# Security-by-Design (SbD) for Integrated Robust Cybersecurity of CPS

**Invited Talk 2023 – VIT University, AP**

**Guntur, India, 22 July 2023**

**Homepage**


Prof./Dr. Saraju Mohanty

University of North Texas, USA.

# Outline

- IoT/CPS – Big Picture
- Challenges in IoT/CPS Design
- Cybersecurity Solution for IoT/CPS
- Drawbacks of Existing Cybersecurity Solutions
- Security-by-Design (SbD) – The Principle
- Security-by-Design (SbD) - Specific Examples
- Physical Unclonable Function (PUF) – Introduction
- PUF – Types and Topologies
- PUF - Characteristics
- PUF - Challenges and Research
- Conclusion

# 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

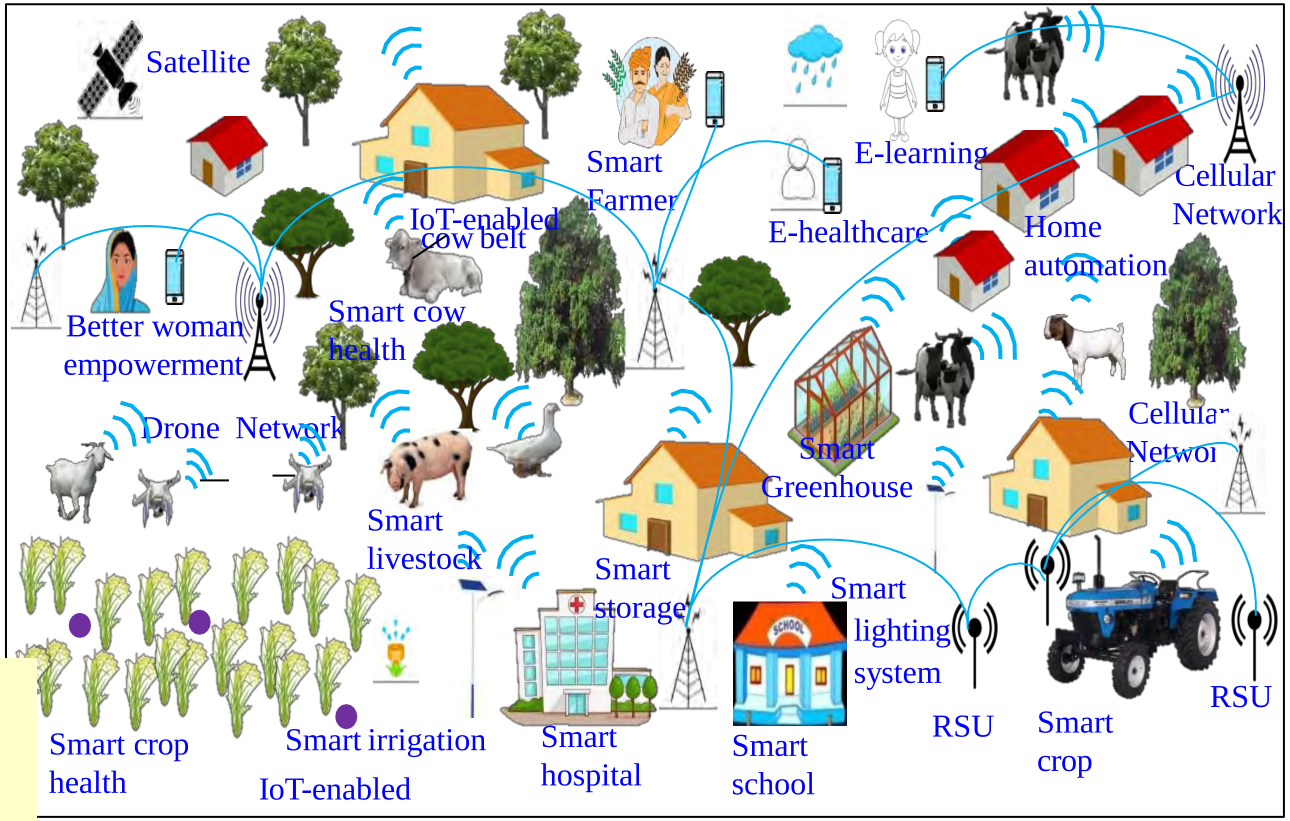

Source: http://edwingarcia.info/2014/04/26/principal/

## 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



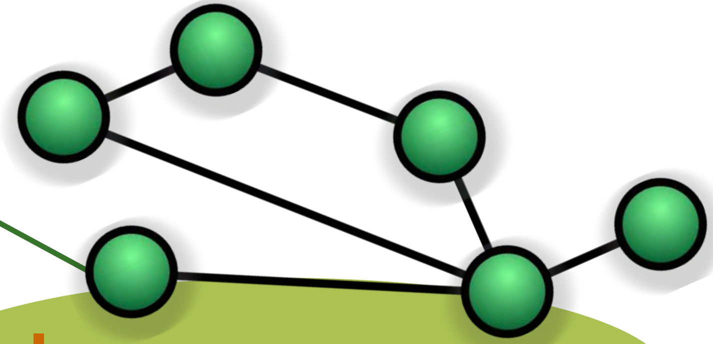

Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

# Smart Cities or Smart Villages - 3 Is


Instrumentation

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

Smart Cities

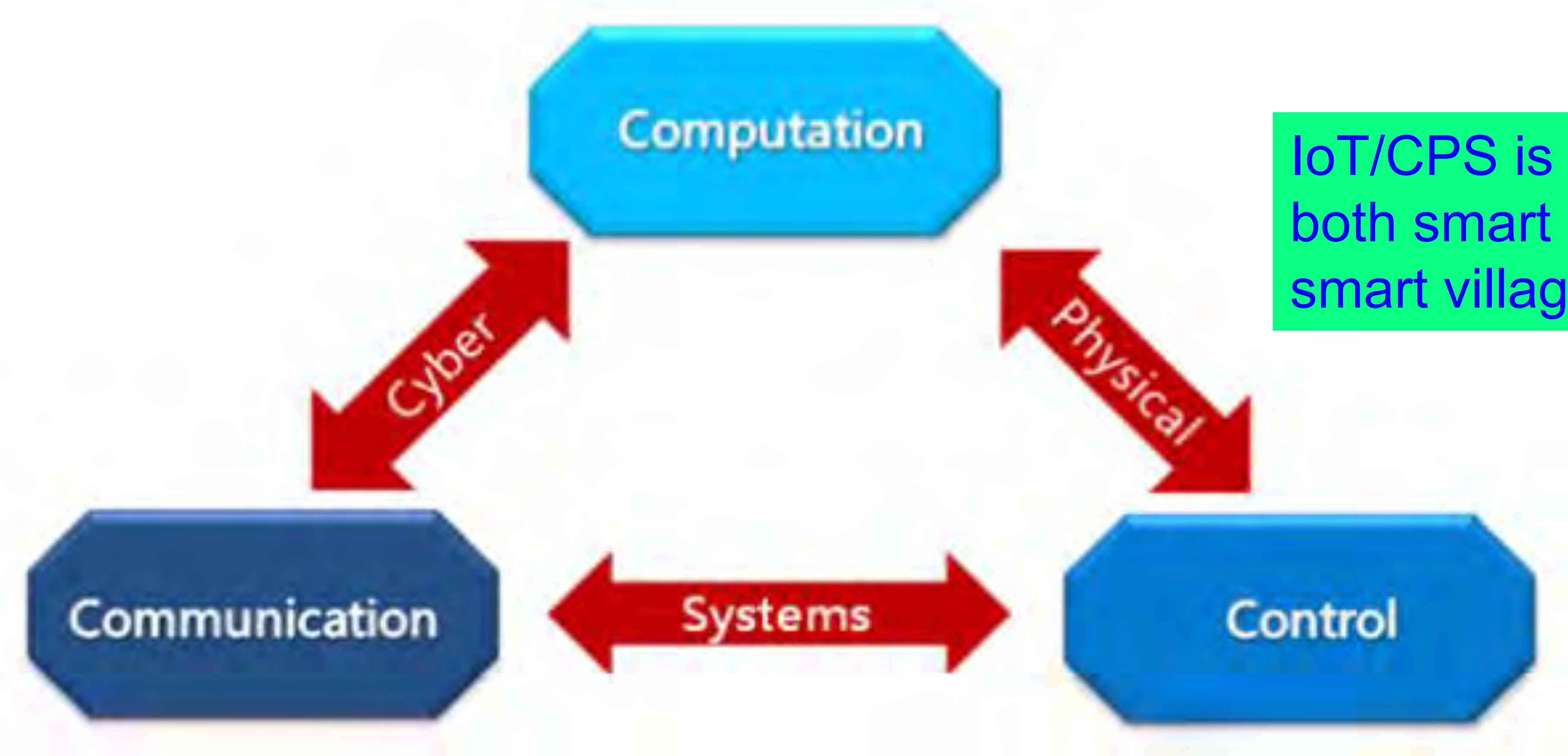


Intelligence

Interconnection

Source: Mohanty ISC2 2019 Keynote

# Cyber-Physical Systems (CPS) - 3 Cs

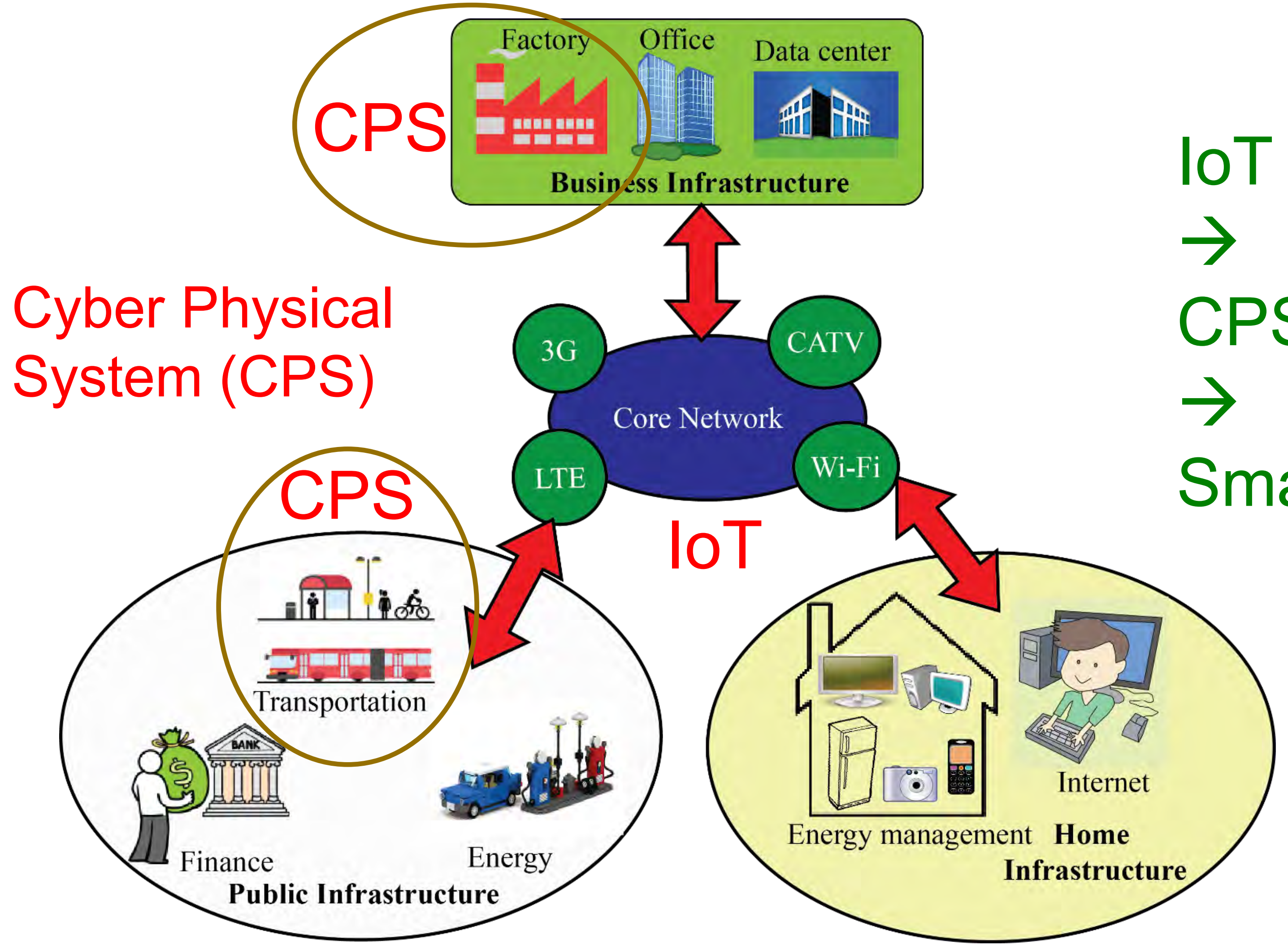



IoT/CPS is needed in both smart cities and smart villages.

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

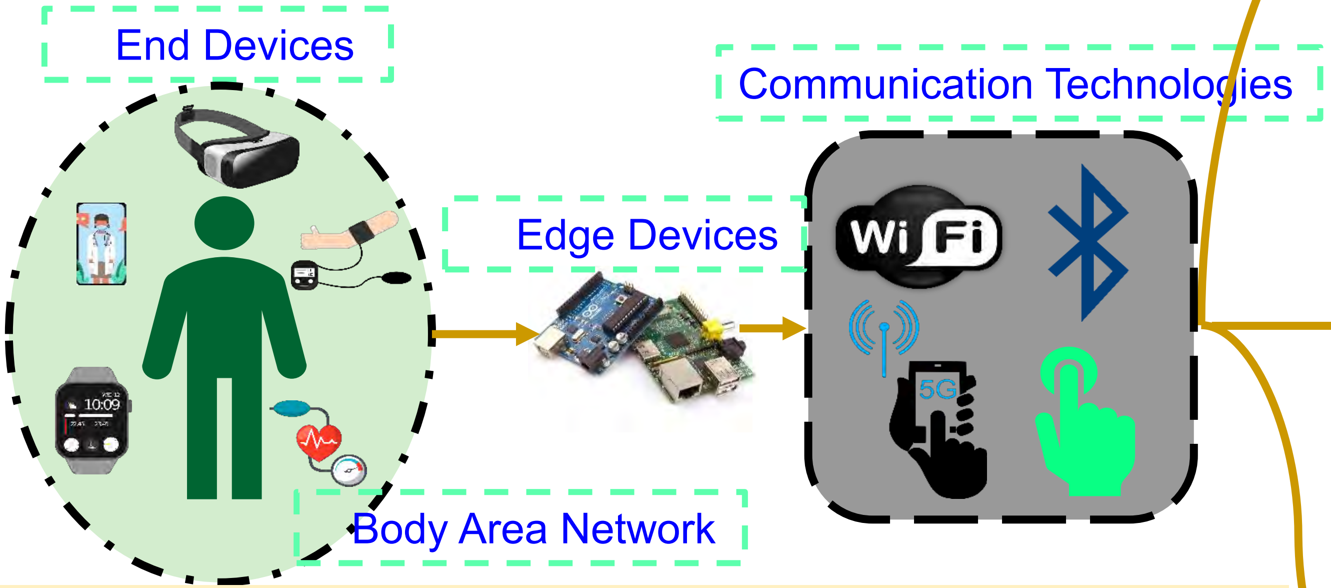


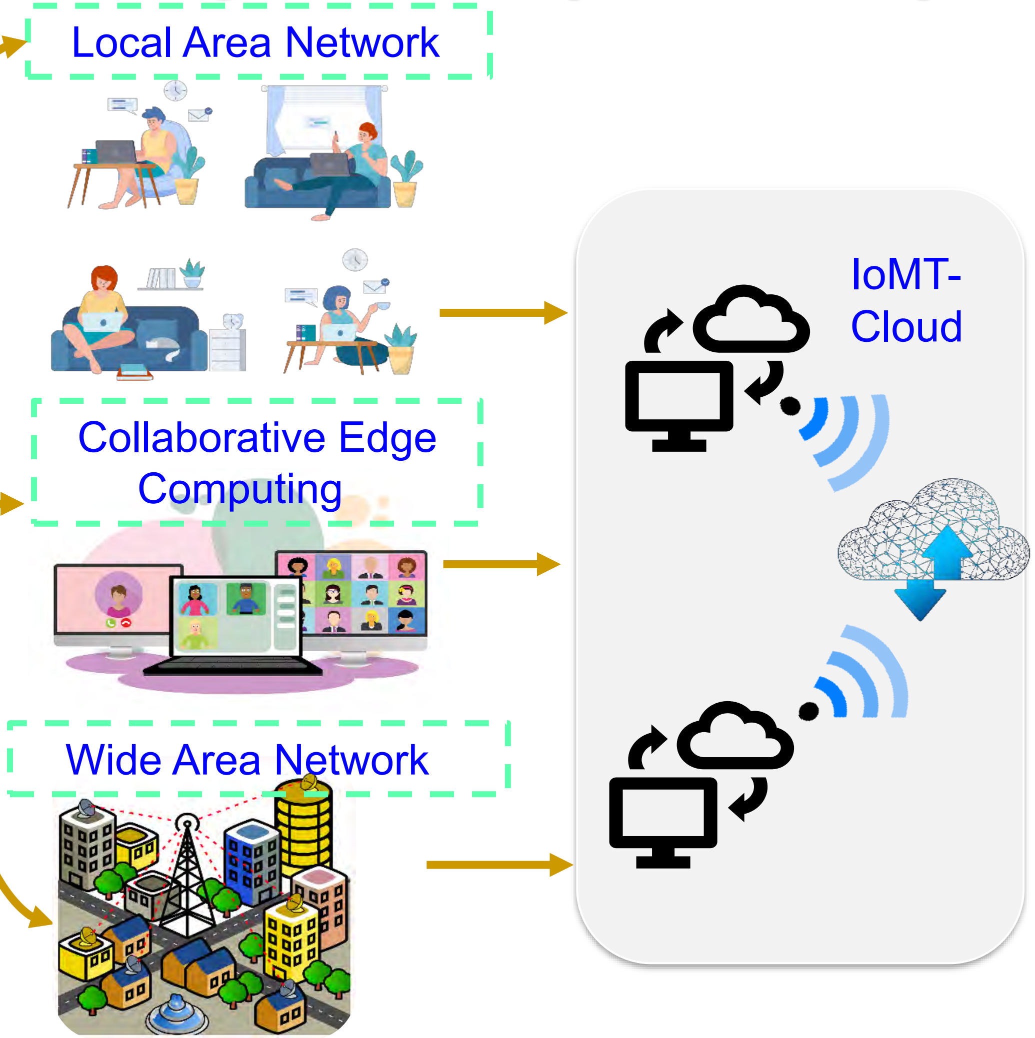

IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

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)

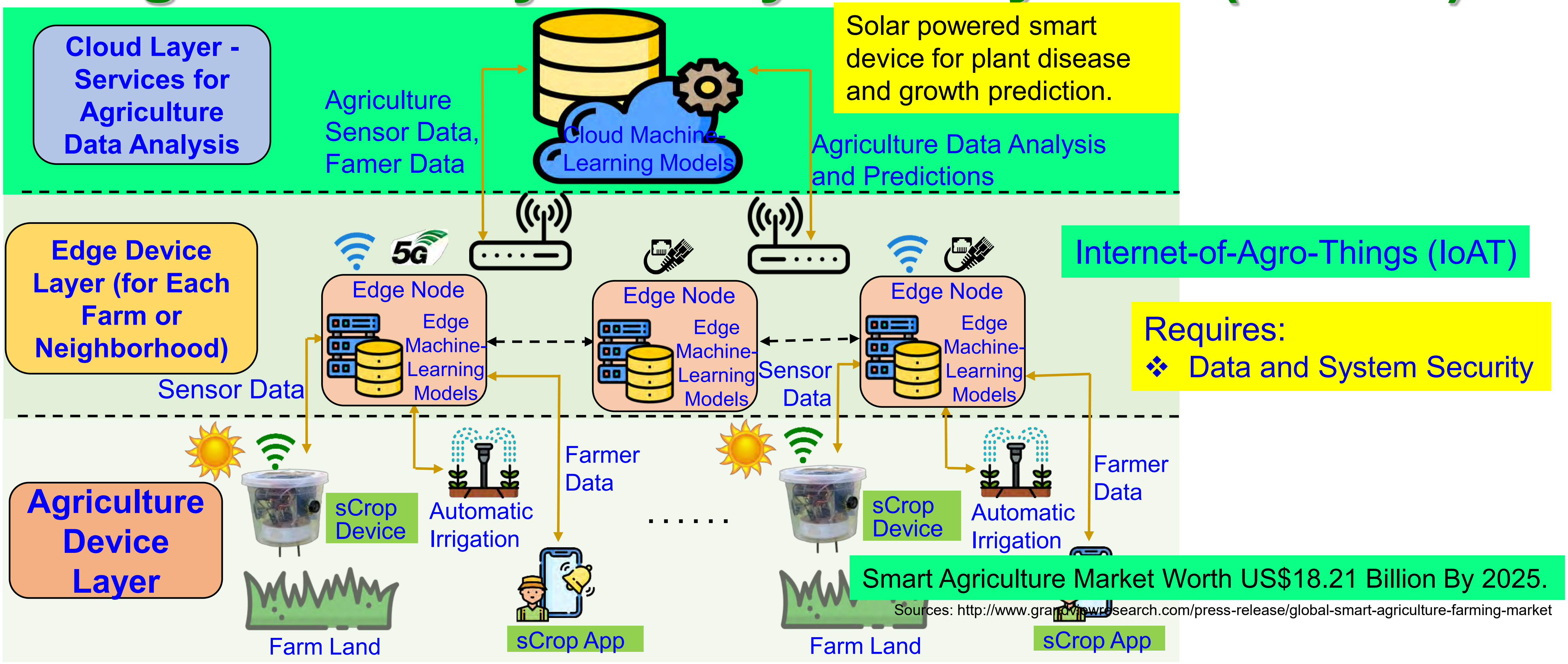



H-CPS ← Biosensors + Medical Devices + Wearable Medical Devices (WMDs) + Implantable Medical Devices (IMDs) + Internet + Healthcare database + AI/ML + Applications that connected through Internet.

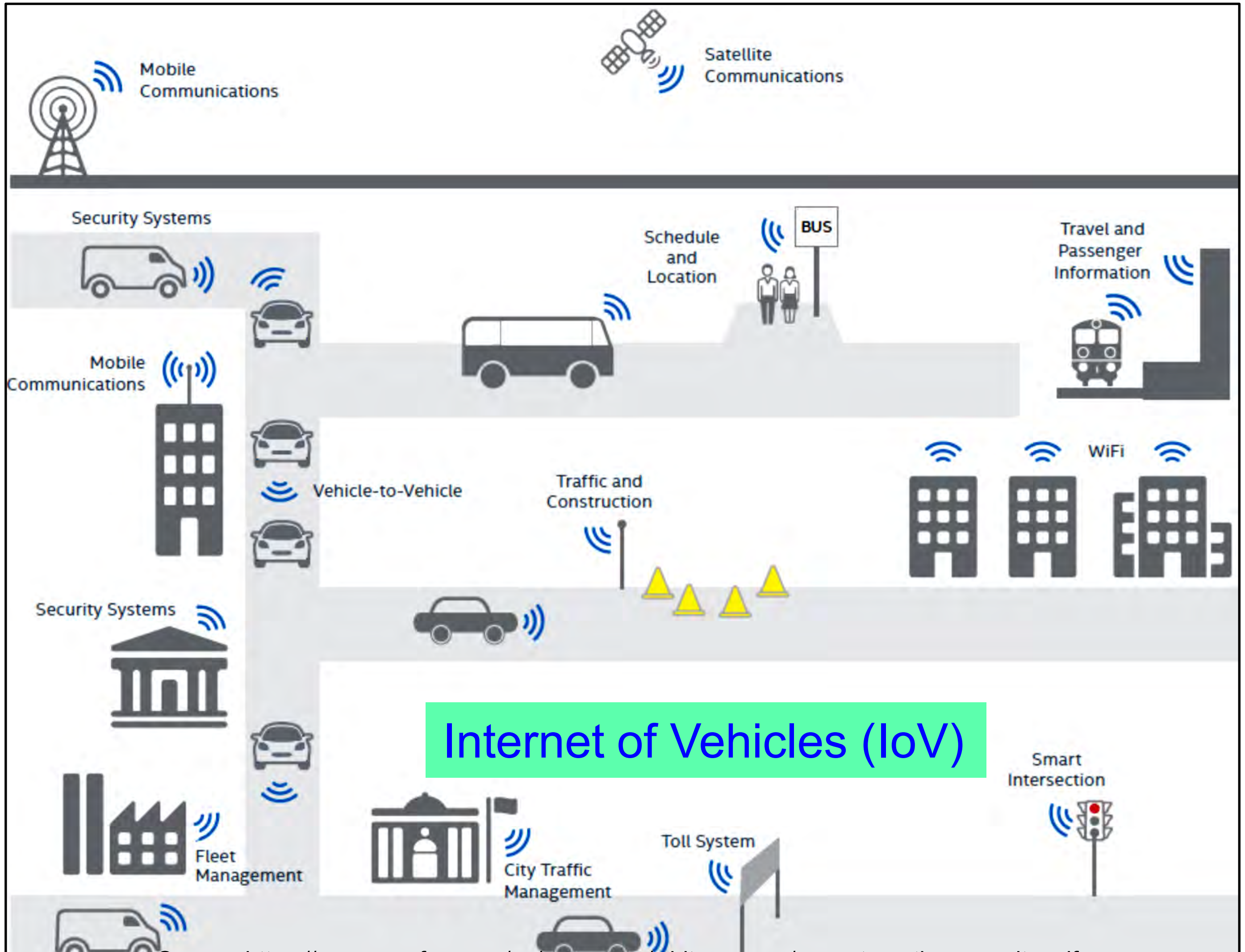
Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

# 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

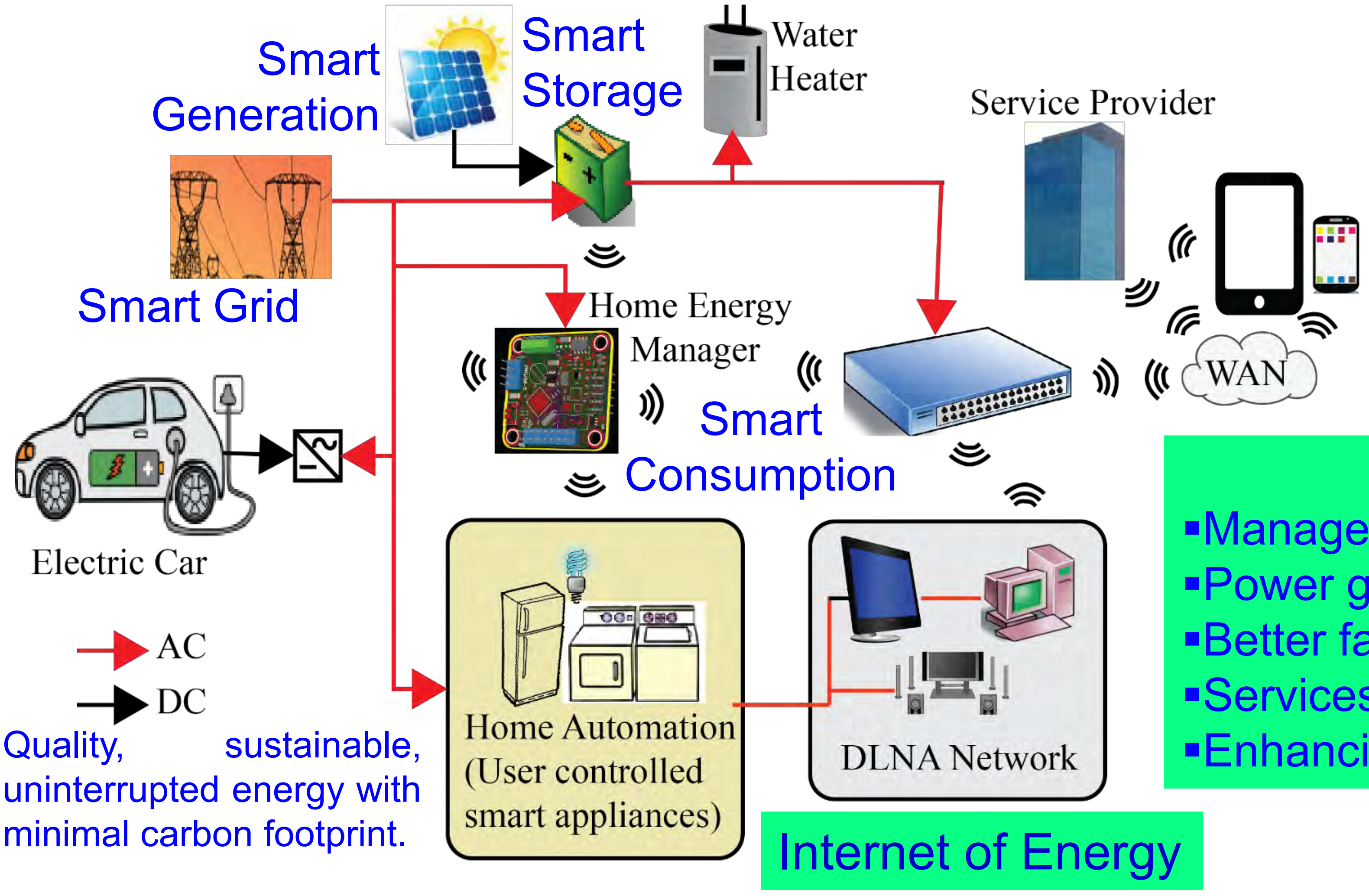
Requires:

- ❖ 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)




**Requires:**

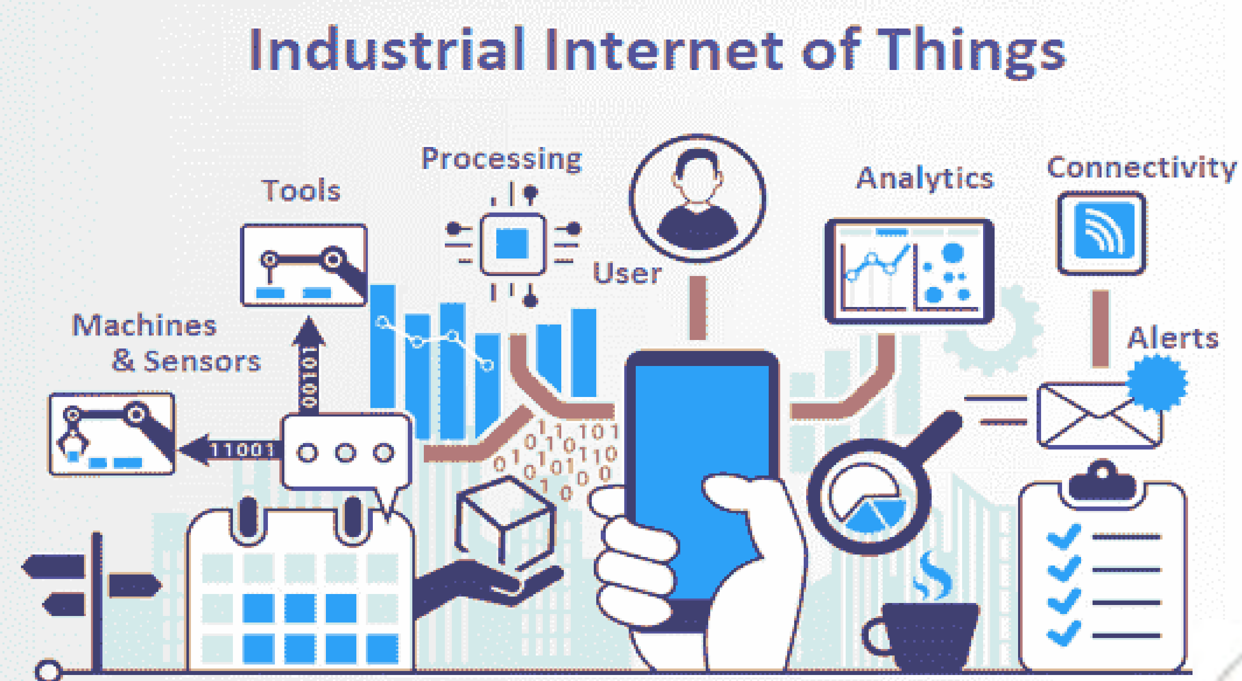
- ❖ Data, Device, and System Security

**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

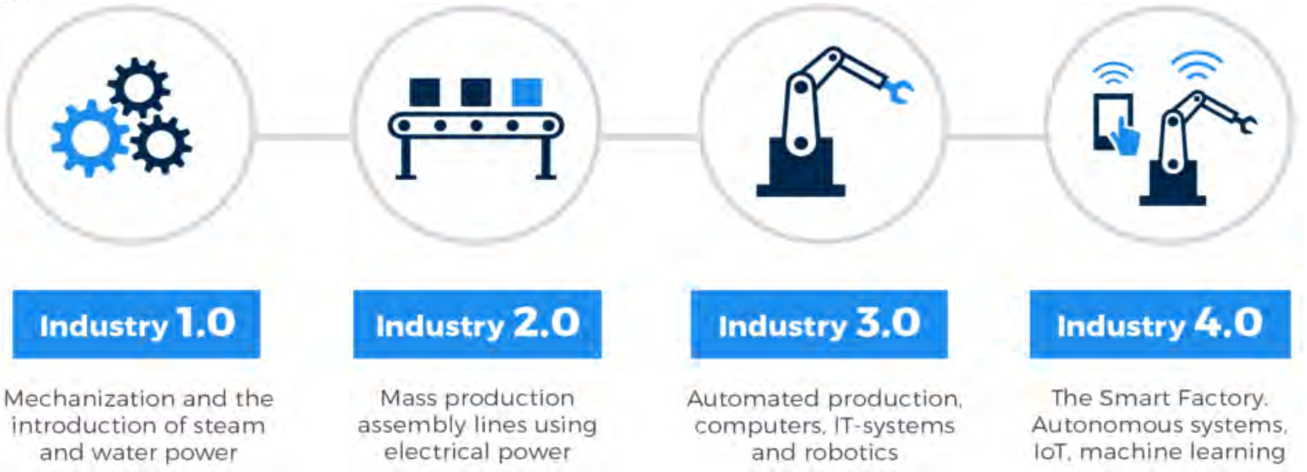
Source: S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything You wanted to Know about Smart Cities”, *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

# Industrial Internet of Things (IIoT)



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

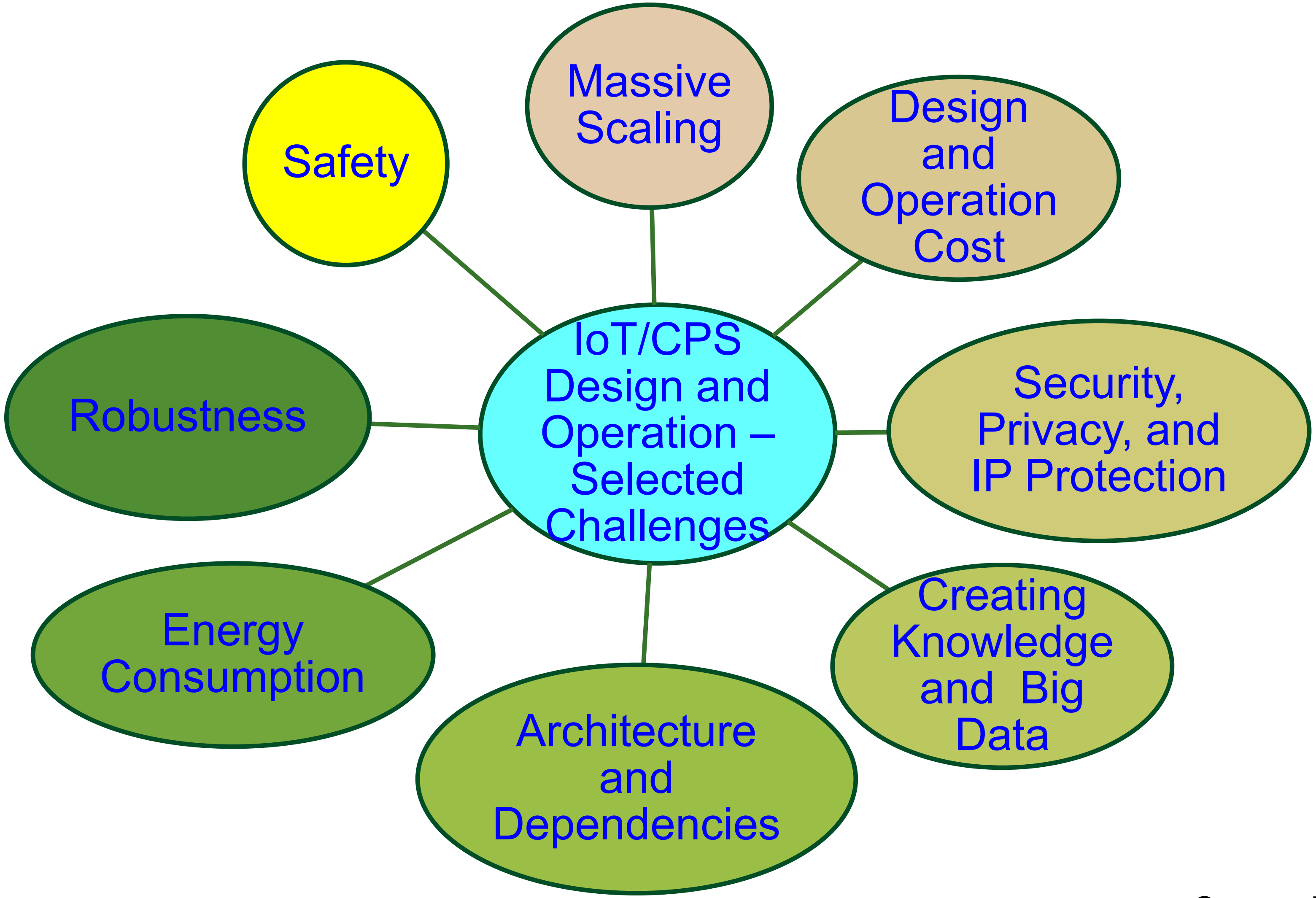
Applications
- Industrial Automation
- Smart Robotics
- Predictive Maintenance
- Integration of Tools / Wearables
- Smart Logistics



