Physical Unclonable Function (PUF) as the Security-by-Design (SbD) Primitive for CPS

Expert Lecture - AICTE Training and Learning Academy Faculty Development Program (ATAL-FDP)

National Institute of Technology (NIT), Rourkela, India, 06 Dec 2022

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu **Website:** http://www.smohanty.org

The Big Picture

Issues Challenging City Sustainability

Pollution

Water Crisis

Energy Crisis

Traffic

Smart City Technology - As a Solution

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

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

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

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

Smart Cities Vs Smart Villages

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

-- Merriam-Webster

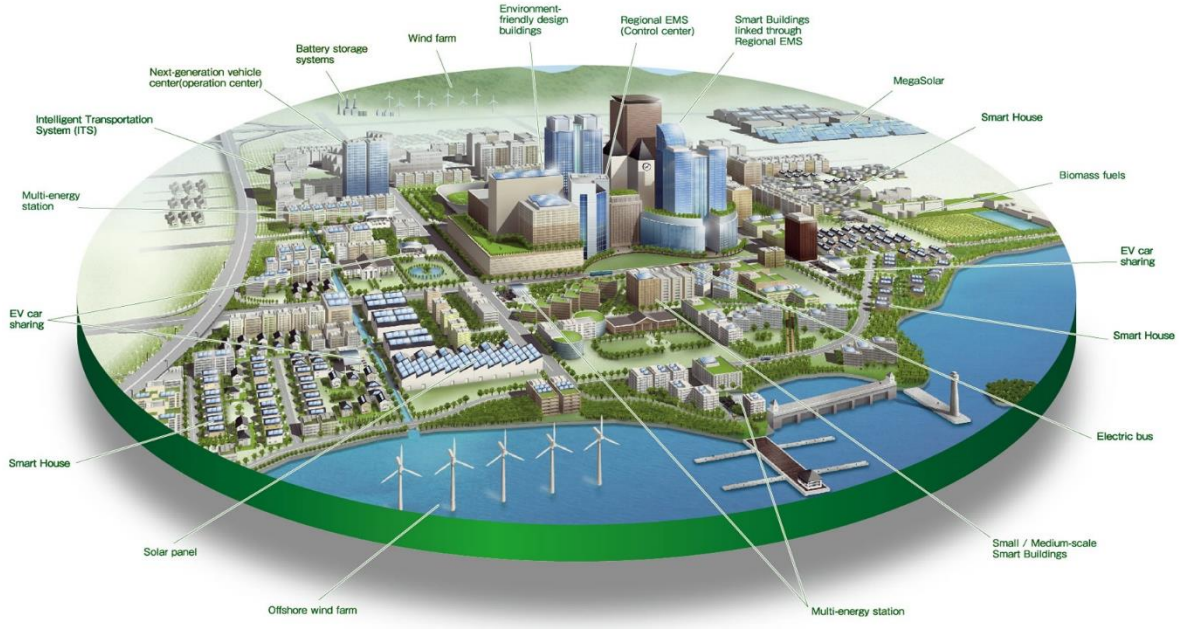
Smart City: A city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city".

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

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

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

Smart Cities Vs Smart Villages



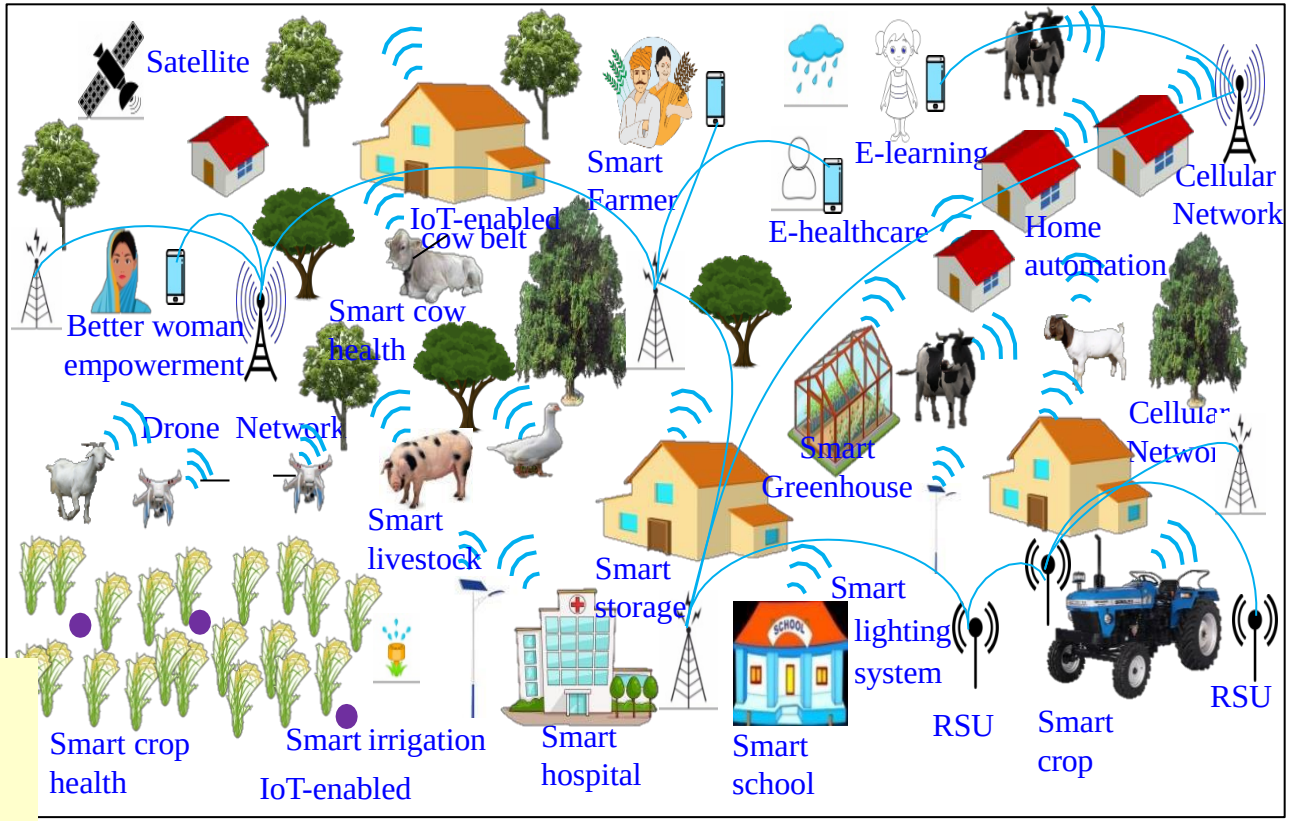
Source: http://edwingarcia.info/2014/04/26/principal/

Smart Cities

CPS Types - More
Design Cost - High
Operation Cost – High
Energy Requirement - High

Smart Villages

CPS Types - Less
Design Cost - Low
Operation Cost – Low
Energy Requirement - Low



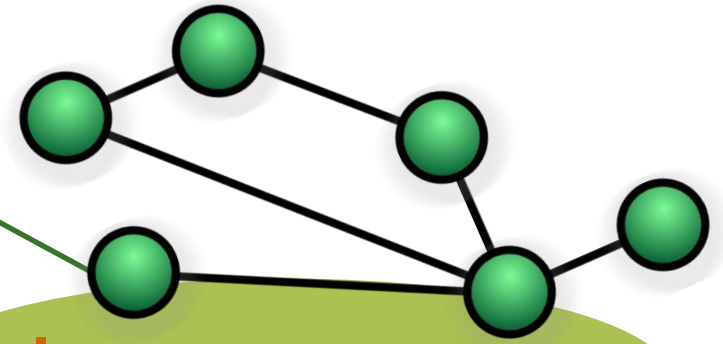
Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

Smart Cities or Smart Villages - 3 Is

Instrumentation

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

Smart Cities

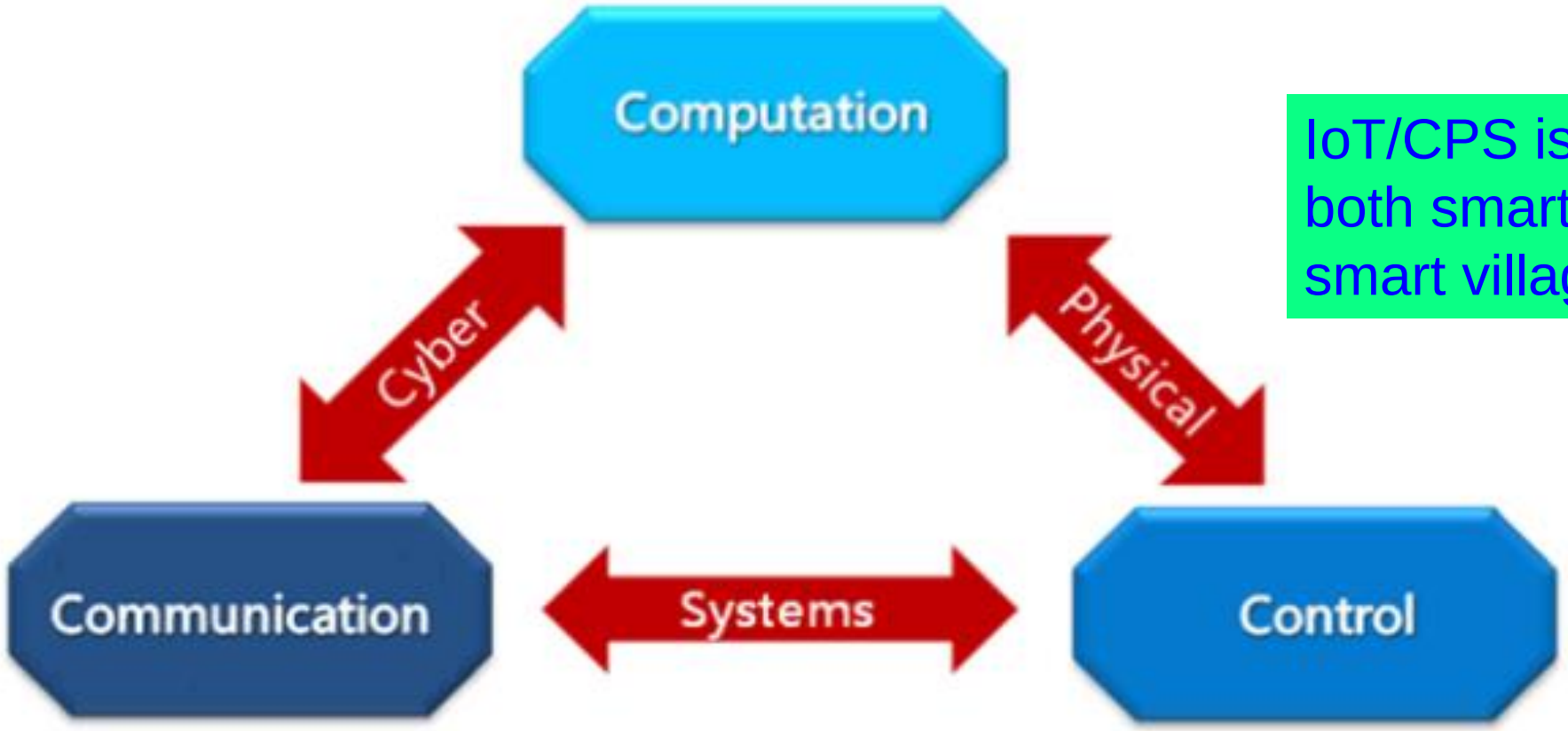


Intelligence

Interconnection

Source: Mohanty ISC2 2019 Keynote

Cyber-Physical Systems (CPS) - 3 Cs

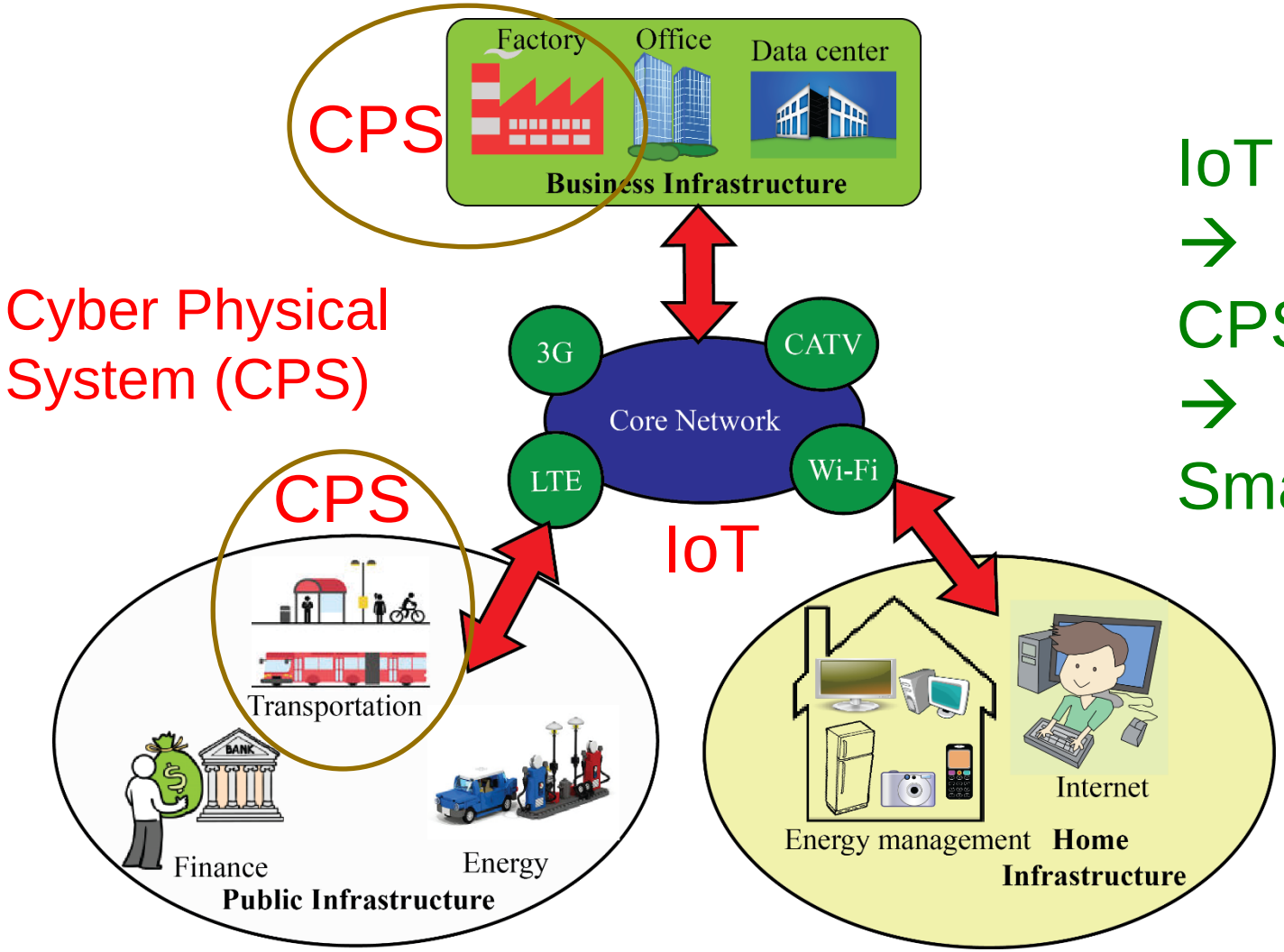


IoT/CPS is needed in both smart cities and smart villages.

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.

IoT → CPS → Smart Cities or Smart Villages

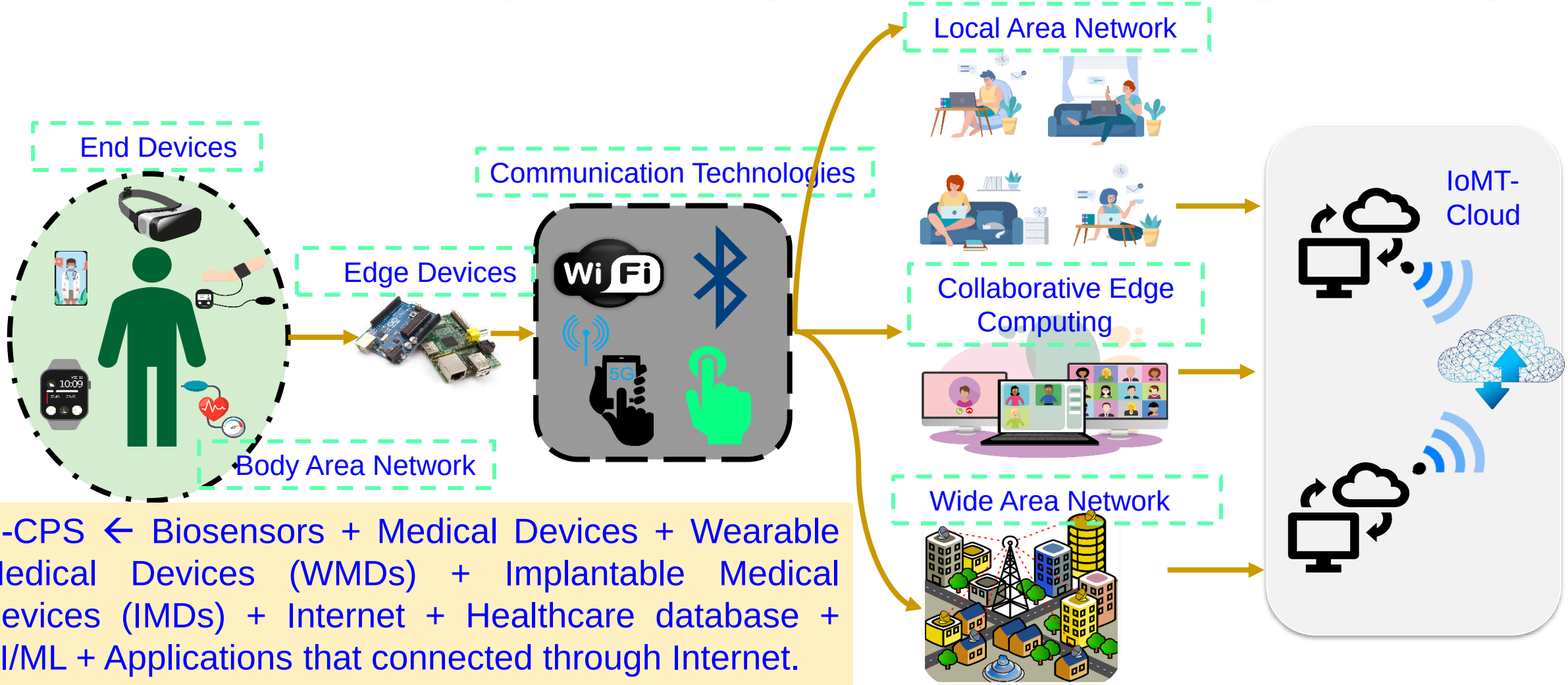


IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

IoT is the backbone

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

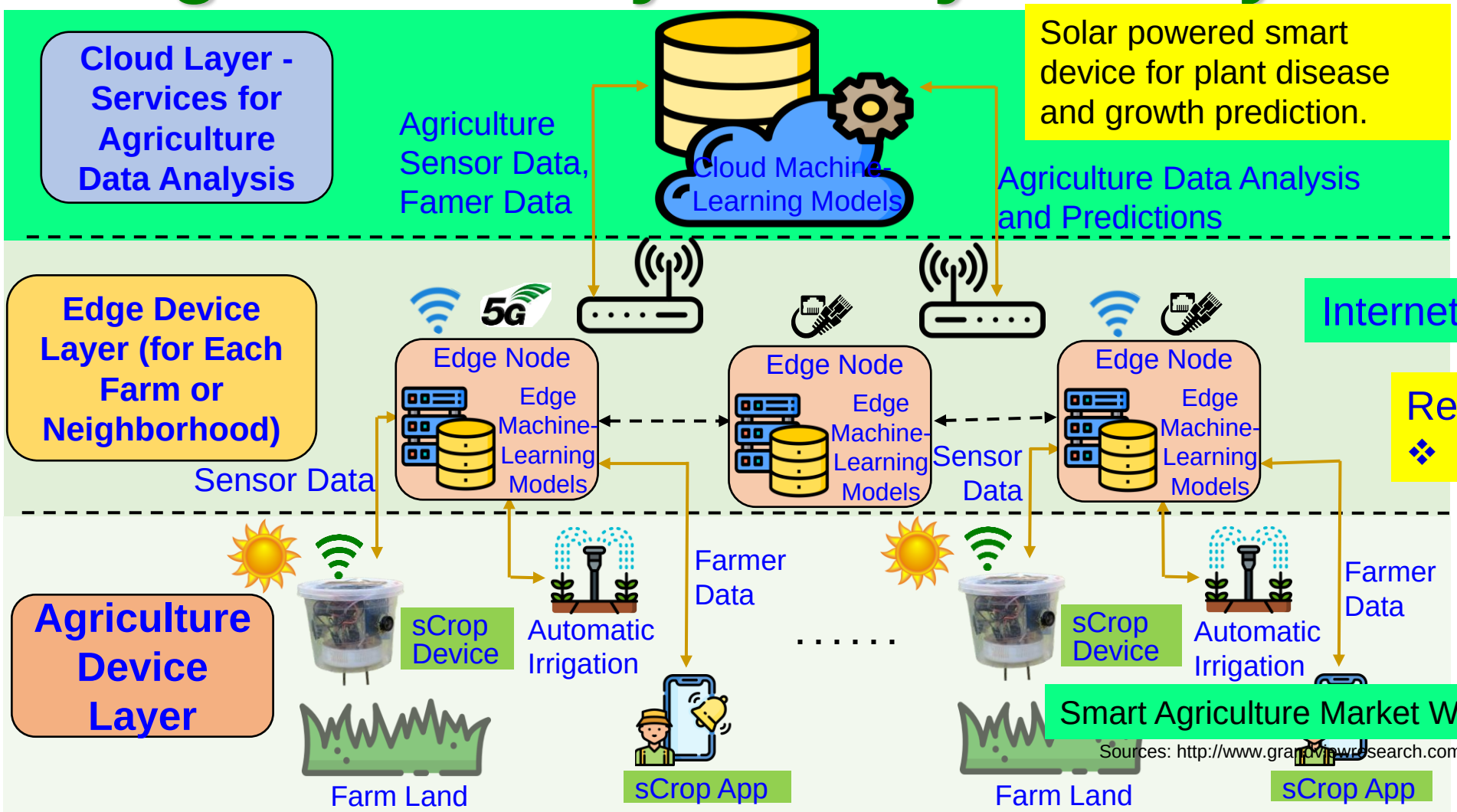
Healthcare Cyber-Physical System (H-CPS)



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

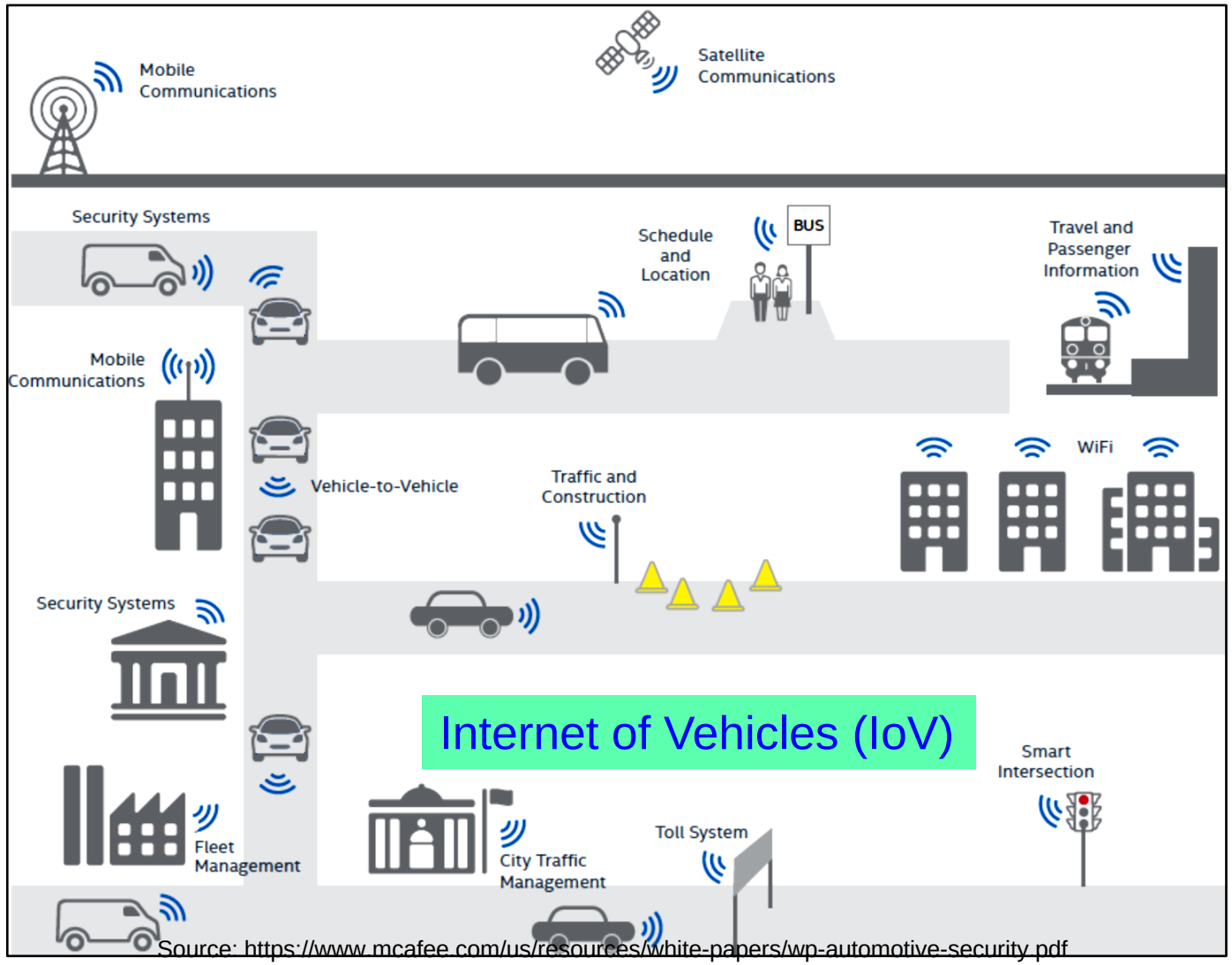
Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

Agriculture Cyber-Physical System (A-CPS)



Source: V. Udutalapally, S. P. Mohanty, V. Pallagani, and V. Khandelwal, "sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture", *IEEE Sensors Journal*, Vol. 21, No. 16, August 2021, pp. 17525--17538, DOI: 10.1109/JSEN.2020.3032438.

Transportation Cyber-Physical System (T-CPS)



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

IoT Role Includes:

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

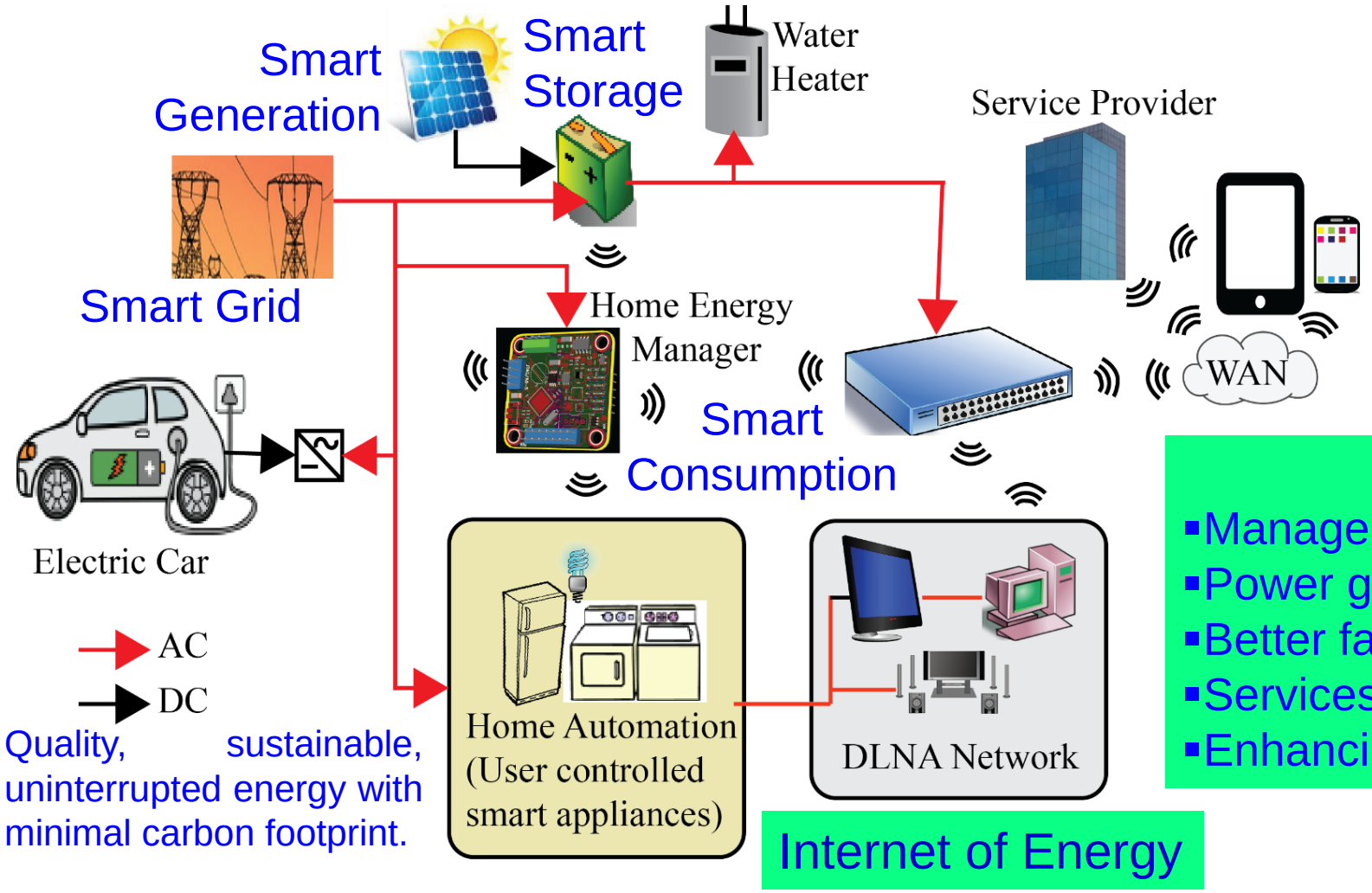
Requires:

- Data, Device, and System Security
- Location Privacy

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

Source: Datta 2017, CE Magazine Oct 2017

Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

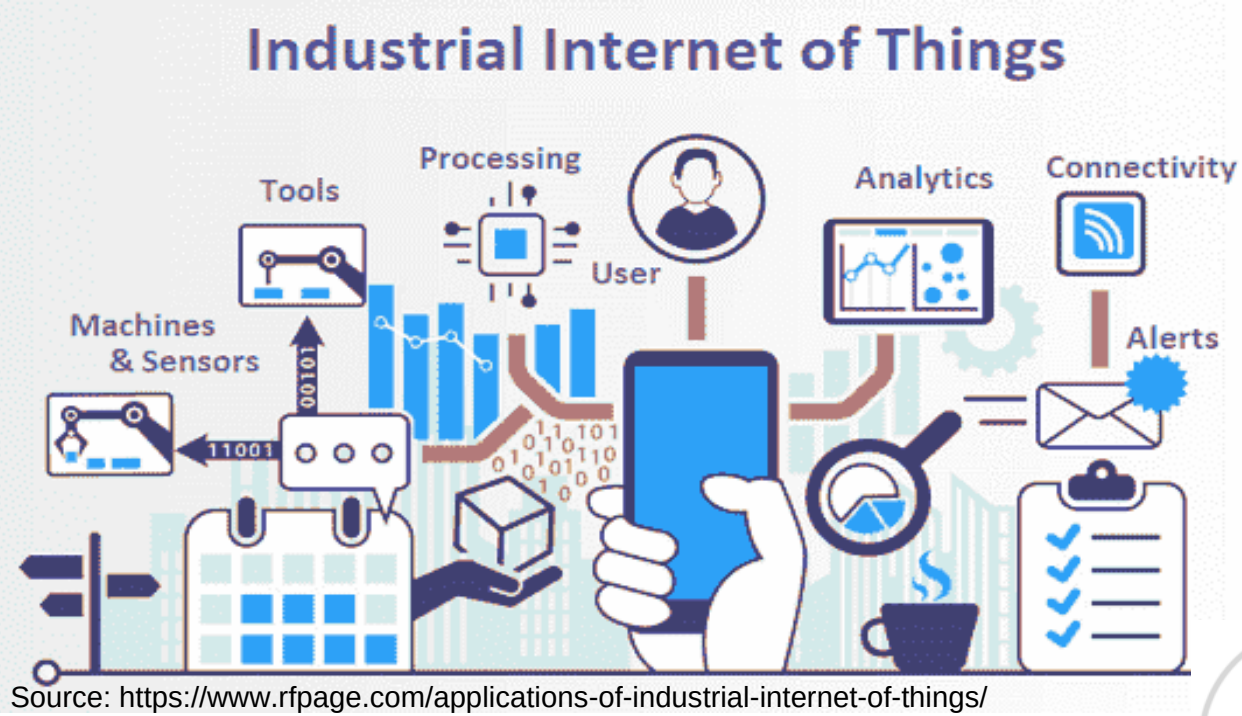
Internet of Energy

Requires:
- Data, Device, and System Security

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

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.

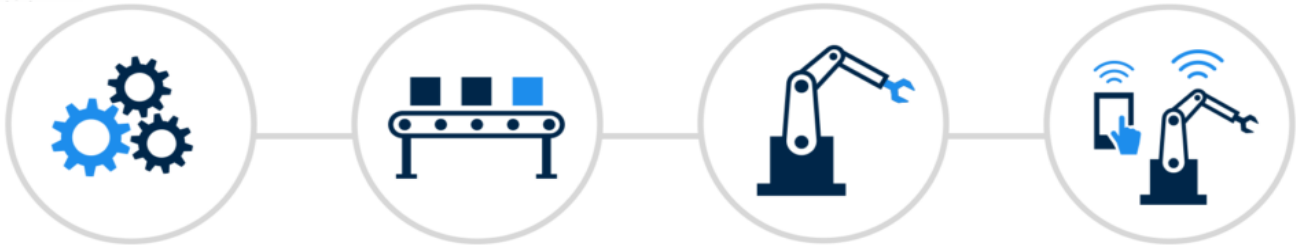
Industrial Internet of Things (IIoT)



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

Applications

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

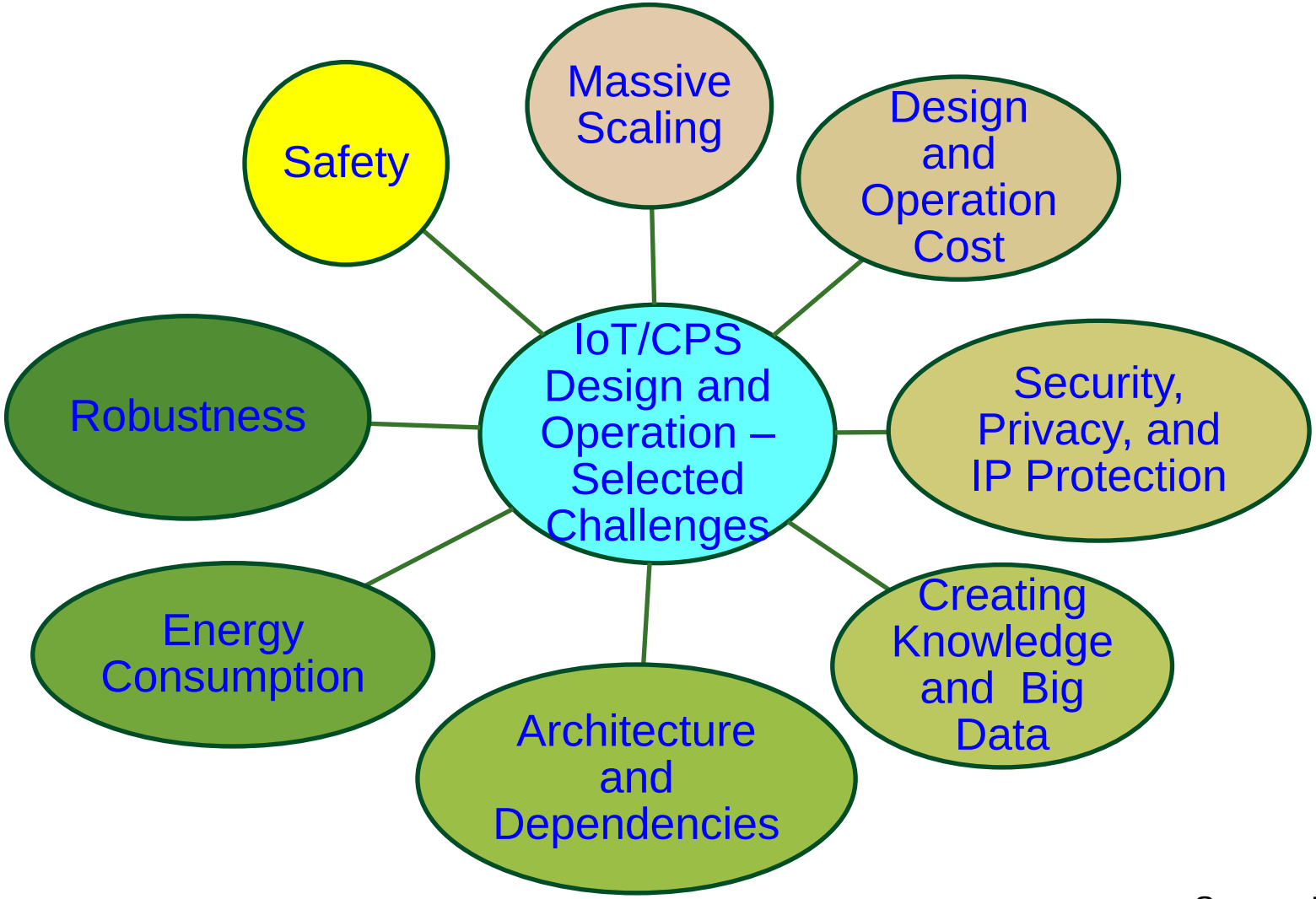


Industry 1.0	Industry 2.0	Industry 3.0	Industry 4.0
Mechanization and the introduction of steam and water power	Mass production assembly lines using electrical power	Automated production, computers, IT-systems and robotics	The Smart Factory. Autonomous systems, IoT, machine learning

Source: https://www.spectralengines.com/articles/industry-4-0-and-how-smart-sensors-make-the-difference

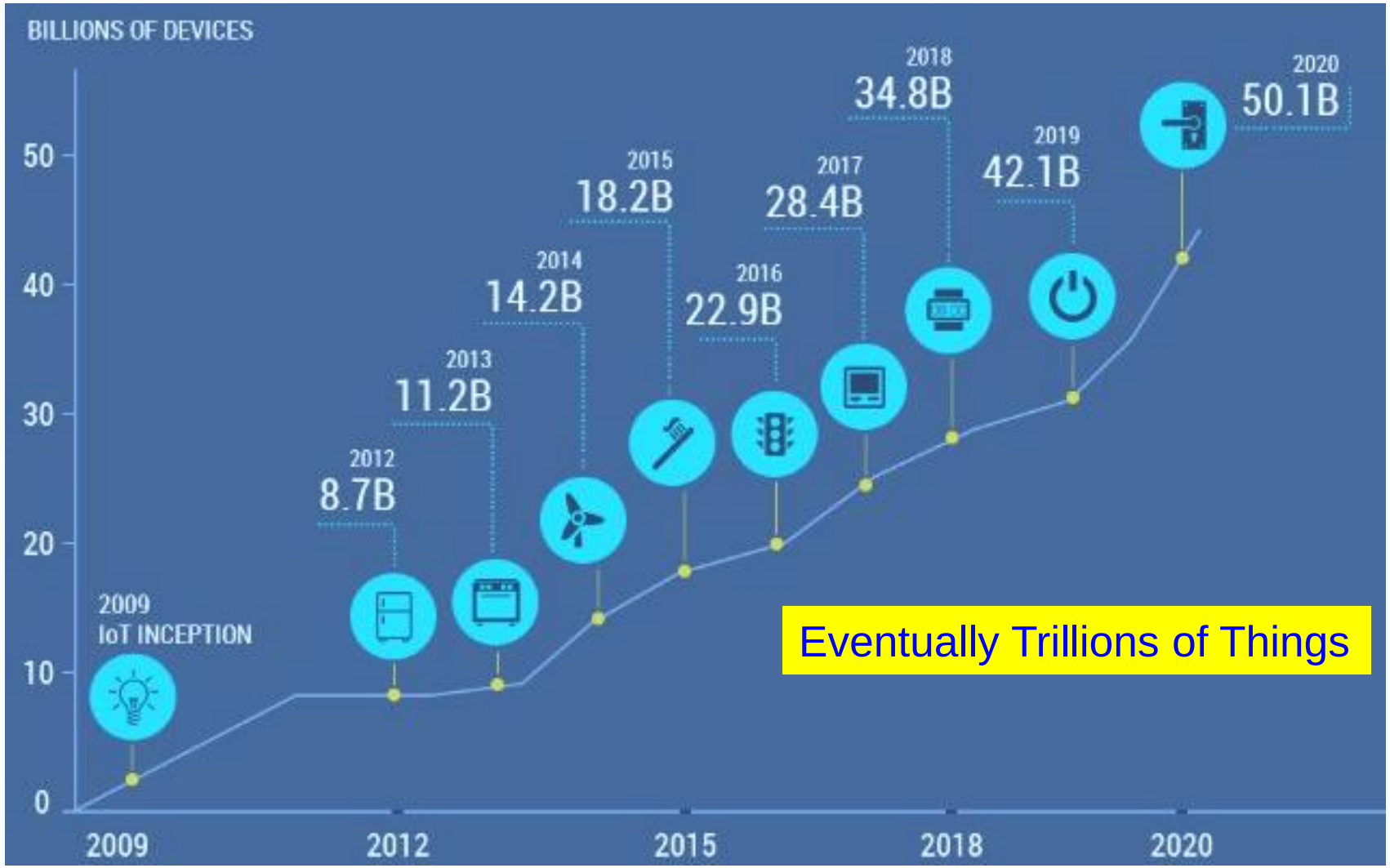
Challenges in IoT/CPS Design

IoT/CPS – Selected Challenges



Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things



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

Security Challenges – Information

Online Banking

Credit Card Theft

Hacked: Linkedin, Tumbler, & Myspace

LinkedIn tumblr. myspace

Who did it: A hacker going by the name Peace.

What was done: 500 million passwords were stolen.

Details: Peace had the following for sale on a Dark Web Store:

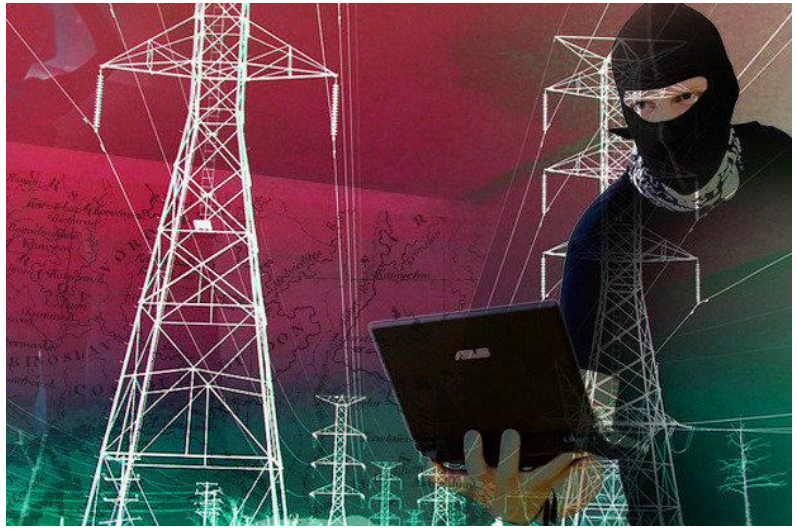
- 167 million Linkedin passwords
- 360 million Myspace passwords
- 68 million Tumbler passwords
- 100 million VK.com passwords
- 71 million Twitter passwords

Personal Information

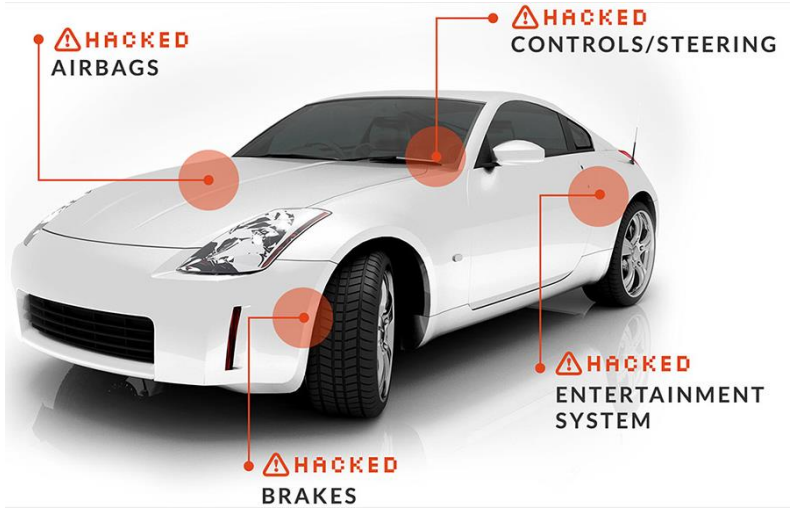
Credit Card/Unauthorized Shopping

Cybersecurity Challenges - System

Power Grid Attack



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

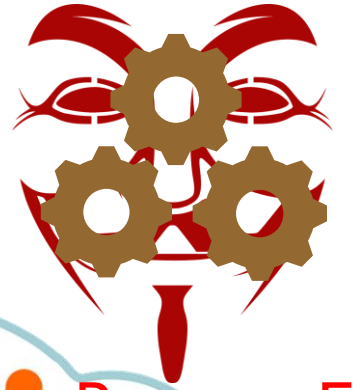


Source: http://money.cnn.com/2014/06/01/technology/security/car-hack/

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

Attacks on IoT Devices

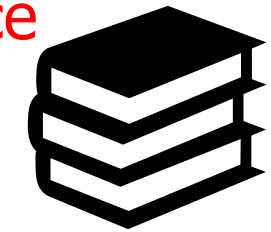
Impersonation Attack



Reverse Engineering Attack

Denial of Service Attack

Dictionary and Brute Force Attack

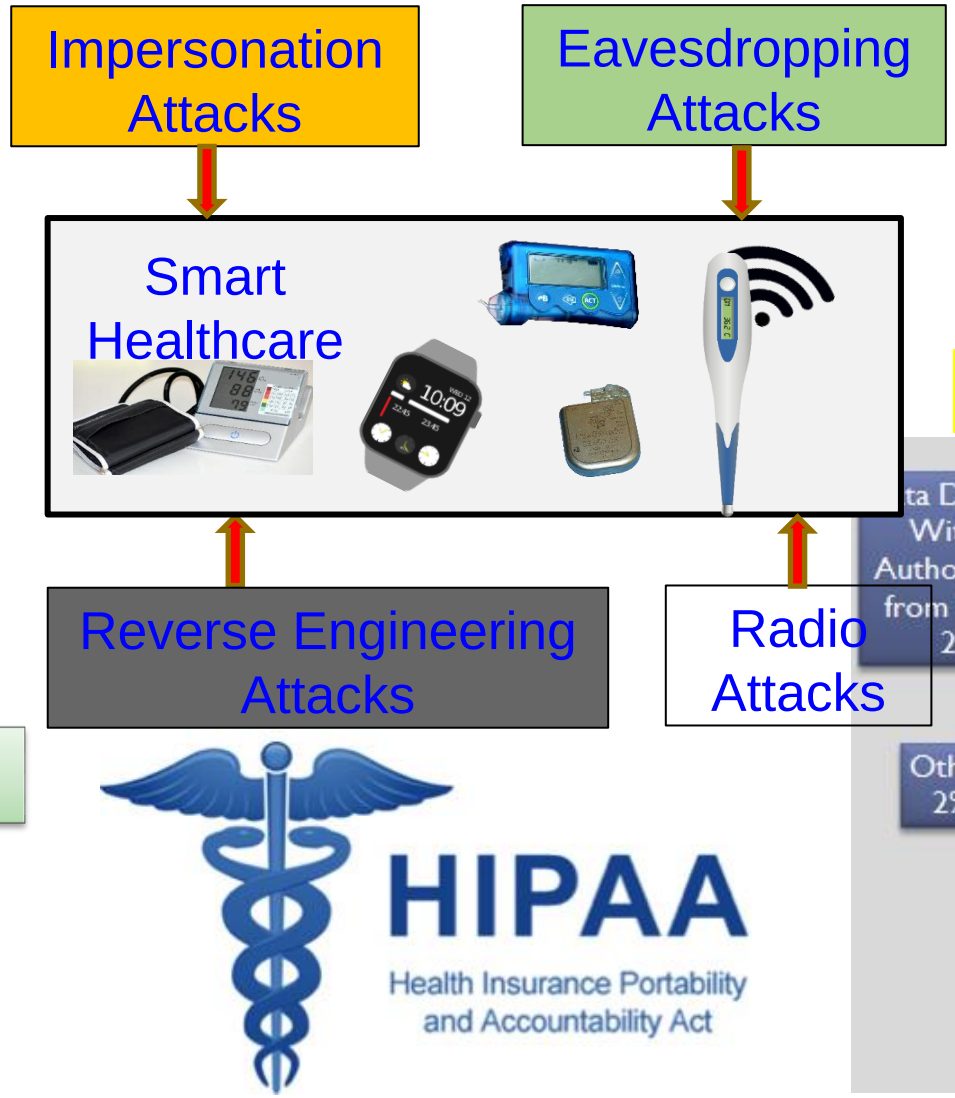


Eavesdropping Attack

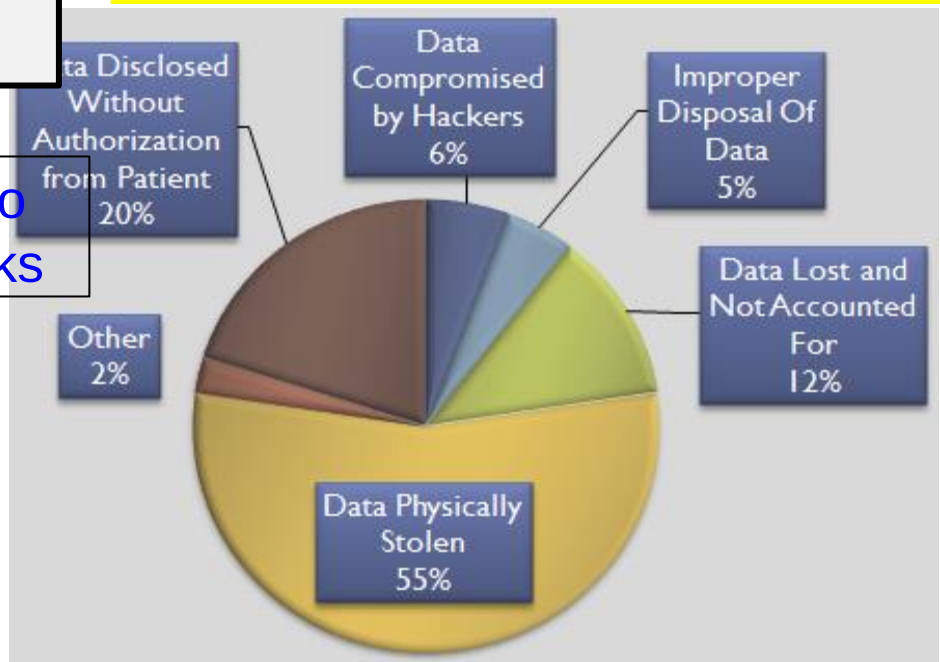
Smart Healthcare - Cybersecurity and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

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



HIPPA Privacy Violation by Types



IoMT/H-CPS Security Issue is Real and Scary

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

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

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

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

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

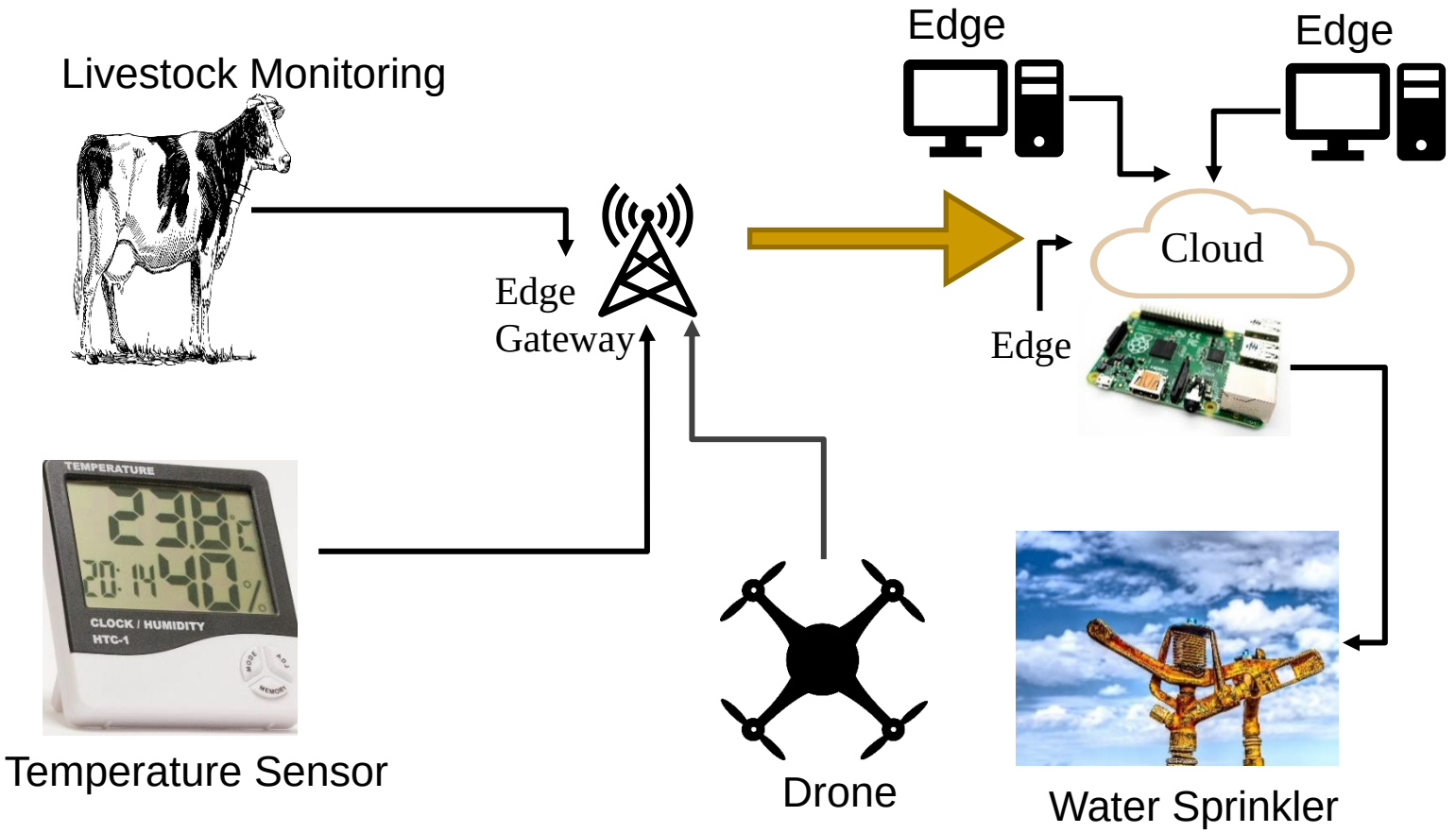
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

Implantable Medical Devices - Attacks

- The vulnerabilities affect implantable cardiac devices and the external equipment used to communicate with them.
- The devices emit RF signals that can be detected up to several meters from the body.
- A malicious individual nearby could conceivably hack into the signal to jam it, alter it, or snoop on it.

