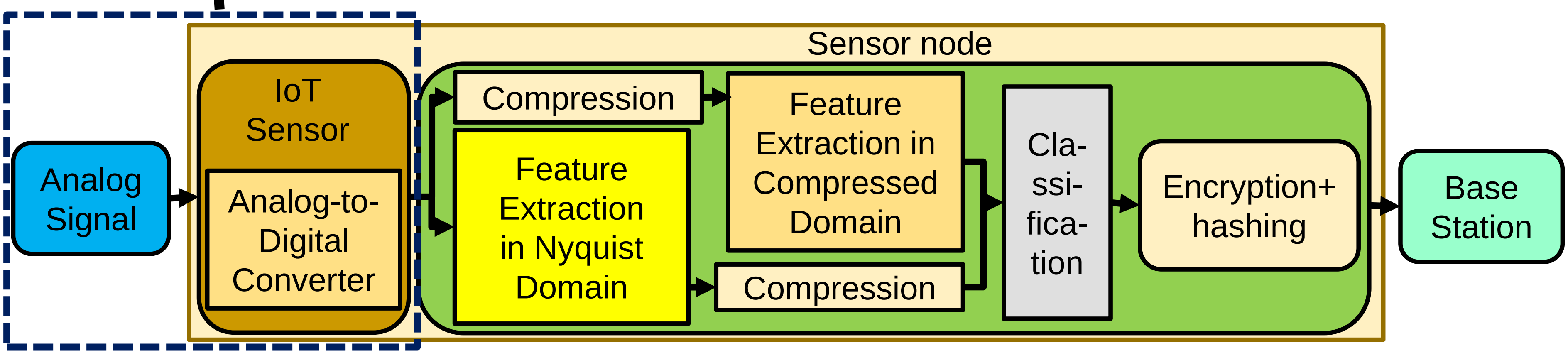
Source: Mohanty 2006, TCAS-II May 2006; Mohanty 2009, JSA Oct 2009; Mohanty 2016, Access 2016

ESR-Smart – Sensor Level



Scenarios in IoT sensor data processing

Traditional IoT sensor

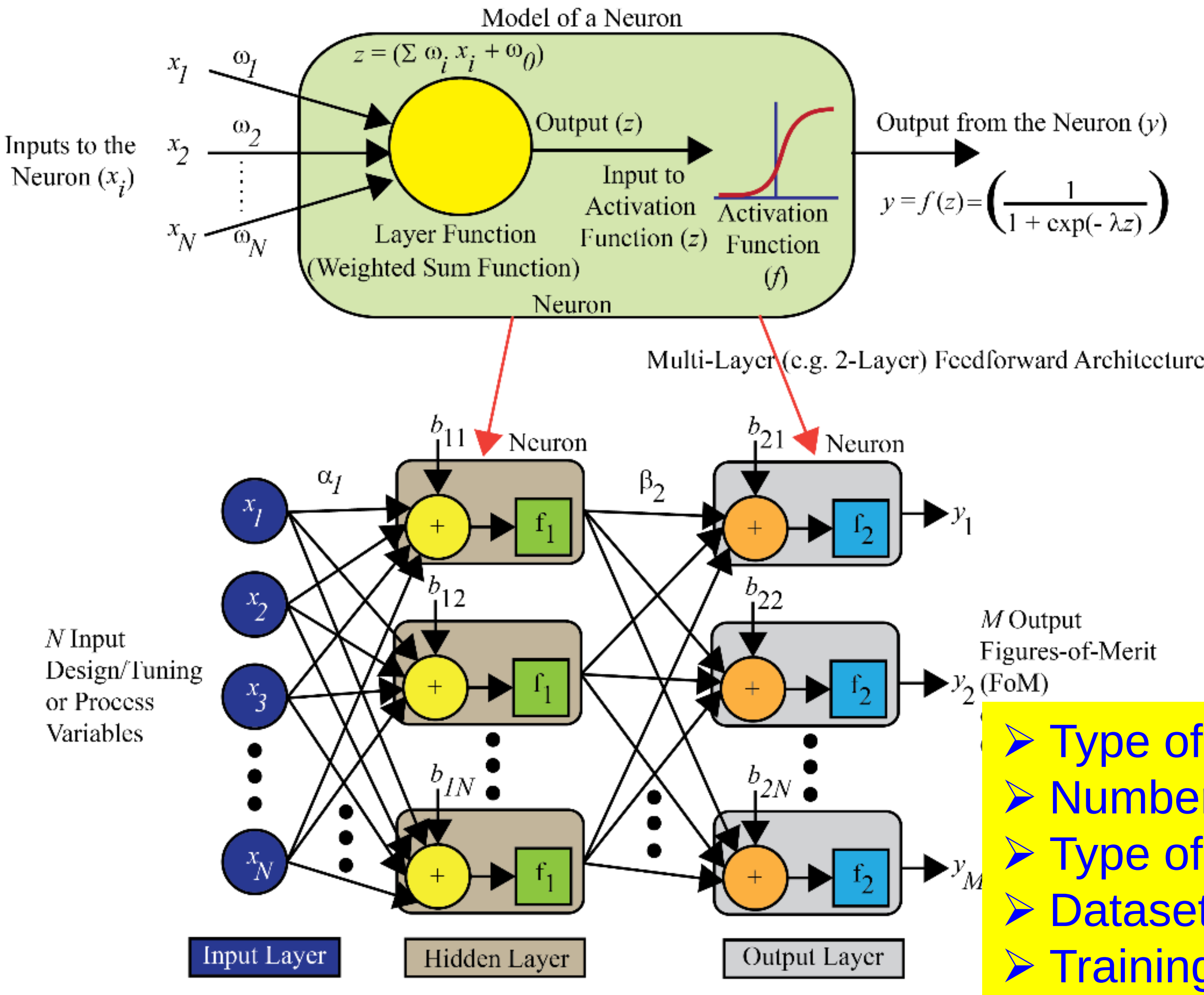


Smart, secure, and energy-efficient IoT sensor architecture

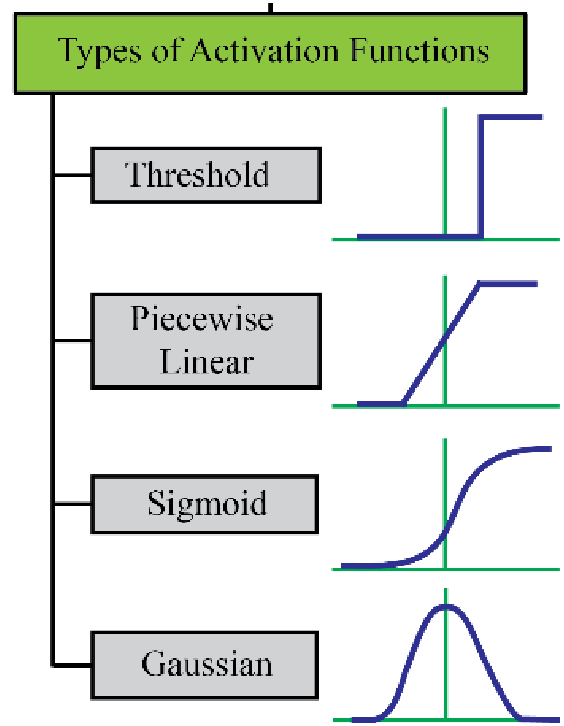
Source: Akmandor and Jha 2018: CICC 2018

