Secure Cyber-Physical Systems by Design

Faculty Development Program

Sponsored by TEQIP-III, Govt. of India

Govt. College of Engineering and Technology, Bhubaneswar

19 Sep - 23 Sep 2020

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu

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

Talk - Outline

- Smart City Components as Cyber-Physical Systems (CPS)
- Security Challenges in Cyber-Physical Systems
- Drawbacks of Existing Security Solutions
- Selected Proposed Hardware-Assisted Security (HAS) or Secure-by-Design (SbD) Solutions
- Conclusions and Future Directions

The Big Picture

Smart Cities is a Solution for Urban Migration

- 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

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

July 2016

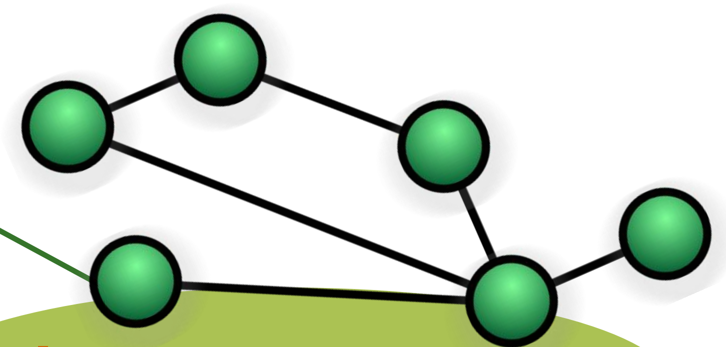
Source: S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything You wanted to Know about Smart Cities”, *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Smart Cities - 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

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

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

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

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

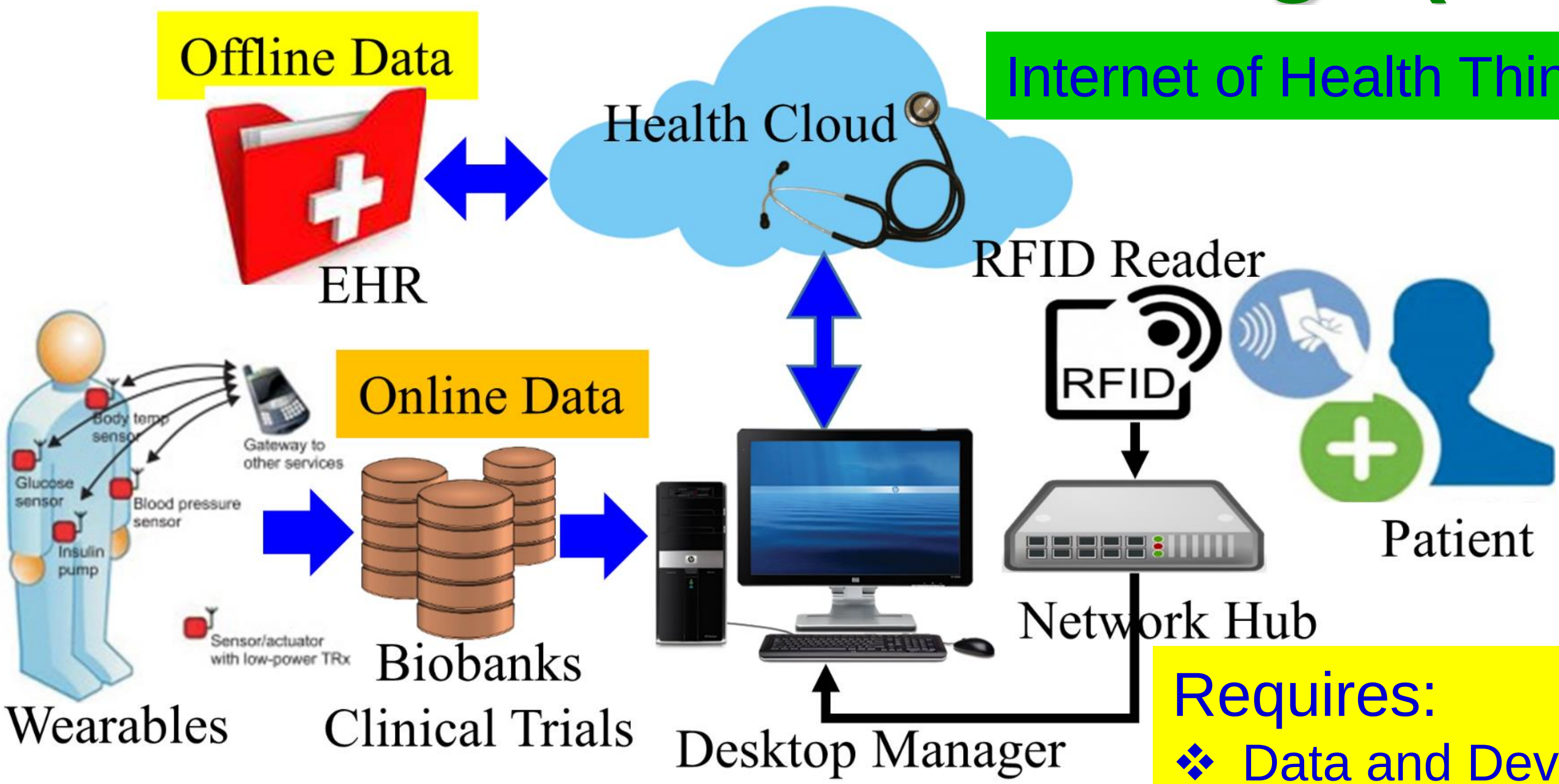
Connected Electronic Systems
Smart phones, devices, cars, wearables which are connected to the Things

Overall architecture:

- A configurable dynamic global network of networks
- Systems-of-Systems

Source: Mohanty ICIT 2017 Keynote

Internet of Medical Things (IoMT)

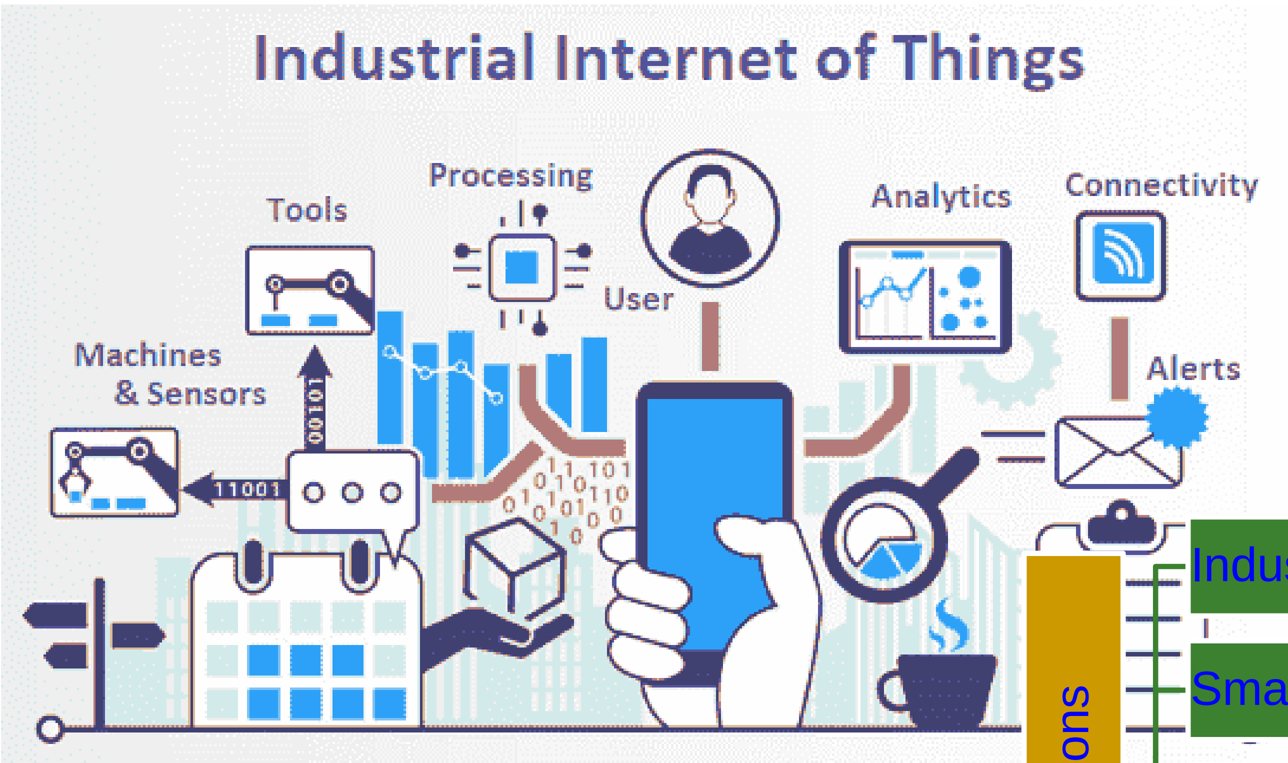


Requires:
- ❖ Data and Device Security
- ❖ Data Privacy

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

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

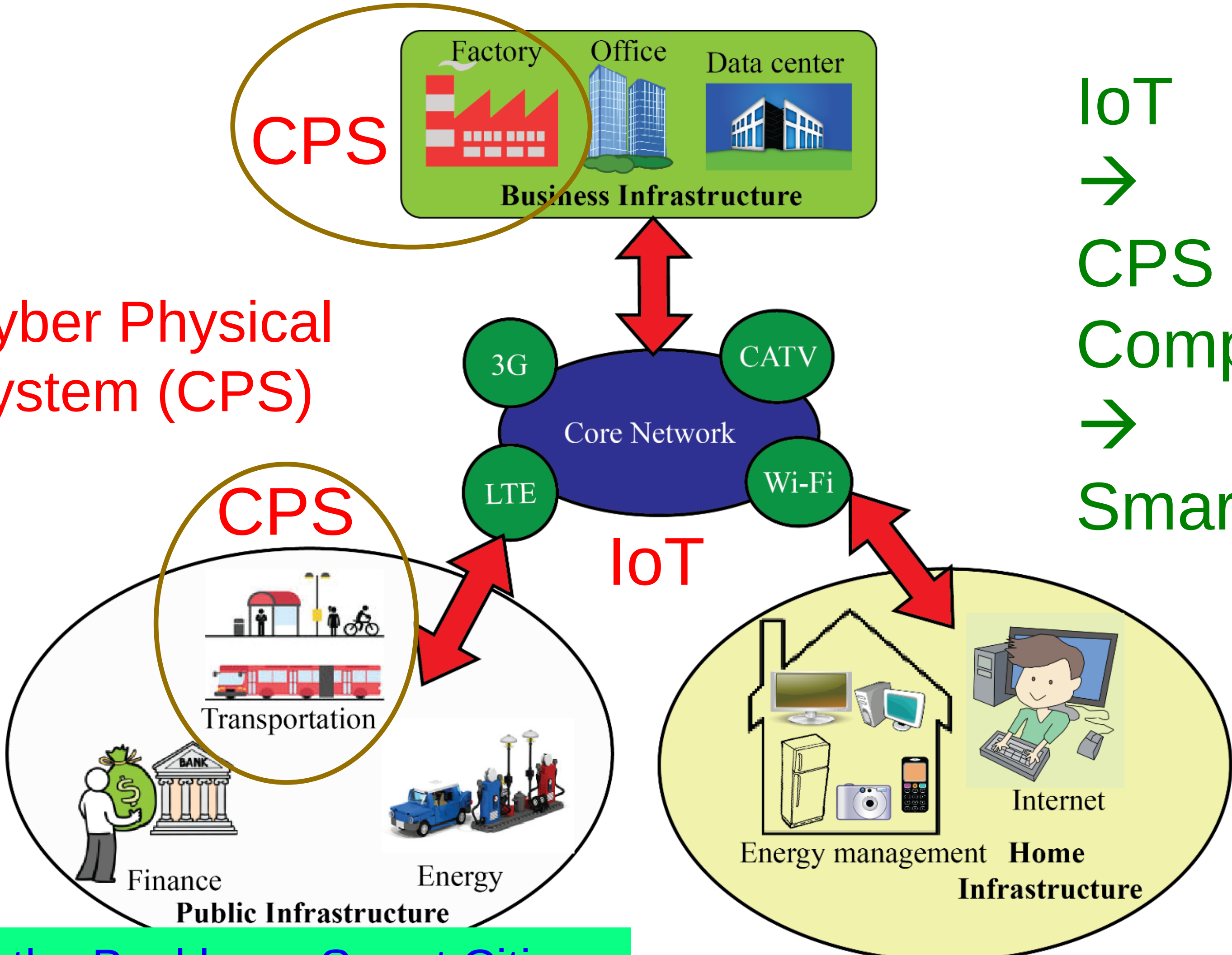
Industrial Internet of Things (IIoT)



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

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

IoT → CPS → Smart Cities



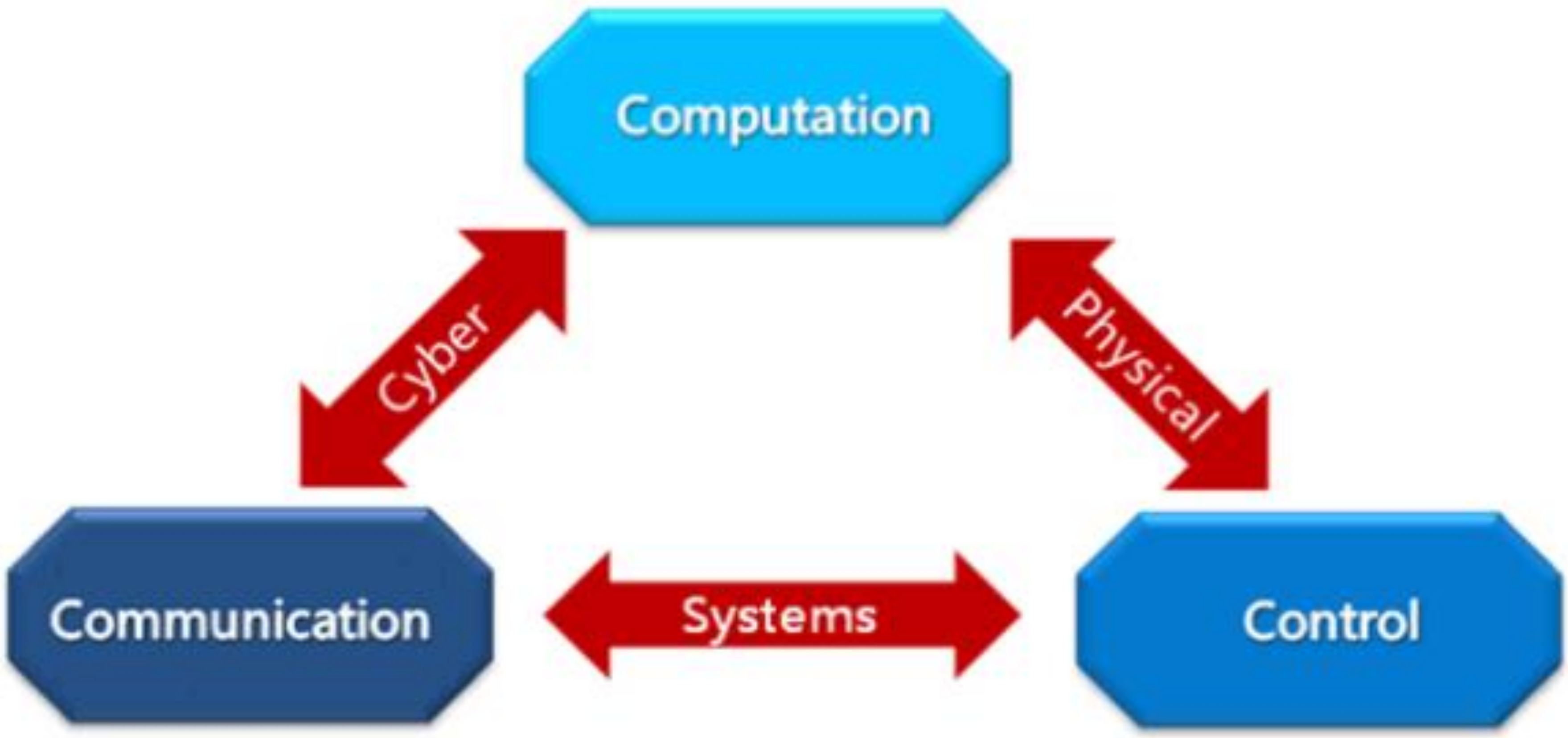
Cyber Physical System (CPS)

IoT → CPS (Smart Components) → Smart Cities

IoT is the Backbone Smart Cities.

Source: Mohanty CE Magazine July 2016

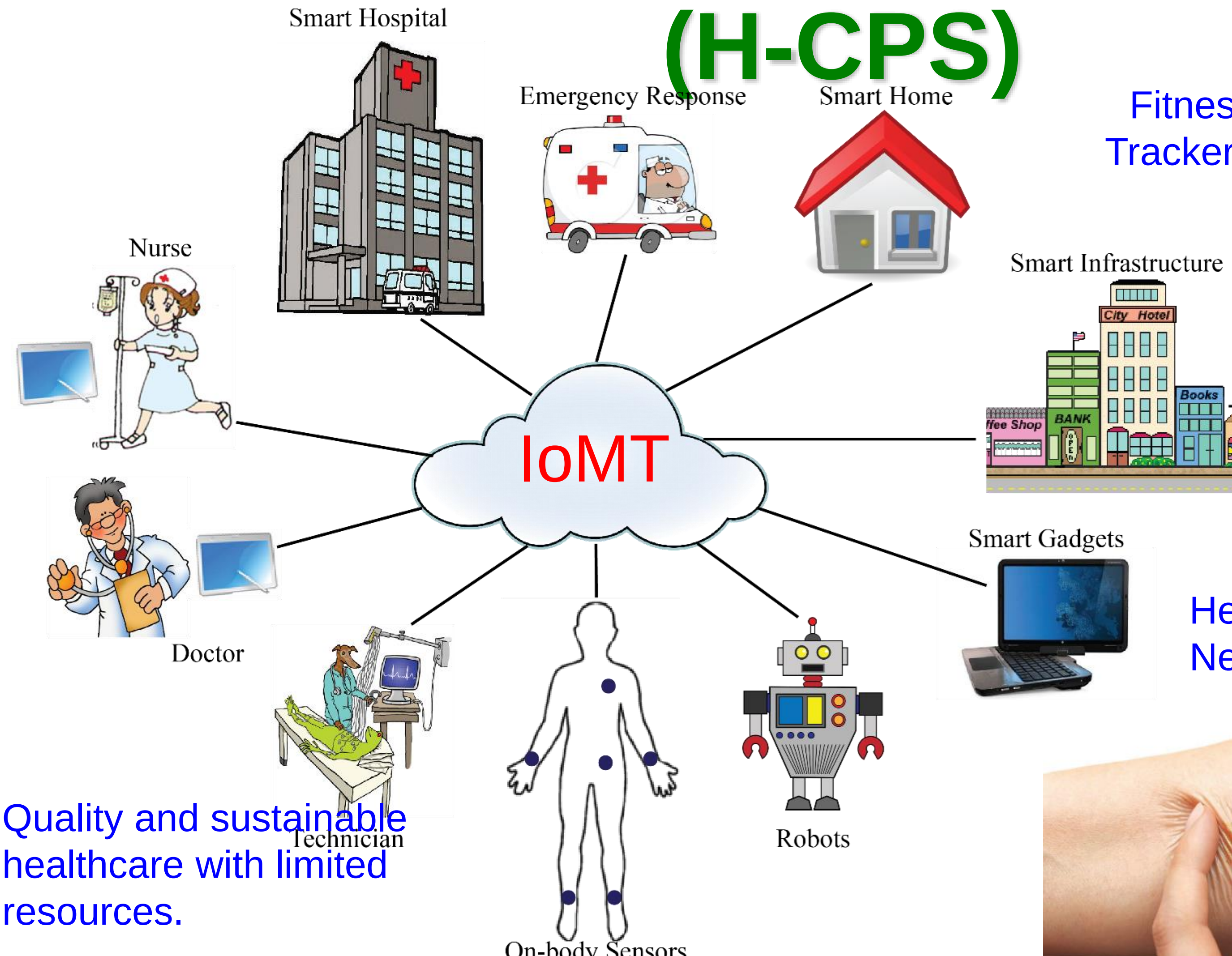
Cyber-Physical Systems (CPS) - 3 Cs



3 Cs of IoT - Connect, Compute, Communicate

Source: G. Jinghong, H. Ziwei, Z. Yan, Z. Tao, L. Yajie and Z. Fuxing, "An overview on cyber-physical systems of energy interconnection," in *Proc. IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2017, pp. 15-21.

Healthcare Cyber-Physical System (H-CPS)

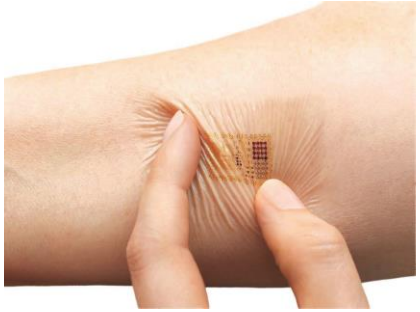


Quality and sustainable healthcare with limited resources.

Source: Mohanty CE Magazine July 2016

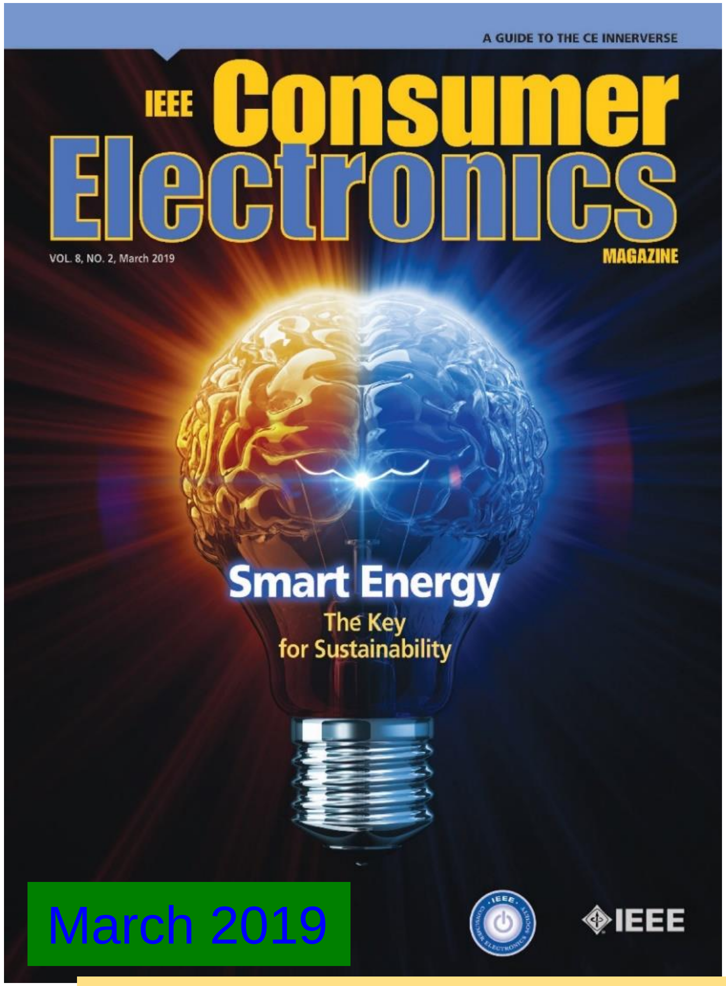
Fitness Trackers

Headband with Embedded Neurosensors



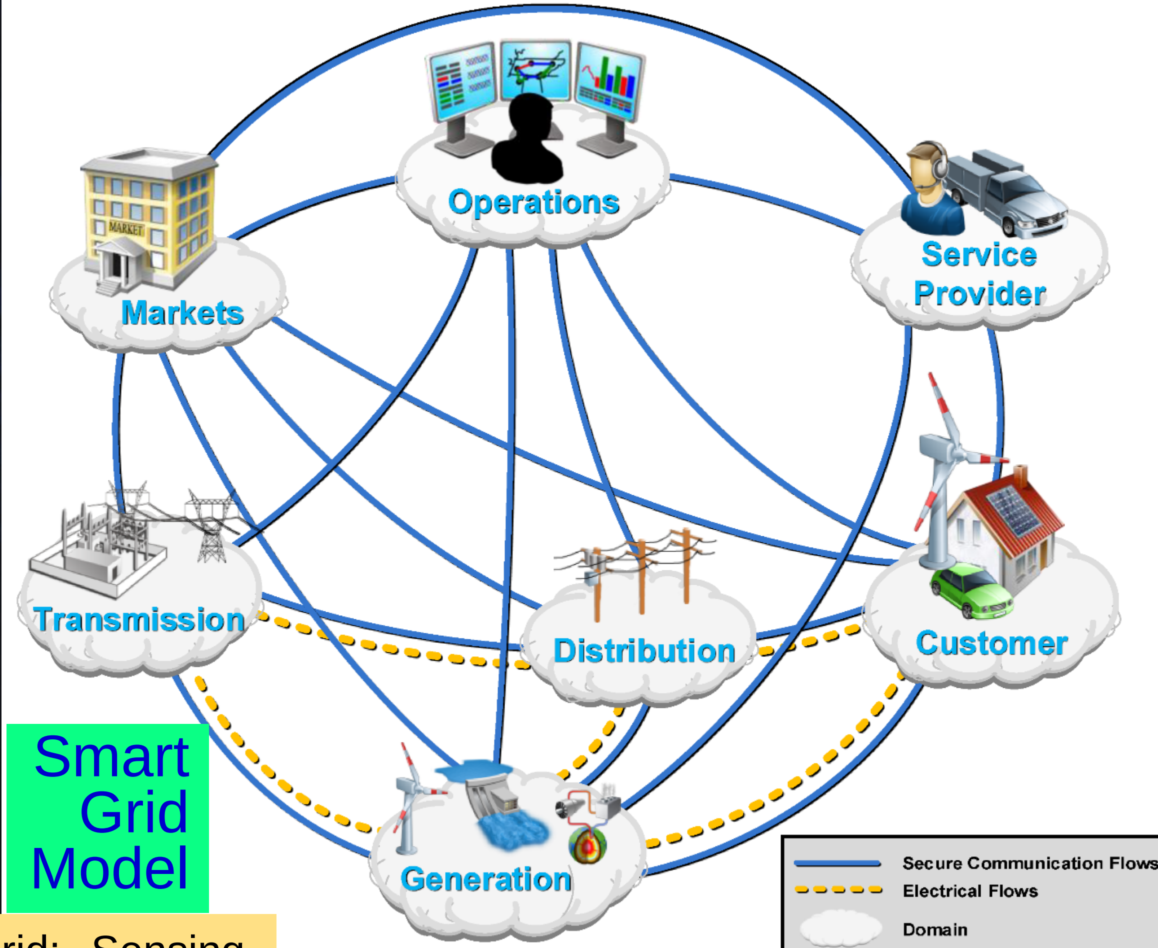
Embedded Skin Patches

Energy Cyber-Physical Systems (E-CPS)



March 2019

Smart Grid Model

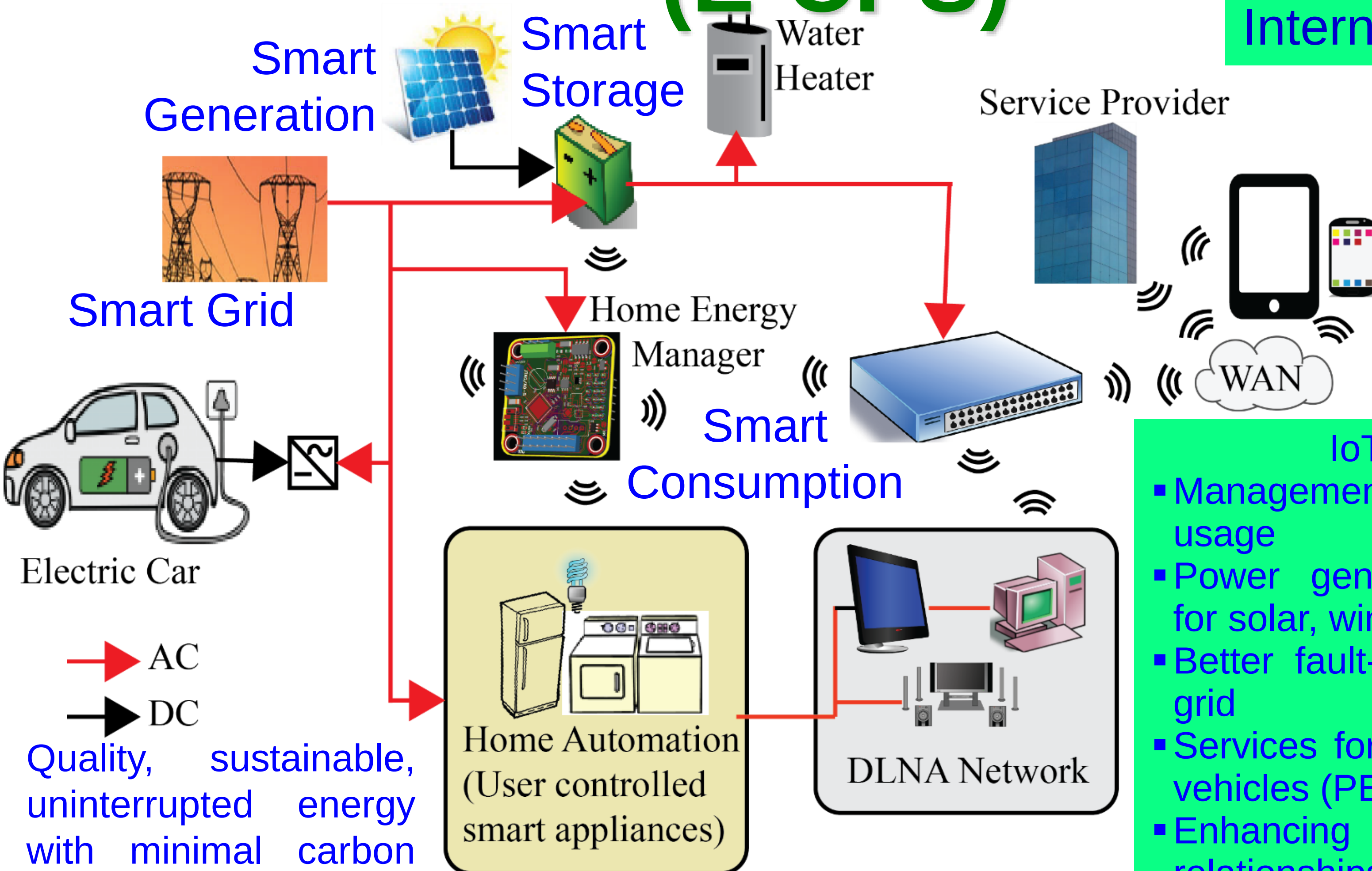


Four key features of smart grid: Sensing, Measurement, Control, and Communications

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

Energy Cyber-Physical Systems (E-CPS)

Internet of Energy



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Source: Mohanty CE Magazine July 2016

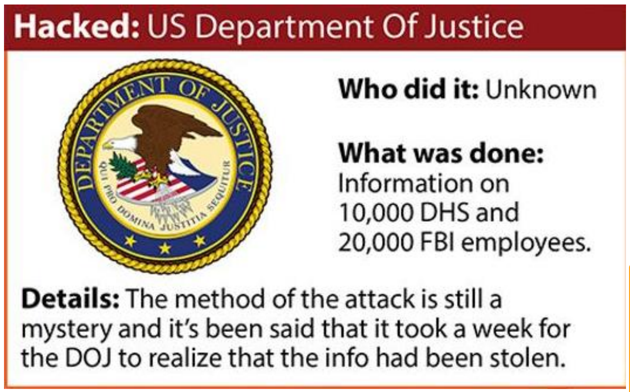
IoT Role:

- 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

Security Challenges in Cyber-Physical Systems (CPS)

Cyber Attacks

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

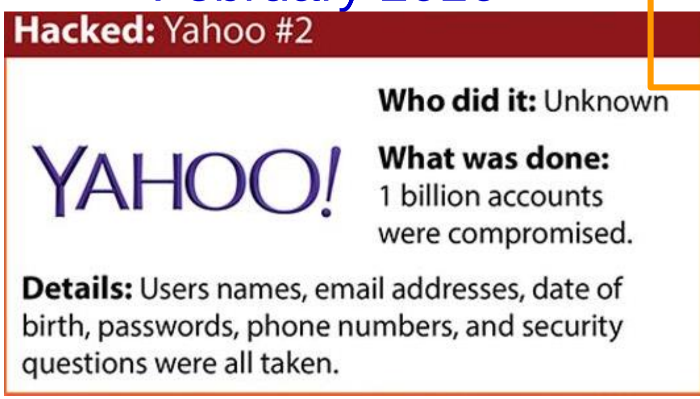

Hacked: US Department Of Justice

Who did it: Unknown

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

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

February 2016


Hacked: Yahoo #2

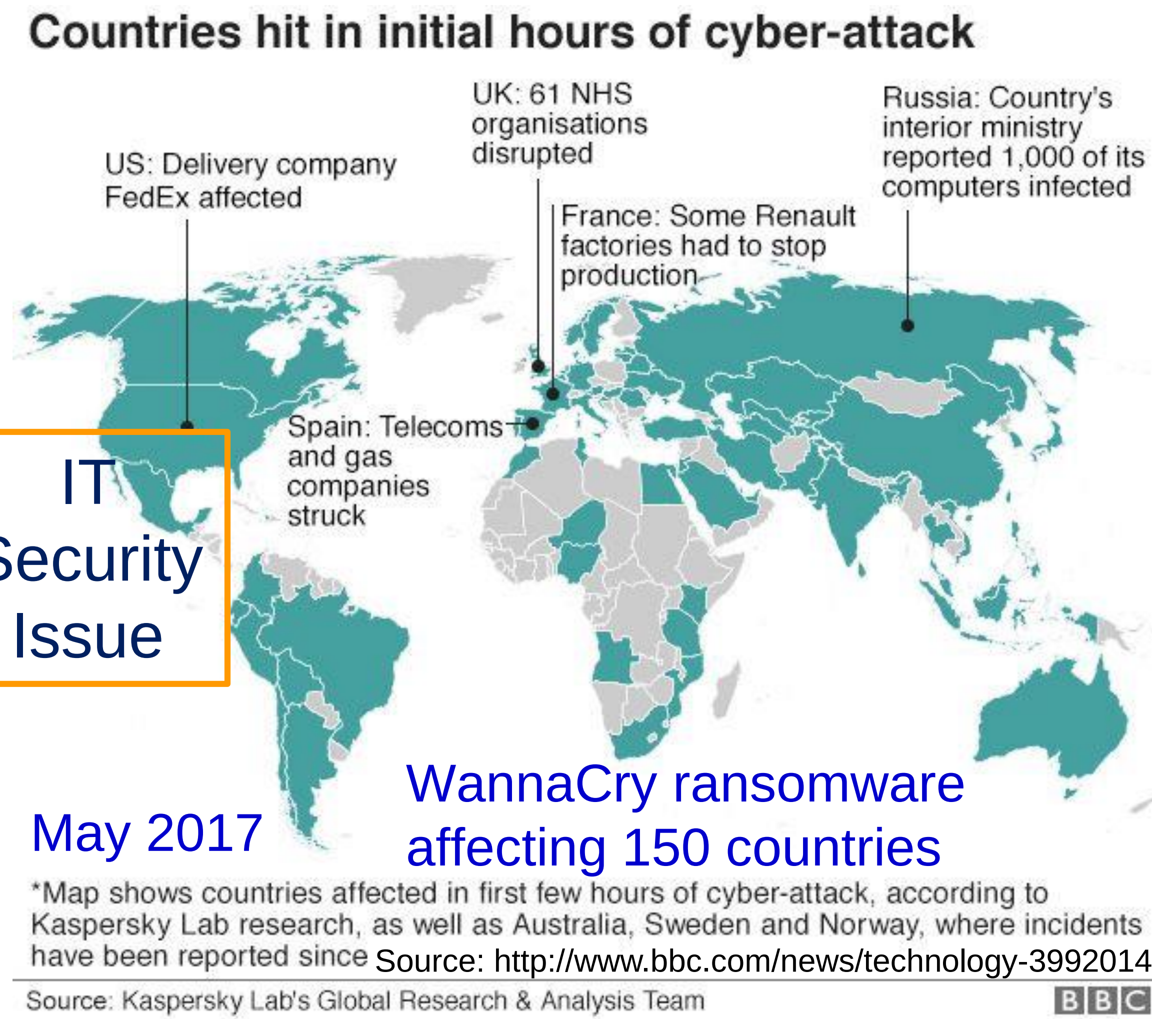
Who did it: Unknown

What was done: 1 billion accounts were compromised.

