Security by Design for Cyber-Physical Systems

Invited Talk - National Workshop On IoT and Sensor Embedded Applications

Silicon Institute of Technology, Bhubaneswar

20 Dec 2019

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.

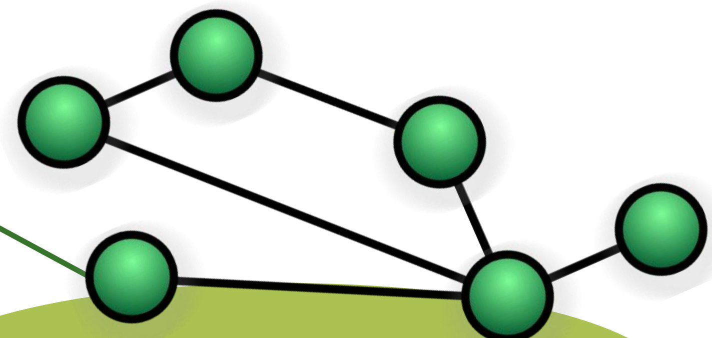
Smart Cities - 3 Is

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)

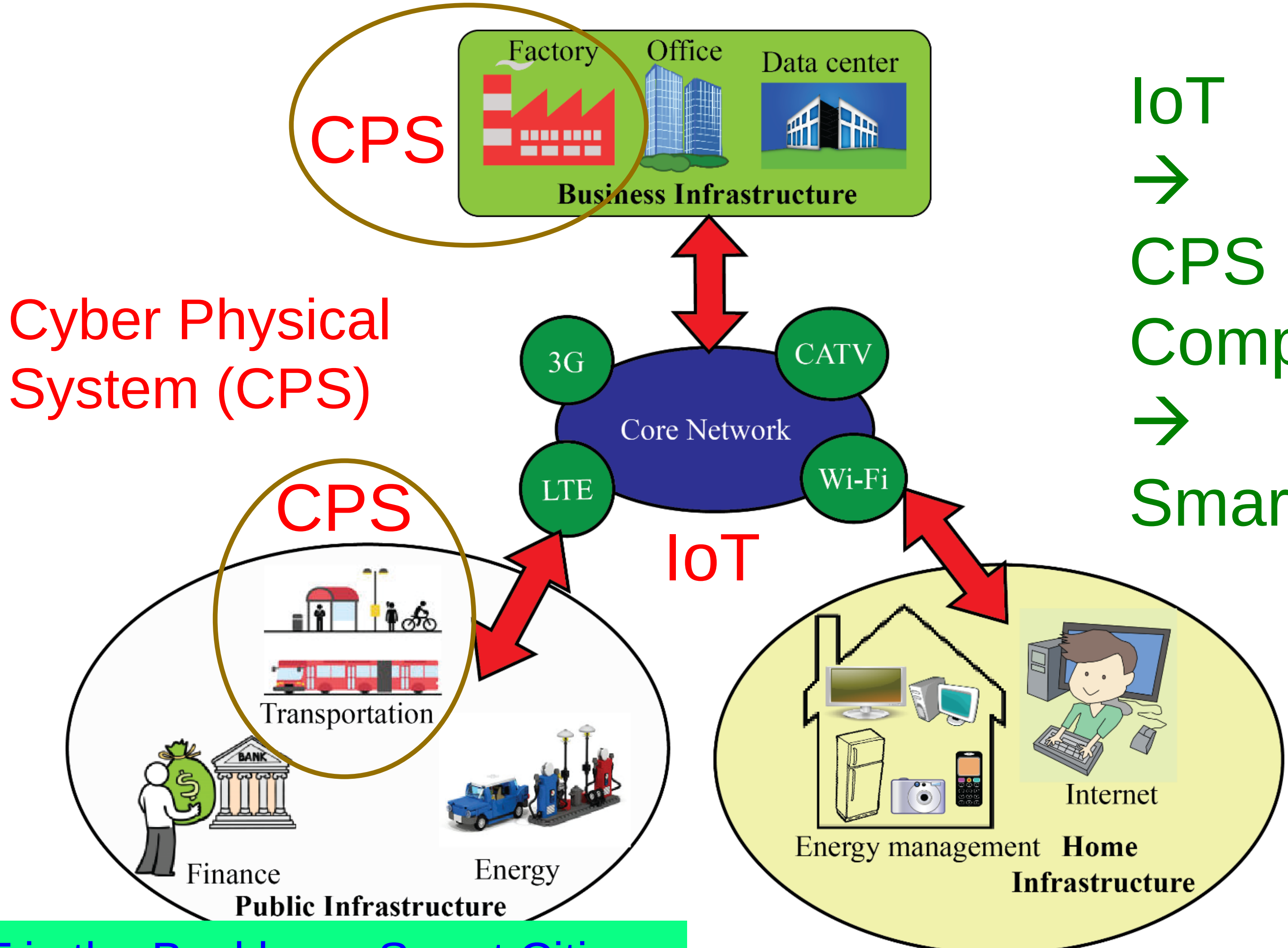
Global Network
Connecting bridge between the local network, cloud services and connected consumer devices

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

IoT → CPS → Smart Cities

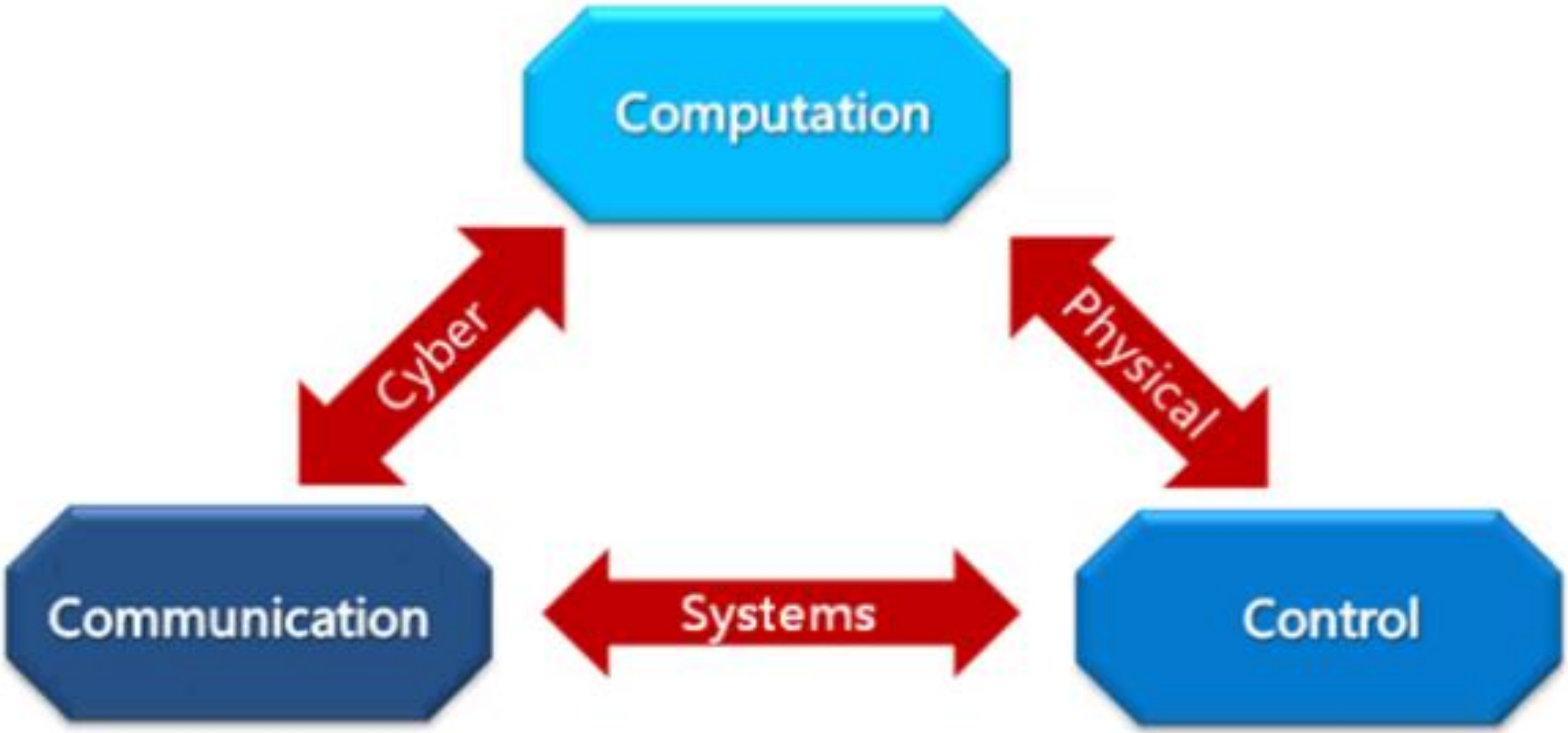


IoT
→
CPS (Smart Components)
→
Smart Cities

IoT is the Backbone Smart Cities.

Source: Mohanty CE Magazine July 2016

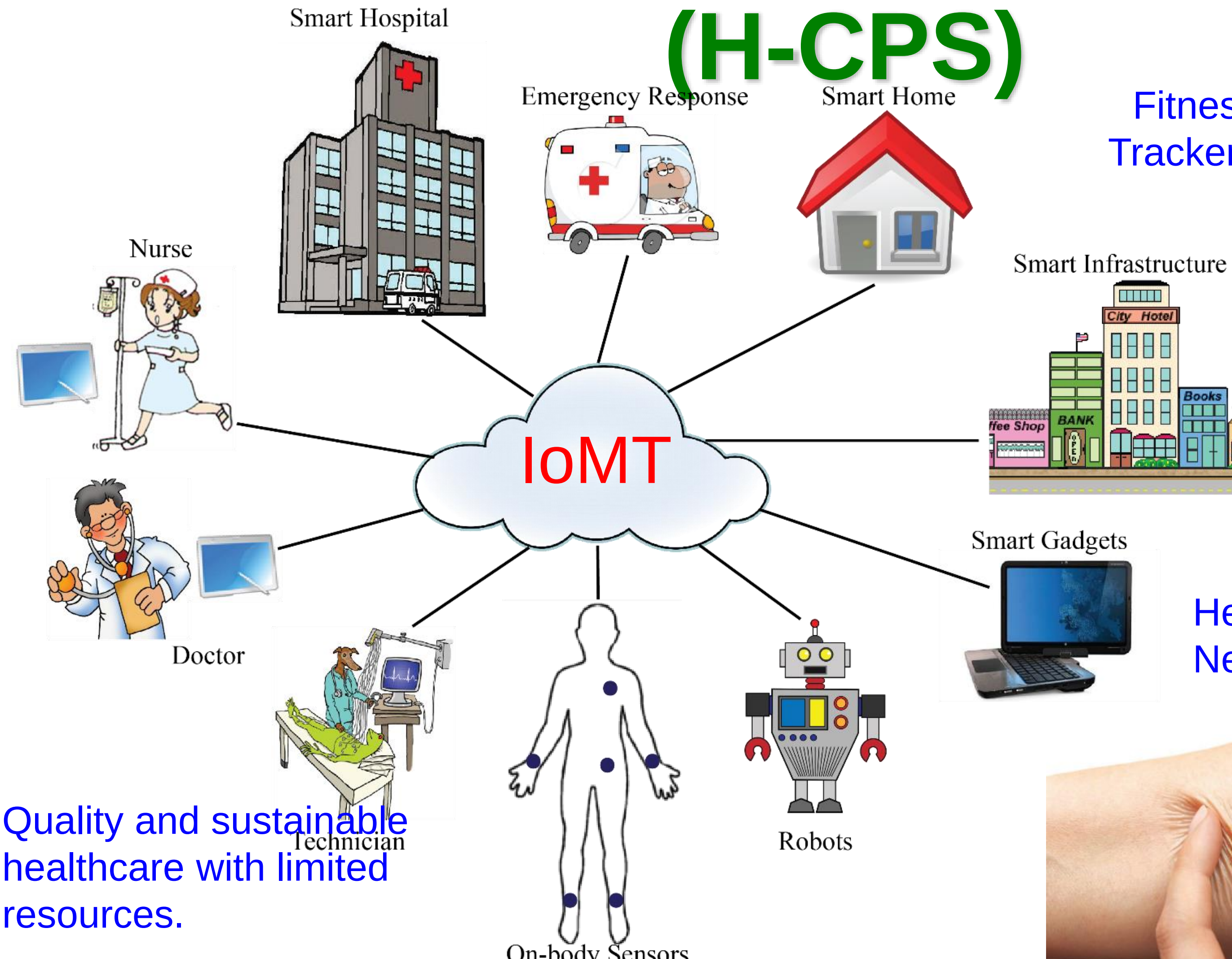
Cyber-Physical Systems (CPS) - 3 Cs



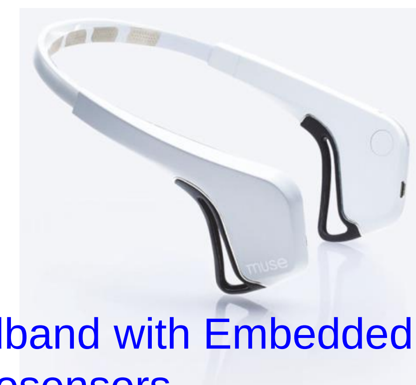
3 Cs of IoT - Connect, Compute, Communicate

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.

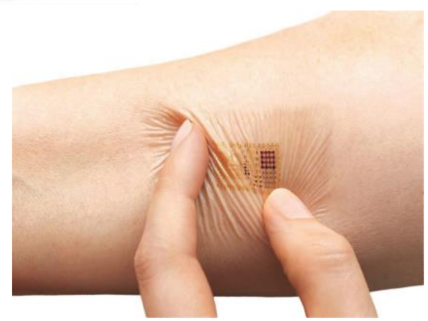
Healthcare Cyber-Physical System (H-CPS)



Fitness Trackers



Headband with Embedded Neurosensors



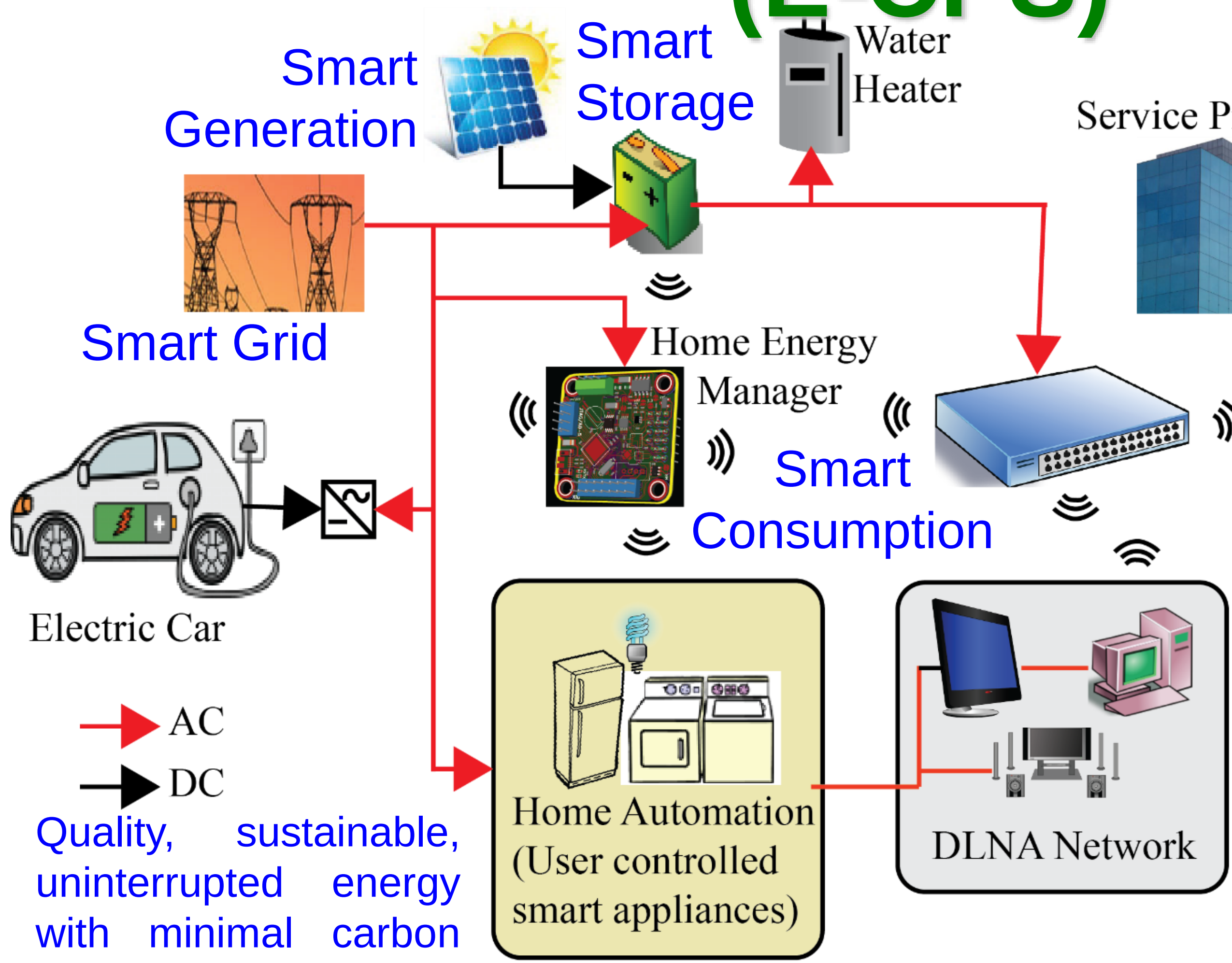
Embedded Skin Patches

Quality and sustainable healthcare with limited resources.

Source: Mohanty CE Magazine July 2016

Energy Cyber-Physical Systems (E-CPS)

Internet of Energy



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Source: Mohanty CE Magazine July 2016

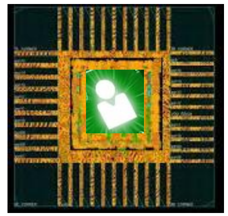
IoT Role:

- 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)

Security, Privacy, and IP Rights

Hardware Trojan



July 2017

System Security

Data Security

System Privacy

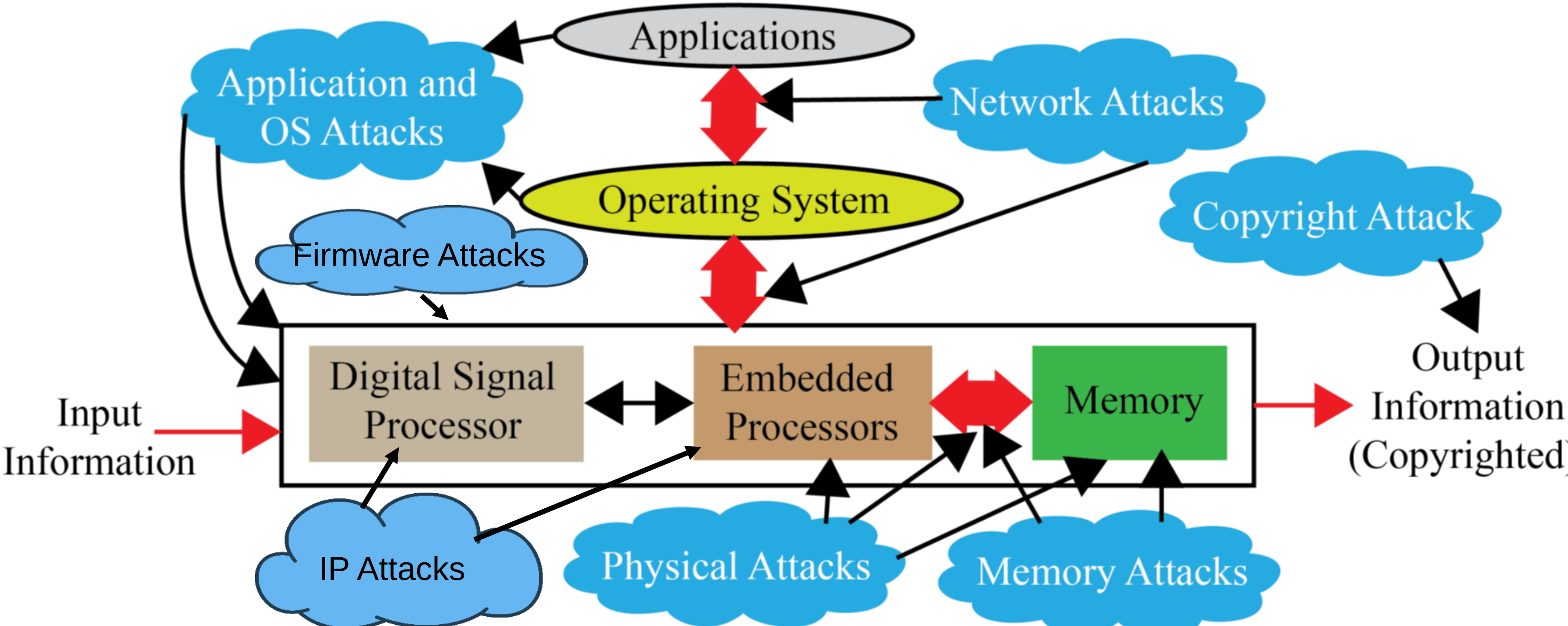
Data Privacy

Counterfeit Hardware
(IP Rights Violation)

Data Ownership

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

IoT Security - Attacks and Countermeasures

Edge nodes	Computing nodes	
	RFID tags	
Communication		
Edge computing		

Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
Denial of Service (DoS)	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non-standard frameworks and inadequate testing	All
Insufficient/Inessential logging	C,AC,NR,P

Countermeasures
Side-channel signal analysis
Trojan activation methods
Intrusion Detection Systems (IDSs)
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning and Decentralization
Role-based authorization
Information Flooding
Pre-testing
Outlier detection

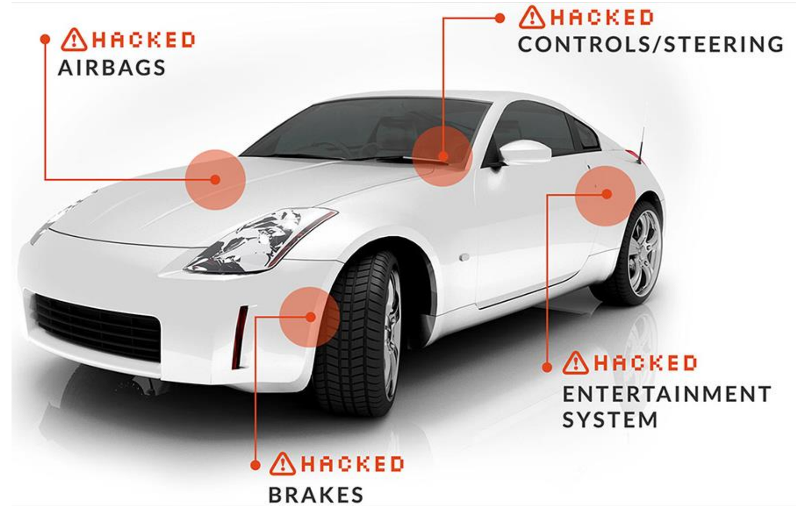
C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

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 Challenge - System

Power Grid Attack

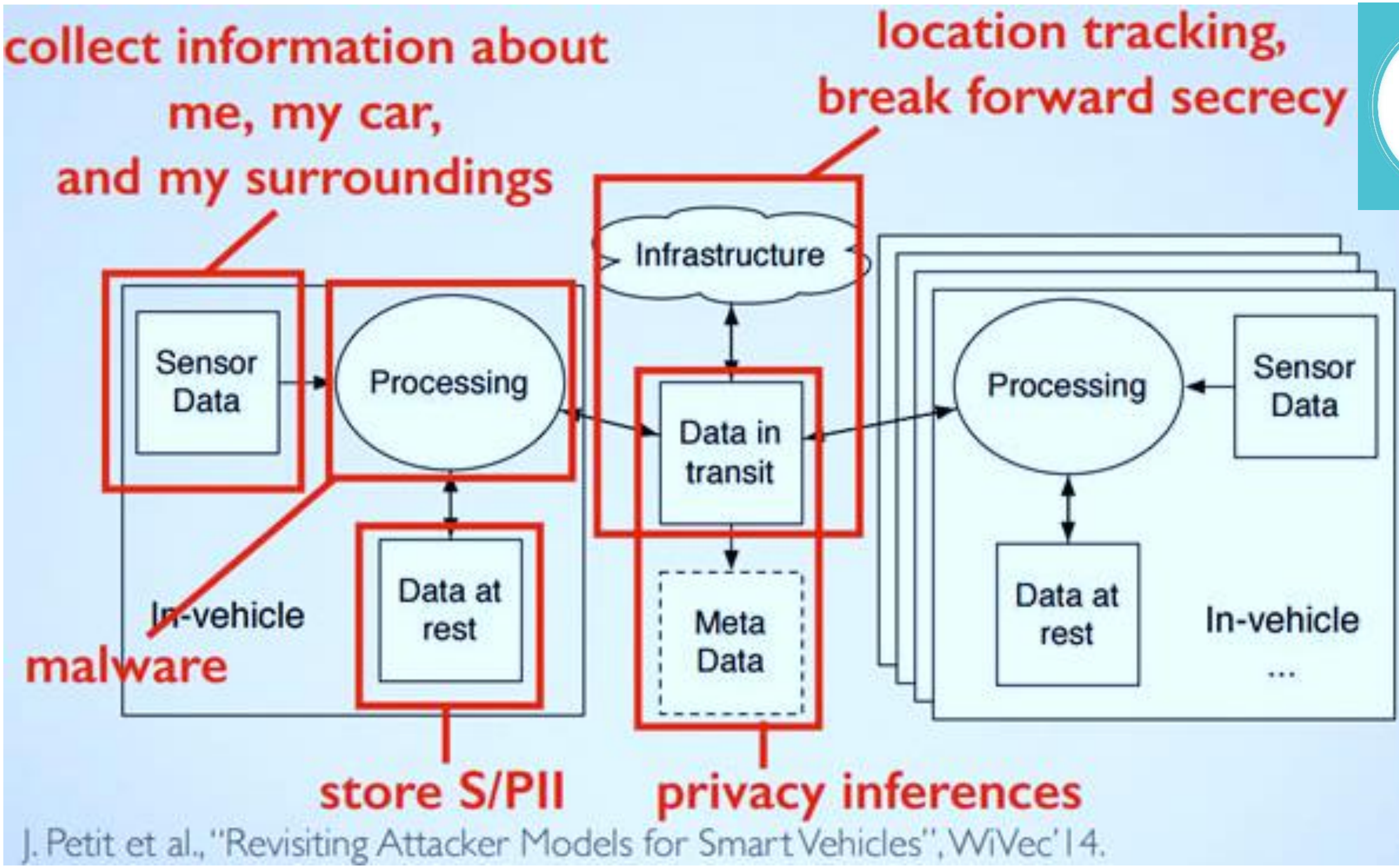
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