Challenges in Making Smart

Artificial Neural Networks



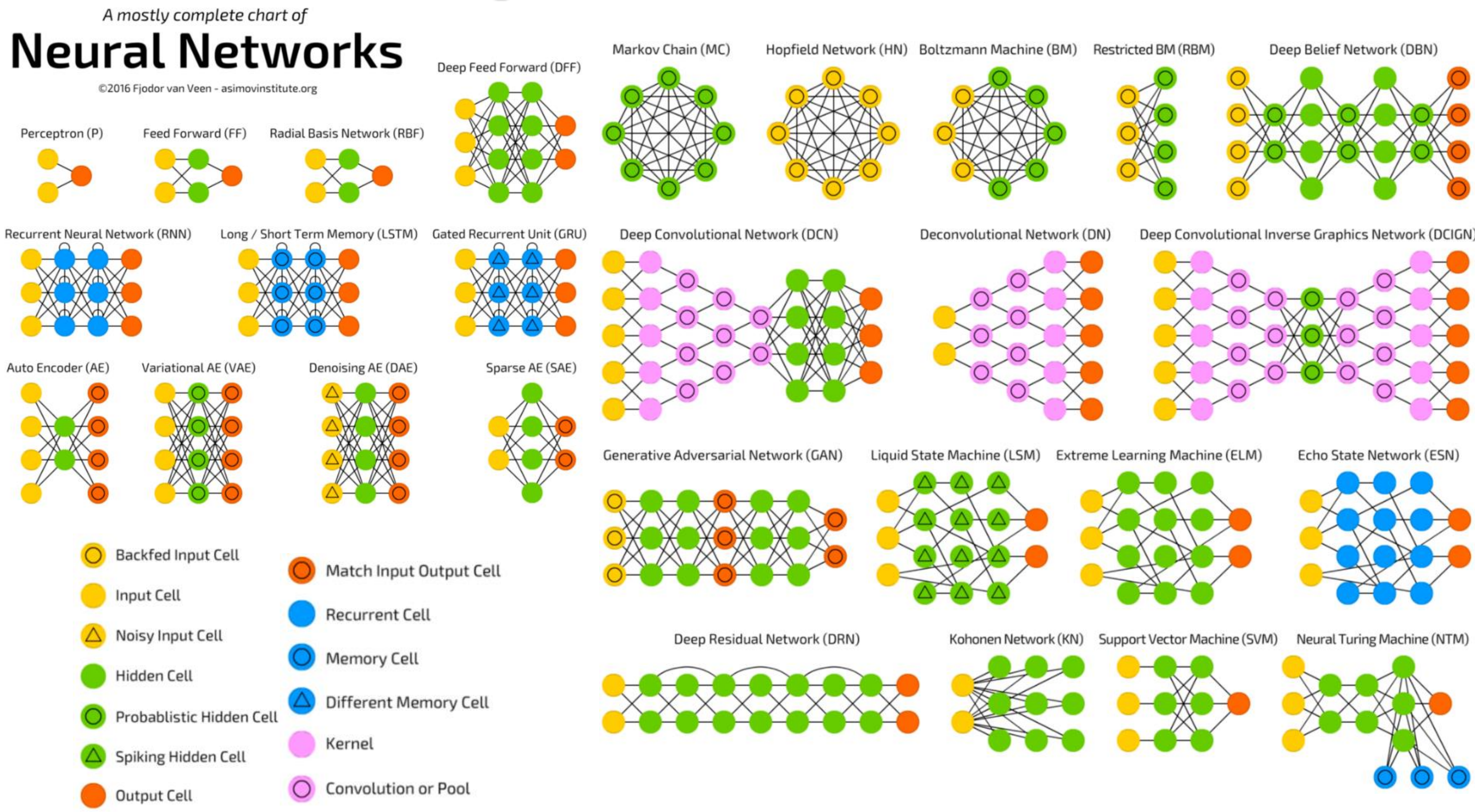
(a) Architecture of Neural Network (NN)



- Type of architecture?
- Number of layers?
- Type of activation function?
- Datasets: training and verification?
- Training algorithm?
- Accuracy metric?

Source: Mohanty McGraw-Hill 2015

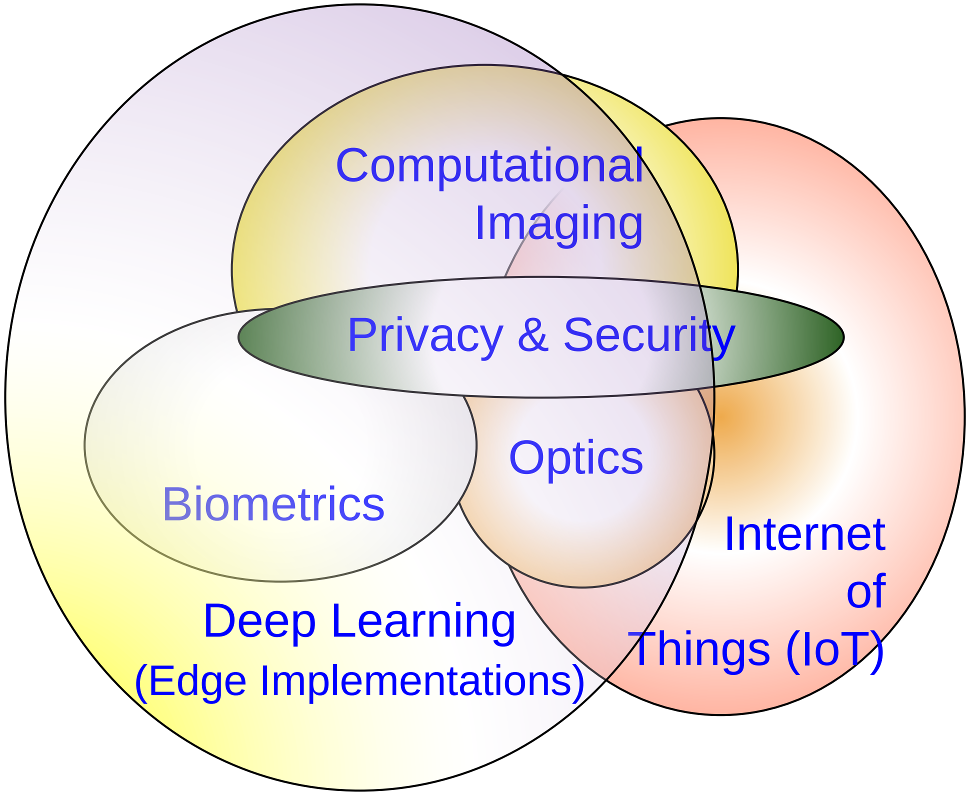
Various Options for ANN Models



Source: https://towardsdatascience.com/the-mostly-complete-chart-of-neural-networks-explained-3fb6f2367464