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

December 2016

IT Security Issue



May 2017

WannaCry ransomware affecting 150 countries

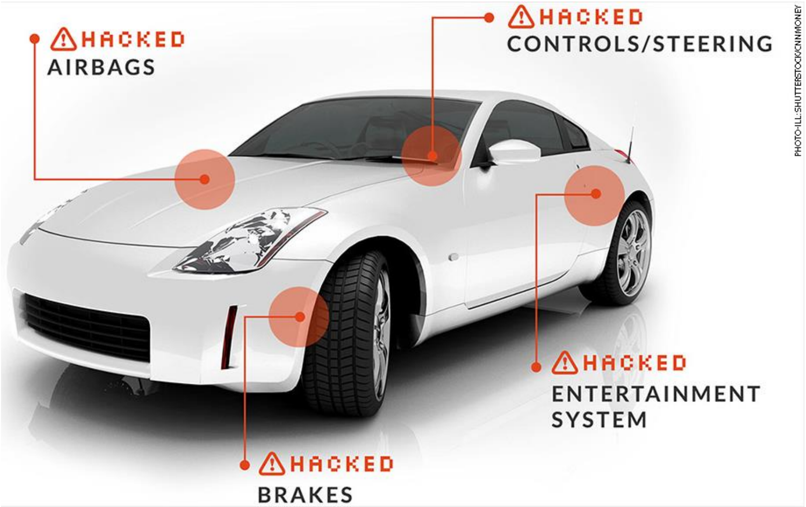
Source: http://www.bbc.com/news/technology-39920141

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

Security Challenge - System

Power Grid Attack

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



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

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

CE Systems – Diverse Security/ Privacy/ Ownership Requirements

Medical Devices

RFID Chip

Pace maker

Insulin Pump

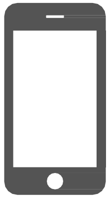
Heart Rate Monitor

Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices



Smart Phones/ Tablets

Wearable Devices

Smart Clothing

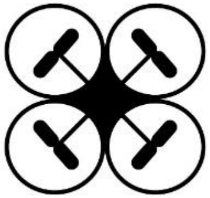
Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

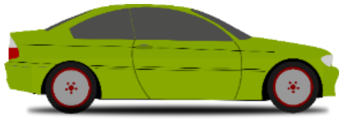
Entertainment Devices



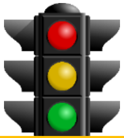
Drones /UAVs

Video Games

Transportation Devices



Smart Vehicles/ Autonomous Vehicles

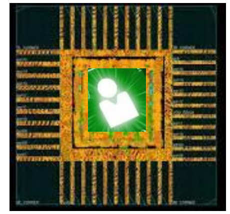


Smart Traffic Controllers

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

Security, Privacy, and IP Rights

Hardware Trojan



System Security

Data Security

System Privacy

Data Privacy

Counterfeit Hardware (IP Rights Violation)

Data Ownership

A GUIDE TO THE CE INNERVERSE

IEEE Consumer Electronics MAGAZINE

VOL. 6, NO. 3, July 2017

Feeling Secure?

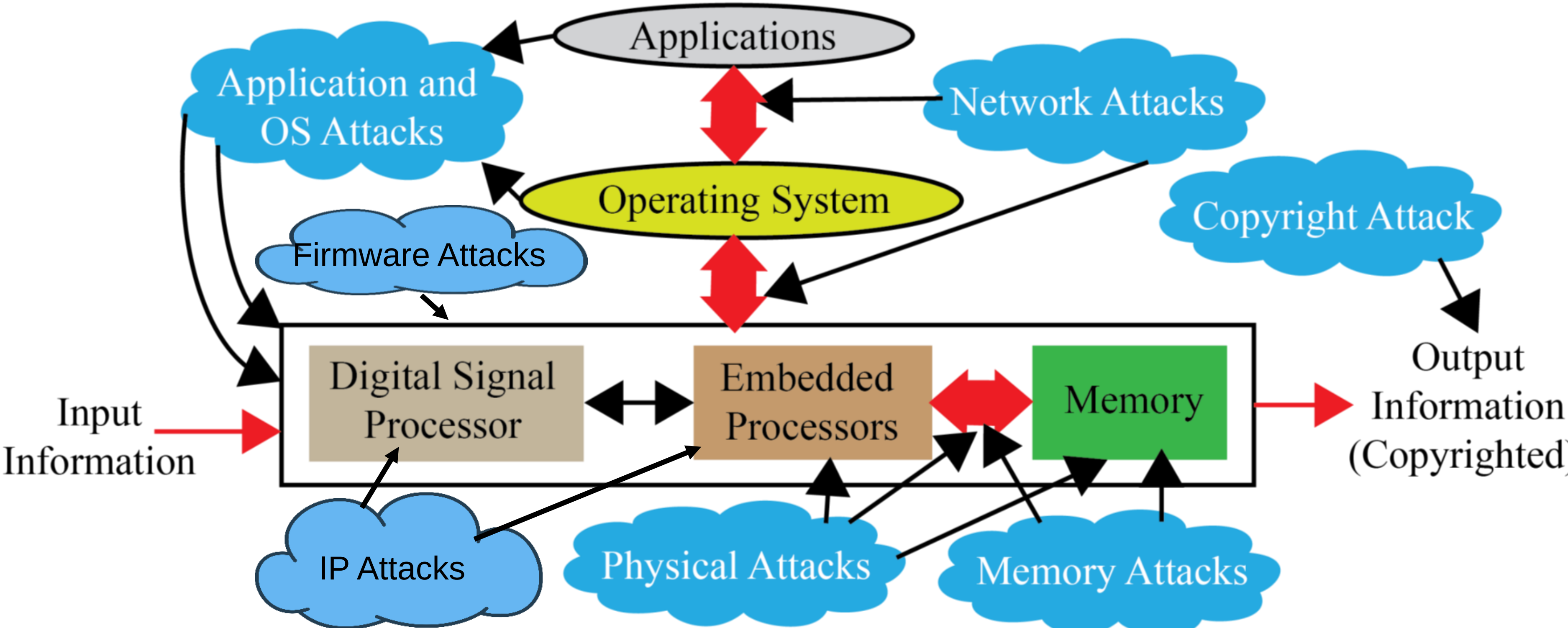
Examining Hardware IP Protection and Trojans

IEEE

July 2017

Source: Mohanty ICIT 2017 Keynote

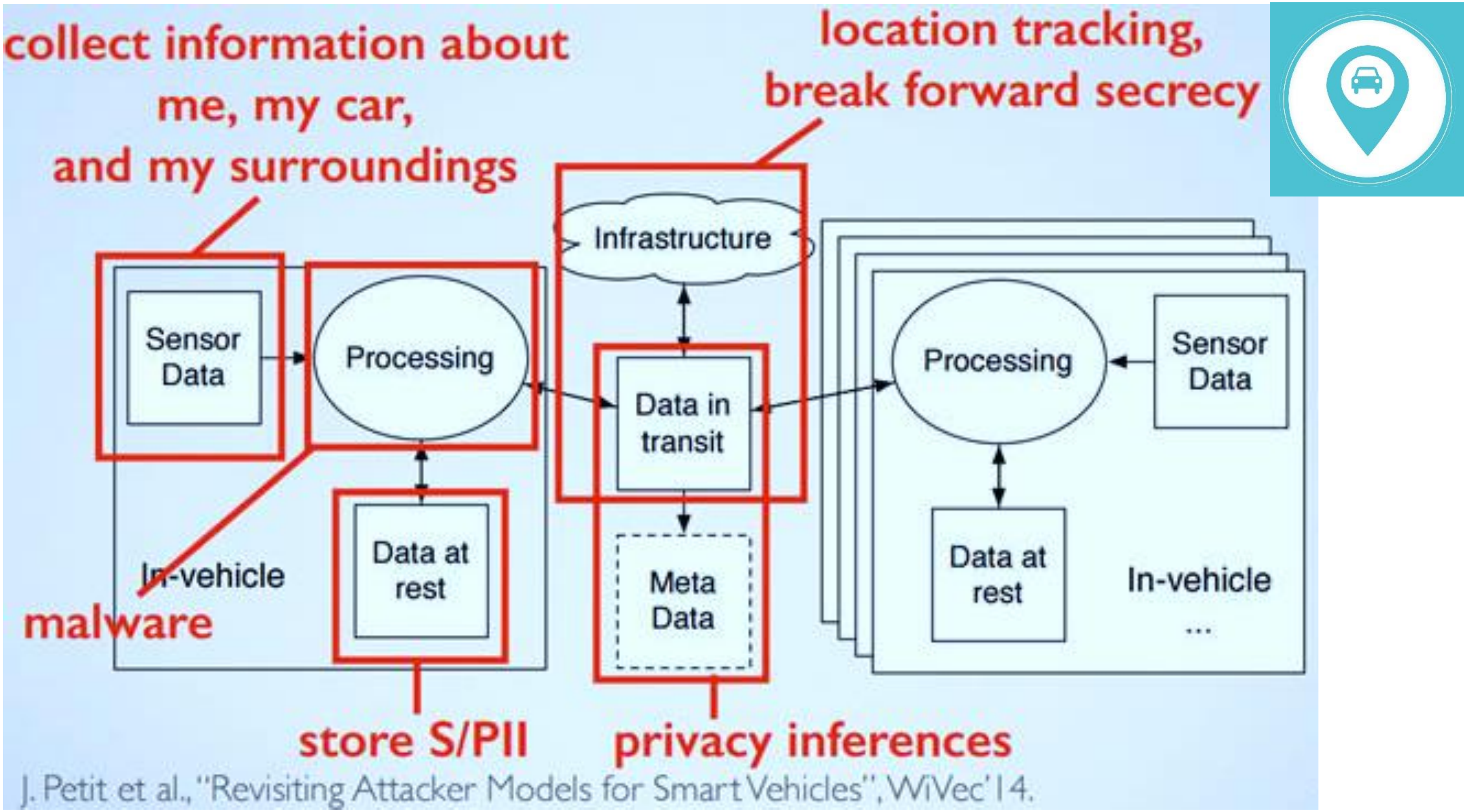
Selected Attacks on an Embedded System – Security, Privacy, IP Rights



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

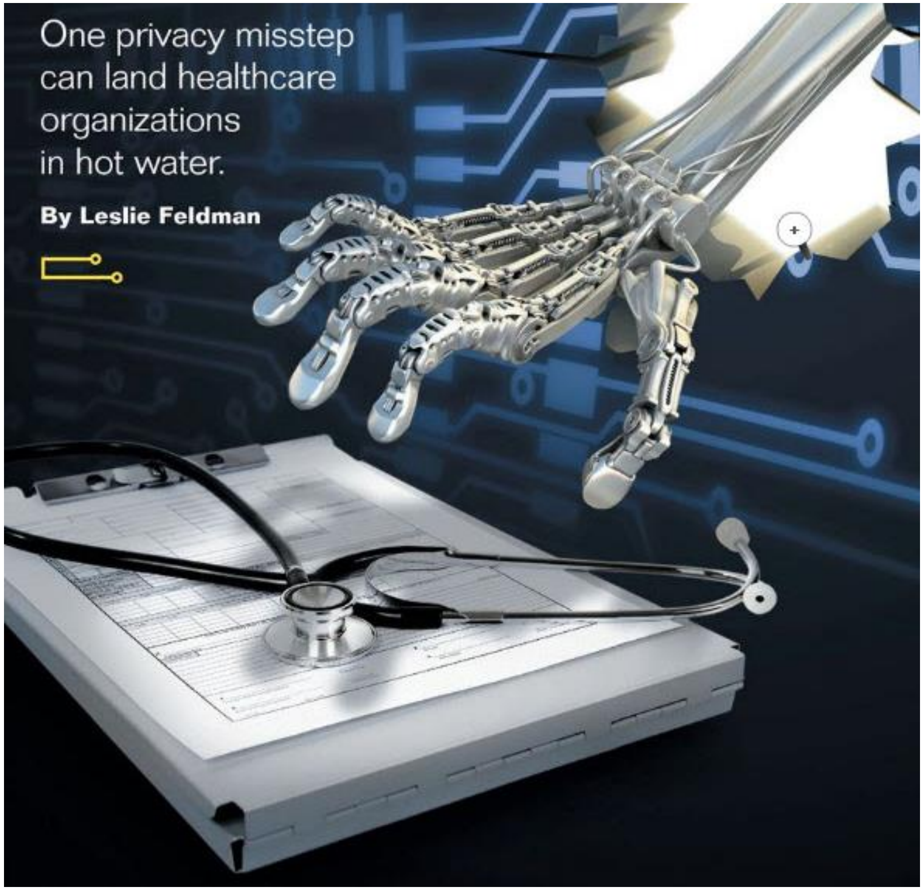
Privacy Challenge – System, Location



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

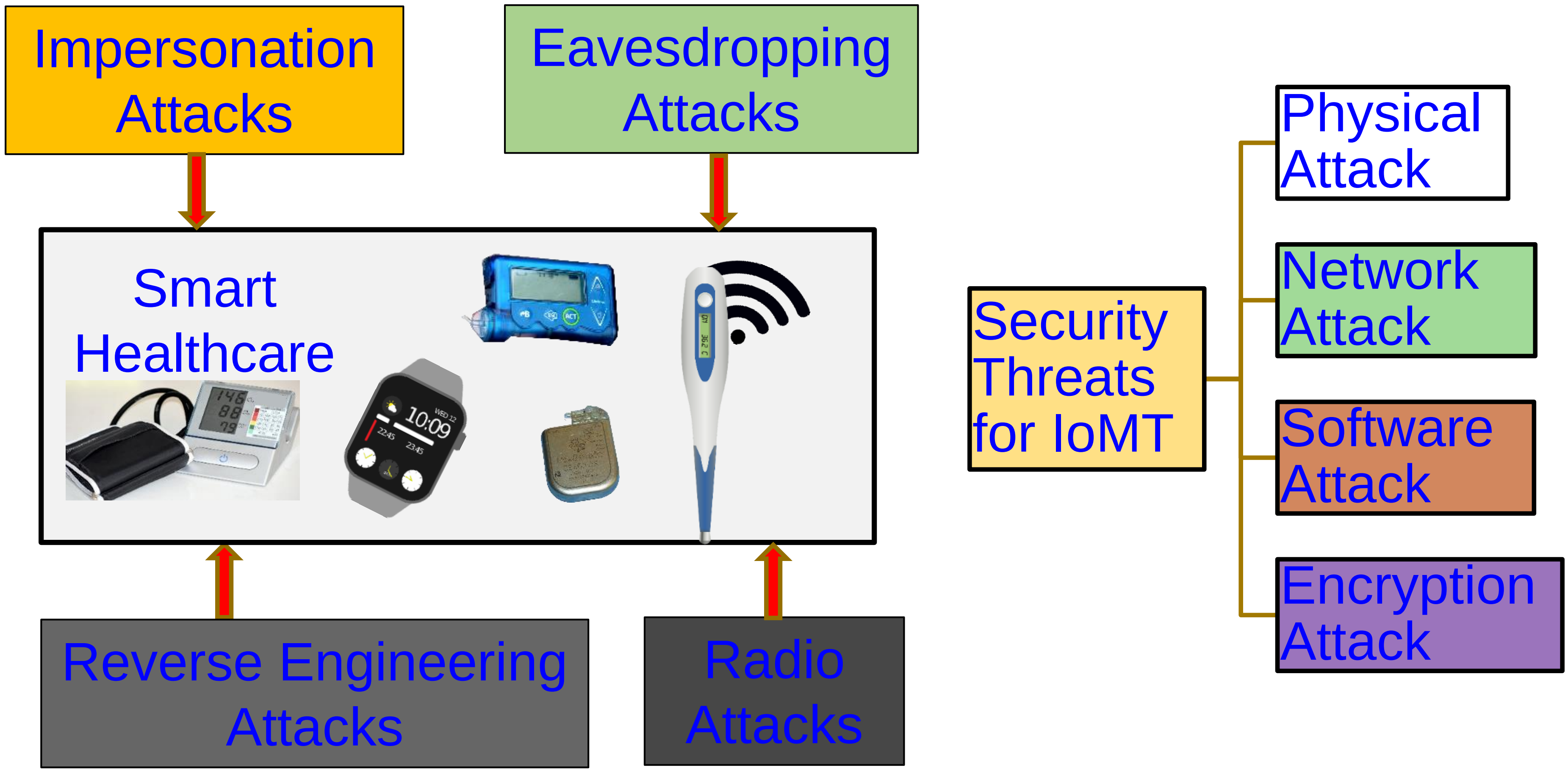
Privacy Challenge – Personal Data

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



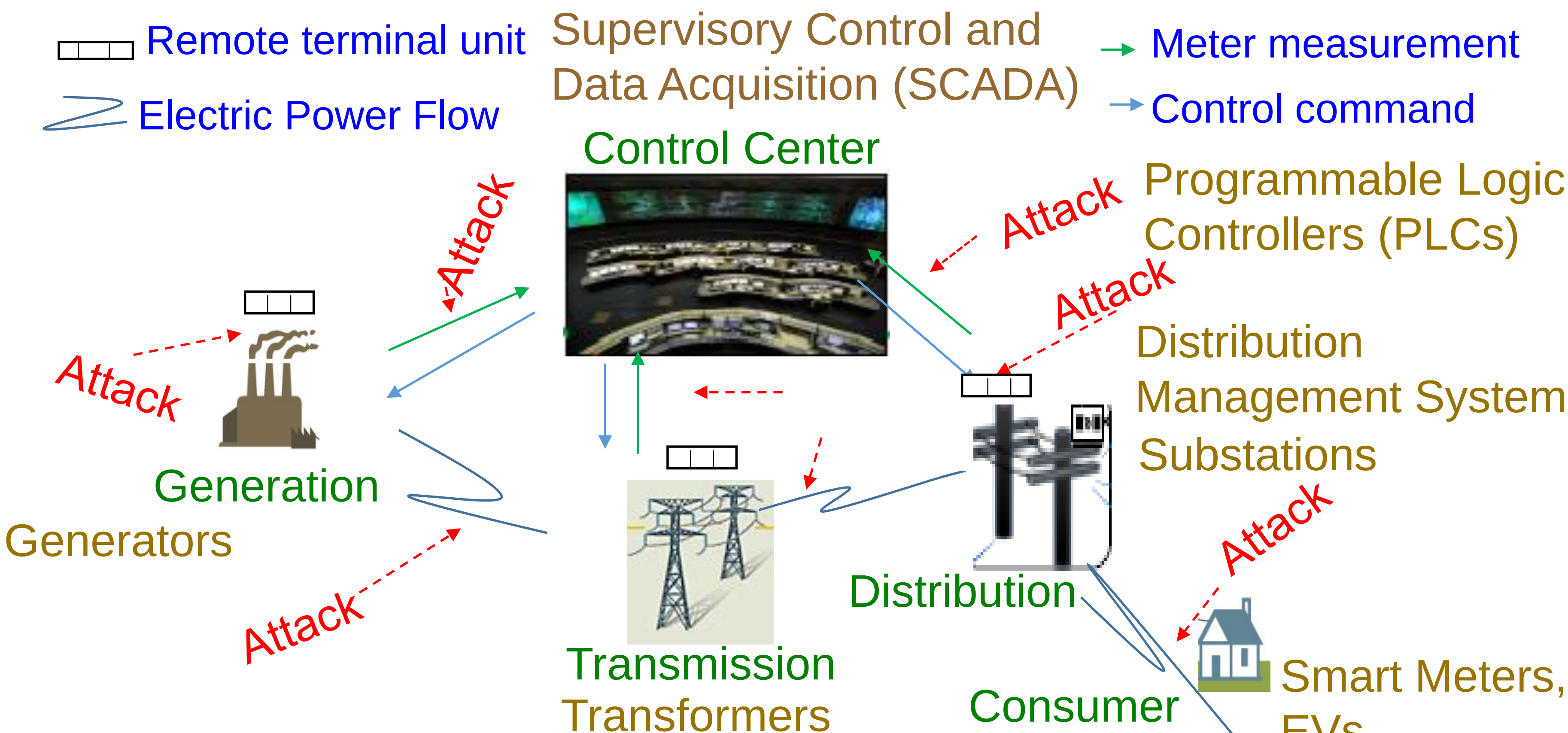
Source: http://blog.veriphyr.com/2012/06/electronic-medical-records-security-and.html

IoMT Security – Selected Attacks



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

Smart Grid - Vulnerability



ICT components of smart grid is cyber vulnerable.

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

Smart Grid Attacks can be Catastrophic

Vulnerabilities

Threats

- Security group knowledge
  - Management deficiencies of network access rules
  - Inaccurate critical assests documentation
- Information leakage
  - Unencrypted services in IT systems
  - Weak protection credentials
- Access point
  - Improper access point
  - Remote access deficiency
  - Firewall filtering deficiency
- Unpatched System
  - Unpatched operating system
  - Unpatched third party application
- Weak cyber security
  - Buffer overflow in control system services
  - SQL injection vulnerability

Source of Threats

- Phishers
- Nation
- Hacker
- Insider
- Terrorist
- Spammers
- Spyware /Malware authors

Attacks

- Stuxnet
- Night Dragon
- Virus
- Denial of service
- Trojan horse
- Worm
- Zero day exploit
- Logical bomb
- Phishing
- Distributed DoS
- False data Injection attack

Impacts

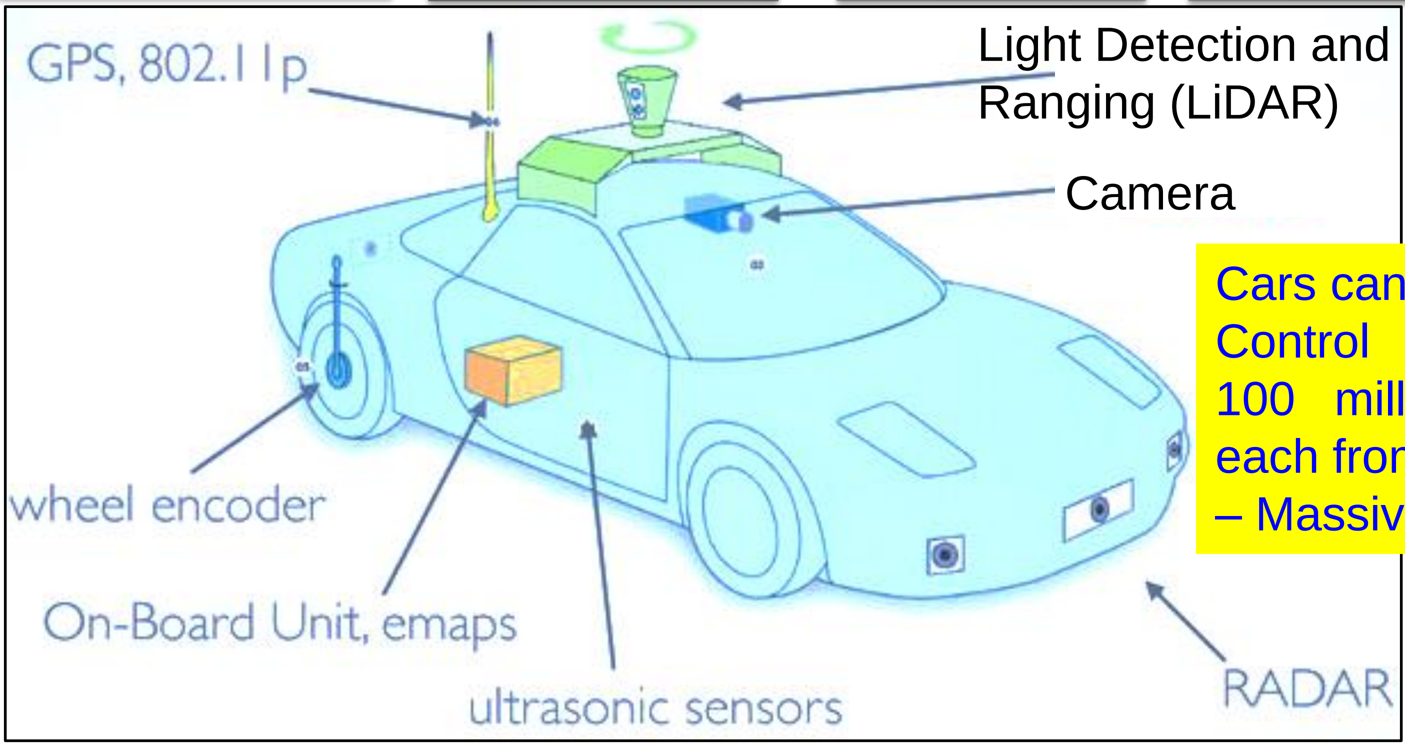
- Ukraine power attack, 2015
- Stuxnet attack in Iran, 2010
- Browns Ferry plant, Alabama 2006
- Emergency shut down of Hatch Nuclear Power Plant, 2008
- Slammer attack at Davis-Besse power plant, 2001
- Attacks at South Korea NPP, 2015

Source: R. K. Kaur, L. K. Singh and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 10-15, March 2019.

System Security – Smart Car

Selected Attacks on Autonomous Cars

- Replay
- Relay
- Jamming
- Spoofing
- Tracking



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

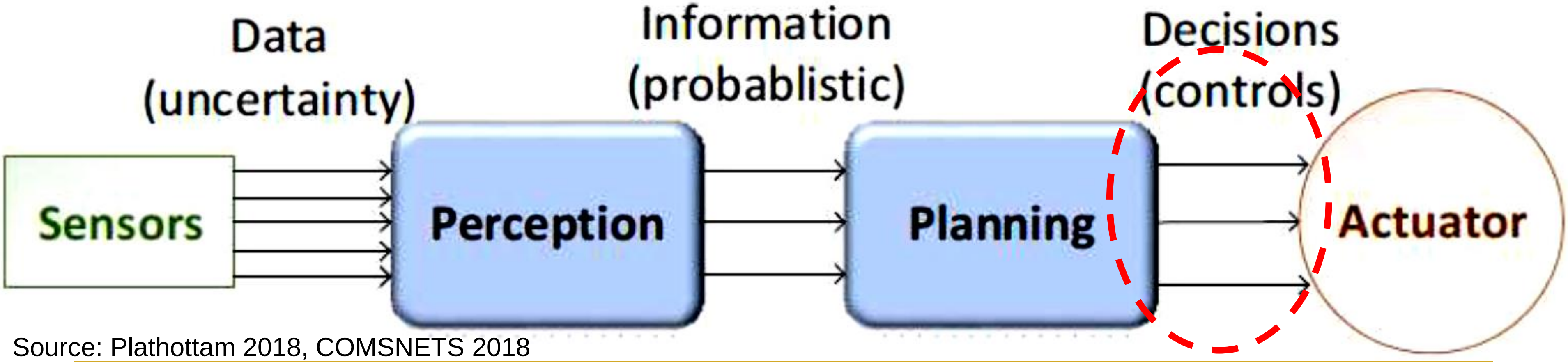
Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

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

Source: Petit 2015: IEEE-TITS Apr 2015

Smart Car – 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.



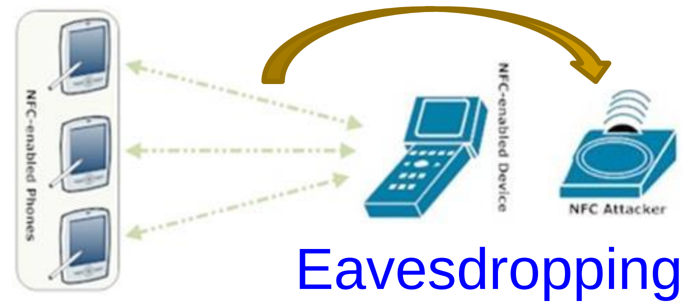
Source: Plathottam 2018, COMSNETS 2018

NFC Security - Attacks

Selected NFC Attacks

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

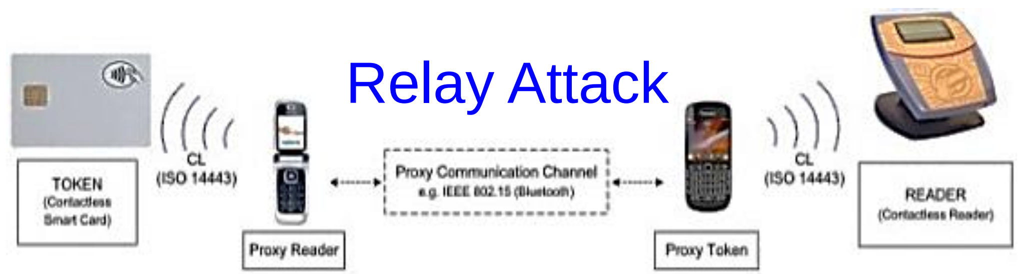
Source: http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497



Eavesdropping

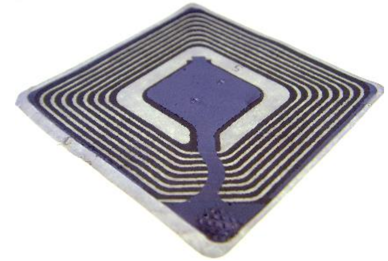
Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

Relay Attack



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

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

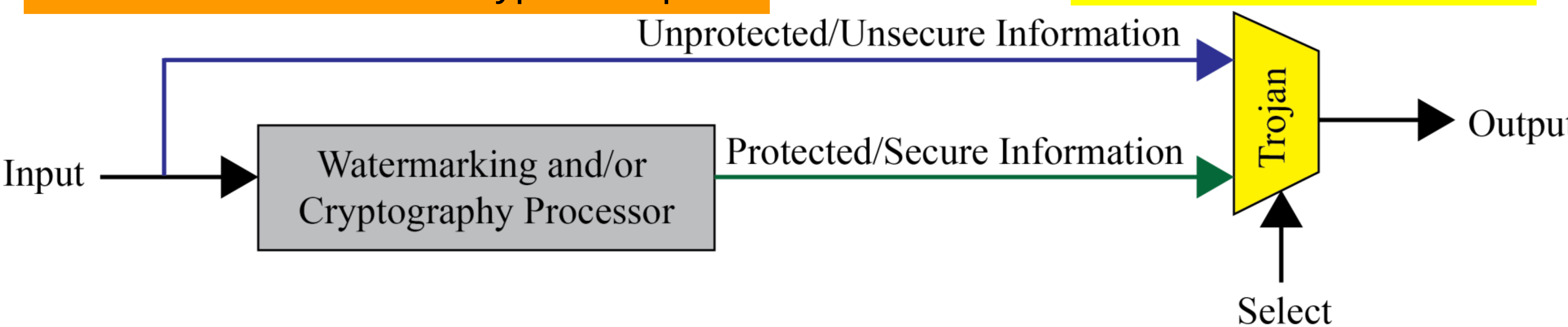
Source: Khattab 2017: Springer 2017 RFID Security

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

How Secure is AES Encryption?