Source: Emily Waltz, Can "Internet-of-Body" Thwart Cyber Attacks on Implanted Medical Devices?, *IEEE Spectrum*, 28 Mar 2019, https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices.amp.html.

Broadview of Internet of Agro-Things (IoAT)



Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Security Issues in IoAT

- Smart Farms are Hackable Farms: IoT in Agriculture can improve the efficiency in productivity and feed 8.5 billion people by 2030. But it can also become vulnerable to various cyber security threats.

  https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked

  https://cacm.acm.org/news/251235-cybersecurity-report-smart-farms-are-hackable-farms/fulltext

- DHS report highlights that implementation of advanced precision farming technology in livestock monitoring and crop management sectors is also bringing new security issues along with efficiency

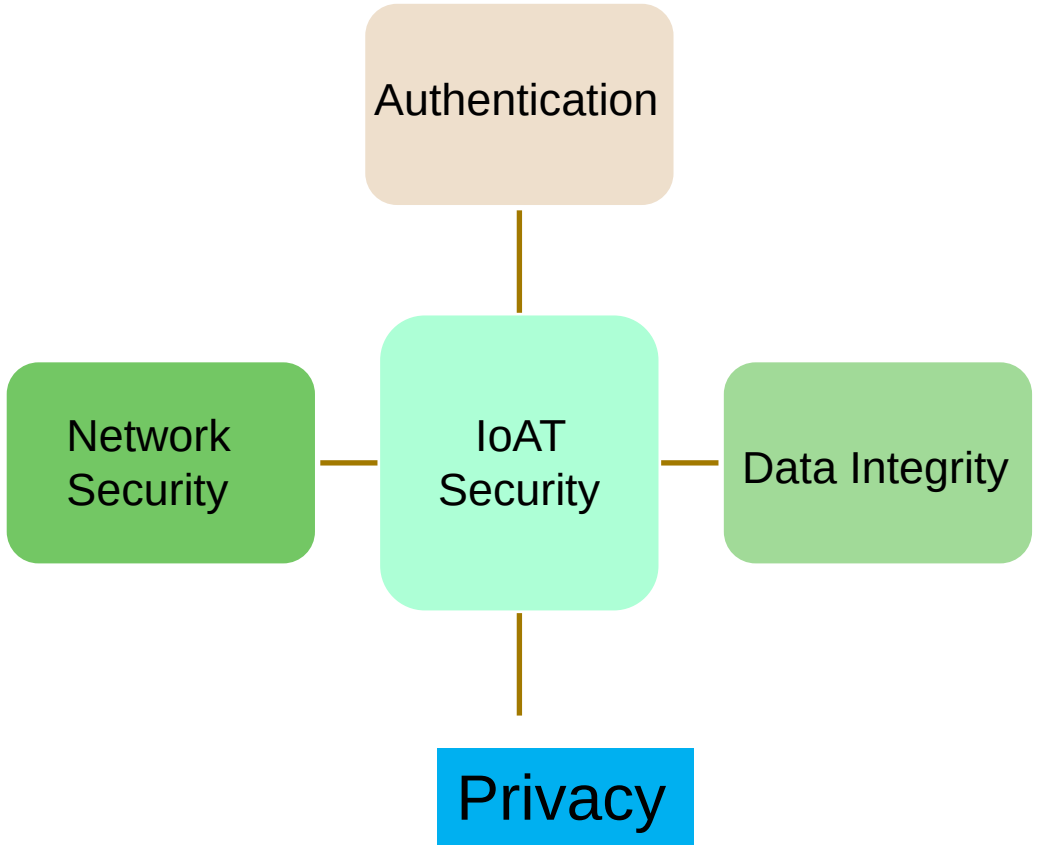
https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Smart Agriculture - Security Challenges

- Access Control
  - Develop farm specific access control mechanisms.
  - Develop data sharing and ownership policies.
- Trust
  - Prevent insider data leakage.
  - Zero day attack detection.
- Information Sharing
- Machine Learning and Artificial Intelligence Attacks
- Next Generation Network Security implementation
- Trustworthy Supply chain and Compliance

Source: M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584.

Cybersecurity Requirements for IoAT



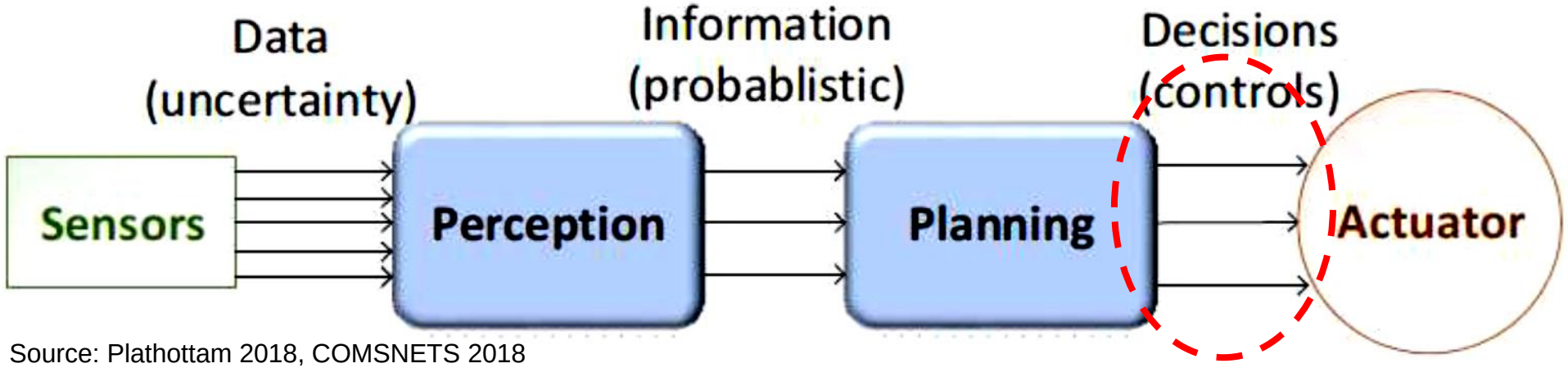
Internet of Agro-Things Characteristics:

- ✓ Smaller Size
- ✓ Smaller weight
- ✓ Safer Device
- ✓ Less Computational resources

Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

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

- Typically vehicles are controlled by human drivers
- Designing an Autonomous Vehicle (AV) requires decision chains.
- AV actuators controlled by algorithms.
- Decision chain involves sensor data, perception, planning and actuation.
- Perception transforms sensory data to useful information.
- Planning involves decision making.



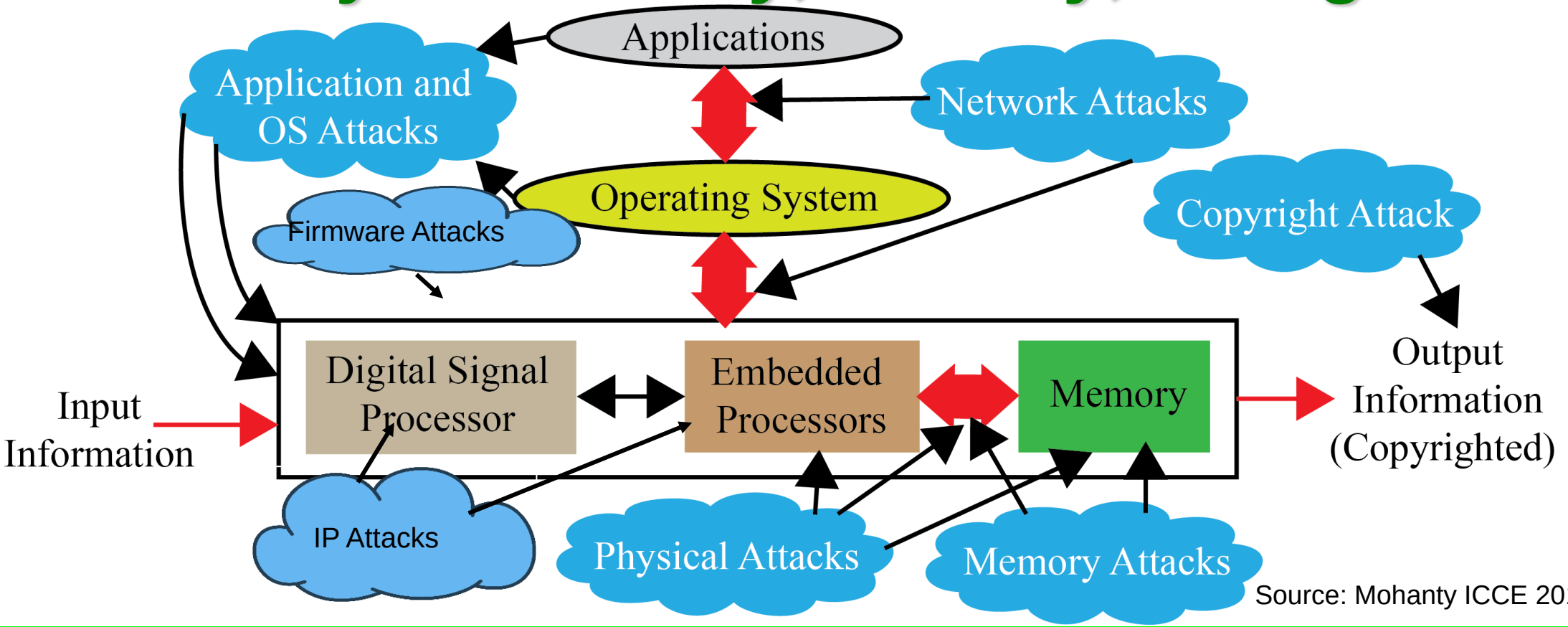
Source: Plathottam 2018, COMSNETS 2018

Smart Grid Attacks can be Catastrophic

Threats	Vulnerabilities	Source of Threats	Attacks	Impacts
Security group knowledge	Management deficiencies of network access rules Inaccurate critical assests documentation	Phishers Nation Hacker Insider Terrorist Spammers Spyware / Malware authors	Stuxnet Night Dragon Virus Denial of service Trojan horse Worm Zero day exploit Logical bomb Phishing Distributed DoS False data Injection	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
Information leakage	Unencrypted services in IT 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: 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, Mar 2019.

Selected Attacks on an Electronic System – Cybersecurity, Privacy, IP Rights



Source: Mohanty ICCE 2018 Keynote

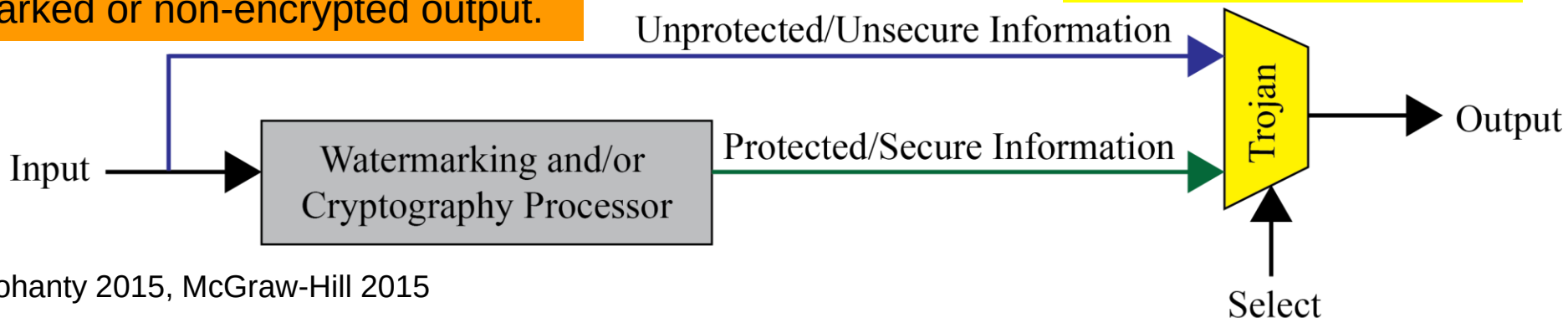
Diverse forms of Attacks, following are not the same: System Security, Device Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

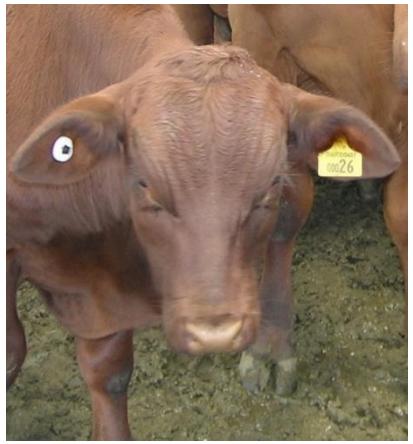
Information may bypass giving a non-watermarked or non-encrypted output.

Hardware Trojans



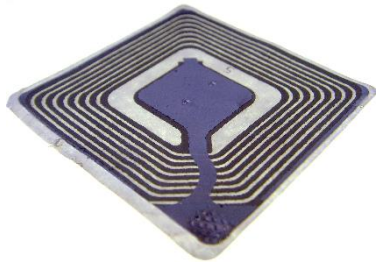
Source: Mohanty 2015, McGraw-Hill 2015

RFID Security - Attacks



Selected RFID Attacks

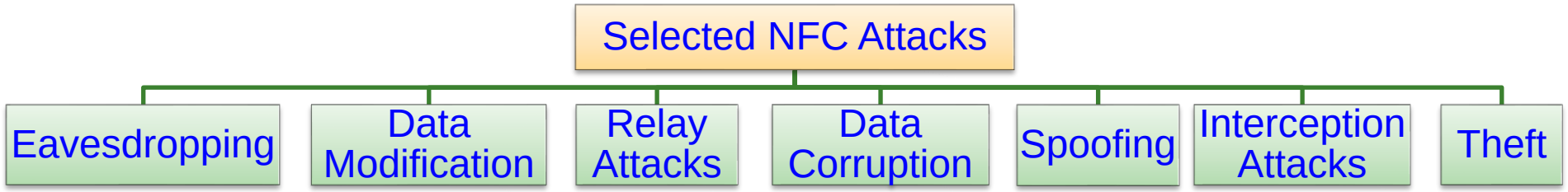
- Physical RFID Threats
  - Disabling Tags
  - Tag Modification
  - Cloning Tags
  - Reverse Engineering and Physical Exploration
- RFID Channel Threats
  - Eavesdropping
  - Snooping
  - Skimming
  - Replay Attack
  - Relay Attacks
  - Electromagnetic Interference
- System Threats
  - Counterfeiting and Spoofing Attacks
  - Tracing and Tracking
  - Password Decoding
  - Denial of Service (DoS) Attacks



Numerous Applications

Source: Khattab 2017: Springer 2017 RFID Security

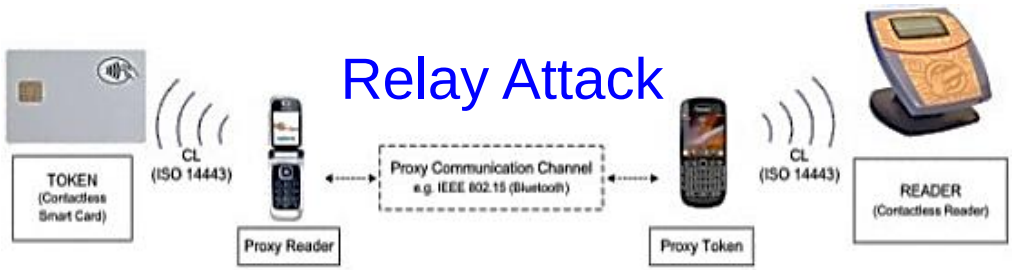
NFC Security - Attacks



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

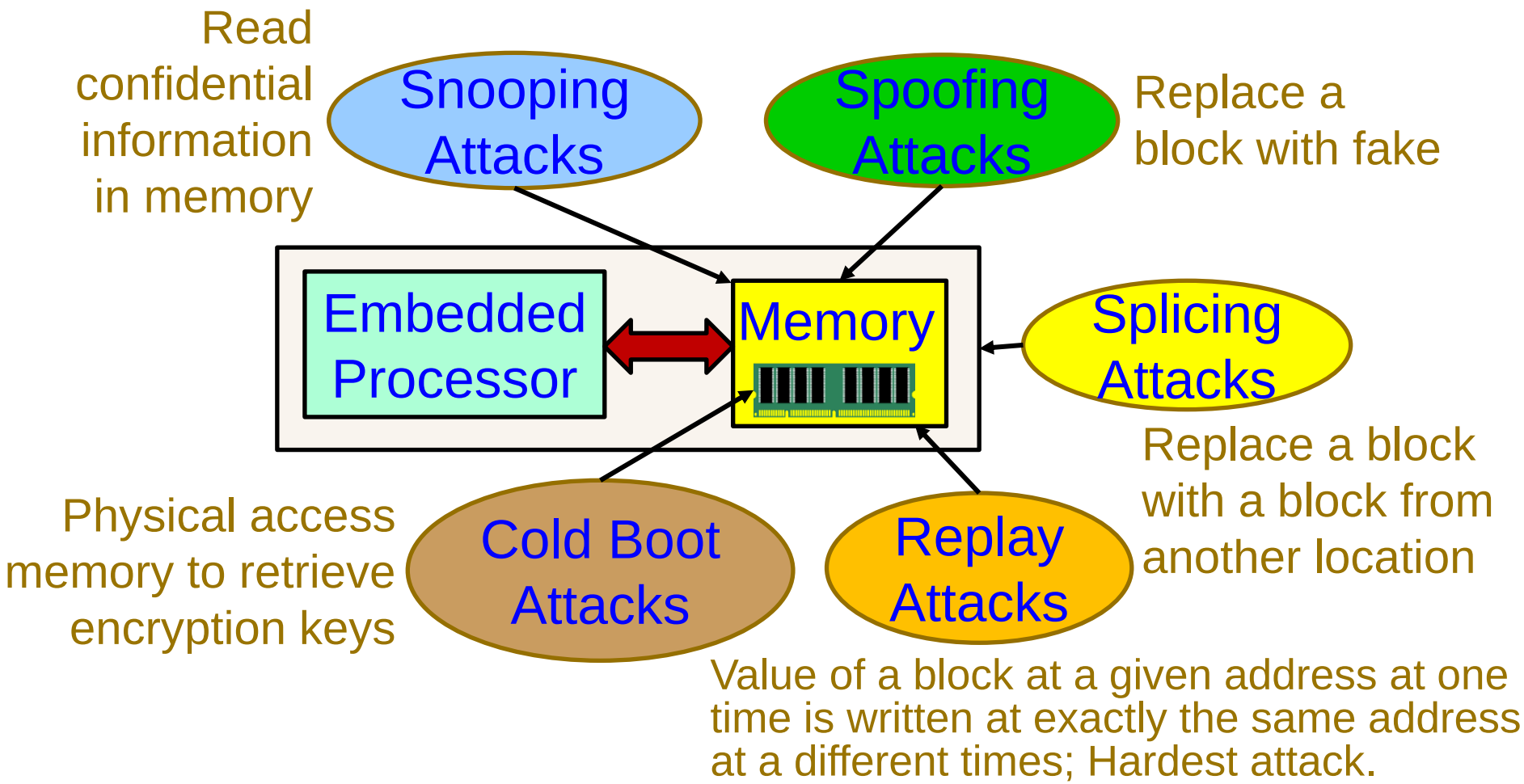
Eavesdropping

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



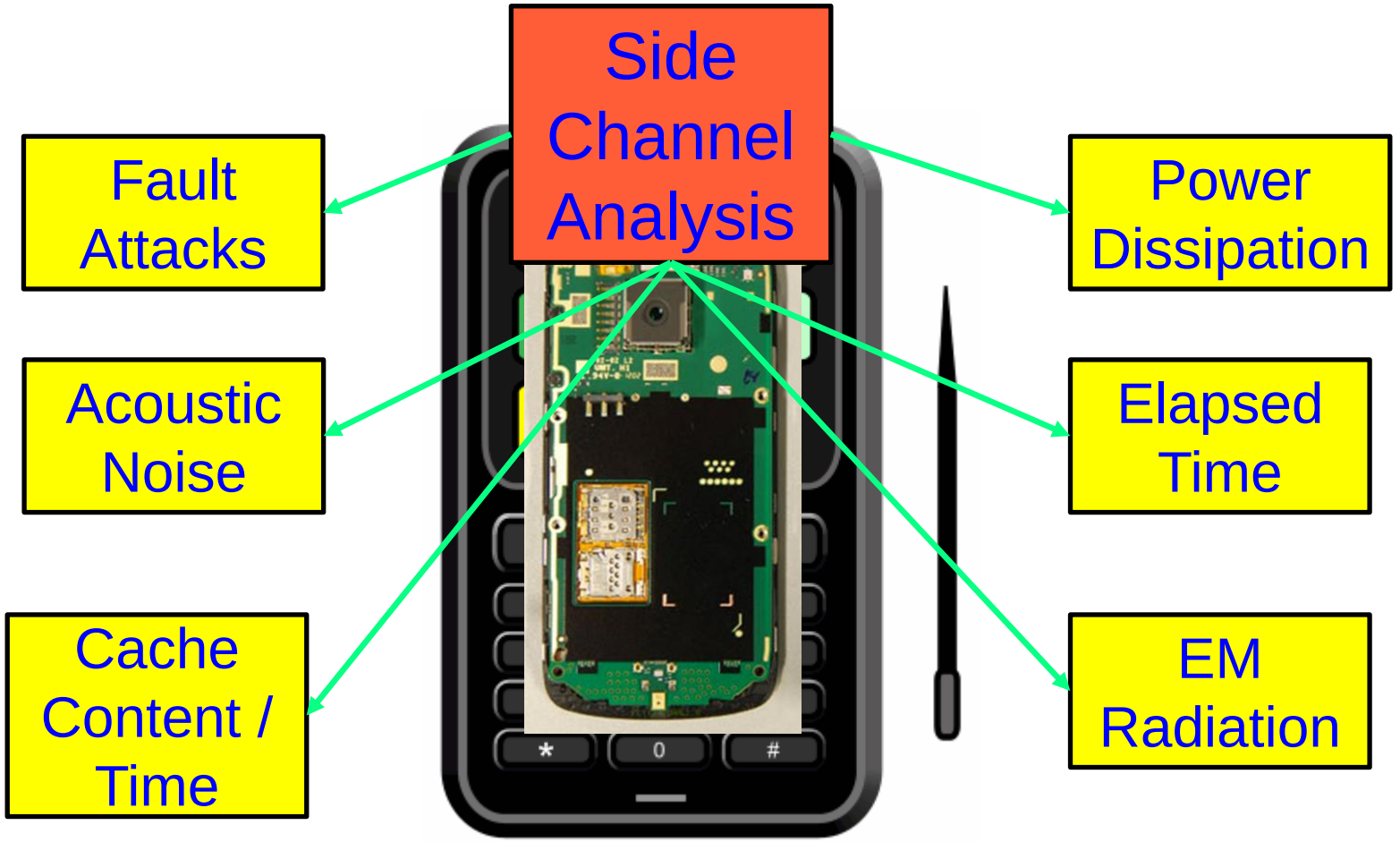
Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

Attacks on Embedded Systems' Memory



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

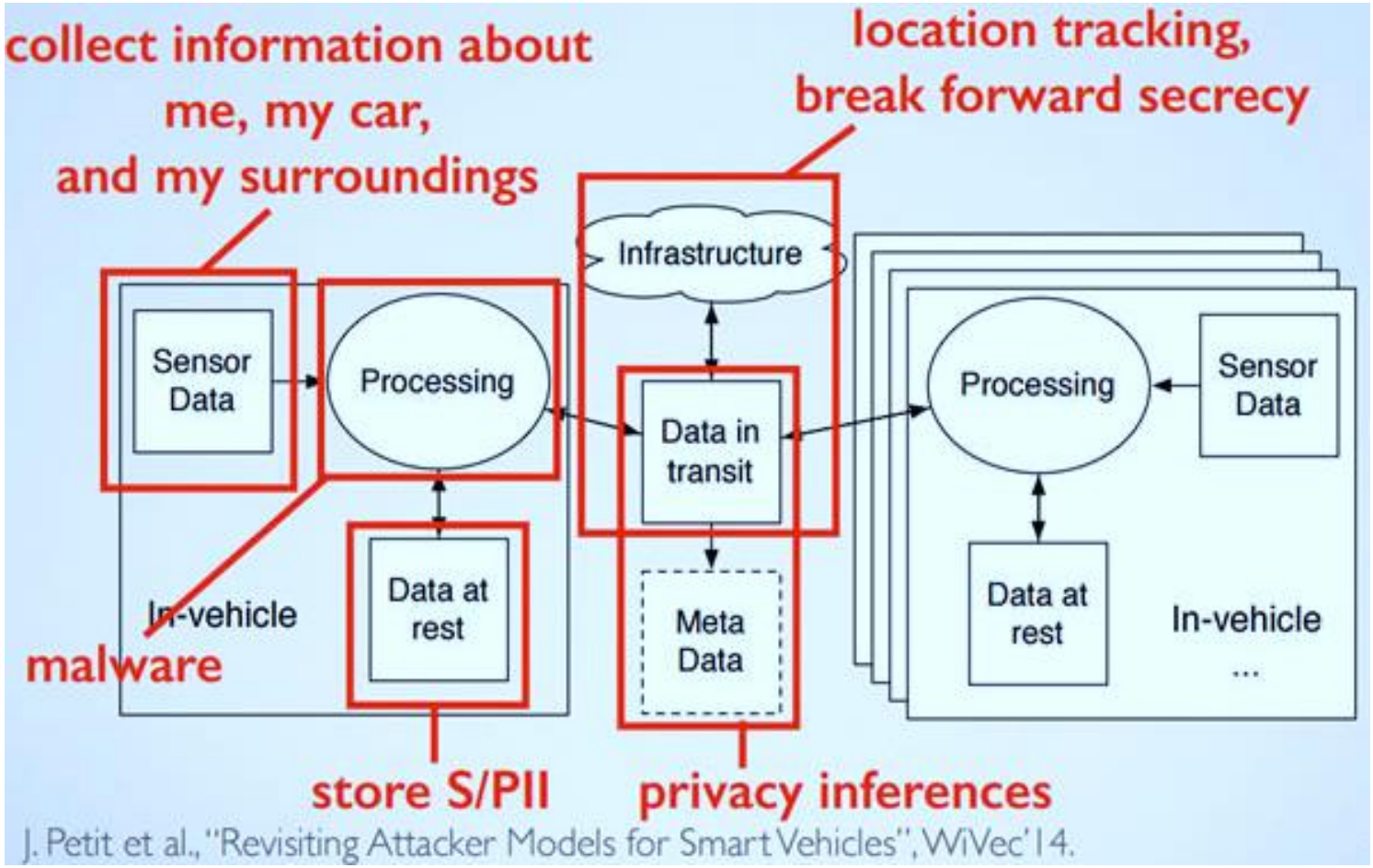
Side Channel Analysis Attacks

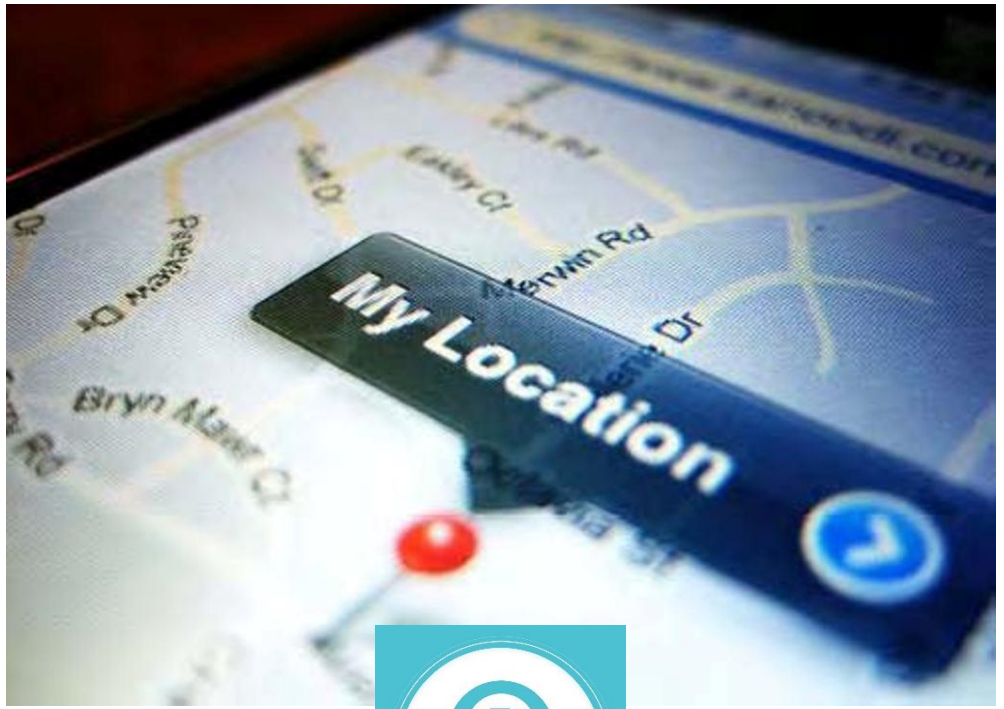


Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

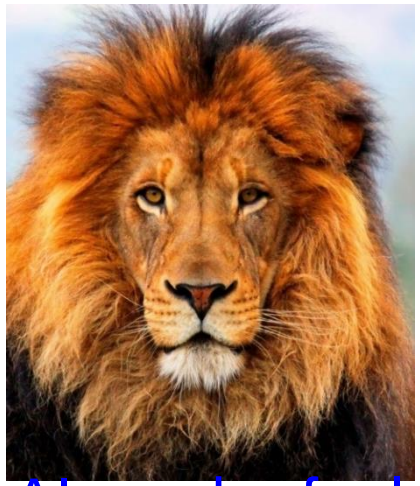
Privacy Challenge – System, Location





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

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

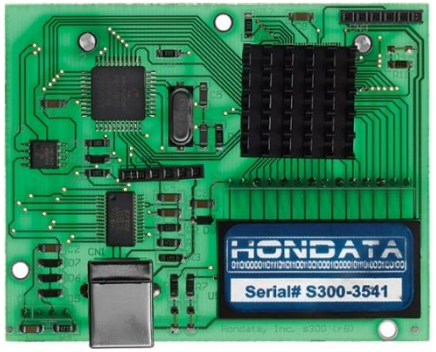


AI can be fooled by fake data

AI can create fake data (Deepfake)

Authentic Fake

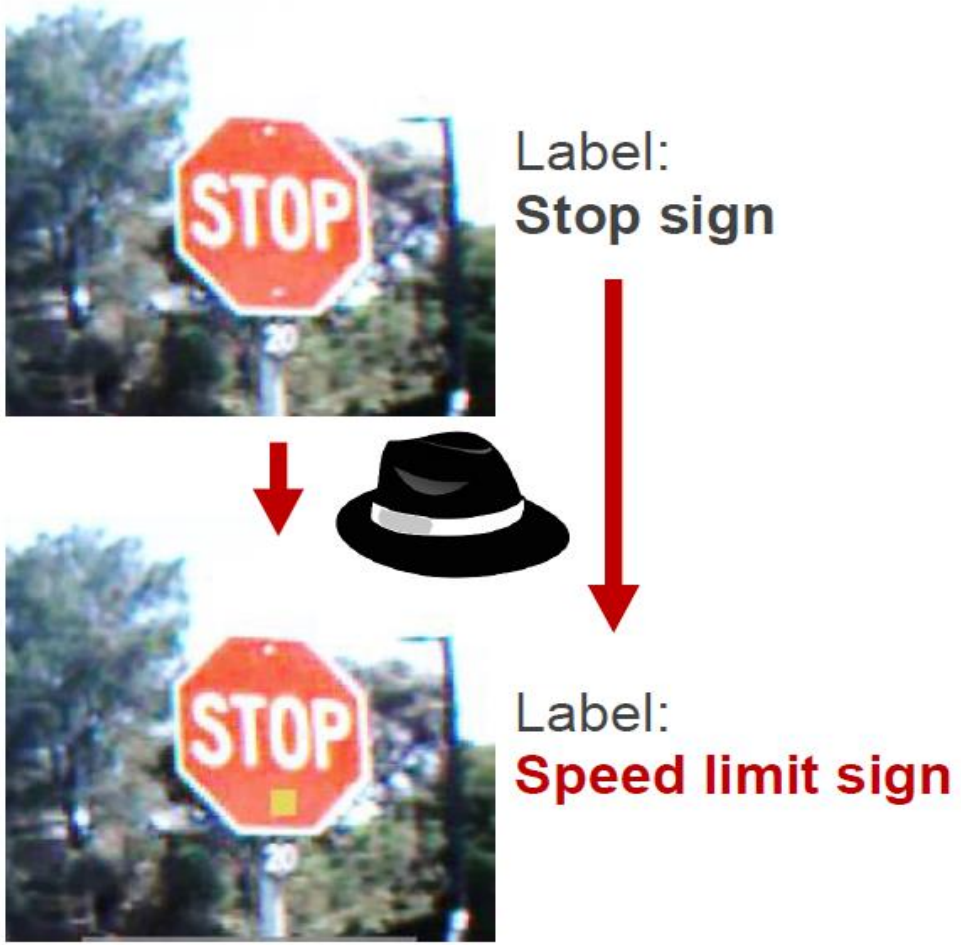
An implantable medical device



Authentic Fake

A plug-in for car-engine computers

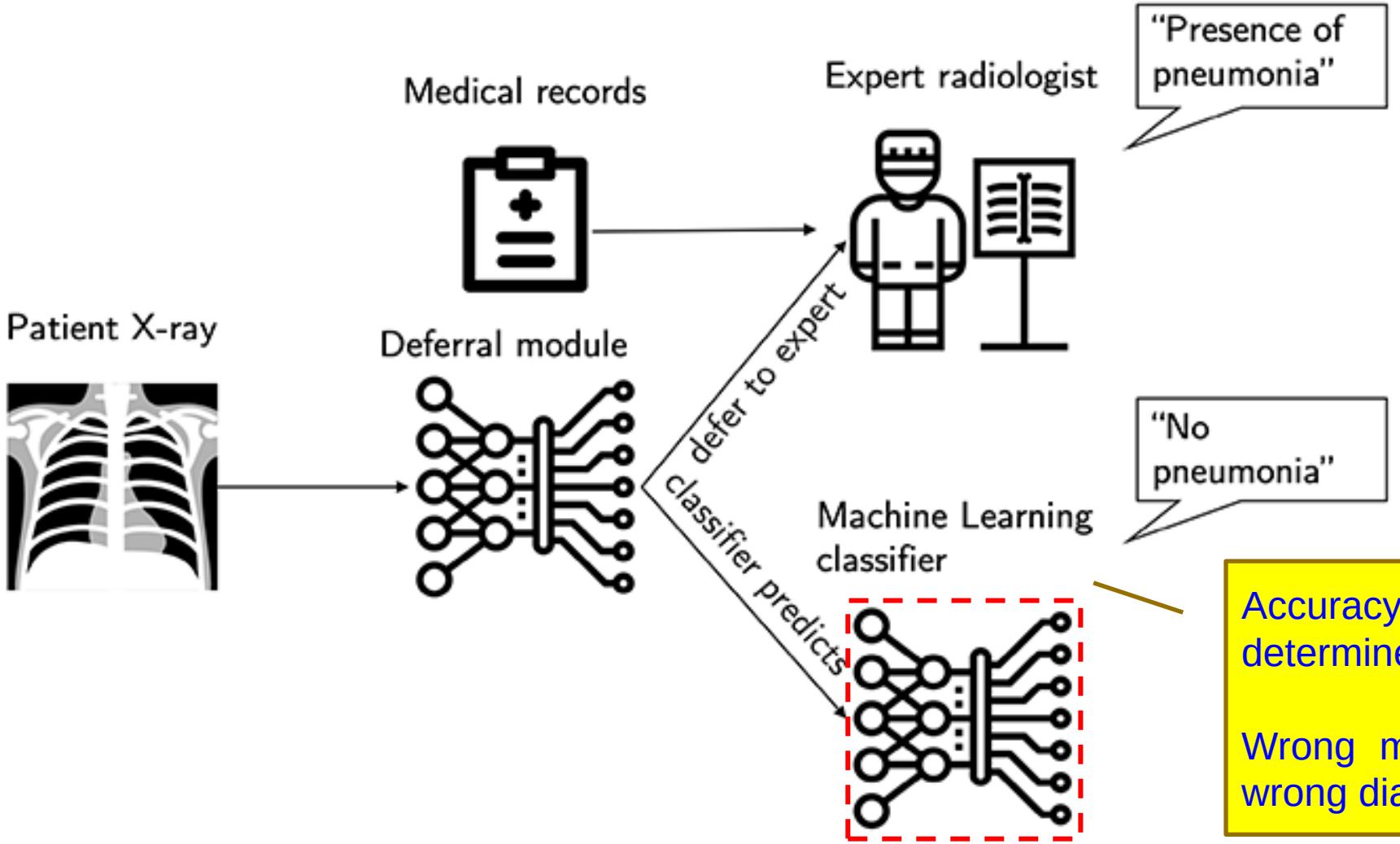
AI Security - Trojans in Artificial Intelligence (TrojAI)



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

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

Wrong ML Model → Wrong Diagnosis

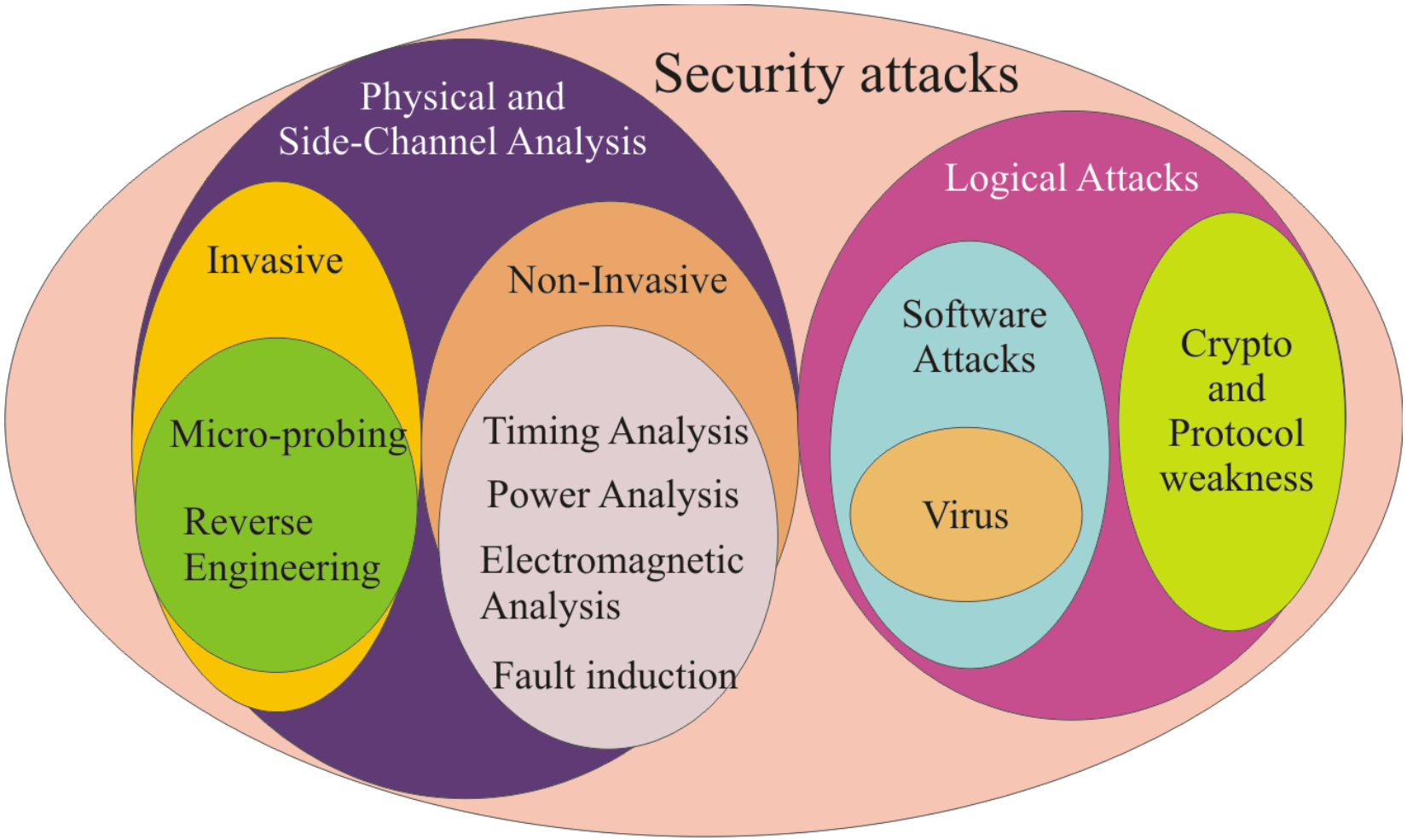


Accuracy is important determine pneumonia

Wrong model can lead to wrong diagnosis altogether

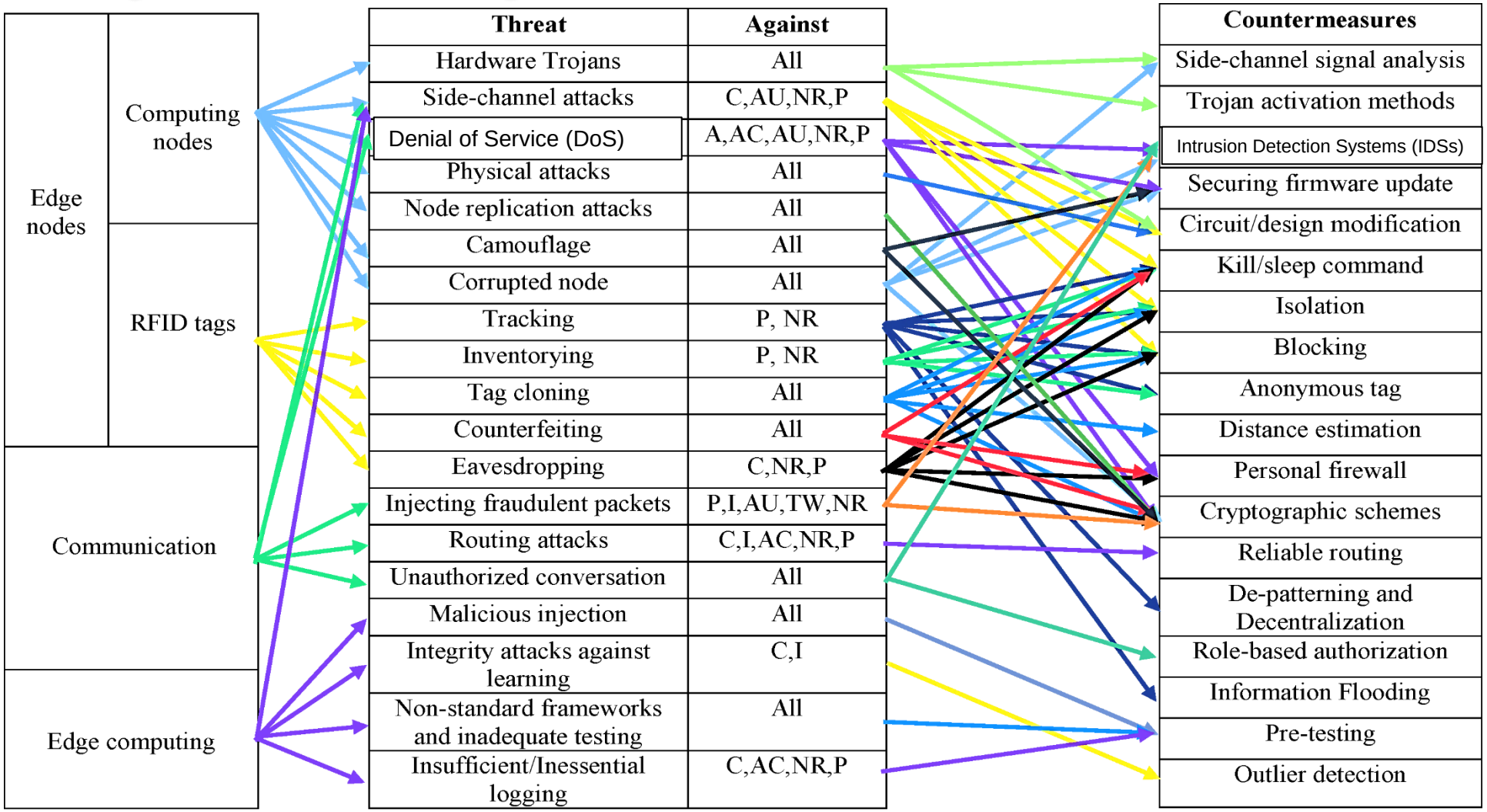
Source: https://www.healthcareitnews.com/news/new-ai-diagnostic-tool-knows-when-defer-human-mit-researchers-say

Different Attacks on a Typical Electronic System



Cybrsecurity Solution for IoT/CPS

IoT Cybersecurity - Attacks and Countermeasures



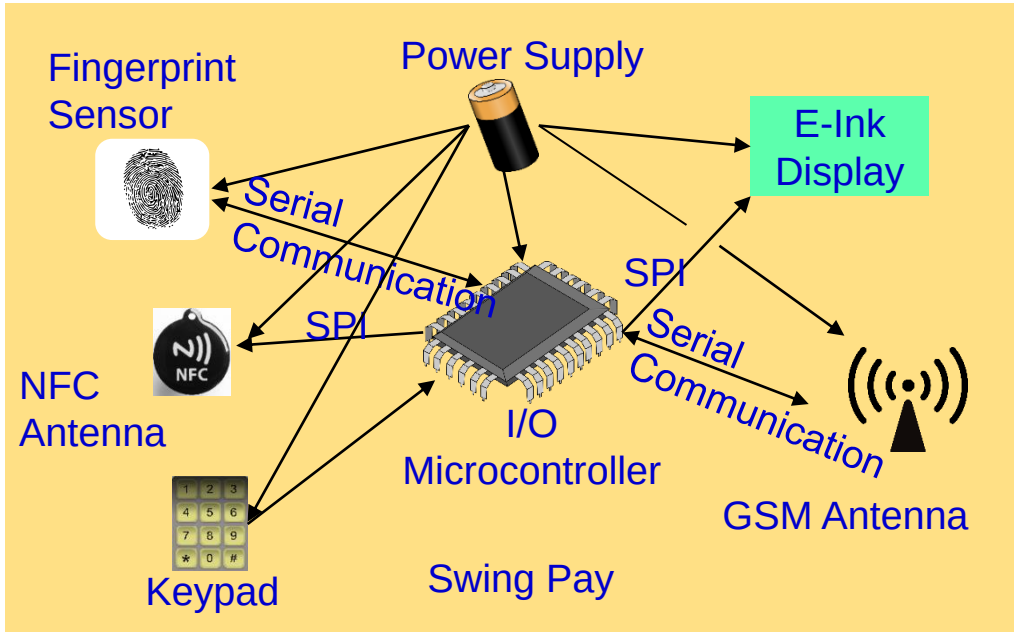
Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
Denial of Service (DoS)	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	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

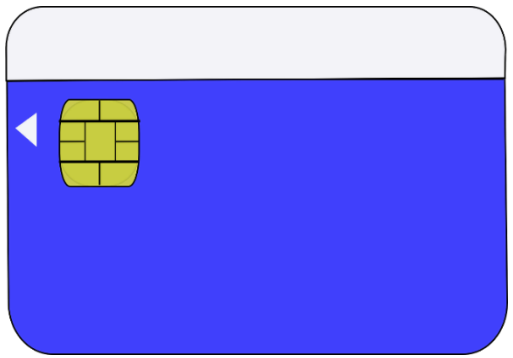
Countermeasures
Side-channel signal analysis
Trojan activation methods
Intrusion Detection Systems (IDSs)
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning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

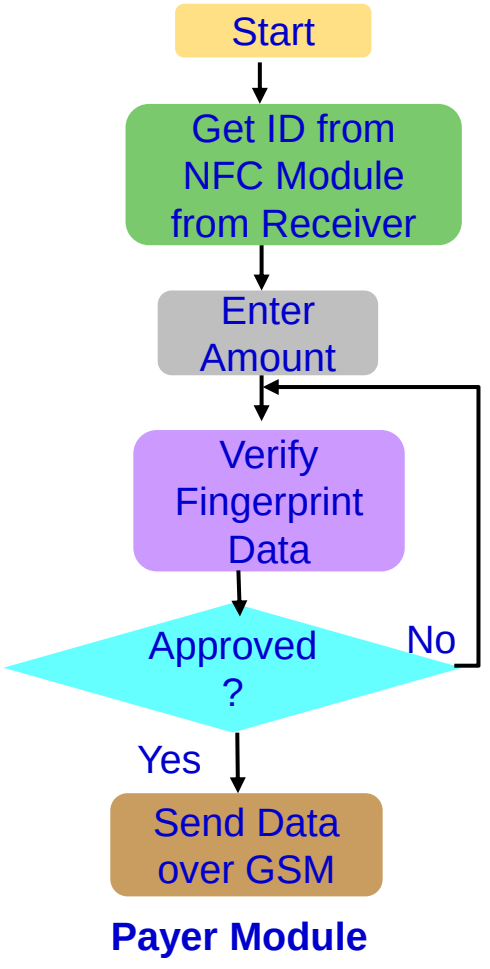
C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

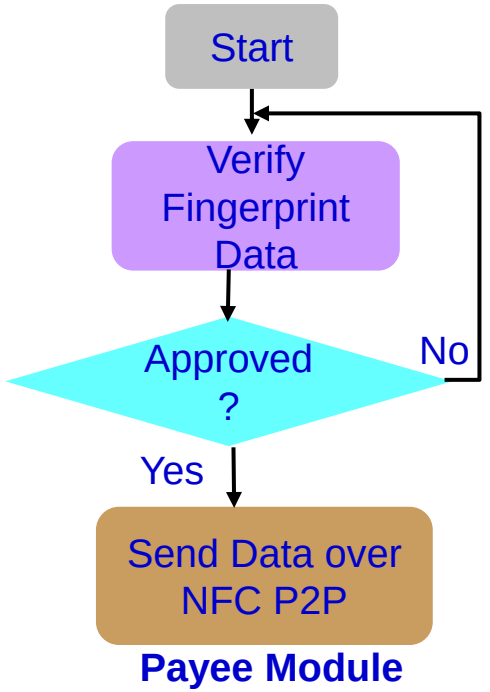
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

Our Swing-Pay: NFC Cybersecurity Solution



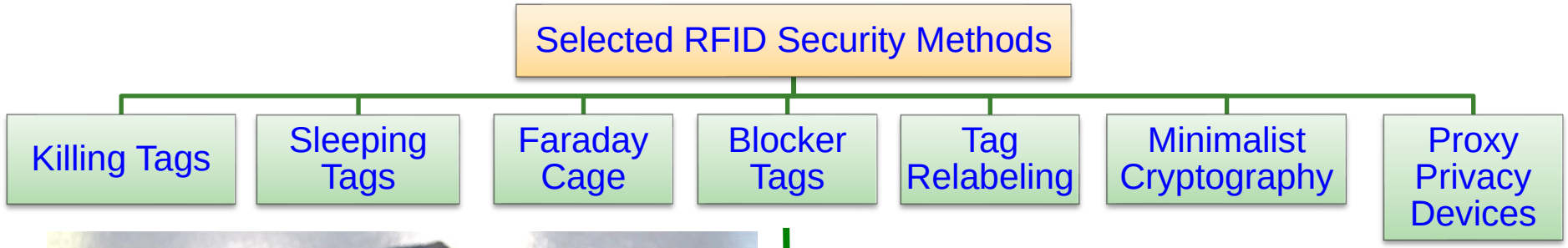




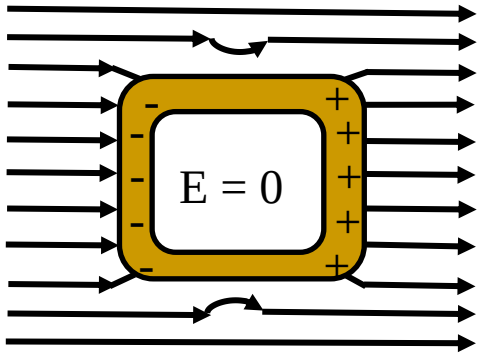


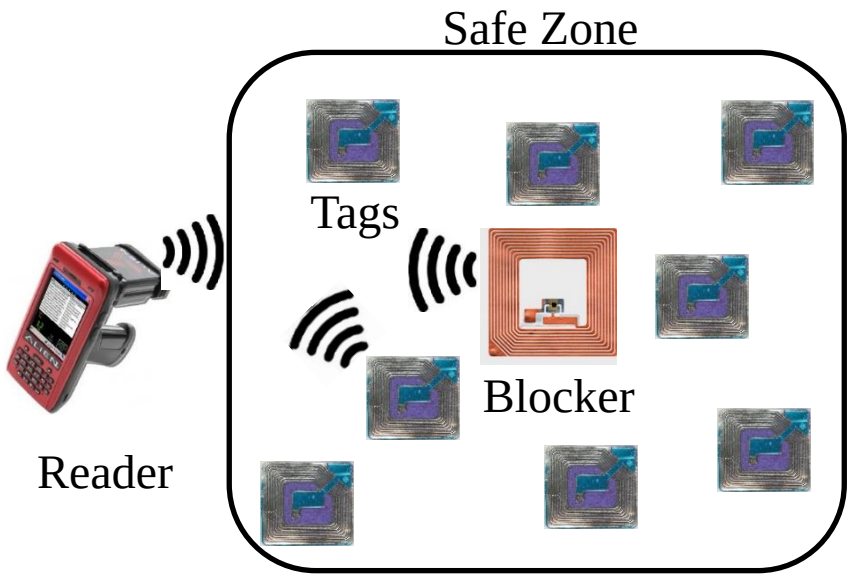
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