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

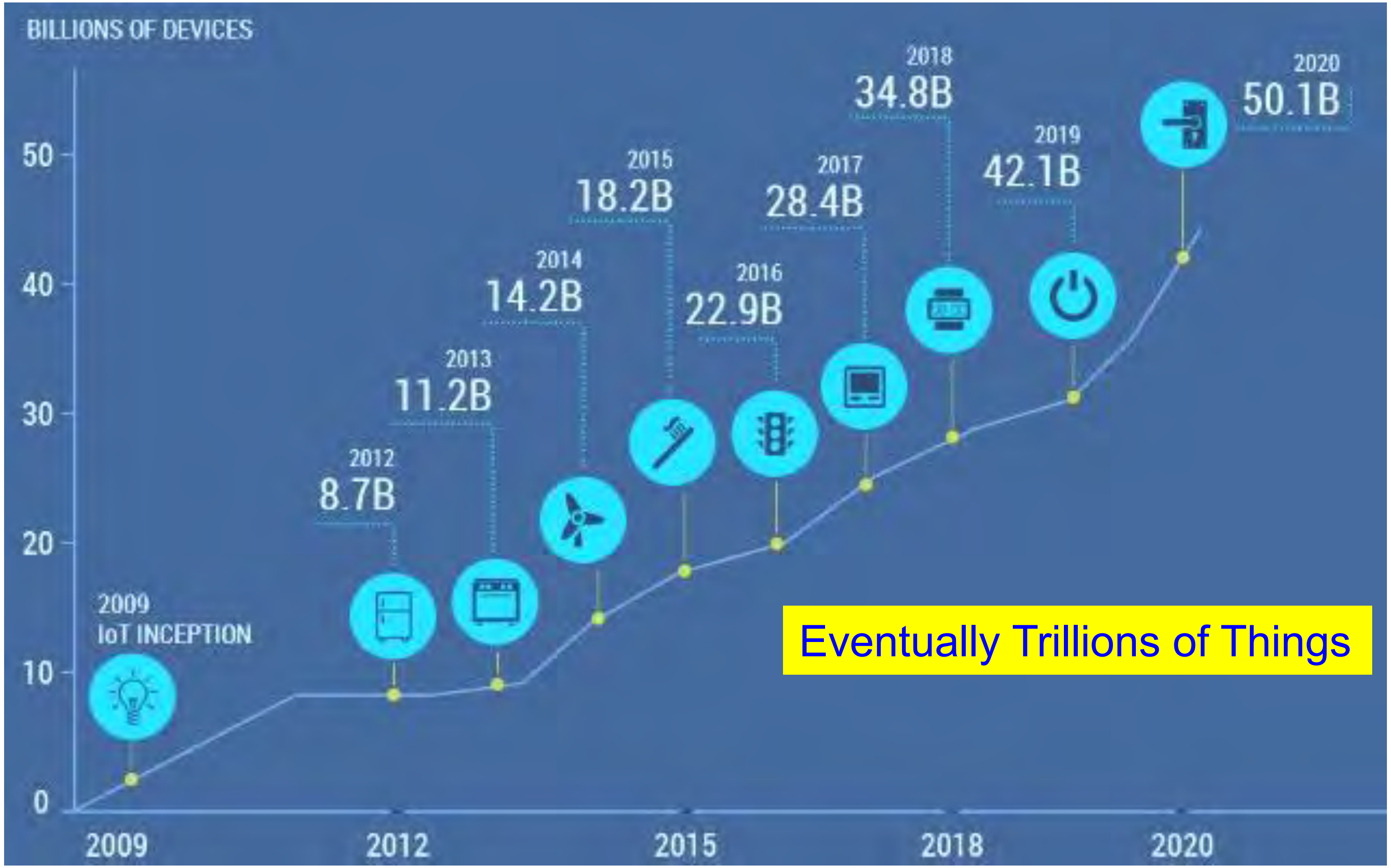
# Challenges in IoT/CPS Design

# 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

Linked in
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

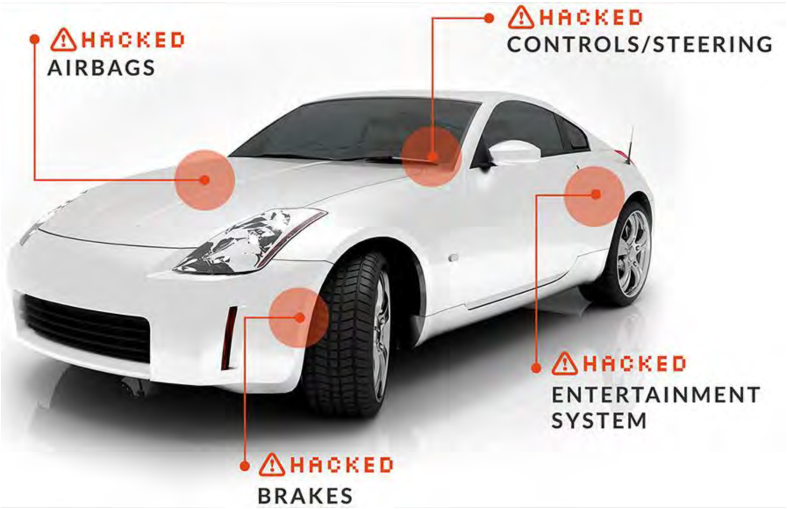
Personal Information


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

# 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

Impersonation Attacks

Eavesdropping Attacks

Smart Healthcare

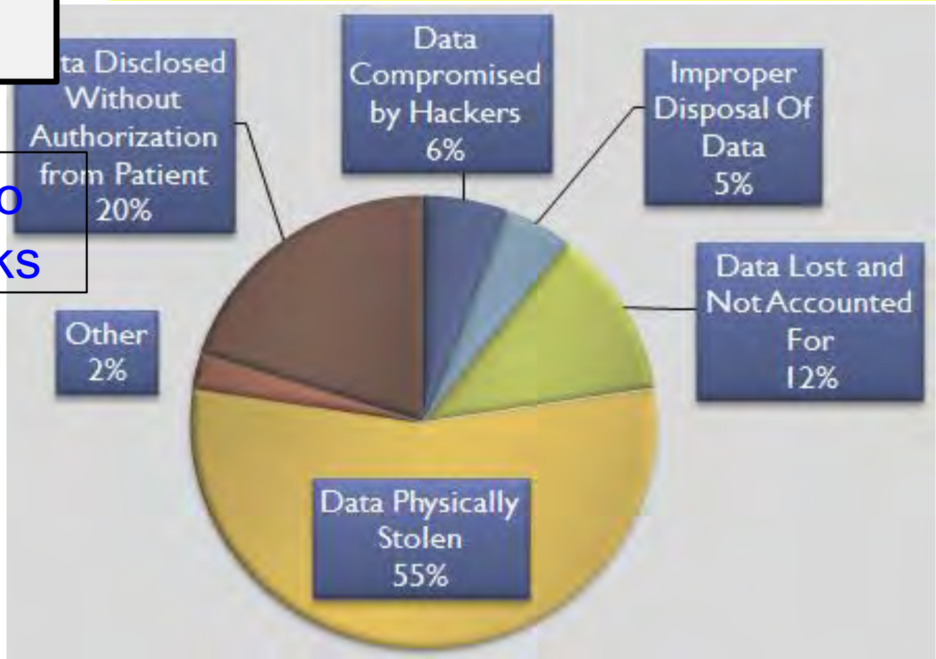
Reverse Engineering Attacks

Radio Attacks

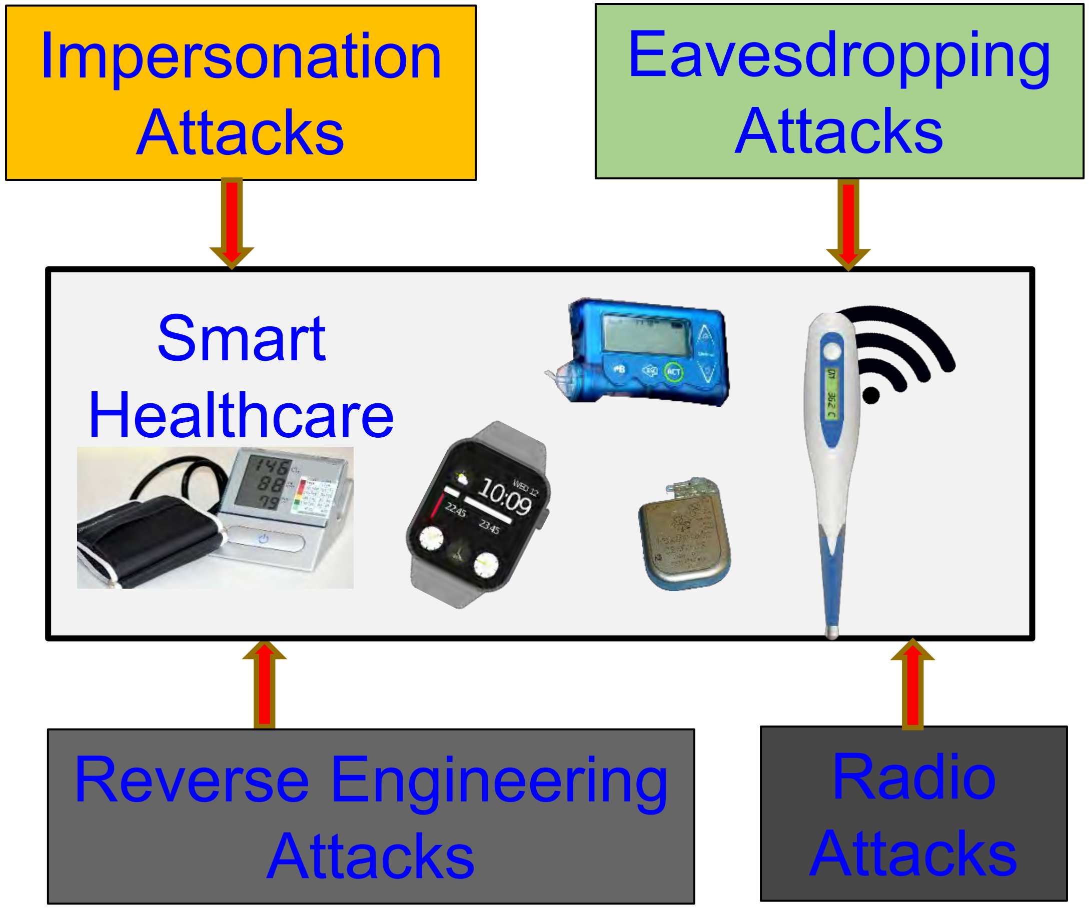
HIPAA

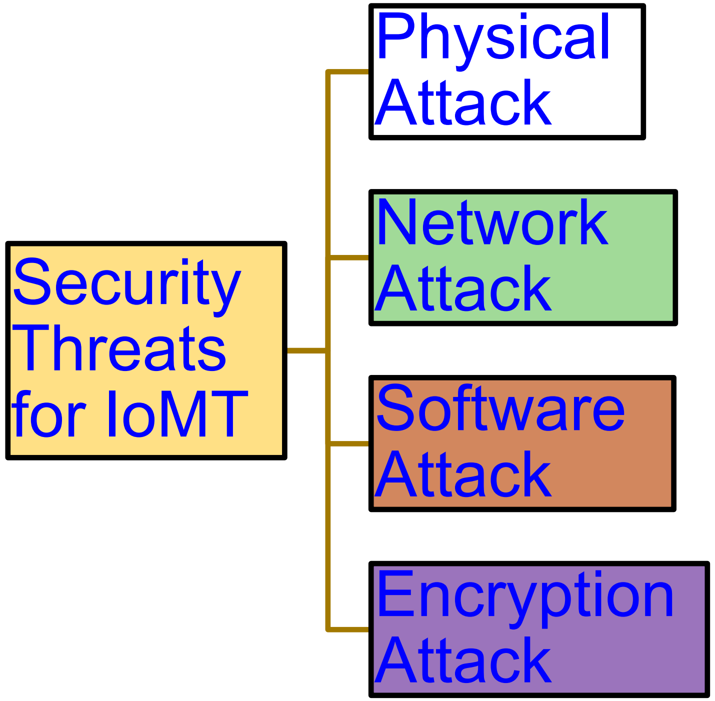
Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types



# IoMT Security – Selected Attacks




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

# 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/

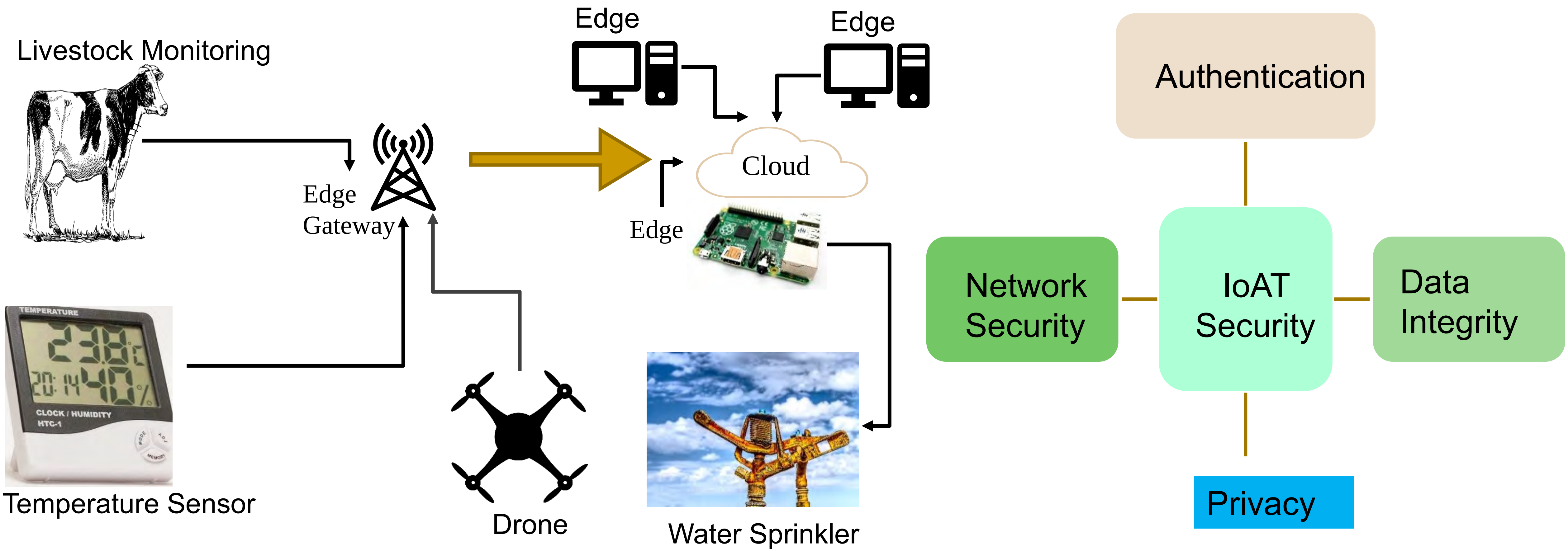
- Software vulnerabilities in some medical devices could leave them susceptible to hackers, FDA warns:

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

# Internet of Agro-Things (IoAT) - Cybersecurity Issue




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

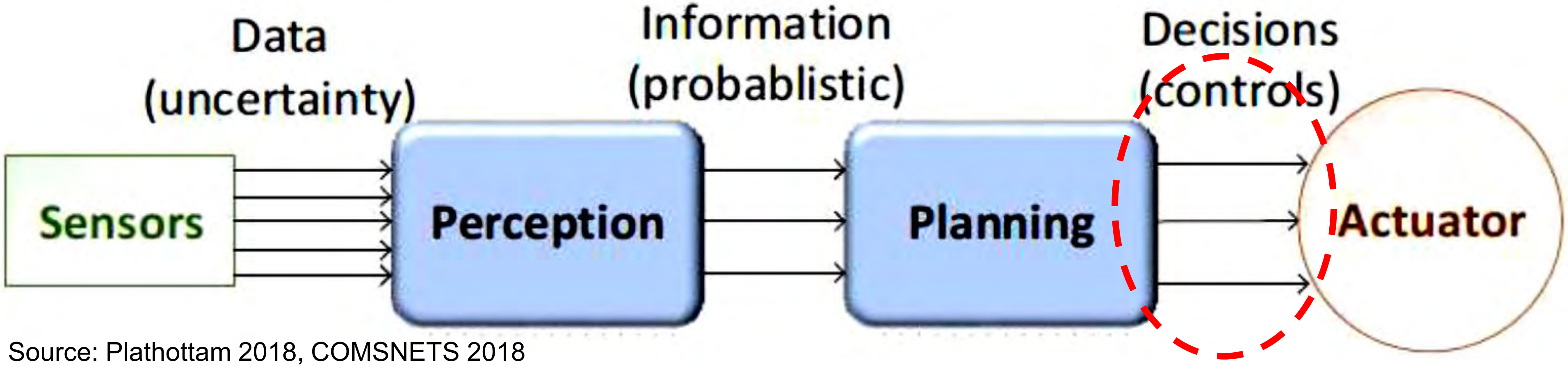
# Smart Agriculture - Security Challenges

- 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.

# 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.



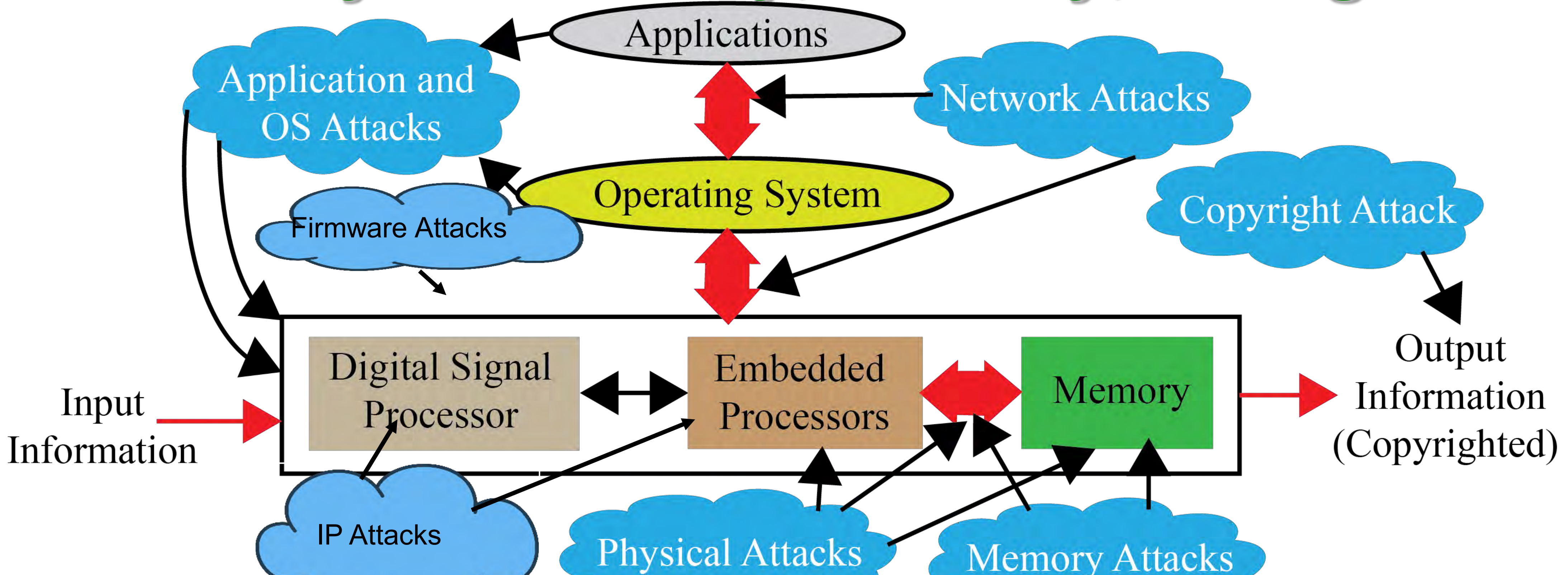

Source: Plathottam 2018, COMSNETS 2018

# Smart Grid Attacks can be Catastrophic

| Threats | Vulnerabilities | Source of Threats | Attacks | Impacts |
|---|---|---|---|---|
| Security group knowledge | Management deficiencies of network access rules<br>Inaccurate critical assests documentation | Phishers<br>Nation<br>Hacker<br>Insider<br>Terrorist<br>Spammers<br>Spyware / Malware authors | Stuxnet<br>Night Dragon<br>Virus<br>Denial of service<br>Trojan horse<br>Worm<br>Zero day exploit<br>Logical bomb<br>Phishing<br>Distributed DoS<br>False data Injection | Ukraine power attack, 2015<br>Stuxnet attack in Iran, 2010<br>Browns Ferry plant, Alabama 2006<br>Emergency shut down of Hatch Nuclear Power Plant, 2008<br>Slammer attack at Davis-Besse power plant, 2001<br>Attacks at South Korea NPP, 2015 |
| Information leakage | Unencrypted services in IT<br>Weak protection credentials | | | |
| Access point | Improper access point<br>Remote access deficiency<br>Firewall filtering deficiency | | | |
| Unpatched System | Unpatched operating system<br>Unpatched third party application | | | |
| Weak cyber security | Buffer overflow in control system services<br>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

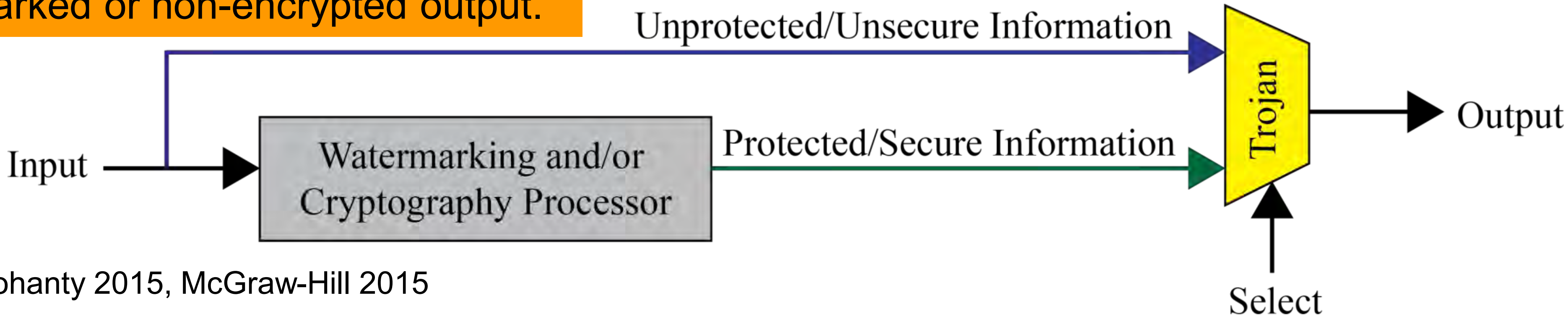
Diverse forms of Attacks, following are not the same: System Security, Device Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

# Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

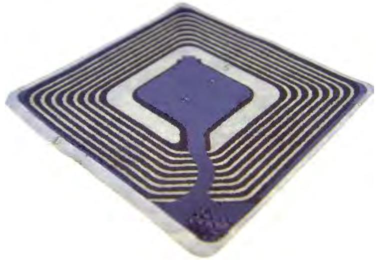
Information may bypass giving a non-watermarked or non-encrypted output.

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

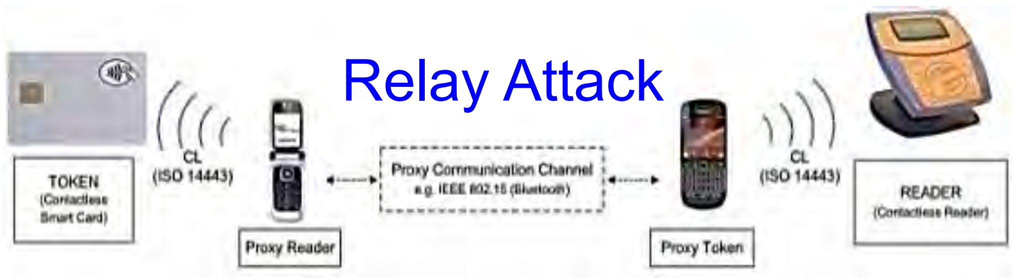
# NFC Security - Attacks

**Selected NFC Attacks**
- Eavesdropping
- Data Modification
- Relay Attacks
- Data Corruption
- Spoofing
- Interception Attacks
- Theft


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


## Eavesdropping

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

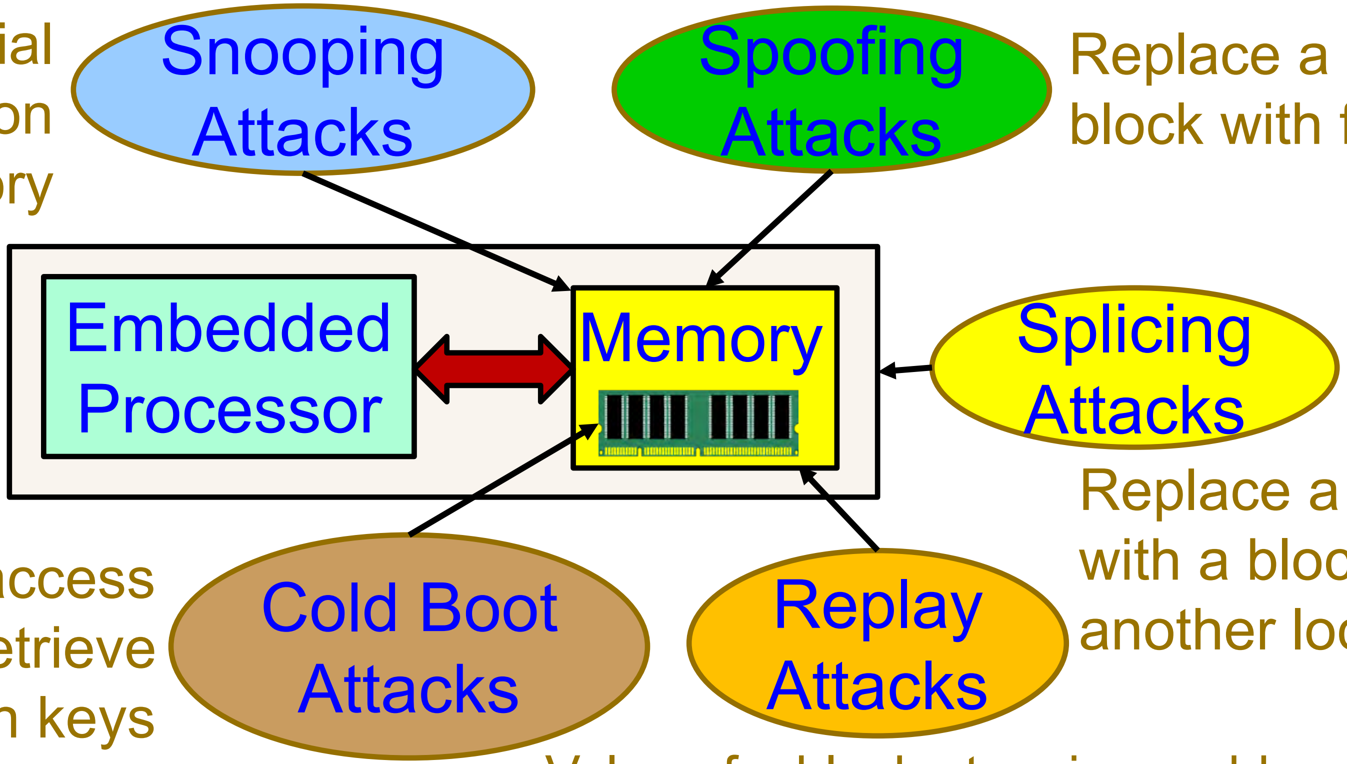



Source: https://www.slideshare.net/cgvwzq/on-relaying-nfc-payment-transactions-using-android-devices

# Attacks on Embedded Systems' Memory

Read confidential information in memory

Replace a block with fake



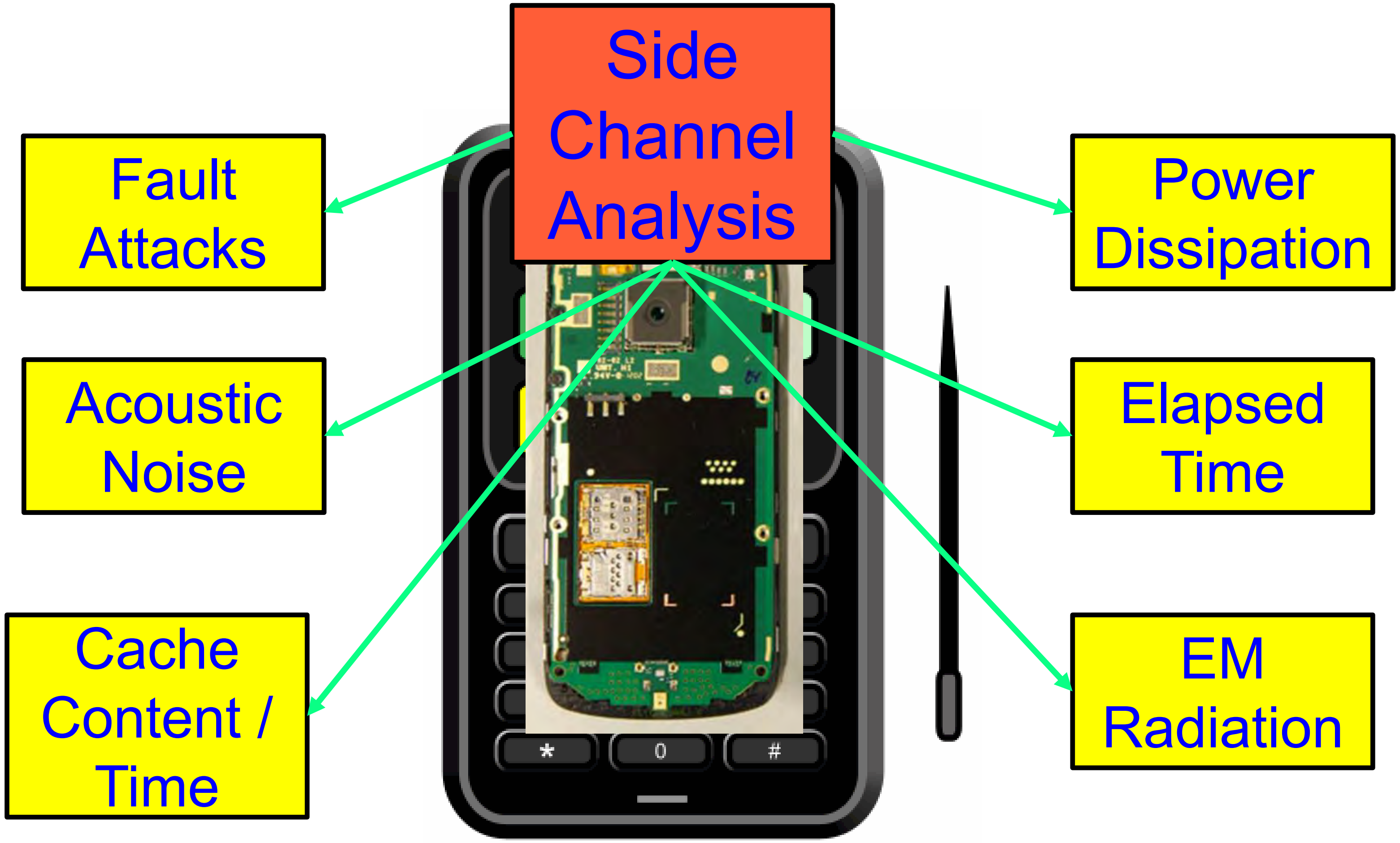

Replace a block with a block from another location

Physical access memory to retrieve encryption keys

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

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

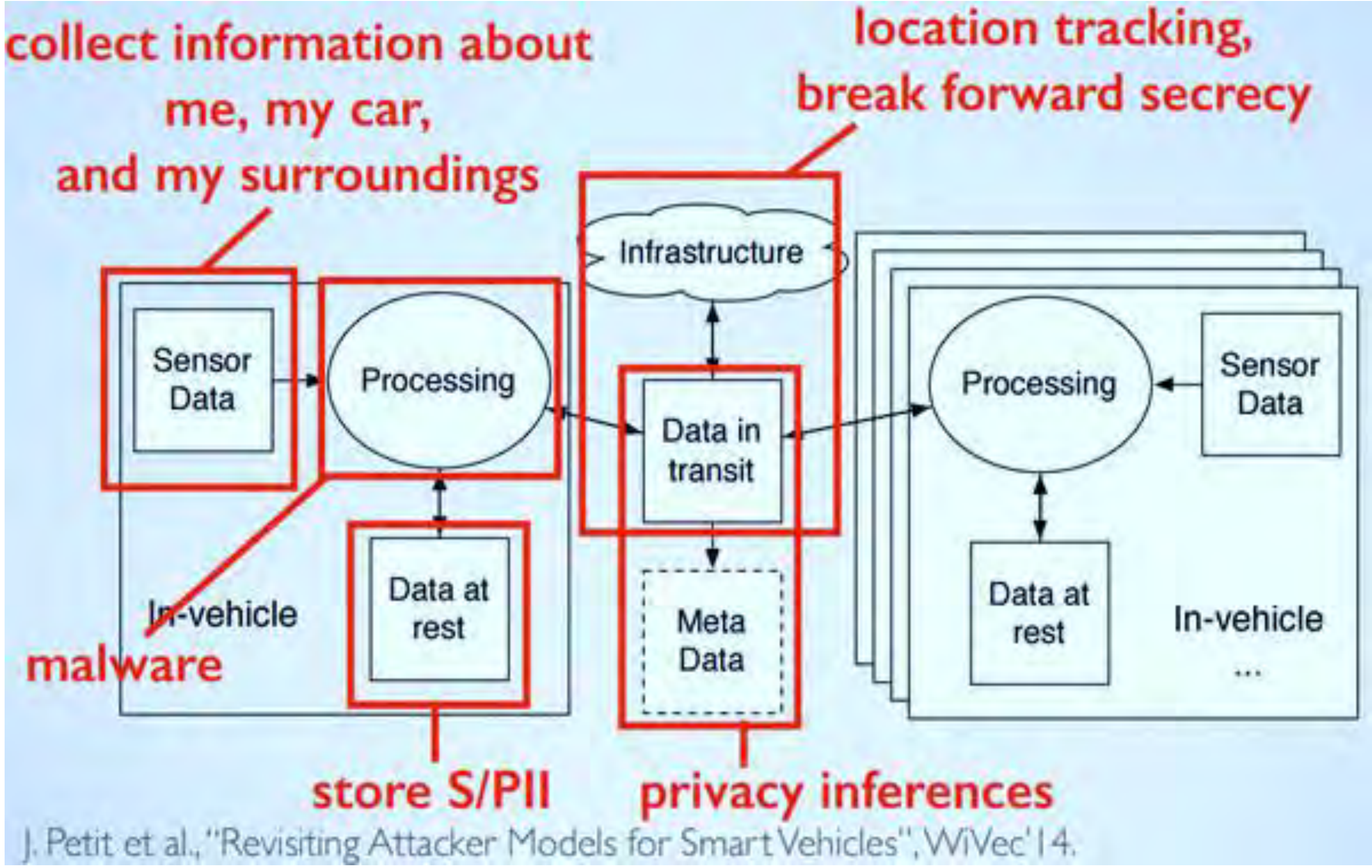
# Side Channel Analysis Attacks



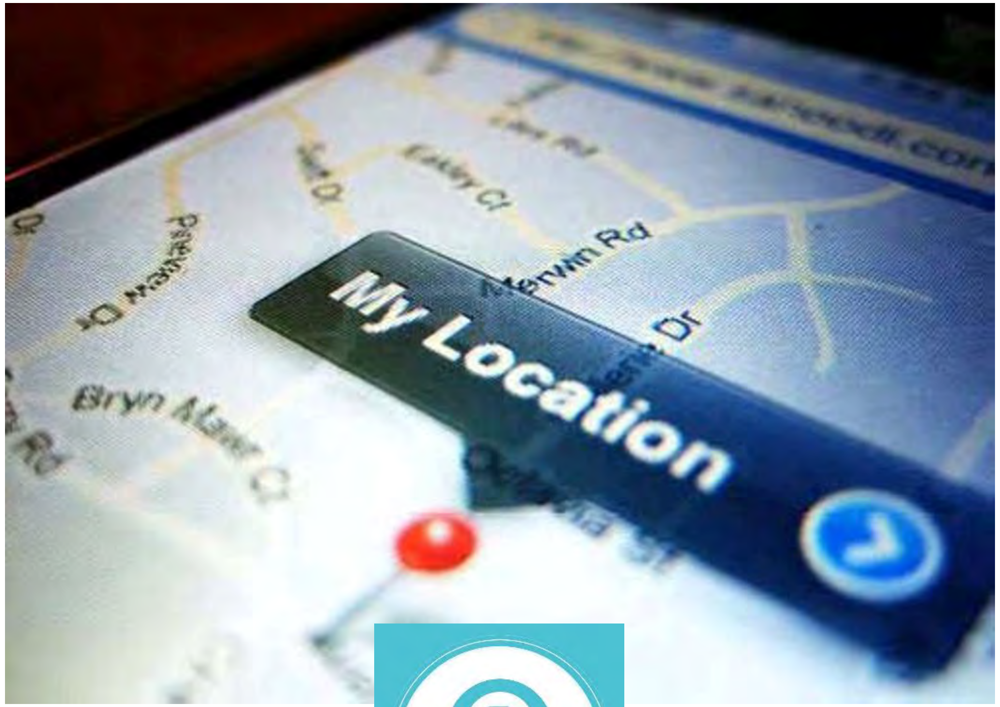

Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

# Privacy Challenge – System, Location



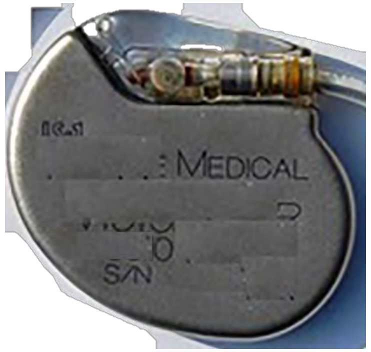

Source: http://www.computerworld.com/article/3005436/cybercrime-hacking/black-hat-europe-it-s-easy-and-costs-only-60-to-hack-self-driving-car-sensors.html




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

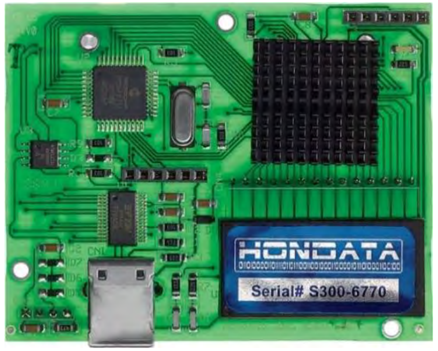

AI can be fooled by fake data

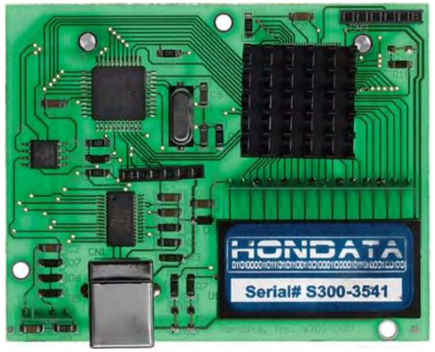
AI can create fake data (Deepfake)




Authentic Fake

An implantable medical device

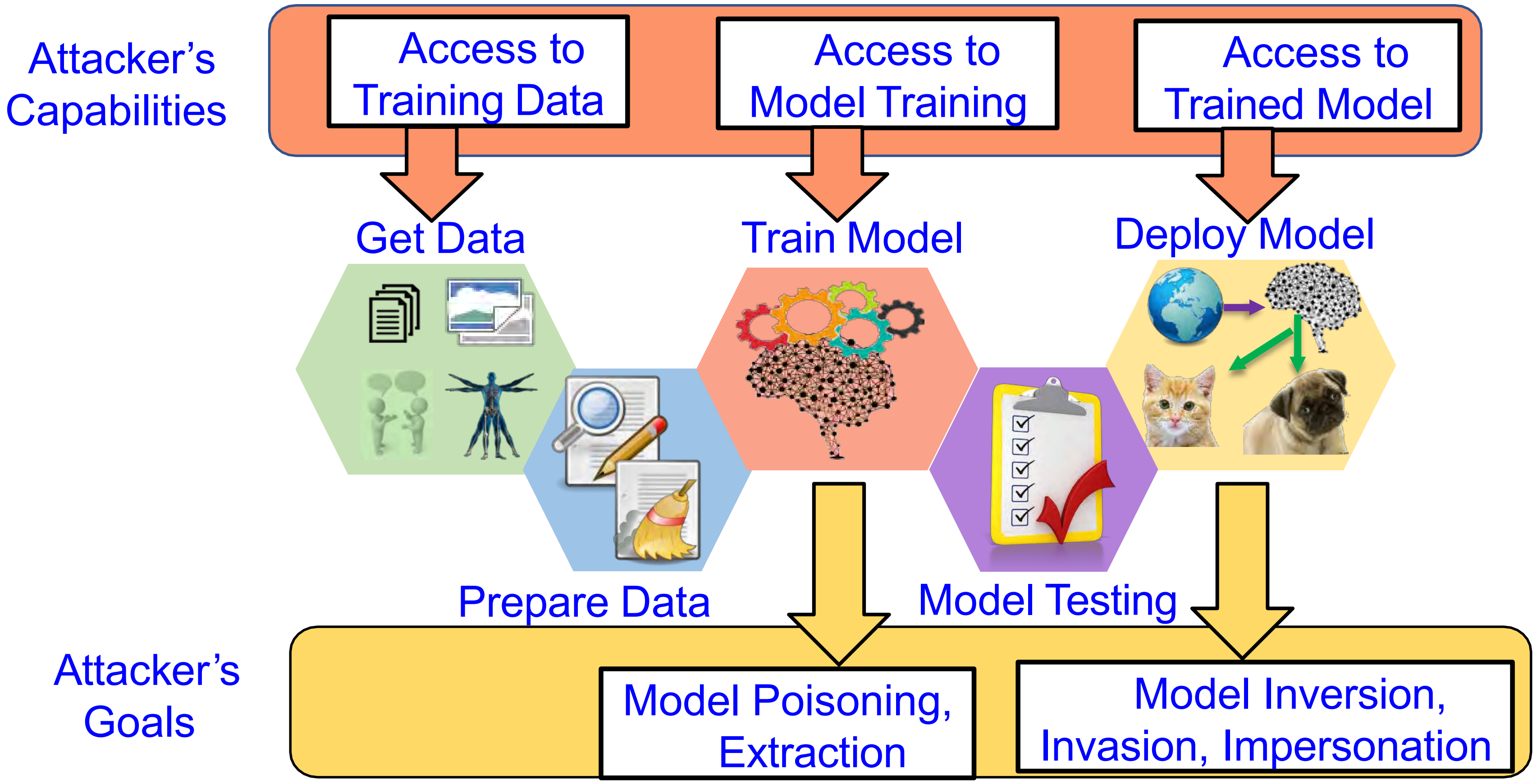





Authentic Fake

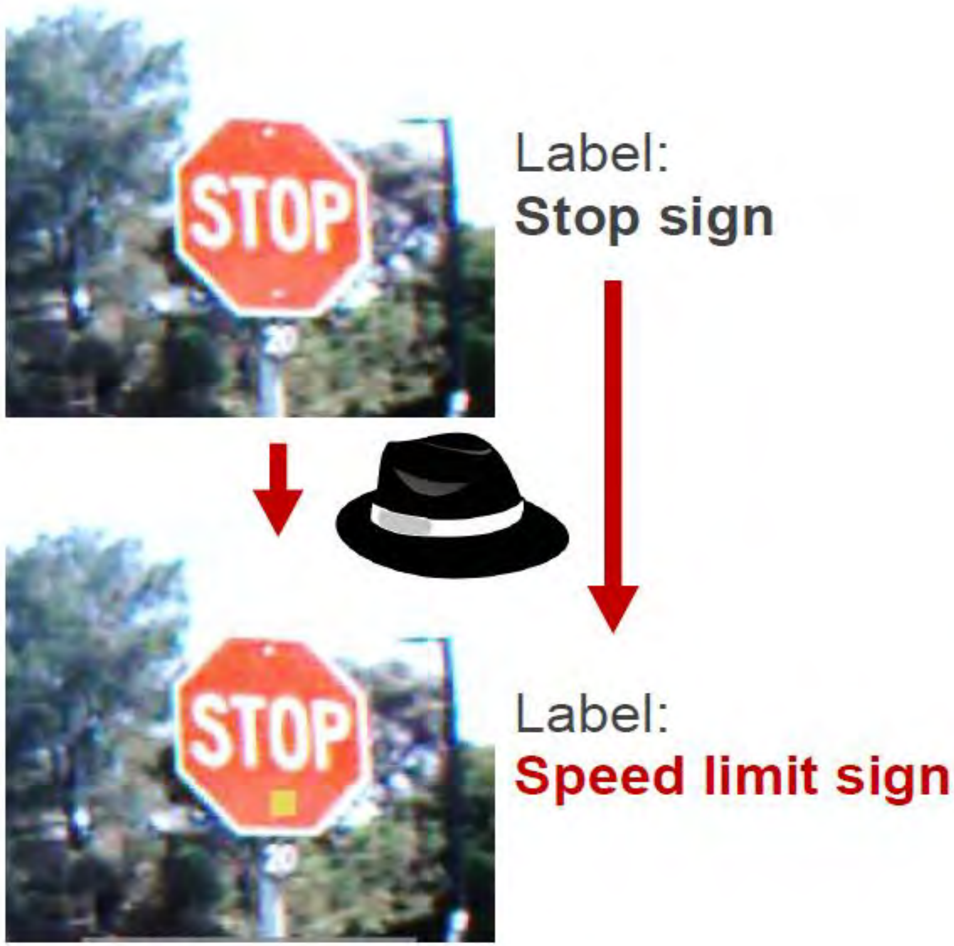
A plug-in for car-engine computers

# AI Security - Attacks




Source: Sandip Kundu ISVLSI 2019 Keynote.

