Cybersecurity, Energy, and Intelligence Tradeoffs in IoT

Faculty Development Program, Sponsored by AICTE, Govt. of India

Govt. College of Engineering and Technology, Bhubaneswar

05-09 July 2021

Saraju P. Mohanty, University of North Texas, USA.

Email: smohanty@ieee.org Website: http://www.smohanty.org

The Big Picture

Population Trend – Urban Migration

"India is to be found not in its few cities, but in its 700,000 villages."
- Mahatma Gandhi

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

Source: http://www.urbangateway.org

Issues Challenging City Sustainability

Pollution

Water Crisis

Energy Crisis

Traffic

Smart City Technology - As a Solution

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

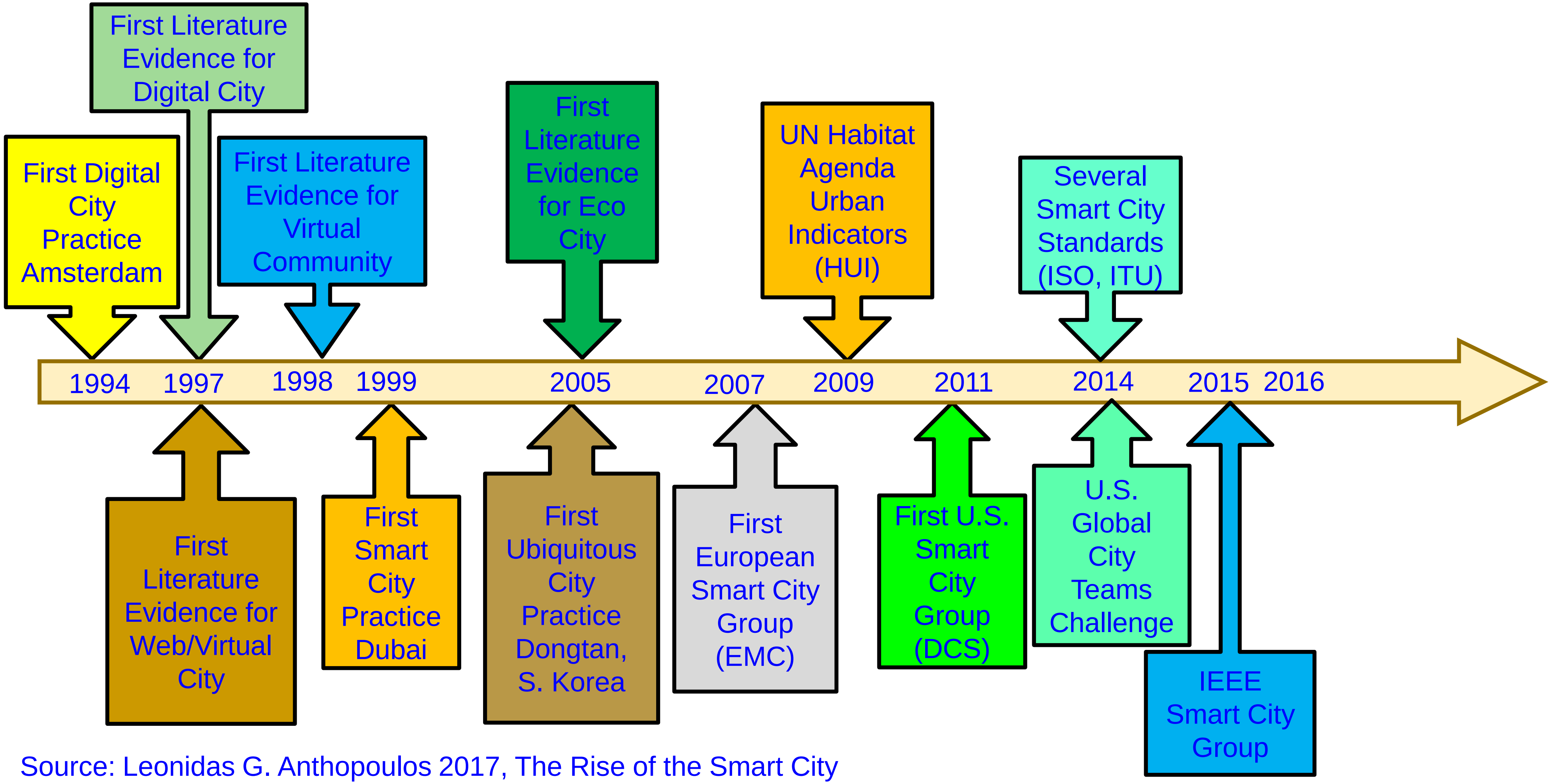
At Different Levels:
- Smart Village
- Smart State
- Smart Country

July 2016

- Year 2050: 70% of world population will be urban

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

Smart Cities - History



Source: Leonidas G. Anthopoulos 2017, The Rise of the Smart City

Smart Cities Vs Smart Villages

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

-- Merriam-Webster

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

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

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

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

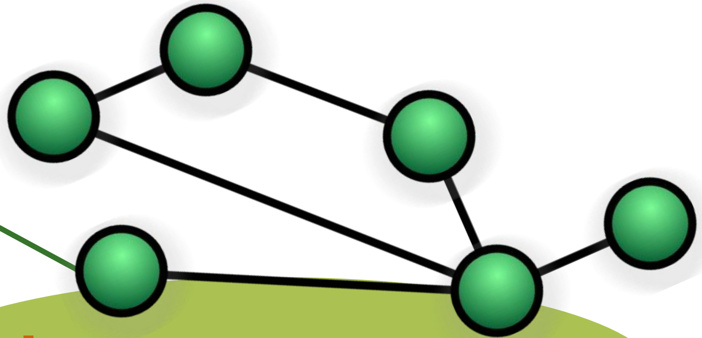
Smart Cities - 3 Is

Instrumentation

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

Smart Cities

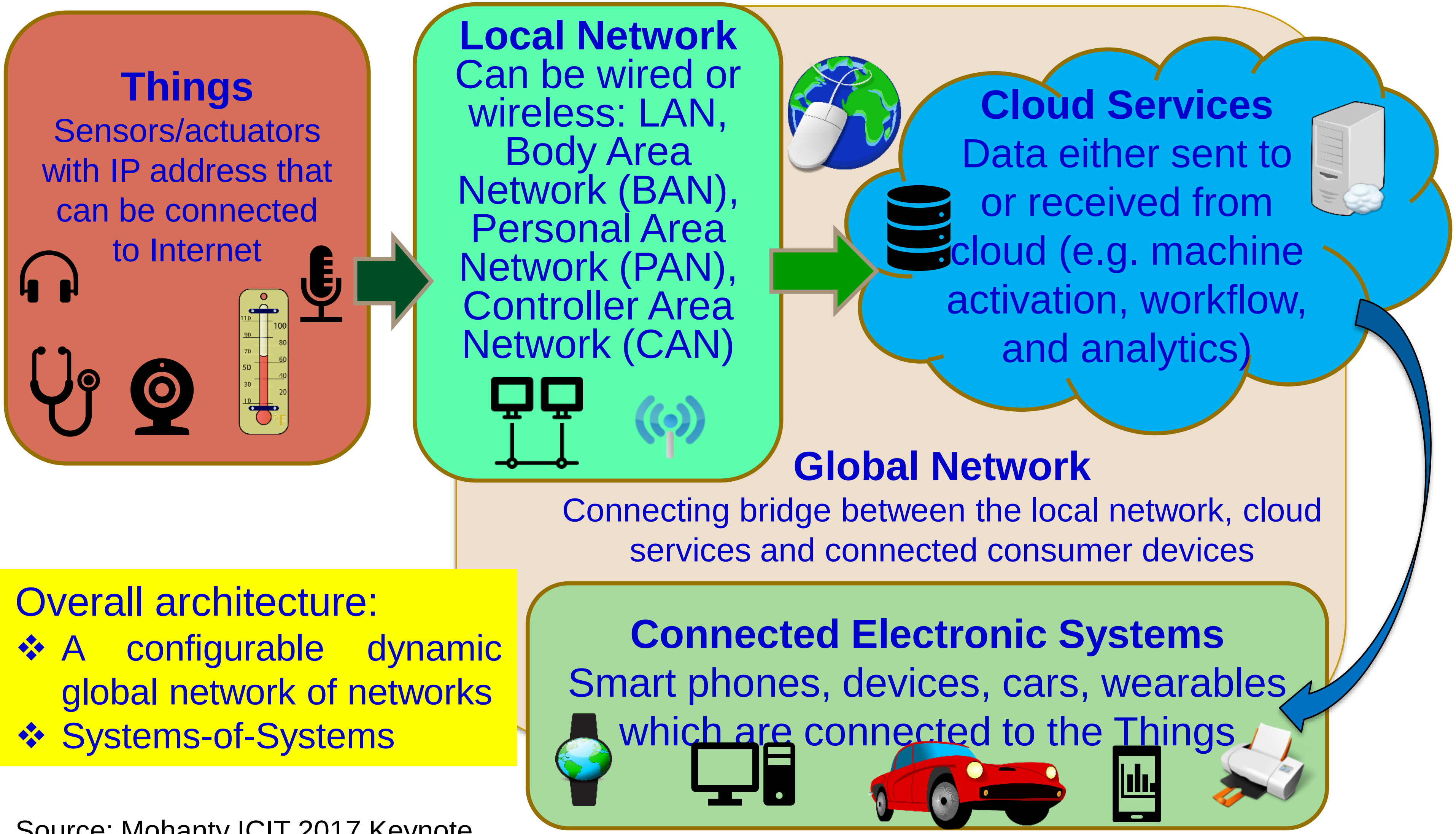
Intelligence



Interconnection

Source: Mohanty ISC2 2019 Keynote

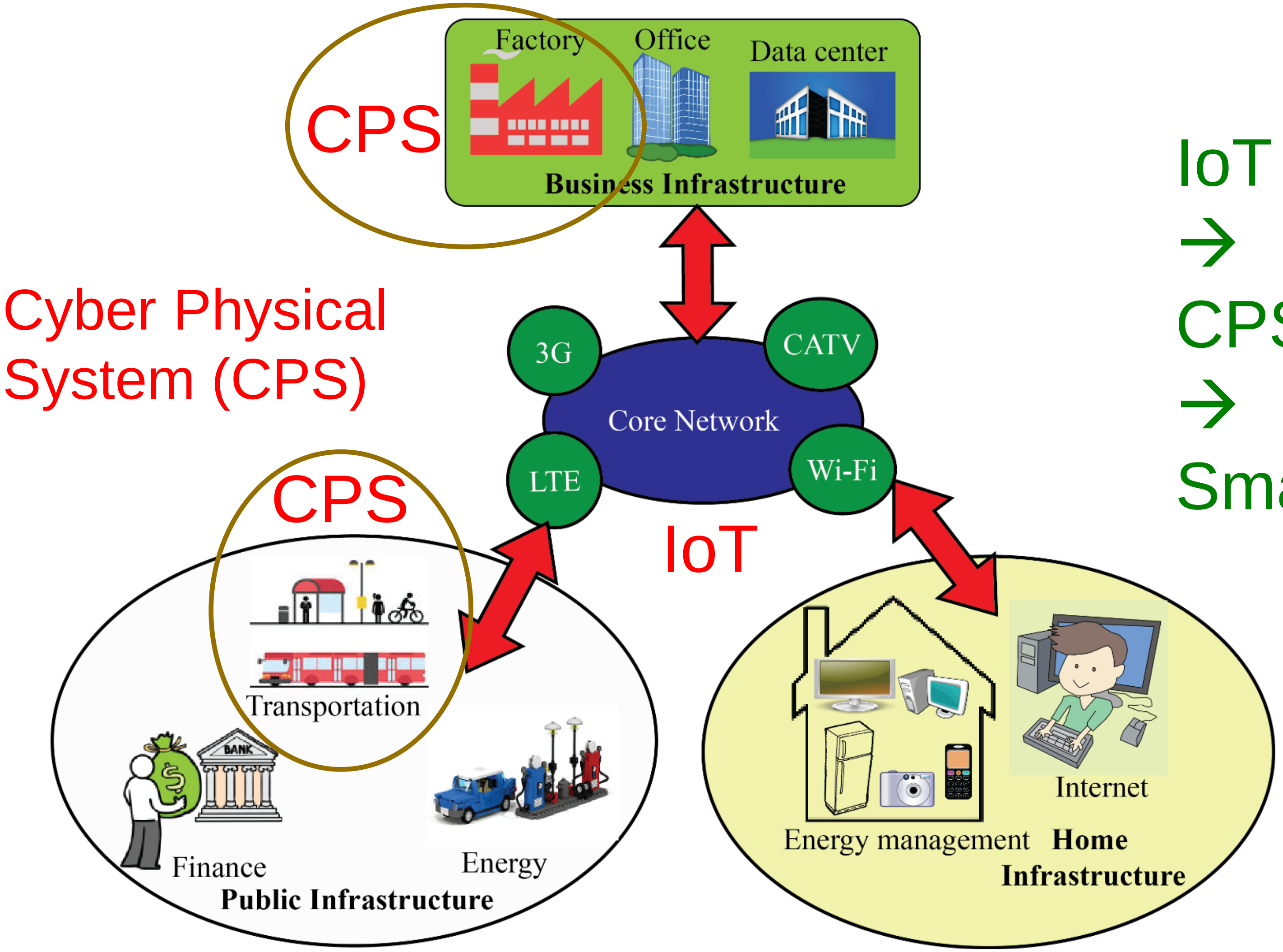
Internet of Things (IoT) – Concept



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

Source: Mohanty ICIT 2017 Keynote

IoT → CPS → Smart Cities or Smart Villages

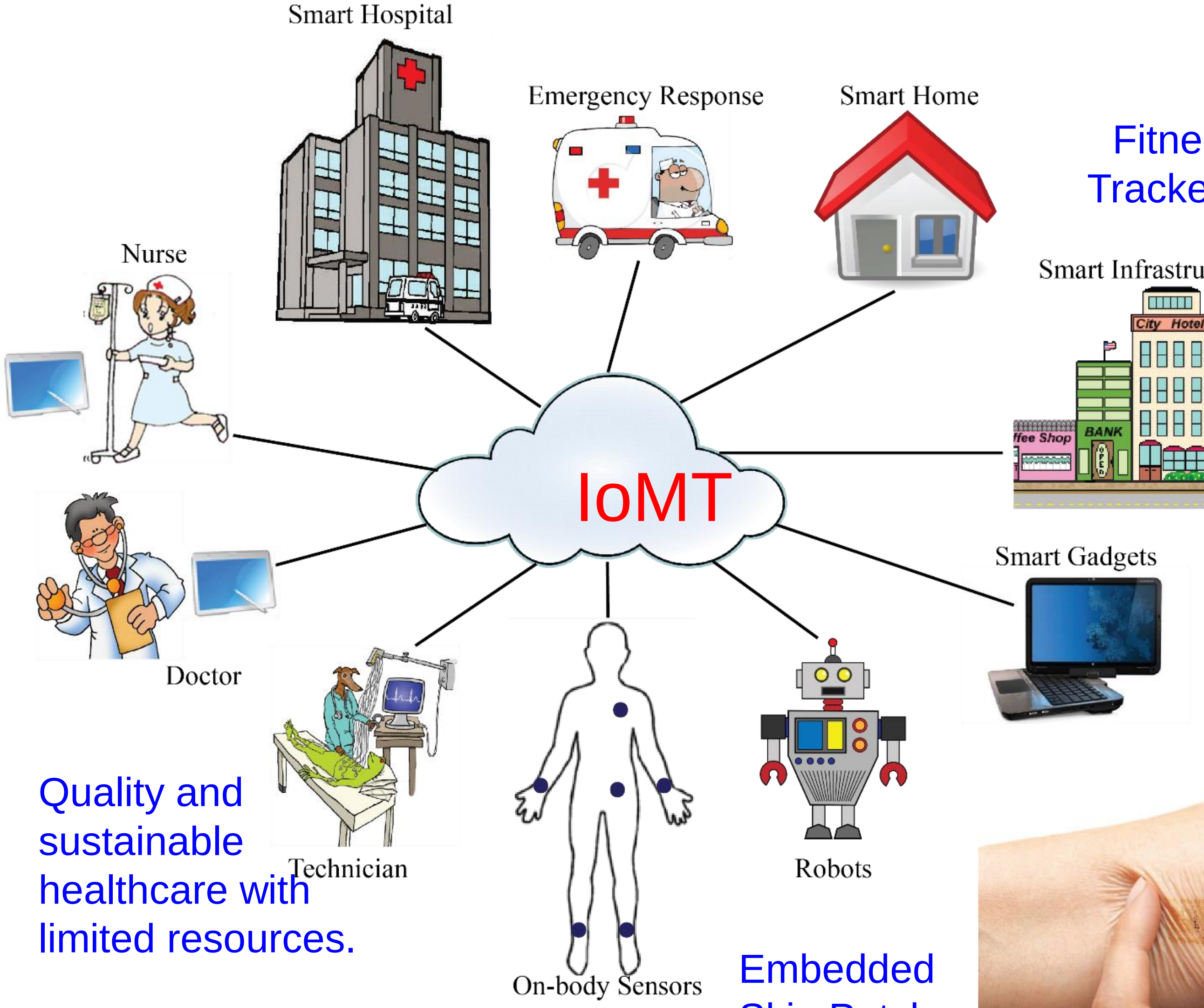


IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

IoT is the backbone

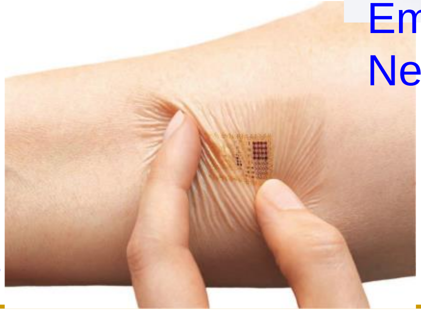
Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Smart Healthcare



Fitness Trackers

Headband with Embedded Neurosensors



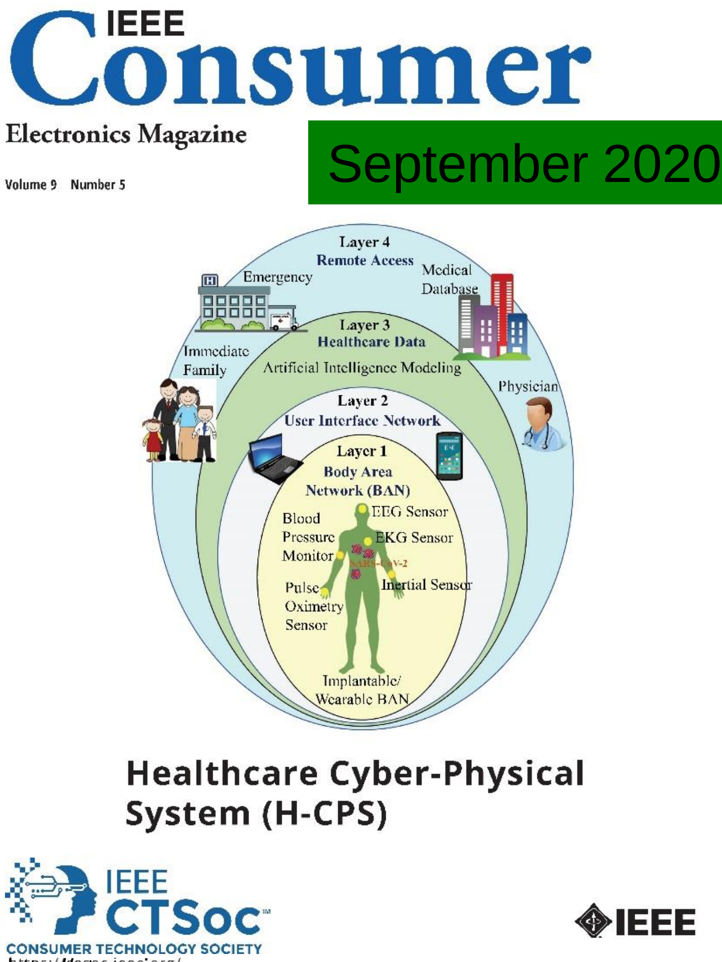
Embedded Skin Patches

January 2018

Quality and sustainable healthcare with limited resources.

Source: Mohanty CE Magazine July 2016

Healthcare Cyber-Physical System (H-CPS)



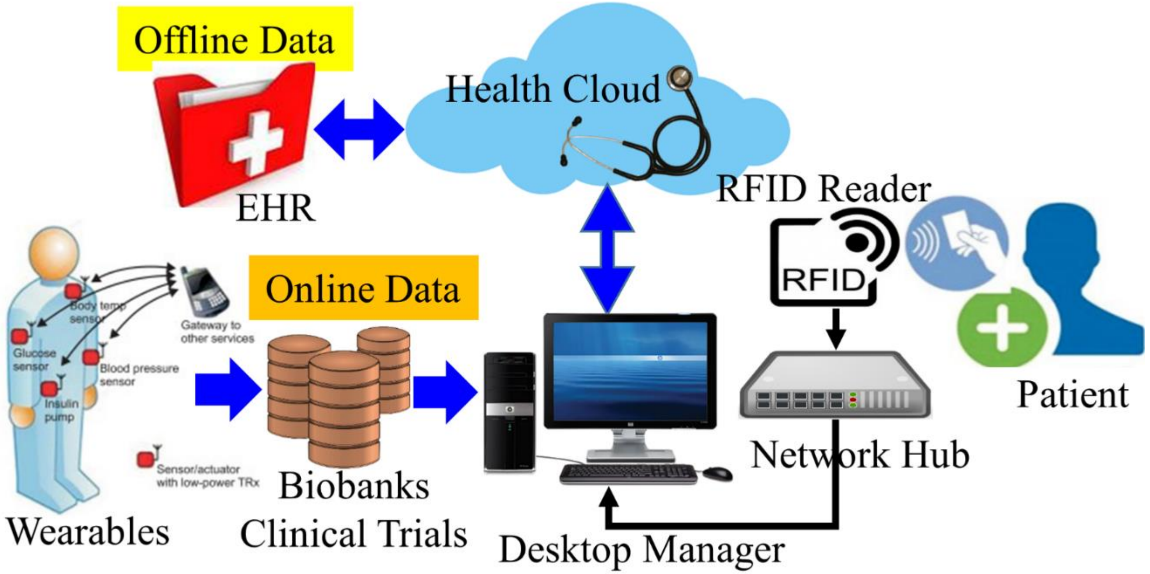
September 2020

http://ctsoc.ieee.org

Internet-of-Medical-Things (IoMT)

OR

Internet-of-Health-Things (IoHT)

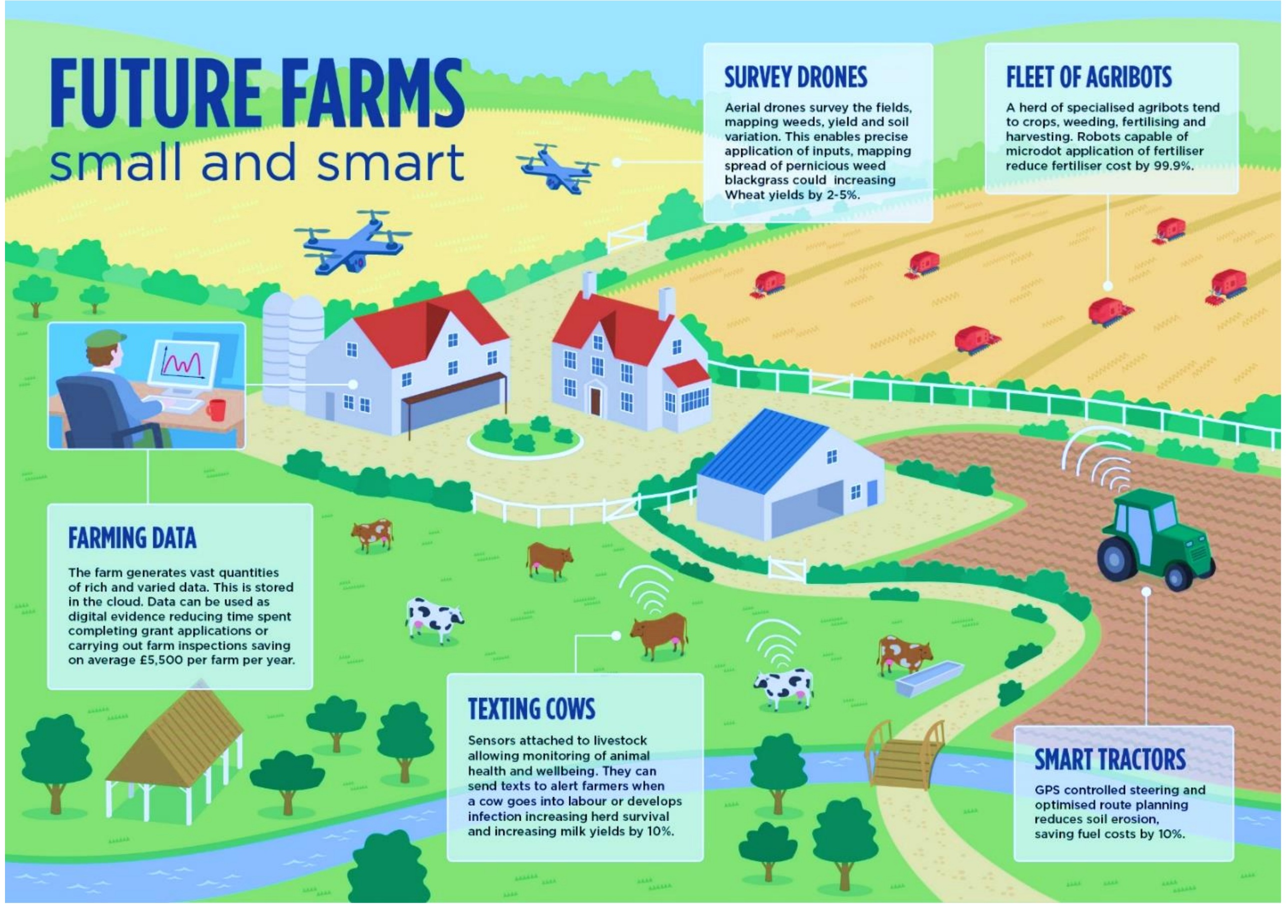


Requires:
- ❖ Data and Device Security
- ❖ Data Privacy

H-CPS ← Biosensors + Medical Devices + Wearable Medical Devices (WMDs) + Implantable Medical Devices (IMDs) + Internet + Healthcare database + AI/ML + Applications that connected through Internet.

Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

Smart Agriculture



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

Smart Agriculture/Farming Market Worth $18.21 Billion By 2025

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

Climate-Smart Agriculture Objectives:

- Increasing agricultural productivity
- Resilience to climate change
- Reducing greenhouse gas

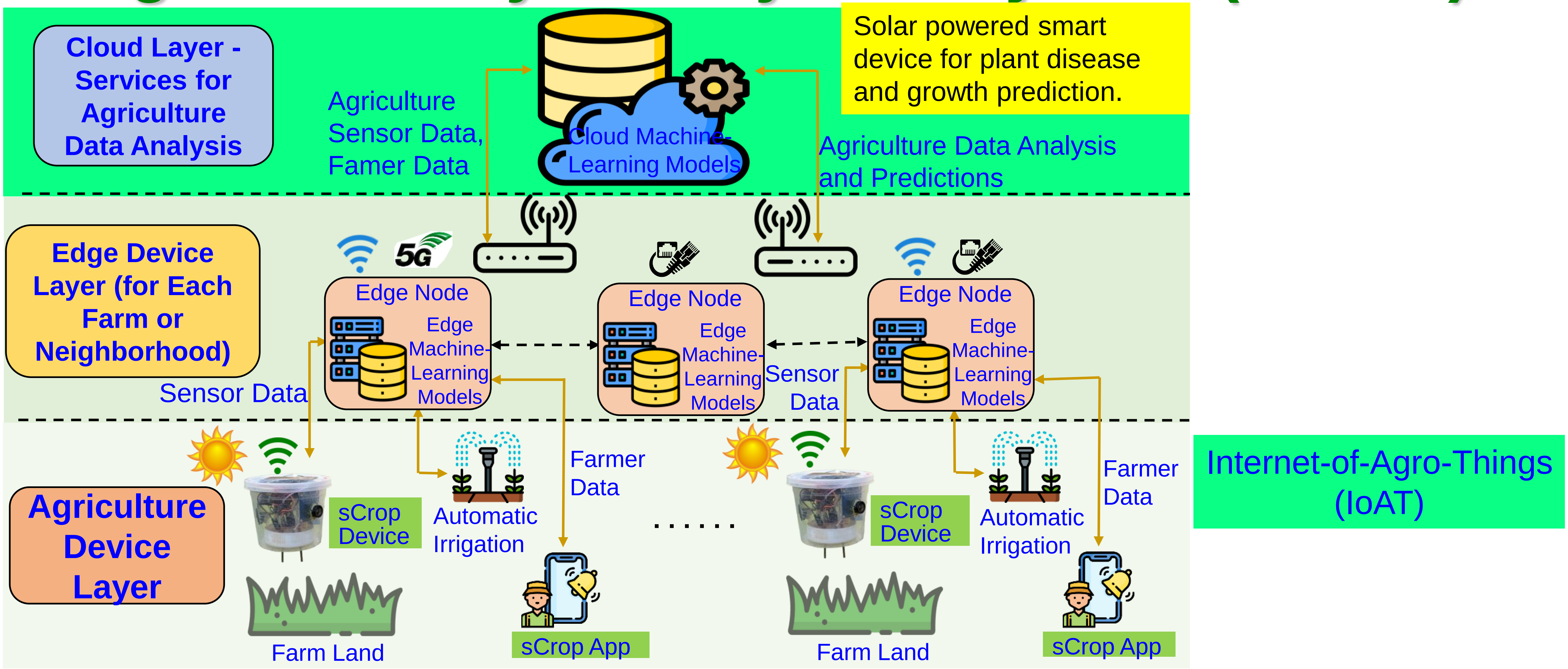
http://www.fao.org

Internet-of-Agro-Things (IoAT)

Automatic Irrigation System

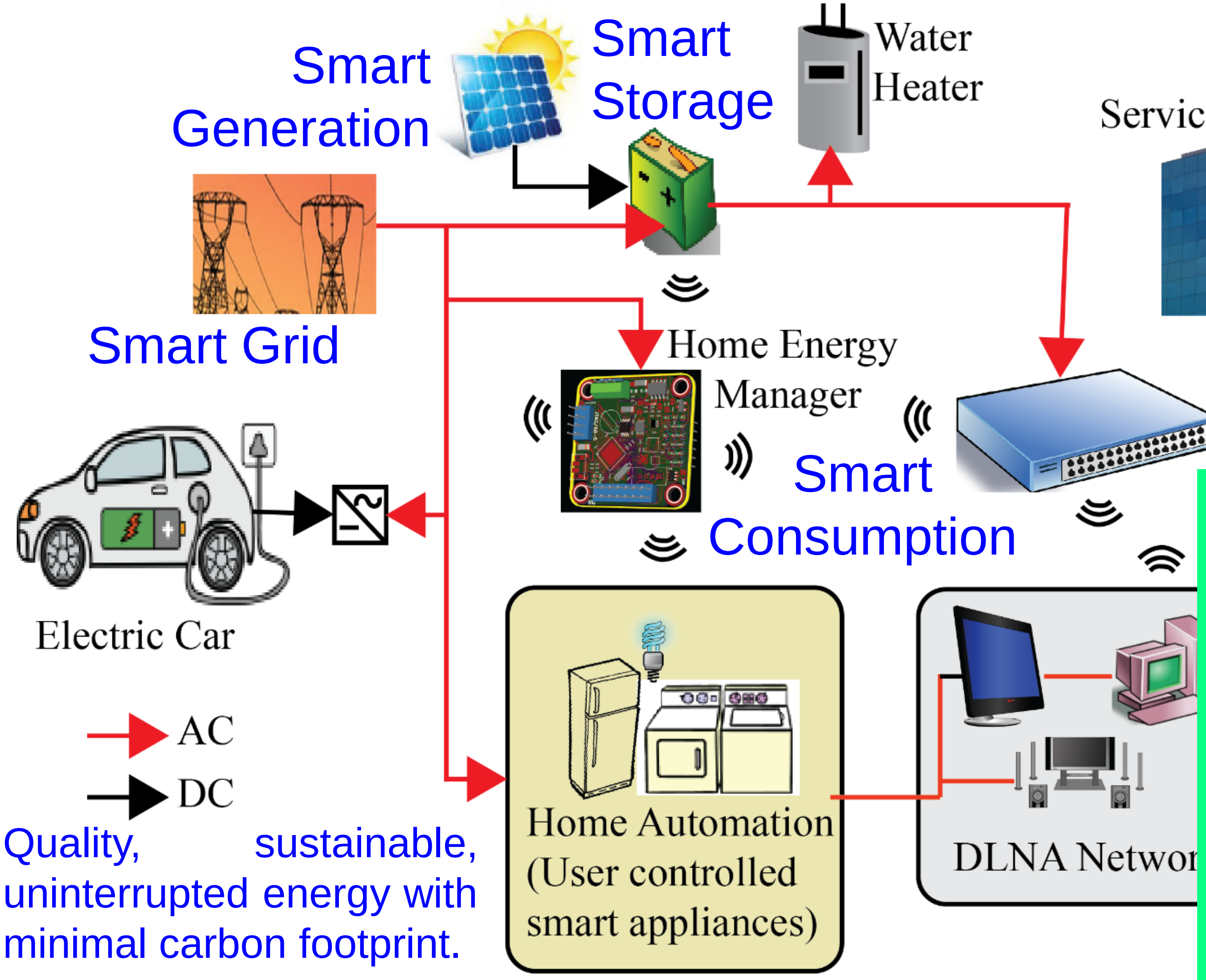
Source: Maurya 2017, CE Magazine July 2017

Agriculture Cyber-Physical System (A-CPS)



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

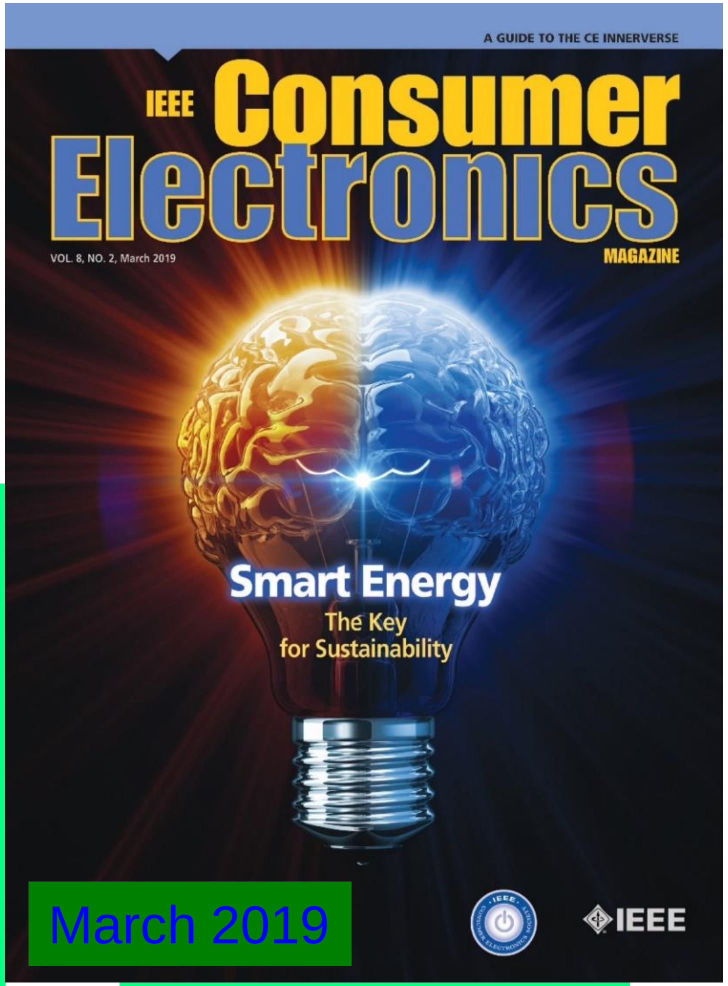
Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

IoT Role:

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

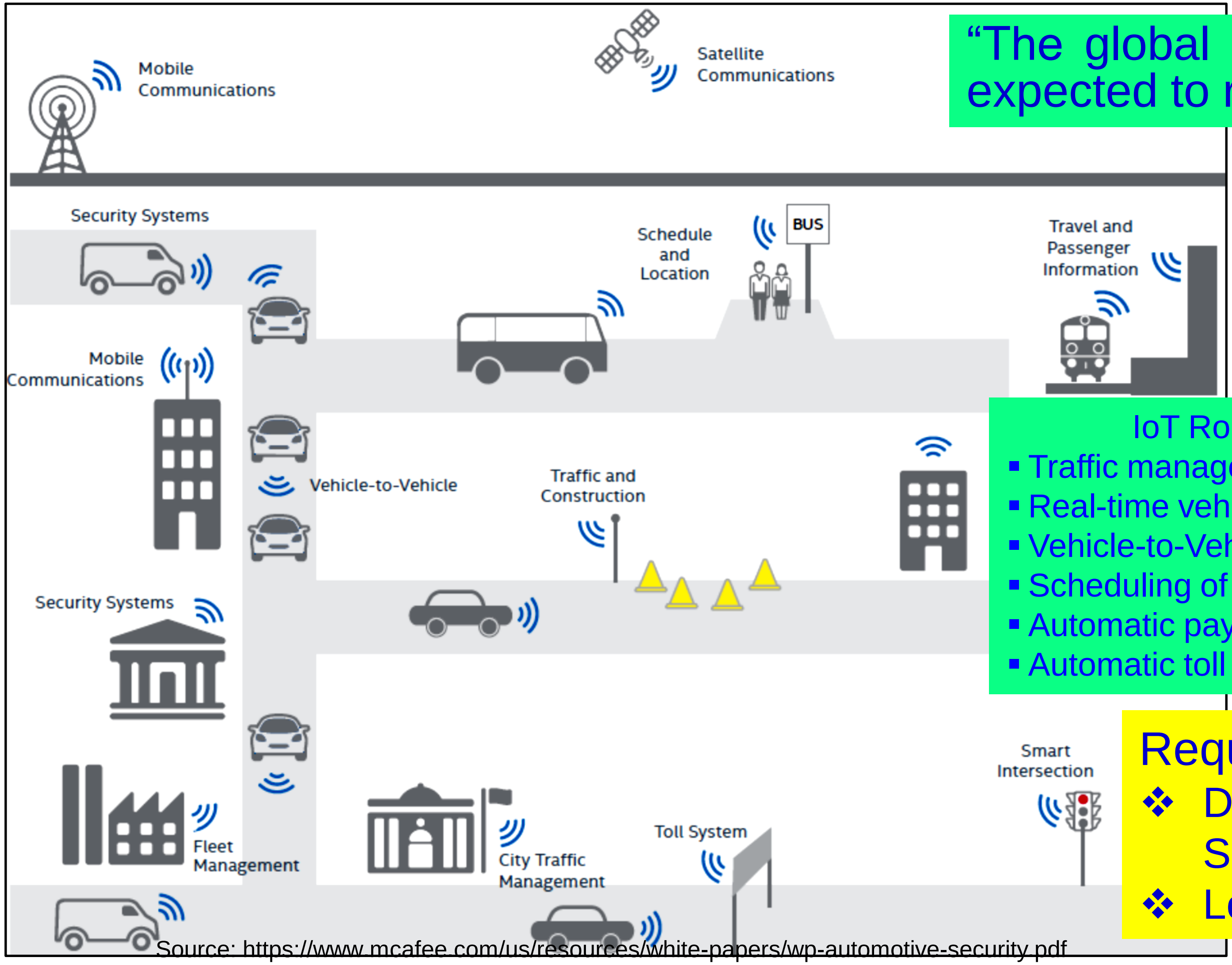


March 2019

Internet of Energy

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

Transportation Cyber-Physical System (T-CPS)



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

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

Source: Datta 2017, CE Magazine Oct 2017

IoT Role Includes:

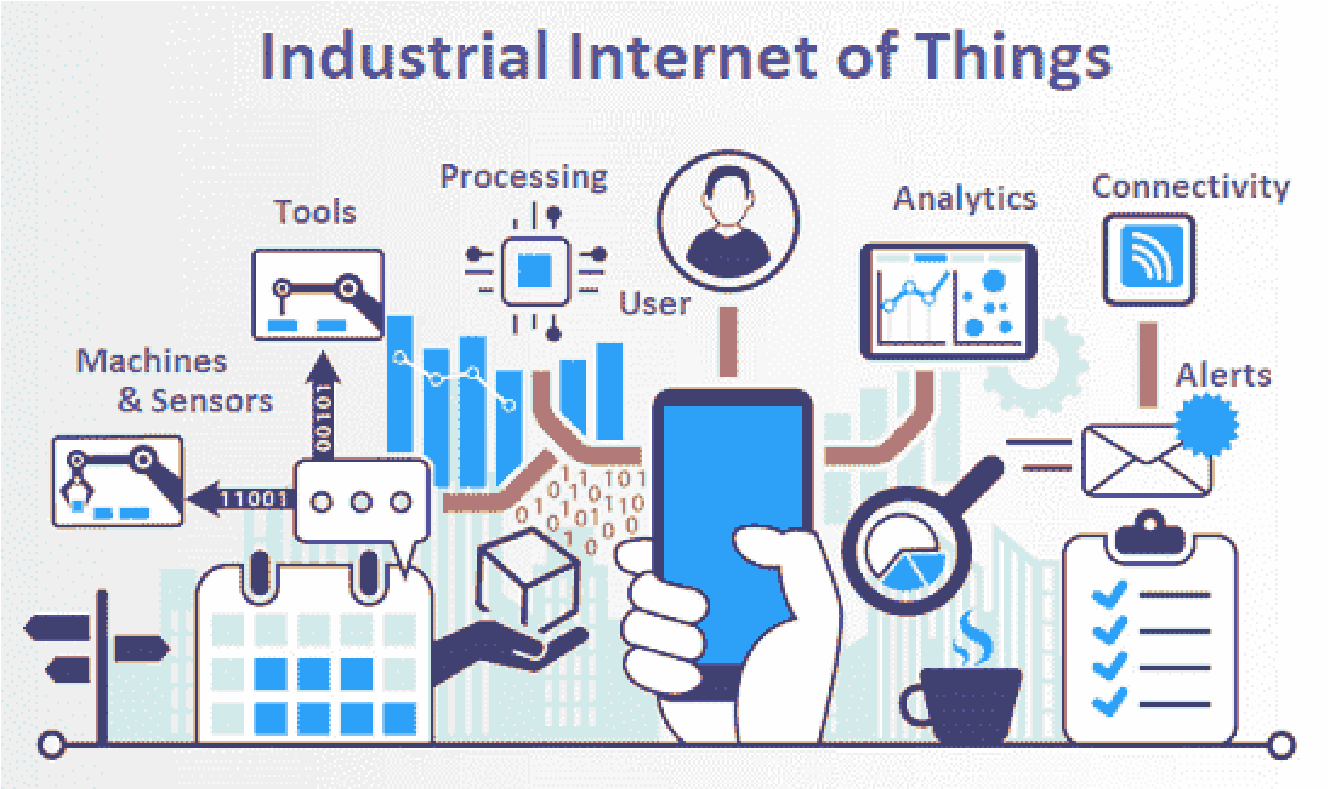
- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

Requires:

- ❖ Data and Device Security
- ❖ Location Privacy

July 2020

Industrial Internet of Things (IIoT)

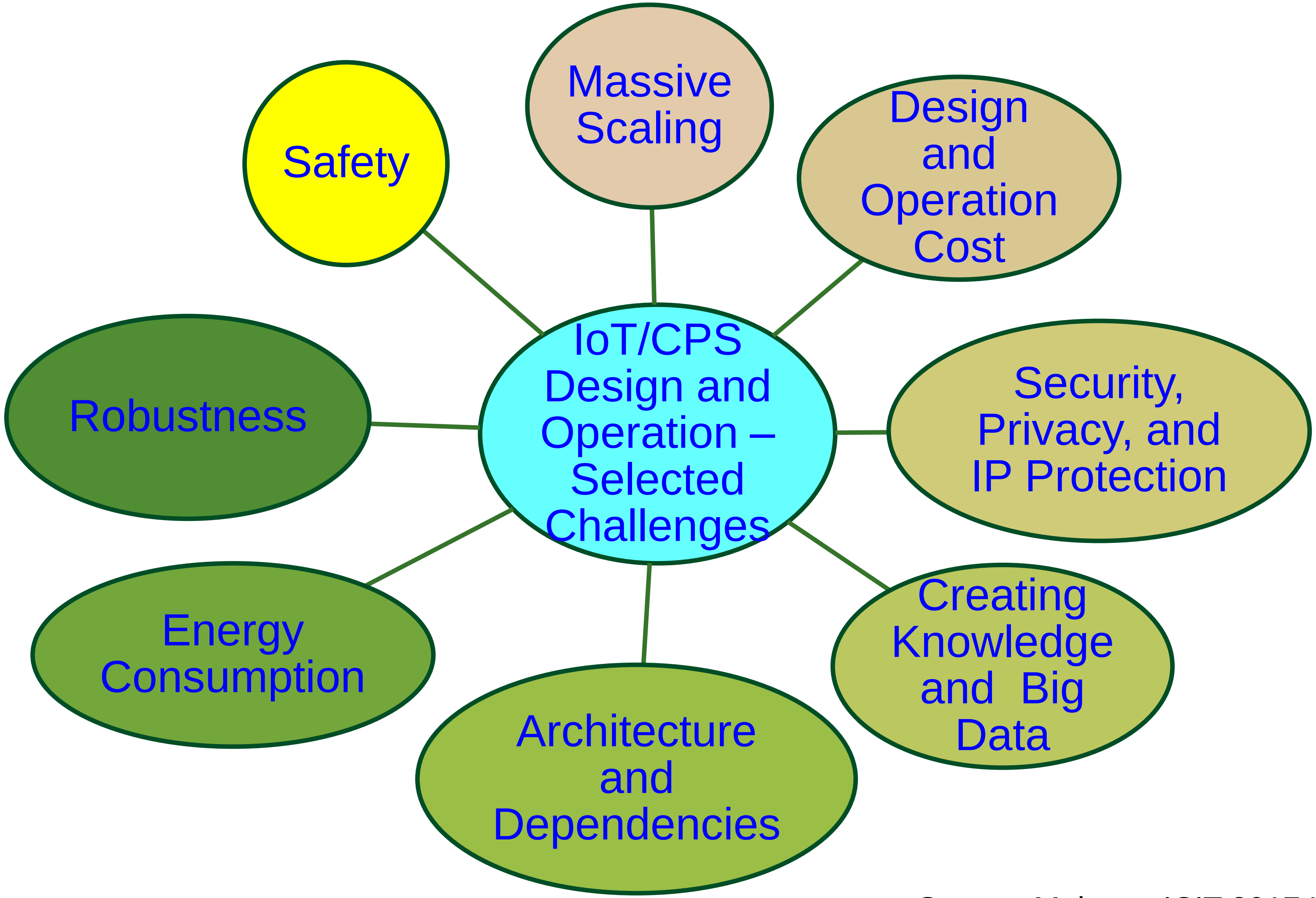


Source: https://www.rfpage.com/applications-of-industrial-internet-of-things/

Applications
- Industrial Automation
- Smart Robotics
- Predictive Maintenance
- Integration of Tools / Wearables
- Smart Logistics

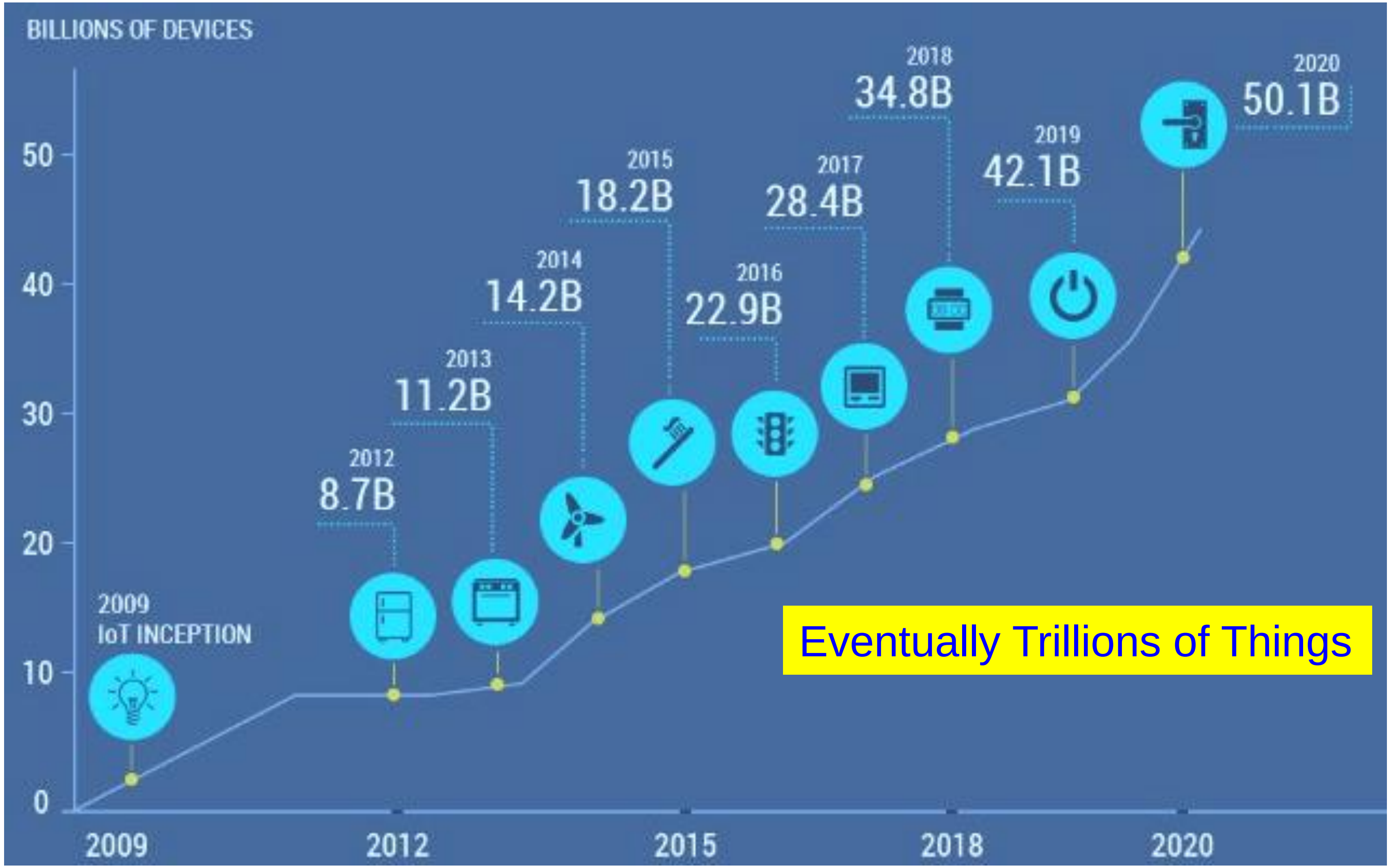
Challenges in IoT/CPS Design

IoT/CPS – Selected Challenges



Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things



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

Security Challenges – Information

Online Banking

Credit Card Theft


Hacked: Linkedin, Tumbler, & Myspace

LinkedIn
tumblr.
myspace

Who did it: A hacker going by the name Peace.
What was done: 500 million passwords were stolen.

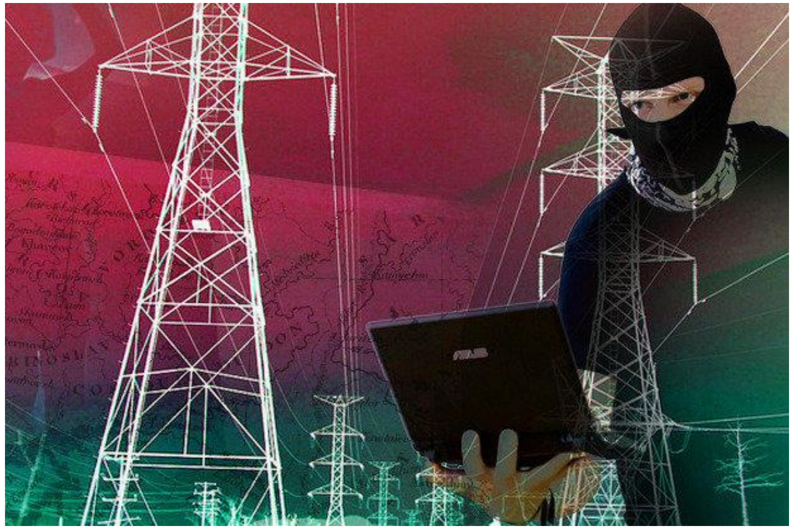
Details: Peace had the following for sale on a Dark Web Store:
167 million Linkedin passwords
360 million Myspace passwords
68 million Tumbler passwords
100 million VK.com passwords
71 million Twitter passwords

Personal Information

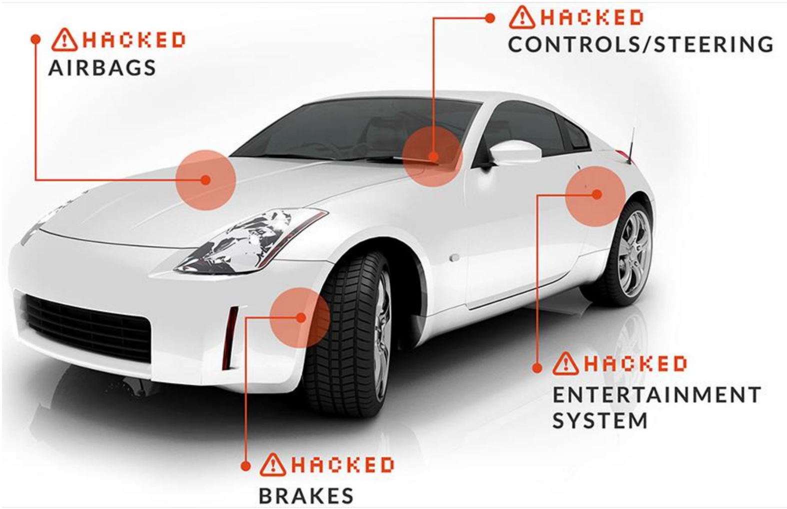
Credit Card/Unauthorized Shopping

Cybersecurity Challenges - System

Power Grid Attack



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



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

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

Smart Healthcare - Security and Privacy Issue

September 2020

http://ctsoc.ieee.org

Selected Smart Healthcare Security/Privacy Challenges

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

IoMT Security Issue is Real & Scary

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

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

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

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

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

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

Reliable Supply Chain: Food Supply Chain: Farm → Dinning

How to ensure quality food through legitimate supply chain?

Trading

Consumption
By Users

Retails Service of Food

Processing

Transportation

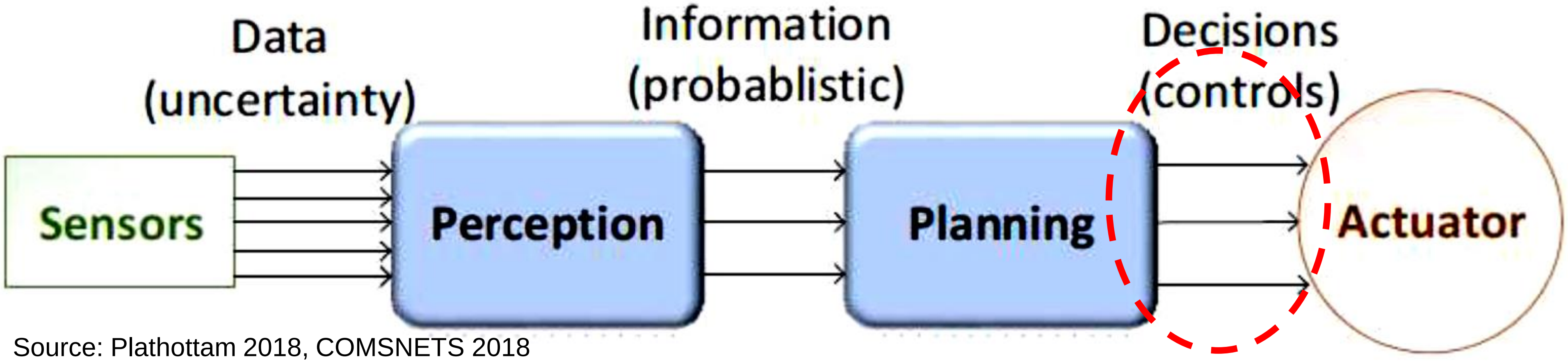
Farming & Growing

Similarly, Pharmaceutical Supply Chain

Source: A. M. Joshi, U. P. Shukla, and S. P. Mohanty, "Smart Healthcare for Diabetes: A COVID-19 Perspective", *arXiv Quantitative Biology*, arXiv:2008.11153, August 2020, 18-pages.