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

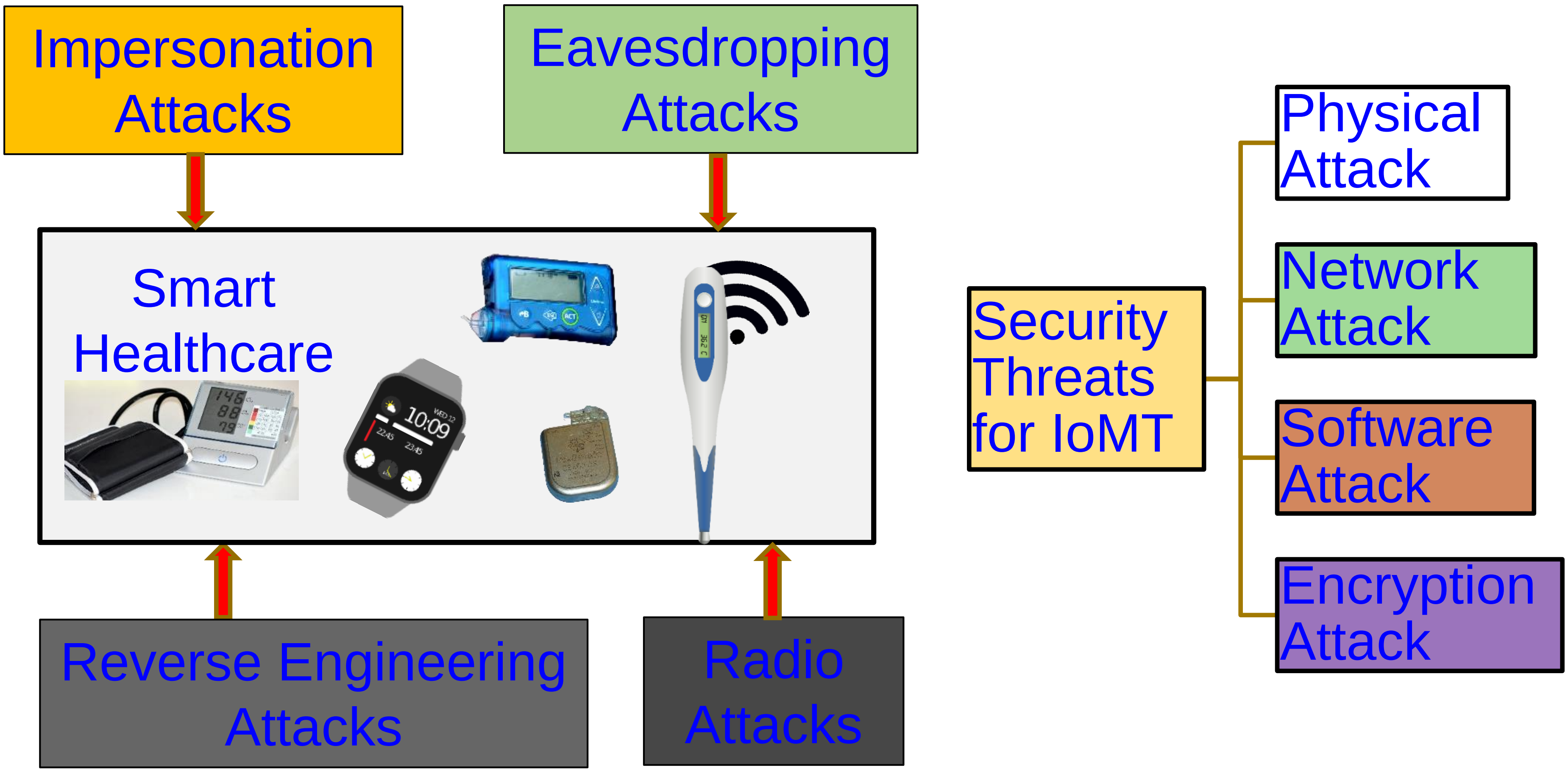
Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Privacy Challenge – System, Location



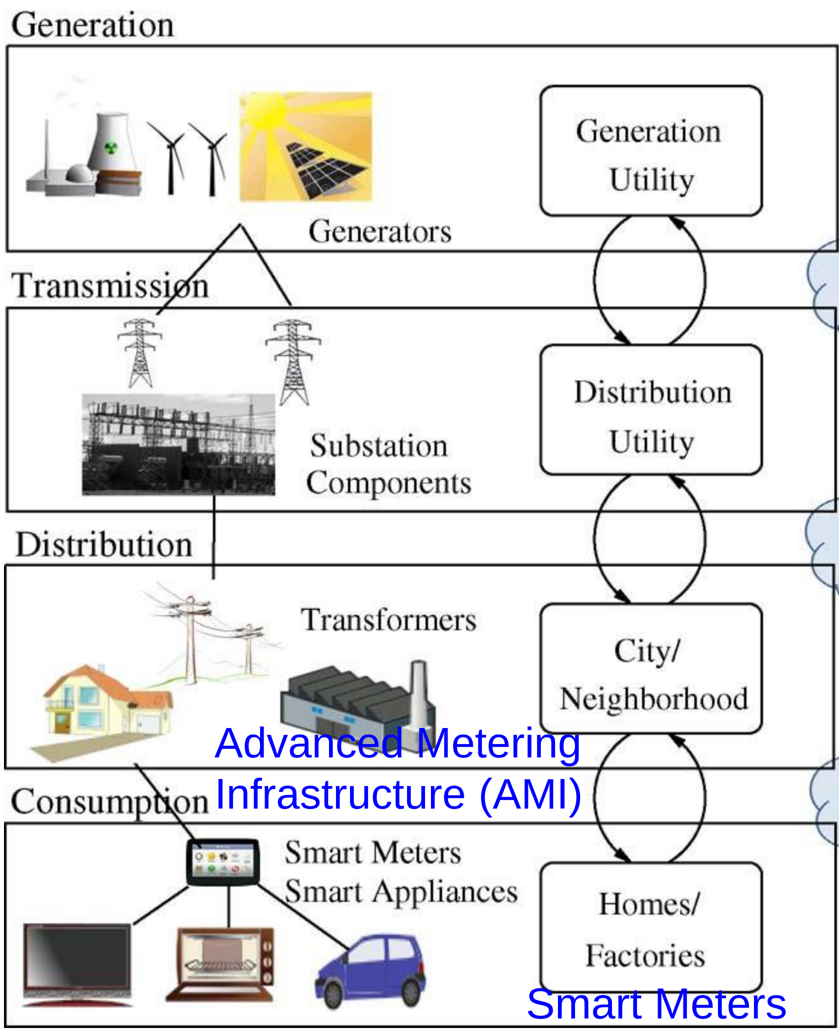
Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html

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



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)

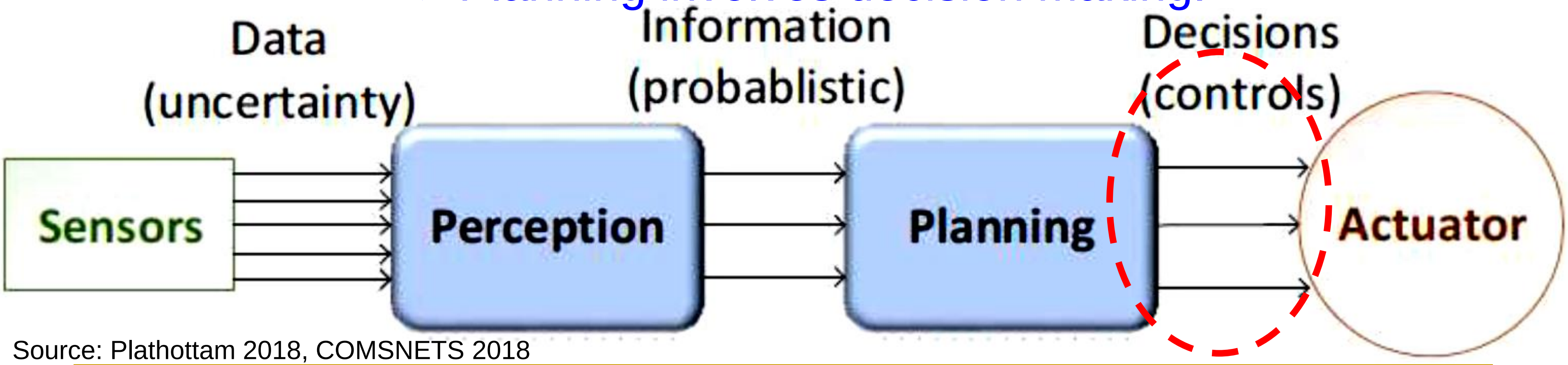
Smart Meters

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.

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.



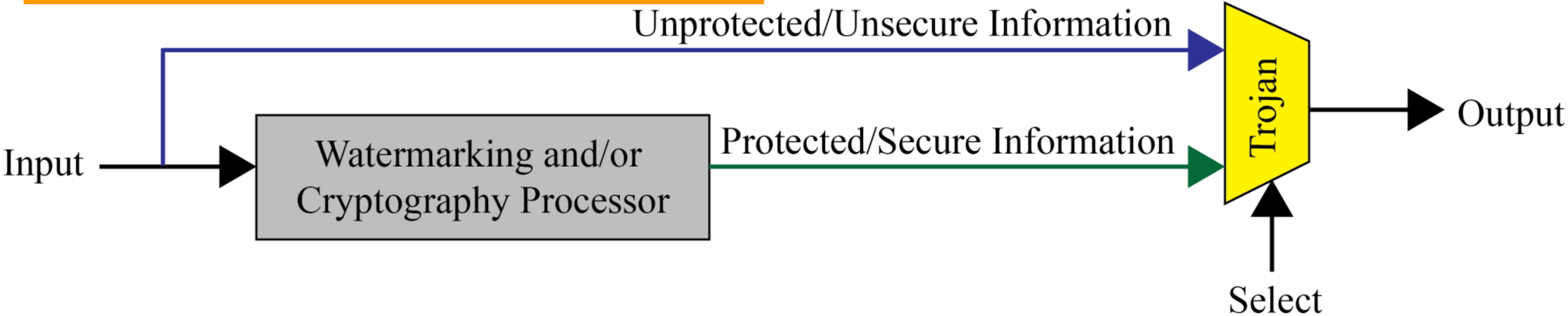
Source: Plathottam 2018, COMSNETS 2018

Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

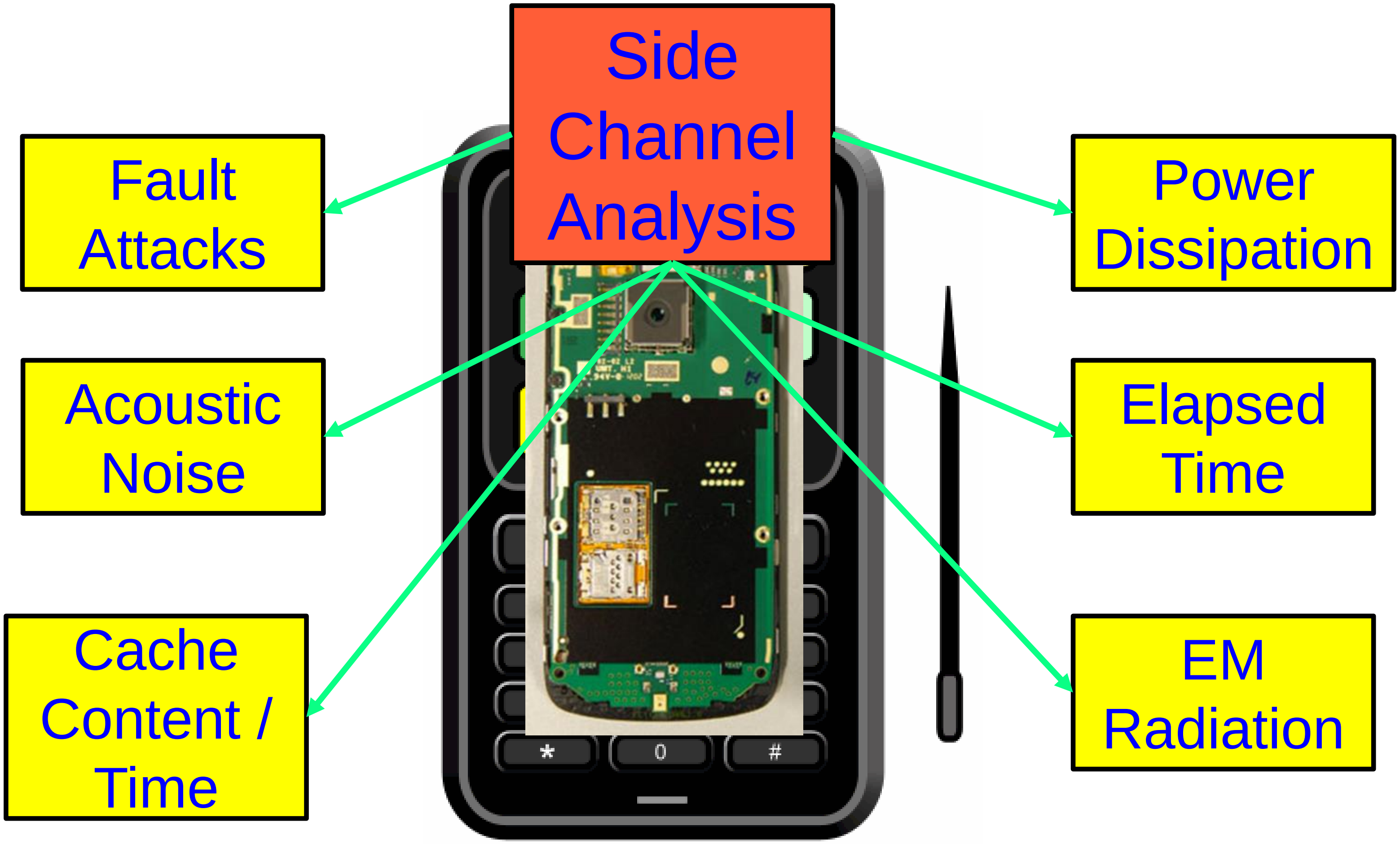
Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans



Source: Mohanty 2015, McGraw-Hill 2015

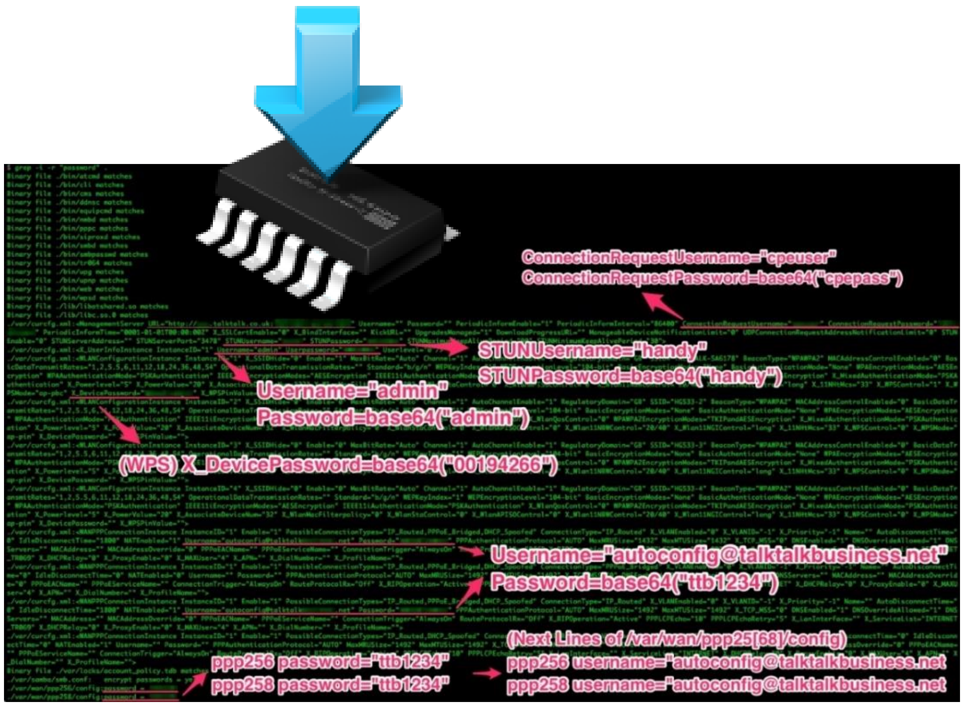
Side Channel Analysis Attacks



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

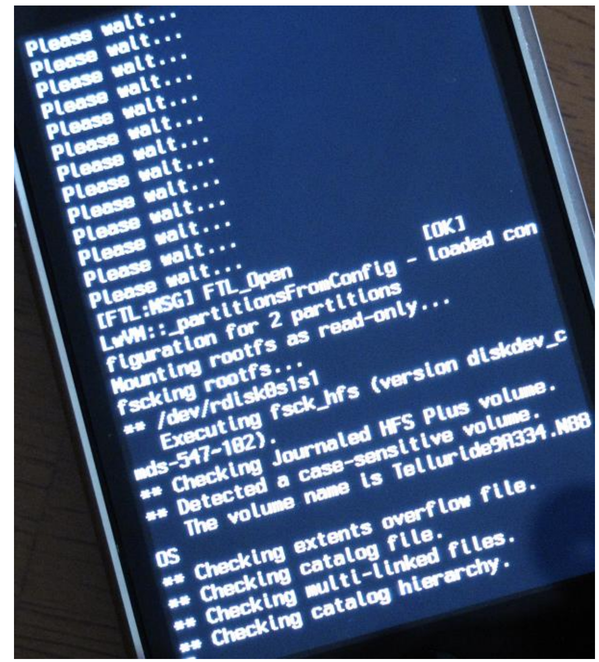
Source: Parameswaran Keynote iNIS-2017

Firmware Reverse Engineering is Security Threat for any Embedded Systems



Extract, modify, or reprogram code

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



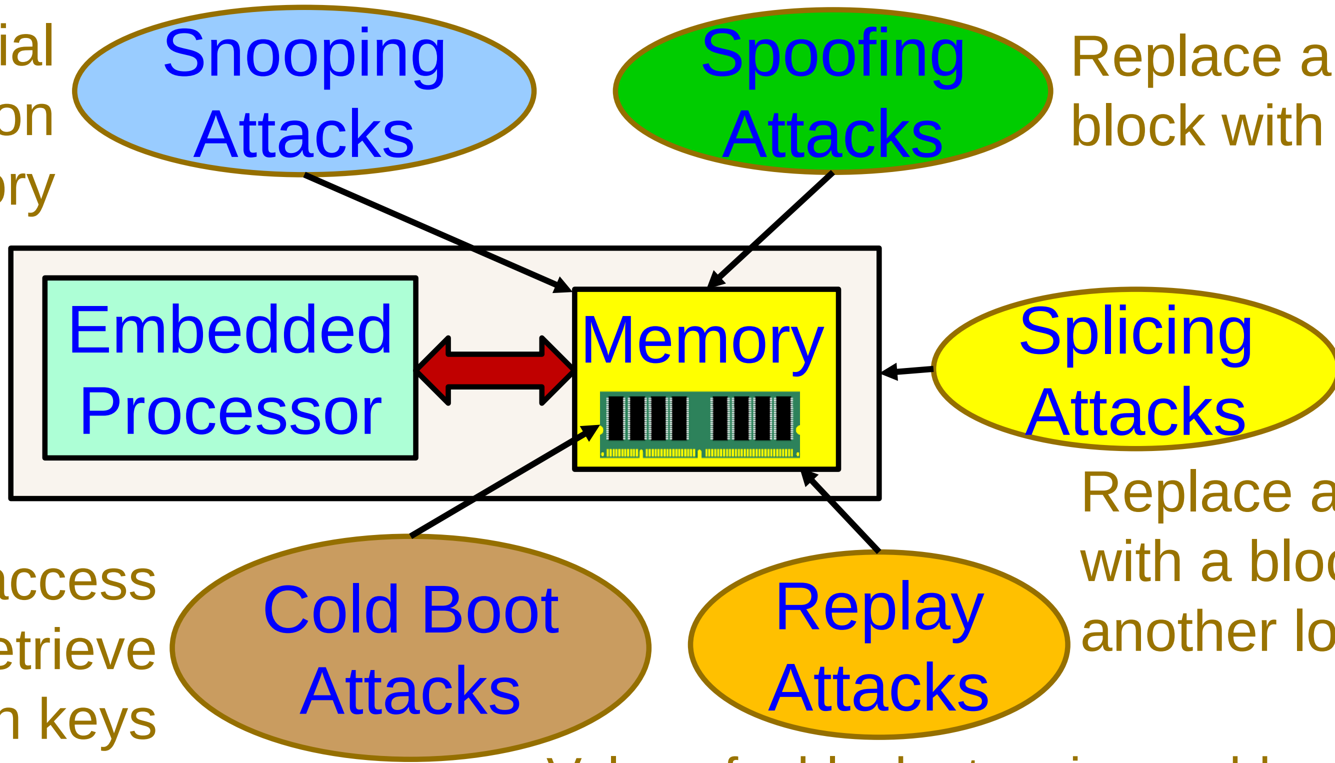
OS exploitation, Device jailbreaking

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.

Drawbacks of Existing Security Solutions

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

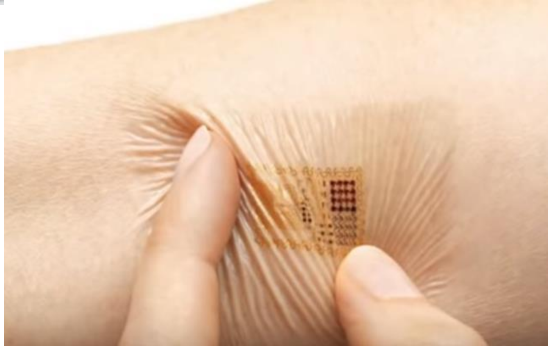
- IoT may be deployed in open hostile environments
- Significantly large variety of IoT devices
- Billions of IoT devices
- May not have computational power to run security solutions
- IoT security breach (e.g. in a IoMT device like pacemaker, insulin pump) can be life threatening

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

Wearable Medical Devices (WMDs)

Fitness Trackers

Headband with Embedded Neurosensors



Embedded Skin Patch

Source: http://www.sciencetimes.com/articles/8087/20160107/ces-loreals-smart-skin-patch-reveals-long-exposed-sun.htm

Source: https://www.empatica.com/embrace2/

Smart watch to detect seizure

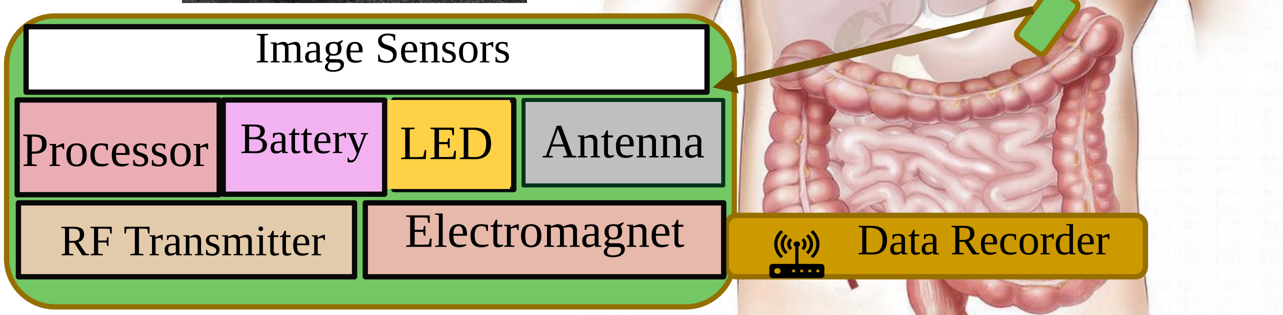
Wearable Medical Devices (WMDs) → Battery Constrained

Insulin Pump

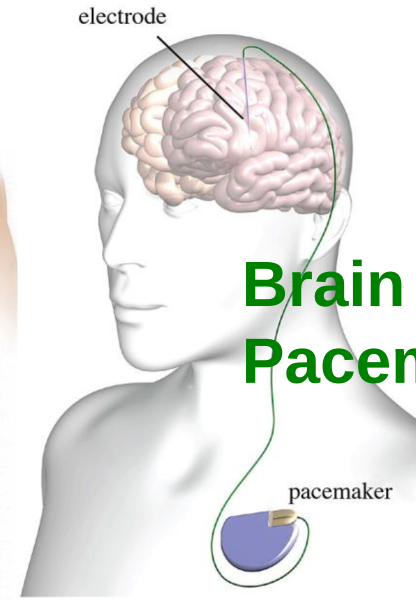
Source: https://www.webmd.com

Implantable Medical Devices (IMDs)

Pill Camera



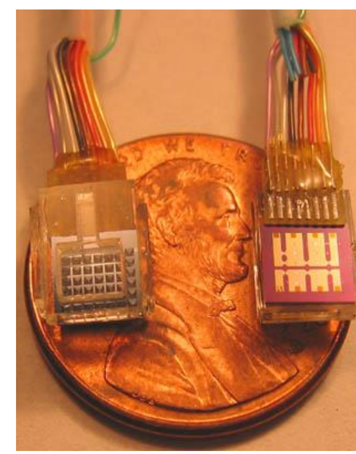
Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, *IEEE Consumer Electronics Magazine (CEM)*, Vol. 7, No. 1, January 2018, pp. 18-28.