Deep Learning is the Key

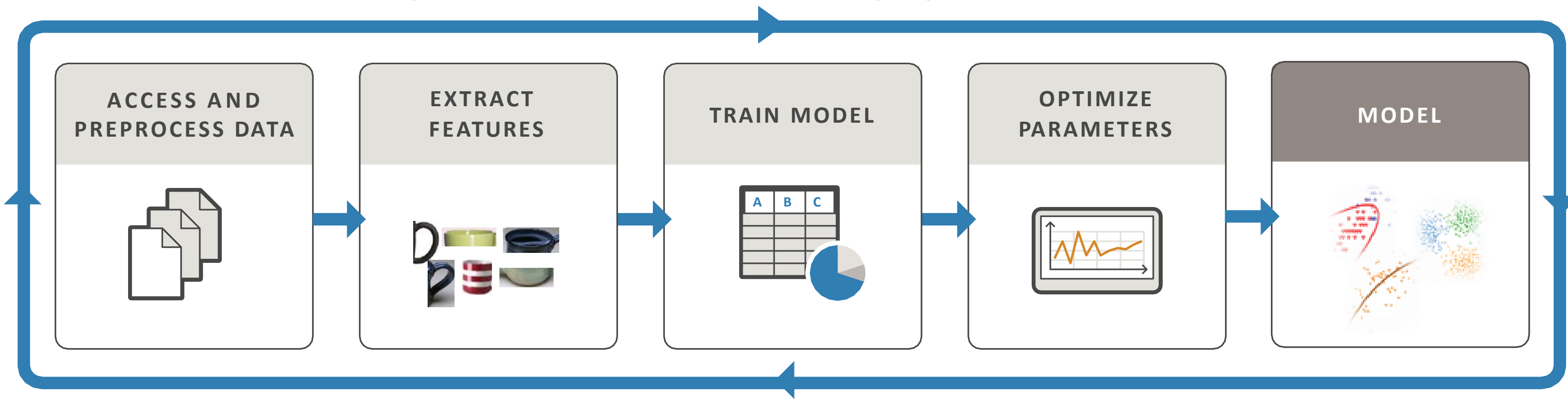
- "DL at the Edge" overlaps all of these research areas.
- New Foundation Technologies, enhance data curation, improved AI, and Networks accuracy.



Source: Corcoran Keynote 2018

Deep Neural Network (DNN) - Resource and Energy Costs

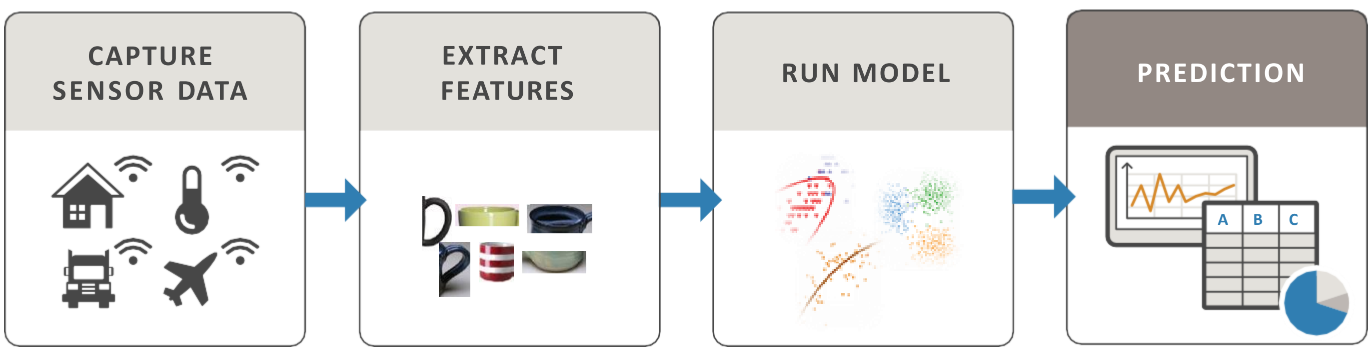
TRAIN: Iterate until you achieve satisfactory performance.



Needs Significant:

- ➢ Resource
- ➢ Energy

PREDICT: Integrate trained models into applications.