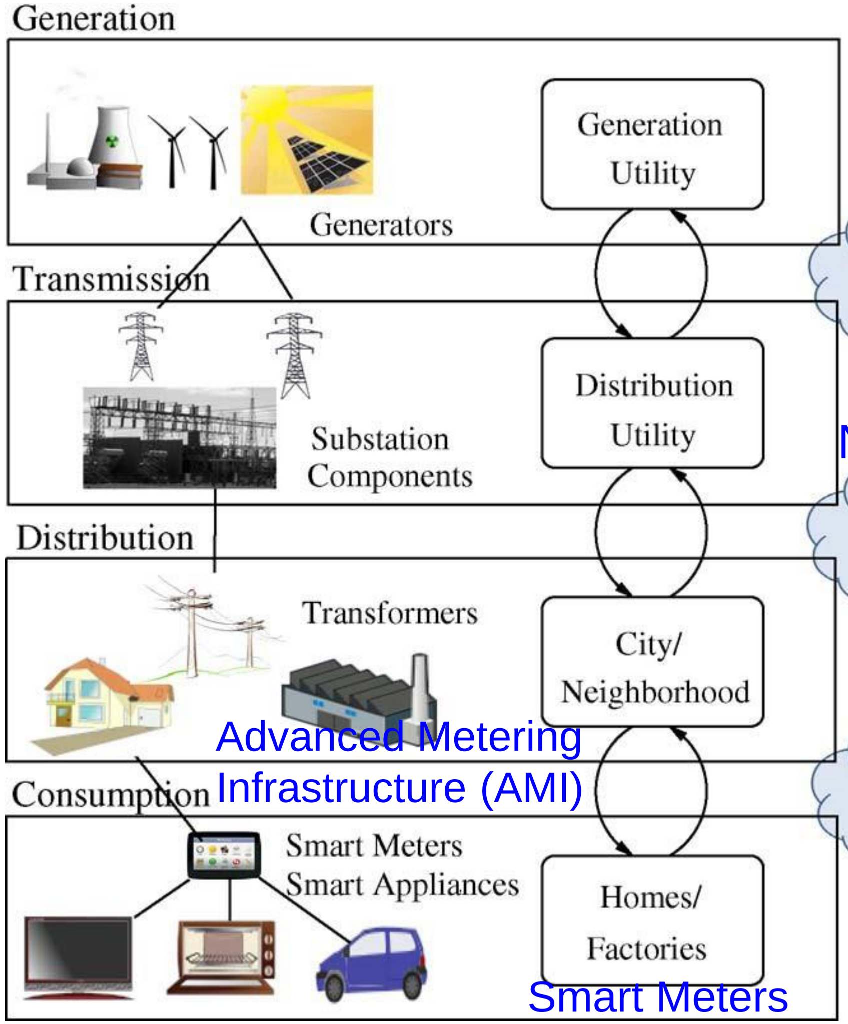
Smart Car – Modification of Input Signal of Control Can be Dangerous

- Typically vehicles are controlled by human drivers
- Designing an Autonomous Vehicle (AV) requires decision chains.
- 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

Smart Grid - Vulnerability



Advanced Metering Infrastructure (AMI)

Smart Meters

Wide-Area Network (WAN)

Neighbor-Area Network (NAN)

Home-Area Network (HAN)

Control Center

Supervisory Control and Data Acquisition (SCADA)

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

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

Network/Communication Components

Phasor Measurement Units (PMU)

Phasor Data Concentrators (PDC)

Energy Storage Systems (ESS)

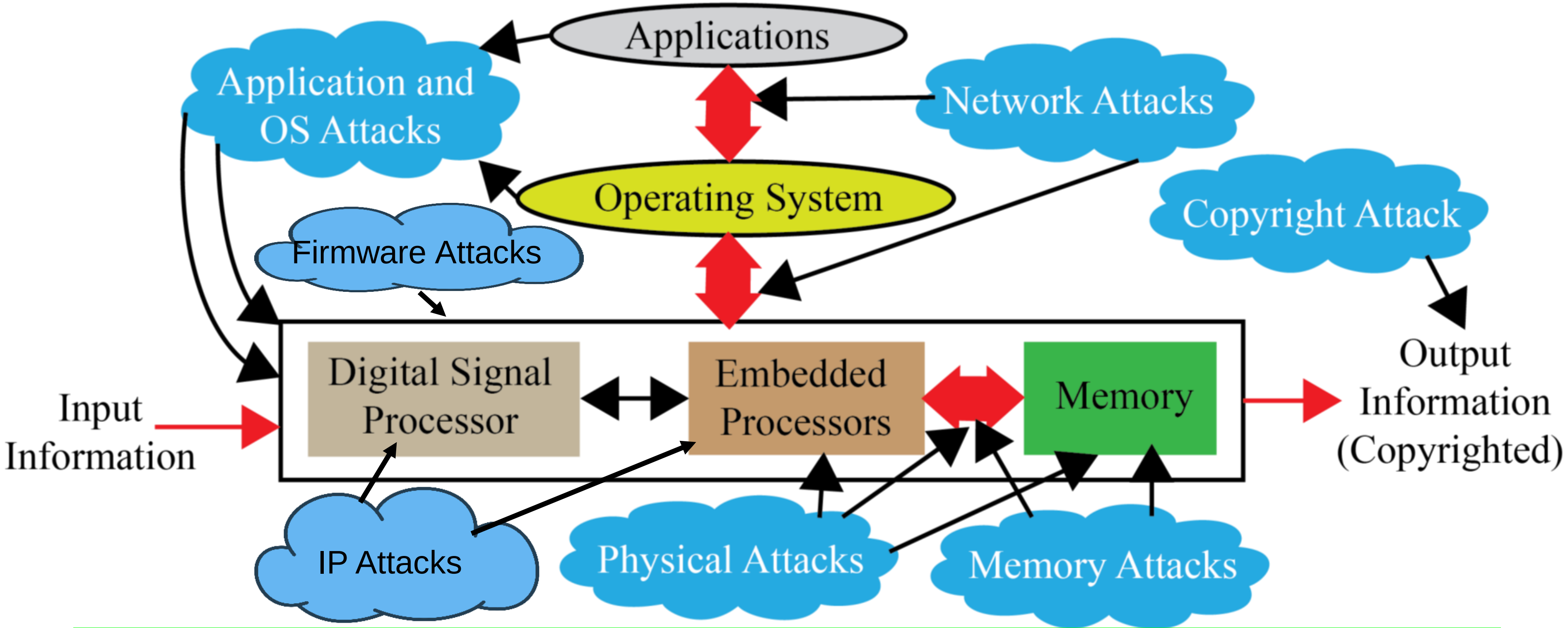
Programmable Logic Controllers (PLCs)

Smart Meters

Smart Grid Model – CPS Security Perspective

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

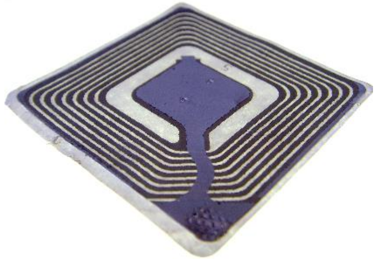
Selected Attacks on a CE System – Security, Privacy, IP Rights



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

Source: Mohanty ZINC 2018 Keynote

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

NFC Security - Attacks

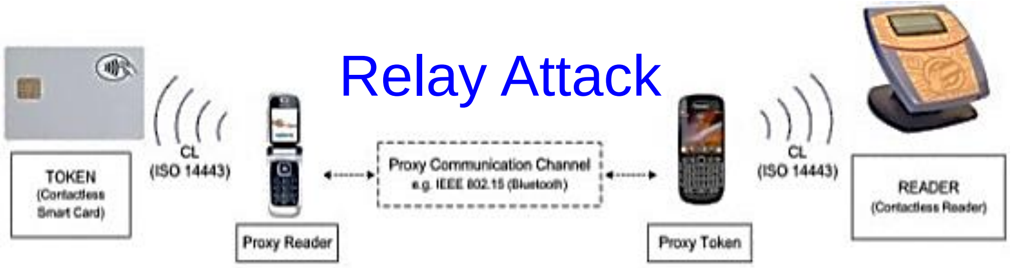
Selected NFC Attacks

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

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

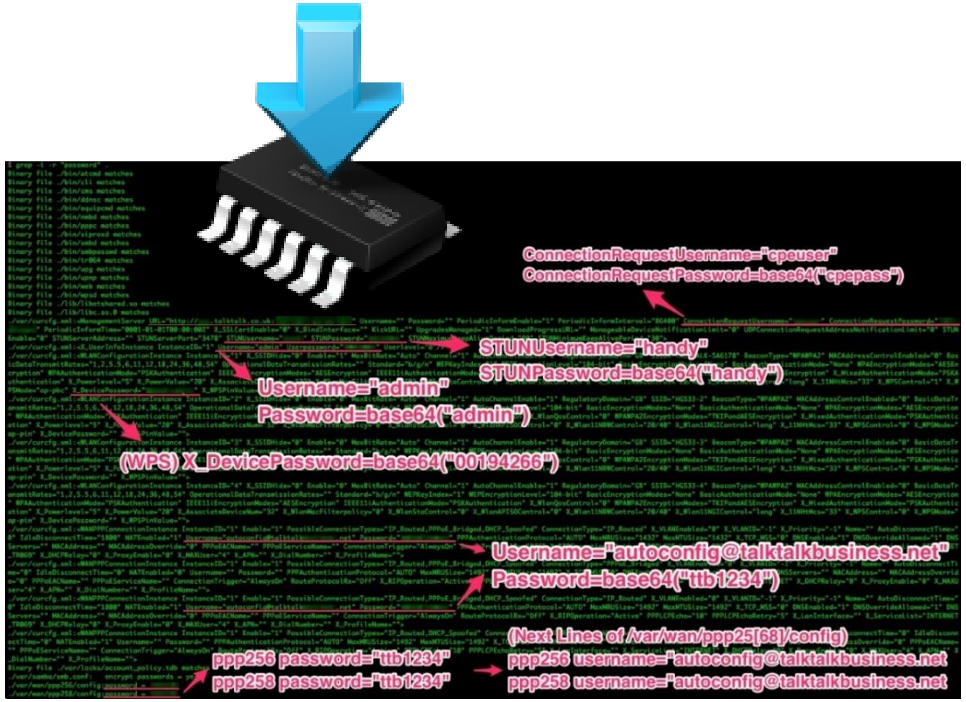
Eavesdropping

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

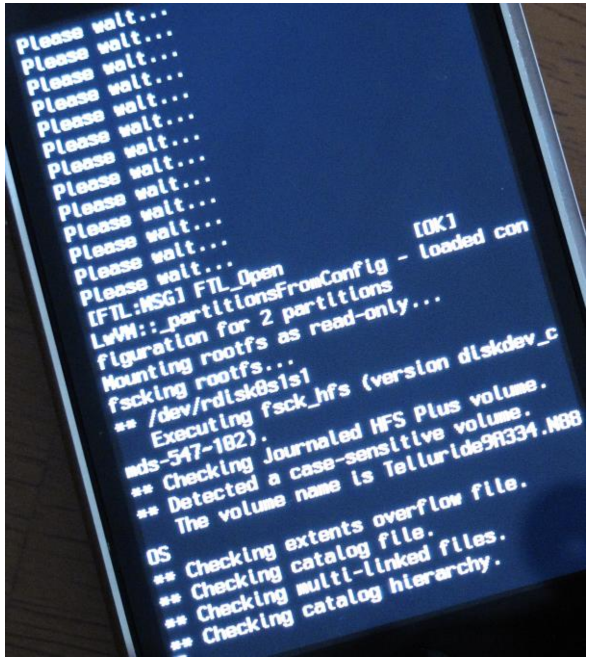


Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

Firmware Reverse Engineering – Security Threat for Embedded System



Extract, modify, or reprogram code

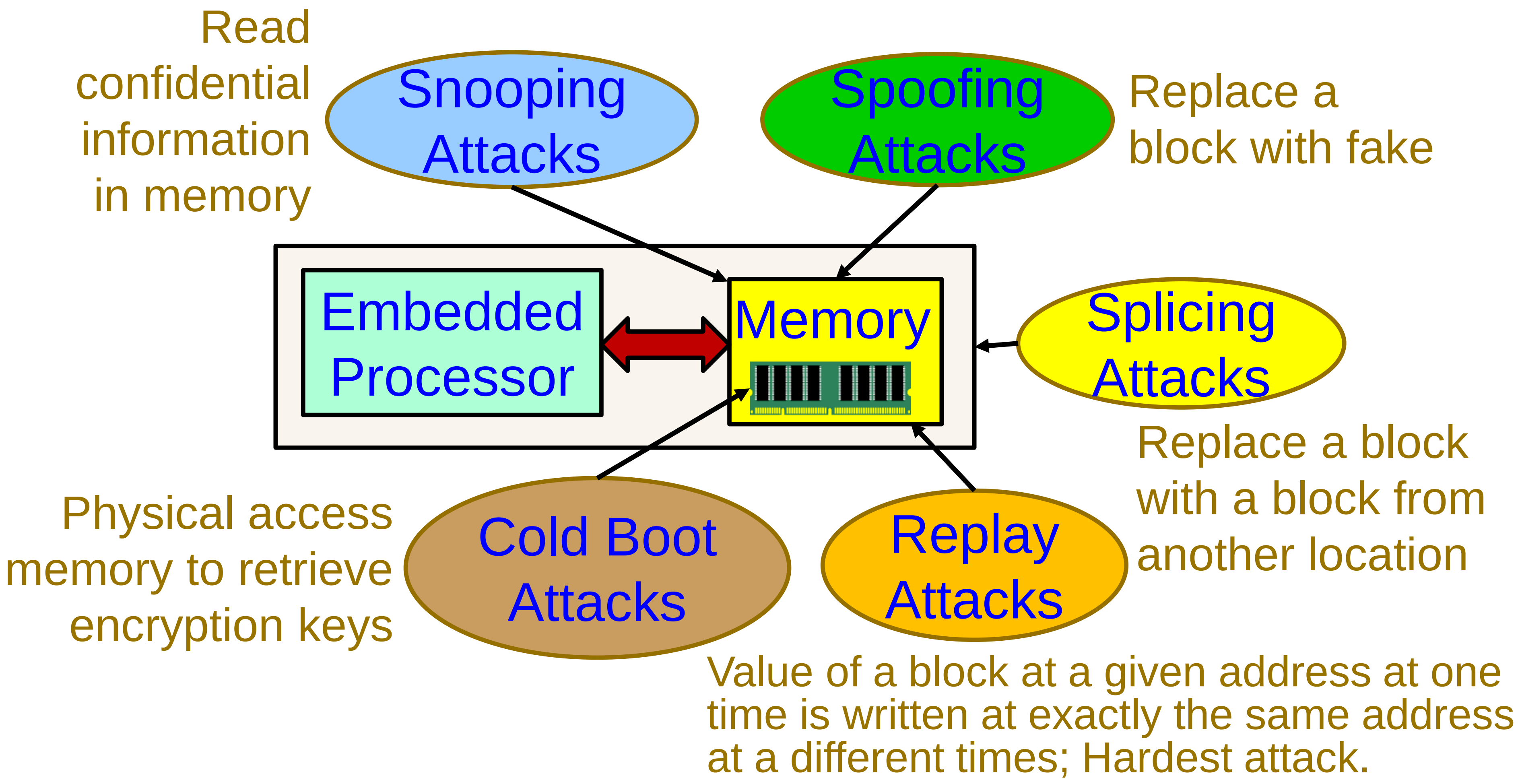


OS exploitation,
Device jailbreaking

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

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

Attacks on Embedded Systems' Memory



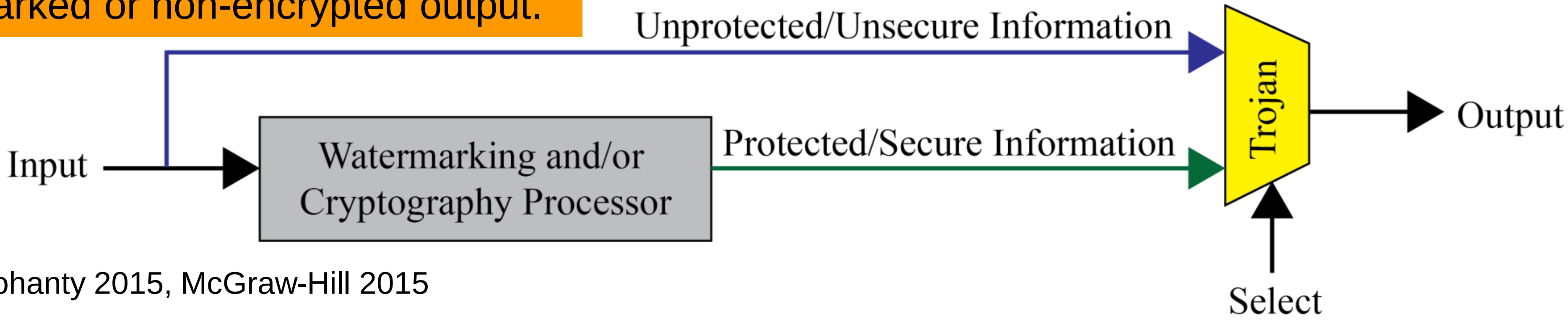
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "TSV: A Novel Energy Efficient Memory Integrity Verification Scheme for Embedded Systems", *Elsevier Journal of Systems Architecture*, Vol. 59, No. 7, Aug 2013, pp. 400-411.

Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

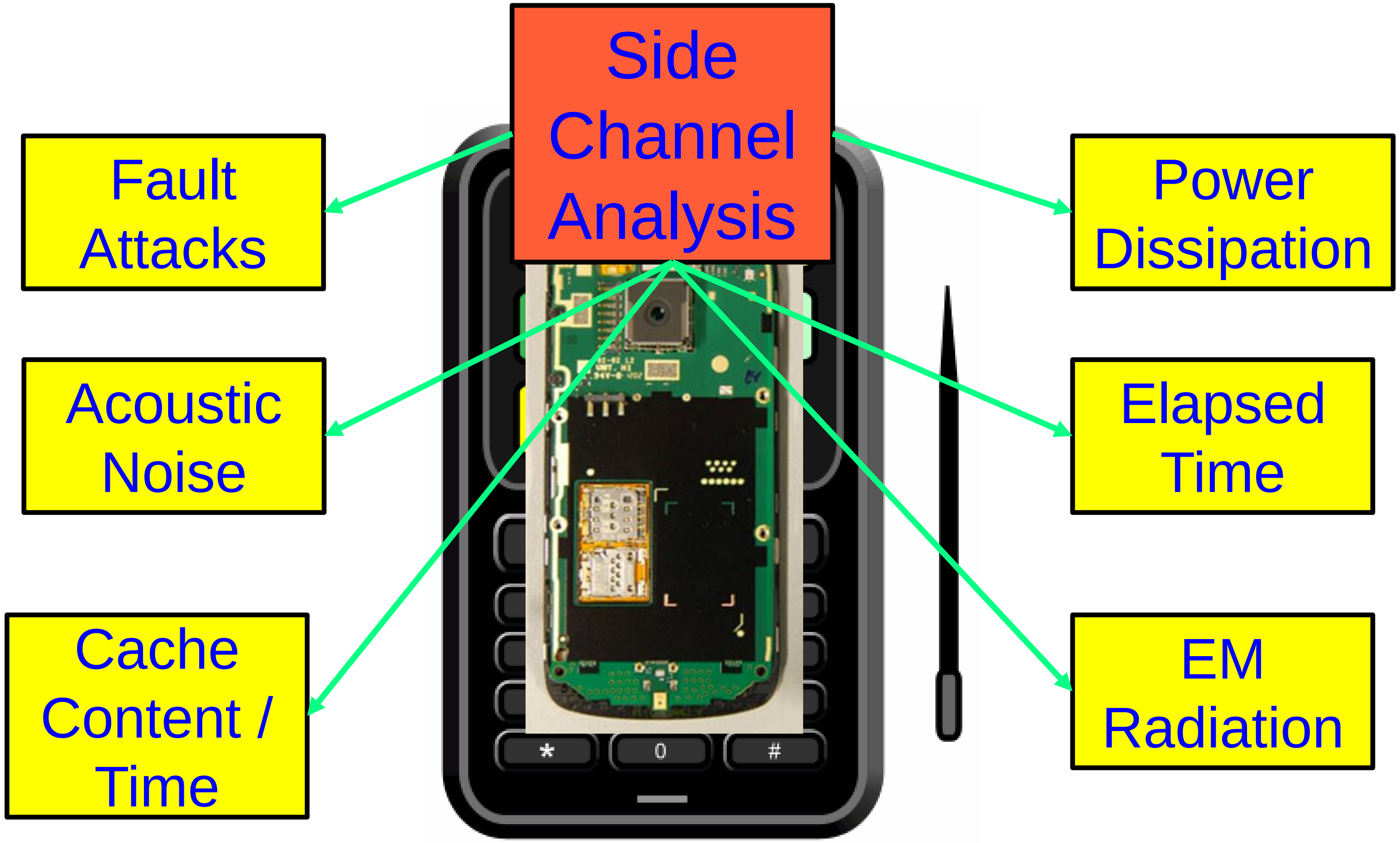
Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans



Source: Mohanty 2015, McGraw-Hill 2015

Side Channel Analysis Attacks

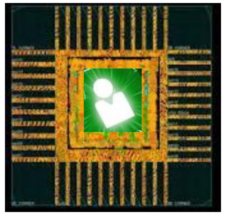


Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

Security, Privacy, and IP Rights

Hardware
Trojan



System Security

Data Security

System Privacy

Data Privacy

Counterfeit Hardware
(IP Rights Violation)

Data Ownership

July 2017

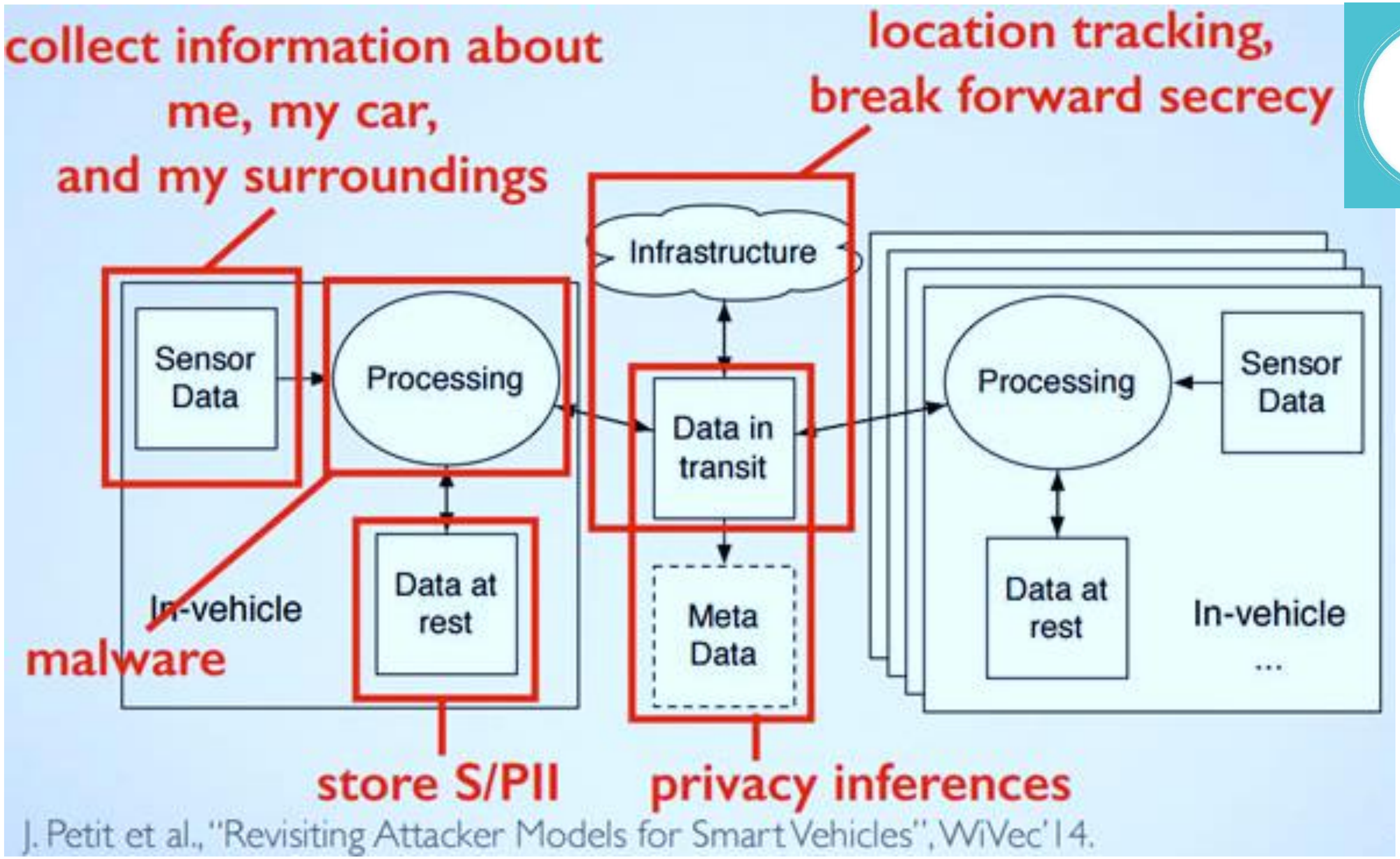
Source: Mohanty ICIT 2017 Keynote

Privacy Challenge – Personal Data

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

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

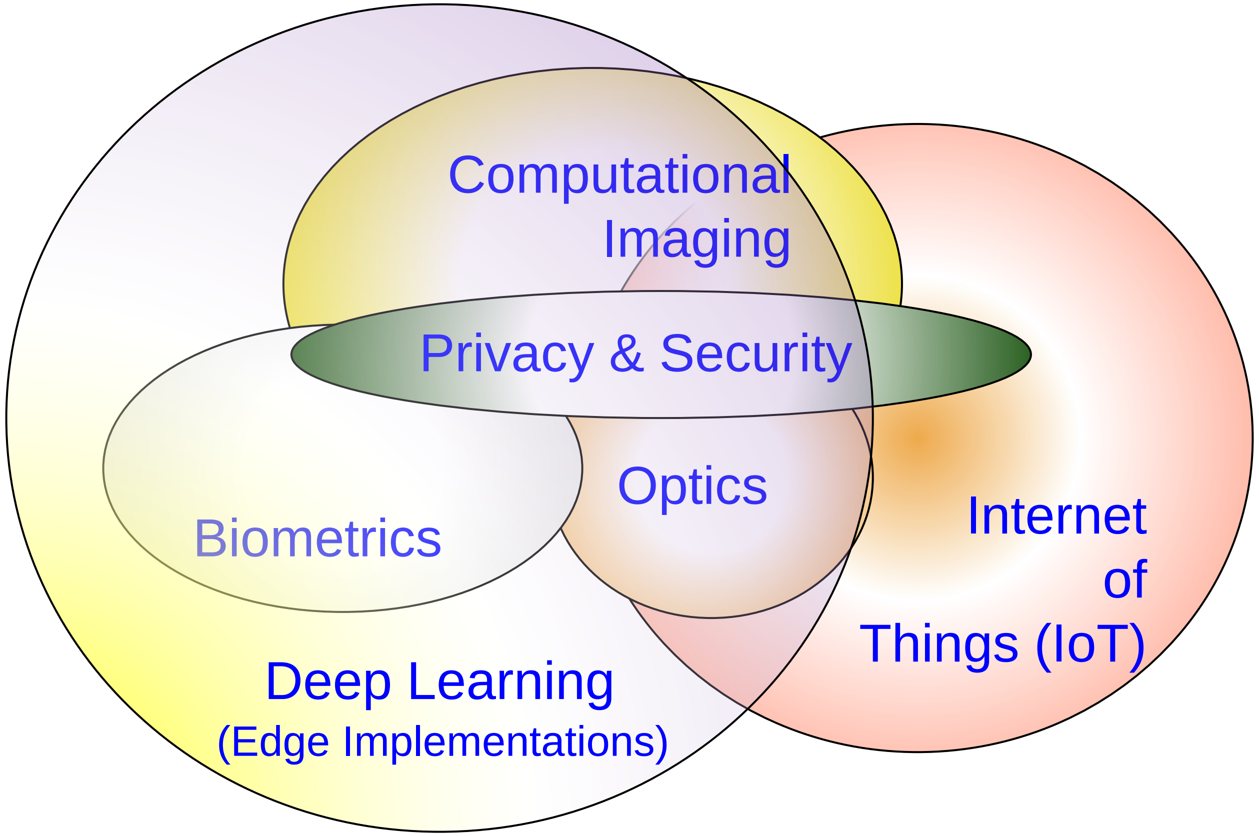
Privacy Challenge – System, Location



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

Bigdata → Intelligence – 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.

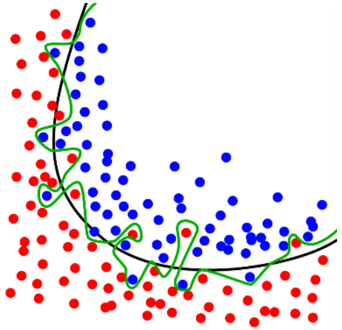


Source: Corcoran Keynote 2018

ML Modeling Issues

Machine Learning Issues

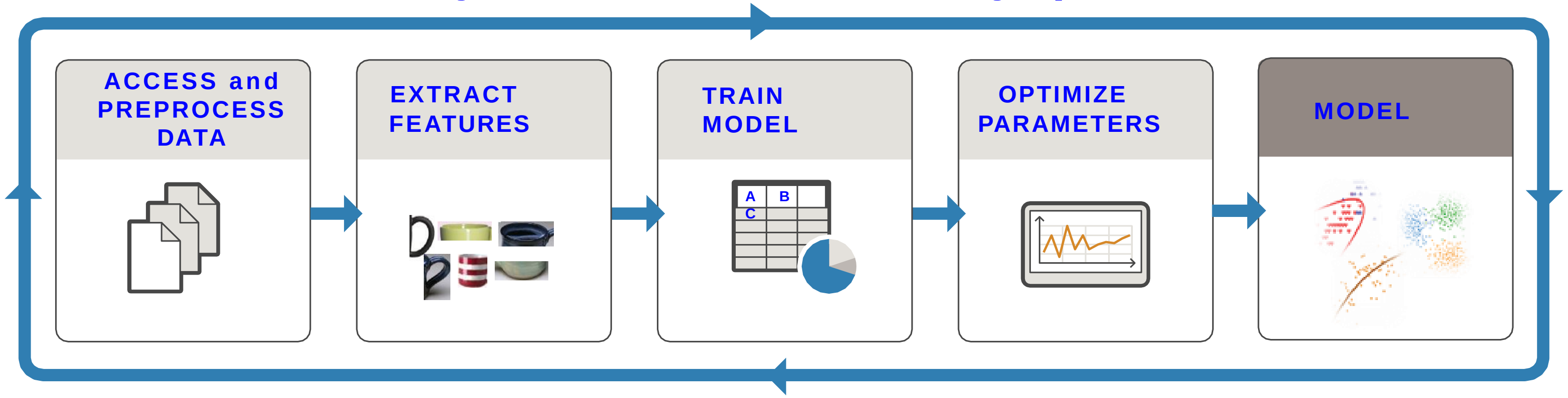
- High Energy Requirements
- High Computational Resource Requirements
- Large Amount of Data Requirements
- Underfitting/Overfitting Issue
- Class Imbalance Issue
- Fake Data Issue



Source: Mohanty ISCT Keynote 2019

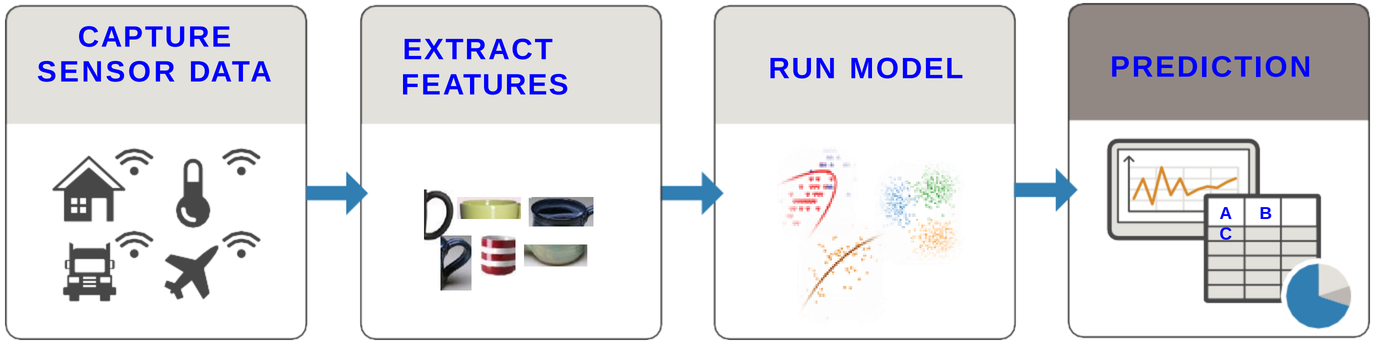
Deep Neural Network (DNN) - Resource and Energy Costs

TRAIN: Iterate until you achieve satisfactory performance.



Needs Significant:
- ➢ Computational Resource
- ➢ Computation Energy

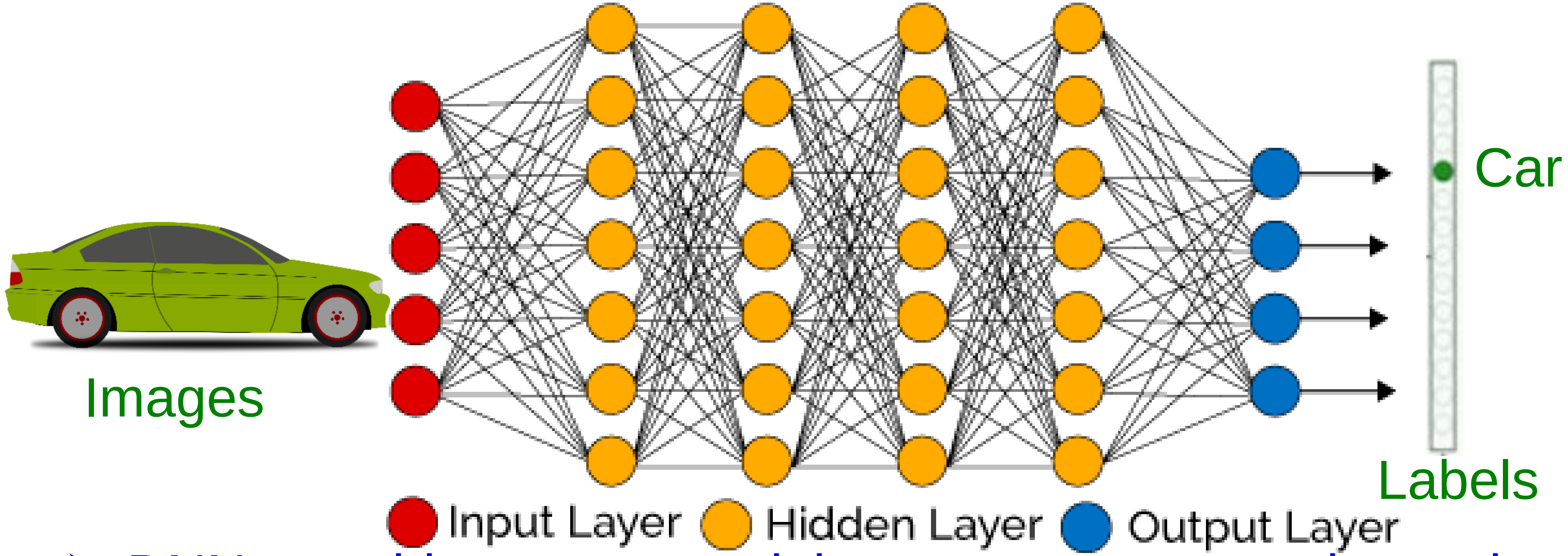
PREDICT: Integrate trained models into applications.



Needs:
- ➢ Computational Resource
- ➢ Computation Energy

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

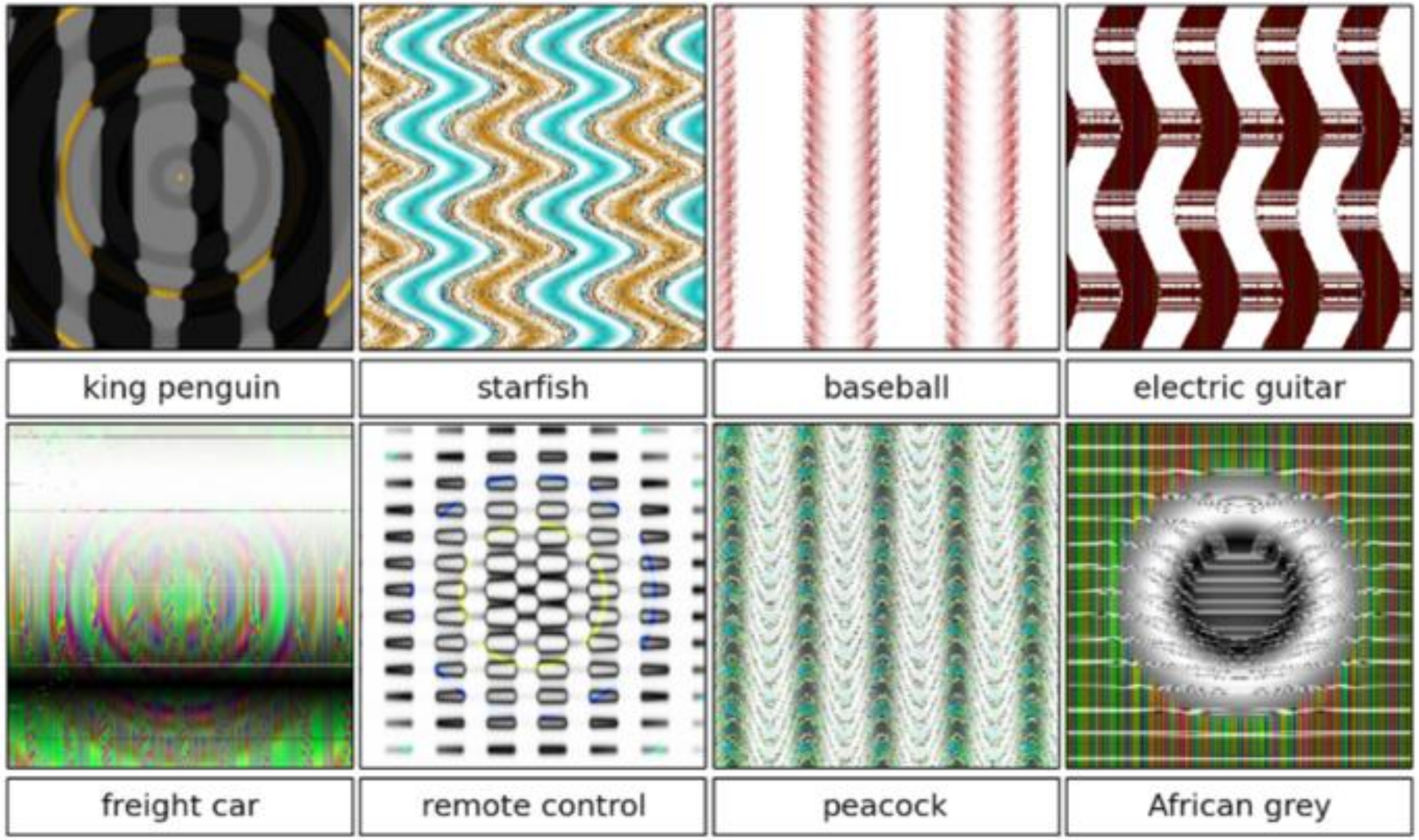
DNN Training - Energy Issue



- 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

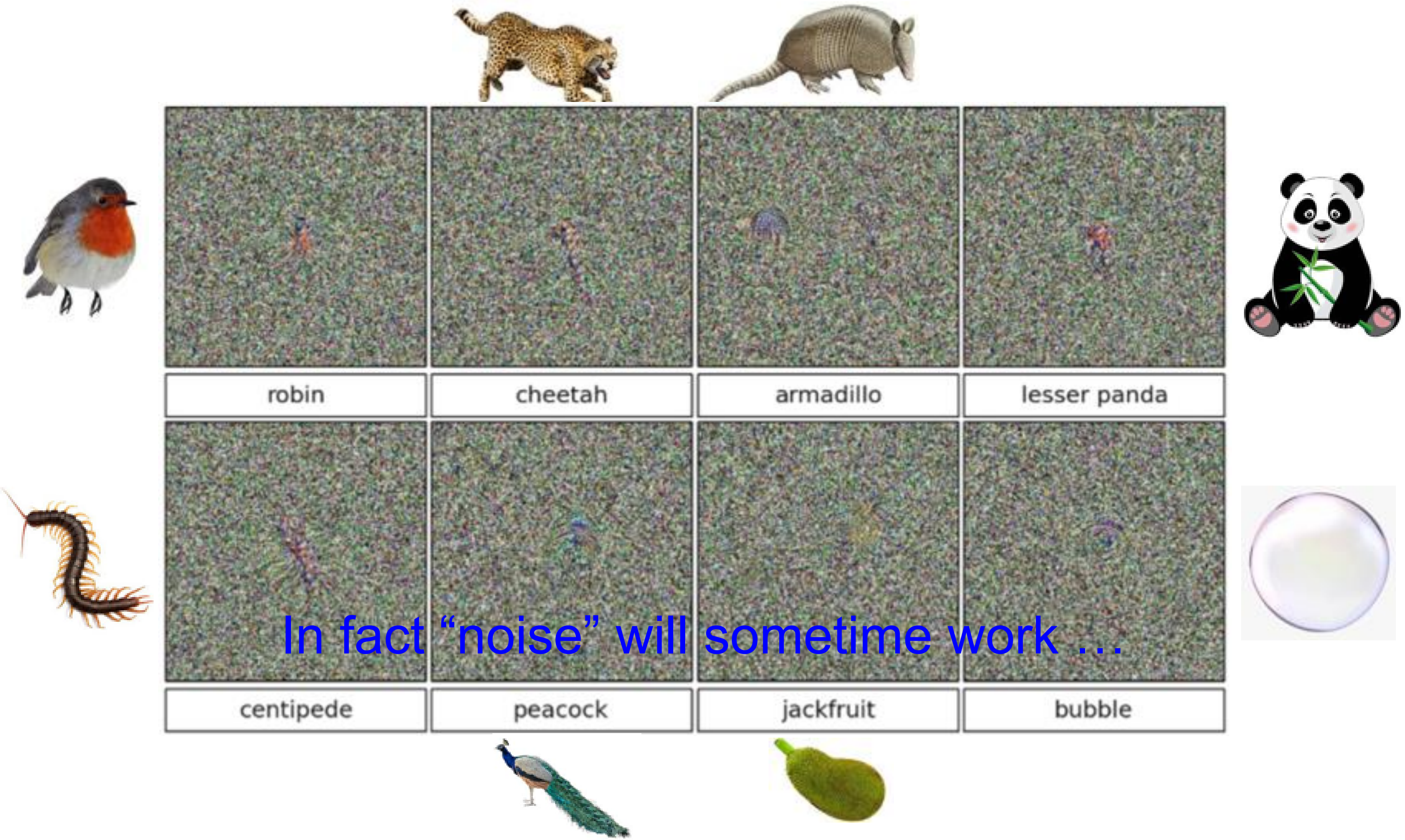
DNNs are not Always Smart



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

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

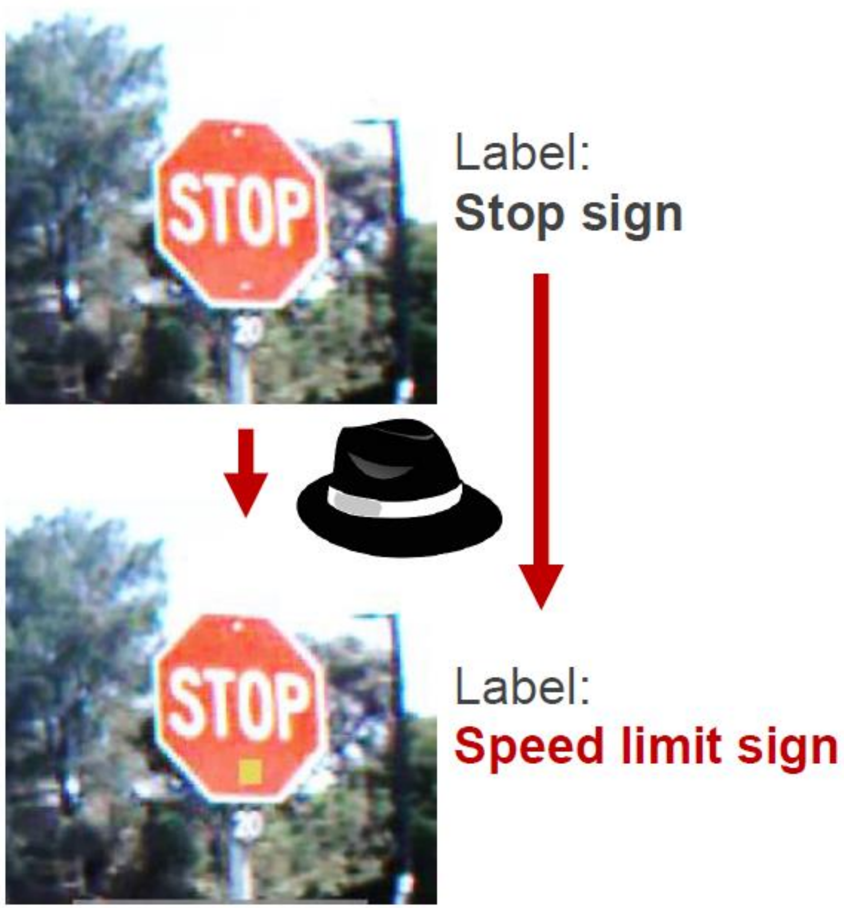
DNNs are not Always Smart



In fact “noise” will sometime work …

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

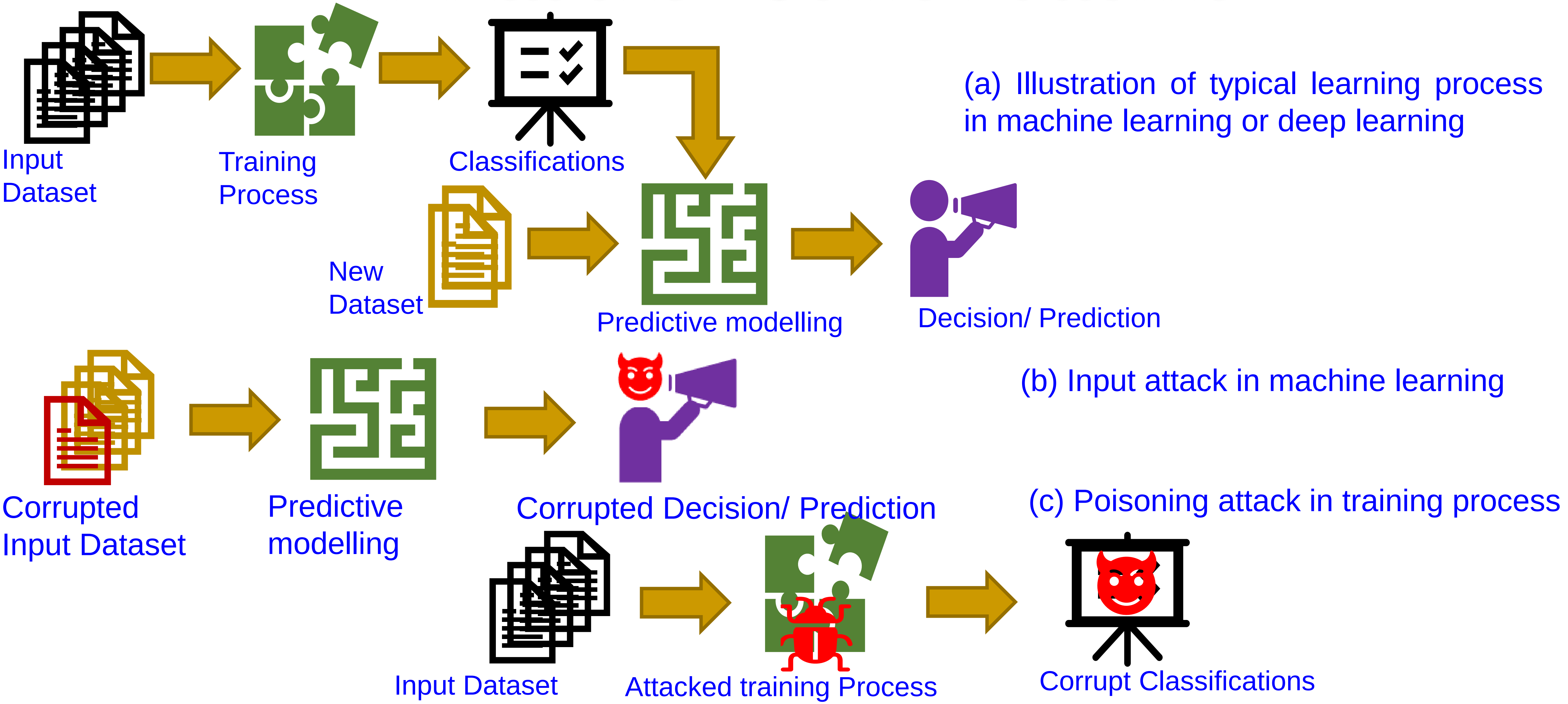
AI Security - Trojans in Artificial Intelligence (TrojAI)



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

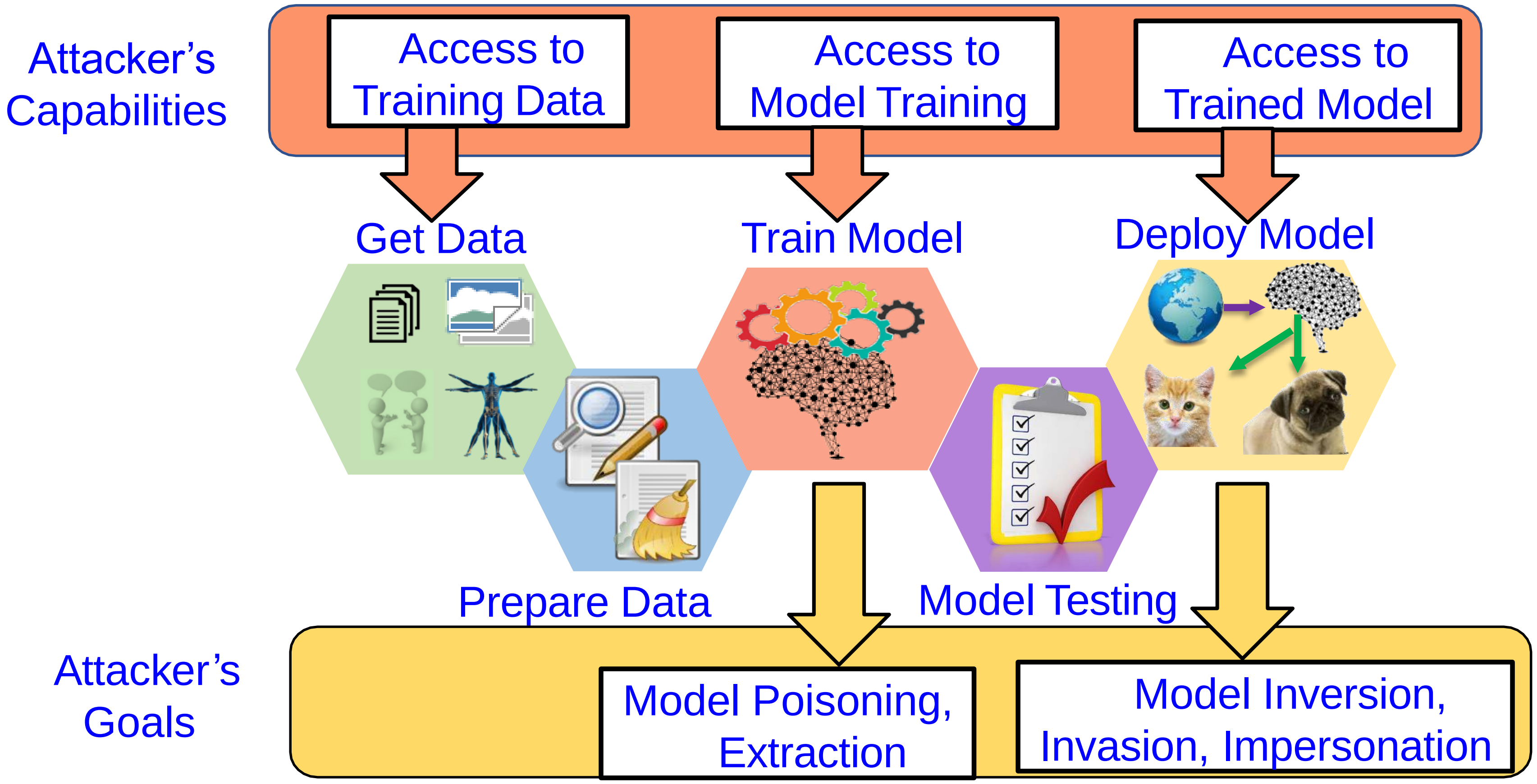
Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

AI Attacks - Some Patterns



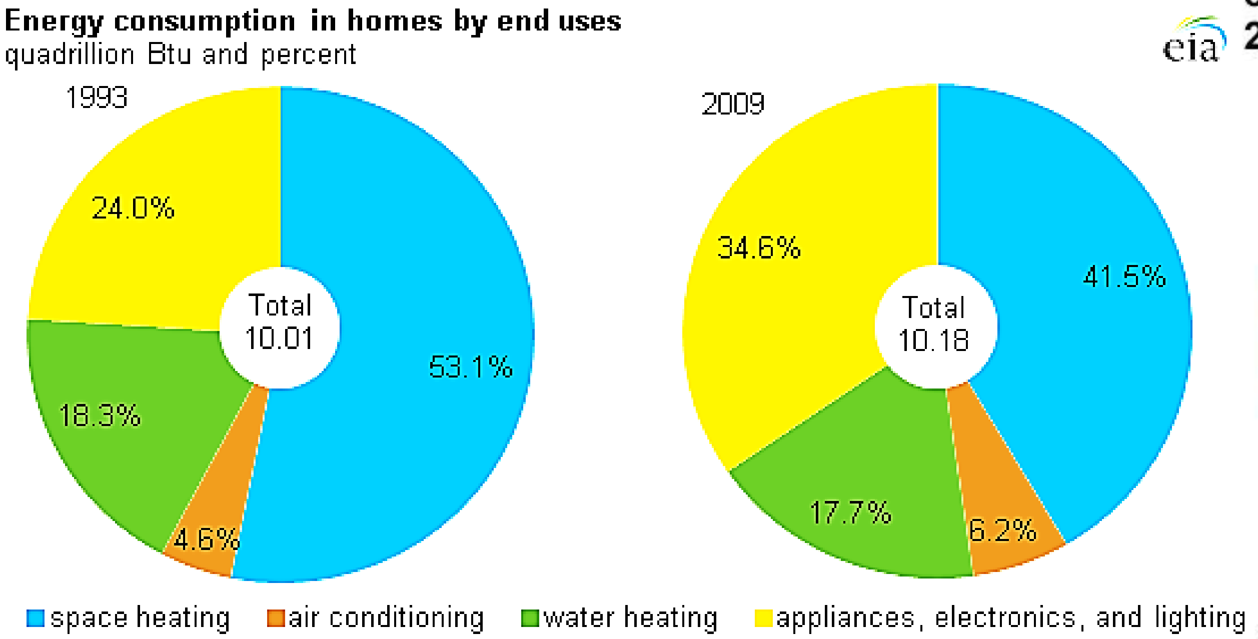
Source: D. Puthal, and S. P. Mohanty, "Cybersecurity Issues in AI", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 33--35.