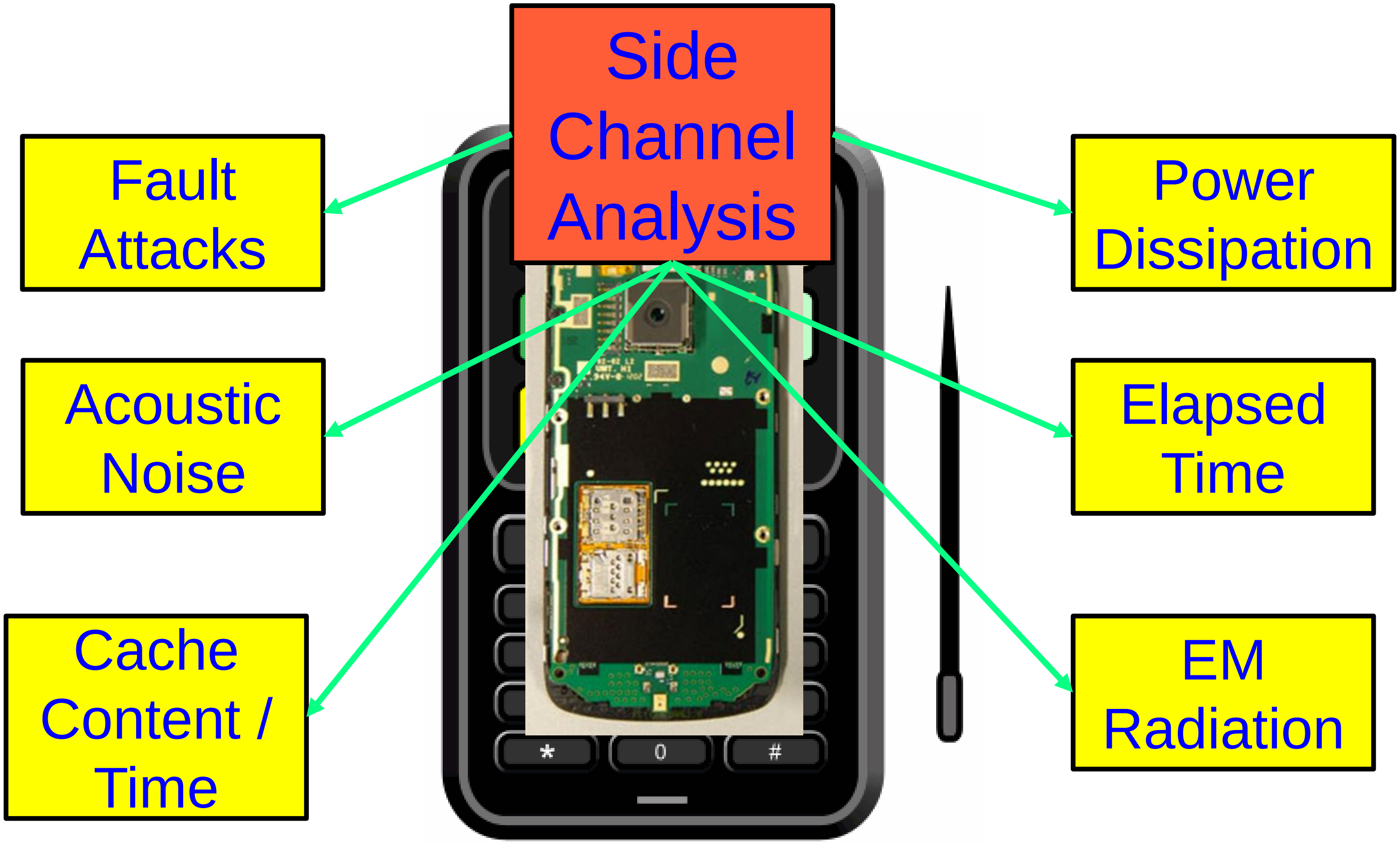
- Brute force a 128 bit key ?
- If you assume
  - Every person on the planet owns 10 computers
  - Each of these computers can test 1 billion key combinations per second
  - There are 7 billion people on the planet
  - On average, you can crack the key after testing 50% of the possibilities
  - Then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

Age of the Earth 4.54 ± 0.05 billion years

Age of the Universe 13.799 ± 0.021 billion years

Source: Parameswaran Keynote iNIS-2017

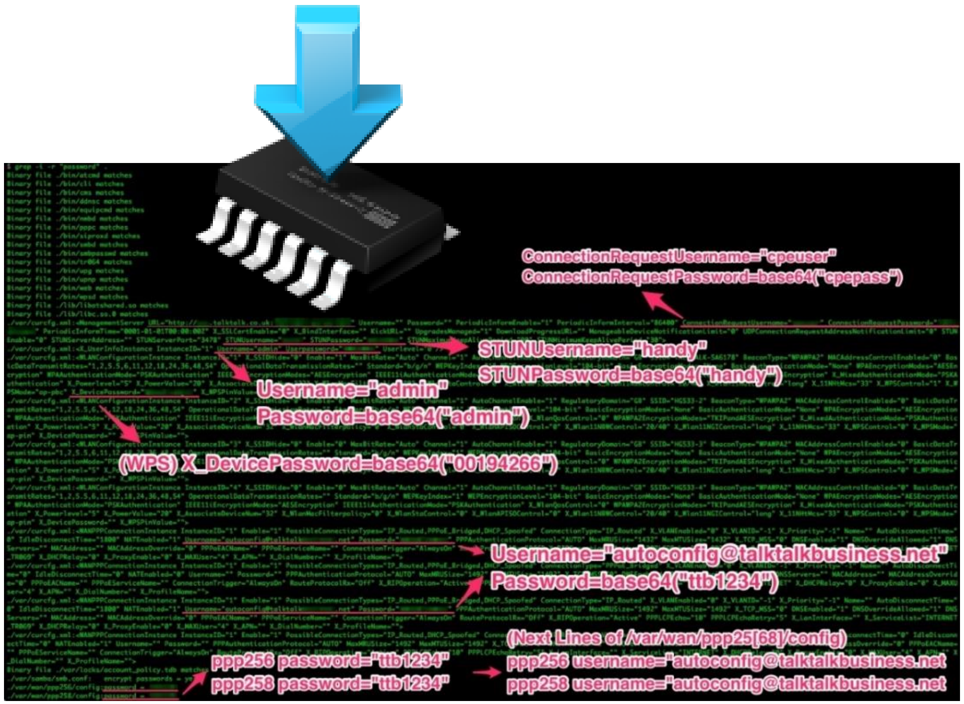
Side Channel Analysis Attacks



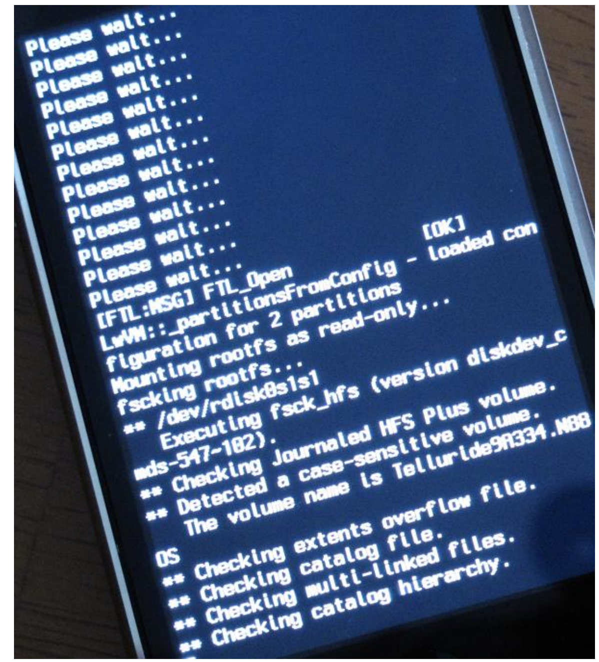
Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

Firmware Reverse Engineering – Security Threat for Embedded System



Extract, modify, or reprogram code



OS exploitation, Device jailbreaking

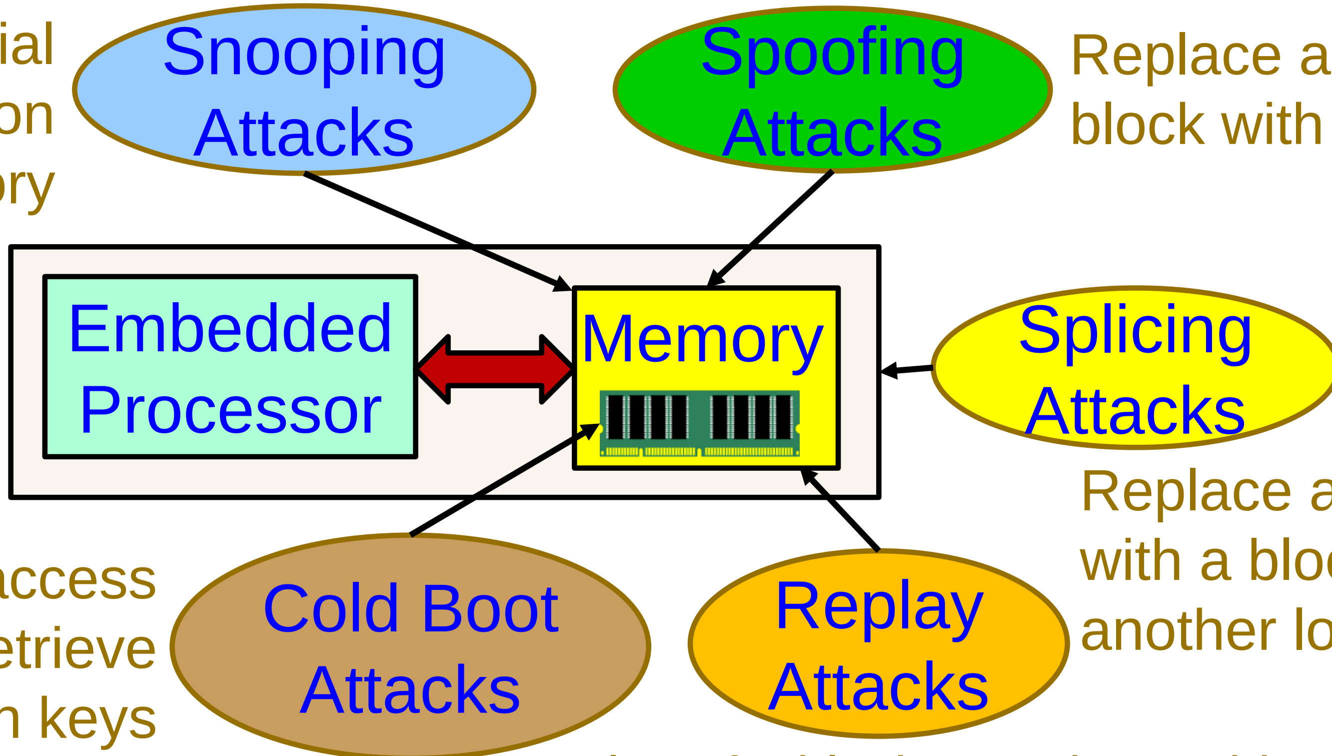
Source: http://jcjc-dev.com/

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

Attacks on Embedded Systems' Memory

Read confidential information in memory

Replace a block with fake



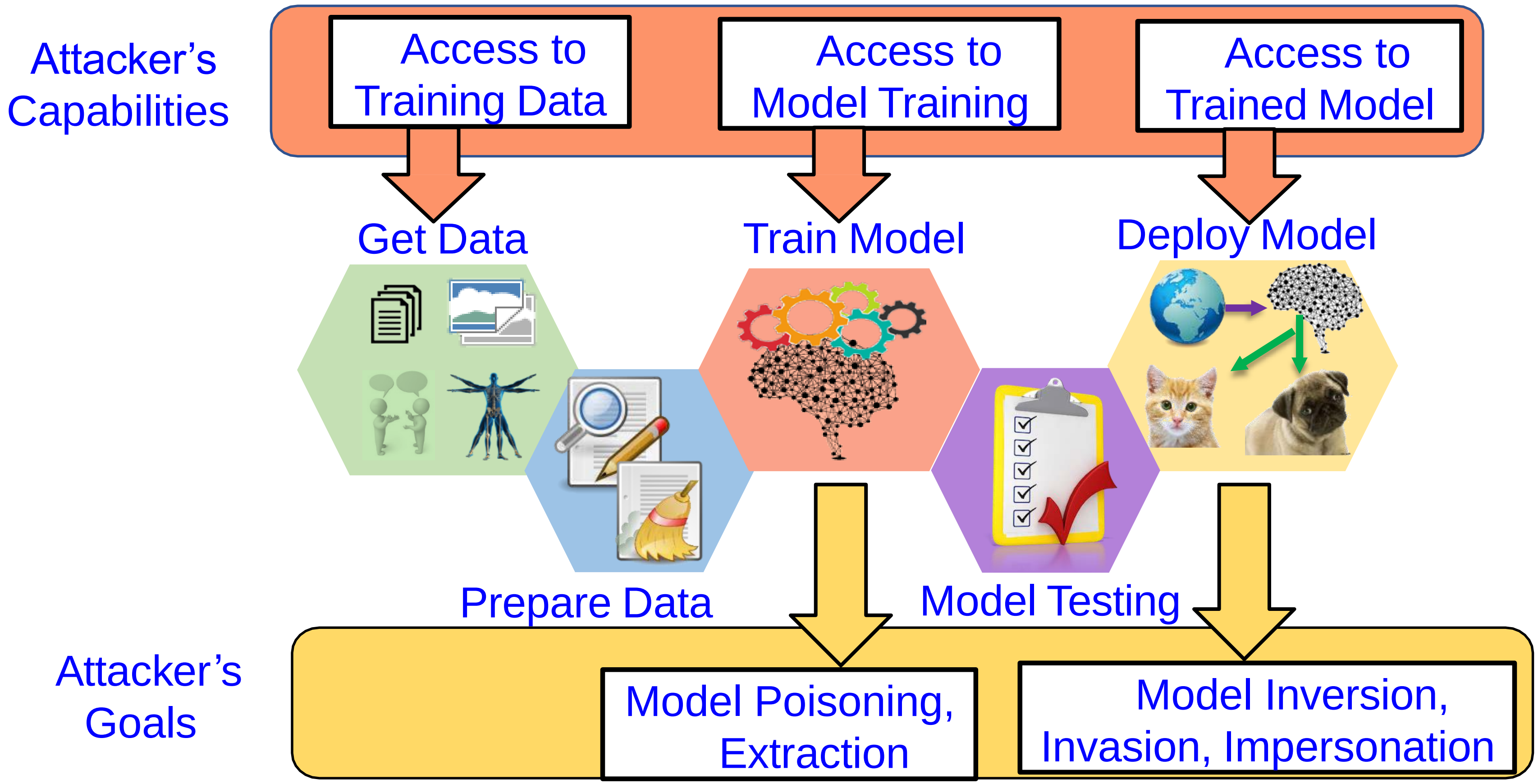
Replace a block with a block from another location

Physical access memory to retrieve encryption keys

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

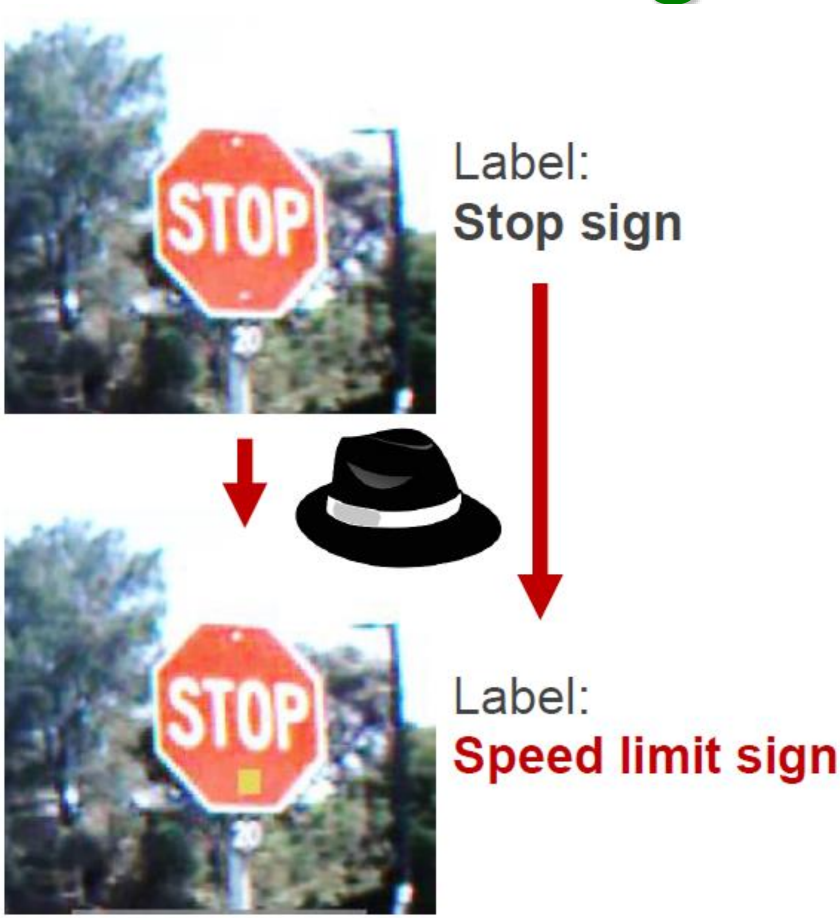
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "TSV: A Novel Energy Efficient Memory Integrity Verification Scheme for Embedded Systems", *Elsevier Journal of Systems Architecture*, Vol. 59, No. 7, Aug 2013, pp. 400-411.

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

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

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

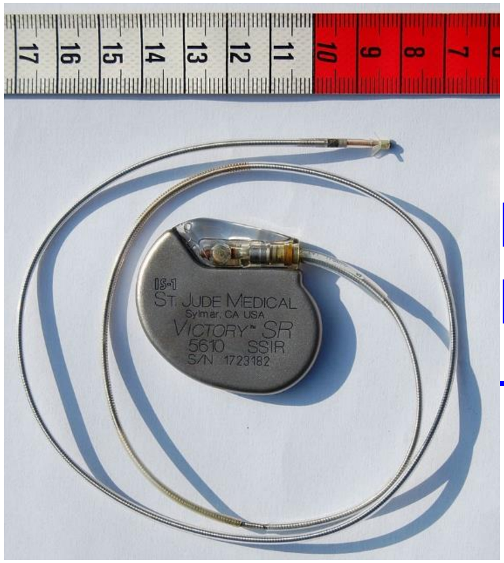
Source: D. A. Hahn, A. Munir, and S. P. Mohanty, “Security and Privacy Issues in Contemporary Consumer Electronics”, *IEEE Consumer Electronics Magazine*, Volume 8, Issue 1, January 2019, pp. 95--99.

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

IT Security	IoT Security
IT infrastructure may be well protected rooms	IoT may be deployed in open hostile environments
Limited variety of IT network devices	Significantly large variety of IoT devices
Millions of IT devices	Billions of IoT devices
Significant computational power to run heavy-duty security solutions	May not have computational power to run security solutions
IT security breach can be costly	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.

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

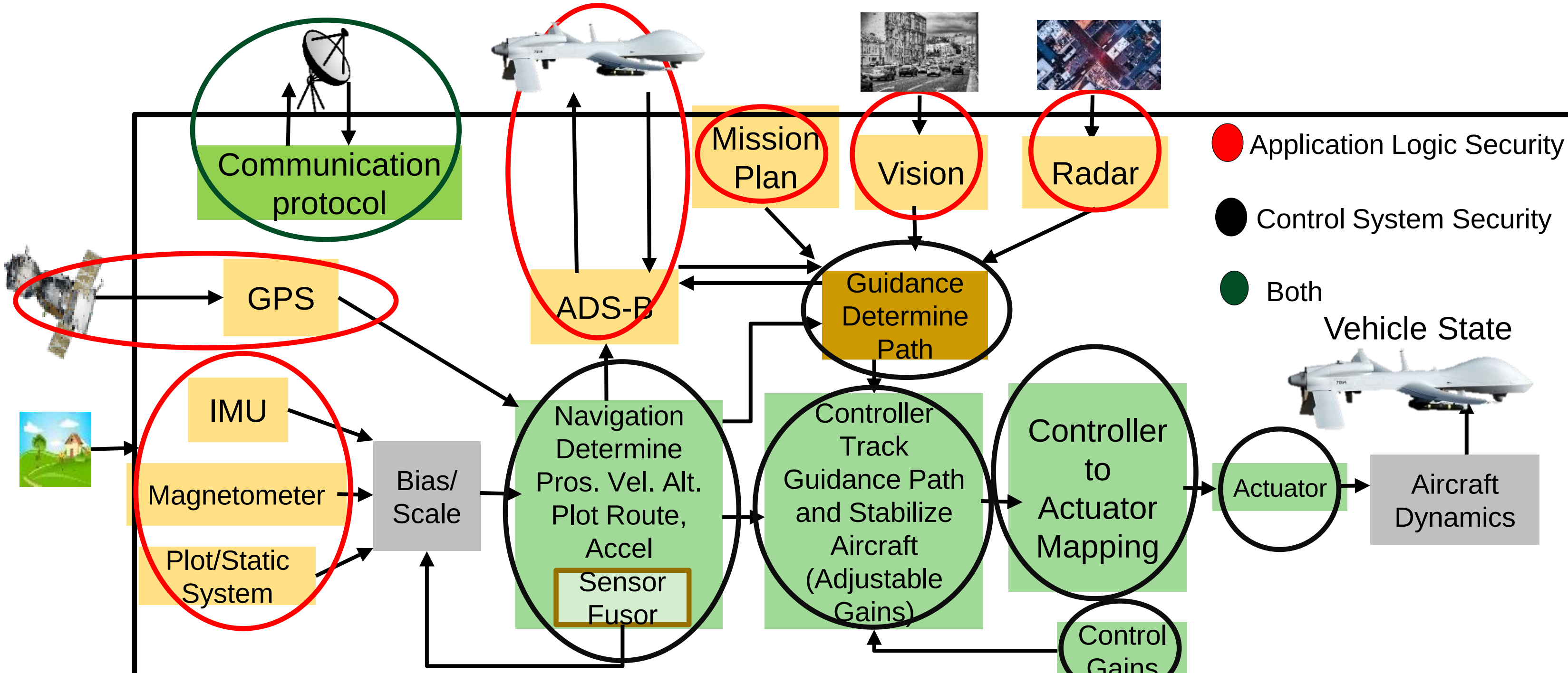
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

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

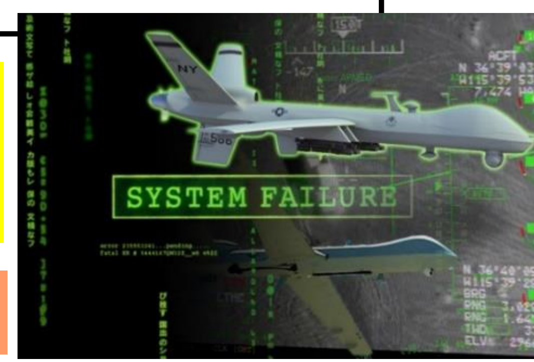


Source: http://www.secmation.com/control-design/

Security Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints



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

Smart Grid Security Constraints

Smart Grid – Security Objectives

- Availability
- Integrity
- Confidentiality

Smart Grid – Security Requirements

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

Smart Grid – Security Solution Constraints

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

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

Blockchain has Many Challenges

Blockchain Challenges

- Fake Block Generation
- High Energy Consumption
- Lack of Scalability
- High Latency
- Lack of Privacy
- Limited Onchain Storage Capability
- 51% Attack

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 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

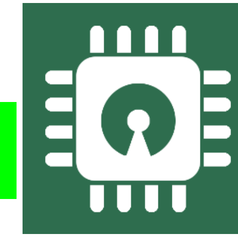
Source: J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019.

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.

Security Attacks Can be Software and Hardware Based



Software Based

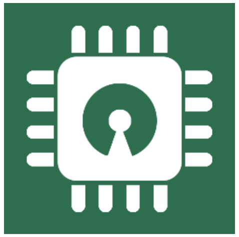
- Software attacks via communication channels
- Typically from remote
- More frequent
- Selected Software based:
  - Denial-of-Service (DoS)
  - Routing Attacks
  - Malicious Injection
  - Injection of fraudulent packets
  - Snooping attack of memory
  - Spoofing attack of memory and IP address
  - Password-based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

Security - Software Vs Hardware



Software Based

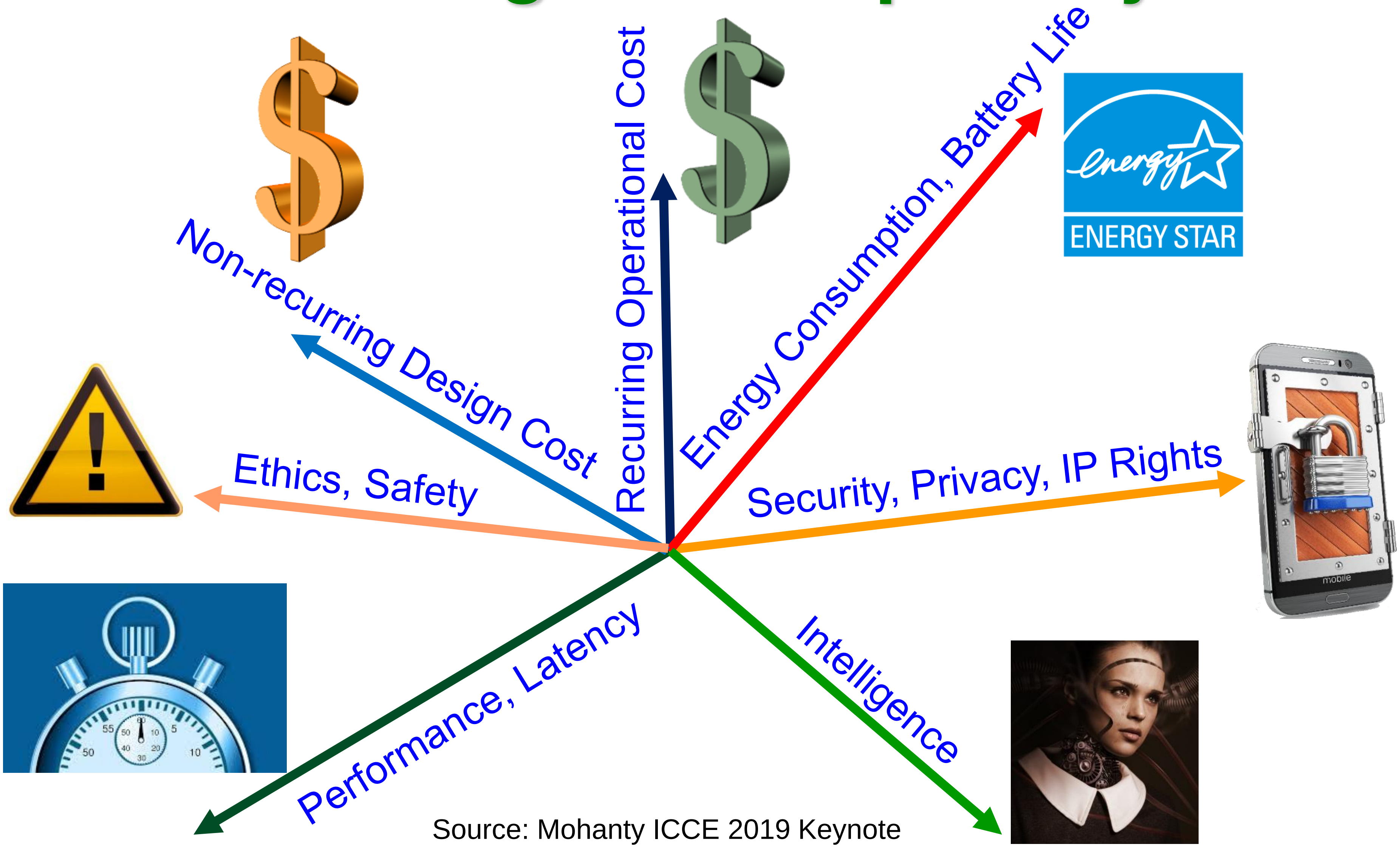
- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can’t stop hardware reverse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

Hardware Based

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

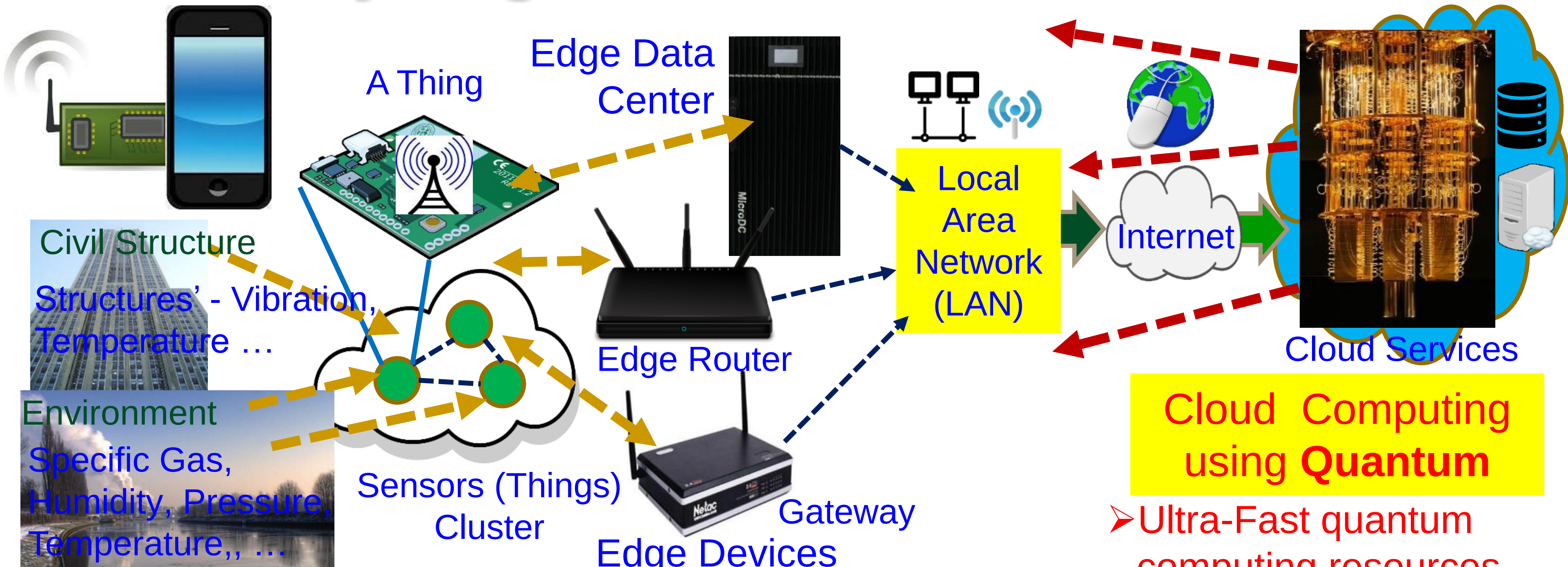
Source: Mohanty ICCE Panel 2018

IoT/CPS Design – Multiple Objectives



Source: Mohanty ICCE 2019 Keynote

A Security Nightmare - by Quantum Computing



Cloud Computing using **Quantum**

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

In-Sensor/End-Device Computing

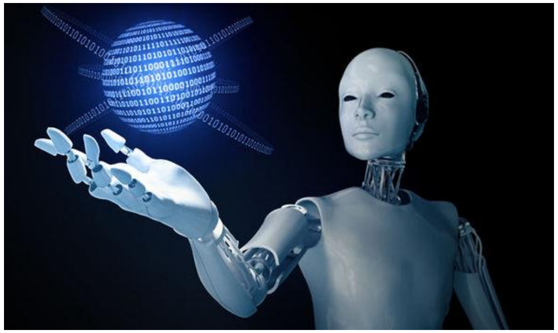
- Minimal computational resource
- Negligible latency in network
- Very lightweight security

Edge Computing

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

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

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



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

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

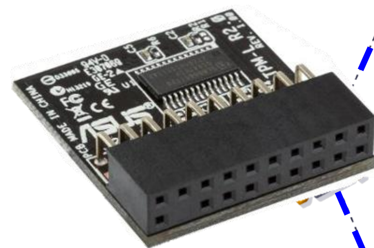
Memory Protection

Digital Core IP Protection

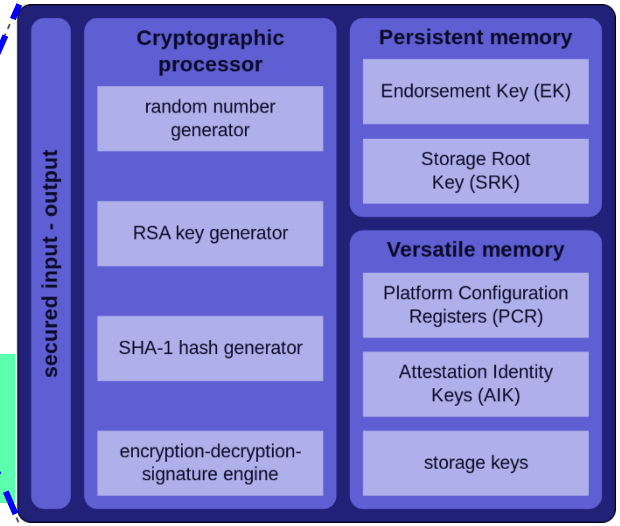
Source: Mohanty ICCE 2018 Panel

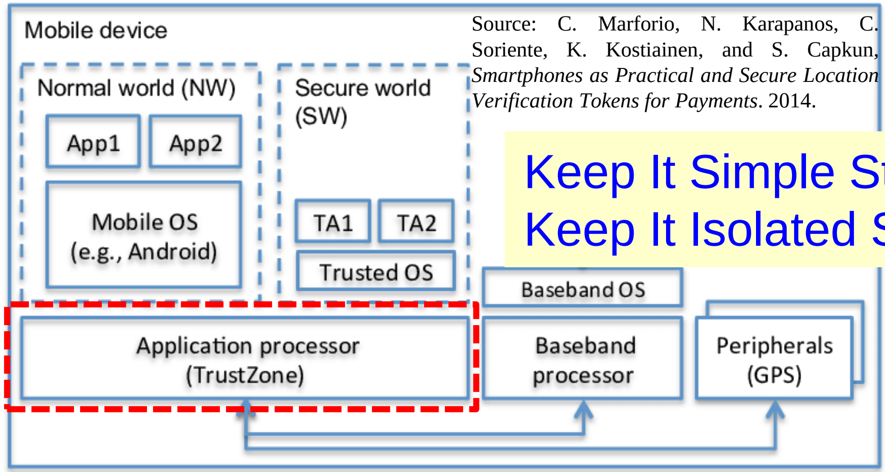
Hardware Security Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



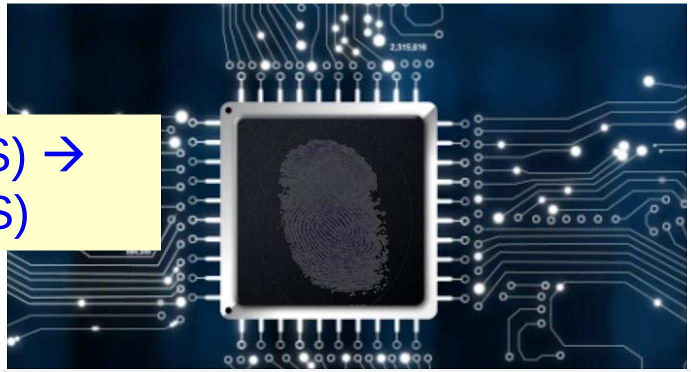
Trusted Platform Module (TPM)