# AI Security - Trojans in Artificial Intelligence (TrojAI)

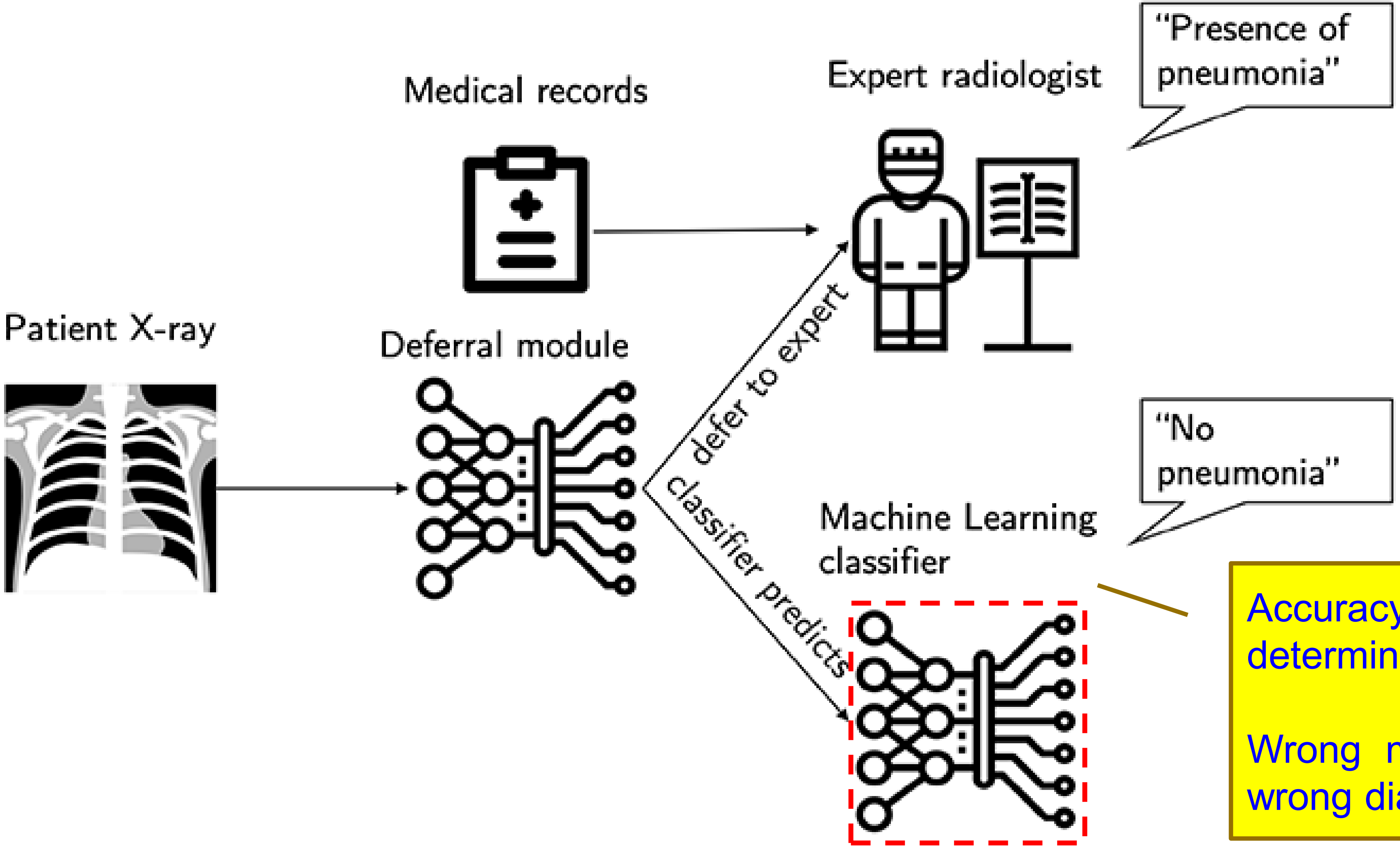




Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

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

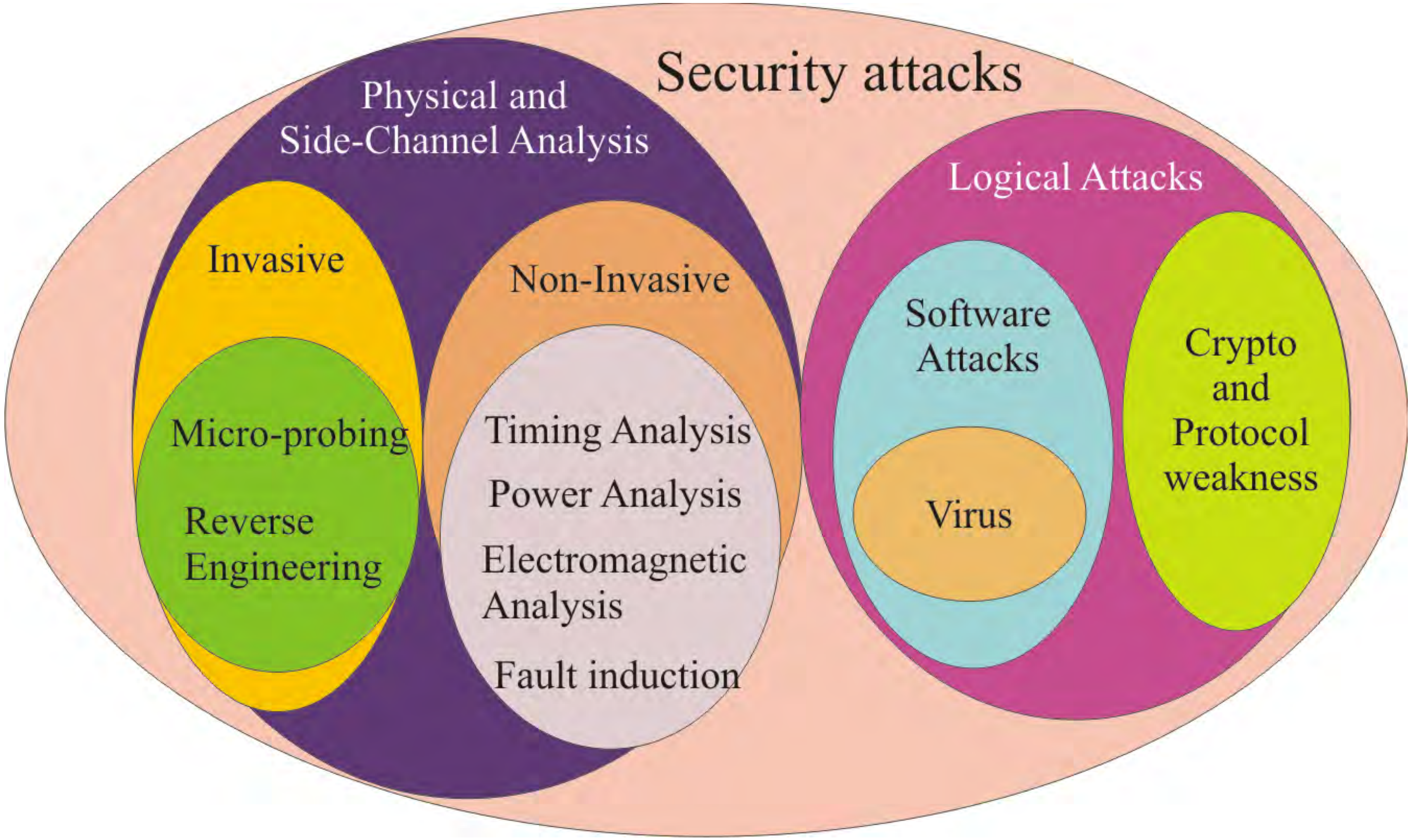



Accuracy is important determine pneumonia

Wrong model can lead to wrong diagnosis altogether

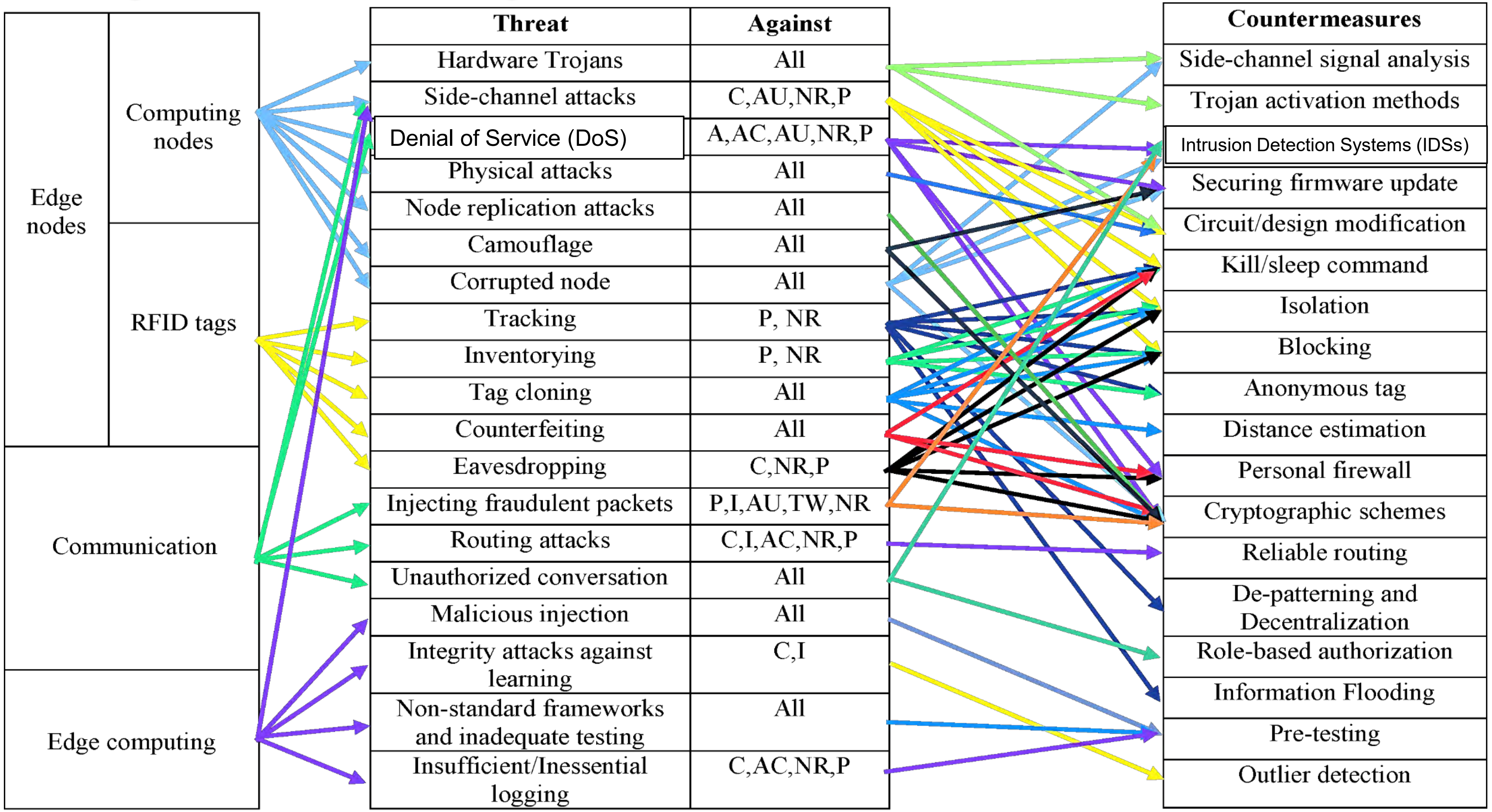
Source: https://www.healthcareitnews.com/news/new-ai-diagnostic-tool-knows-when-defer-human-mit-researchers-say

# Different Attacks on a Typical Electronic System



# Cybersecurity Solution for IoT/CPS

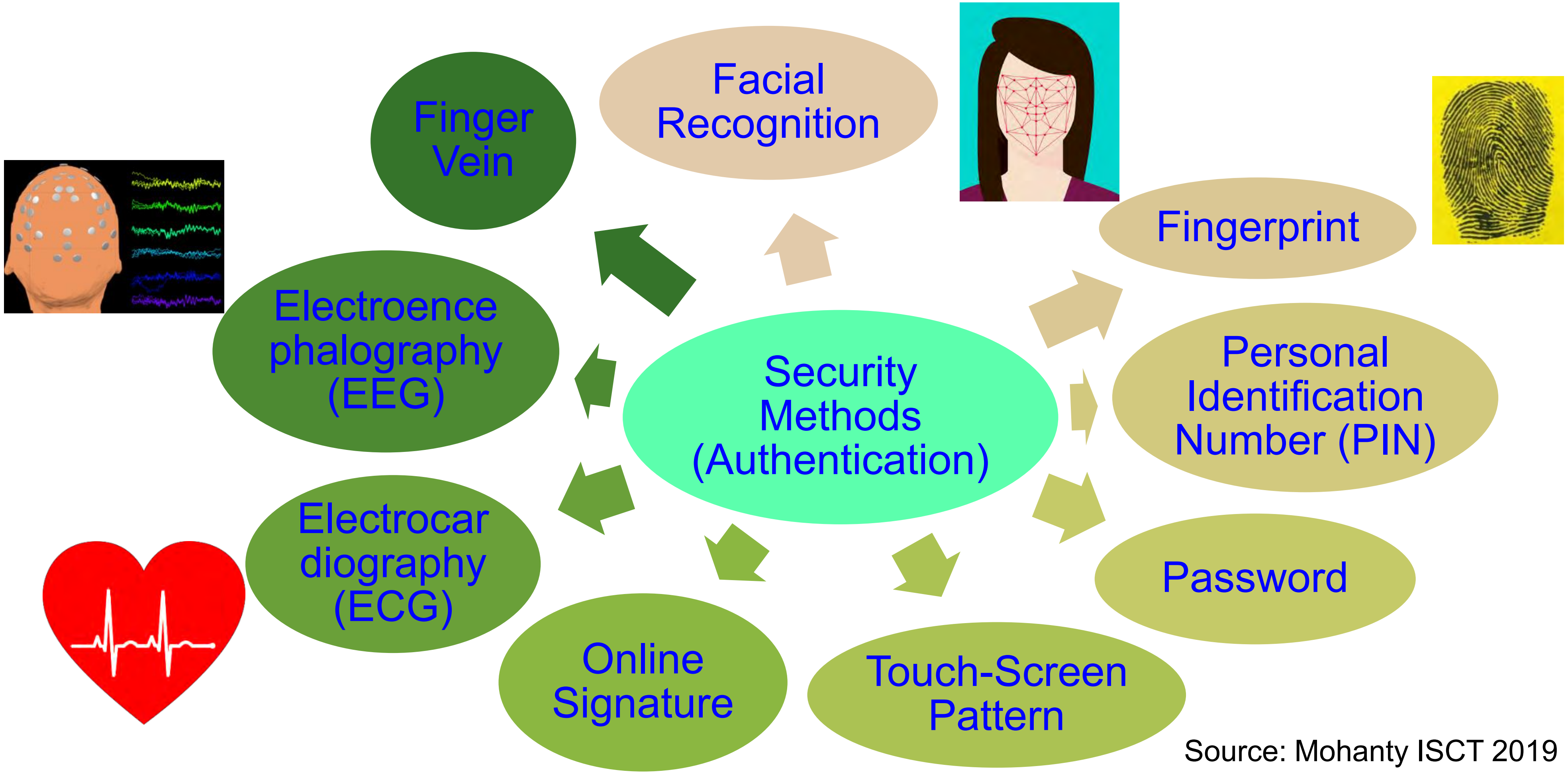
# IoT Cybersecurity - Attacks and Countermeasures




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

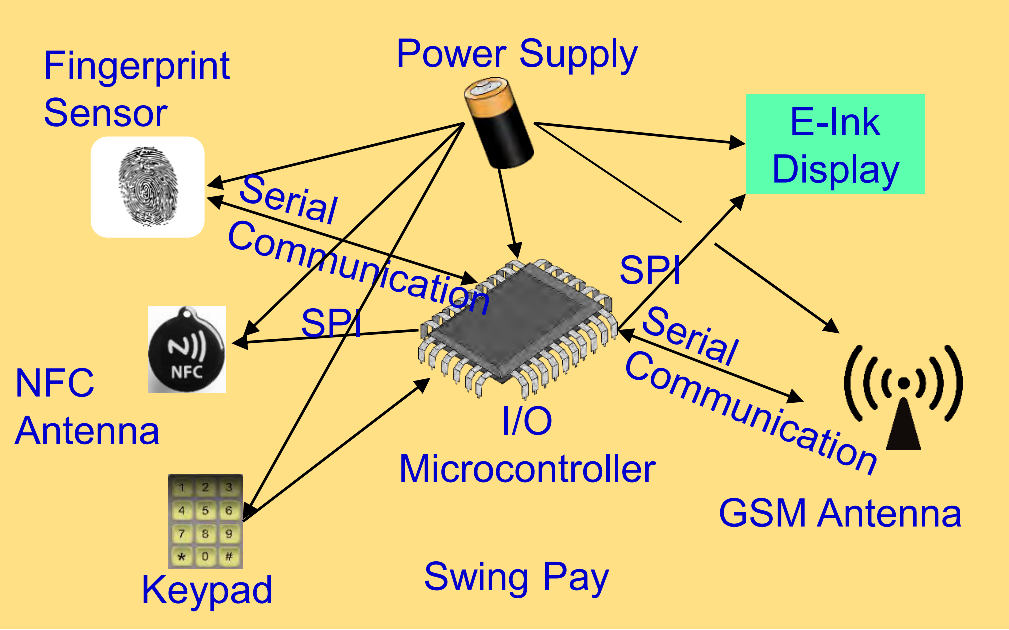
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

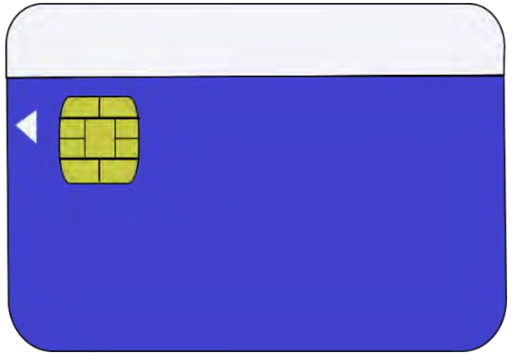
# Security, Authentication, Access Control – Home, Facilities, ...

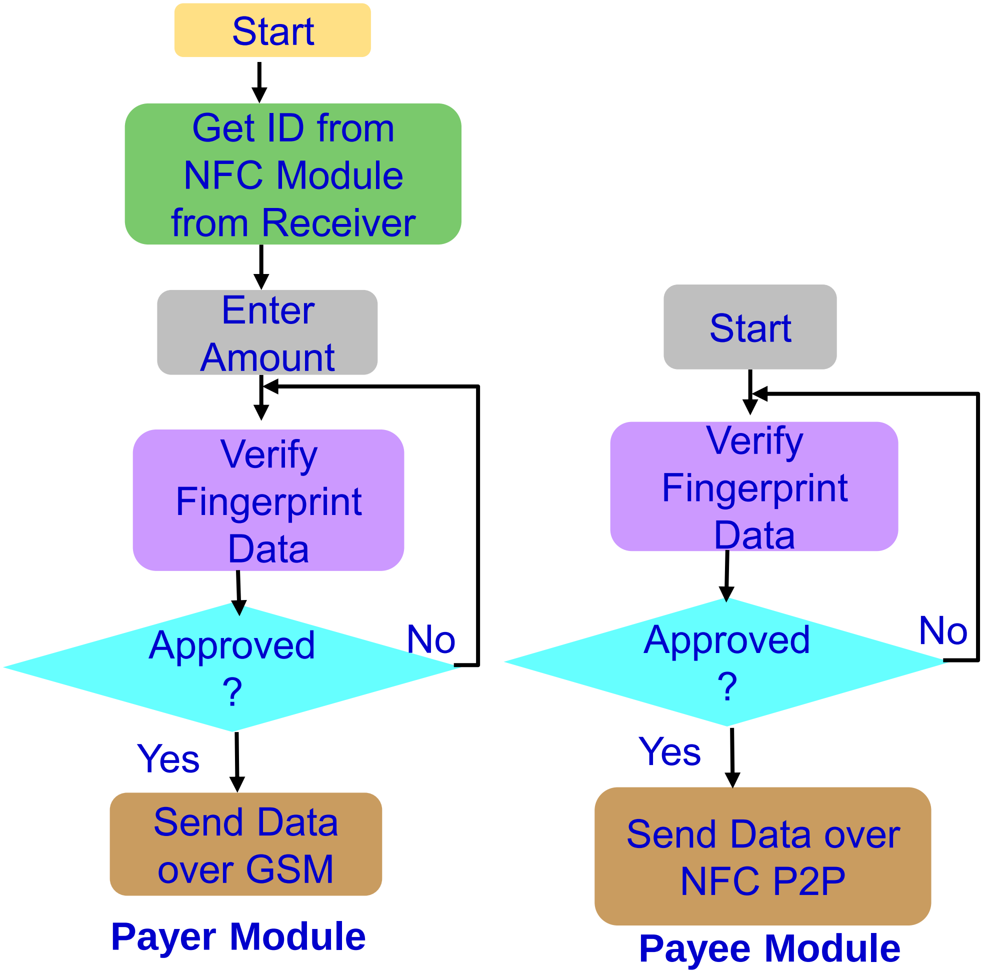



Source: Mohanty ISCT 2019 Keynote

# Our Swing-Pay: NFC Cybersecurity Solution





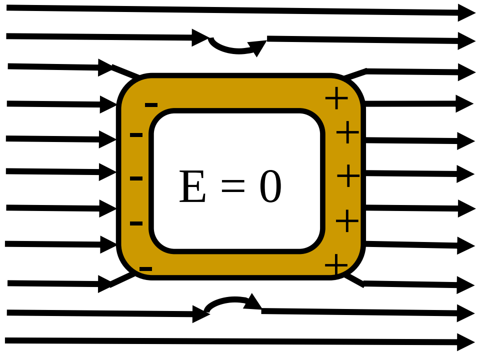

Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

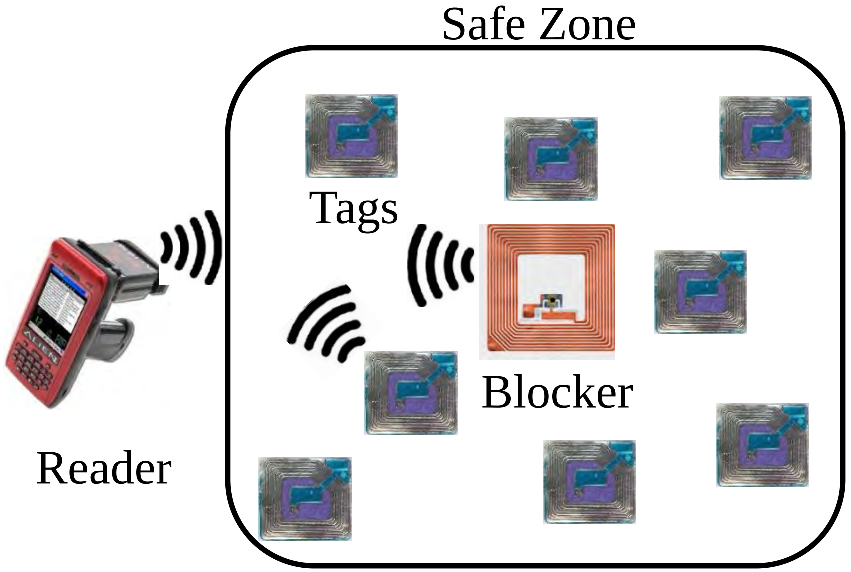
# RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

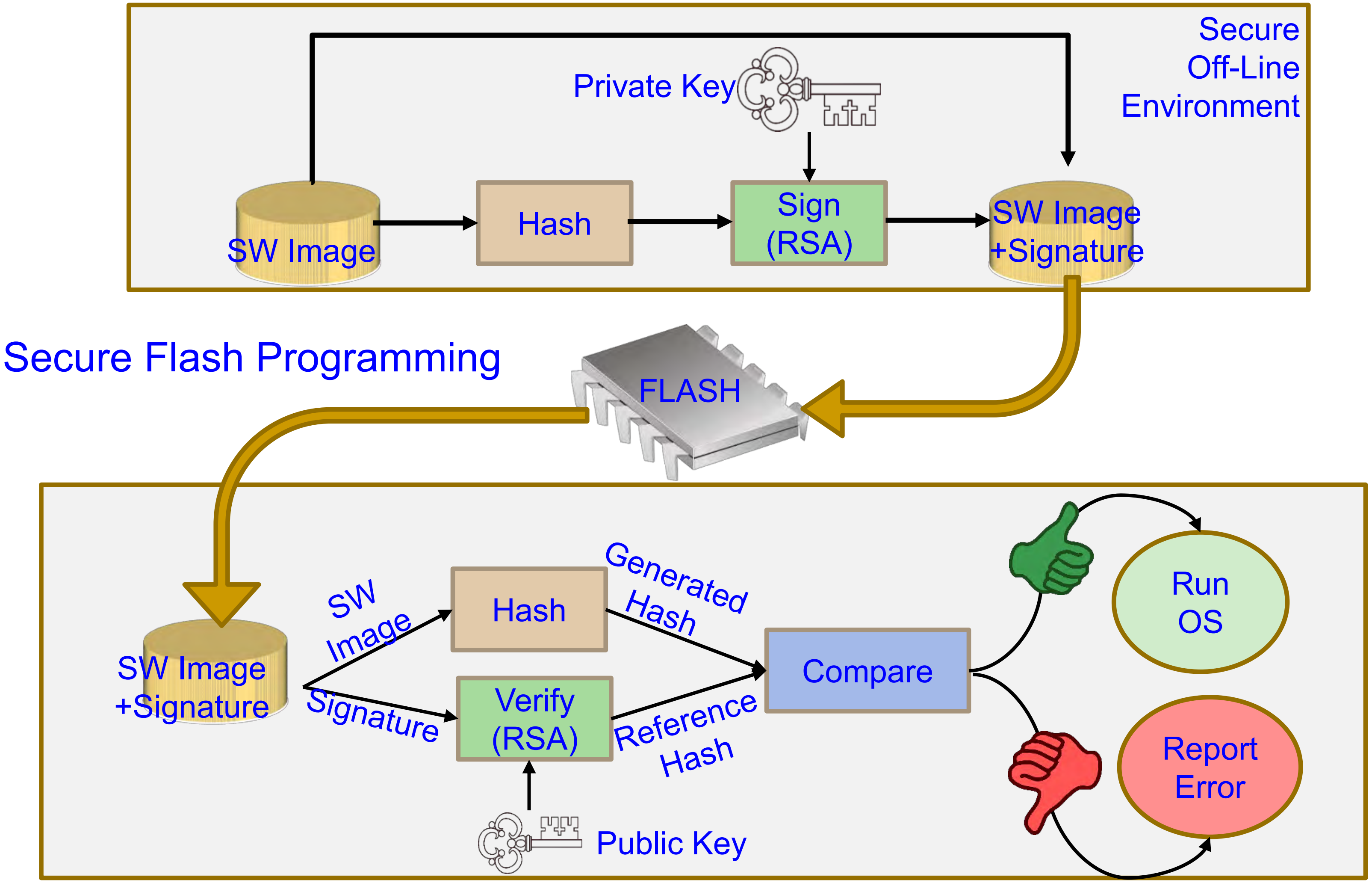



Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

# 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

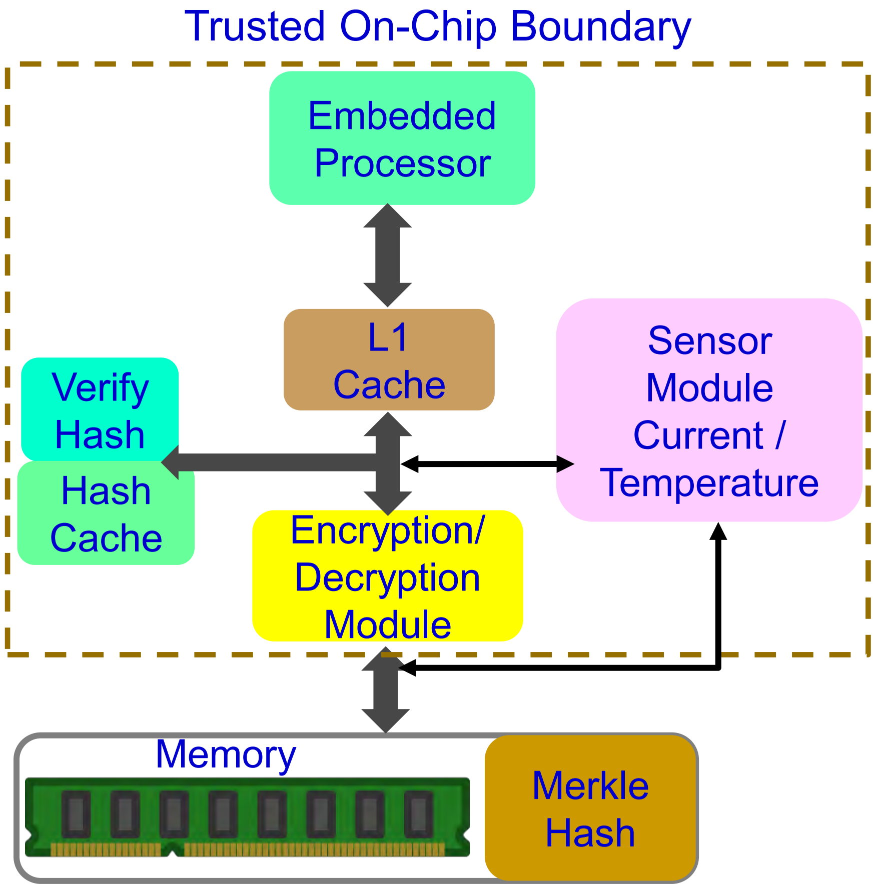
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

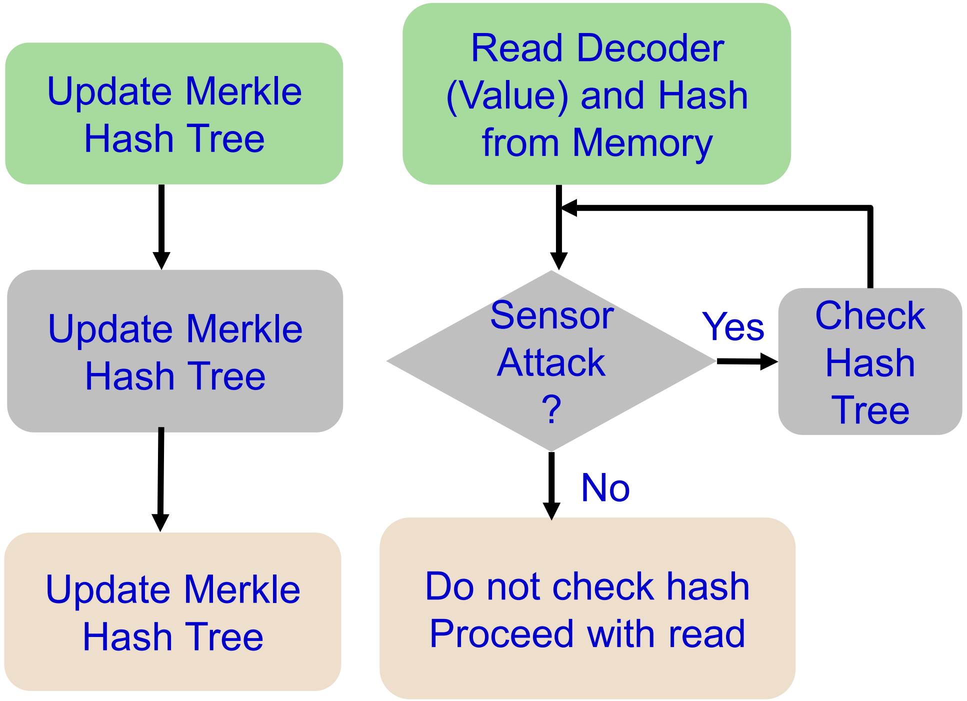
Some performance penalty due to increase in latency!

How Cloud storage changes this scenario?

# Embedded Memory Security




On-Chip/On-Board Memory Protection



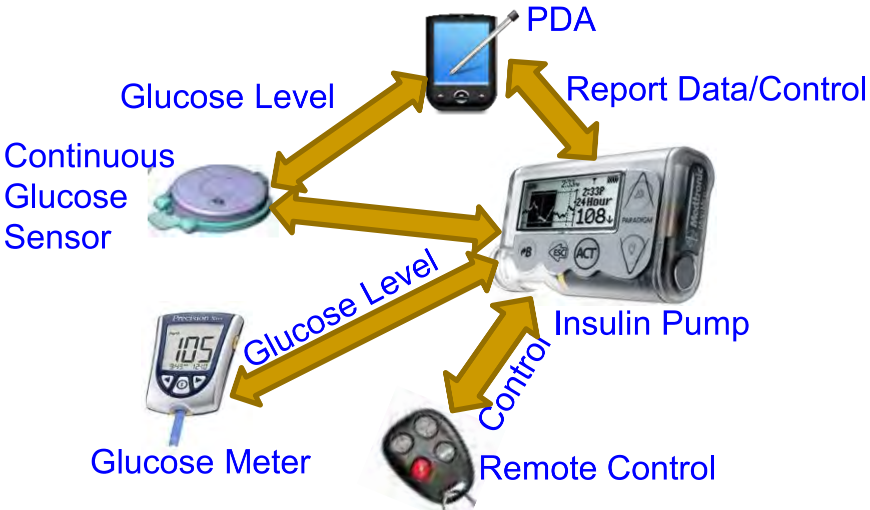

Write Operation

Read Operation

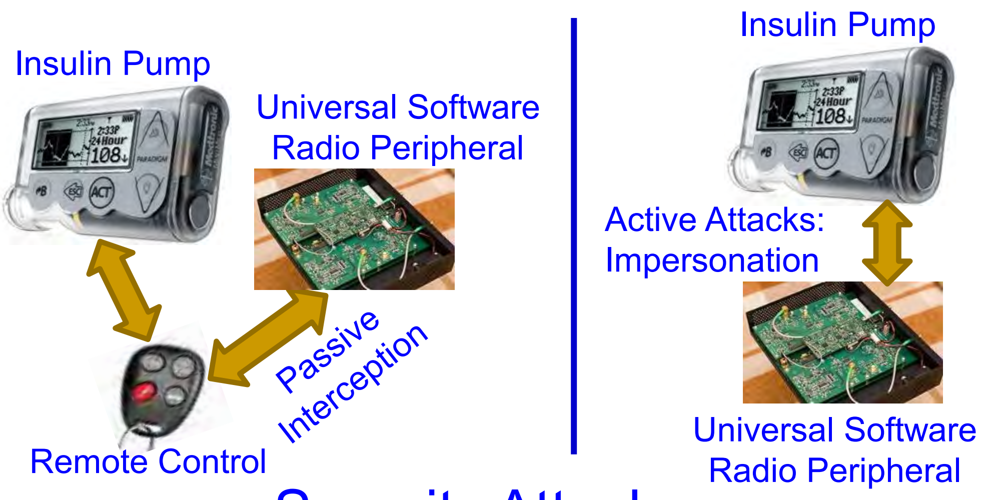
Memory integrity verification with 85% energy savings with minimal performance overhead.