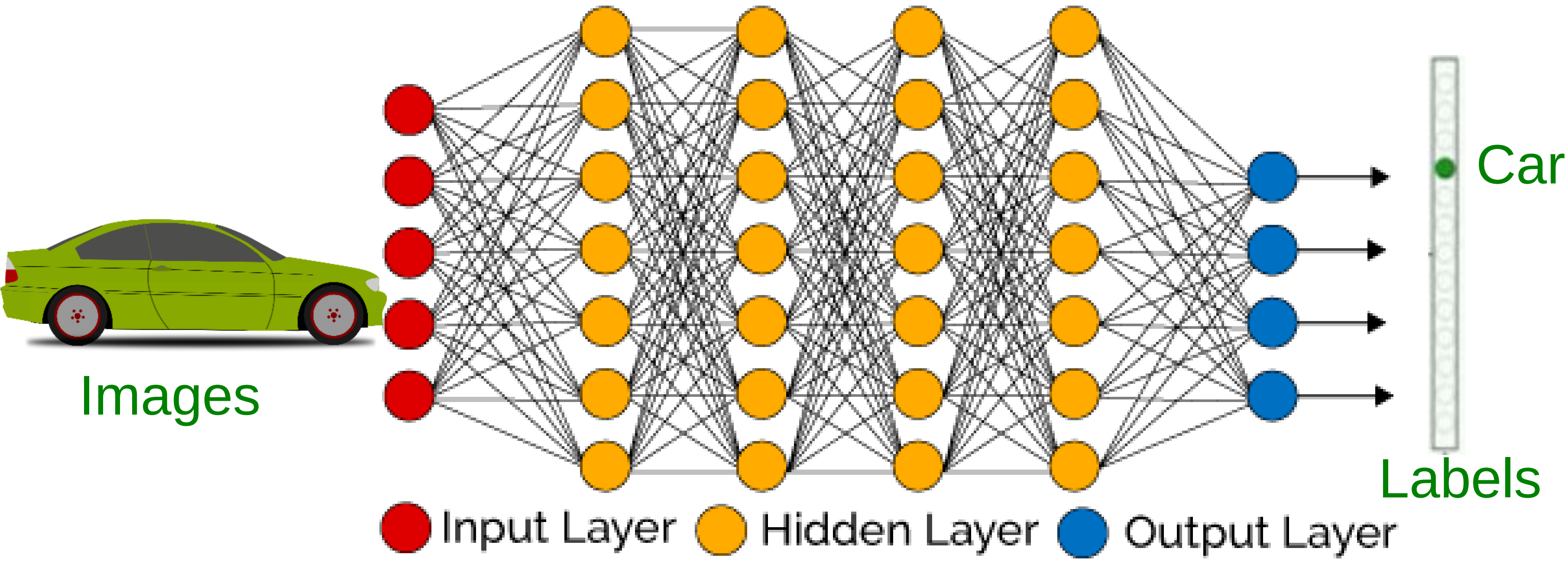


Needs:

- ➢ Resource
- ➢ Energy

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

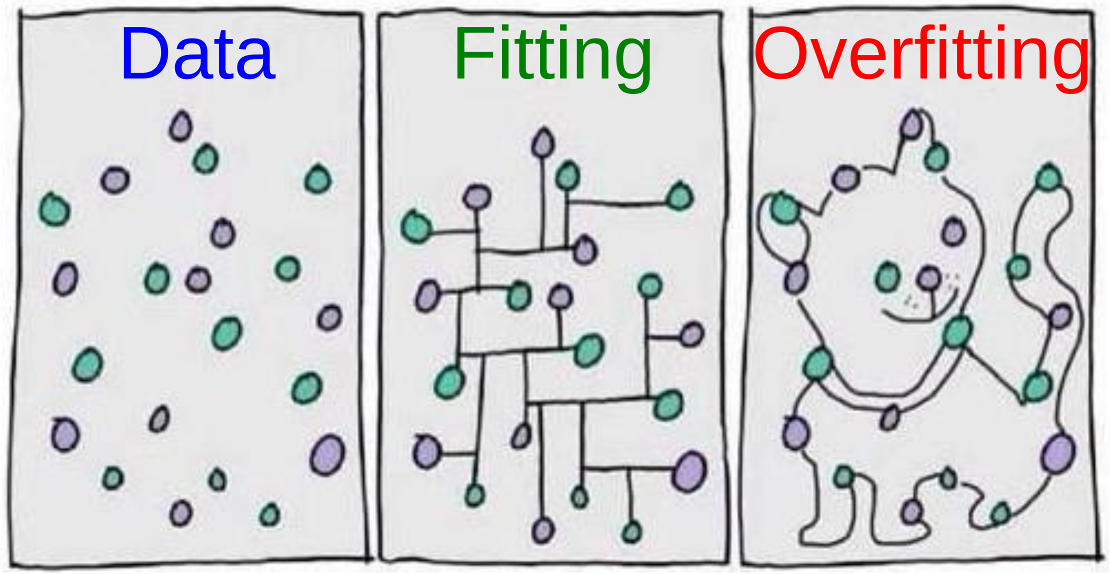
DNN Training - Energy Issue



- 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.

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

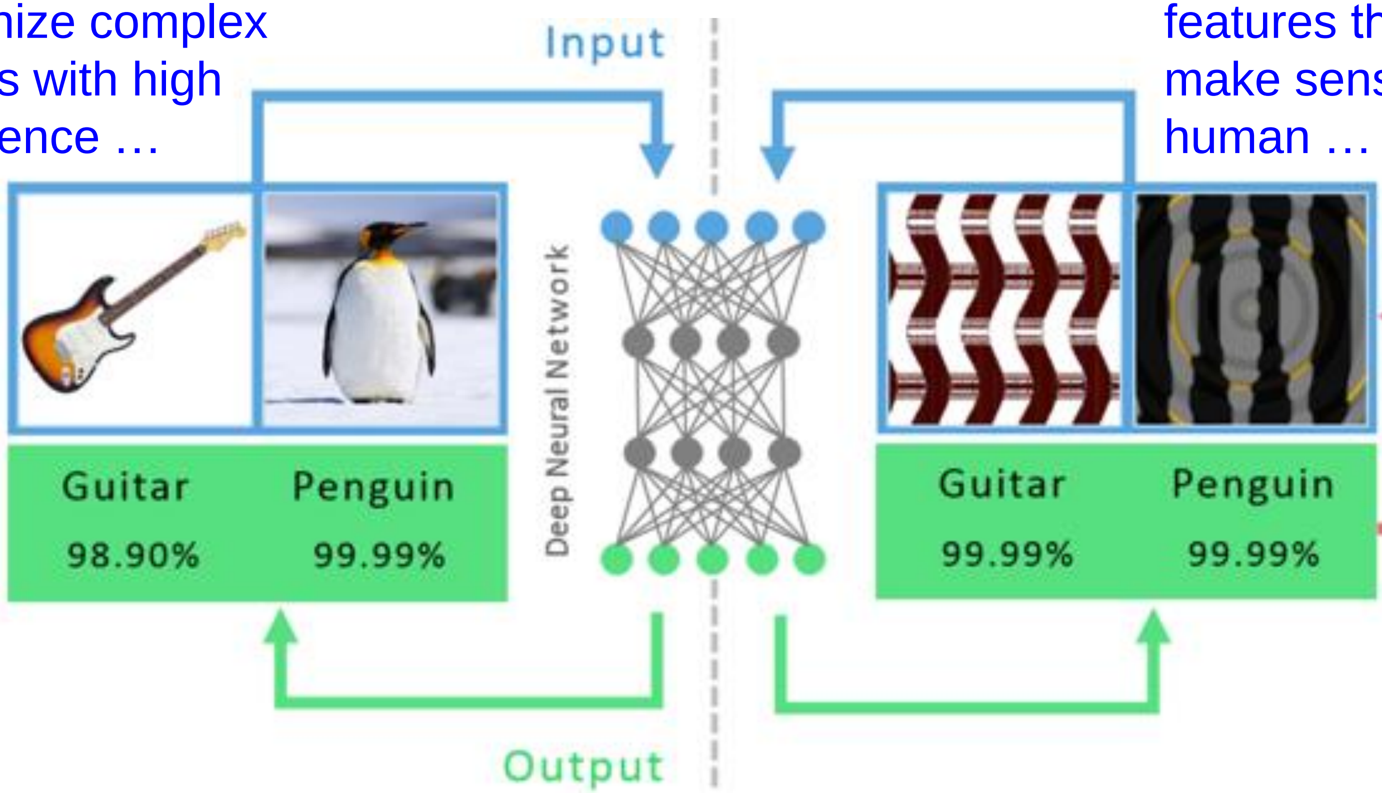
- Class imbalance is a classification problems where the classes are not represented equally.
- Solutions: Use Precision, Recall, F-measure metrics