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)

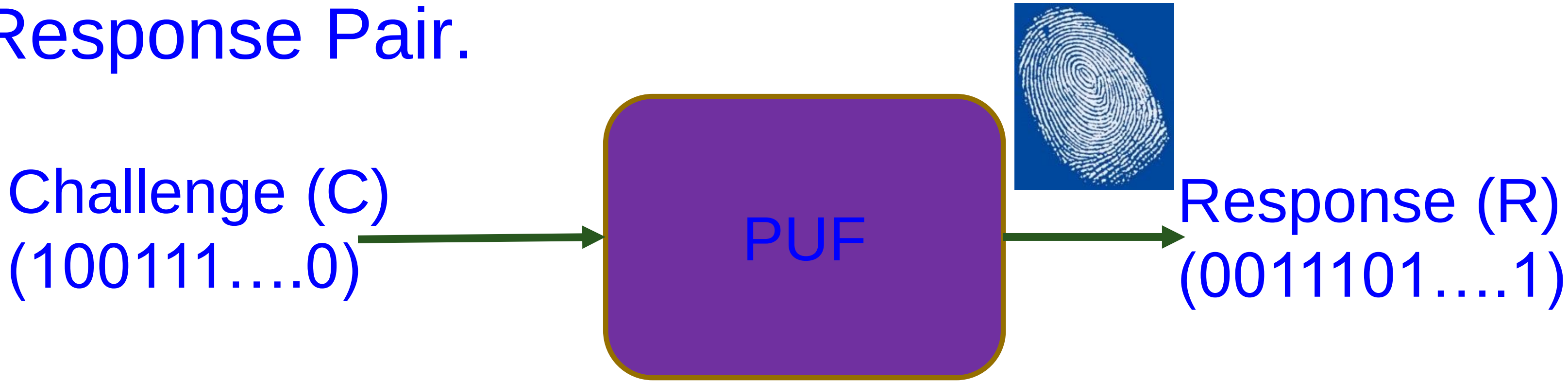


Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Physical Unclonable Functions (PUFs)

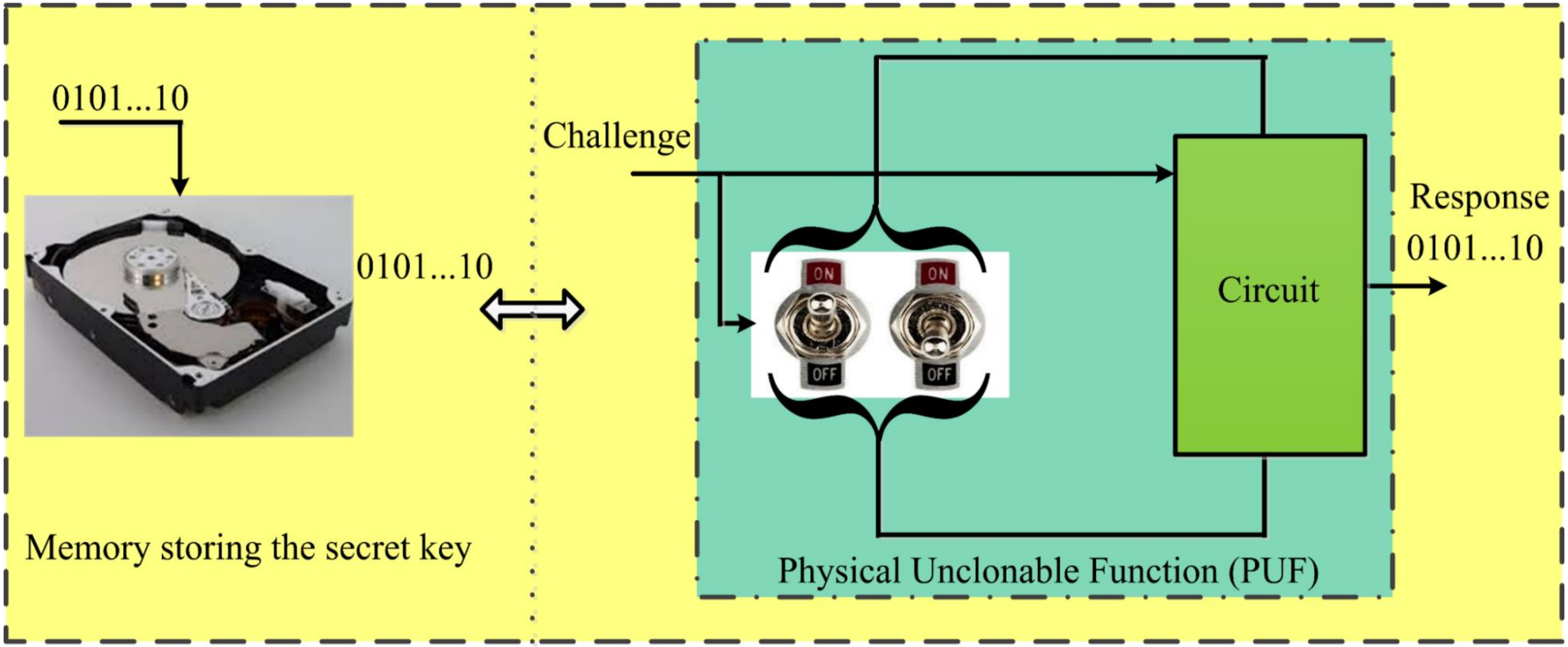
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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.

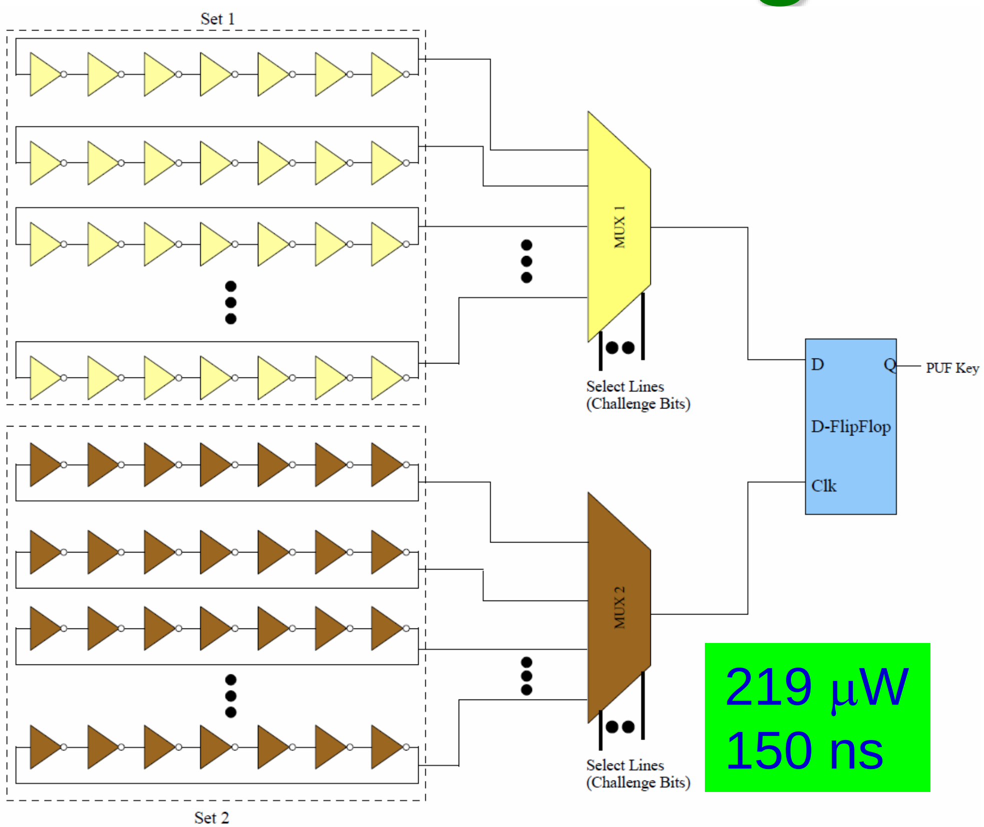
PUFs Don't Store Keys



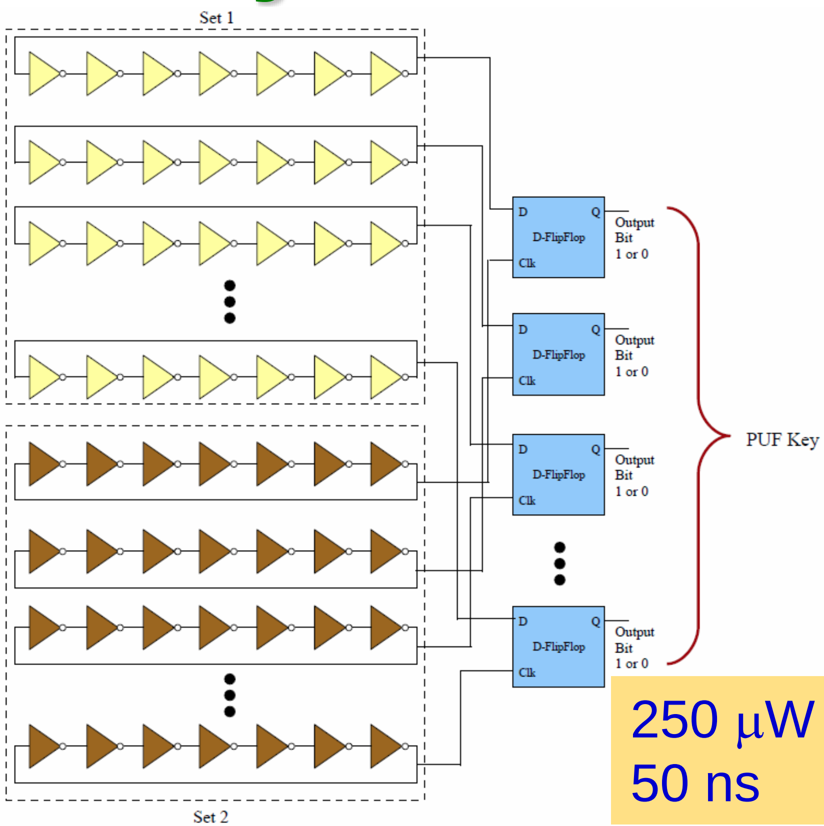
PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

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.

We Have Design a Variety of PUFs



219 μW
150 ns



250 μW
50 ns

Power Optimized Hybrid Oscillator Arbiter PUF

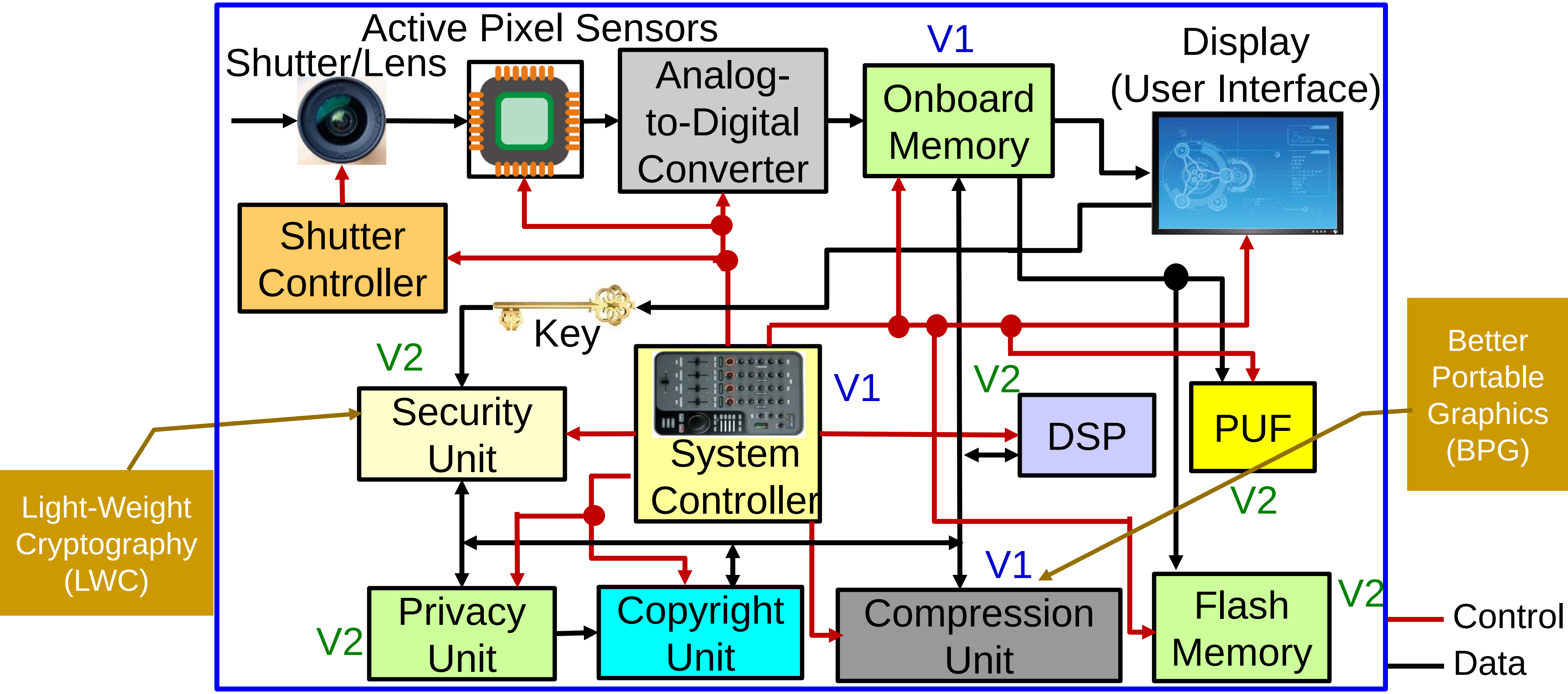
Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS

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.

Secure Digital Camera – My Invention

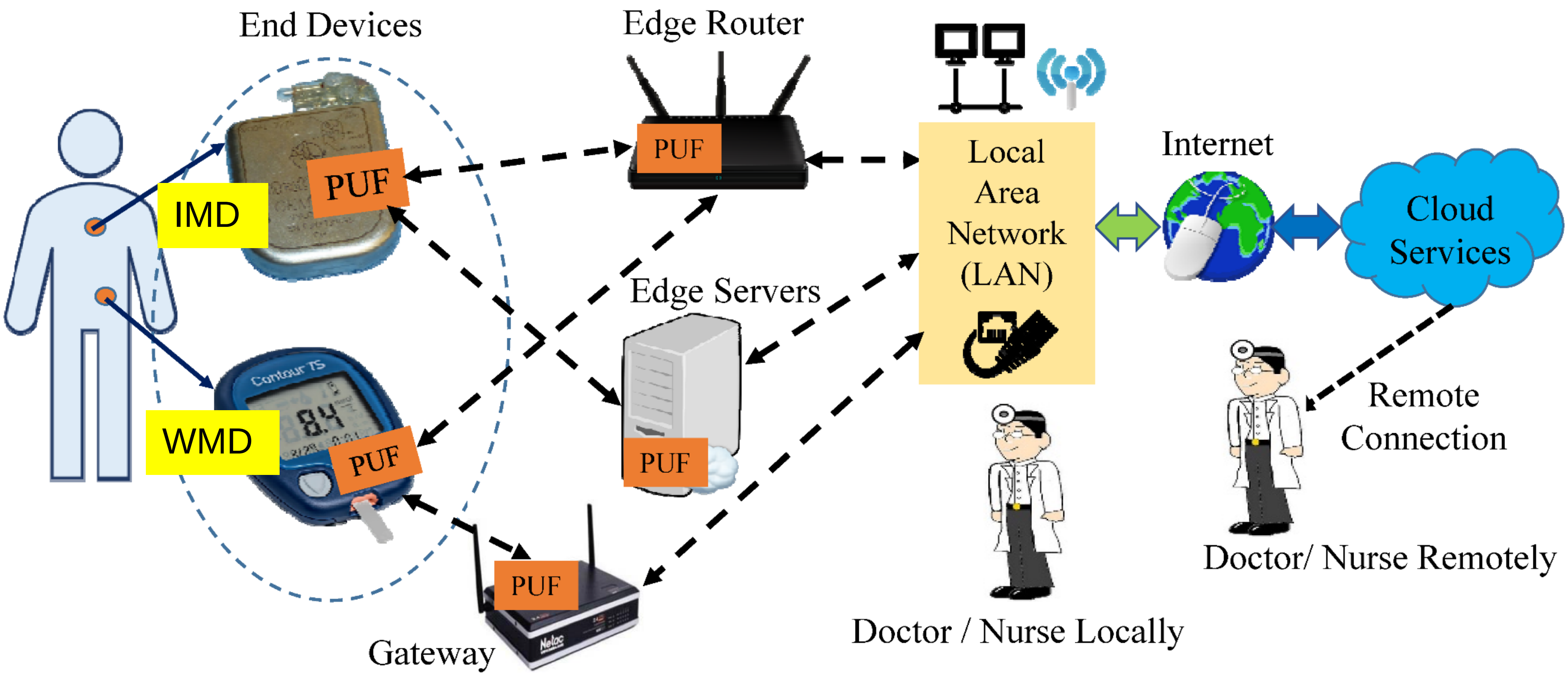


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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

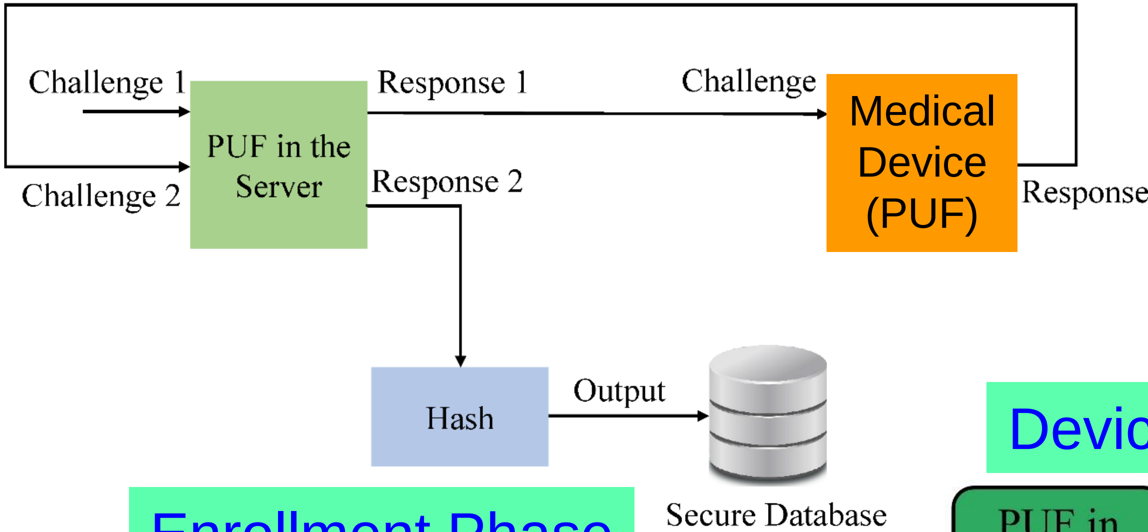
Source: S. P. Mohanty, “A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management”, Elsevier Journal of Systems Architecture (JSA), Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

Our Secure by Design Approach for Robust Security in Healthcare CPS



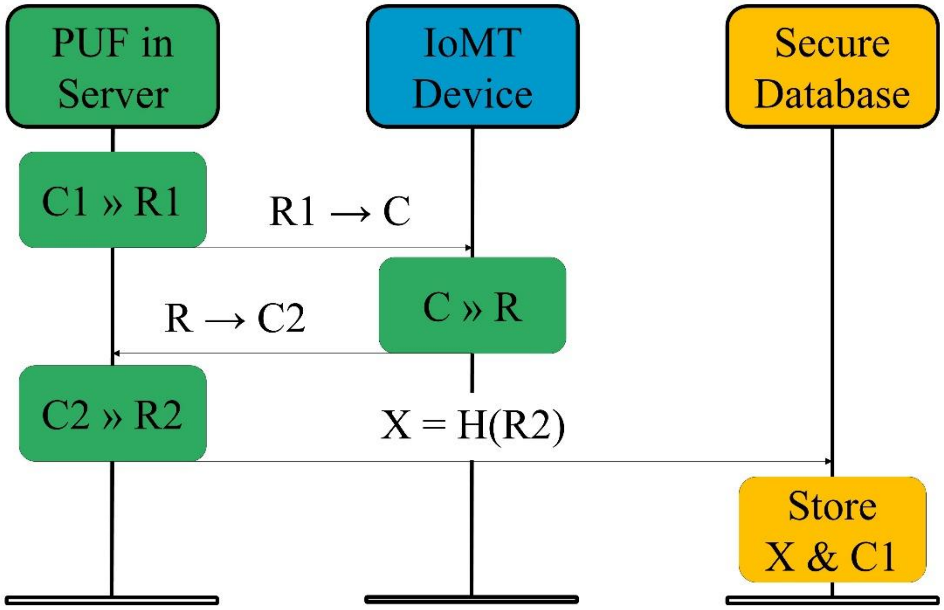
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec



At the Doctor
- as a new Device comes for an User

Device Registration Procedure

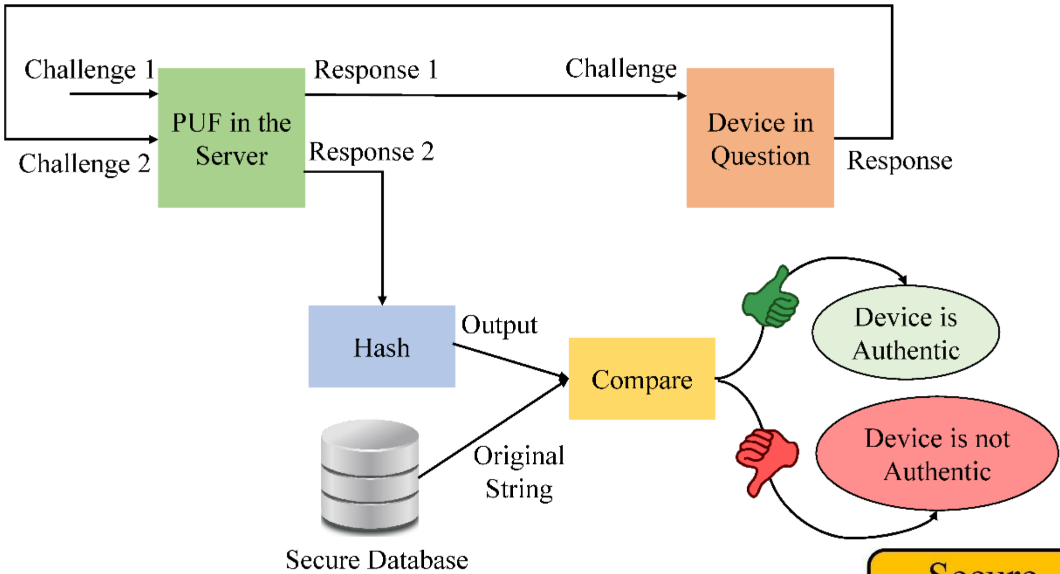


Enrollment Phase

PUF Security Full Proof:
- Only server PUF Challenges are stored, not Responses
- Impossible to generate Responses without PUF

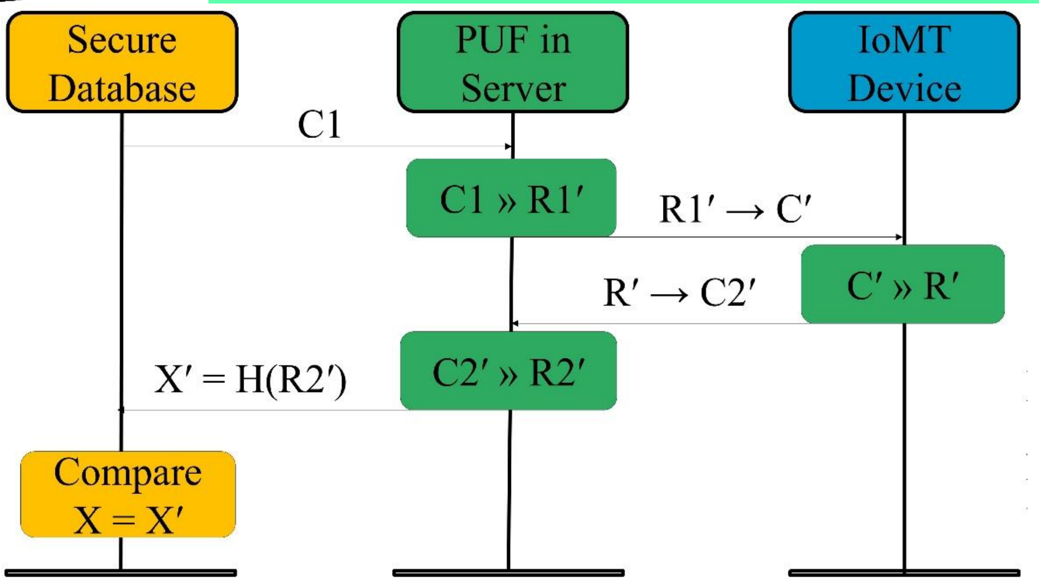
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec



Authentication Phase

Device Authentication Procedure



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

IoMT Security – Our PMsec in Action

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

Output from Server during Enrollment

COM4

Send

```
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 1011100001011100101111000101111000101101001101110010100101000011
Sending key for authentication
```

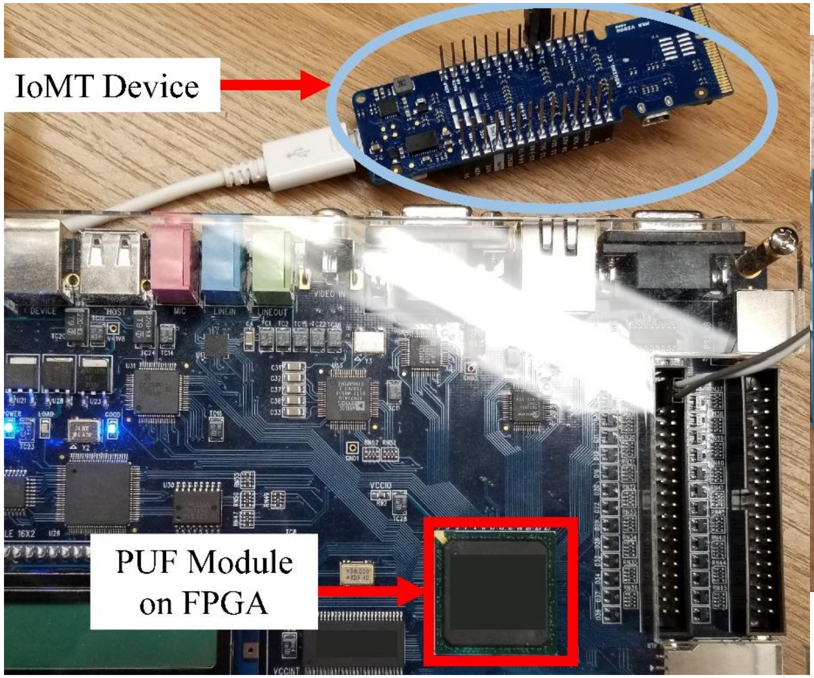
Output from IoMT Device

```
>>>
Hello
-----------Authentication Phase-----------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  1011100001011100101111000101111000101101001101110010100101000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>> |
```

Output from Server during Authentication

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

IoMT Security – Our Proposed PMsec



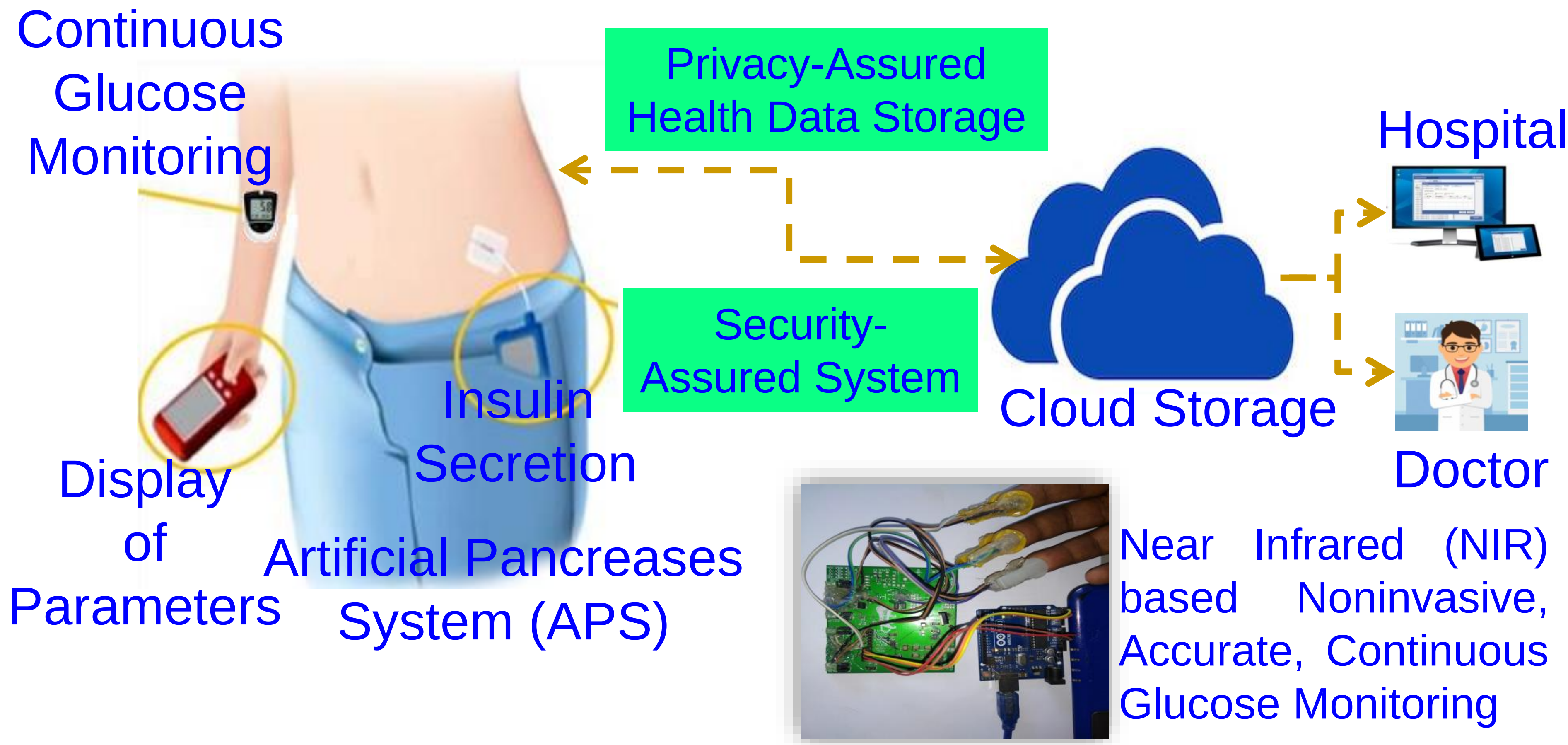
Average Power Overhead – 200 μW

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

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

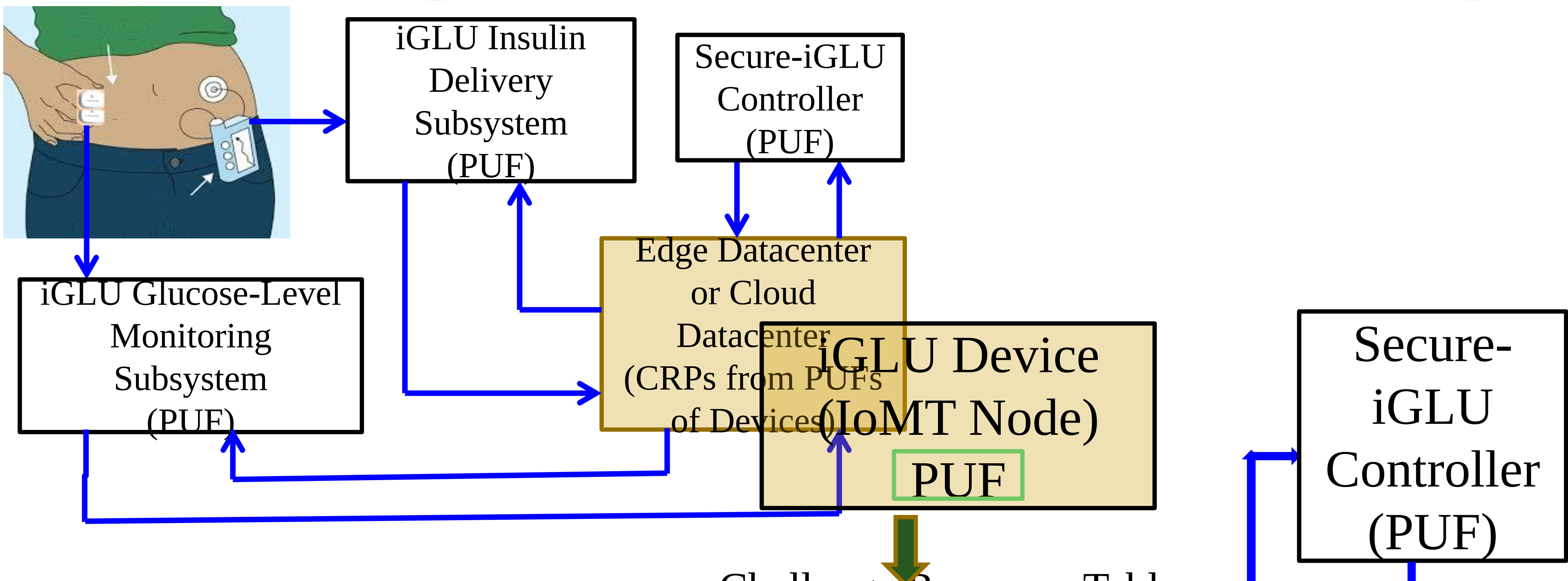
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics*, Vol 65, No 3, Aug 2019, pp. 388--397.