Brain Pacemaker

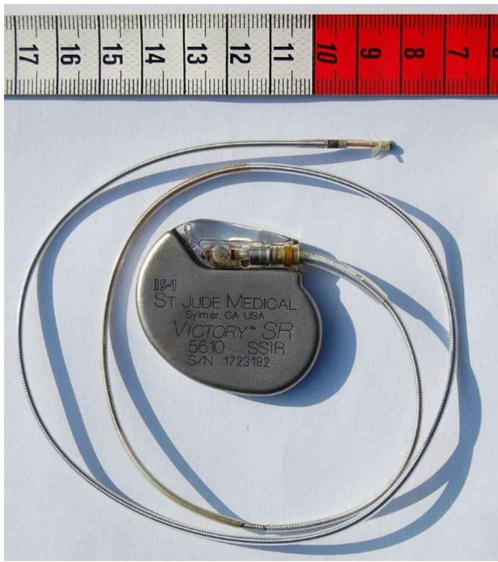
Collectively: Implantable and Wearable Medical Devices (IWMDs)

Implantable MEMS Device



Source: http://web.mit.edu/cprl/www/research.shtml

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

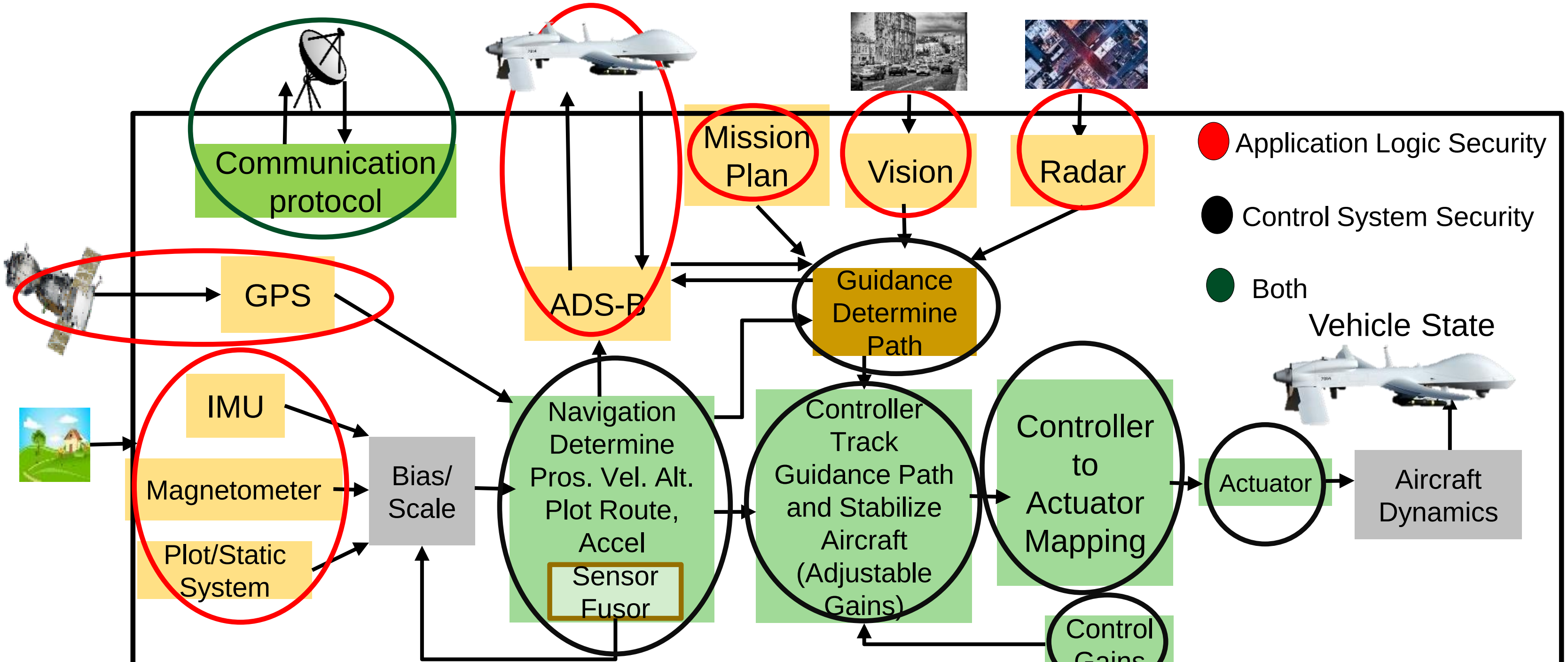
- Connected cars require latency of ms to communicate and avoid impending crash:
  - Faster connection
  - Low latency
  - Energy efficiency

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

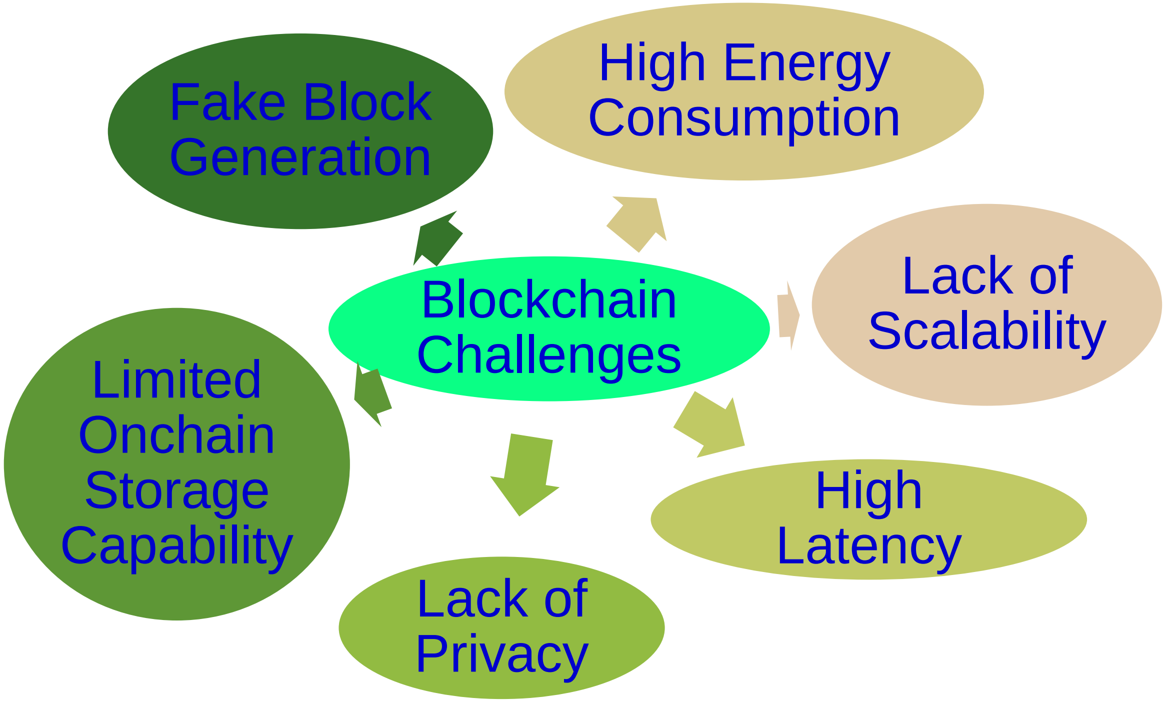
- Identification
- Authentication
- Authorization
- Trust
- Access Control
- Privacy

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



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

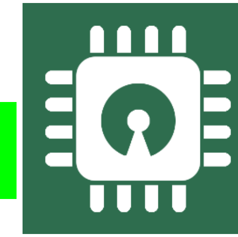
Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

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.

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

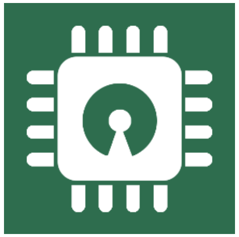
Hardware Based

- 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	Hardware Based



Software Based

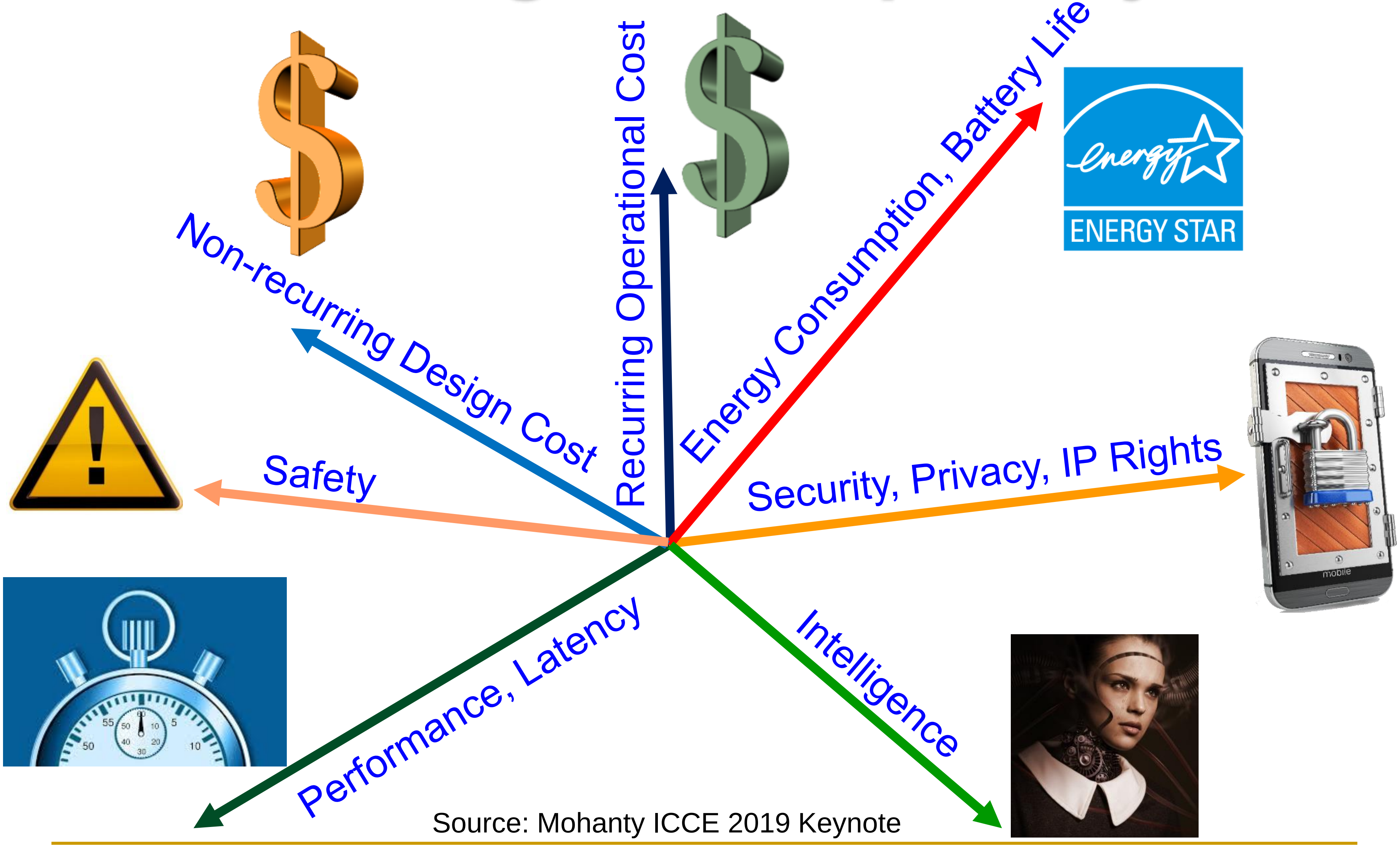
- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can’t stop hardware reverse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

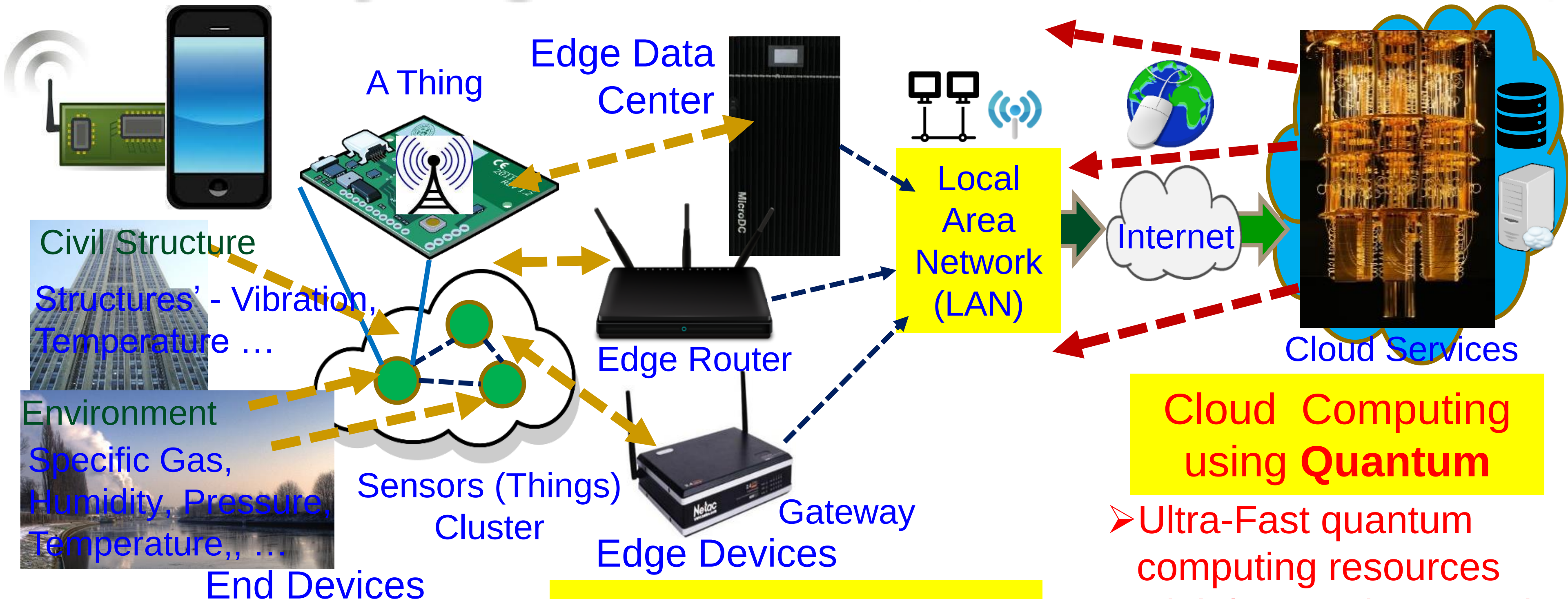
Source: Mohanty ICCE Panel 2018

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

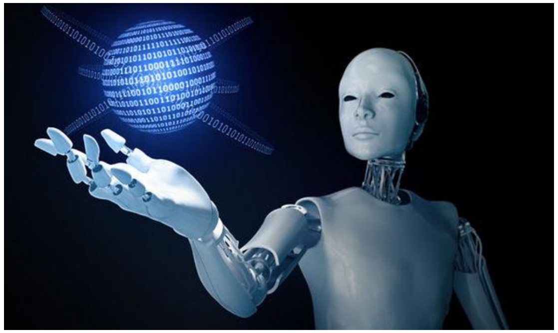
- Minimal computational resource
- Negligible latency in network
- Very lightweight security

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

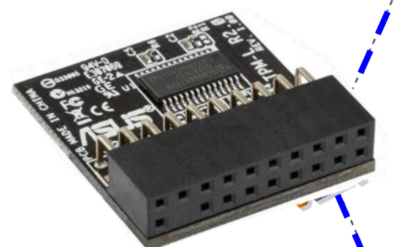
Source: Mohanty ICCE 2018 Panel

Hardware-Assisted Security (HAS)

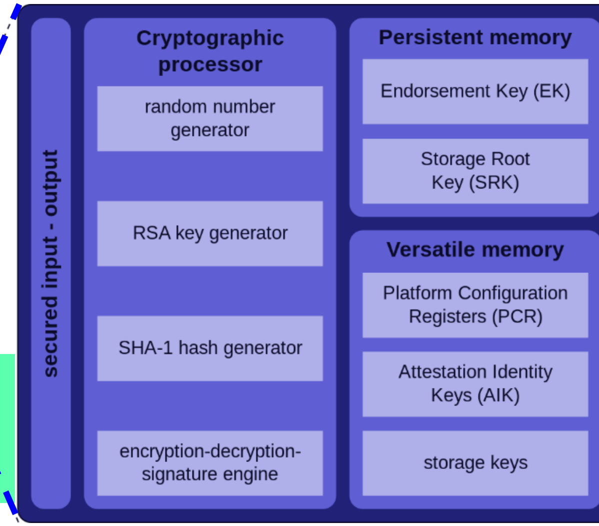
- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
  - Software based security approaches that rely on some form of encryption can't be full proof as breaking them is just matter of time.
  - It is projected that quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security: Security/Protection provided by the hardware: for information being processed by a CE system, for hardware itself, and/or for the CE system.

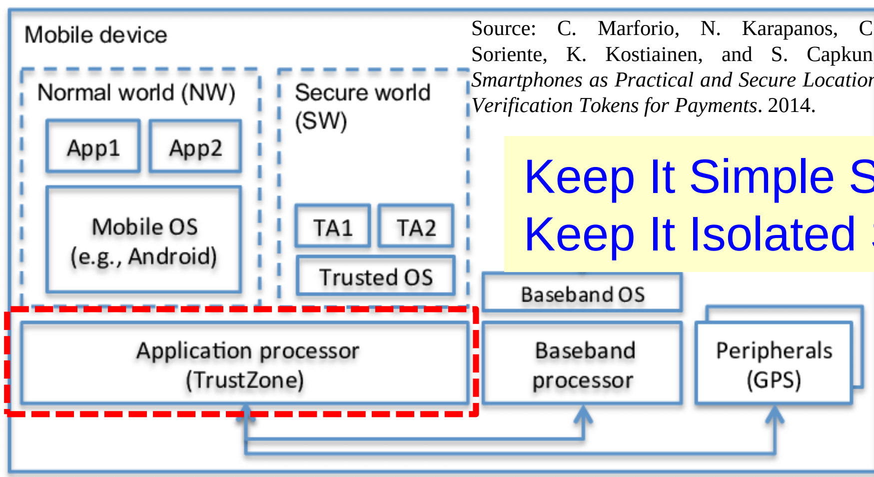
Hardware Security Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



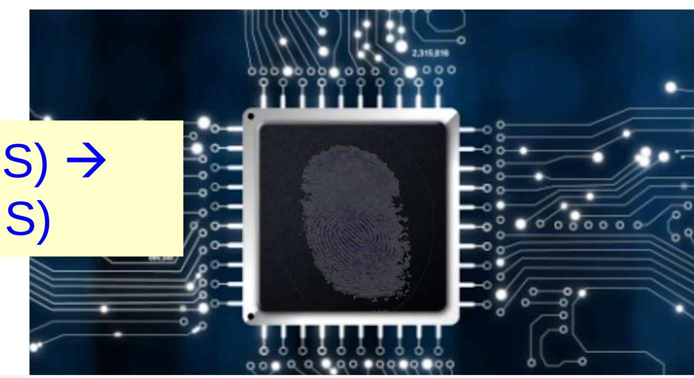
Trusted Platform Module (TPM)





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)

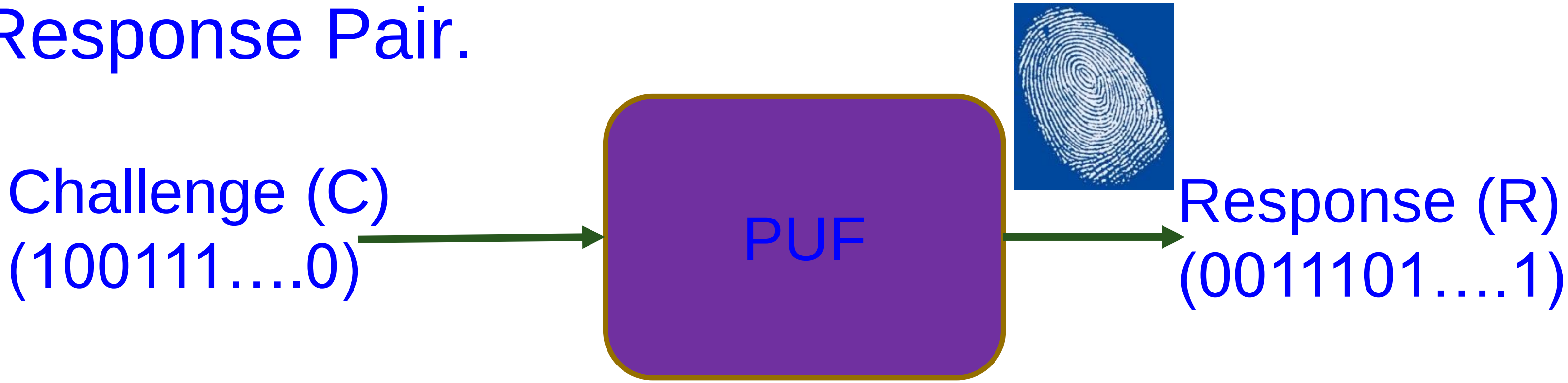


Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Physical Unclonable Functions (PUFs)

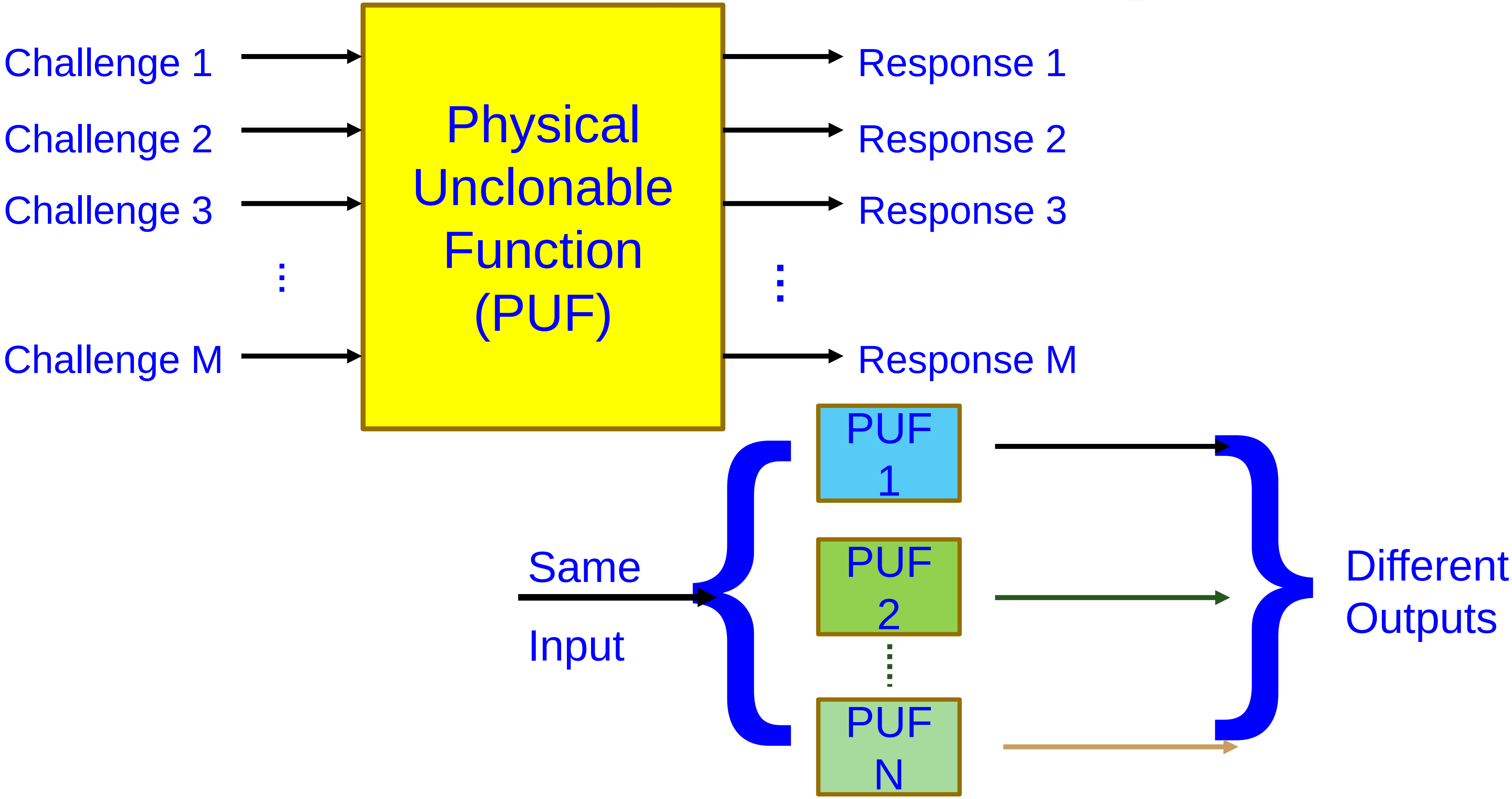
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



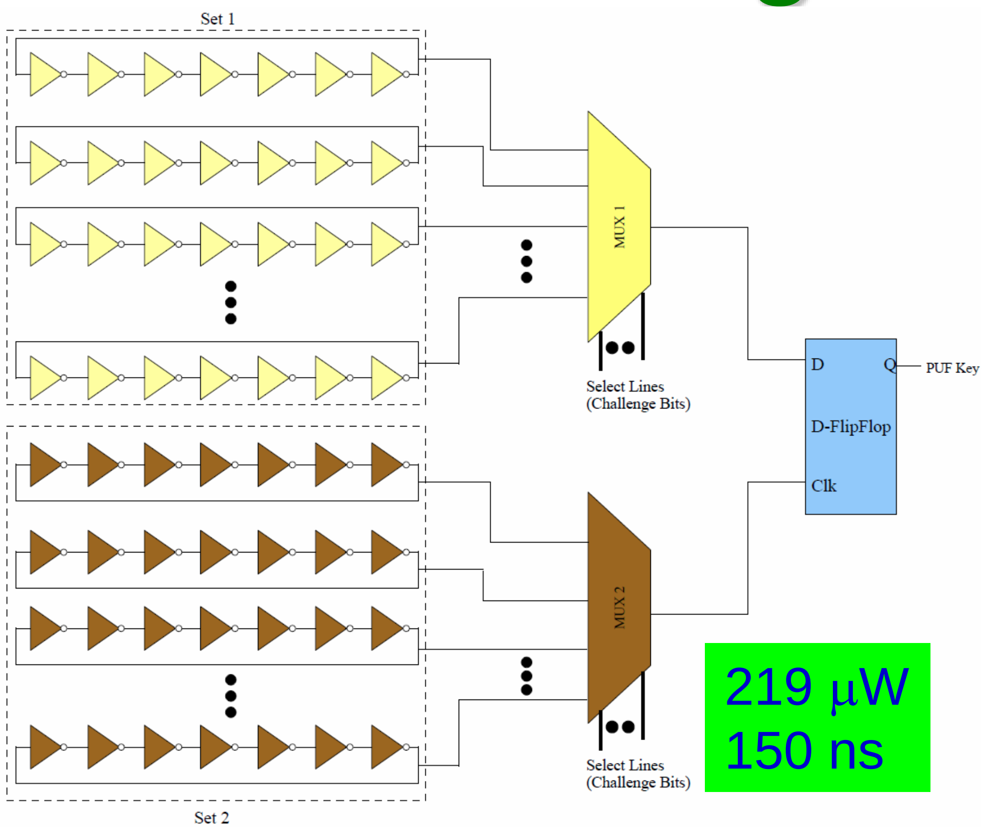
PUFs don’t store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.

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.