  Not only RMSE like accuracy metrics

DNNs are not Always Smart

DNNs can learn to recognize complex objects with high confidence …

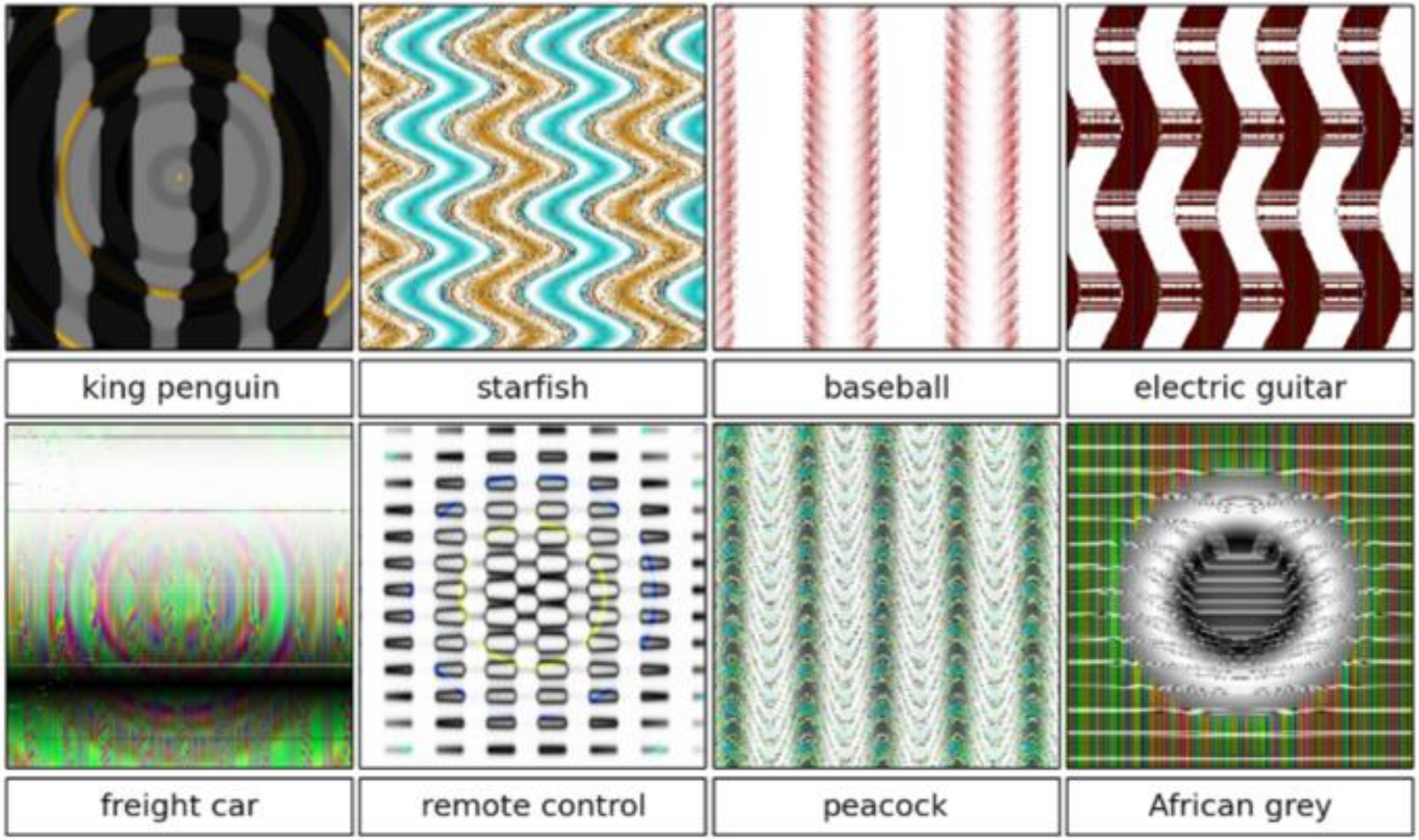
But often they learn features that don't make sense to a human …