RFID Cybersecurity - Solutions



Faraday Cage

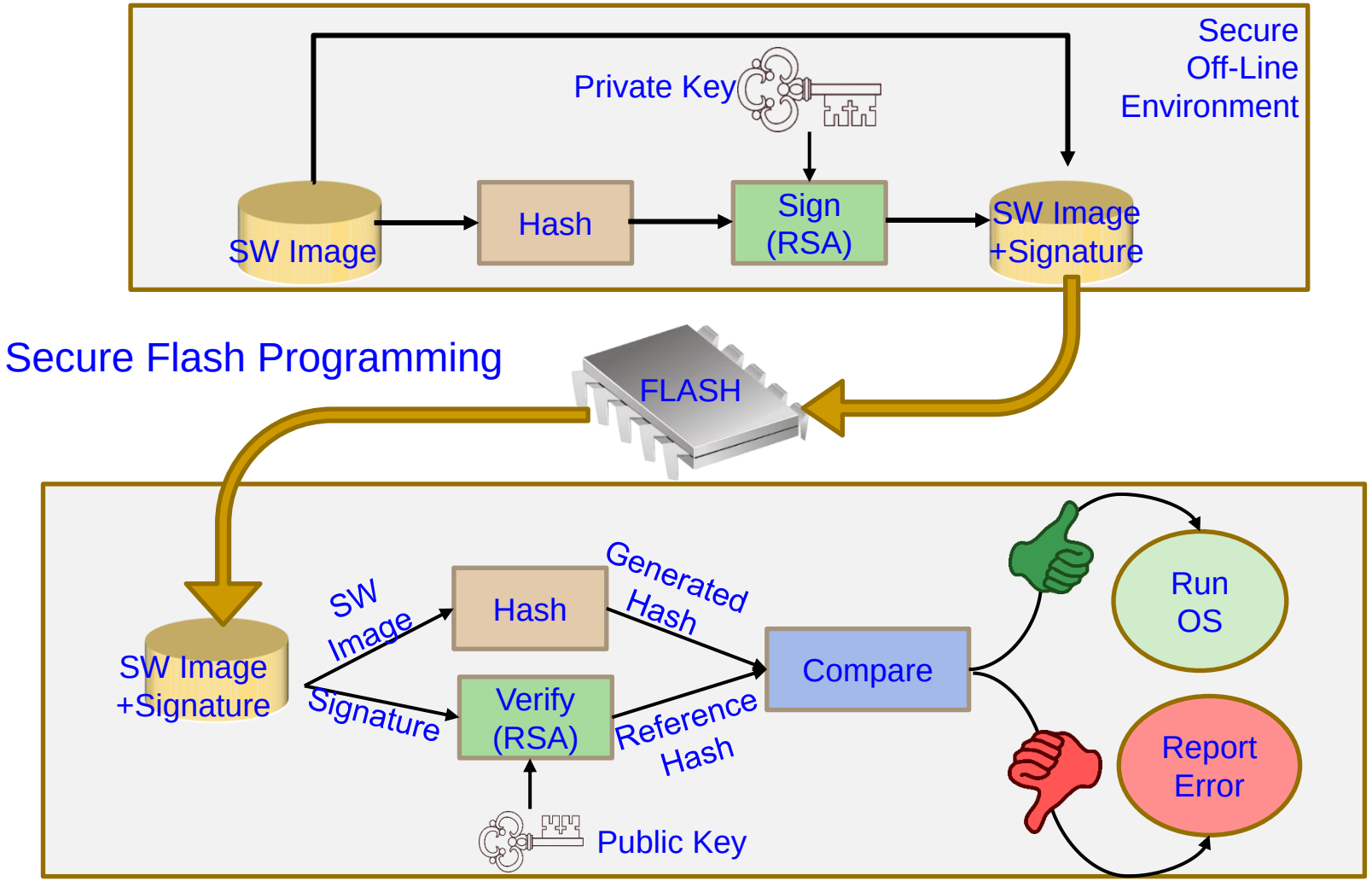




Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution



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

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

Nonvolatile / Harddrive Storage

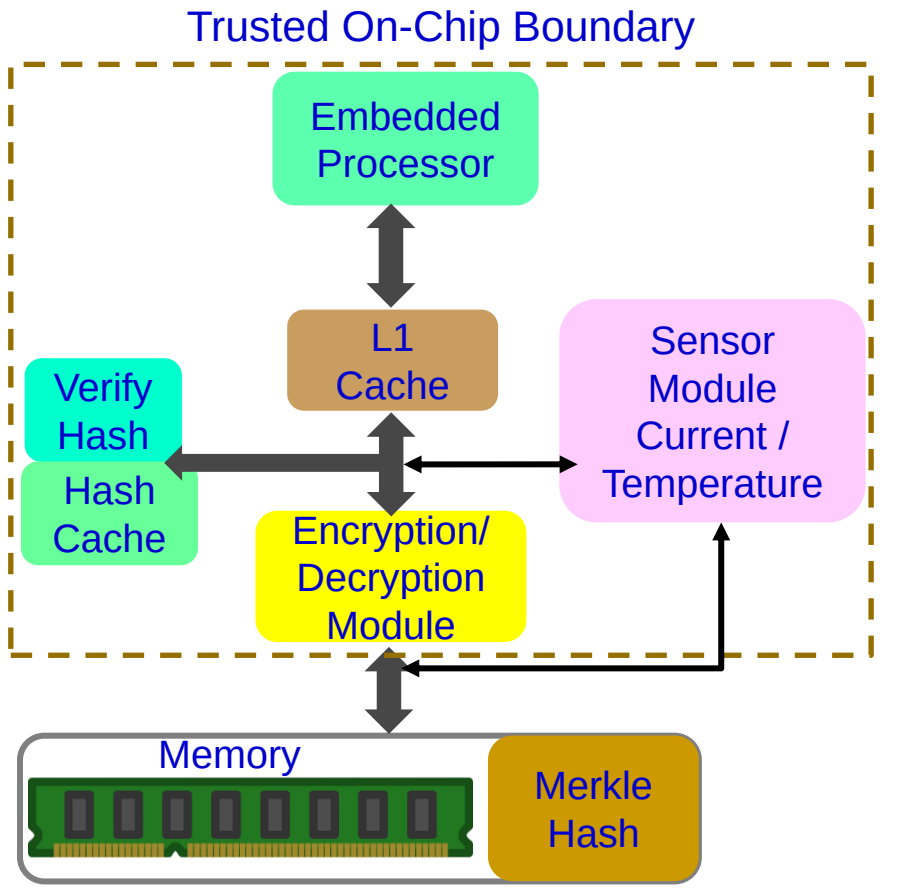
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

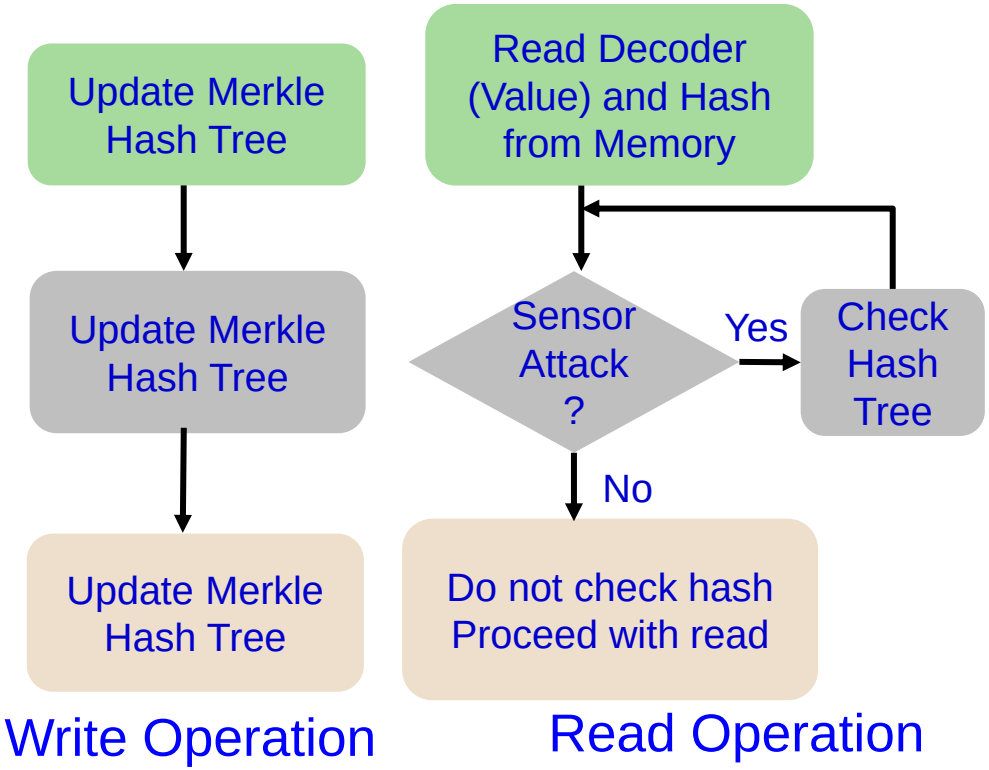
Some performance penalty due to increase in latency!

How Cloud storage changes this scenario?

Embedded Memory Security



On-Chip/On-Board Memory Protection

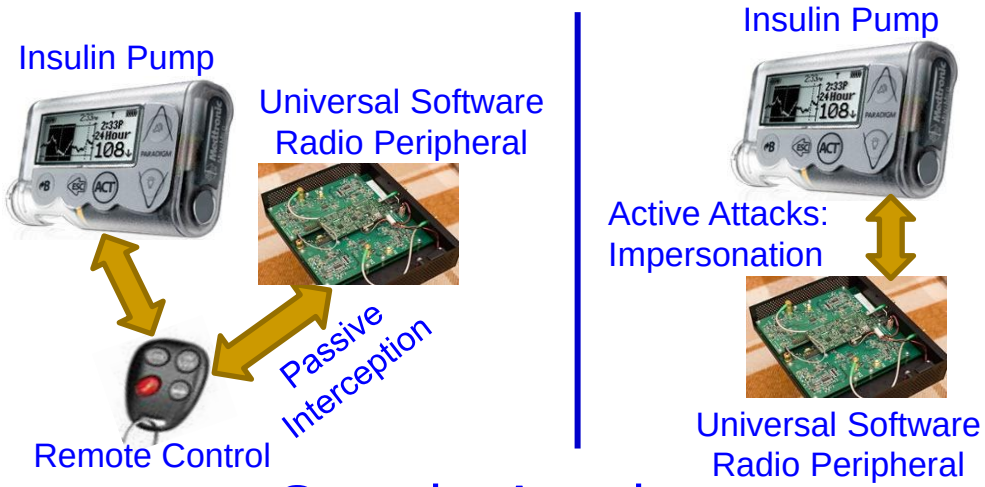


Memory integrity verification with 85% energy savings with minimal performance overhead.

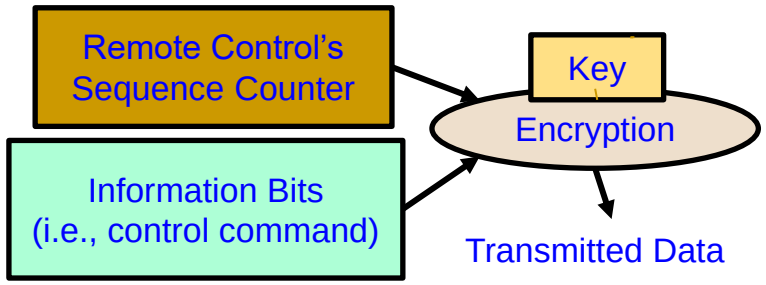
Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", *Springer Circuits, Systems, and Signal Processing Journal (CSSP)*, Volume 32, Issue 6, December 2013, pp. 2581--2604.

Smart Healthcare Cybersecurity

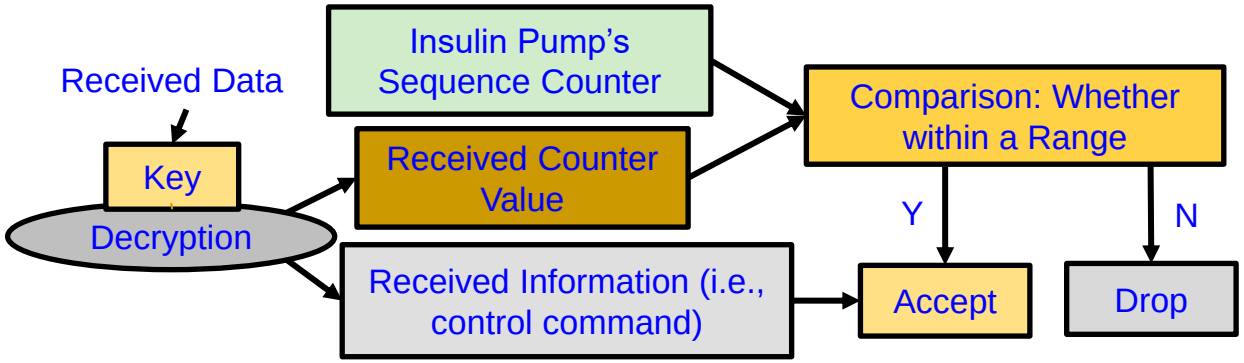
Insulin Delivery System



Security Attacks



Rolling Code Encoder in Remote Control



Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Drawbacks of Existing Cybersecurity Solutions

IoT/CPS Cybersecurity Solutions – Advantages and Disadvantages

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*, Vol 8, No. 1, Jan 2019, pp. 95--99.

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

IT Cybersecurity

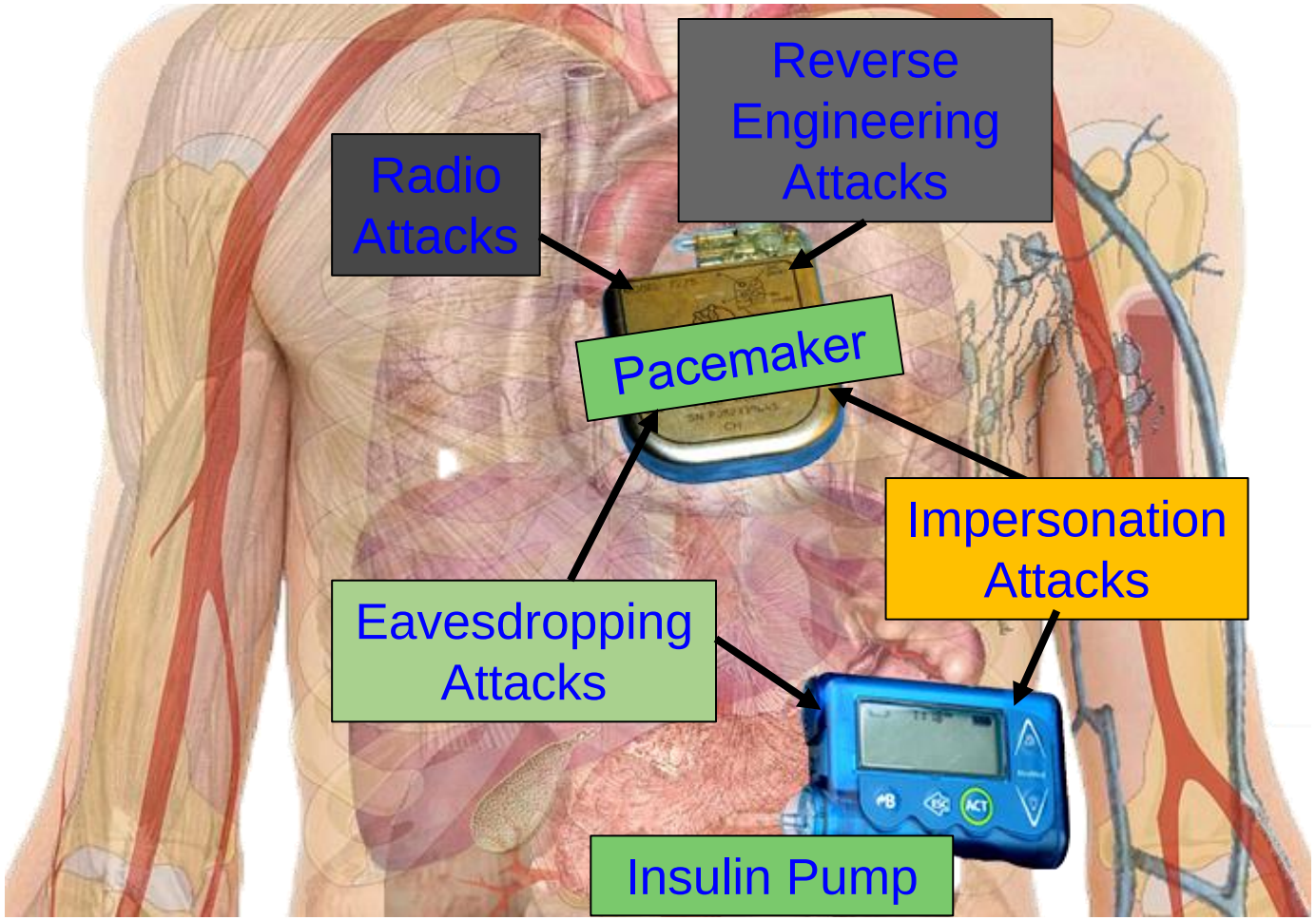
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

IoT Cybersecurity

- 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 Cybersecurity of Electronic Systems, IoT, CPS, needs Energy, and affects performance.

Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard

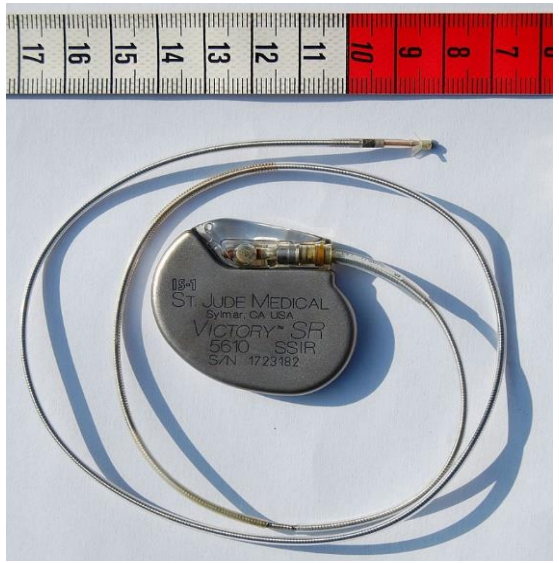


Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs):

→ Longer Battery life
→ Safer device
→ Smaller size
→ Smaller weight
→ Not much computational capability

H-CPS Cybersecurity 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: C. Camara, P. Peris-Lopeza, and J. 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 Cybersecurity - 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 cybersecurity issues.

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

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

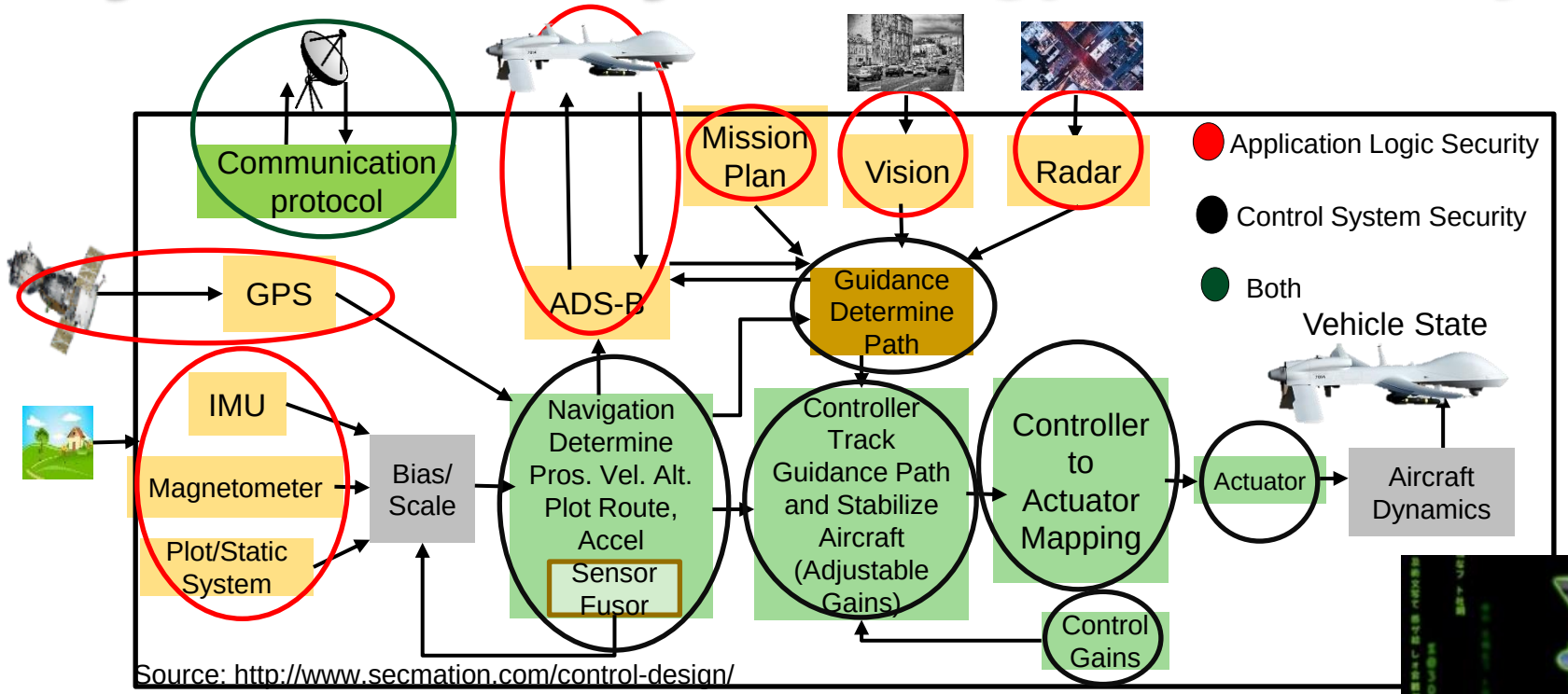
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

- 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 Cybersecurity – Latency Constrained

UAV Cybersecurity - Energy & Latency Constrained



Cybersecurity 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

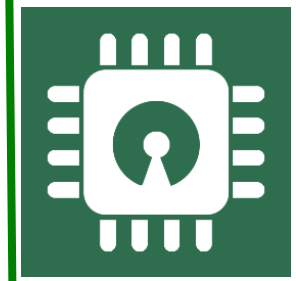
- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

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

Cybersecurity Attacks – Software Vs Hardware Based

Software Based

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



Hardware Based

- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
  - Hardware backdoors (e.g. Trojan)
  - Inducing faults
  - Electronic system tampering/ jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - Hardware counterfeiting

Source: Mohanty ICCE Panel 2018

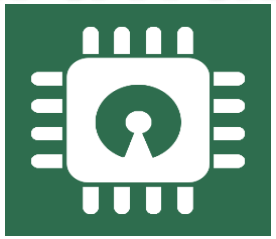
Cybersecurity Solutions – Software Vs Hardware Based

Software Based

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

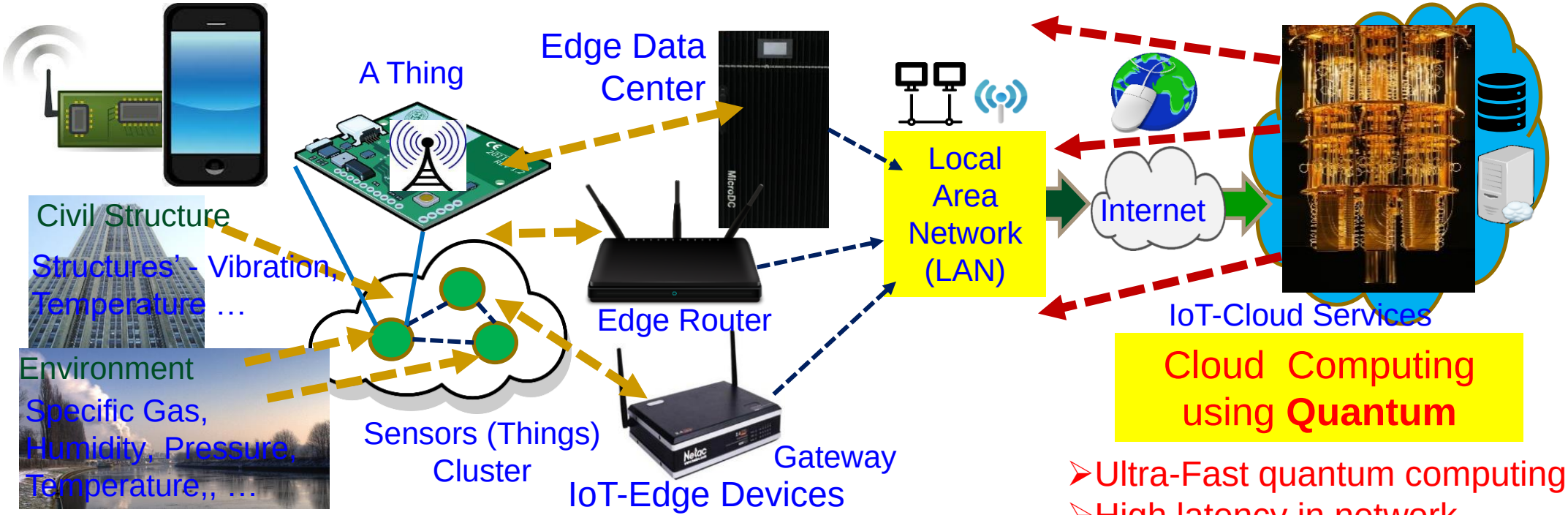
Source: Mohanty ICCE Panel 2018

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

Cybersecurity Nightmare ← Quantum Computing



In-Sensor/End-Device Computing

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

Edge Computing

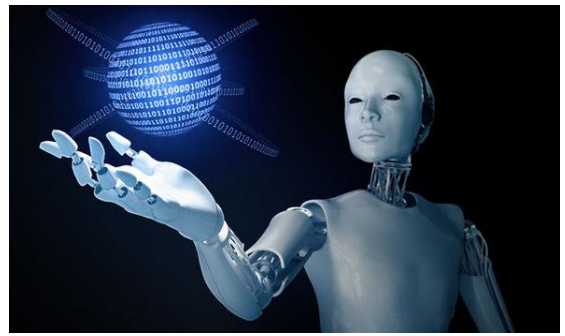
- Less computational resource
- Minimal latency in network
- Lightweight security

Cloud Computing using Quantum

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

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

Security-by-Design (SbD) – The Principle



IoT/CPS Design – Multiple Objectives

Non-recurring Design Cost

Recurring Operational Cost

Energy Consumption, Battery Life

Ethics, Safety

Security, Privacy, IP Rights

Smart Cities
Vs
Smart Villages

Performance, Latency

Intelligence

Source: Mohanty ICCE 2019 Keynote

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)

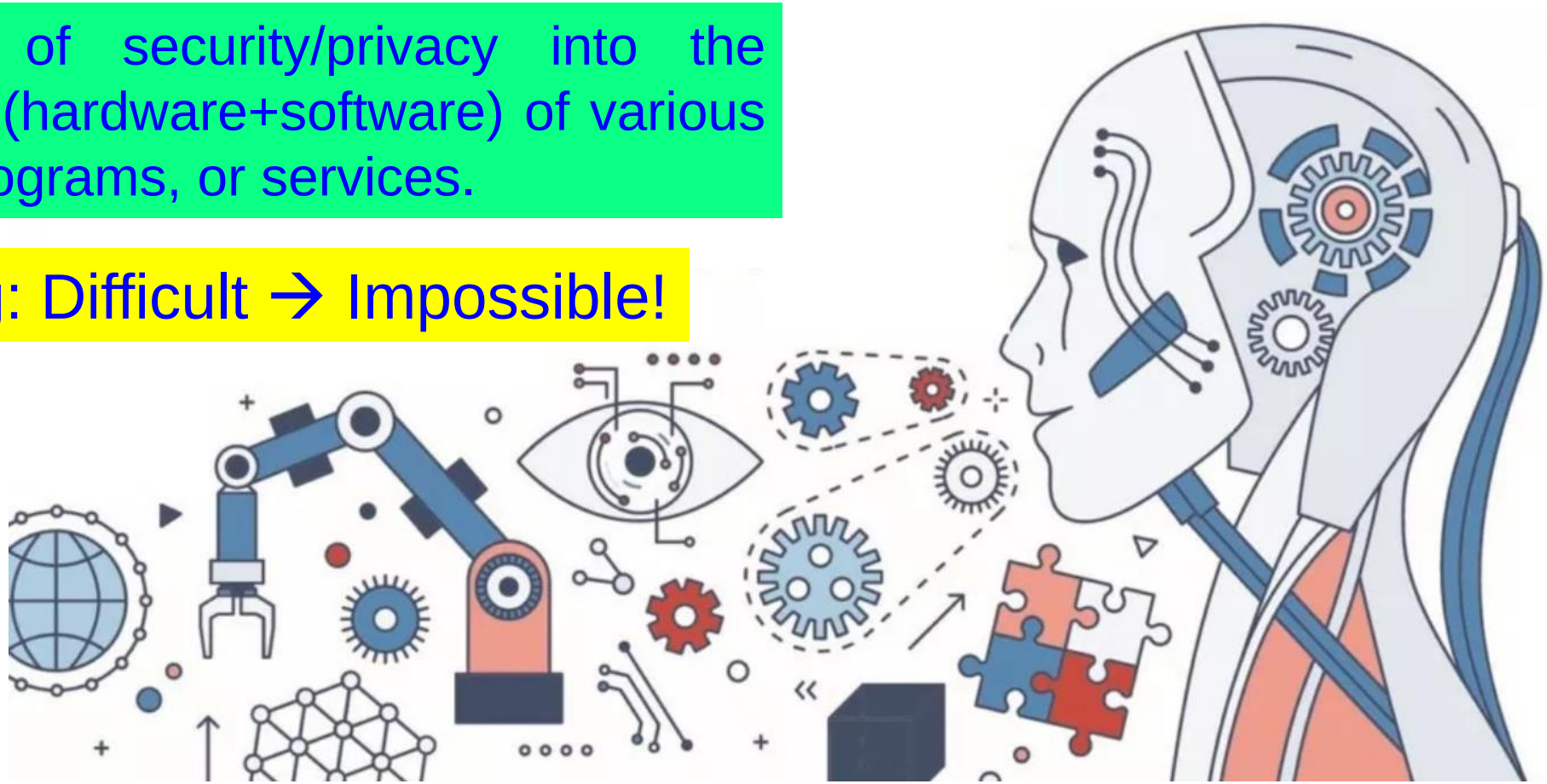
- GDPR makes Privacy by Design (PbD) a legal requirement

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)

7 Fundamental Principles

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

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

CEI Tradeoffs for Smart Electronic Systems

Security of systems and data.

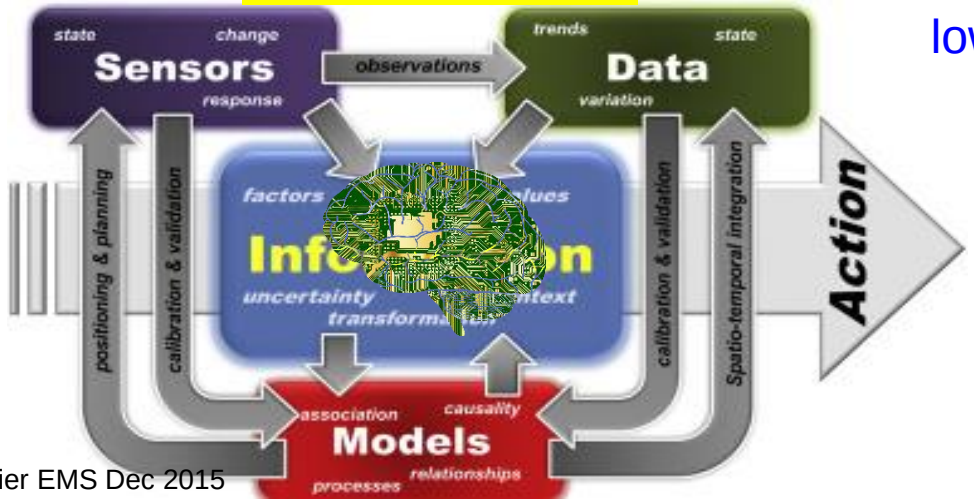
Cybersecurity

Energy

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

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

Intelligence



Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Source: Mohanty iSES 2018 Keynote

Hardware-Assisted Security (HAS)

- 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 (HAS): Security/Protection provided by the hardware: for information being processed by an electronic system, for hardware itself, and/or for the system.

Hardware-Assisted Security (HAS)

- Hardware-Assisted Security: Security provided by hardware for:
  (1) information being processed,
  (2) hardware itself,
  (3) overall system

Privacy by Design (PbD)

Security/Secure by Design (SbD)

- Additional hardware components used for cybersecurity.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

Bluetooth Hardware Security

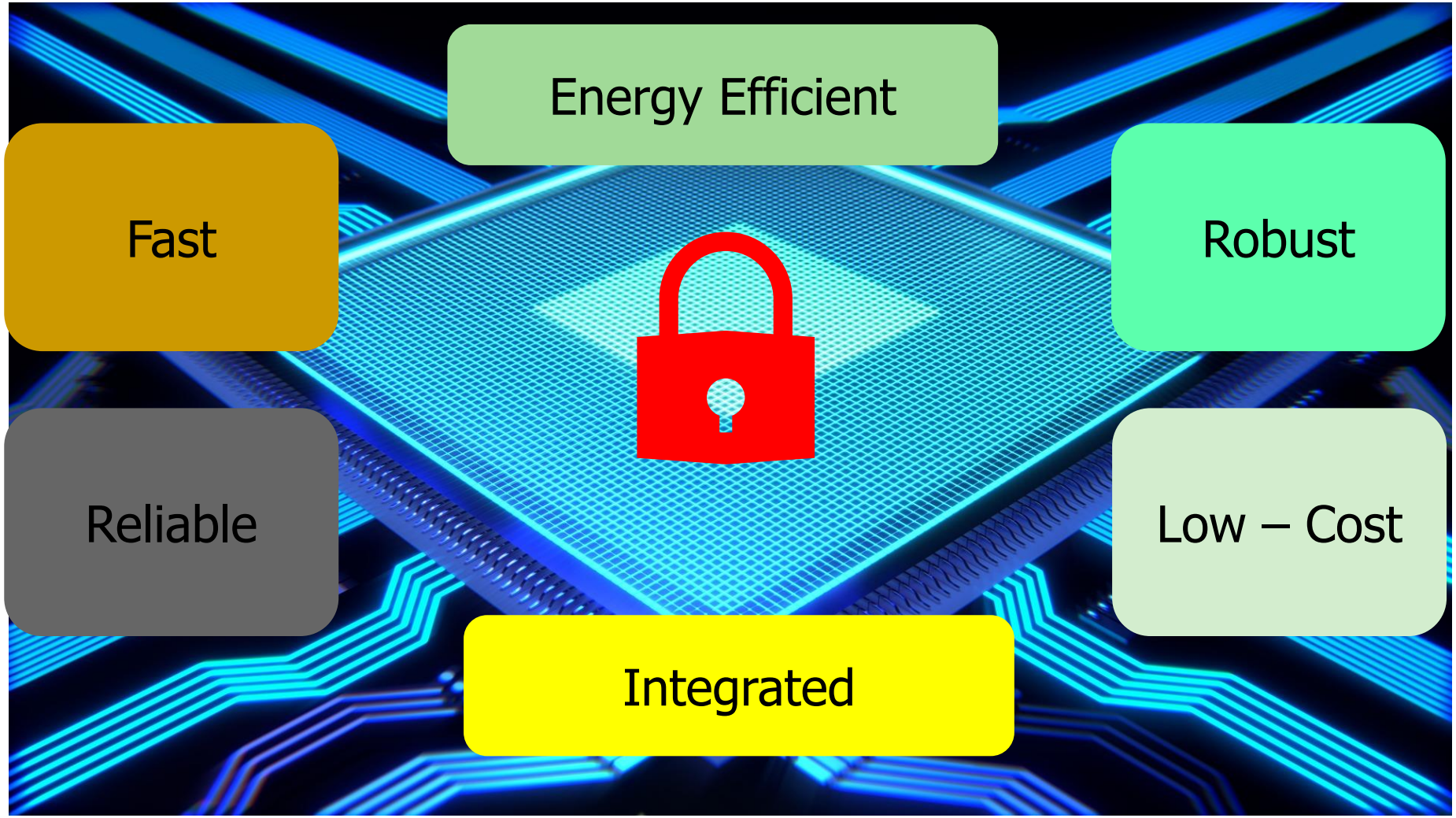
Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

Source: E. Kougianos, S. P. Mohanty, and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", Special Issue on Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia, Elsevier International Journal on Computers and Electrical Engineering, Vol 35, No. 2, Mar 2009, pp. 339-358..

Hardware Assisted Security (HAS)



Secure SoC Design: Alternatives

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

Secure SoC - Alternatives

Development of hardware amenable algorithms.

Building efficient VLSI architectures.

Hardware-software co-design for security, power, and performance tradeoffs.

SoC design for cybersecurity, power, and performance tradeoffs.

Secure SoC: Different Design Alternatives

New CMOS sensor with security.

New data converters with security.

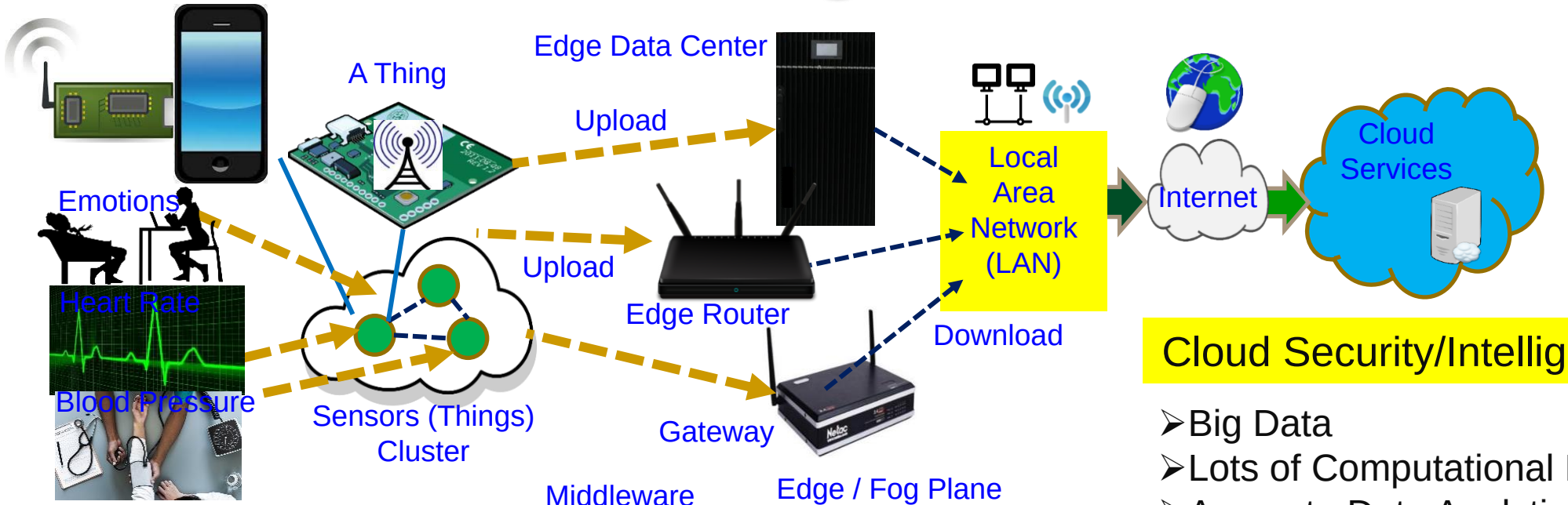
Independent security and AI processing cores.

New instruction set architecture for RISC to support security at micro-architecture level.

Trustworthy Electronic System

- A selective attributes of electronic system to be trustworthy:
  - It must maintain integrity of information it is processing.
  - It must conceal any information about the computation performed through any side channels such as power analysis or timing analysis.
  - It must perform only the functionality it is designed for, nothing more and nothing less.
  - It must not malfunction during operations in critical applications.
  - It must be transparent only to its owner in terms of design details and states.
  - It must be designed using components from trusted vendors.
  - It must be built/fabricated using trusted fabs.

CPS – IoT-Edge Vs IoT-Cloud



Cloud Security/Intelligence

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

End Security/Intelligence

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

Edge Security/Intelligence

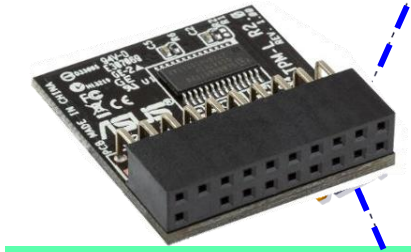
- Less Data
- Less Computational Resource
- Less Accurate Data Analytics
- Rapid Response

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

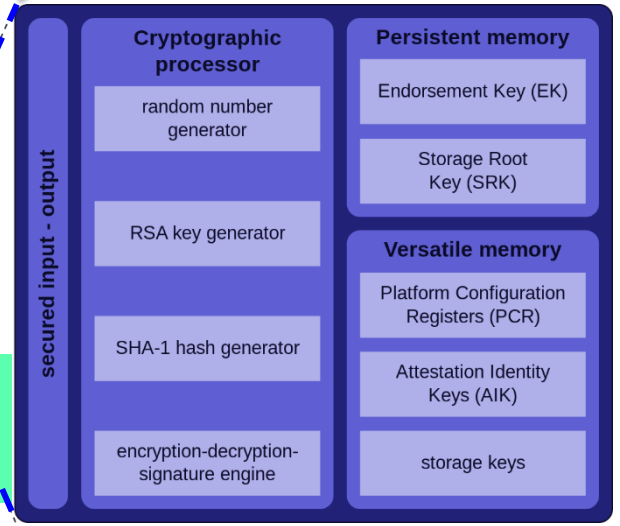
Heavy-Duty ML is more suitable for smart cities

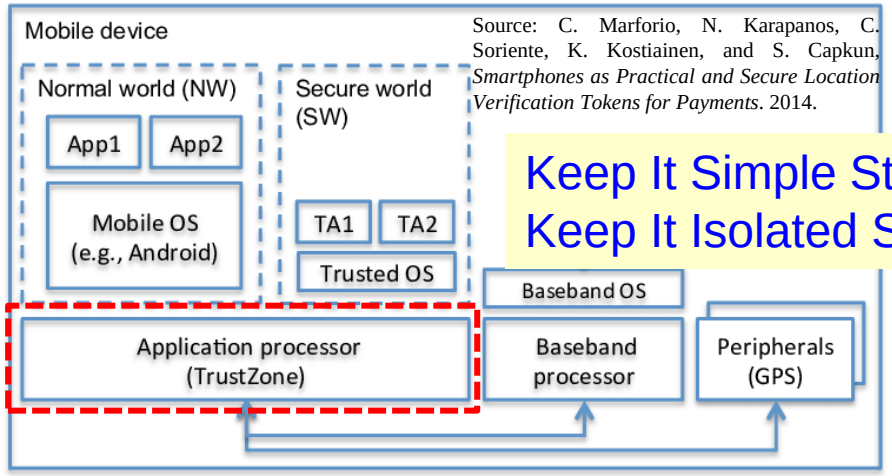
Hardware Cybersecurity Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



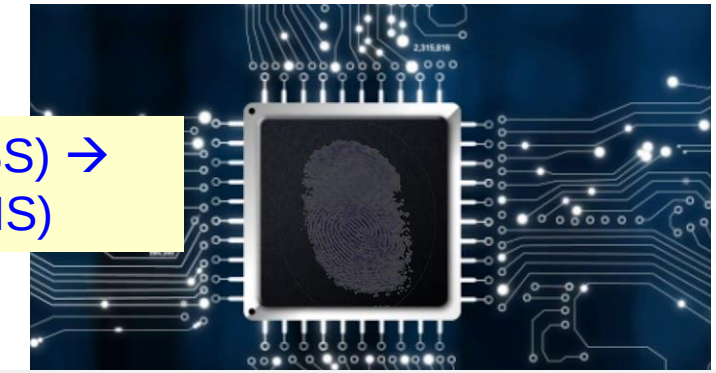
Trusted Platform Module (TPM)





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

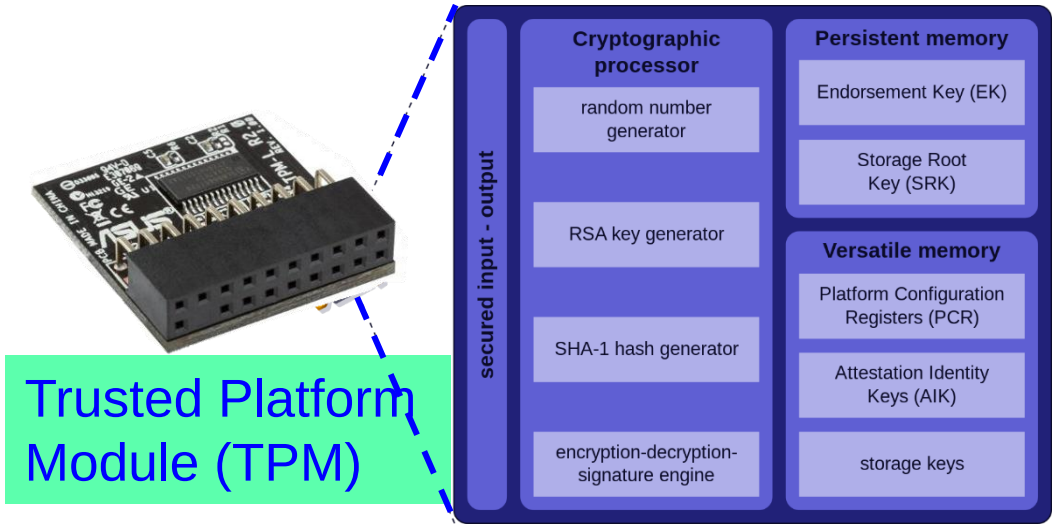
Keep It Simple Stupid (KISS) →
Keep It Isolated Stupid (KIIS)

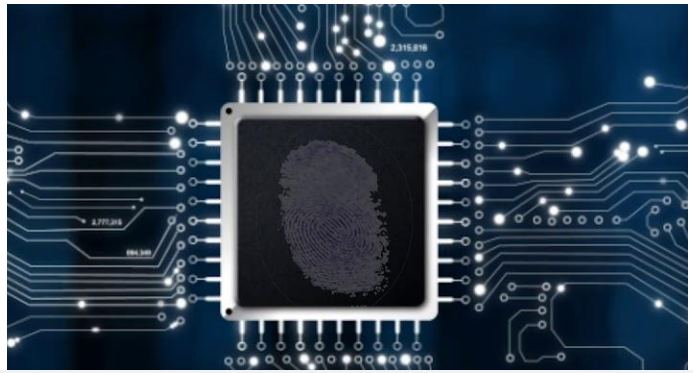


Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

PUF versus TPM





Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

TPM:

1) The set of specifications for a secure crypto- processor and
2) The implementation of these specifications on a chip

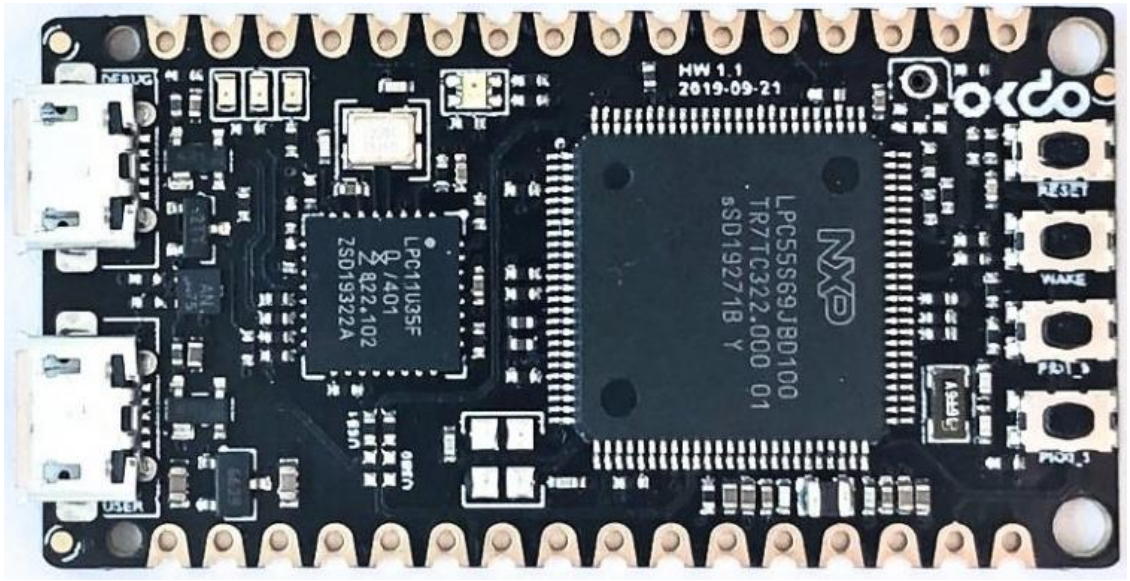
PUF:

1) Based on a physical system
2) Generates random output values

Why PUFs?

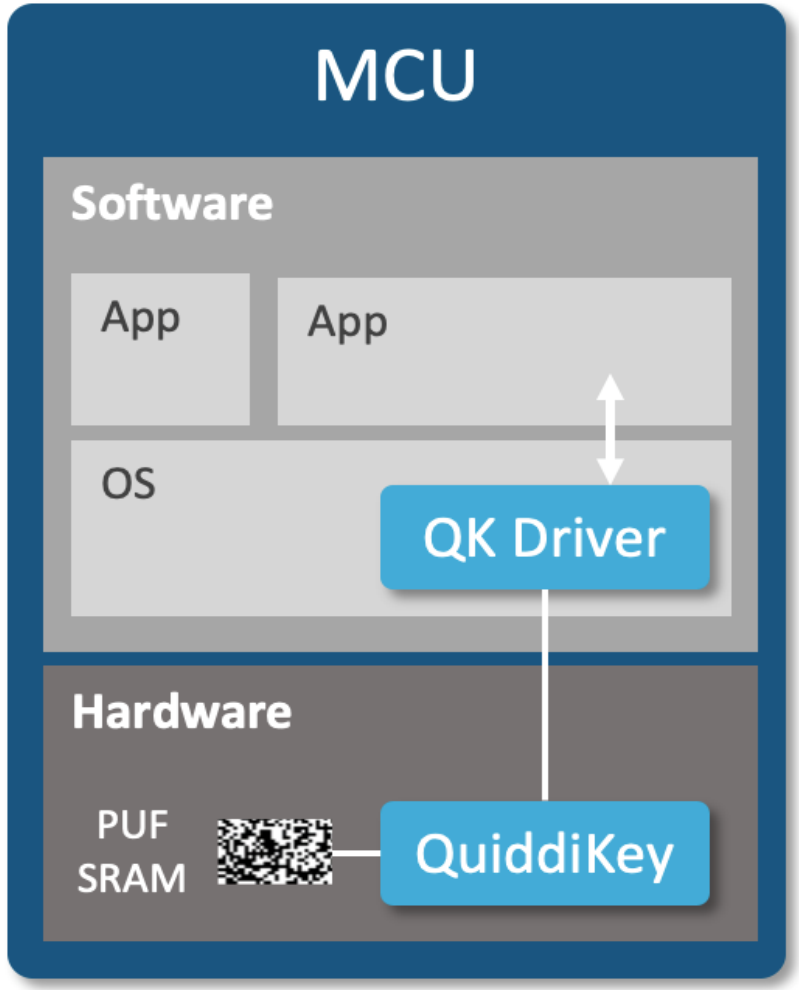
- Hardware-assisted security.
- Key not stored in memory.
- Not possible to generate the same key on another module.
- Robust and low power consuming.
- Can use different architectures with different designs.

PUF Hardware Modules



Source: https://asvin.io/physically-unclonable-function-setup/

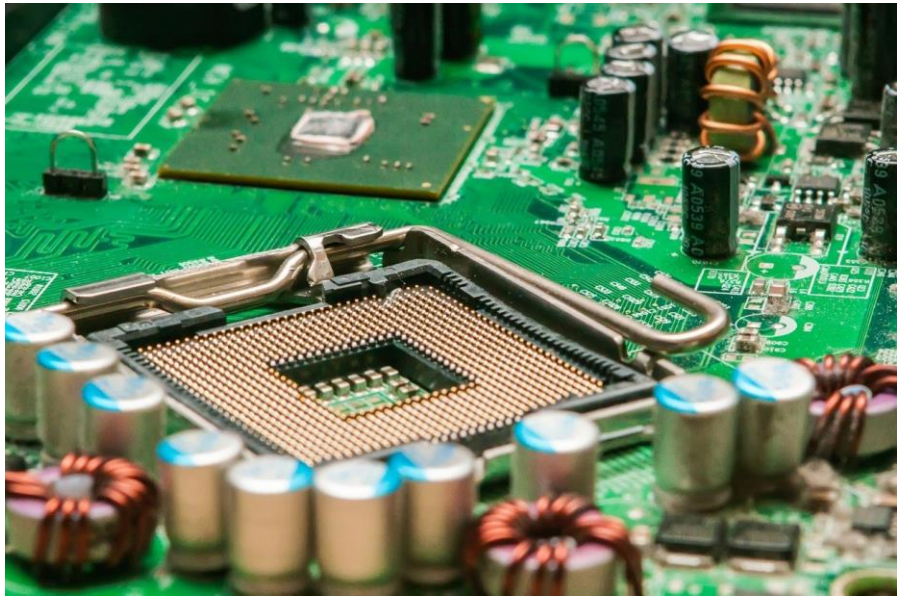
- This development board is based on LPC55S69xx microcontroller from NXP.
- The microcontroller contains onboard PUF using dedicated SRAM.