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

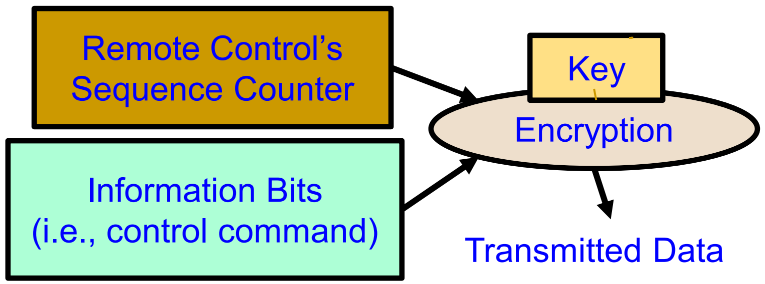
# Smart Healthcare Cybersecurity



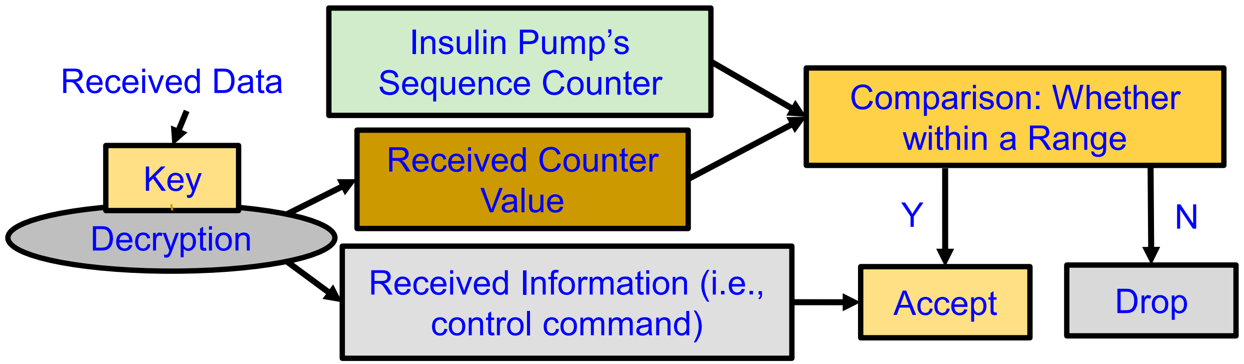

Insulin Delivery System




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 challenging |
| | 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

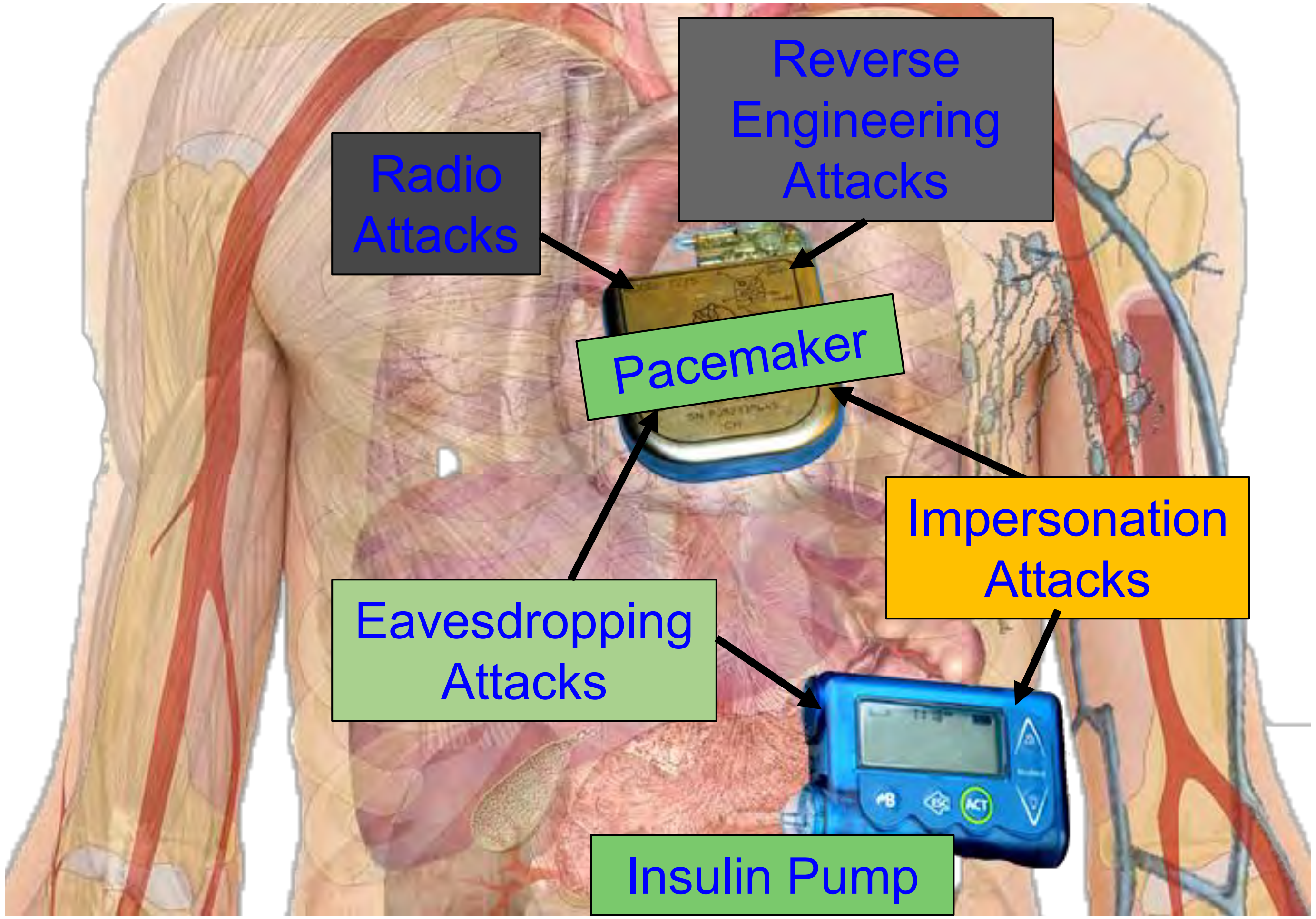
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

## 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.

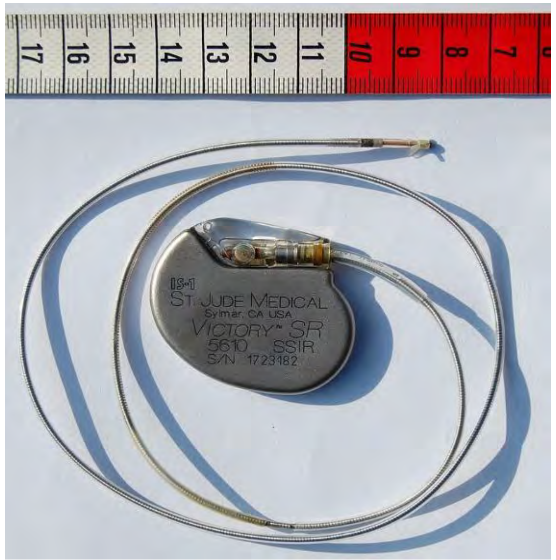
# Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard




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

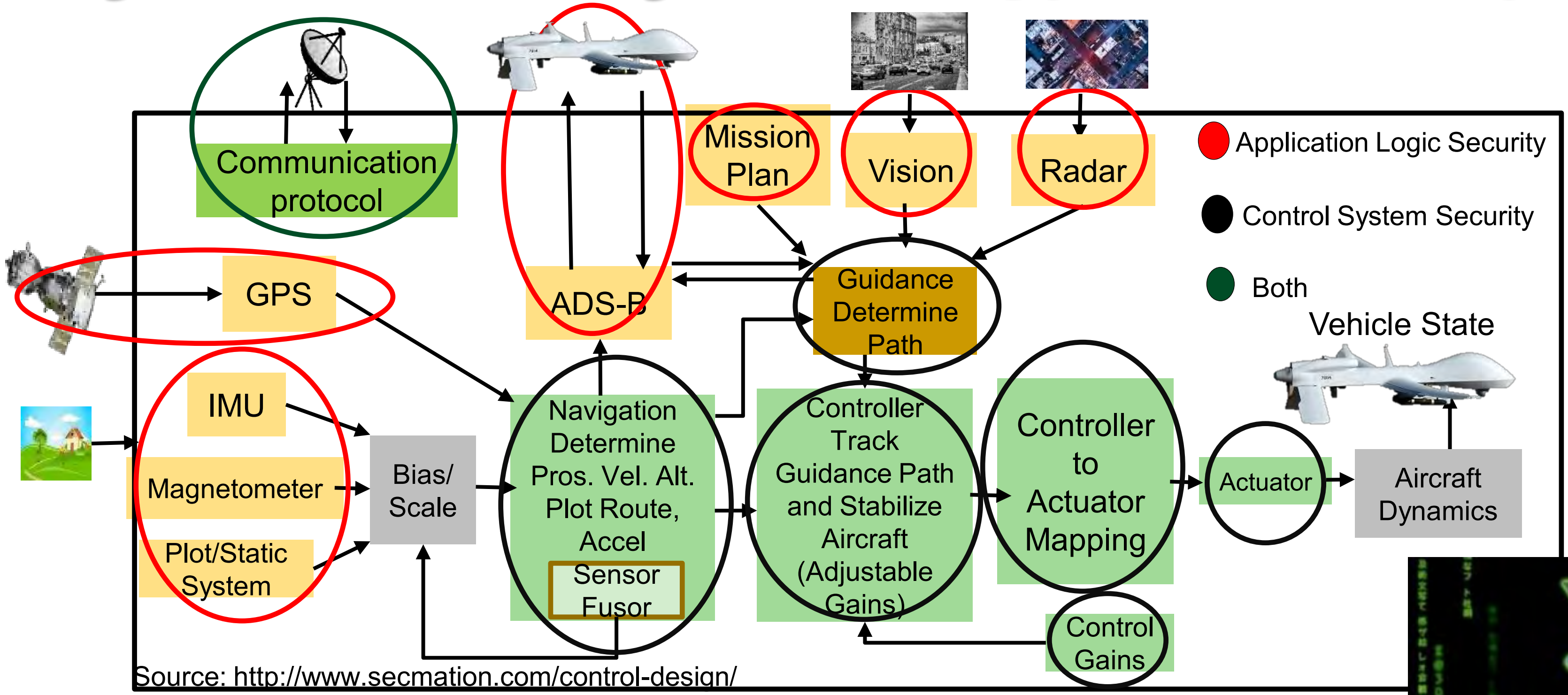
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

- 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




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


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

Cybersecurity Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

# 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

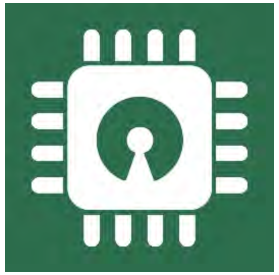
- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

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

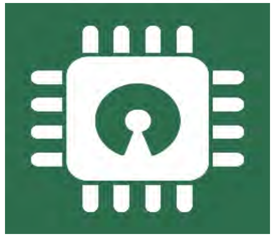


## Hardware Based

- 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

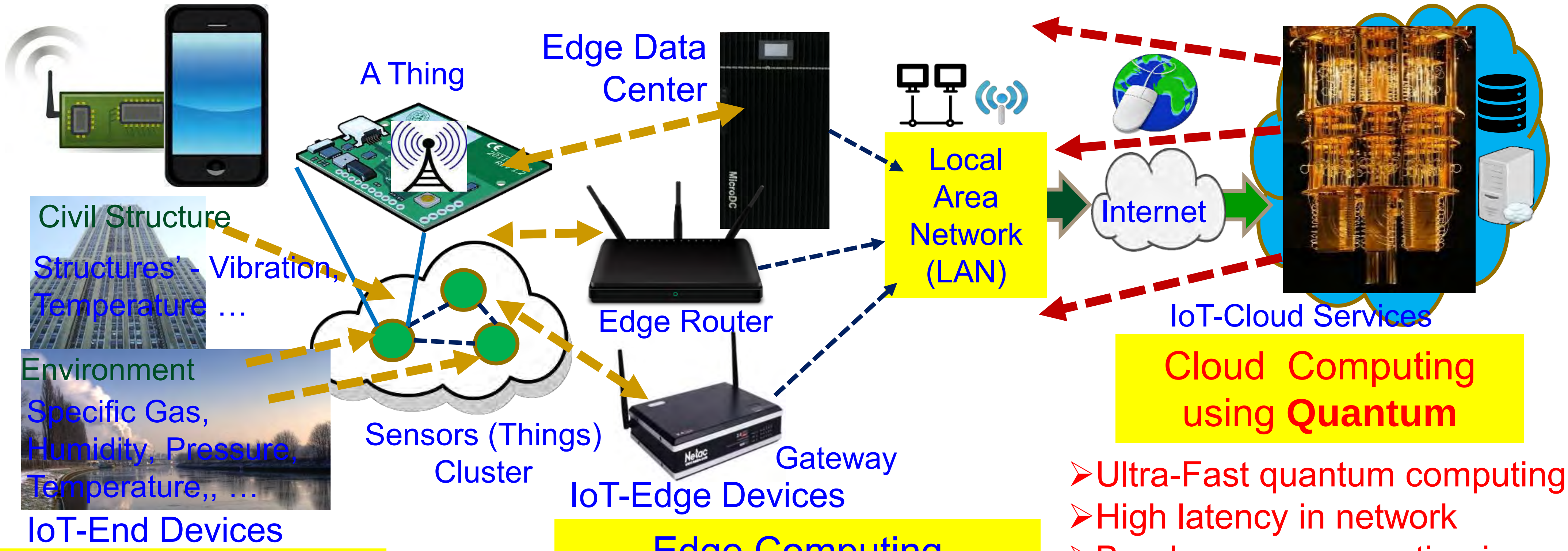
- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can't stop hardware reverse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

## Hardware Based

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

Source: Mohanty ICCE Panel 2018

# Cybersecurity Nightmare ← Quantum Computing




**Cloud Computing using Quantum**

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

**Edge Computing**

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

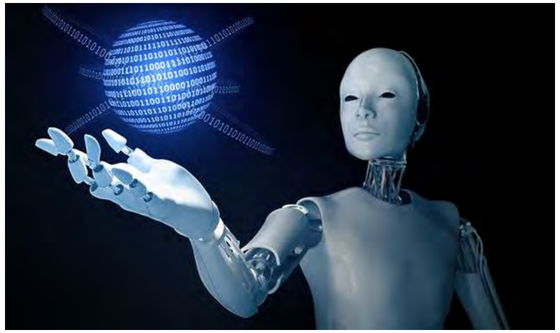
**In-Sensor/End-Device Computing**

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

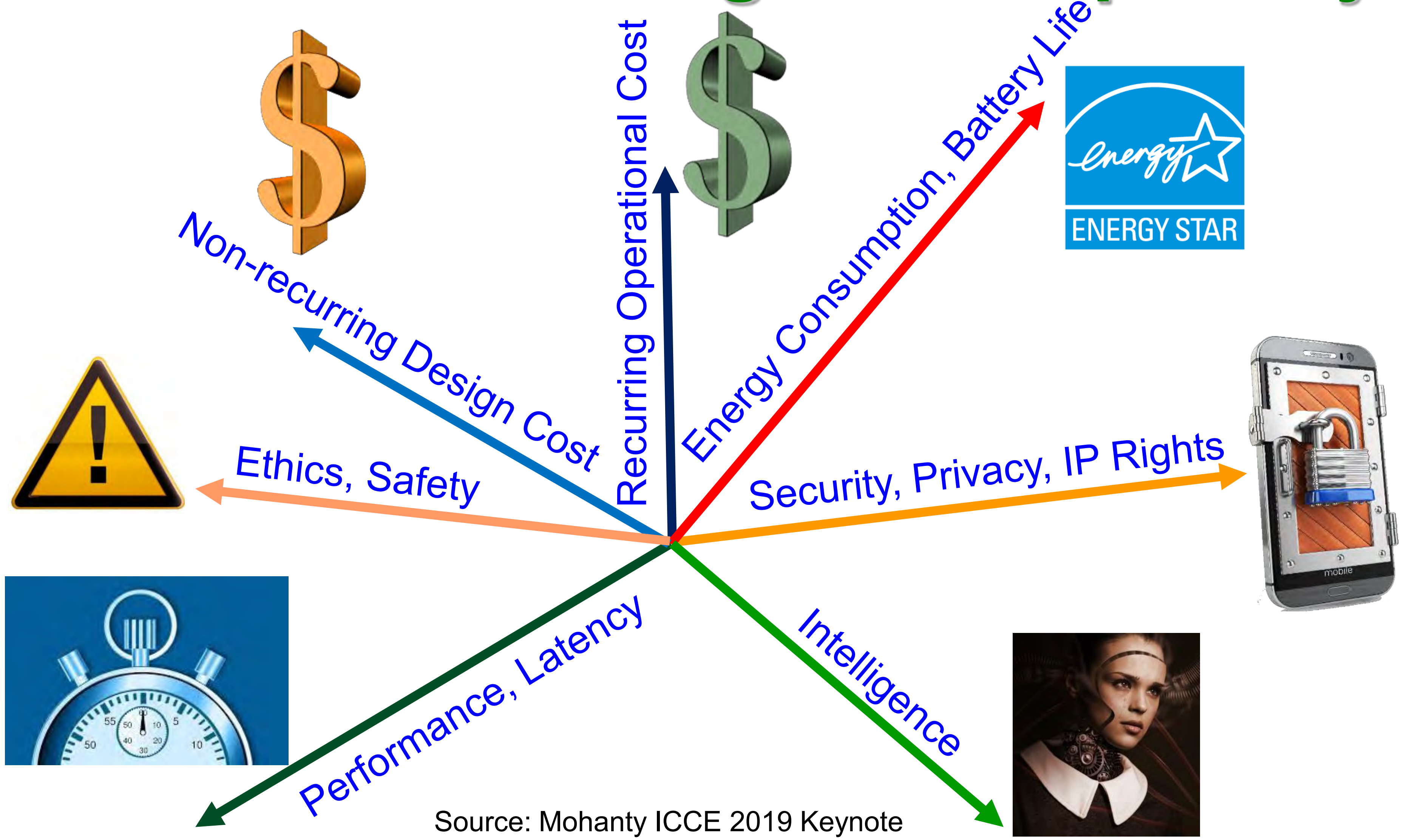
A quantum computer could break a 2048-bit RSA encryption in 8 hours.

# Security-by-Design (SbD) – The Principle





# IoT/CPS Design – Multiple Objectives




Source: Mohanty ICCE 2019 Keynote

Smart Cities
Vs
Smart Villages

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

1995
Privacy by Design (PbD)

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

2018
General Data Protection Regulation (GDPR)

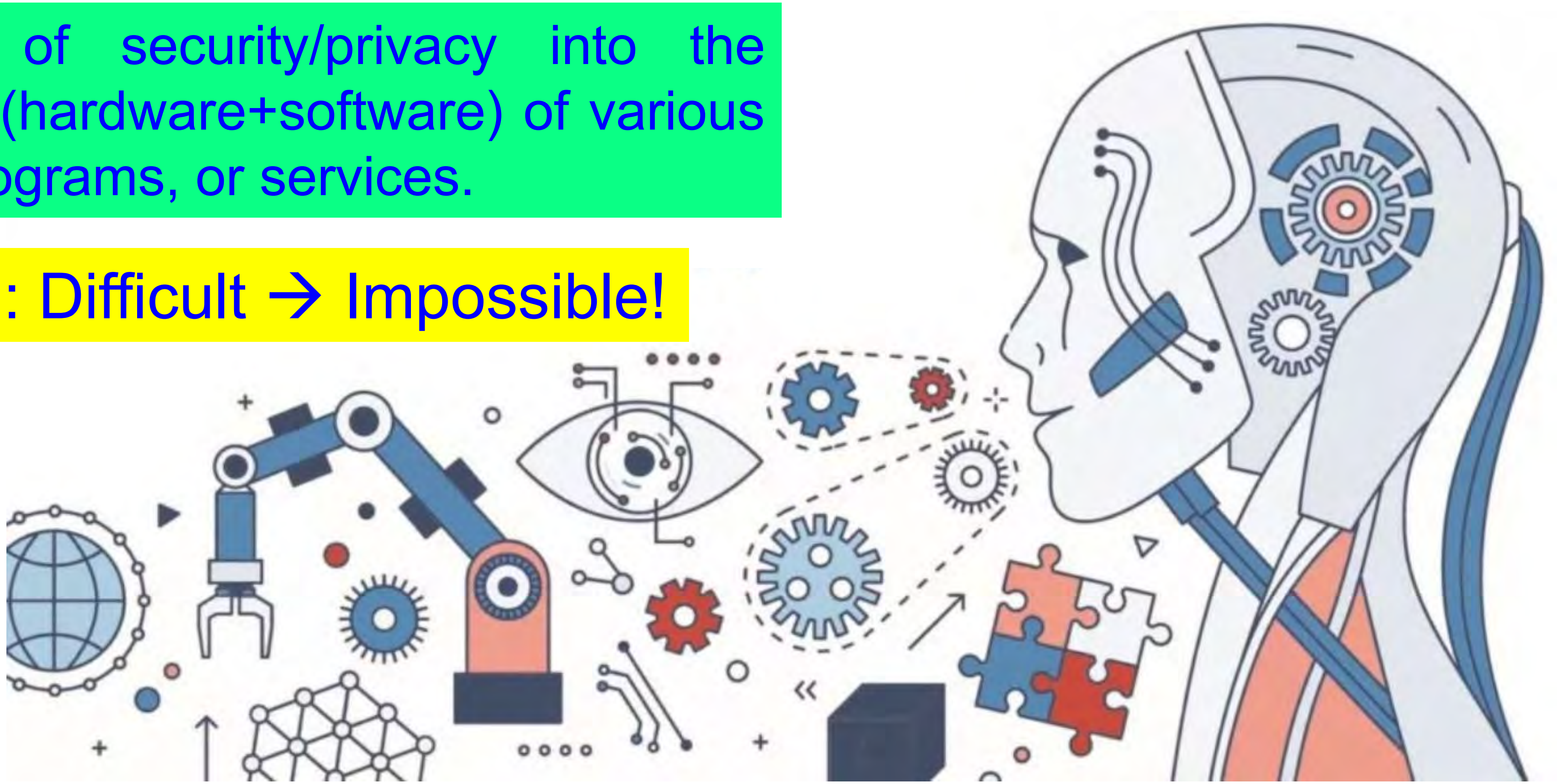
- GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

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

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

Retrofitting: Difficult → Impossible!



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

# Security by Design (SbD)

**7 Fundamental Principles**

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

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

# Hardware-Assisted Security (HAS)

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

Privacy by Design (PbD)

Security/Secure by Design (SbD)

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

Bluetooth Hardware Security

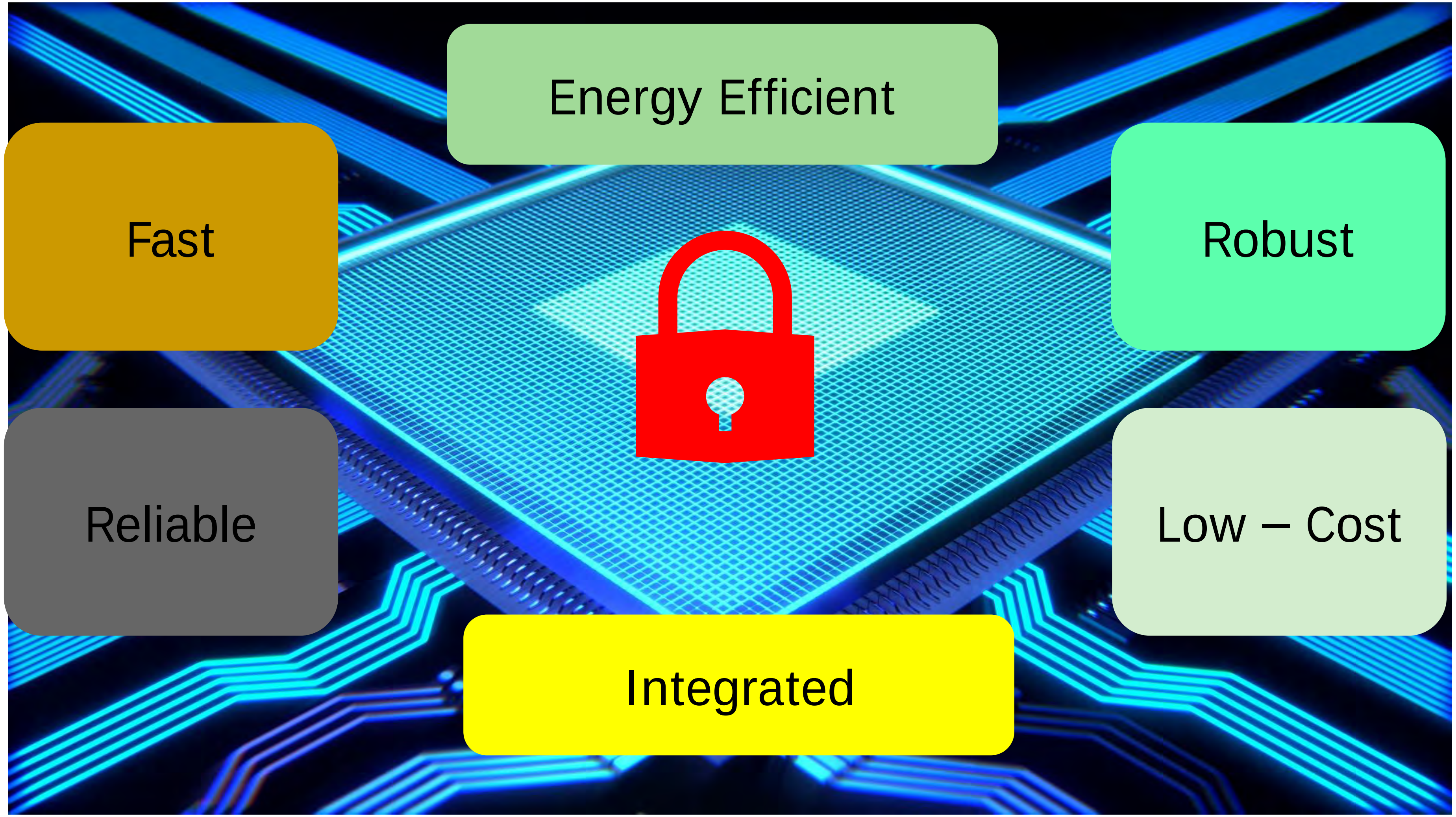
Memory Protection

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.

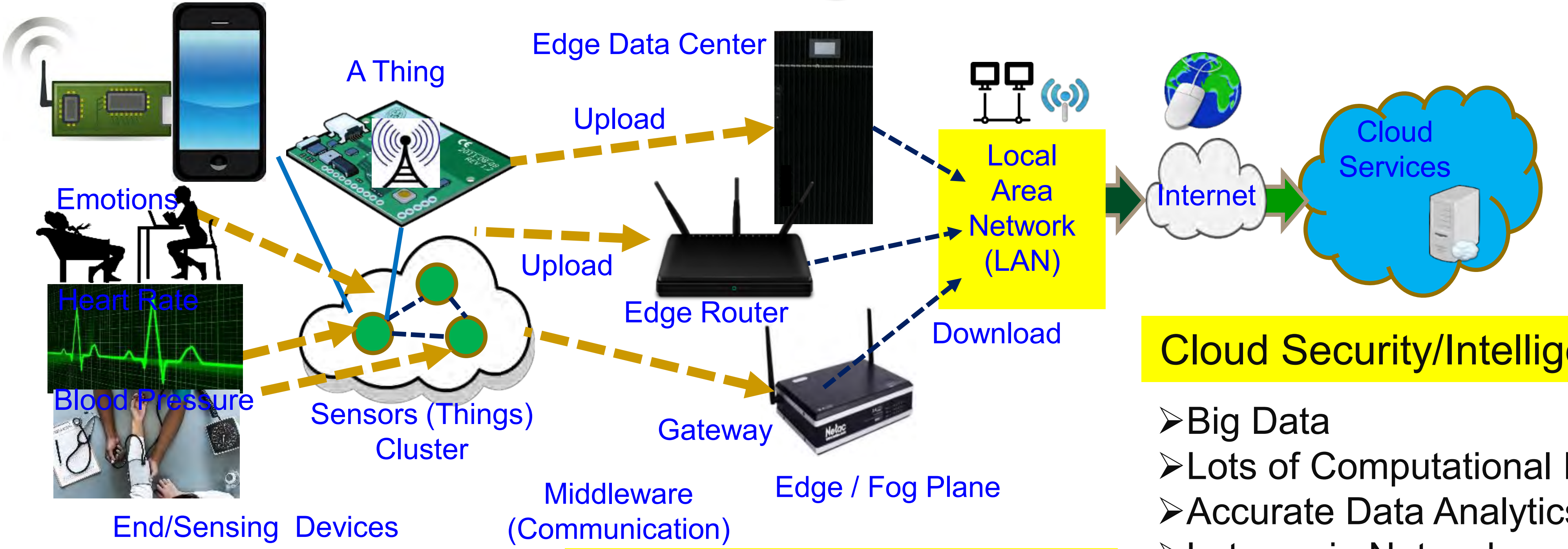
# Secure SoC: Different Design Alternatives

- 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




## End Security/Intelligence

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

## Edge Security/Intelligence

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

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

## Cloud Security/Intelligence

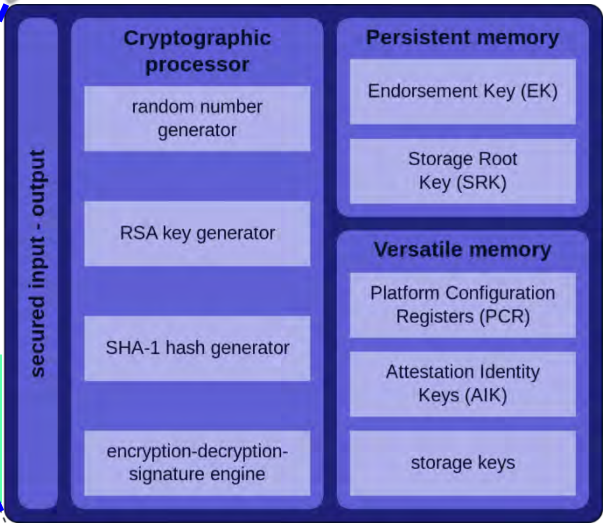
- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy Overhead in Communications

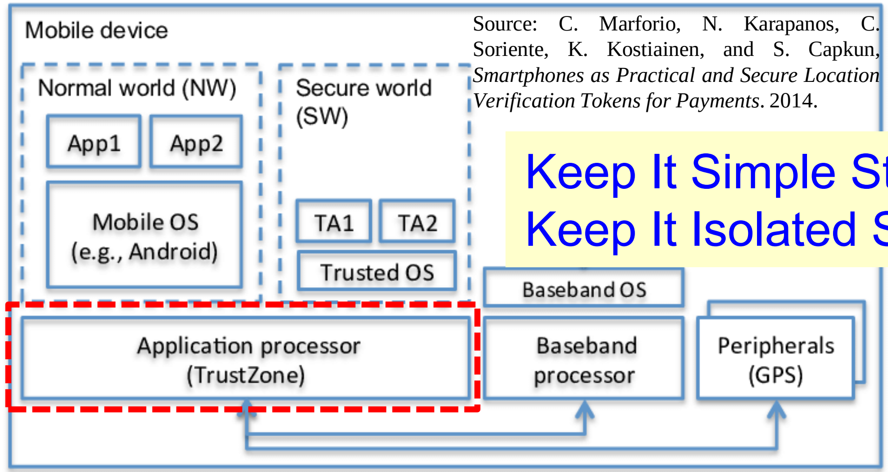
Heavy-Duty ML is more suitable for smart cities

# 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.

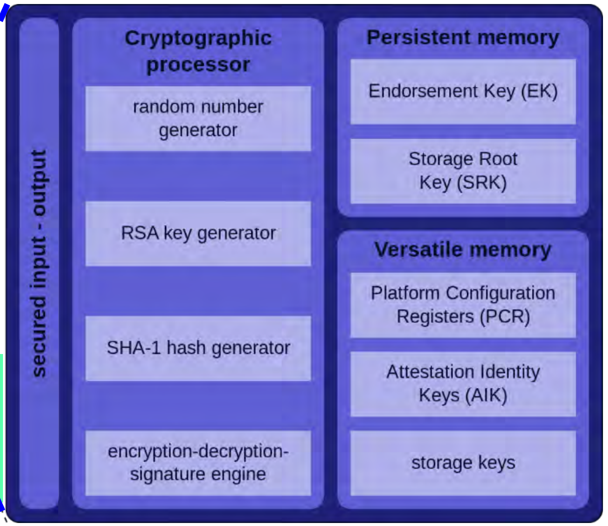
Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

# PUF versus TPM

Trusted Platform Module (TPM)




Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

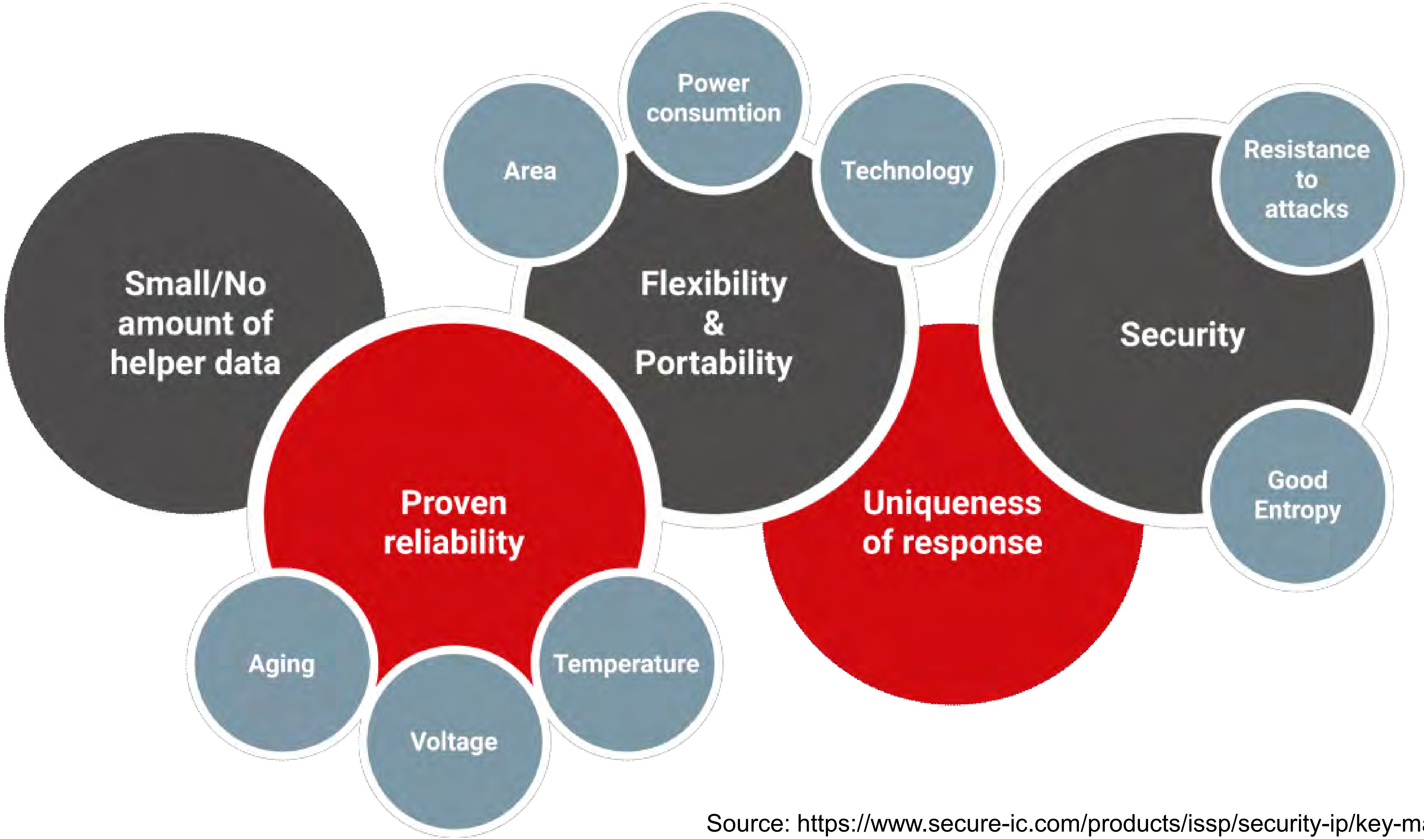
**TPM**:

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

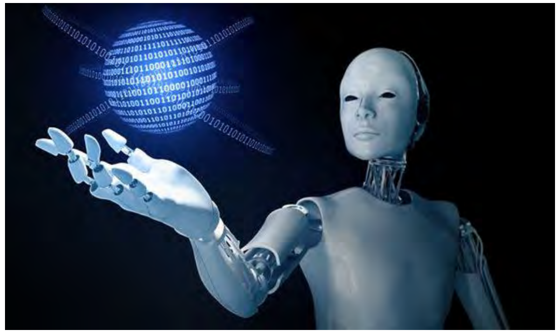
# PUF: Advantages



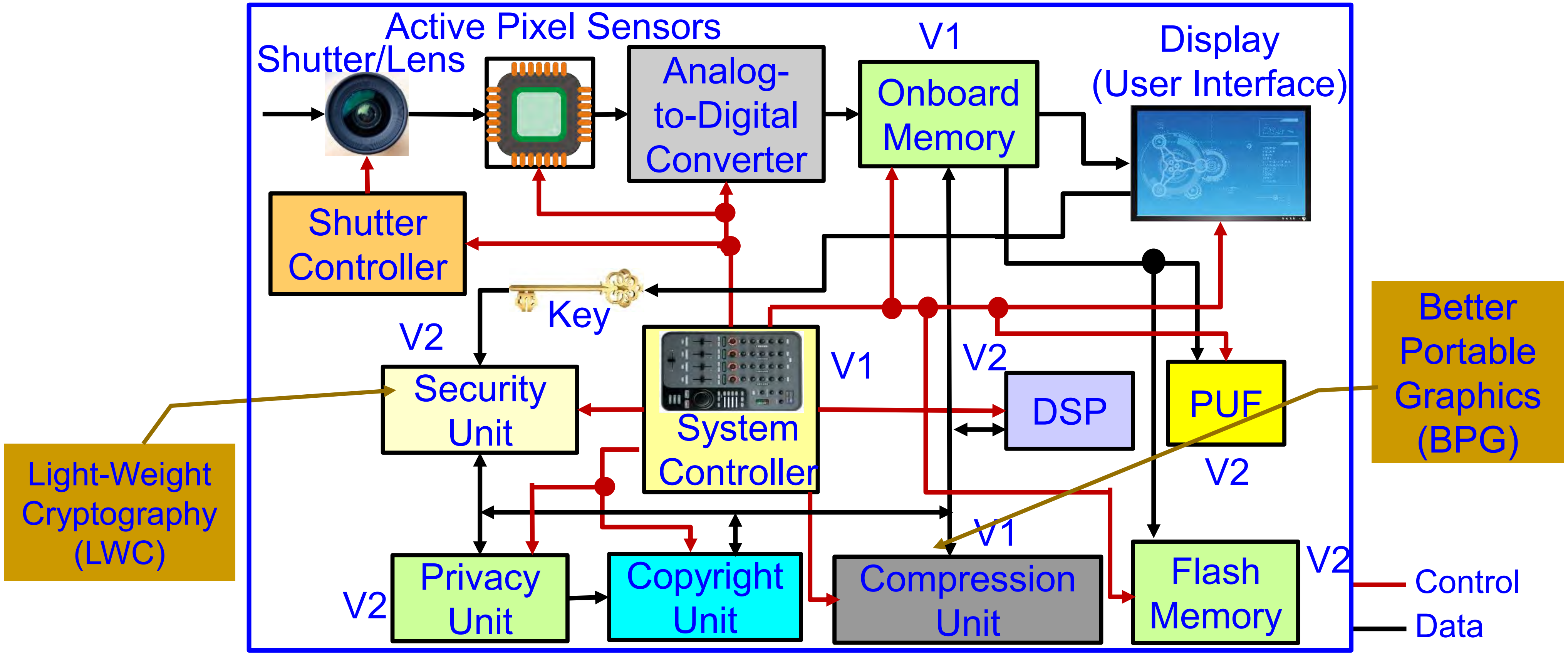

Source: https://www.secure-ic.com/products/issp/security-ip/key-management/puf-ip/

# Security-by-Design (SbD) – Specific Examples





# Secure Digital Camera (SDC) – My Invention

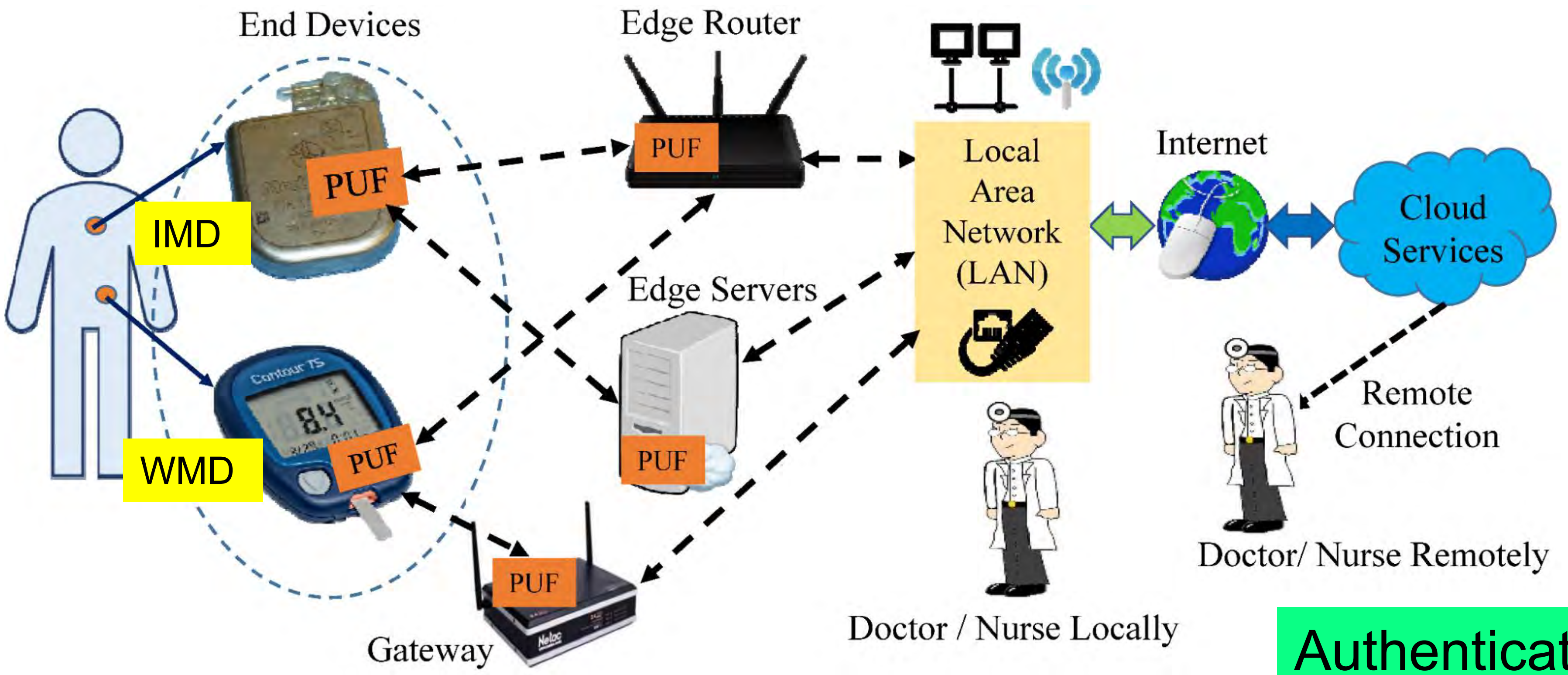



Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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.