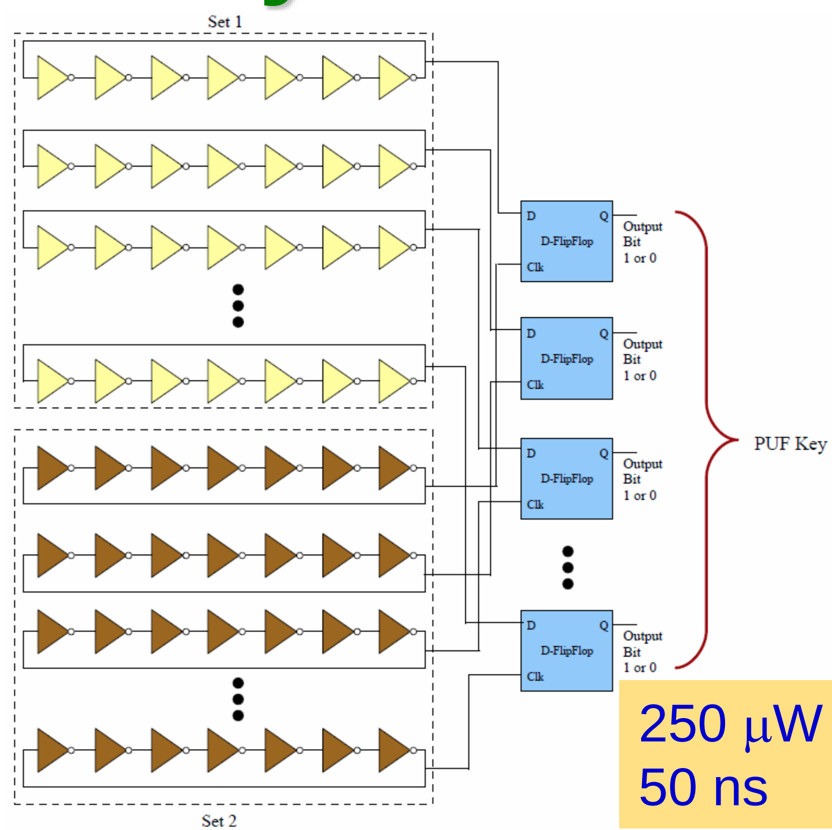
Principle of Generating Multiple Random Response using PUF



We Have Design a Variety of PUFs



219 µW
150 ns



250 µW
50 ns

Power Optimized Hybrid Oscillator Arbiter PUF

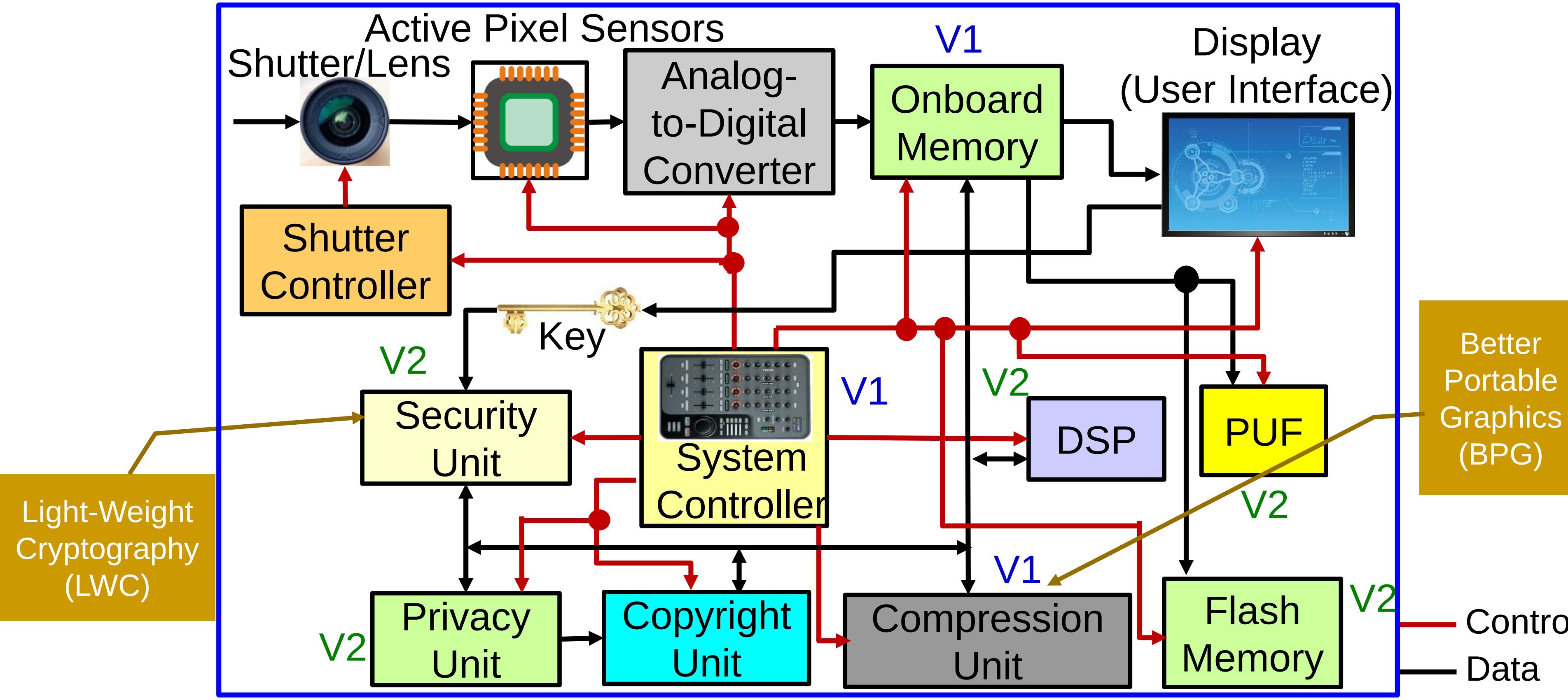
Speed Optimized Hybrid Oscillator Arbiter PUF

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

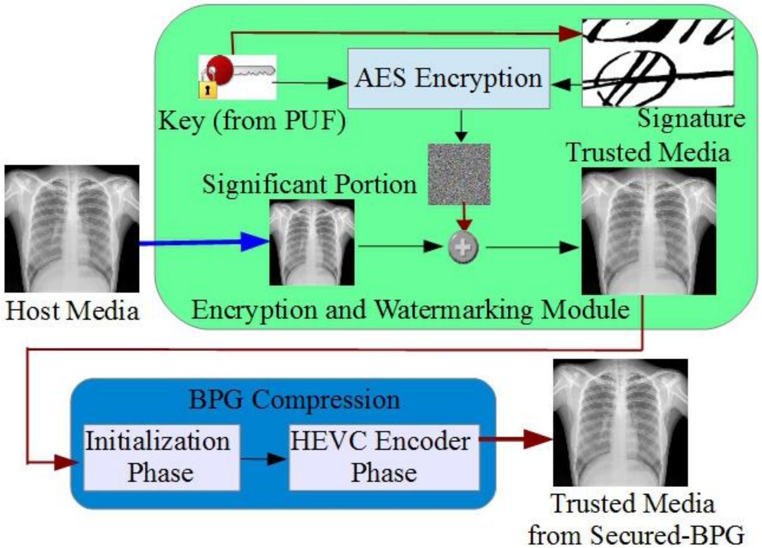


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

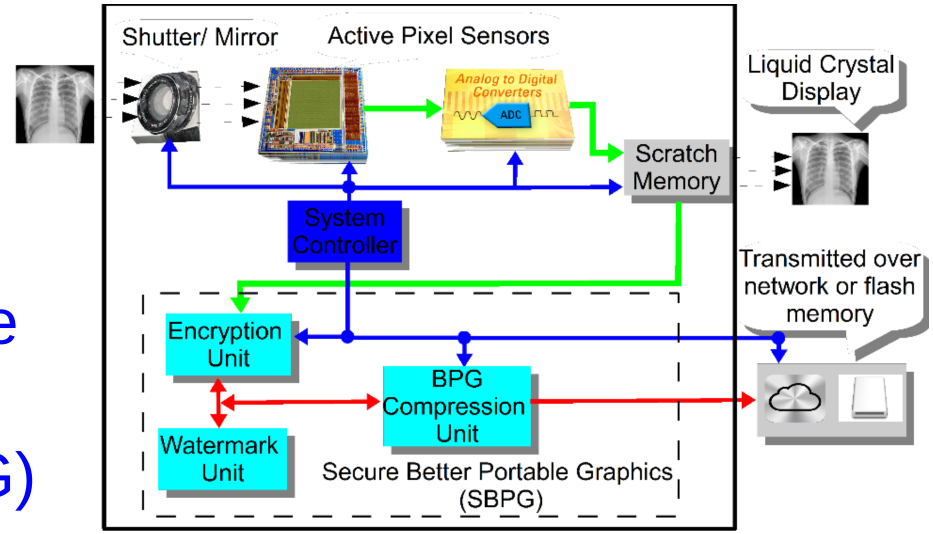
Security and/or Privacy by Design (SbD and/or PbD)

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.

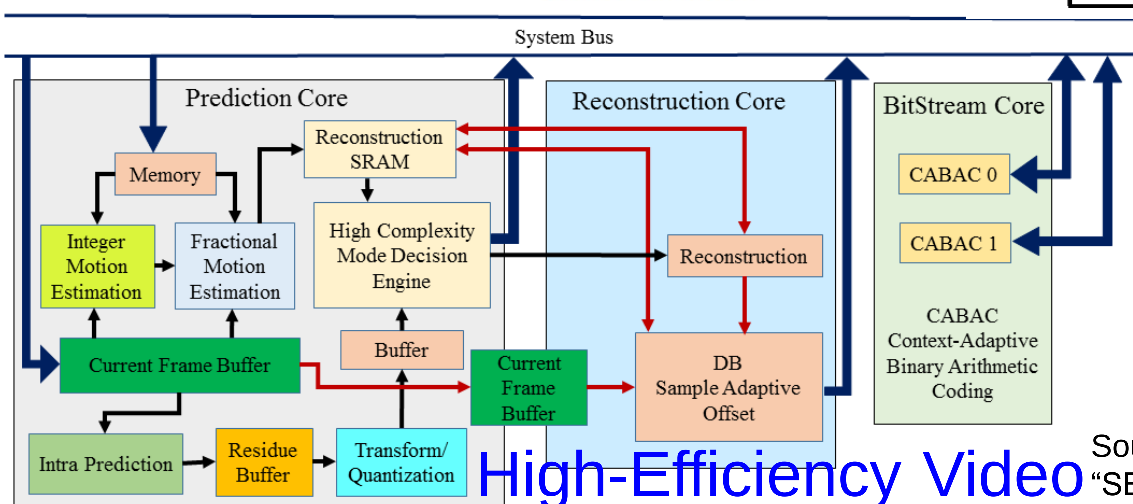
Secure Better Portable Graphics (SBPG)



Secure BPG (SBPG)



Secure Digital Camera (SDC) with SBPG

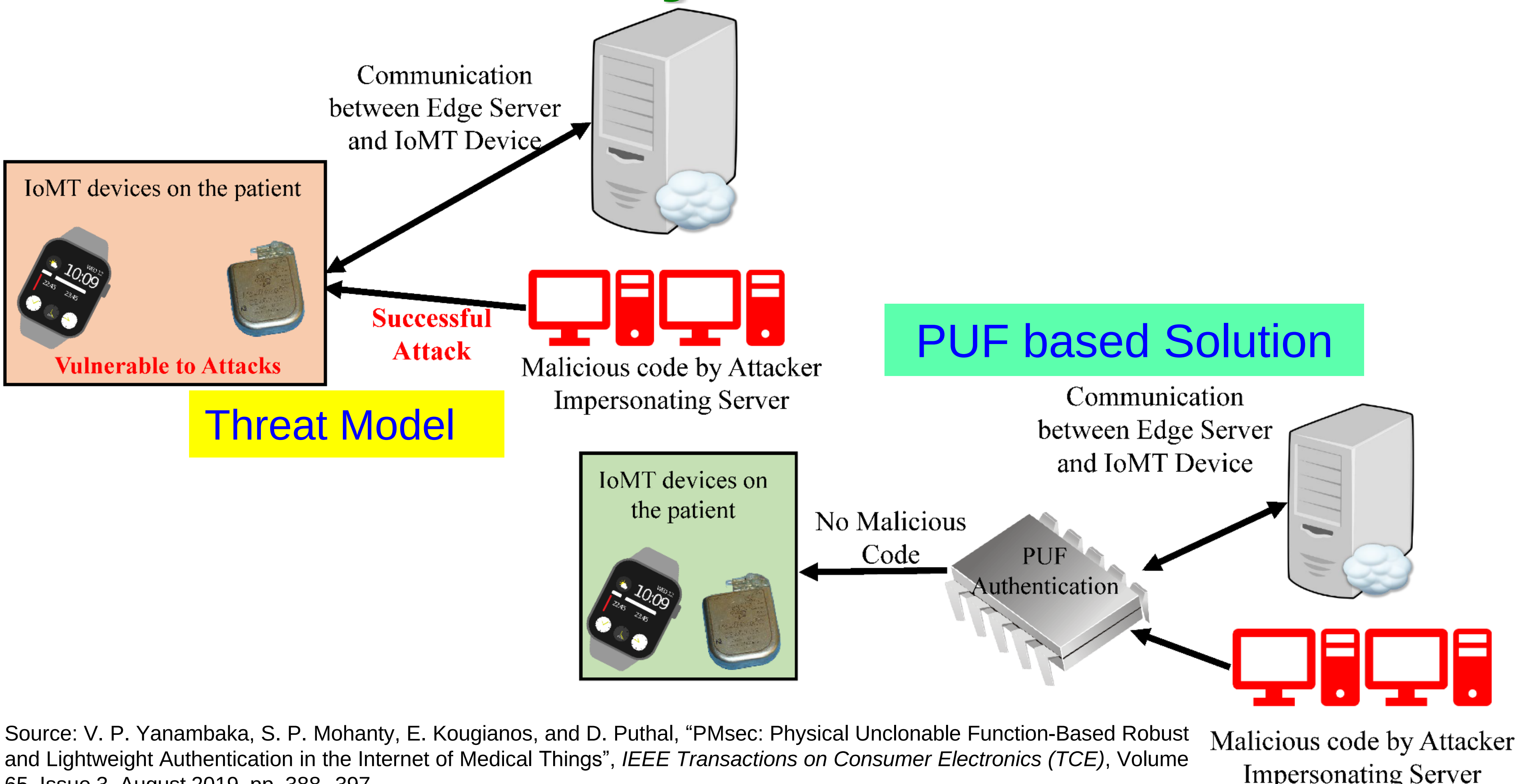


High-Efficiency Video Coding Architecture

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

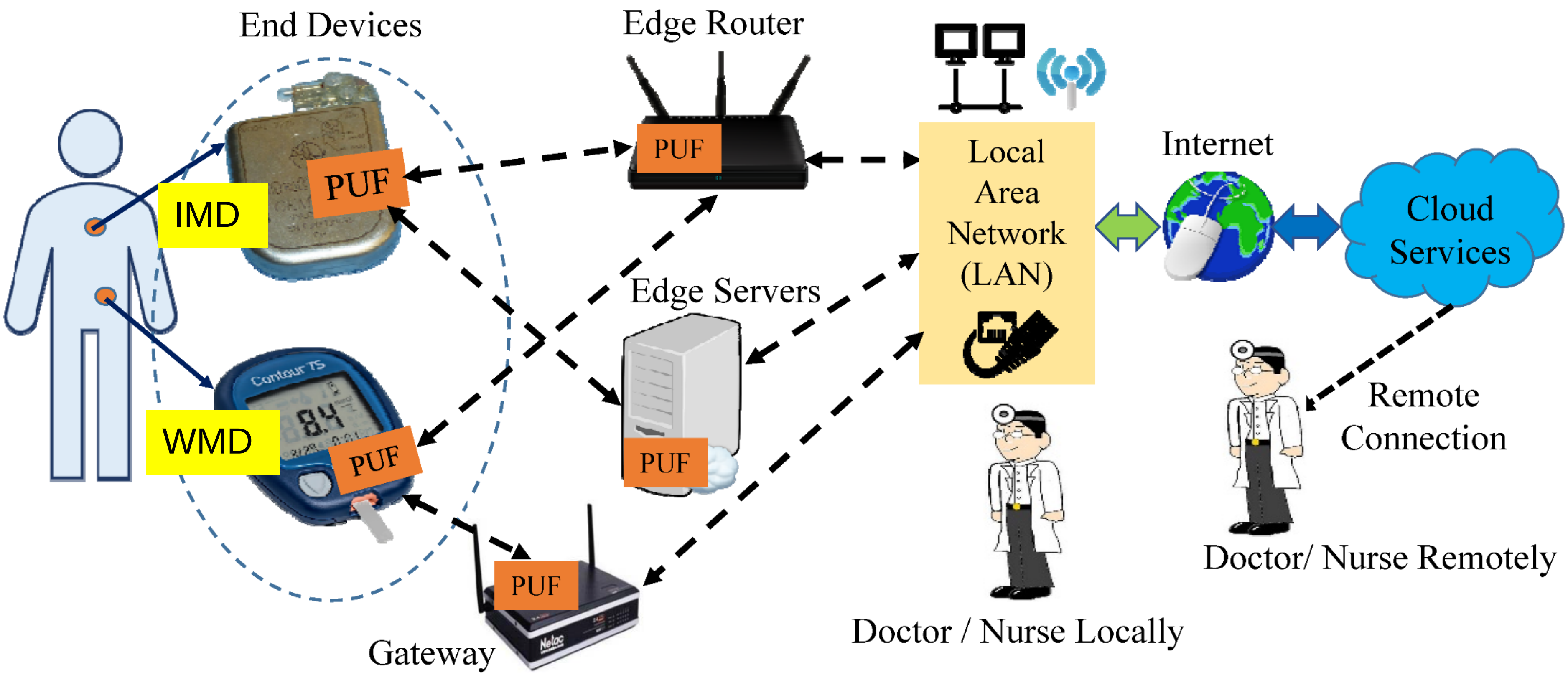
Source: S. P. Mohanty, E. Kougianos, and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT (Invited Paper)", IEEE Access Journal, Volume 6, 2018, pp. 5939--5953.

Our Secure by Design Approach for Robust Security in Healthcare CPS



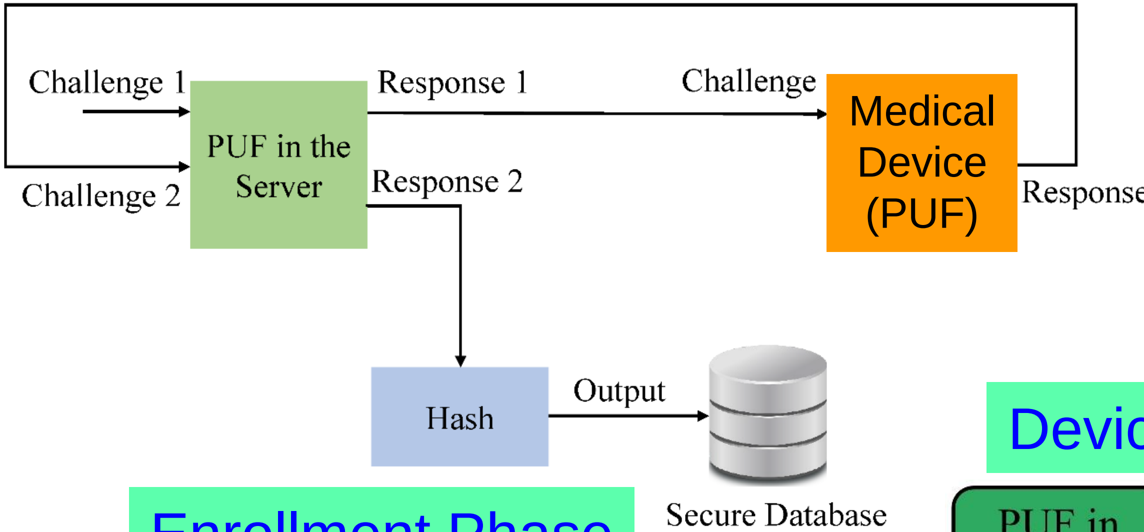
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

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.

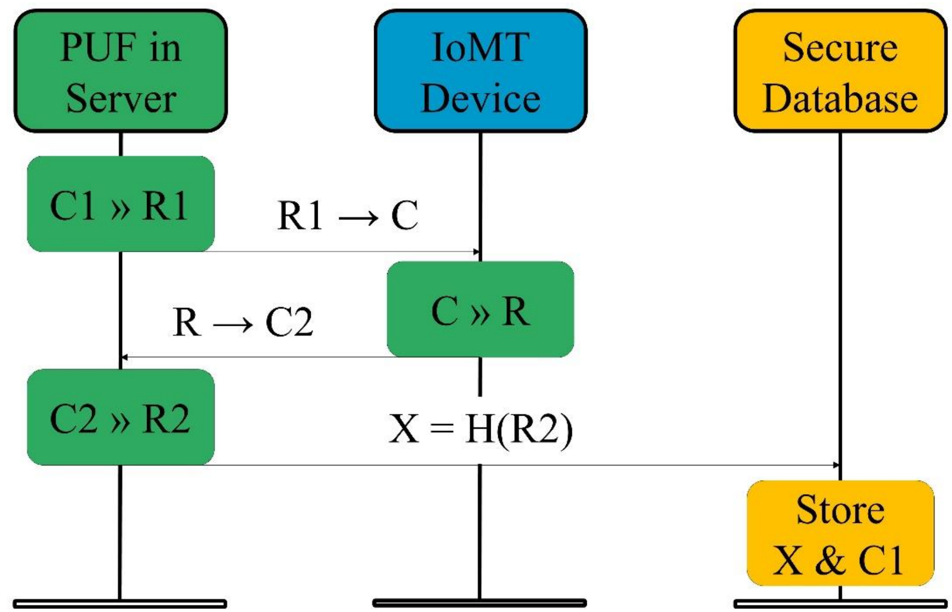
IoMT Security – Our Proposed PMsec



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

Enrollment Phase

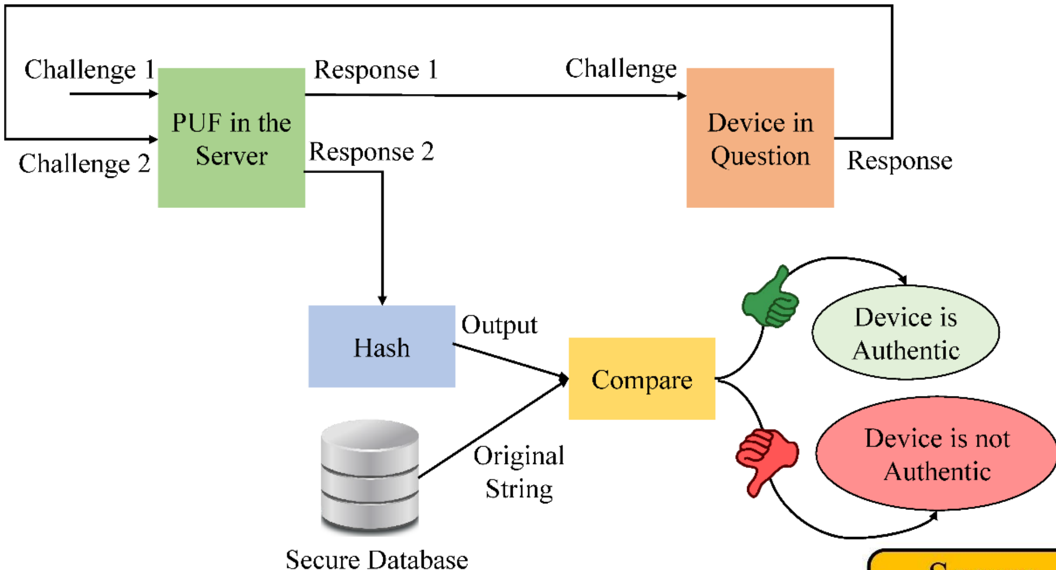
Device Registration Procedure



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

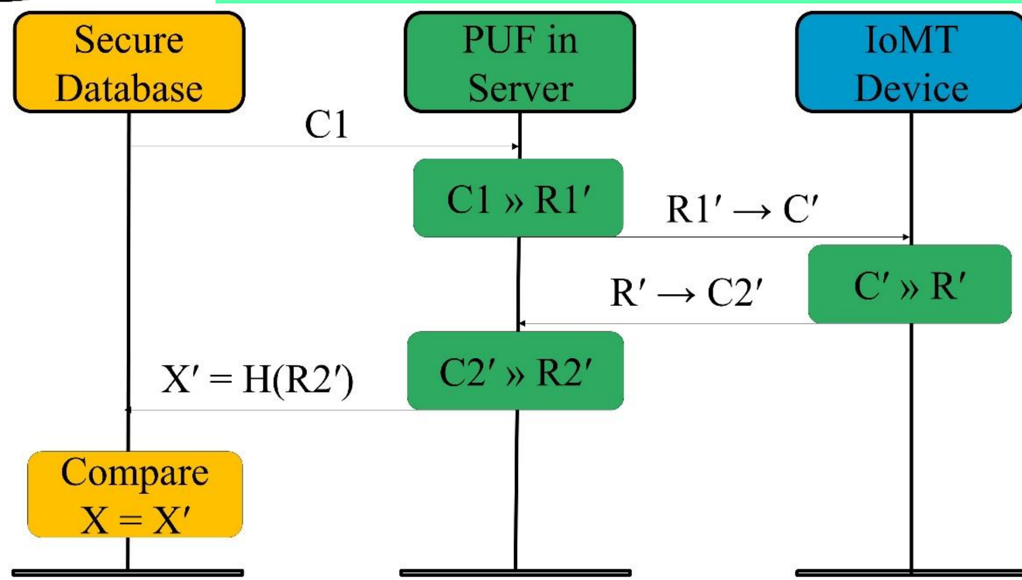
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