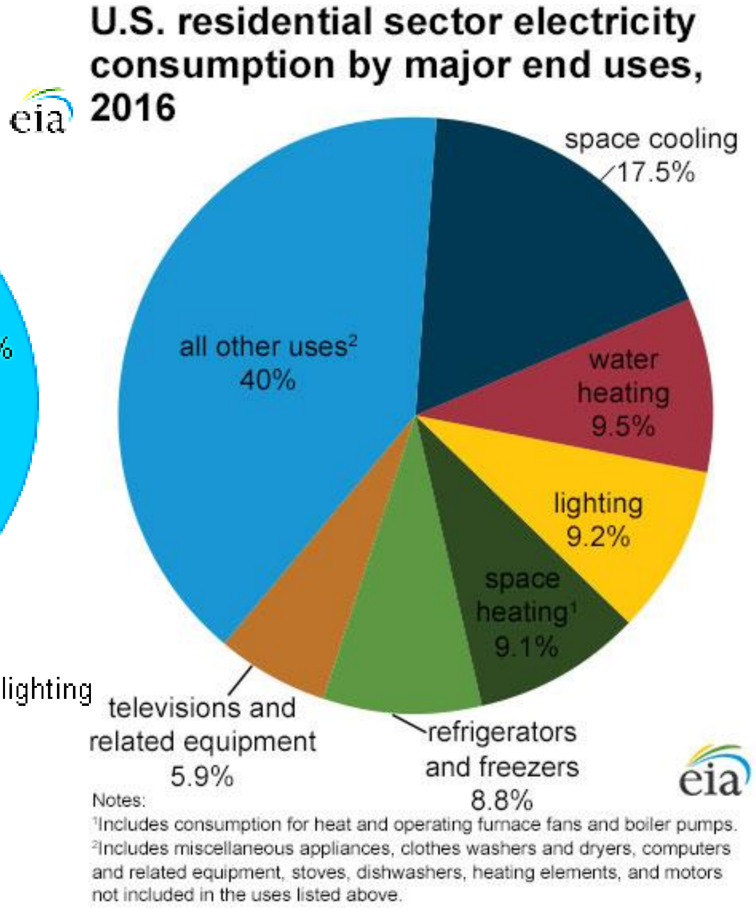
AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

Consumer Electronics Demand More and More Energy

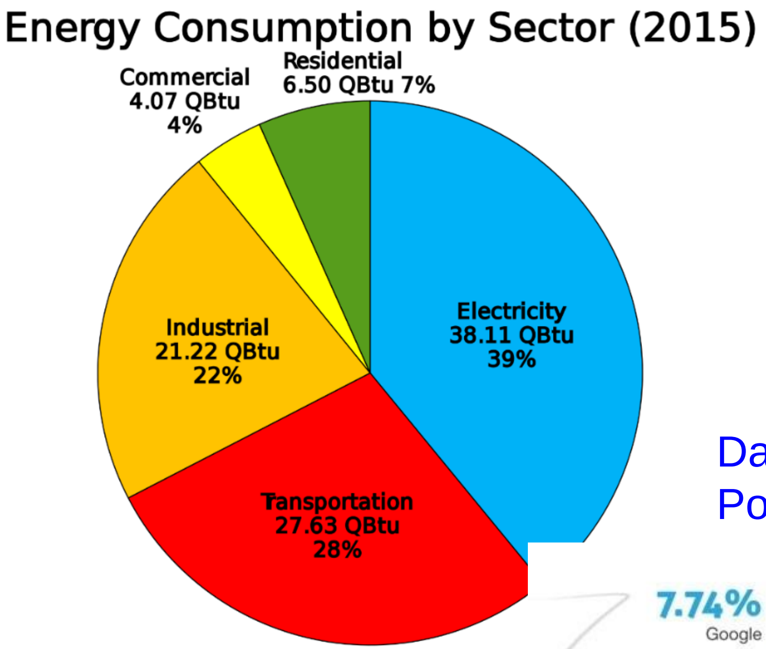


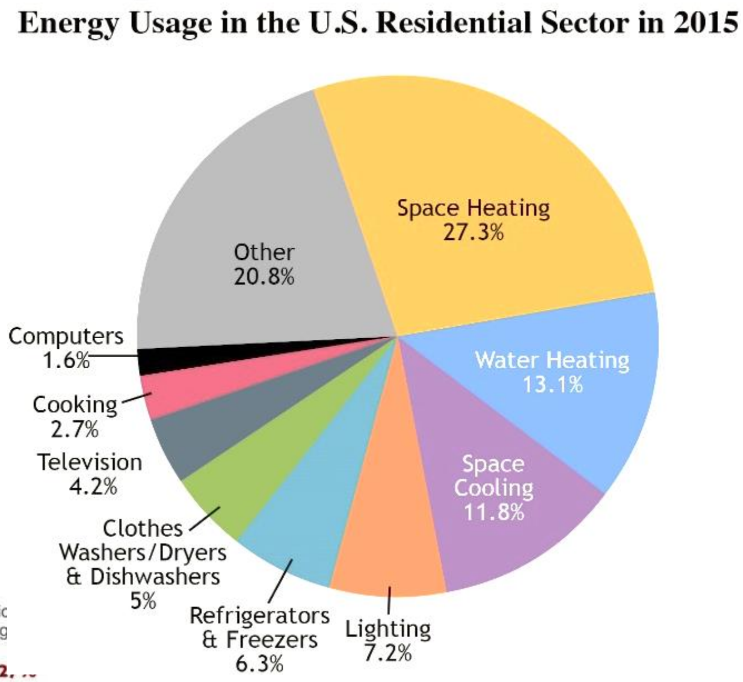


Quadrillion BTU (or quad): 1 quad = 10^{15} BTU = 1.055 Exa Joule (EJ).

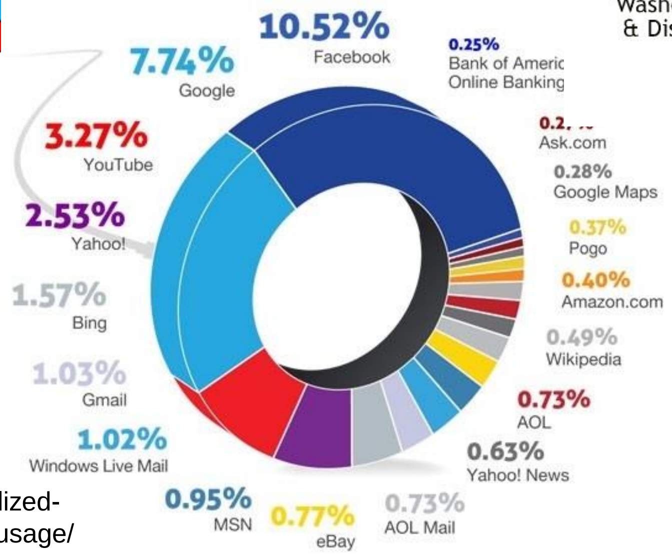
Source: U.S. Energy Information Administration.

Energy Consumption





Data Center Power Usage



ENERGY STAR

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

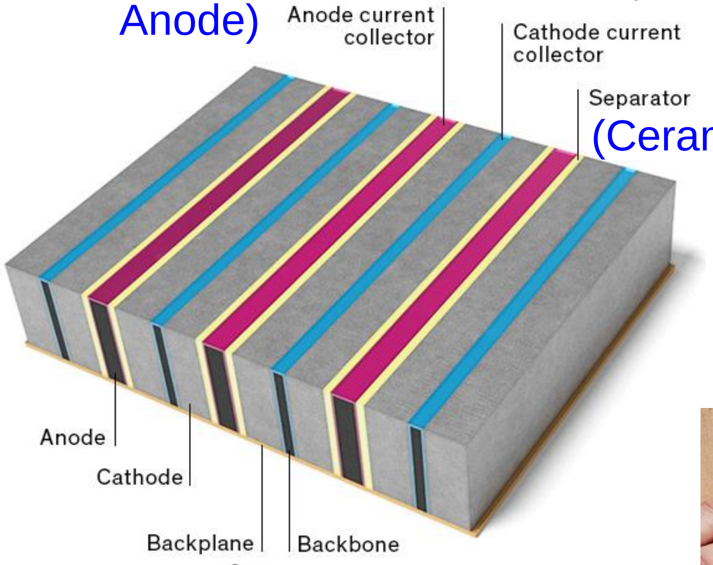
Source: https://www.engadget.com/2011/04/26/visualized-ring-around-the-world-of-data-center-power-usage/

Energy Storage - High Capacity and Safer Needed

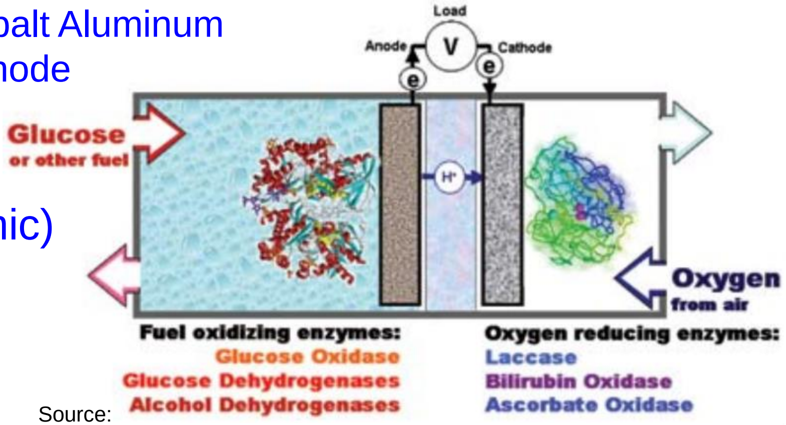
(Silicon Anode)

(Lithium Nickel Cobalt Aluminum Oxide - NCA) Cathode

(Ceramic)

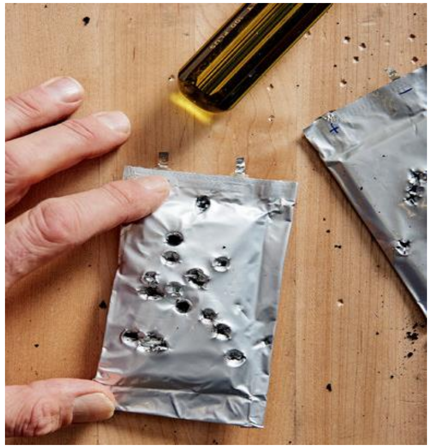


Source: http://spectrum.ieee.org/semiconductors/design/how-to-build-a-safer-more-energydense-lithiumion-battery



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

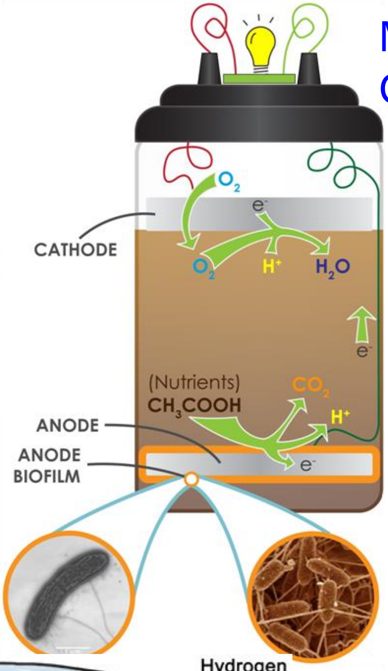
Enzymatic Biofuel Cell



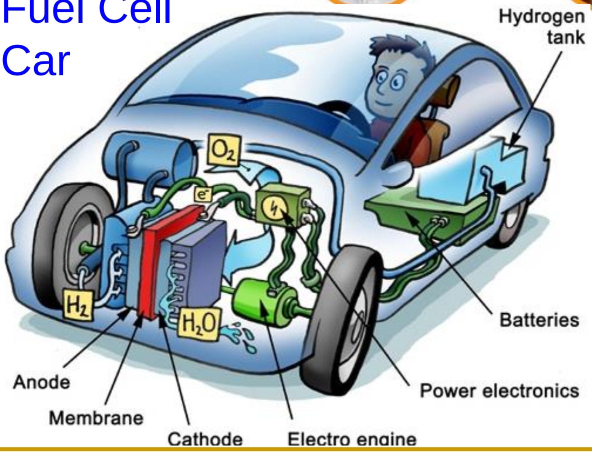
Solid Polymer Lithium Metal Battery

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

Microbial Fuel Cell (MFC)



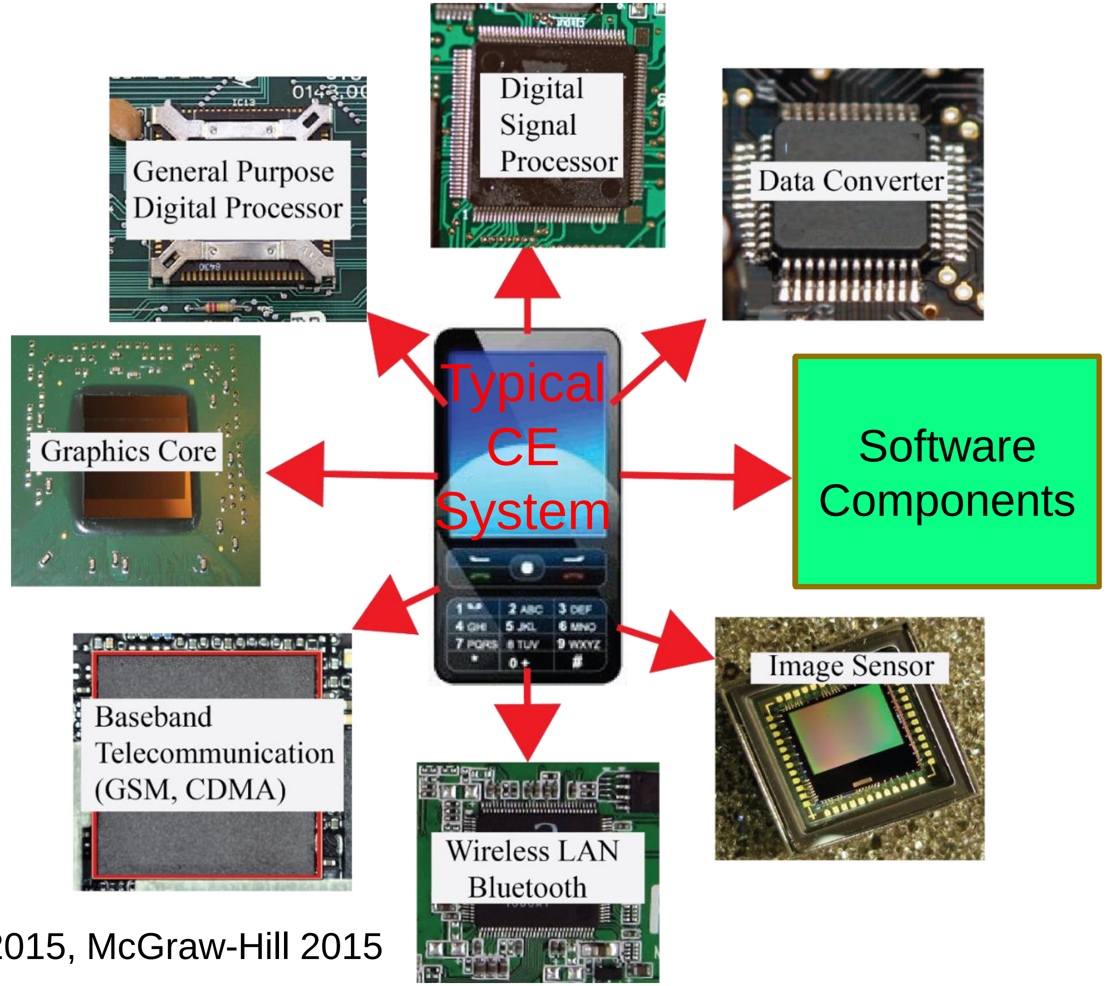
Fuel Cell Car

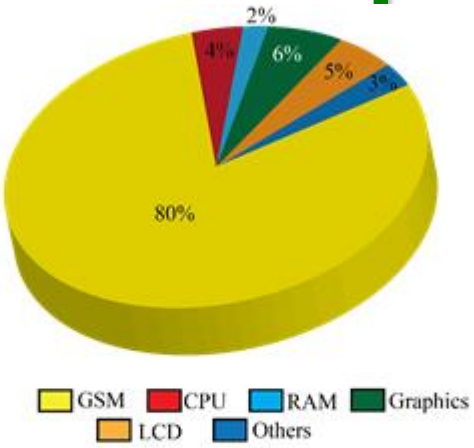


Smart Electronic Systems Laboratory (SESL)

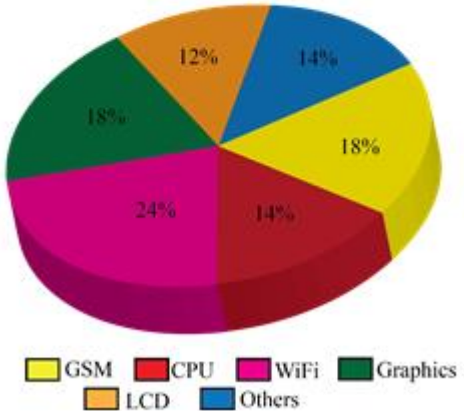
UNT EST. 1890 DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering

Energy Optimization of CE System is difficult due to a Variety of Components





During GSM Communications

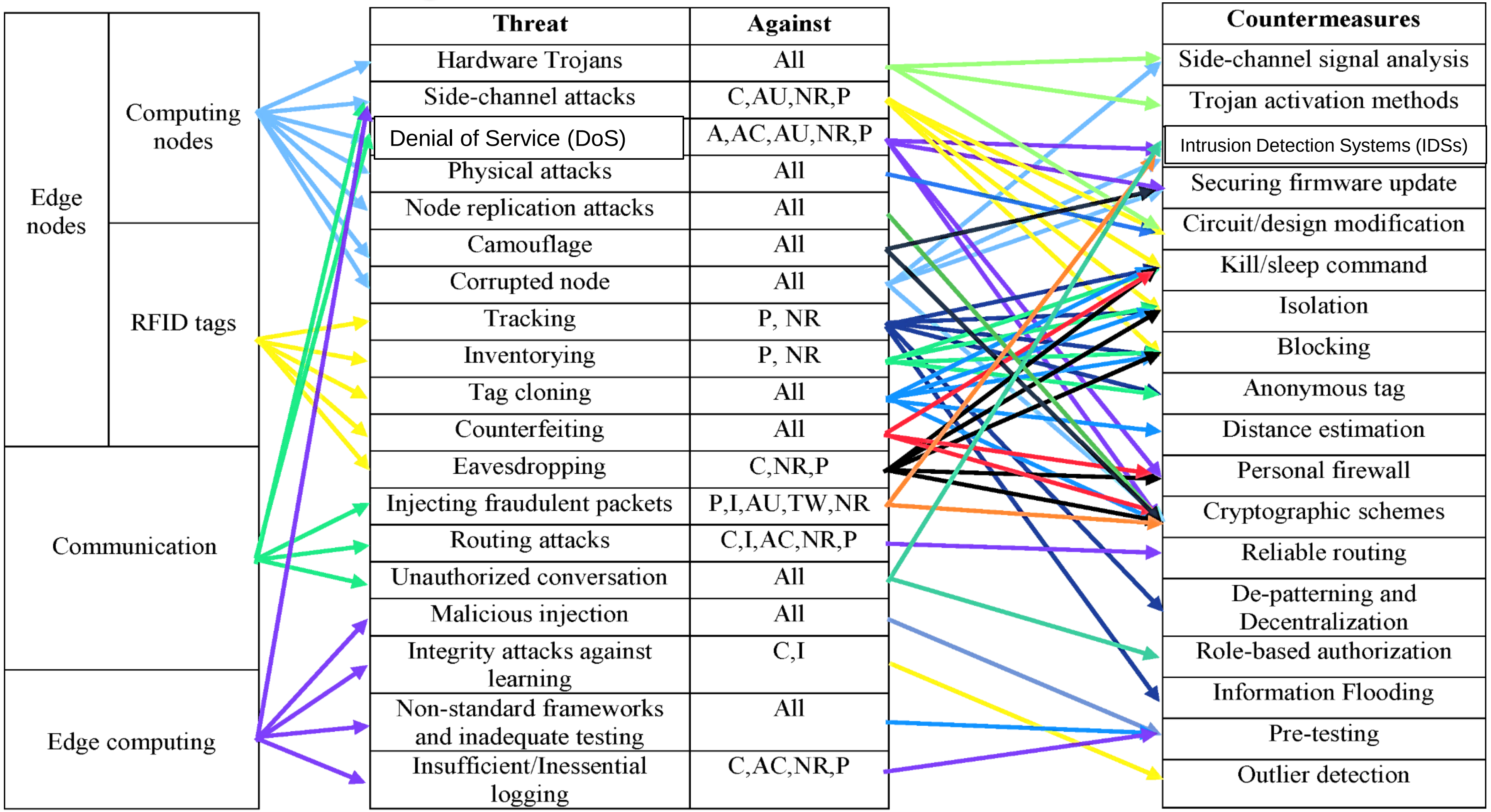


During WiFi Communications

Source: Mohanty 2015, McGraw-Hill 2015

Cybrsecurity Solution for IoT/CPS

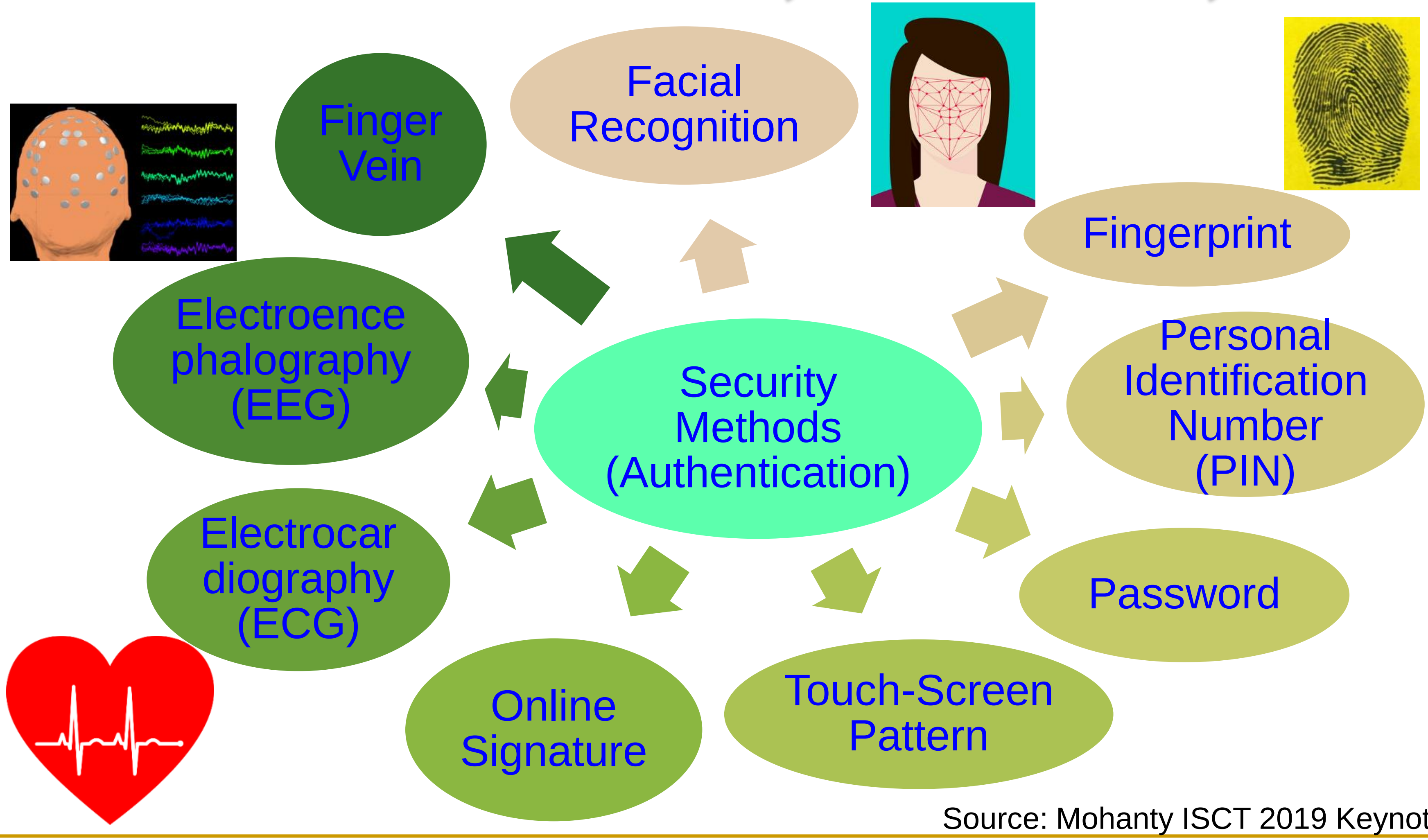
IoT Security - Attacks and Countermeasures



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

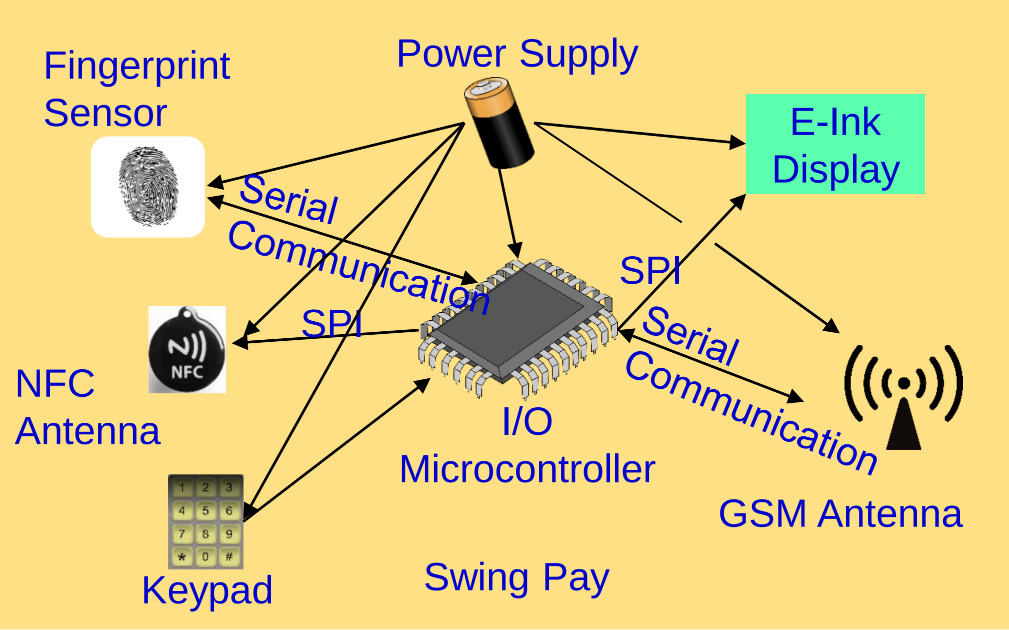
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

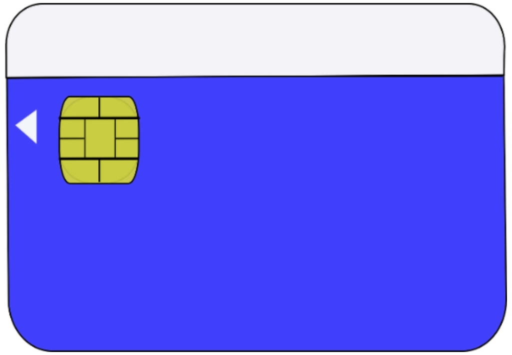
Security, Authentication, Access Control – Home, Facilities, ...

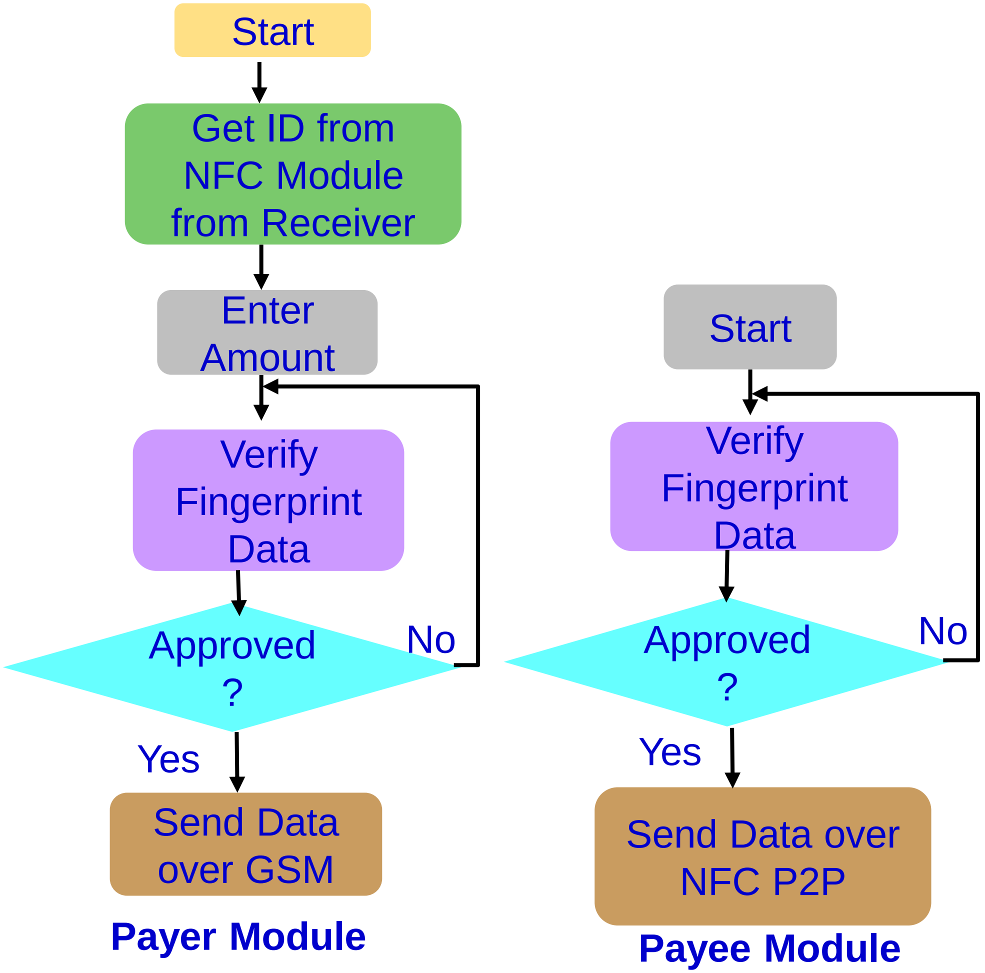


Source: Mohanty ISCT 2019 Keynote

Our Swing-Pay: NFC Cybersecurity Solution







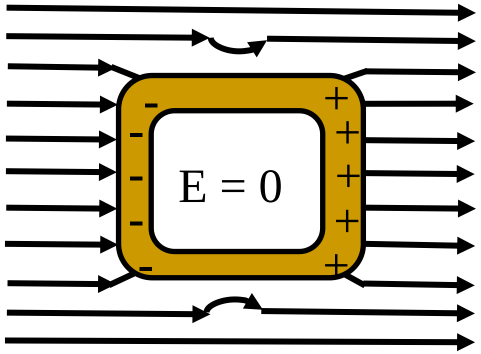
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

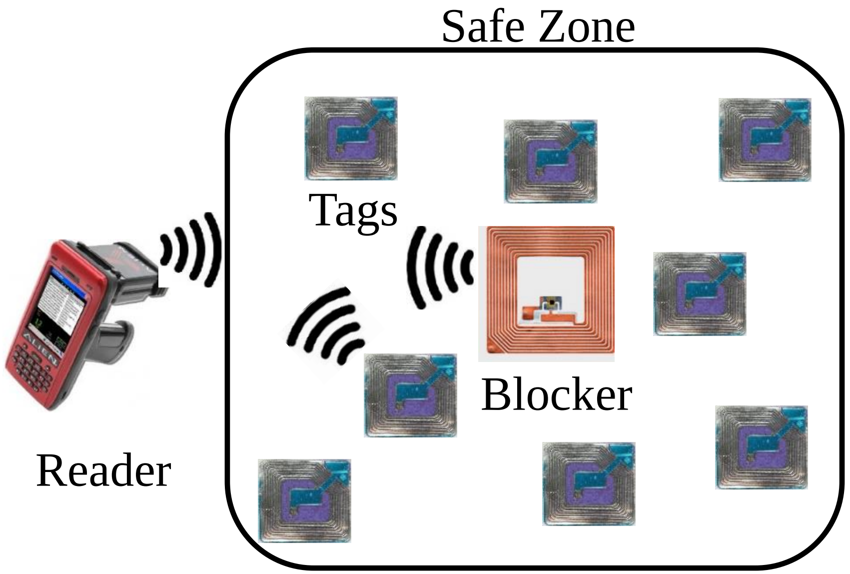
RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

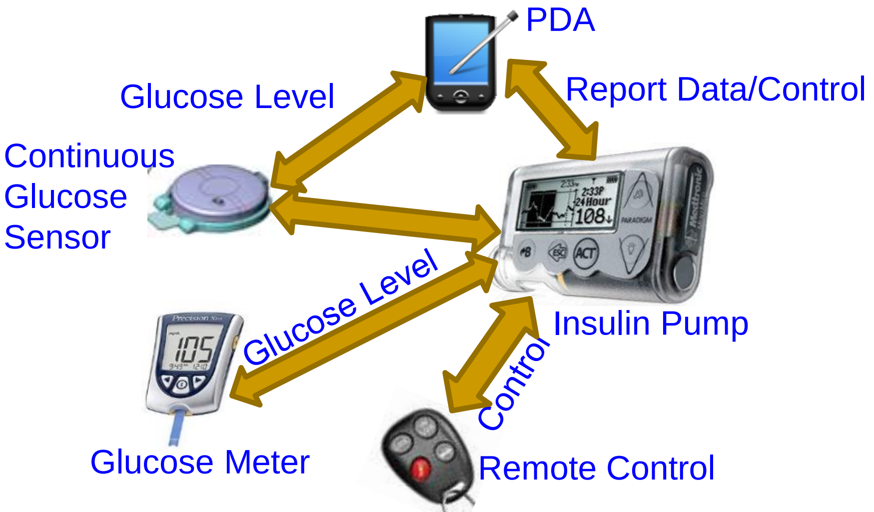




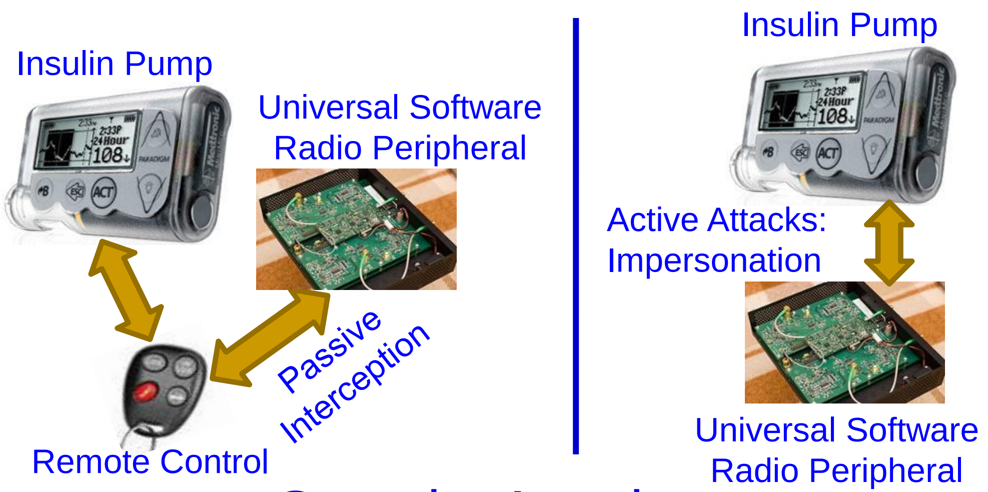
Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

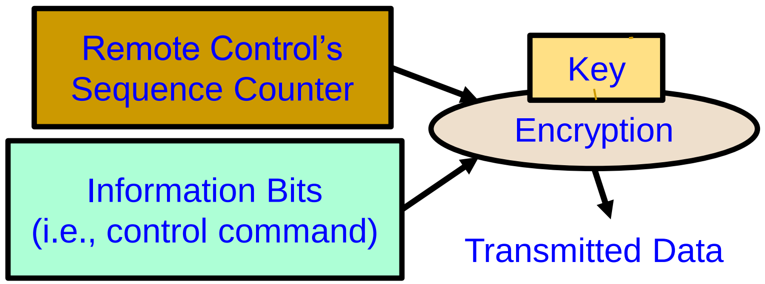
Smart Healthcare Security



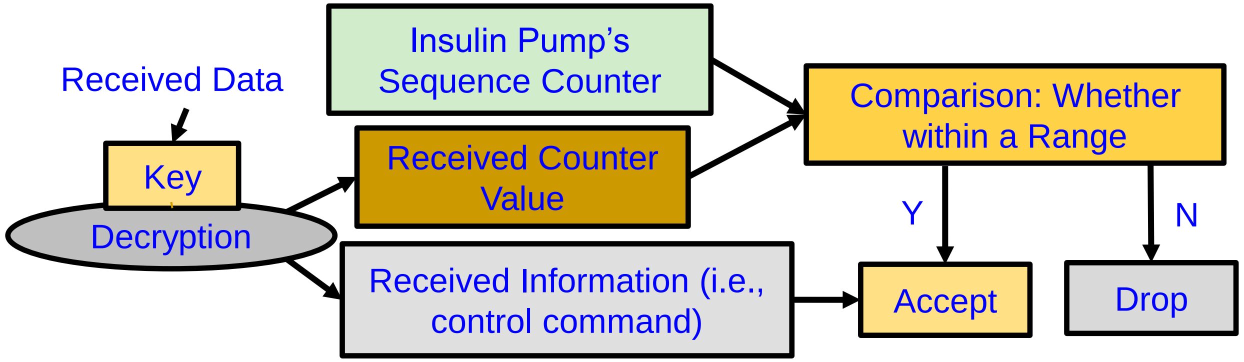
Insulin Delivery System



Security Attacks



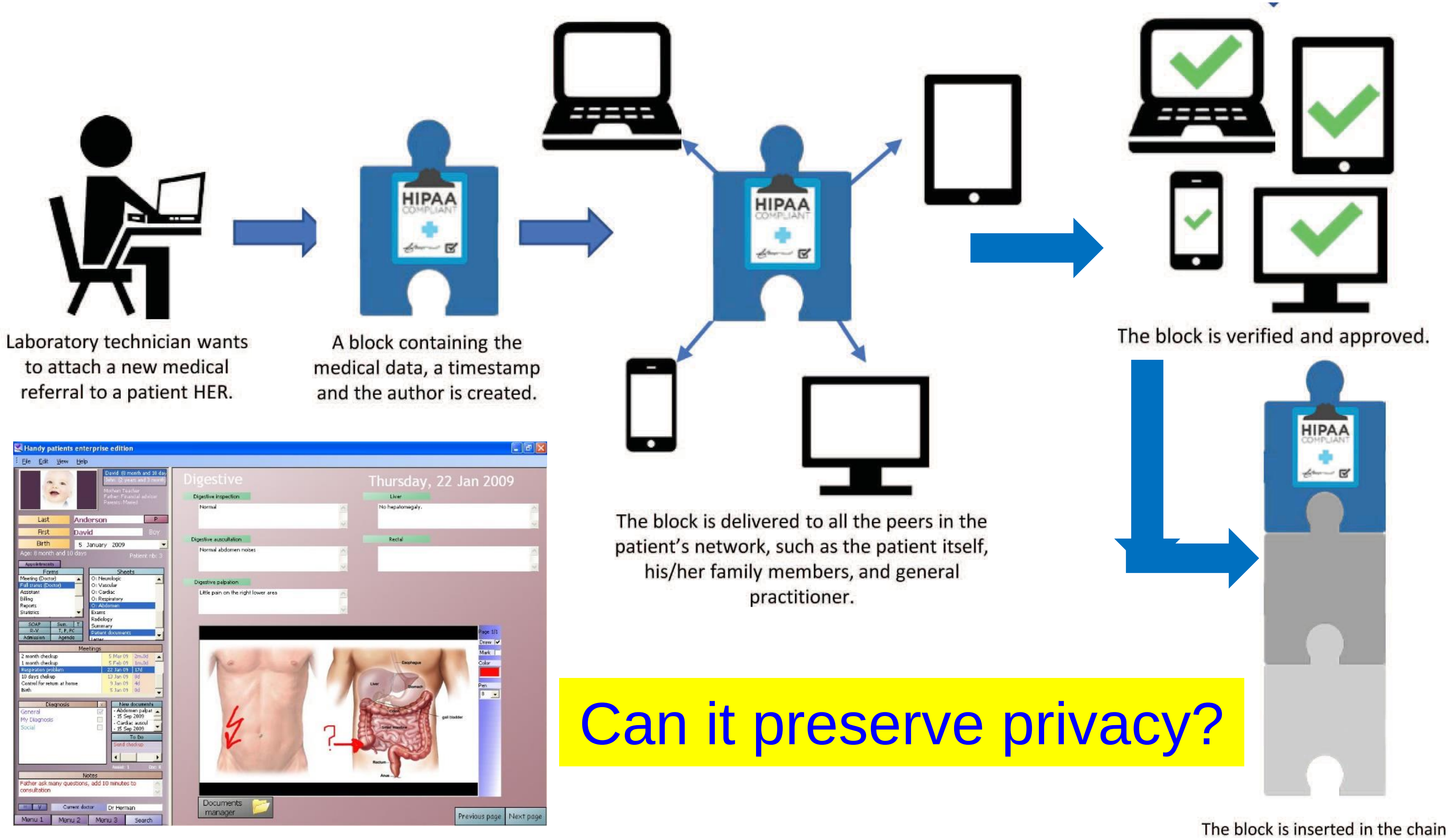
Rolling Code Encoder in Remote Control



Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Blockchain in Smart Healthcare

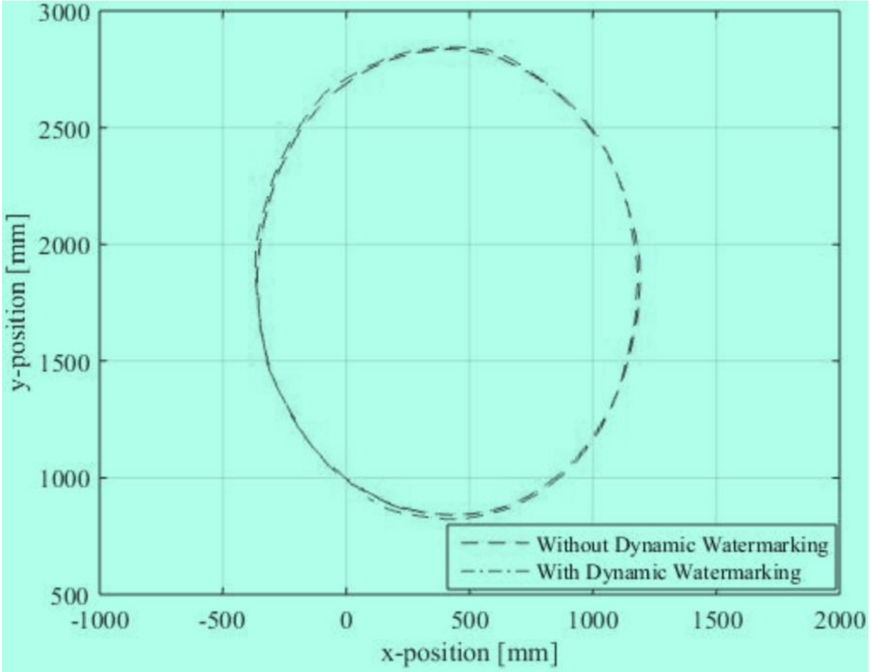


Can it preserve privacy?

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.

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

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

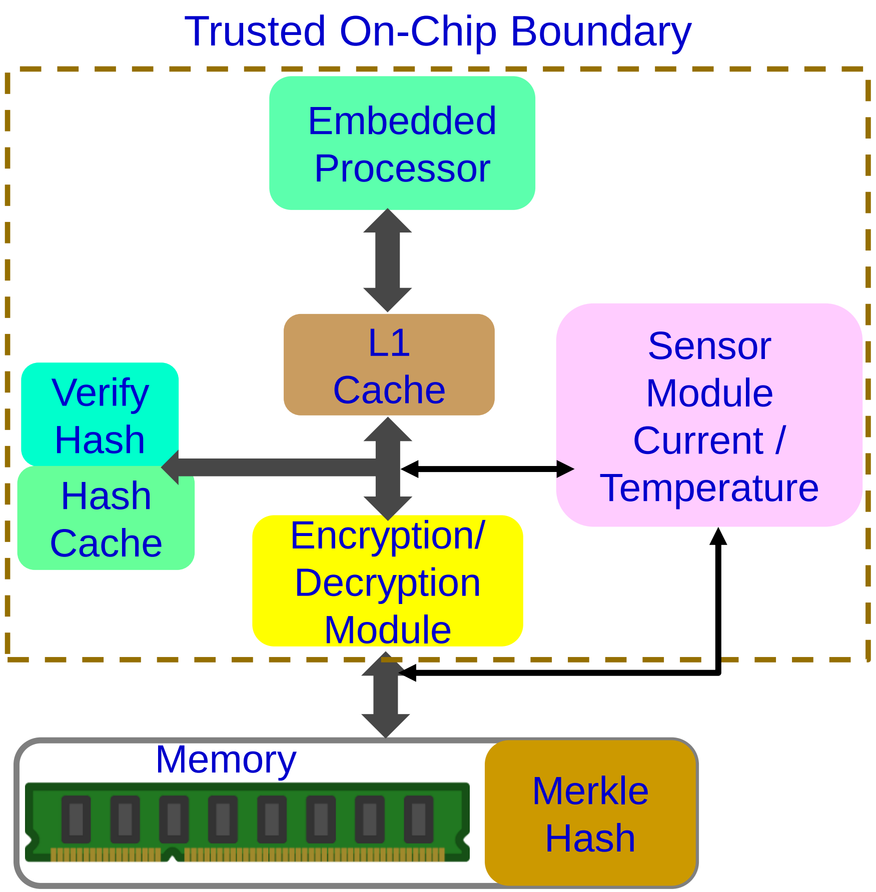
Nonvolatile / Harddrive Storage

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

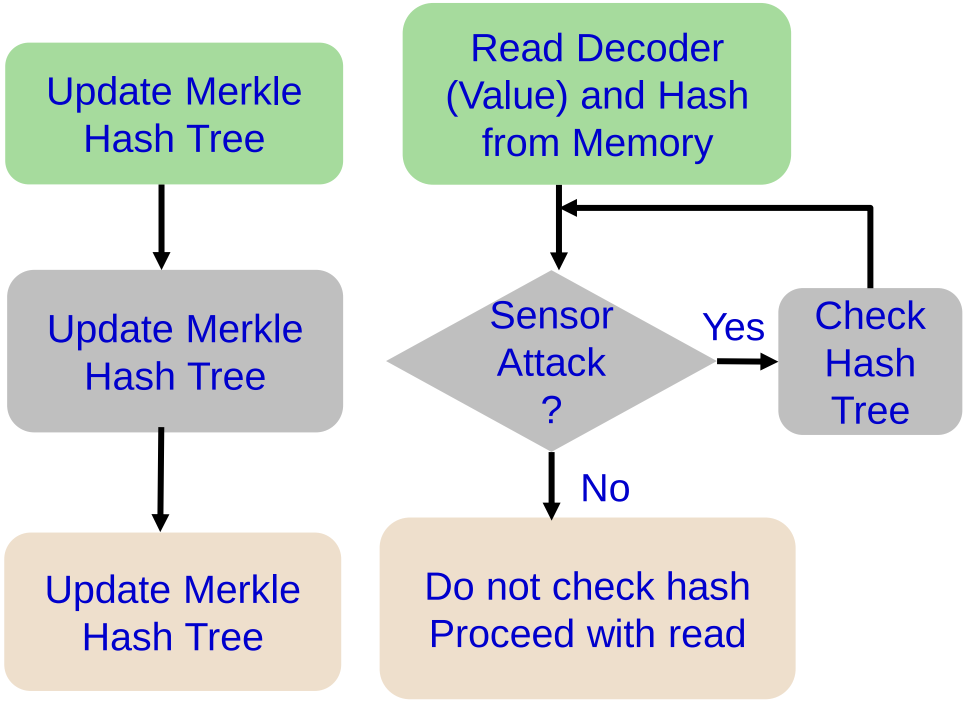
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

Embedded Memory Security



On-Chip/On-Board Memory Protection



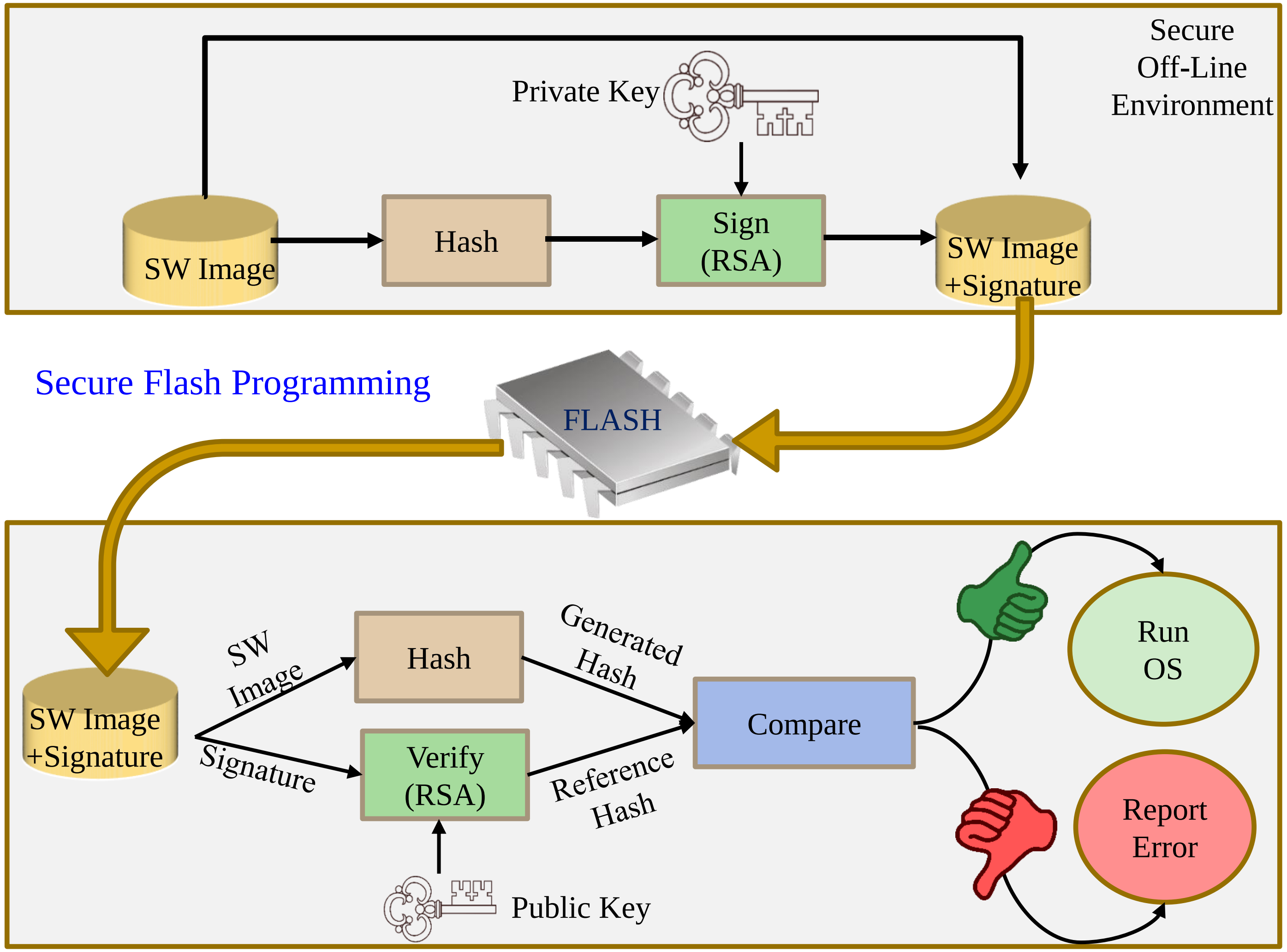
Write Operation

Read Operation

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

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

Firmware Security - Solution



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

Energy Solutions for IoT/CPS

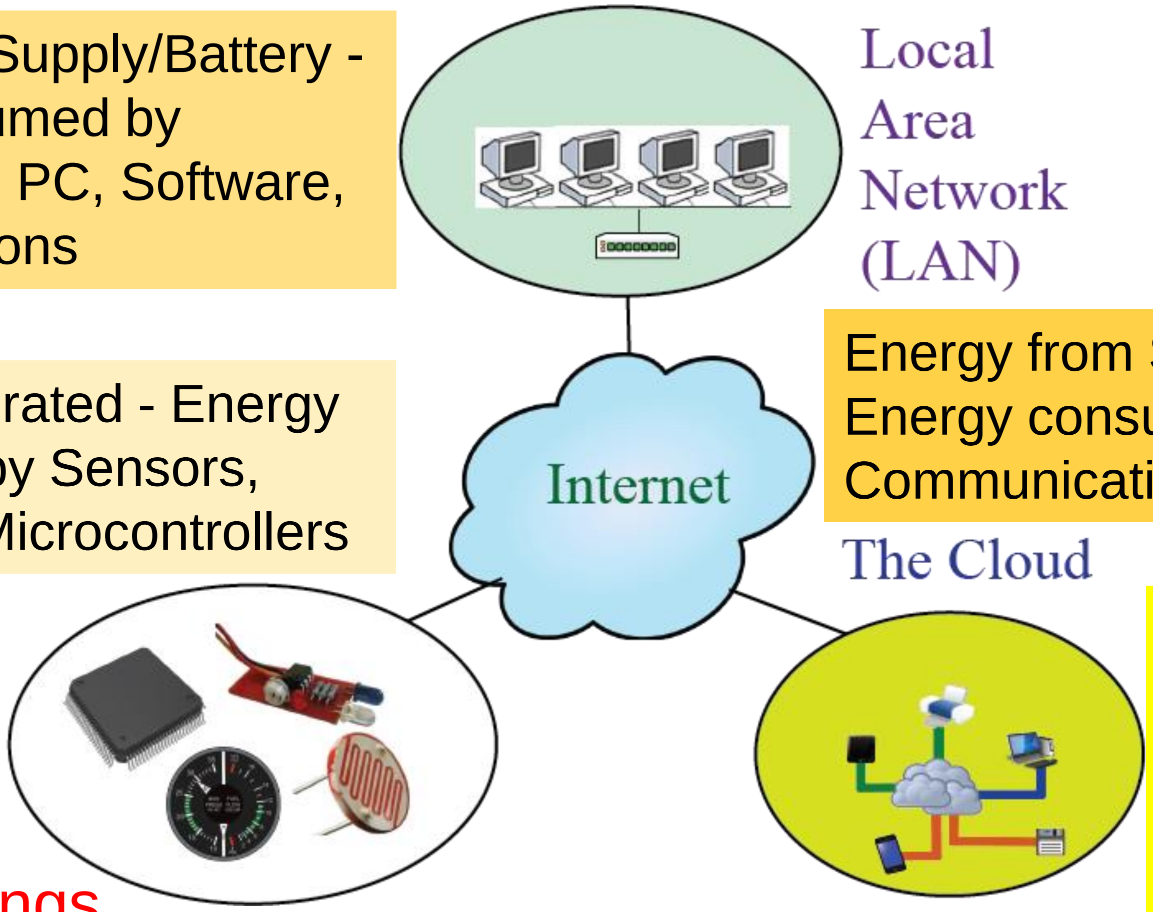
Energy Consumption Challenge in IoT

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

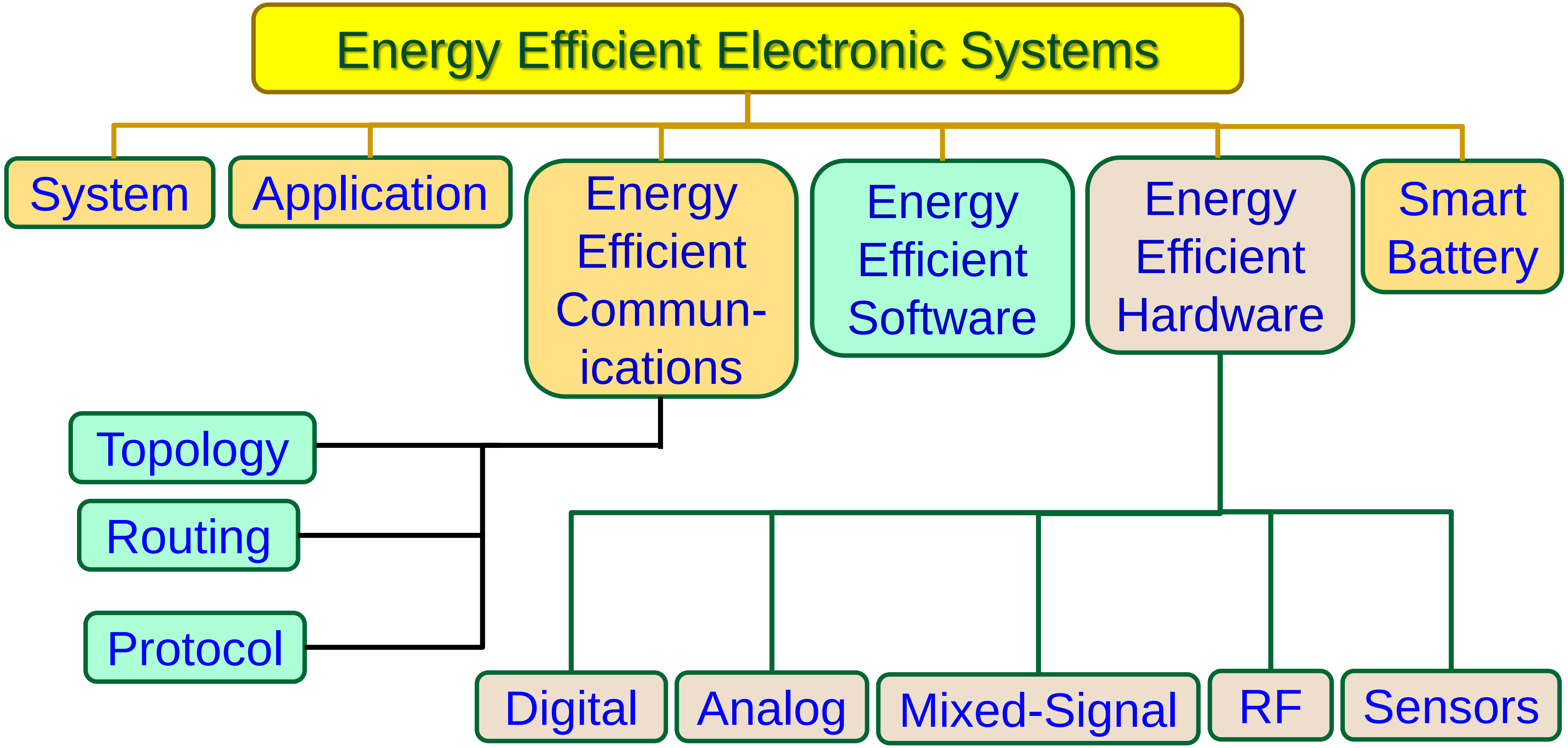
Energy from Supply - Energy consumed in Server, Storage, Software, Communications



Four Main Components of IoT.