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

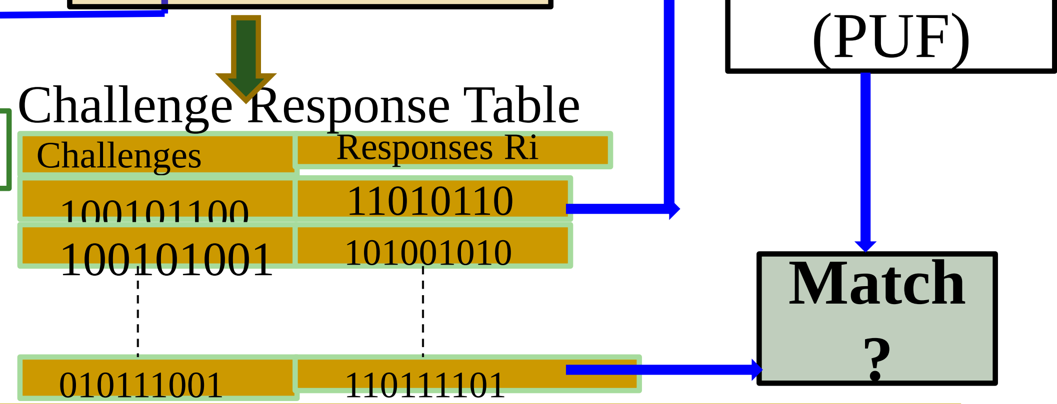


P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare", *IEEE Consumer Electronics Magazine (MCE),* Vol. 9, No. 1, January 2020, pp. 35–42.

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

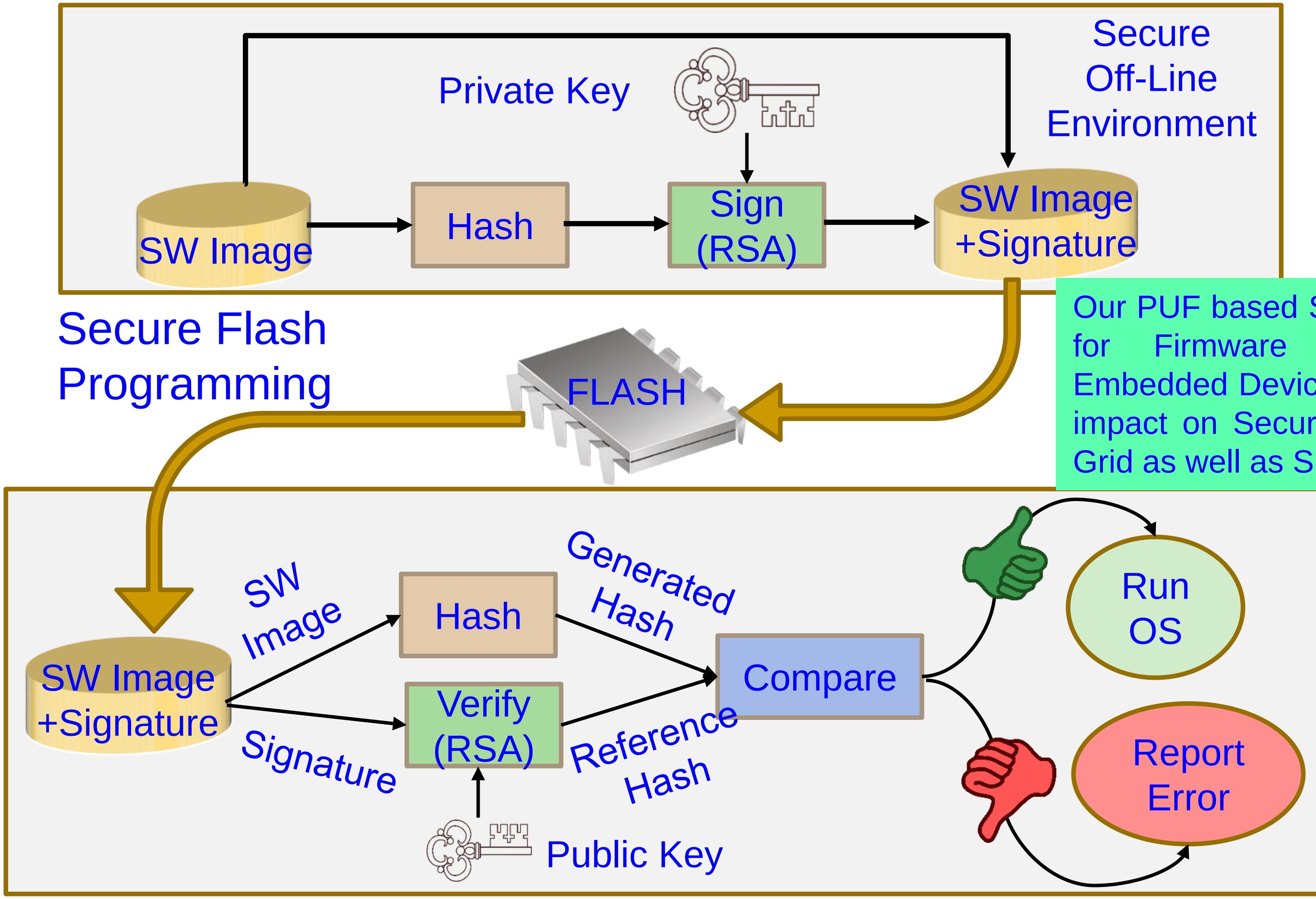


Arbiter PUF – 64-bit, 128-bit, 256 bit …



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

Firmware Security - Solution



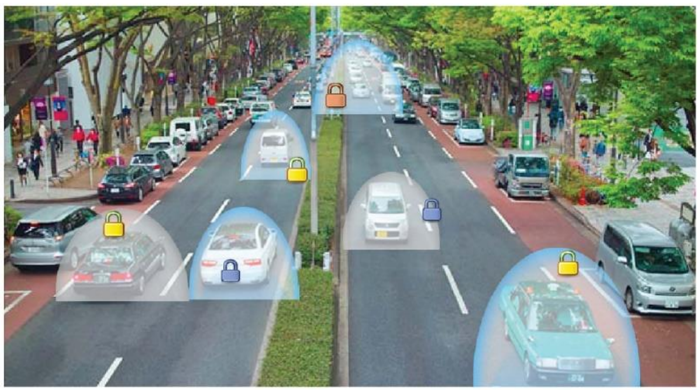
Our PUF based Solution can be used for Firmware Security of any Embedded Devices – Has significant impact on Security issues of Smart Grid as well as Smart Healthcare

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

Vehicular Security

IEEE Consumer Electronics Magazine

Volume 8 Number 6 NOVEMBER/DECEMBER 2019

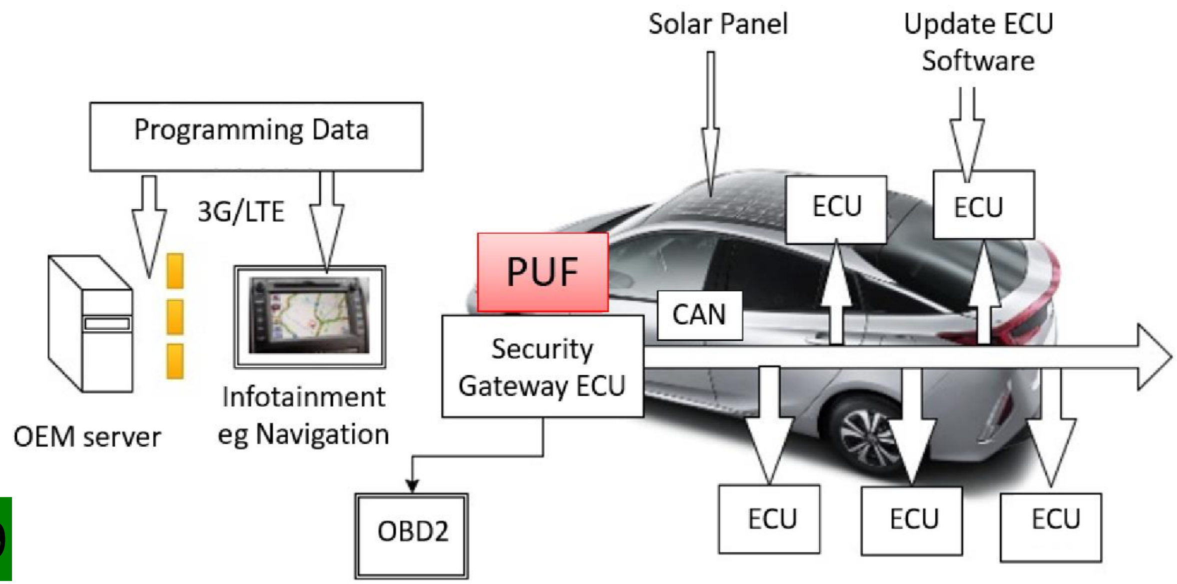


Vehicular Security

IEEE

November 2019

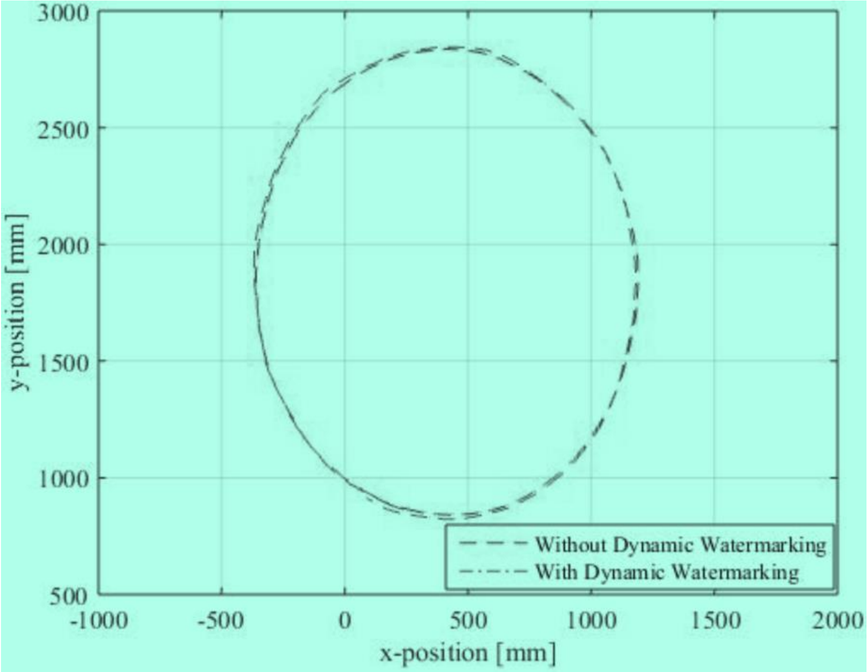
https://cesoc.ieee.org/



Source: C. Labrado and H. Thapliyal, "Hardware Security Primitives for Vehicles," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 99-103, Nov. 2019.

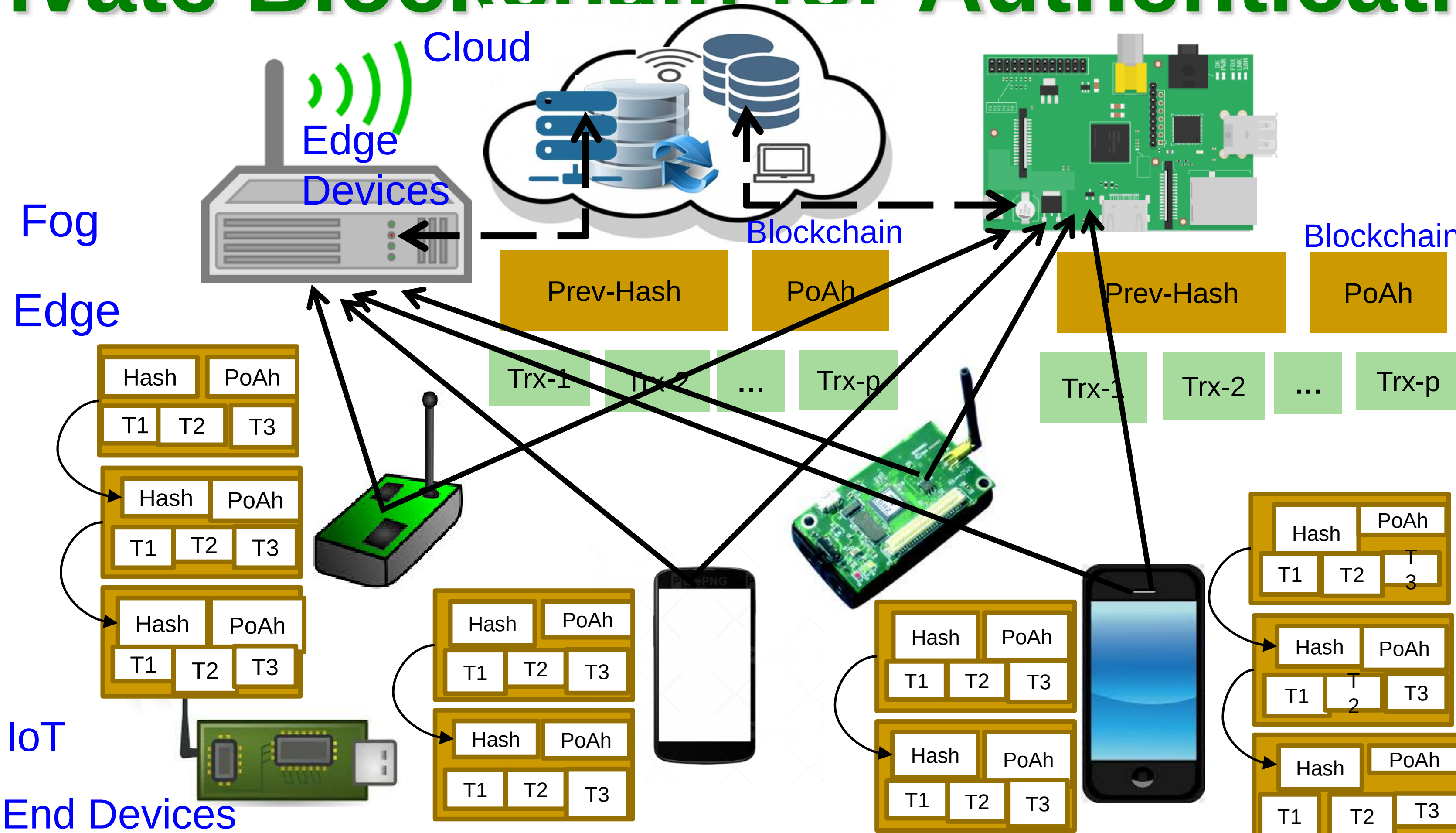
Autonomous Car Security – Collision Avoidance

- 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

Our PoAh-Chain: The IoT Friendly Private Blockchain for Authentication



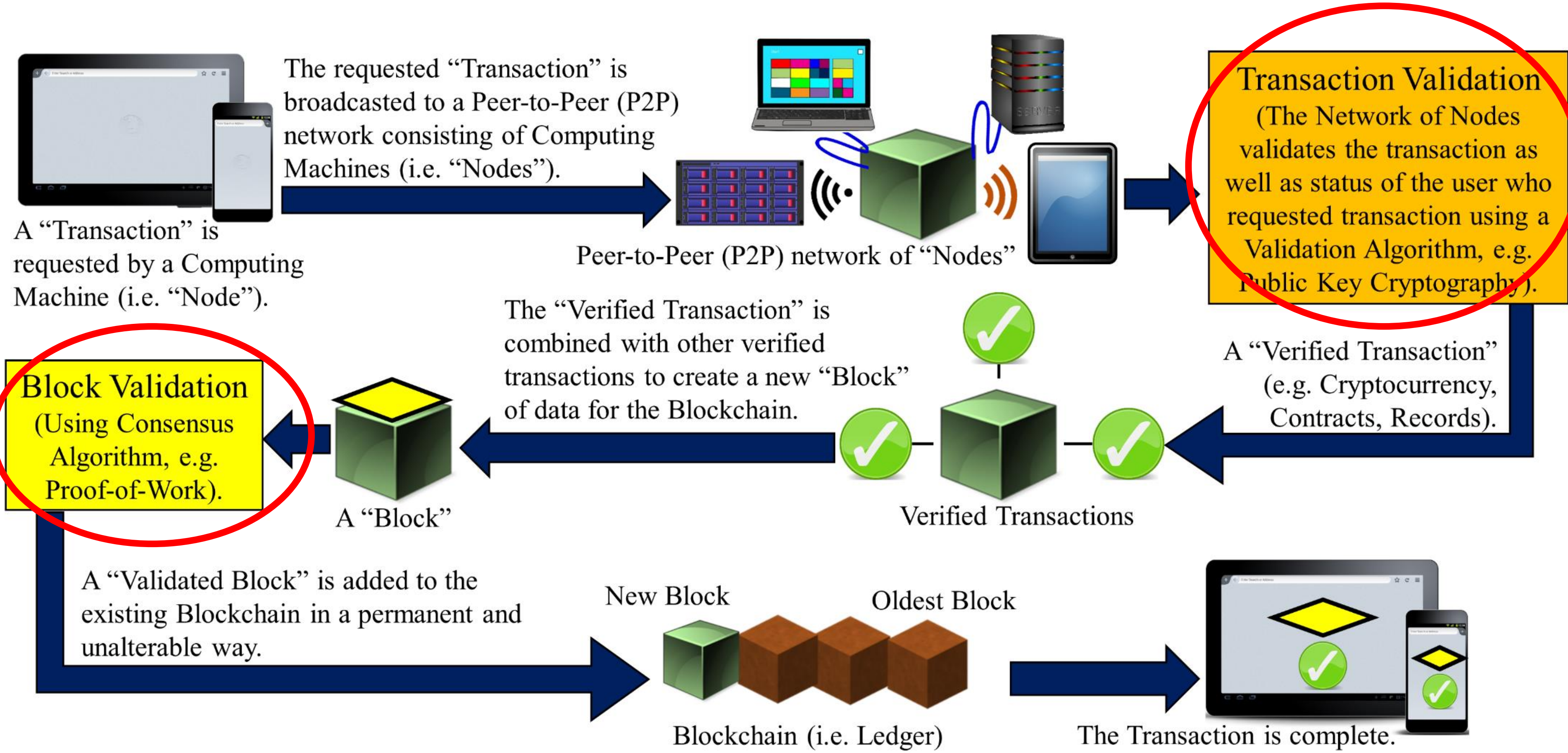
Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Volume 38, Issue 1, January 2019, pp. 26--29.

Blockchain Consensus Types

Blockchain Consensus Algorithm

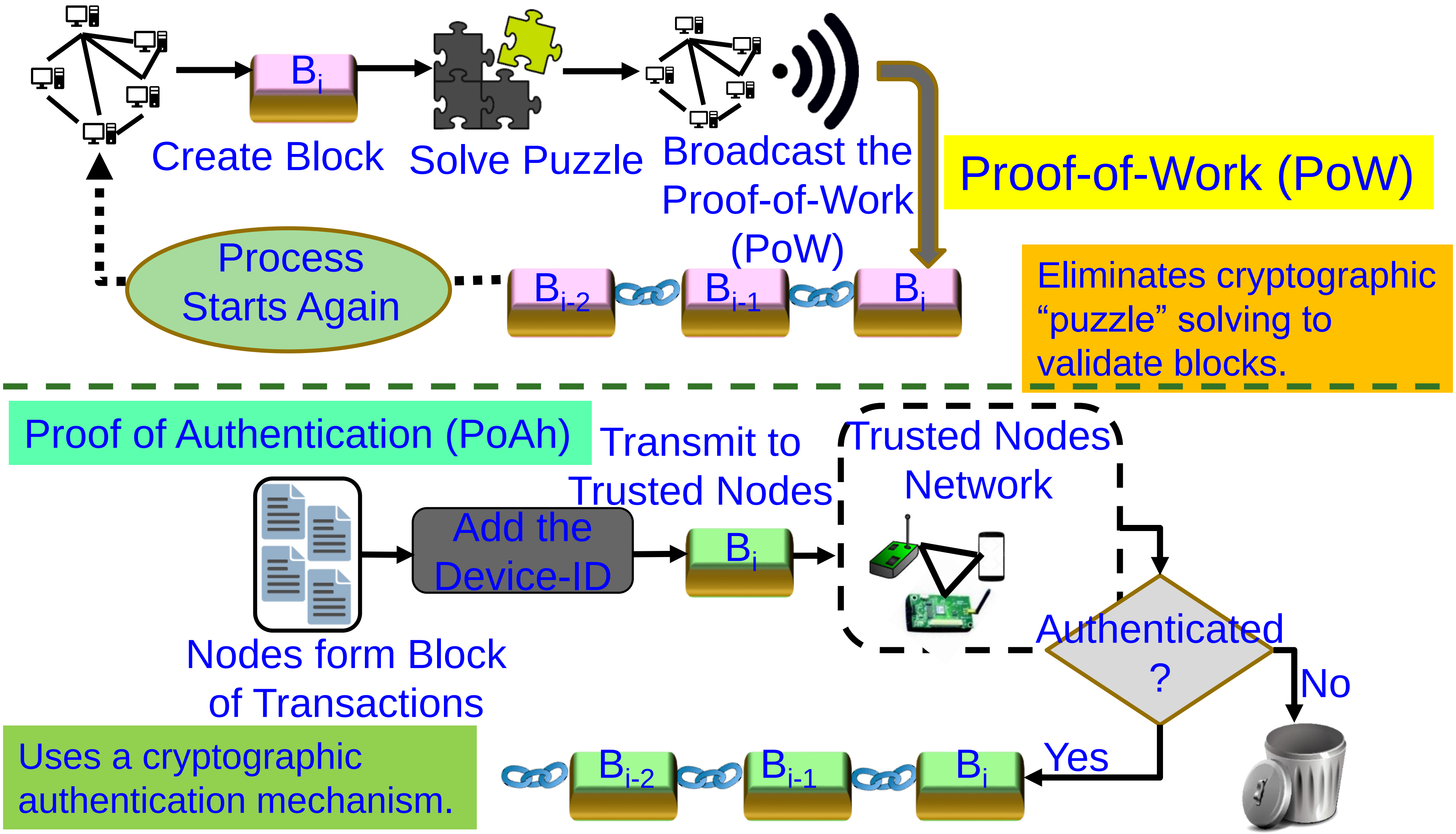
- **Validation Based**
  - Proof of Work (PoW)
  - Proof of Stack (PoS)
  - Proof of Activity (PoA)
  - Proof of Relevance (PoR)
  - Proof of Elapsed Time
- **Voting Based**
  - Ripple
  - Proof of Vote
  - Proof of Trust
- **Authentication Based**
  - Proof of Authentication (PoAh)
  - Proof of PUF-Enabled Authentication (PoP) (**Current Paper**)

Blockchain Challenges - Energy

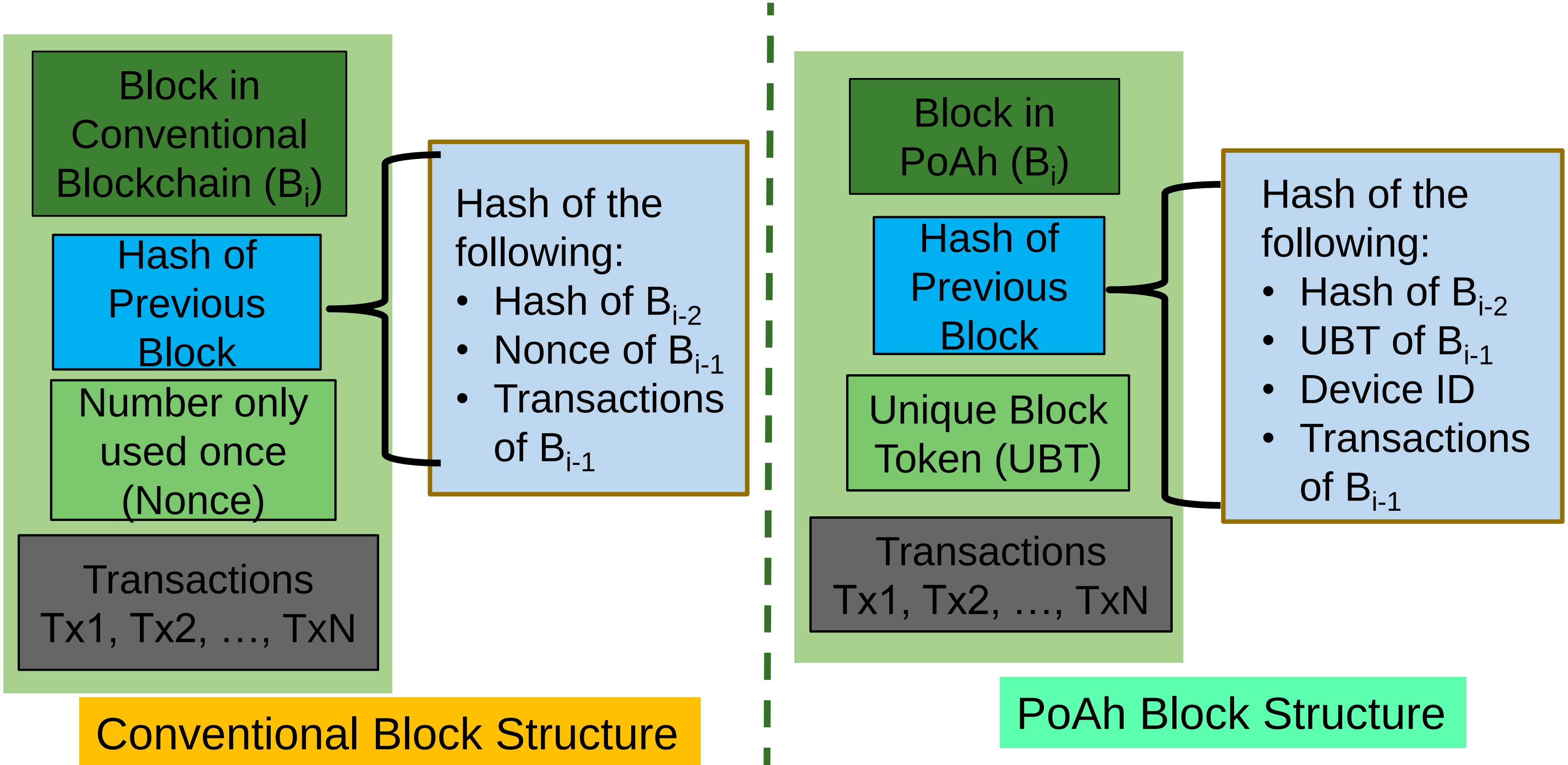


Source: D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 4, July 2018, pp. 06--14.

Our Proof-of-Authentication (PoAh)

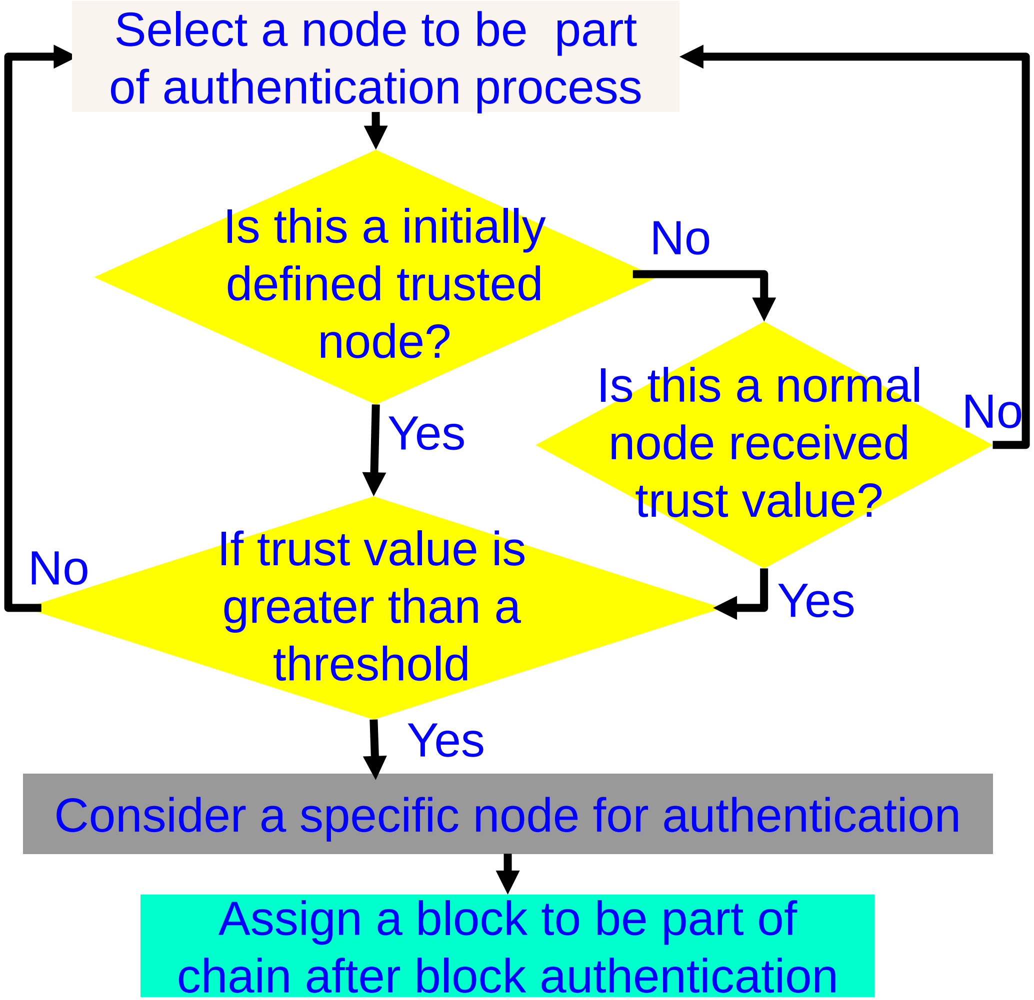


Our PoAh-Chain: Proposed New Block Structure



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) $\rightarrow$ broadcast

(3) Trusted node verifies signature with source public key

V_{PuK}(block) $\rightarrow$ MAC Checking

(4) If (Authenticated)

Block||PoAh(ID) $\rightarrow$ broadcast

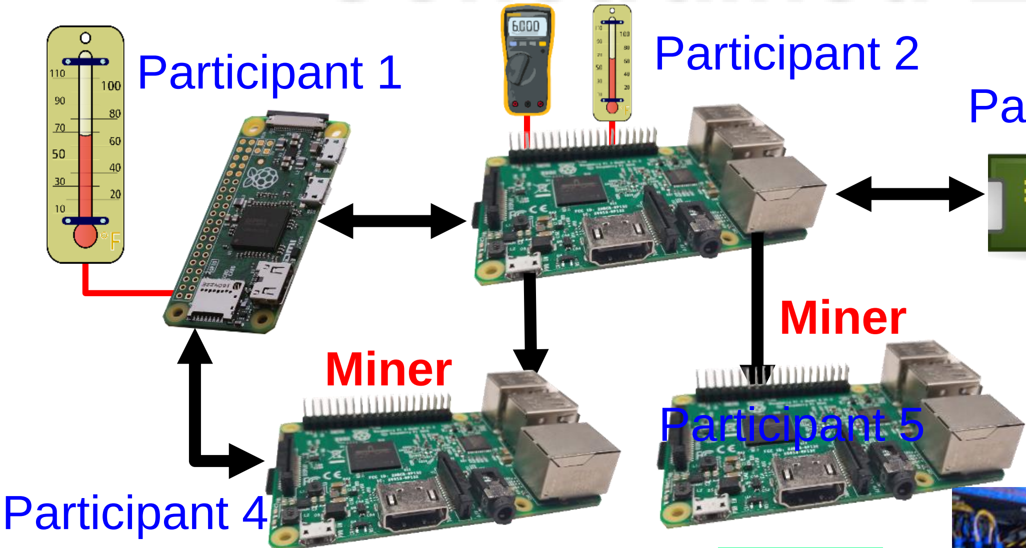
H(block) $\rightarrow$ Add blocks into chain