IoMT Security – Our Proposed PMsec



Authentication Phase

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

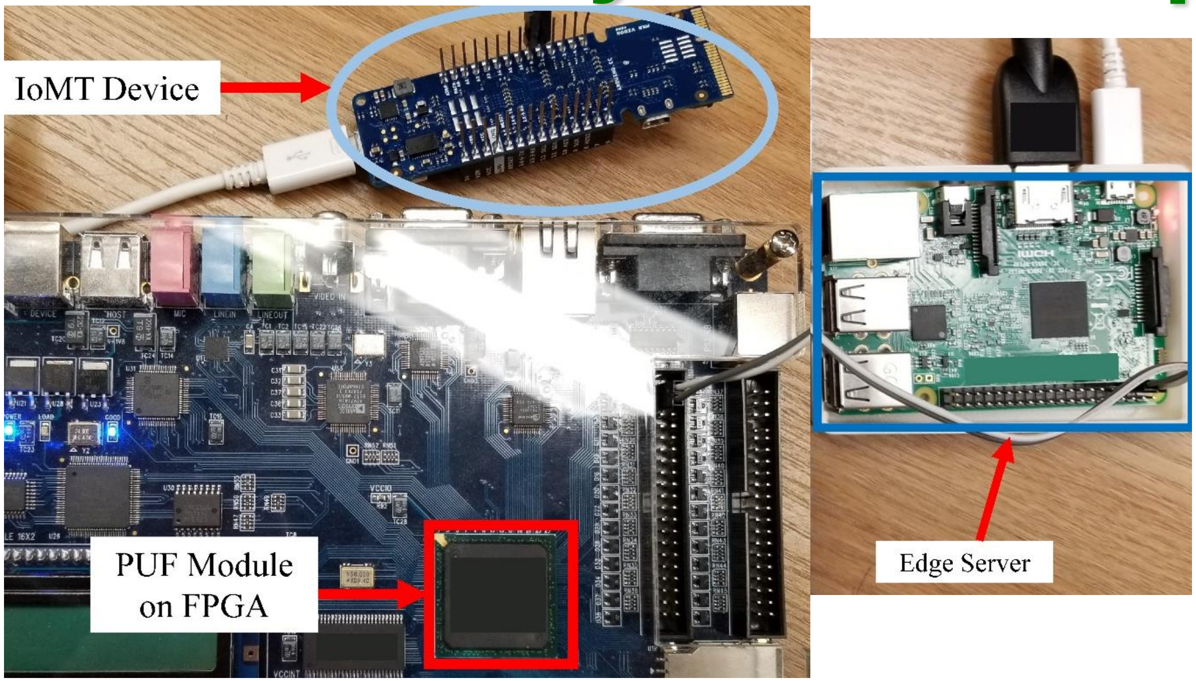
Output from IoMT Device

```
>>>
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

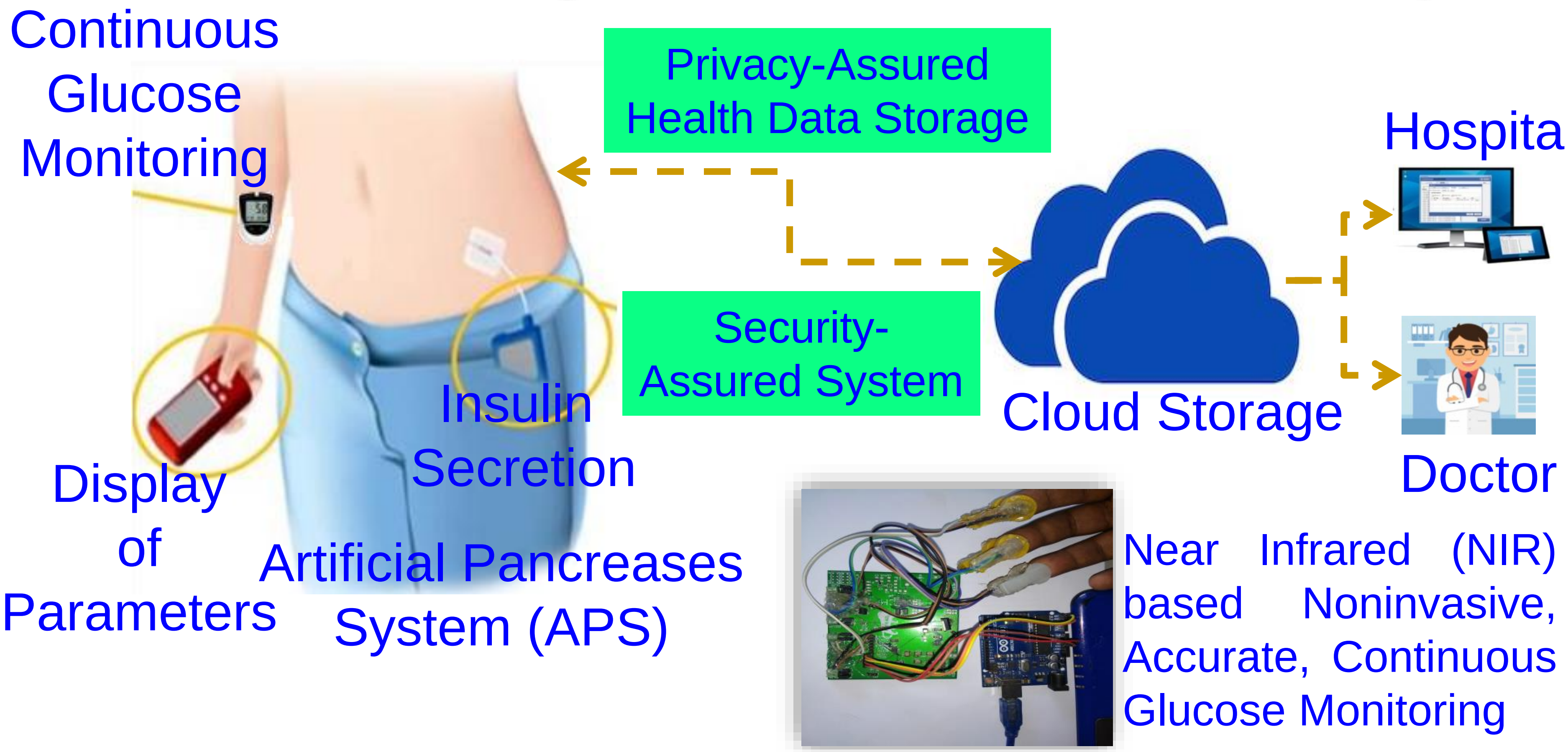


Average Power Overhead – 200 μW

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

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

iGLU: Accurate Glucose Level Monitoring and Insulin Delivery



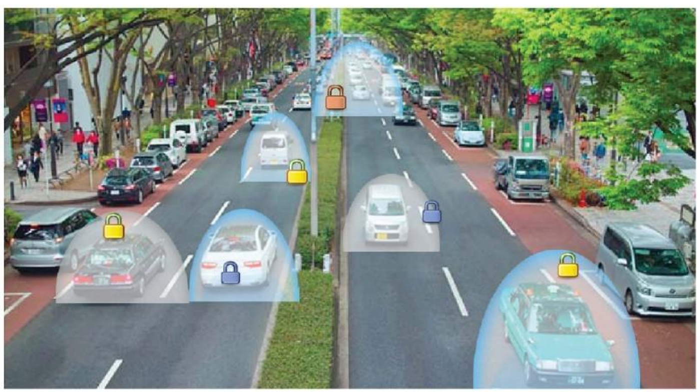
P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare", *IEEE Consumer Electronics Magazine (MCE),* Vol. 9, No. 1, January 2020, pp. 35–42.

Vehicular Security

IEEE Consumer Electronics Magazine

Volume 8 Number 6

NOVEMBER/DECEMBER 2019

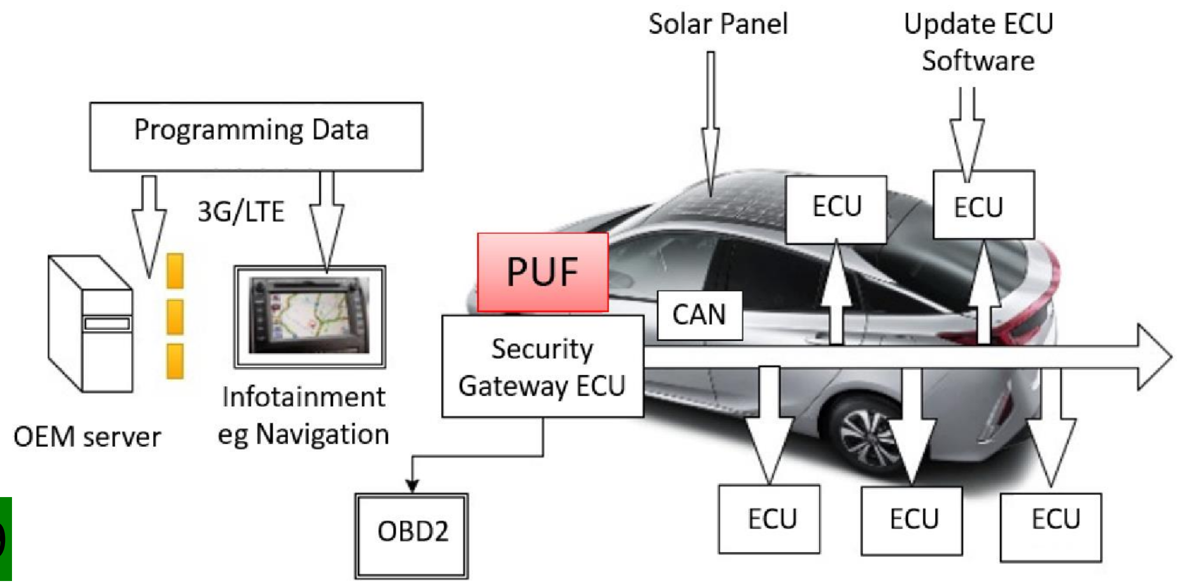


Vehicular Security

November 2019

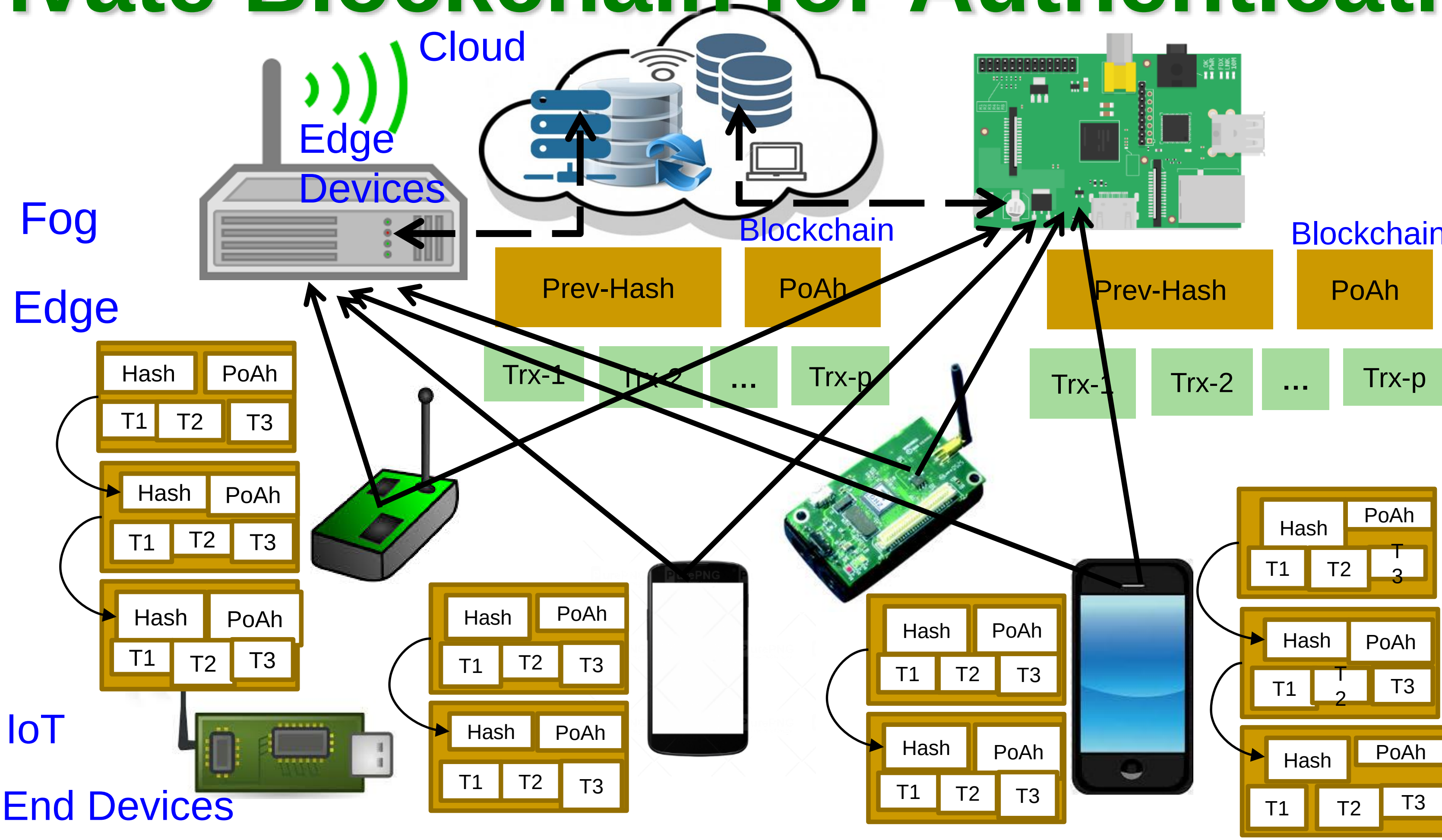
IEEE

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.

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

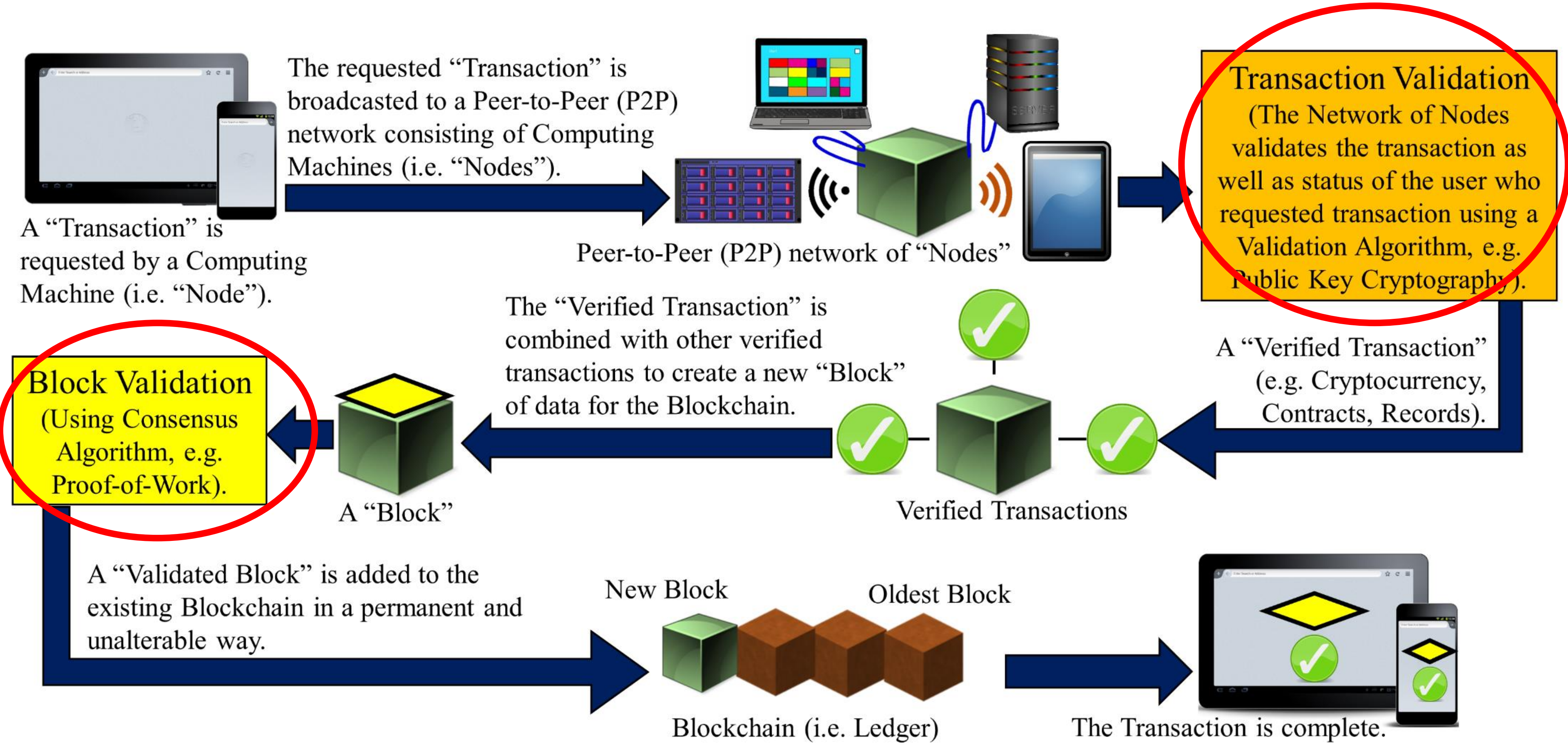


Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Volume 38, Issue 1, January 2019, pp. 26--29.

Blockchain Consensus Types

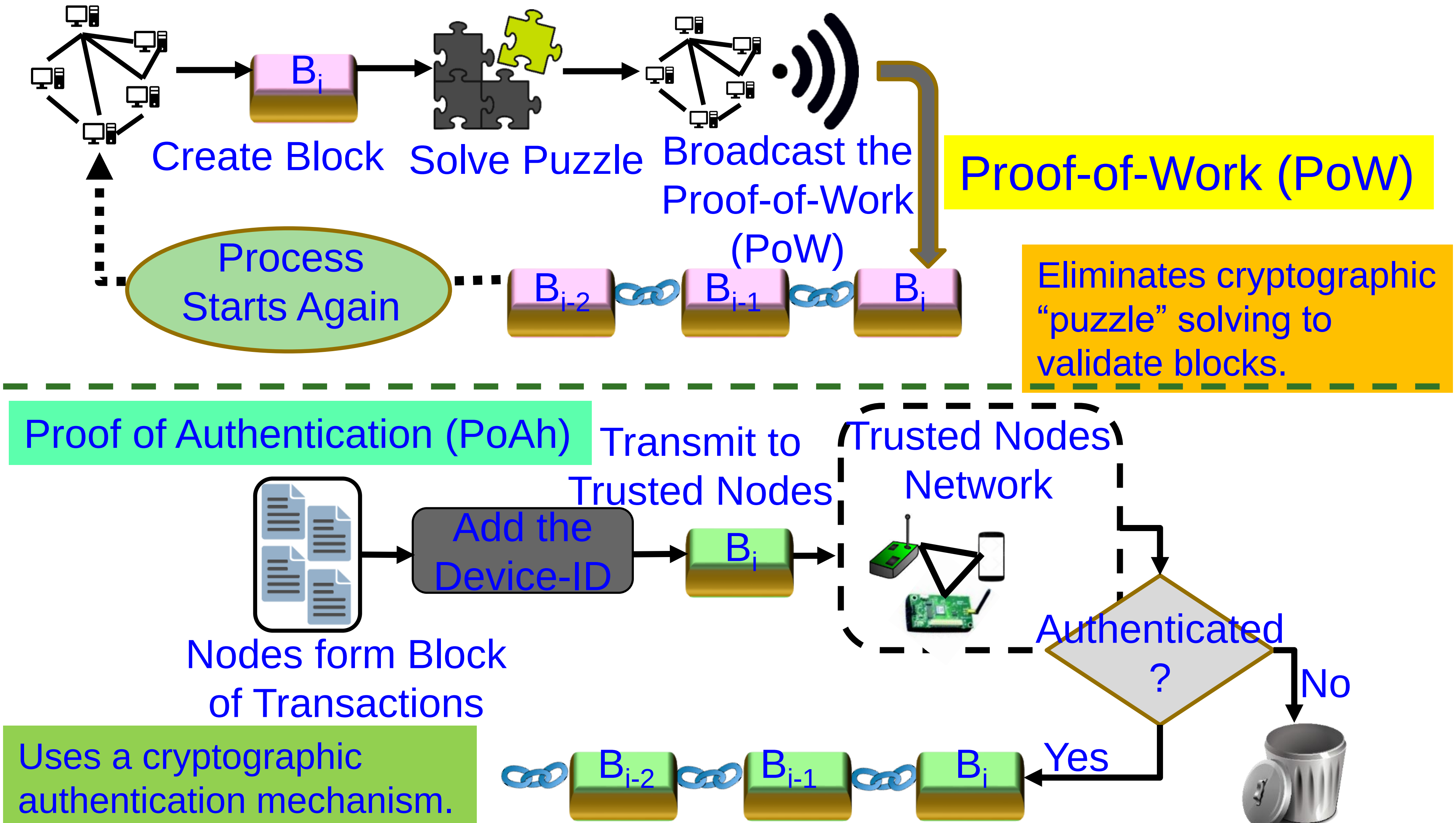
- Blockchain Consensus Algorithm
  - Validation Based
    - Proof of Work (PoW)
    - Proof of Stack (PoS)
    - Proof of Activity (PoA)
    - Proof of Relevance (PoR)
    - Proof of Elapsed Time
  - Voting Based
    - Ripple
    - Proof of Vote
    - Proof of Trust
  - Authentication Based
    - Proof 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

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 PoAh (B_i)

- Hash of Previous Block
- Unique Block Token (UBT)
- Transactions Tx1, Tx2, …, TxN

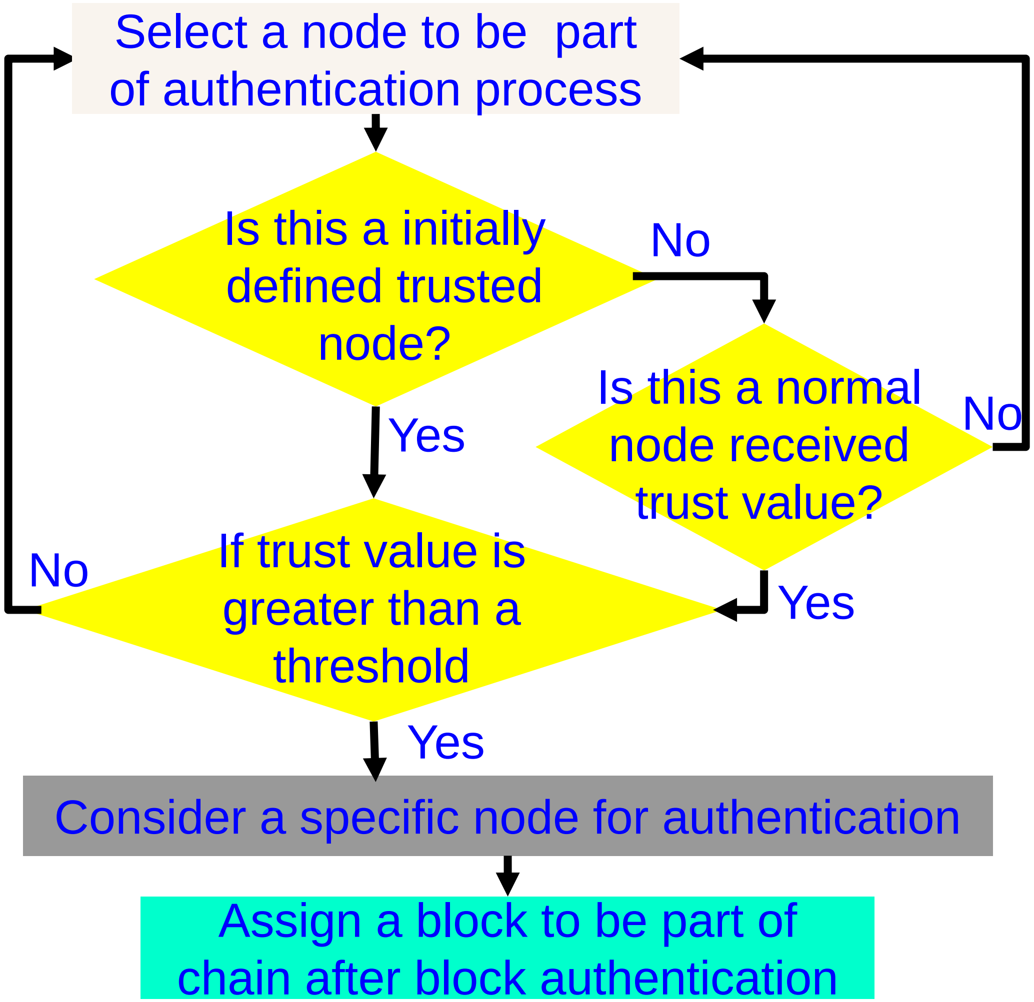
Hash of the following:

- Hash of B_{i-2}
- UBT of B_{i-1}
- Device ID
- Transactions of B_{i-1}

PoAh 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

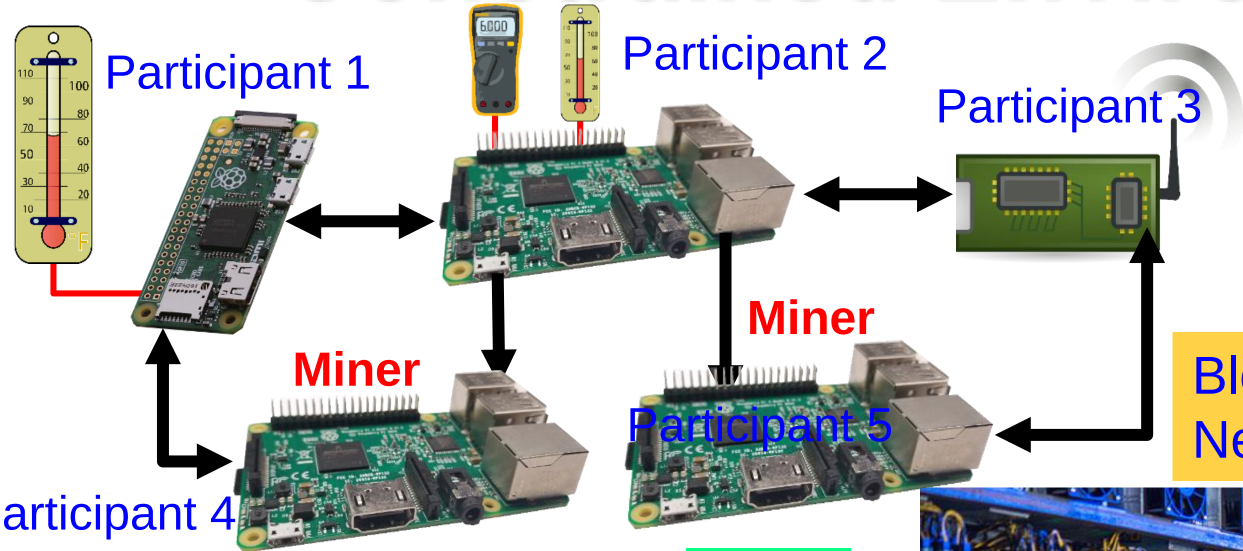


Steps to find a Trusted Node which will Authenticate a Block.

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



Our PoAh-Chain Runs here

5 W

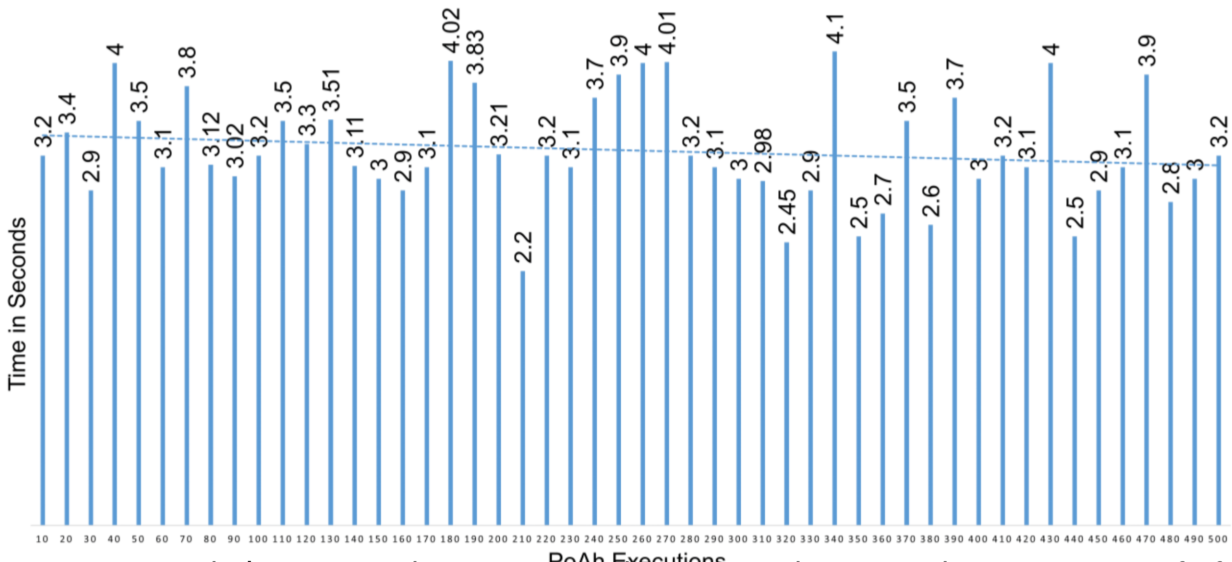
Blockchain using PoW Needs Significant Resource

Source: https://www.iea.org/newsroom/news/2019/july/bitcoin-energy-use-mined-the-gap.html

500,0000 W

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