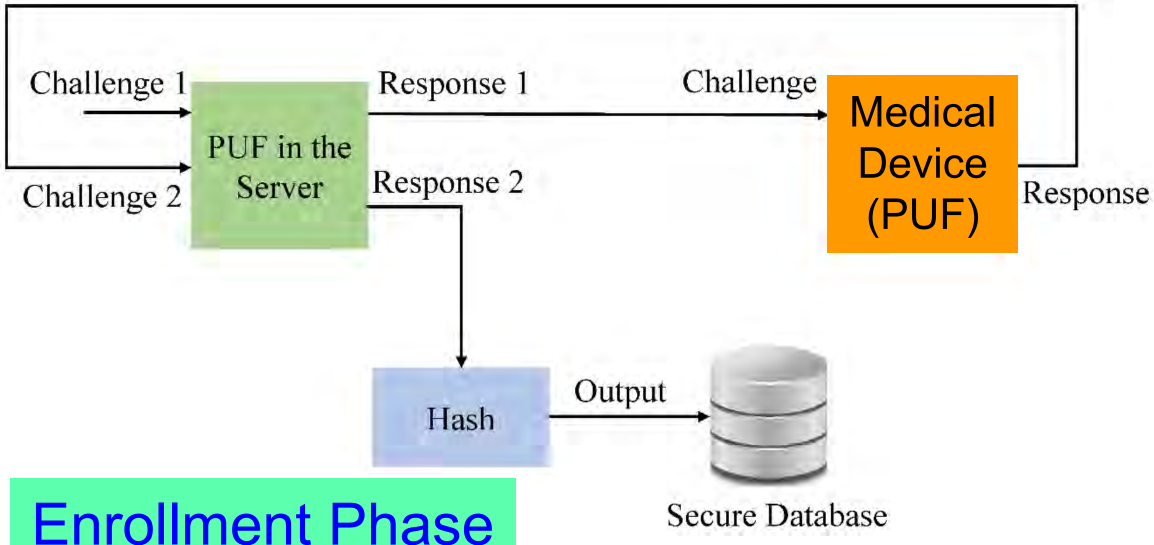
# PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS




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

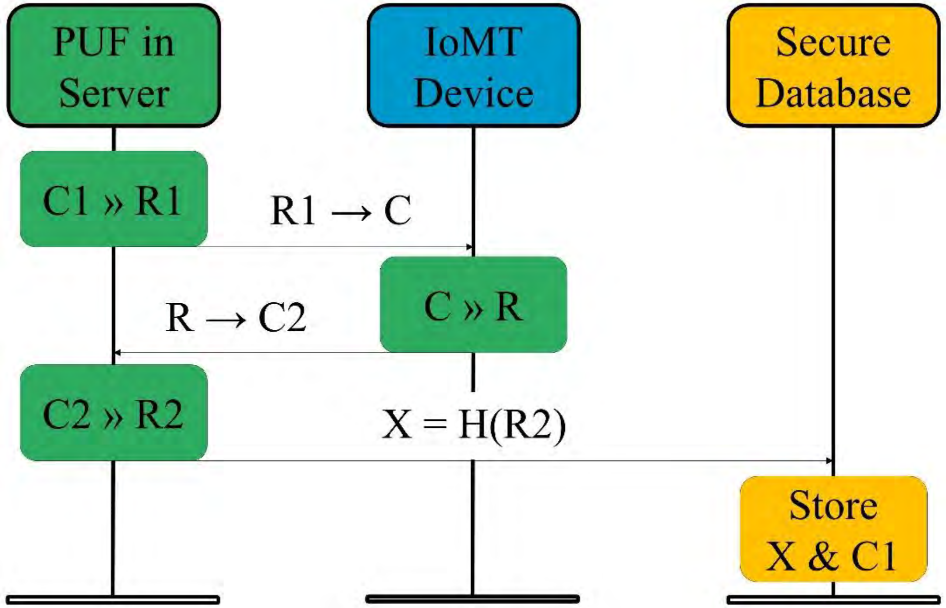



Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

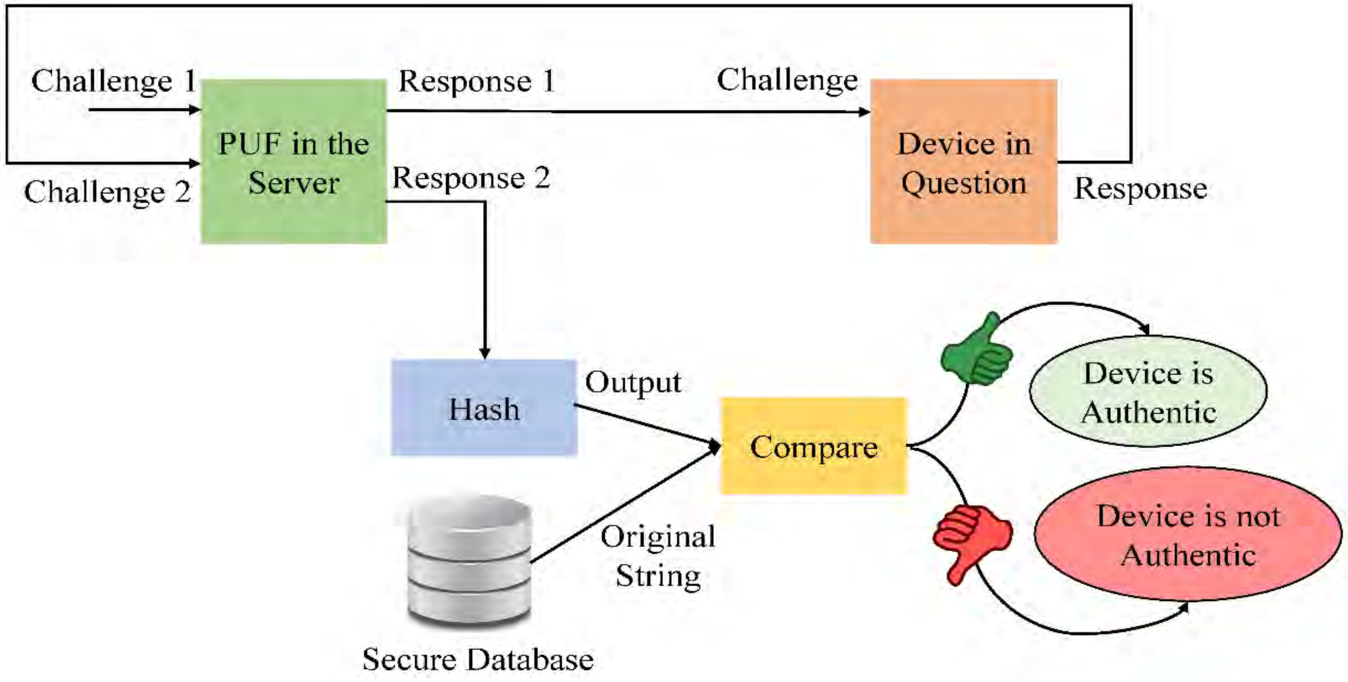



PUF Security Full Proof:

- 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

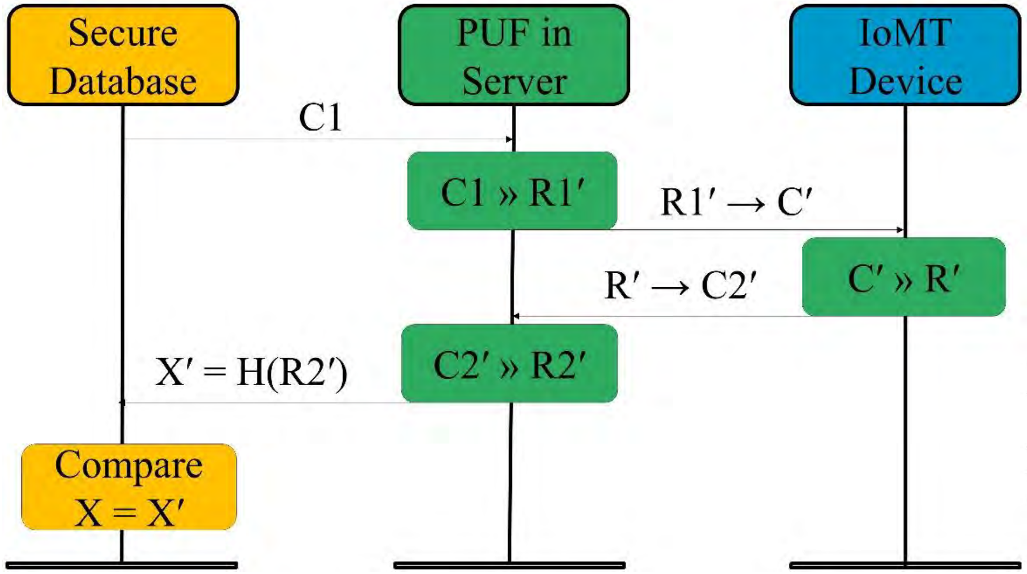



Authentication Phase

At the Doctor

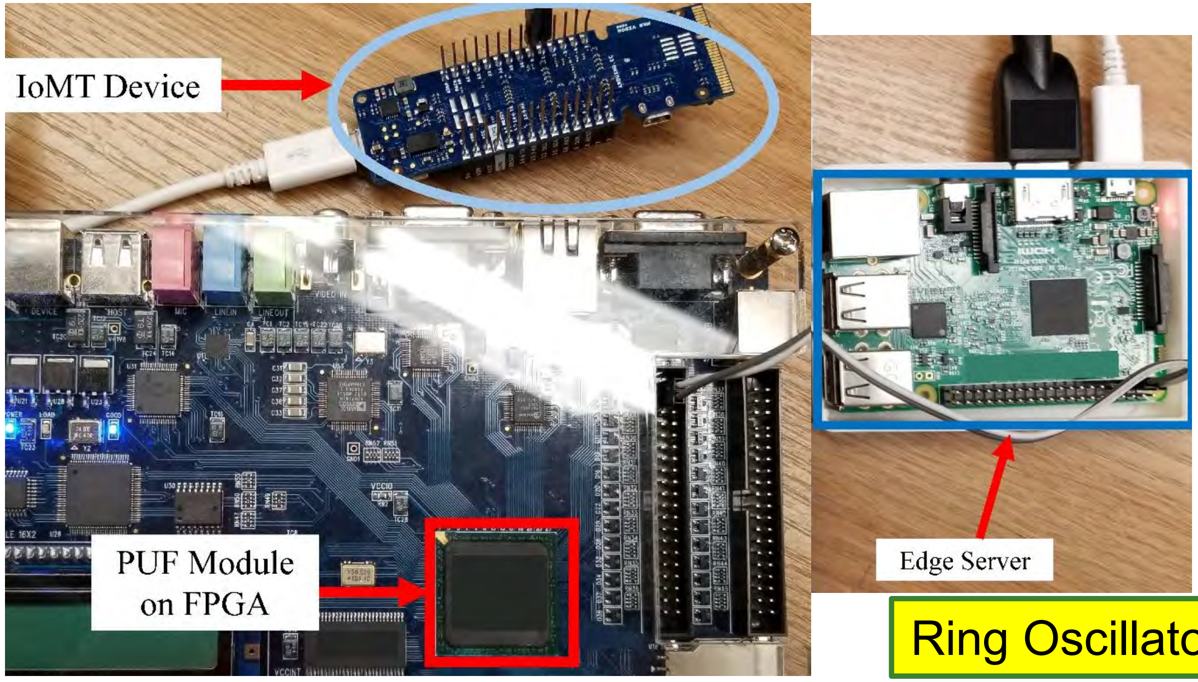
- When doctor needs to access an existing IoMT-device

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



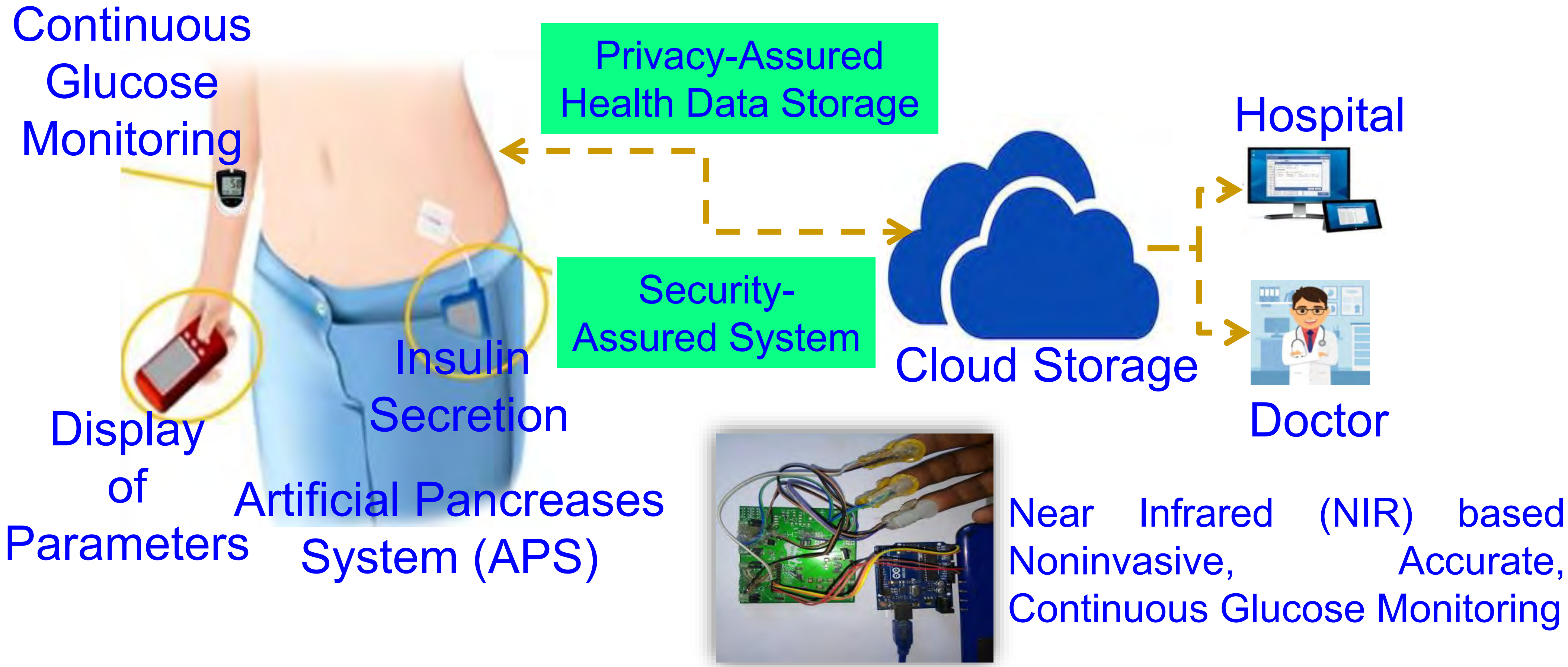

Average Power Overhead – 200 μW

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 |

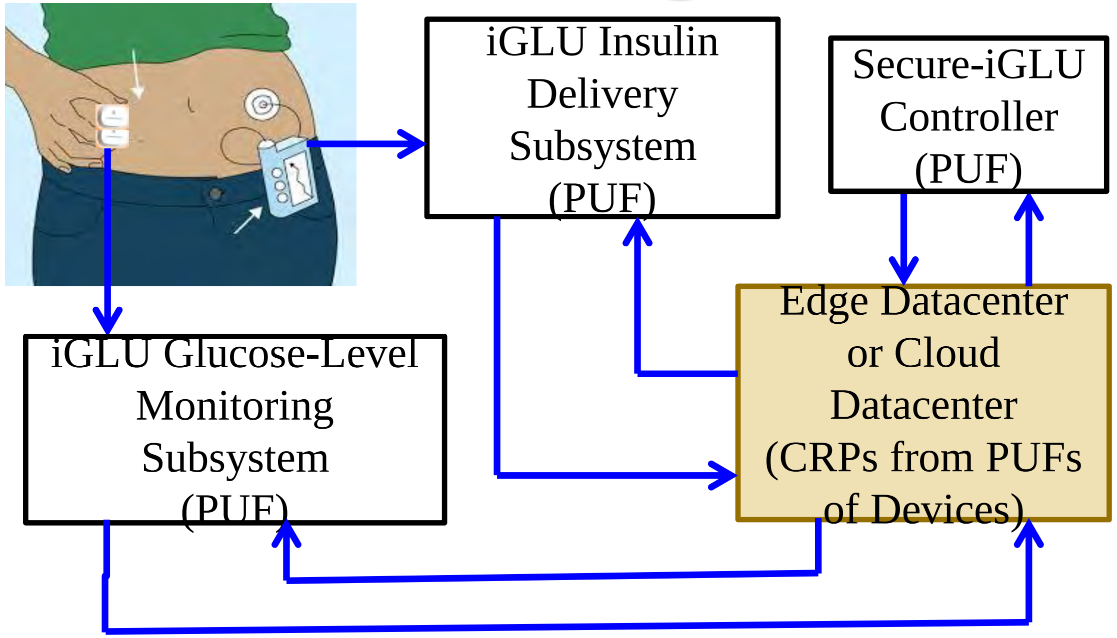
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics*, Vol 65, No 3, Aug 2019, pp. 388--397.

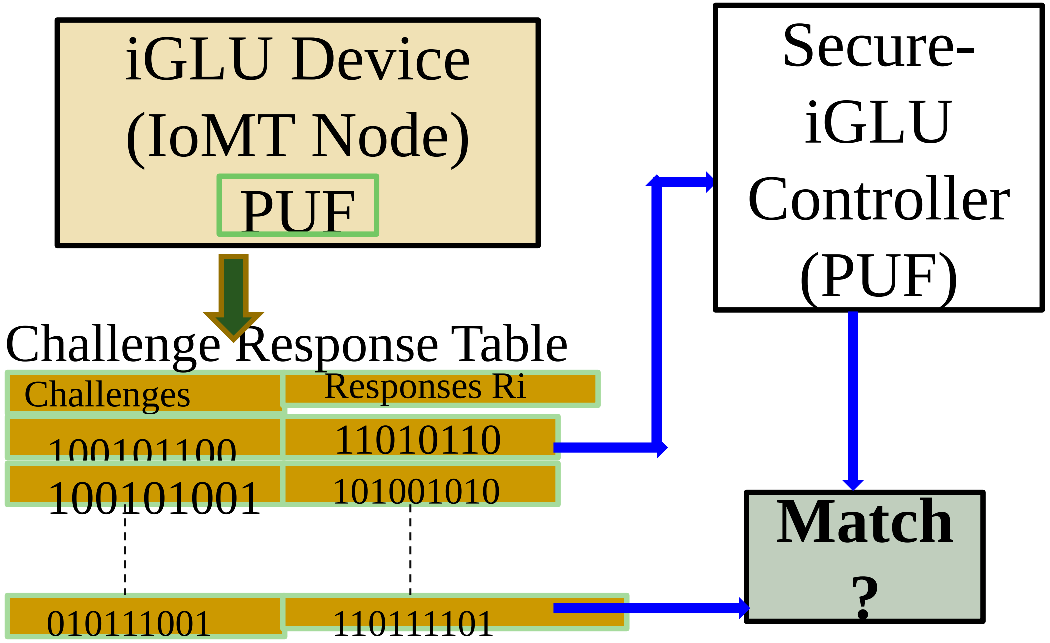
# iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery




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

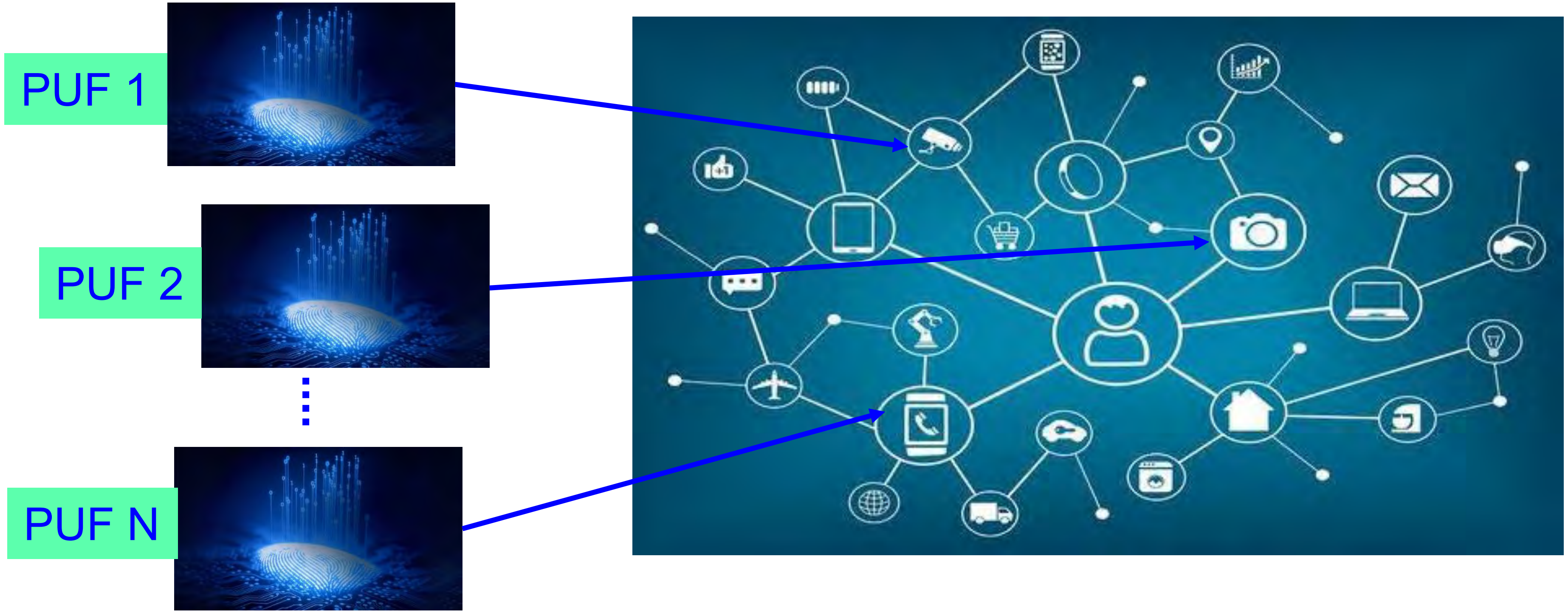



Arbiter PUF – 64-bit, 128-bit, 256 bit …

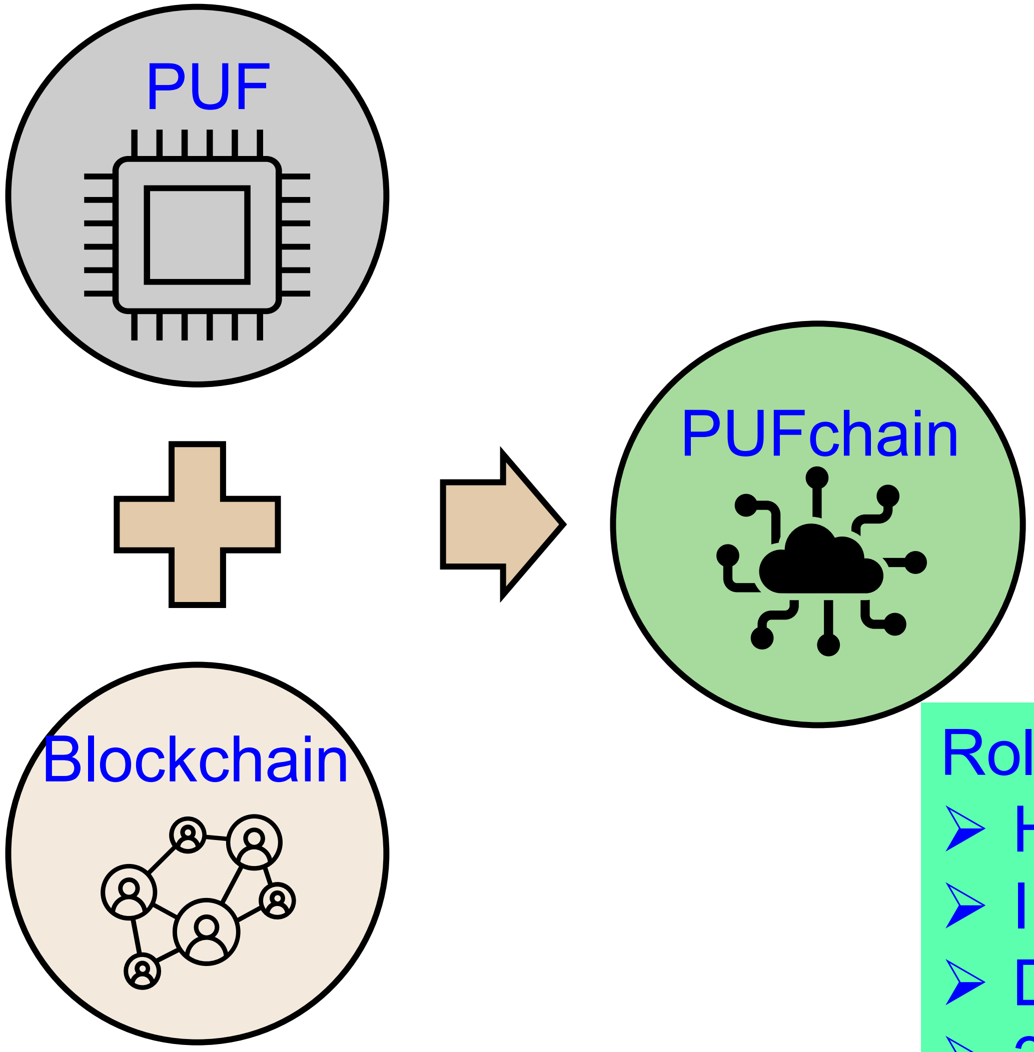
Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

# 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

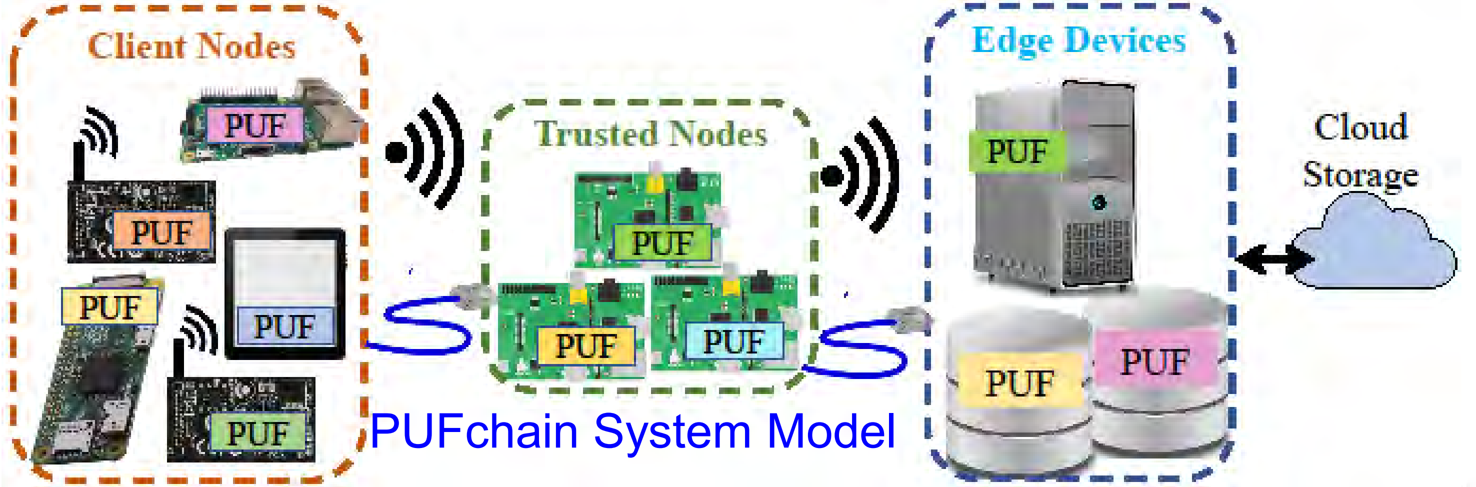
Roles of PUF:

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

# Our PUFchain – 3 Variants

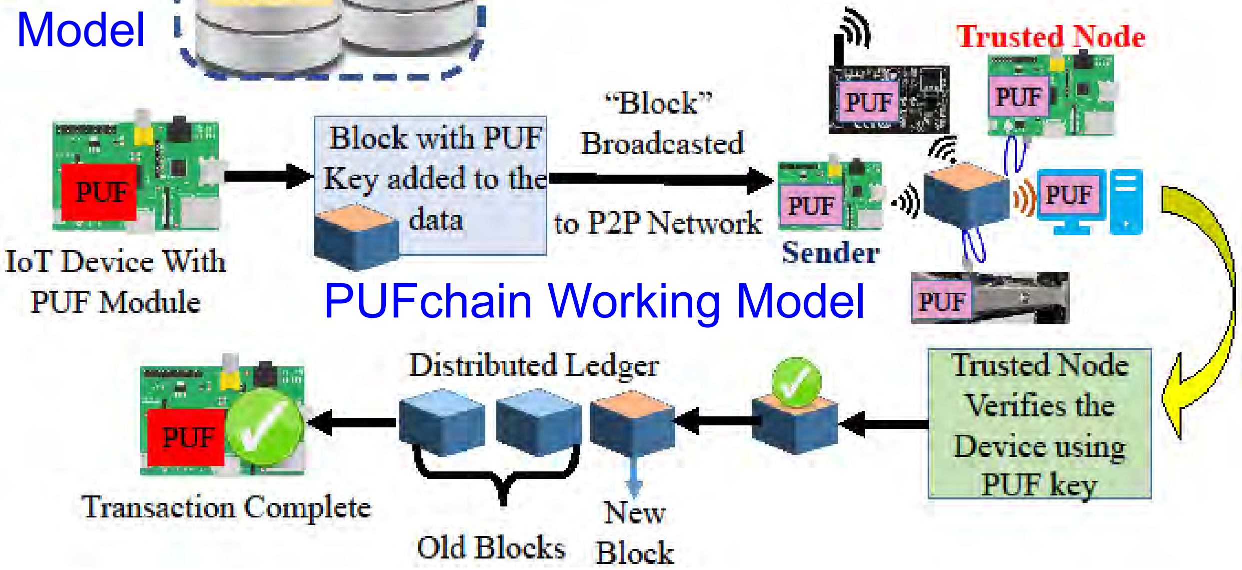
| Research Works | Distributed Ledger Technology | Focus Area | Security Approach | Security Primitive | Security Principle |
|---|---|---|---|---|---|
| PUFchain | Blockchain | IoT / CPS (Device and Data) | Proof of Physical Unclonable Function (PUF) Enabled Authentication | PUF + Blockchain | Hardware 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



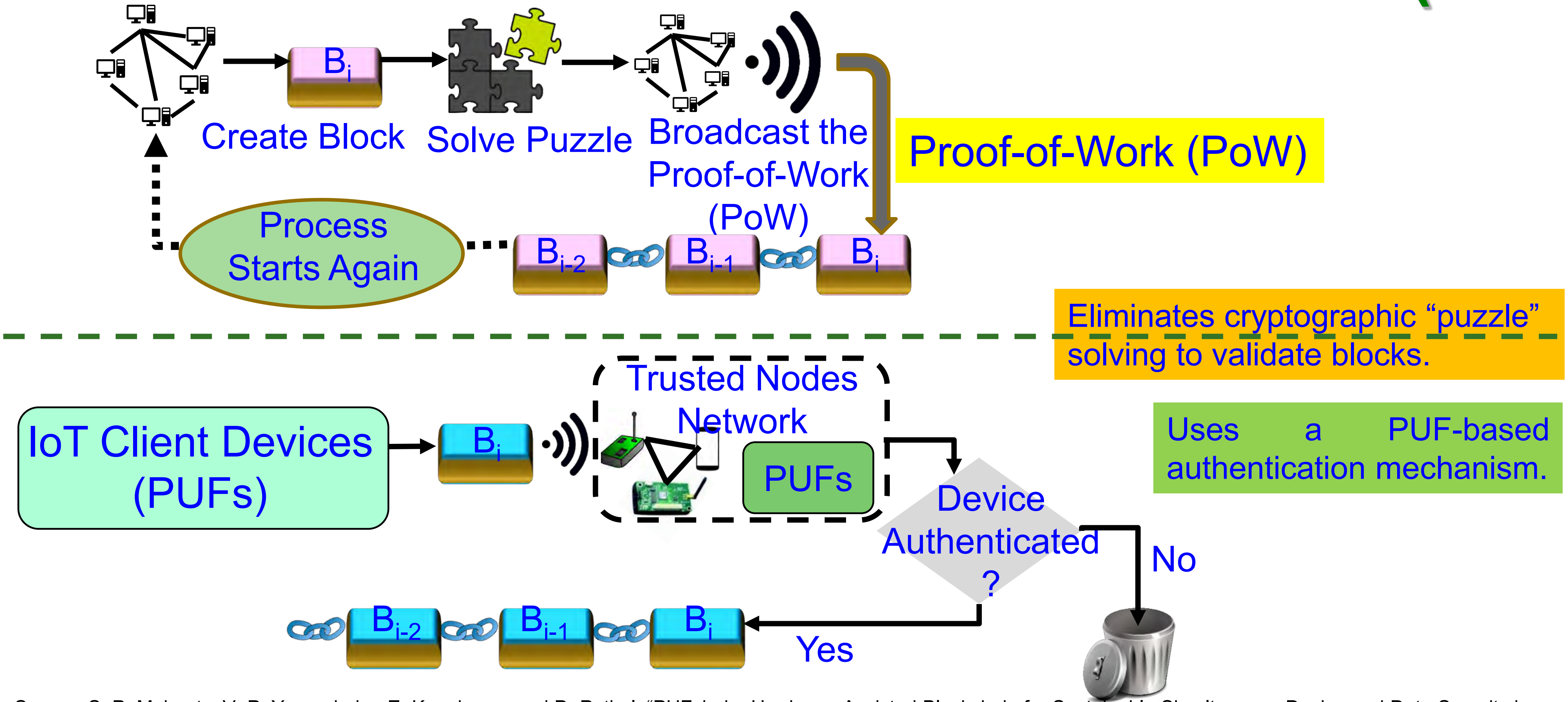

PUFchain Working Model

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

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

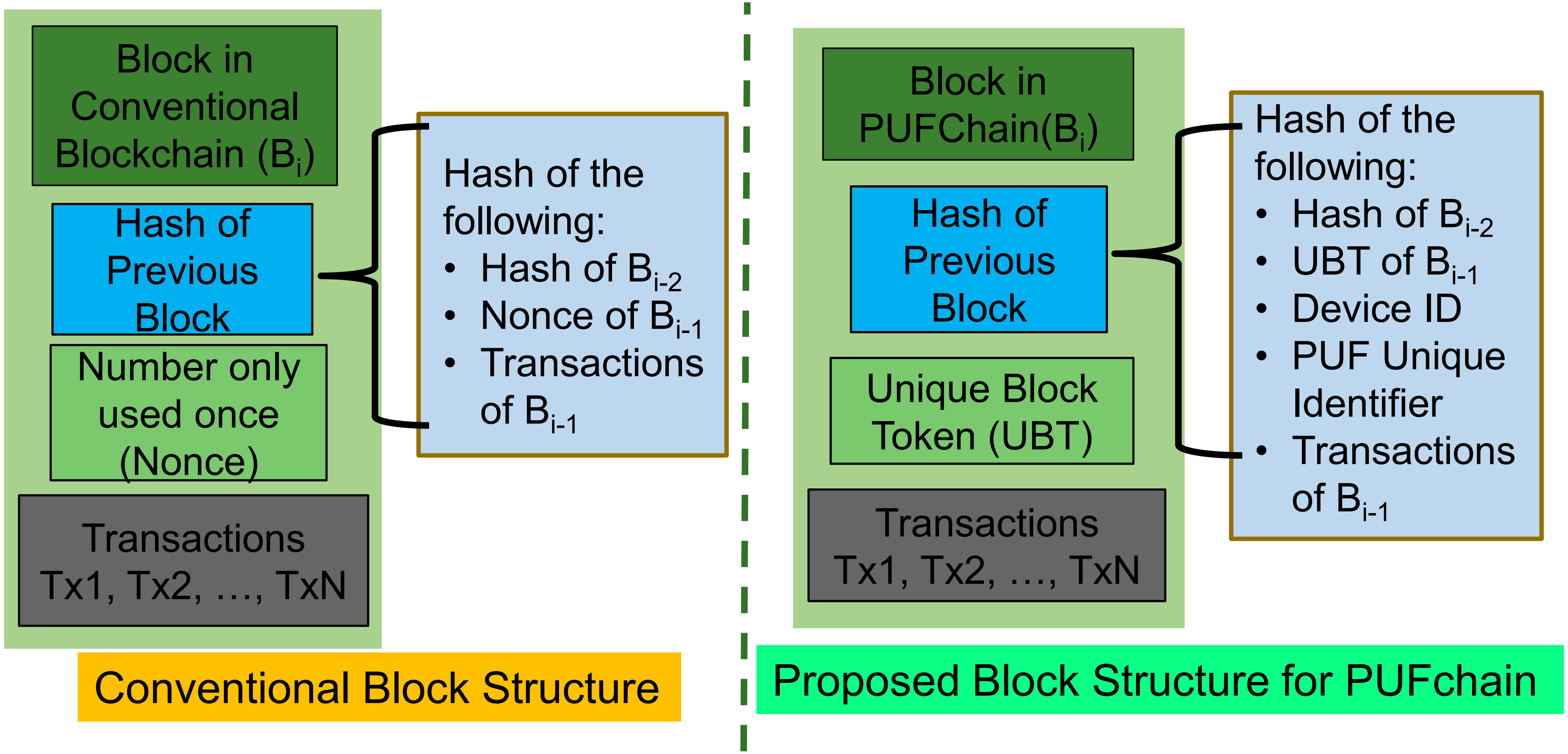
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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

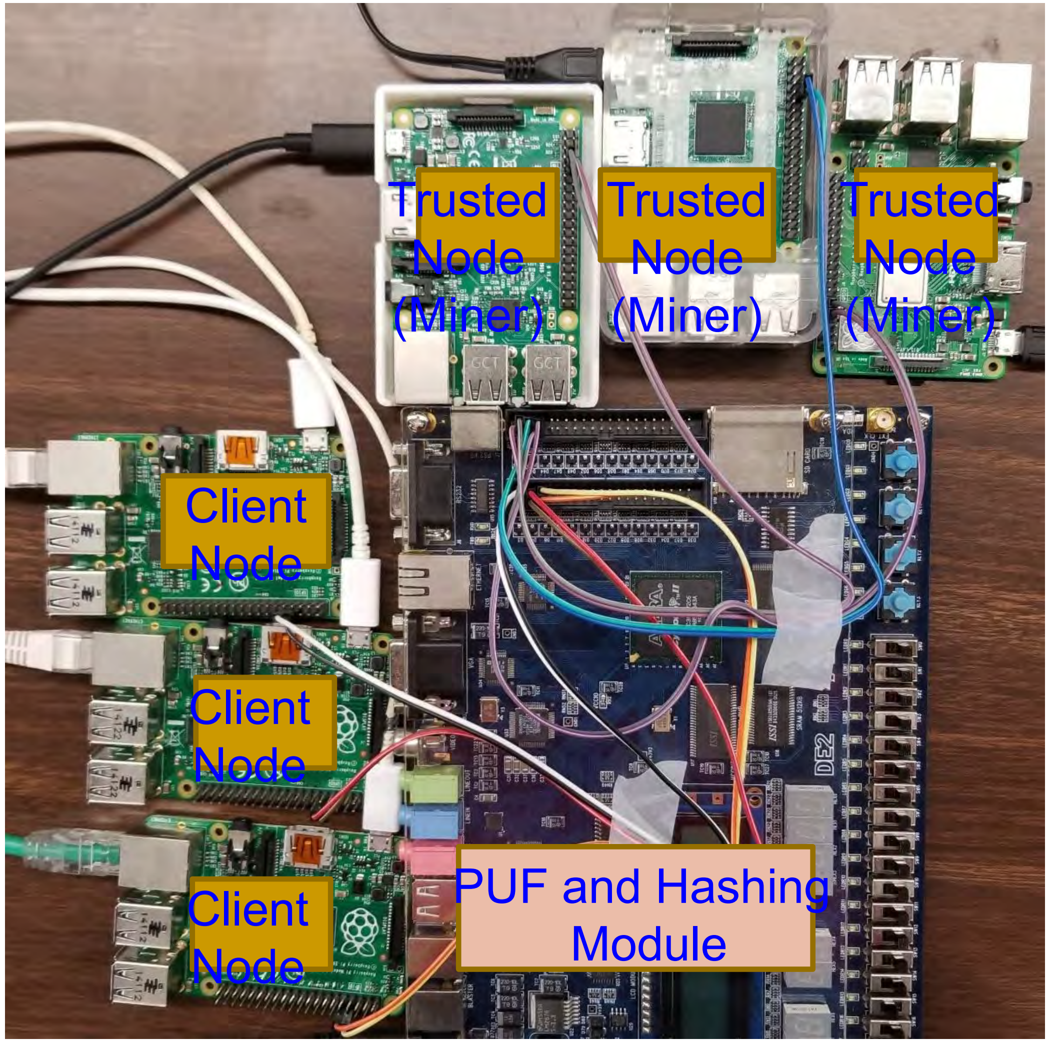



Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

# PUFchain: Proposed New Block Structure



# Our PoP is 1000X Faster than PoW

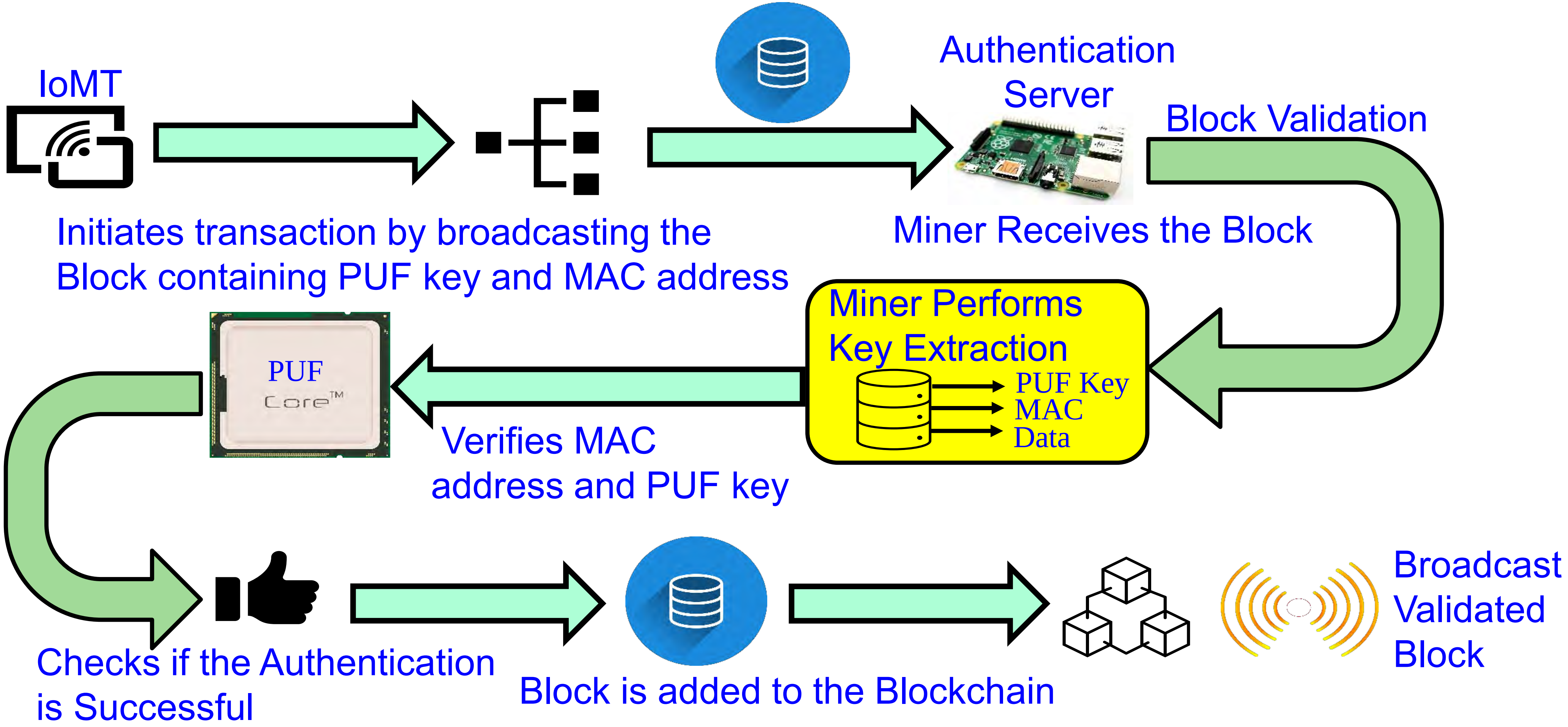



| | | |
|---|---|---|
| PoW - 10 min in cloud | PoAh – 950ms in Raspberry Pi | PoP - 192ms in Raspberry Pi |
| High Power | 3 W Power | 5 W Power |