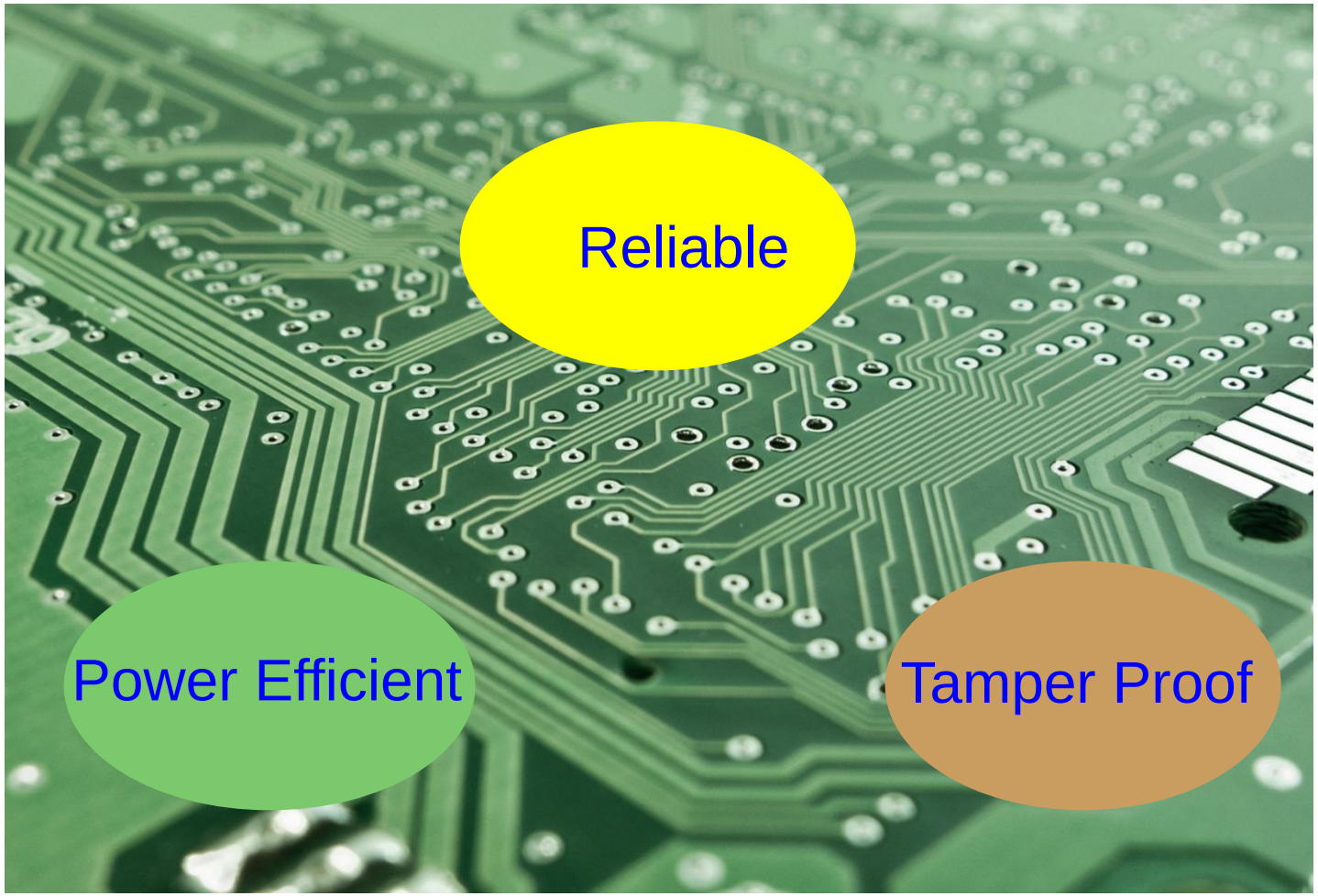
Source: https://www.intrinsic-id.com/products/quiddikey/

PUF: A Hardware-Assisted Security Primitive

- PUF has a Challenge as an Input and Response as an Output
- Response output from the PUF design will be unique for the challenge input on that PUF design
- Arbiter PUF and Ring Oscillator PUF are the most widely used PUF designs for IoT applications
- Delay based PUF designs support higher number of Challenge Response pairs (CRP)

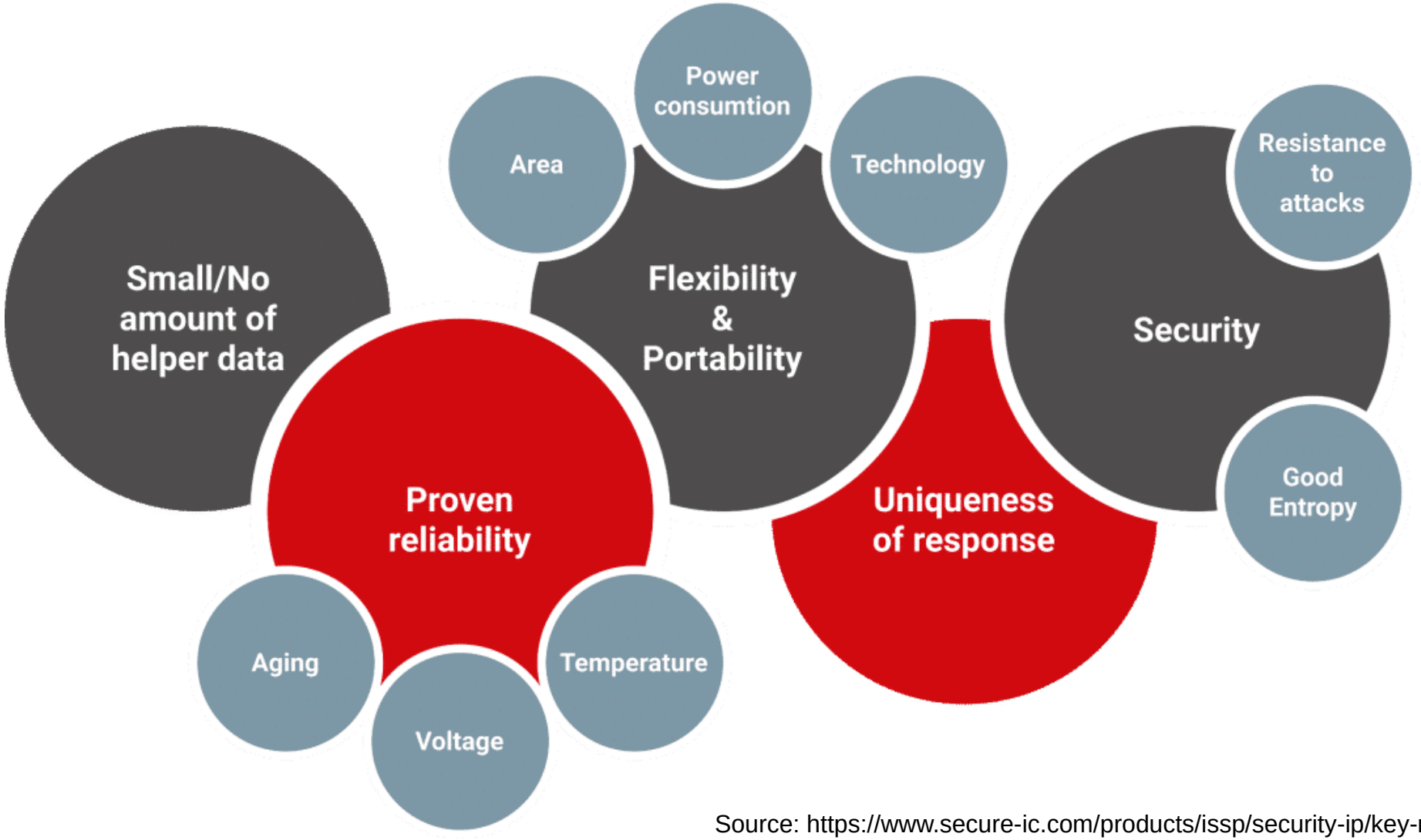


PUF: Advantages



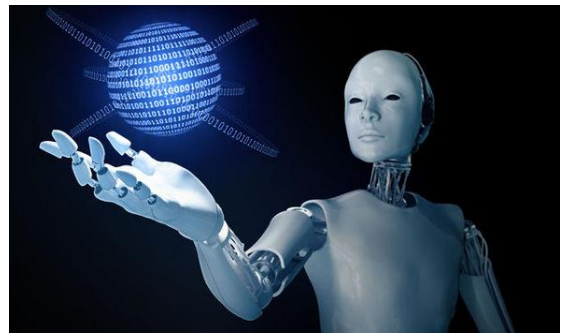
- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device authentication

PUF: Advantages

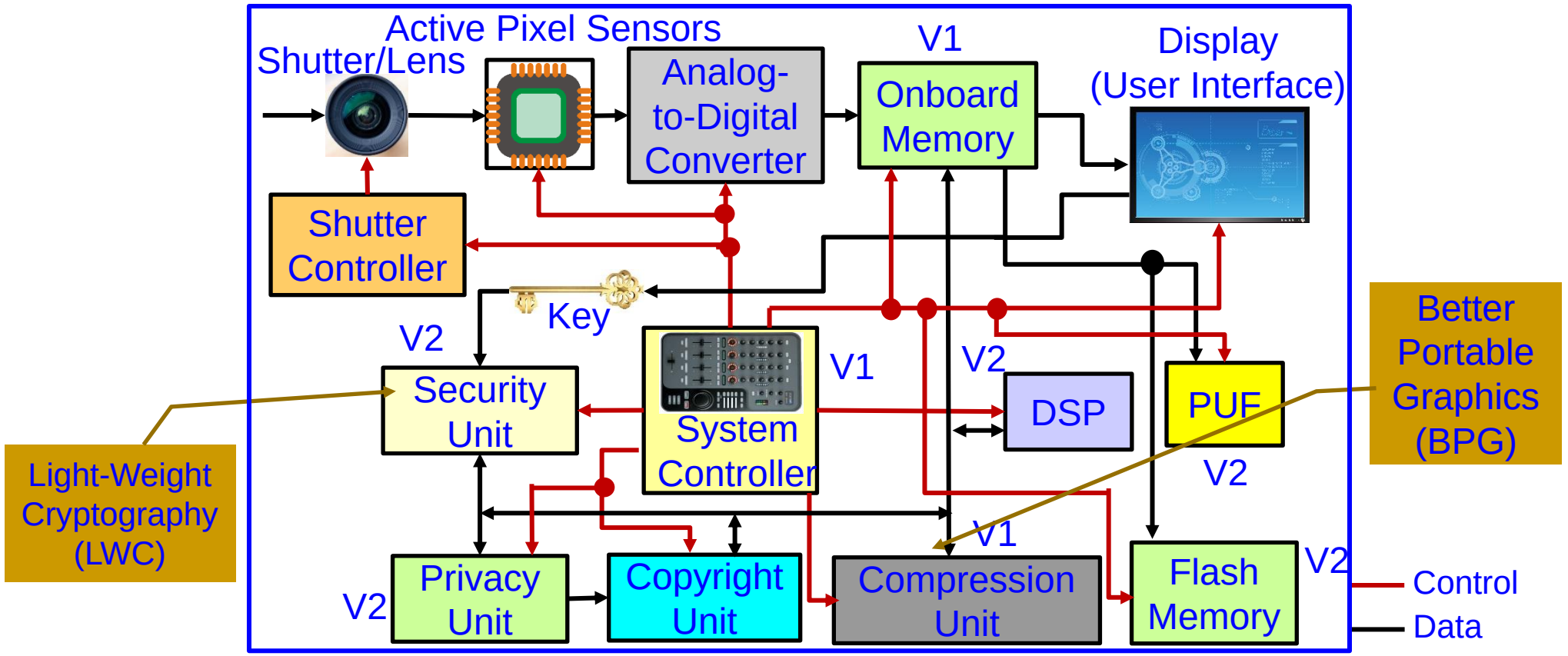


Source: https://www.secure-ic.com/products/issp/security-ip/key-management/puf-ip/

Security-by-Design (SbD) – Specific Examples



Secure Digital Camera (SDC) – My Invention

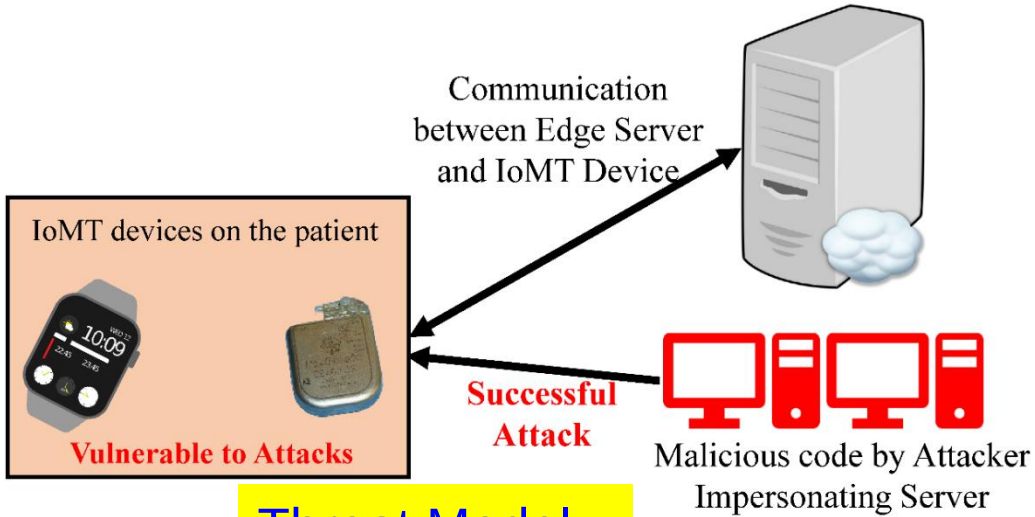


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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

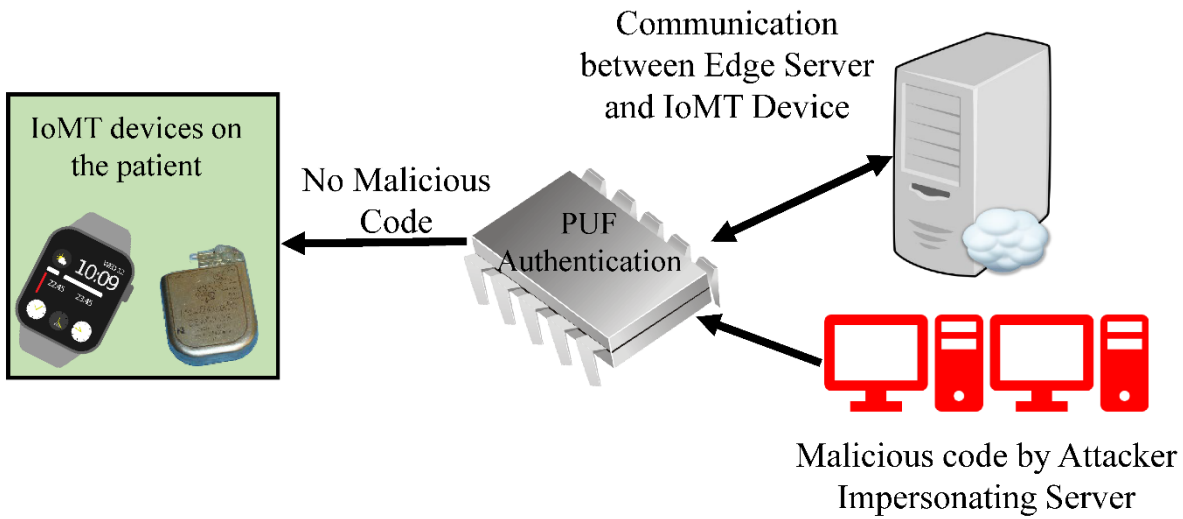
Source: S. P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management", *Elsevier Journal of Systems Architecture (JSA)*, Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

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



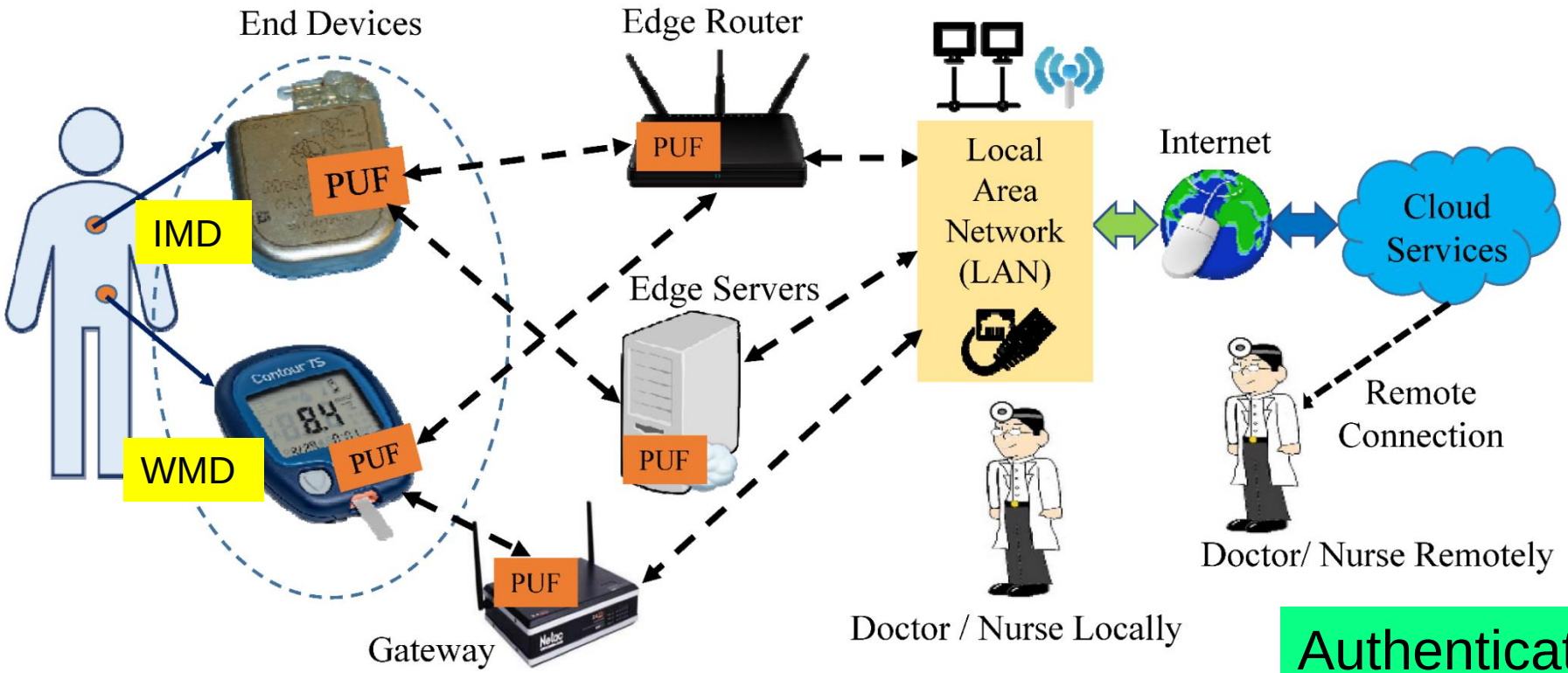
Threat Model

PUF based Solution



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.

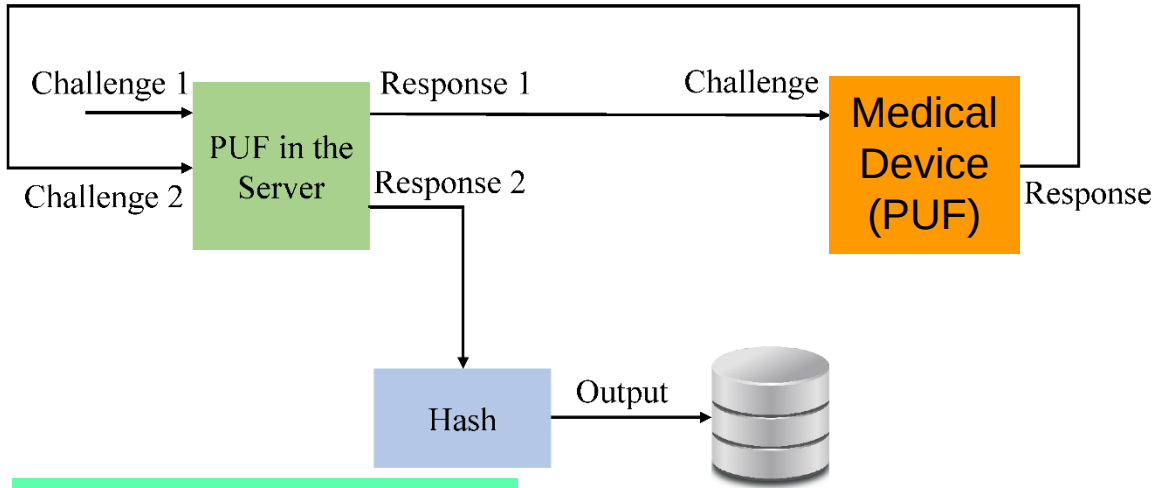
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

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

IoMT Security – Our Proposed PMsec

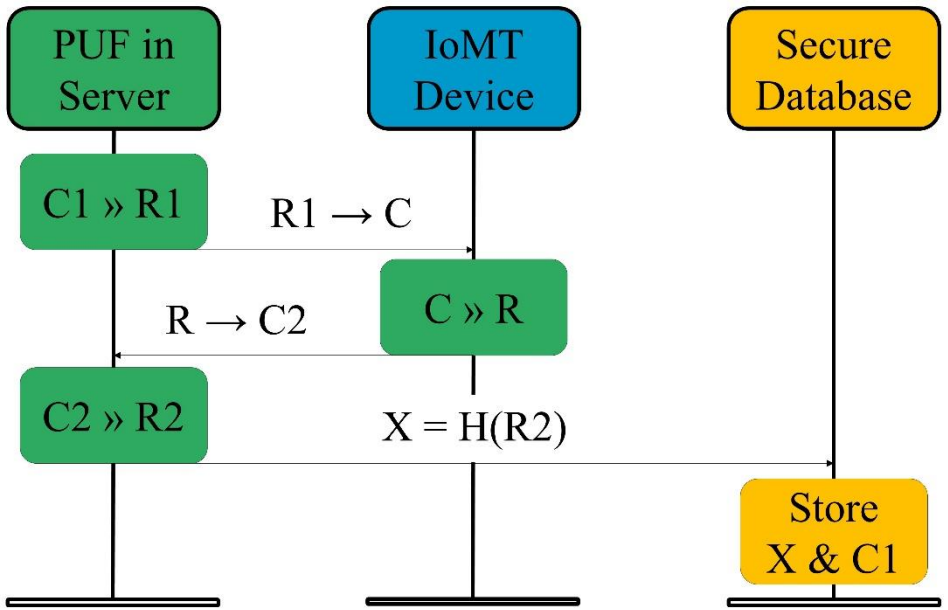


Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

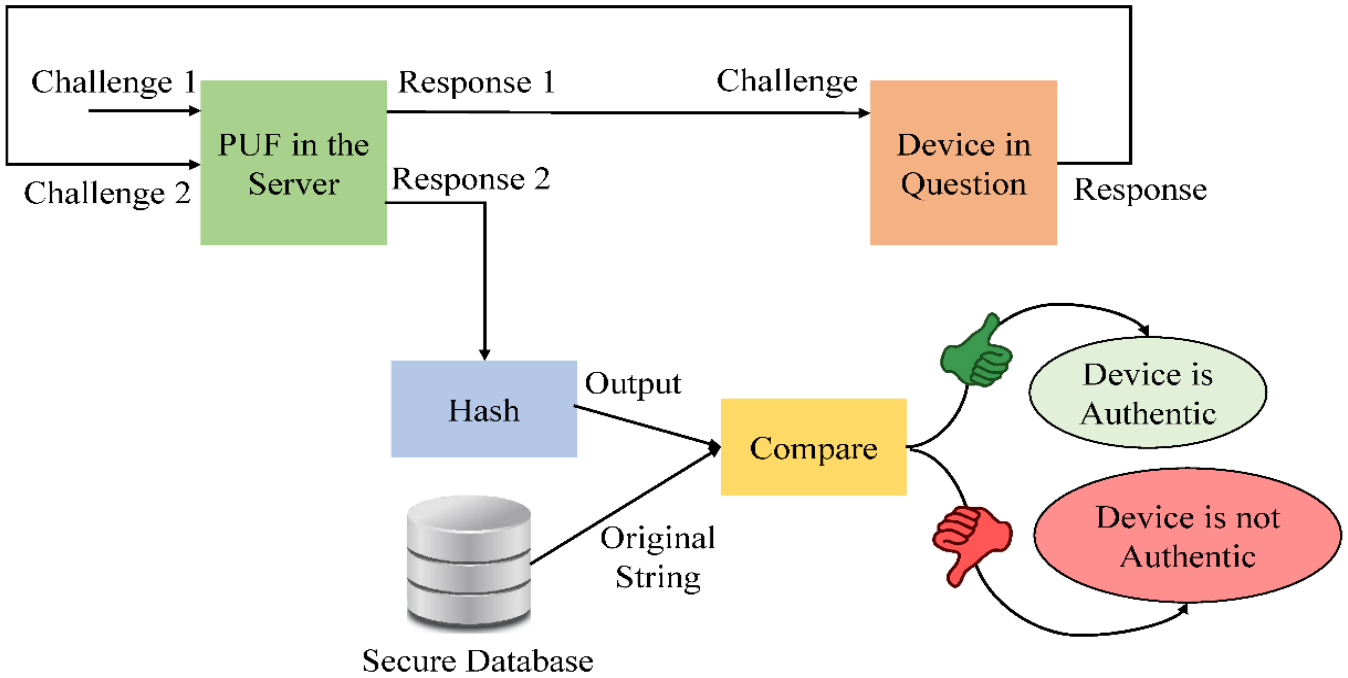


PUF Security Full Proof:

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

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

IoMT Security – Our Proposed PMsec

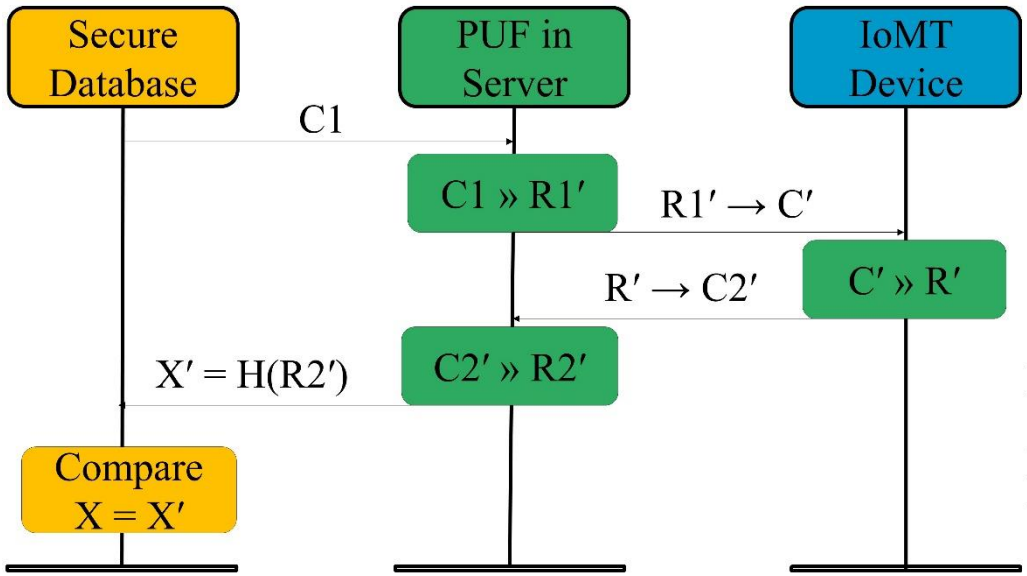


Authentication Phase

At the Doctor

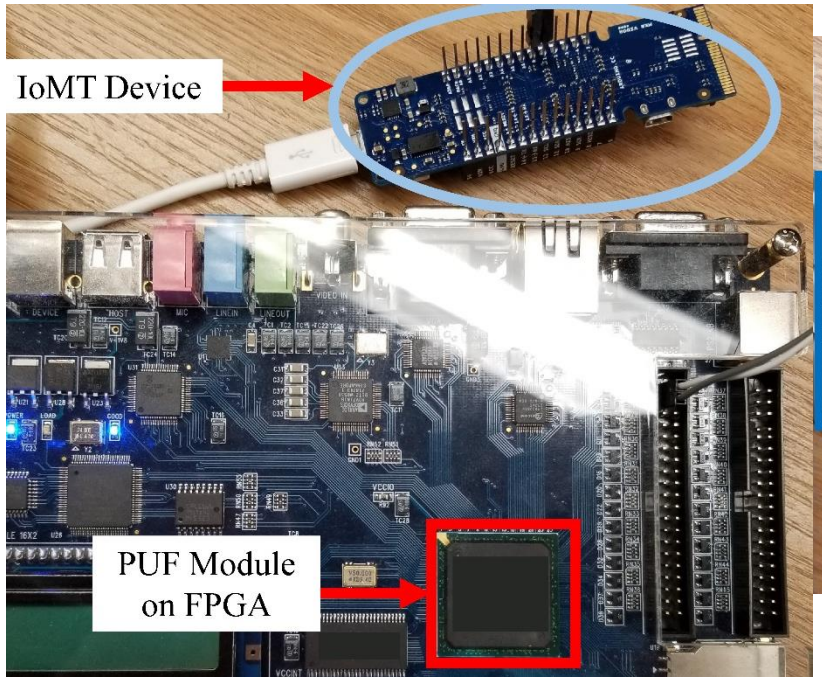
- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



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

IoMT Security – Our Proposed PMsec



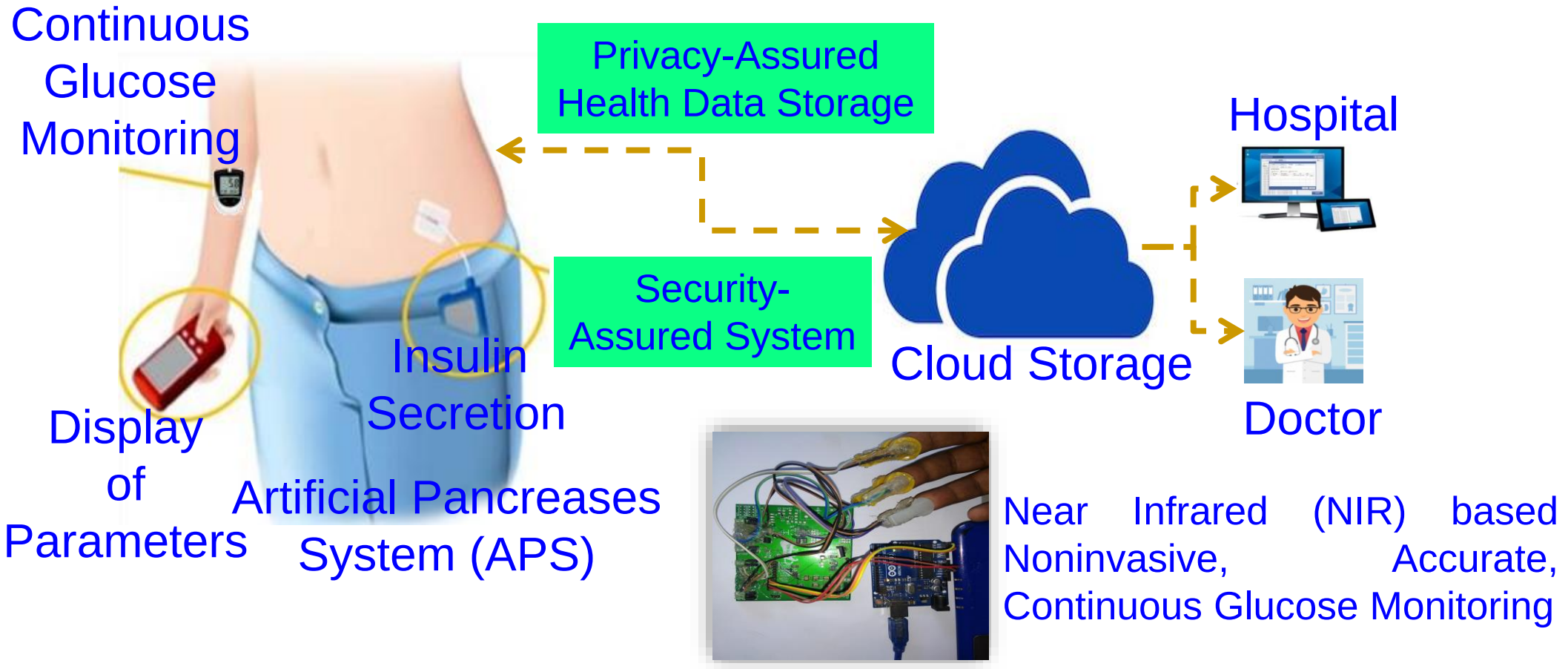
Average Power Overhead – 200 μW

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

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

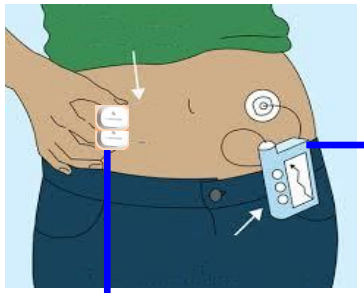
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics*, Vol 65, No 3, Aug 2019, pp. 388--397.

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



iGLU Insulin Delivery Subsystem (PUF)

Secure-iGLU Controller (PUF)

Edge Datacenter or Cloud Datacenter (CRPs from PUFs of Devices)

iGLU Glucose-Level Monitoring Subsystem (PUF)

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

iGLU Device (IoMT Node)

PUF

Challenge Response Table

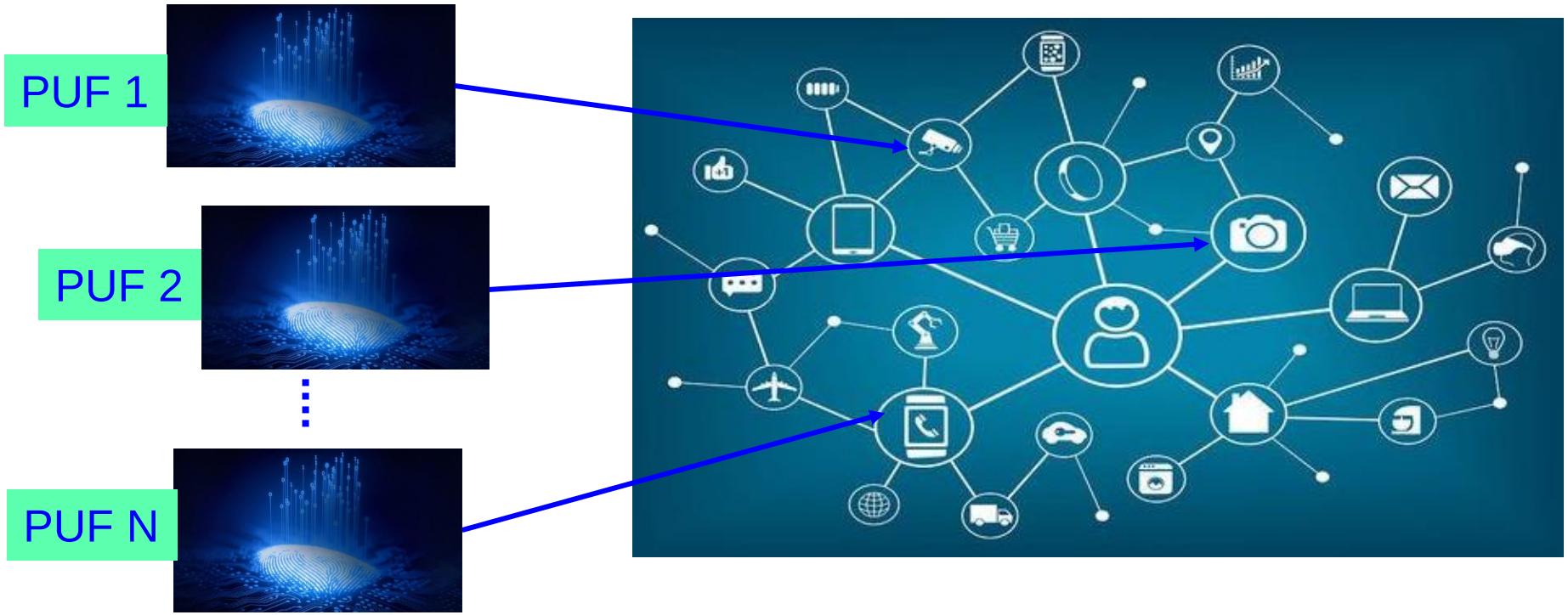
Challenges	Responses Ri
100101100	11010110
100101001	101001010
010111001	110111101

Secure-iGLU Controller (PUF)

Match ?

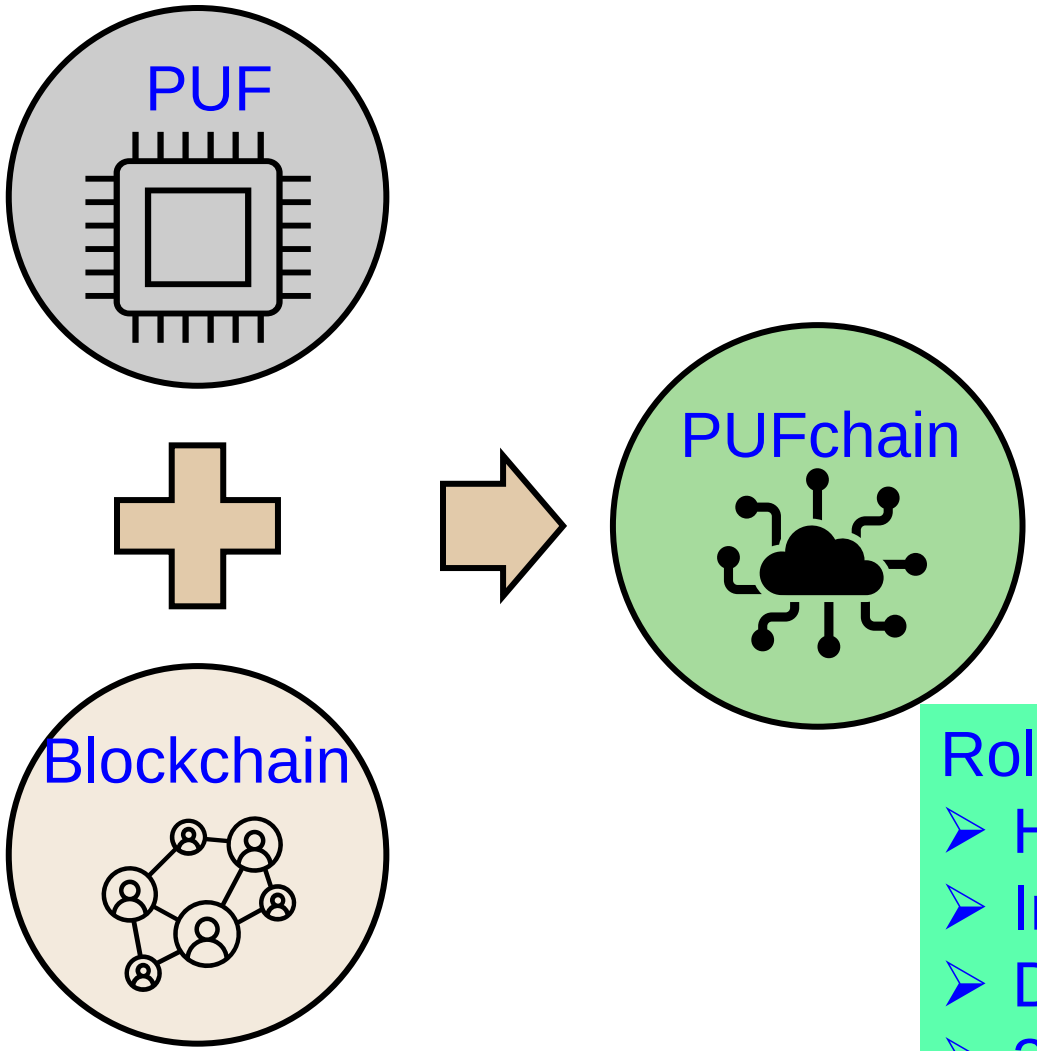
Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

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



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

PUFchain – The Big Idea



Blockchain Technology is integrated with Physically Unclonable Functions as PUFchain by storing the PUF Key into immutable Blockchain

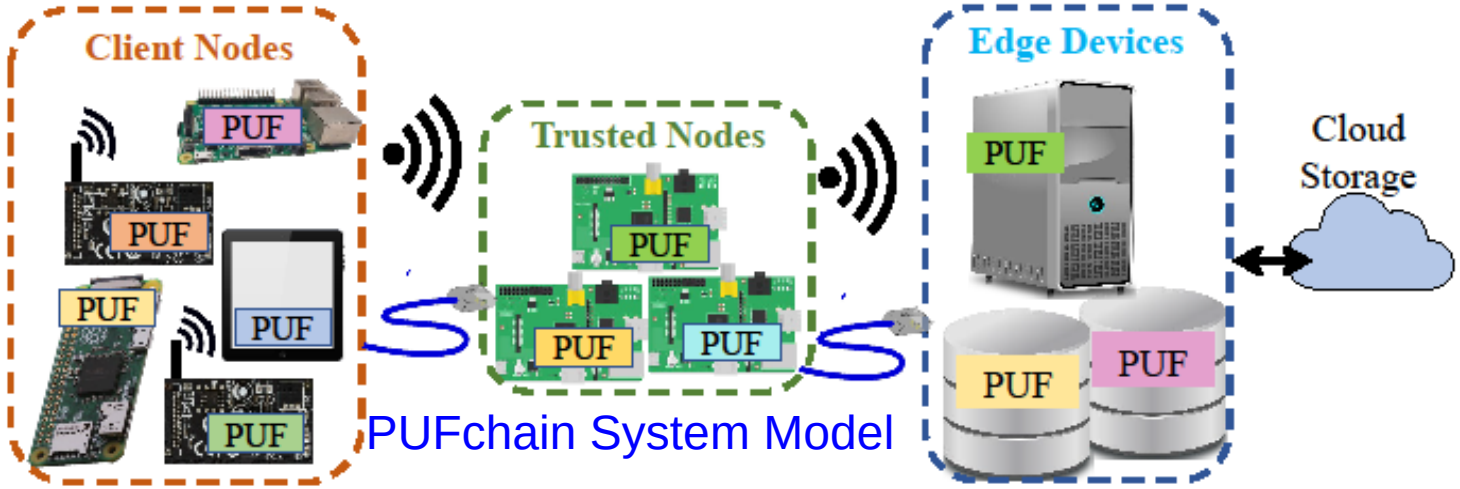
Roles of PUF:

- Hardware Accelerator for Blockchain
- Independent Authentication
- Double-Layer Protection
- 3 modes: PUF, Blockchain, PUF+Blockchain

Our PUFchain – 3 Variants

Research Works	Distributed Ledger Technology	Focus Area	Security Approach	Security Primitive	Security Principle
PUFchain	Blockchain	IoT / CPS (Device and Data)	Proof of Physical Unclonable Function (PUF) Enabled Authentication	PUF + Blockchain	Hardware Assisted Security (HAS) or Security-by-Design (SbD)
PUFchain 2.0	Blockchain	IoT/CPS (Device and Data)	Media Access Control (MAC) & PUF Based Authentication	PUF + Blockchain	Hardware Assisted Security (HAS) or Security-by-Design (SbD)
PUFchain 3.0	Tangle	IoT/CPS (Device and Data)	Masked Authentication Messaging (MAM)	PUF + Tangle	Hardware Assisted Security (HAS) or Security-by-Design (SbD)

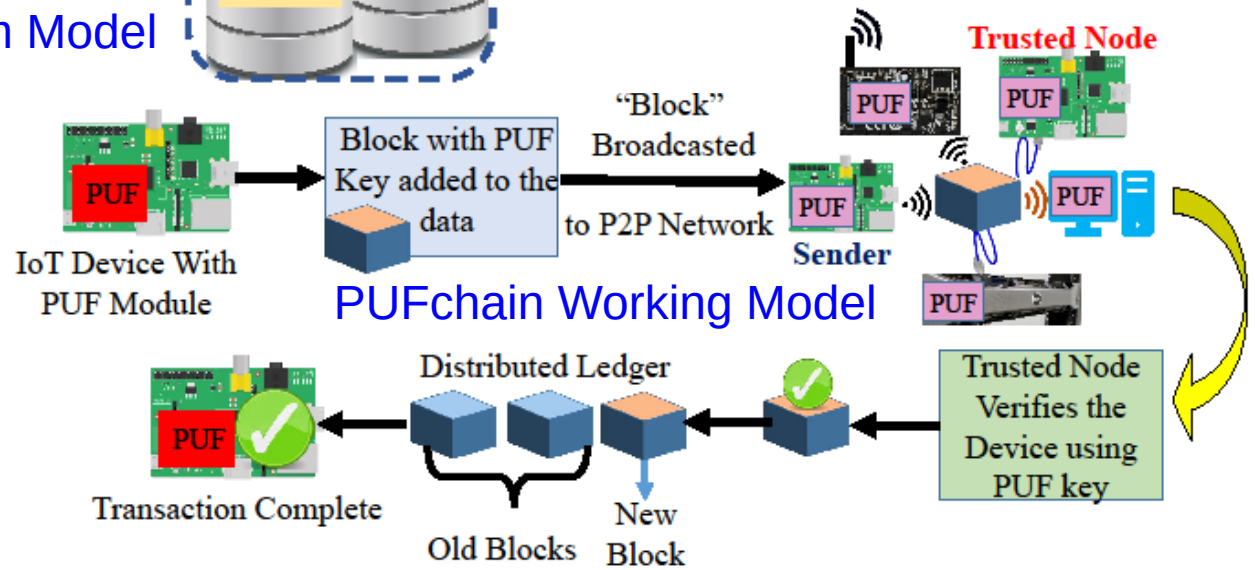
PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

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

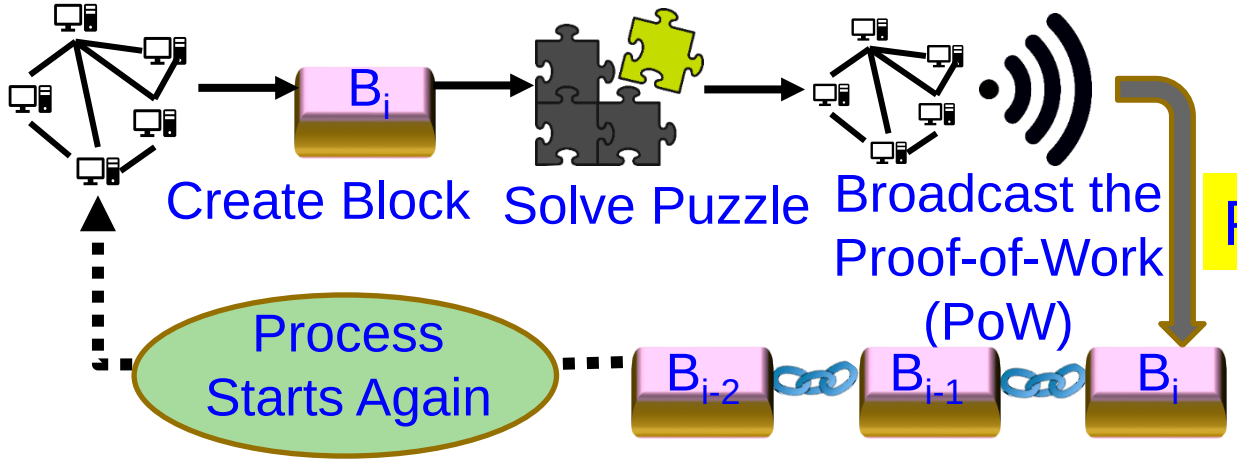


PUFchain Working Model

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

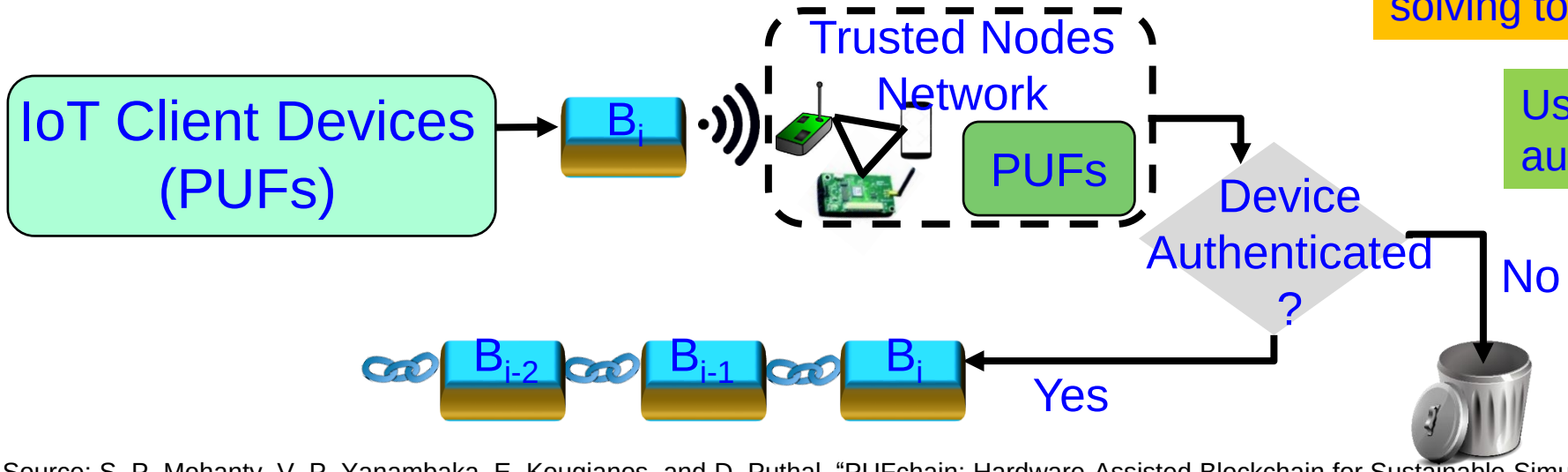
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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



Proof-of-Work (PoW)

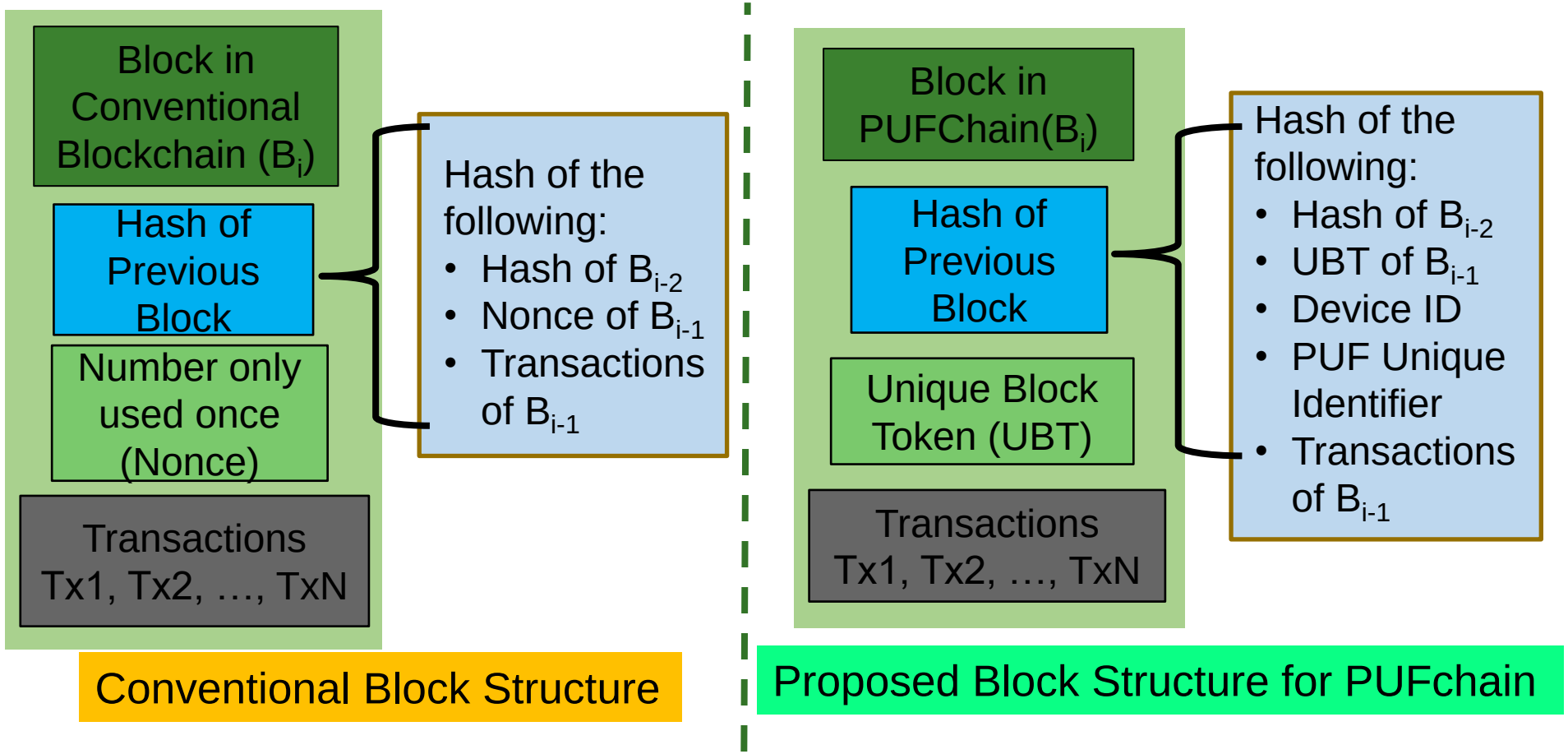
Eliminates cryptographic "puzzle" solving to validate blocks.