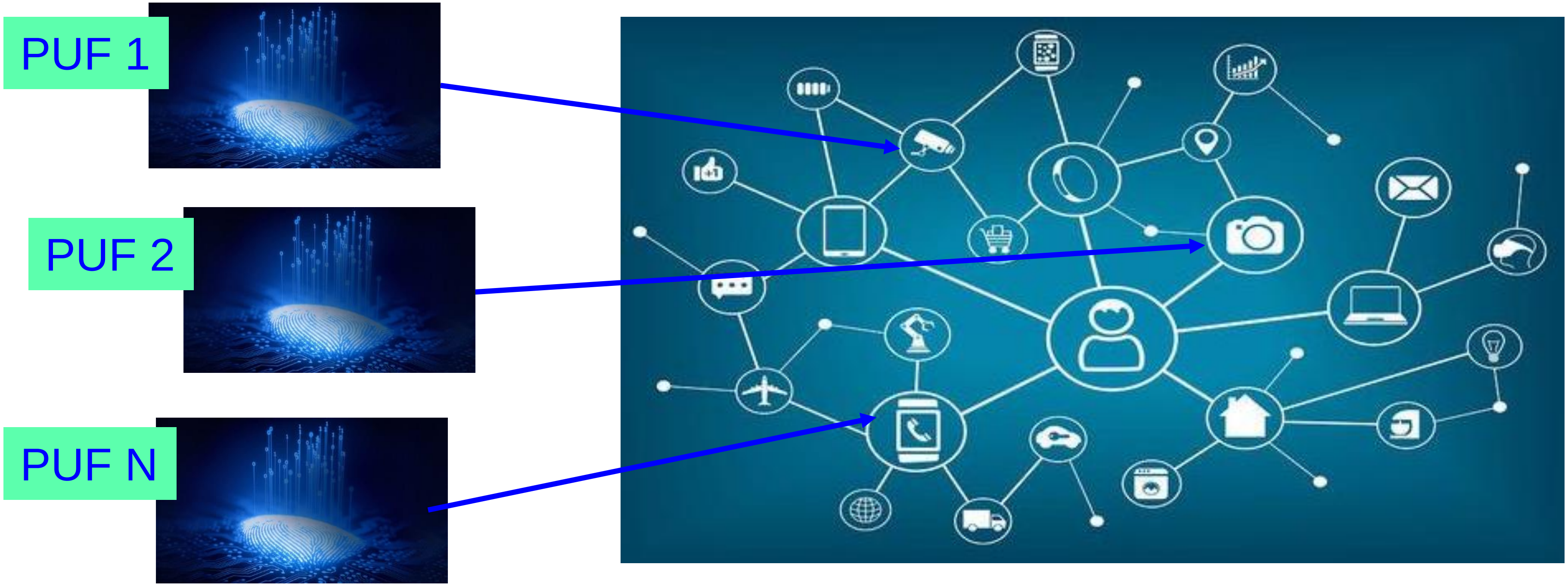
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, Dos	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



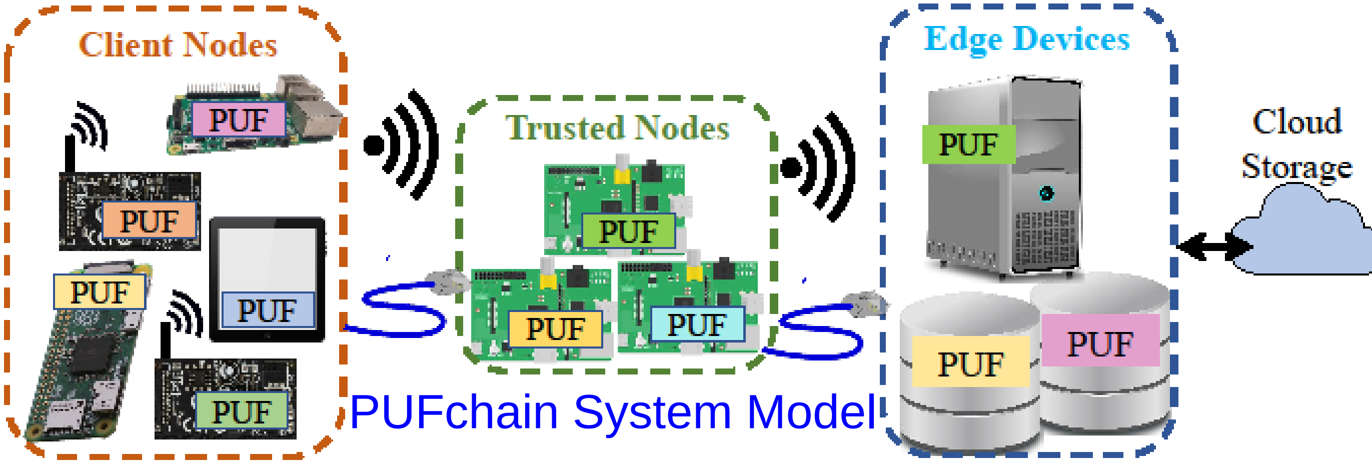
PoAh Execution for 100s of Nodes

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



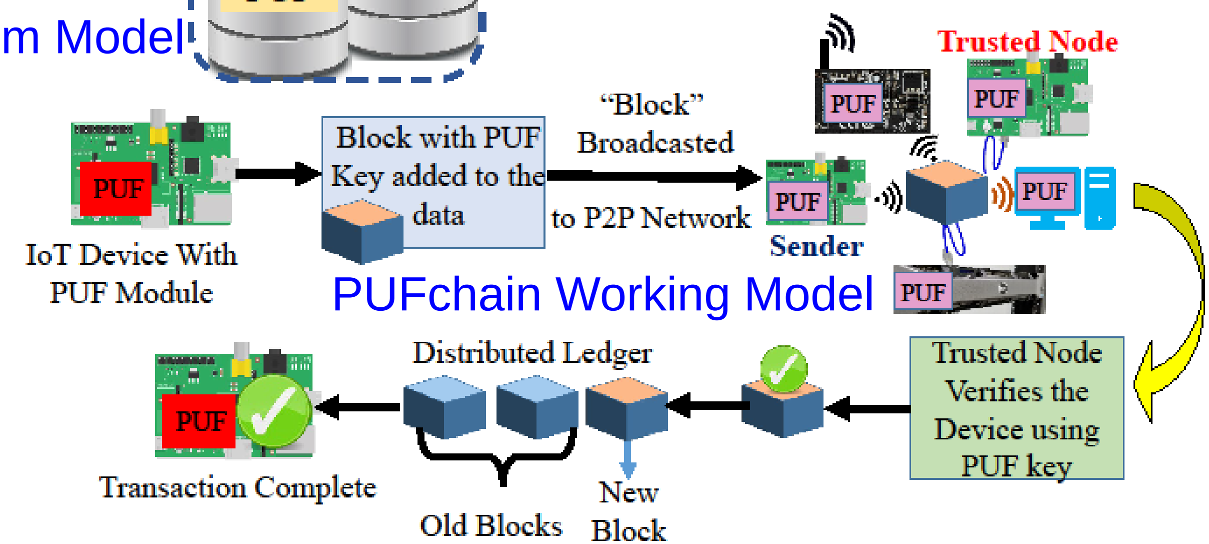
PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

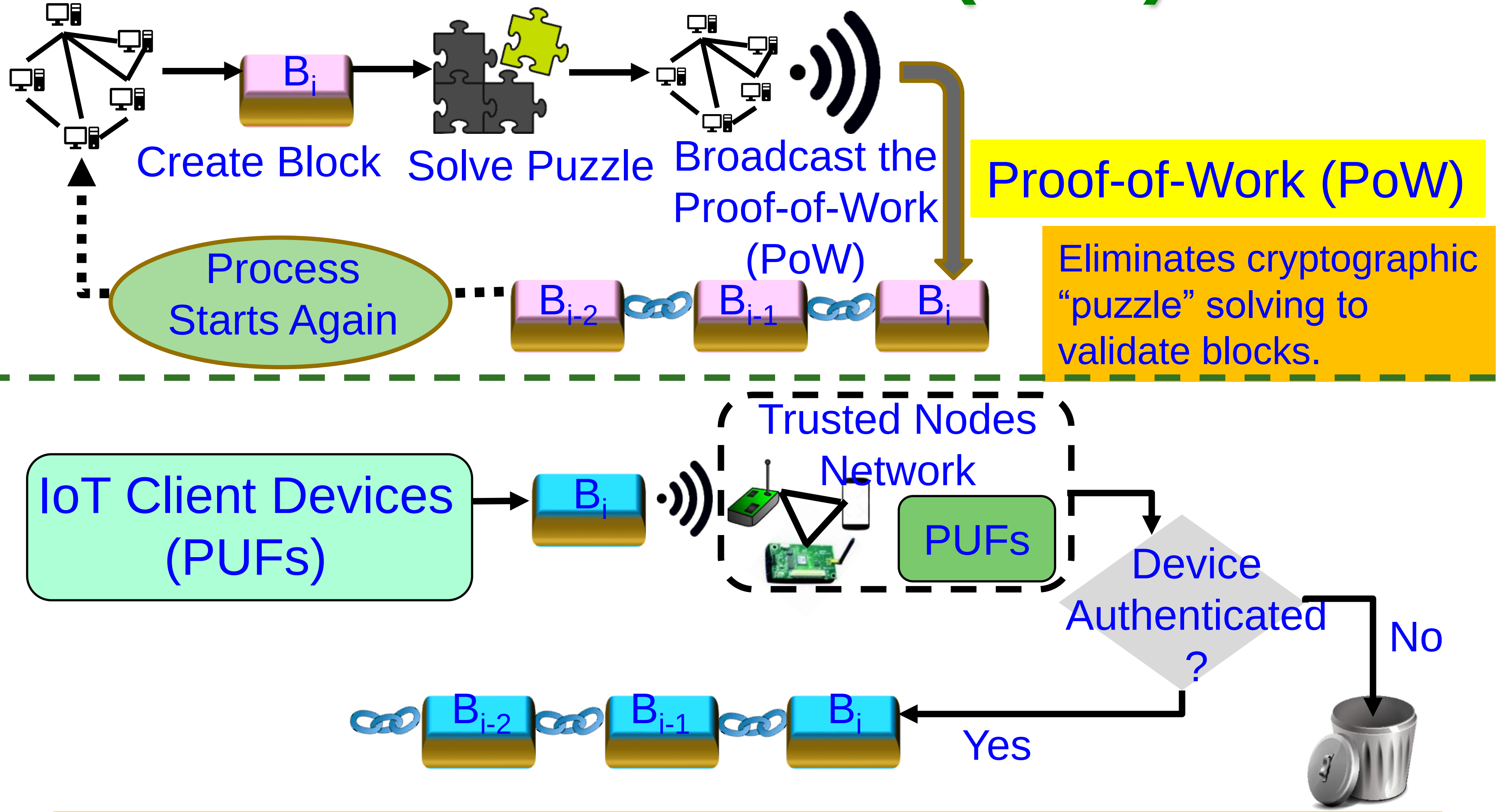
PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode



PUFchain Working Model

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)



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)

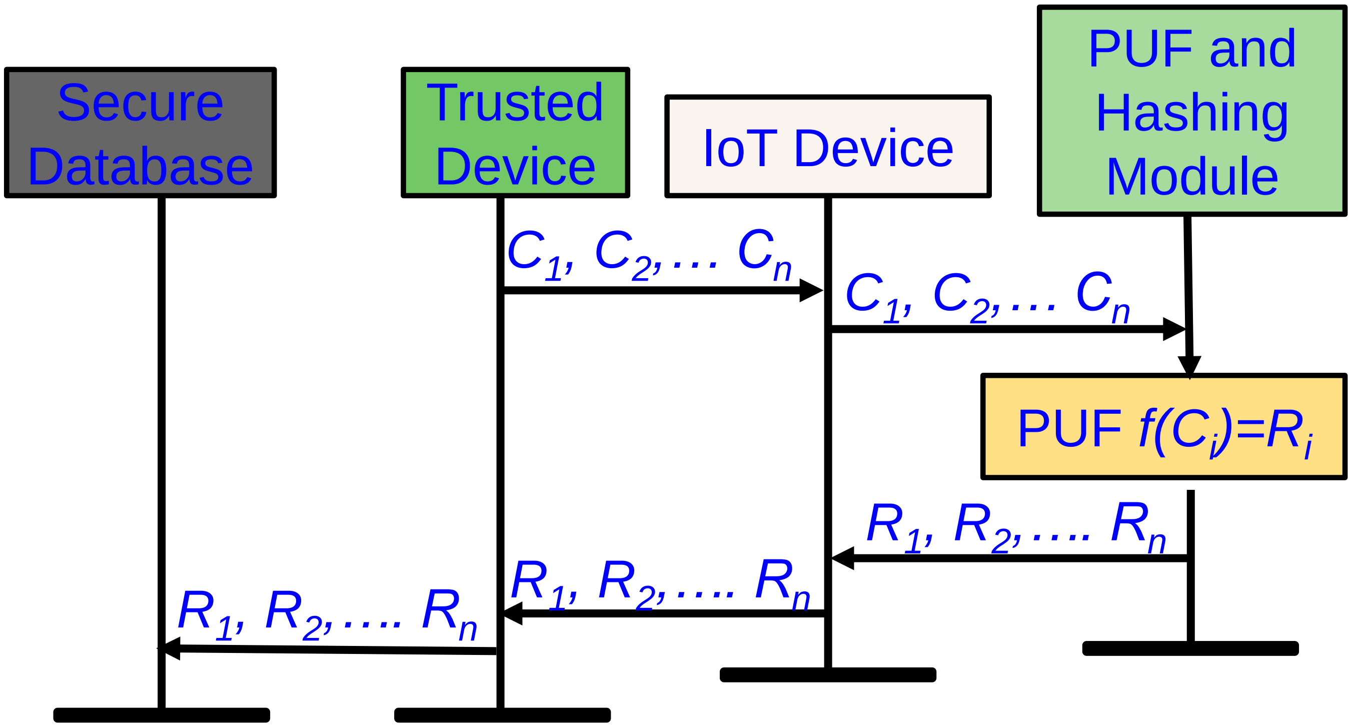
Transactions Tx1, Tx2, …, TxN

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

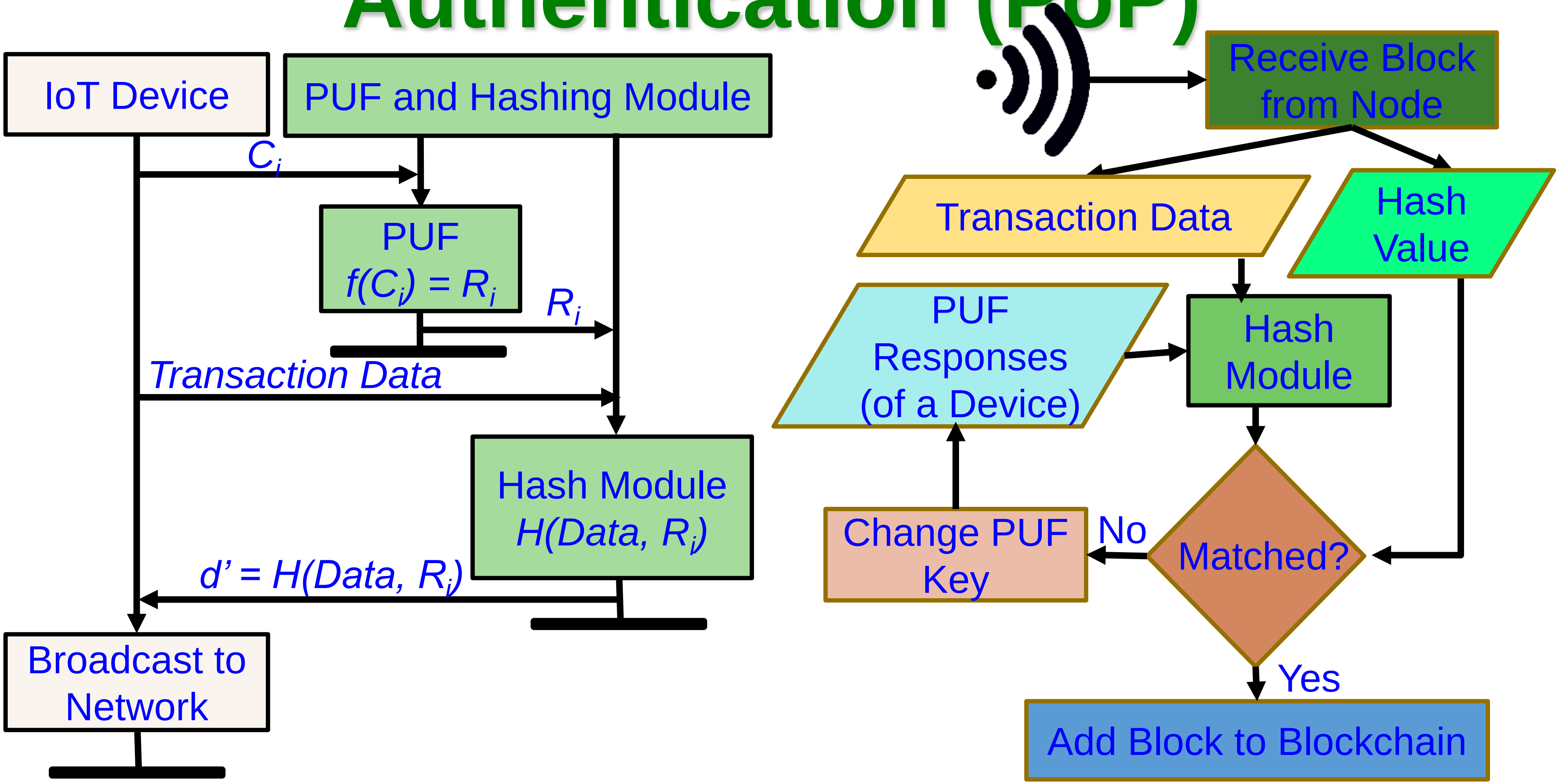
PUFchain: Device Enrollment Steps



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.

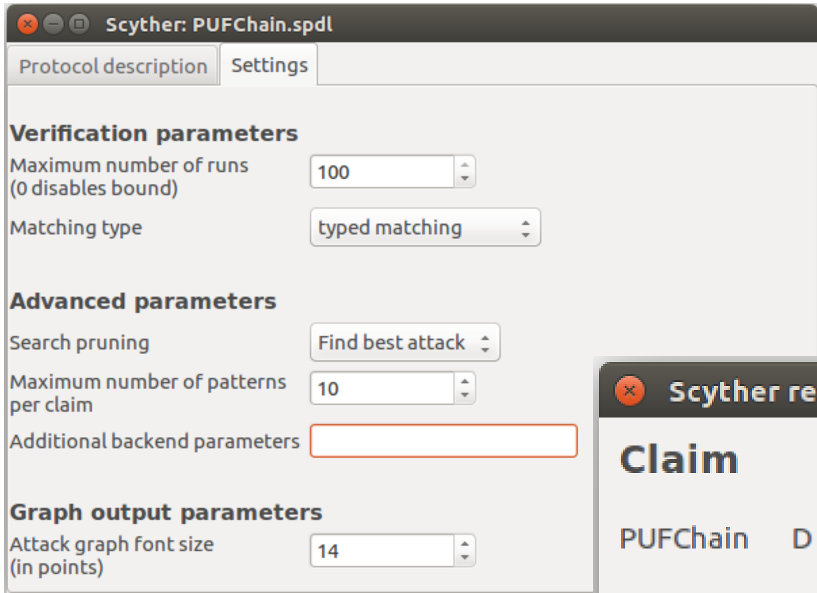
Steps of Proof-of-PUF-Enabled-Authentication (PoP)



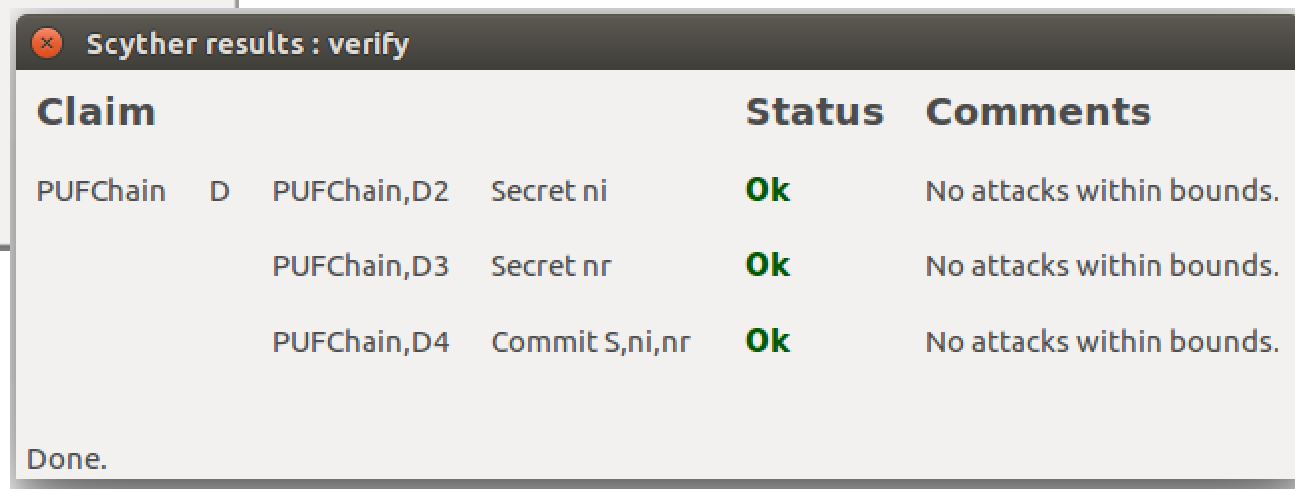
Steps for Transactions Initiation

Steps for Device Authentication

PUFchain Security Validation

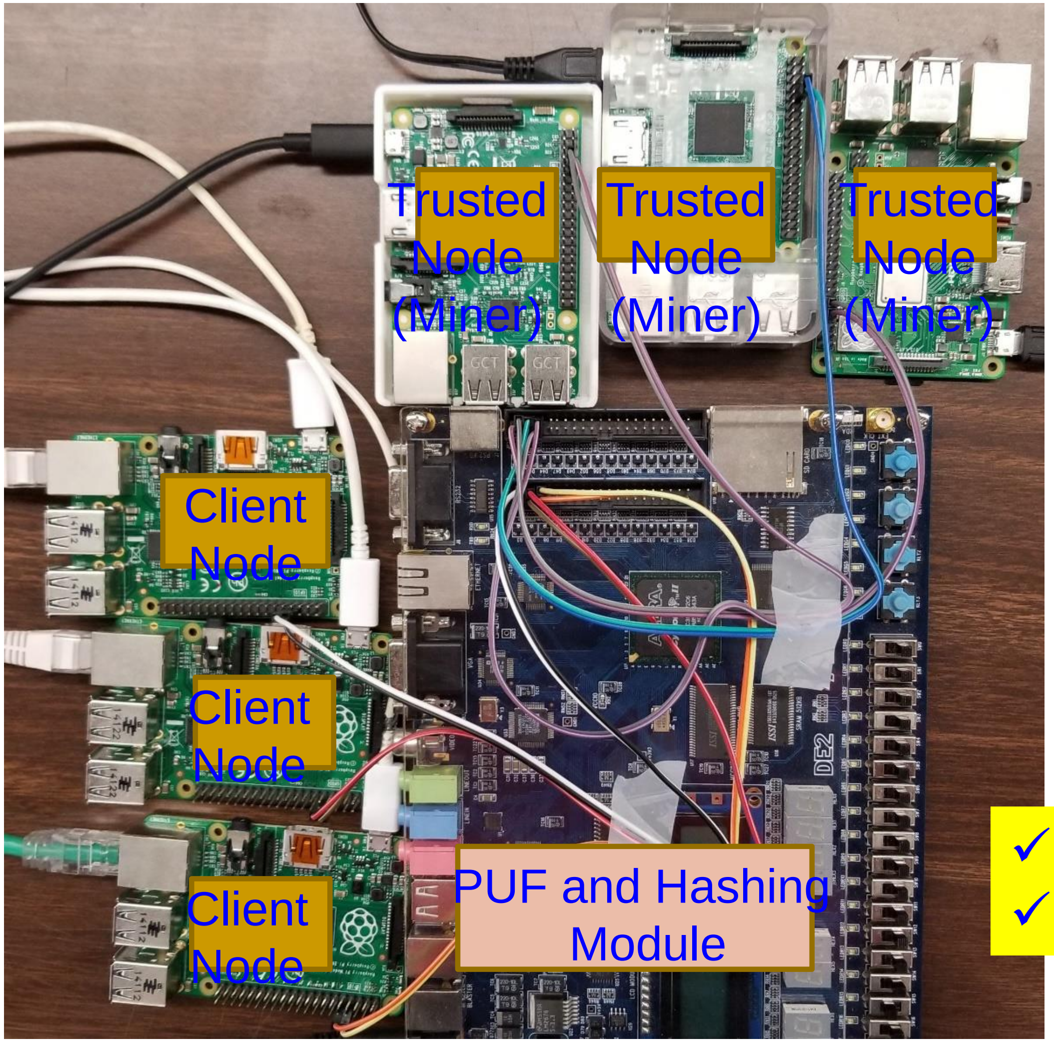


S - the source of the block
D - the miner or authenticator node in the networks



PUFchain Security Verification in Scyther simulation environment proves that PUFChain is secure against potential network threats.

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.

Smart Grid Security - Solutions

Smart Grid – Security Solutions

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

Smart Meter

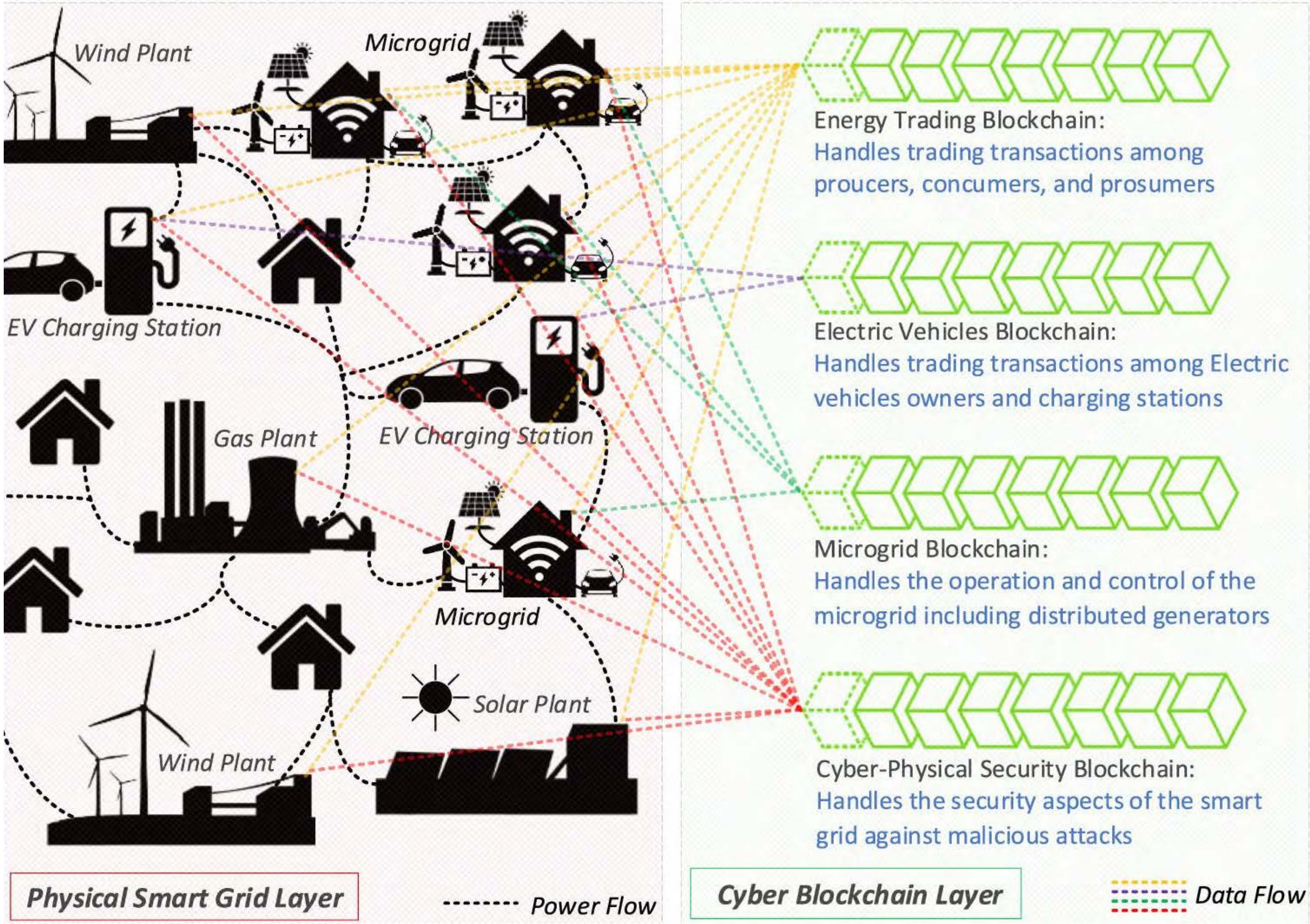

Phasor Measurement Unit (PMU)

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

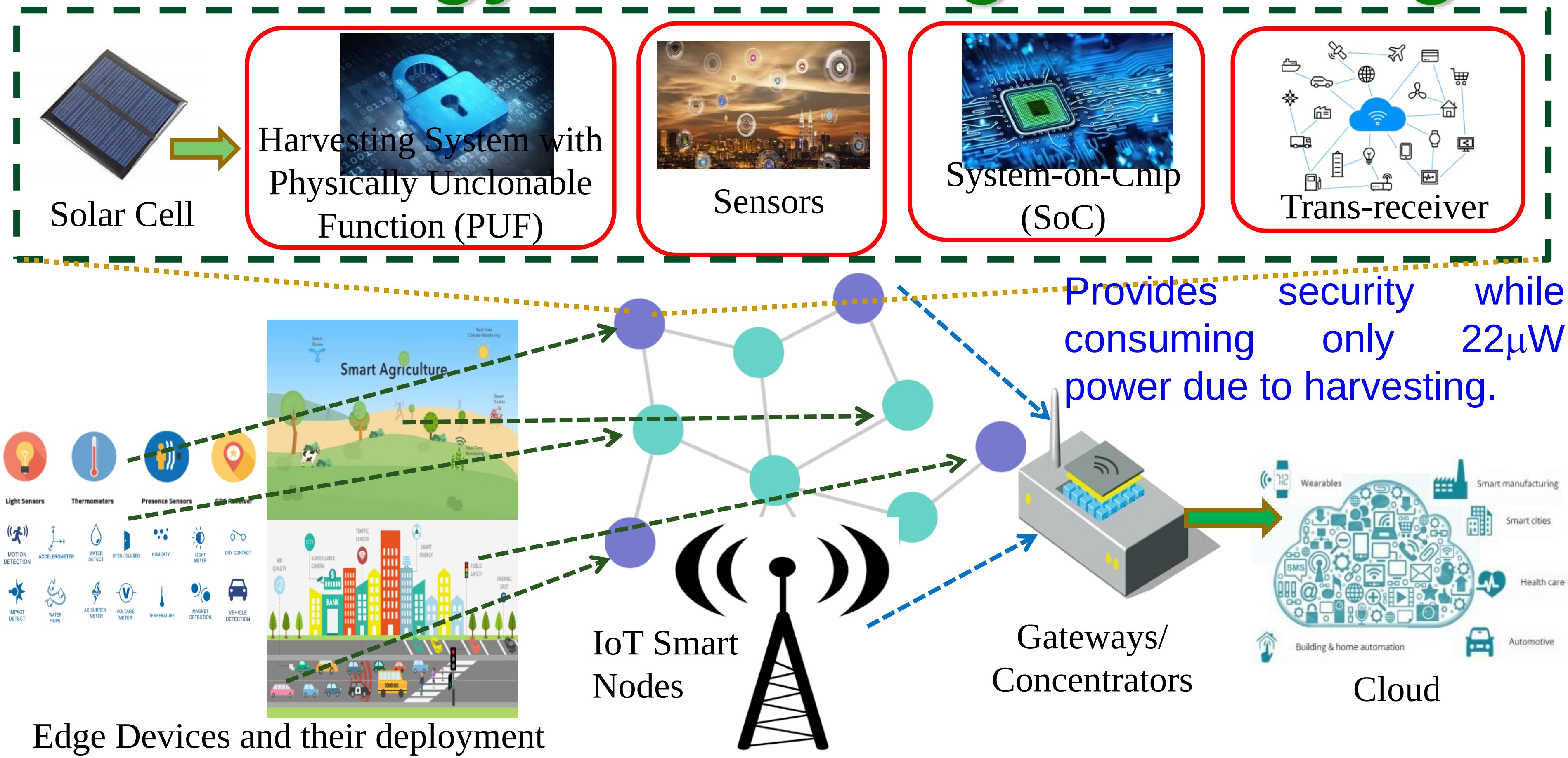
Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids“, *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

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.

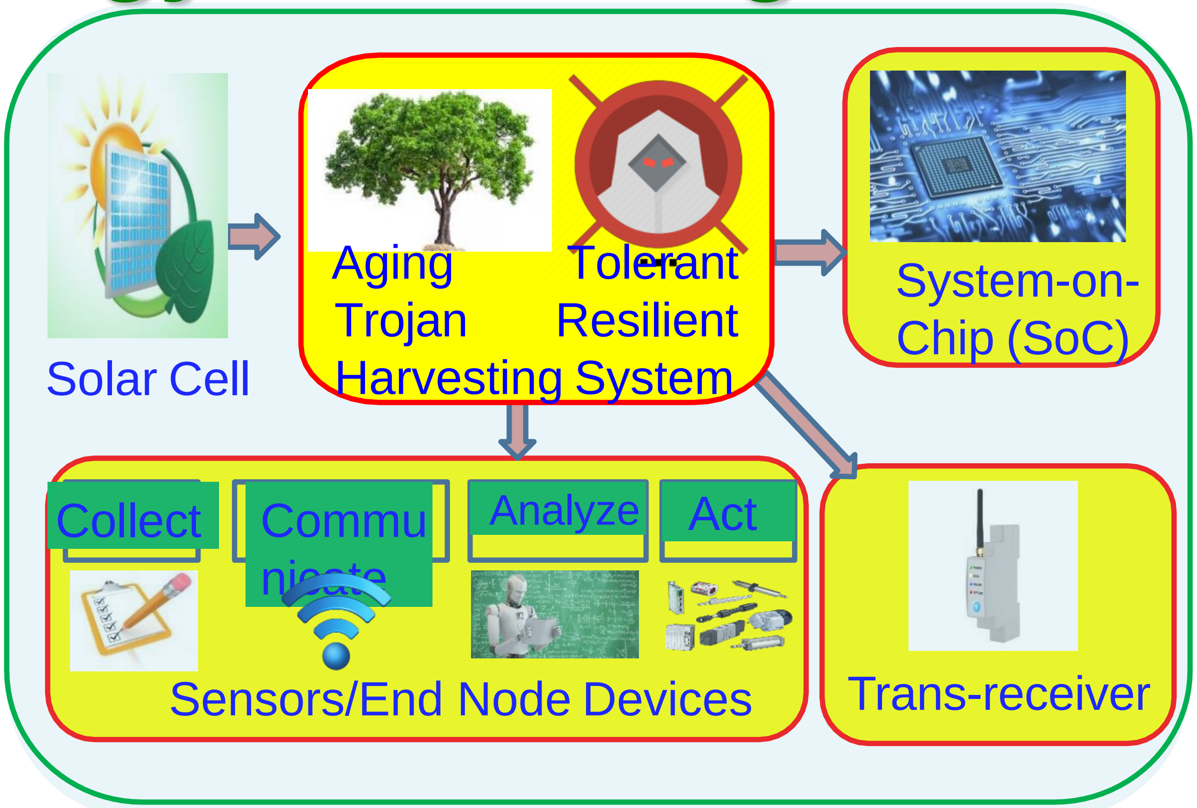
Eternal-Thing: Combines Security and Energy Harvesting at the Edge



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

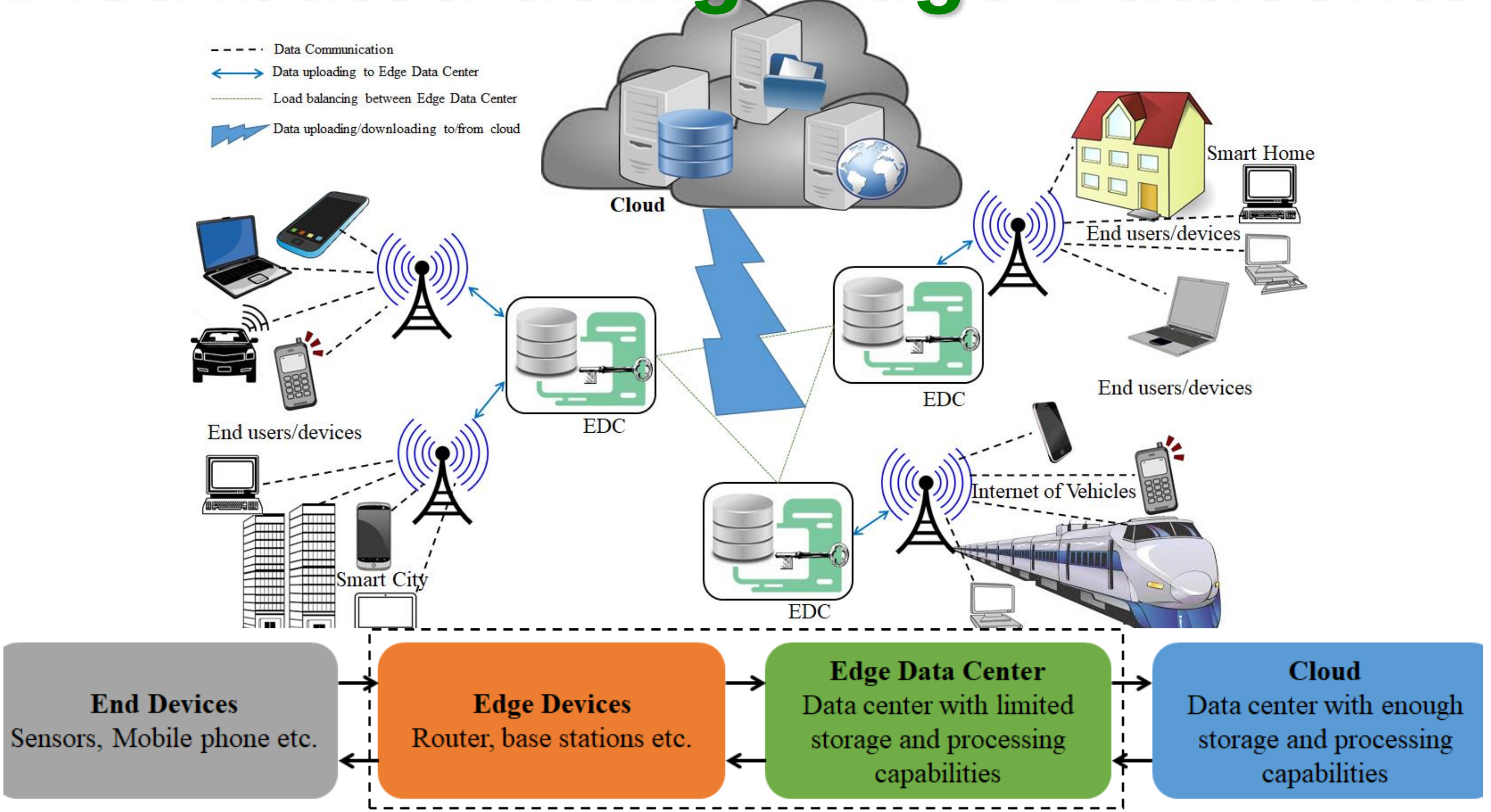
Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, “Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT”, *IEEE Transactions on Sustainable Computing*, Vol. XX, No. YY, ZZ 2019, pp. Under Review.