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

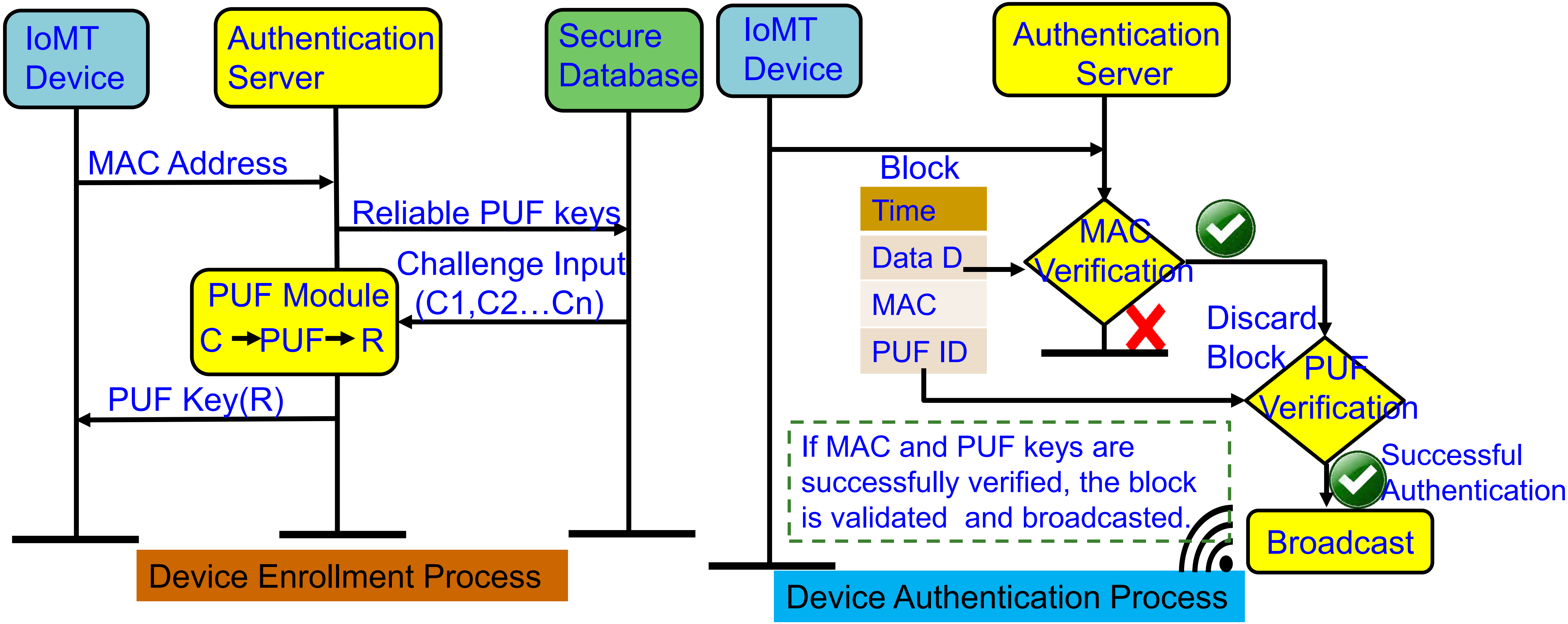
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

# 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 …



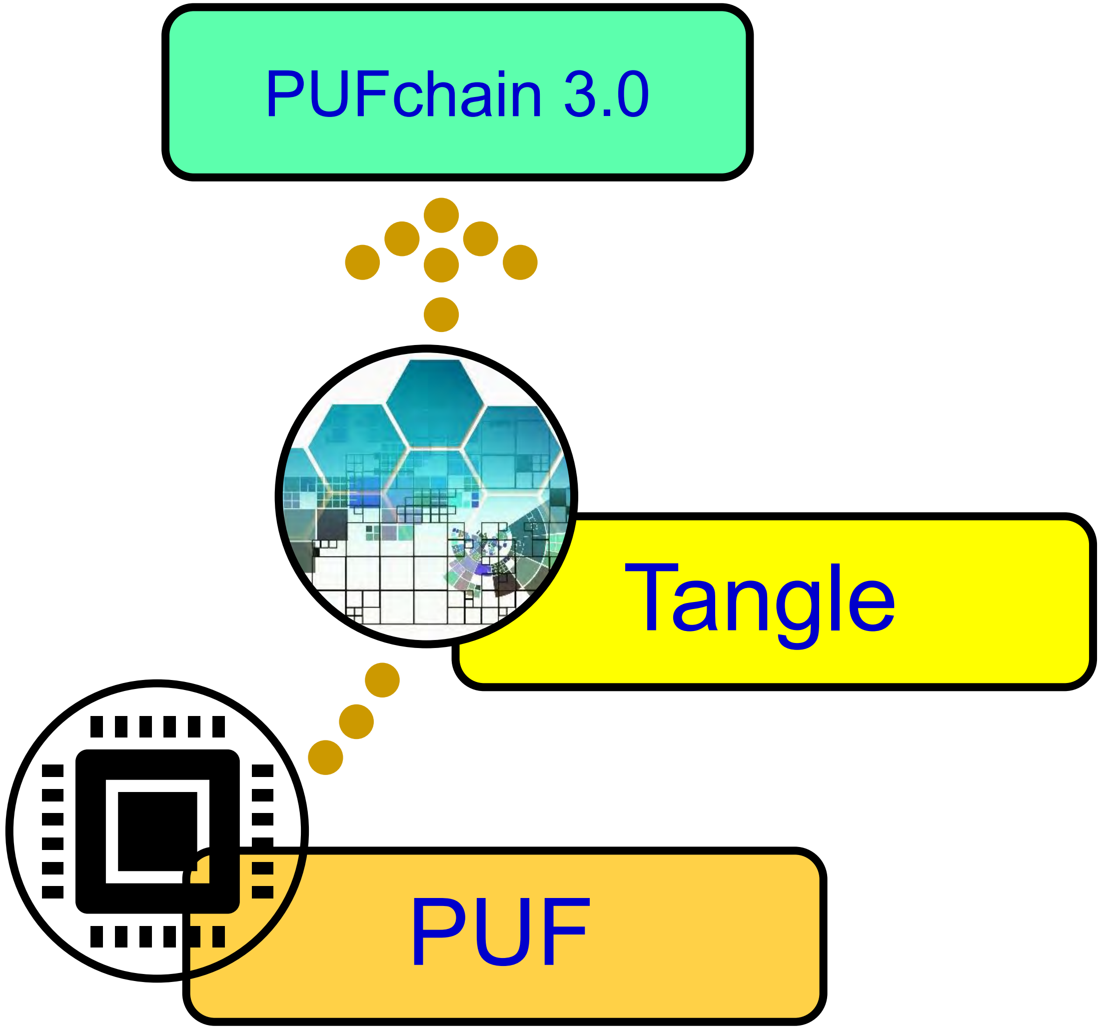

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

# 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.

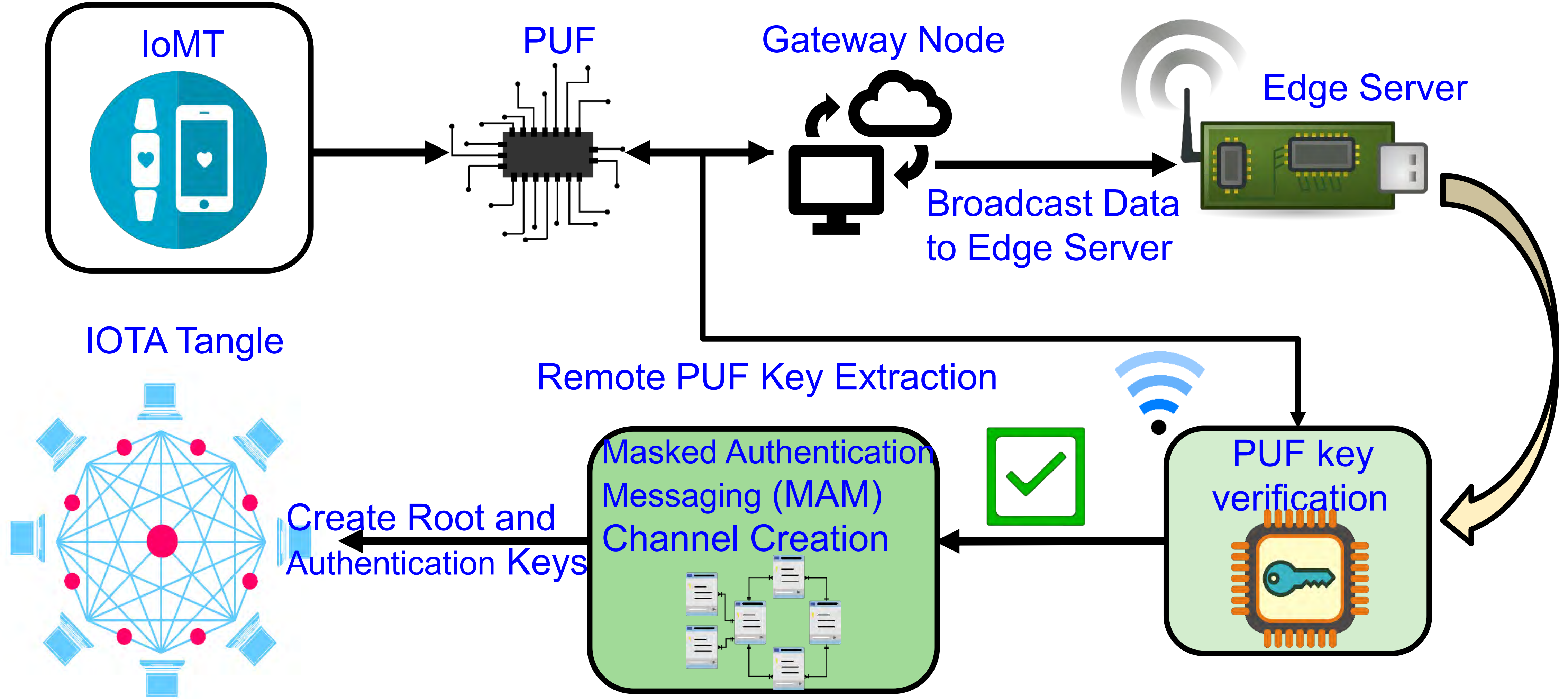
# PUFchain 3.0 - Conceptual Idea




- 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

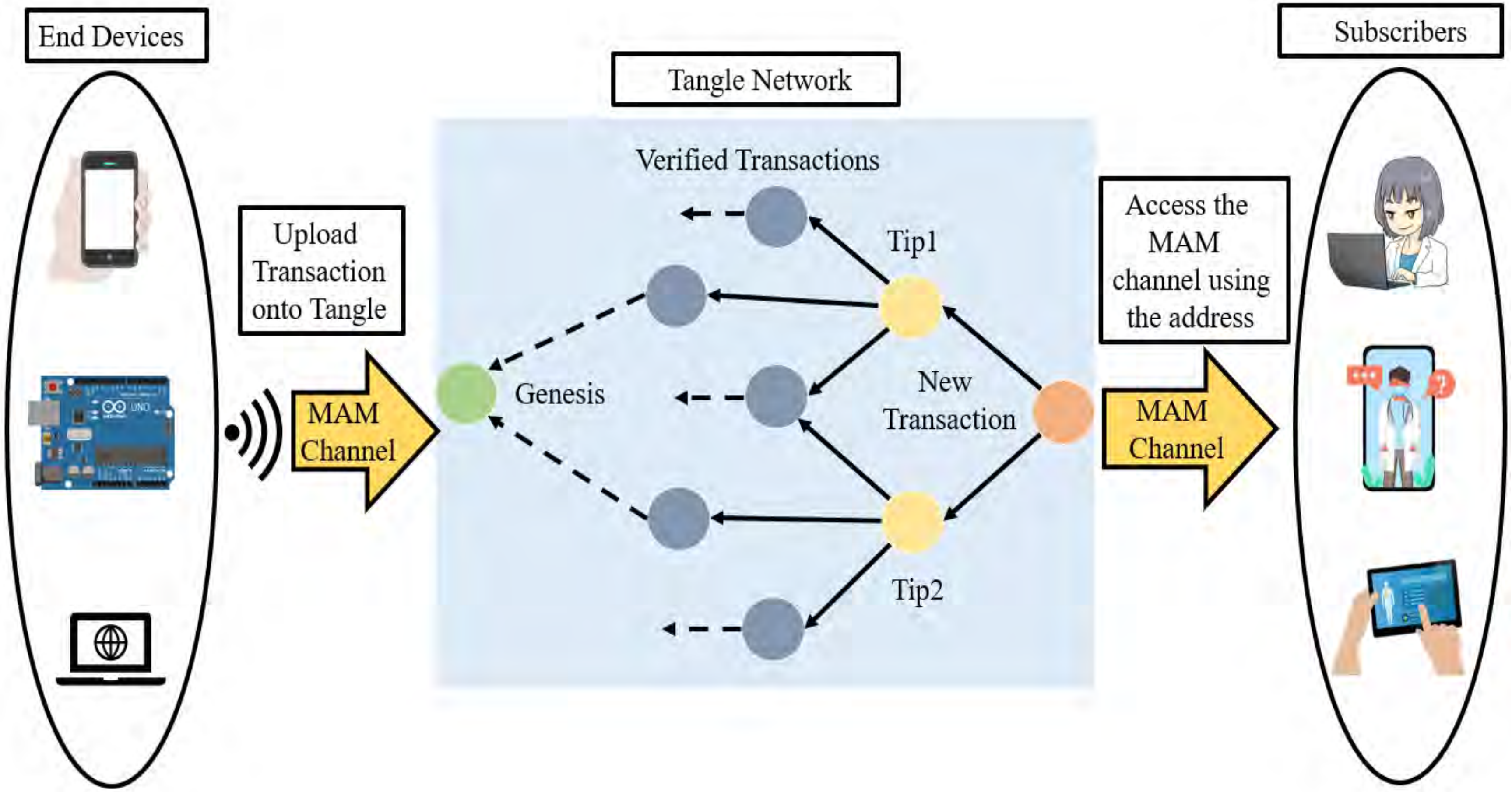
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40, 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



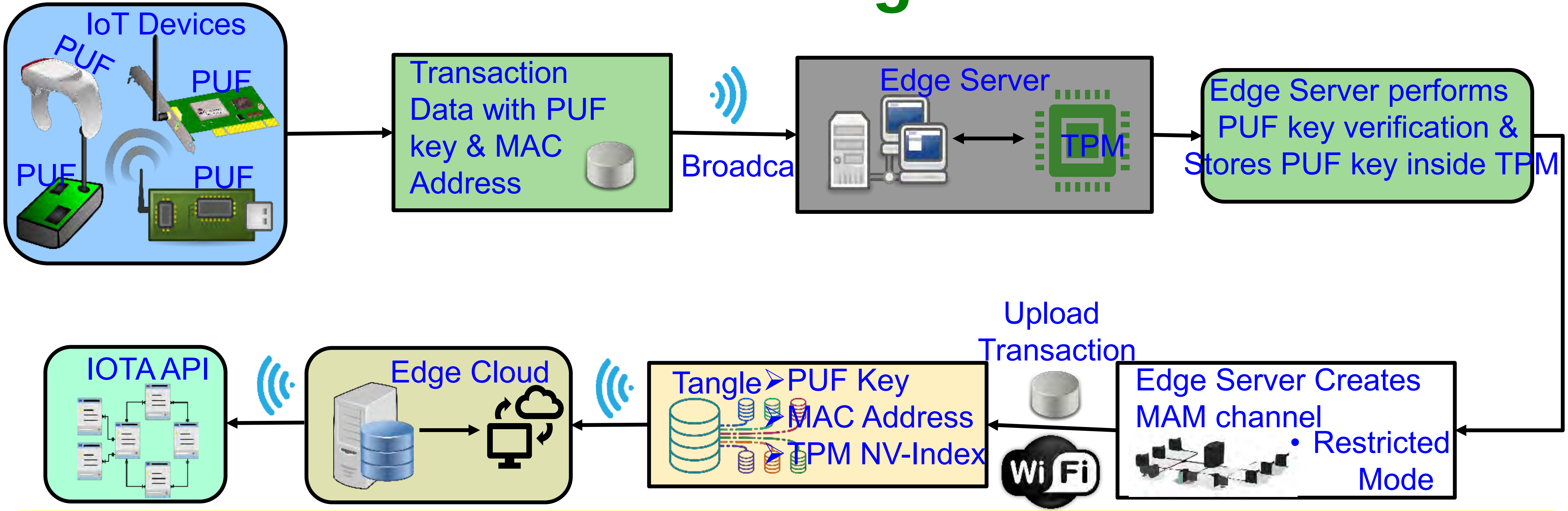

- Provides Device and Data security in IoT
- Works in Three modes: Public, Private and Restricted

# PUFchain 3.0: 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.

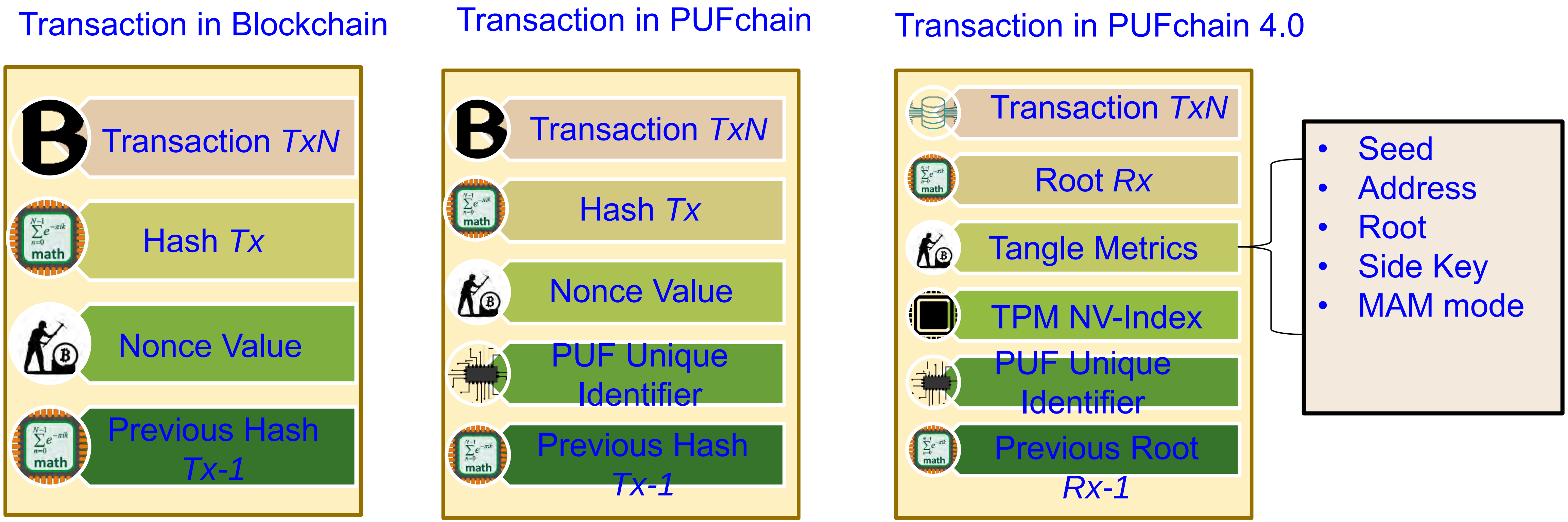
# Our PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for SbD of IoT




- Tangle is a simple fee-less, miner less Distributed Ledger Technology
- In Tangle, Incoming transactions must validate tips (Unverified Transactions) to become part of the Network.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 231--236, DOI: https://doi.org/10.1145/3583781.3590206.

# Our PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for SbD of IoT




Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 231--236, DOI: https://doi.org/10.1145/3583781.3590206.

# Our PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for SbD of IoT

| Research Works | Application | DLT or Blockchain | Authentication Mechanism | Performance Metrics |
|---|---|---|---|---|
| Mohanty et al. 2020 - PUFchain | IoT (Device and Data) | Blockchain | Proof-of-PUF-Enabled Authentication | PUF Design Uniqueness - 47.02%, Reliability-1.25% |
| Chaudhary et al. 2021 - Auto-PUFchain | Hardware 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 % |
| PUFchain 3.0 in 2022 | IoMT (Device) | Tangle | Masked Authentication Messaging | Authentication 2.72 sec, Reliability - 100% (Approx), MAM Mode-Restricted |
| **PUFchain 4.0 (This Paper)** | **IoT( Device & Data)** | **Tangle** | **PUF Based TPM (SbD)** | **PUF Key Generation Time-87 ms, PUF Reliability-99% Power Consumption-2.7-3.3 Watt** |

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 231--236, DOI: https://doi.org/10.1145/3583781.3590206.

# Smart Grid Cybersecurity - Solutions

**Smart Grid – Security Solutions**

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


Smart Meter

**Smart Grid Cybersecurity - Strategies**

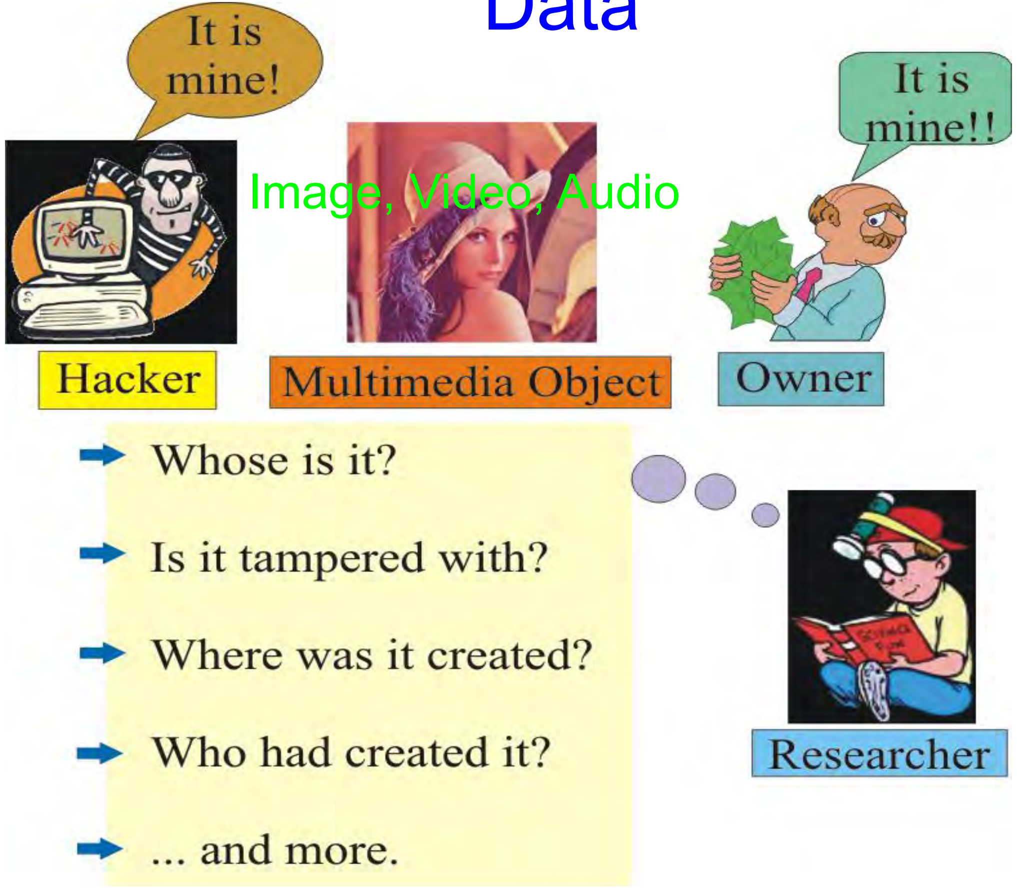
- Make Smart Grids Survivable
- Use Scalable Security Measures
- Integrate Security and Privacy by Design
- Deploy a Defense-in-Depth Approach
- Enhance Traditional Security Measures

Phasor Measurement Unit (PMU)

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

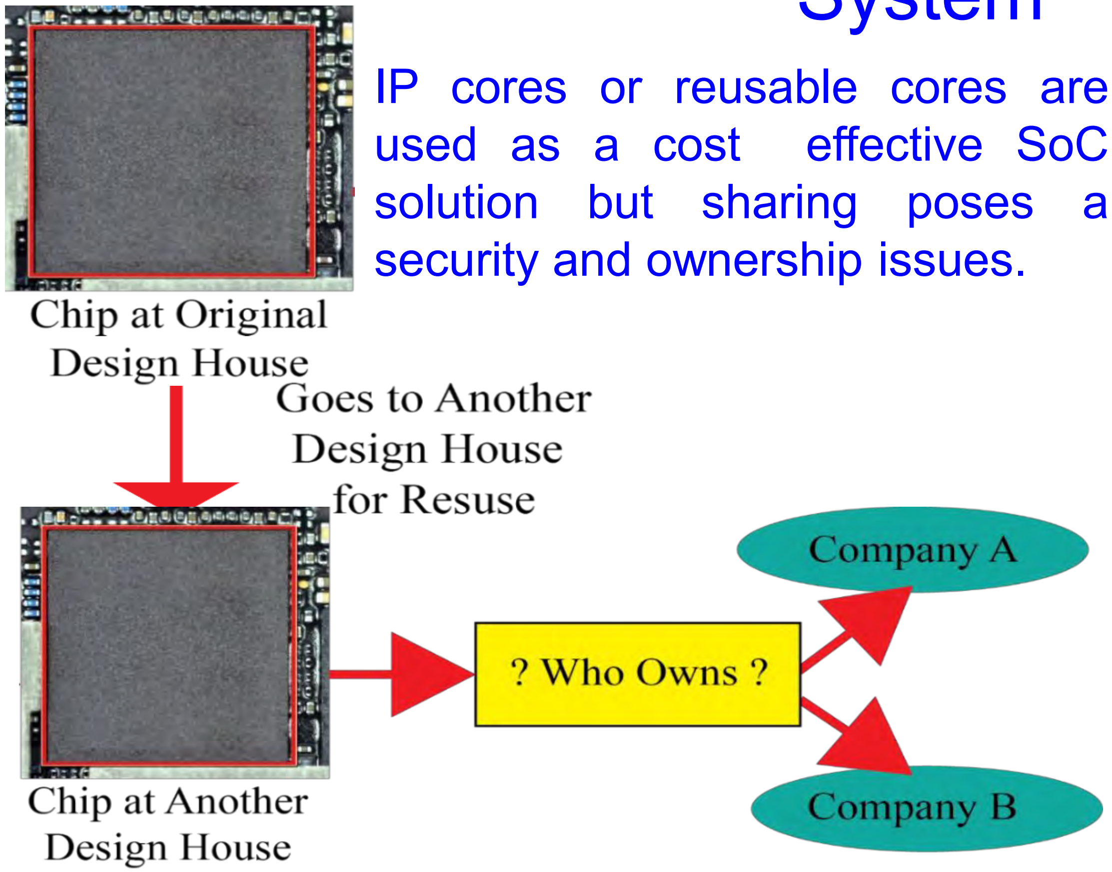
# Data and System Authentication and Ownership Protection – My 20 Years of Experiences

## Data



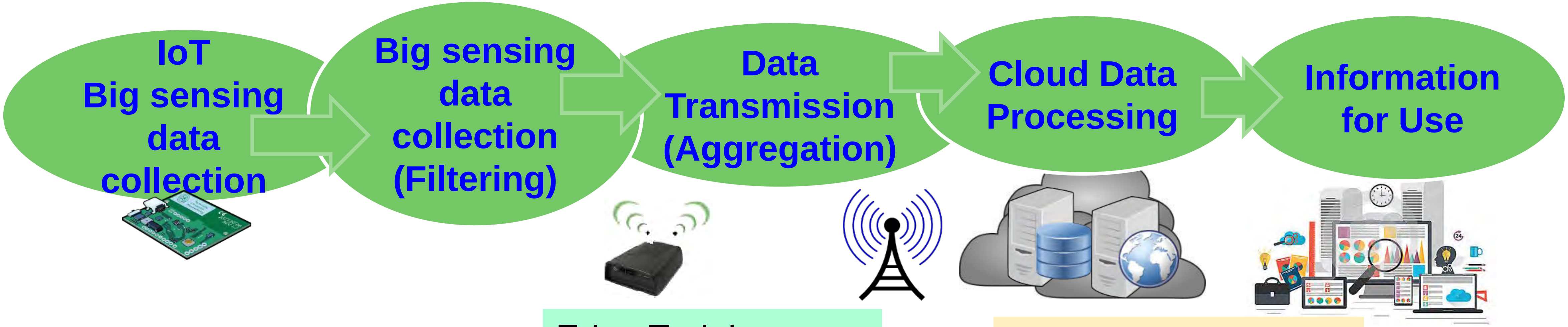

## System

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




Edge Training:
- ➢ Data Signature
- ➢ Model Signature

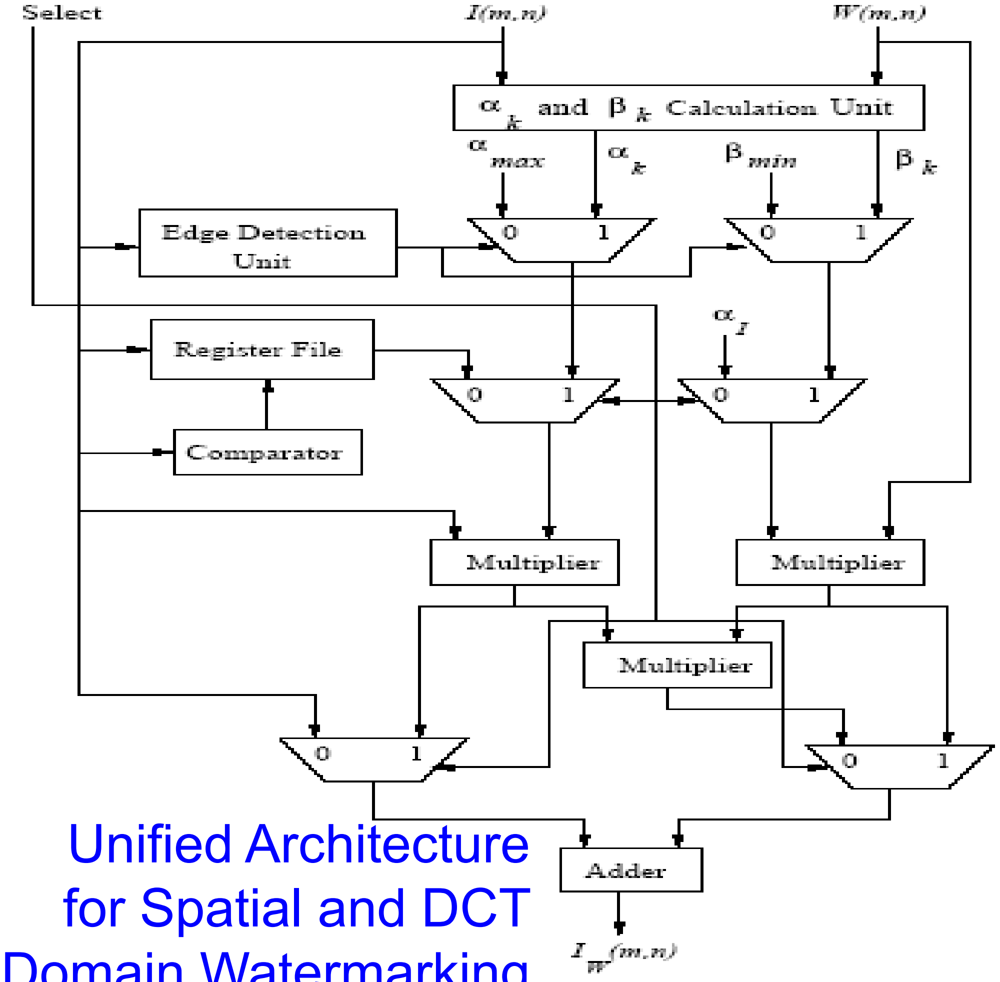
Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

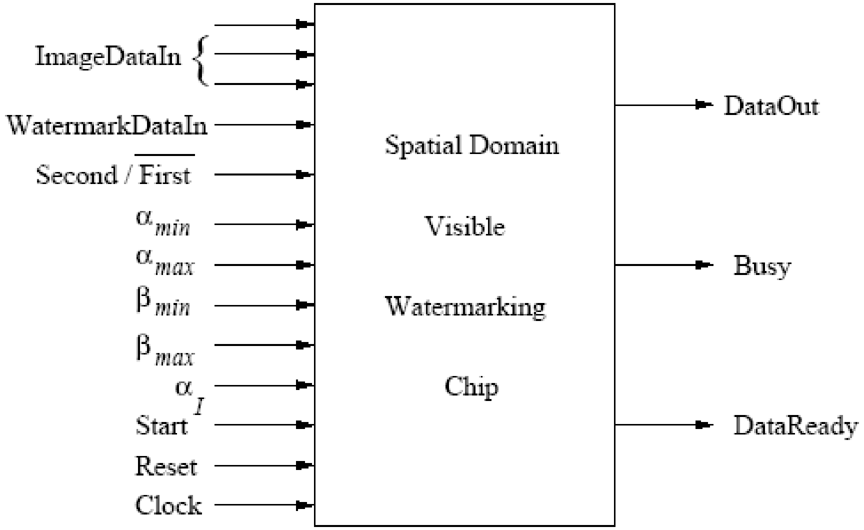
Secure data curation a solution for fake data?

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.

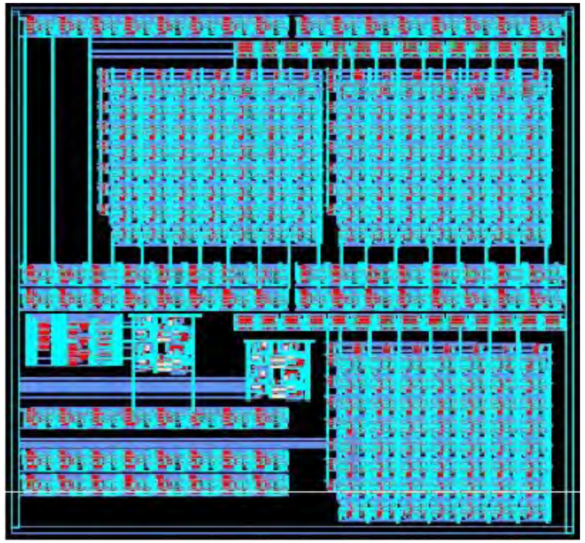
# Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection




Unified Architecture for Spatial and DCT Domain Watermarking




Pin Diagram



Chip Layout

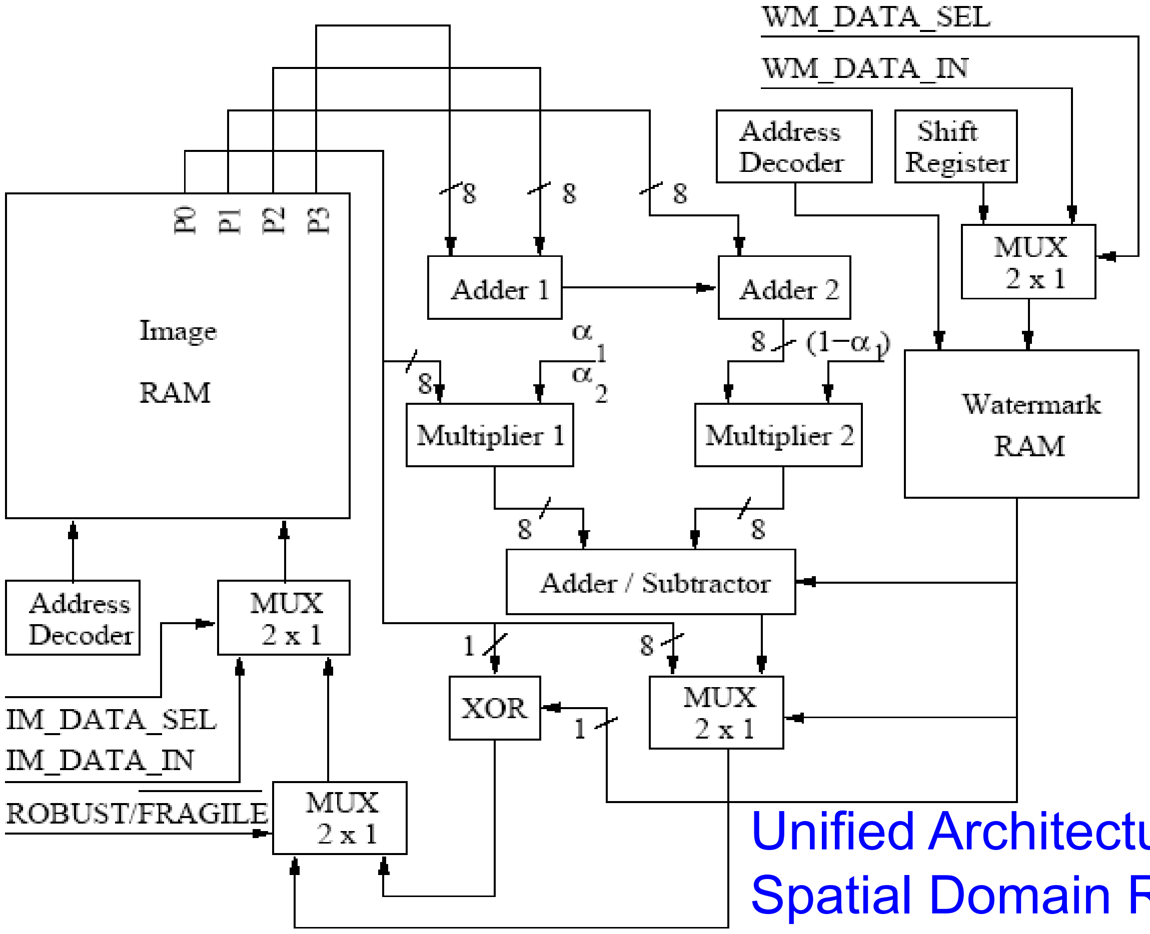
**Chip Design Data**

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

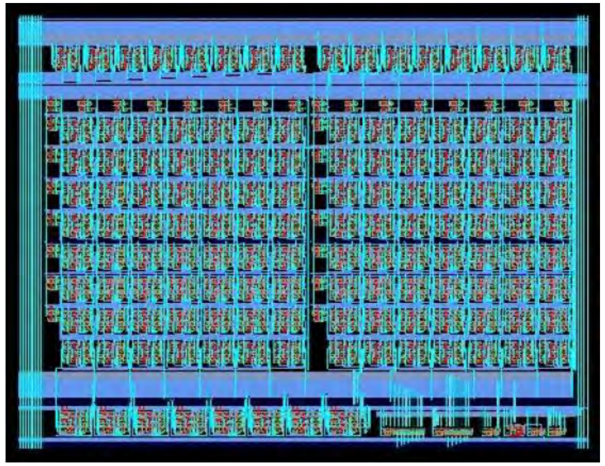
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

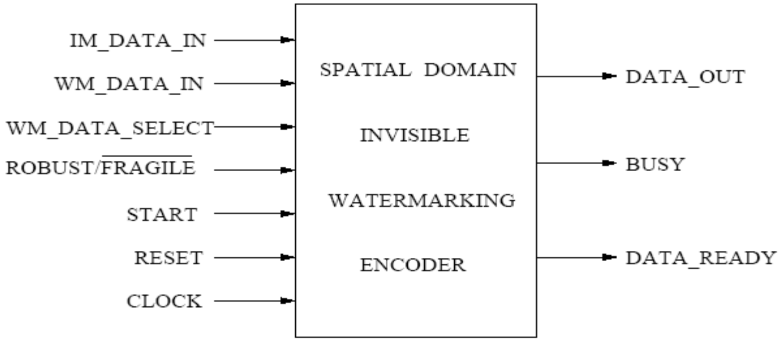
# Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity




Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout




Pin Diagram

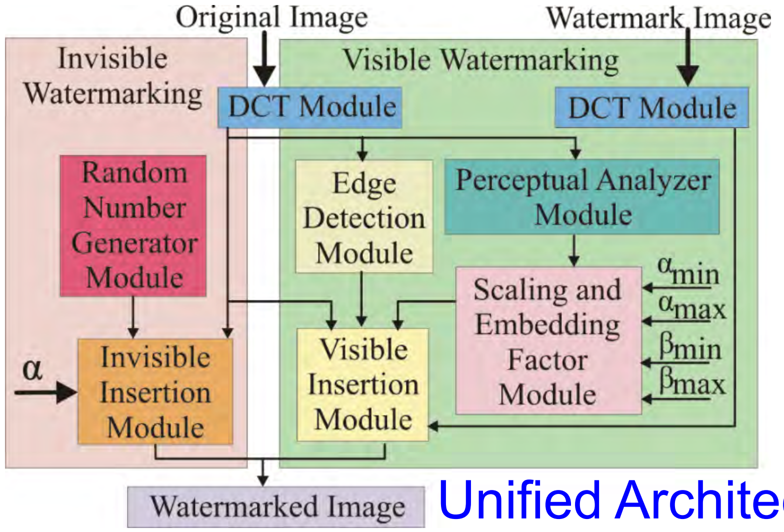
**Chip Design Data**

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

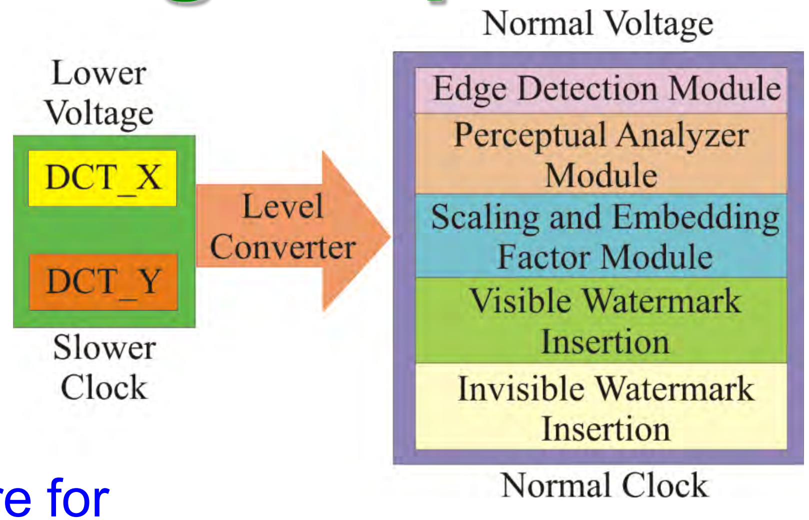
Power Consumption: 2.0 mW, Frequency: 500 MHz

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.