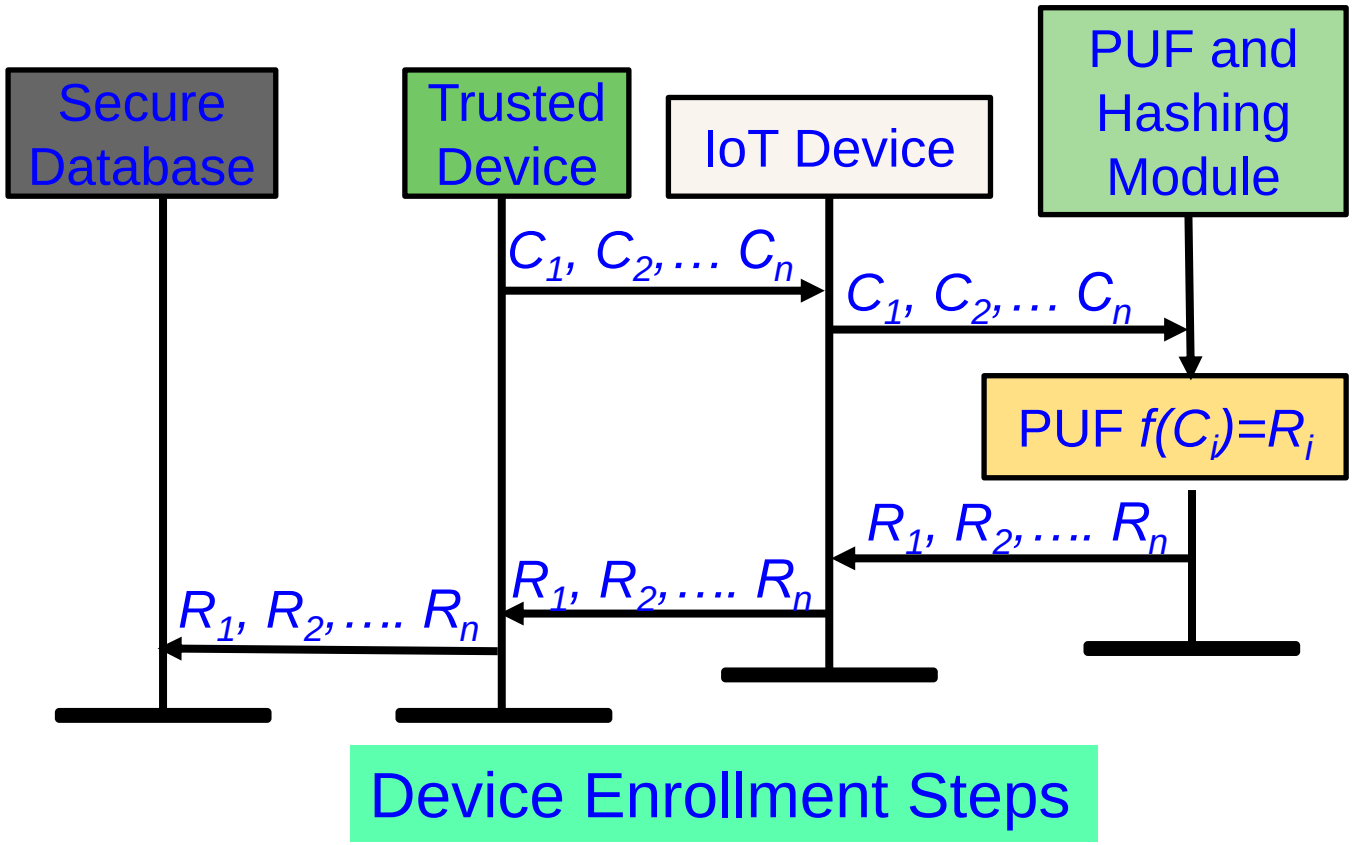
Uses a PUF-based authentication mechanism.

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

PUFchain: Proposed New Block Structure

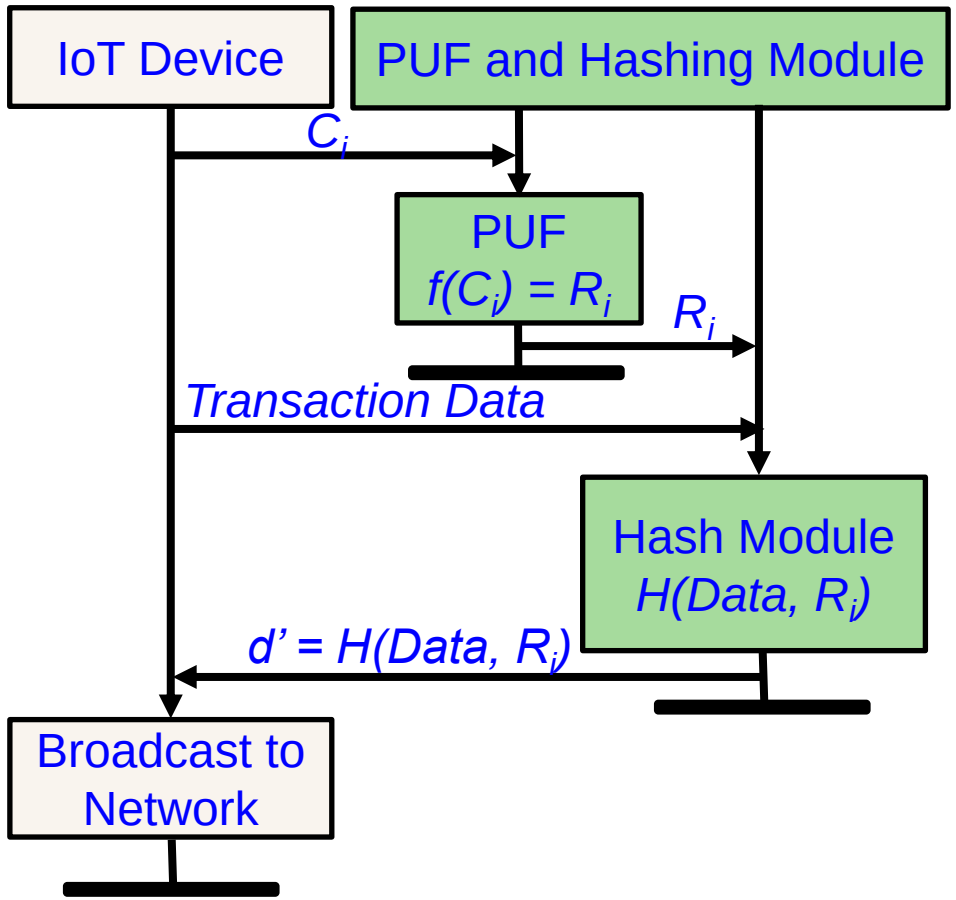


PUFchain: Device Enrollment Steps

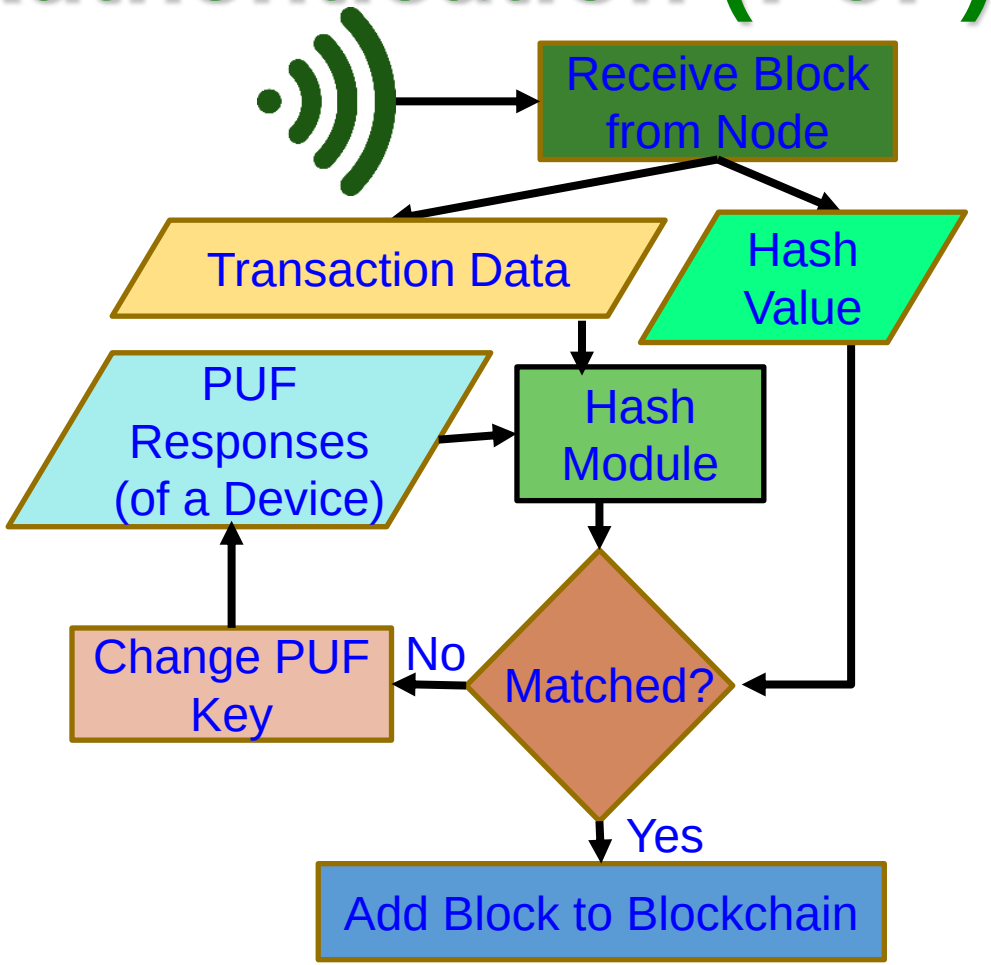


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. in Press.

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



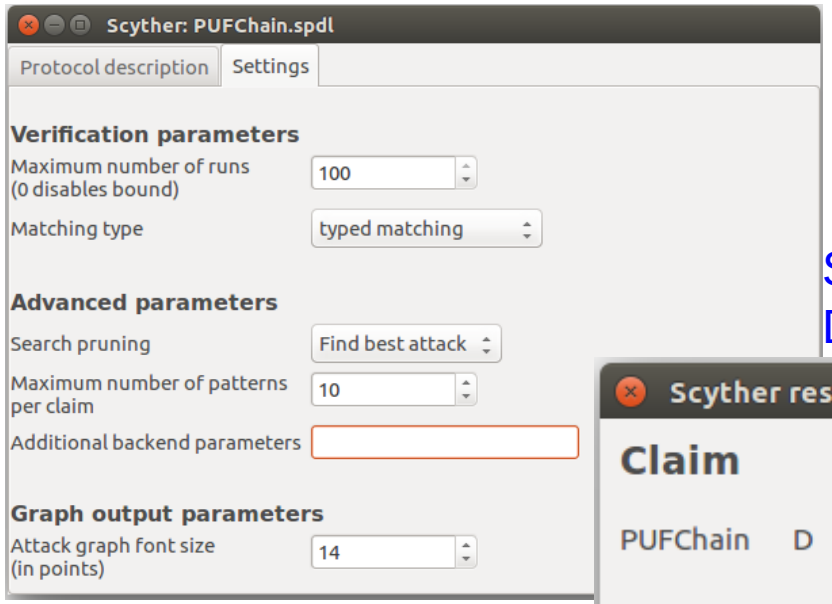
Steps for Transactions Initiation



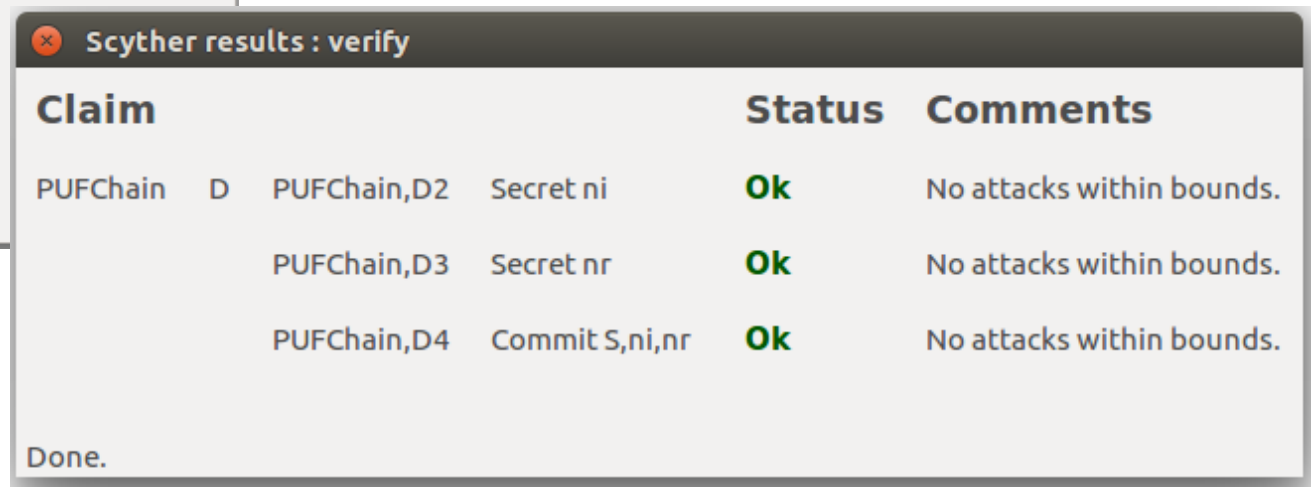
Steps for Device Authentication

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

PUFchain Security Validation



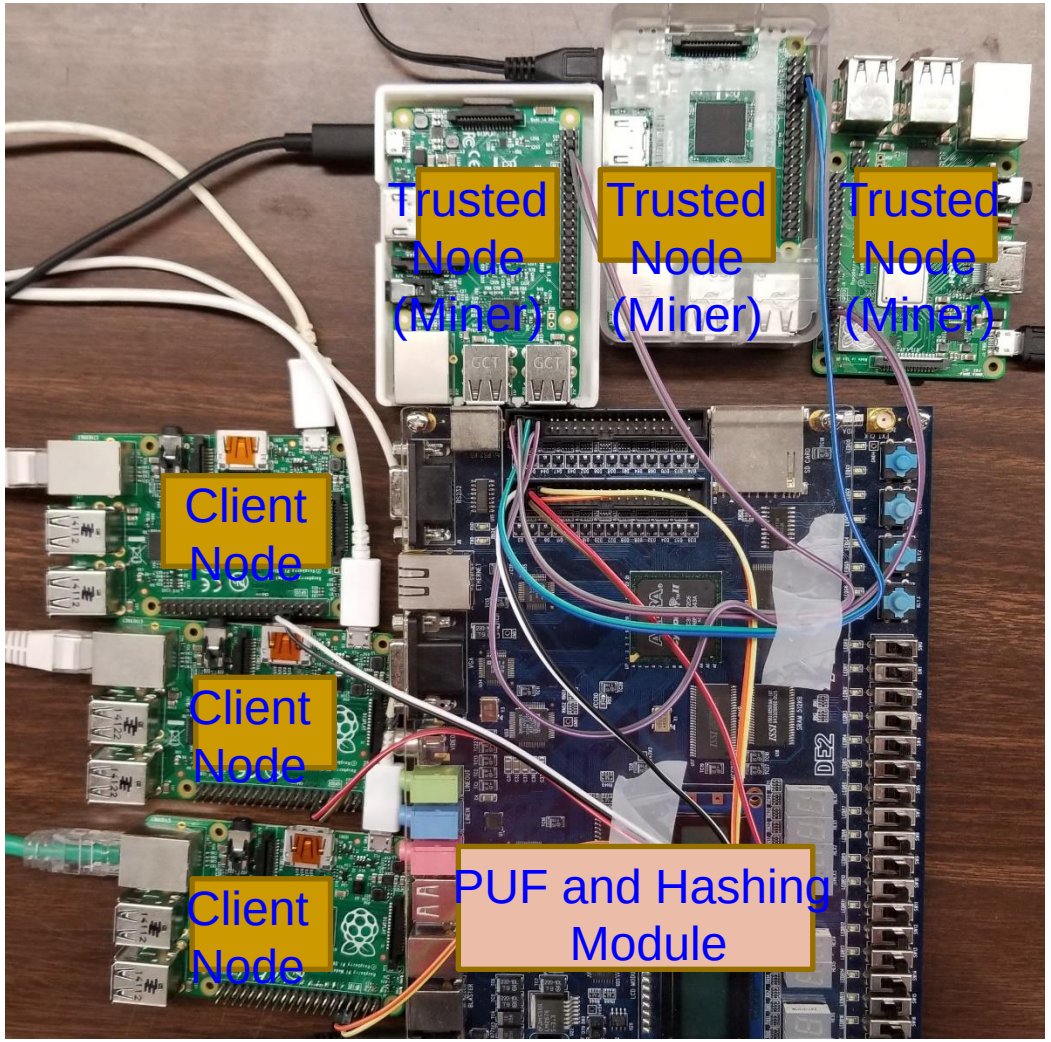
S - the source of the block
D - the miner or authenticator node in the networks



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

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

Our PoP is 1000X Faster than PoW

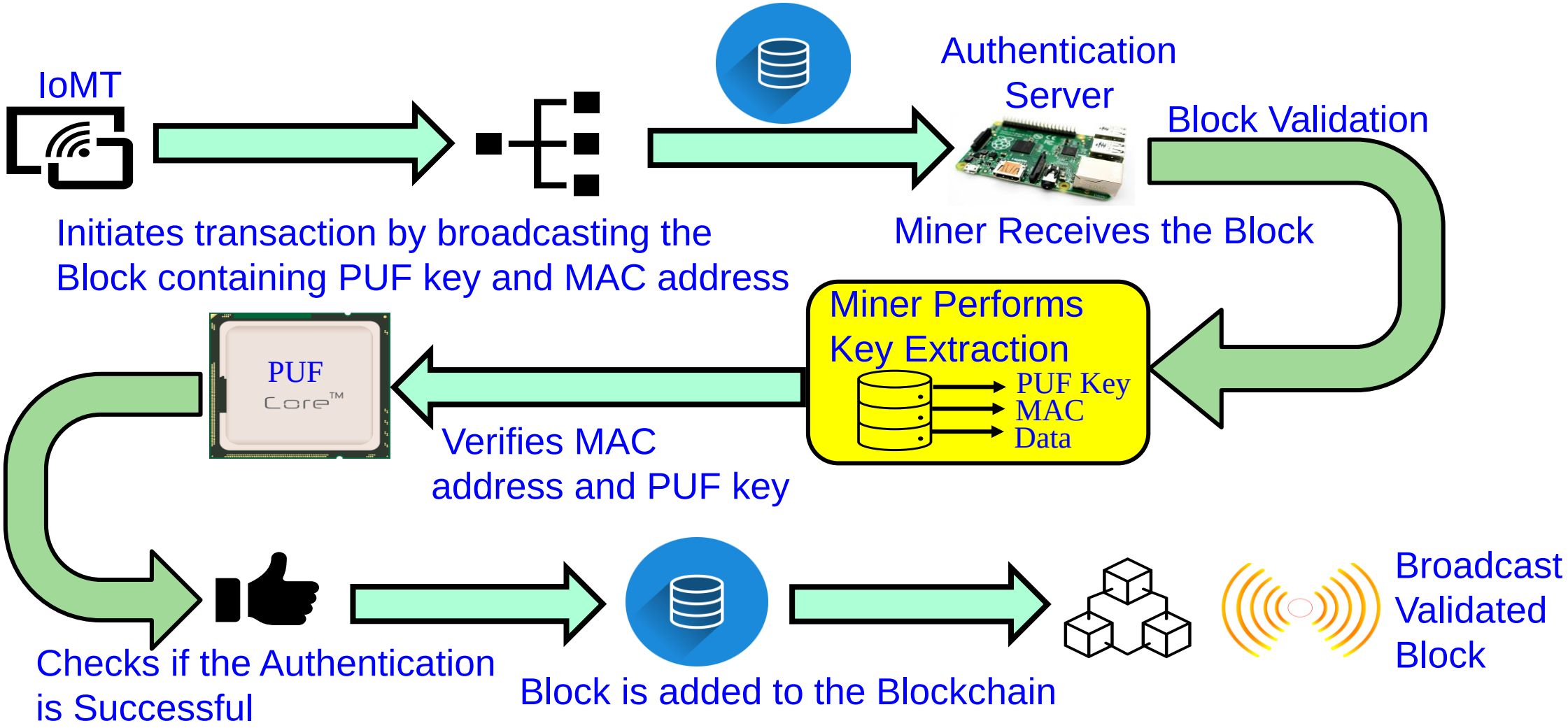


PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

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

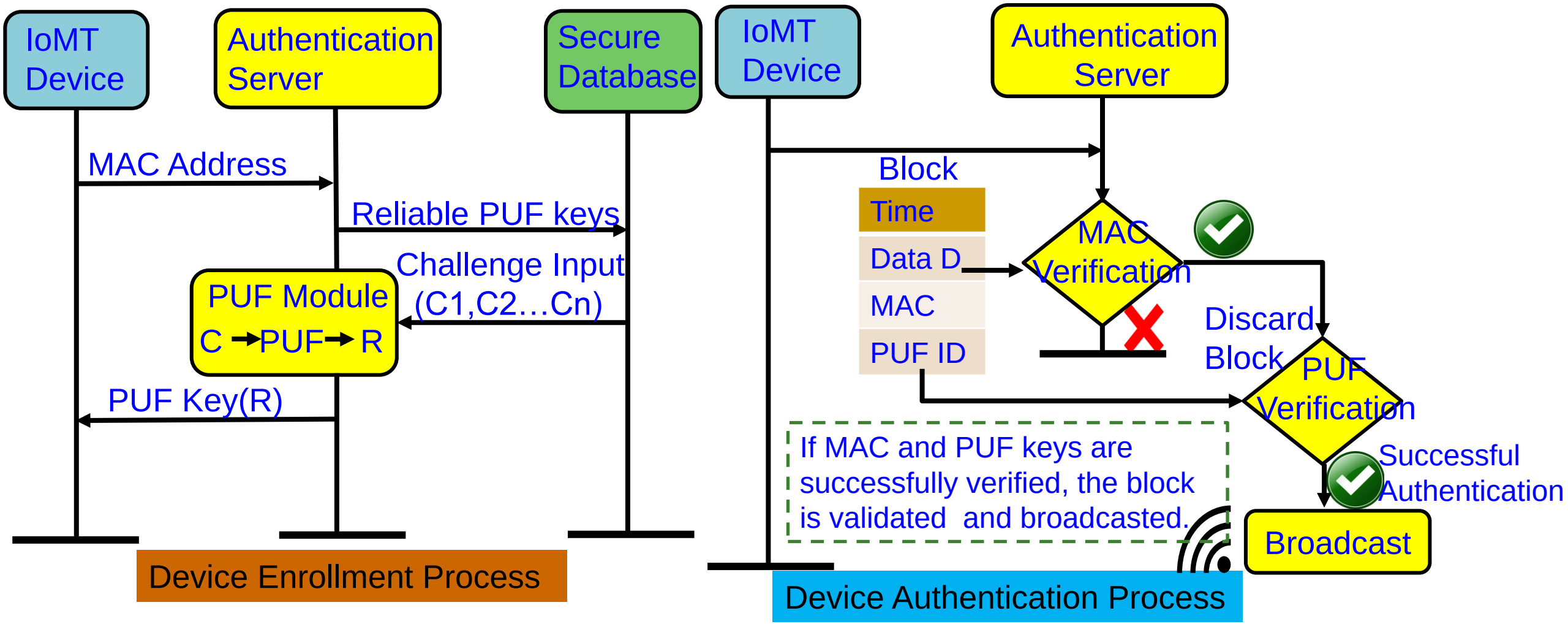
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

PUFchain 2.0: PUF Integrated Blockchain …



Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

Implementation and Validation of PUFchain 2.0

```
Shell
Python 3.7.3 (/usr/bin/python3)
>>> %Run PUFchain_Client_1.py
UDP target IP: 192.168.1.189
UDP target Port: 12345
dc:a6:32:c8:d7:50
0110010001100100011001000110010001100100011001000110010001100100
0110010001100100011001000110010001100100011001000110010001100100
['1645424009.6885517', '23.5', 'dc:a6:32:c8:d7:50', '0110010001100100011001000110010001100100011001000110010001
1100100011001001
["'1645424009.6885517'", "'23.5'", 'dc:a6:32:c8:d7:50', "'0110010001100100011001000110010001100100011001000110
0100011001000110010'"]
Validated Block is:
["'1645424009.6885517'", "'23.5'", 'dc:a6:32:c8:d7:50', "'0110010001100100011001000110010001100100011001000110
0100011001000110010'", '5258e870c1ce3466d240b740c29576dd616827cb36d6d563b7f66b71485303ef', 'c040ad863
53466df832c4474bdfa2852d417bed277937f0b3298f71056de4a3a']
Time taken to add the Block to the Blockchain
0.3086230754852295
```

```
Shell
>>> %Run PUFchain2_Server.py
Waiting for client...
Given Encrypted Message: b'mlCj?C<;Ck?CjBCjj'  from ('192.168.1.104', 37298)
Waiting for client...
Message after decryption: dc:a6:32:b6:a9:aa
dc:a6:32:b6:a9:aa
1001000110010001100100011001000110010001100100011001000110010001
[74, 81, 54, 71, 84, 11, 3, 77]
['1645429578.71013' '24.6' 'dc:a6:32:b6:a9:aa' '1001000110010001100100011001000110010001100100011001000110010001']
'1001000110010001100100011001000110010001100100011001000110010001'
1001000110010001100100011001000110010001100100011001000110010001
Device is Authenticated
'1645429578.71013''24.6''dc:a6:32:b6:a9:aa''1001000110010001100100011001000110010001100100011001000110010001'595b521744857db0951b4fd679f038570f80492da2d731aa729eed
bf0efa63a7
["'1645429578.71013'", "'24.6'", "'dc:a6:32:b6:a9:aa'", "'1001000110010001100100011001000110010001100100011001000110010001'", 'e29a368bc110472496afc9ba4b5a1a5c7dbd
beaf4a9cb405c6b863fa83dbaa13', '595b521744857db0951b4fd679f038570f80492da2d731aa729eedbf0efa63a7']
Time taken to add the Block to the Blockchain
3.6917524337768555
>>>
```

Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

PUFchain 2.0 Results

Table: PROOJECT

	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
491	'164542358...	'23.5'	'dc:a6:32:c...	'011001000...	a8609d84a...	bbdb09358f...
492	'164542400...	'23.5'	'dc:a6:32:c...	'011001000...	f1cb3b914c...	a8609d84a...
493	'164542425...	'24.6'	'dc:a6:32:b...	'011001000...	4993cd538...	f1cb3b914c...
494	'164542431...	'23.5'	'dc:a6:32:c...	'011001000...	5c51a406e...	4993cd538...
495	'164542432...	'23.5'	'dc:a6:32:c...	'011001000...	b52392032...	5c51a406e...
496	'164542436...	'23.5'	'dc:a6:32:c...	'011001000...	8b3aea799...	b52392032...
497	'164542939...	'24.6'	'dc:a6:32:b...	'100100011...	6e95ad295...	8b3aea799...
498	'164542941...	'24.6'	'dc:a6:32:b...	'100100011...	70ddb5c7fe...	6e95ad295...
499	'164542943...	'24.6'	'dc:a6:32:b...	'100100011...	8baf2d2b68...	70ddb5c7fe...
500	'164542956...	'24.6'	'dc:a6:32:b...	'100100011...	595b52174...	8baf2d2b68...
501	'164542957...	'24.6'	'dc:a6:32:b...	'100100011...	e29a368bc...	595b52174...
502	'164542975...	'24.6'	'dc:a6:32:b...	'100100011...	0ed1b03d1...	e29a368bc...
503	'164542979...	'24.6'	'dc:a6:32:b...	'100100011...	cf66a49c17...	0ed1b03d1...
504	'164542983...	'24.6'	'dc:a6:32:b...	'100100011...	4aa649f57e...	cf66a49c17...
505	'164543086...	'24.6'	'dc:a6:32:b...	'100100011...	98c15369e...	4aa649f57e...
506	'164543087...	'24.6'	'dc:a6:32:b...	'100100011...	57a40602c...	98c15369e...
507	'164543088...	'24.6'	'dc:a6:32:b...	'100100011...	203eff57fac...	57a40602c...
508	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	b4945b251...	203eff57fac...
509	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	25e41c514...	b4945b251...
510	'164543090...	'24.6'	'dc:a6:32:b...	'100100011...	76cfb52fec...	25e41c514...
511	'164543091...	'24.6'	'dc:a6:32:b...	'100100011...	ce357cd16...	76cfb52fec...
512	'164543092...	'24.6'	'dc:a6:32:b...	'100100011...	d55132425...	ce357cd16...
513	'164543093...	'24.6'	'dc:a6:32:b...	'100100011...	895a199ffa...	d55132425...
514	'164543095...	'24.6'	'dc:a6:32:b...	'100100011...	f957d0ed92...	895a199ffa...
515	'164543107...	'24.6'	'dc:a6:32:b...	'100100011...	797ea49b2...	f957d0ed92...
516	'164543108...	'24.6'	'dc:a6:32:b...	'100100011...	b73abae5e...	797ea49b2...

	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
28	'1644686449.9660056'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	b38f4e2c81e0351546d2acd389644b2e87...	ab884ea51eac38cd7d5603c08630cbf0545...
29	'1644686593.6336515'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	d3f44a110cd592d483c41ac1ecddebdce0e...	b38f4e2c81e0351546d2acd389644b2e87...
30	'1644686603.9765272'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	0882092393b4ae5eb9ce15dd01e6773bea...	d3f44a110cd592d483c41ac1ecddebdce0e...
31	'1644686614.4211583'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	6e28f0f930495f2510ad2e5fade3be8207f1...	0882092393b4ae5eb9ce15dd01e6773bea...
32	'1644686624.865872'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	de6b884ba48915127ef8ec59d0eb903e2cf...	6e28f0f930495f2510ad2e5fade3be8207f1...
33	'1644686645.9601705'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	62d4069859edfa3713be78b94507fbf2b6b...	de6b884ba48915127ef8ec59d0eb903e2cf...
34	'1644686656.4047632'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...	62d4069859edfa3713be78b94507fbf2b6b...
35	'1644686666.849594'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	ae28a86fca44f7898ee0a64c25d84fffcc6b...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...
36	'1644686677.294728'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...	ae28a86fca44f7898ee0a64c25d84fffcc6b...
37	'1644686687.739273'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...
38	'1644686708.6280165'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	f14b596a9741684cd42137569afb9cc9ffa9...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...
39	'1644686719.0736935'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	70b906e51c0d0eb9174c0438e320365440...	f14b596a9741684cd42137569afb9cc9ffa9...
40	'1644686841.1356113'	'23.5'	dc:a6:32:c8:d7:50	'10000011100000111000001110000011...	b318c9a9c5d6ae591ac48d37e57d40fcbc1...	70b906e51c0d0eb9174c0438e320365440...

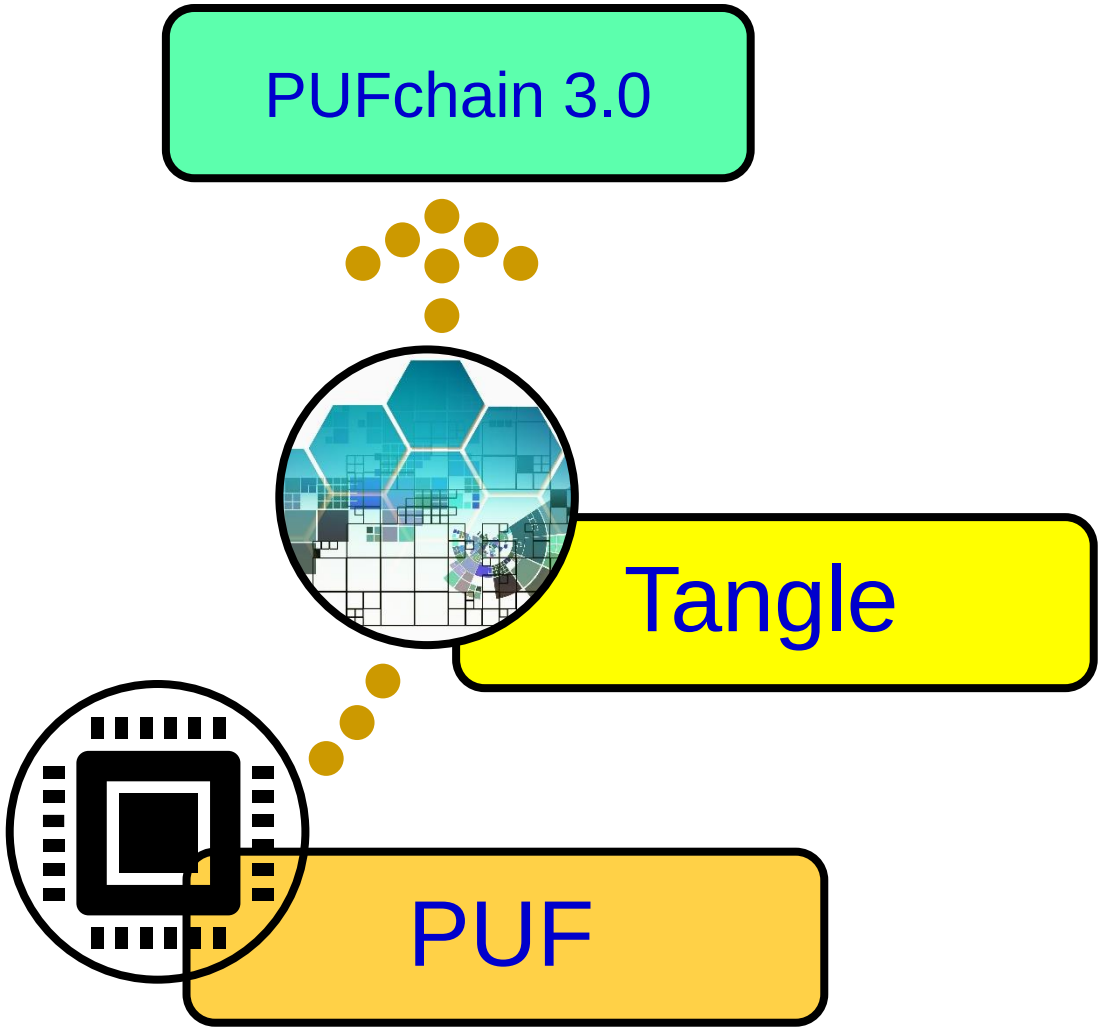
Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

PUFchain 2.0: Comparative Perspectives

Research Works	Application	PUF Design	Hardware	PUF Reliability	Blockchain	Security Levels
Yanambaka et al. 2019 - PMsec	IoMT (Device)	Hybrid Oscillator Arbiter PUF	FPGA, 32-bit Microcontroller	0.85%	No Blockchain	Single Level Authentication (PUF)
Mohanty, et al. 2020 - PUFchain	IoMT (Device and Data)	Ring Oscillators	Altera DE-2, Single Board Computer	1.25%	Private Blockchain	Single Level Authentication (PUF)
Kim et al. 2019 - PUF-based IoT Device Authentication [14]	IoT (Device)	NA	Cortex-M4 STM32F4-MCU	NA	No Blockchain	Single Level Authentication (PUF)
Our PUFchain 2.0 in 2022	**IoMT (Device and Data)**	**Arbiter PUF**	**Xilinx-Artix-7-Basys-3 FPGA**	**75% of the keys are reliable**	**Permissioned Blockchain**	**Two Level Authentication (MAC & PUF)**

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344, 19-pages, DOI: https://doi.org/10.1007/s42979-022-01238-2.

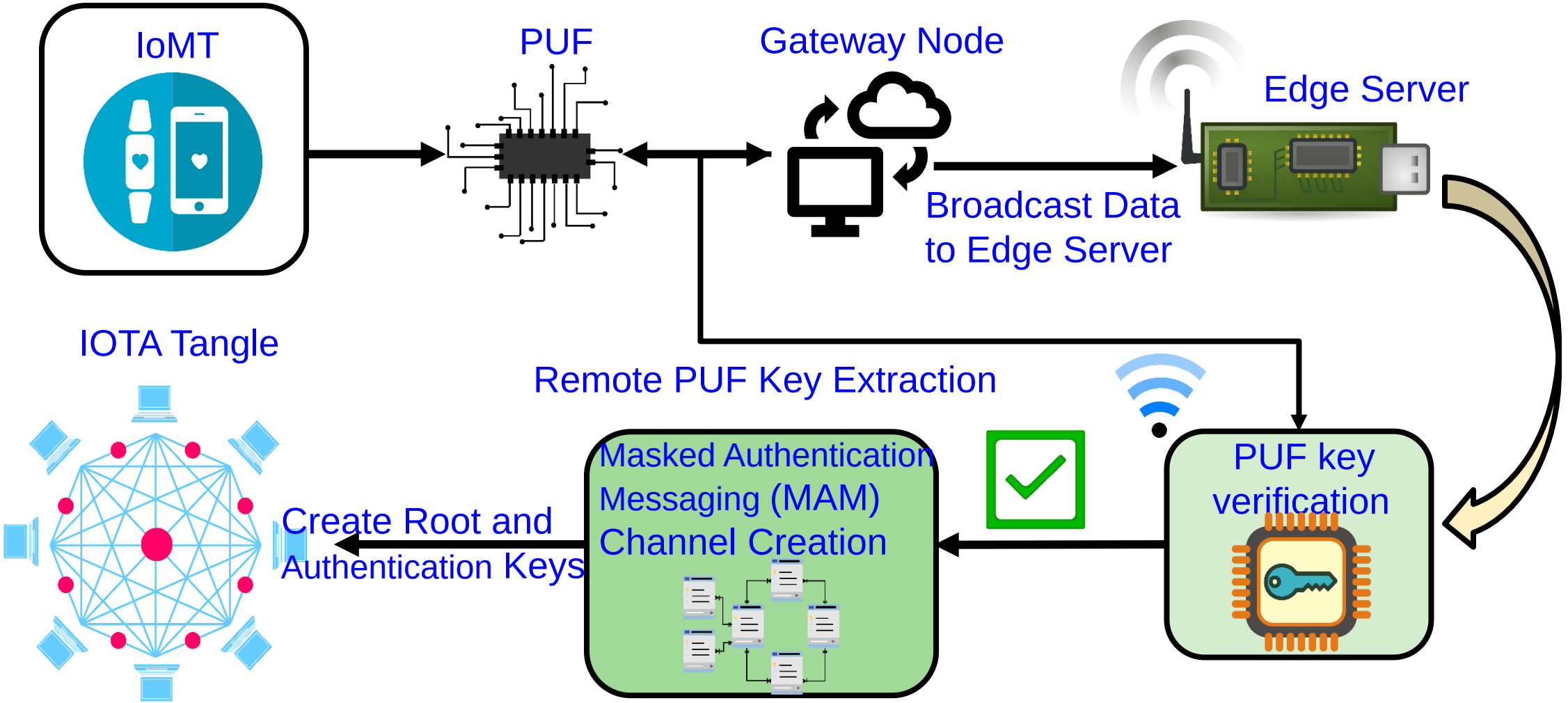
PUFchain 3.0 - Conceptual Idea



- PUFchain 3.0 is the idea of integrating PUF with scalable Tangle DLT using MAM communication protocol by creating a MAM communication channel in Tangle using PUF key

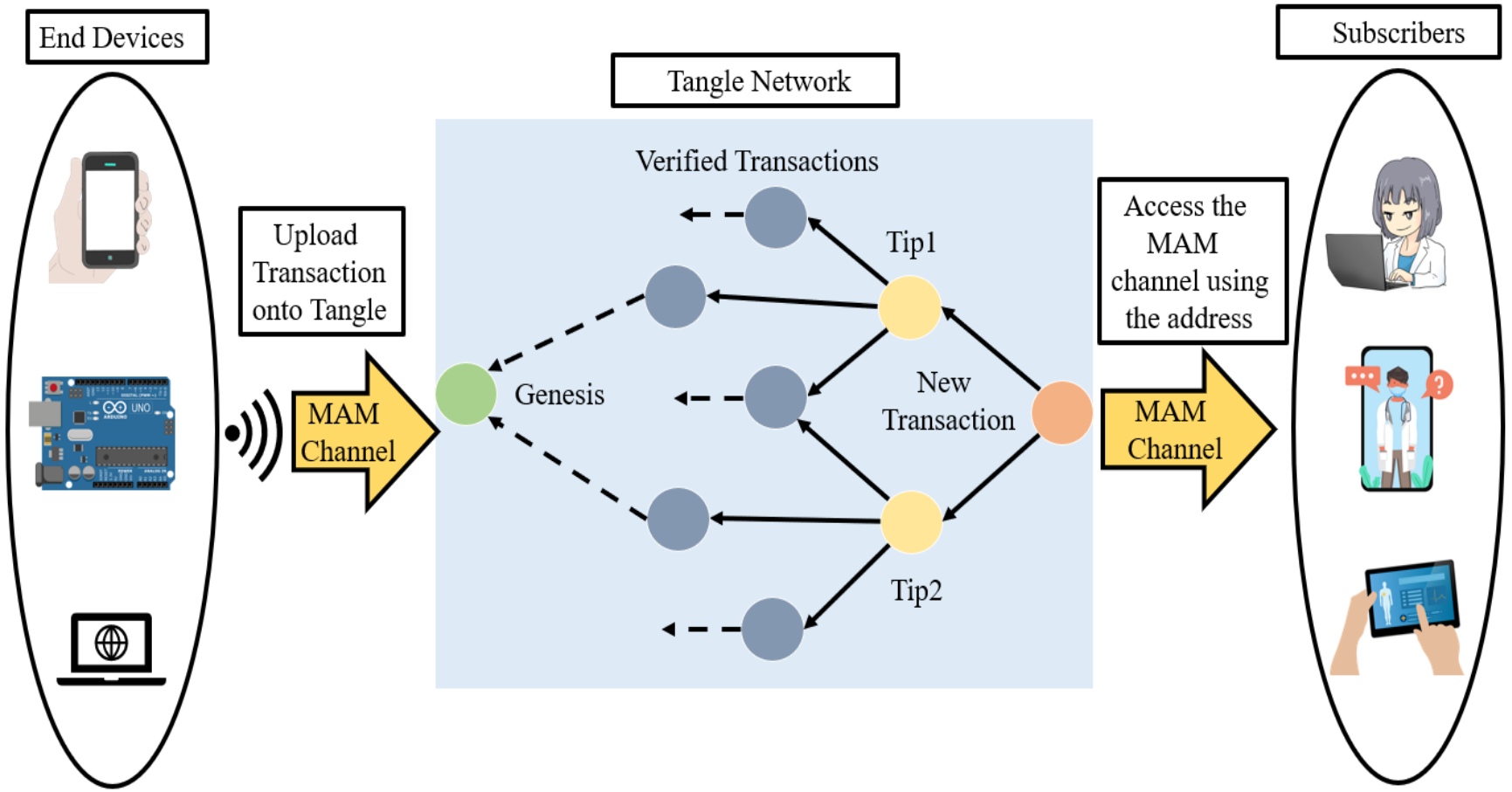
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40, DOI: https://doi.org/10.1007/978-3-031-18872-5_2.

PUFchain 3.0 - Architecture



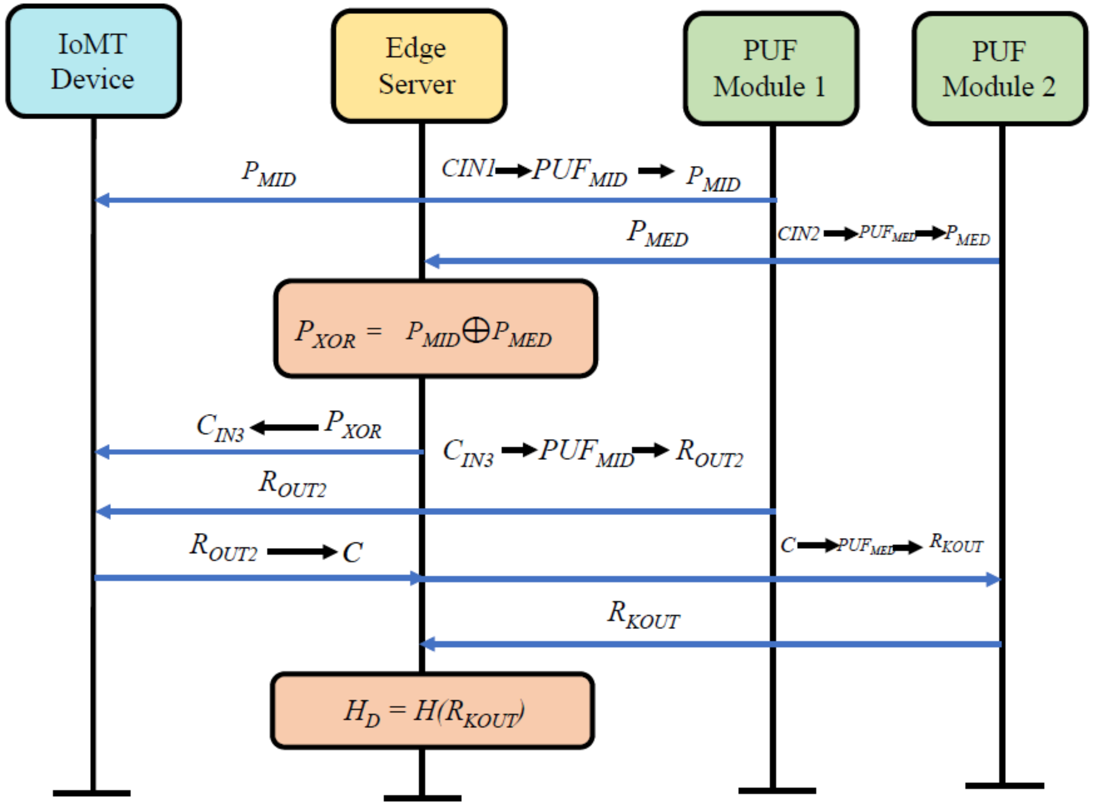
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40, DOI: https://doi.org/10.1007/978-3-031-18872-5_2.

Masked Authentication Messaging (MAM) in IOTA Tangle

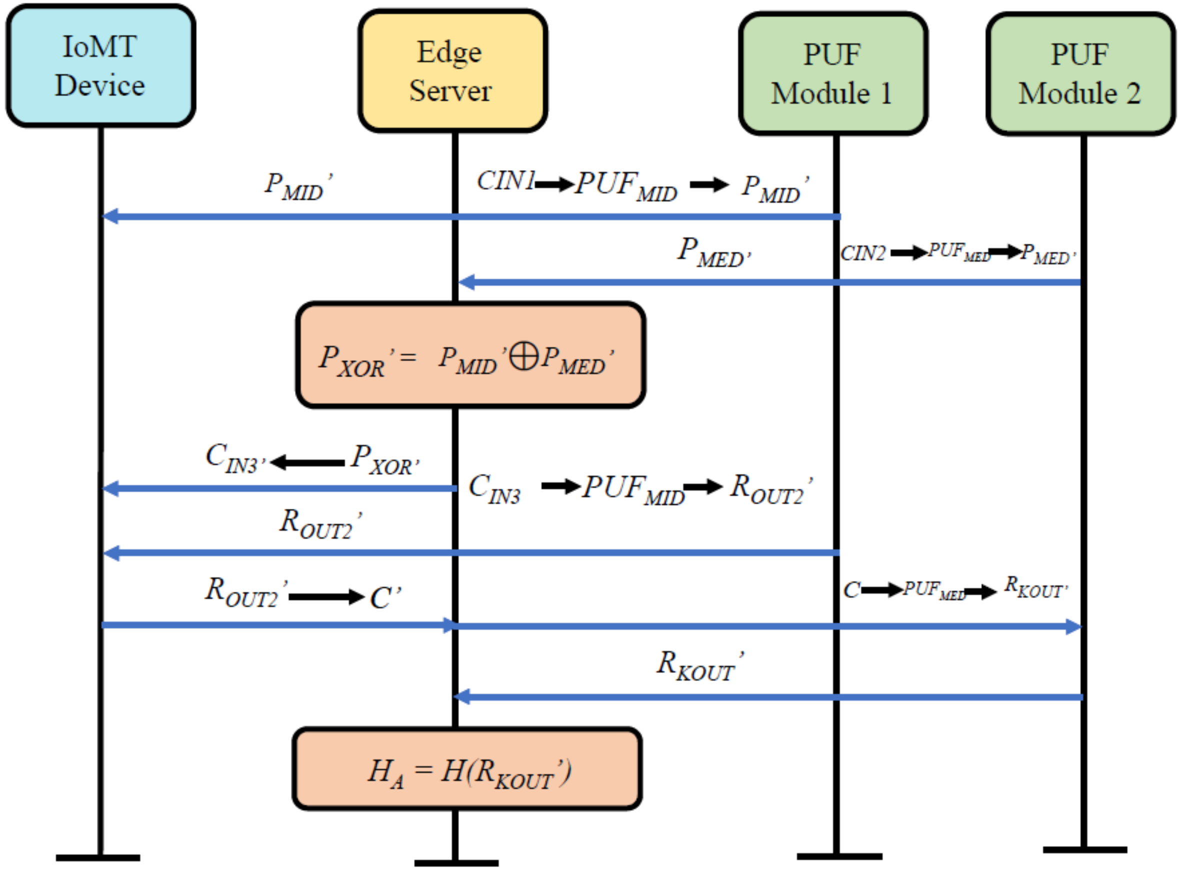


- Provides Device and Data security in IoT
- Works in Three modes: Public, Private and Restricted

PUFchain 3.0 - Working Flow

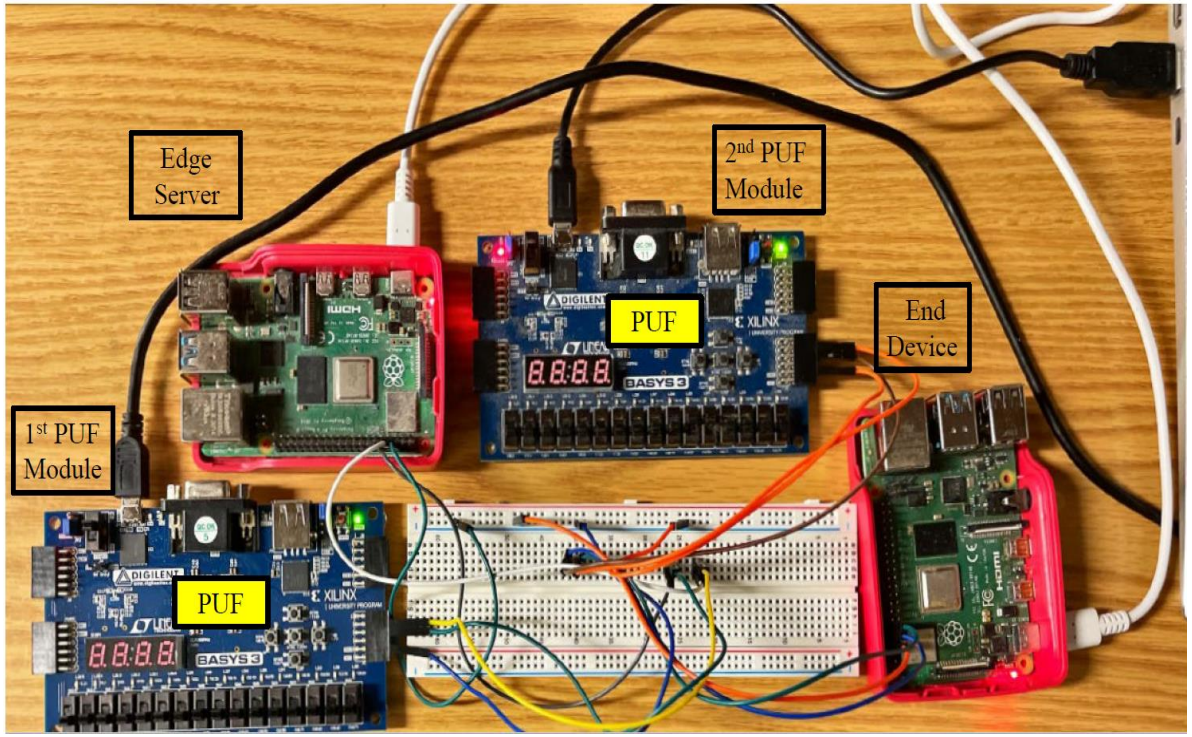


Steps for Device Registration



Steps for Authentication

PUFchain 3.0: Prototype



PUFchain 3.0 Parameters	Specifications
Application	Internet-of-Medical Things
Database	Tangle
Programming Languages	JavaScript, Verilog, and Python
PUF Keys Extracted	500
PUF Design	Arbiter PUF
PUF Module	Xilinx xc7a35tcpg236-1
IOTA Network	Mainnet
Communication Protocol	Masked Authentication Messaging
Edge Server	Single Board Computer

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40, DOI: https://doi.org/10.1007/978-3-031-18872-5_2.

PUFchain 3.0: Performance Evaluation

Research Works	Application	DLT or Blockchain	Authentication Mechanism	Performance Metrics
Mohanty et al. 2020 - PUFchain	IoMT (Device and Data)	Blockchain	Proof-of-PUF-Enabled Authentication	PUF Design Uniqueness - 47.02%, Reliability-1.25%
Chaudhary et al. 2021 - Auto-PUFchain	Hawrdware Supply Chain	Blockchain	Smart Contracts	Gas Cost for Ethereum transaction 21.56 USD (5-Stage)
Al-Joboury et al. 2021 - PoQDB	IoT (Data)	Blockchain & Cobweb	IoT M2M Messaging (MQTT)	Transaction Time - 15 ms
Wang et al. 2022 - PUF-Based Authentication	IoMT (Device)	Blockchain	Smart Contracts	NA
Hellani et al. 2021- Tangle the Blockchain	IoT (Data)	Blockchain & Tangle	Smart Contracts	NA
Bathalapalli et al. 2022-PUFchain 2.0	IoMT (Device)	Blockchain	Media Access Control (MAC) & PUF based Authentication	Total On-Chip Power - 0.081 W, PUF Hamming Distance - 48.02 %
Our PUFchain 3.0 in 2022	**IoMT (Device)**	**Tangle**	**Masked Authentication Messaging**	**Authentication 2.72 sec, Reliability - 100% (Approx), MAM Mode-Restricted**

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40, DOI: https://doi.org/10.1007/978-3-031-18872-5_2.