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

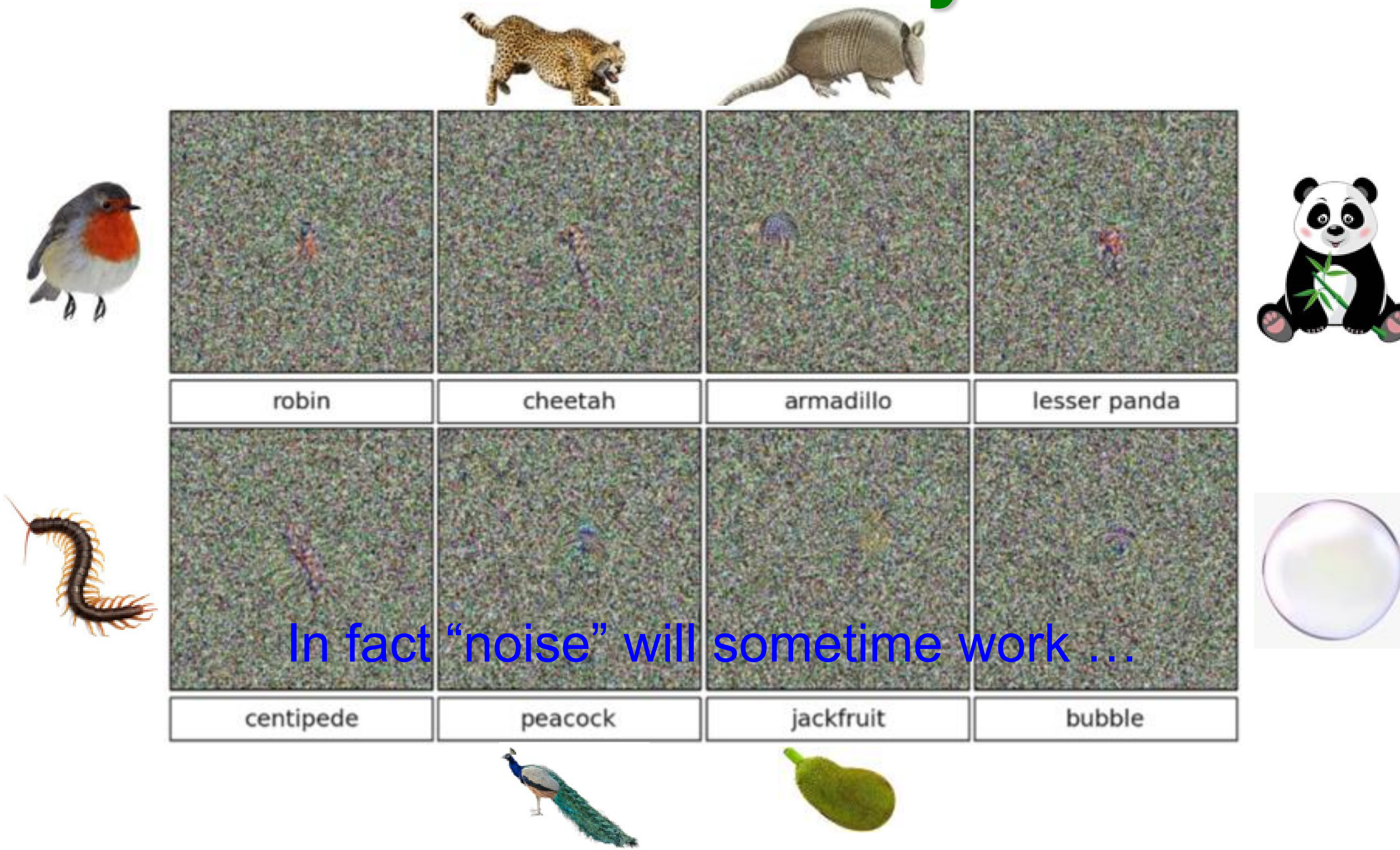


DNNs can be fooled by certain "learned" (Adversarial) patterns …

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



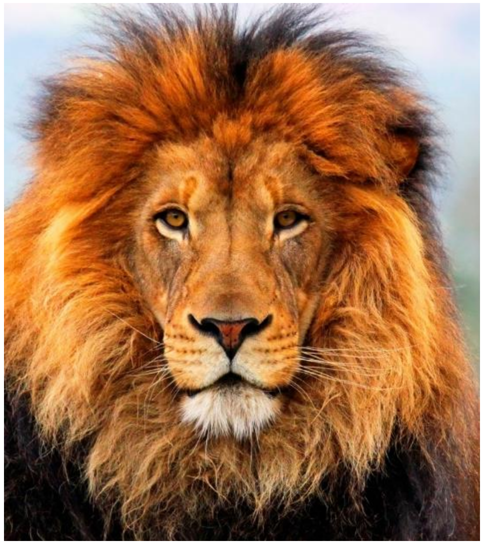
In fact “noise” will sometime work …

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



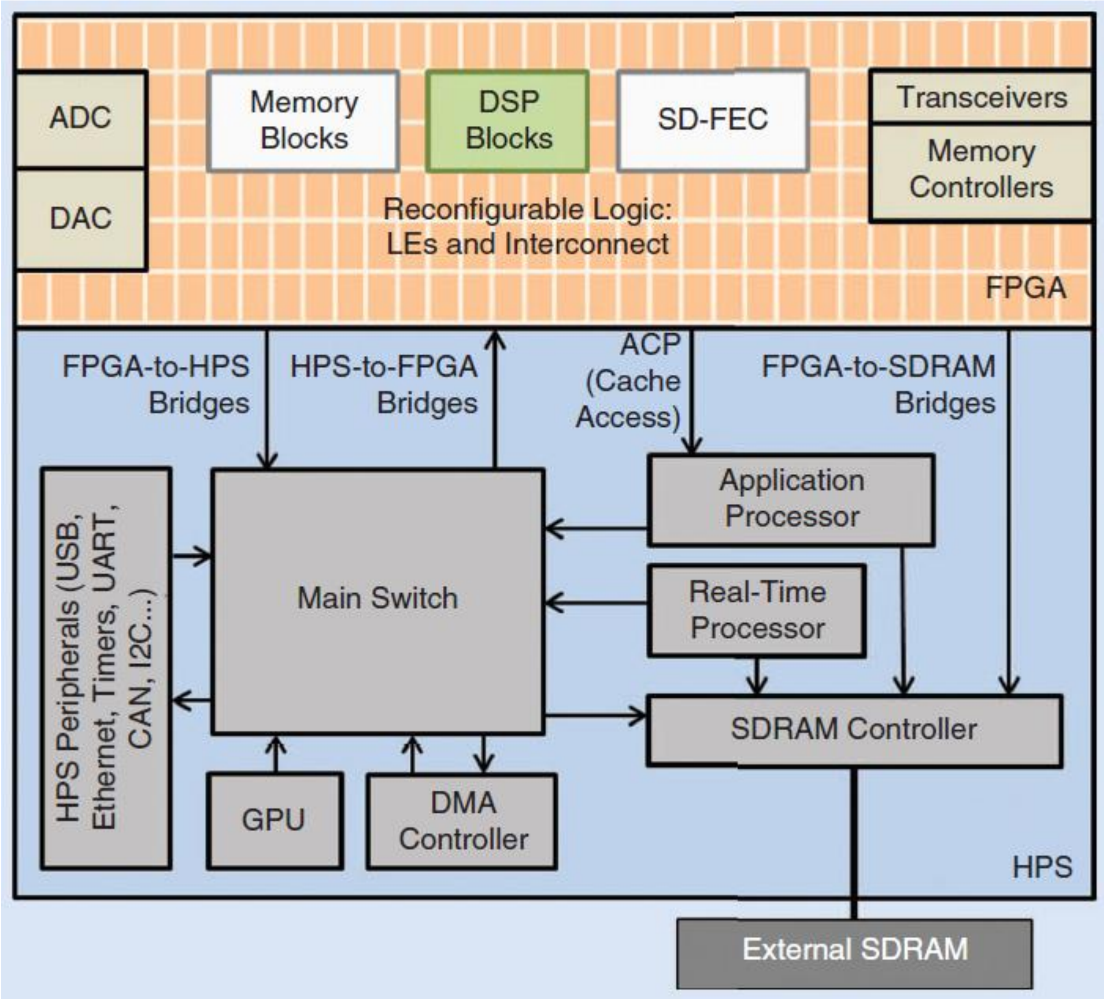
Source: Corcoran Keynote 2018

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_

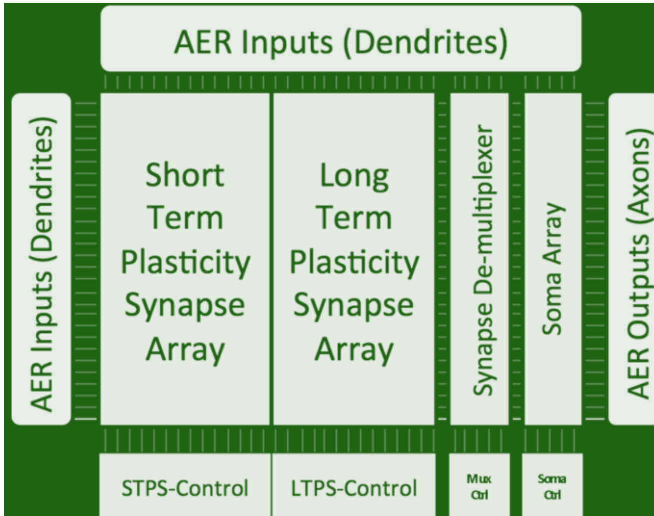
ML Hardware Accelerators – Field-Programmable System-On-Chip (FPSoC)



FPSoCs feature a hard processing system (HPS) and FPGA fabric on the same chip.