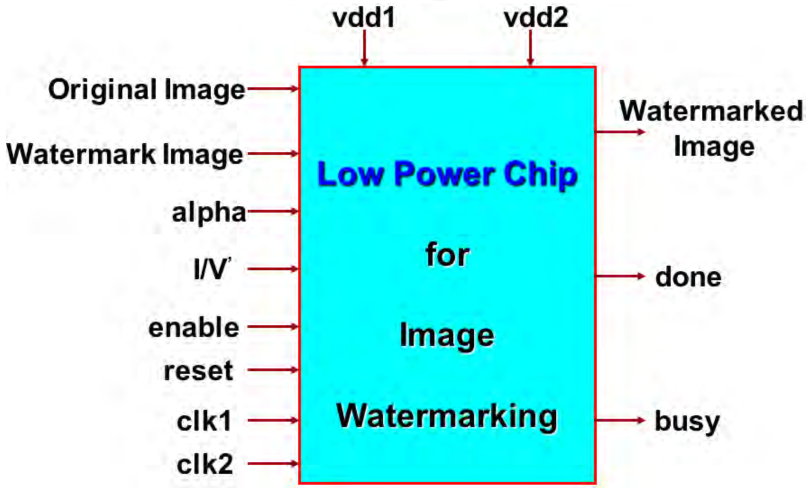
# Our Design: First Ever Low-Power Watermarking Chip for Data Quality



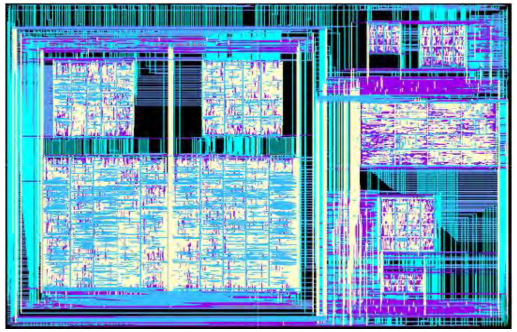

Unified Architecture for DCT Domain Watermarking




DVDF Low-Power Design




Pin Diagram



Chip Layout

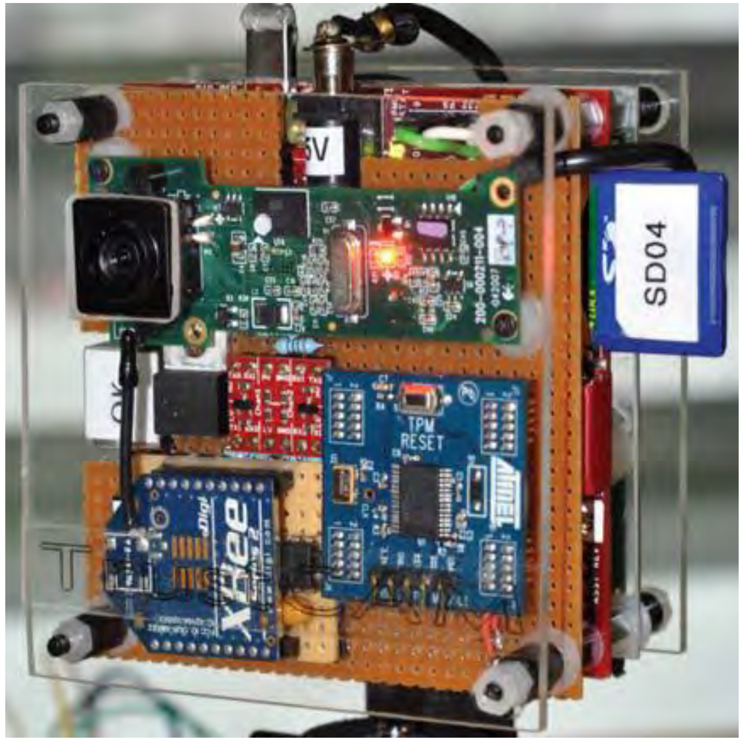
Chip Design Data

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

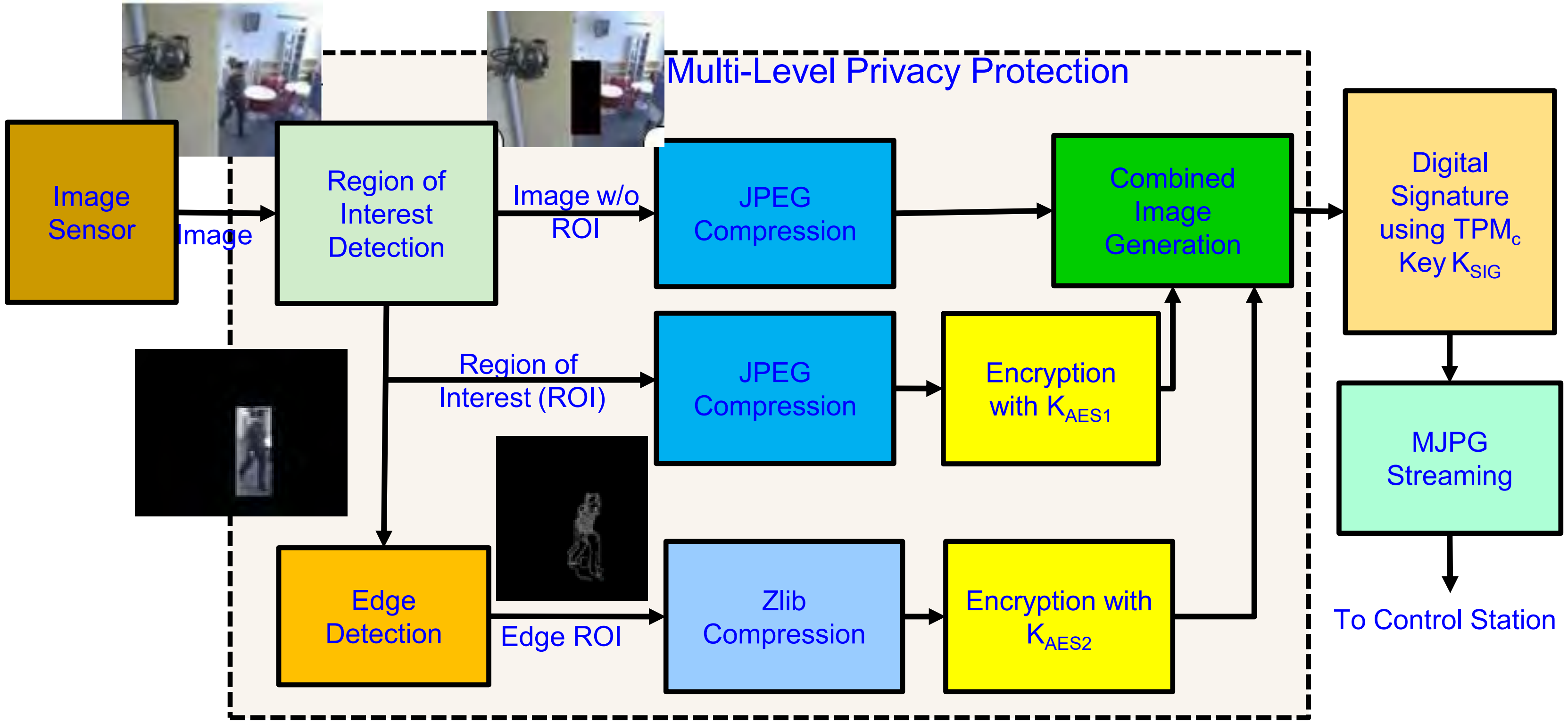
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

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.

# My Watermarking Research Inspired - TrustCAM



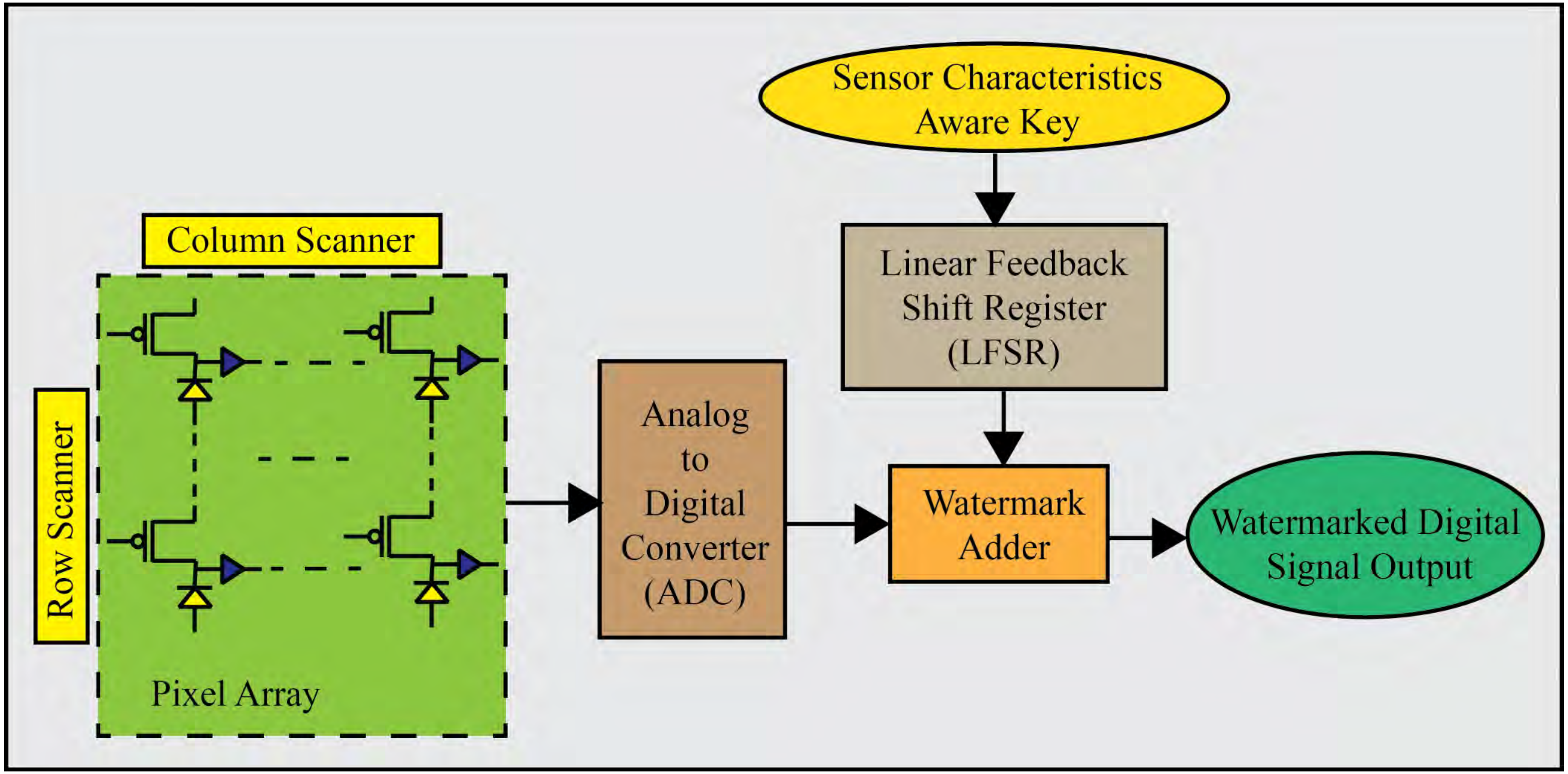

Source: https://pervasive.aau.at/BR/pubs/2010/Winkler_AVSS2010.pdf




For integrity protection, authenticity and confidentiality of image data.

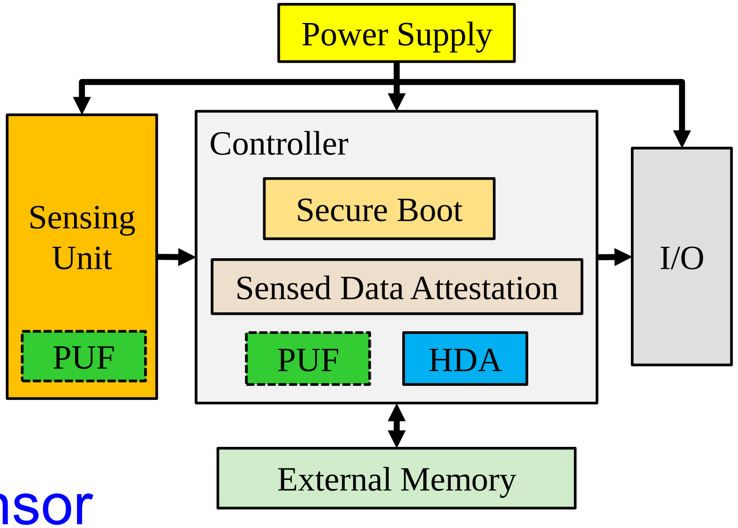
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

# My Watermarking Research Inspired – Secured Sensor

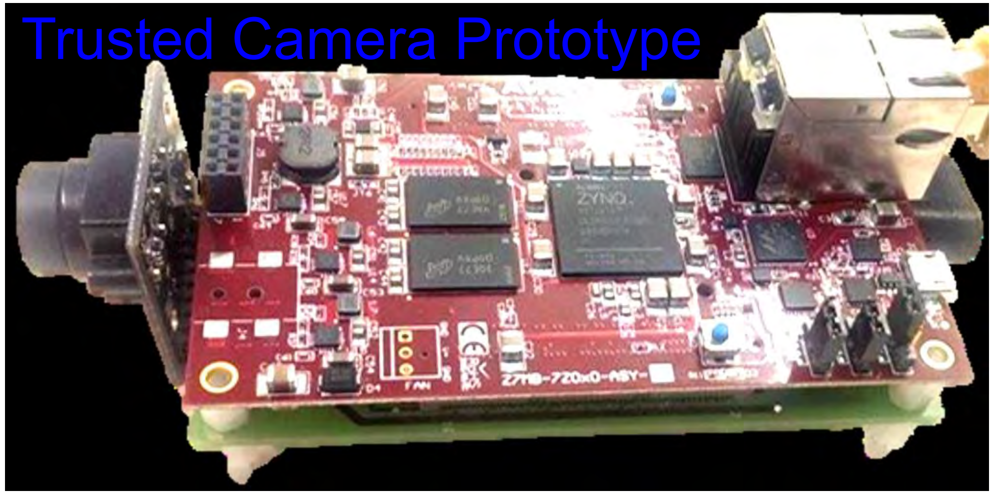



Source: G. R. Nelson, G. A. Jullien, O. Yadid-Pecht, "CMOS Image Sensor With Watermarking Capabilities", in *Proc. IEEE International Symposium on Circuits and Systems* (*ISCAS*), 2005, pp. 5326–5329.

# 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:

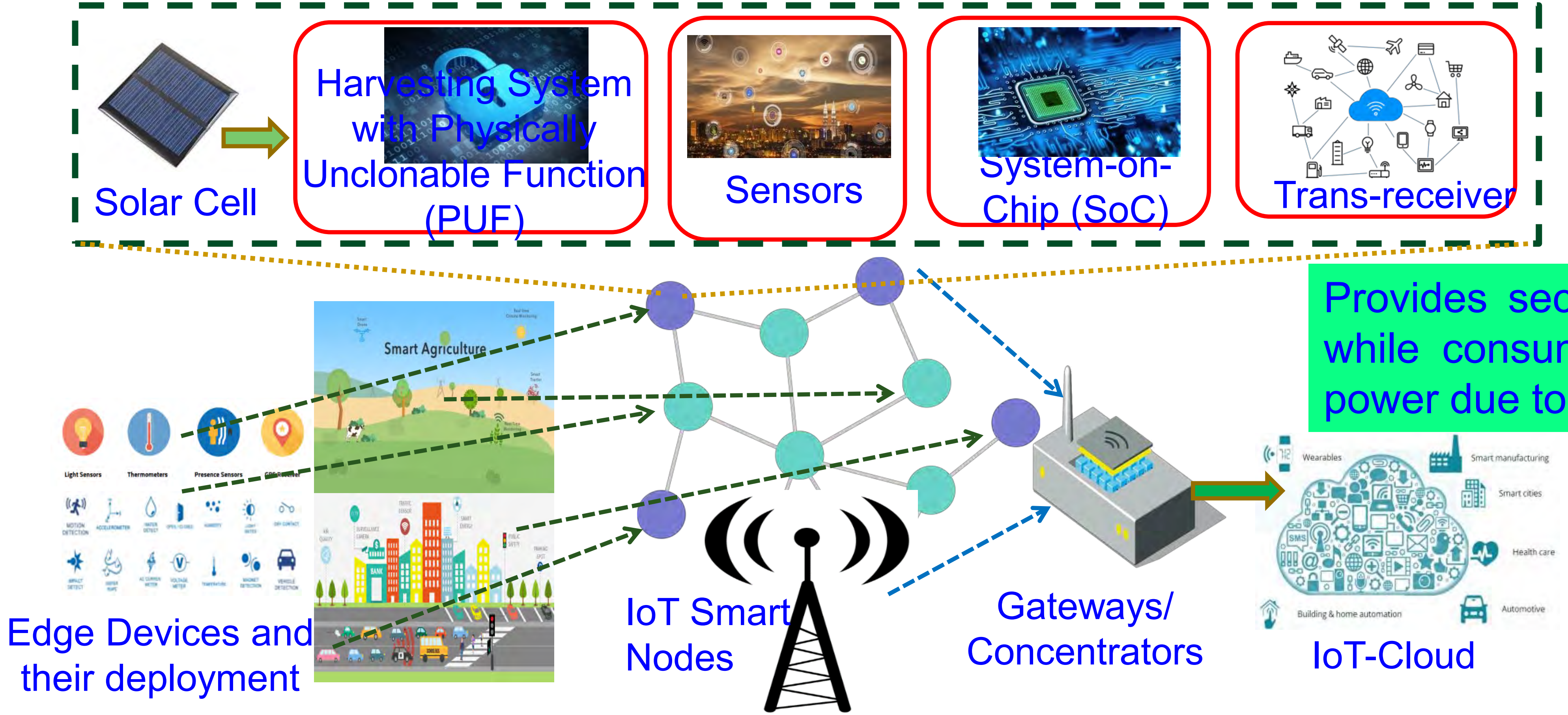
- Sensed data attestation to ensure integrity and authenticity.
- Secure boot of sensor controller to ensure integrity of the platform at booting.

❖ 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

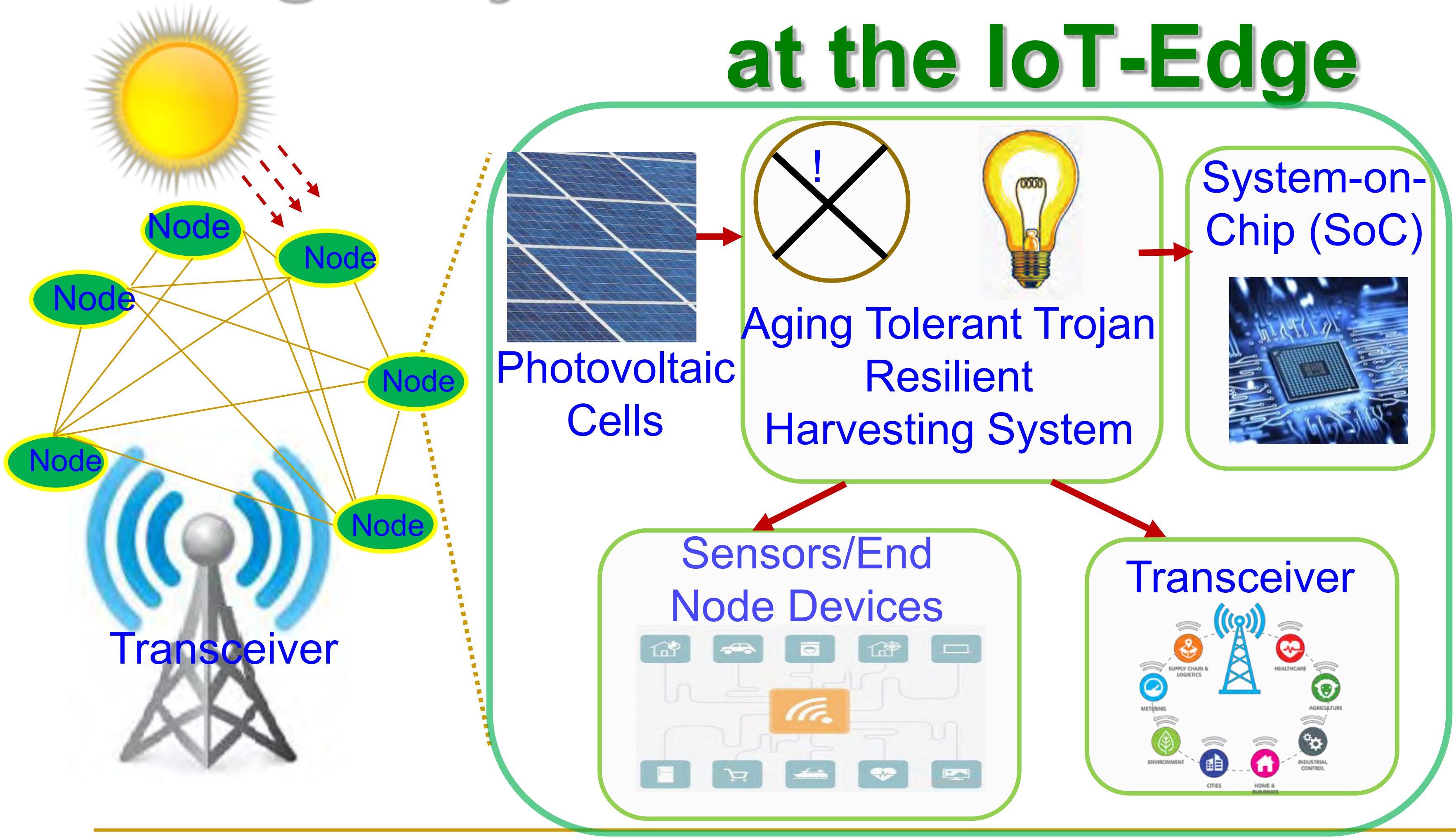
# Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge




Provides security using PUFs 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: 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.

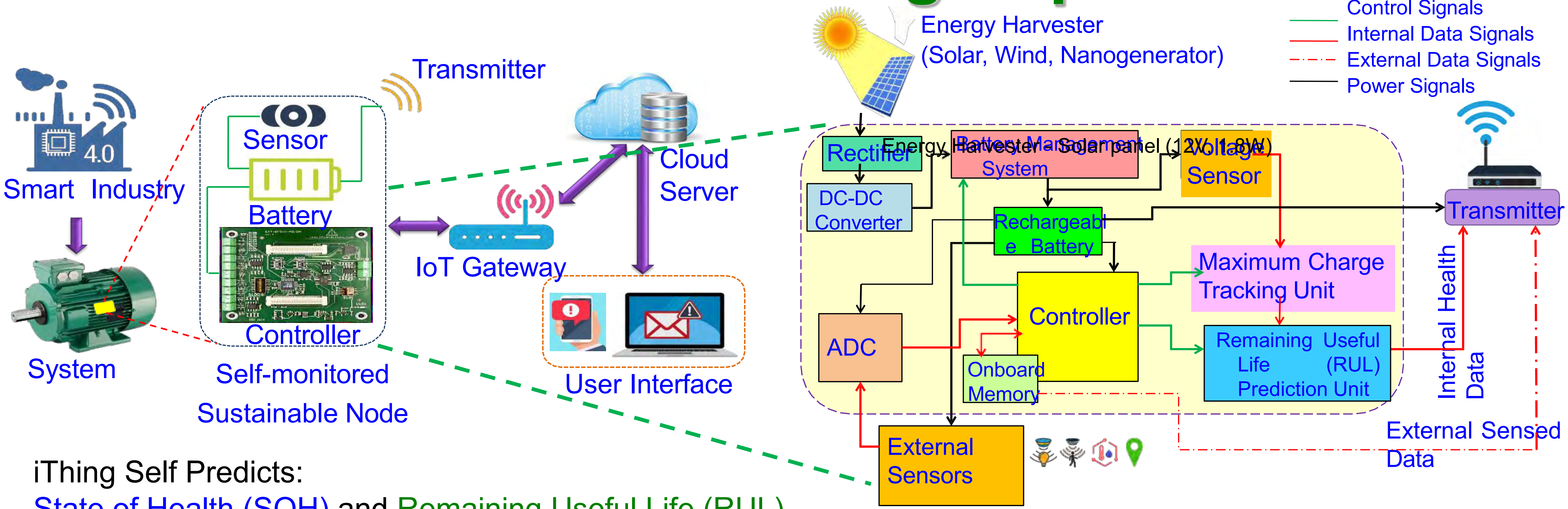
# Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge




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.

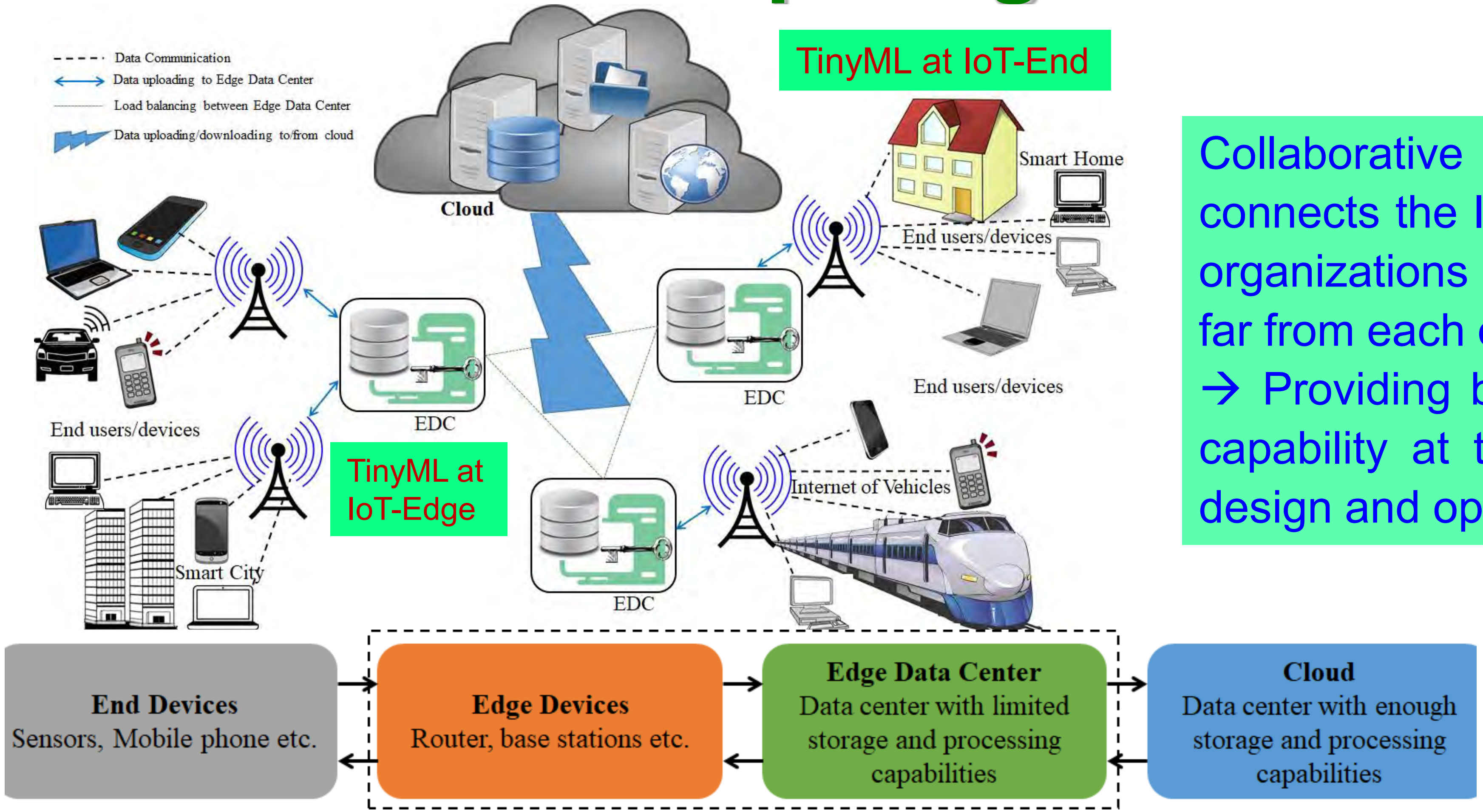
# iThing: Next-Generation Things with Battery Health Self-Monitoring Capabilities




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.

# Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages

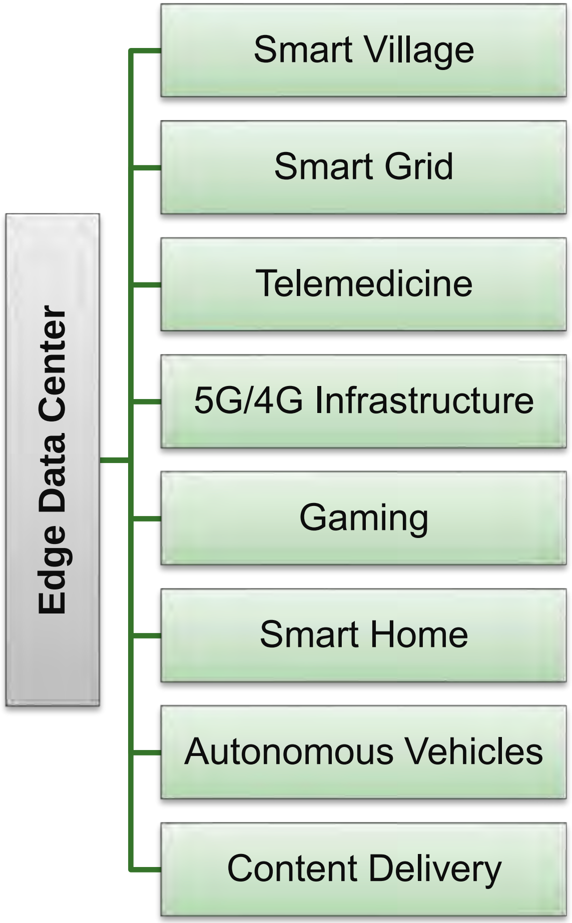



Collaborative edge computing connects the IoT-edges of multiple organizations that can be near or far from each other
→ Providing bigger computational capability at the edge with lower design and operation cost.

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.

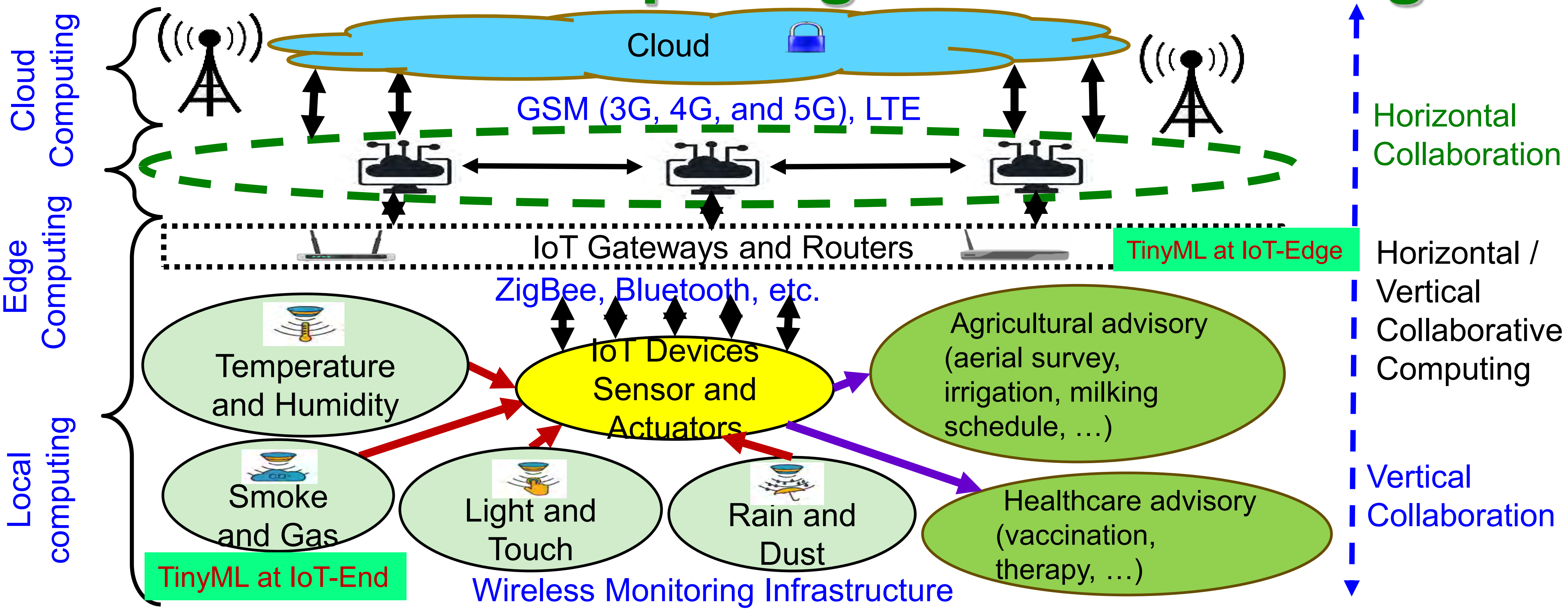
# Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages

- Collaborative Edge Computing is a distributed processing environment
- CEC is a collaboration of distributed edge
- Smart control of heterogenous network
- Reduced Bandwidth and Transmission costs
- CEC enables seamless processing through load balancing



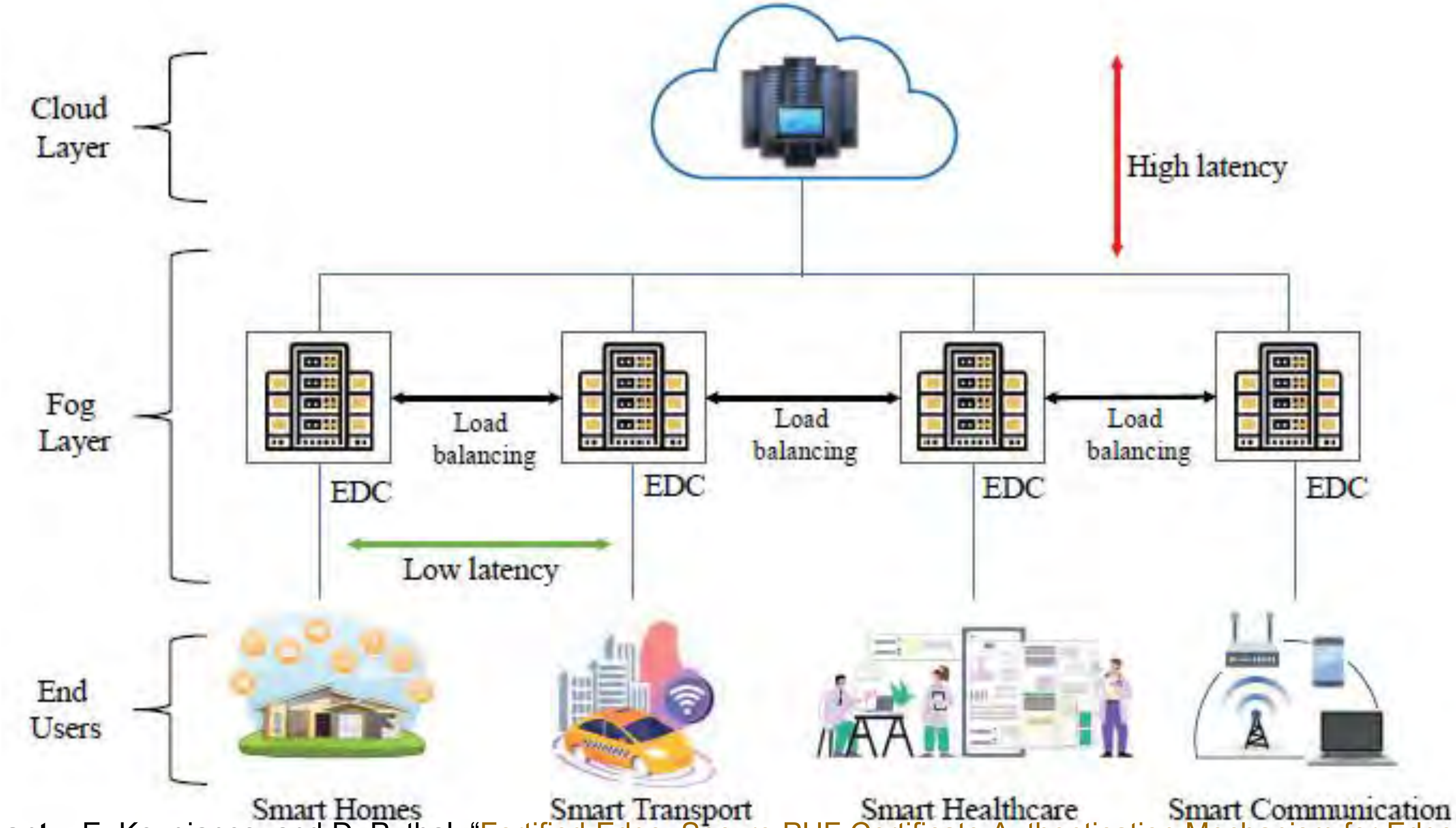

Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

# Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



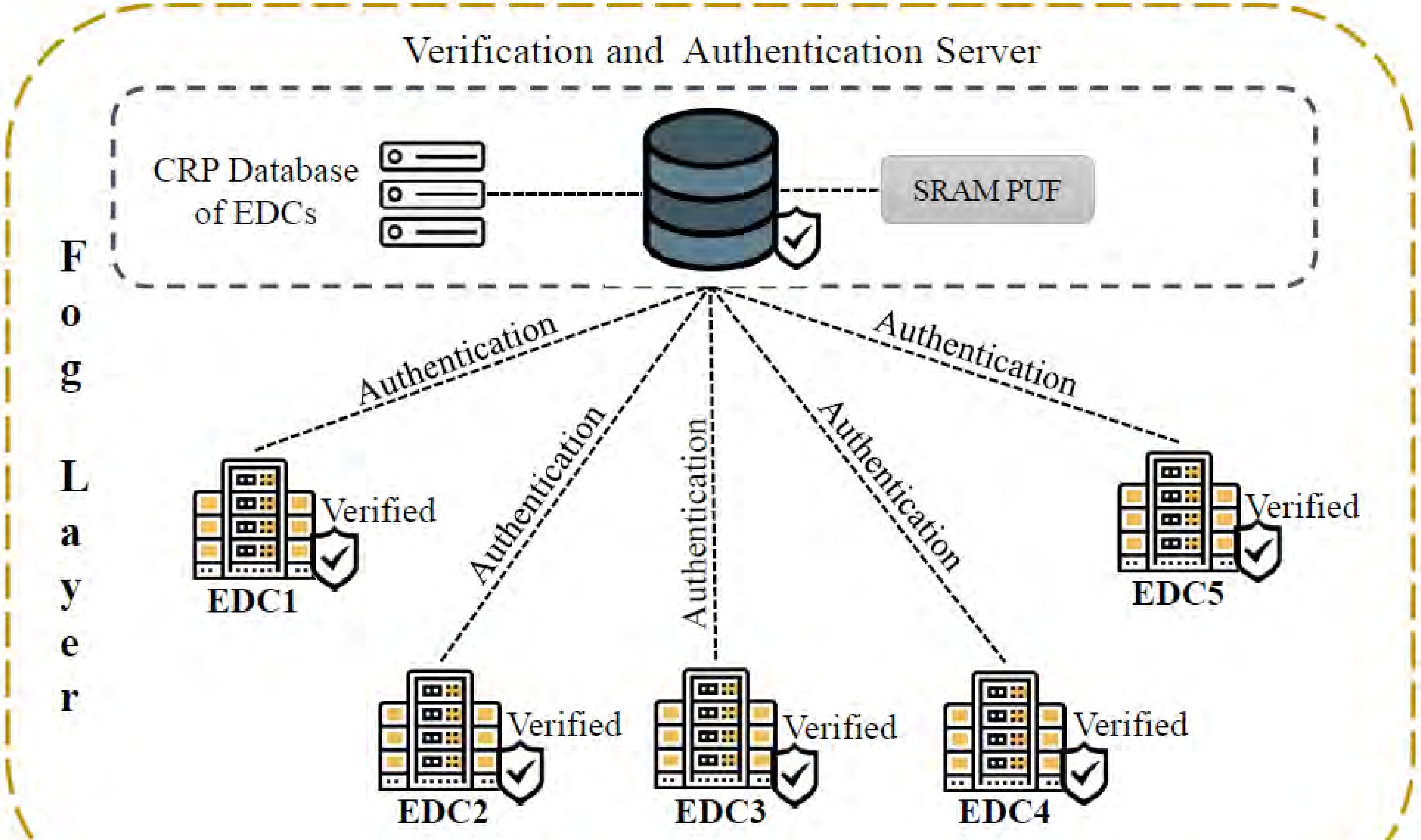

Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, "Collaborative Edge Computing for Smart Villages", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

# Our Fortified-Edge: PUF based Authentication in Collaborative Edge Computing



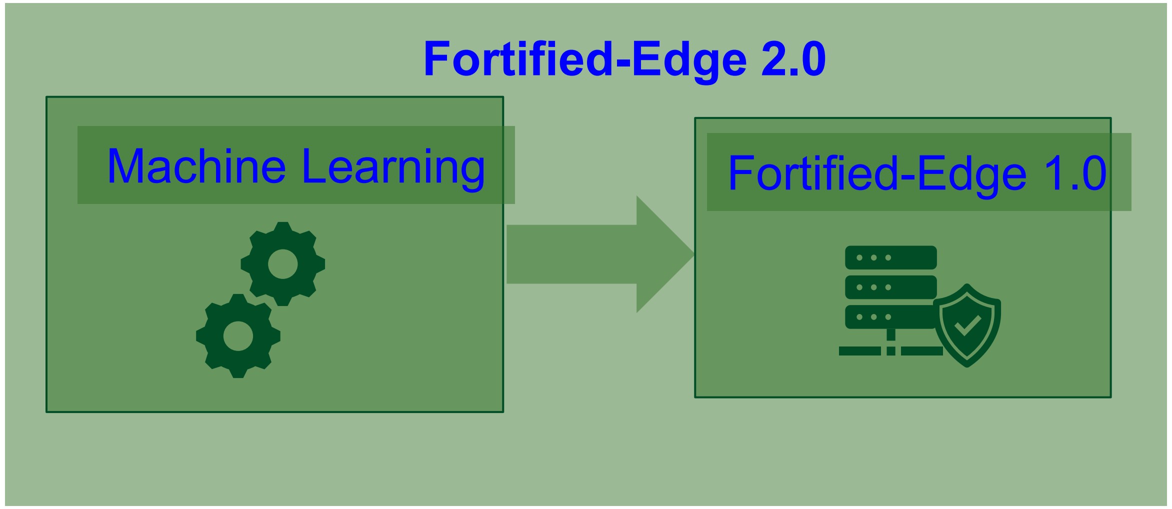

Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 249--254, DOI: https://doi.org/10.1145/3583781.3590249.