Smart Grid Cybersecurity - 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

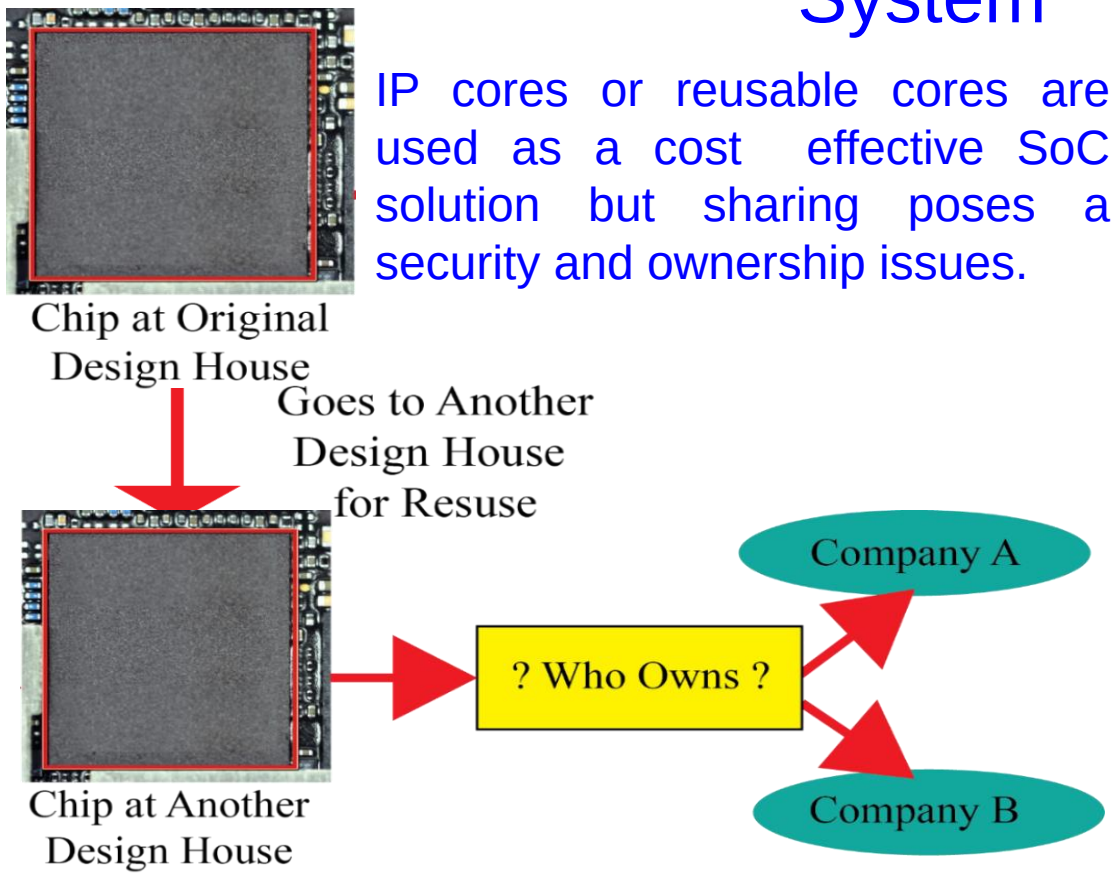
Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids“, *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

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 Quality Assurance in IoT/CPS

IoT Big sensing data collection

Big sensing data collection (Filtering)

Data Transmission (Aggregation)

Cloud Data Processing

Information for Use

Edge Training:
- ➢ Data Signature
- ➢ Model Signature

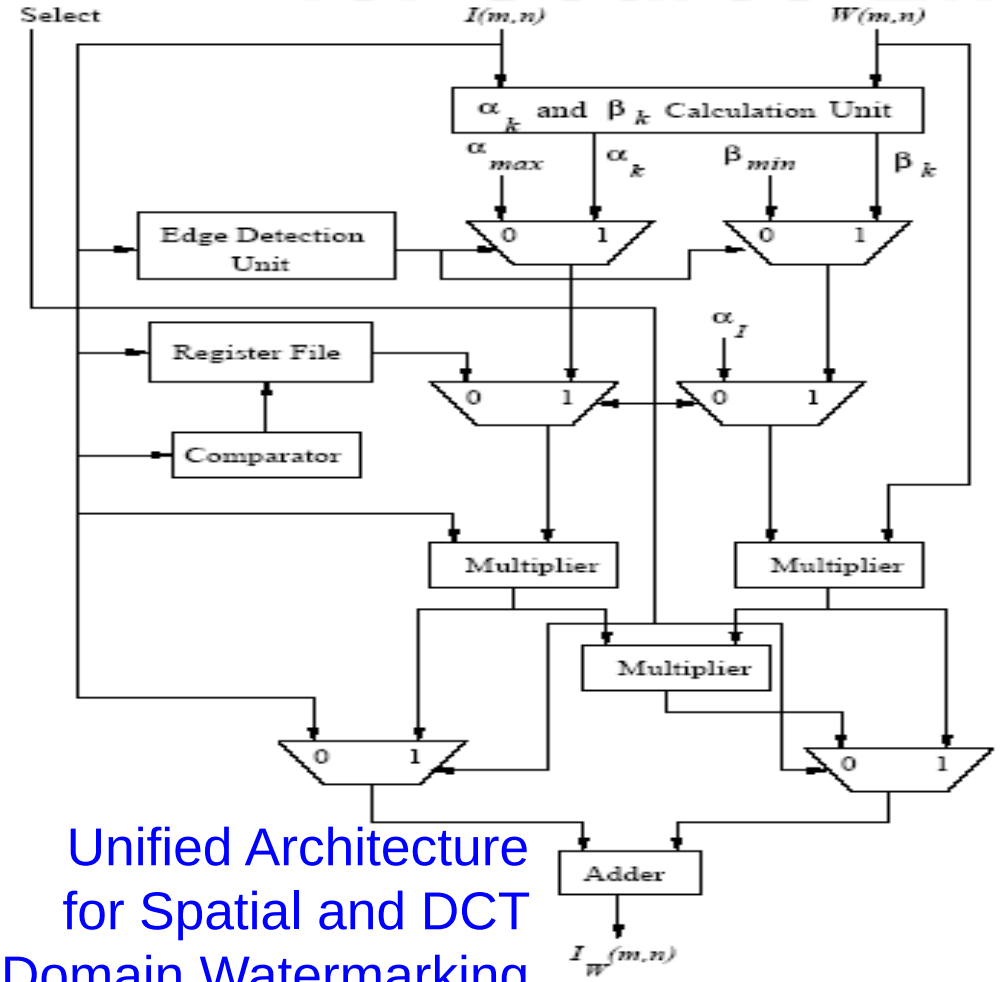
Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

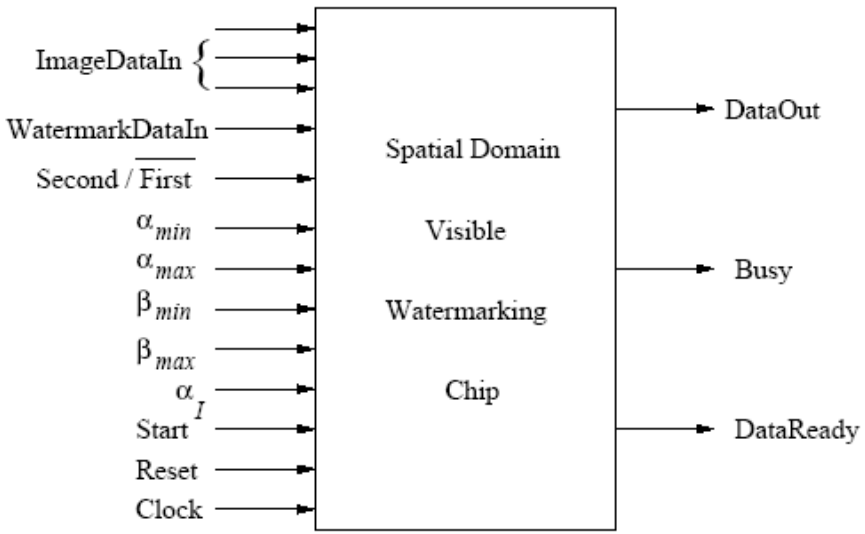
Secure data curation a solution for fake data?

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

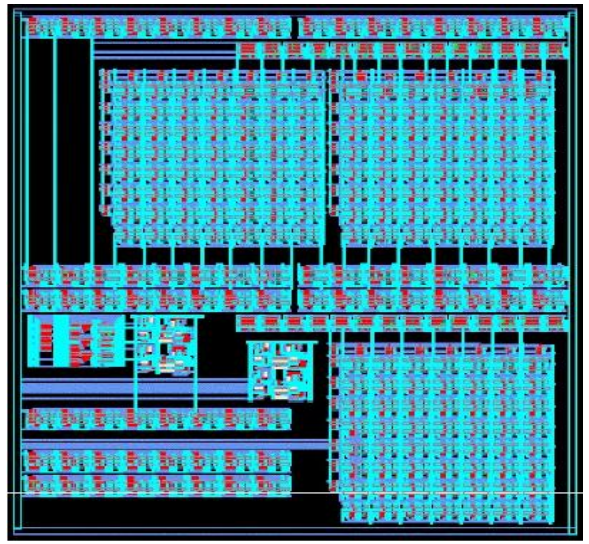
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

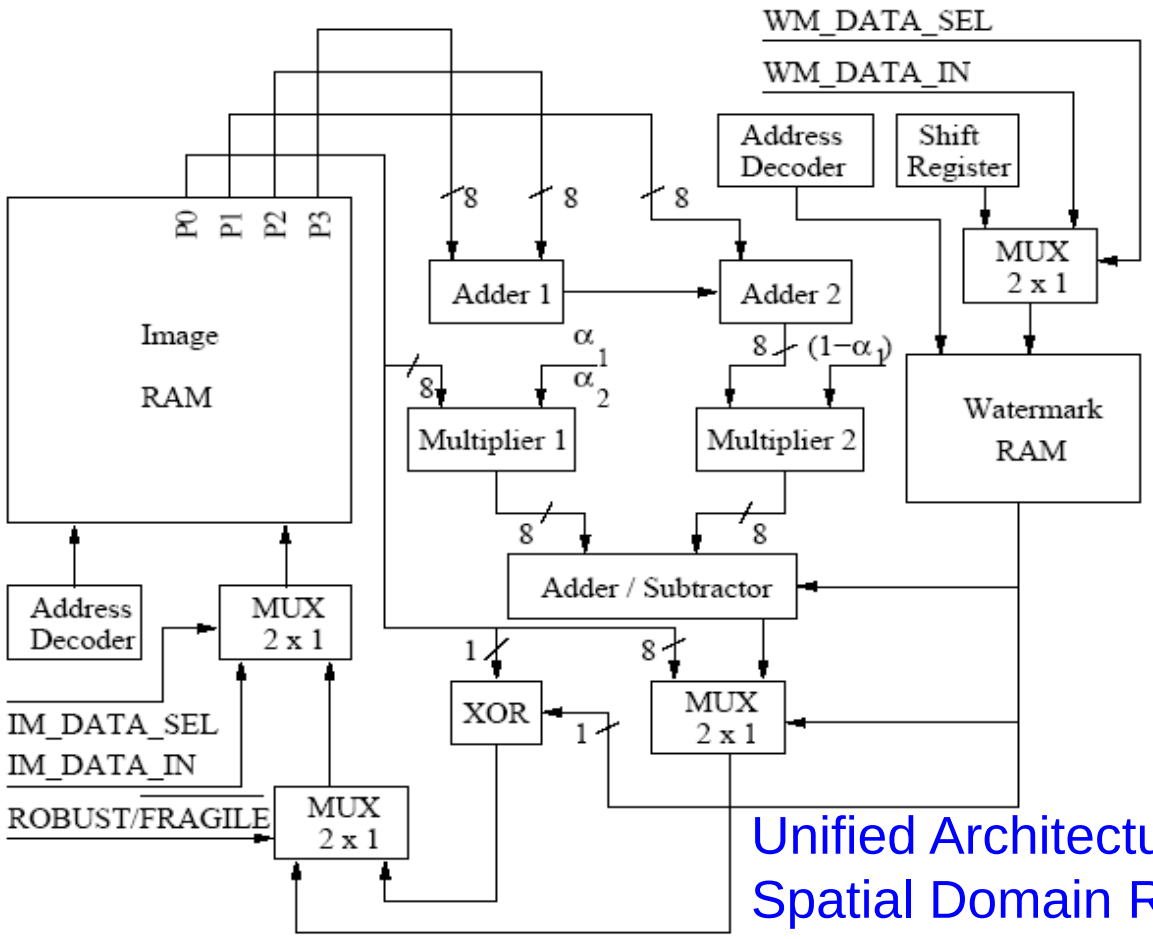
Chip Design Data

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

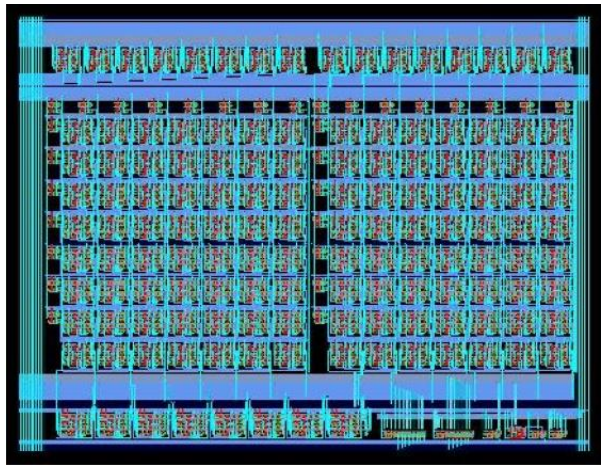
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

Source: **S. P. Mohanty**, N. Ranganathan, and R. K. Namballa, "A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S²DC) Design", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 13, No. 8, August 2005, pp. 1002-1012.

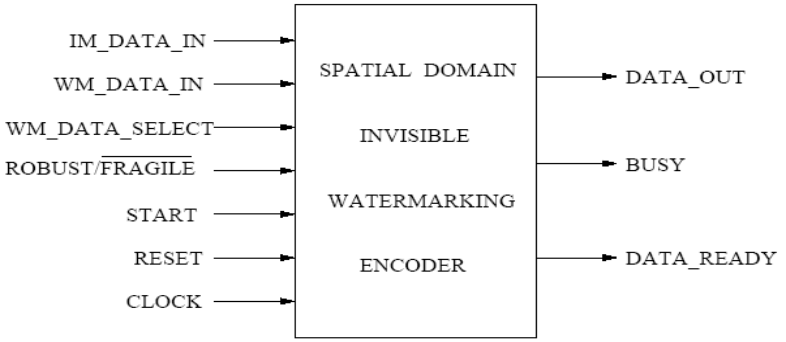
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

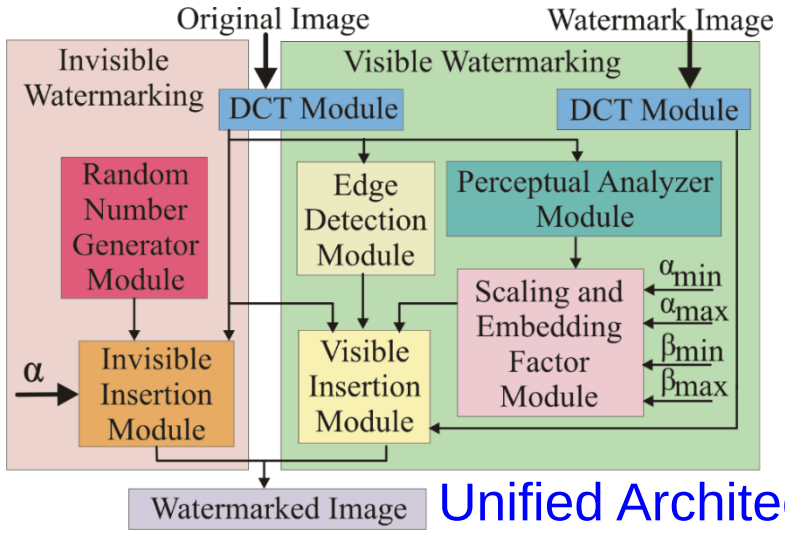
Chip Design Data

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

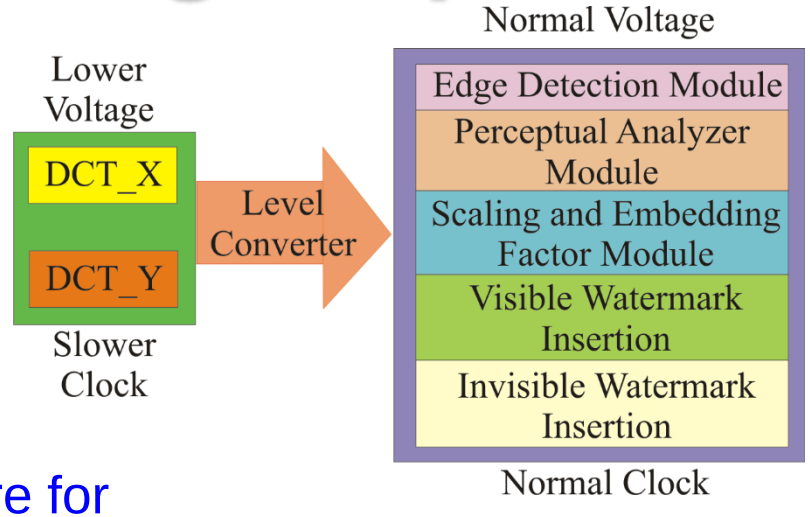
Power Consumption: 2.0 mW, Frequency: 500 MHz

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

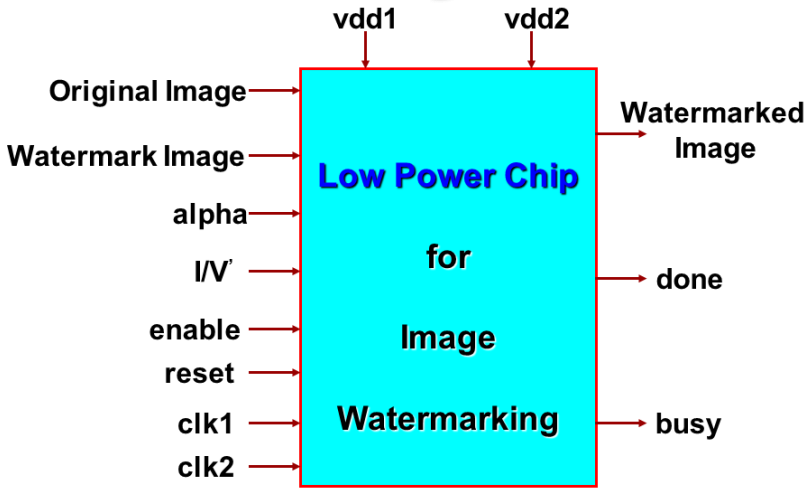
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



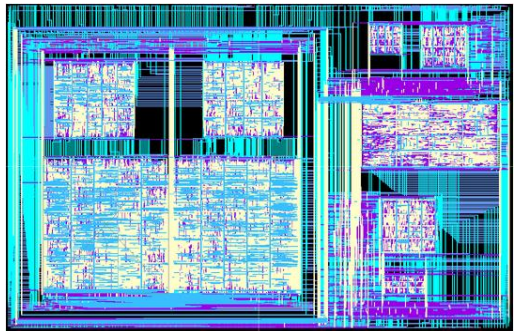
Unified Architecture for DCT Domain Watermarking



DVDF Low-Power Design



Pin Diagram



Chip Layout

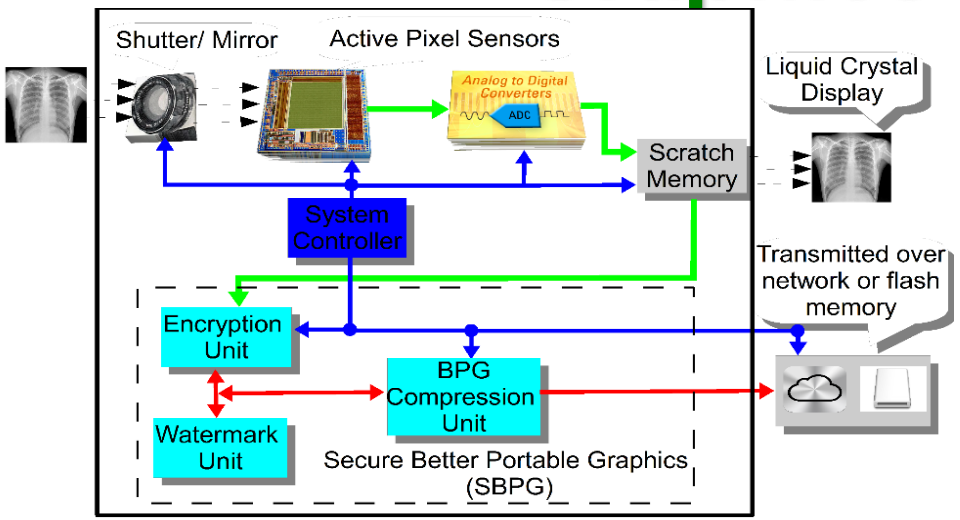
Chip Design Data

Total Area : 16.2 sq mm, No. of Transistors: 1.4 million

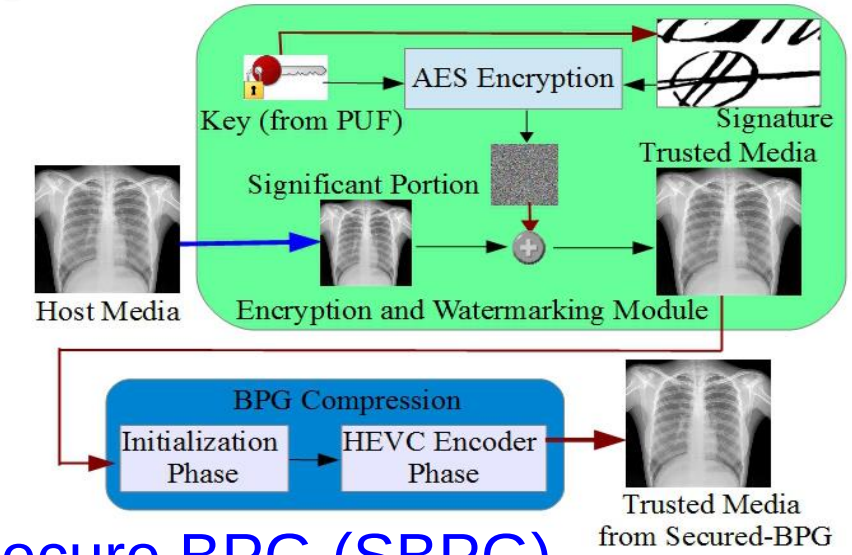
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

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

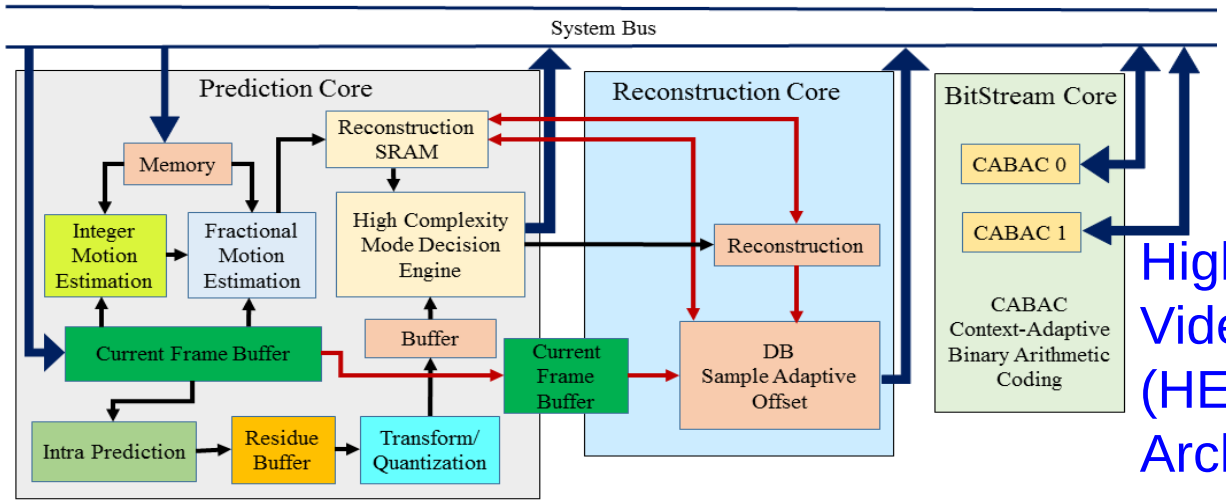
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)

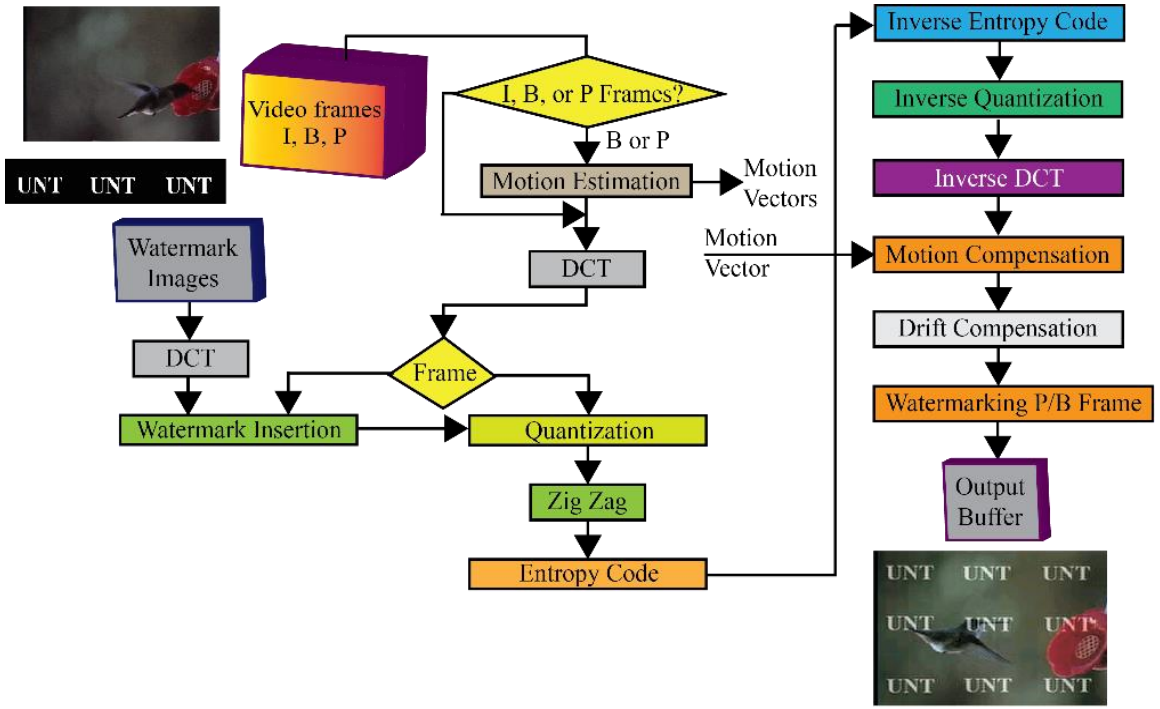


High-Efficiency Video Coding (HEVC) Architecture

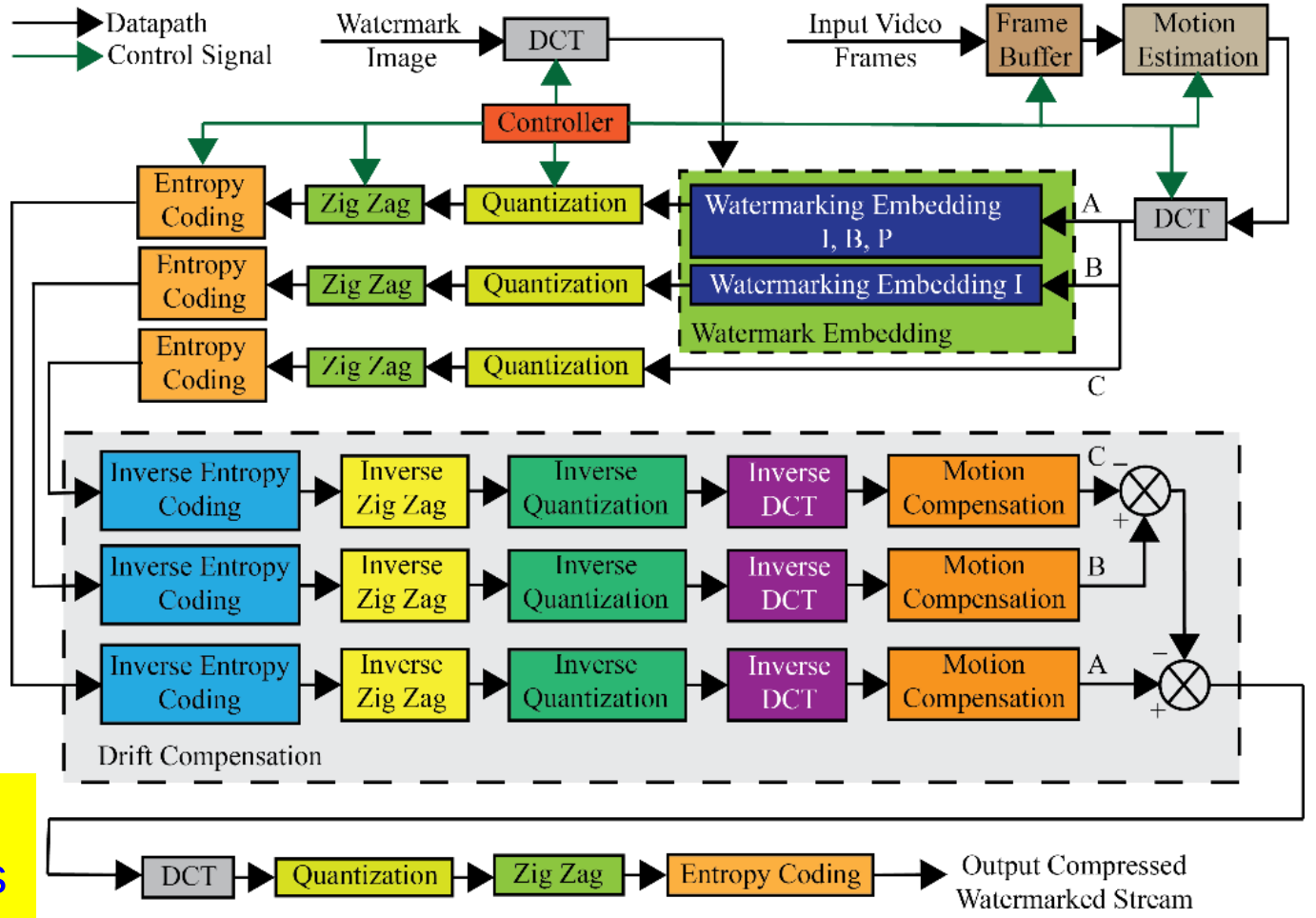
Simulink Prototyping
Throughput: 44 frames/sec
Power Dissipation: 8 nW

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

Our Hardware for Real-Time Video Watermarking



(a) Video Watermarking Algorithm as a Flow Chart

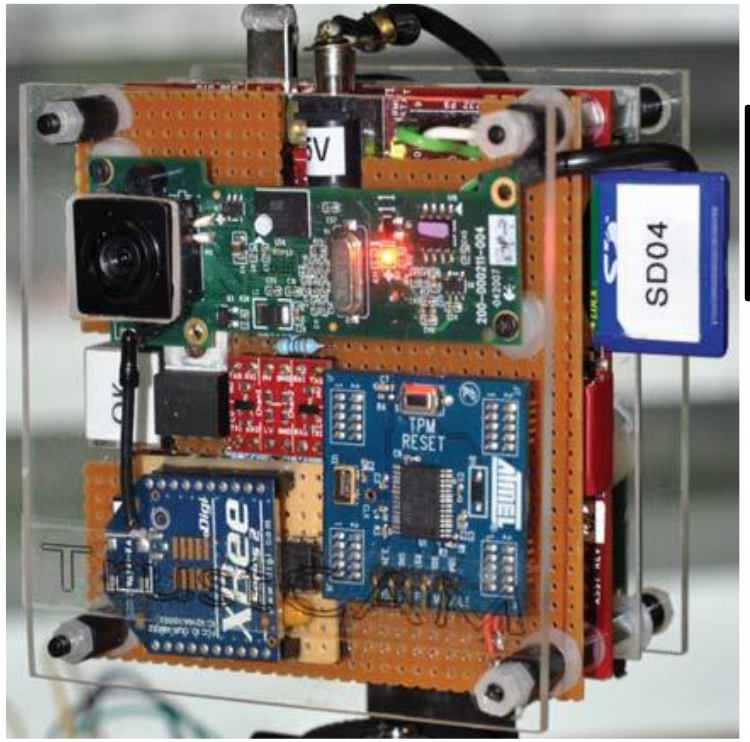


(b) Architecture of the Video Watermrking Algorithm

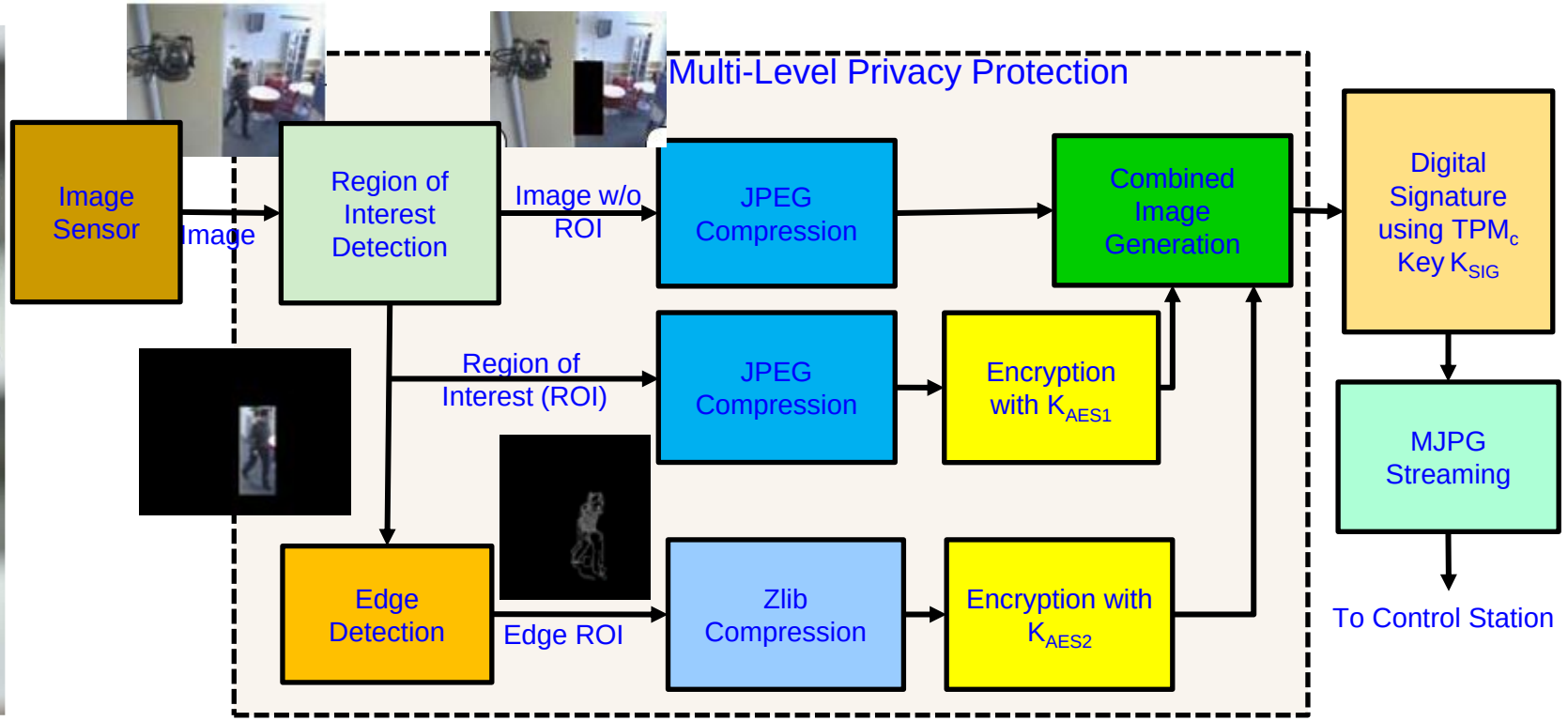
FPGA based Design Data
Resource: 28322 LE, 16532 Registers, 9 MUXes
Operating Frequency: 100 MHz
Throughput: 43 fps

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

My Watermarking Research Inspired - TrustCAM



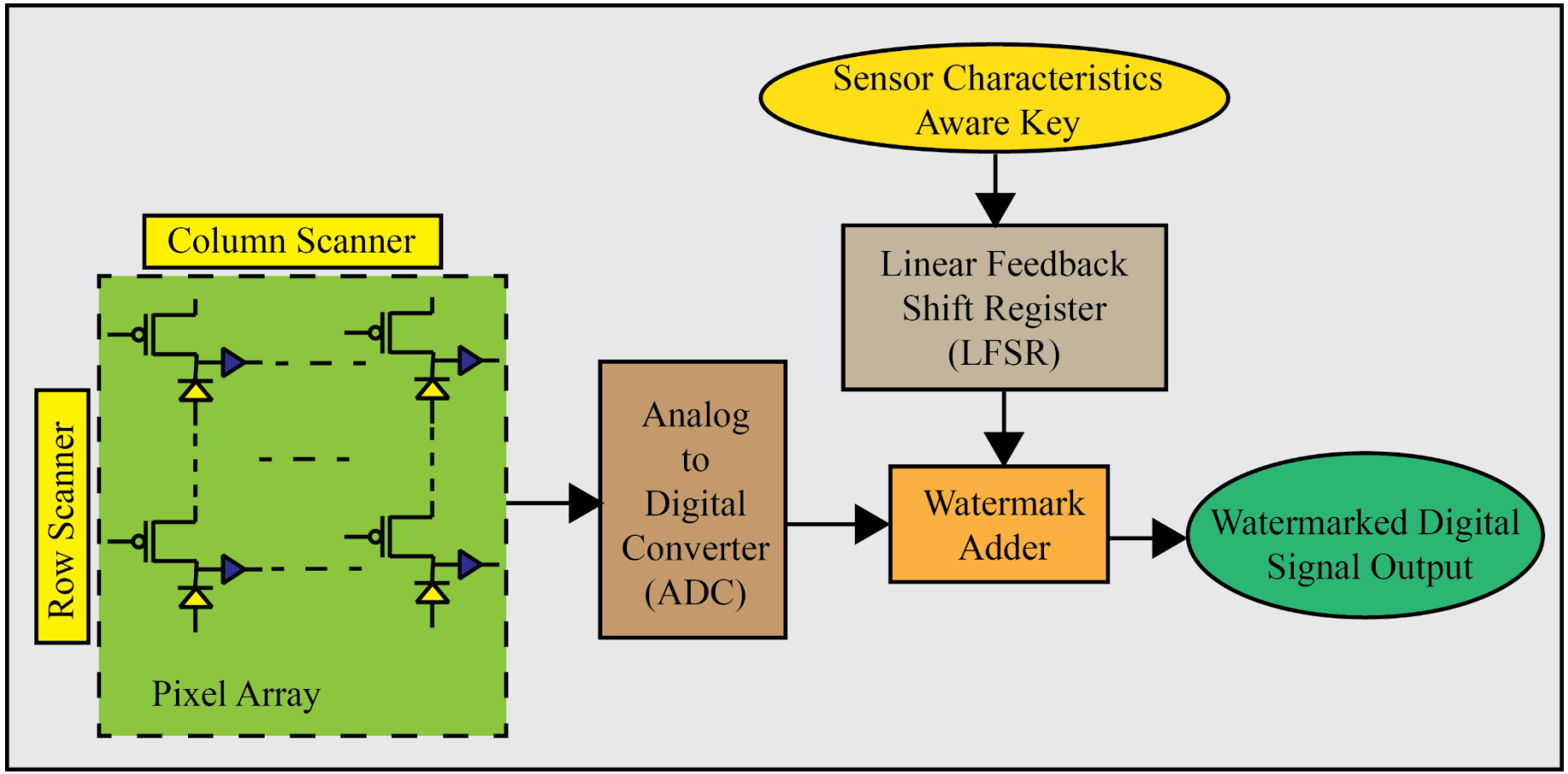
Source: https://pervasive.aau.at/BR/pubs/2010/Winkler_AVSS2010.pdf



For integrity protection, authenticity and confidentiality of image data.

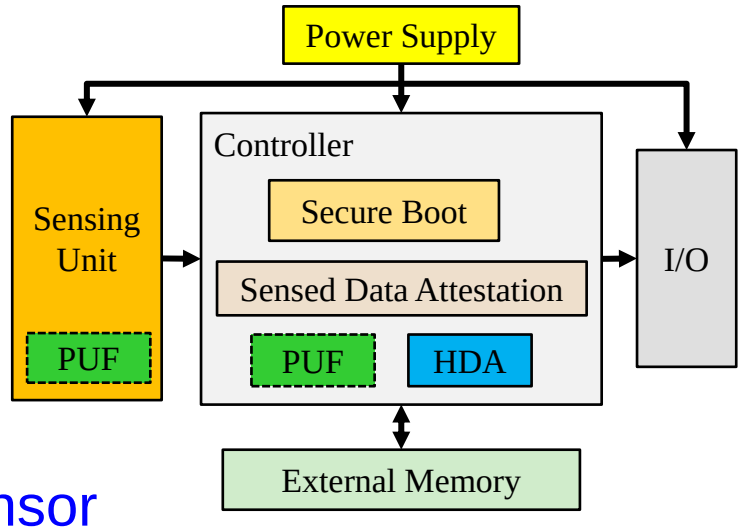
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor

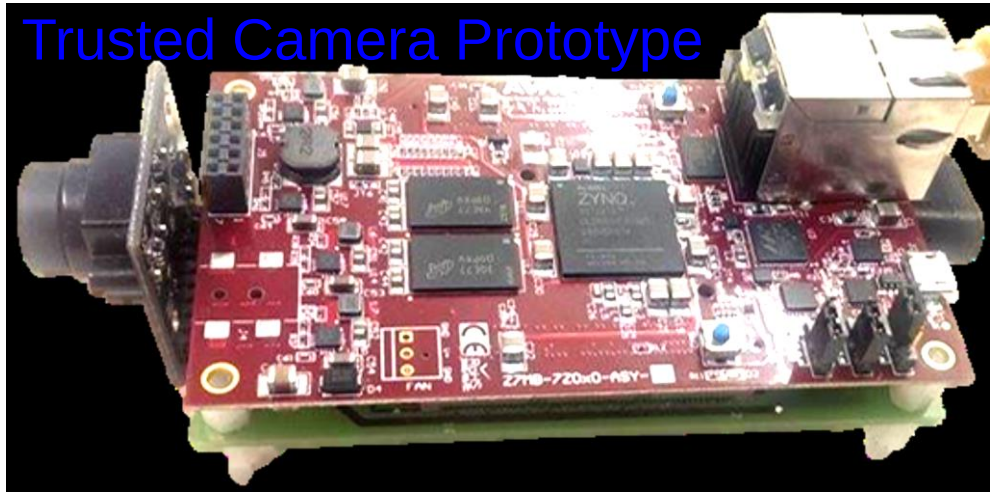


Source: G. R. Nelson, G. A. Jullien, O. Yadid-Pecht, "CMOS Image Sensor With Watermarking Capabilities", in *Proc. IEEE International Symposium on Circuits and Systems* (*ISCAS*), 2005, pp. 5326–5329.

PUF-based Trusted Sensor



PUF-based Trusted Sensor



Source: https://pervasive.aau.at/BR/pubs/2016/Haider_IOTPTS2016.pdf

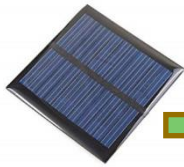
PUF-based Secure Key Generation and Storage module provides key:

- Sensed data attestation to ensure integrity and authenticity.
- Secure boot of sensor controller to ensure integrity of the platform at booting.

- On board SRAM of Xilinx Zynq7010 SoC cannot be used as a PUF.
- A total 1344 number of 3-stage Ring Oscillators were implemented using the Hard Macro utility of Xilinx ISE.

Process Speed: 15 fps
Key Length: 128 bit

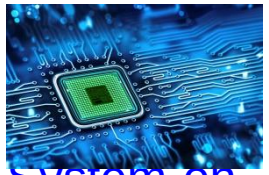
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge



Solar Cell

Harvesting System with Physically Unclonable Function (PUF)

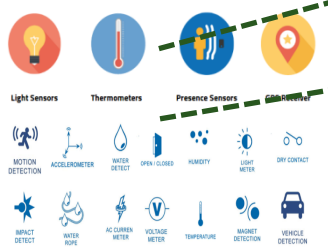
Sensors

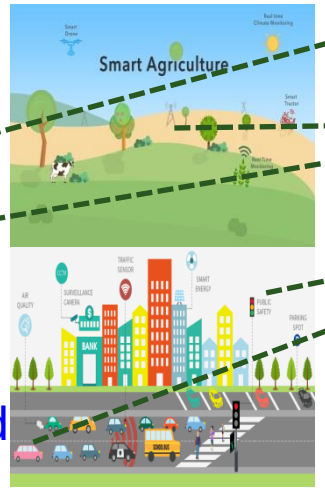


System-on-Chip (SoC)

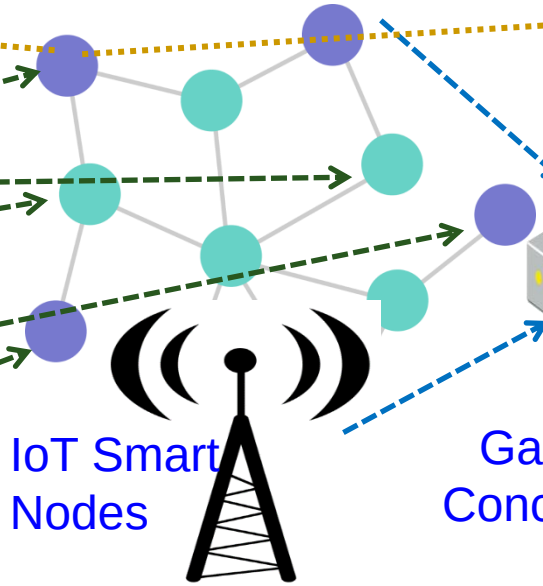
Trans-receiver

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

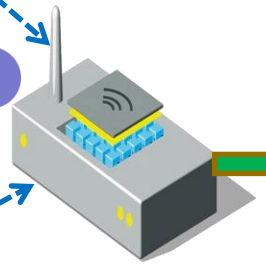




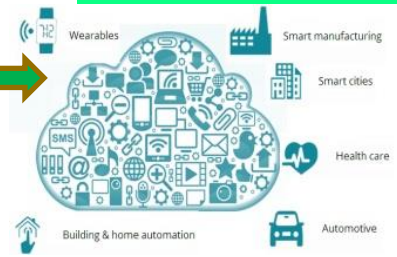
Edge Devices and their deployment



IoT Smart Nodes



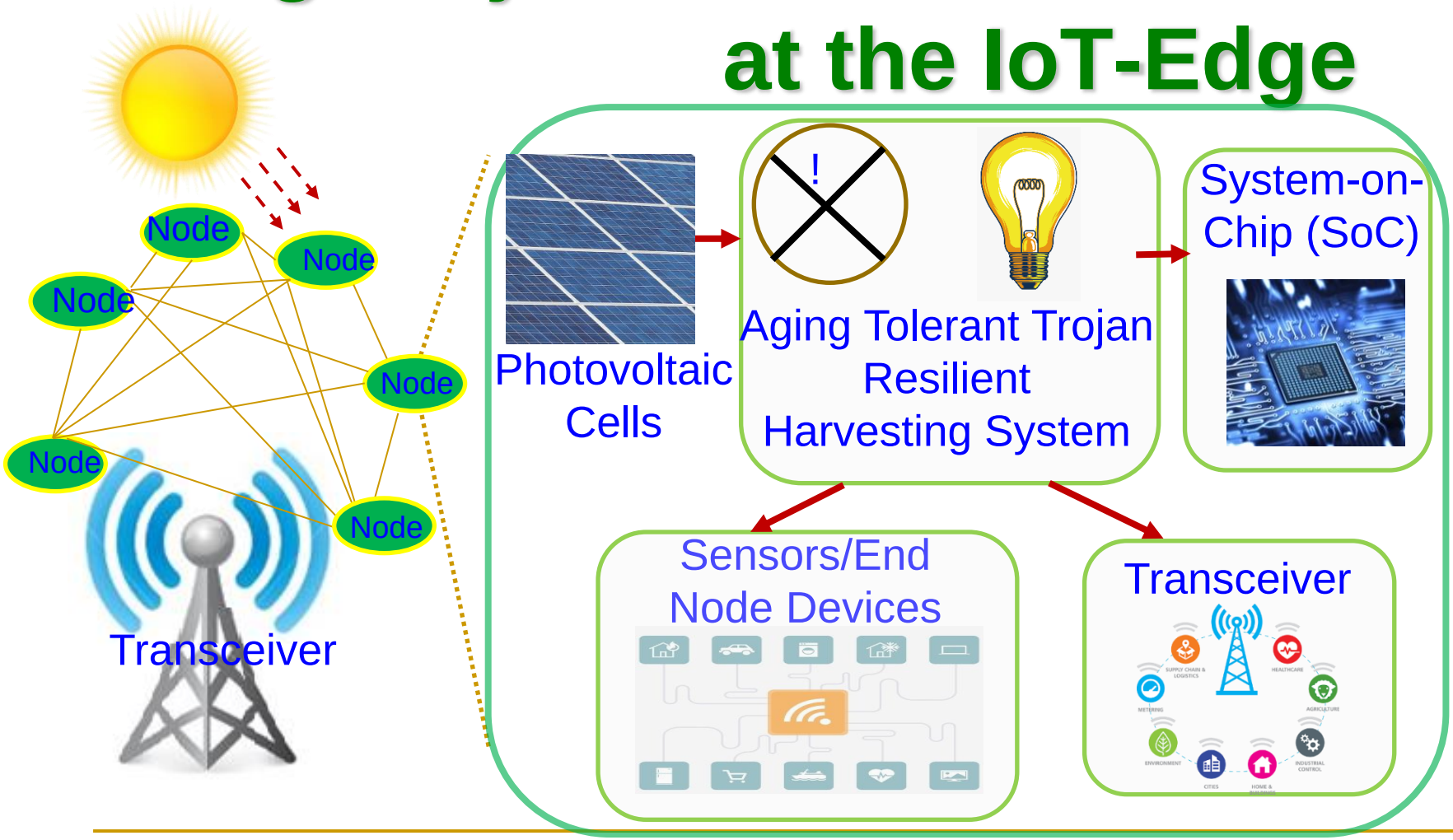
Gateways/ Concentrators



IoT-Cloud

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

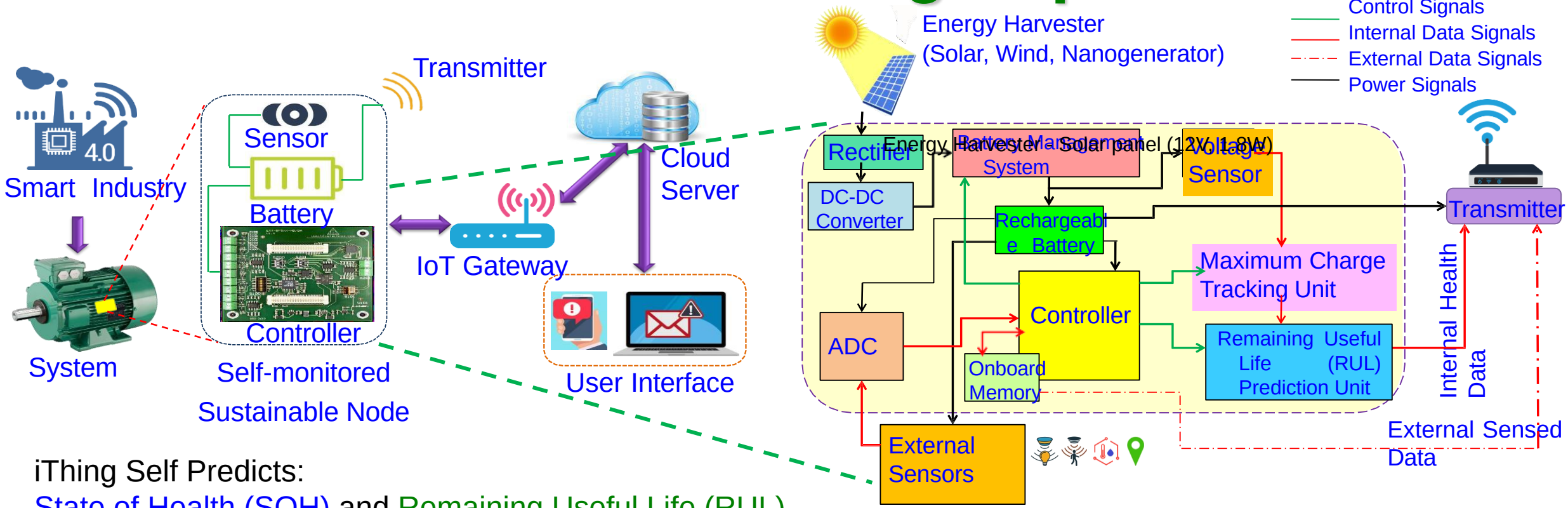
Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge



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

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", arXiv Computer Science, arXiv:2103.05615, March 2021, 24-pages.

iThing: Next-Generation Things with Battery Health Self-Monitoring Capabilities



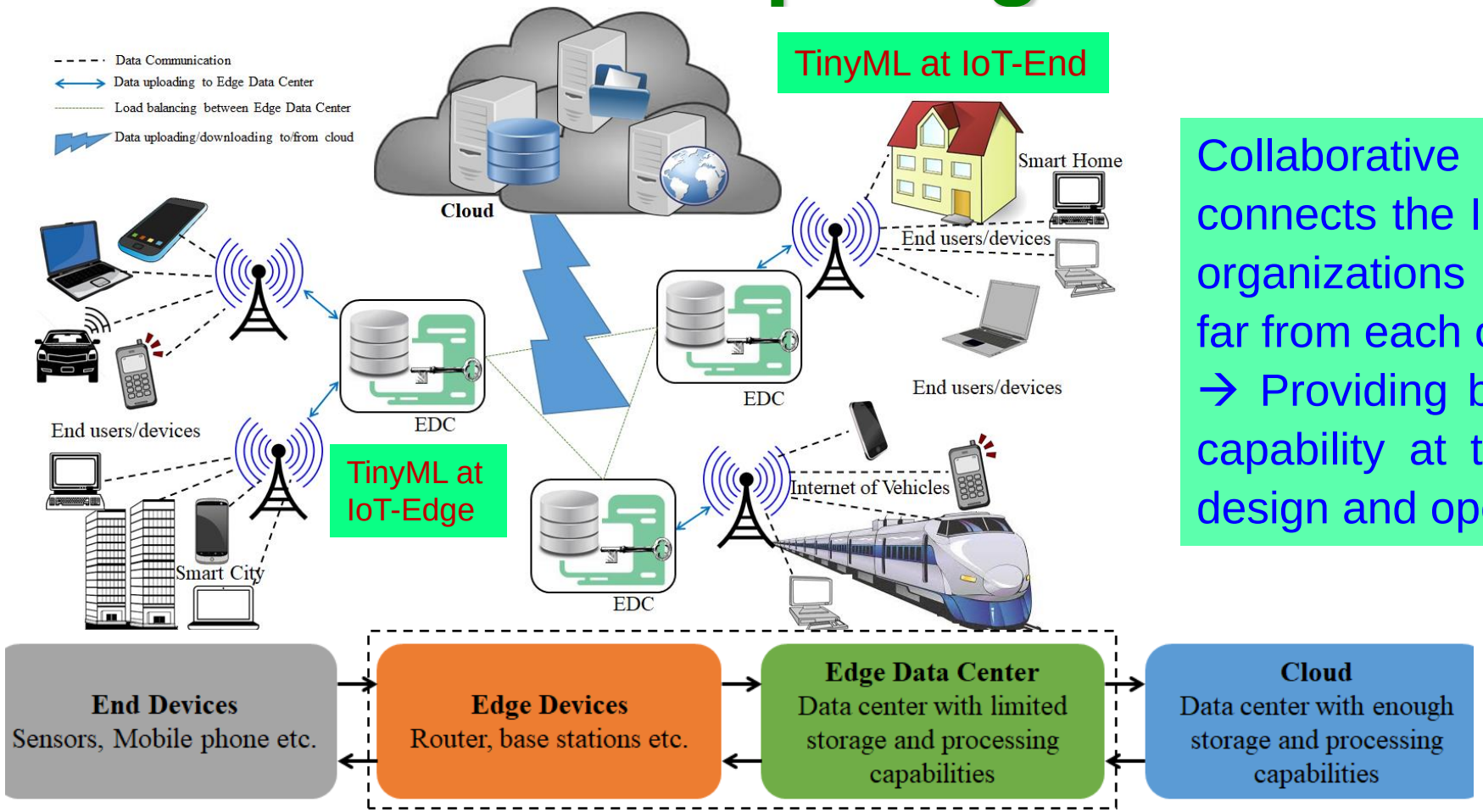
iThing Self Predicts:
State of Health (SOH) and Remaining Useful Life (RUL)
of its on-board battery

Source: A. Sinha, D. Das, V. Udutalapally, and **S. P. Mohanty**, "iThing: Designing Next-Generation Things with Battery Health Self-Monitoring Capabilities for Sustainable IIoT", *IEEE Transactions on Instrumentation and Measurement (TIM)*, Vol. 71, No. 3528409, Nov 2022, pp. 1--9, DOI: https://doi.org/10.1109/TIM.2022.3216594.