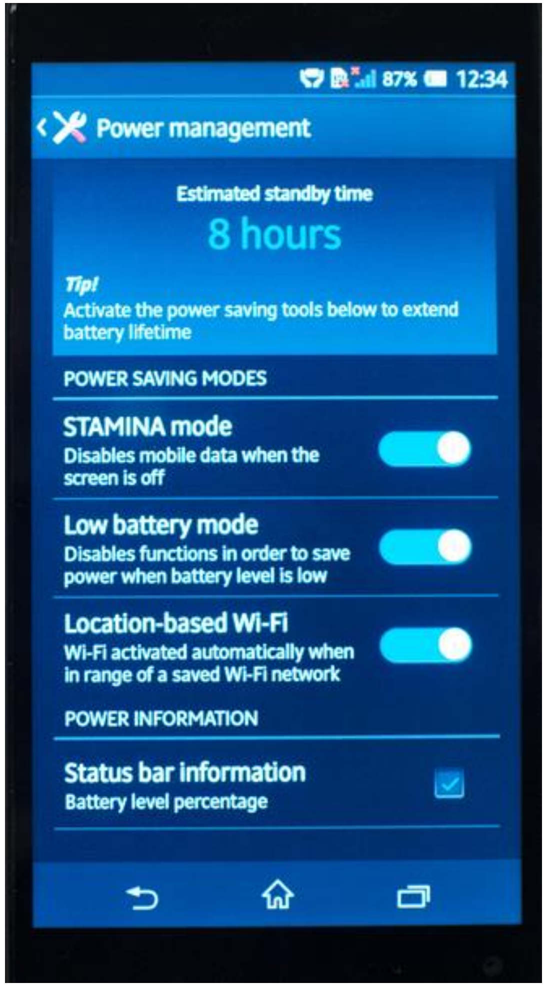
Source: Mohanty iSES 2018 Keynote

Energy Efficient Electronics: Possible Solution Fronts



Source: Mohanty ZINC 2018 Keynote

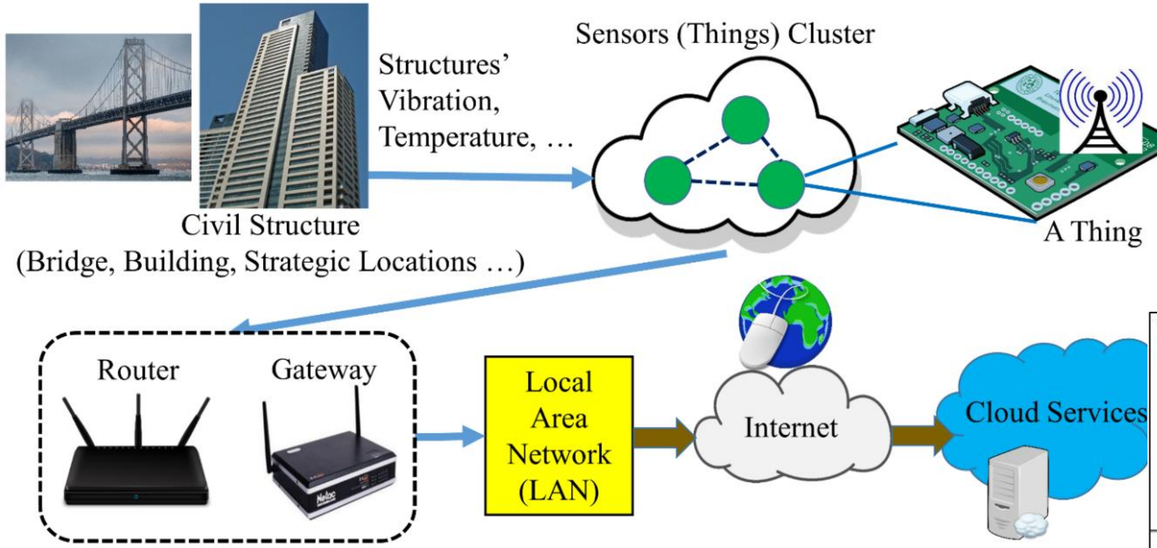
Smart Energy – Smart Consumption

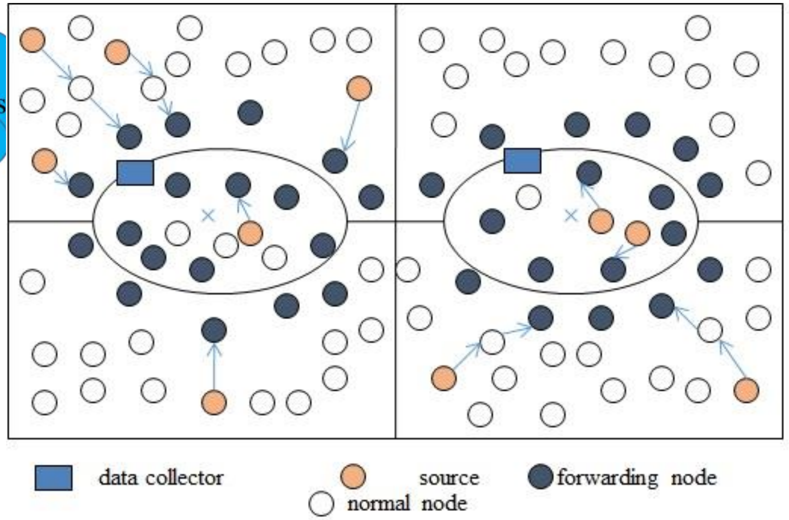


Battery Saver

Smart Home

Sustainable IoT - Low-Power Sensors and Efficient Routing

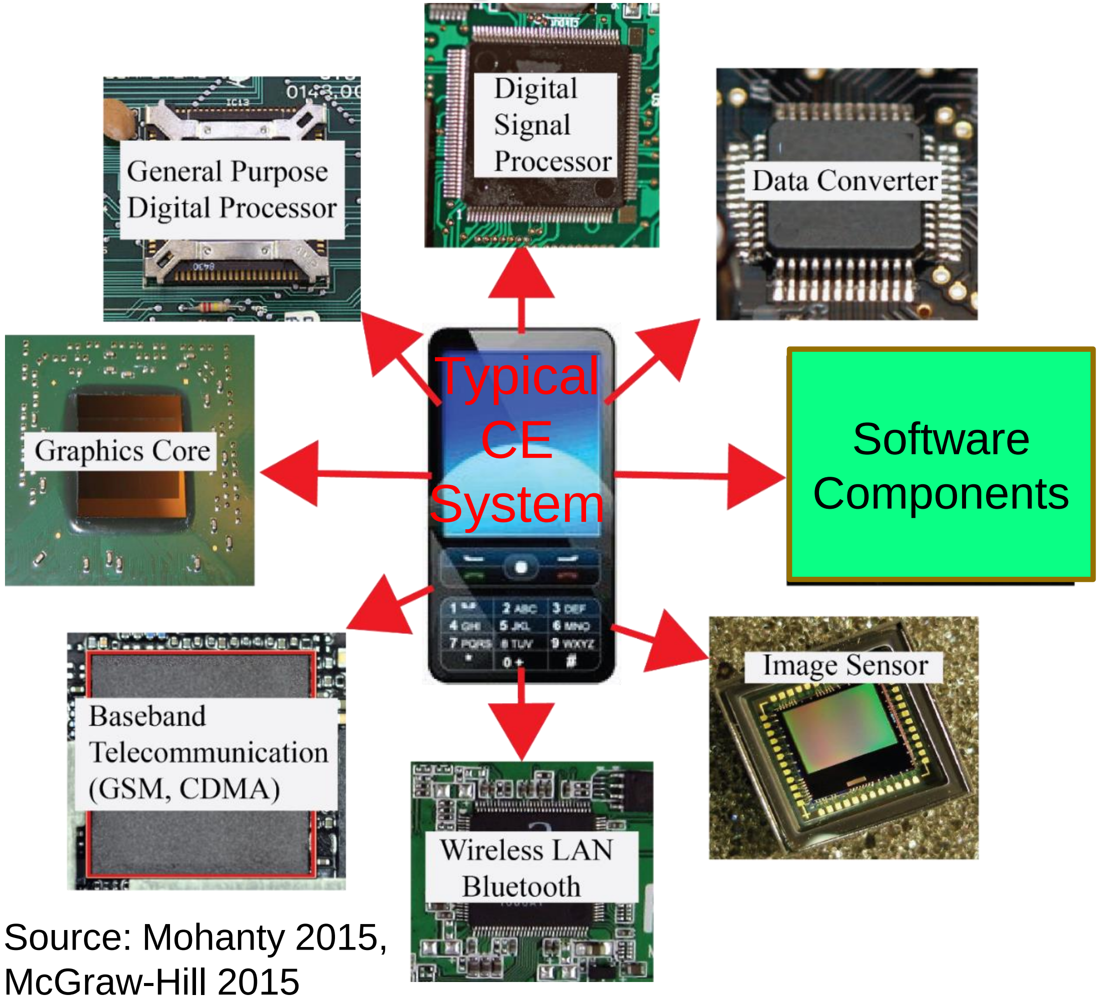




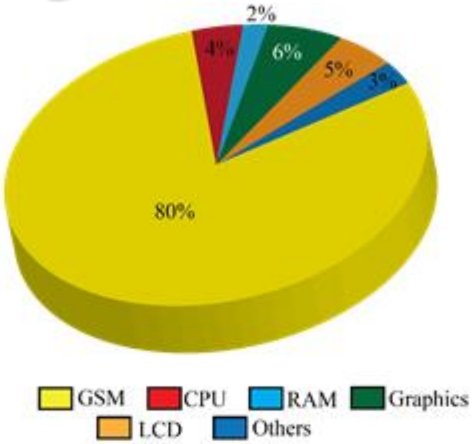
- IoT - sensors near the data collector drain energy faster than other nodes.
- Solution Idea - Mobile sink in which the network is balanced with node energy consumption.
- Solution Need: New data routing to forward data towards base station using mobile data collector, in which two data collectors follow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

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

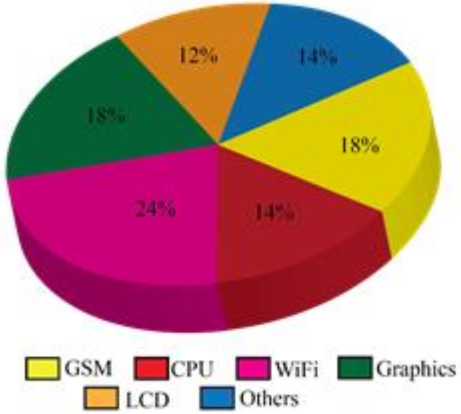
Energy Consumption of Sensors, Components, and Systems



Source: Mohanty 2015, McGraw-Hill 2015

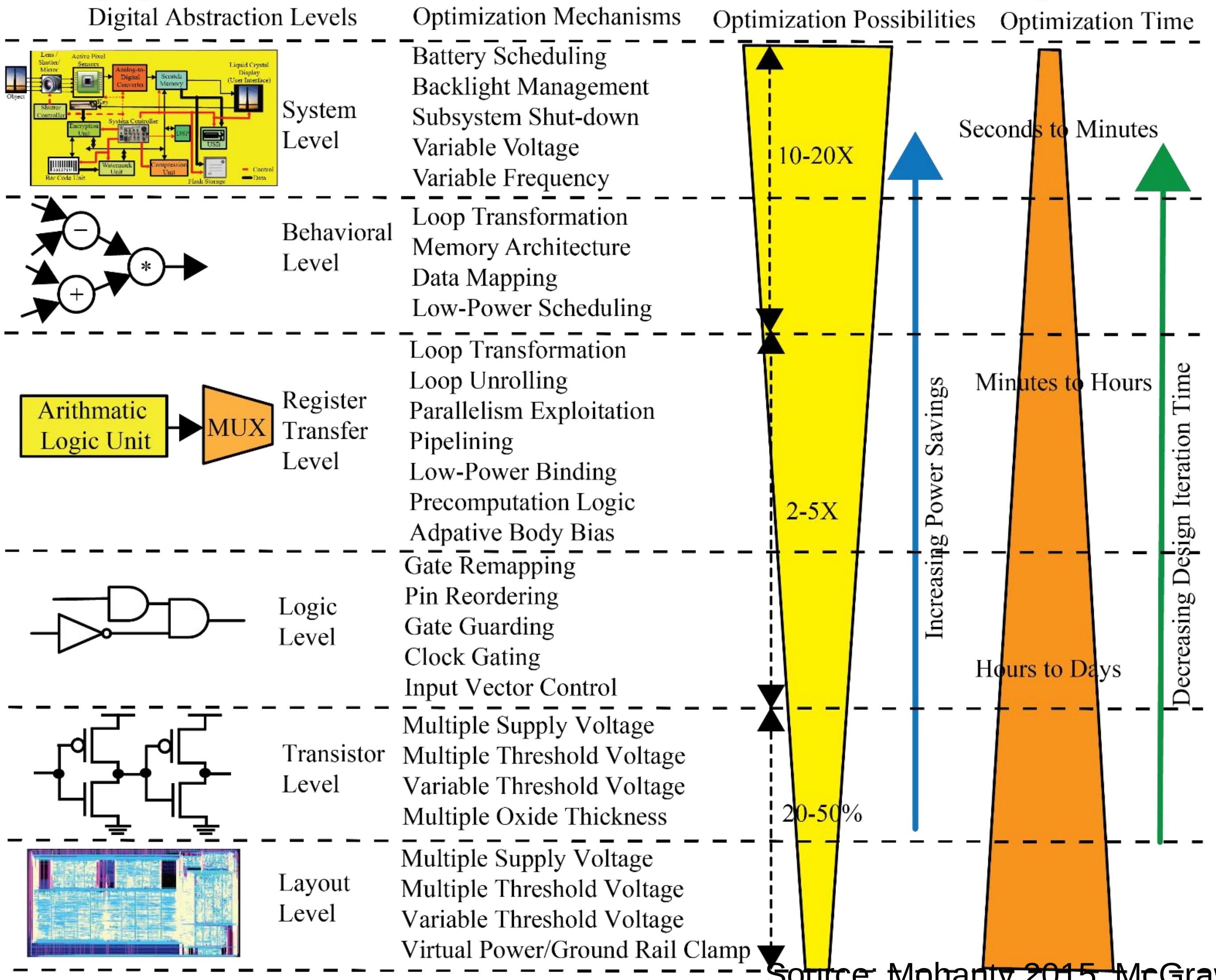


During GSM Communications



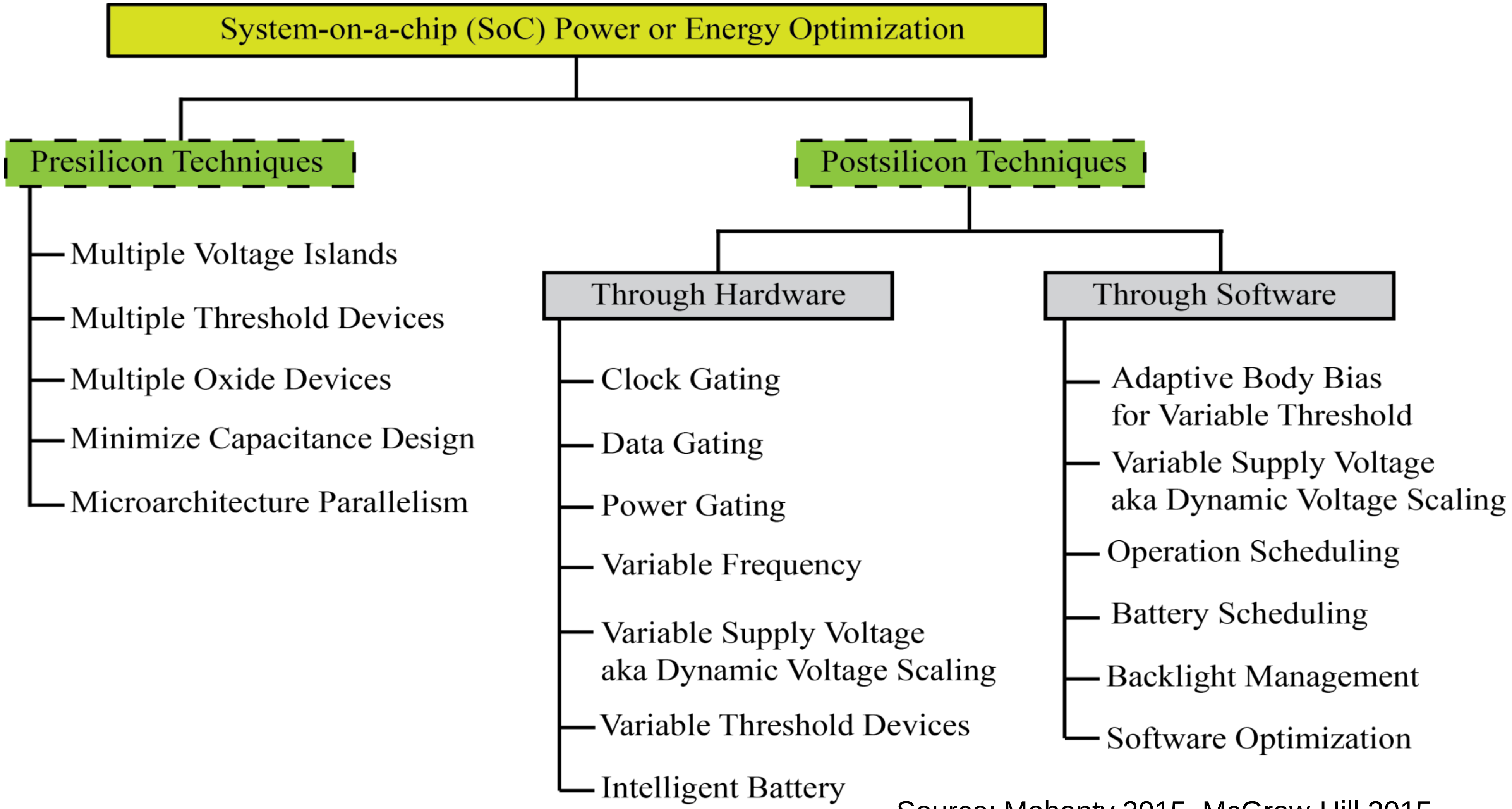
During WiFi Communications

Energy Reduction in CE Systems



Source: Mohanty 2015, McGraw-Hill 2015

Energy Reduction in CE Hardware



Source: Mohanty 2015, McGraw-Hill 2015

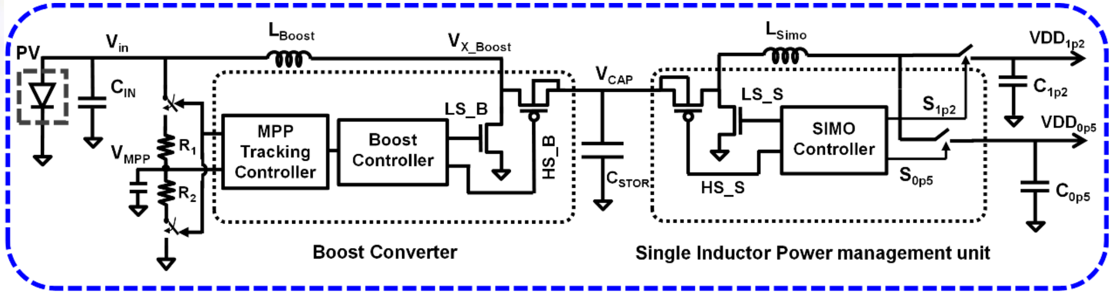
Battery-Less IoT

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

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

Batter-Less SoC

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



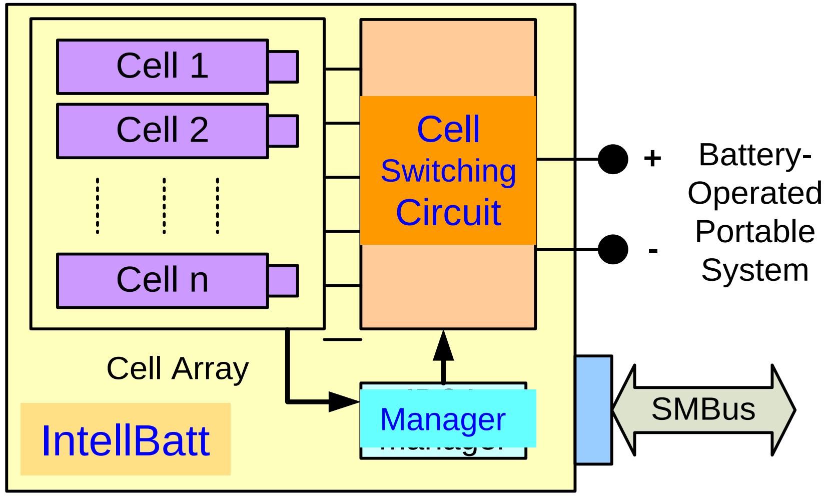
Energy Harvesting and Power Management

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

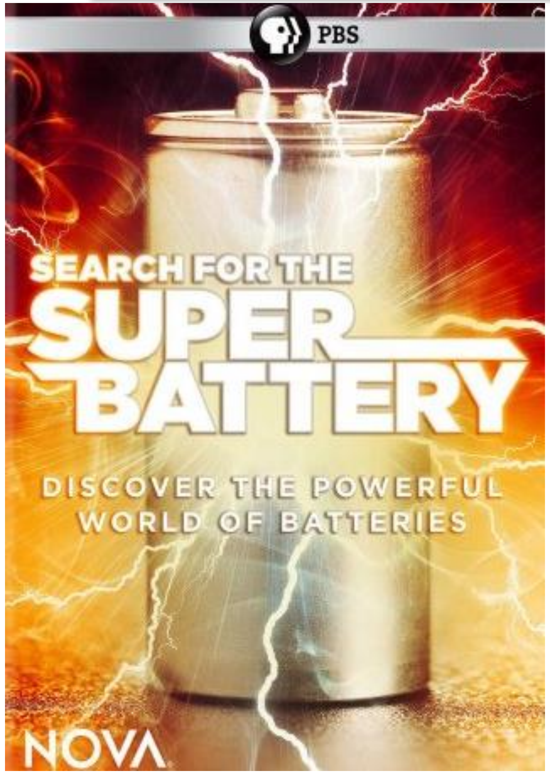
Energy Storage - High Capacity and Efficiency Needed

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

Intelligent Battery



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

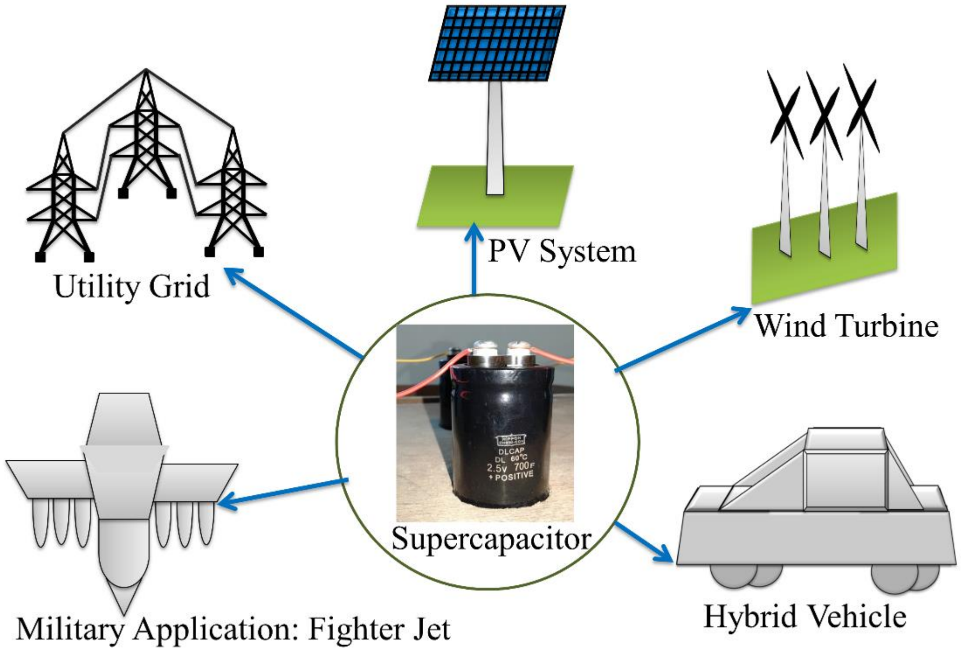


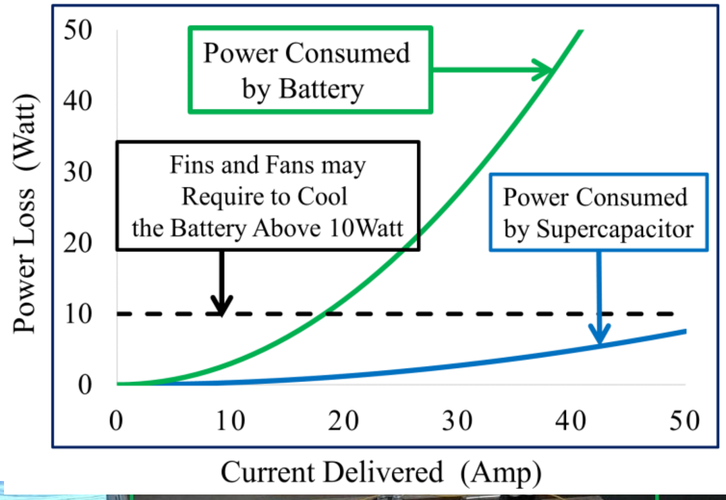
Lithium Polymer Battery

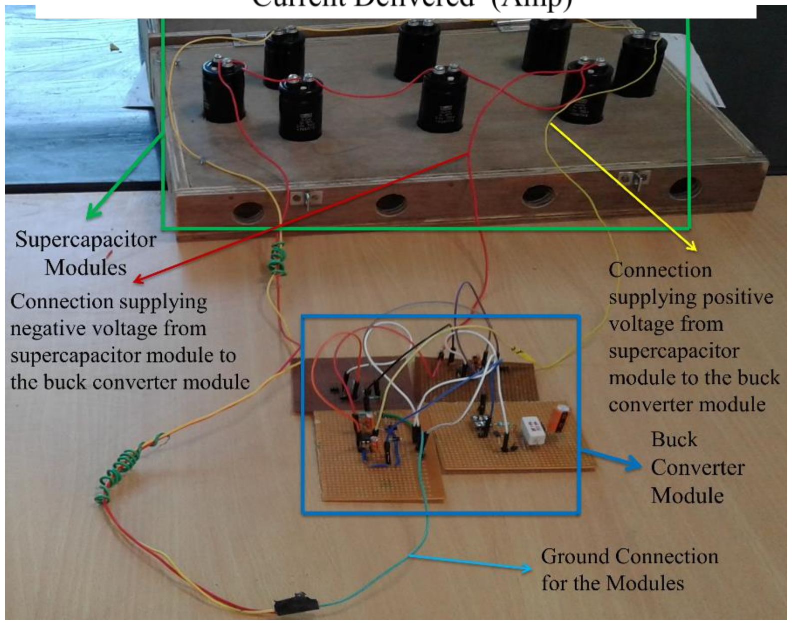
Supercapacitor

Source: Mohanty MAMI 2017 Keynote

Supercapacitor based Power for CE







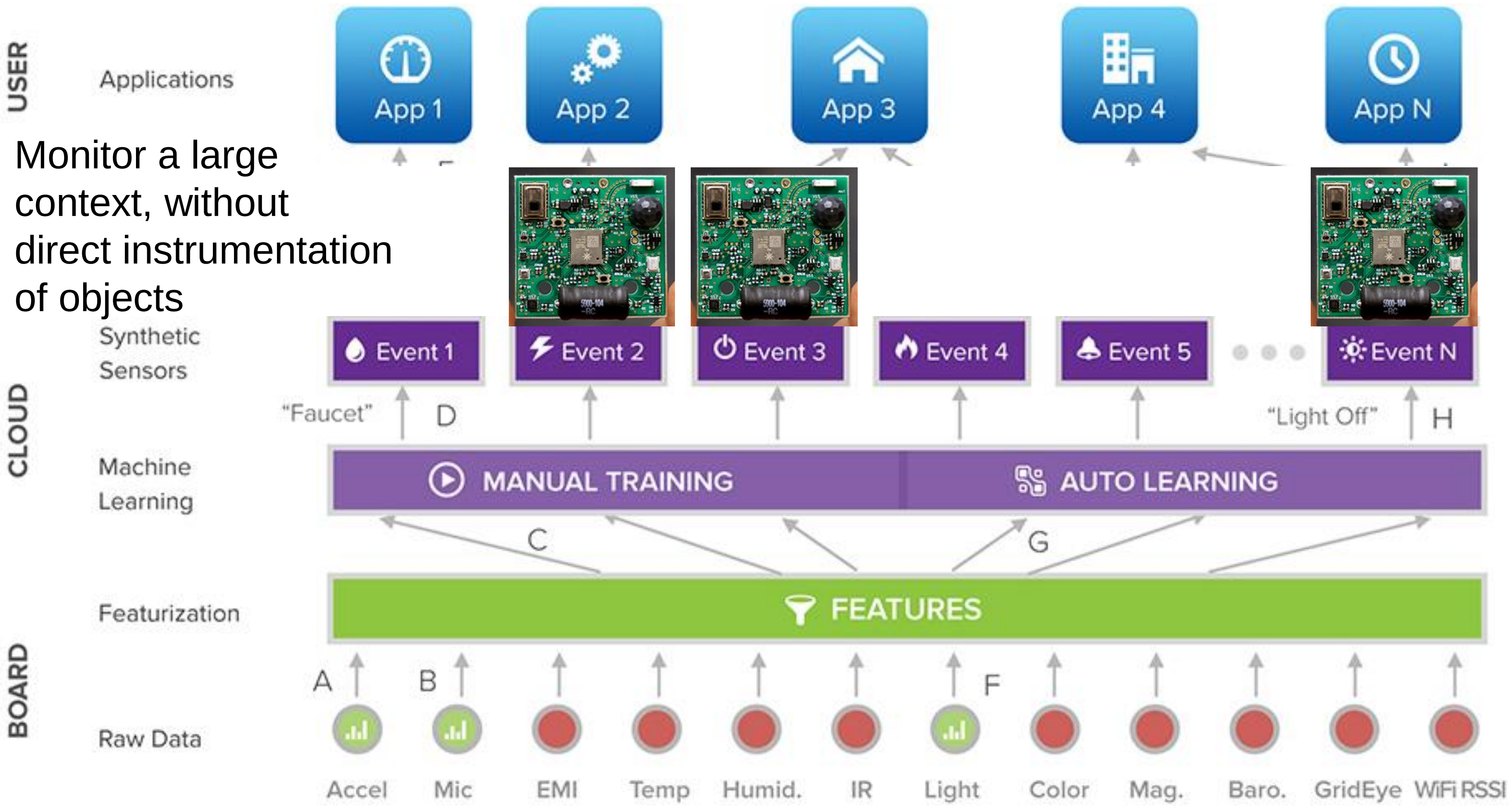
Source: A. S. Sengupta, S. Satpathy, S. P. Mohanty, D. Baral, and B. K. Bhattacharyya, "Supercapacitors Outperform Conventional Batteries", IEEE Consumer Electronics Magazine (CEM), Volume 7, Issue 5, September 2018, pp. 50--53.

Energy Management Solutions Don’t Target Cybersecurity and AI Problems

AI Solutions for IoT/CPS

Smart Sensors - General-Purpose/ Synthetic Sensors

Monitor a large context, without direct instrumentation of objects



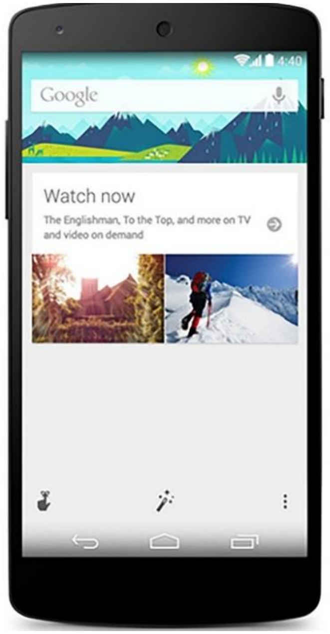
Source: Laput 2017, http://www.gierad.com/projects/supersensor/

Systems – End Devices

Alexa

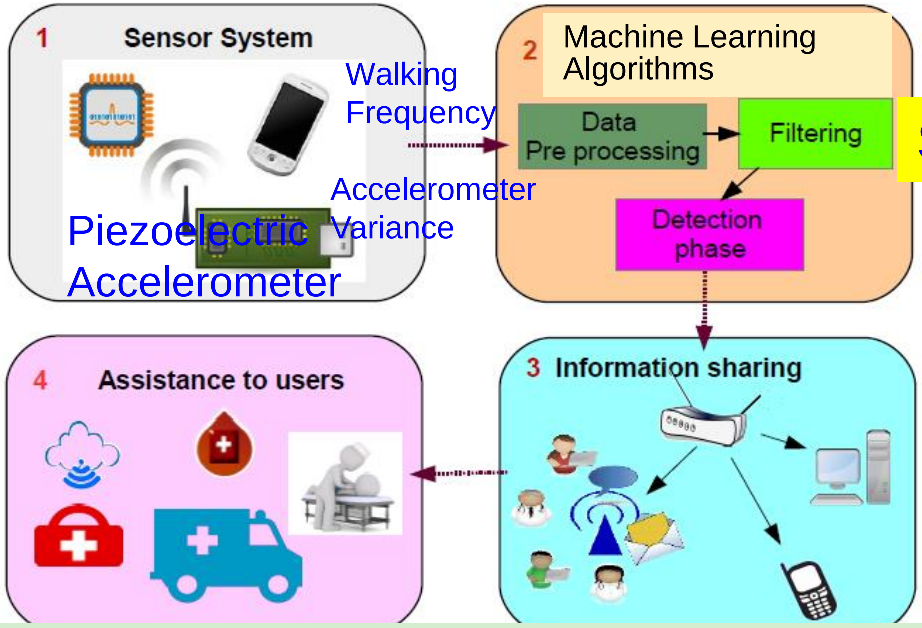
Apple Siri

Google Now

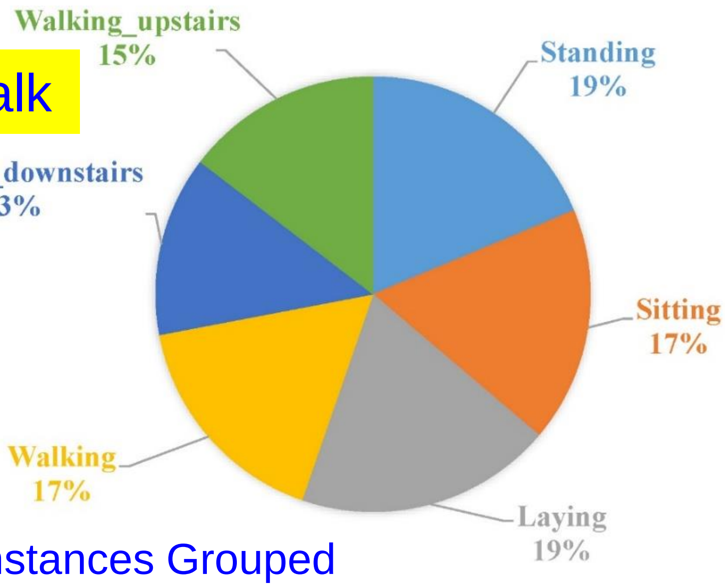


Windows Cortana

Smart Healthcare - Activity Monitoring



Smart-Walk



Automated Physiological Monitoring System

10291 Instances Grouped Under 6 Activities - Kaggle

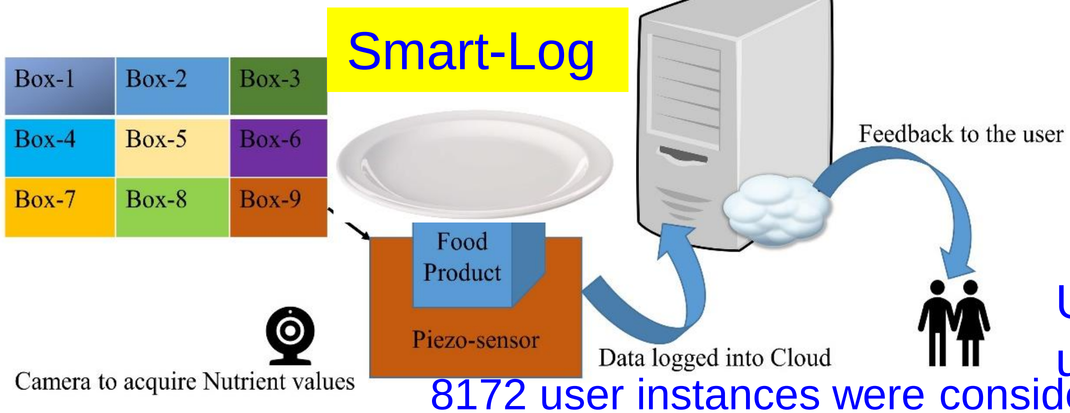
Research Works	**Method** (WEKA)	**Features considered**	**Activities**	**Accuracy (%)**
This Work	Adaptive algorithm based on feature extraction	Step detection and Step length estimation	Walking, sitting, standing, etc.	97.9

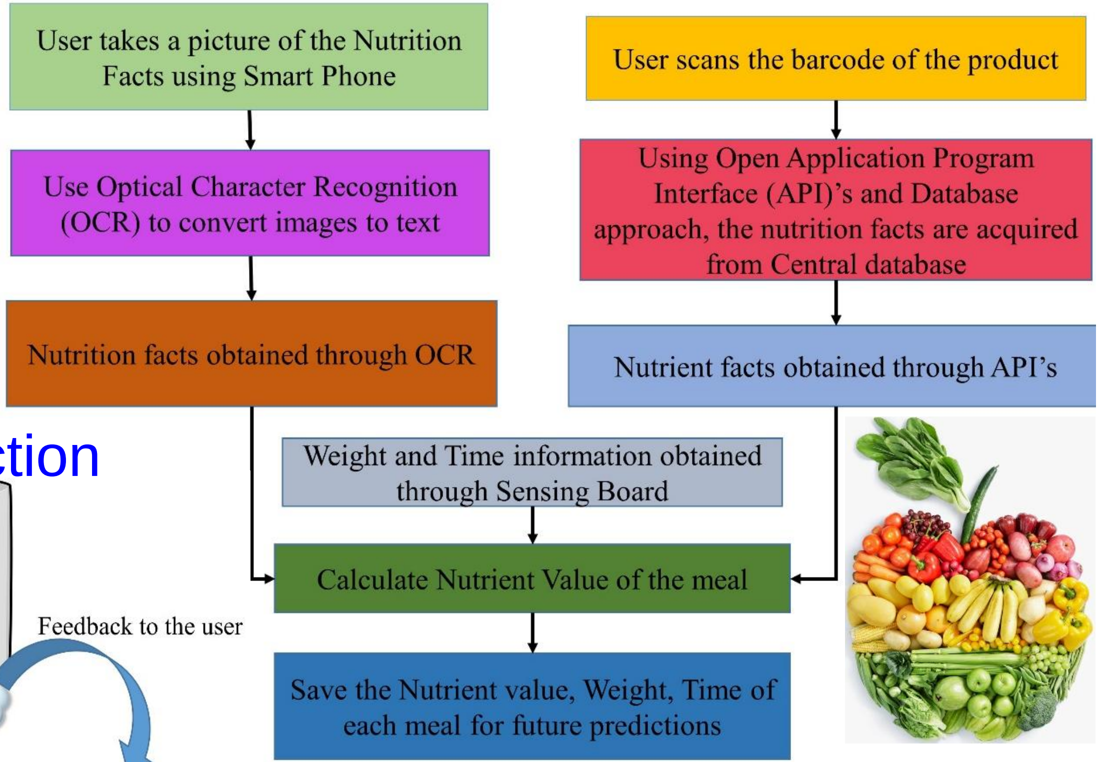
P. Sundaravadivel, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, and M. K. Ganapathiraju, “Smart-Walk: An Intelligent Physiological Monitoring System for Smart Families”, in Proc. 36th IEEE International Conf. Consumer Electronics (ICCE), 2018.

Smart Healthcare – Diet Monitoring

Automated Food intake Monitoring and Diet Prediction System

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





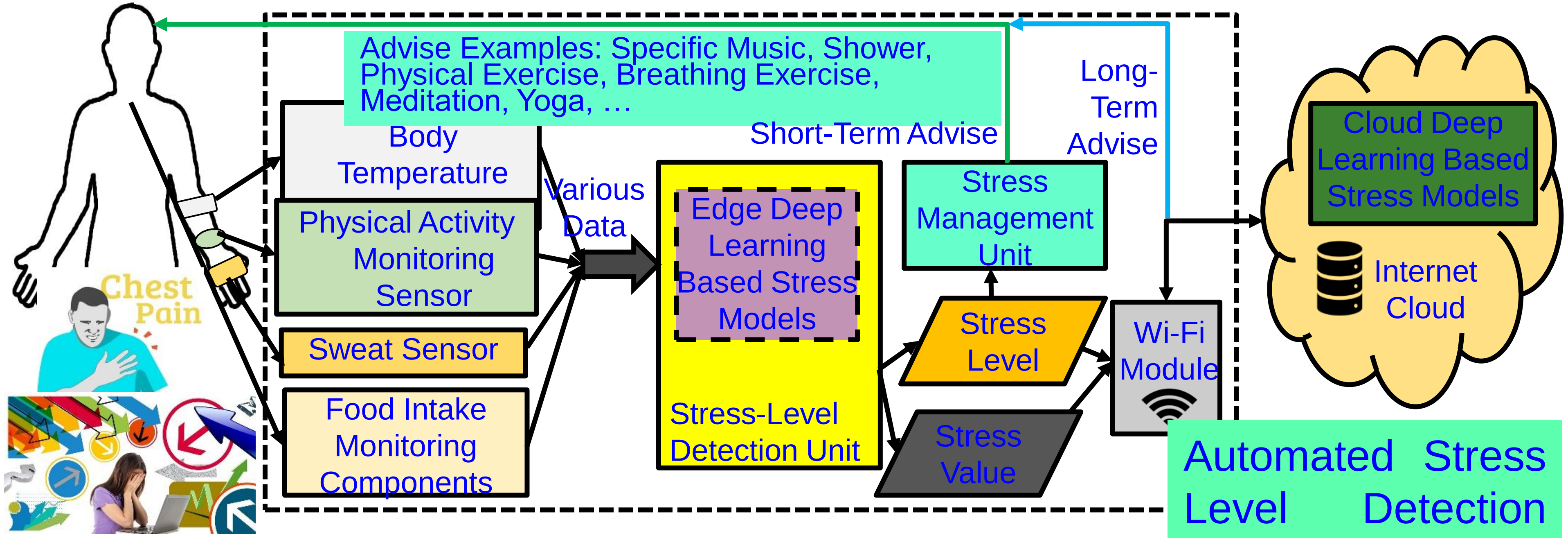
USDA National Nutrient Database used for nutrient values of 8791 items.

8172 user instances were considered

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

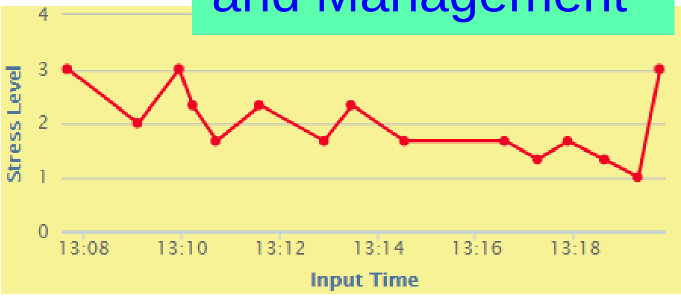
Source: P. Sundaravadivel, K. Kesavan, L. Kesavan, S. P. Mohanty, and E. Kougianos, "Smart-Log: A Deep-Learning based Automated Nutrition Monitoring System in the IoT", IEEE Trans. on Consumer Electronics, Vol 64, No 3, Aug 2018, pp. 390-398.

Smart Healthcare - Stress Monitoring & Control



Automated Stress Level Detection and Management

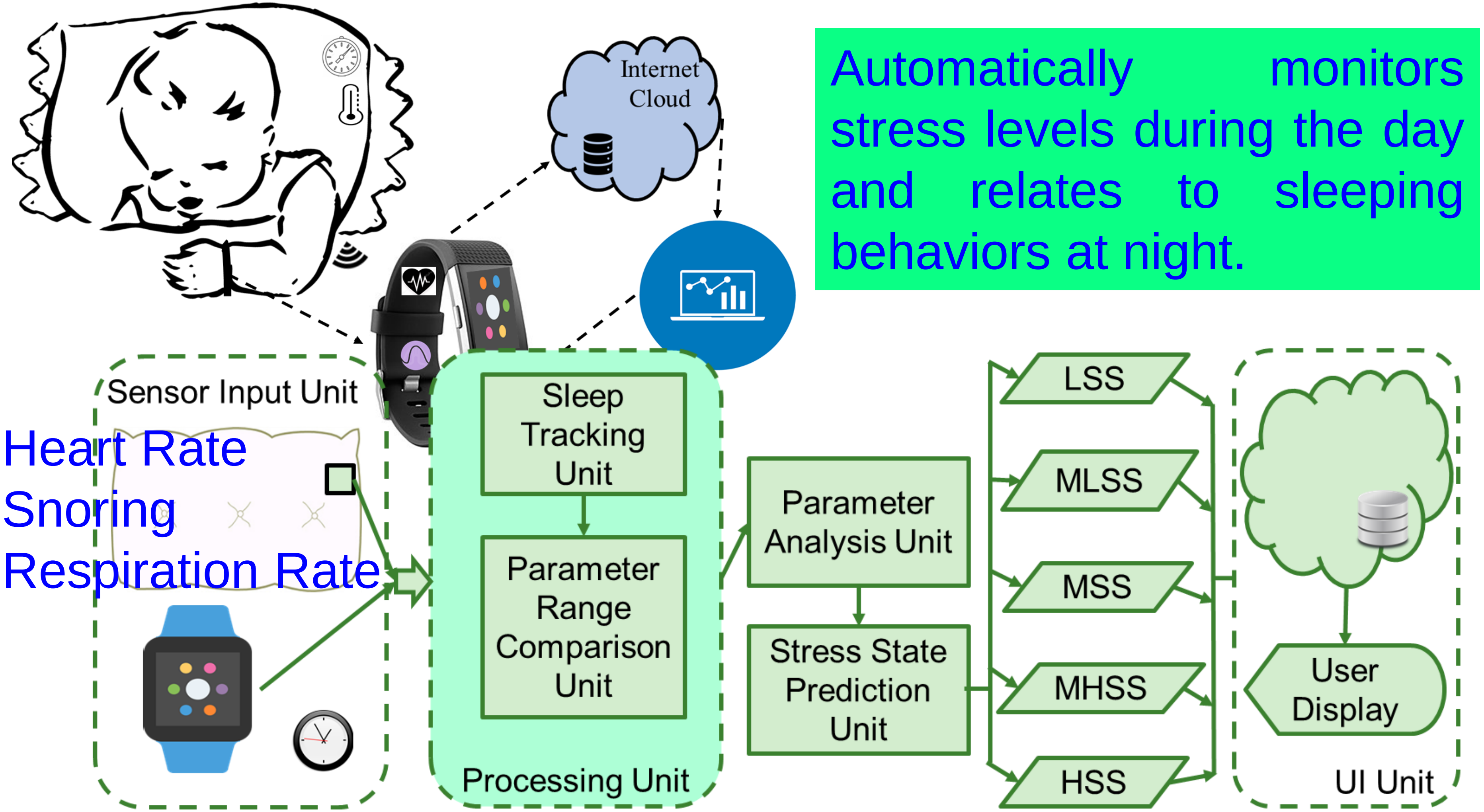
Sensor	Low Stress	Normal Stress	High Stress
Accelerometer (steps/min)	0-75	75-100	101-200
Humidity (RH%)	27-65	66-91	91-120
Temperature ℉	98-100	90-97	80-90



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.

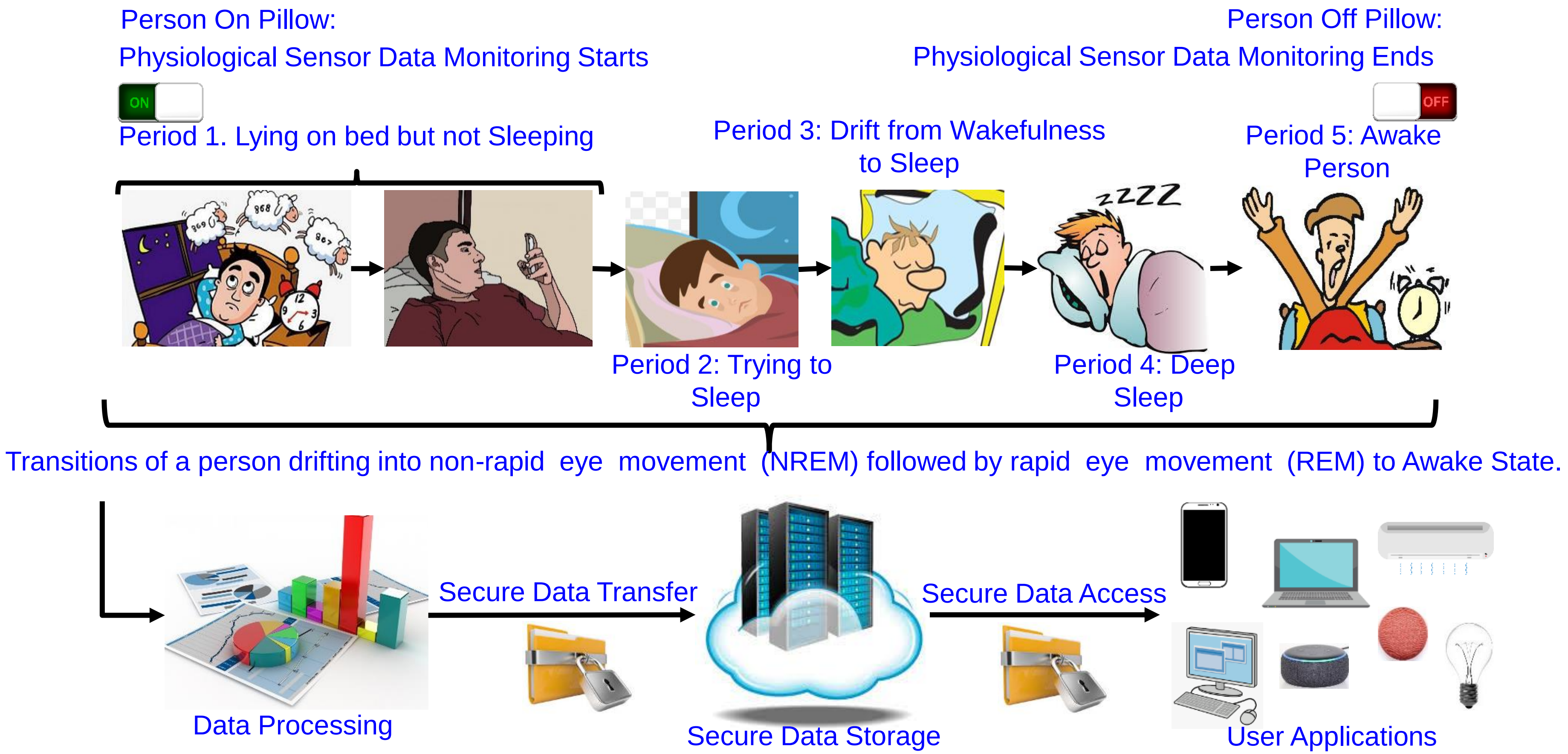
Smart Healthcare – Smart-Pillow

Automatically monitors stress levels during the day and relates to sleeping behaviors at night.



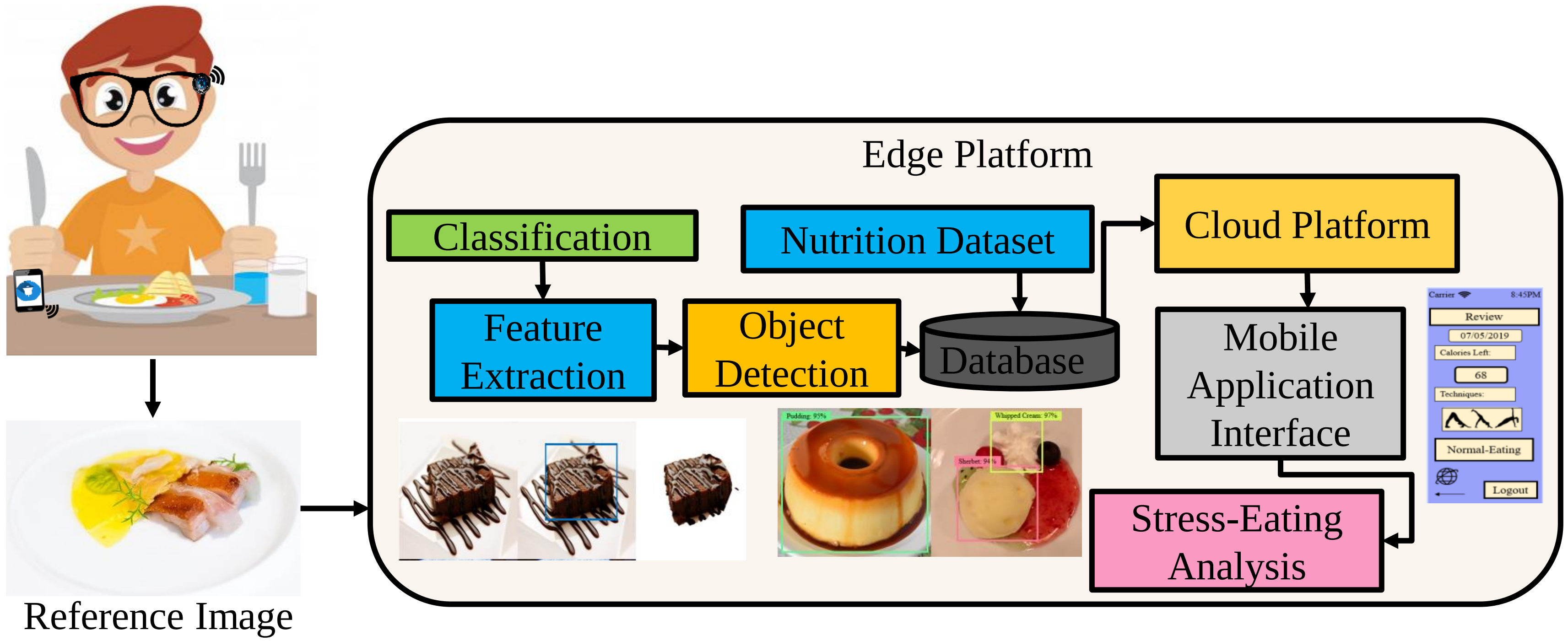
Source: Mohanty iSES 2018: "Smart-Pillow: An IoT based Device for Stress Detection Considering Sleeping Habits", in *Proc. of 4th IEEE International Symposium on Smart Electronic Systems (iSES)* 2018.