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



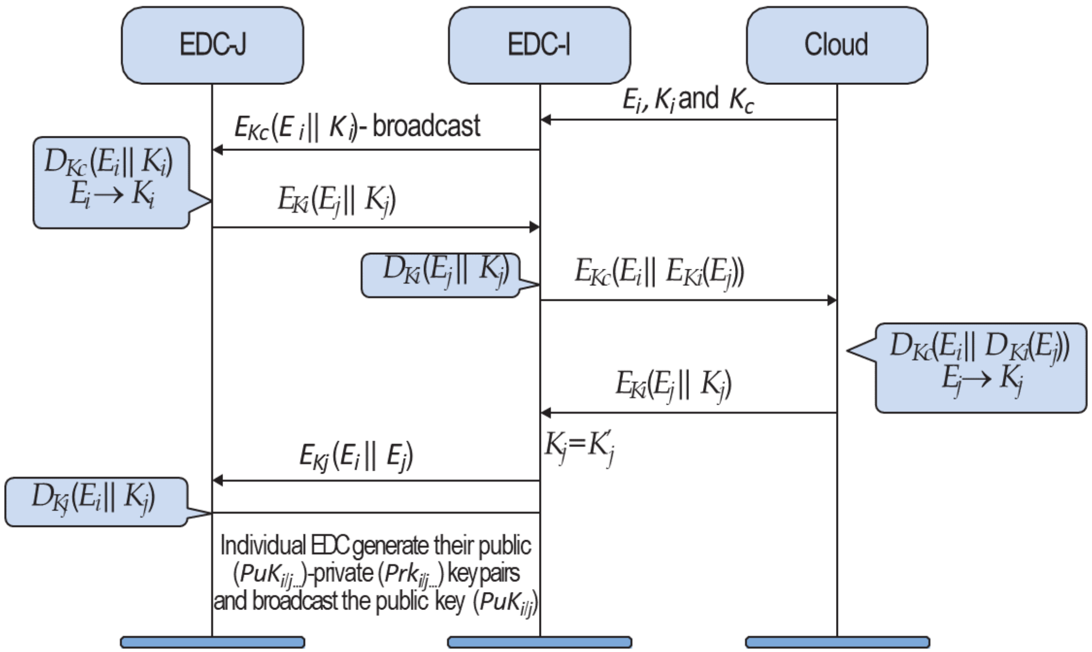
Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, "Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT", *ACM Journal on Emerging Technology in Computing*, Vol. XX, No. YY, ZZ 2019, pp. Under Review.

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

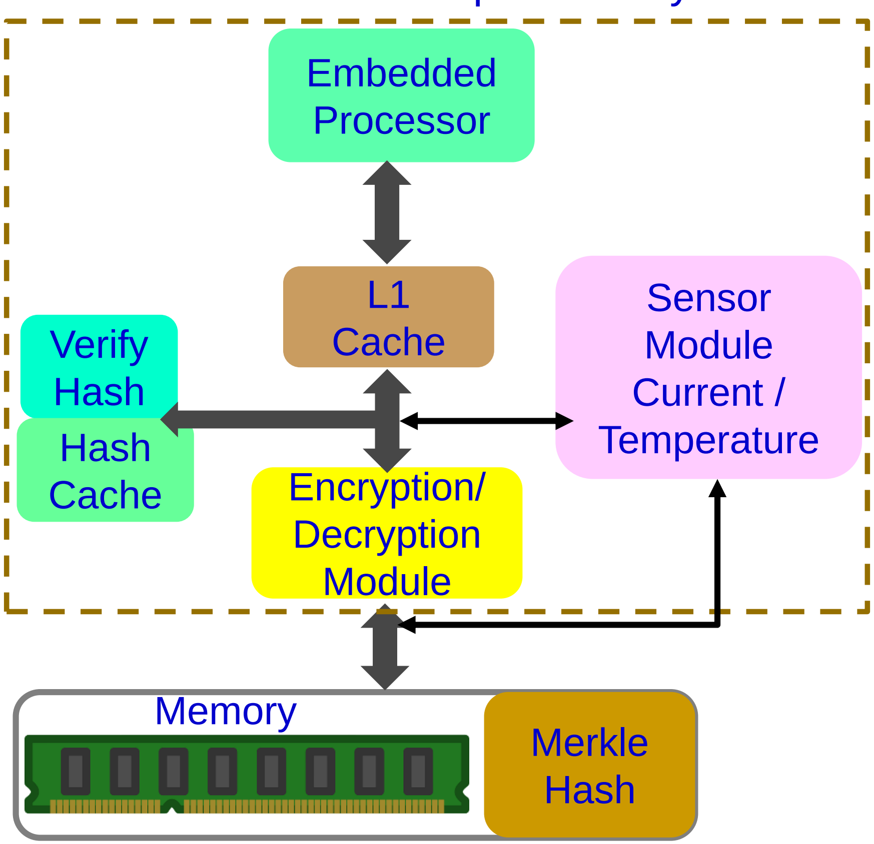
1. If (EDC-I is overloaded)
2. EDC-I broadcast (E_i, L_i)
3. EDC-J (neighbor EDC) verifies:
4. If (E_i is in database) & ($p \leq 0.6$ & $L_i << (n-m)$)
5. Response $E_{Kpu_i}(E_j || K_j || p)$
6. EDC-I perform $D_{Kpr_i}(E_j || K_j || p)$
7. $k_j' \leftarrow E_j$
8. If ($k_j' = k_j$)
9. EDC-I select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

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

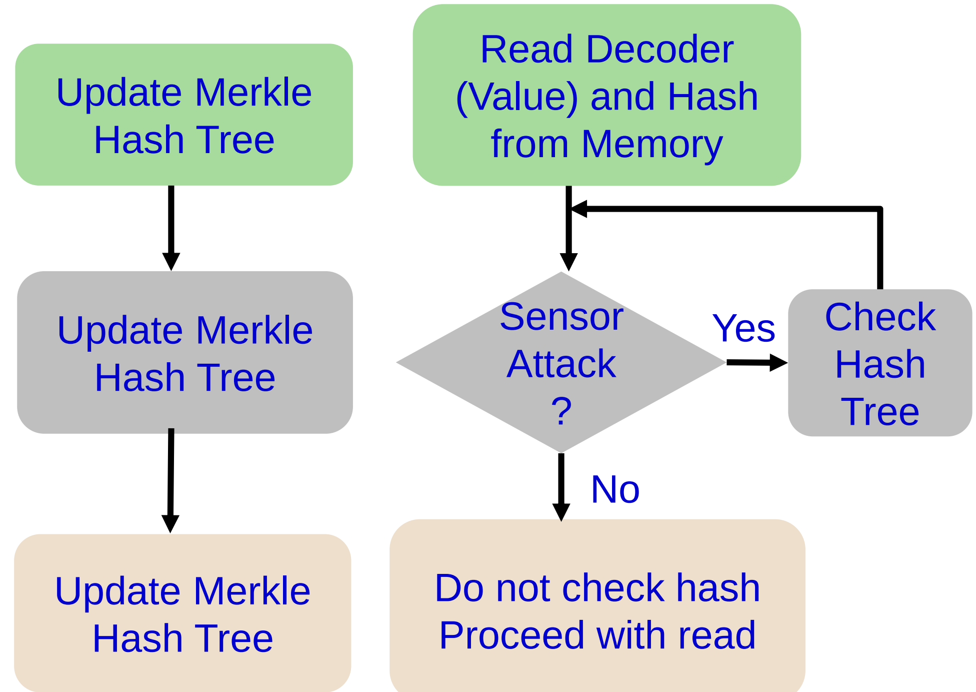
Response time of the destination EDC has reduced by 20-30% using the proposed allocation approach.

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.

Embedded Memory Security



On-Chip/On-Board Memory Protection

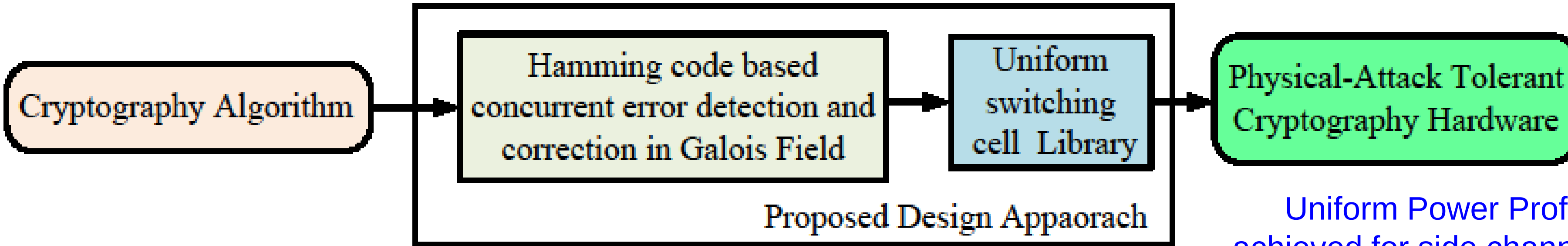


Write Operation Read Operation

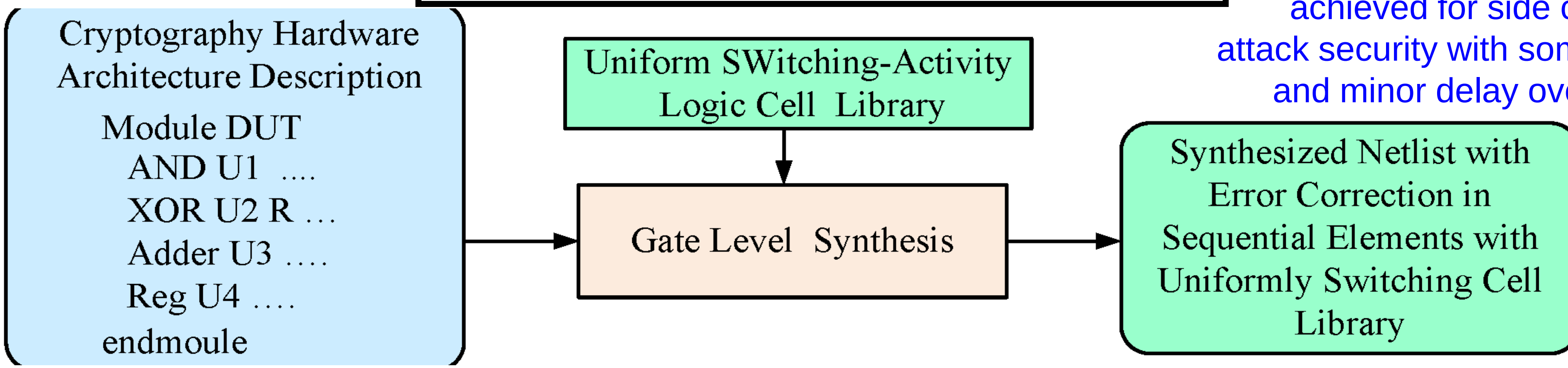
Memory integrity verification with 85% energy savings with minimal performance overhead.

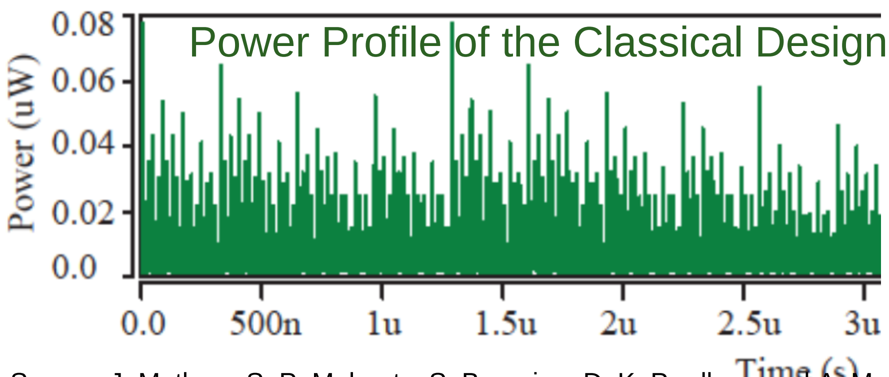
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", Springer Circuits, Systems, and Signal Processing Journal (CSSP), Volume 32, Issue 6, December 2013, pp. 2581--2604.

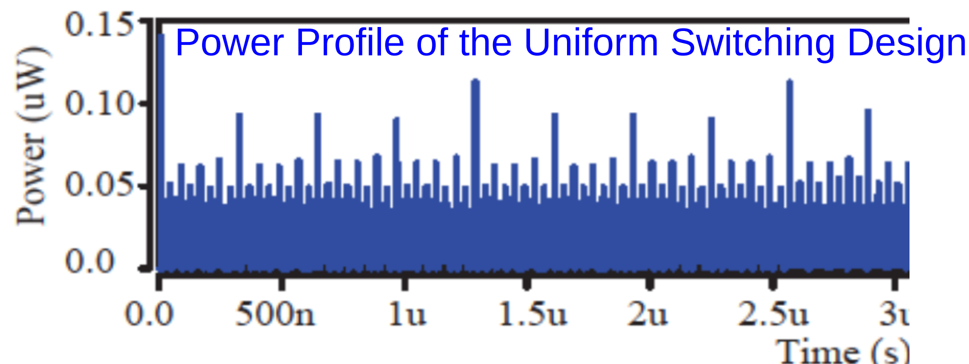
DPA Resilience Hardware Design



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

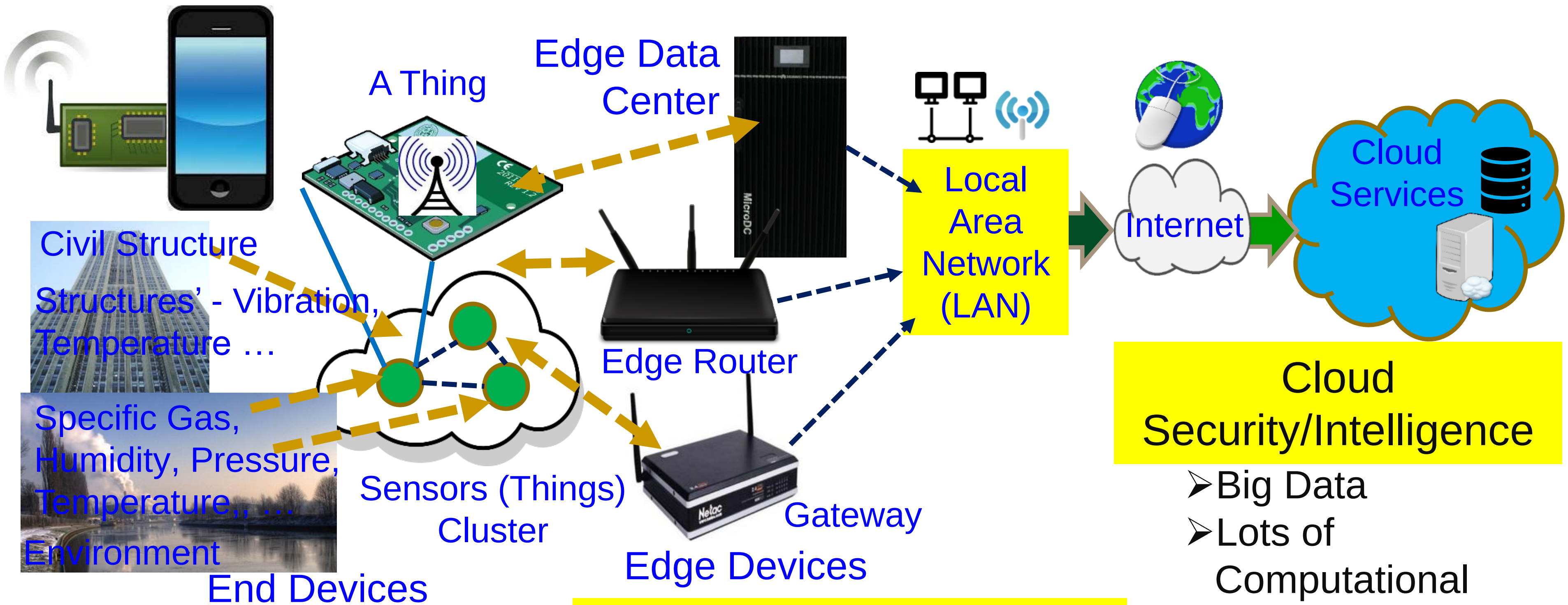






Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", *Elsevier Computers and Electrical Engineering*, Vol. 39, No. 4, May 2013, pp. 1077--1087.

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

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

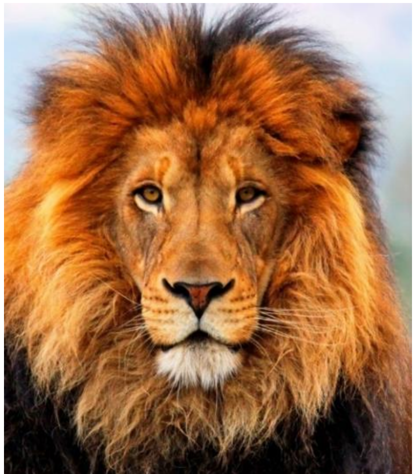
Systems & Analytics
- Clinical Decision Support Systems (CDSSs)
- Electronic Health Records (EHRs)

Machine Learning Engine

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

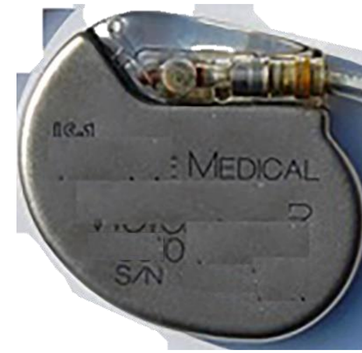
Source: Hongxu Yin, Ayten Ozge Akmandor, Arsalan Mosenia and Niraj K. Jha (2018), "Smart Healthcare", *Foundations and Trends® in Electronic Design Automation*, Vol. 12: No. 4, pp 401-466. http://dx.doi.org/10.1561/1000000054