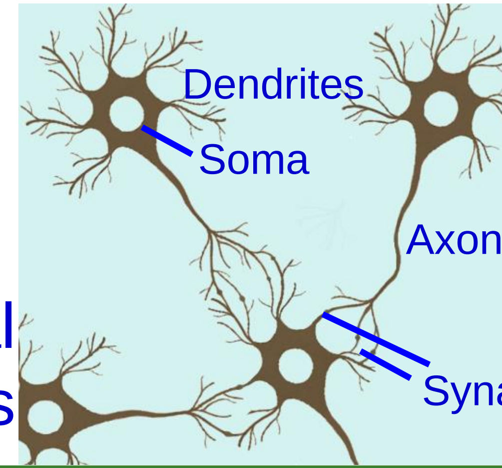
Source: Molanes 2018: IEEE IEM Jun 2018

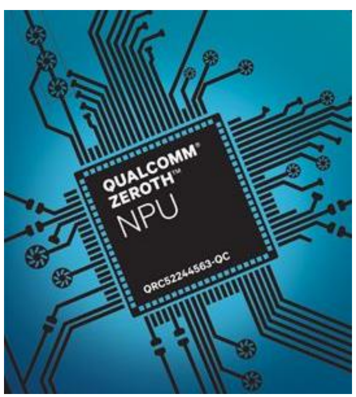
Neuromorphic Computing or Brain-Inspired Computing



Neuromorphic Architecture

Neuronal Circuits





Processing Powers MIT Technical Review

Types of Chips	Functions	Applications
Traditional Chips (von Neumann Architecture)	Reliably make precision calculations	Any numerical problem, Complex problems require more amount of energy
Neuromorphic Chips	Detect and Predict Patterns in complex data using minimal energy	Applications with significant visual/ auditory data requiring a system to adjust its behavior as it interacts with the world

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

Neuromorphic Computing or Brain-Inspired Computing

Application 1: Integrate into assistive glasses for visually impaired people for navigating through complex environments, even without the need for a WiFi connection.

Application 2: Neuromorphic-based, solar-powered "sensor leaves" equipped with sensors for sight, smell or sound can help to monitor natural disasters.

Source: https://blogs.scientificamerican.com/observations/brain-inspired-computing-reaches-a-new-milestone/

Smart Electronics - Applications

The Problem - The Big Picture

- Uncontrolled growth of urban population
- Limited natural and man-made resources
- Rapid urbanization
- Demand for better quality of life

Source: https://humanitycollege.org

Air Pollution Management

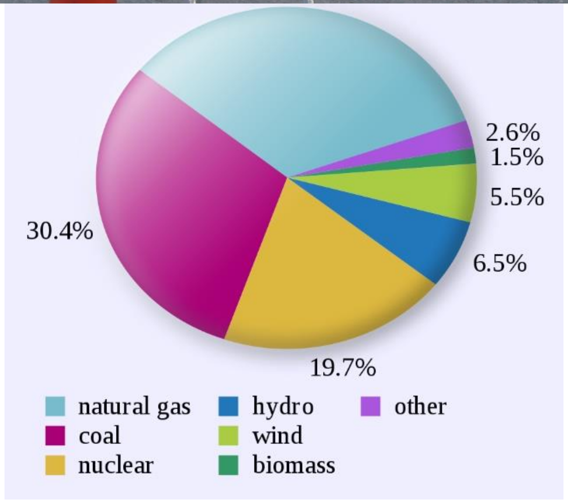
- Pollutions

Water Pollution Management

- Water crisis

Energy Management

- ➢ Energy crisis



Traffic and Transportation Management

- Traffic

Population Trend Management

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

"Cities around the world could spend as much as $41 trillion on smart tech over the next 20 years."

Source: http://www.cnbc.com/2016/10/25/spending-on-smart-cities-around-the-world-could-reach-41-trillion.html