Our Long-Term Vision

- How to facilitate AI/ML modeling in smart villages where the computing resources are limited?

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages

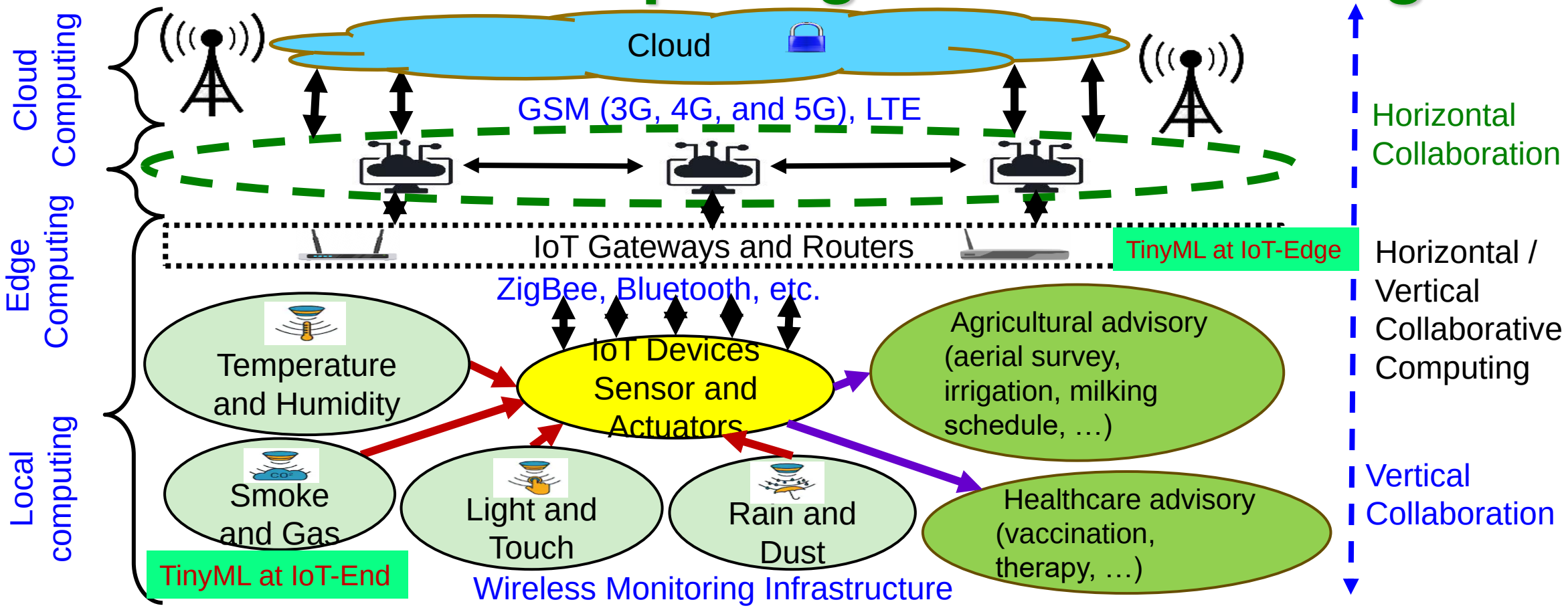


Collaborative edge computing connects the IoT-edges of multiple organizations that can be near or far from each other

→ Providing bigger computational capability at the edge with lower design and operation cost.

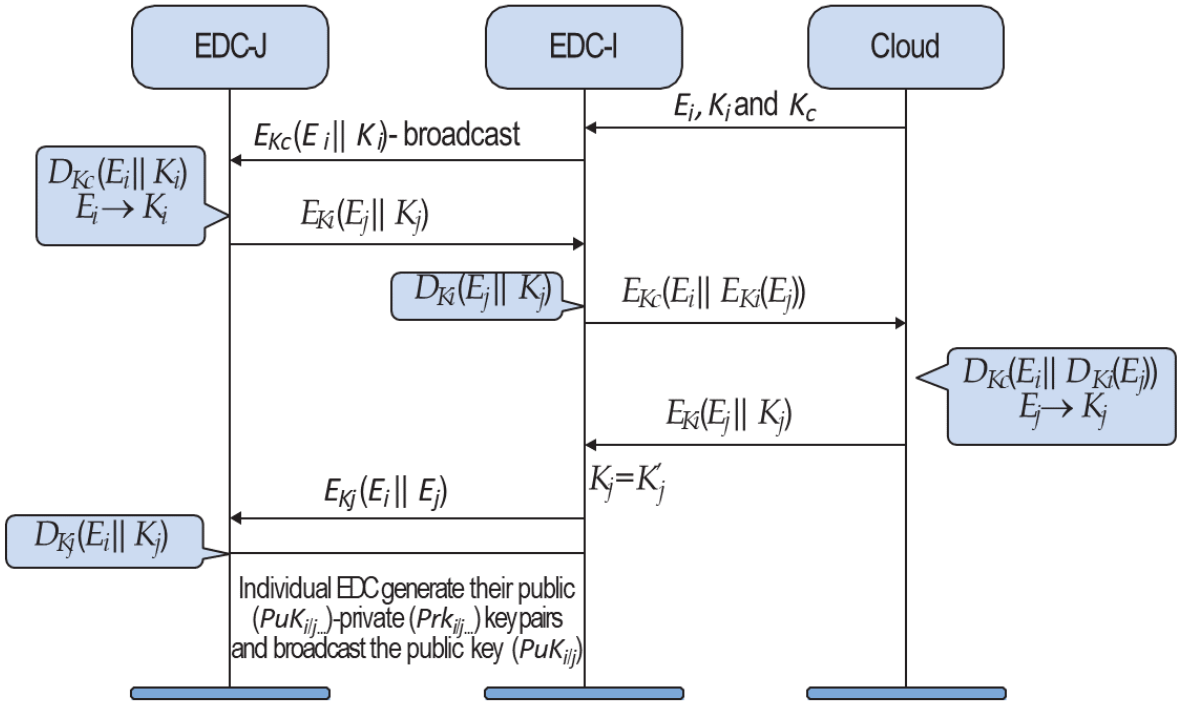
Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing", *IEEE Communications Mag*, Vol. 56, No 5, May 2018, pp. 60--65.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



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

Our Proposed Secure EDC Load Balancing Method



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

Algorithm 1: Load Balancing Technique

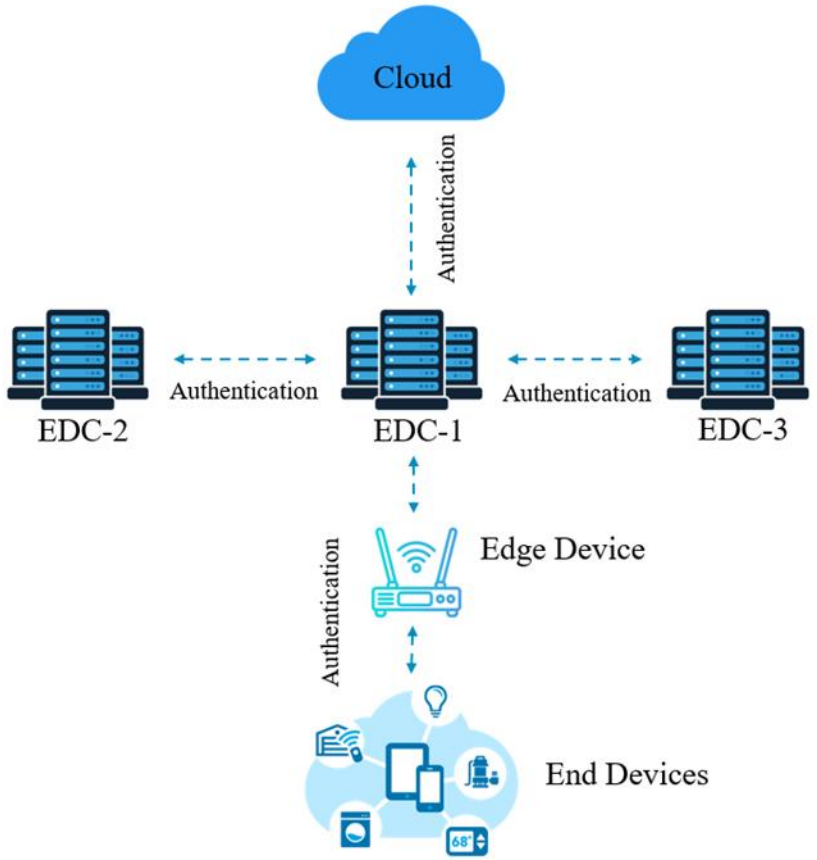
1. If (EDC-I is overloaded)
2. EDC-I broadcast (E_i, L_i)
3. EDC-J (neighbor EDC) verifies:
4. If (E_i is in database) & ($p \leq 0.6 \& L_i << (n-m)$)
5. Response $E_{Kpu_i}(E_j || K_j || p)$
6. EDC-I perform $D_{Kpr_i}(E_j || K_j || p)$
7. $k'_j \leftarrow E_j$
8. If ($k'_j = k_j$)
9. EDC-I select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

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.

Our PUF based CEC Load Balancing

- A PUF-based authentication scheme for Load Balancing
- Virtual XORArbiter PUFs to authenticate the EDCs
- A Mutual Authentication scheme for the EDCs during load balancing
- XORArbiter PUFs to authenticate the user devices connected in the fog environment



Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PUF-based Authentication Scheme for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

Our PUF based EDC Authentication in CEC

EDC Authentication by Cloud

- The EDC in CEC is verified and authenticated by cloud
- Authentication is done based on PUF challenge-Response
- EDC sends authentication request to server
- Server verifies the digital signature
- Sends challenge to client EDC, and verifies the response in Database
- If the CRPs match the EDC is authenticated

EDC-1 Authenticating EDC-2 without Cloud

- EDC authenticate each other without cloud to reduce latency
- EDC-1 sends a request to EDC-2, which will respond back with the payload encrypted with EDC-2's Pu(Public Key)
- EDC-1 decrypts the payload with its Pr(Private Key), once the EDC-2 is verified
- It sends the 64 bit PUF Challenge, C1, and receives the Response R2 from EDC-2
- If the response matches with the response in the Database the EDC-2 is authenticated and data transfer is initiated

Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PUF-based Authentication Scheme for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

Our PUF based … CEC: Comparative Analysis

Research	Algorithm	Hamming Distance	Randomness	Authentication Time
Long et al.[2019]	Double PUF Authentication	46.84%	48.64%	NA
Zhang et al. [2021]	PUF based Multi-Server Authentication	NA	NA	3302.9 ms
Current Paper	XORArbiter PUF	44.86%	48.47%	< 1500 ms

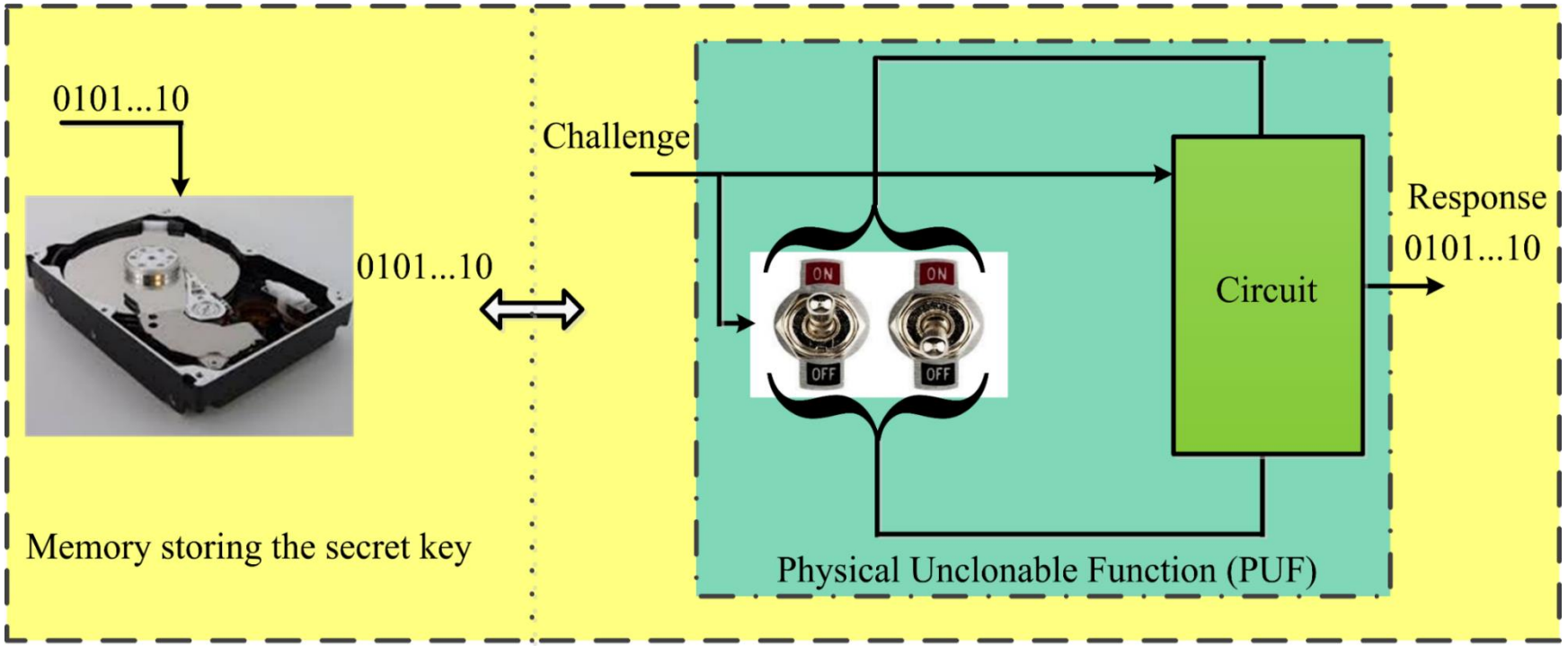
Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, “PUF-based Authentication Scheme for Edge Data Centers in Collaborative Edge Computing”, in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

Physical Unclonable Function – Introduction

Lock and Key

- Earliest mechanical lock found dates back 4000 years.
- Even today, we keep things under LOCK and KEY – but digitally.
- Digital keys are stored in Non – Volatile Memory (NVM) for cryptographic applications.

PUFs Don’t Store Keys

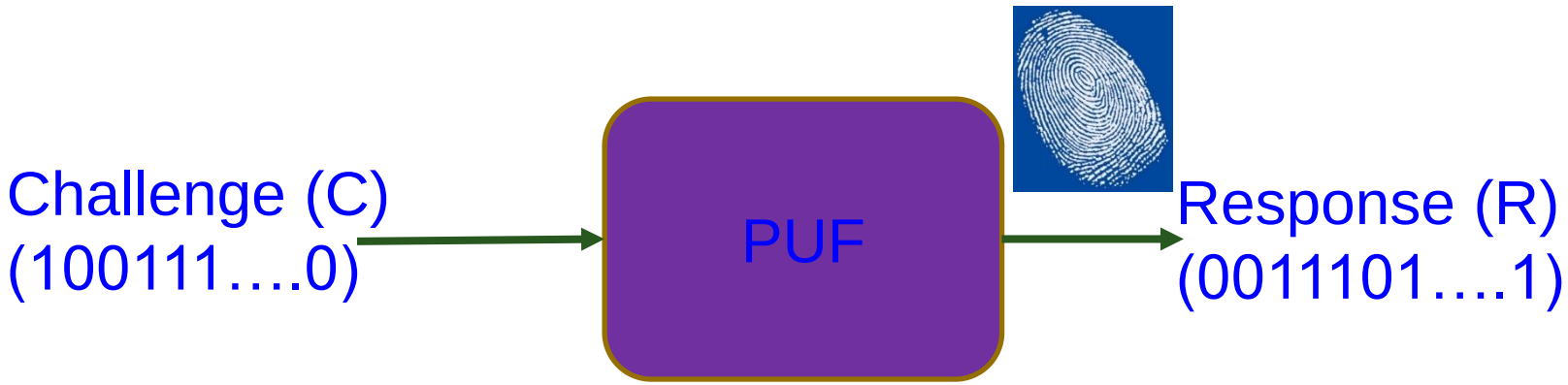


Source: S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything You Wanted to Know about PUFs”, *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

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

Physical Unclonable Functions (PUFs) - Principle

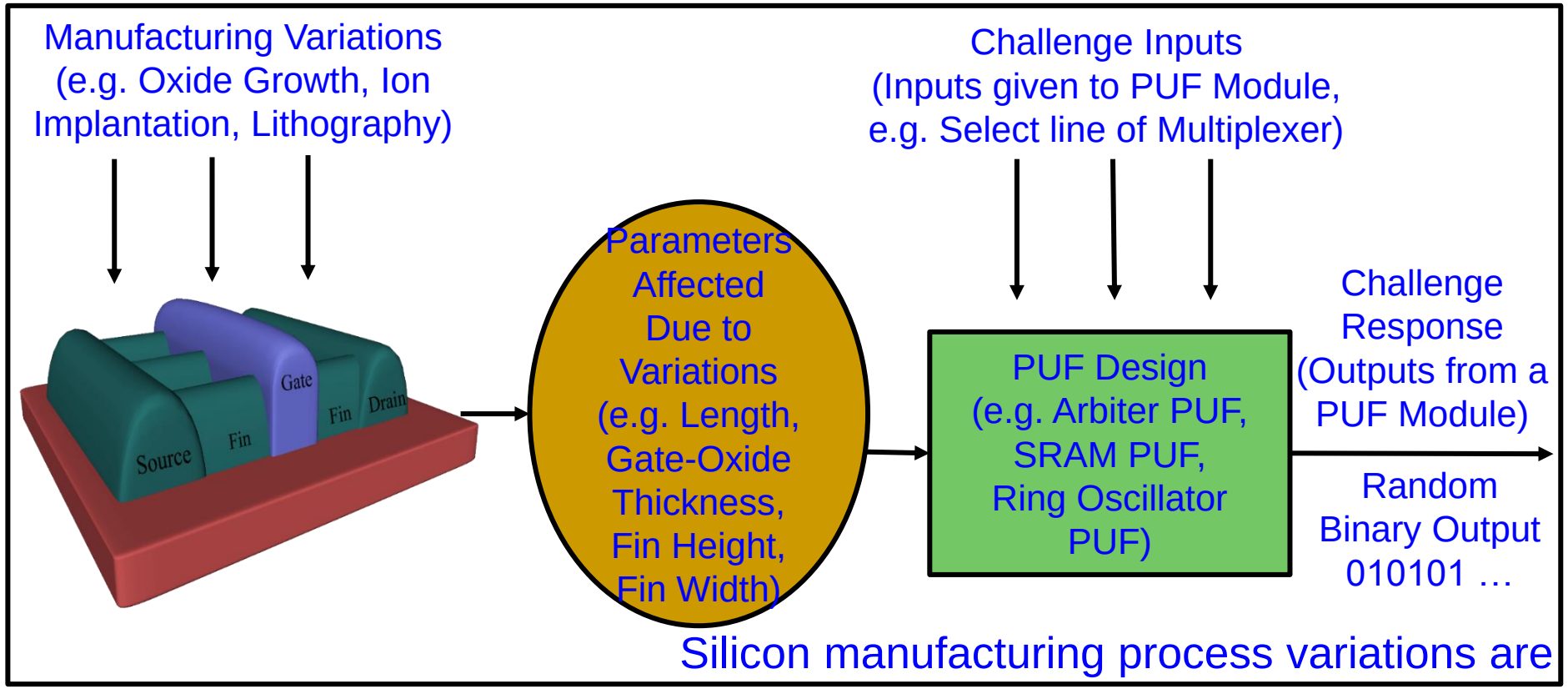
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

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

PUF - Principle

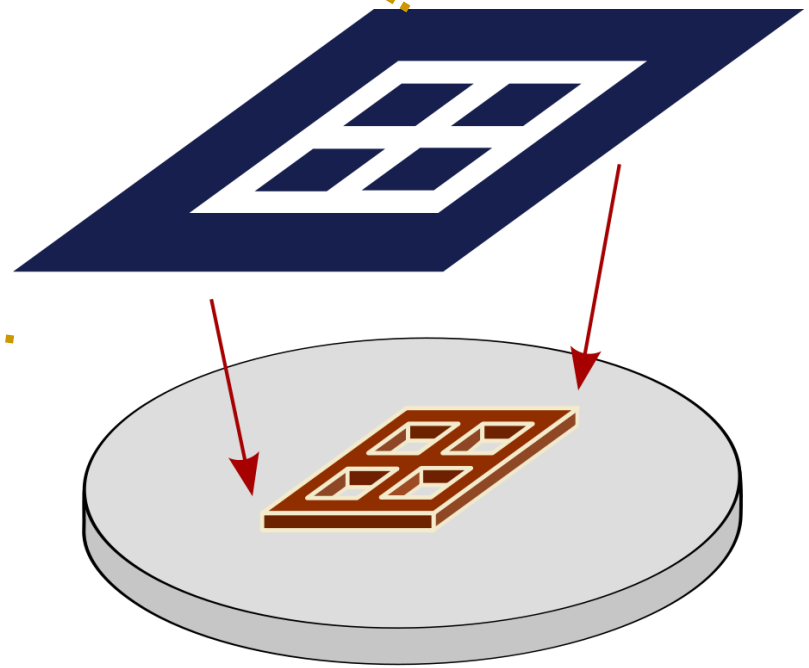


Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT", *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3,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

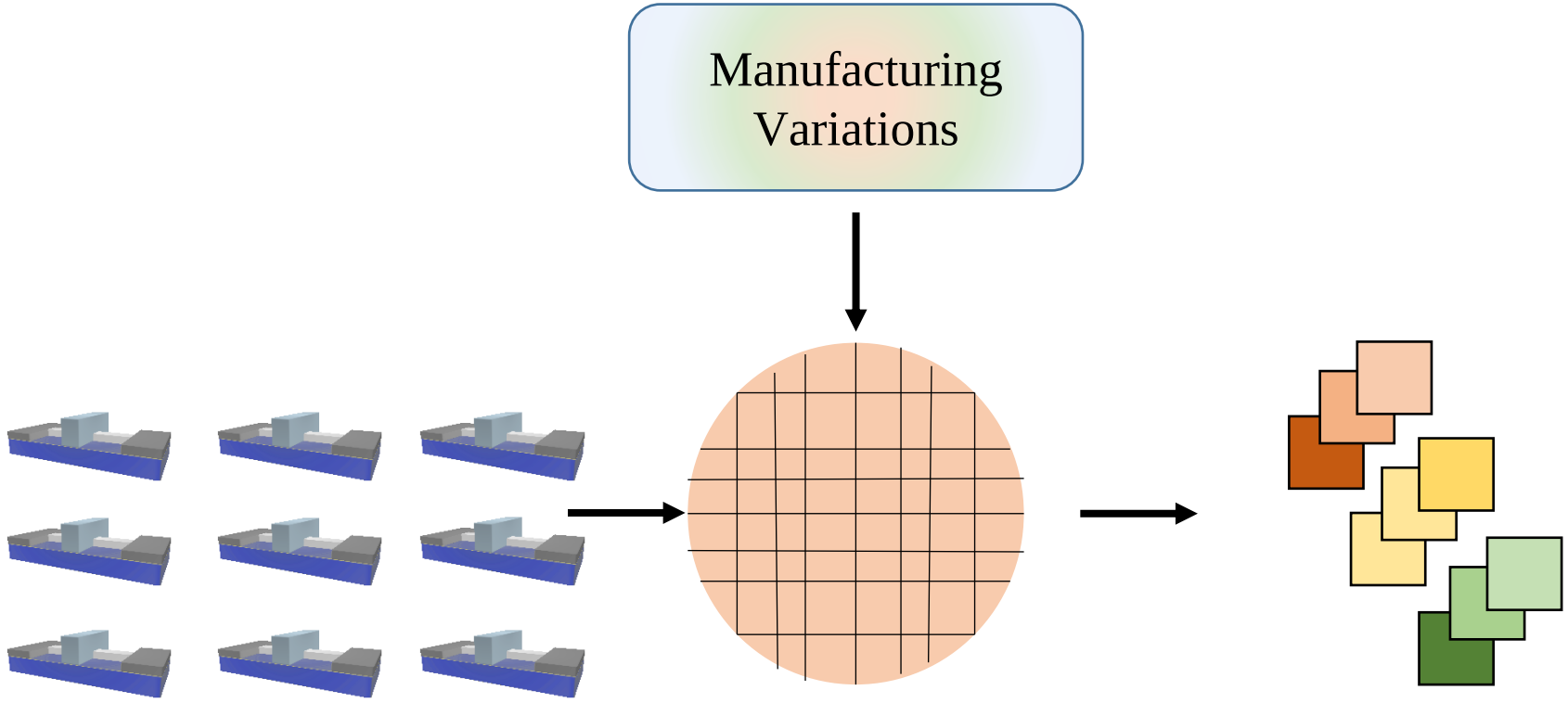
How PUF Works?

Process Variation

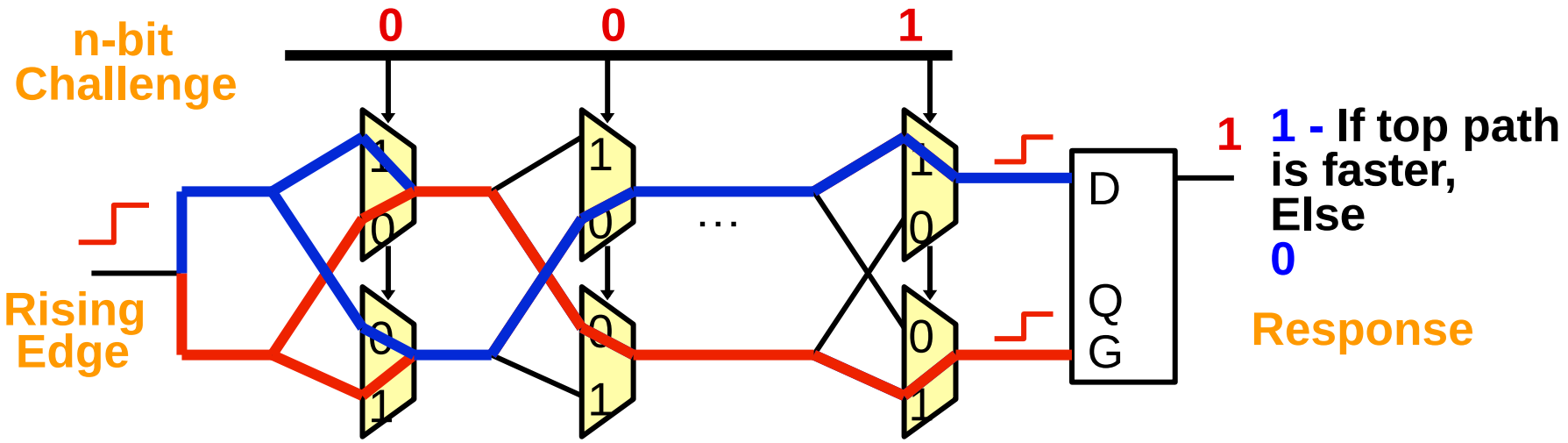
Mismatch Variation



How PUFs Work?



Principle of Generating Random Response using PUF

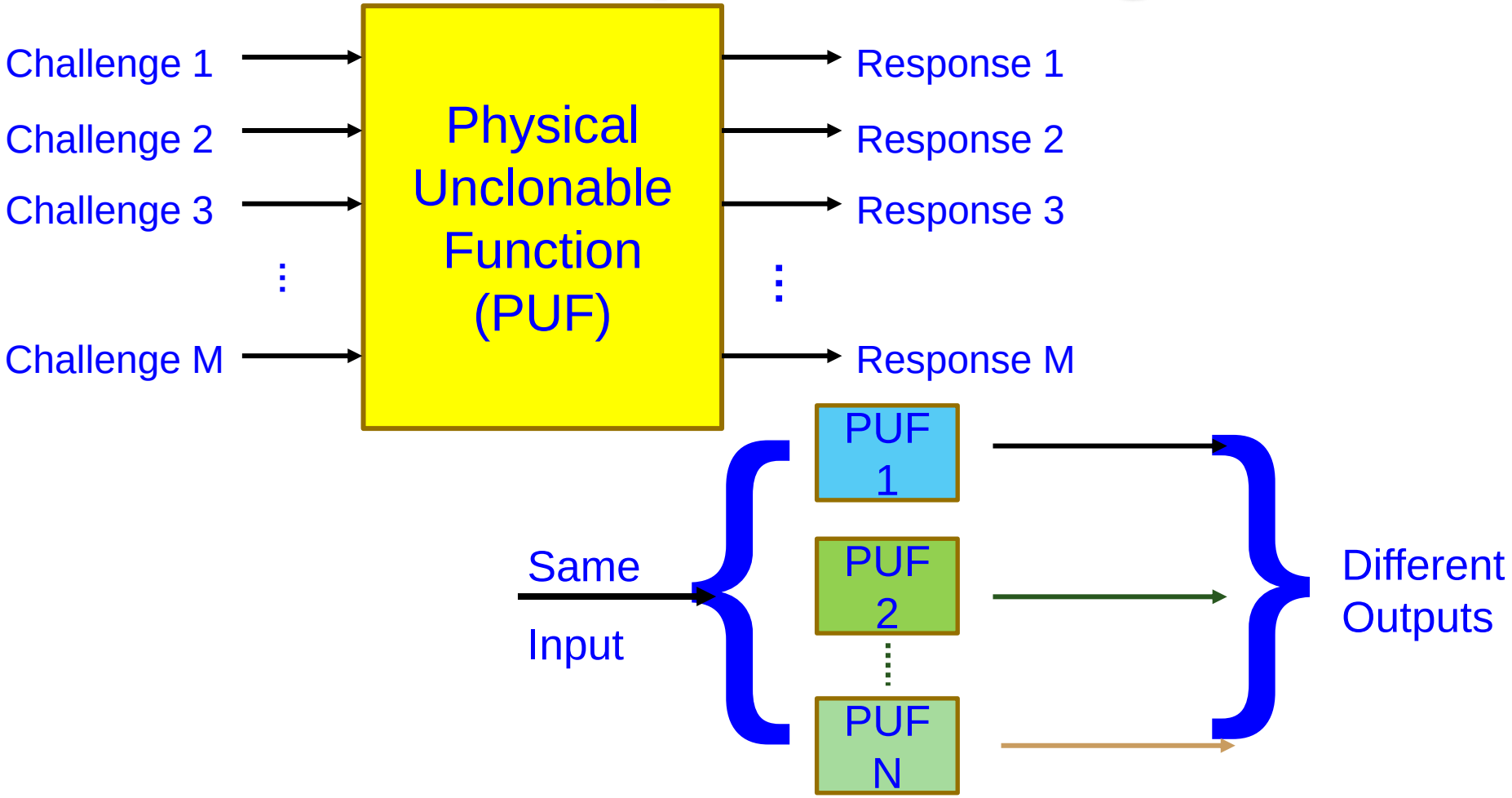


Compare two paths with an identical delay in design

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

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

Principle of Generating Multiple Random Response using PUF



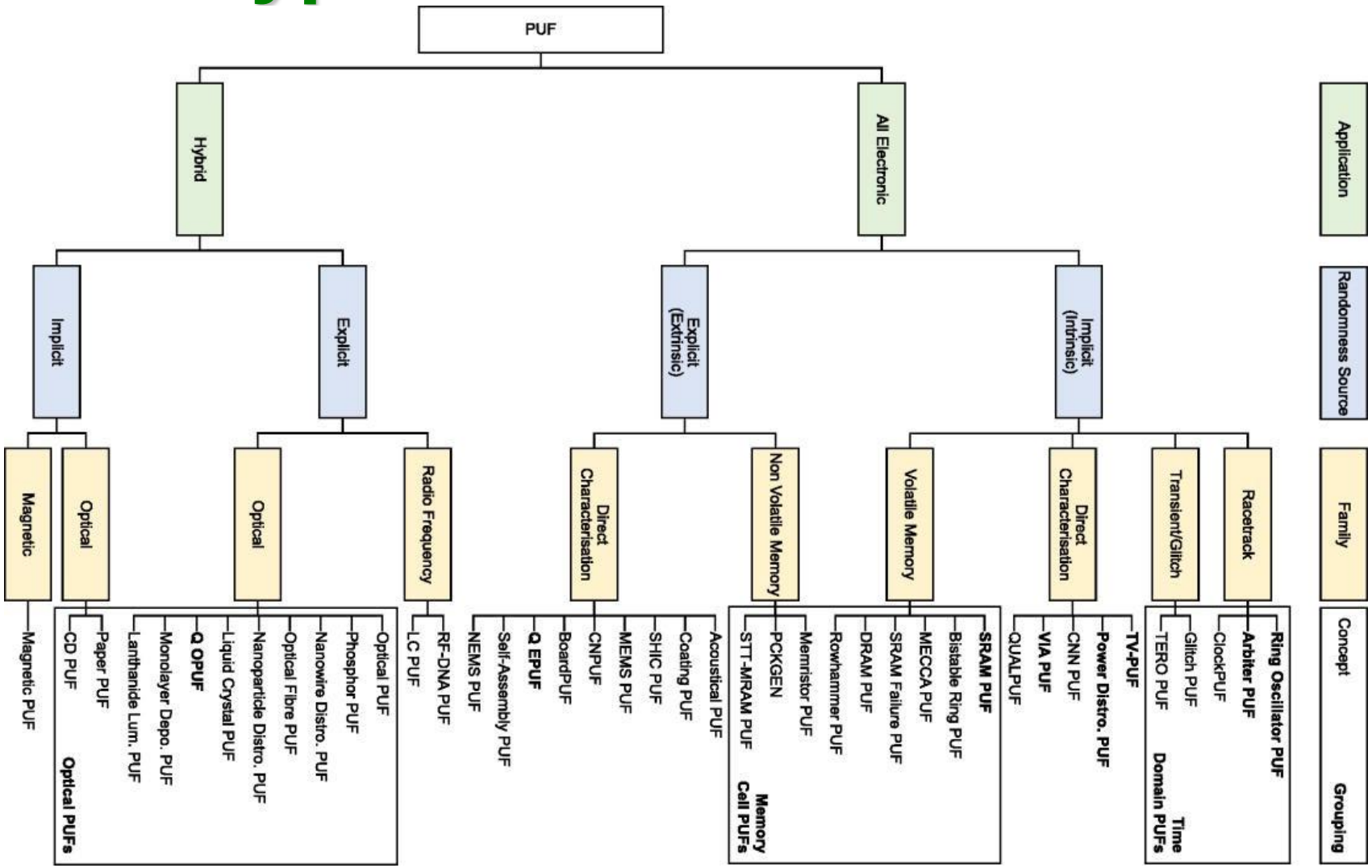
PUF Response is *not* Same as Encryption

PUF vs Encryption

- In classic encryption, decryption key is stored in memory.
- If memory gets attacked, key is compromised.
- Key generated by PUF is not stored in memory.
- PUF extracts manufacturing variations in an IC.
- So PUF generated key acts as fingerprint for the module.

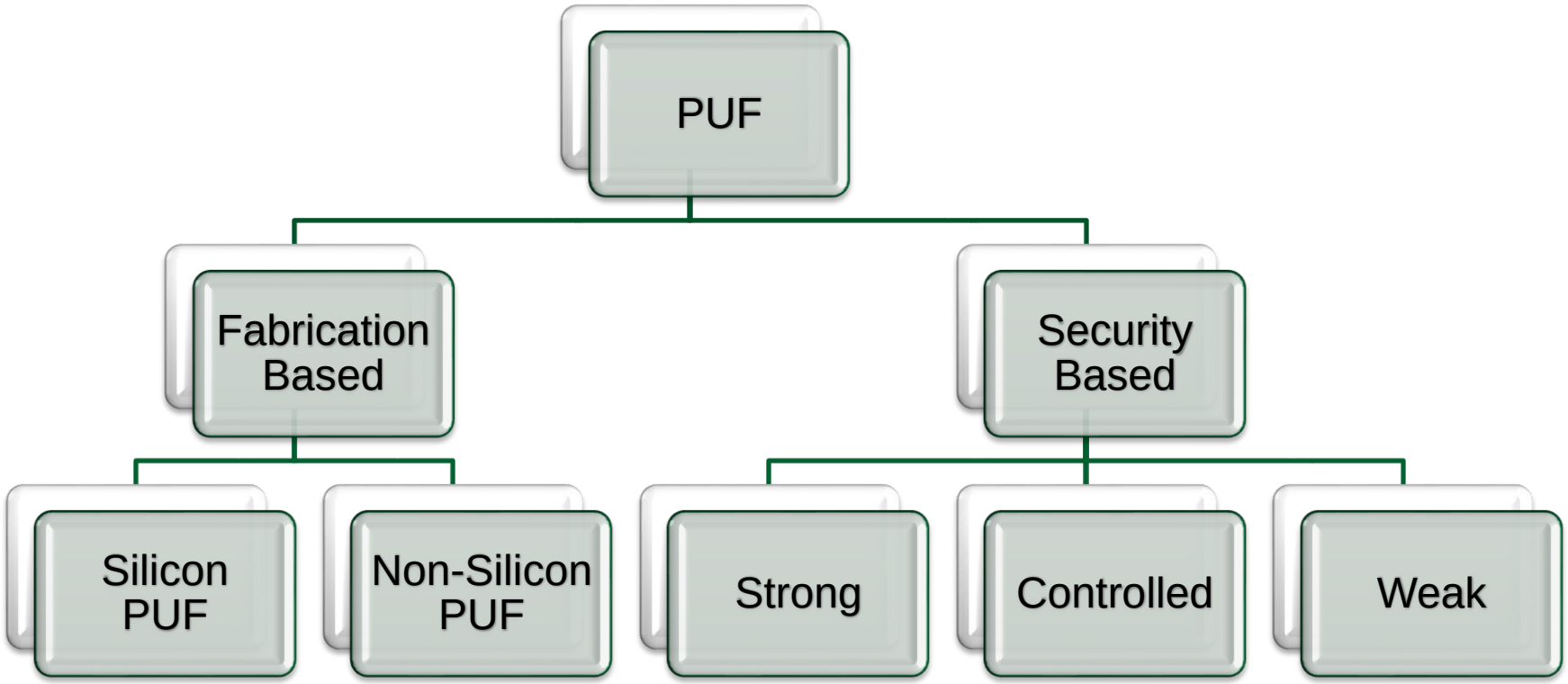
Physical Unclonable Function - Types and Topologies

PUF Types – At Least 40 Different



Source: Thomas McGrath, Ibrahim E. Bagci, Zhiming M. Wang, Utz Roedig, *and* Robert J. Young, "A PUF taxonomy", Applied Physics Reviews 6, 011303 (2019) https://doi.org/10.1063/1.5079407

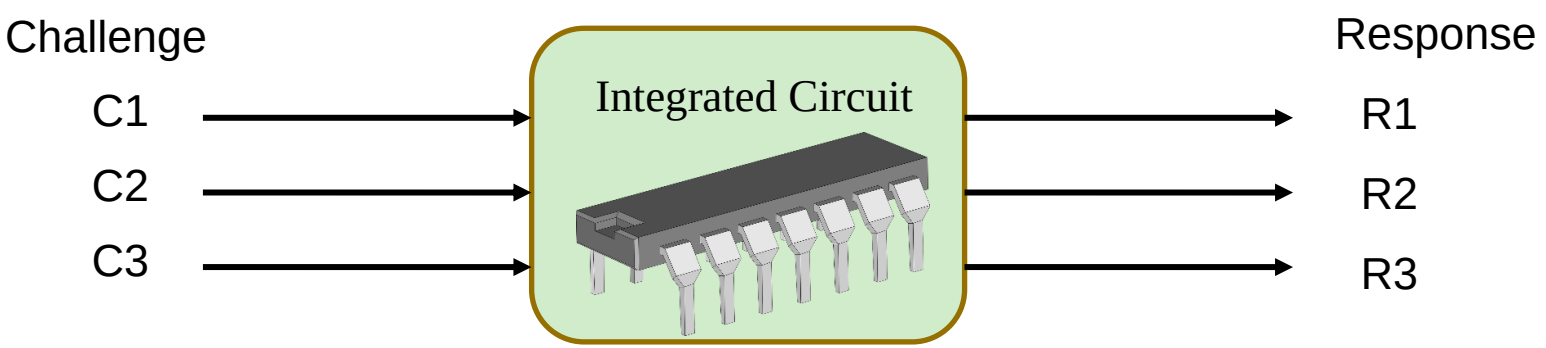
Classification of PUF

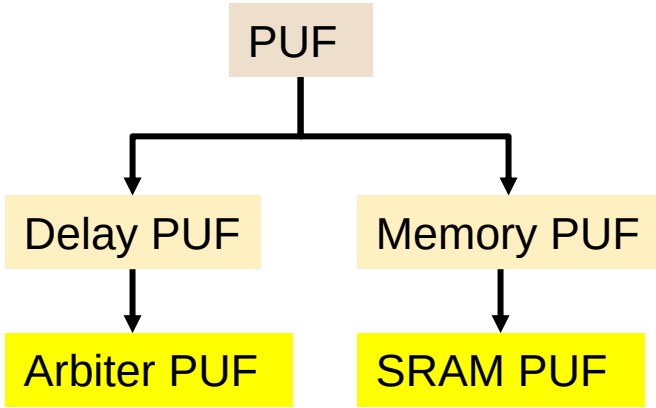


Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Classification of PUF …

- Input to a PUF is called as Challenge and Output from a PUF is called Response.





- A PUF generating large number of CRP is a strong PUF and PUF supporting small number of CRP is considered as Weak PUF.
- A PUF can be categorized as Delay and Memory based PUF. Delay PUF is based on the variations in wiring and variations at gates in silicon. Memory based PUF is based on the instability in the startup phase of SRAM cell.

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.

Classification of PUF …

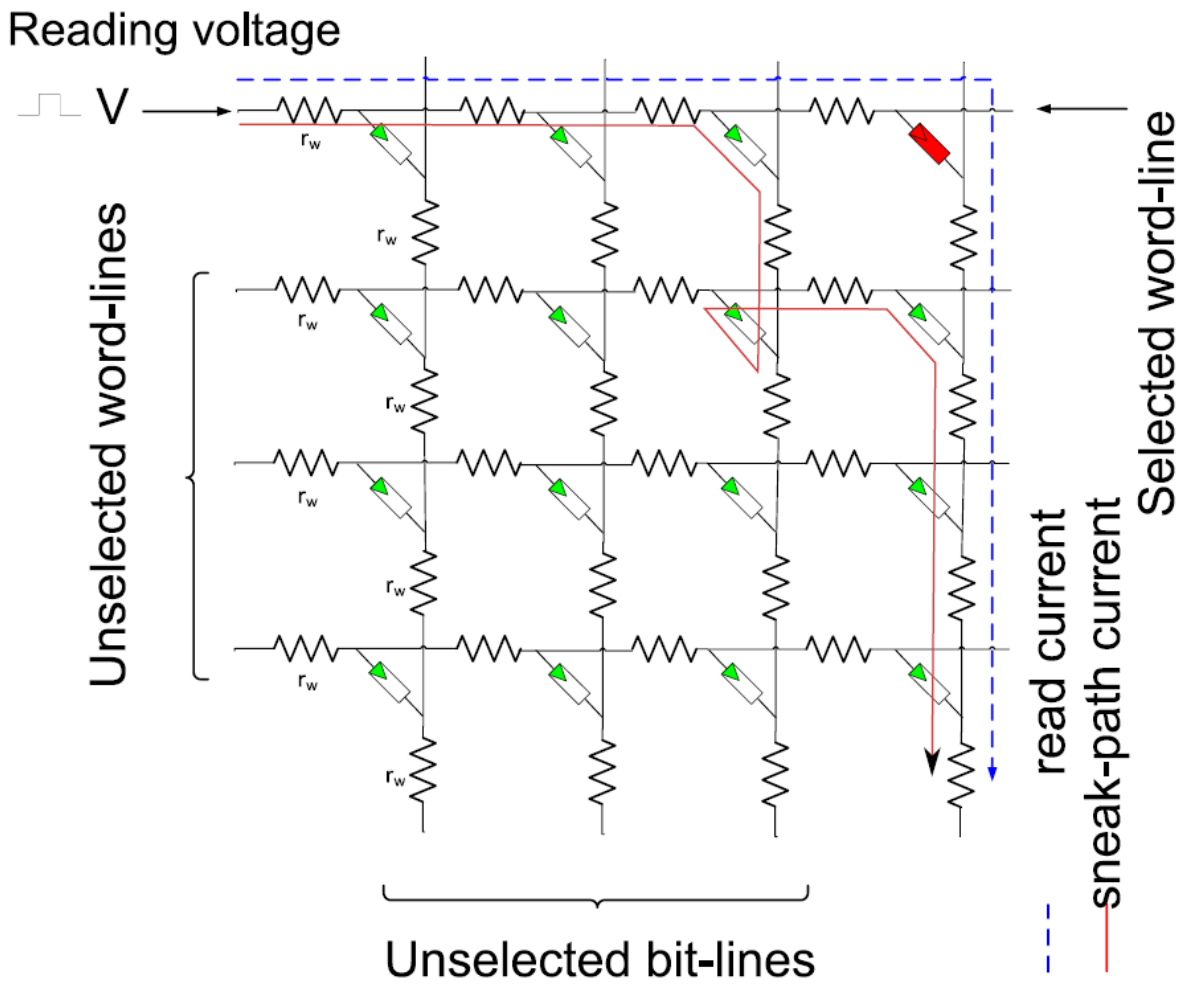
Fabrication Based :

- Silicon based Integrated Circuits can be used for PUF.
- There are also Non-Silicon based PUF like optical PUF, RF PUF and so on.

Security Based :

- Strong PUF generates very high number of Challenge Response Pairs.
- Weak PUF generates low number of Challenge Response Pairs and lowest being ‘1’.
- In a Controlled PUF, inputs and outputs are processed.

Memristor PUF (Weak–Write–Based)



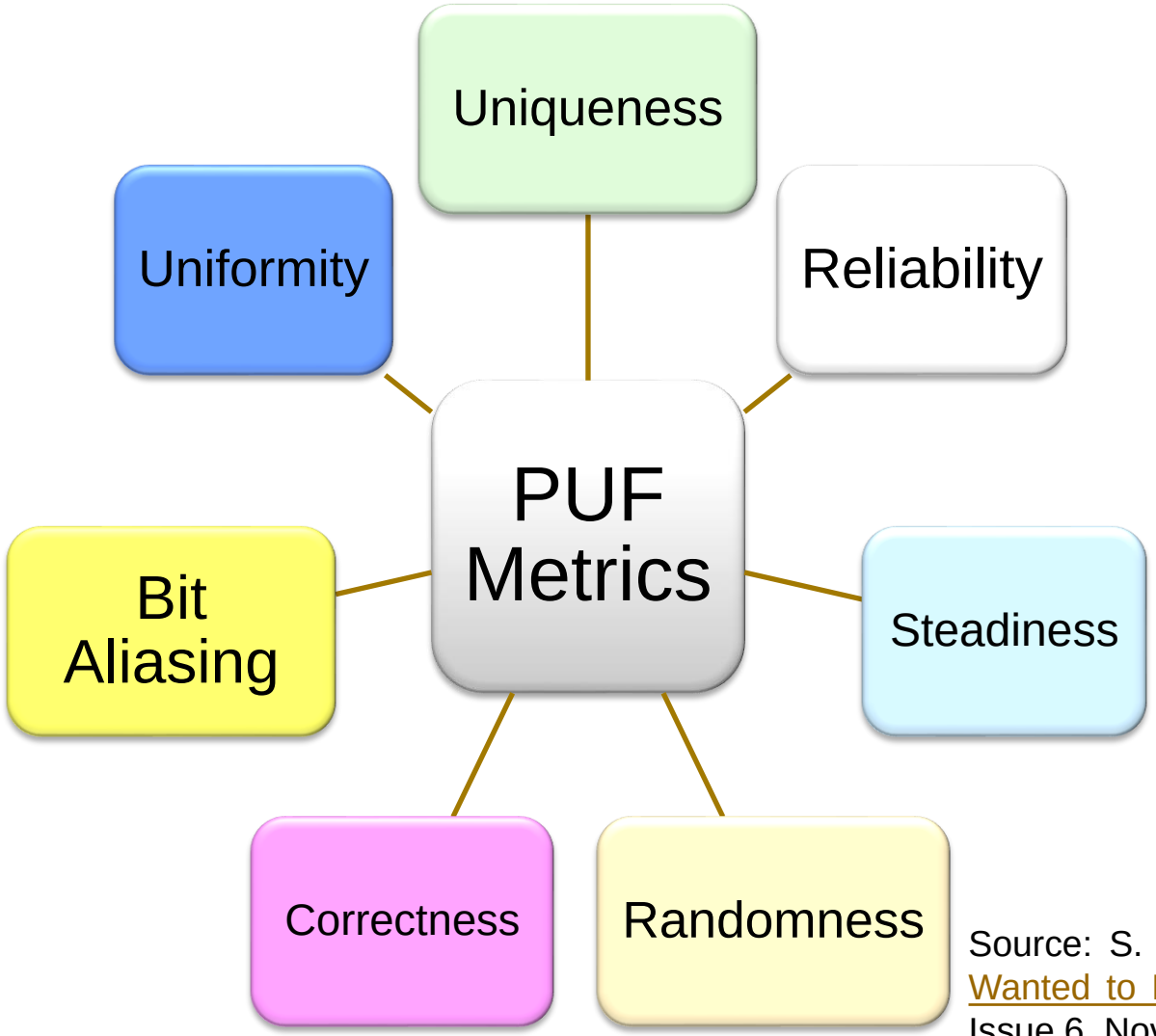
Source: Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," in *IEEE Access*, vol. 4, pp. 61-80, 2016, doi: 10.1109/ACCESS.2015.2503432.

Physical Unclonable Function - Characteristics

Performance Metrics …

Can any circuit become PUF?

PUF - Performance Metrics



AKA - Figure of Merits

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.

Performance Metrics …

- Uniqueness:
  - Measure of average inter-chip Hamming Distance of response. Ideal is 50%.
- Reliability:
  - Measure of how much reliable CRP under noise and environmental variations. Ideal is 0% - Hamming Distance should be 0.
- Randomness:
  - Number of 0's and 1's in a PUF key. There should be 50% 1's and 50% 0's.

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.

Performance Metrics …

- Correctness:
  - Measure of correctness of response under different operating conditions.
- Bit Aliasing:
  - It is measure of biasness of particular response bit across several chips. Ideal value is 50%. There should be no correlation between any of the outputs generated by different PUF modules.
- Steadiness:
  - Measure of biasness of response bit for a given number of 0's and 1's over total number of samples gives the steadiness. Ideal value is 100%.

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.