(5) Else

Drop blocks

(6) GOTO (Step-1) for next block

Our PoAh-Chain Runs in Resource Constrained Environment



Blockchain using PoW Needs Significant Resource

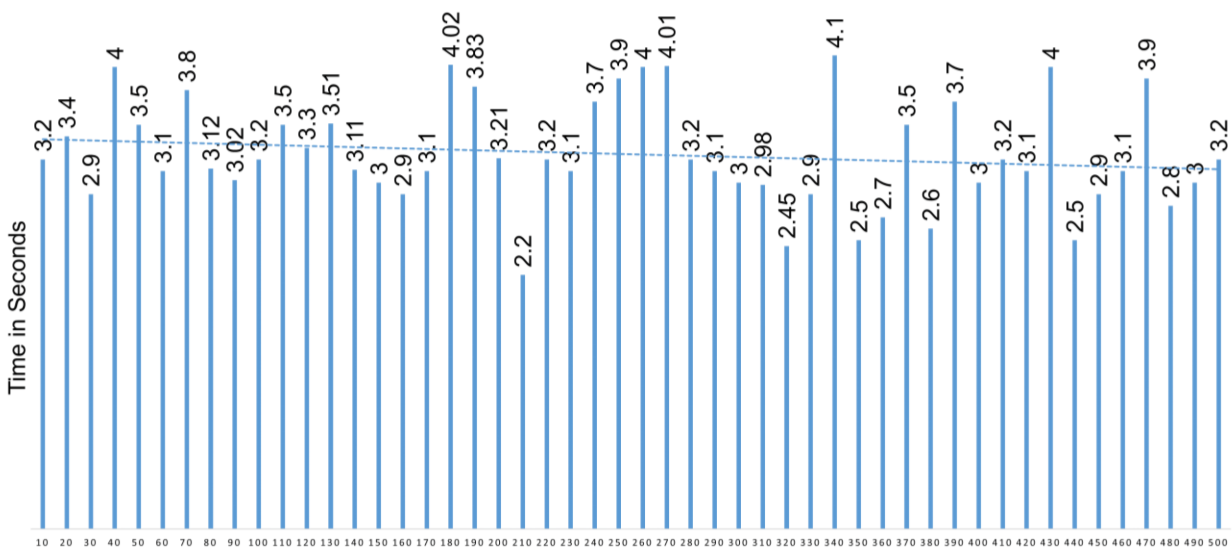
Our PoAh-Chain Runs here

5 W

500,0000 W

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

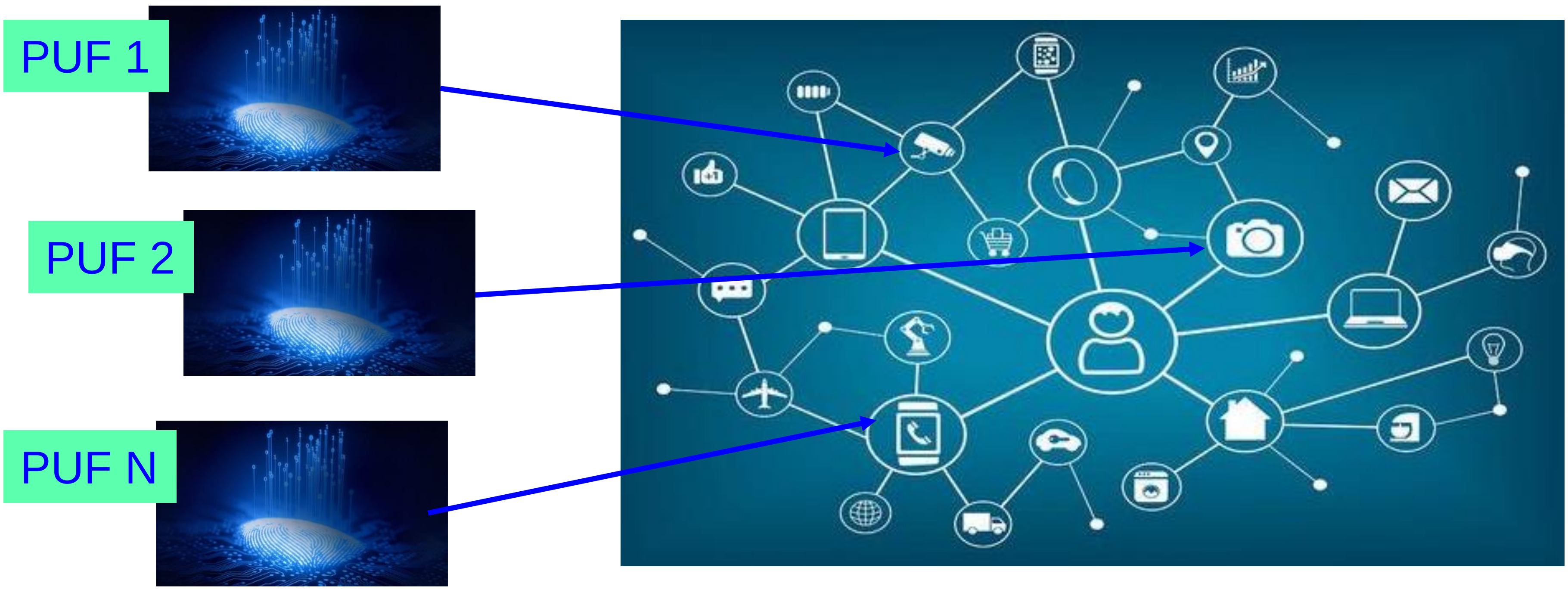
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



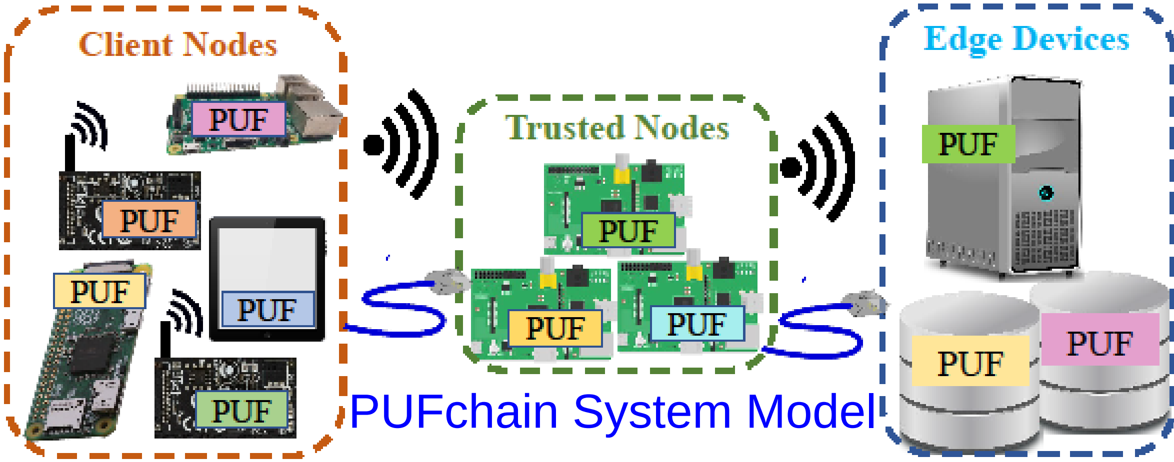
PoAh Execution for 100s of Nodes

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

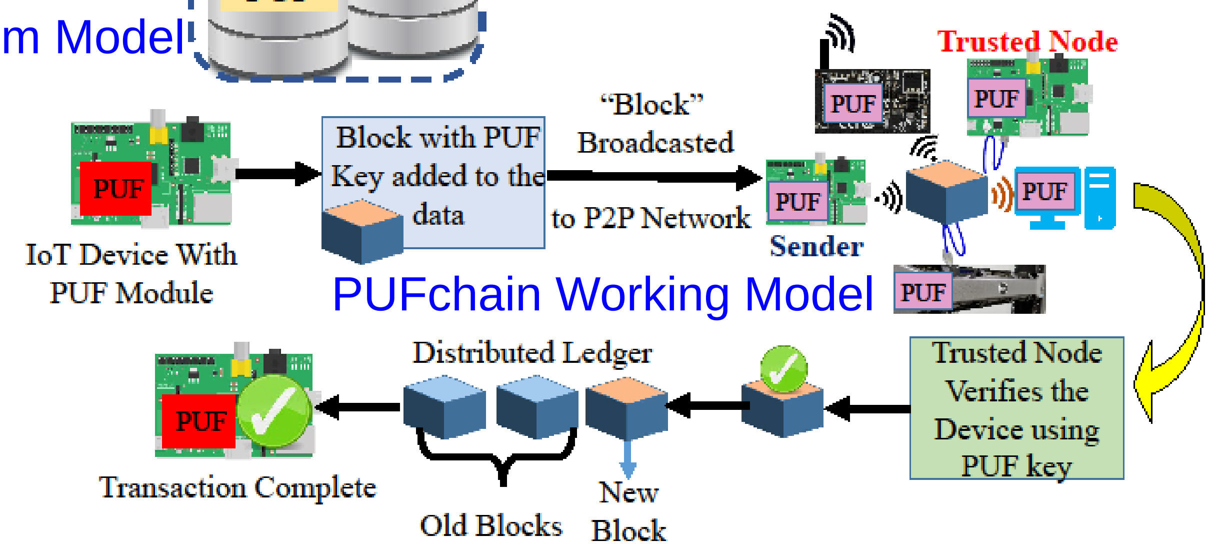


PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

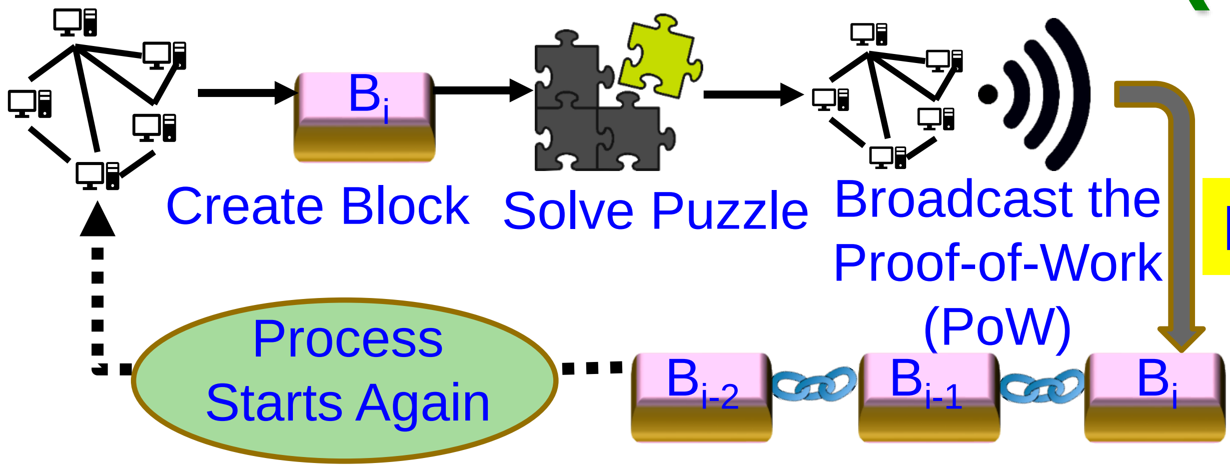


PUFchain Working Model

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

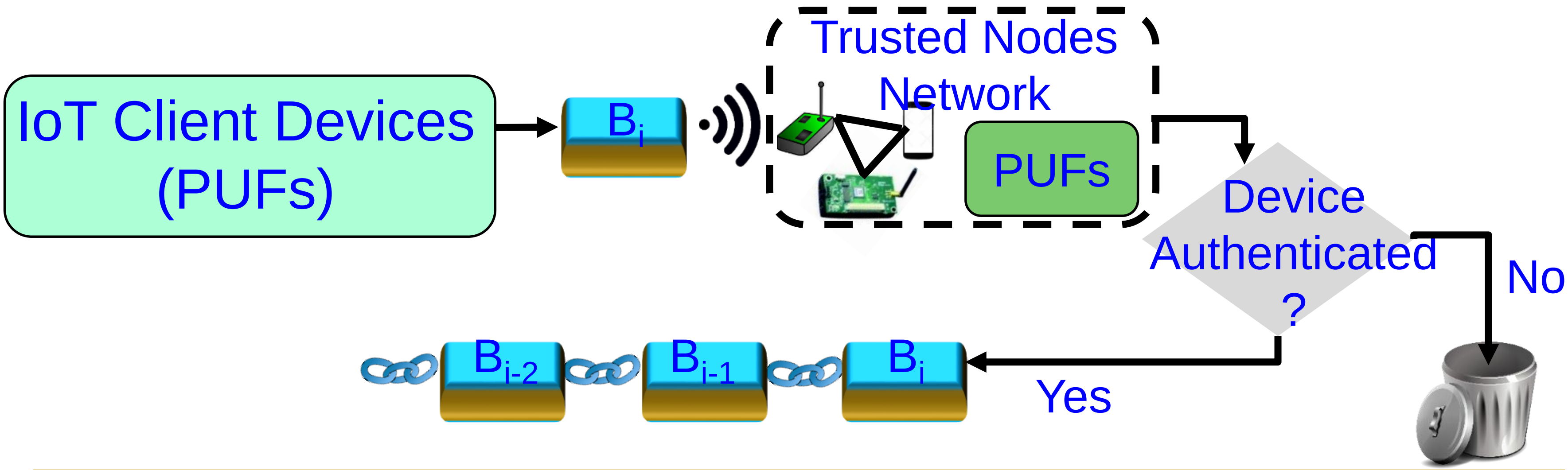
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

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



Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.



PUFchain: Proposed New Block Structure

Block in Conventional Blockchain (B_i)

Hash of Previous Block

Number only used once (Nonce)

Transactions Tx1, Tx2, …, TxN

Hash of the following:
- Hash of B_{i-2}
- Nonce of B_{i-1}
- Transactions of B_{i-1}

Conventional Block Structure

Block in PUFChain(B_i)

Hash of Previous Block

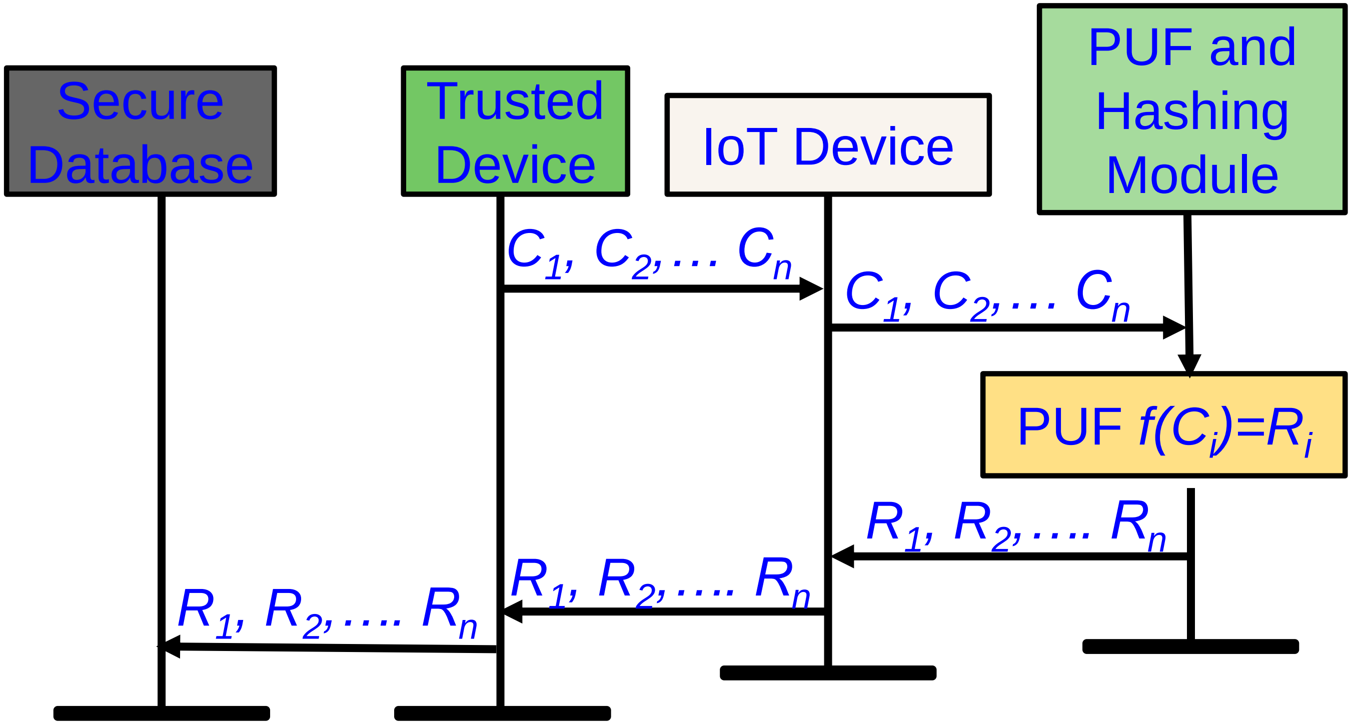
Unique Block Token (UBT)

Transactions Tx1, Tx2, …, TxN

Hash of the following:
- Hash of B_{i-2}
- UBT of B_{i-1}
- Device ID
- PUF Unique Identifier
- Transactions of B_{i-1}

Proposed Block Structure for PUFchain

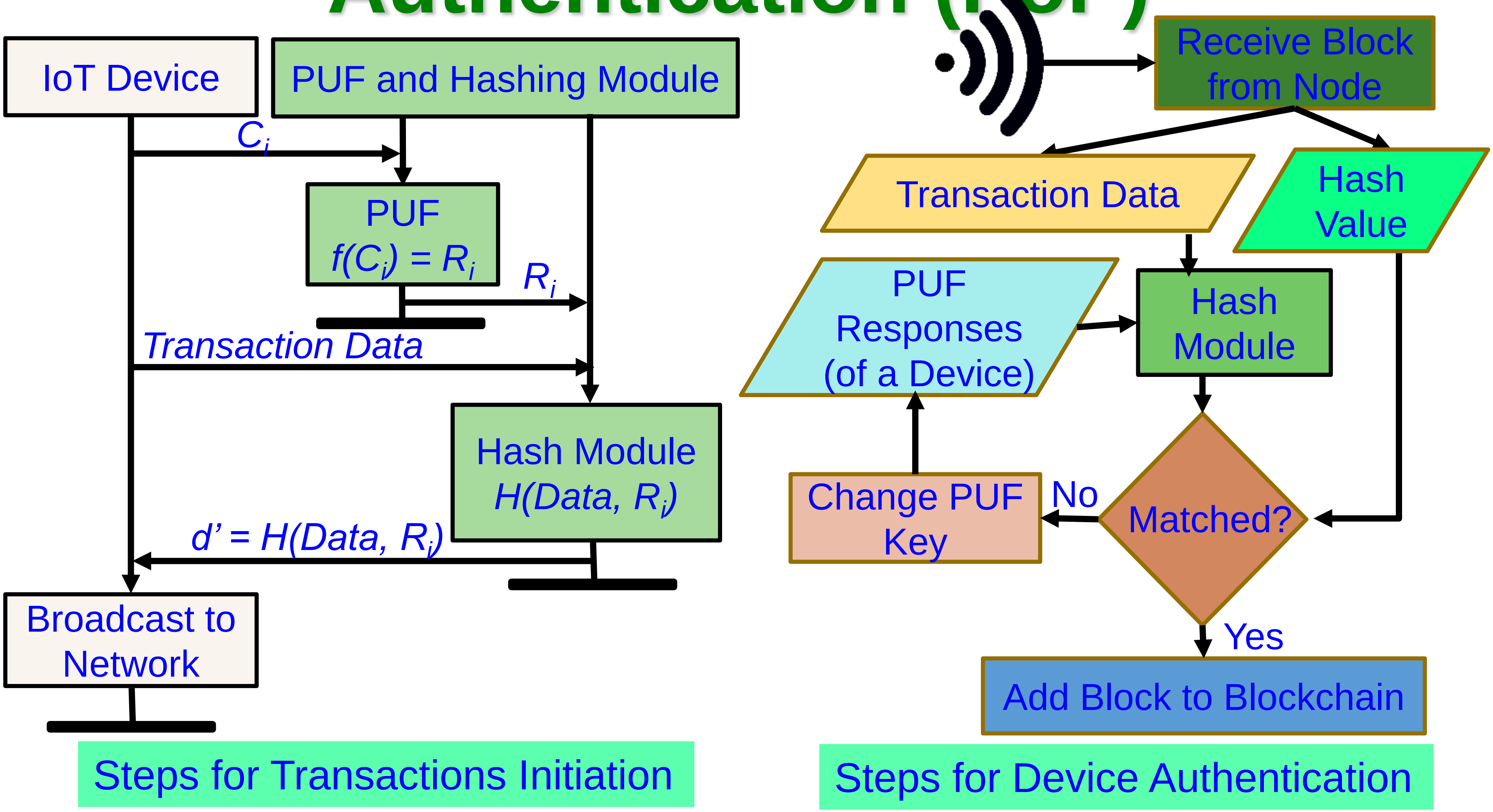
PUFchain: Device Enrollment Steps



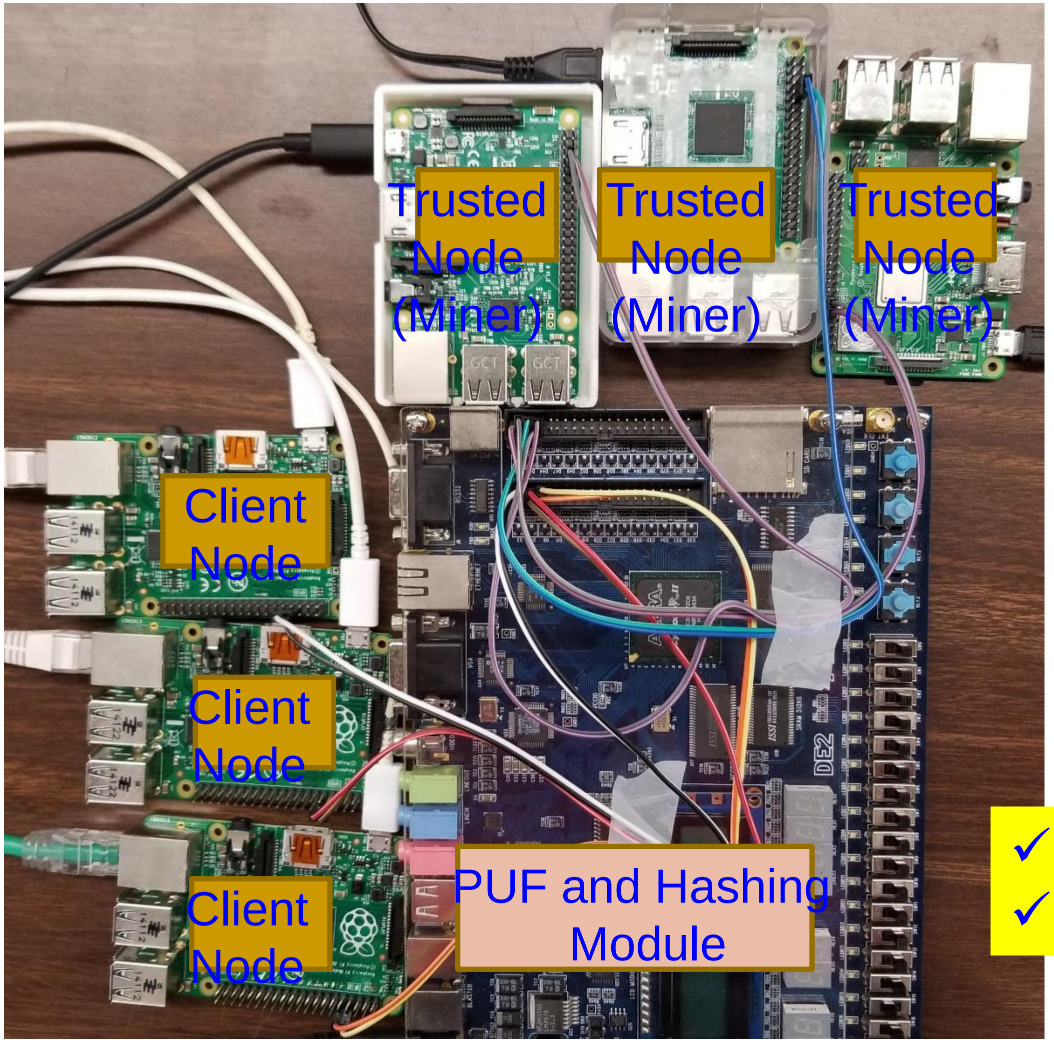
Device Enrollment Steps

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.

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



Our PoP is 1000X Faster than PoW

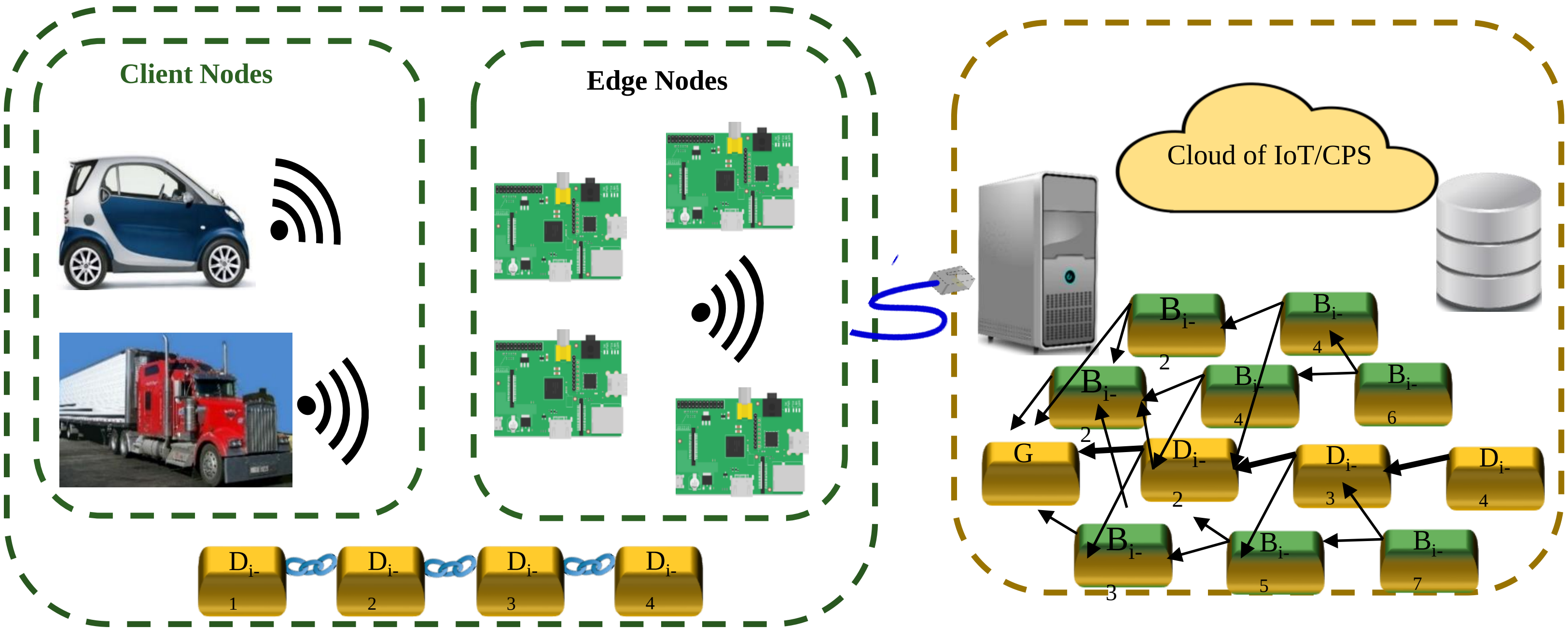


PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

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

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 Multi-Chain Technology to Enhance Scalability



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

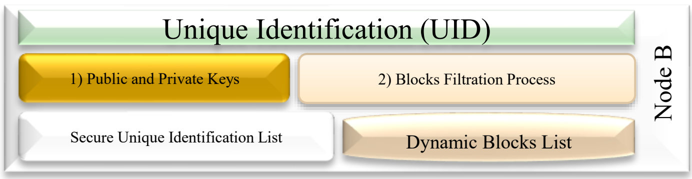
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020

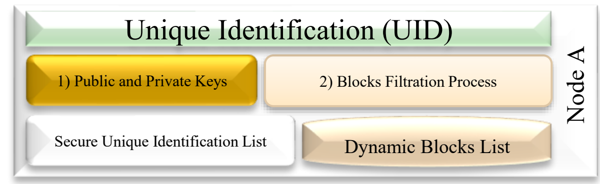
A Perspective of BC, Tangle Vs Our Multichain

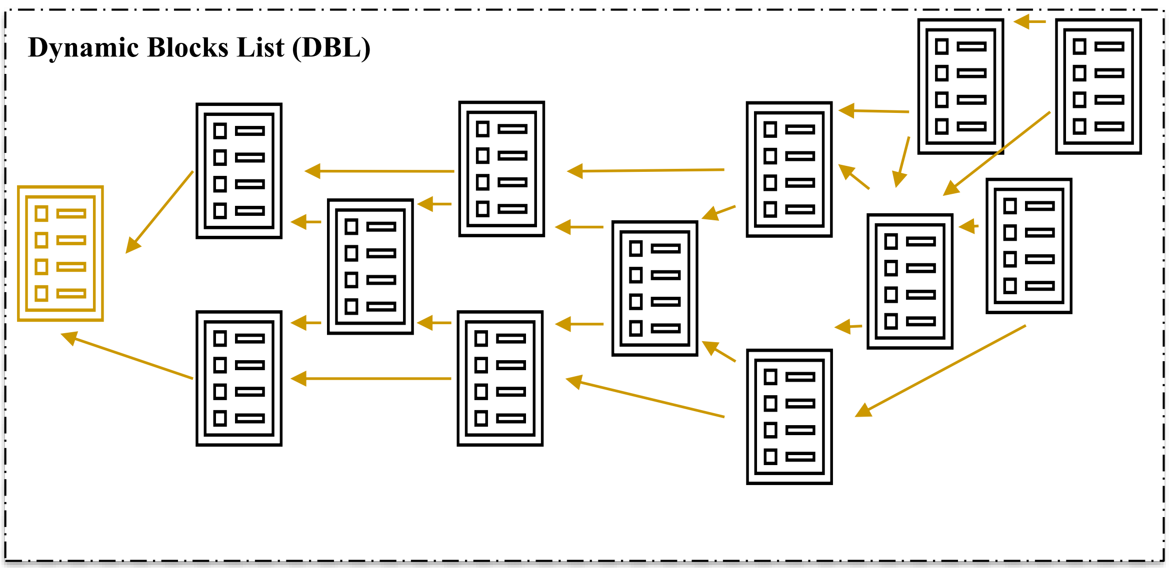
Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRA (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions 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 Components







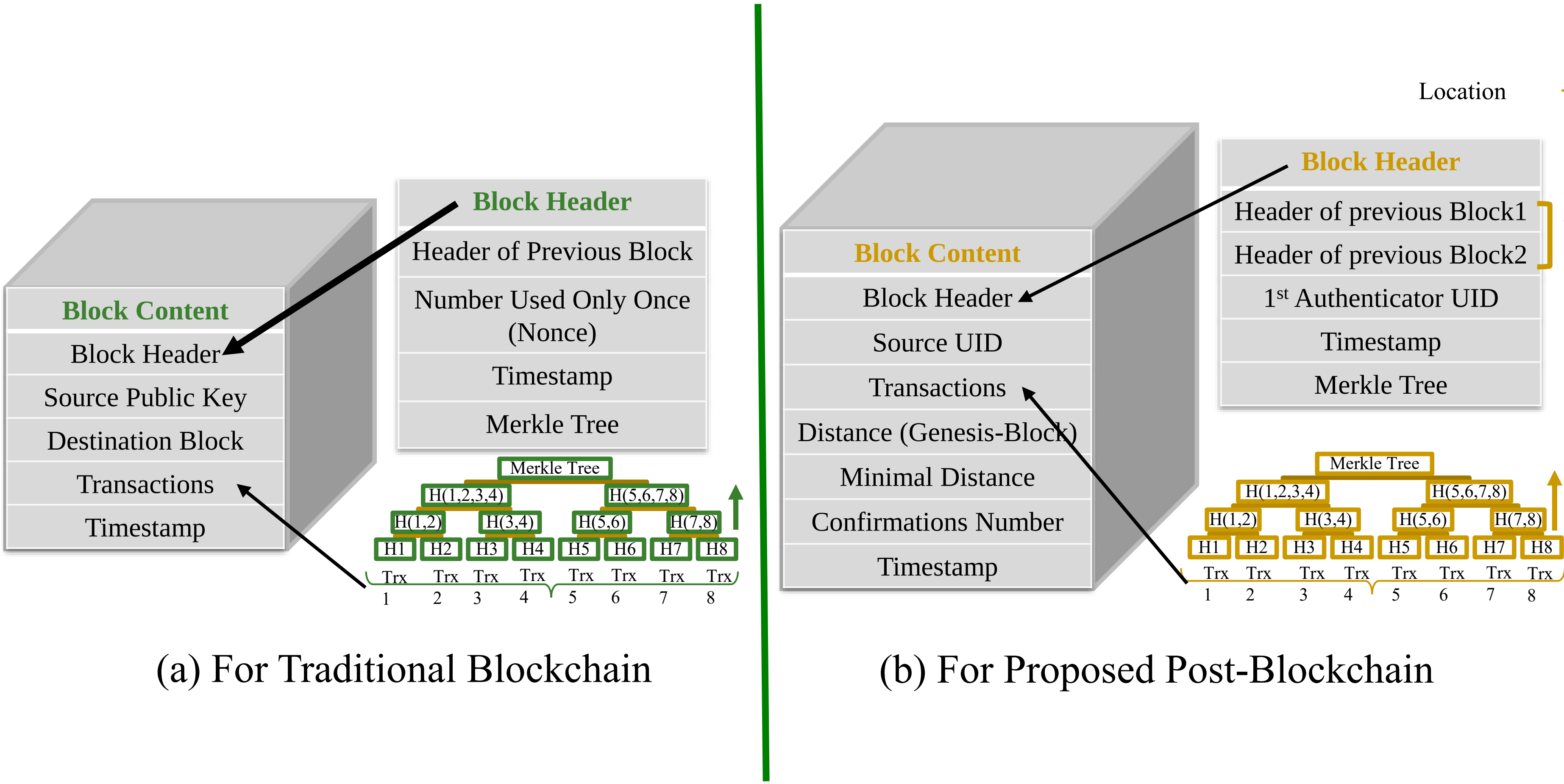
Secure Unique Identification List (SUIL)

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)

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

Block Structure in McPoRA



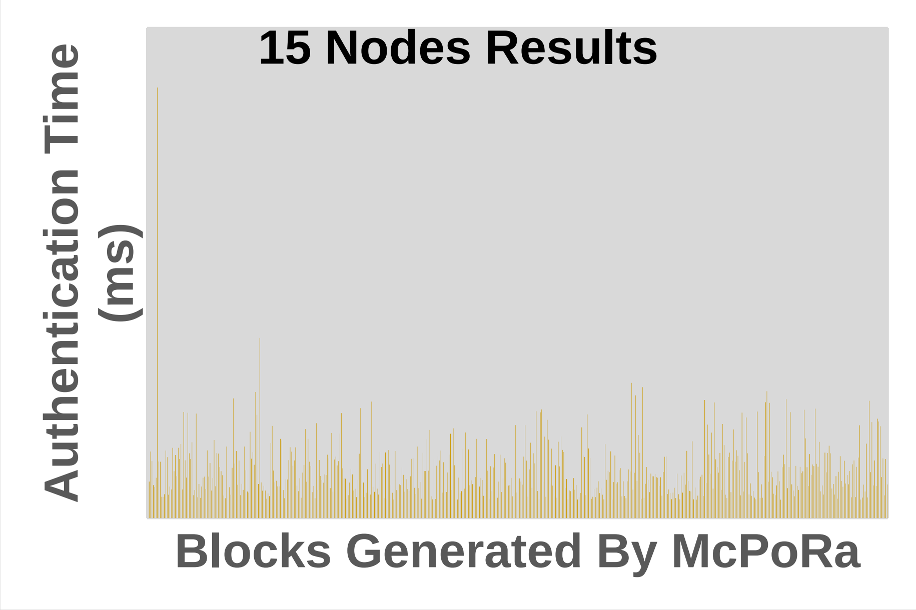
(a) For Traditional Blockchain

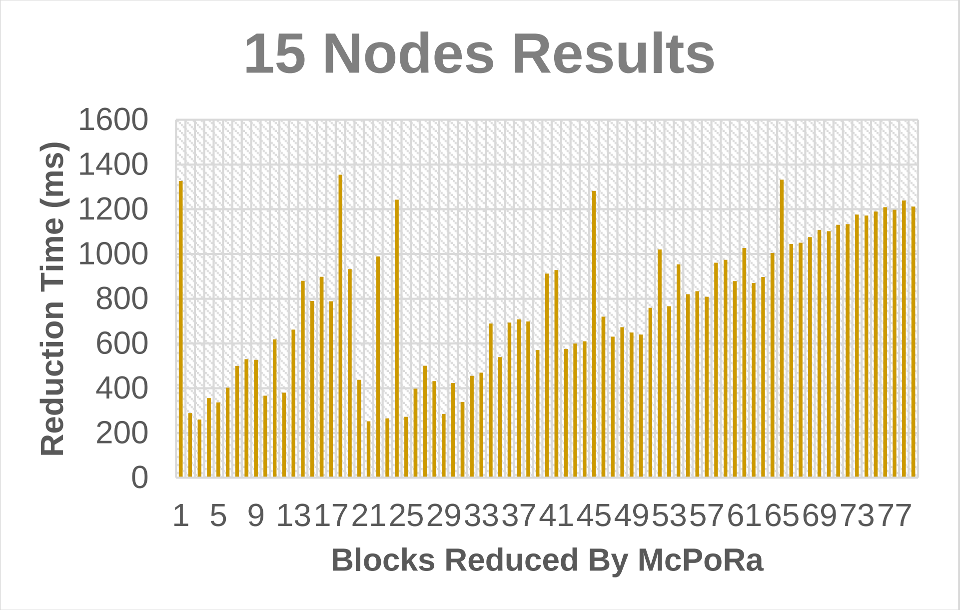
(b) For Proposed Post-Blockchain

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 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