Smart-Yoga Pillow (SaYoPillow) - Sleeping Pattern



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

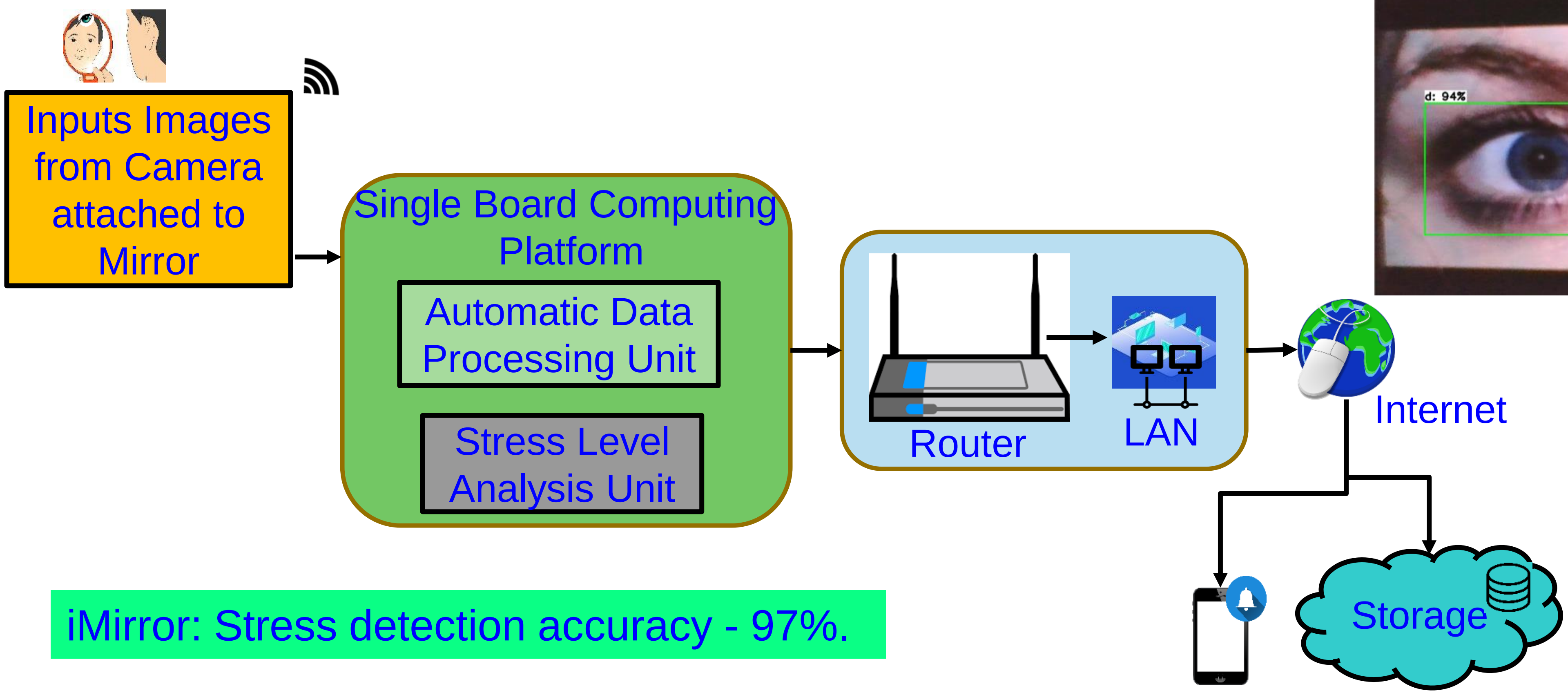
Smart Healthcare – iLog

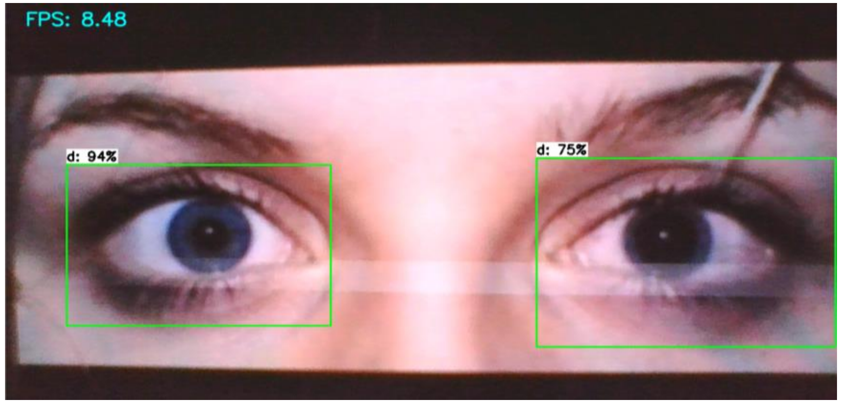


iLog- Fully Automated Detection System with 98% accuracy.

Source: L. Rachakonda, S. P. Mohanty, and E. Kougianos, “iLog: An Intelligent Device for Automatic Food Intake Monitoring and Stress Detection in the IoMT”, *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 66, No. 2, May 2020, pp. 115--124.

iMirror: Our Smart Mirror for Stress Detection from Facial Features

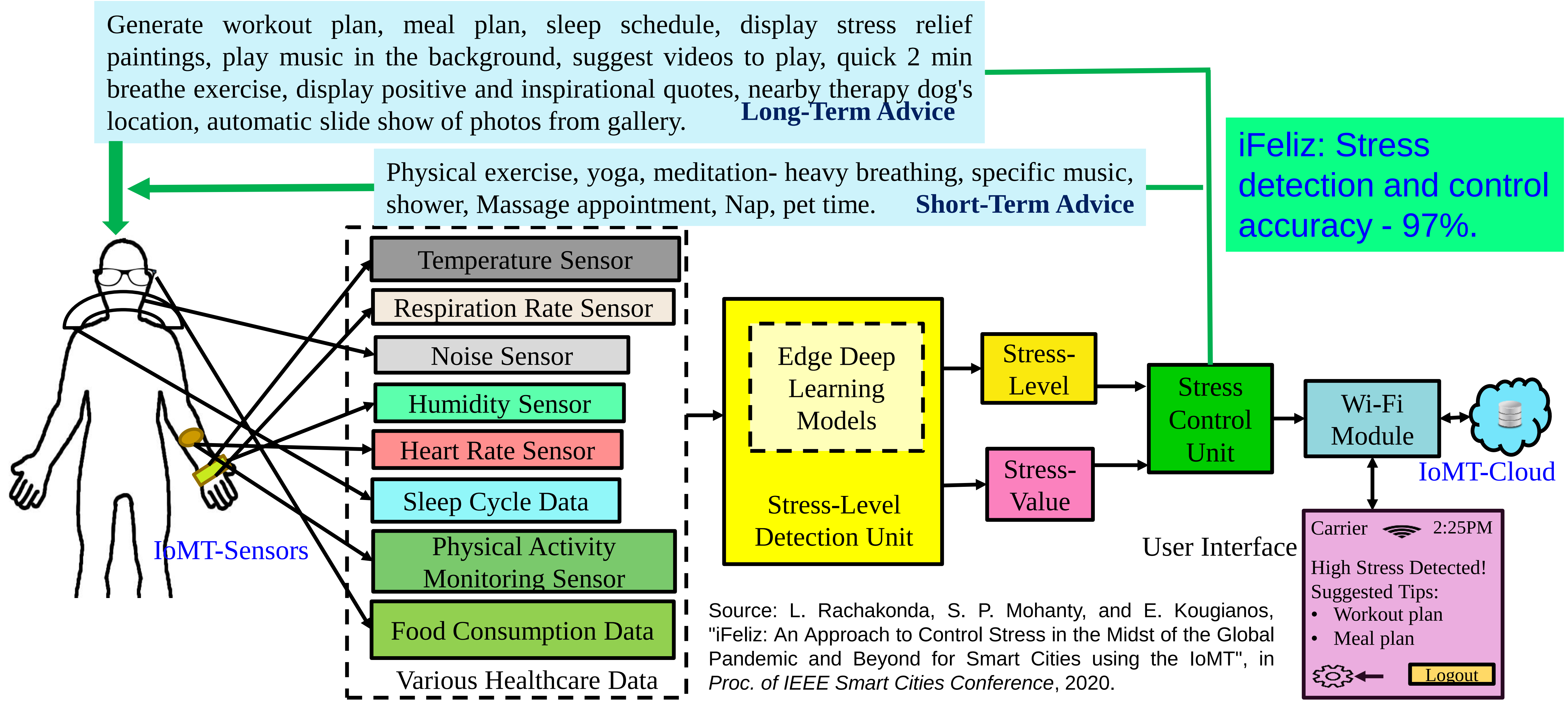




iMirror: Stress detection accuracy - 97%.

Source: L. Rachakonda, P. Rajkumar, **S. P. Mohanty**, and E. Kougianos, “iMirror: A Smart Mirror for Stress Detection in the IoMT Framework for Advancements in Smart Cities”, *Proceedings of the 6th IEEE Smart Cities Conference (ISC2)*, 2020.

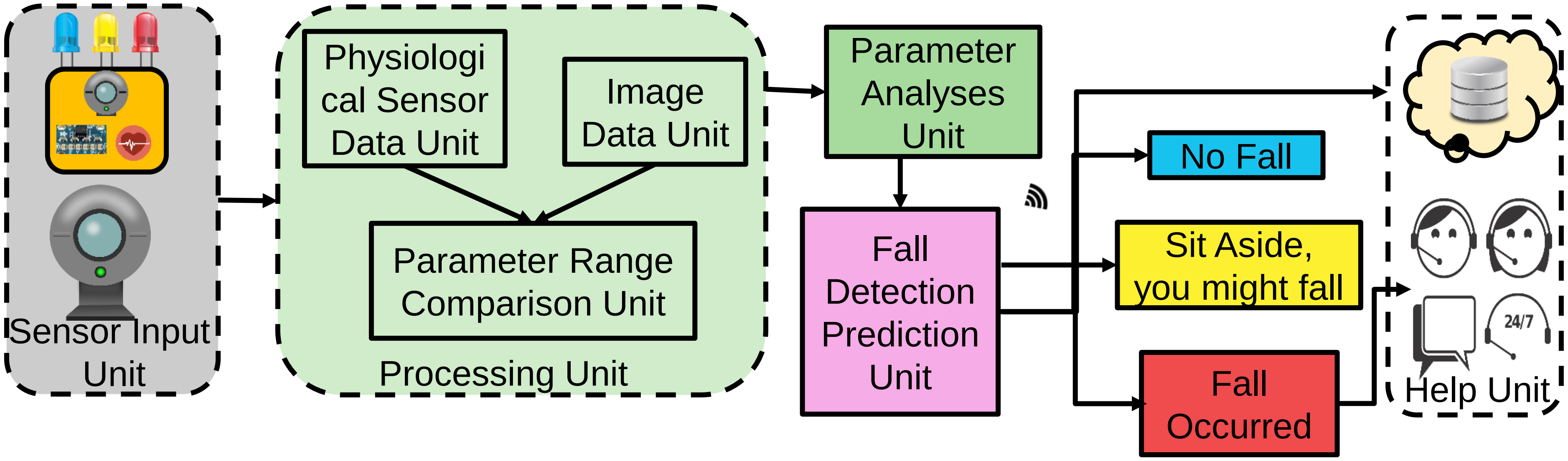
iFeliz: Our Framework for Automatic Stress Control



iFeliz: Stress detection and control accuracy - 97%.

Source: L. Rachakonda, S. P. Mohanty, and E. Kougianos, "iFeliz: An Approach to Control Stress in the Midst of the Global Pandemic and Beyond for Smart Cities using the IoMT", in *Proc. of IEEE Smart Cities Conference*, 2020.

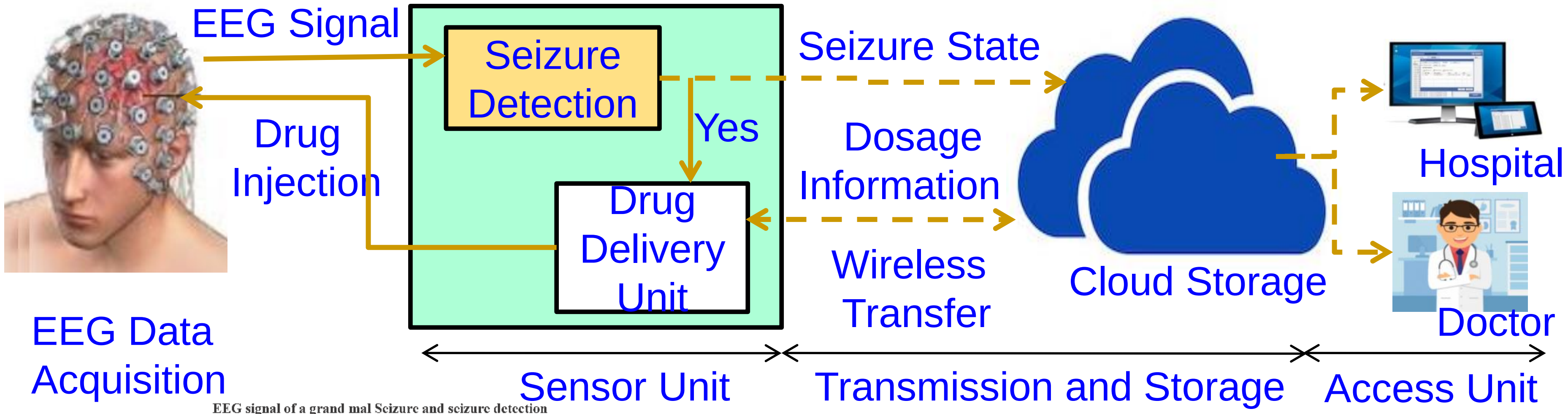
Good-Eye: Our Multimodal Sensor System for Elderly Fall Prediction and Detection



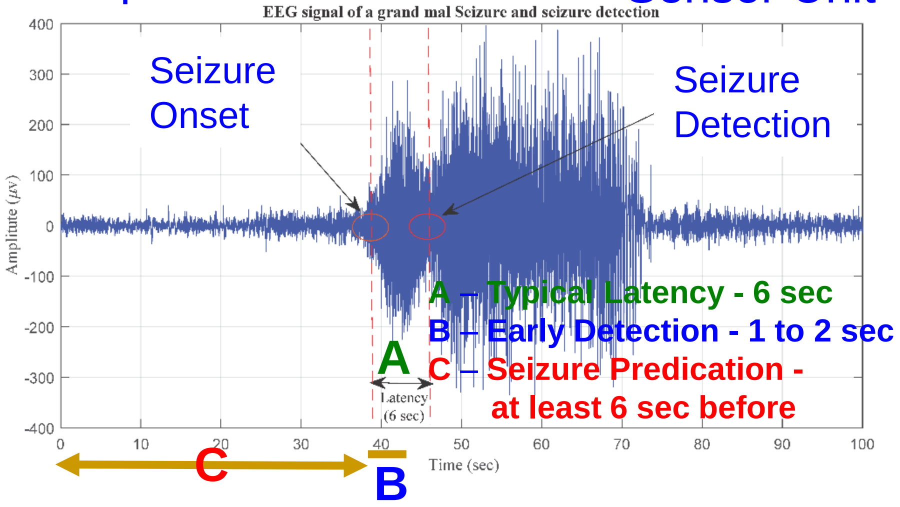
Good-Eye: Fall detection and prediction Accuracy - 95%.

Source: L. Rachakonda, A. Sharma, S. P. Mohanty, and E. Kougianos, "Good-Eye: A Combined Computer-Vision and Physiological-Sensor based Device for Full-Proof Prediction and Detection of Fall of Adults", in *Proceedings of the 2nd IFIP International Internet of Things (IoT) Conference (IFIP-IoT)*, 2019, pp. 273--288.

Smart Healthcare - Seizure Detection & Control



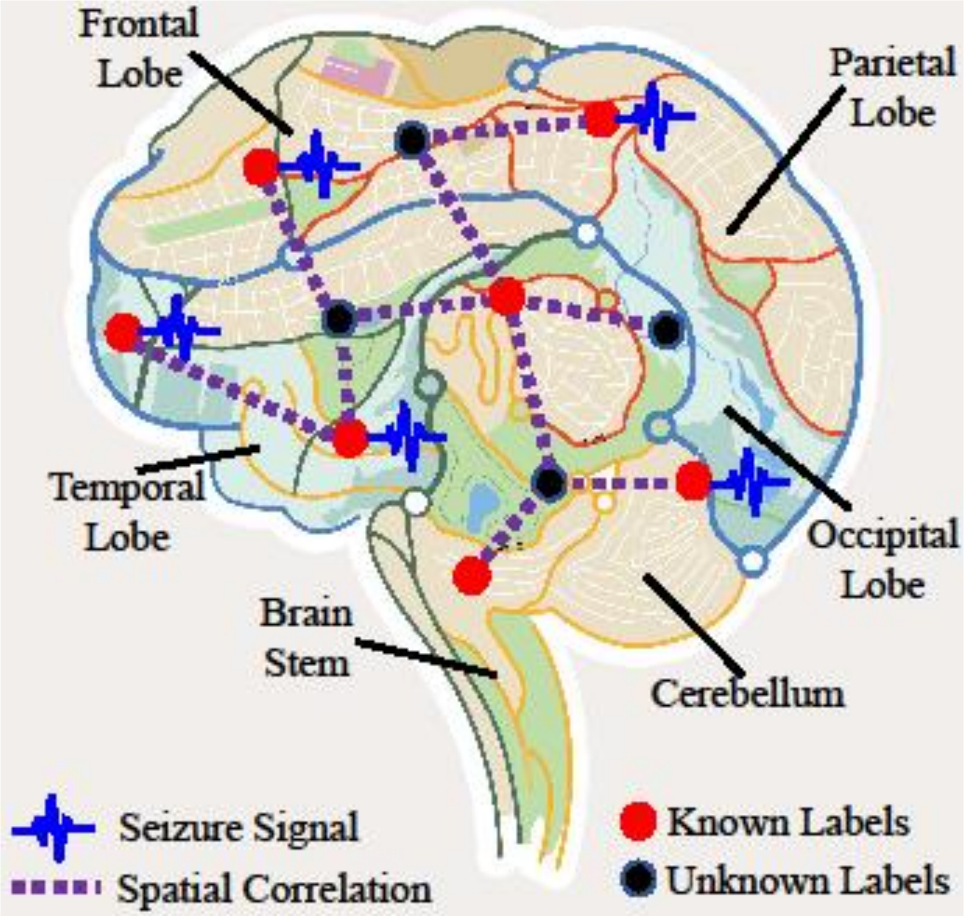
Automated Epileptic Seizure Detection and Control System

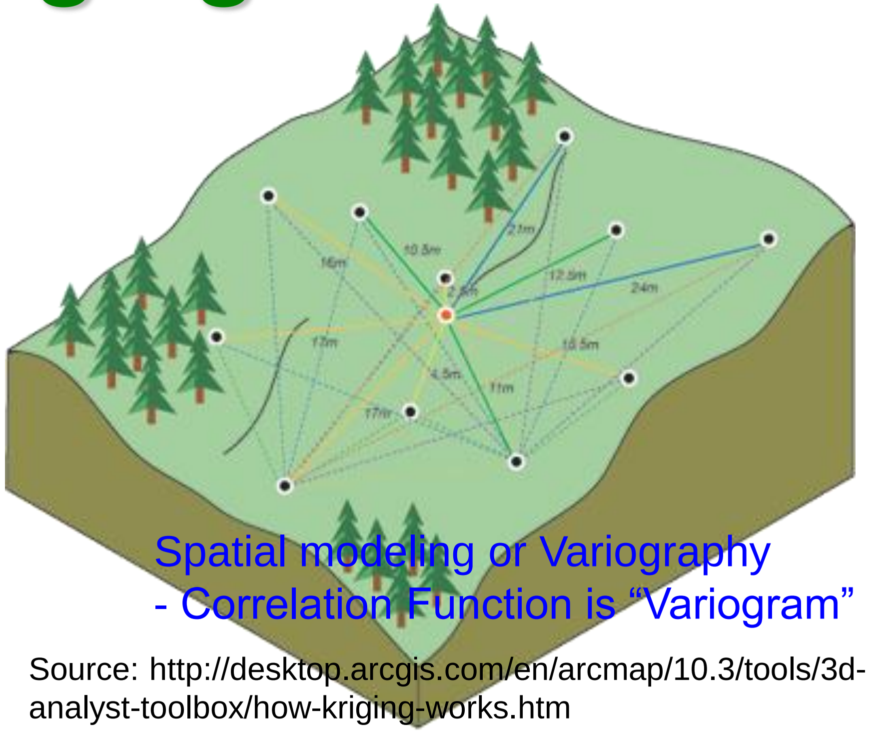


Cloud Vs Edge	Latency	Accuracy
Cloud-IoT based Detection	2.5 sec	98.65%
Edge-IoT based Detection	1.4 sec	98.65%

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 Healthcare – Brain as a Spatial Map → Kriging Methods





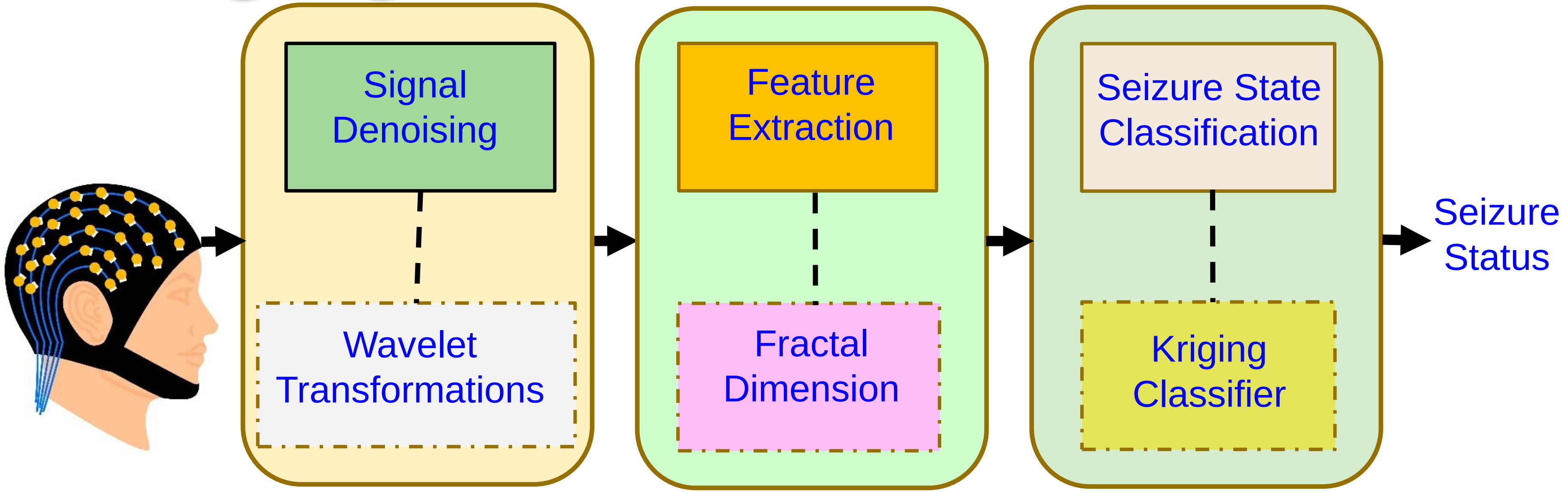
Spatial modeling or Variography
- Correlation Function is “Variogram”

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

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

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

Kriging based Seizure Detection



Works	Extracted Features	Classification Algorithm	Sensitivity	Latency
Zandi, et al. 2012 [23]	Regularity, energy & combined seizure indices	Cumulative Sum thresholding	91.00%	9 sec.
Altaf,etal. 2015 [24]	Digital hysteresis	Support Vector Machine	95.70%	1 sec
Vidyaratne, et al. 2017 [25]	Fractal dimension, spatial/ temporal features	Relevance Vector Machine (RVM)	96.00%	1.89 sec
Our Proposed	Petrosian fractal dimension	Kriging Classifier	100.0%	0.85 s

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

AI Solutions Don’t Target Energy Issues and Cybersecurity Problems

Drawbacks of Existing Security Solutions

CPS 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*, Volume 8, Issue 1, January 2019, pp. 95--99.

IT Security Solutions Can't be Directly Extended to IoT/CPS Security

IT Security

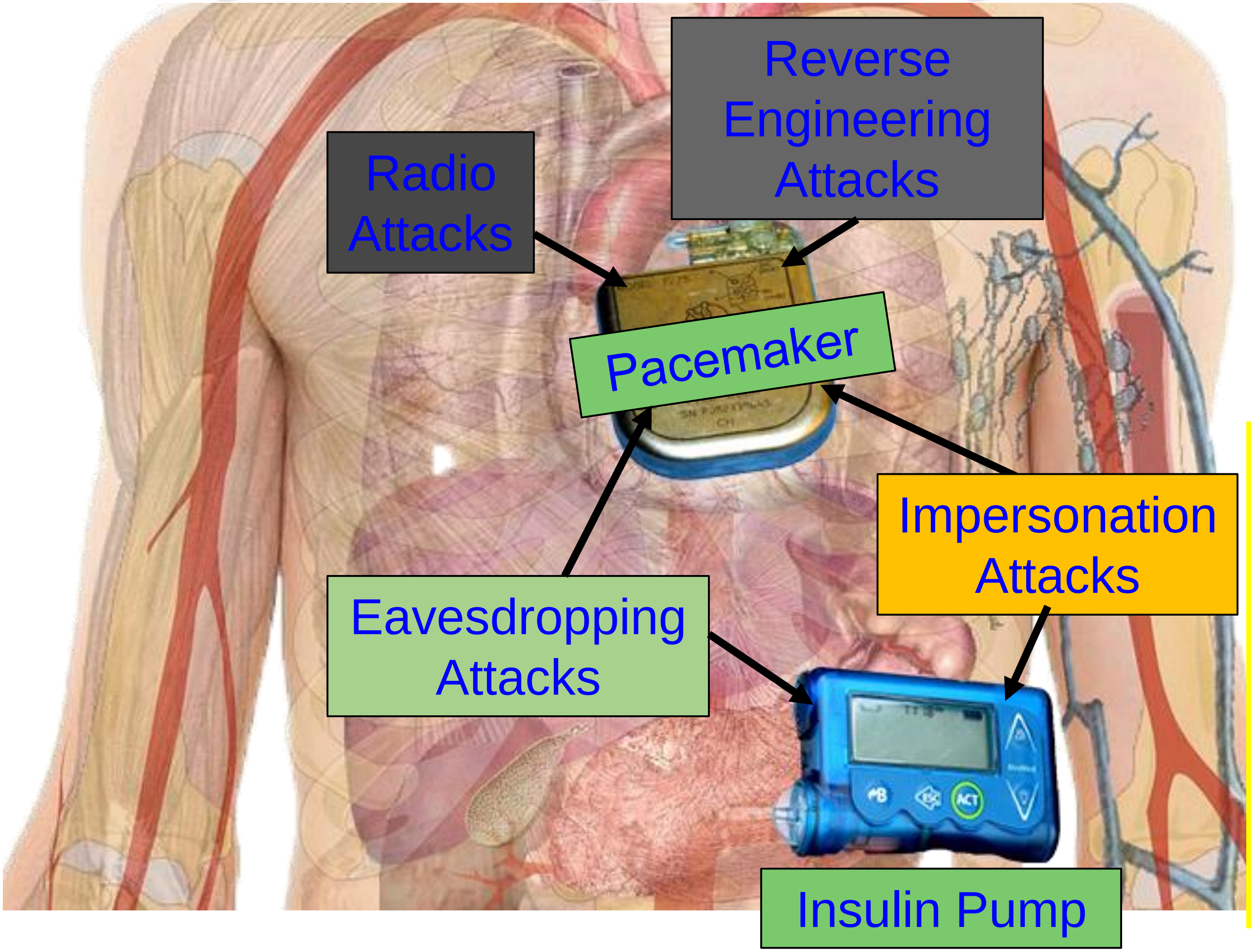
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

IoT Security

- IoT may be deployed in open hostile environments
- Significantly large variety of IoT devices
- Billions of IoT devices
- May not have computational power to run security solutions
- IoT security breach (e.g. in a IoMT device like pacemaker, insulin pump) can be life threatening

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

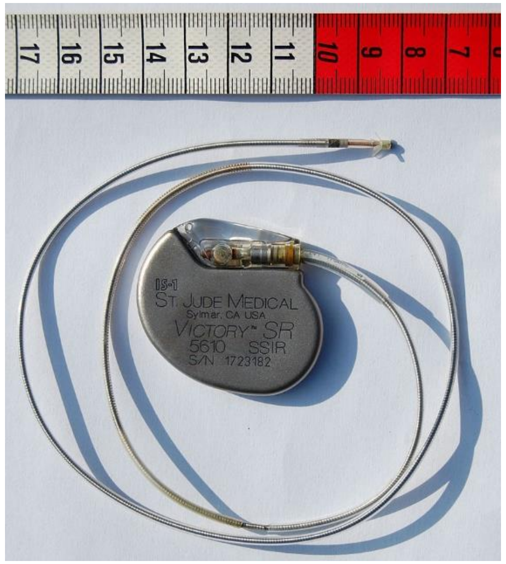
Security Measures in Healthcare Cyber-Physical Systems is Hard



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

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

H-CPS Security Measures is Hard - Energy Constrained



Pacemaker
Battery Life
- 10 years

Neurostimulator
Battery Life
- 8 years

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

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

Smart Car Security - Latency Constrained

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

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

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

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

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

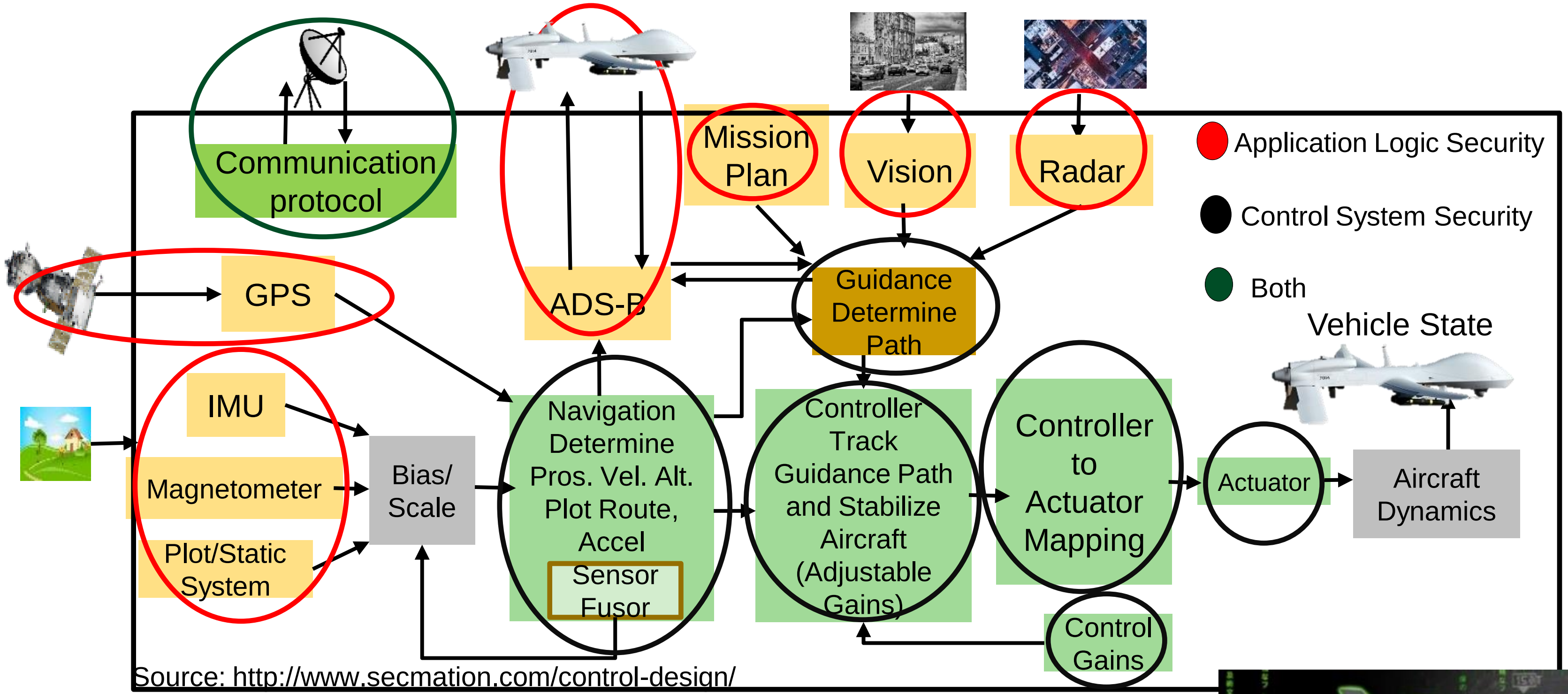
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Security – Latency Constraints

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

UAV Security - Energy & Latency Constrained



Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

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

Smart Grid Security Constraints

Smart Grid – Security Objectives

- Availability
- Integrity
- Confidentiality

Smart Grid – Security Requirements

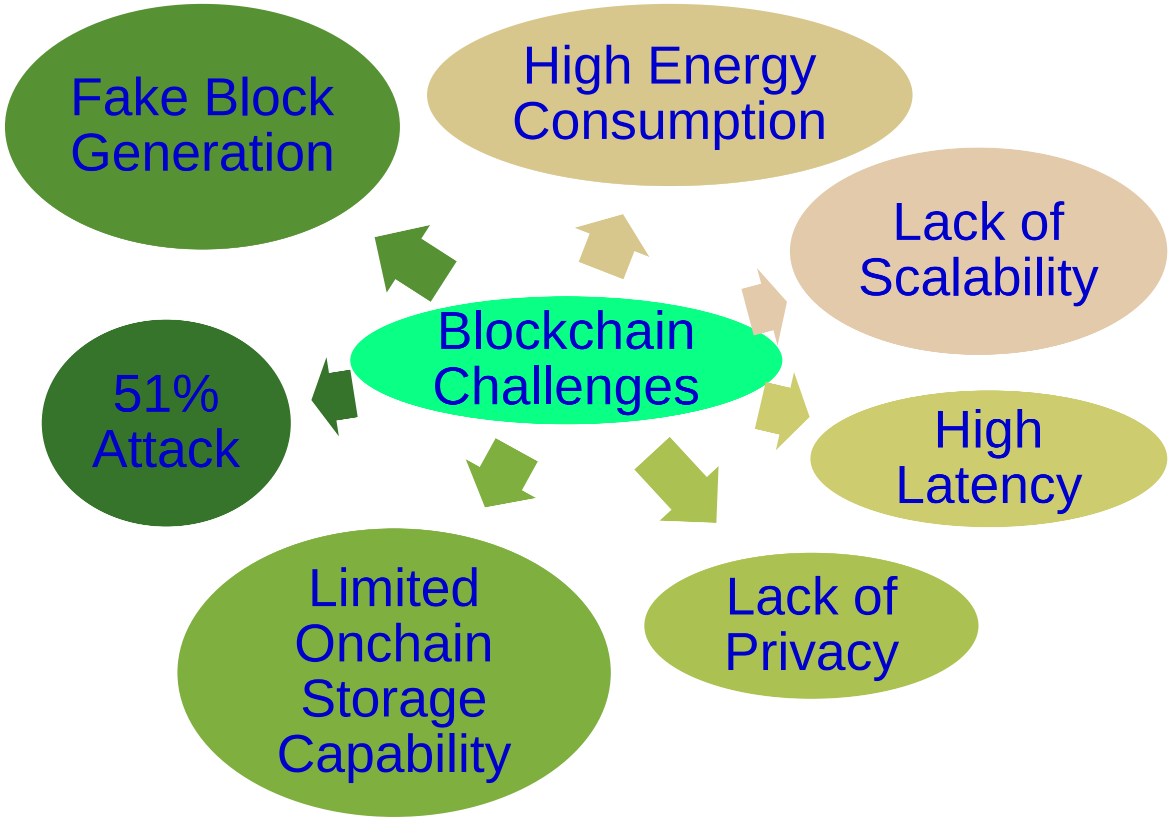
- Identification
- Authentication
- Authorization
- Trust
- Access Control
- Privacy

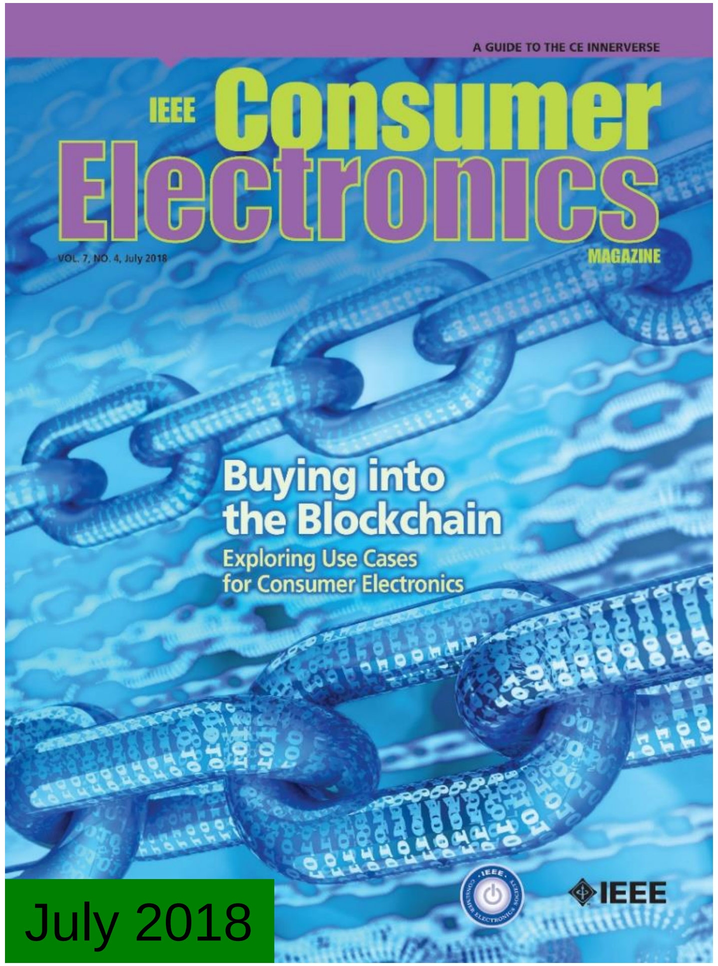
Smart Grid – Security Solution Constraints

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

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

Blockchain has Many Challenges





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

Blockchain Energy Need is Huge

Energy for mining of 1 bitcoin

=

Energy consumption 2 years of a US household

Energy consumption for each bitcoin transaction

=

80,000X

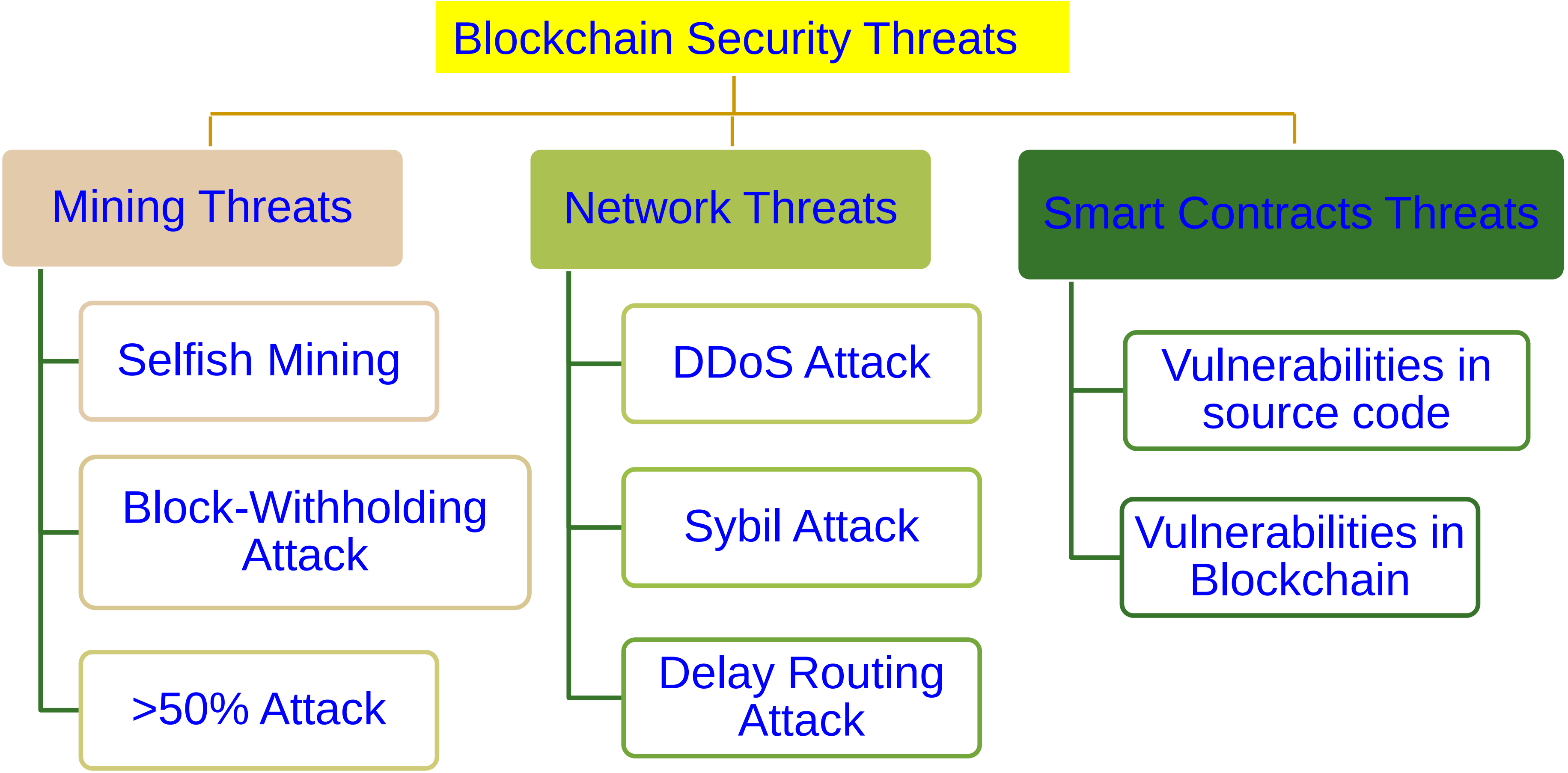
Energy consumption of a credit card processing

Blockchain has Security Challenges

Selected attacks on the blockchain and defences		
Attacks	**Descriptions**	**Defence**
Double spending	Many payments are made with a body of funds	Complexity of mining process
Record hacking	Blocks are modified, and fraudulent transactions are inserted	Distributed consensus
51% attack	A miner with more than half of the network's computational power dominates the verification process	Detection methods and design of incentives
Identity theft	An entity's private key is stolen	Reputation of the blockchain on identities
System hacking	The software systems that implement a blockchain are compromised	Advanced intrusion detection systems

Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

Blockchain Security Threats



Source: D. Puthal, S. P. Mohanty, E. Kougianos and G. Das, "When Do We Need the Blockchain?," *IEEE Consumer Electronics Magazine*, Vol 10, No. 2, Mar 2021, doi: 10.1109/MCE.2020.3015606.

Blockchain has Serious Privacy Issue

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

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

Smart Contracts - Vulnerabilities

Vulnerability	Cause	Level
Call to unknown	The called function does not exist	Contract's source code
Out-of-gas send	Fallback of the callee is executed	Contract's source code
Exception disorder	Exception handling irregularity	Contract's source code
Type casts	Contract execution type-check error	Contract's source code
Reentrance flaw	Function reentered before exit	Contract's source code
Field disclosure	Private value published by miner	Contract's source code
Immutable bug	Contract altering after deployment	Ethereum virtual machine bytecode
Ether lost	Ether sent to orphan address	Ethereum virtual machine bytecode
Unpredicted state	Contract state change before call	Blockchain Mechanism
Randomness bug	Seed biased by malicious miner	Blockchain mechanism
Time-stamp failure	Malicious miner alters time stamp	Blockchain mechanism

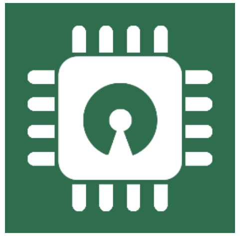
Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

Cybersecurity Attacks - Software and Hardware Based

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
  - Electronic system tampering/ jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - Hardware counterfeiting

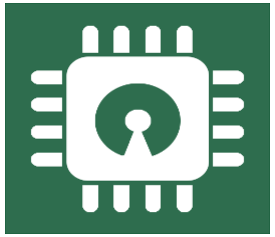
Source: Mohanty ICCE Panel 2018

Cybersecurity Solutions - Software Vs Hardware Based

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

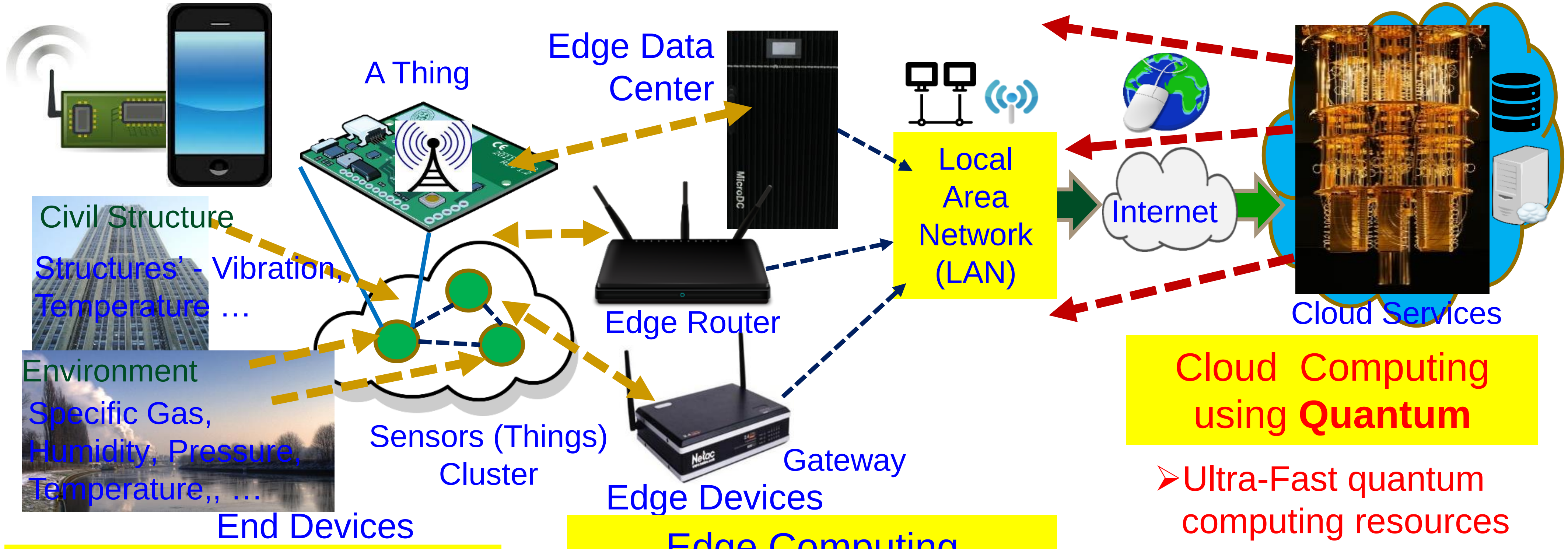
Hardware Based



- 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

Source: Mohanty ICCE Panel 2018

A Security Nightmare - by Quantum Computing



In-Sensor/End-Device Computing

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

Edge Computing

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

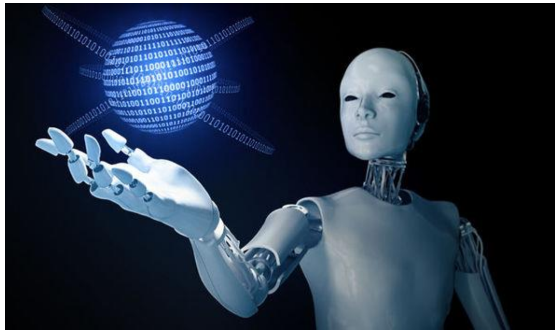
Cloud Computing using **Quantum**

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

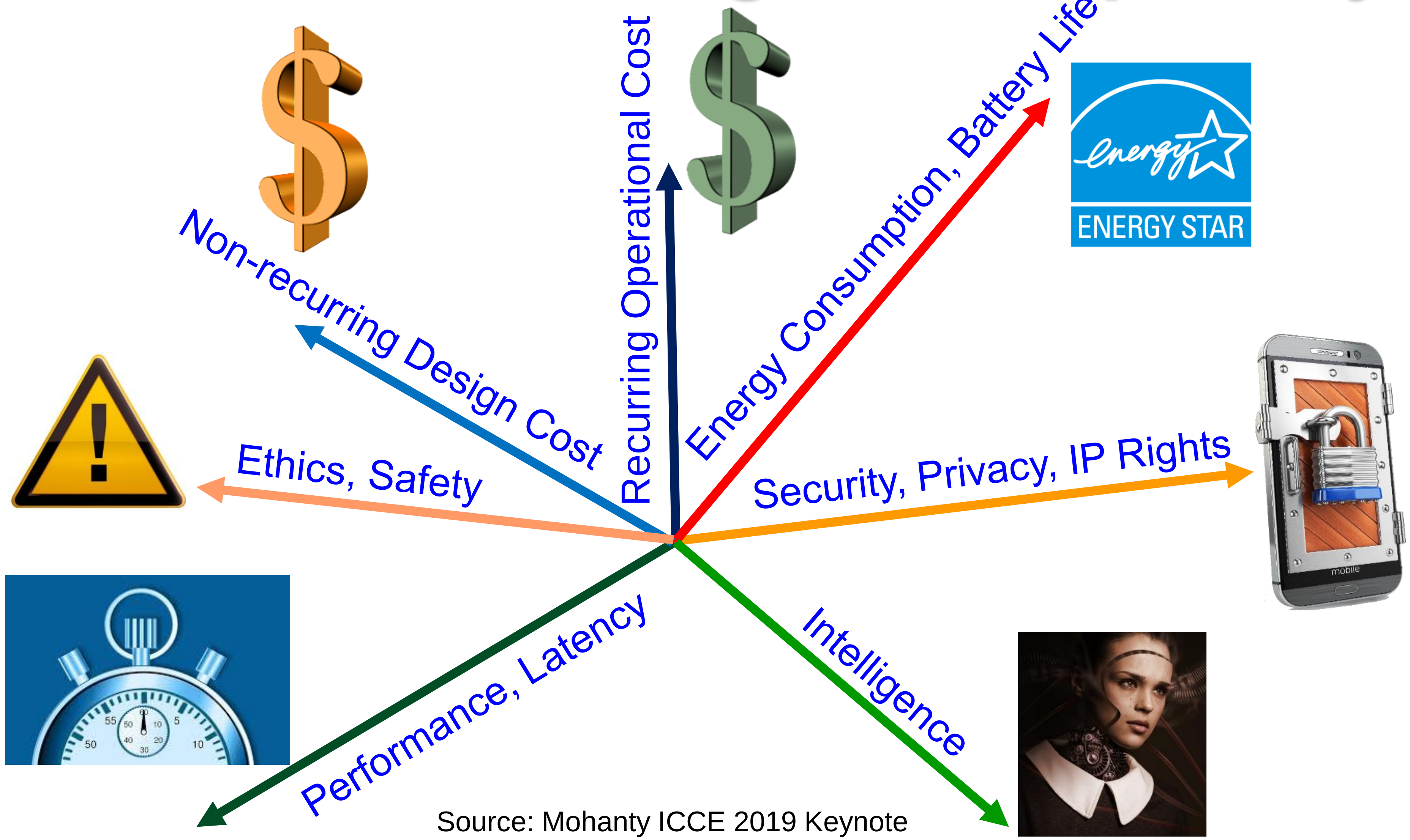
A quantum computer could break a 2048-bit RSA encryption in 8 hours.

Cybersecurity Solutions Don't Target Energy Issues and AI Problems

Hardware-Assisted Security (HAS) or Secure-by-Design (SbD)



IoT/CPS Design – Multiple Objectives



Source: Mohanty ICCE 2019 Keynote

Smart Cities
Vs
Smart Villages

Privacy by Design (PbD) → General Data Protection Regulation (GPDR)

1995
Privacy by Design (PbD)

- ❖ Treat privacy concerns as design requirements when developing technology, rather than trying to retrofit privacy controls after it is built

2018
General Data Protection Regulation (GDPR)

- ❖ GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design aka Secure by Design (SbD)

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

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

Retrofitting: Difficult → Impossible!

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

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

7 Fundamental Principles

- Proactive not Reactive
- Security/Privacy as the Default
- Security/Privacy Embedded into Design
- Full Functionality - Positive-Sum, not Zero-Sum
- End-to-End Security/Privacy - Lifecycle Protection
- Visibility and Transparency
- Respect for Users

Source: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf

CEI Tradeoffs for Smart Electronic Systems

Security of
systems
and data.

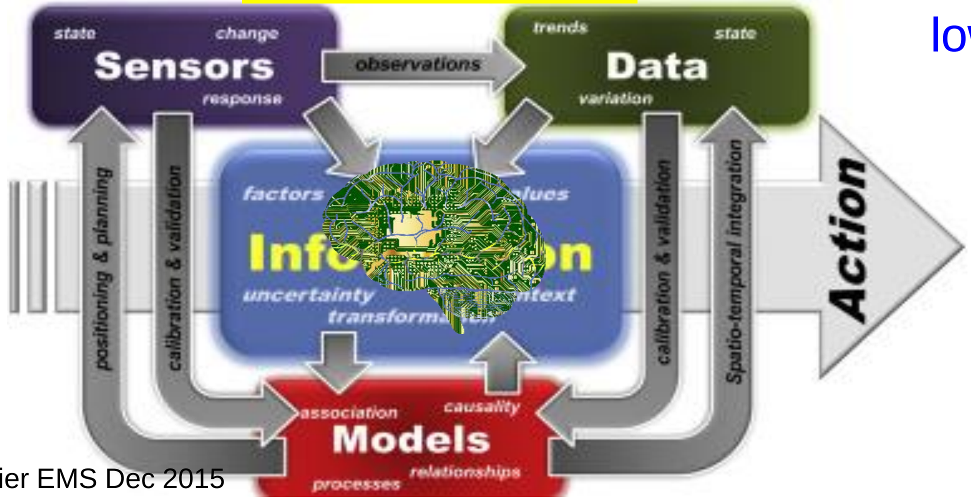
Cybersecurity

Energy

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

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

Intelligence



Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Source: Mohanty iSES 2018 Keynote

Hardware-Assisted Security (HAS)

- 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.

Privacy by Design (PbD)

Security/Secure by Design (SbD)

RF Hardware Security | Digital Hardware Security – Side Channel

Hardware Trojan Protection | Information Security, Privacy, Protection

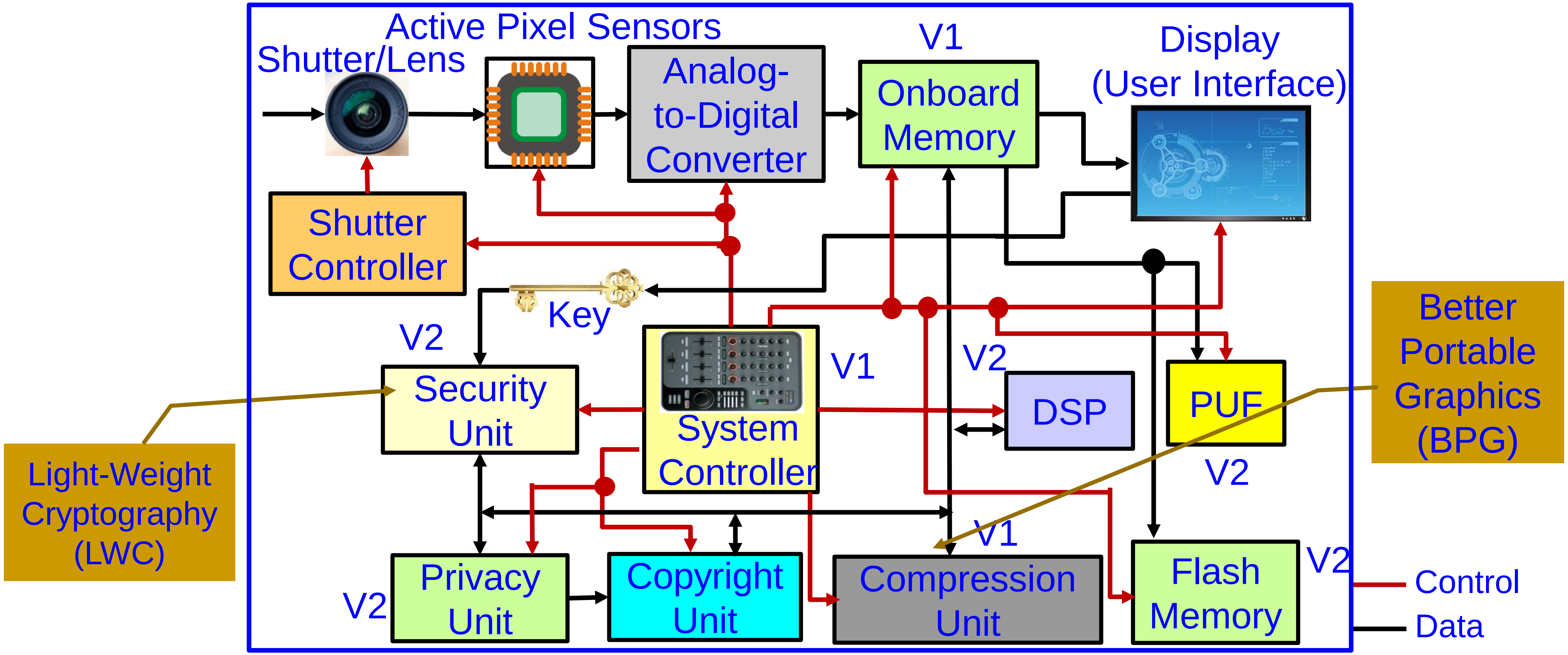
IR Hardware Security | Memory Protection | Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

Secure SoC Design : Two Modes

- Addition of security and AI features in SoC:
  - Algorithms
  - Protocols
  - Architectures
  - Accelerators / Engines – Cybersecurity and AI Instructions
- Consideration of security as a dimension in the design flow:
  - New design methodology
  - Design automation or computer aided design (CAD) tools for fast design space exploration.