More Performance Metrics …

- Tamper Sensitivity:
  - The PUF module designed and deployed should be Tamper Resistant.
- Indistinguishability:
  - PUF key generated should not be similar to any random string of numbers
- Unpredictability:
  - PUF responses generated should not be predicted by any algorithm or machine learning.

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.

More Performance Metrics …

- Average Power consumption:
  - The average power consumed by the entire PUF module.
- Speed:
  - The output key generation latency should be low.

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

Physical Unclonable Function - Challenges and Research

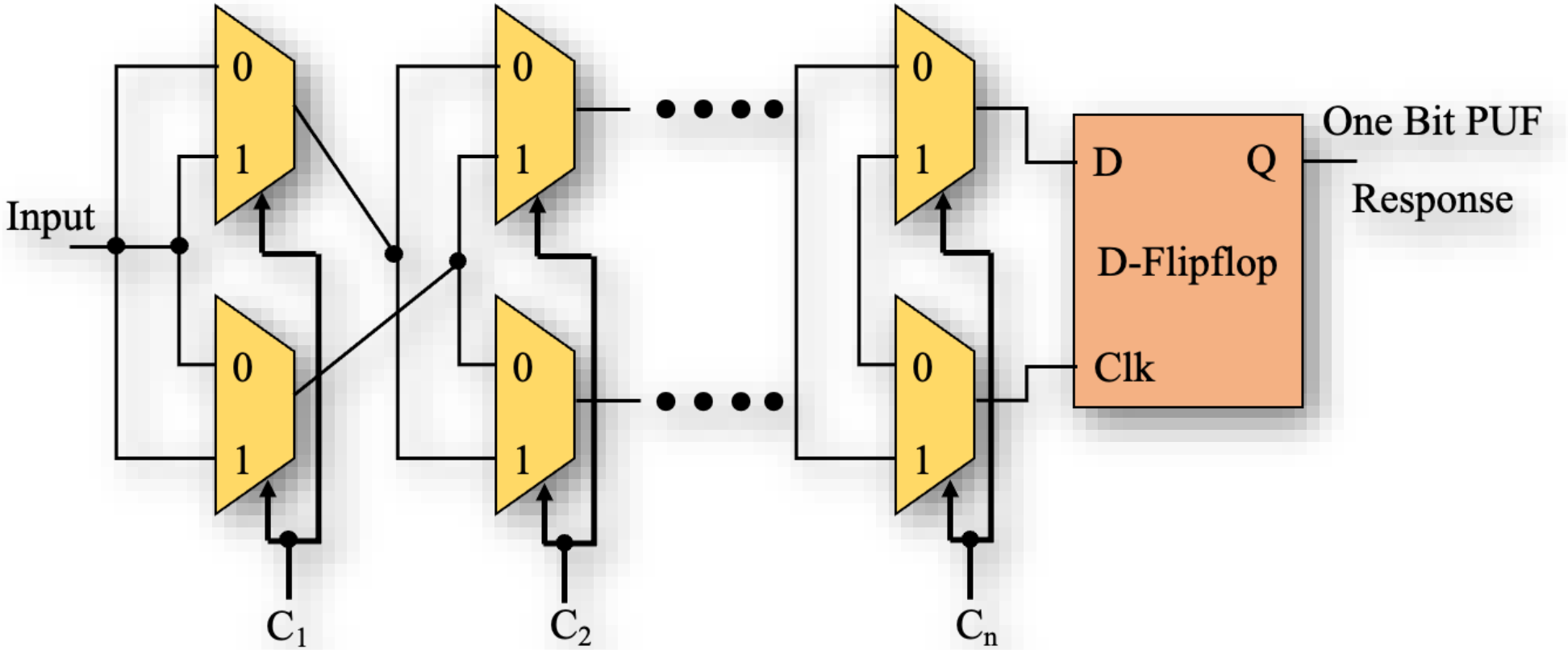
If PUF is So Great, Why Isn't Everyone Using It?

- PUF technology is difficult to implement well.
- In addition to security system expertise, one needs analog circuit expertise to harness the minute variances in silicon and do it reliably.
- Some PUF implementations plan for a certain amount of marginality in the analog designs, so they create a PUF field of 256 bits (for example), knowing that only 50 percent of those PUF features might produce reliable bits, then mark which features are used on each production part.
- PUF technology relies on such minor variances, long-term quality can be a concern: will a PUF bit flip given the stresses of time, temperature, and other environmental factors?
- Overall the unique mix of security, analog expertise, and quality control is a formidable challenge to implementing a good PUF technology.

Source: https://embeddedcomputing.com/technology/processing/semiconductor-ip/demystifying-the-physically-unclonable-function-puf

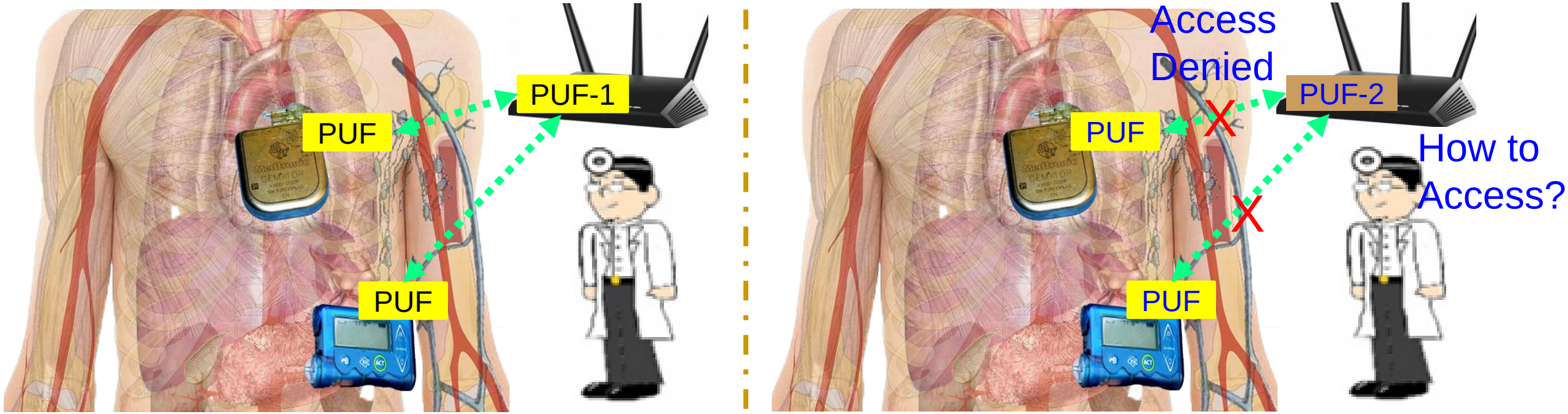
PUF Limitations – Larger Key Needs Large ICs

- Larger key requires larger chip circuit.



1 – Bit Arbiter PUF Architecture

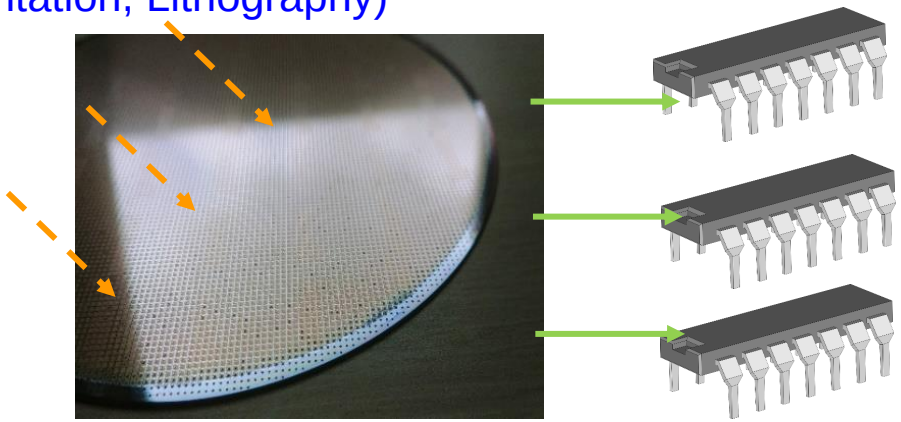
PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma



IC for PUF – Variability versus Variability-Aware Design

Variability → Randomness for PUF

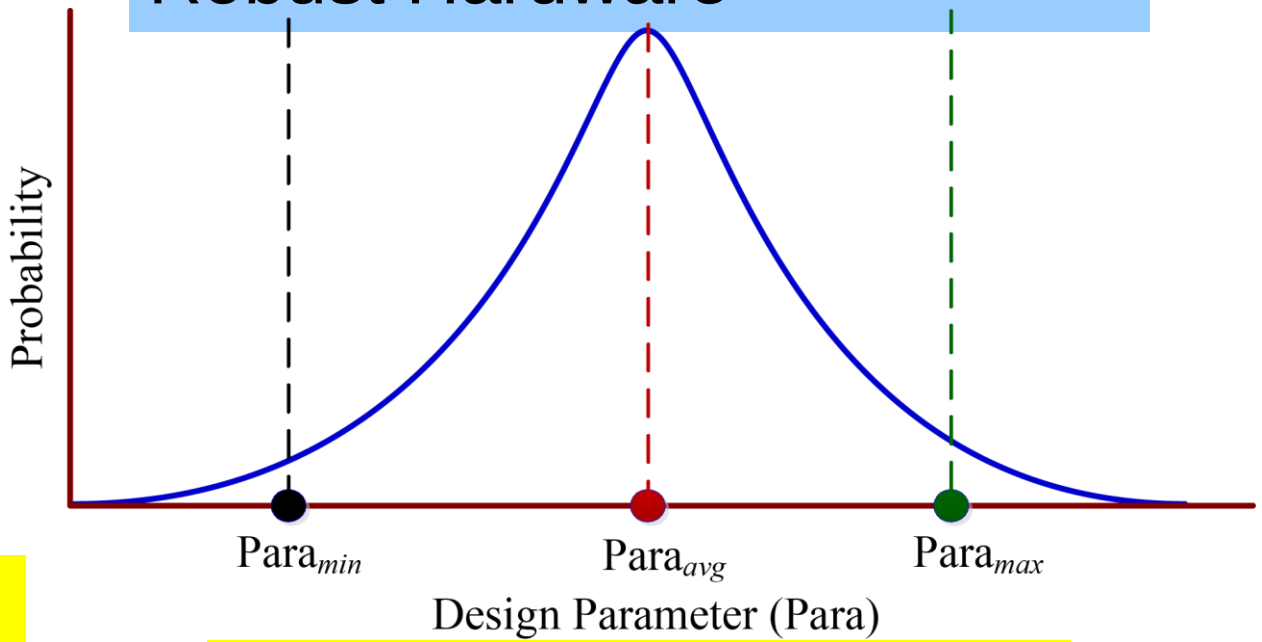
Manufacturing Variations (e.g. Oxide Growth, Ion Implantation, Lithography)



Variability Features → Randomness → PUF

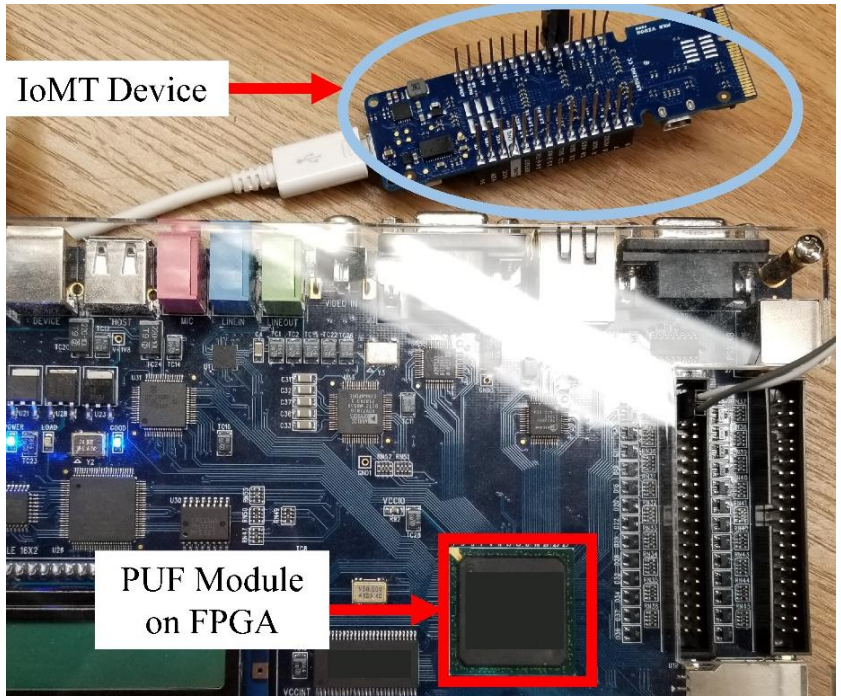
Is it not case of Conflicting Objectives?
How to have a Robust-IC design that functions as a PUF?

Variability-Aware Design → Robust Hardware



Optimize ($\mu+n\sigma$) to reduce variability for Robust Design

PUF – FPGA versus IC



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.

- Faster prototyping
- Lesser design effort
- Minimal skills
- Cheap
- Rely on already existing post fabrication variability

Source: **S. P. Mohanty** and E. Kougianos, "Incorporating Manufacturing Process Variation Awareness in Fast Design Optimization of Nanoscale CMOS VCOs", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 27, Issue 1, February 2014, pp. 22--31.

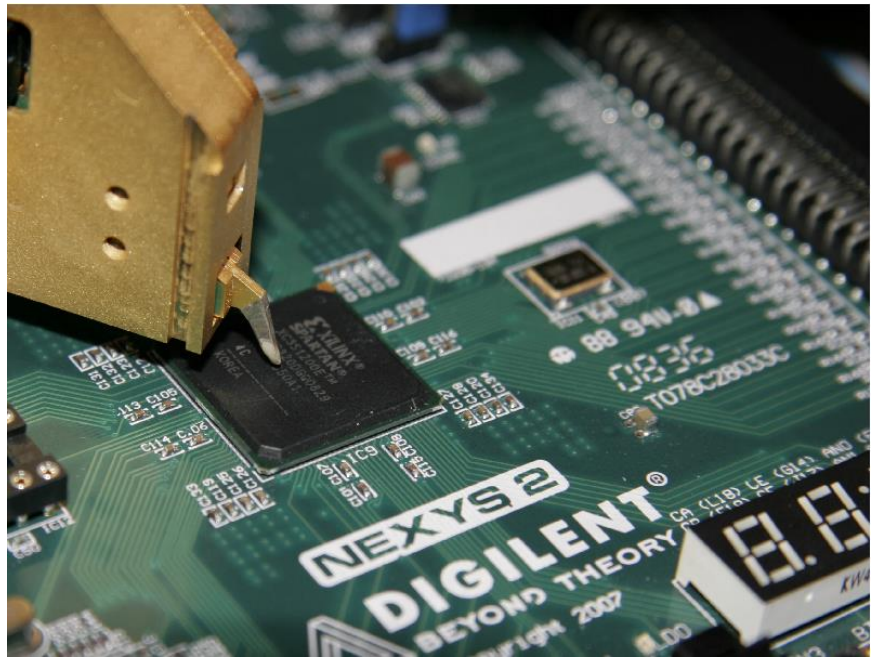
- Takes time to get it from fab
- More design effort
- Needs analog design skills
- Can be expensive
- Choice to send to fab as per the need

PUF - Side Channel Leakage

- Cryptography and watermarking hardwares provide low-power consumption, real-time performance, higher reliability and low-cost along with easy integration in multimedia hardware.
- Cryptography and watermarking hardware which are implemented using CMOS technology are susceptible to side channel attacks which collects information from physical implementation rather than software weakness.
- DFX targeted for information leakage proof is very in the current information driven society.

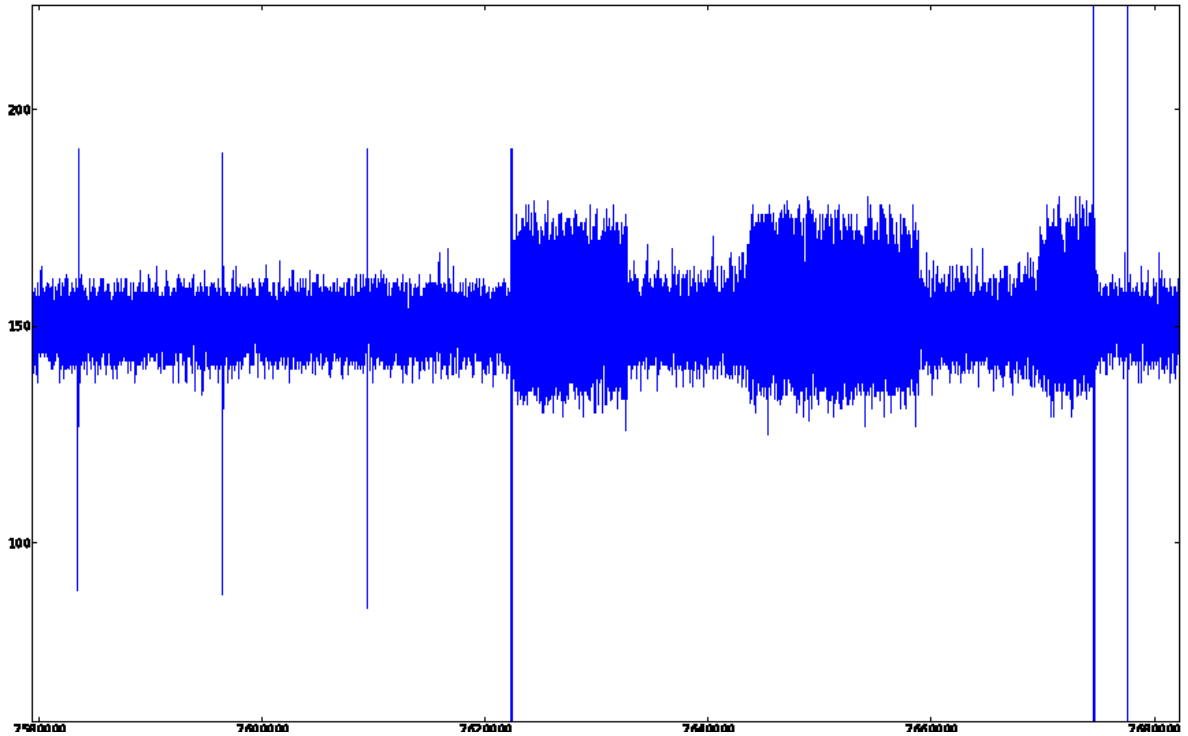
PUF - Side Channel Leakage

- Delay-based PUF implementations are vulnerable to side-channel attacks.



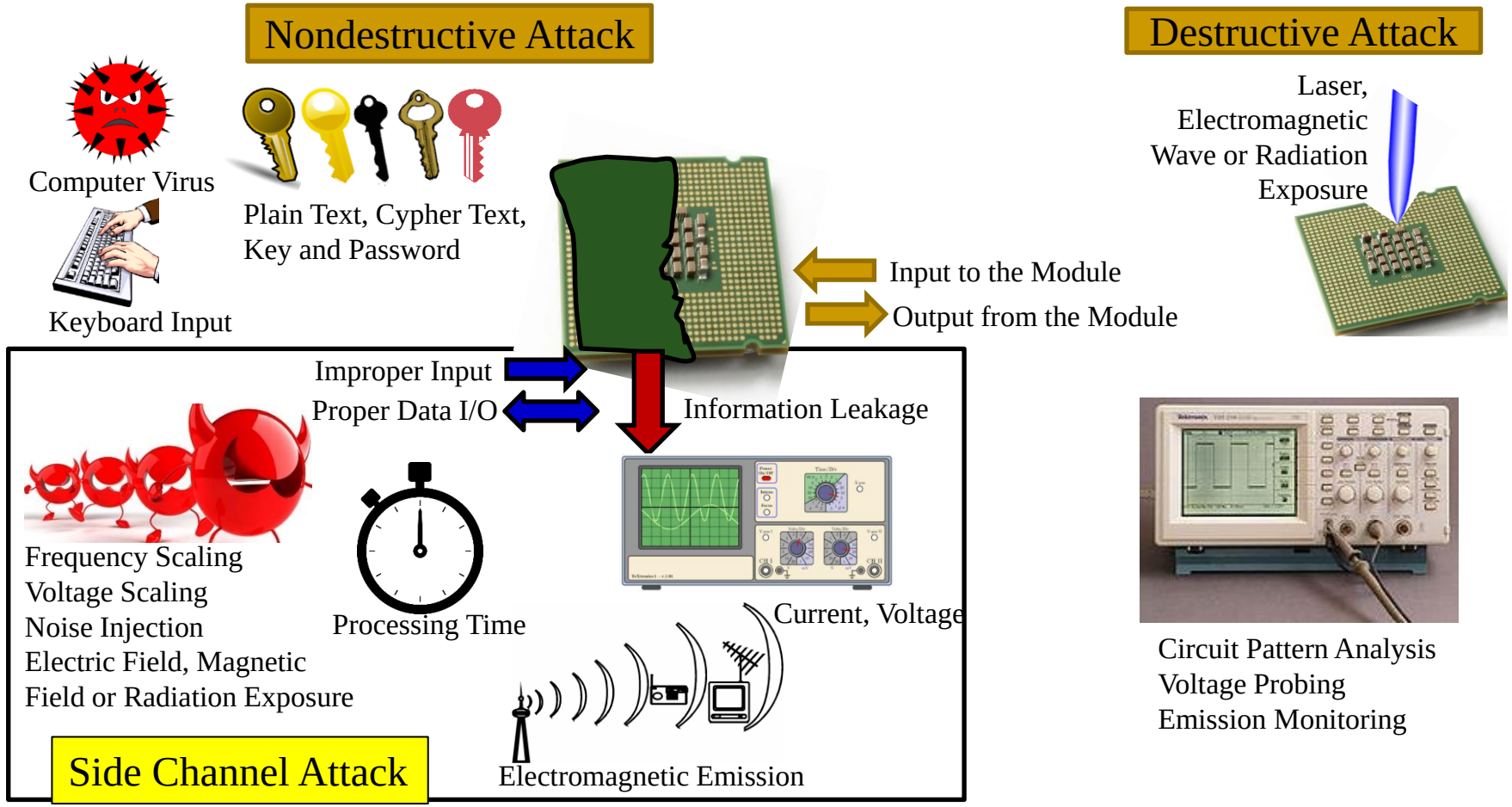
Langer ICR HH 150 probe over Xilinx Spartan3E-1200 FPGA

Source: Merli, D., Schuster, D., Stumpf, F., Sigl, G. (2011). Side-Channel Analysis of PUFs and Fuzzy Extractors. In: McCune, J.M., Balacheff, B., Perrig, A., Sadeghi, AR., Sasse, A., Beres, Y. (eds) Trust and Trustworthy Computing. Trust 2011. Lecture Notes in Computer Science, vol 6740. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21599-5_3



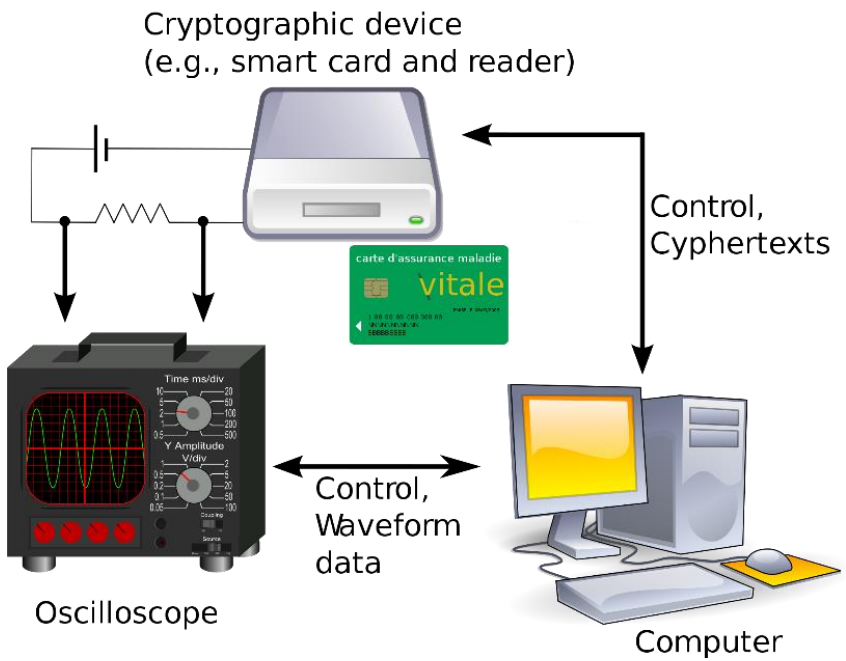
Magnification of the last part of the complete trace. Three trigger signals can be identified: (1) between oscillator phase and error correction phase, (2) between error correction and hashing, and (3) at the end of hashing.

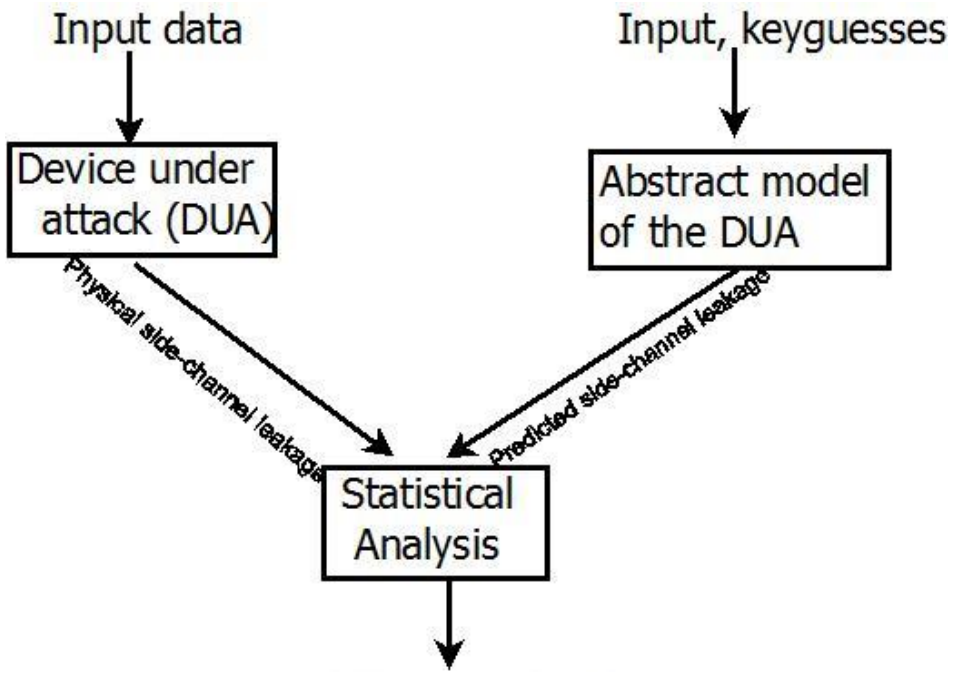
Side Channel Attacks



Source: http://www.keirex.com/e/Kti072_SecurityMeasure_e.html

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





Side Channel Attacks - Correlation Power Analysis (CPA)

- CPA analyzes the correlative relationship between the plaintext/ cipher-text and instantaneous power consumption of the cryptographic device.
- CPA is a more effective attacking method compared with DPA.

Differential Power Analysis (DPA)

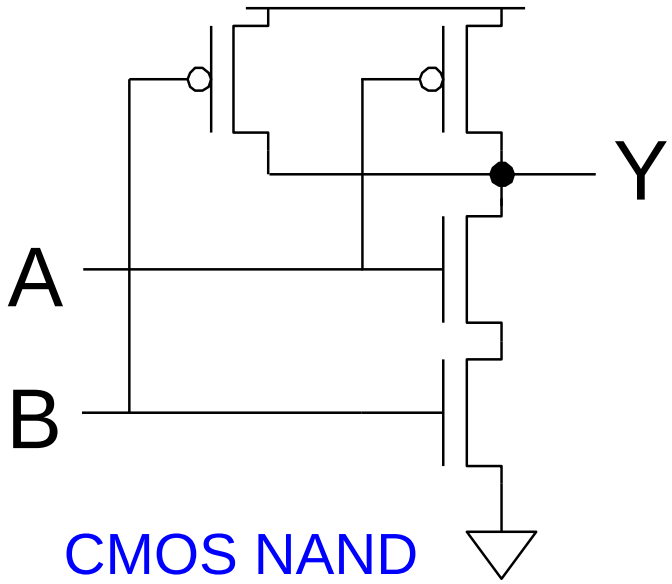
- Attacks using relationship between data and power.
- Looks at difference of category averages for all key guess.
- Requires more power traces than CPA.
- Slower and less efficient than CPA.

Correlation Power Analysis (CPA)

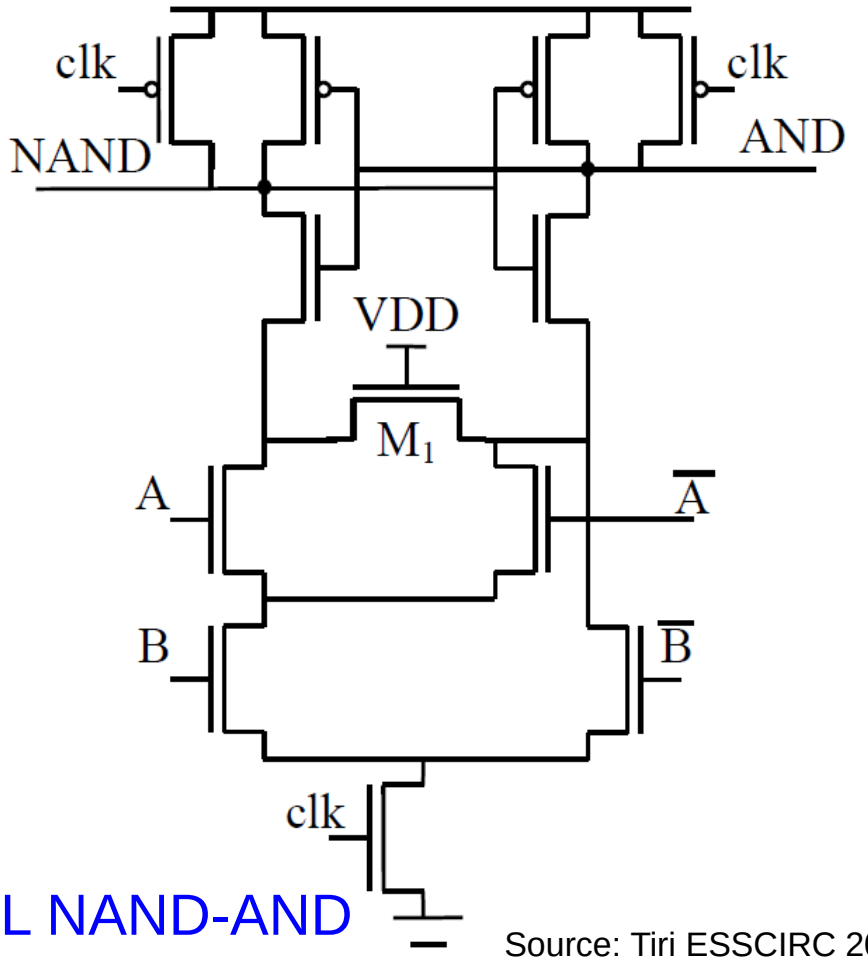
- Attacks using relationship between data and power.
- Looks at correlation between all key guesses.
- Requires less power traces than DPA.
- Faster, more accurate than DPA.

Source: Zhang and Shi ITNG 2011

DPA Resilience Hardware:
Sense Amplifier Basic Logic (SABL)



CMOS NAND

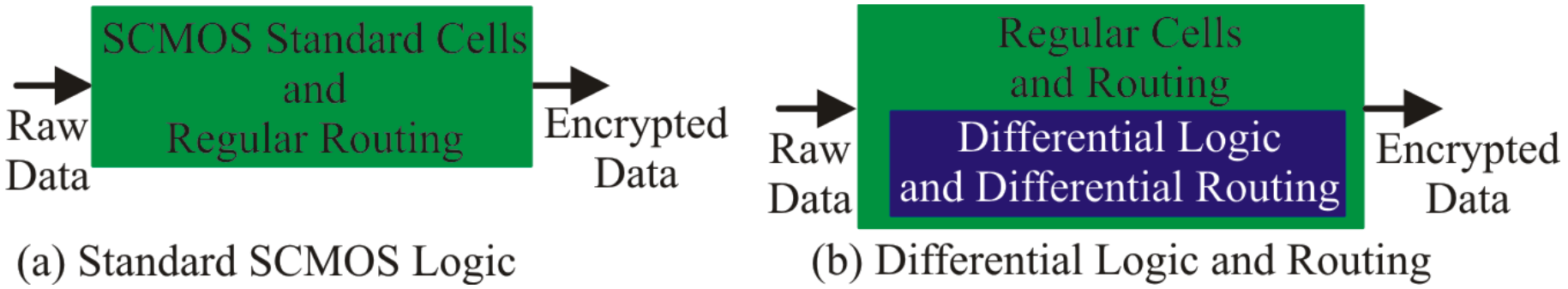


SABL NAND-AND

Source: Tiri ESSCIRC 2002

DPA Resilience Hardware: Differential Logic and Routing

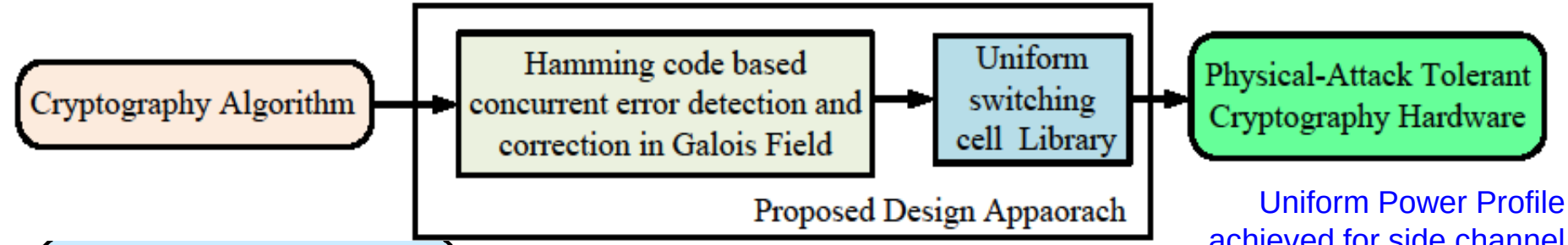
- Develop logic styles and routing techniques such that power consumption per cycle is constant and capacitance charged at a node is constant.



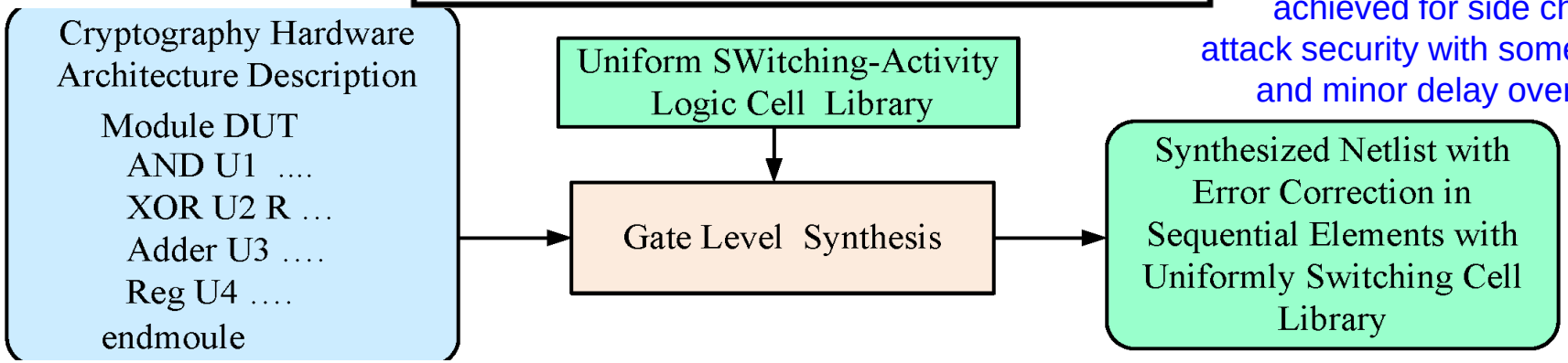
Vulnerable to side channel attack.

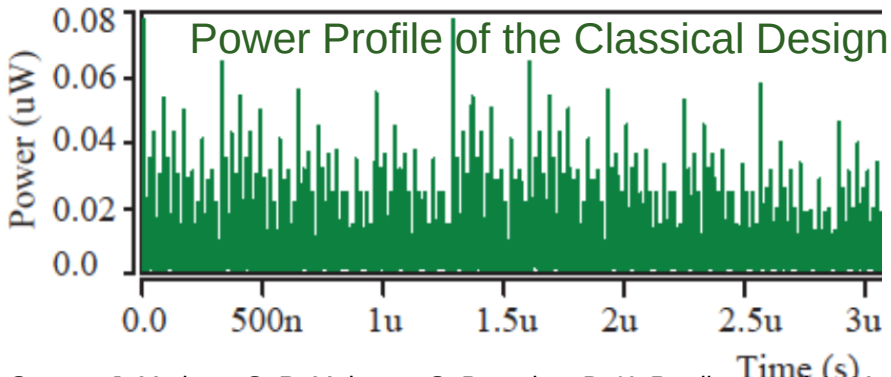
May abstract switching activity and reduce information leaking.

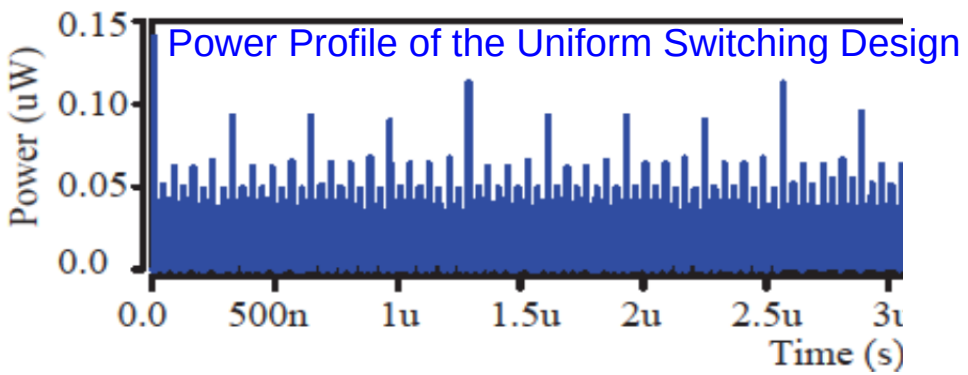
Our SdD: Approach for DPA Resilience Hardware



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

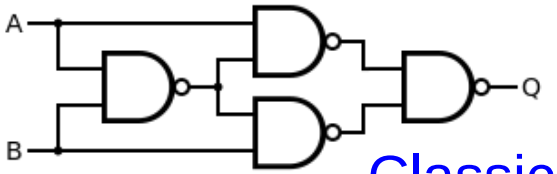




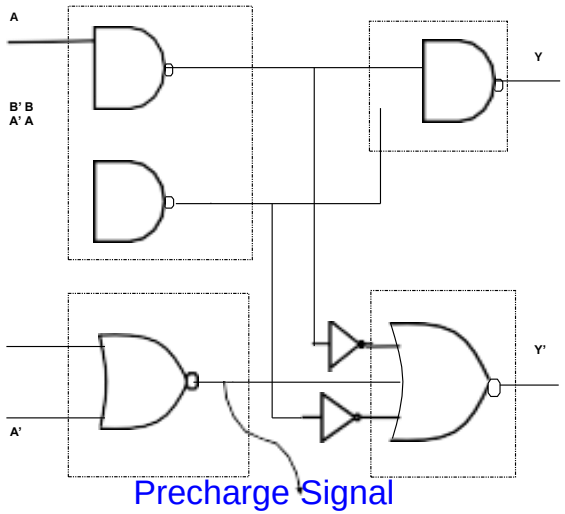


Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", *Elsevier Computers and Electrical Engineering*, Vol. 39, No. 4, May 2013, pp. 1077--1087.

DPA Resilience Hardware: Differential Logic and Routing

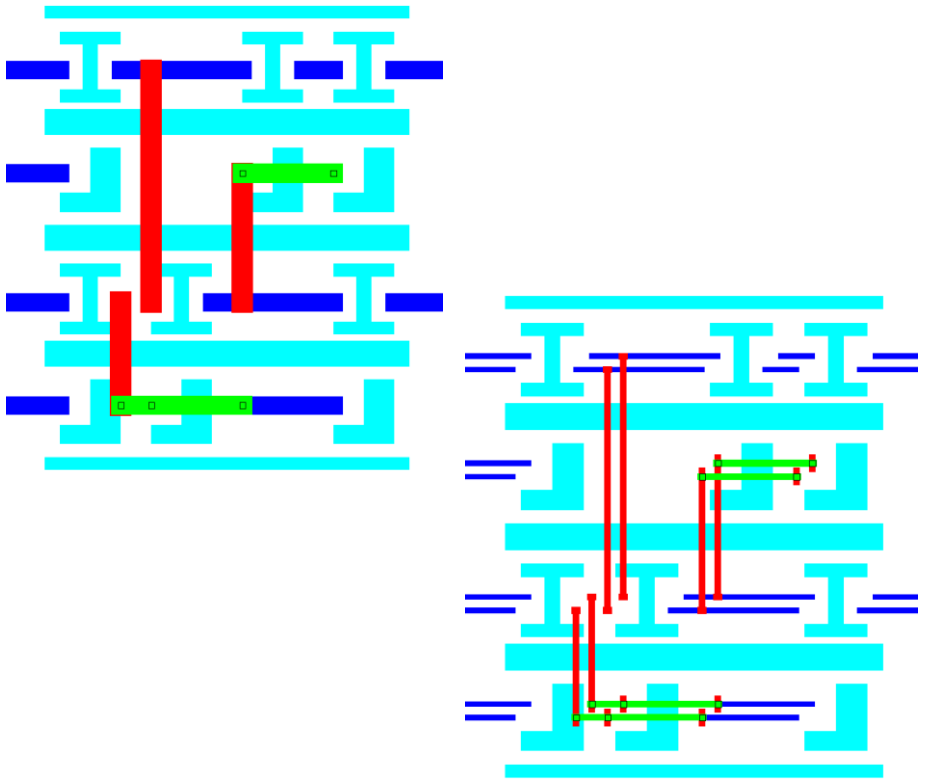


Classic XOR



Reduced Complementary Dynamic and Differential Logic (RCDDL) XOR

Source: Rammohan VLSID 2008



Differential Routing

Source: Schaumont IWLS 2005

PUF – Trojan Issue

- Improper implementation of PUF could introduce "backdoors" to an otherwise secure system.
- PUF introduces more entry points for hacking into a cryptographic system.

Provide backdoor to adversary.
Chip fails during critical needs.

Source: Rührmair, Ulrich; van Dijk, Marten (2013). *PUFs in Security Protocols: Attack Models and Security Evaluations* (PDF), in *Proc. IEEE Symposium on Security and Privacy*, May 19–22, 2013

PUF – Machine Learning Attack

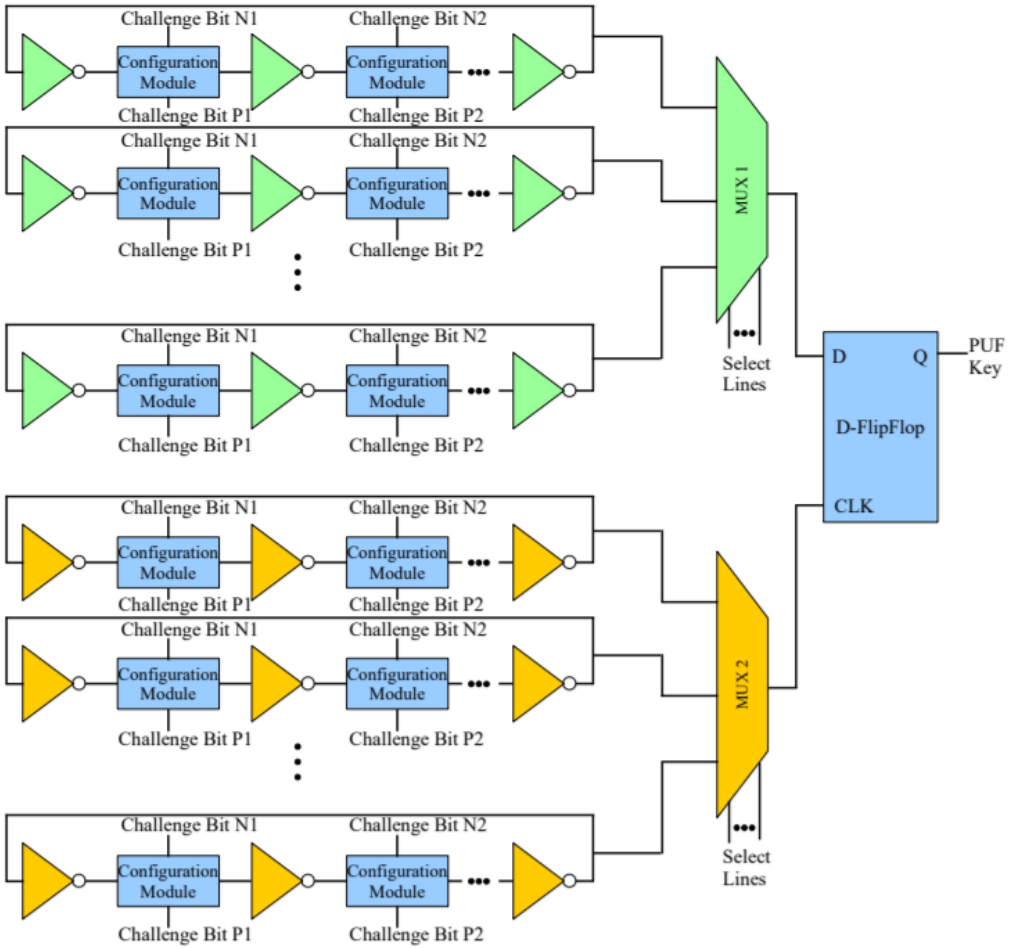
- One types of non-invasive attacks is machine learning (ML) attacks.
- ML attacks are possible for PUFs as the pre- and post-processing methods ignore the effect of correlations between PUF outputs.
- Many ML algorithms are available against known families of PUFs.

Source: Ganji, Fatemeh (2018), "On the learnability of physically unclonable functions", Springer. ISBN 978-3-319-76716-1.

Why Reconfigurability?

- Increased robustness.
- More Challenge Response Pairs.
- Lower chip area.

Reconfigurable Power Optimized Hybrid Oscillator Arbiter PUF



How to implement?

Research Publishing – Best Practices

Publishing Venue – Where to Publish?

- Magazine, Transactions, Letters, or Conference Proceedings?
- Depends on the content of a manuscript.
- First fix a venue → Write? OR First Write → venue?
- Magazine Article – Broad scope
- Journal/Transactions Papers – Focused scope and concrete results
- Letters Papers – Focused scope and brief results
- Conference Proceedings Papers – Focused scope and quick dissemination to receive direct feedback from peers

Publishing Venue – Magazine?

- Articles should be broadly scoped.
- Technical articles may be suitable, but these should be of general interest to an engineering audience and of broader scope than archival technical papers or conference proceedings papers.
- Articles related to the background story behind engineering standards or practical experiences in product specification and design of mainstream systems.
- Tutorials on related technologies or techniques are also strongly encouraged.

Publishing Venue – Journal/Transactions?

- Journal/Transactions are archival venues, just not intended for quick dissemination of research.
- Articles should have both depth and breadth.
- The work should have strong novelty. It must advance the state-of-the-art the to be published.
- The work should stand for decades without being outdated.
- The experimental results need to be rigorous.
- Manuscript need to survive multiple iterations of review process.
- Long Review Cycles. So authors should pay attention to every minor details. It may get one more round of revision just for a minor issue.

Publishing Venue – Conference Proceedings?

- Conference Publishing may be for quick dissemination.
- Conference Presentations facilitates direct interaction with peers.
- Conference attendance may help researchers in their career advancement.
- Conference reviews can help to improve the work further which may then eventually become a journal publishing.
- Work-in-Progress (WIP) and Research-Session-Demo (RDS) are alternative modes of dissemination to get feedback on ongoing research from the peers.

Conference → Journal OR Journal → Conference?

- Conference publishing first → corresponding journal

  OR

  Journal publishing first → corresponding conference
- To my experience: I see that most of the researchers follow the first option and few researchers follow the second option.
- In either case one shouldn't have the same text and figures.
  - These are two distinct publications for the authors.
  - After acceptance both the journal paper and conference paper appear in digital library, a similarity software will flag the similarity.

Shall I Target Journal/Transactions Submission Directly Without a Conference Paper of the Work?

- Short Answer: No
- Reviews received from the Initial Conference Version of the work can strengthen the work to become a journal paper eventually.
- Reviewers of the journal manuscript can have better impression if they find that it is already based on a quality conference paper.
- Journal have longer review cycle which may not correctly timestamp the idea published in the journal paper. Imagine rejection of the journal manuscript after 6-8 months of review cycle, loosing the time.

Conference → Journal: How to Do it?

- Publisher need anywhere between 30%-70% additional materials over the conference version for a journal article.
- Final judgement is typically up to the Editor-in-Chief (EiC) of specific journal/transactions.
- Key aspects of extending a conference paper to a journal article: additional novel contributions, thorough literature analysis, more experimental results, additional figures, and additional Tables.
- Complete rewriting of the text and redrawing of any figures used is a good idea to avoid similarity issues and the copyright aspects as in many cases the publishers conference proceedings and the journal/transactions may not the same.
- Remember to cite the conference paper on the current journal paper; may be even write in the acknowledgement.

Journal → Conference: How to Do it?

- It is not common to present a journal published paper as a a conference paper.
- Things are changing – Too many conference looking for audience
- Short conference paper as possible option
- Research Demo Session (RDS) papers is another option
- Complete rewriting of the text and redrawing of any figures used is a good idea to avoid similarity issues and the copyright aspects as in many cases the publishers of conference proceedings and the journal/transactions may be different.
- Remember to cite the journal paper on the current conference paper; may be even write in the acknowledgement.

Is it Important to Suggest Reviewers Names when Submitting a Journal/Transactions Manuscript?

- Short Answer: Yes
- Associate Editors are typically overloaded, they may pick few of the reviewers from your suggested list.
- The manuscript may be handled by an AE who is working on a closely, but no exactly on the area of the manuscript, so may take time to find sufficient reviewers.
- You never know your preferred reviewer may see your work favorably!

How Important is Open-Access Publishing?

- Thoughts on the current state of academic publishing
  - Journal papers are important OR Conference papers
  - Open Access is better OR traditional closed access
- Thoughts on Open-Access:
  - Arxiv (https://arxiv.org/), TechRxiv (https://www.techrxiv.org/)
  - Data Regulation – Quality Data is key
- One aspect of academic publishing that is very important/significant these days
  - Open Access and Research Reproducibility

Journal Review Process Takes Long Time, Should I Only Publish in Conference?

- Short Answer – No
- Journals are archival purposes and publish thoroughly reviewed works. So quality of work can improve if reviews are good.
- Option to time stamp the idea, before submitting to Journal:
  - Make a conference paper
  - Put it in open access depository like arXiv, TechRxiv, etc.

Journal Review Process Takes Long Time, Should I Submit to Multiple Venues for Faster Publishing?

- Short Answer: No
- Submitting same manuscript to multiple journals/transactions at a time is not allowed.
- Submitting same manuscript to a journals/transactions and a conference at a time is not allowed.
- Danger of being rejected without review from multiple venues.

I Can Publish in Journals, Why Should I Bother for Conferences?

- Short Answer – Yes
- Networking with Global Peers
- Direct Interaction with Peers → Boost Researcher's Confidence
- Meet people who can help in job search
- Meet people who can your reference for job search
- Meet people who can be reviewer of your next papers
- Meet people who can be external examiner of thesis/dissertation (if applicable)

Does the Look and Formatting of the Manuscript Matter during Submission?

- Short Answer: Yes
- Note: First Impression Lasts Long
- Reviewer maynot be interested to read details if the manuscript doesn't look professional and clear.
- Look and legibility are important to attract attention.
- Danger of the manuscript being returned without review.

How important is author ordering in a publication?

- Short Answer: No definite answer
- In some disciplines the faculty mentor is typically the last author.
- In some cases, the primary contributor is the first author and other is made based on level of contributions to the work.

How Important is Social Media for Researchers?

- Short Answer: Not Much
- How important is social media for researchers? Should Ph.D. students invest time in building profiles & networks social media?
  - Neutral – Publicity + Typical Negativity of social media (Privacy issues)
- How challenging do you feel it is for new Ph.D. researchers to get published? Any advice/tips?
  - Reasonable challenging for new researchers, Conference → Journals

Why Should I Spend Time as a Reviewer?

- Short Answer - Yes
- Early Learning: Researchers who are engaged in cutting-edge research can't find learning materials from the text books. By the time a research findings appear in text book, they are outdated. A researcher can stay up to date and learn from other researcher if he/she reviews their manuscripts.
- Learning Quality expected in a specific journal/conference. Accordingly, one can use that experience to improve own manuscripts before submissions.
- Service to the profession and community.

What are the Best Practices of Publishing?

- Short Answer: No definite answer
- Differs in one area of research to another area of research, from disciplines to another, and from publisher to another publisher. Some rule of thumb:
  - Publish one idea in one venue
  - Do best job for all text including references
  - Give credit to existing literature
  - Read articles/papers from a target venue before preparing own manuscript
  - Pay attention to each minor or major aspects; too many small → rejection
  - Learn to handle rejection

A Big Qeuestion – Where to Publish?

- As an author after I have always asked myself:
  - First Option: My article is an excellent scholarly product because it got published what my peers think as a selective or top venue.

    OR
  - Second Option: My article is an excellent scholarly product because it is read and/or cited my peers and it makes the venue great wherever it is published.
- Most of the researchers have a tendency to choose the first option from the above.
- However, I strongly believe that if an article has real strength then it should be second option.

Conclusions

Conclusions

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

Future Directions

- Privacy and/or Security by Design (PbD or SbD) needs research.
- Cybersecurity, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS) need more research.
- Cybersecurity of IoT-based systems (e.g. Smart Healthcare device/data, Smart Agriculture, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable Smart City and Smart Villages: need sustainable IoT/CPS.
- More research is needed for low-overhead PUF design and protocols that can be integrated in any IoT-enabled systems.

Acknowledgement(s)

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112 and HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.