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

Conclusions

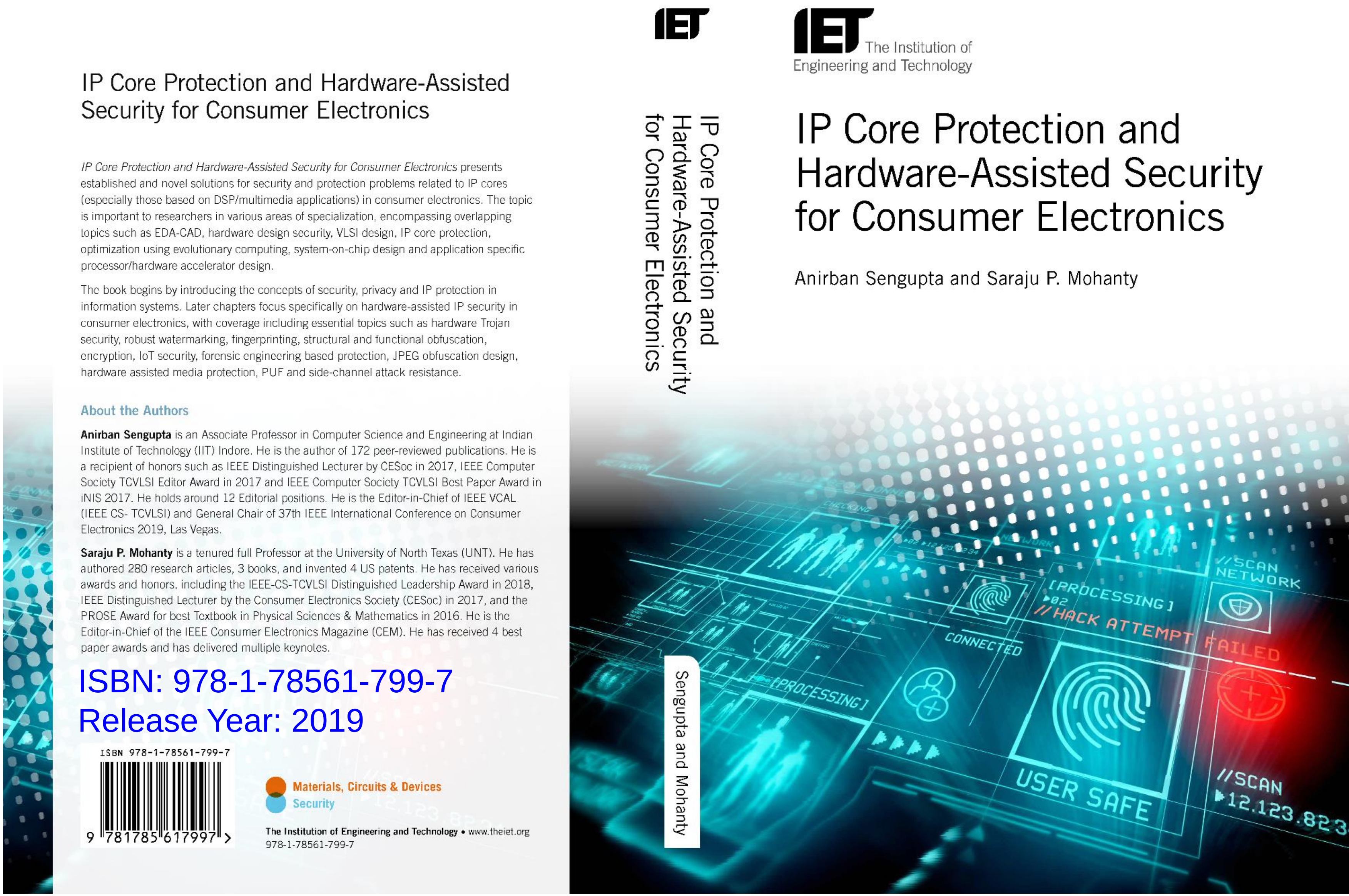
- "Smart" terms is used to present a variety of characteristics of CE.
- Energy smart is important for battery and energy costs point of view.
- Security smart is important for connected CE.
- Response smart is making decisions based on ML data analytics.
- ML has its own cost in terms of training and 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.

Can Any Smartness/Intelligence Solve?

Source: https://www.wilsoncenter.org/article/building-slum-free-mumbai



IET

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

IP Core Protection and Hardware-Assisted Security for Consumer Electronics presents established and novel solutions for security and protection problems related to IP cores (especially those based on DSP/multimedia applications) in consumer electronics. The topic is important to researchers in various areas of specialization, encompassing overlapping topics such as EDA-CAD, hardware design security, VLSI design, IP core protection, optimization using evolutionary computing, system-on-chip design and application specific processor/hardware accelerator design.

The book begins by introducing the concepts of security, privacy and IP protection in information systems. Later chapters focus specifically on hardware-assisted IP security in consumer electronics, with coverage including essential topics such as hardware Trojan security, robust watermarking, fingerprinting, structural and functional obfuscation, encryption, IoT security, forensic engineering based protection, JPEG obfuscation design, hardware assisted media protection, PUF and side-channel attack resistance.

About the Authors

Anirban Sengupta is an Associate Professor in Computer Science and Engineering at Indian Institute of Technology (IIT) Indore. He is the author of 172 peer-reviewed publications. He is a recipient of honors such as IEEE Distinguished Lecturer by CESoc in 2017, IEEE Computer Society TCVLSI Editor Award in 2017 and IEEE Computer Society TCVLSI Best Paper Award in iNIS 2017. He holds around 12 Editorial positions. He is the Editor-in-Chief of IEEE VCAL (IEEE CS- TCVLSI) and General Chair of 37th IEEE International Conference on Consumer Electronics 2019, Las Vegas.

Saraju P. Mohanty is a tenured full Professor at the University of North Texas (UNT). He has authored 280 research articles, 3 books, and invented 4 US patents. He has received various awards and honors, including the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, IEEE Distinguished Lecturer by the Consumer Electronics Society (CESoc) in 2017, and the PROSE Award for best Textbook in Physical Sciences & Mathematics in 2016. He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine (CEM). He has received 4 best paper awards and has delivered multiple keynotes.

ISBN: 978-1-78561-799-7
Release Year: 2019

ISBN 978-1-78561-799-7

Materials, Circuits & Devices
Security

The Institution of Engineering and Technology • www.theiet.org
978-1-78561-799-7

IET

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Sengupta and Mohanty

IET The Institution of Engineering and Technology

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty

2018 IEEE CONSUMER ELECTRONICS SOCIETY NEW MEMBER APPLICATION

Society Website: https://cesoc.ieee.org/

Membership Fee: $20
Student Membership Fee: $10

These offers apply to full conference and full conference attendees during the conference only.

Free CE Society memberships are open to all current IEEE members. Membership periods end Dec 31 2018 and must be renewed by the member through IEEE.

Incomplete or illegible applications cannot be processed. Write legibly
Enter your name as you want it to appear on you membership card and IEEE correspondence.

Your Contact information

Male ☐ Female ☐ Date of Birth (DD/MM/YYYY) / / ____________

Title First/Given Name Middle Name Last/Family Surname

Home

Street Address

City State/Province

Postal Code Country

Home Phone

Home Email

Your Professional Experience

(circle your choices below)

I have graduated from a three-to-five-year academic program with a university-level degree.

This academic institution or program is accredited in the country where the institution is located.
Yes No Do not know

I have _____ years of professional experience in teaching, creating, developing, practicing, or managing within the following field:

Engineering

Computer Sciences and Information Technologies

Physical Sciences

Biological and Medical Sciences

Mathematics

Technical Communications, Education, Management, Law and Policy
Other (please specify): ______________

Are you or were you ever a member of the IEEE? Yes No
If Yes, provide, if known:

Membership Number ____________________

Grade ____________________

Year of Expiration if no longer a member __________

Select Your Membership

☐ **Students, IEEE Members, Joining CE Society**

☐ **IEEE Member, joining CE Society**

Online at: https://cesoc.ieee.org/membership.html

Benefits Include:

1) A nice color magazine arrives at your door step to update you on latest CE
2) Discount in conference registration
3) Networking opportunity with global peers

IEEE Consumer Electronics Magazine

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

The CEM won an Apex Grand Award for excellence in writing in 2013. The CEM is the winner in the Regional 2016 STC Technical Communication Awards - Award of Excellence! The CEM is indexed in Clarivate Analytics (formerly IP Science of Thomson Reuters). The 2017 impact factor of CEM is 1.434.

Aim and Scope

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

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

Submission Instructions

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

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

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

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

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

Thank You !!!

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

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