Secure Digital Camera (SDC) – My Invention

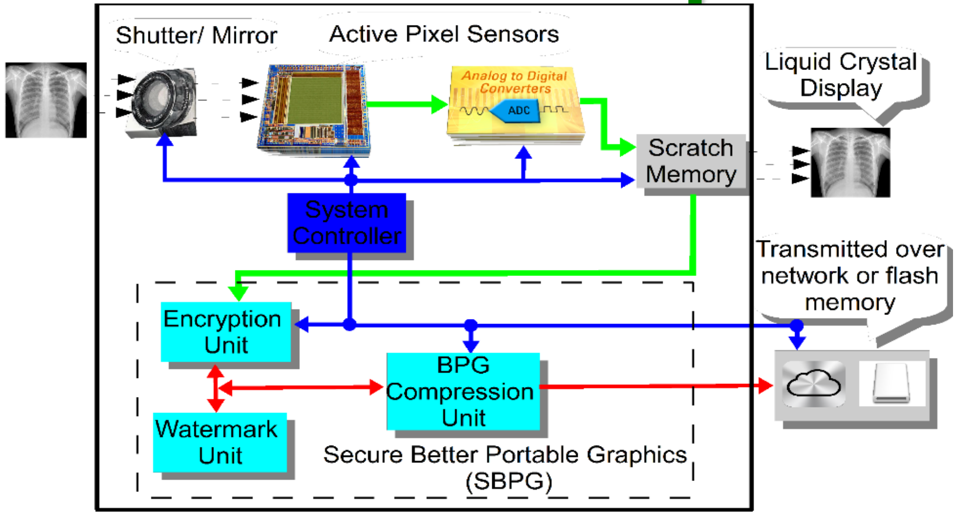


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

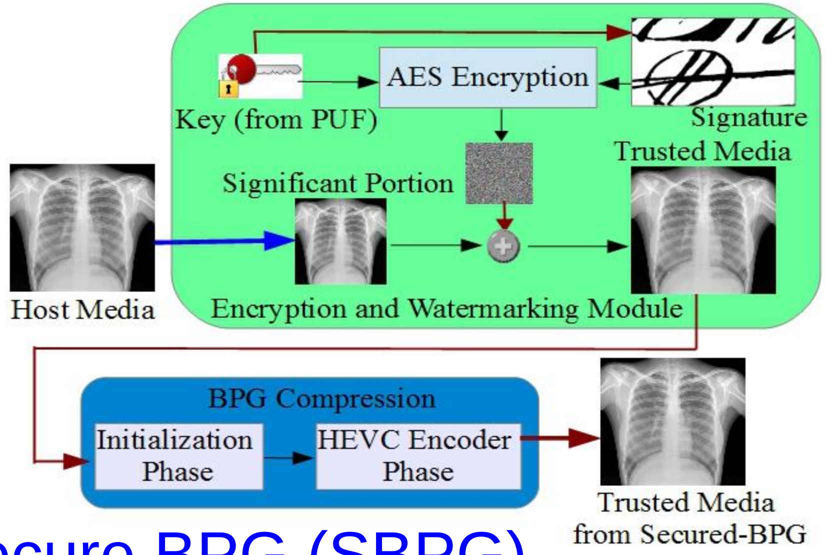
Security and/or Privacy by Design (SbD and/or PbD)

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

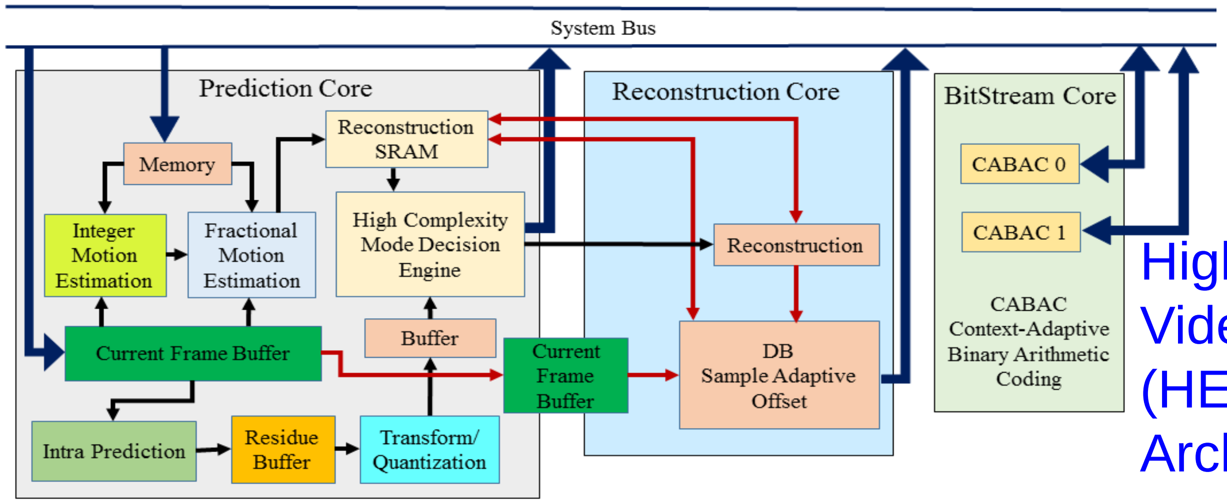
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)

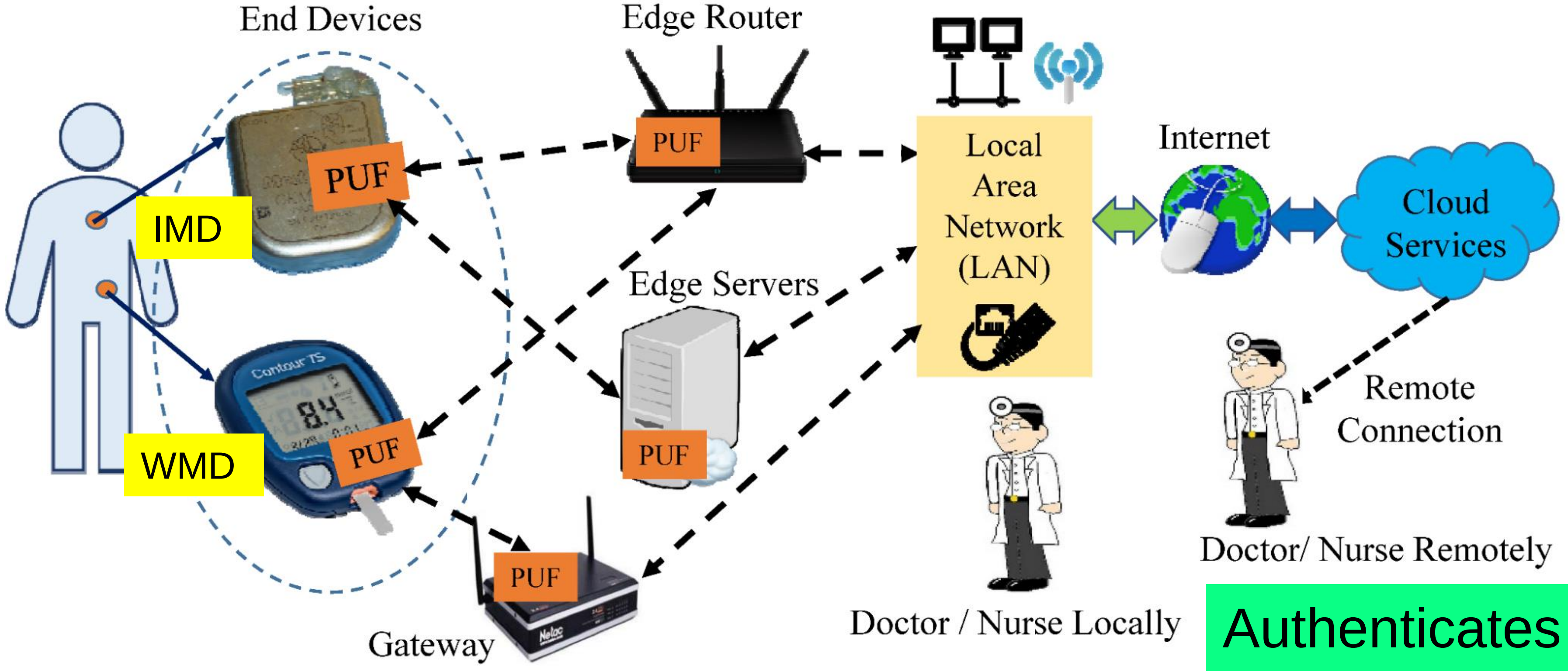


High-Efficiency Video Coding (HEVC) Architecture

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

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

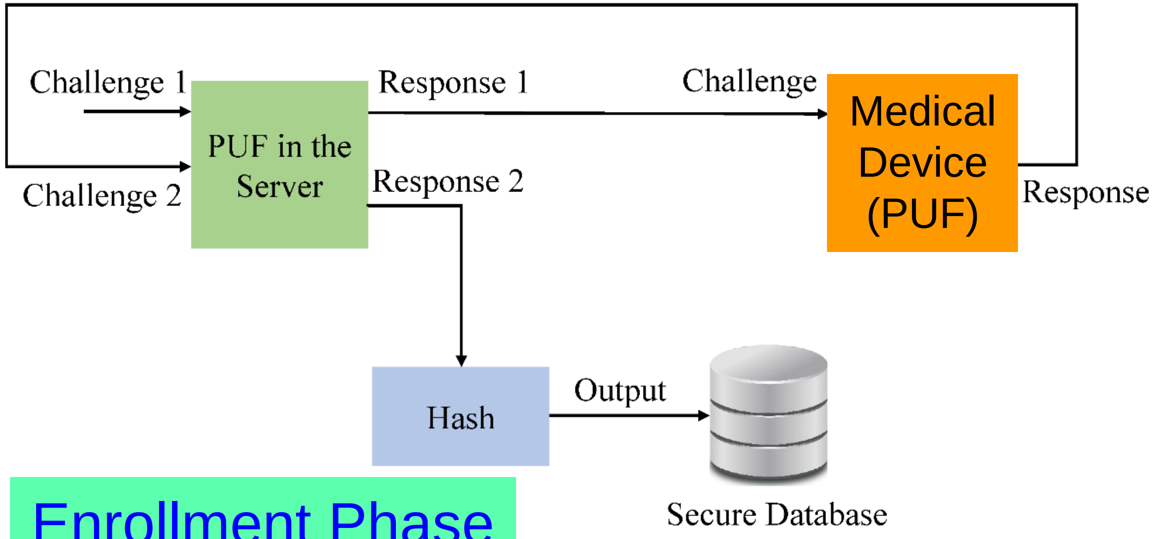
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

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

IoMT Security – Our Proposed PMsec

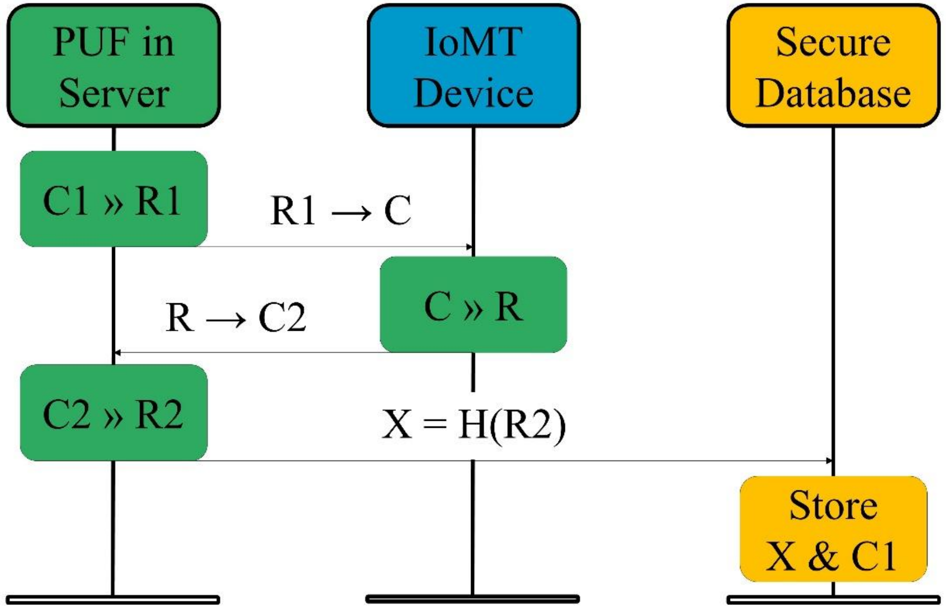


Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

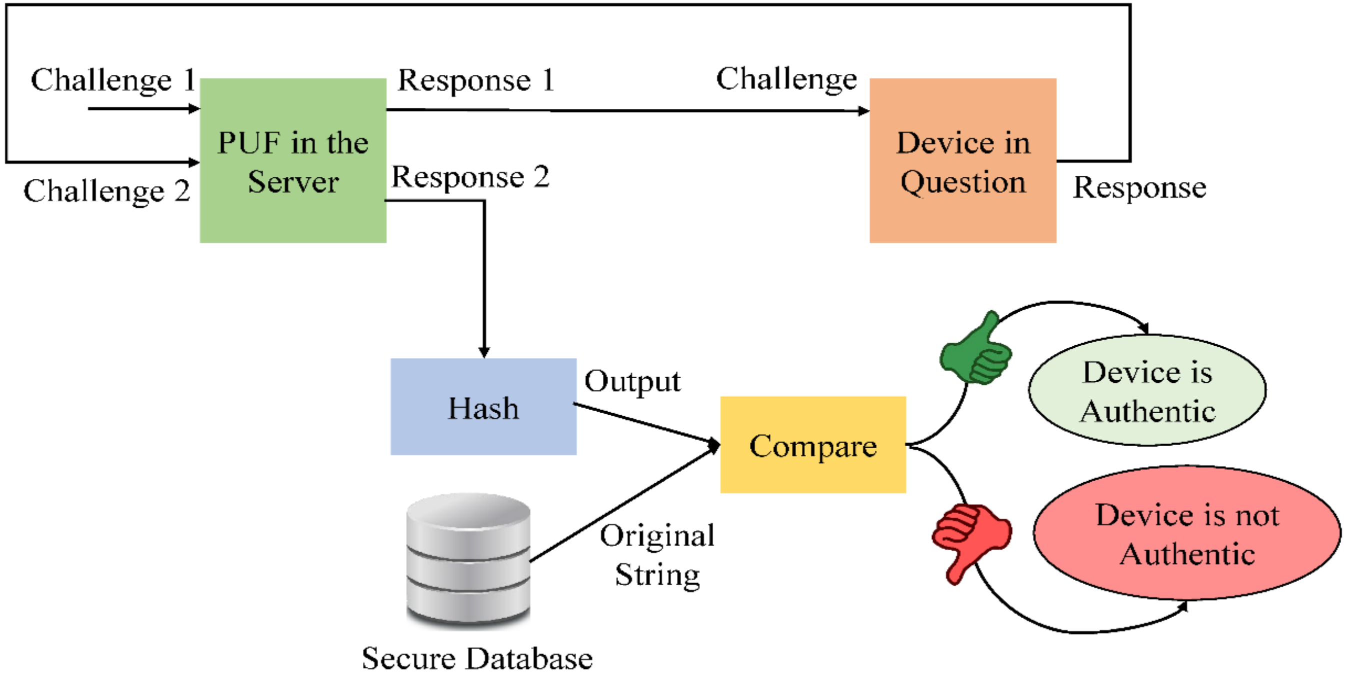


PUF Security Full Proof:

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

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

IoMT Security – Our Proposed PMsec

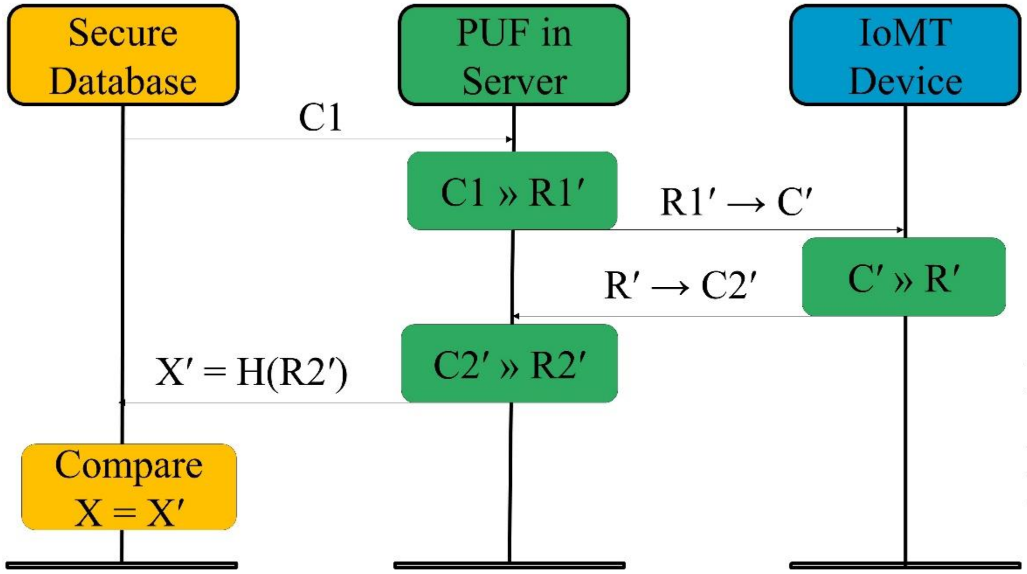


Authentication Phase

At the Doctor

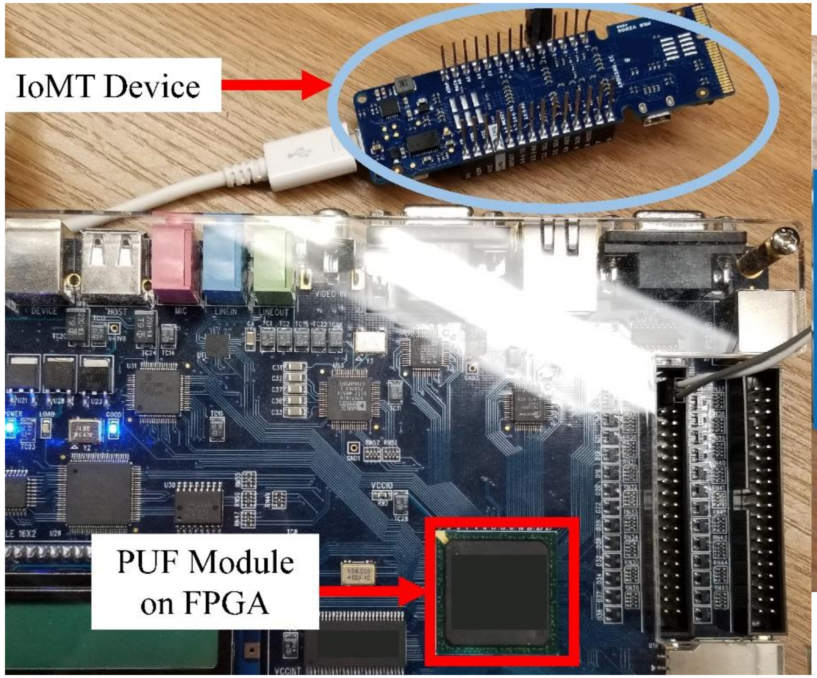
- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



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

IoMT Security – Our Proposed PMsec



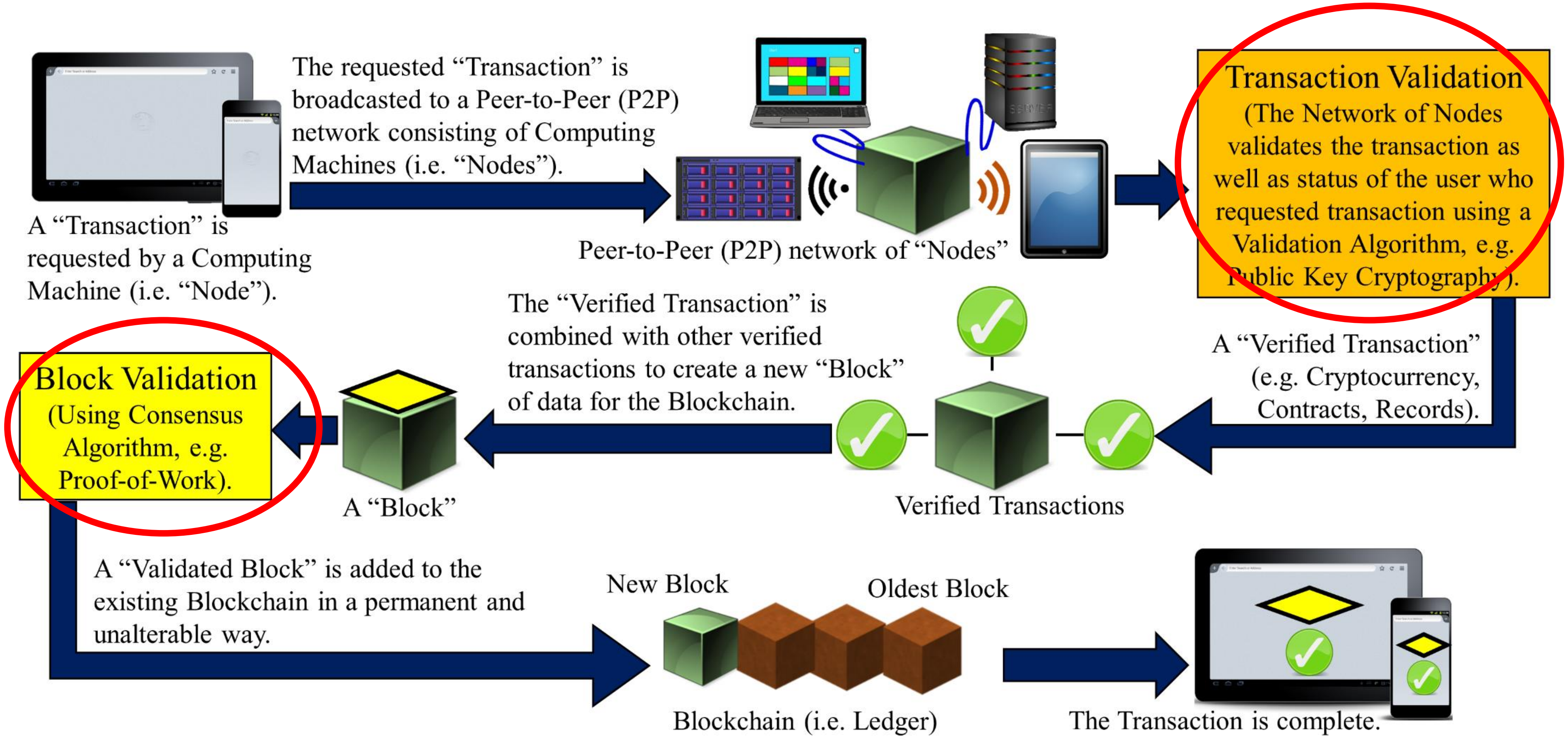
Average Power Overhead – 200 μW

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

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

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

Blockchain Challenges - Energy

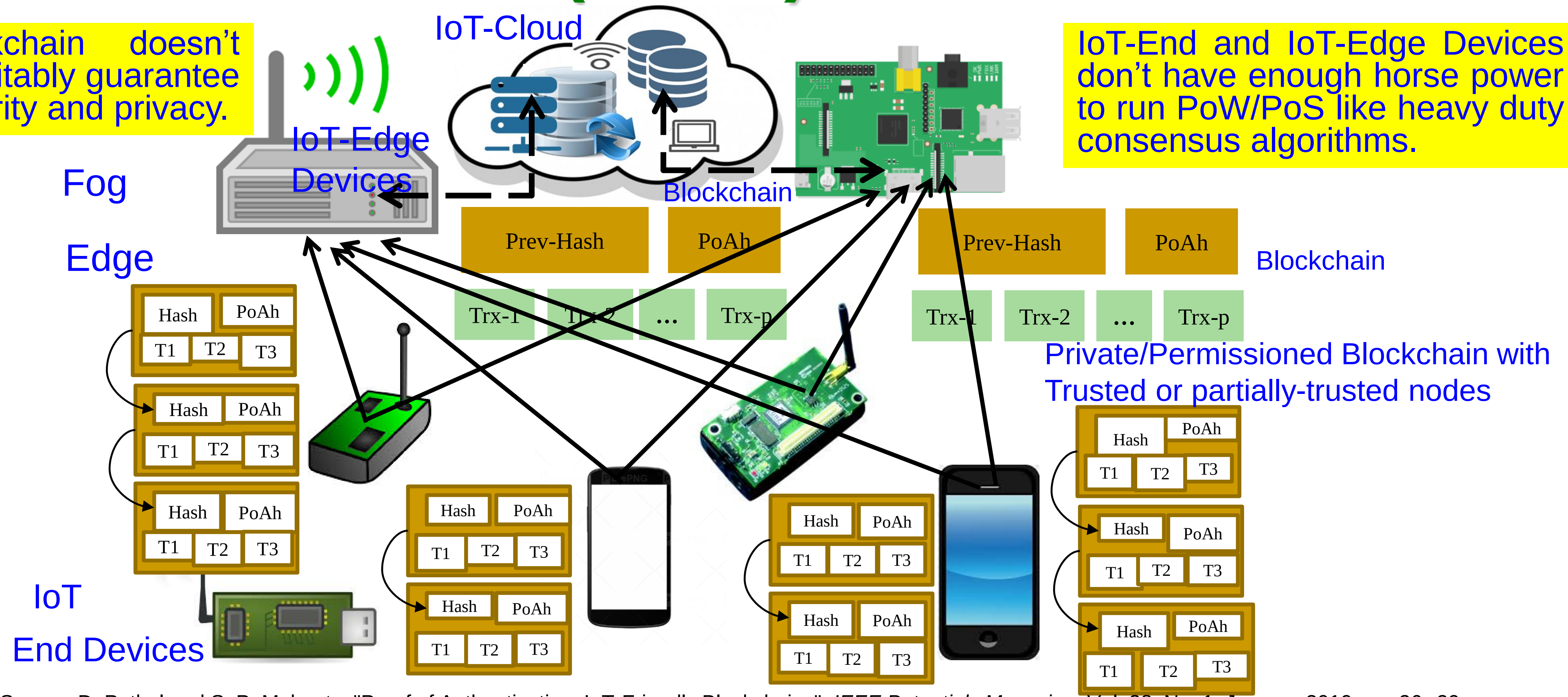


Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

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

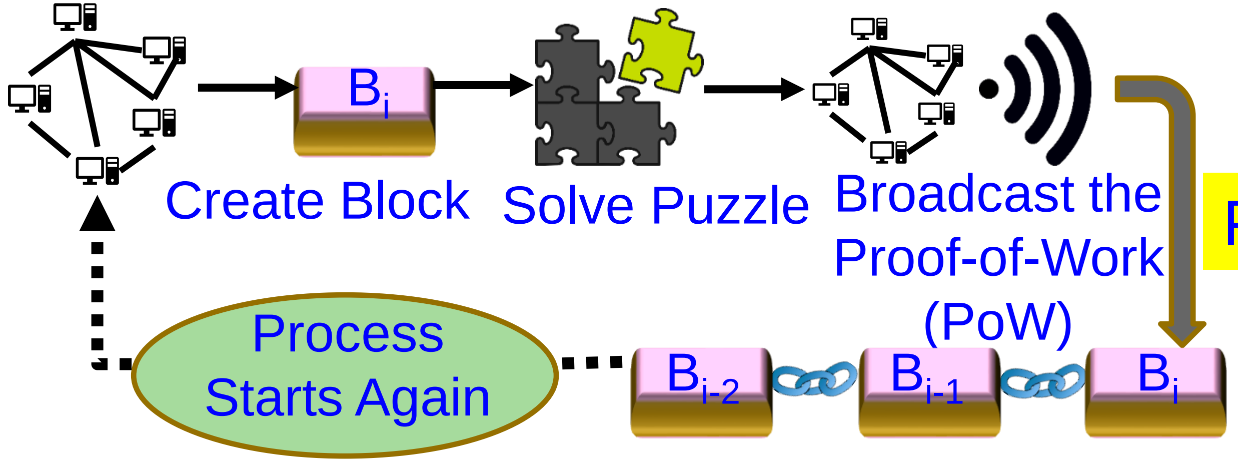
Blockchain doesn't inheritably guarantee security and privacy.

IoT-End and IoT-Edge Devices don't have enough horse power to run PoW/PoS like heavy duty consensus algorithms.



Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

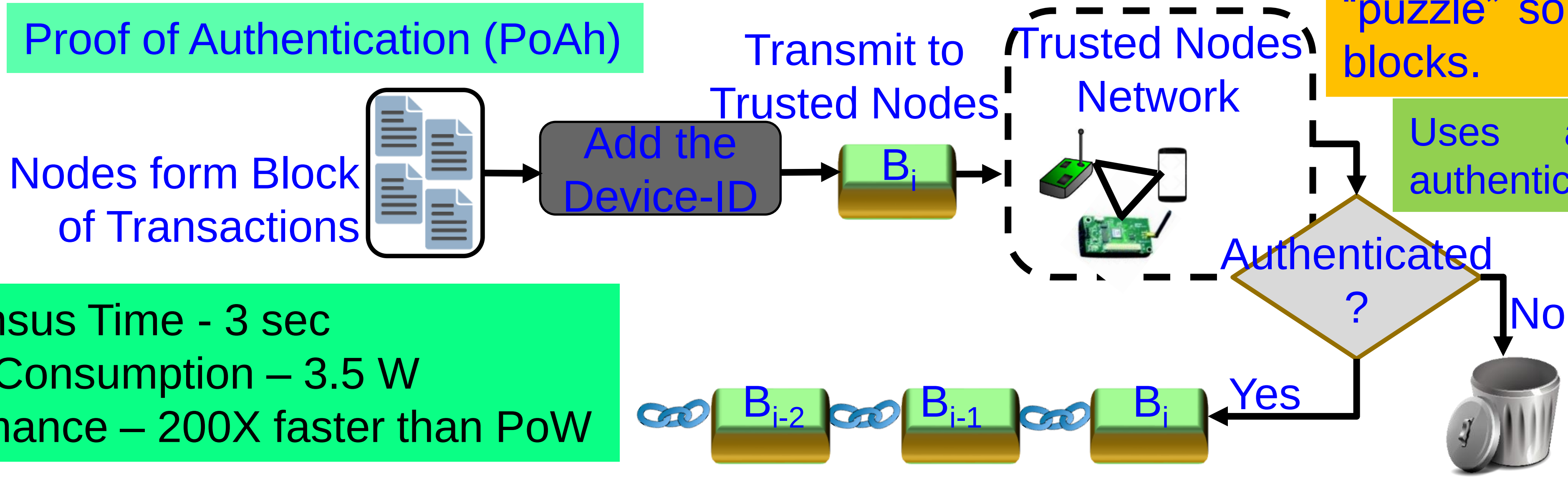
Our Proof-of-Authentication (PoAh)



Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.

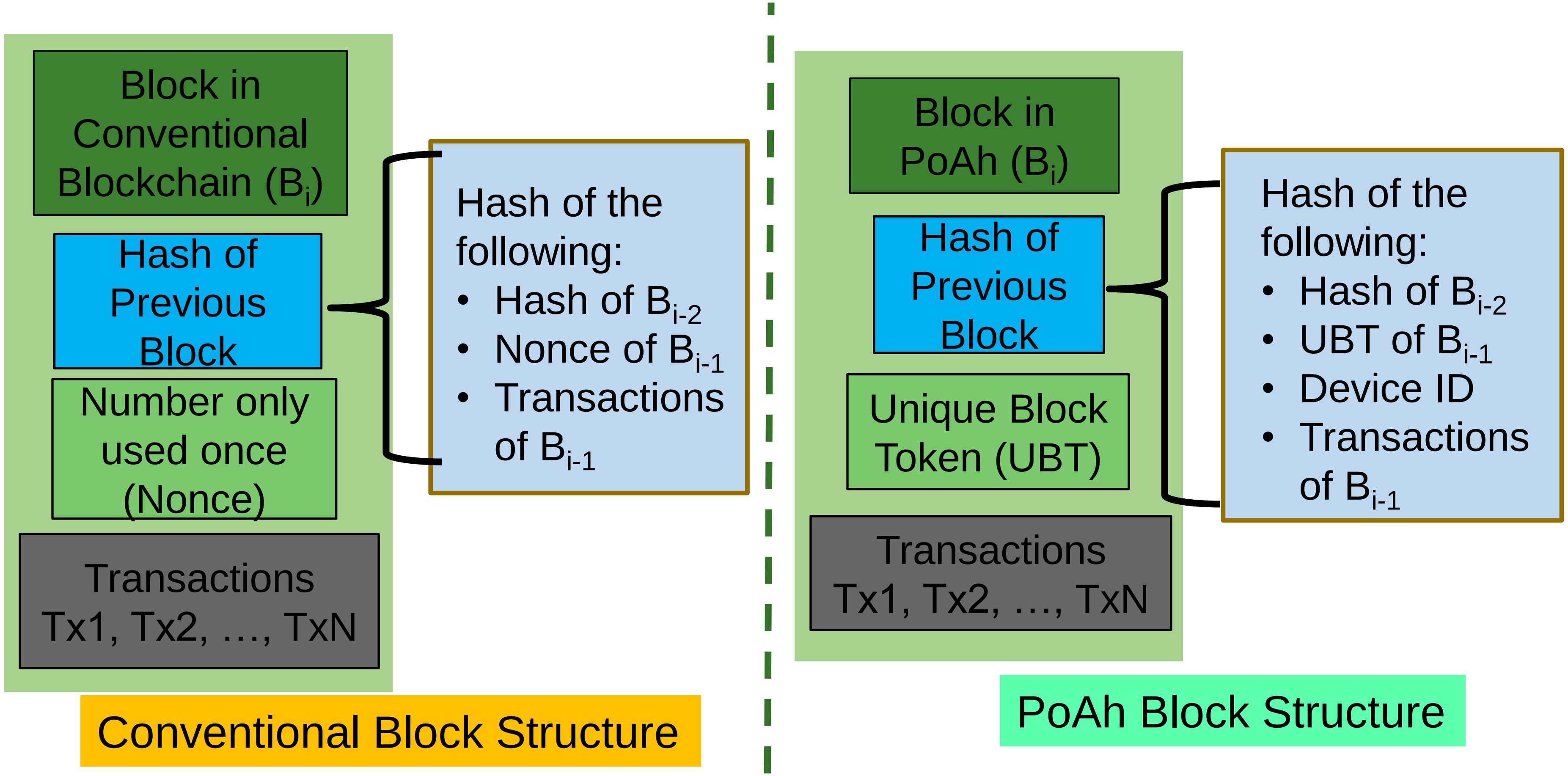
Uses a cryptographic authentication mechanism.



Consensus Time - 3 sec
Power Consumption – 3.5 W
Performance – 200X faster than PoW

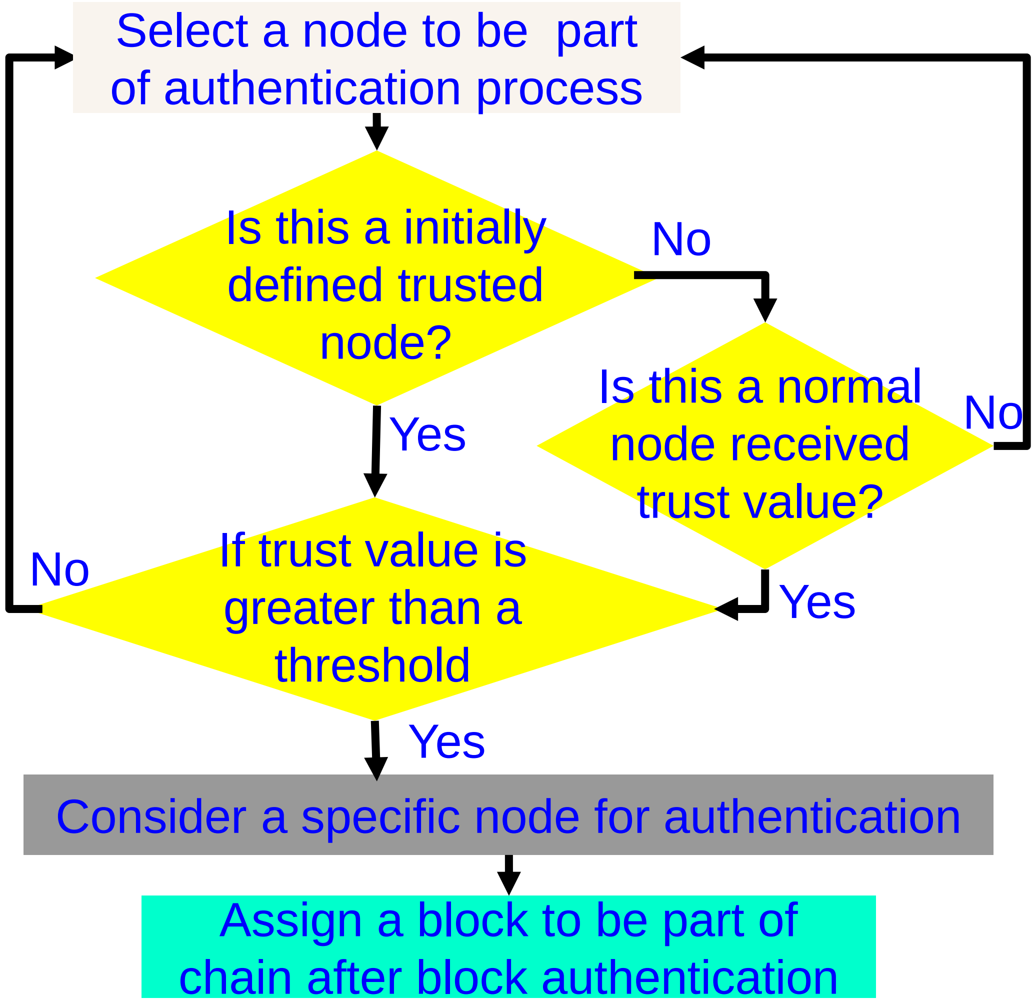
Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

Our PoAh-Chain: Proposed New Block Structure



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

Our PoAh: Authentication Process

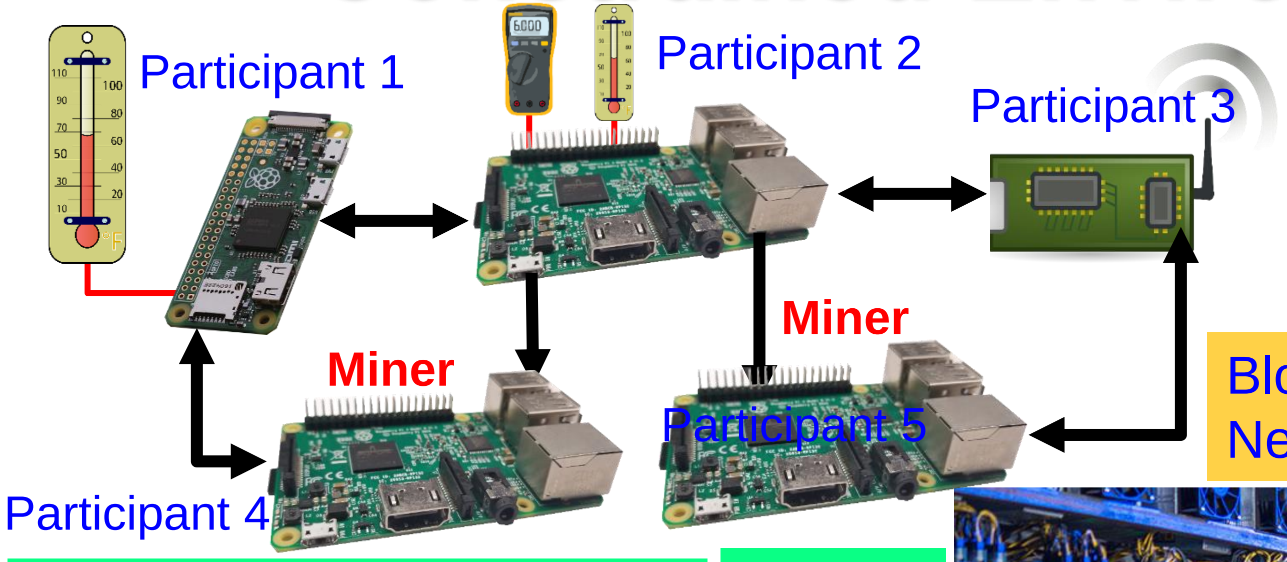


Steps to find a Trusted Node which will Authenticate a Block.

Algorithm 1: PoAh Block Authentication

Provided:
All nodes in the network follow SHA-256 Hash
Individual node has Private (PrK) and Public key (PuK)
Steps:
(1) Nodes combine transactions to form blocks
    $(Trx^{+}) \rightarrow$ blocks
(2) Blocks sign with own private key
    S_{PrK} (block) → broadcast
(3) Trusted node verifies signature with source public key
    V_{PuK}(block) → MAC Checking
(4) If (Authenticated)
    Block||PoAh(ID) → broadcast
    H(block) → Add blocks into chain
(5) Else
    Drop blocks
(6) GOTO (Step-1) for next block

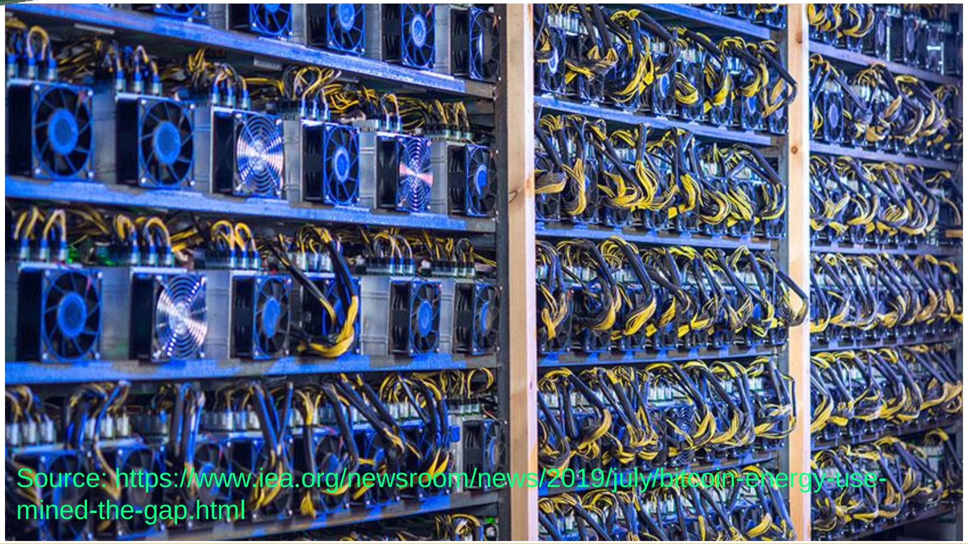
Our PoAh-Chain Runs in Resource Constrained Environment



Our PoAh-Chain Runs here

3-5 W

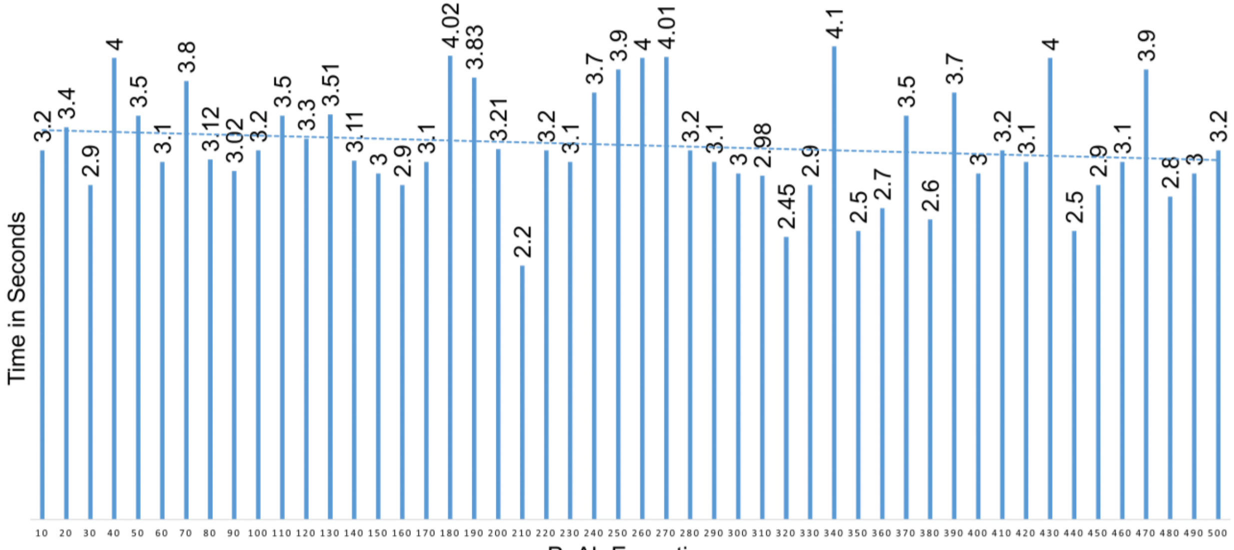
Blockchain using PoW Needs Significant Resource



500,0000 W

Our PoAh is 200X Faster than PoW While Consuming a Very Minimal Energy

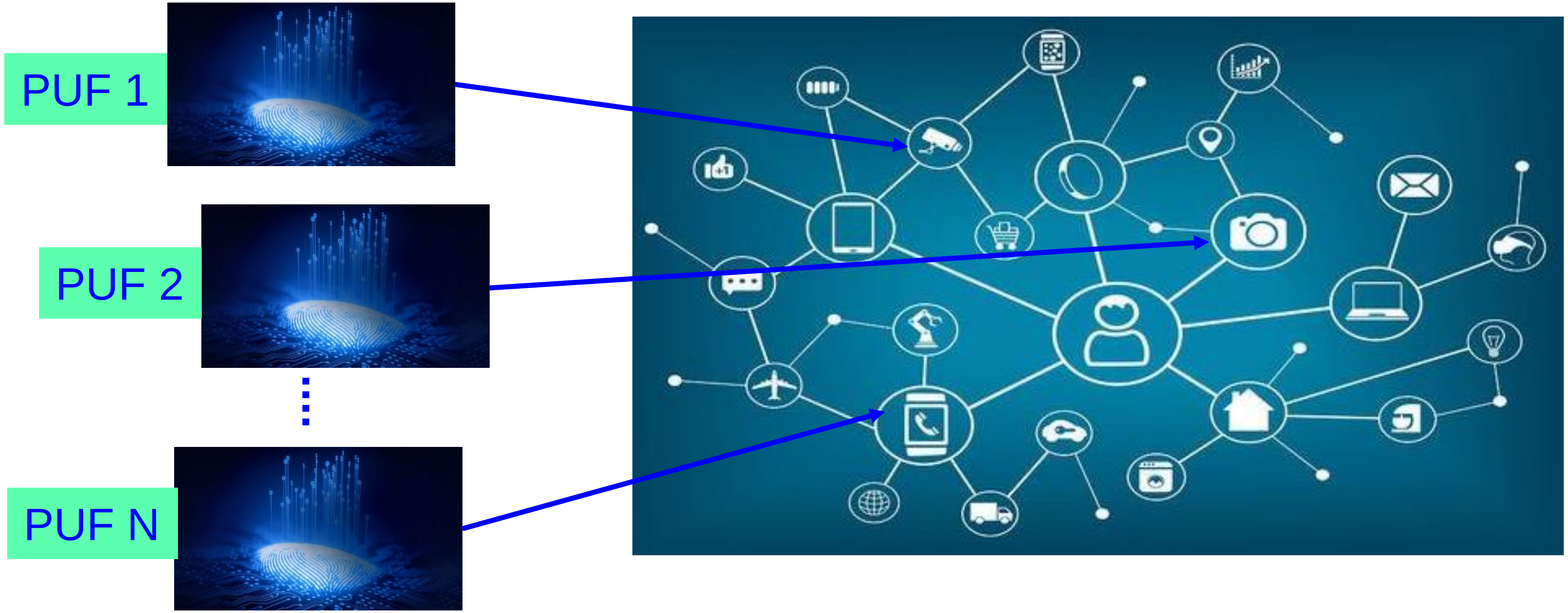
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



PoAh Execution for 100s of Nodes

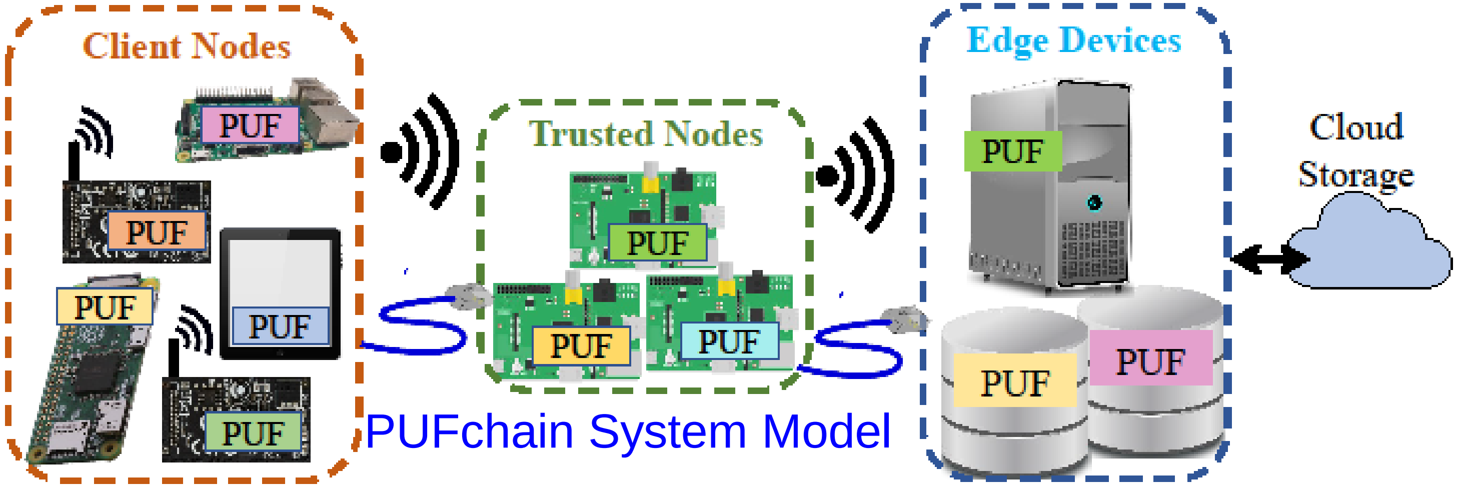
Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

We Proposed World’s First Hardware-Integrated Blockchain (PUFchain) that is Scalable, Energy-Efficient, and Fast



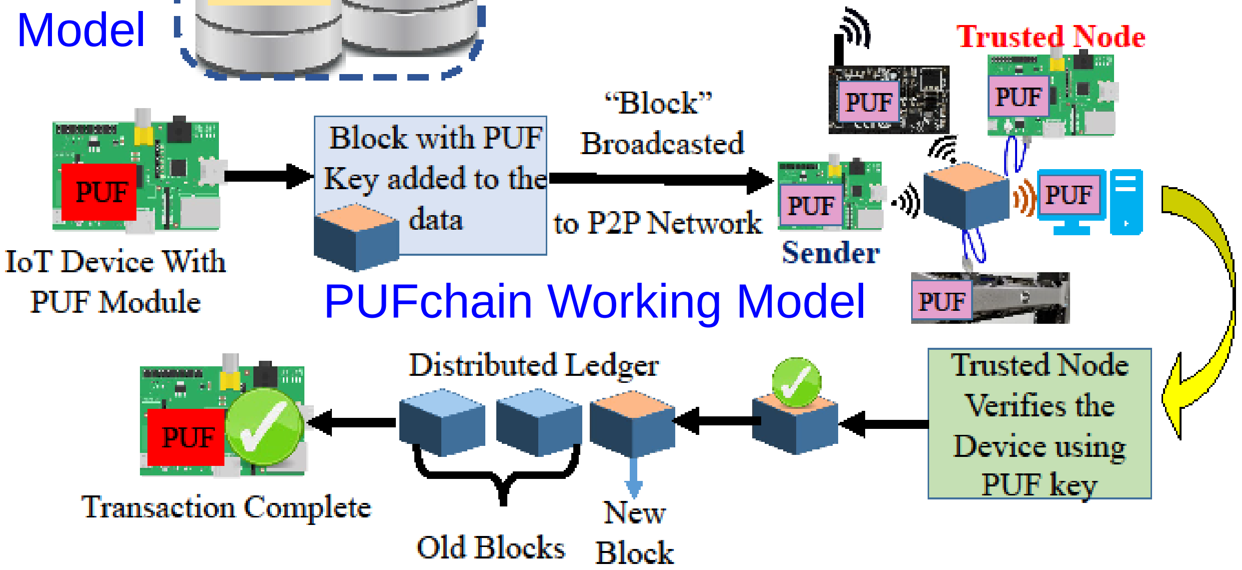
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security



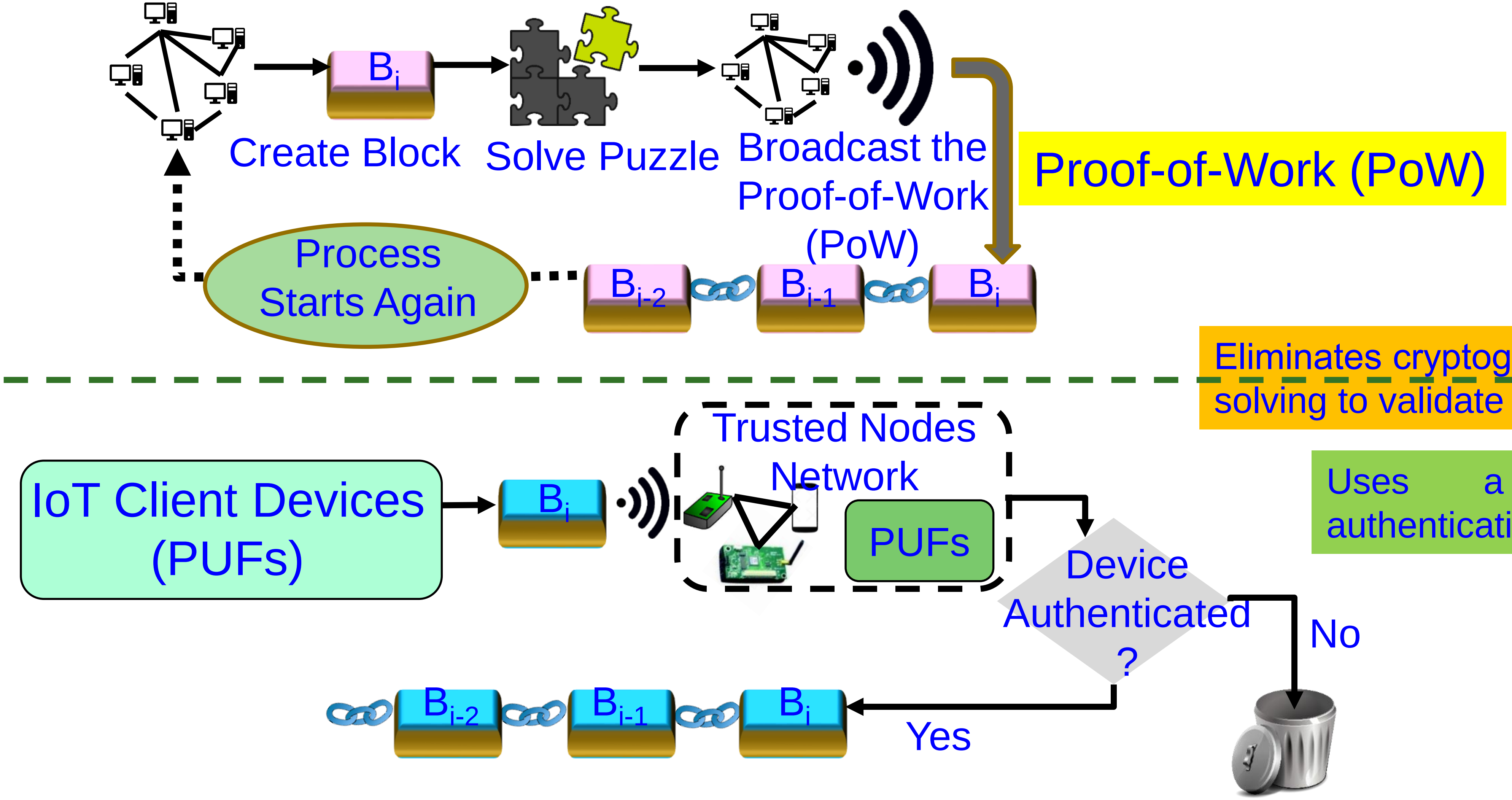
PUFchain Working Model

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

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

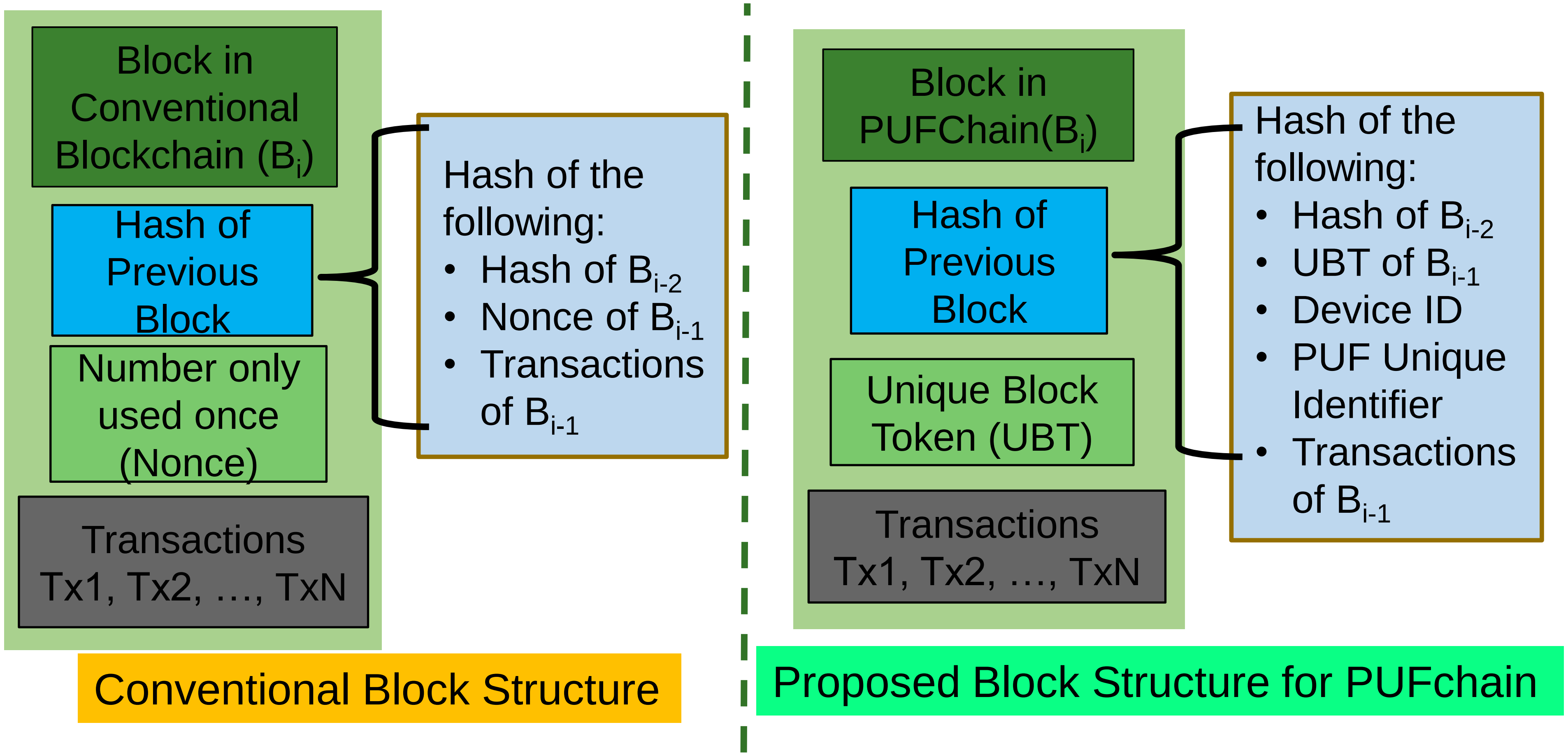
Our Proof-of-PUF-Enabled-Authentication (PoP)



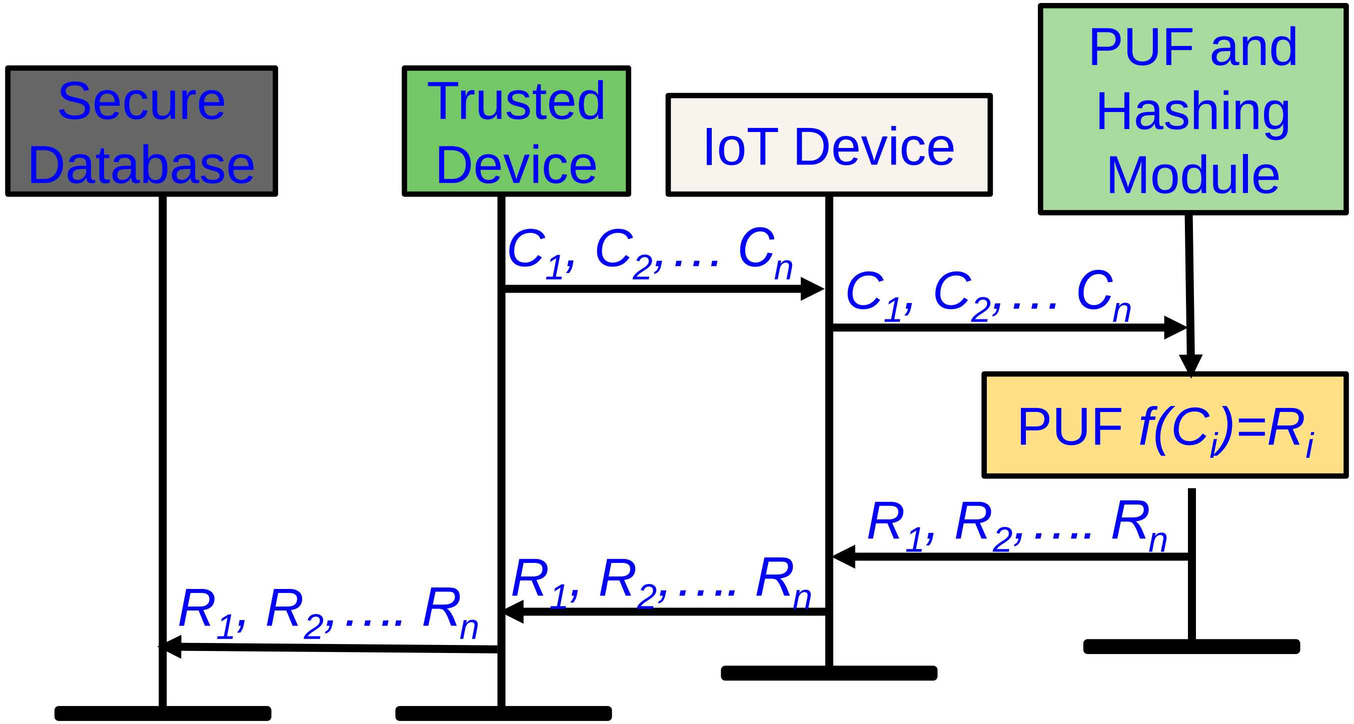
Eliminates cryptographic “puzzle” solving to validate blocks.