Smart Grid Security - Solutions

Smart Grid – Security Solutions

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

Smart Meter

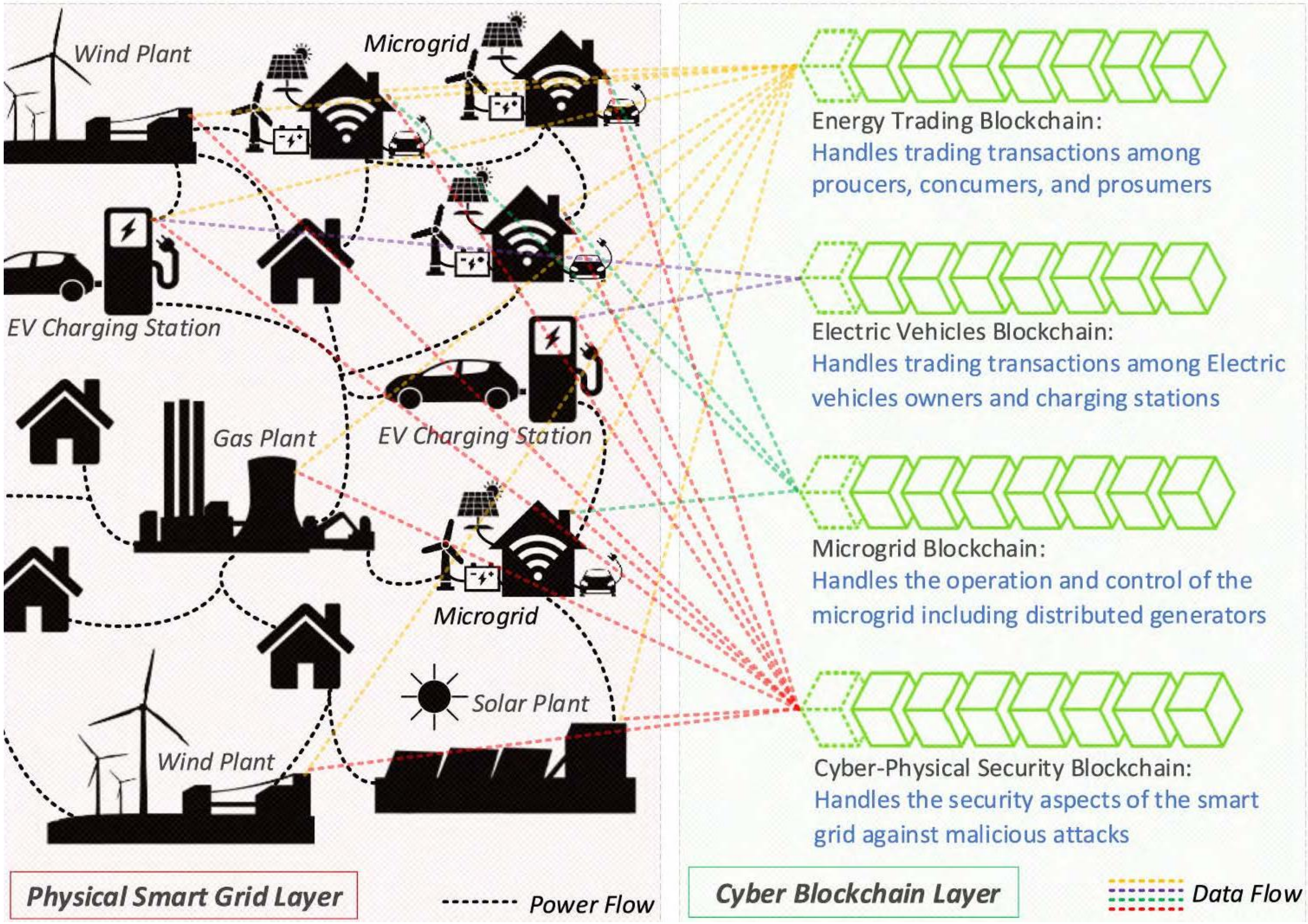

Phasor Measurement Unit (PMU)

Smart Grid Cybersecurity - Strategies

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

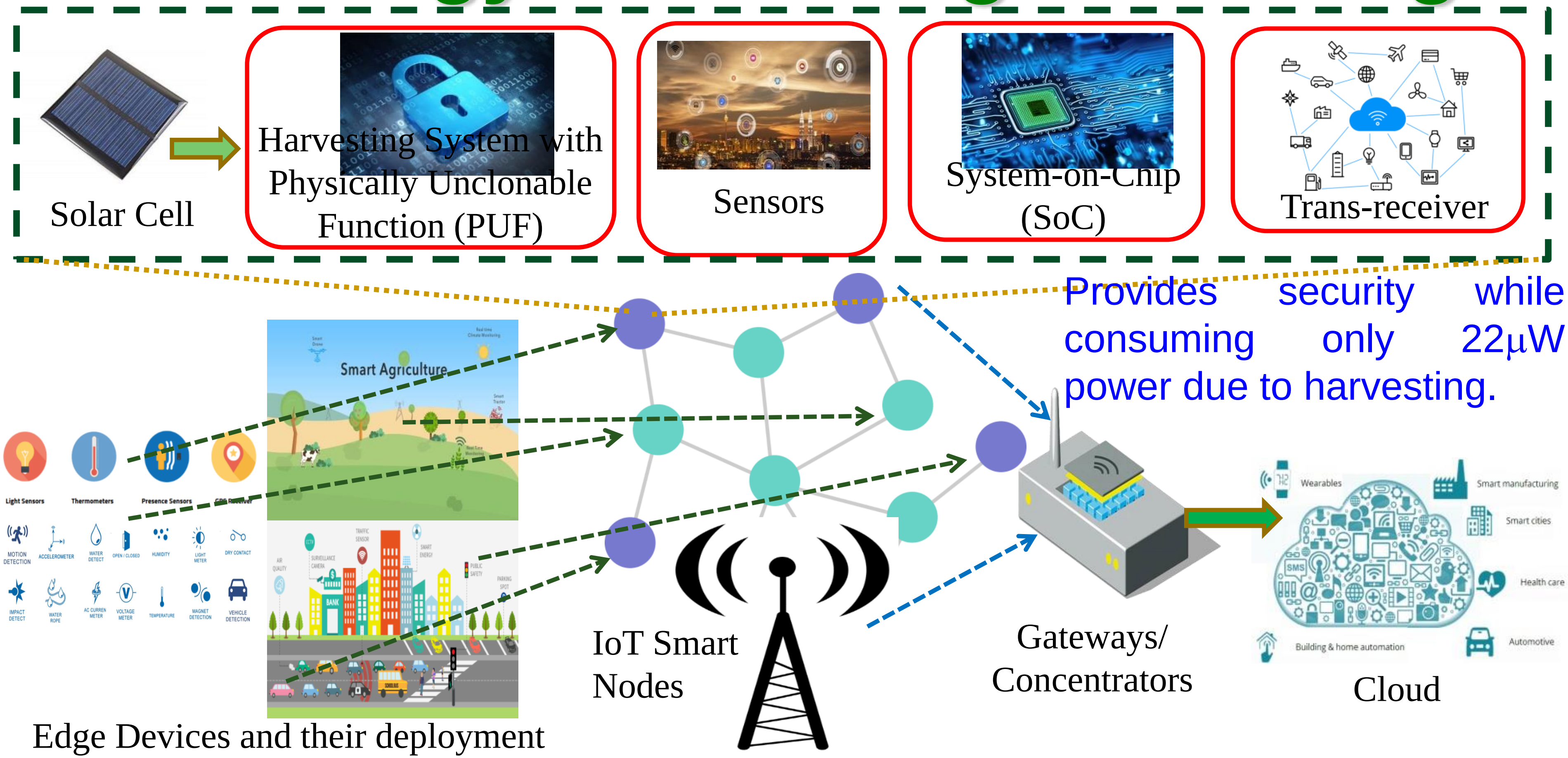
Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids“, *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

Smart Grid Security - Solutions



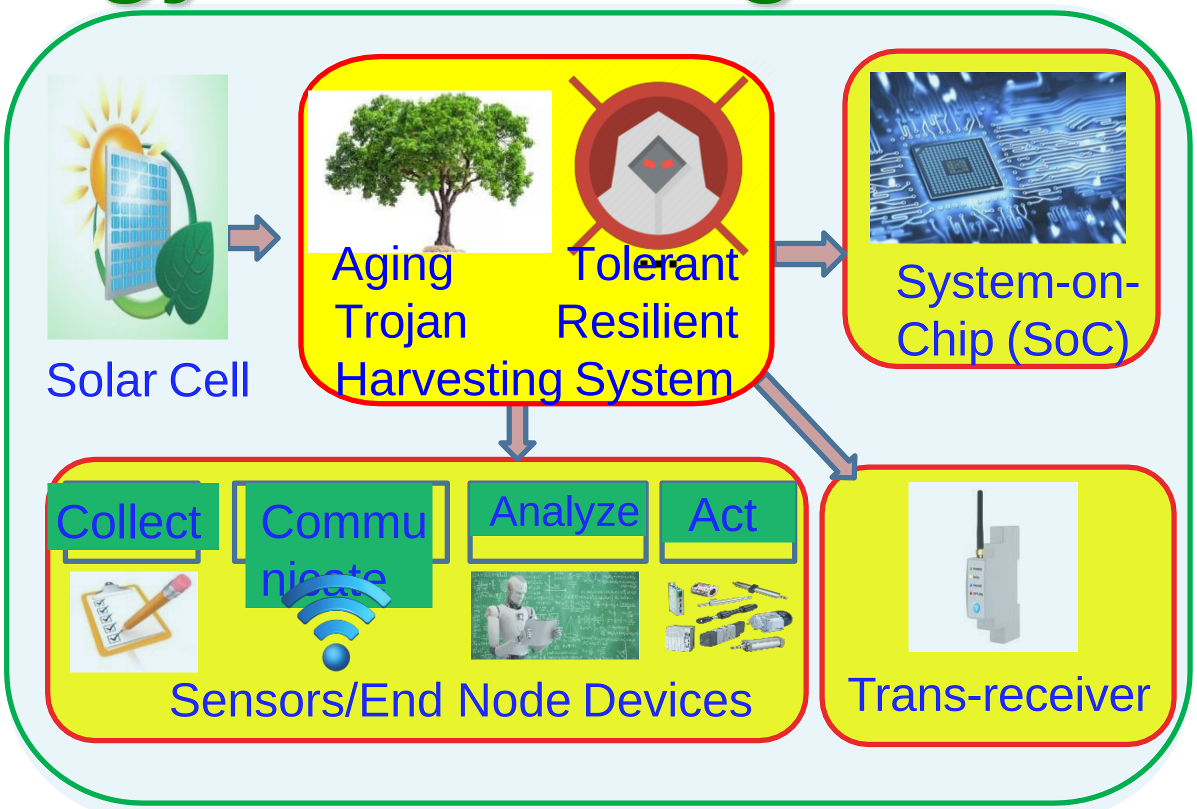
Source: A. S. Musleh, G. Yao and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," IEEE Access, vol. 7, pp. 86746-86757, 2019.

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



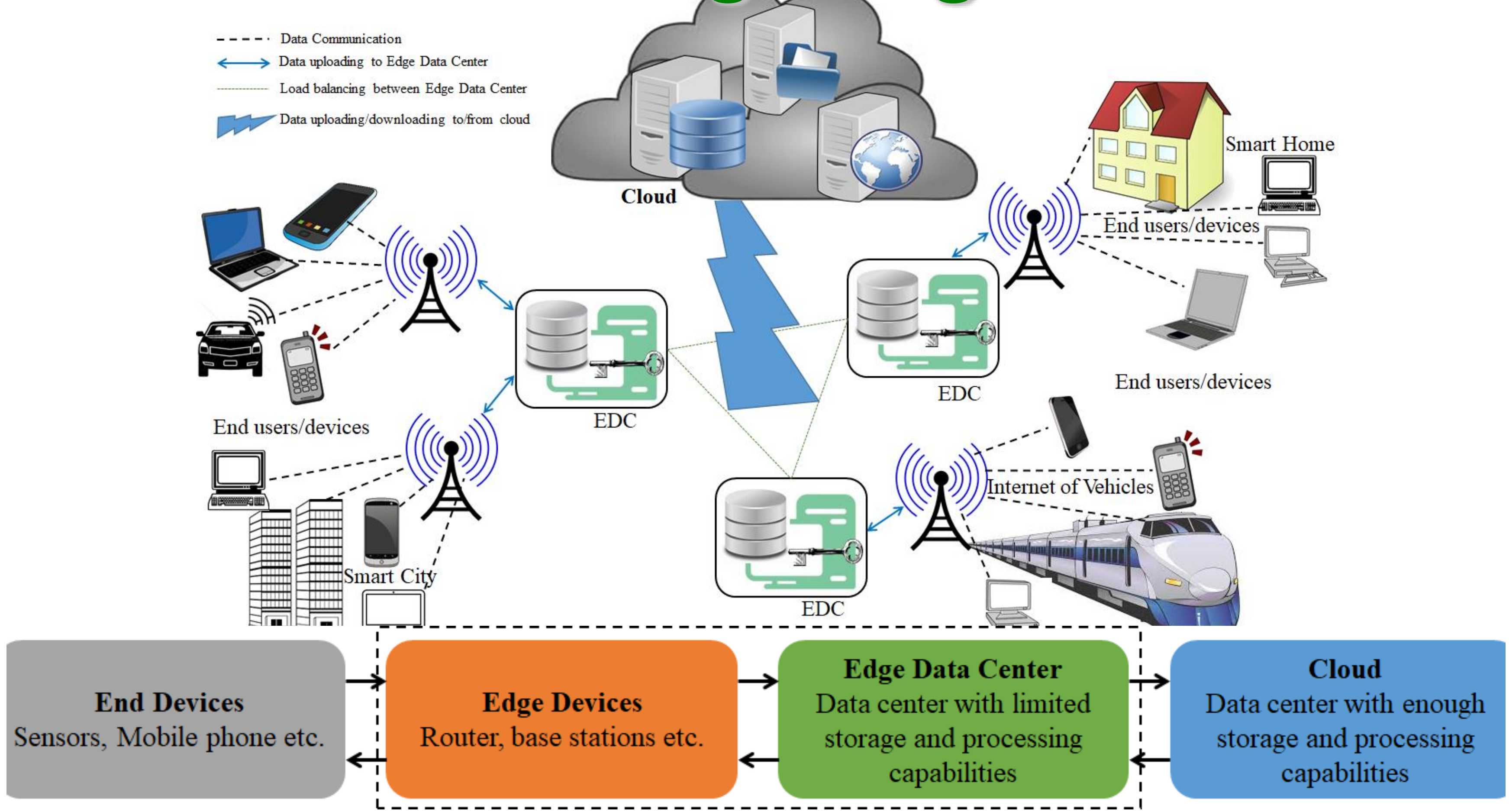
Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, “Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT”, *IEEE Transactions on Sustainable Computing*, Vol. XX, No. YY, ZZ 2019, pp. Under Review.

Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the Edge



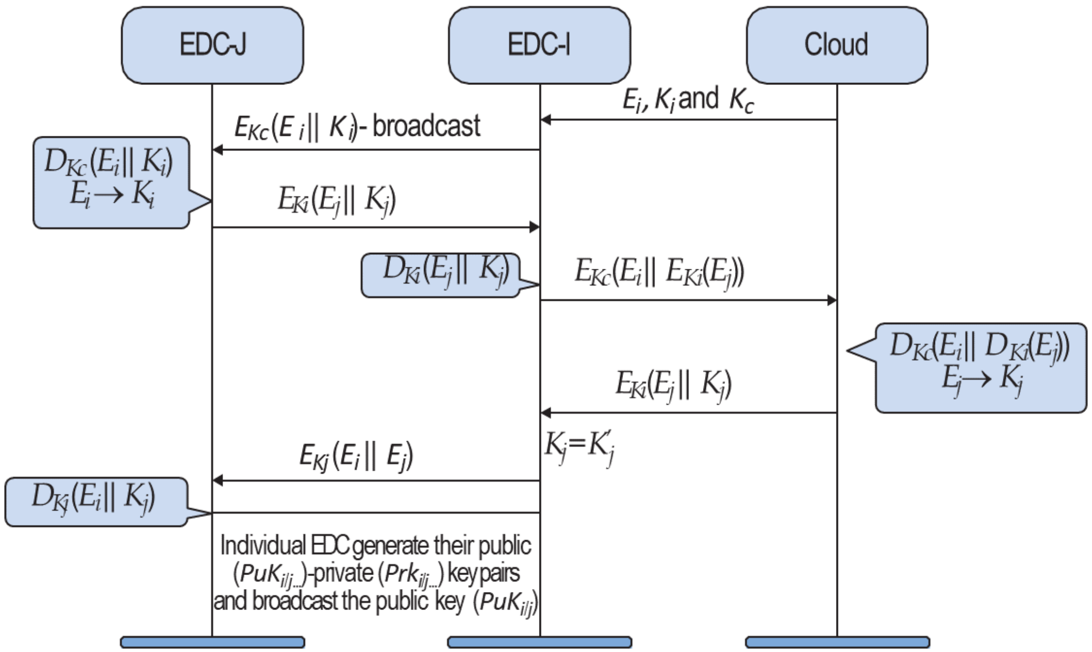
Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, "Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT", *ACM Journal on Emerging Technology in Computing*, Vol. XX, No. YY, ZZ 2019, pp. Under Review.

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.

Our Proposed Secure Edge Datacenter



Algorithm 1: Load Balancing Technique

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

Secure edge datacenter –
- Balances load among the EDCs
- Authenticates EDCs

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

Source: 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.

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

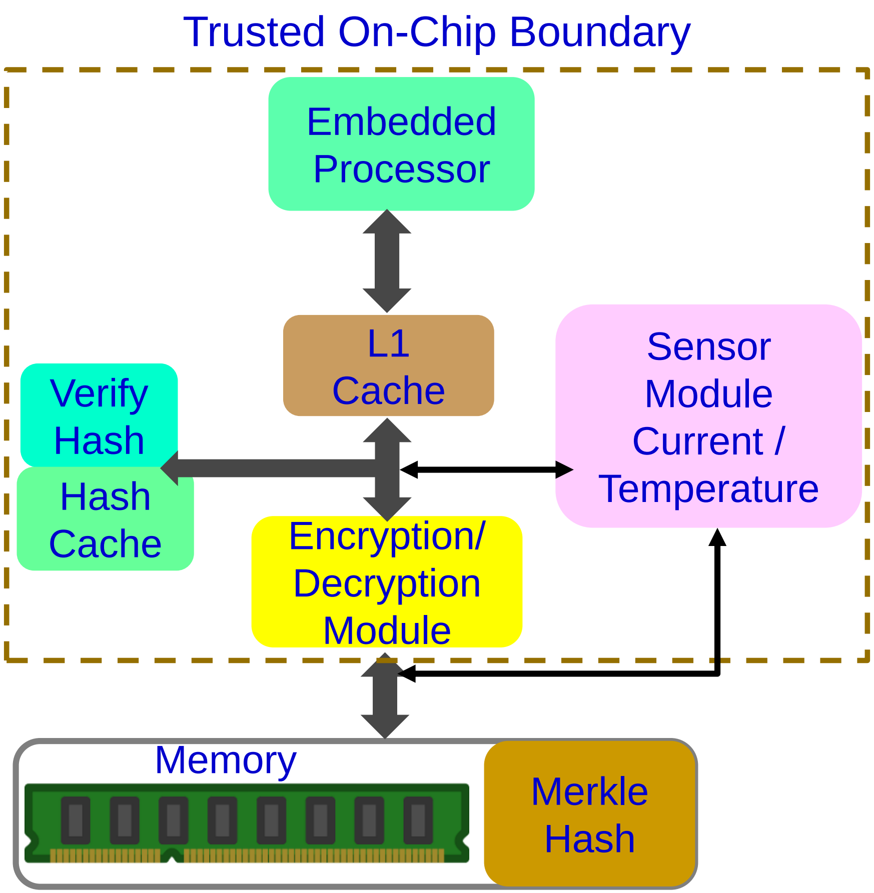
Nonvolatile / Harddrive Storage

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

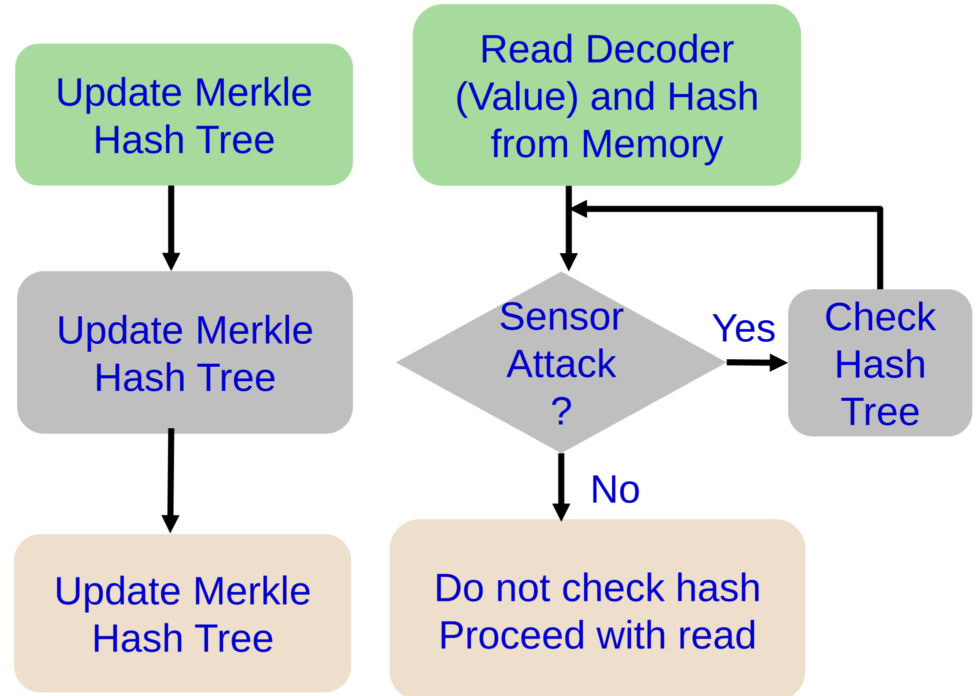
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

Embedded Memory Security



On-Chip/On-Board Memory Protection

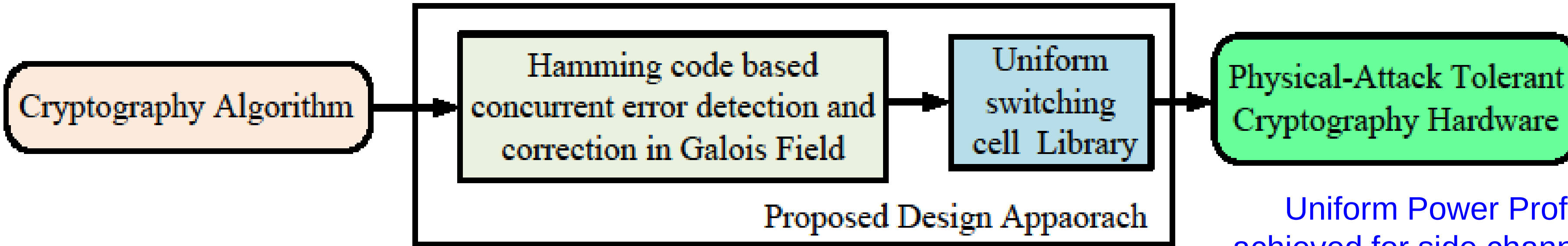


Write Operation   Read Operation

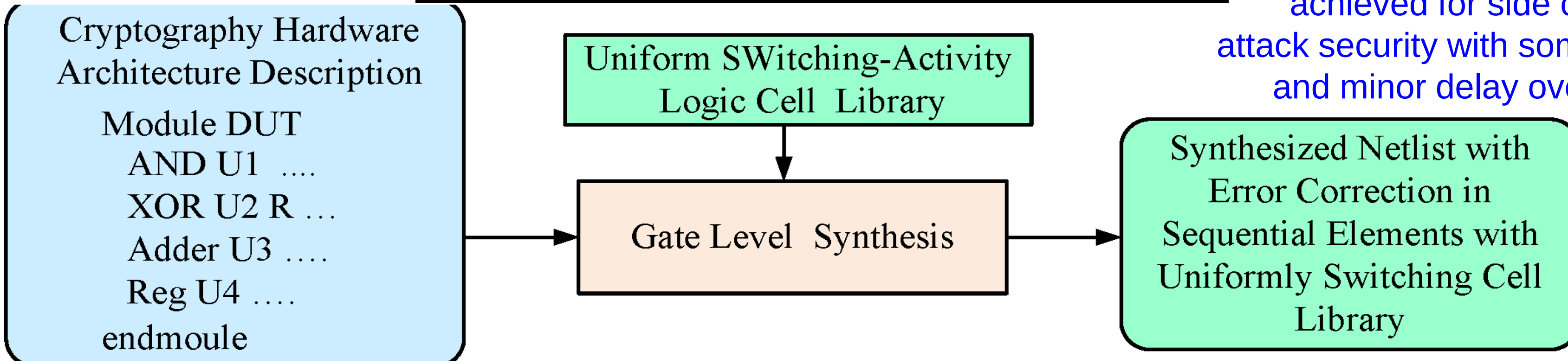
Memory integrity verification with 85% energy savings with minimal performance overhead.

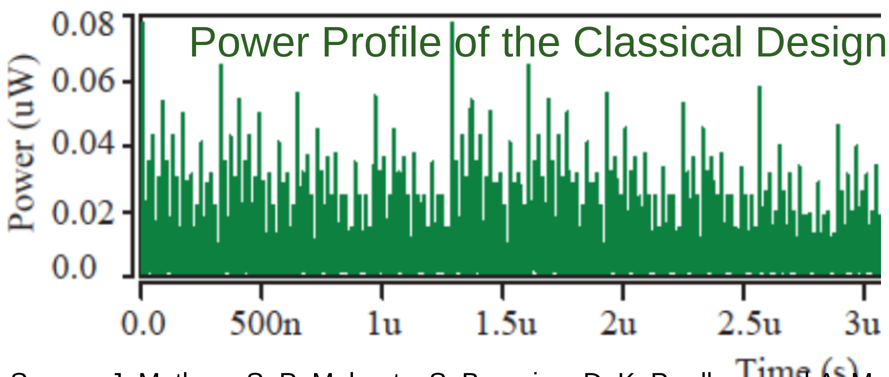
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", Springer Circuits, Systems, and Signal Processing Journal (CSSP), Volume 32, Issue 6, December 2013, pp. 2581--2604.

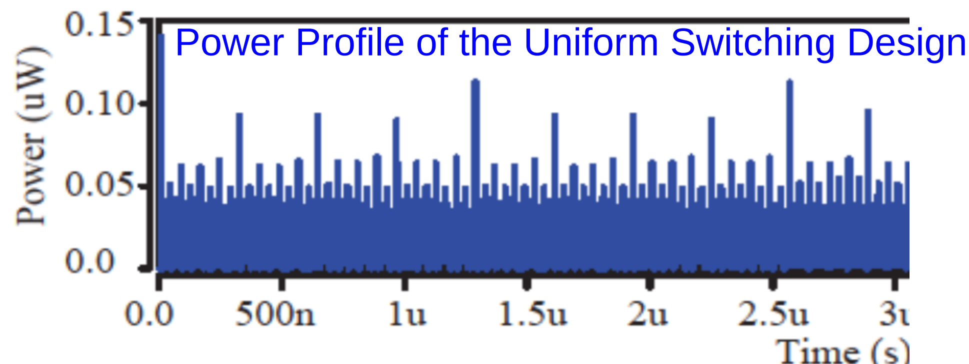
DPA Resilience Hardware Design



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

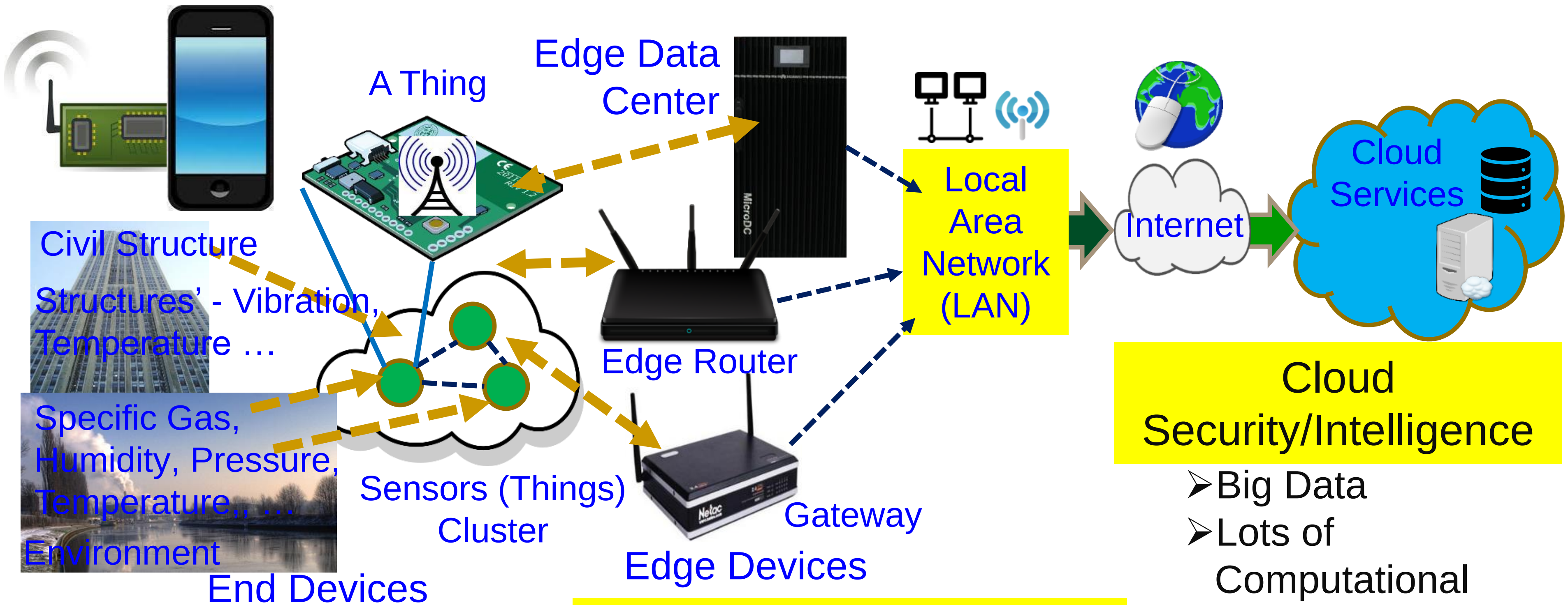






Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", *Elsevier Computers and Electrical Engineering*, Vol. 39, No. 4, May 2013, pp. 1077--1087.