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



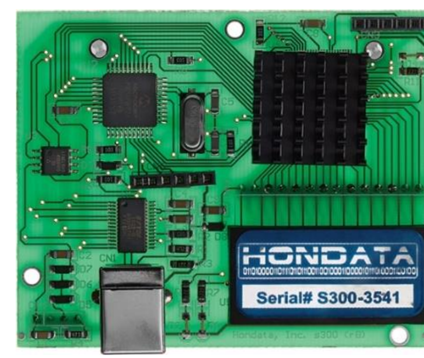
AI can be fooled by fake data

AI can create fake data (Deepfake)



Authentic Fake

An implantable medical device

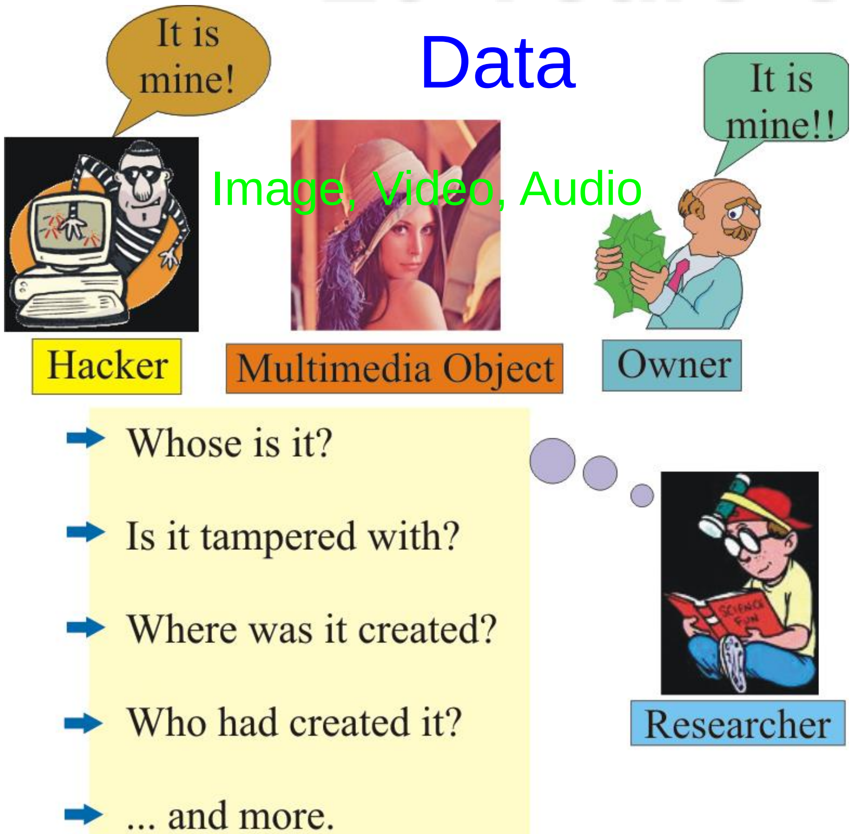


Authentic Fake

A plug-in for car-engine computers

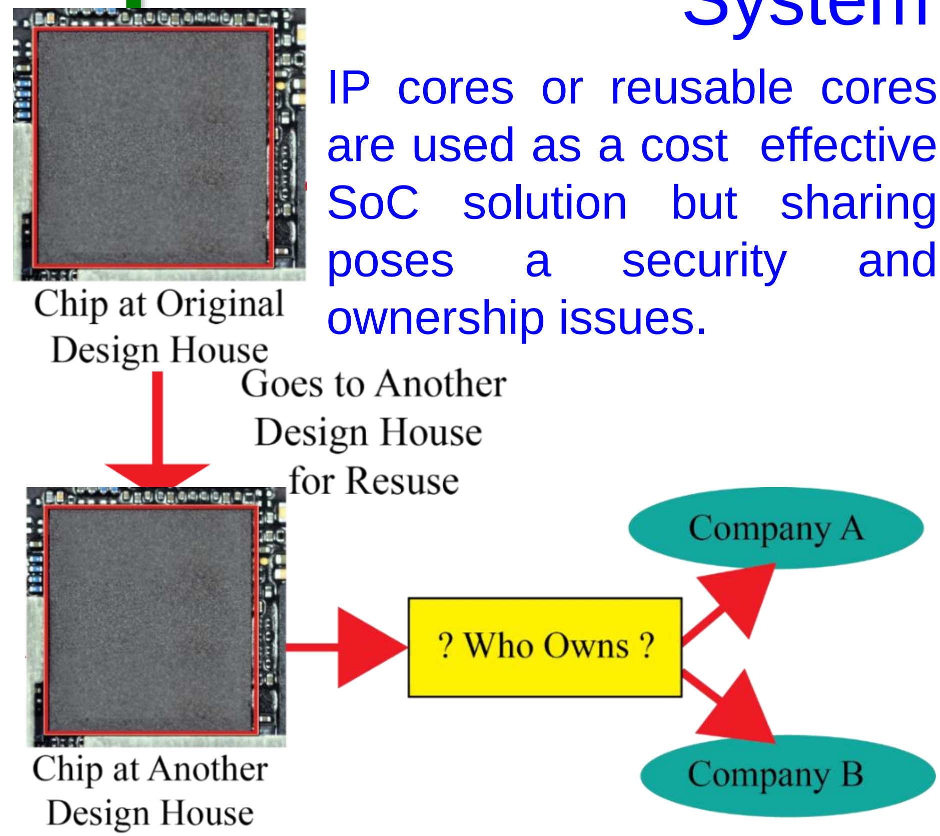
Data and System Authentication and Ownership Protection – My 20 Years of Experiences

Data



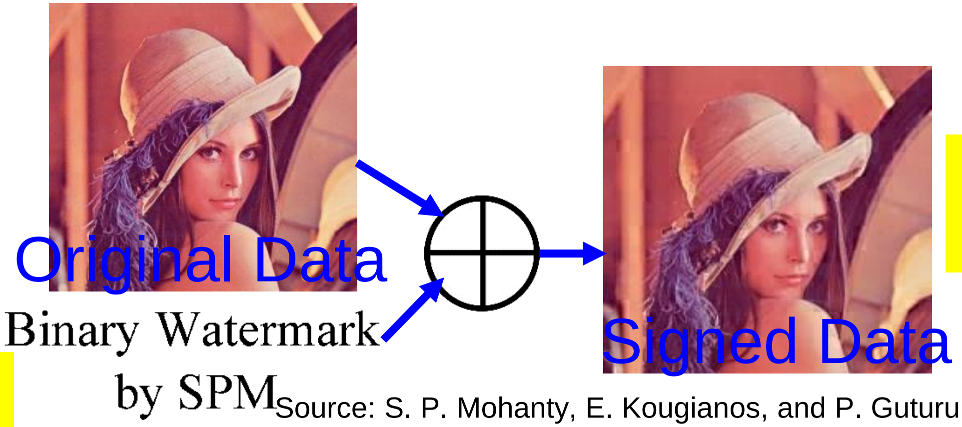
System

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.

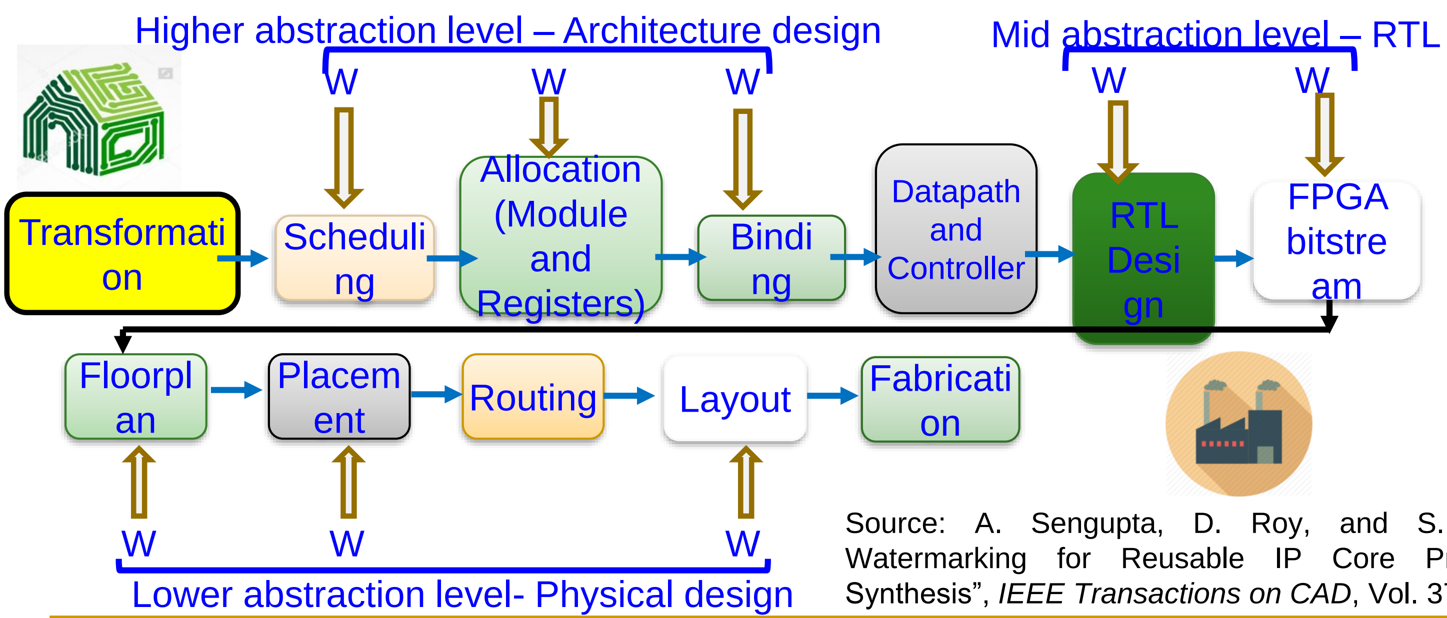
Data and System Authentication …



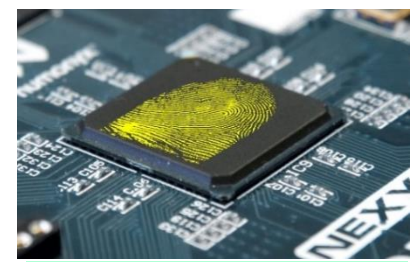
Verify / Authenticate Signature before using the data.

Data

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*, Vol 6, 2018, pp. 5939--5953.



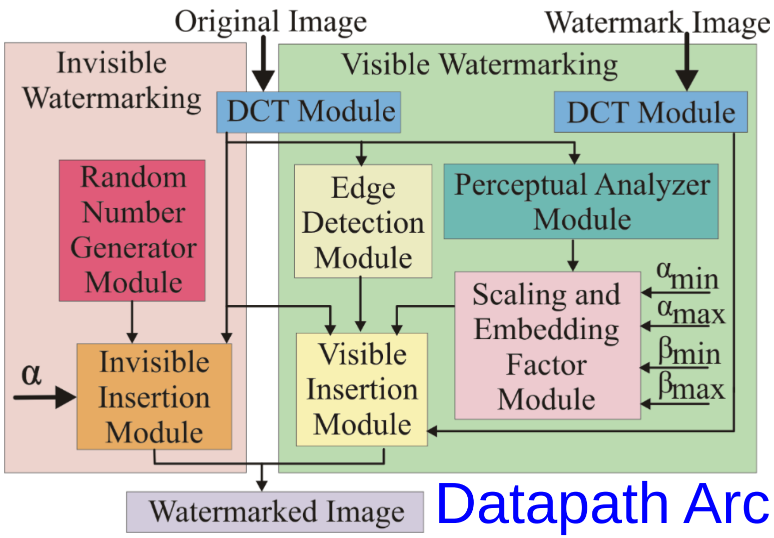
System



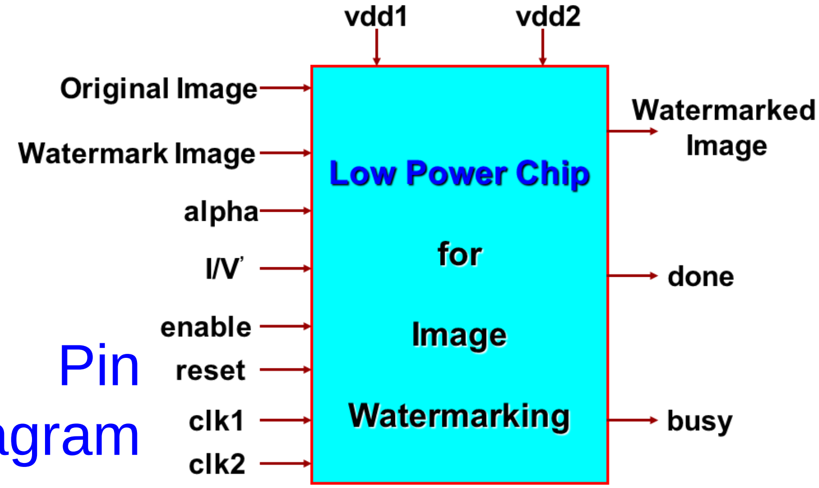
PUF as Hardware Fingerprint

Source: A. Sengupta, D. Roy, and S. P. Mohanty, “Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis”, *IEEE Transactions on CAD*, Vol. 37, No 4, 2018, pp. 742--755.

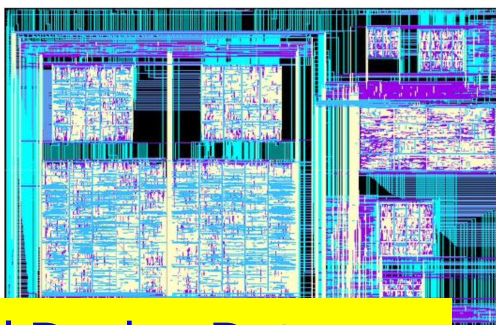
Lowest Power Consuming Watermarking Chip



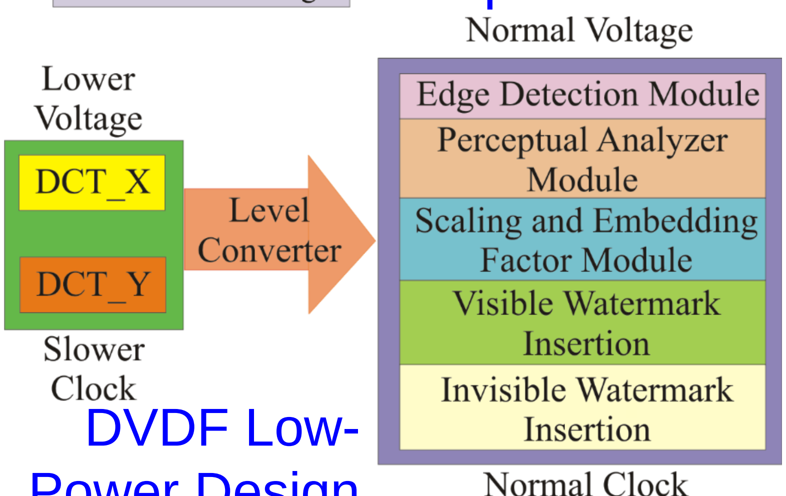
Datapath Architecture



Pin Diagram



Hardware Layout

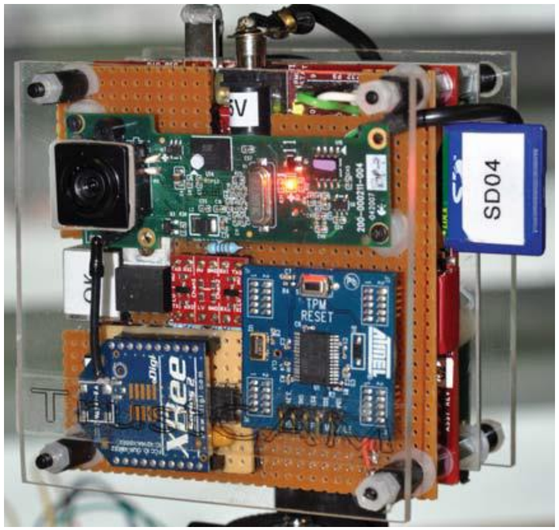


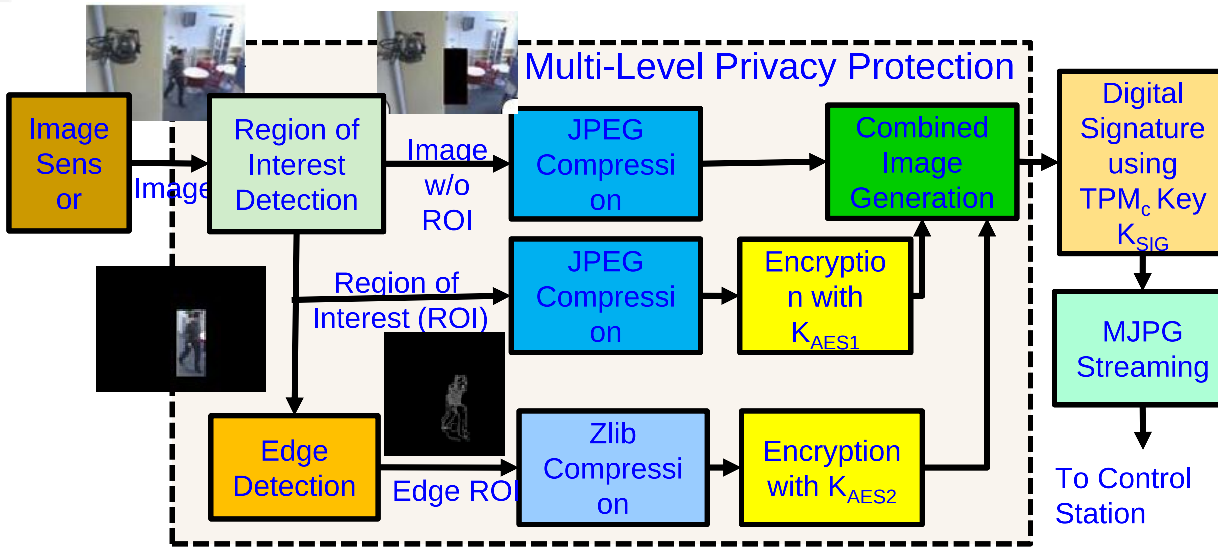
DVDF Low-Power Design

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

Source: 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



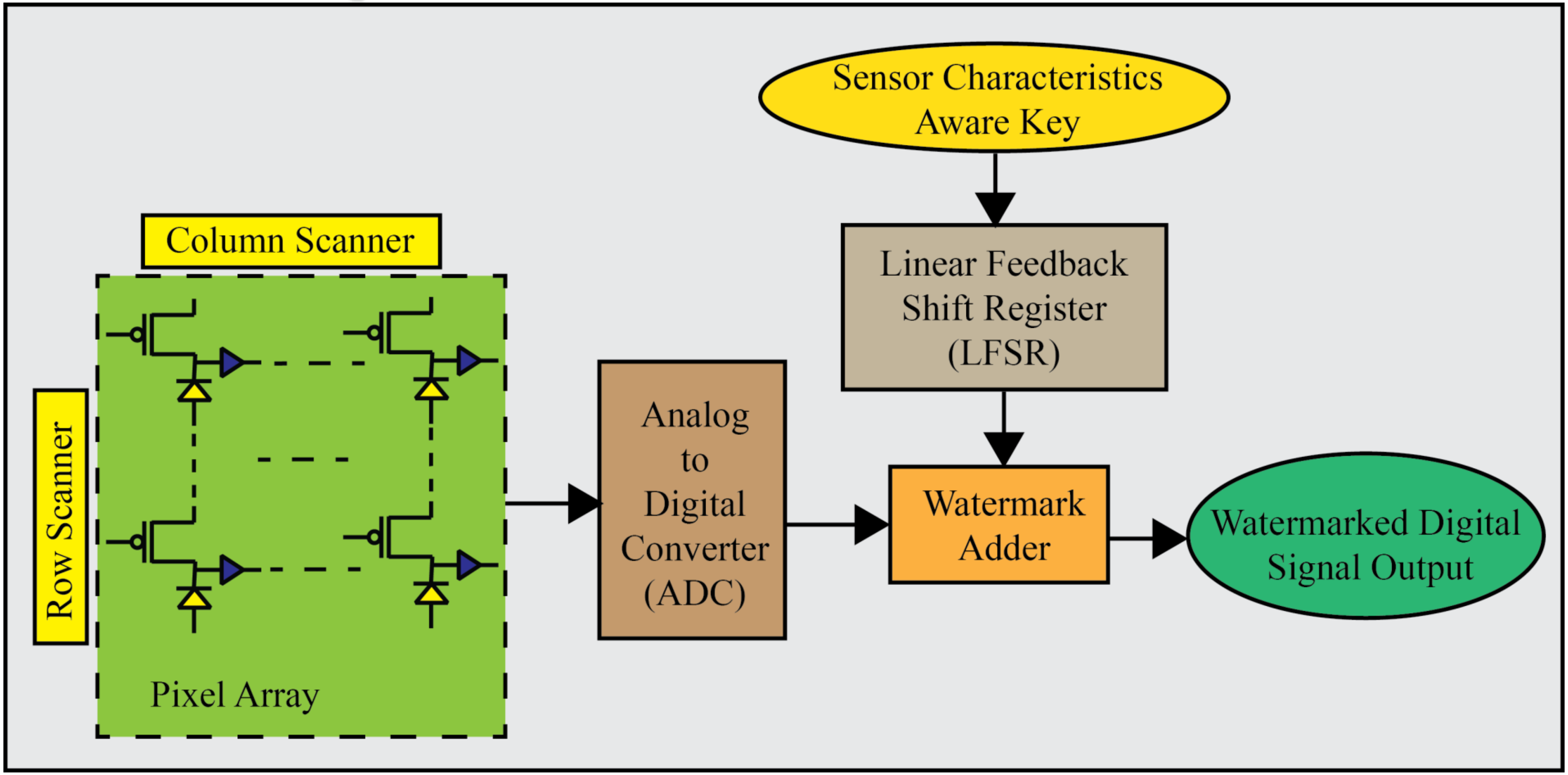


For integrity protection, authenticity and confidentiality of image data.

- 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



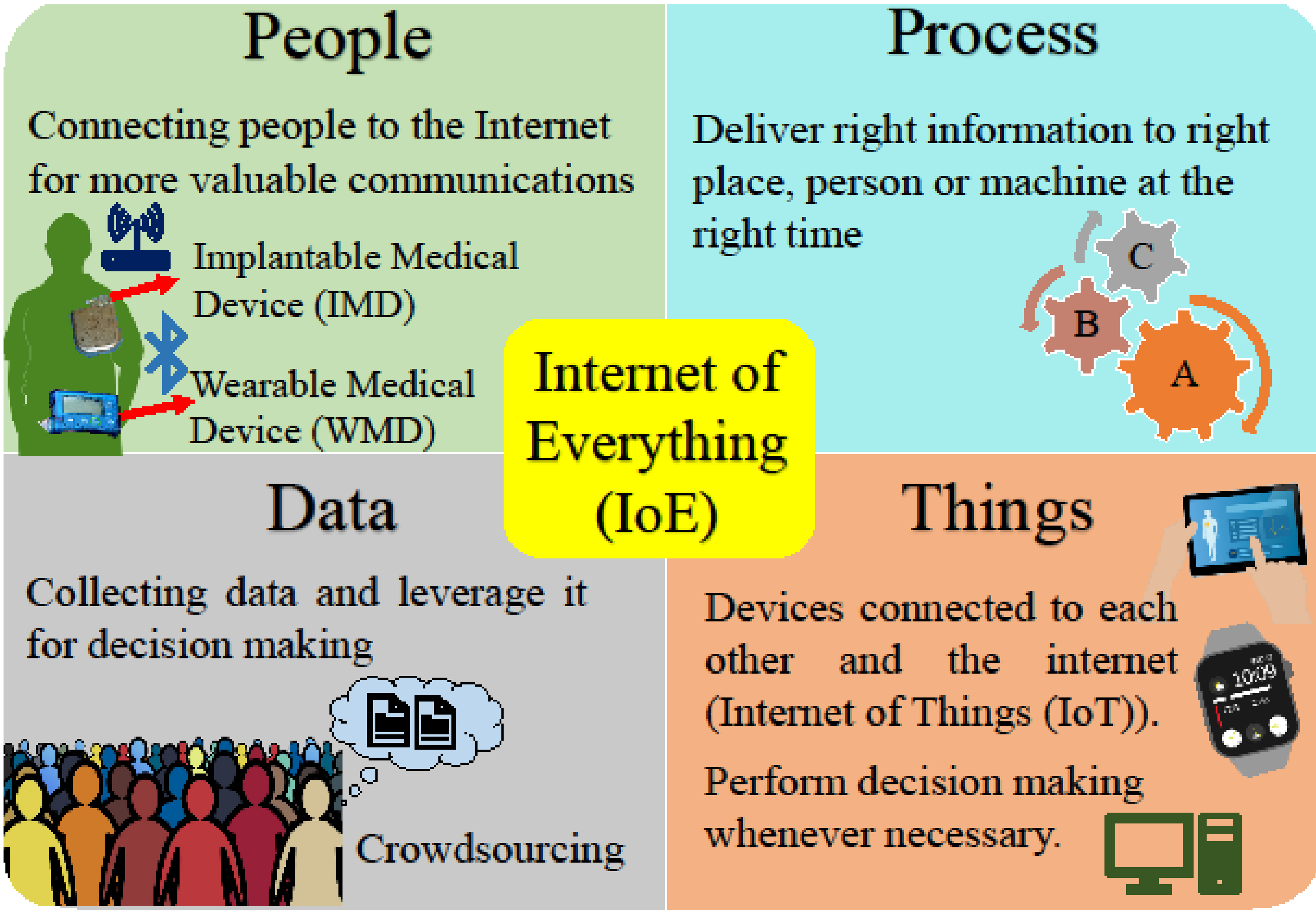
Source: G. R. Nelson, G. A. Jullien, O. Yadid-Pecht, "CMOS Image Sensor With Watermarking Capabilities", in *Proceedings of IEEE International Symposium on Circuits and Systems* (*ISCAS*), 2005, pp. 5326–5329.

Conclusions

Conclusions

- Security, Privacy, IP rights 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.

Internet of Every Things (IoE)



Requires:
- Data, Device, and System Security
- Data, Location, and System Privacy

Need of the Hour:
- Security/Secure by Design (SbD)
- Privacy by Design (PbD)

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