Uses a PUF-based authentication mechanism.

PUFchain: Proposed New Block Structure



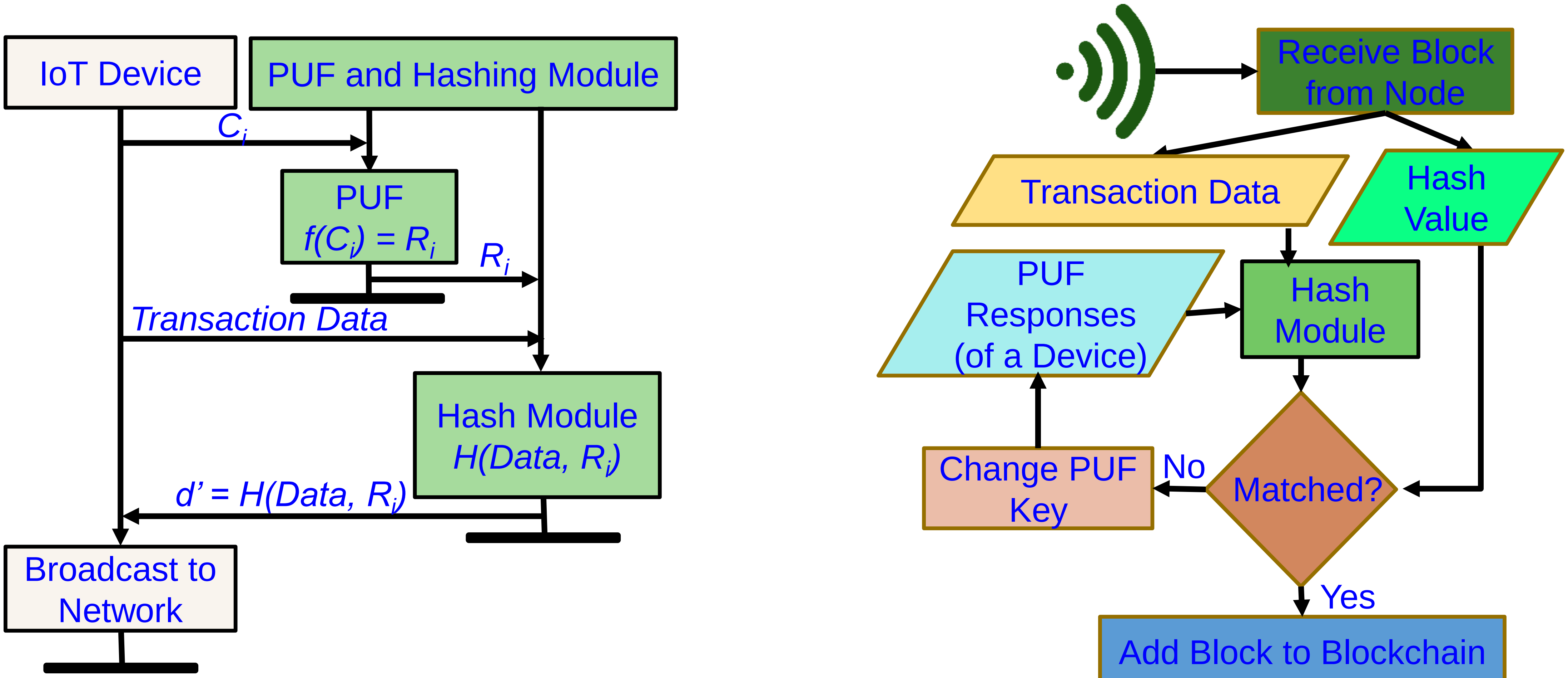
PUFchain: Device Enrollment Steps



Device Enrollment Steps

Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

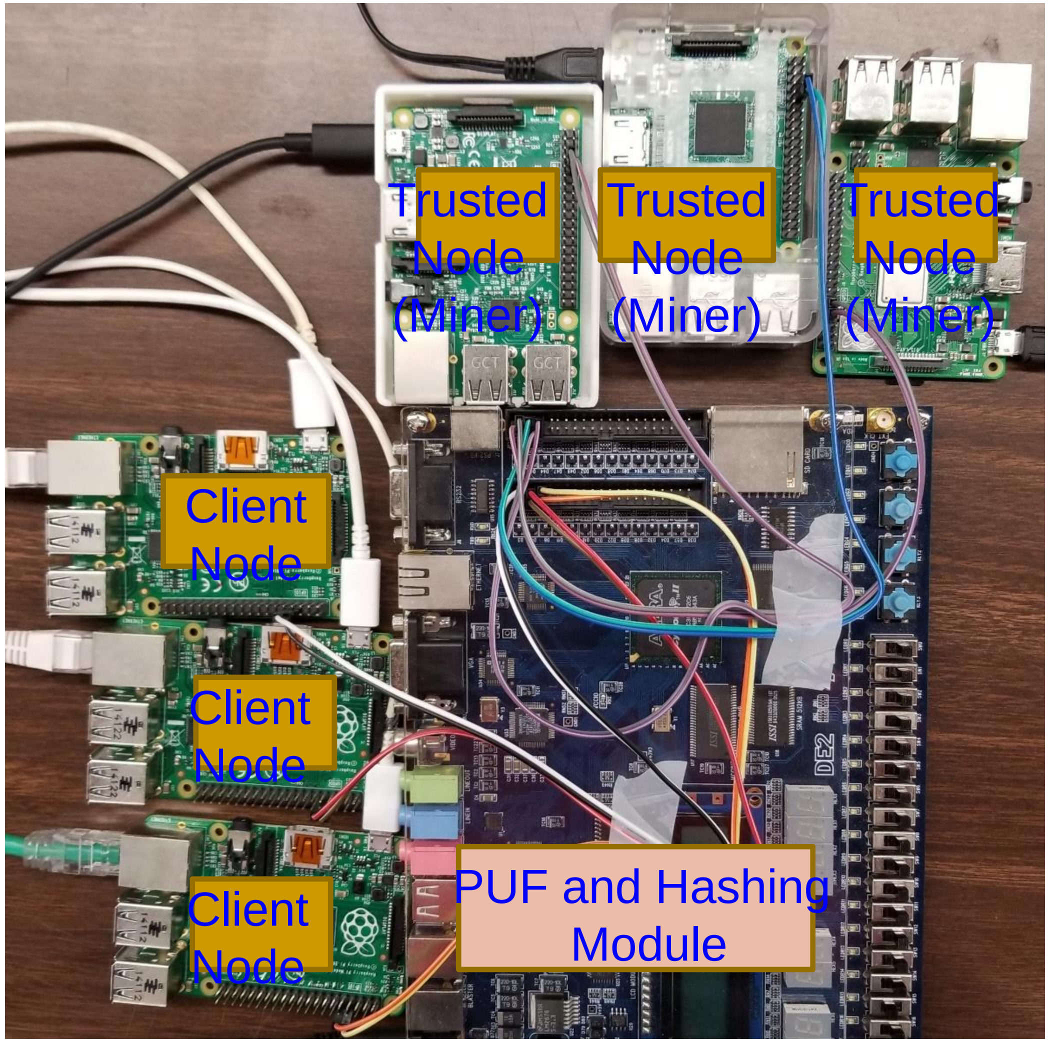
Proof-of-PUF-Enabled-Authentication (PoP)



Steps for Transactions Initiation

Steps for Device Authentication

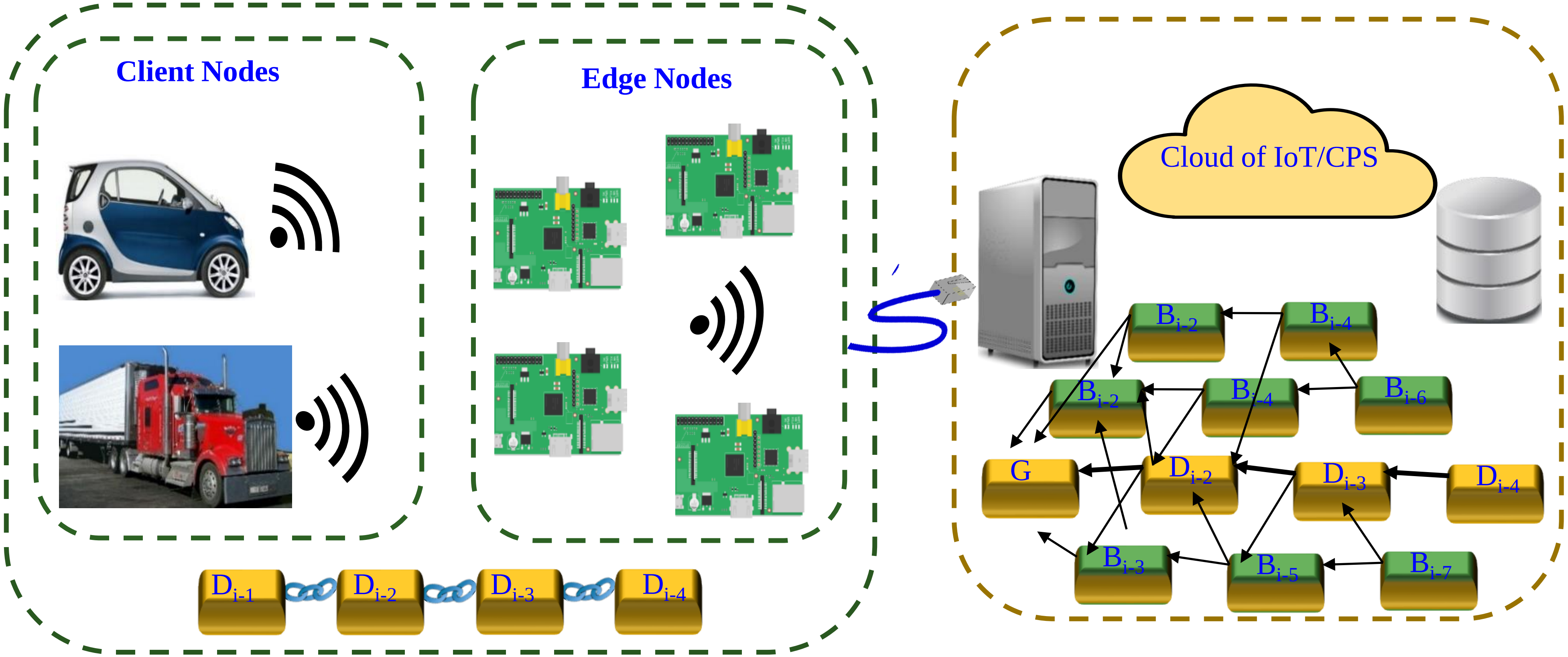
Our PoP is 1000X Faster than PoW



PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

Our Multi-Chain Technology to Enhance Blockchain Scalability



(a) Nodes-Chain (b) Multi-Blockchains

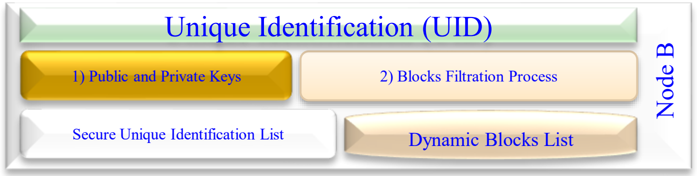
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

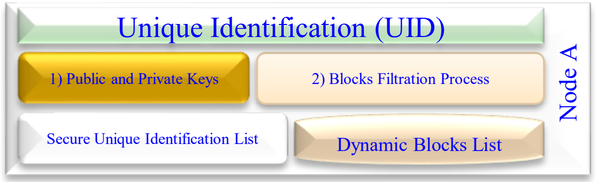
A Perspective of BC, Tangle Vs Our Multichain

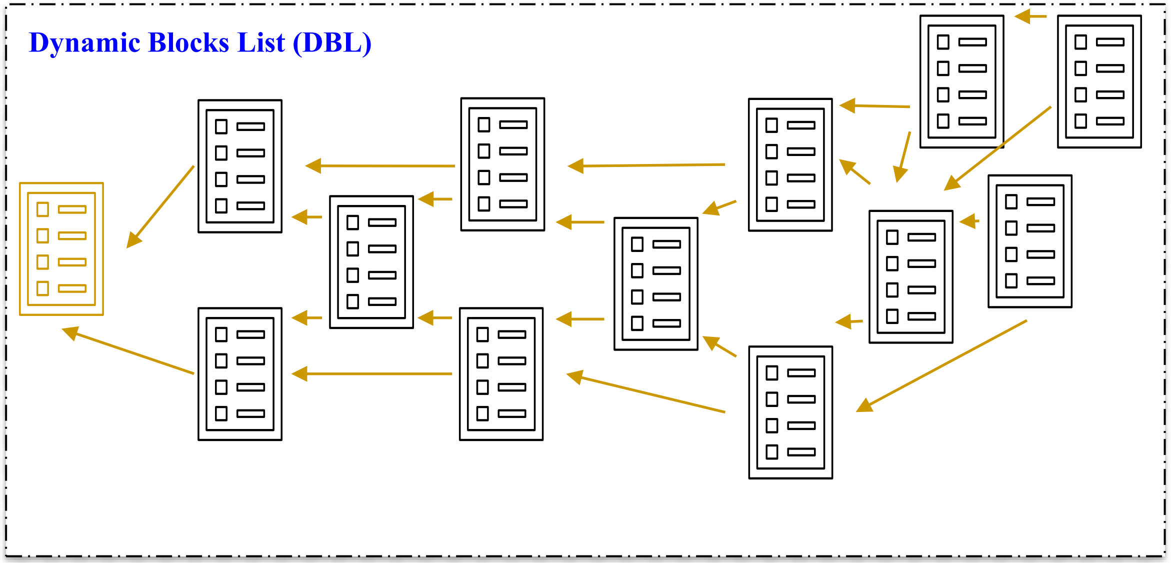
Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRA (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions hash	• DAG linked List. • Block of transactions. • Reduced block.
Validation	Mining	Authentication	Mining	Virtual Voting (witness)	Authentication
Type of validation	Miners	Trusted Nodes	Transactions	Containers	All Nodes
Ledger Requirement	Full ledger required	Full ledger required	Portion based on longest and shortest paths.	Full ledger required	Portion based on authenticators' number
Cryptography	Digital Signatures	Digital Signatures	Quantum key signature	Digital Signatures	Digital Signatures
Hash function	SHA 256	SHA 256	KECCAK-384	SHA 384	SCRYPT
Consensus	Proof of Work	Cryptographic Authentication	Proof of Work	aBFT	Predefined UID
Numeric System	Binary	Binary	Trinity	Binary	Binary
Involved Algorithms	HashCash	No	• Selection Algorithm • HashCash	No	BFP
Decentralization	Partially	Partially	Fully	Fully	Fully
Appending Requirements	Longest chain	One chain	Selection Algorithm	Full Randomness	Filtration Process
Energy Requirements	High	Low	High	Medium	Low
Node Requirements	High Resources Node	Limited Resources Node	High Resources Node	High Resources Node	Limited Resources Node
Design Purpose	Cryptocurrency	IoT applications	IoT/Cryptocurrency	Cryptocurrency	IoT/CPS applications

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020.

McPoRA based MultiChain -- Components







Secure Unique Identification List (SUIL)

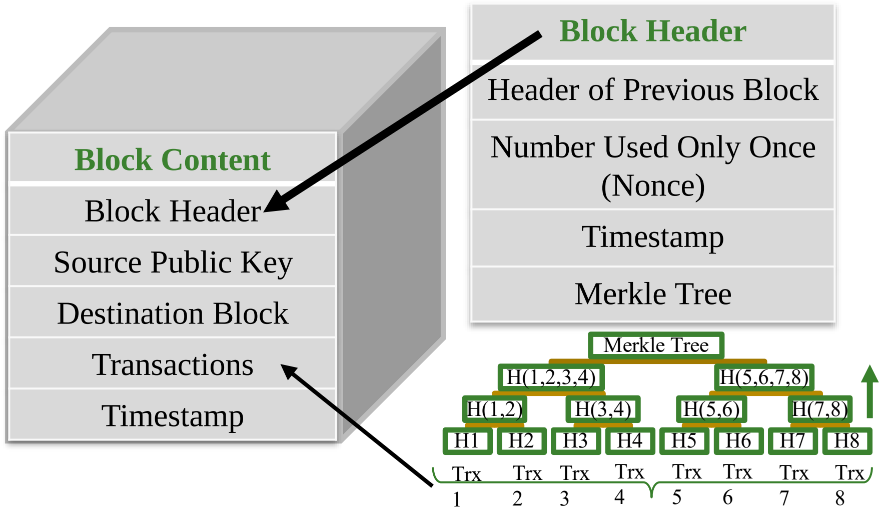
Secure IDs' file consists of all active Nodes joined the Private network.

Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique Identification (UID)

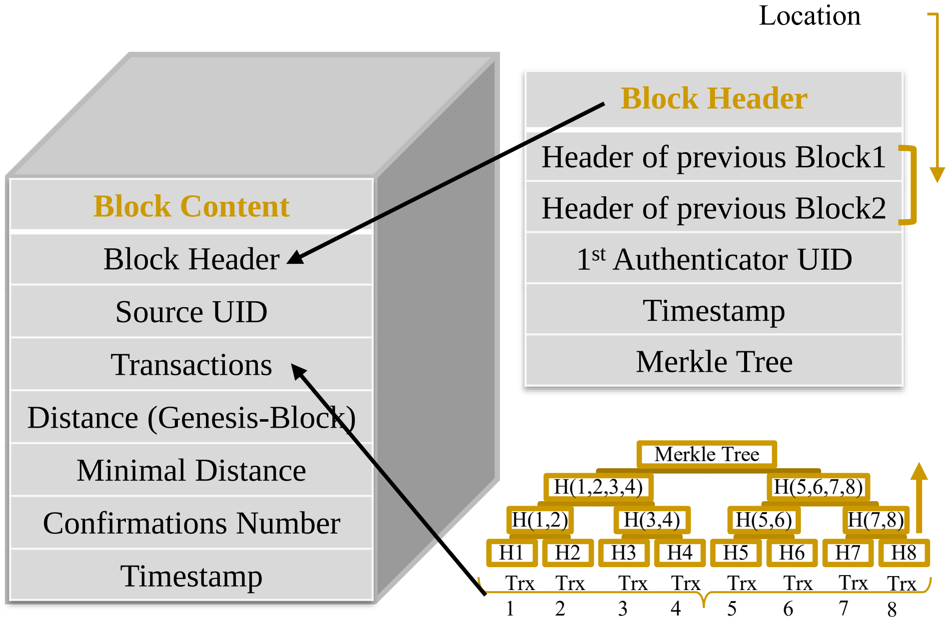
Consensus Time – 0.7 sec (Avg)
Power Consumption – 3.5 W
Performance – 4000X faster than PoW

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

Block Structure in McPoRA



(a) For Traditional Blockchain

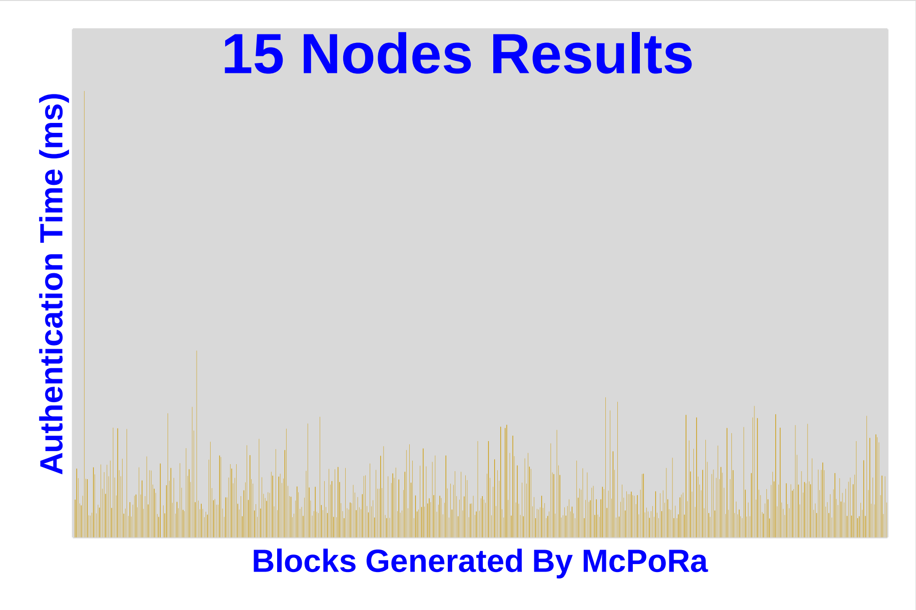


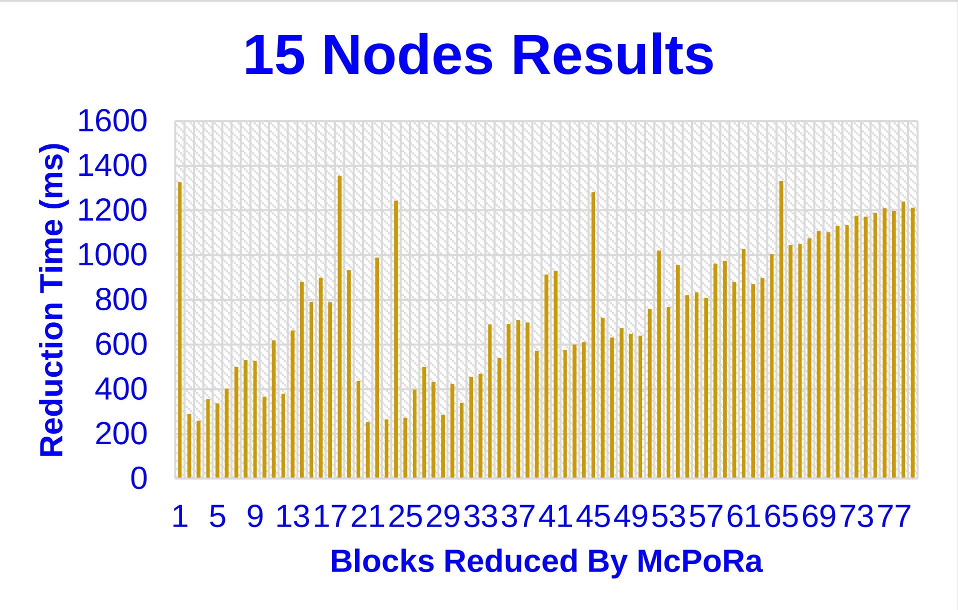
(b) For Proposed Post-Blockchain

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020

McPoRA – Experimental Results

Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.51	252.6
Maximum	35.14	1354.6
Average	3.97	772.53

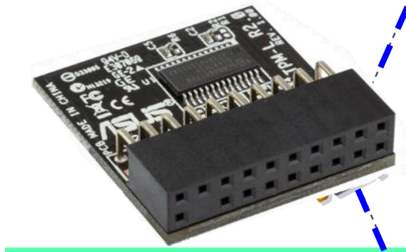




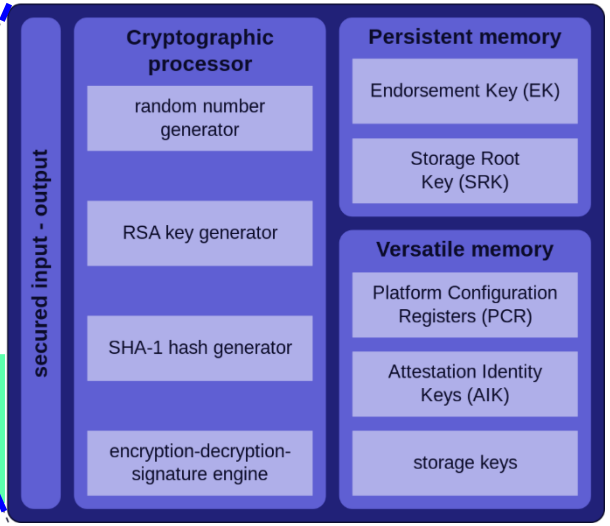
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

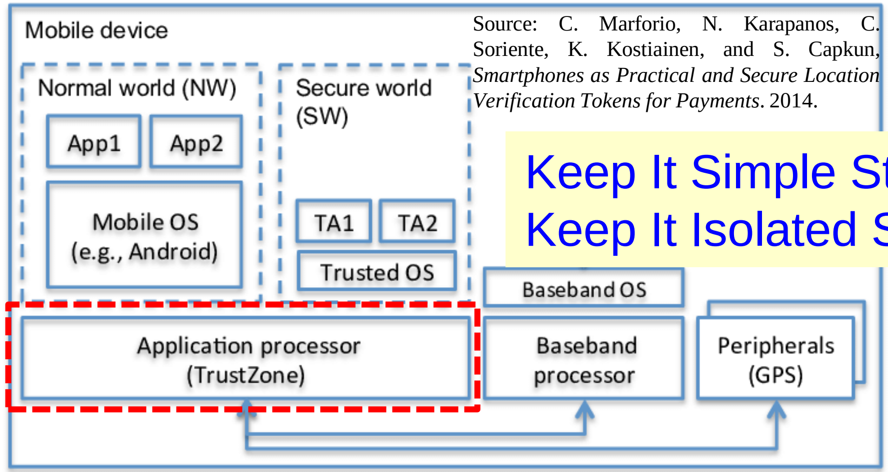
Hardware Security Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



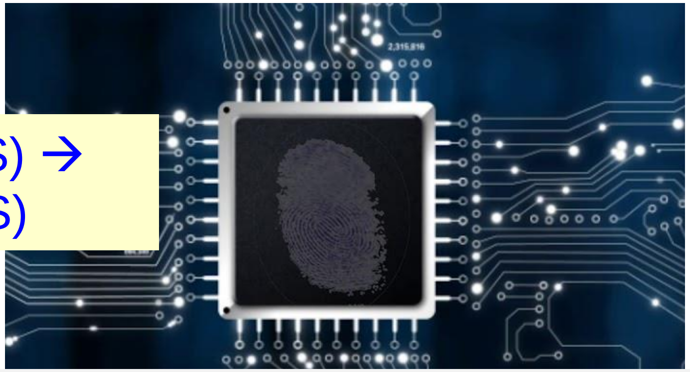
Trusted Platform Module (TPM)





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

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

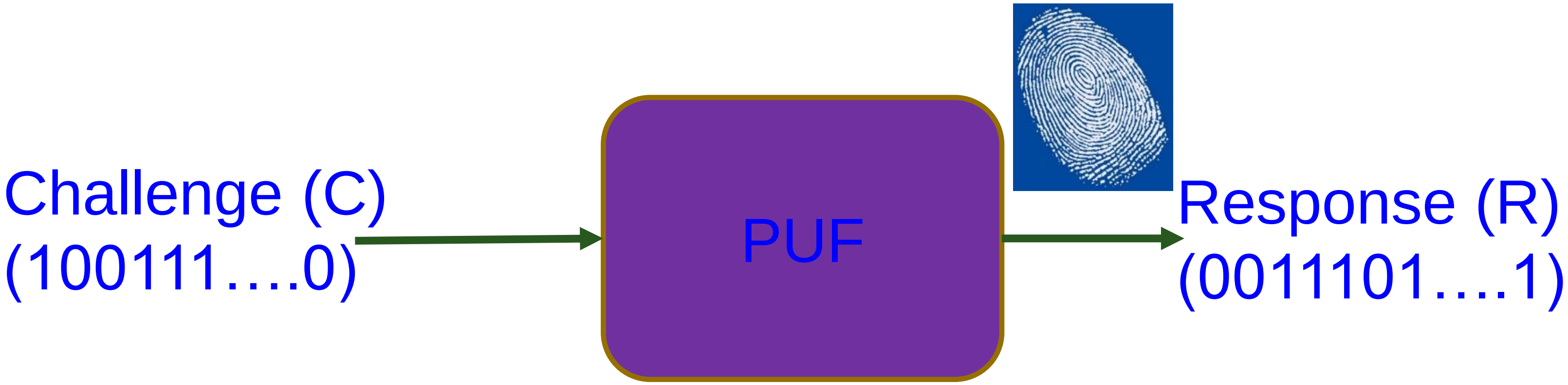


Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Physical Unclonable Functions (PUFs) - Principle

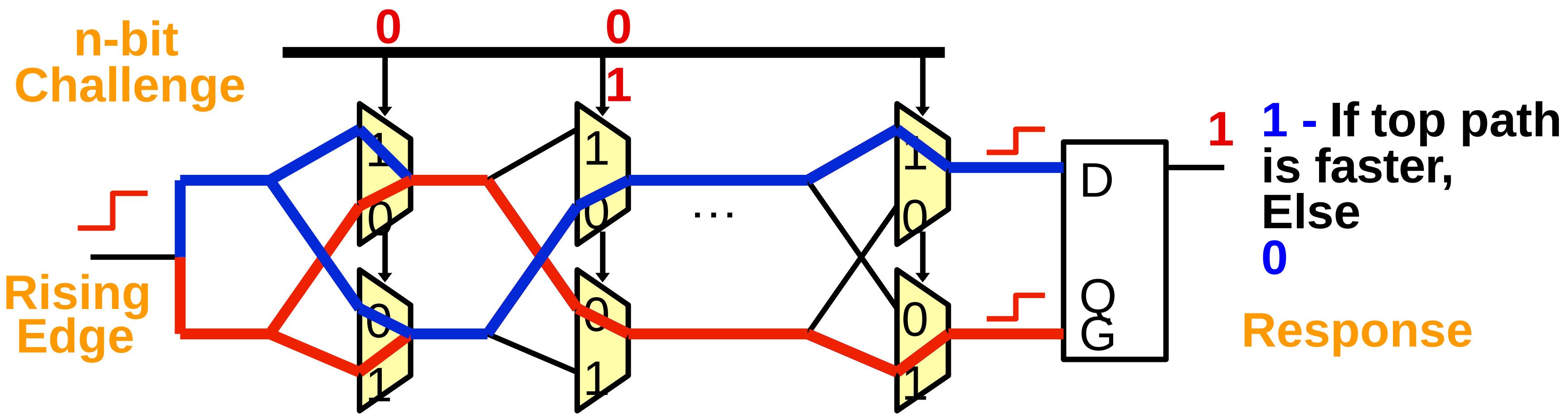
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

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

Principle of Generating Random Response using PUF

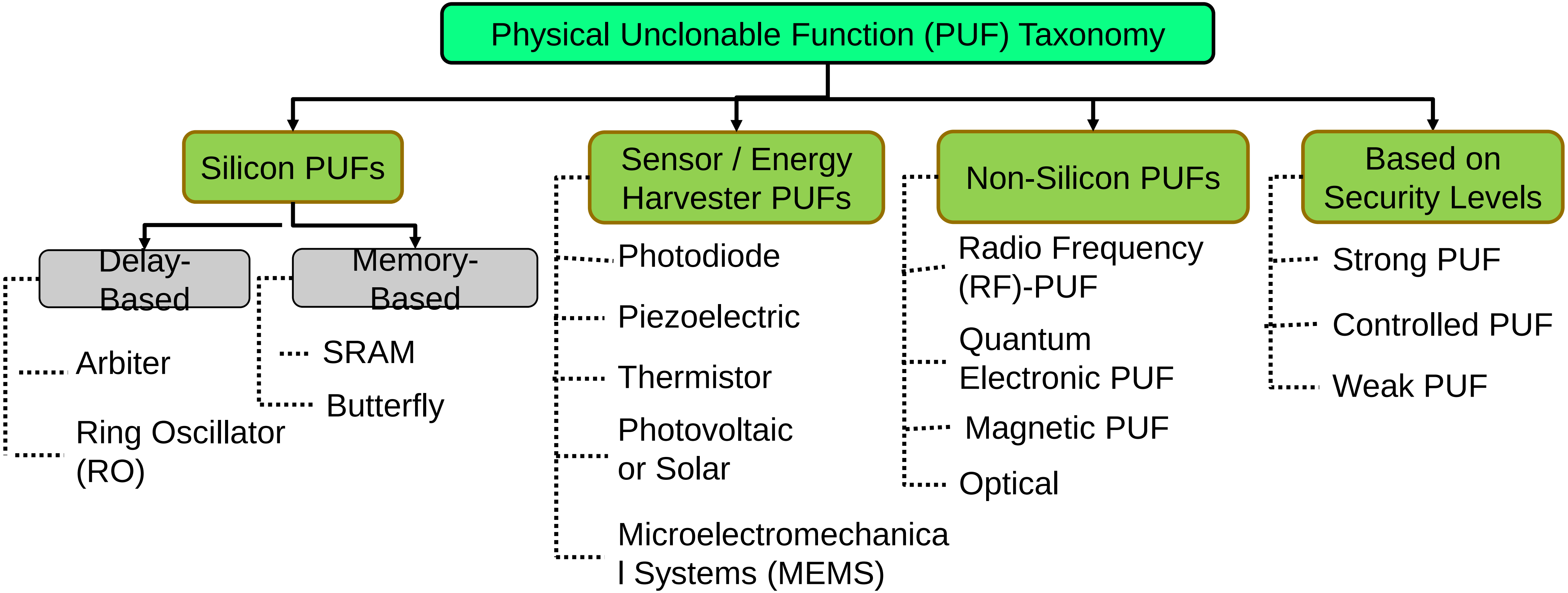


Compare two paths with an identical delay in design

- Random process variation determines which path is faster
- An arbiter outputs 1-bit digital response

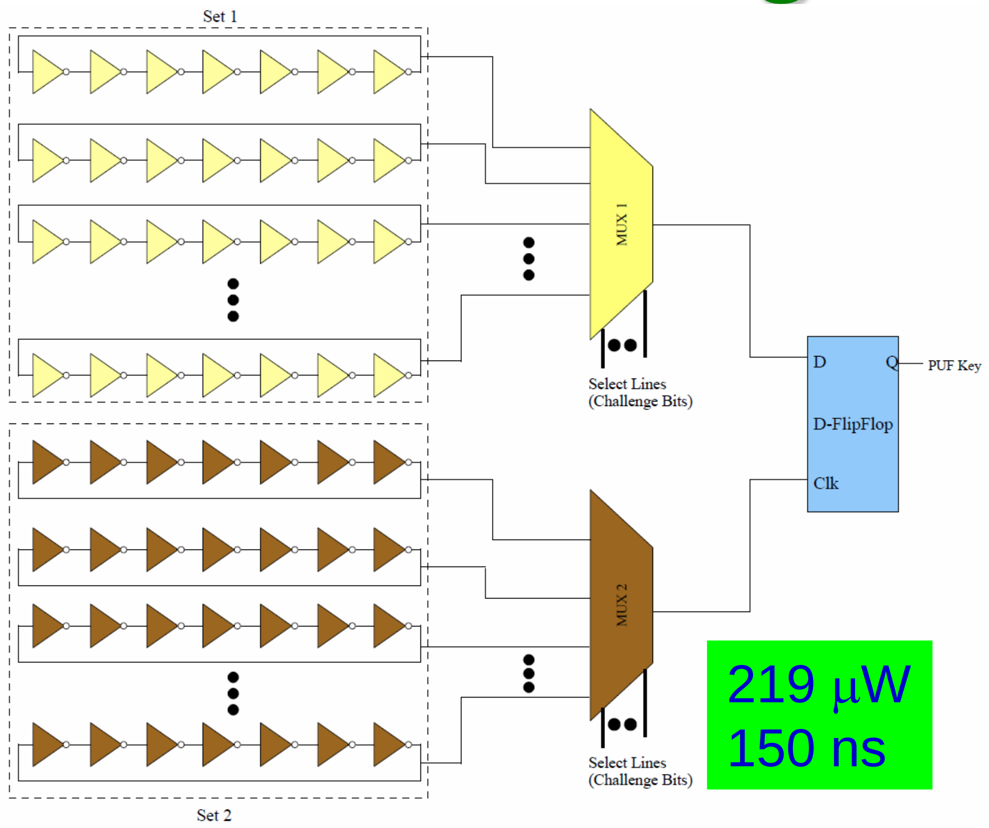
Source: Srini Devadas, Physical Unclonable Functions (PUFs) and Secure Processors, *Cryptographic Hardware and Embedded Systems*, 2009.

Physical Unclonable Function (PUF) Taxonomy

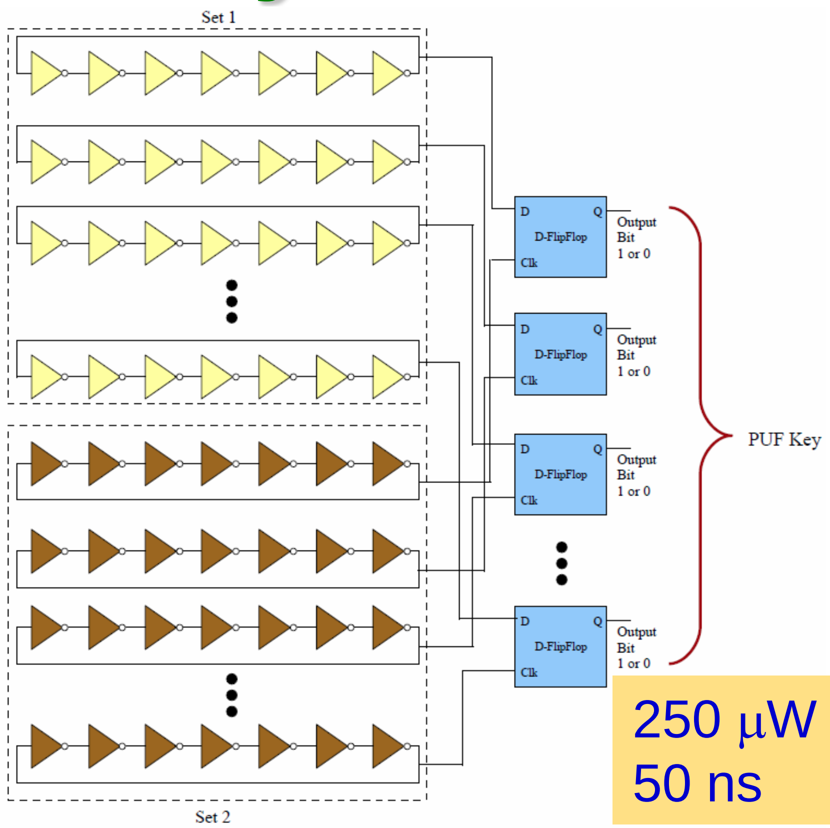


Source: H. Thapliyal, and S. P. Mohanty, "Physical Unclonable Function (PUF)-Based Sustainable Cybersecurity", Guest Editorial, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 79--80.

We Have Design a Variety of PUFs



219 µW
150 ns



250 µW
50 ns

Power Optimized Hybrid Oscillator Arbiter PUF

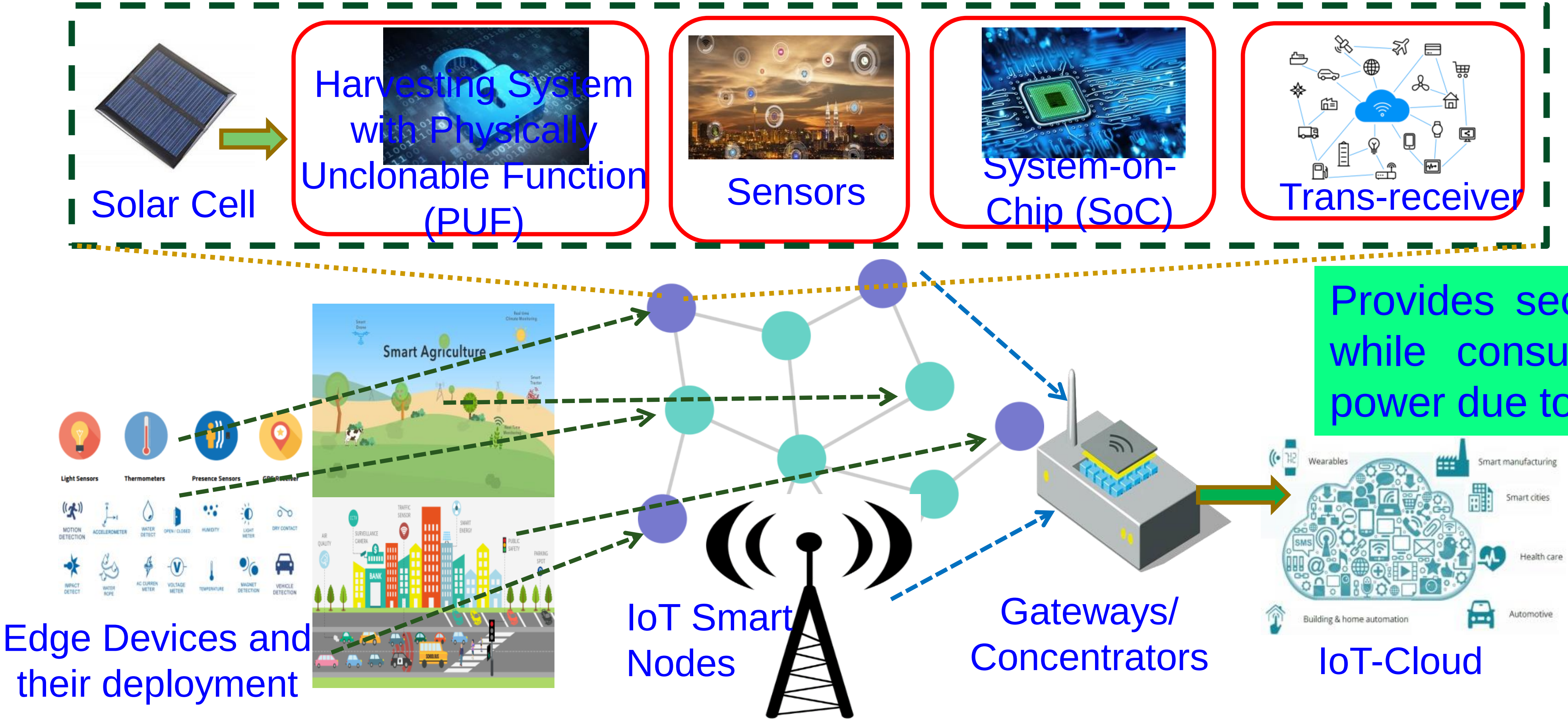
Suitable for Healthcare CPS

Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Transportation and Energy CPS

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.

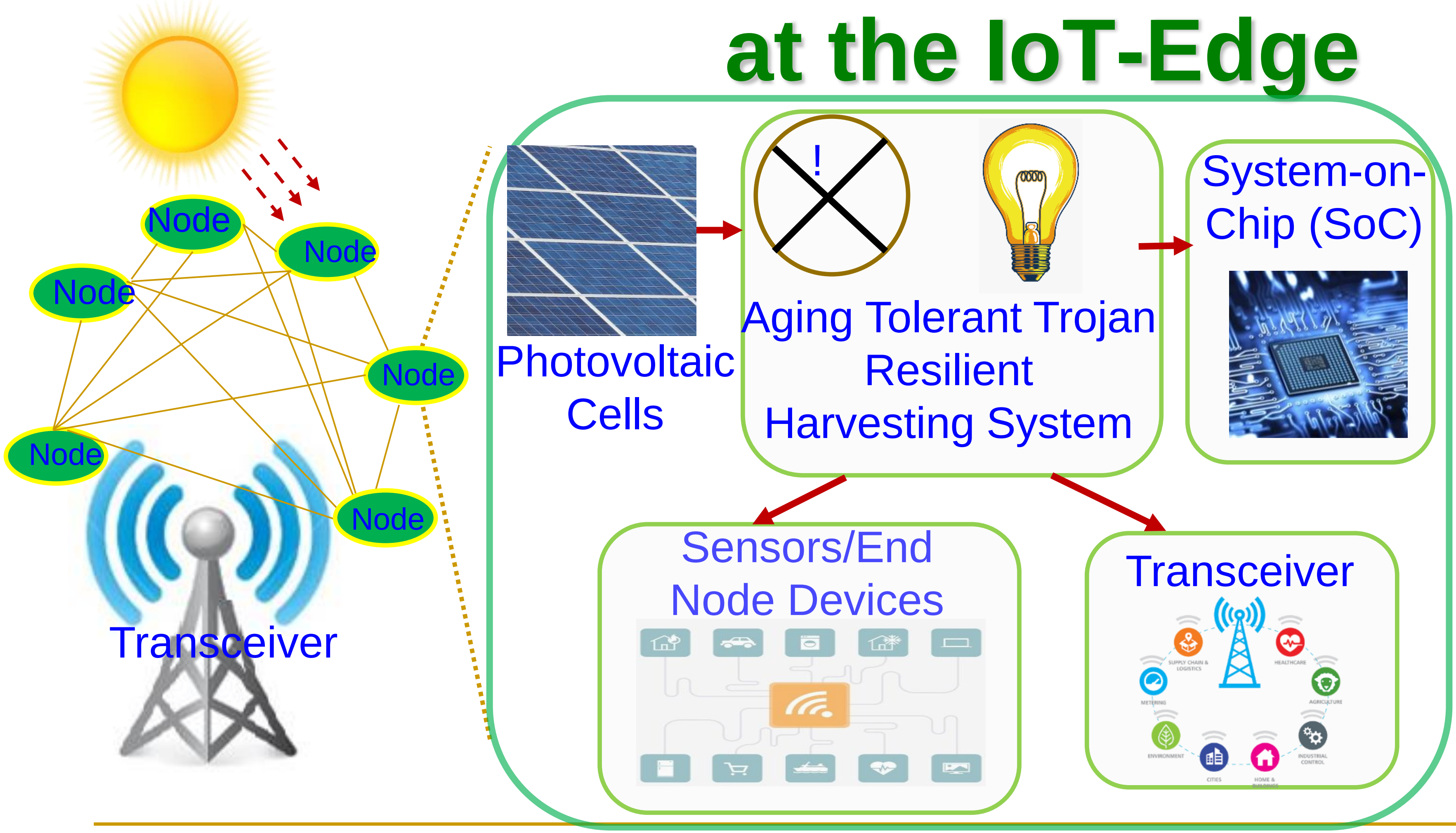
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge



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

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and **S. P. Mohanty**, "Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT", *IEEE Transactions on Sustainable Computing*, Vol. 6, No. 2, April 2021, pp. 320-333, doi: 10.1109/TSUSC.2020.2987616.

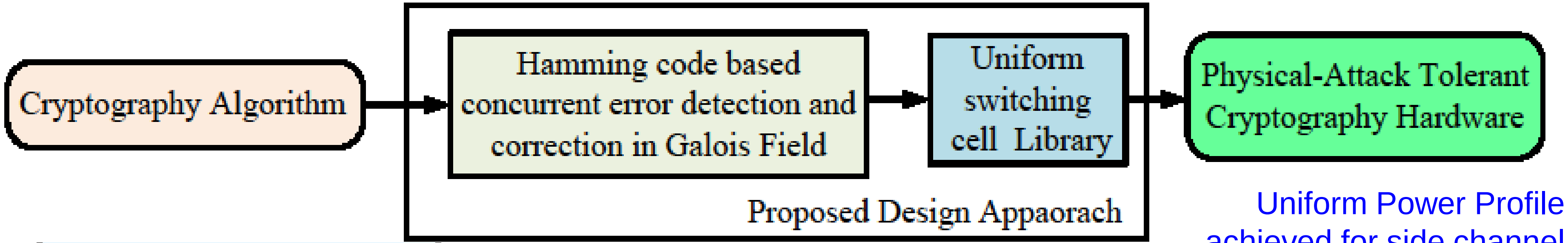
Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge



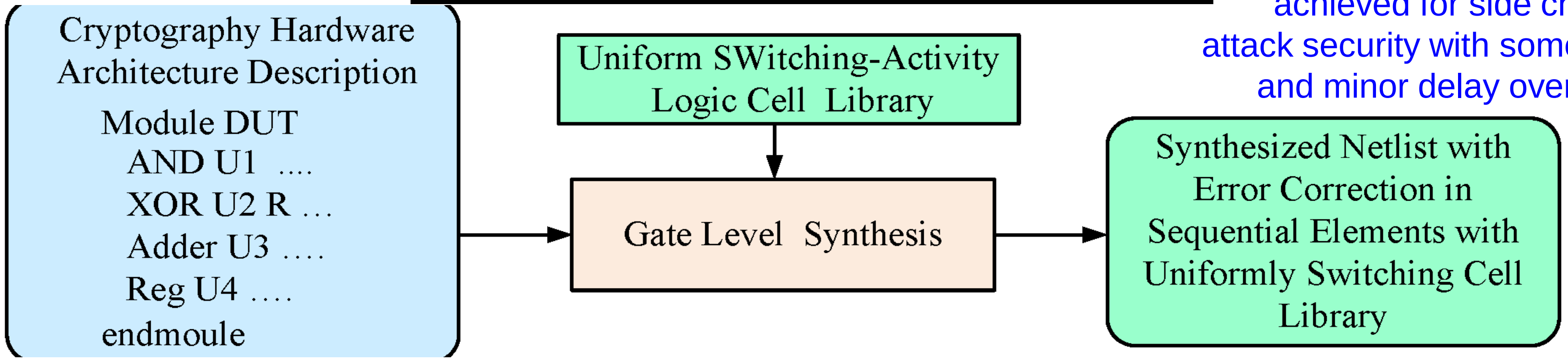
Provides security against analog-Trojan while consuming only 22μW power due to harvesting.

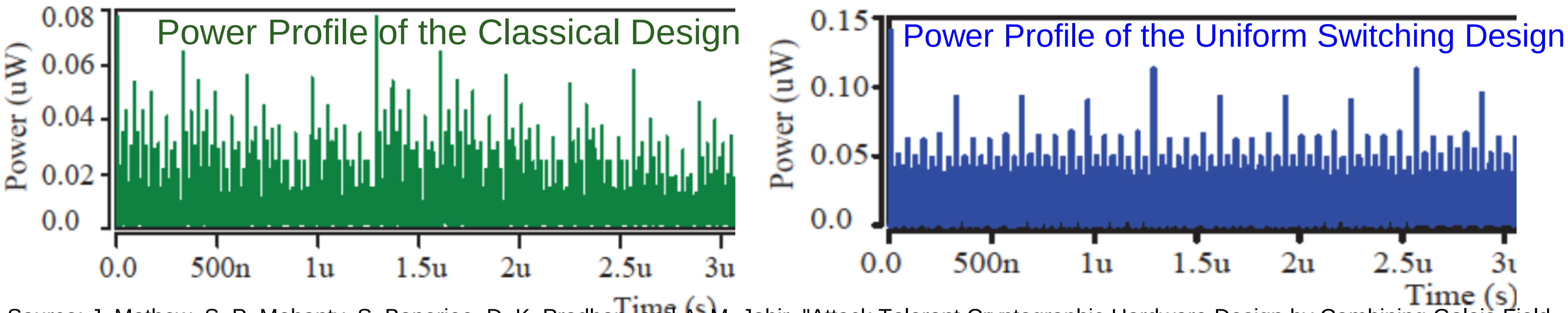
Source: S. K. Ram, S. R. Sahoo, B. B. Das, K. K. Mahapatra, and S. P. Mohanty, "Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Energy Harvesting System for Sustainable IoT in Smart Cities and Smart Villages", *arXiv Computer Science*, arXiv:2103.05615, March 2021, 24-pages.

Our SdD: Approach for DPA Resilience Hardware



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





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

Where to Store and Process Data for ML Modeling, and where to Execute ML models?