End, Edge Vs Cloud - Security, Intelligence



End Security/Intelligence

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

Edge Security/Intelligence

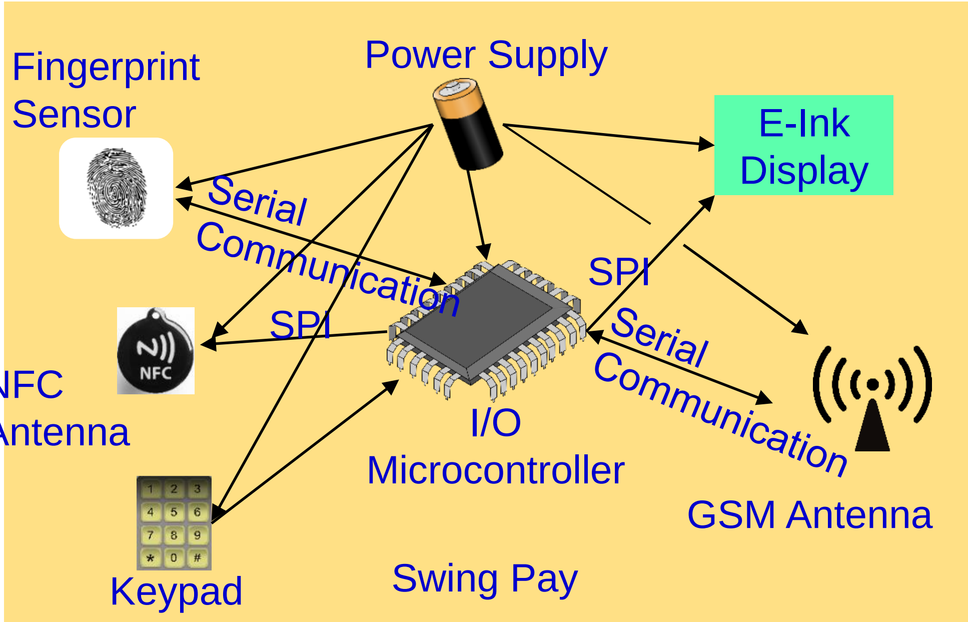
- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

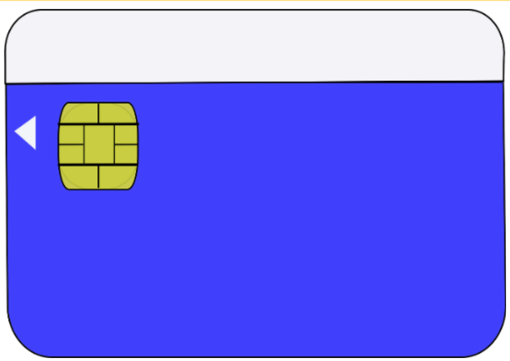
Cloud Security/Intelligence

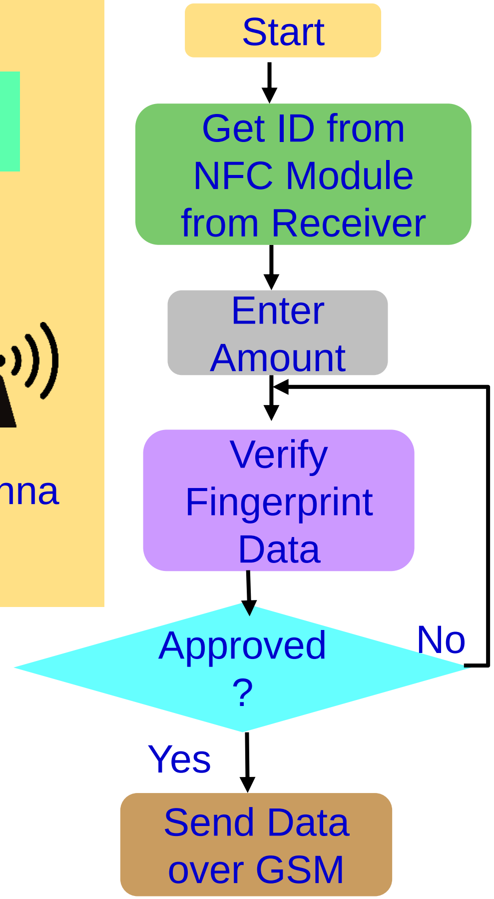
- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy overhead in Communications

Source: Mohanty iSES Keynote 2018 and ICCE 2019 Panel

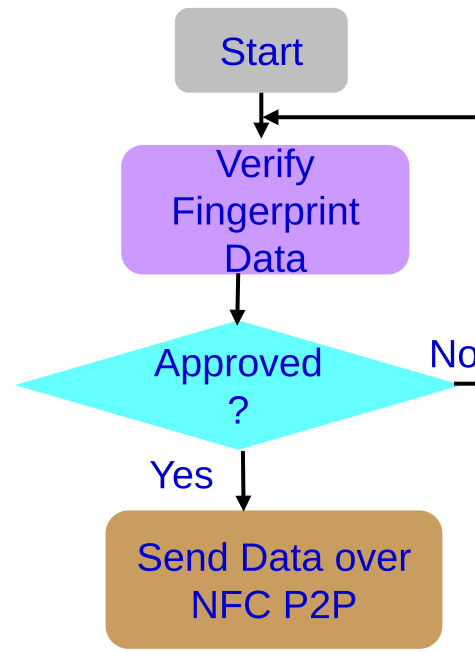
NFC Security - Solution







Payer Module



Payee Module

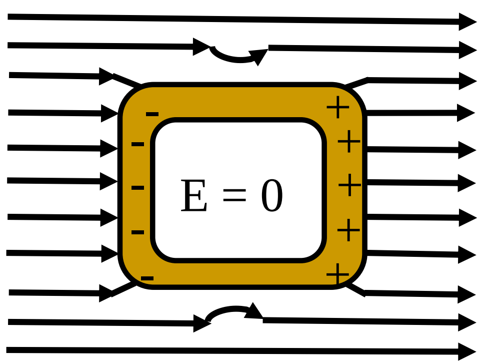
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", IEEE Consumer Electronics Magazine (CEM), Volume 6, Issue 1, January 2017, pp. 82--93.

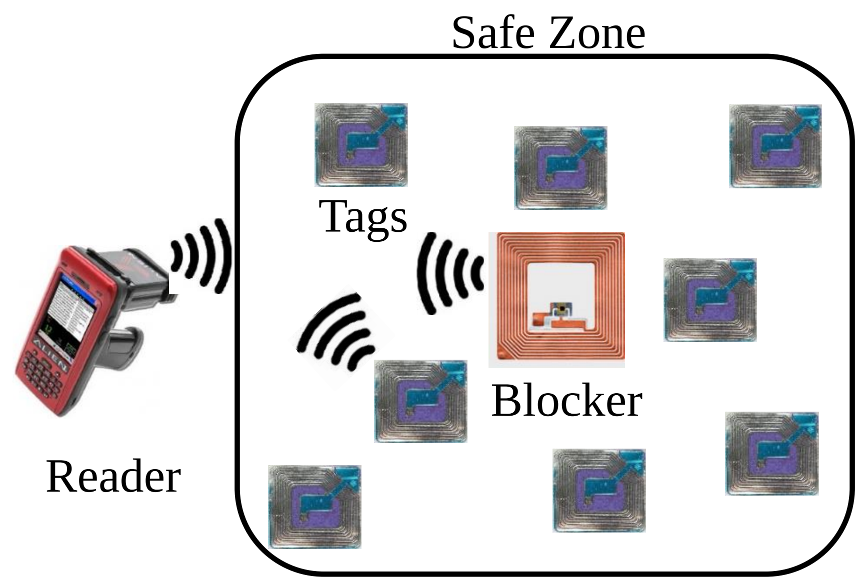
RFID Security - Solutions

Selected RFID Security Methods

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

Faraday Cage





Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

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)

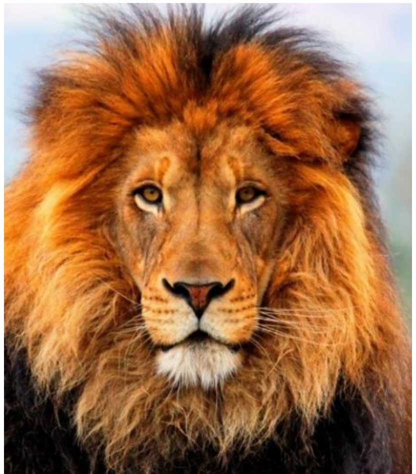
Machine Learning Engine

Data

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

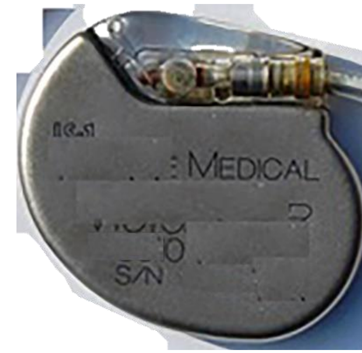
Source: Hongxu Yin, Ayten Ozge Akmandor, Arsalan Mosenia and Niraj K. Jha (2018), "Smart Healthcare", *Foundations and Trends® in Electronic Design Automation*, Vol. 12: No. 4, pp 401-466. http://dx.doi.org/10.1561/1000000054

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



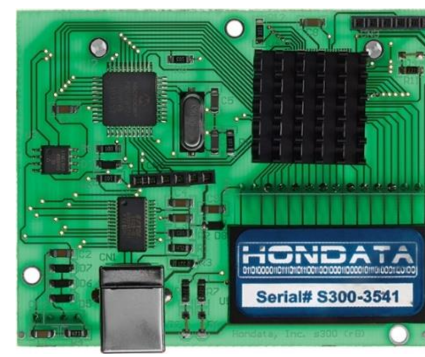
AI can be fooled by fake data

AI can create fake data (Deepfake)



Authentic Fake

An implantable medical device

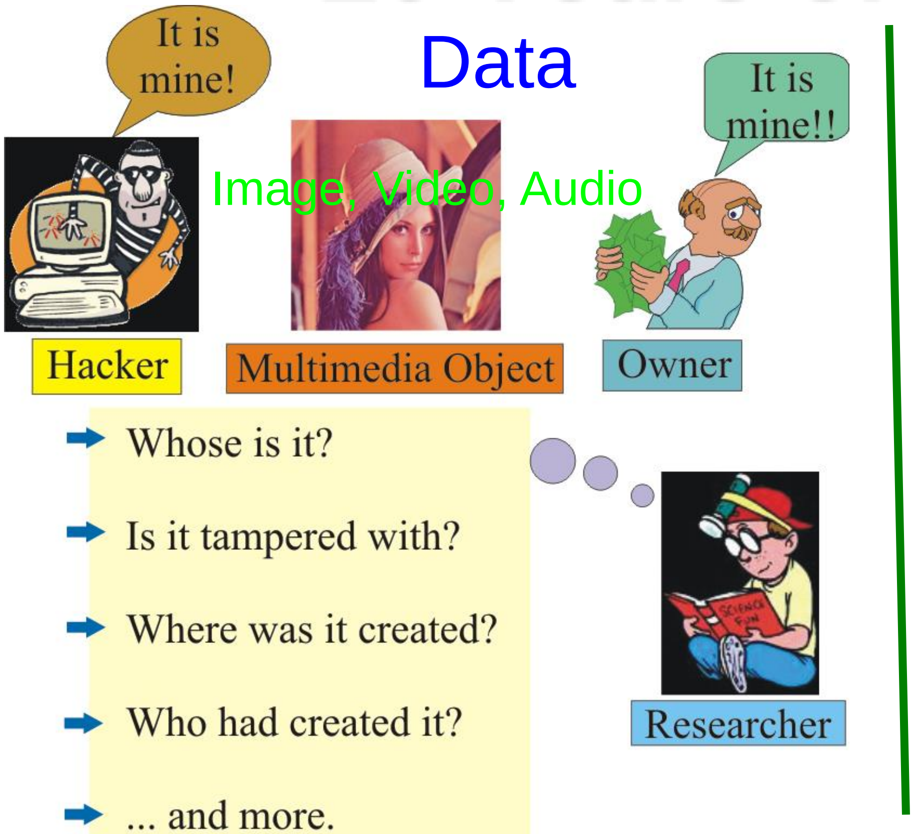


Authentic Fake

A plug-in for car-engine computers

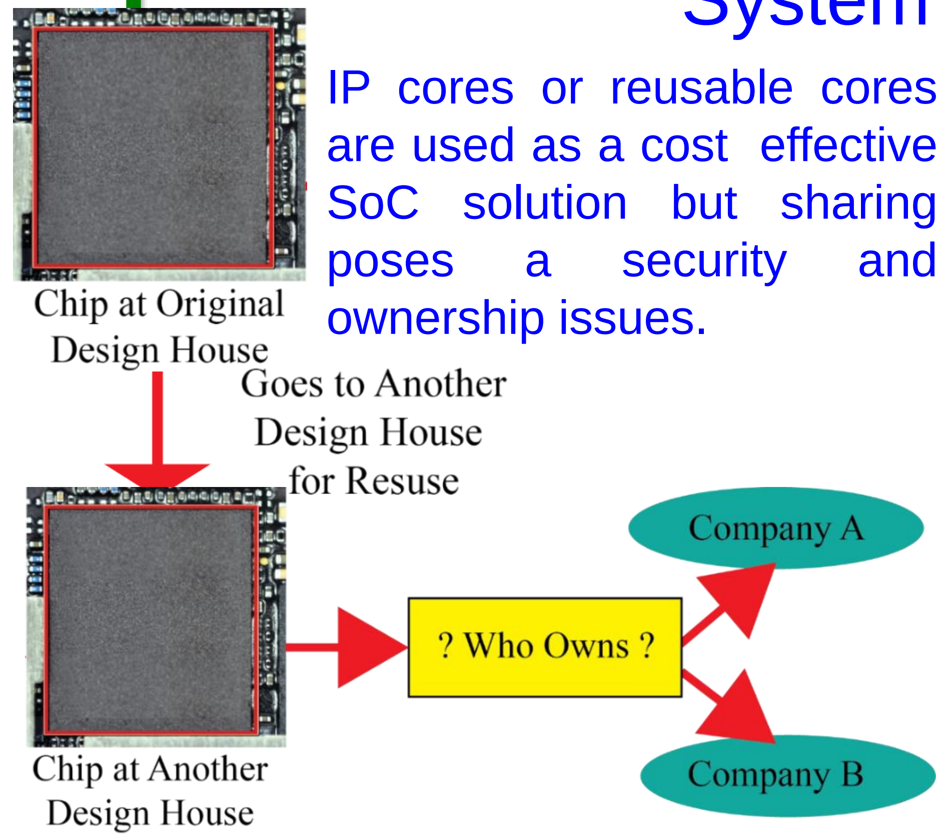
Data and System Authentication and Ownership Protection – My 20 Years of Experiences

Data



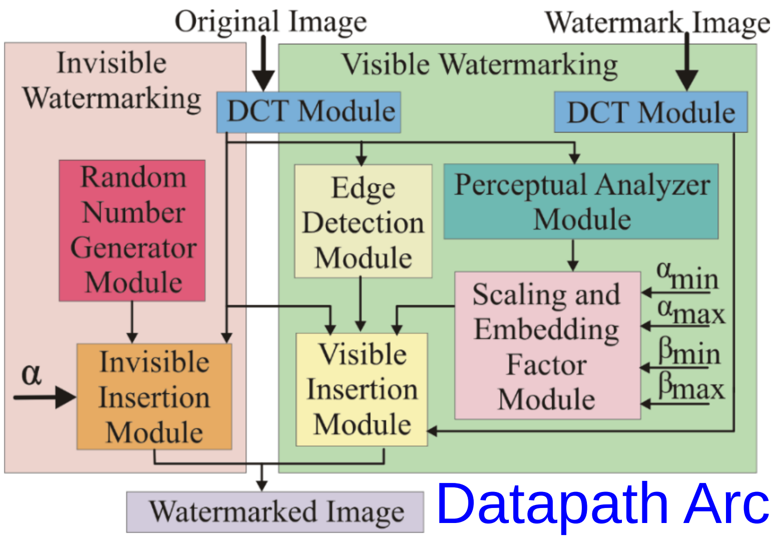
System

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

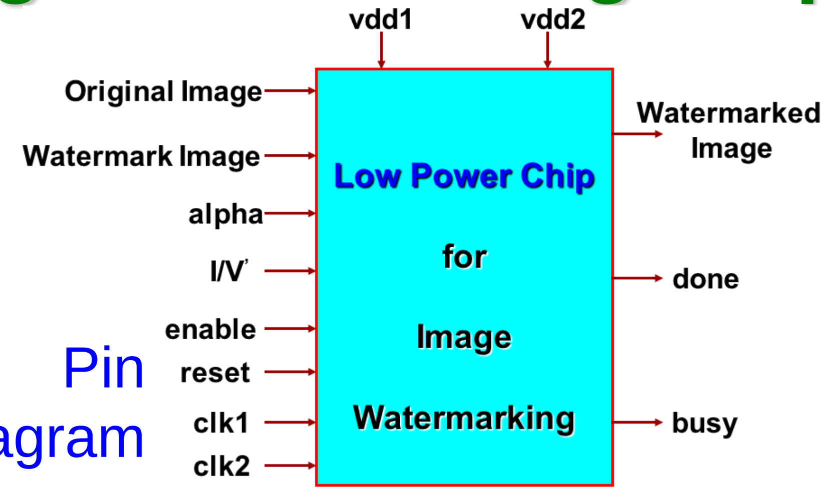


Source: S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking", *IEEE Consumer Electronics Magazine (CEM),* Volume 6, Issue 3, July 2017, pp. 83--91.

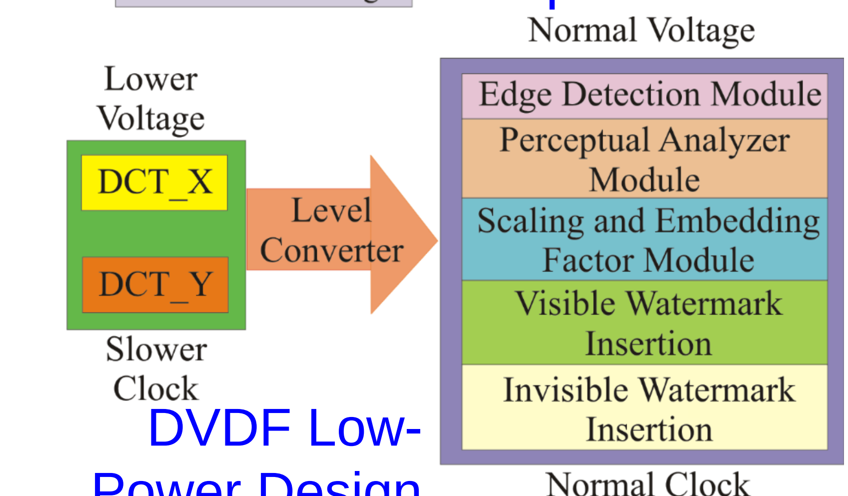
Lowest Power Consuming Watermarking Chip



Datapath Architecture



Pin Diagram



DVDF Low-Power Design

Hardware Layout

Physical Design Data

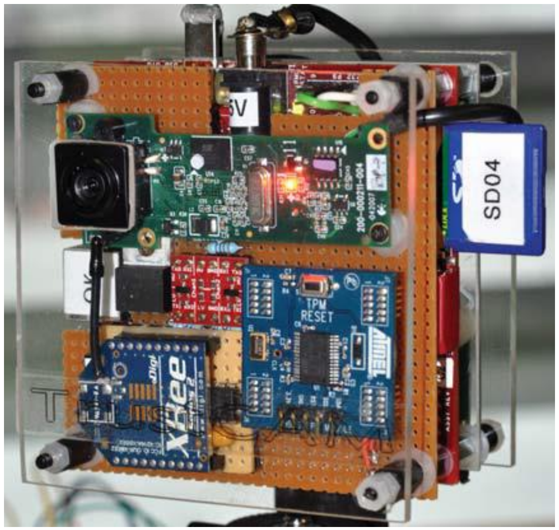
Total Area : 16.2 sq mm

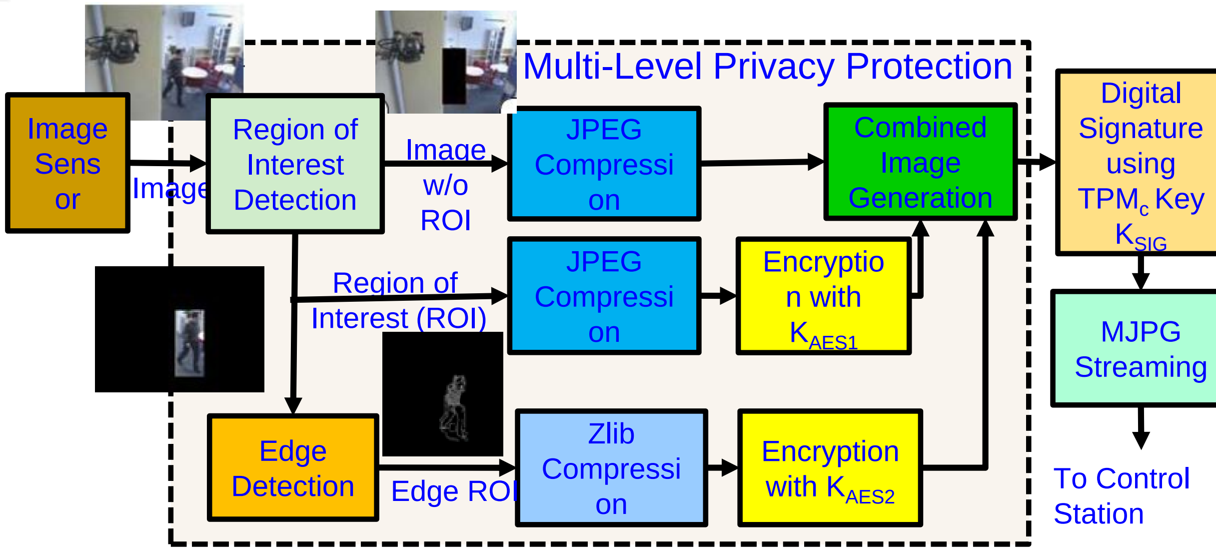
No. of Transistors: 1.4 million

Power Consumption: 0.3 mW

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

My Watermarking Research Inspired - TrustCAM



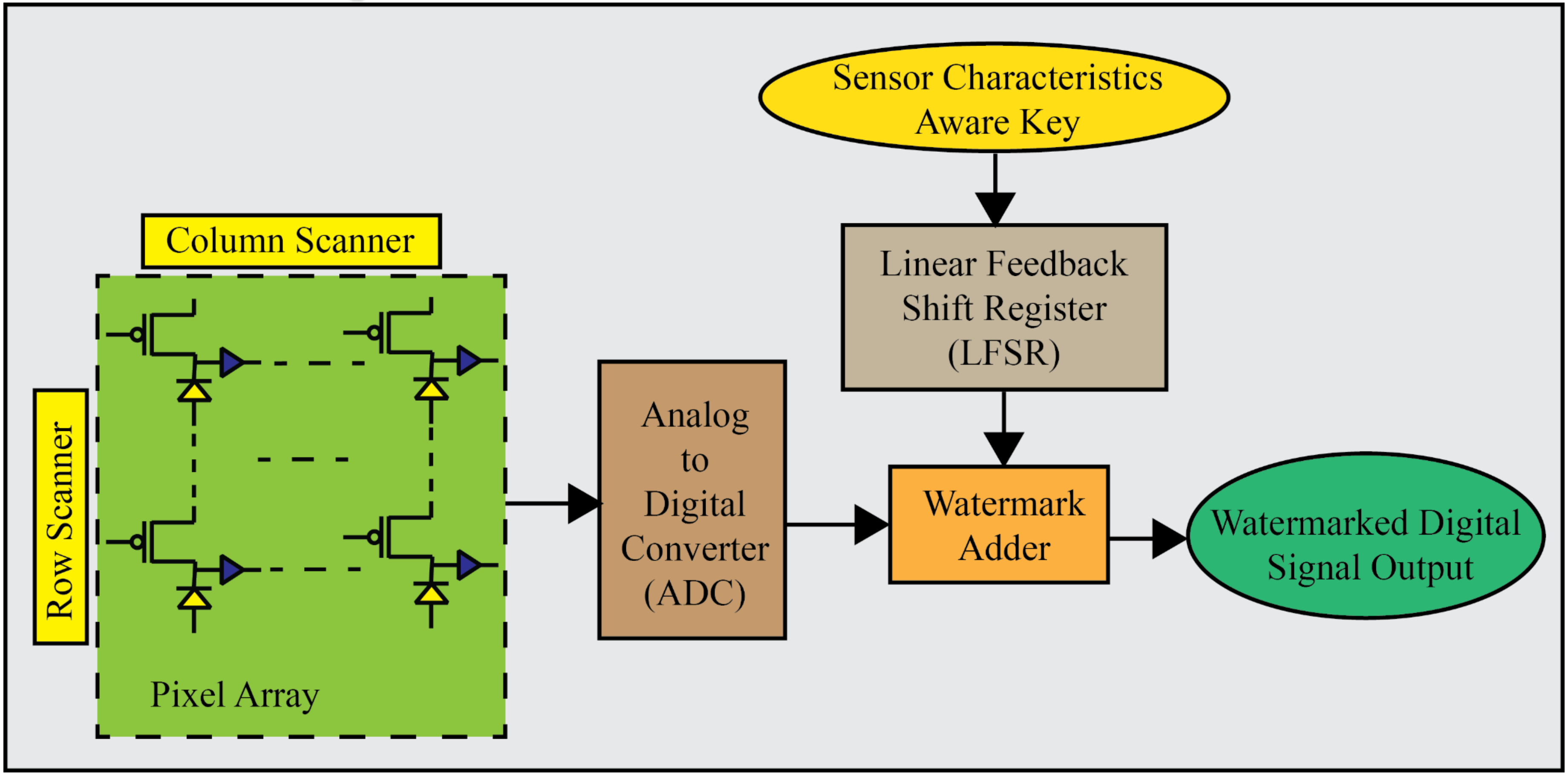


For integrity protection, authenticity and confidentiality of image data.

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

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

My Watermarking Research Inspired – Secured Sensor



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

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: needs sustainable IoT/CPS

JOIN IEEE Consumer Electronics Society

IEEE CESoc - We bring New Technologies to Life

Entertainment, Communications, Information,
Home Automation, Health Care, Education, Convenience
to name just a few focal points and growing each year

Why Join IEEE?

You join a community of over 420,000 technology and engineering professionals united by a common desire to continuously learn, interact, collaborate, and innovate. Get the resources and opportunities you need to keep on top of changes in technology. Get involved in standards development". We can use the similar paragraph to suite CESoc: "CESoc is the premier technical association in the Consumer Electronics Industry striving to advance the theory and practice of electronic engineering in the areas of multimedia entertainment and games, digital audio/ visual systems, smart home products, smart phones, IoT devices, AI, Block Chain and more. You join a Society of technology and engineering professionals united by a common desire to continuously learn, interact, collaborate, and innovate in Consumer Technology. Get the resources and opportunities you need to keep on top of changes and to be updated with latest consumer technology."

Who is CESoc?
The field of interest of the Consumer Electronics Society is engineering and research aspects of the theory, design, construction, manufacture or end use of mass market electronics, systems, software and services for consumers. The society sponsors multiple conferences annually including the International Conference on Consumer Electronics and the International Symposium on Consumer Electronics.

CESoc Membership includes
Monthly Society newsletter (electronic), Bi-Monthly IEEE Consumer Electronics Magazine (electronic and print), Quarterly IEEE Transactions on Consumer Electronics (electronic), Discounts on Conference Registration, Reduced Prices on Affiliated Journals, IEEE Consumer Electronics Society Digital Library (electronic) and IEEE Consumer Electronics Society Resource Center (electronic).

IEEE Membership Includes
Subscription to IEEE Spectrum magazine, The Institute and other relevant newsletters, electronic access to IEEE Potentials, IEEE Collabratec, inclusion in the IEEE Member Directory, members-only IEEE.tv programming, an exclusive ieee.org email account, discounts on products and services, continuing education, philanthropic opportunities, and more. Plus, you are automatically a part of your local IEEE Section and will receive communications about local networking opportunities, meetings, and special events.

Start your CESoc and IEEE membership immediately: Join online www.ieee.org/join and select IEEE Consumer Electronics Society
(costs vary by country of residence -see website)

Enjoy January/February 2020 CE Magazine

Free to Read Online or Download at
http://magazine.ieee-cesoc.org
(download option at top right of page)

The IEEE Consumer Electronics Society (CESoc) will change the society's name to the IEEE Consumer Technology Society (CTSoc) starting from August 2020

IEE... ...nics

IEEE Consumer Electronics Magazine

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

The MCE won an Apex Grand Award for excellence in writing in 2013. The MCE is the winner in the Regional 2016 STC Technical Communication Awards - Award of Excellence! The MCE is indexed in Clarivate Analytics (formerly IP Science of Thomson Reuters). The 2019 impact factor of MCE is 4.016.

Advertise to Billion Dollar Consumer Electronics Industries

Visit: https://www.officialmediaguide.com/ie07/

Aim and Scope

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

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

Submission Instructions

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

I. A manuscript of maximum 6-page length: A pdf of the complete manuscript layout with figures, tables placed within the text. Extra pages (beyond allowed 6 pages) can be purchased.

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

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

Editorial Board

- Saraju P. Mohanty, University of North Texas, Editor in Chief (EiC)
- Peter Corcoran, National University of Ireland Galway, Emeritus EiC
- Katina Michael, Arizona State University
- Stephen Dukes, Dreamerse Inc.
- Tom Wilson, Concured Ltd.
- Bob Frankston, Frankston.com
- Himanshu Thapliyal, University of Kentucky
- Stu Lipoff, IP Action Partners LLC
- Tom Coughlin, Coughlin Associates
- Fabrizio Lamberti, Politecnico di Torino
- Helen (Hai) Li, Duke University
- Theocharis Theocharides, University of Cyprus
- Arslan Munir, Kansas State University
- Soumya Kanti Datta, EURECOM Research Center
- Joseph Wei, SJW Consulting Inc.
- Animesh Kumar, Indian Institute of Technology Bombay
- Xavier Fernando, Ryerson University
- Niranjan Ray, KIIT University, Bhubaneswar
- Fatemeh Tehranipoor, San Francisco State University
- Sudeep Pasricha, Colorado State University
- Shang-Jang Ruan, National Taiwan Univ of Science & Tech
- Yu Yuan, Motiveware Technology Corporation Limited
- Vincent Wang, XPERI Corp, DTS Inc.
- Euee S. Jang, Hanyang University
- Bernard Fong, Auckland University of Technology
- Muhammad K. Khan, King Saud University
- Deepak Puthal, Newcastle University
- Hyoungshick Kim, Sungkyunkwan University
- Jong-Hyouk Lee, Sejong University
- Susanne Wende, Noerr LLP
- Baek-Young Choi, University of Missouri - Kansas City
- Hiten Zaveri, Yale University
- Lia Morra, Politecnico di Torino
- Santanu Mishra, Indian Institute of Technology Kanpur
- Amit K. Mishra, University of Cape Town
- Shingo Yamaguchi, Yamaguchi University
- Haruhiko Okumura, Toshiba Corporation
- Pallab Chatterjee, Media & Entertainment Technologies
- Petronel Bigioi, Xperi Corporation
- Dhruva Ghai, Oriental University
- Mike Borowczak, University of Wyoming
- Konstantin Glasman, Saint Petersburg State University of Film and Television

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

Smart Electronic Systems Laboratory (SESL)

IEEE sumer

IEEE Transactions on Consumer Electronics

The IEEE Transactions on Consumer Electronics Magazine (TCE) is the flagship transactions journal of the consumer technology society (CTSoc) of IEEE. The transactions is published four times year (Feb, May, Aug and Nov) and features a range of topical content on state-of-art consumer electronics systems, services and devices, and associated technologies.

Advertise to Billion Dollar Consumer Electronics Industries

Visit: https://www.officialmediaguide.com/ie07/

Aim and Scope

- The scope of the IEEE Transactions on Consumer Electronics is ***"The engineering and research aspects of the theory, design, construction, manufacture or end use of mass market electronics, systems, software and services for consumers"***.
- Transactions on Consumer Electronics covers the areas or topics that are related to "consumer electronics".
- Topics of interest to consumer electronics among others are: Video technology, Audio technology, Home care products, Mobile communications, Gaming, Air care products, Home medical devices, Fitness devices, Home automation and networking devices, Consumer solar technology, Home theater, Digital imaging, In-vehicle technology, Wireless technology, Home security, Domestic lighting, Human interface, Artificial intelligence, Home computing, Video Technology, Consumer storage technology.

Have questions on submissions or ideas for special issues, contact EiC at fernando.pescador@upm.es

Submission Instructions

Submission should follow IEEE standard template and should consist of a manuscript of maximum 8-page length: A pdf of the complete manuscript layout with figures, tables placed within the text. Additional pages can be submitted with an extra charge per page.

Authors should note that **NOW THERE IS NO SUBMISSION DEADLINE**. The papers are reviewed continuously and the average time to receive an answer is around 8 weeks. When a paper is accepted, it is immediately published on IEEE Early Access and it can be referenced.

The average delay from submission to posting on Xplore is less than 2 months. An IEEE copyright form will be required. The manuscripts need to be submitted online at the URL:
http://mc.manuscriptcentral.com/tce-ieee

More Information at:
https://ctsoc.ieee.org/publications/ieee-transactions-on-consumer-electronics.html

Editorial Board

Fernando Pescador, UPM, Spain, Editor-in-Chief (EiC)
Simon Sherrat, Univ Surrey, UK, Past Editor-in-Chief

Senior Editors

Gustavo Callico. ULP Gran Canaria, Spain.
Ulrich Reiter. Cologne University, Germany.
Ilker Hamzaoglu. Sabanci University, Turkey.
Wen-Chung Kao. National Taiwan Univ., Taiwan.

Associate Editors

Marcelo Knörich Zuffo. Univ Sao Paolo, Brazil.
Muhammad Khurram Khan. King Saud U, Saudi Arabia.
Gordana Velikić. RT-RK Institute. Serbia.
Lucio Ciabattoni. Univ. Politecnica delle Marche, Italy.
Qinglai Wei. Chinese Academy of Sciences, China.
Bo Ai. Beijing Jiaotong University, China
Francisco J. Bellido. Cordoba University, Spain.
Lauren A Christopher. Indiana University, USA.
Peter M. Corcoran. NUI Galway, Ireland.
Thomas M. Coughlin, Coughlin Associates, USA.
Daniel Diaz-Sanchez. Univ. Carlos III, Spain.
A. C. Fong. Glasgow University, Singapore.
Bernard Fong. City University, Hong Kong.
Slawomir Grzonkowski. Symantec, Ireland.
Sung-Jea Ko. Korea University, Korea.
Jong-Hyouk Lee. Sangmyung University, Korea.
Saraju P. Mohanty. Univertsity North Texas, USA.
Yong-Tae Lee. ETRI, Korea.
Andres Marin Lopez. Univ. Carlos III, Spain.
Joonki Paik. Chung-Ang University, Korea.
Dirk Wendel. Intel, Germany.
Anirban Sengupta. Indian Institute of Technology. India
Fabrizio Lamberti. Politecnico de Torino, Italy.
Jong-Moon Chung. Yonsei University, Korea.
Zhenhui Yuan. University of Wollongong, Australia.
Mohammad Shojafar. University of Padua, Italy.
Yeong-Kan Lai. National Chung Hsing Univ, Taiwan
Reinhard Moeller. Wuppertal University, Germany.
Narciso Garcia. Univ. Politécnica de Madrid, Spain

APPLICATIONS FOR NEW ASSOCIATE EDITORS ARE WELCOMMED. Email to Fernando.pescador@upm.es

Smart Electronic Systems Laboratory (SESL)

IEEE International Symposium on Smart Electronic Systems (IEEE-iSES)

https://www.ieee-ises.org

6th IEEE International Symposium on Smart Electronic Systems (iSES)