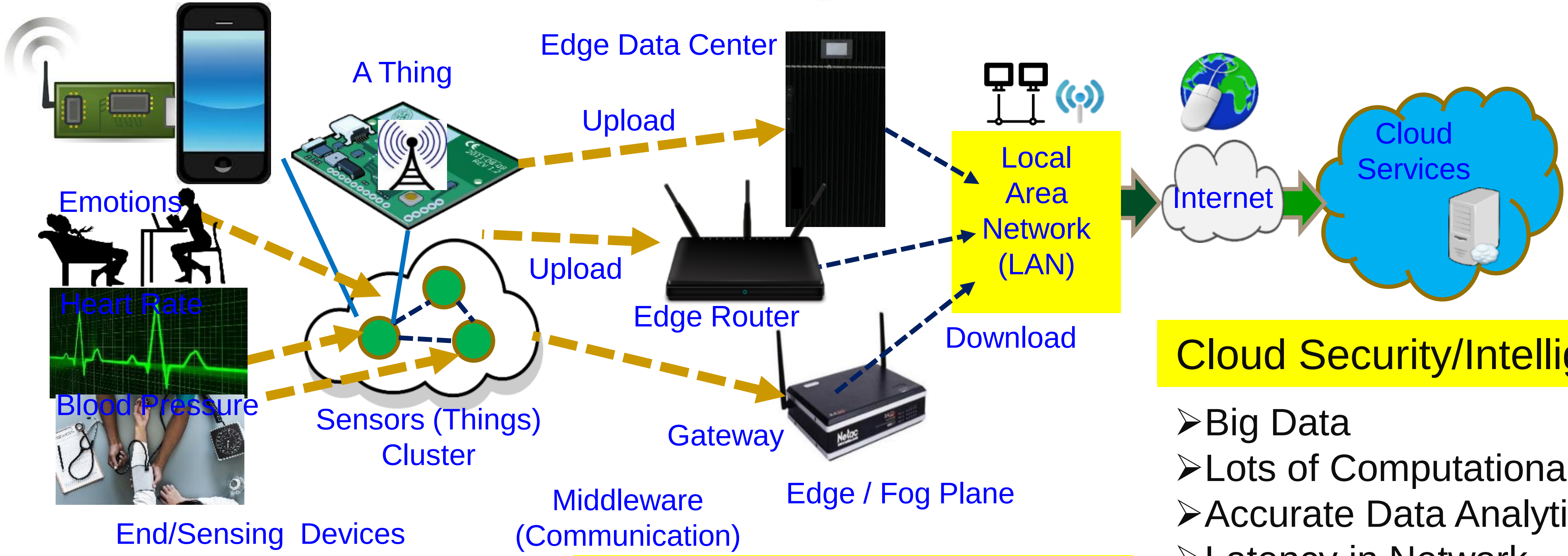
October 2016

Sensor, Edge, Fog, Cloud?

July 2018

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

CPS – IoT-Edge Vs IoT-Cloud



End Security/Intelligence

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

Edge Security/Intelligence

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

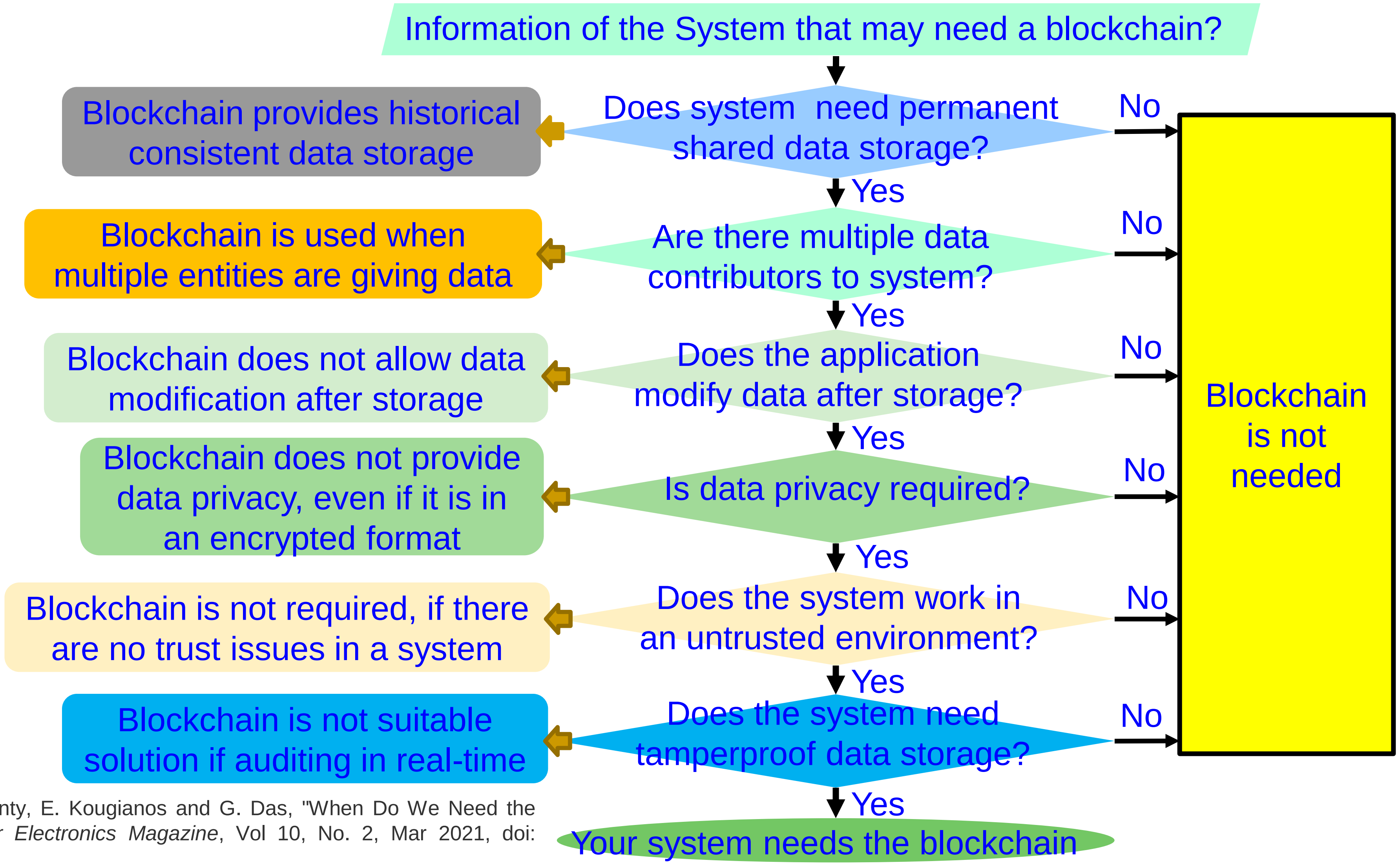
TinyML at End and/or Edge is key for smart villages.

Cloud Security/Intelligence

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

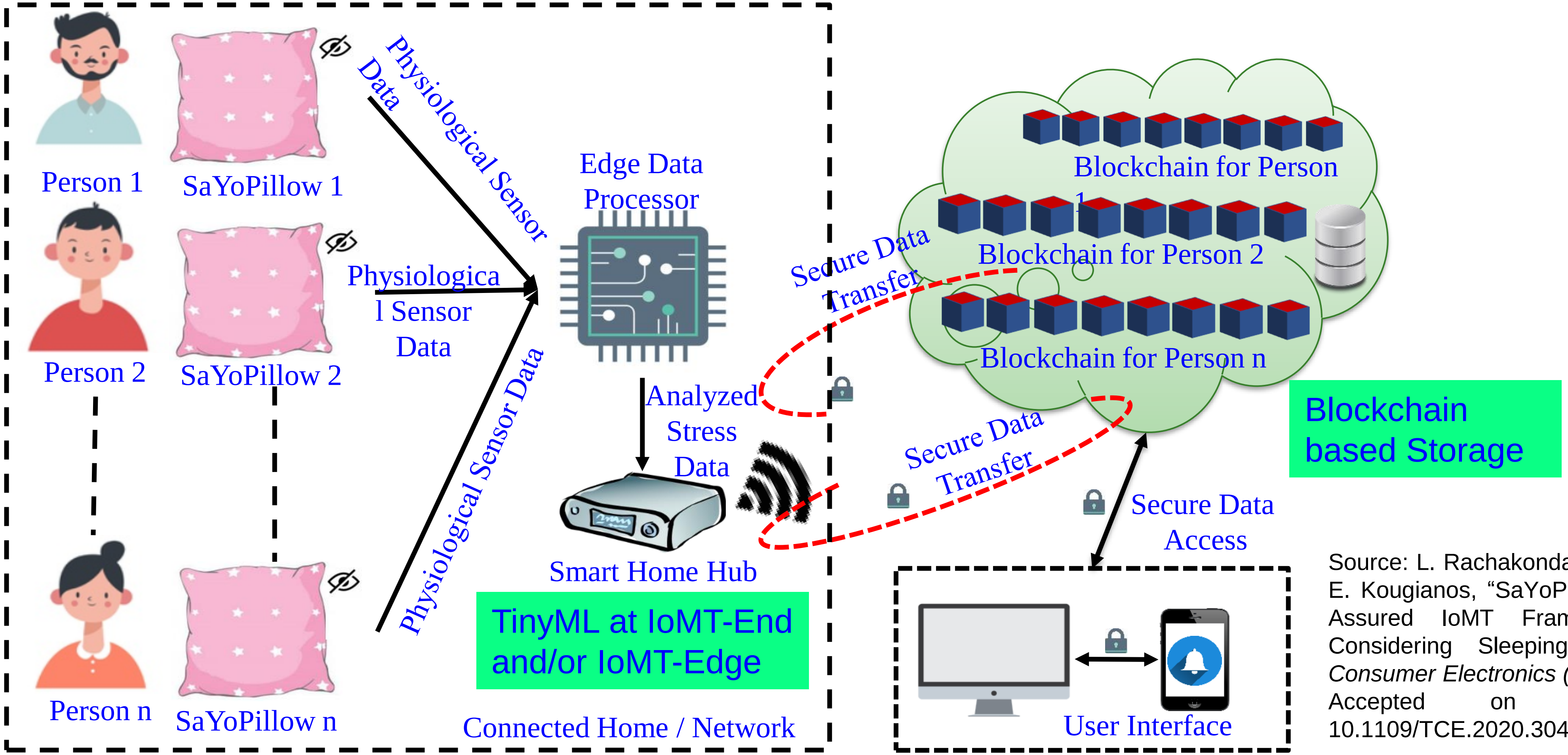
Heavy-Duty ML is more suitable for smart cities

When do You Need the Blockchain?



Source: D. Puthal, S. P. Mohanty, E. Kougianos and G. Das, "When Do We Need the Blockchain?," i*IEEE Consumer Electronics Magazine*, Vol 10, No. 2, Mar 2021, doi: 10.1109/MCE.2020.3015606.

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



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

Data Holds the Key for Intelligence in CPS

Smart Healthcare - System and Data Analytics : To Perform Tasks

Systems & Analytics
- Health cloud server
- Edge server
- Implantable Wearable Medical Devices (IWMDs)

Machine Learning Engine

Data
- Physiological data
- Environmental data
- Genetic data
- Historical records
- Demographics

Systems & Analytics
- Clinical Decision Support Systems (CDSSs)
- Electronic Health Records (EHRs)

Machine Learning Engine

Data
- Physician observations
- Laboratory test results
- Genetic data
- Historical records
- Demographics

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

Challenges of Data in CPS are Multifold

Data Curation

Data Cost

Data Storage

Lots of Data

Data Ownership

Data Modeling

Data Quality

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

AI can be fooled by fake data

AI can create fake data (Deepfake)

Authentic Fake

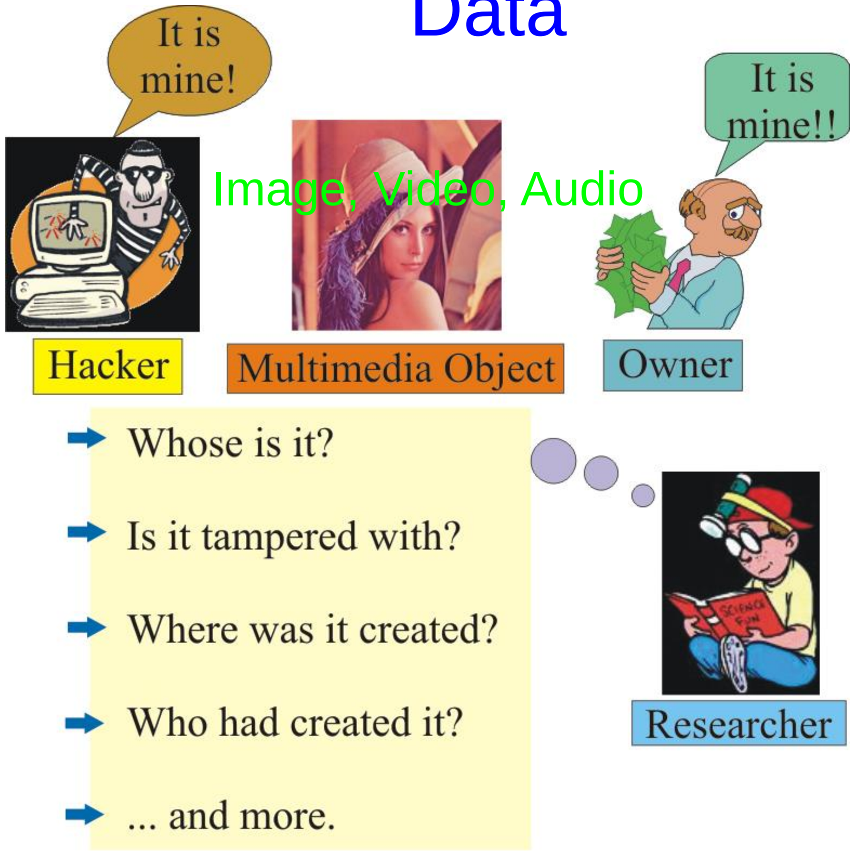
An implantable medical device

Authentic Fake

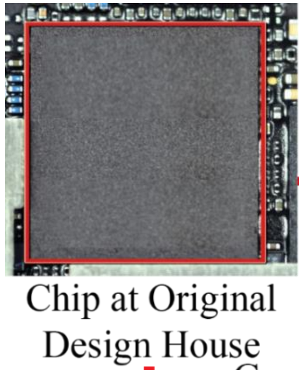
A plug-in for car-engine computers

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

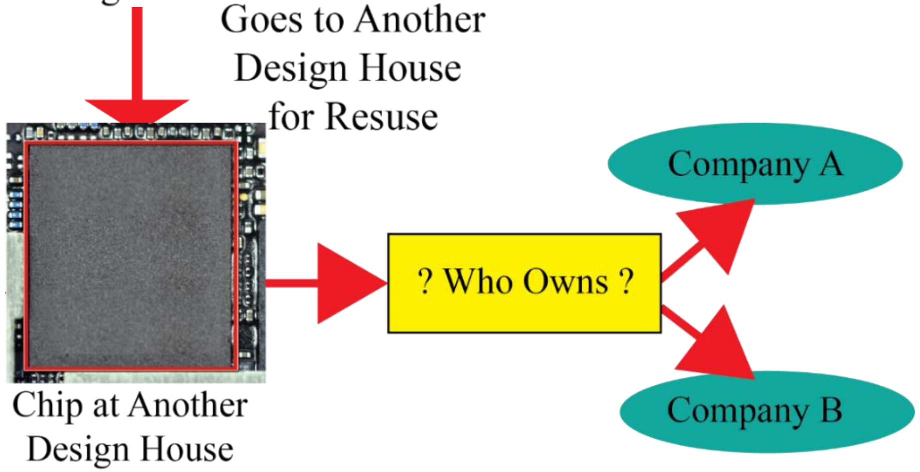
Data



System

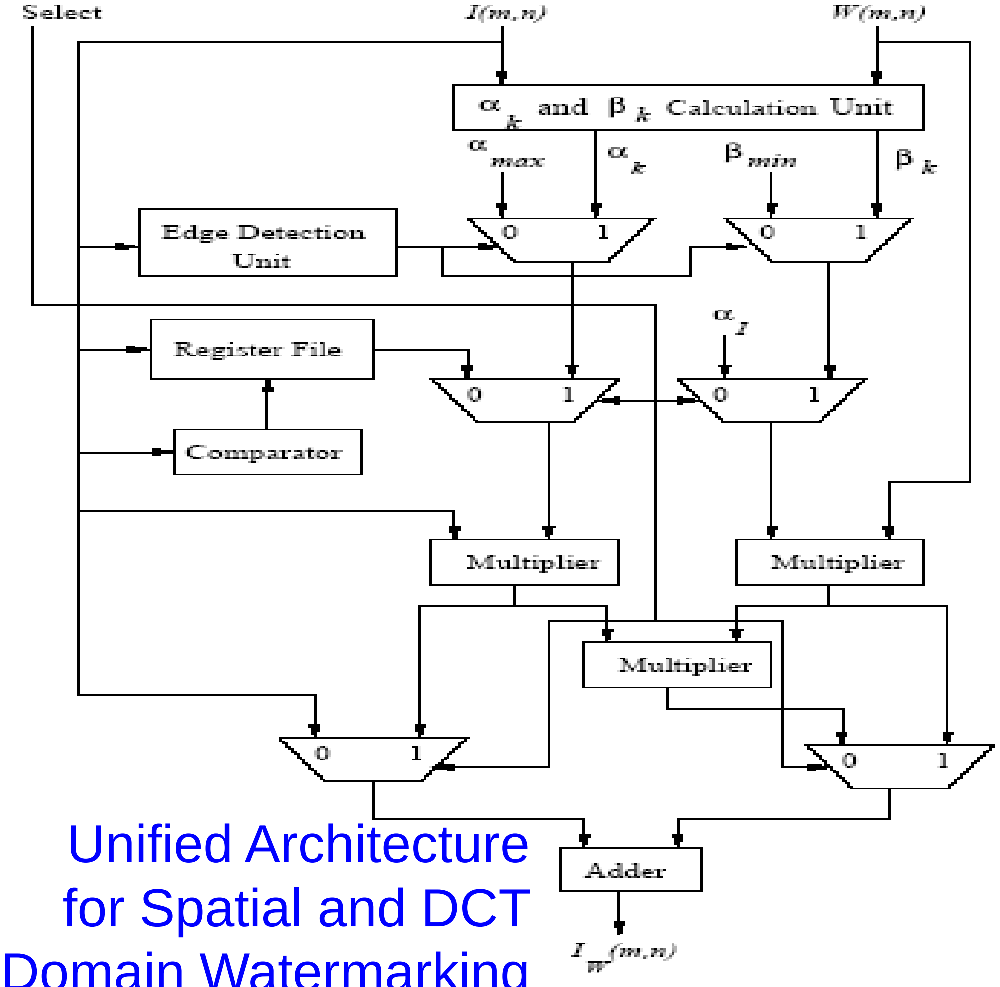


IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.

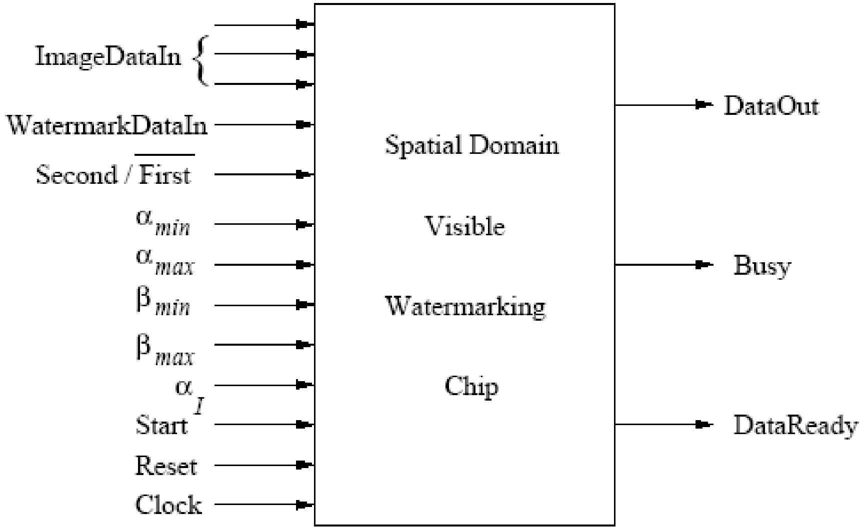


Source: S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking", *IEEE Consumer Electronics Magazine (CEM),* Volume 6, Issue 3, July 2017, pp. 83--91.

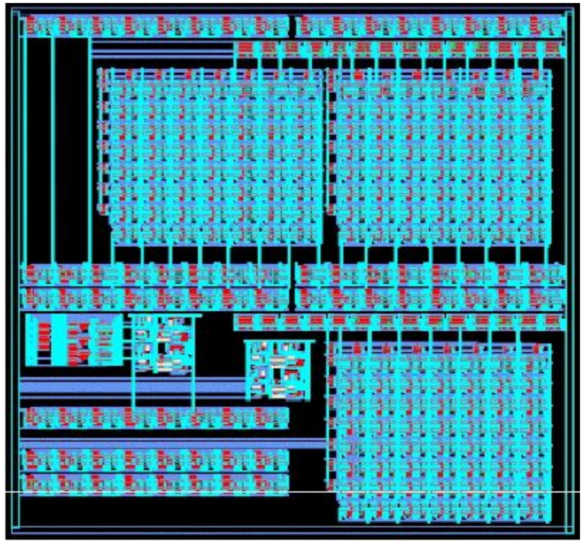
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

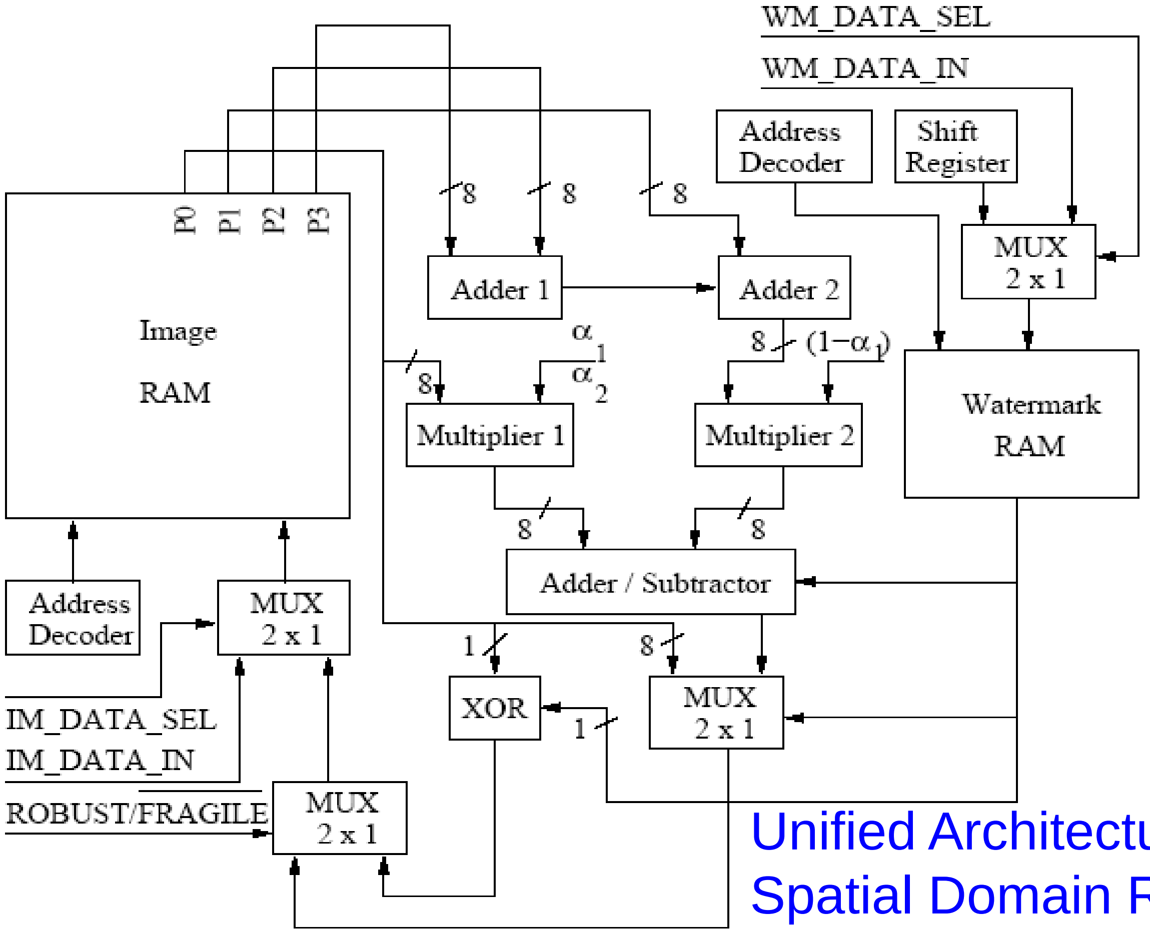
Chip Design Data

Total Area : 9.6 sq mm, No. of Gates: 28,469

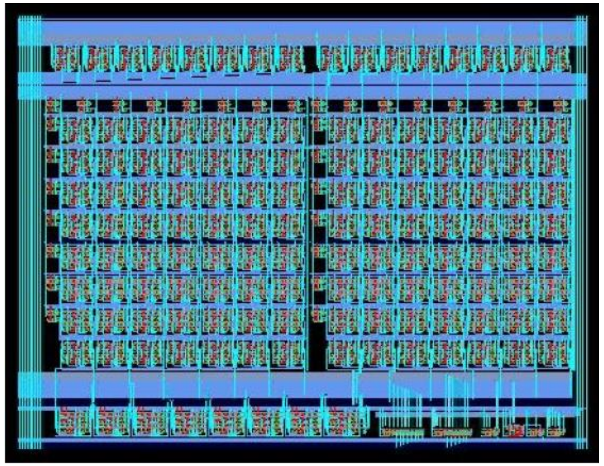
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

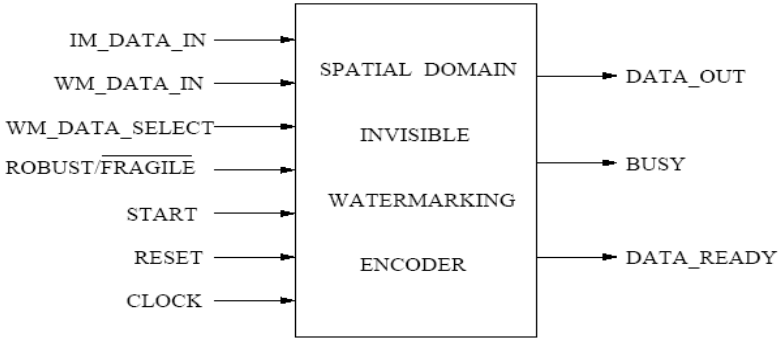
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

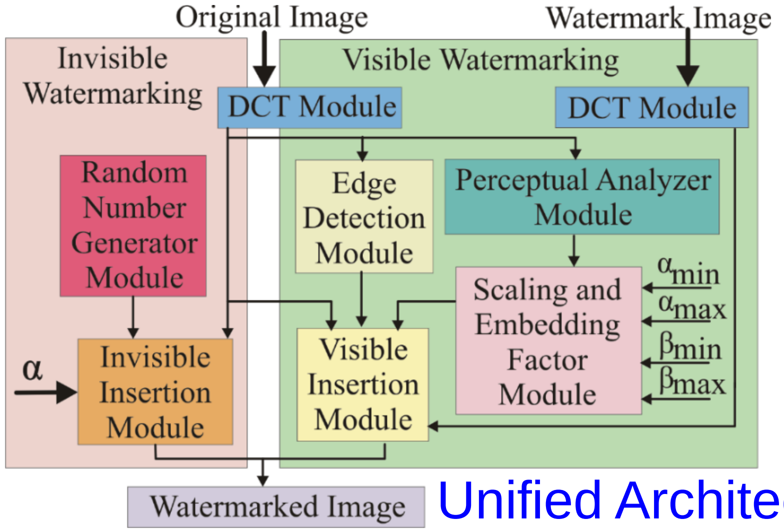
Chip Design Data

Total Area : 0.87 sq mm, No. of Gates: 4,820

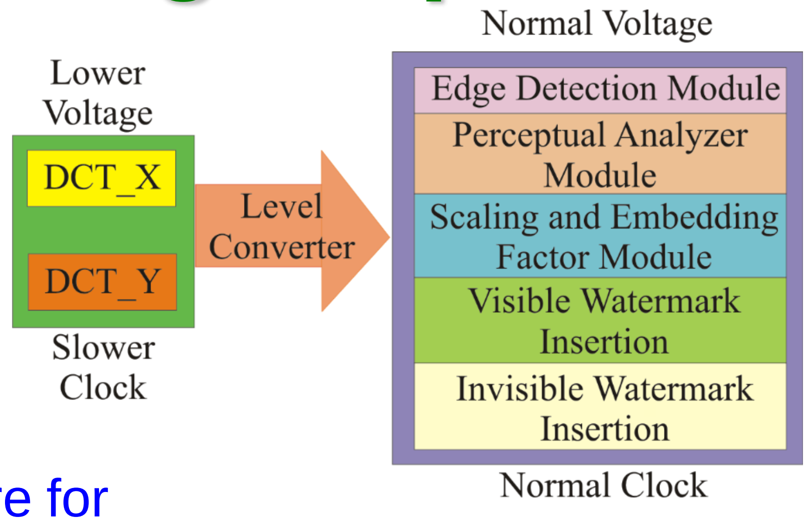
Power Consumption: 2.0 mW, Frequency: 500 MHz

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

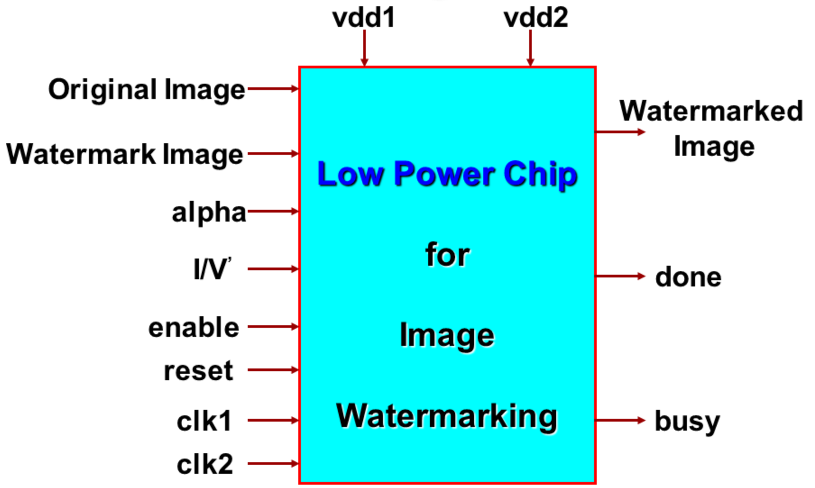
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



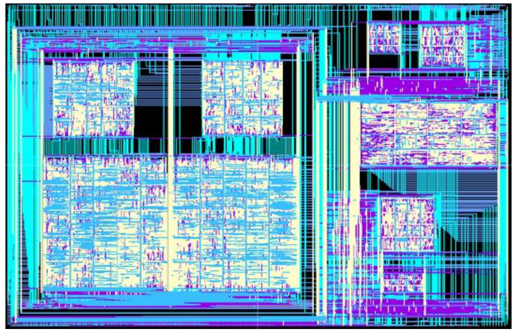
Unified Architecture for DCT Domain Watermarking



DVDF Low-Power Design



Pin Diagram



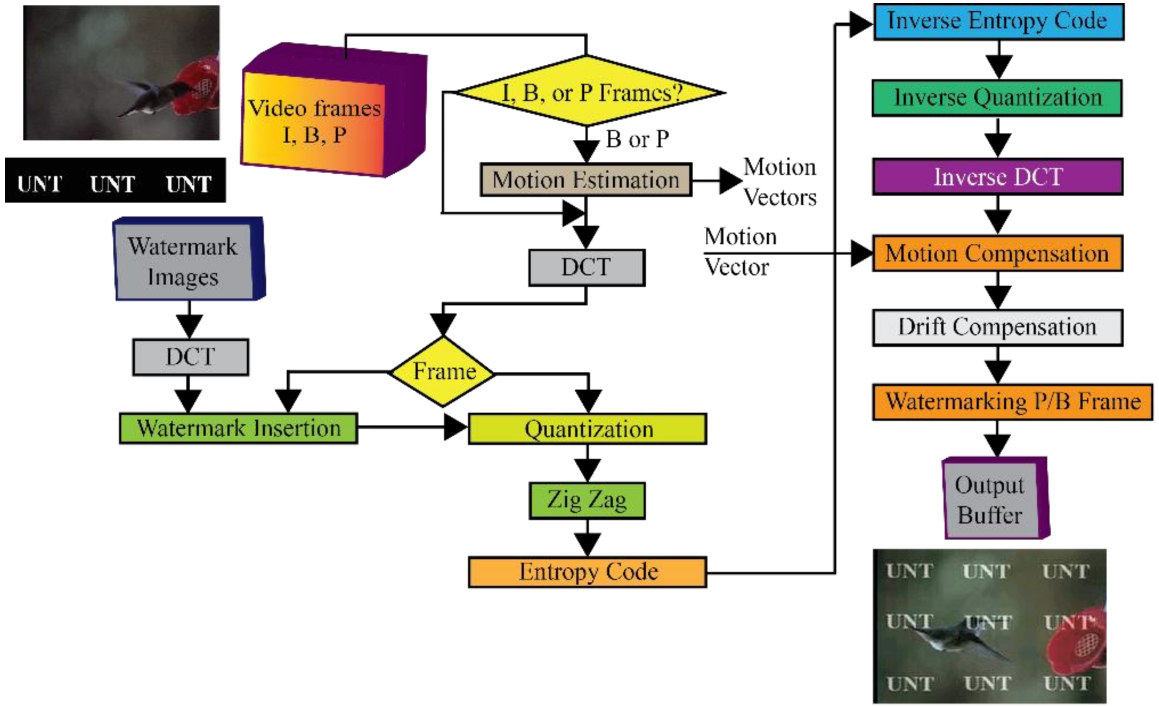
Chip Layout

Chip Design Data

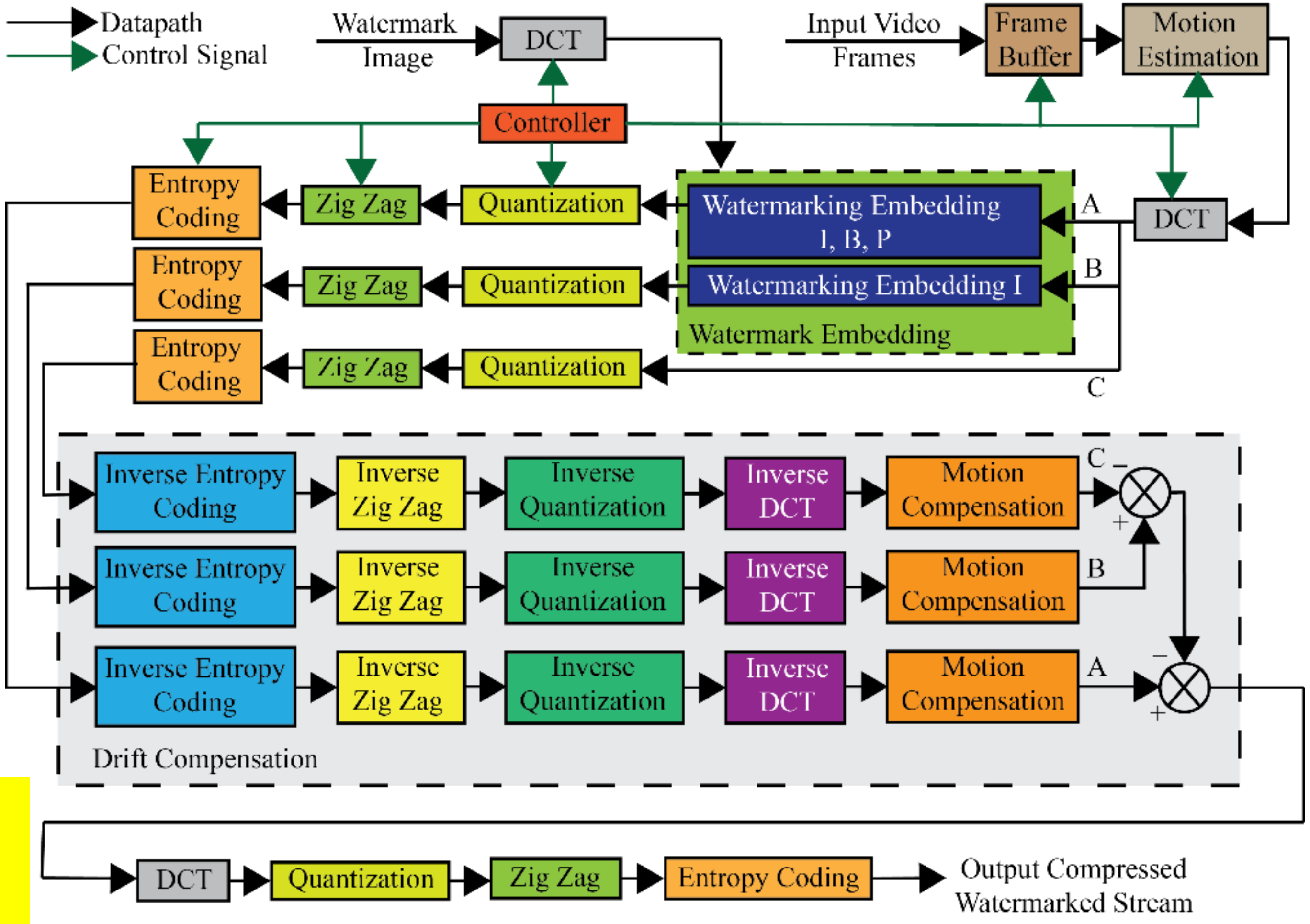
Total Area : 16.2 sq mm, No. of Transistors: 1.4 million
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

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

Our Hardware for Real-Time Video Watermarking



(a) Video Watermarking Algorithm as a Flow Chart



(b) Architecture of the Video Watermrking Algorithm

FPGA based Design Data

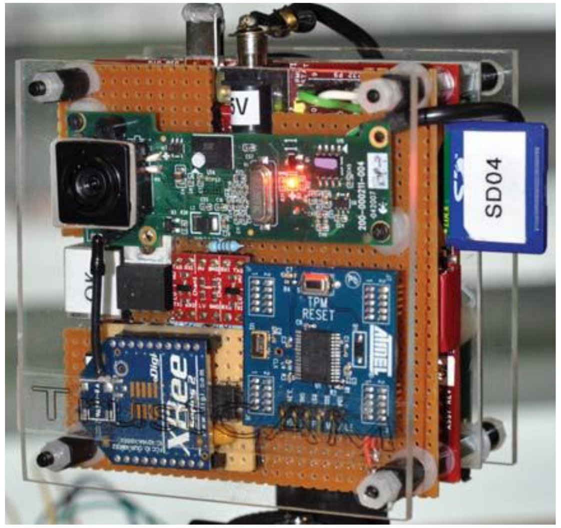
Resource: 28322 LE, 16532 Registers, 9 MUXes

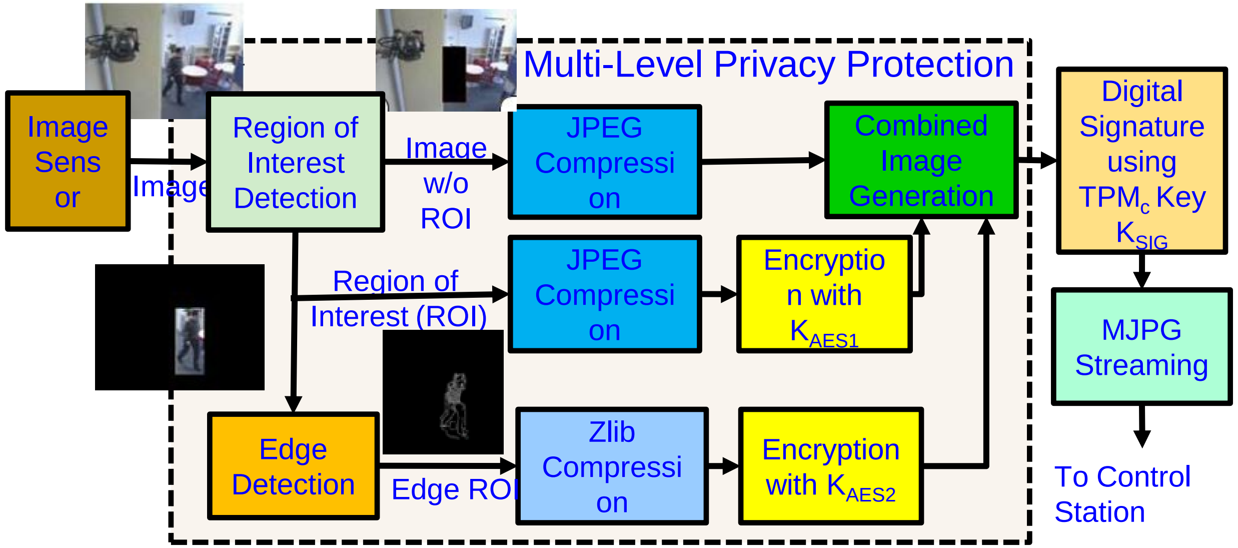
Operating Frequency: 100 MHz

Throughput: 43 fps

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

My Watermarking Research Inspired - TrustCAM



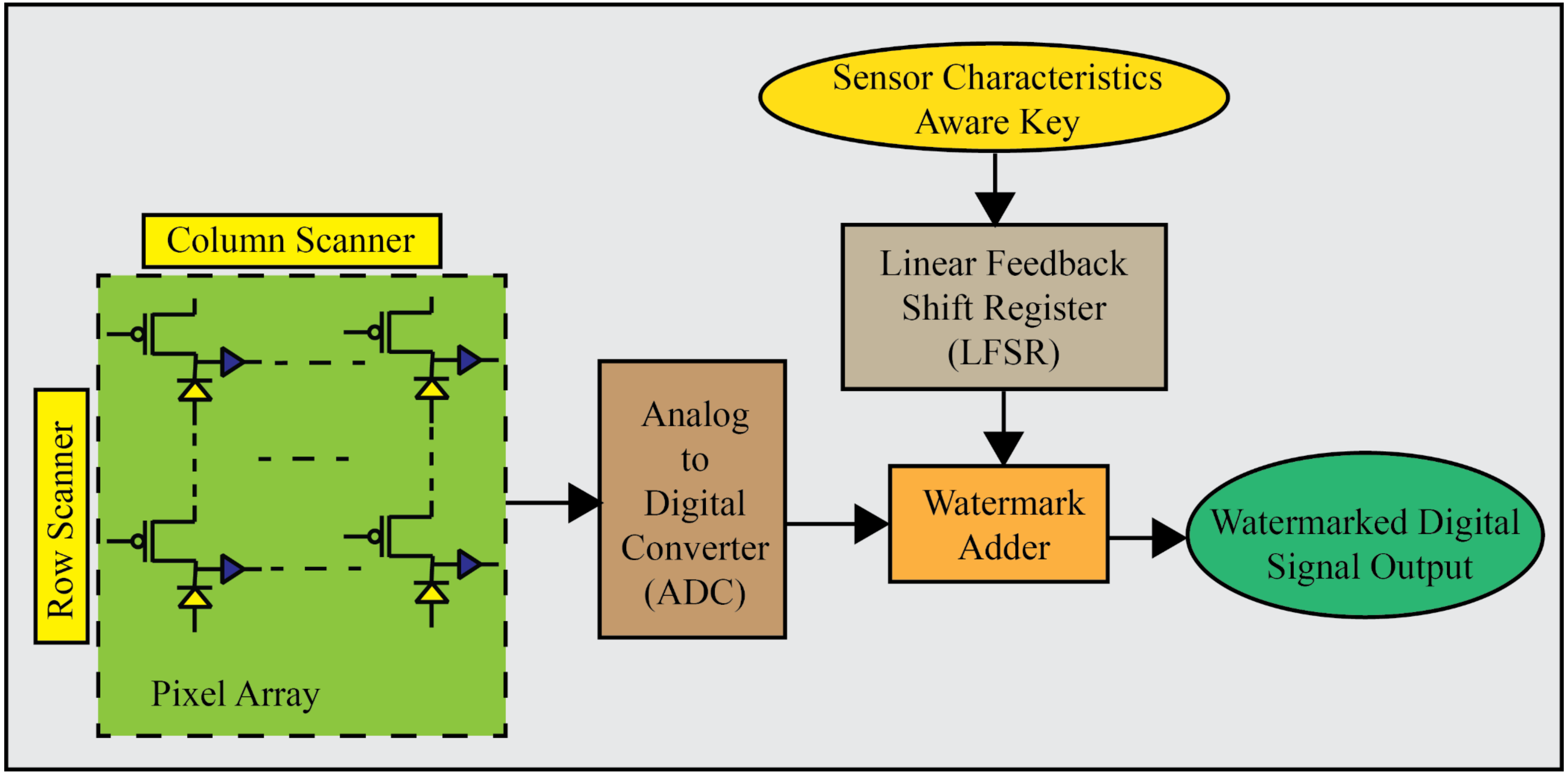


For integrity protection, authenticity and confidentiality of image data.

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

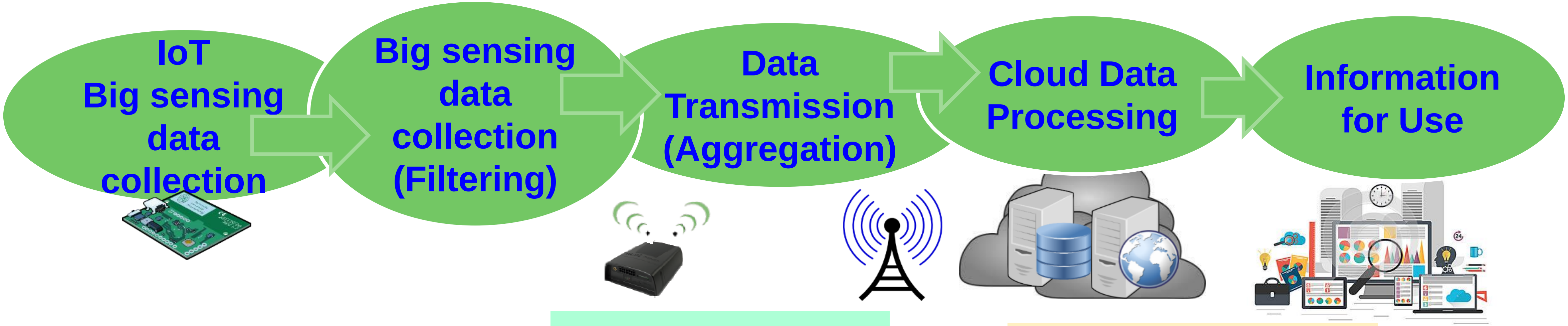
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor



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

Secure Data Curation a Solution for Fake Data?



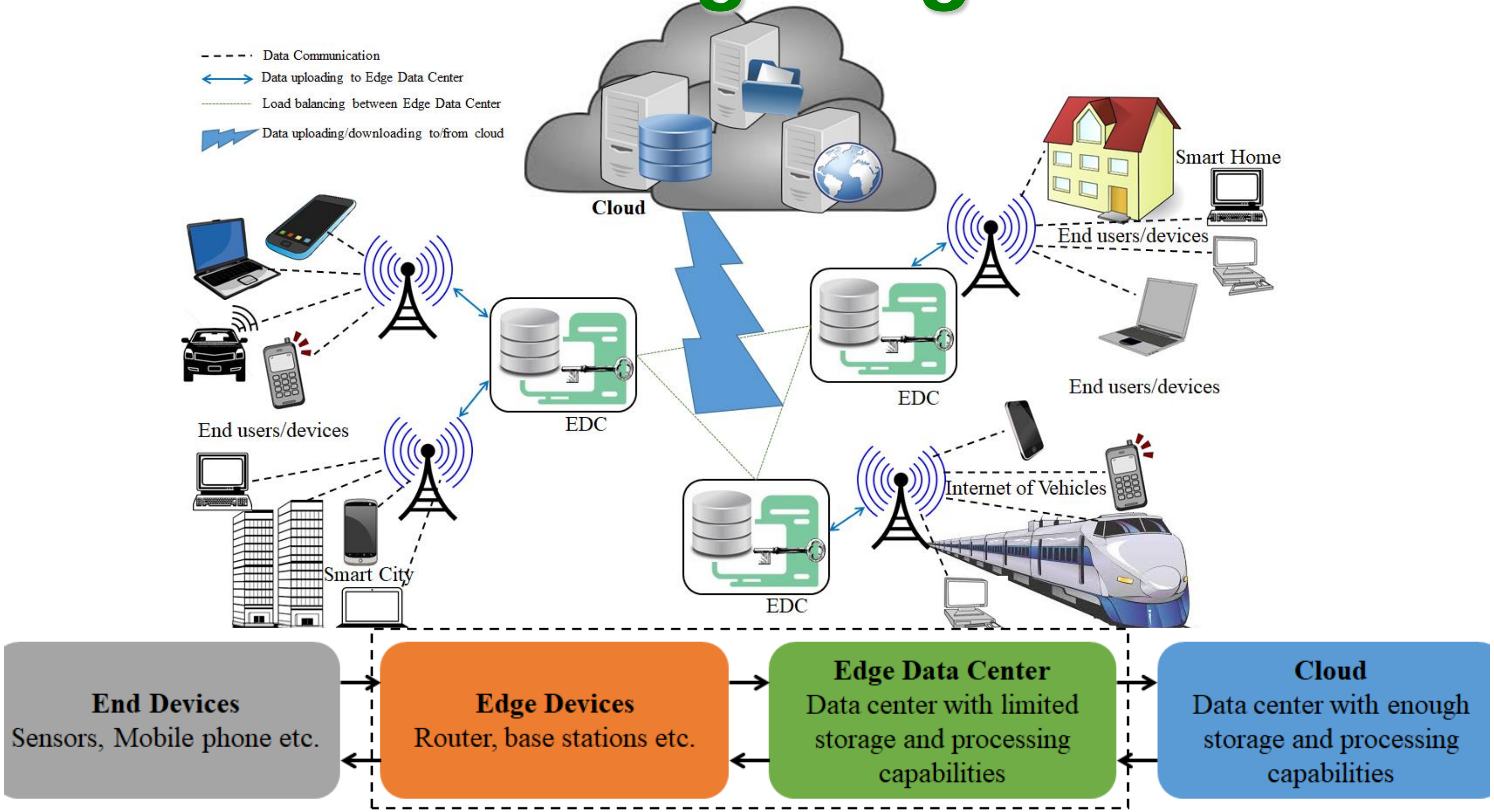
Edge Training:
- ➢ Data Signature
- ➢ Model Signature

Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

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

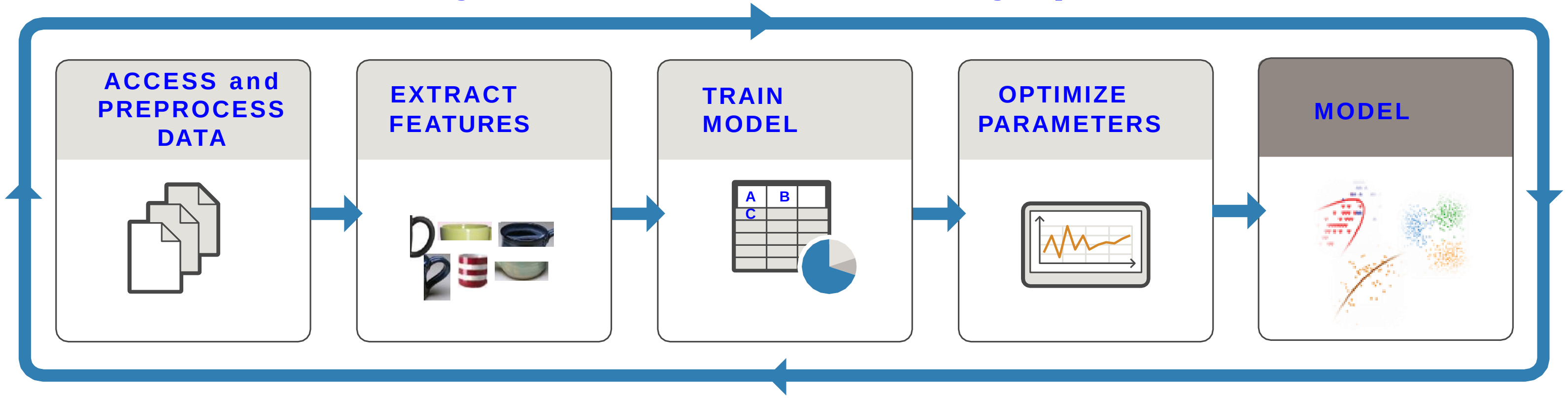
Data and Security Should be Distributed using Edge Datacenter



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

TinyML - Key for Smart Cities and Smart Villages

TRAIN: Iterate until you achieve satisfactory performance.

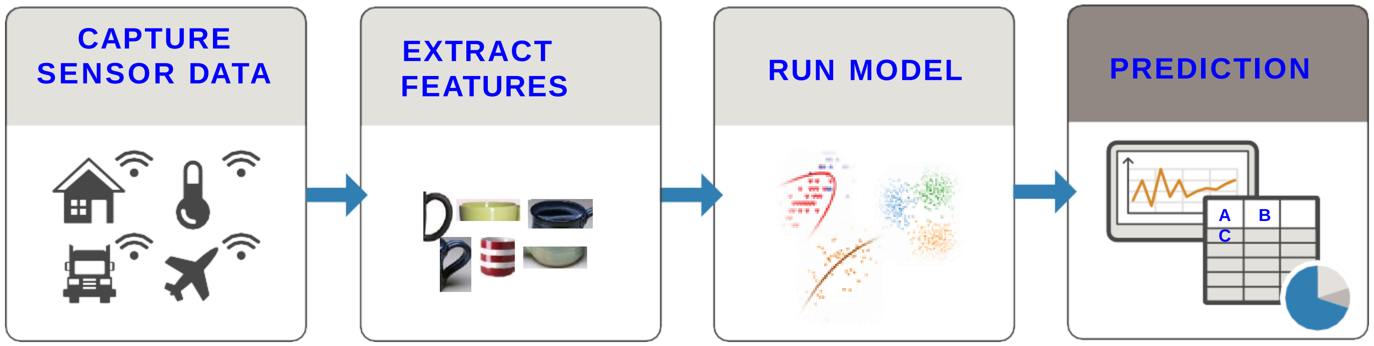


Needs Significant:

- ➢ Computational Resource
- ➢ Computation Energy

Solution: Reduce Training Time and/or Computational Resource

PREDICT: Integrate trained models into applications.



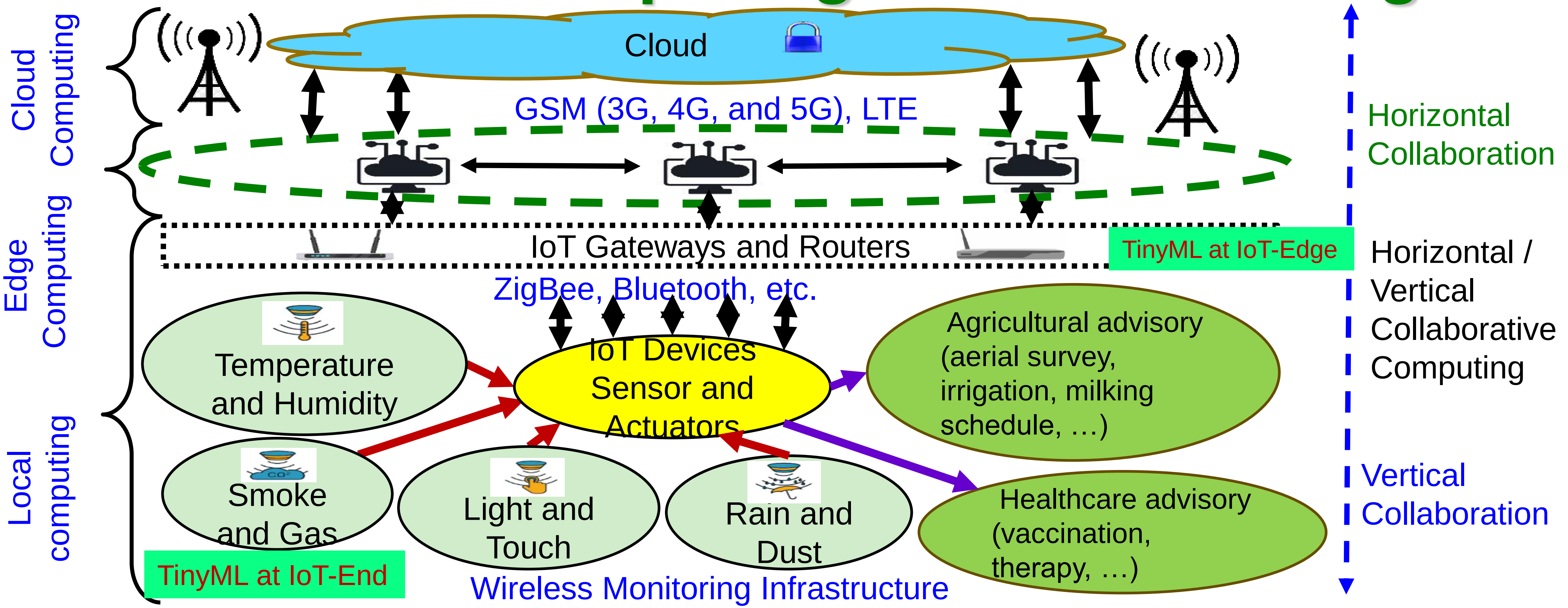
Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

Needs:

- ➢ Computational Resource
- ➢ Computation Energy

Solution: TinyML

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, "Collaborative Edge Computing for Smart Villages", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

Conclusions

Conclusions

- Security and Privacy are important problems in Cyber-Physical Systems (CPS).
- Various elements and components of CPS including Data, Devices, System Components, AI need security.
- Both software and hardware-based attacks and solutions are possible.
- Security in H-CPS, E-CPS, and T-CPS, etc. can have serious consequences.
- Existing security solutions have serious overheads and may not even run in the end-devices (e.g. a medical device) of CPS/IoT.
- Hardware-Assisted Security (HAS): Security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system. HAS/SbD advocate features at early design phases, no-retrofitting.

Future Directions

- Privacy and/or Security by Design (PbD or SbD) needs research.
- Security, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS) need more research.
- Security of systems (e.g. Smart Healthcare device/data, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable Smart City and Smart Villages: need sustainable IoT/CPS