# Our Fortified-Edge: PUF based Authentication in Collaborative Edge Computing




Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 249--254, DOI: https://doi.org/10.1145/3583781.3590249.

# Our Fortified-Edge 2.0: ML based Monitoring and Authentication of PUF-Integrated Secure EDC

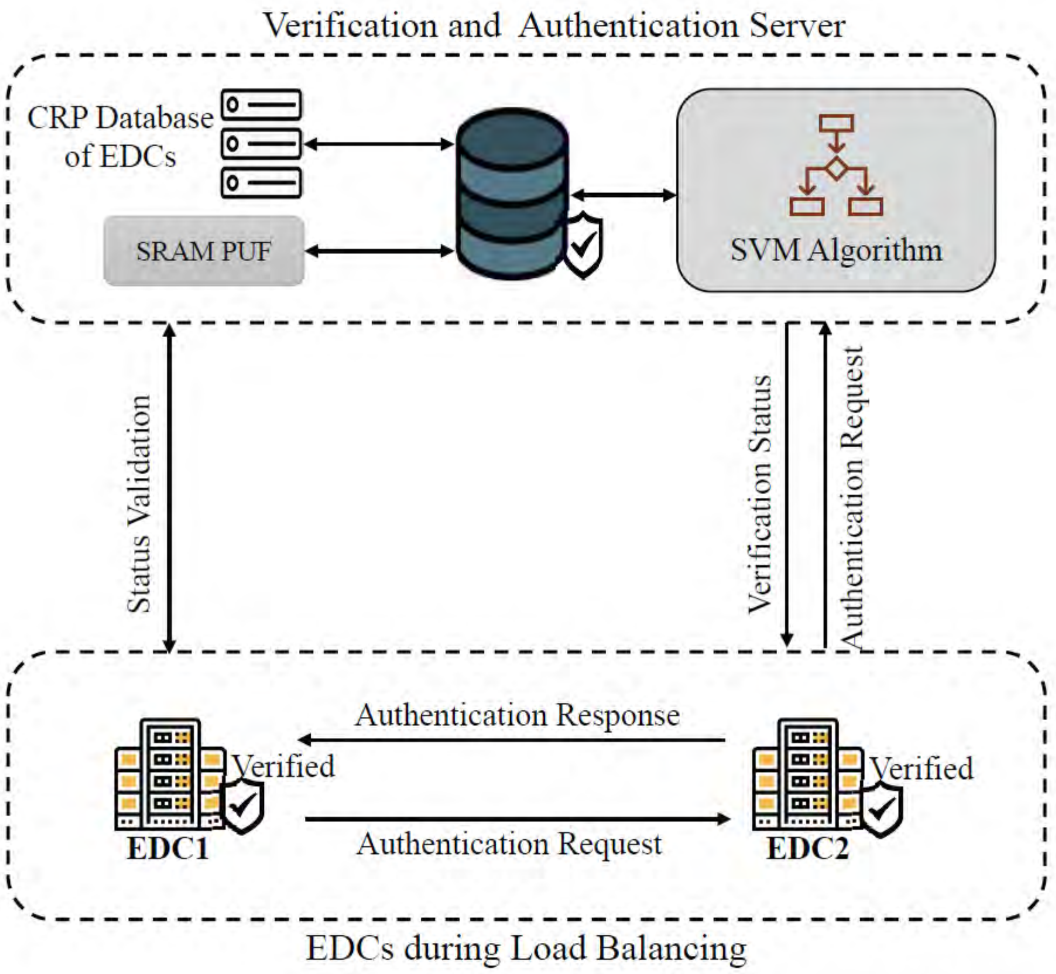



Features

- Secure, Low Latency Authentication
- Device identification
- Intrusion detection
- Attack Prevention
- EDC Monitoring
- Resilient against malicious Requests
- ML model suitable for a smaller dataset

Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

# Our Fortified-Edge 2.0: ML based Monitoring and Authentication of PUF-Integrated Secure EDC




Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

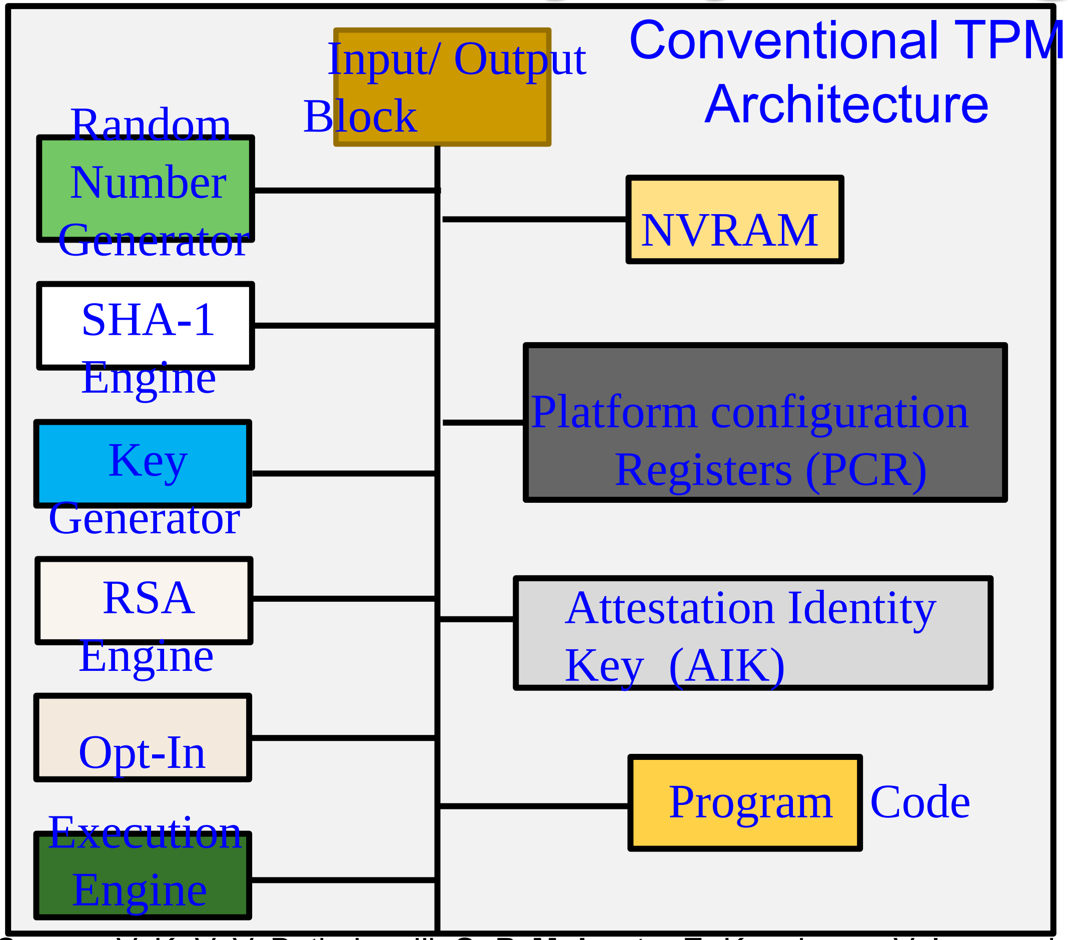
# Our Fortified-Edge 2.0: ML based Monitoring and Authentication of PUF-Integrated Secure EDC

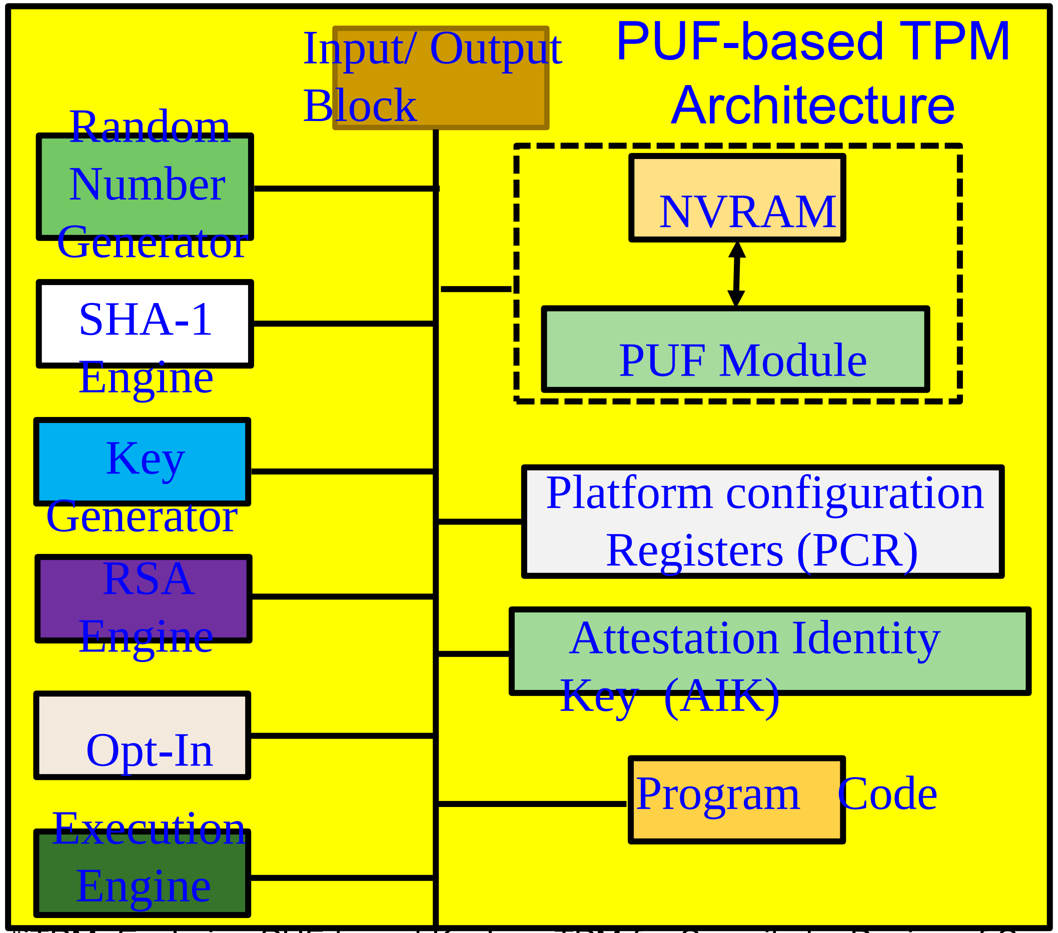
- Mutual authentication of EDCs without cloud dependency
- Reducing the latency by edge-based authentication
- PUF CRP for lightweight and secure authentication
- CA-based verification and authentication for faster and more secure process
- No storage space complexity

- No cloud dependency
- ML for attack detection, intrusion detection, malicious request detection
- ML model suitable for processing at edge
- Improved security over Fortified-Edge 1.0

Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

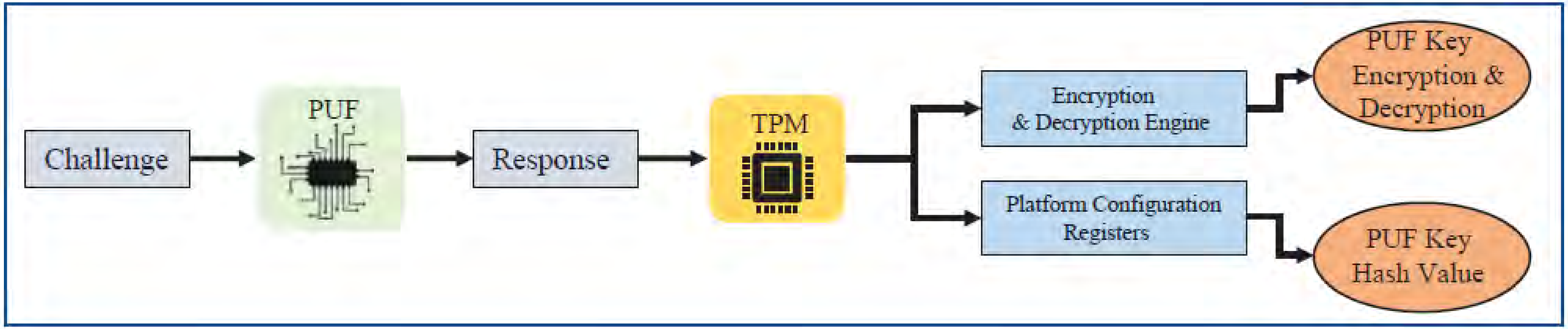
# Our iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics




Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

# Our iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics




- The proposed SbD primitive works by performing secure verification of the PUF key using TPM's Encryption and Decryption engine. The securely verified PUF Key is then bound to TPM using Platform Configuration Registers (PCR).
- By binding PUF with PCR in TPM, a novel PUF-based access control. The policy can be defined, as bringing in a new security ecosystem for the emerging Internet-of-Everything era.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

# Physical Unclonable Function (PUF) - Challenges and Research

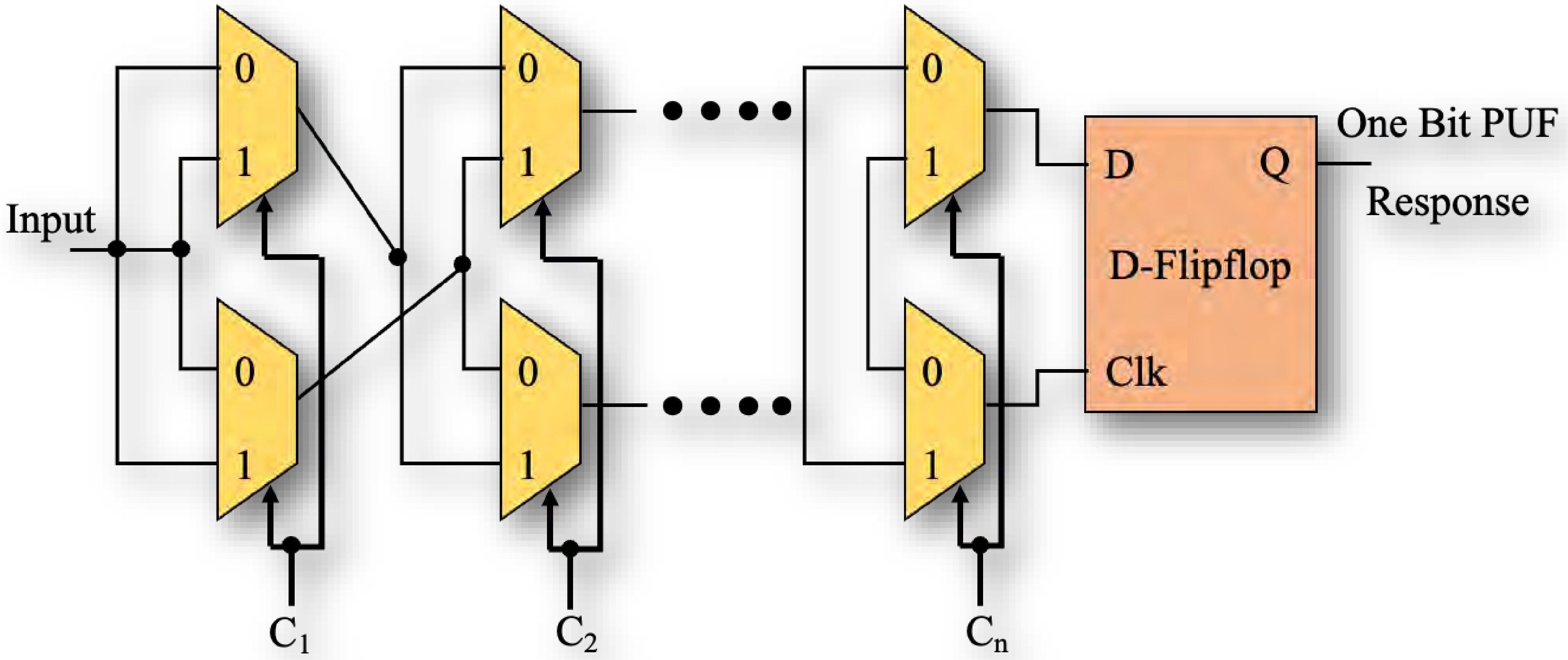
# If PUF is So Great, Why Isn't Everyone Using It?

- 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

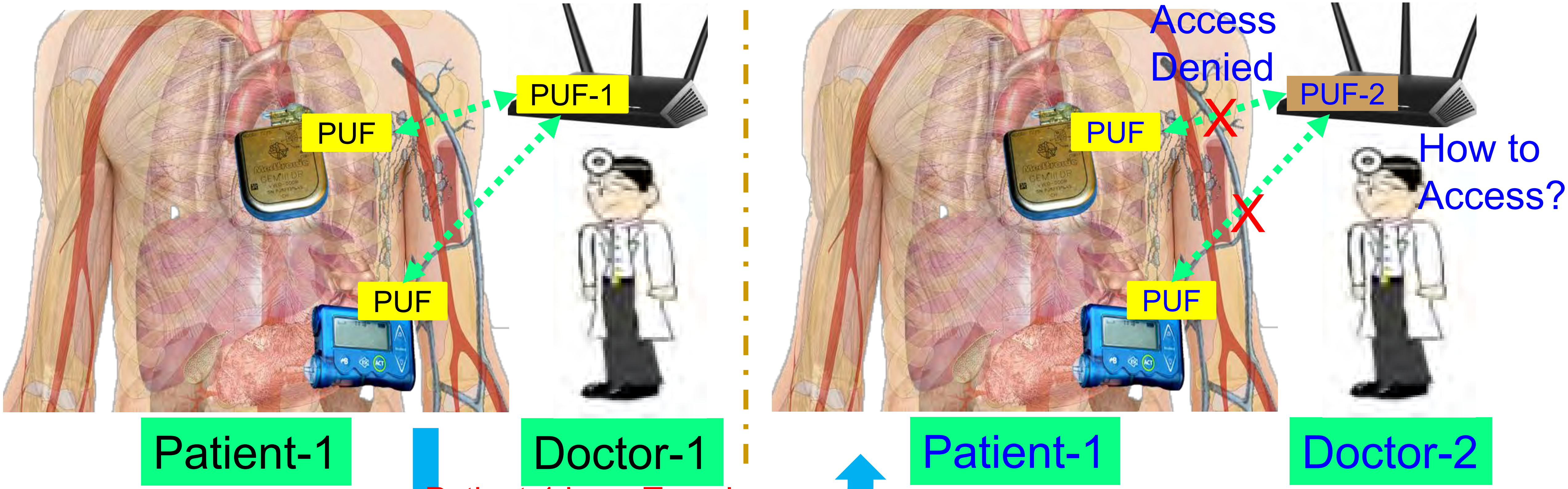
# PUF Limitations – Larger Key Needs Large ICs

- Larger key requires larger chip circuit.




1 – Bit Arbiter PUF Architecture

# PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma

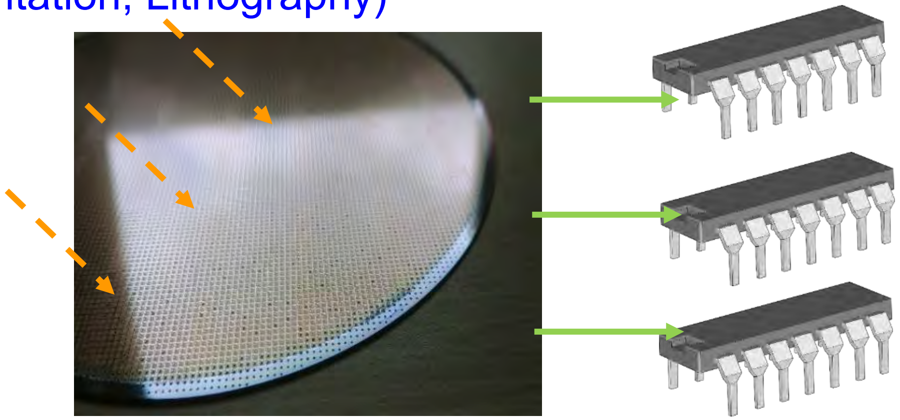



Patient-1 is on Travel
He/She has a Medical Emergency
He/She visits Doctor-2

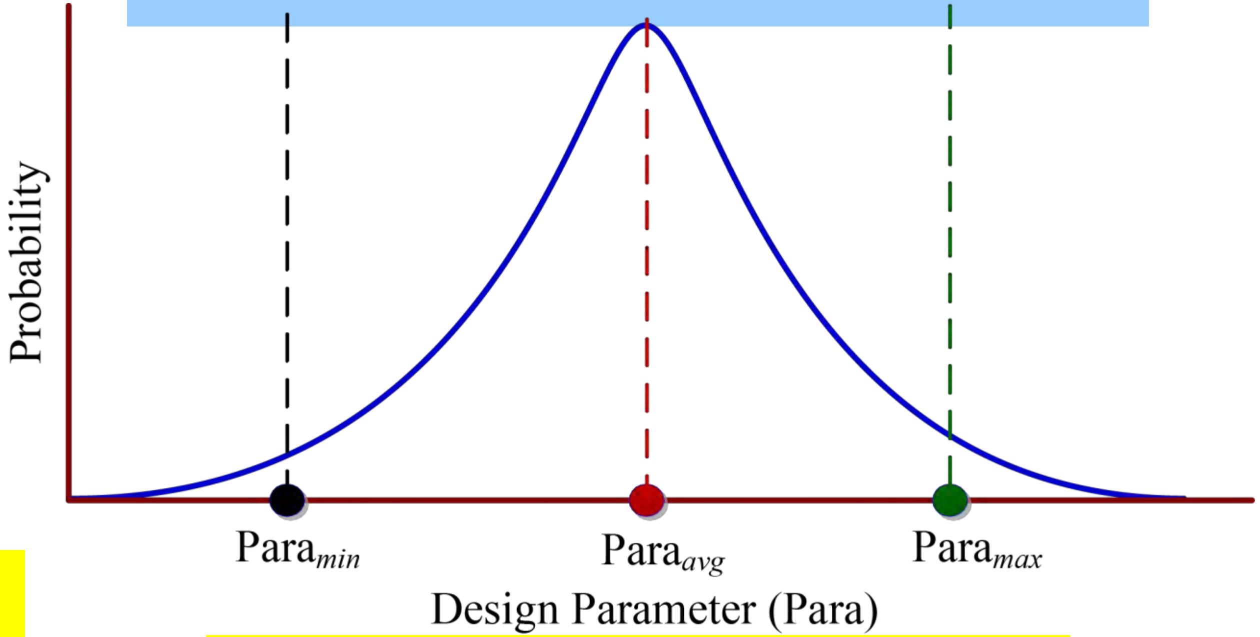
# IC for PUF – Variability versus Variability-Aware Design

**Variability → Randomness for PUF**

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



**Variability-Aware Design → Robust Hardware**

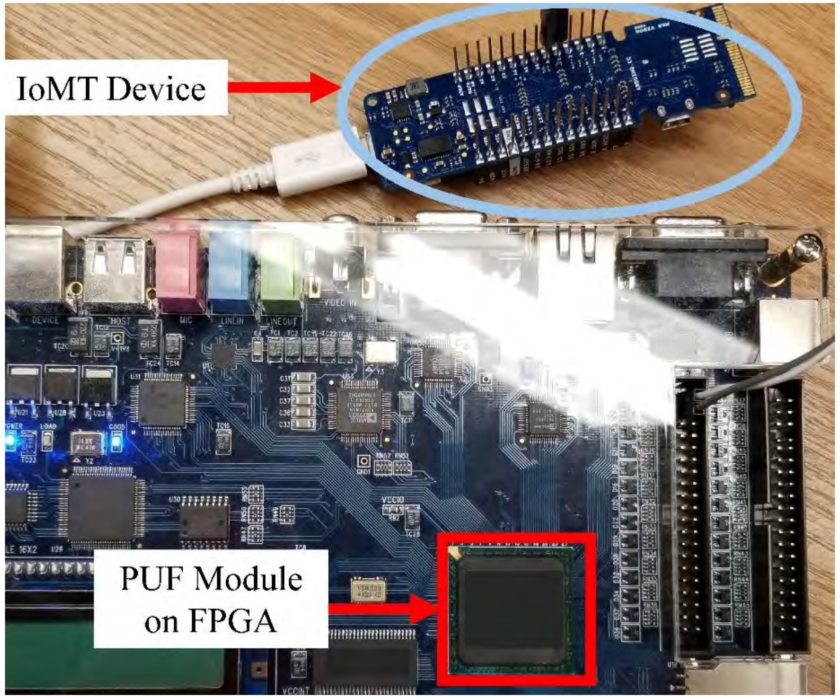



**Variability Features → Randomness → PUF**

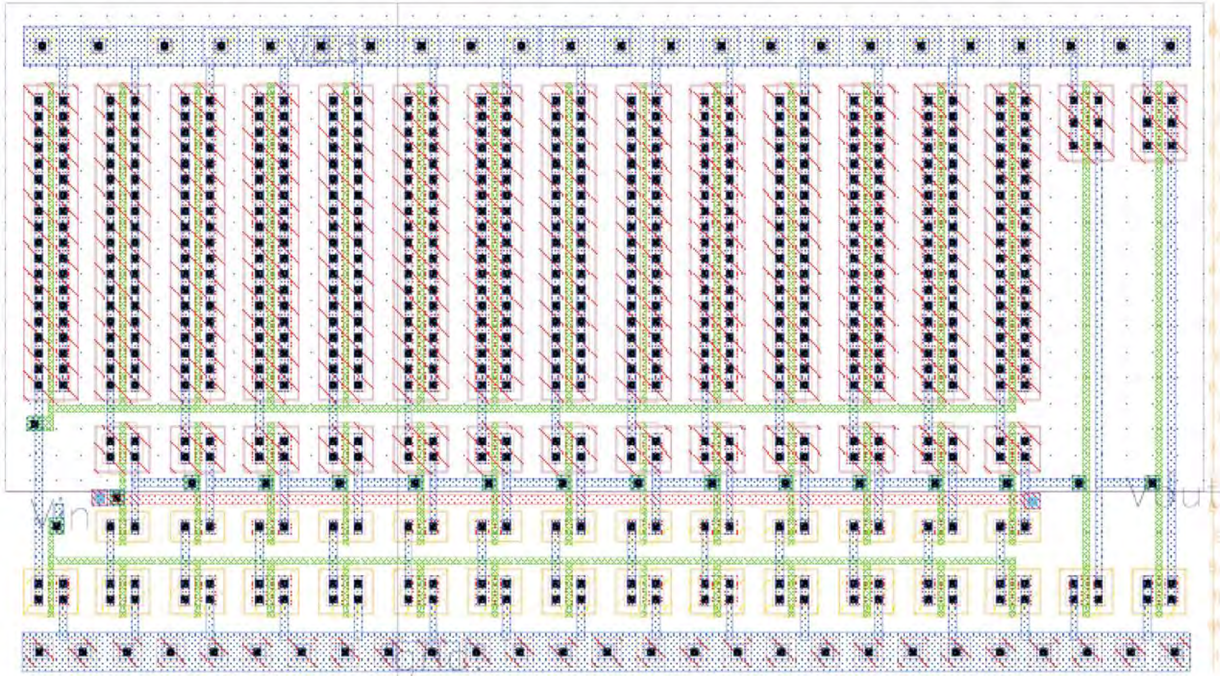
Is it not case of Conflicting Objectives?
How to have a Robust-IC design that functions as a PUF?

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.



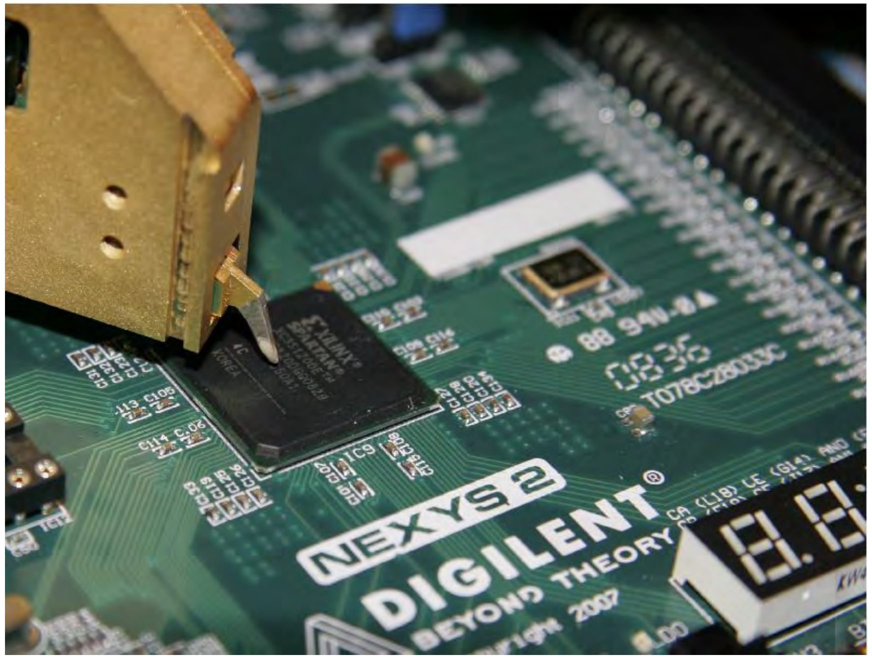
Source: **S. P. Mohanty** and E. Kougianos, "Incorporating Manufacturing Process Variation Awareness in Fast Design Optimization of Nanoscale CMOS VCOs", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 27, Issue 1, February 2014, pp. 22--31.

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

- 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

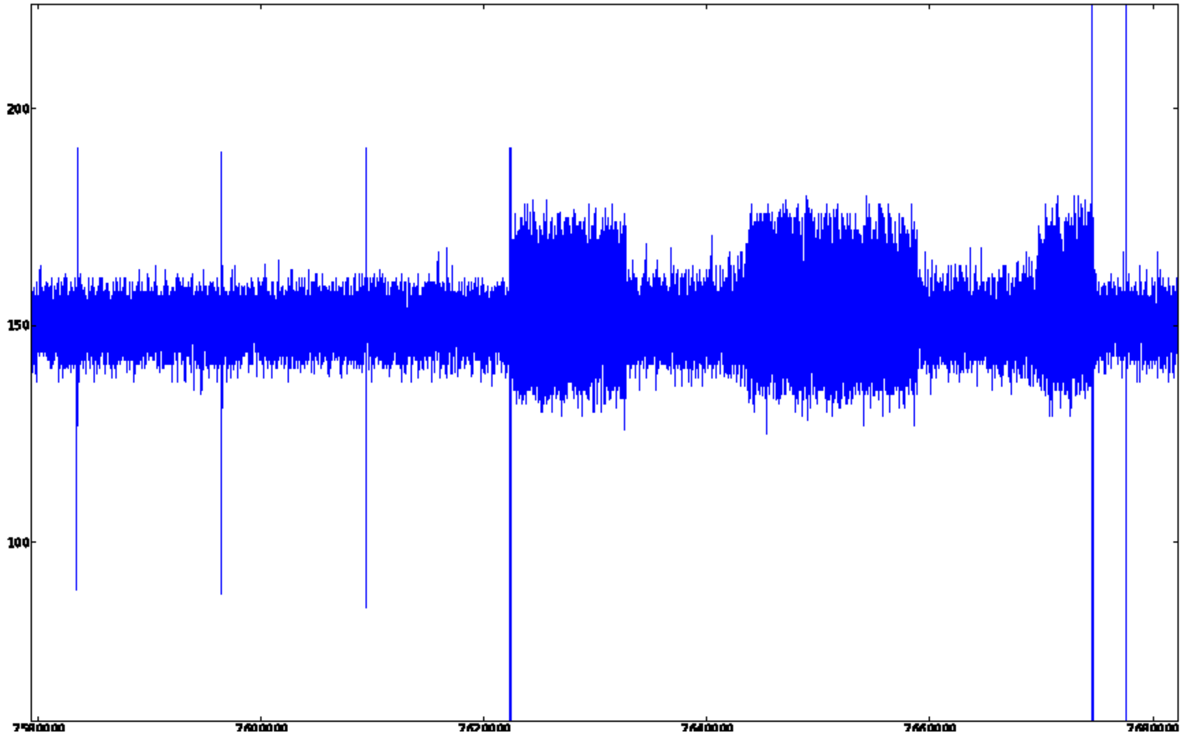
# PUF - Side Channel Leakage

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



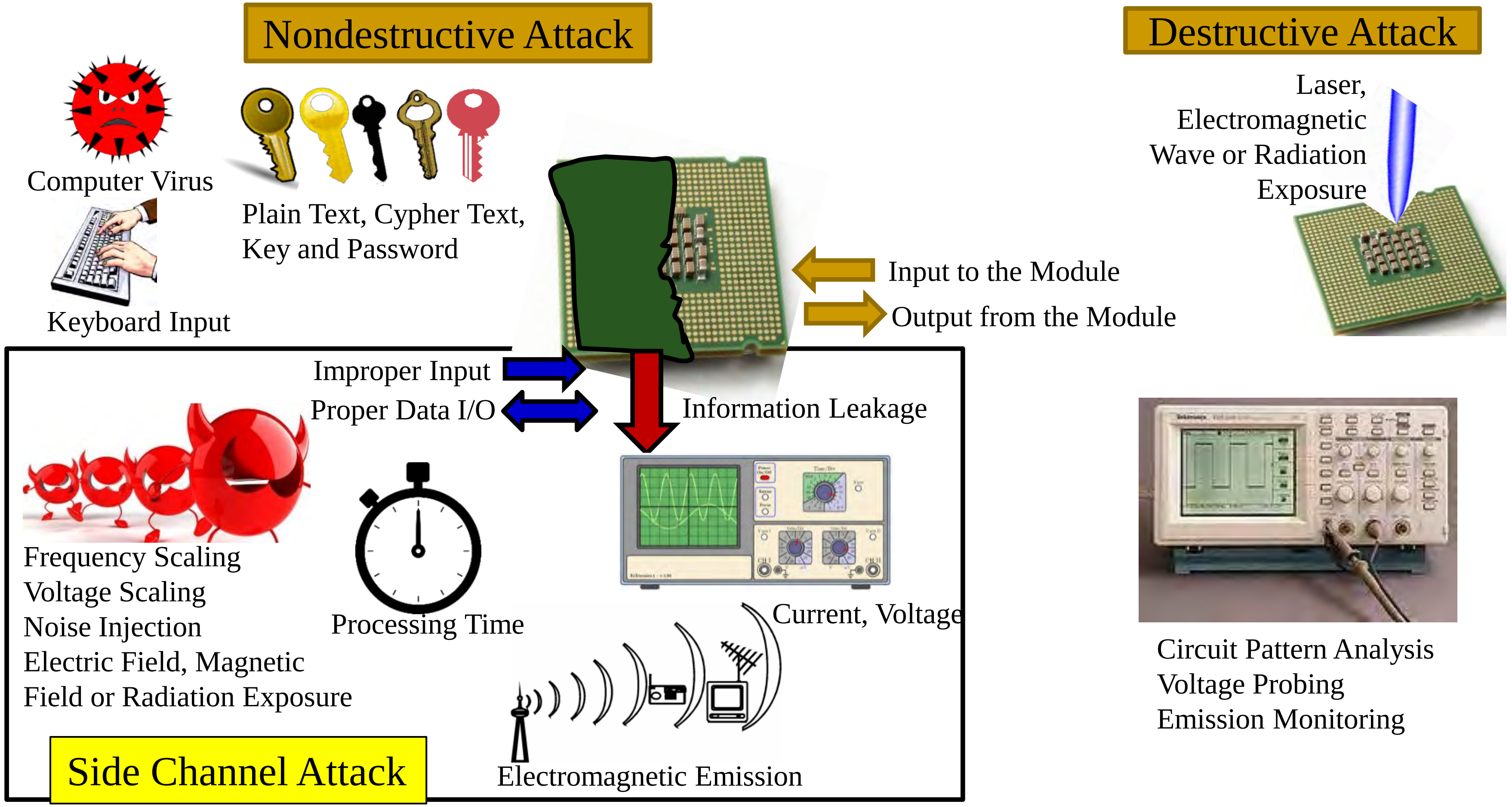

Langer ICR HH 150 probe over Xilinx Spartan3E-1200 FPGA

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



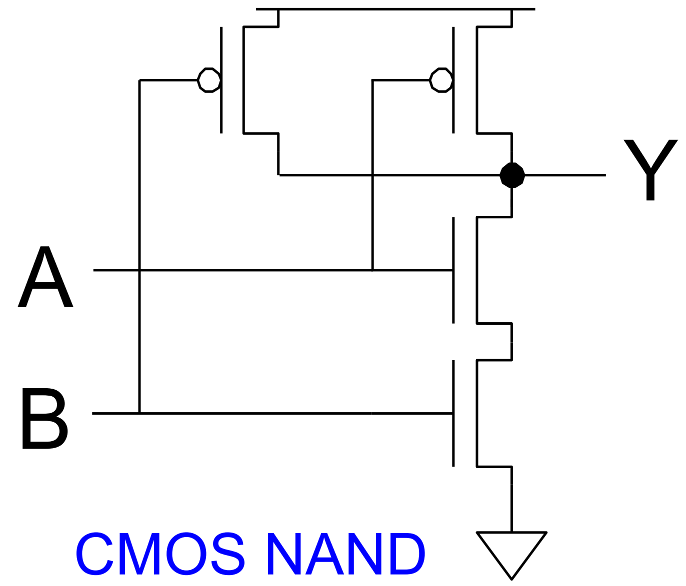

Magnification of the last part of the complete trace. Three trigger signals can be identified: (1) between oscillator phase and error correction phase, (2) between error correction and hashing, and (3) at the end of hashing.

# Side Channel Attacks

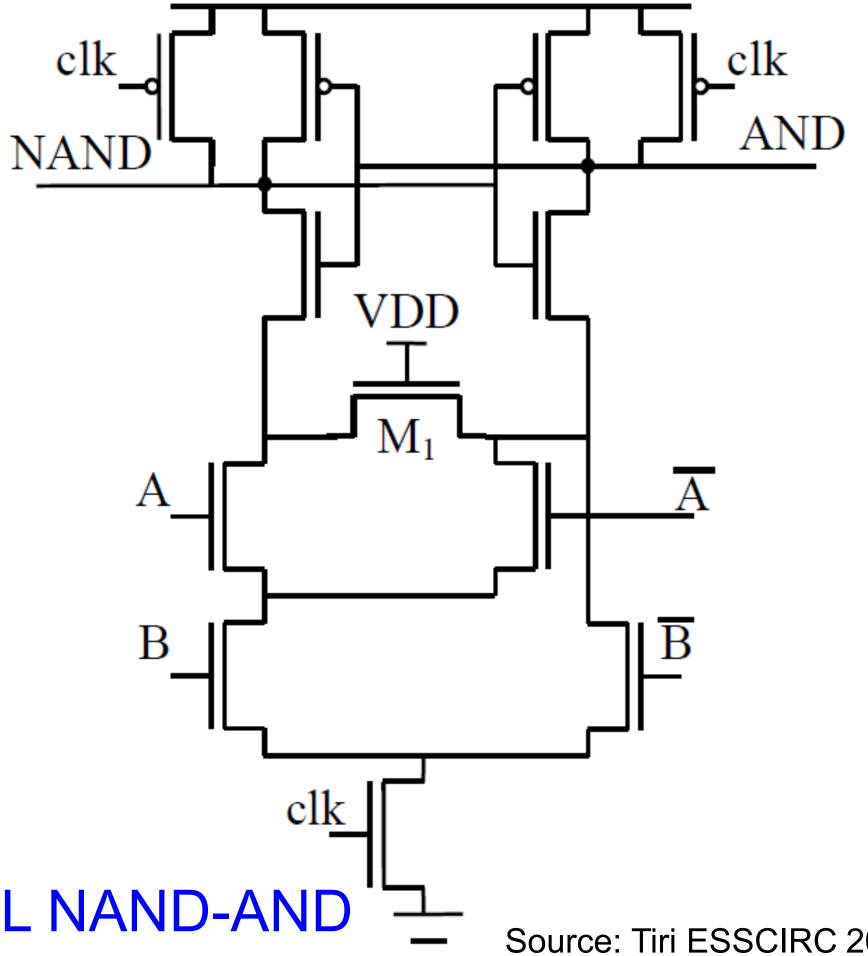



Source: http://www.keirex.com/e/Kti072_SecurityMeasure_e.html

# DPA Resilience Hardware:
# Sense Amplifier Basic Logic (SABL)



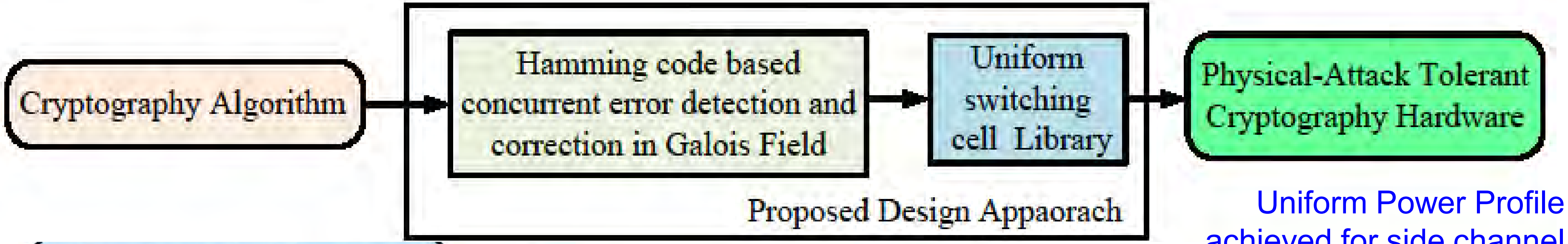

CMOS NAND



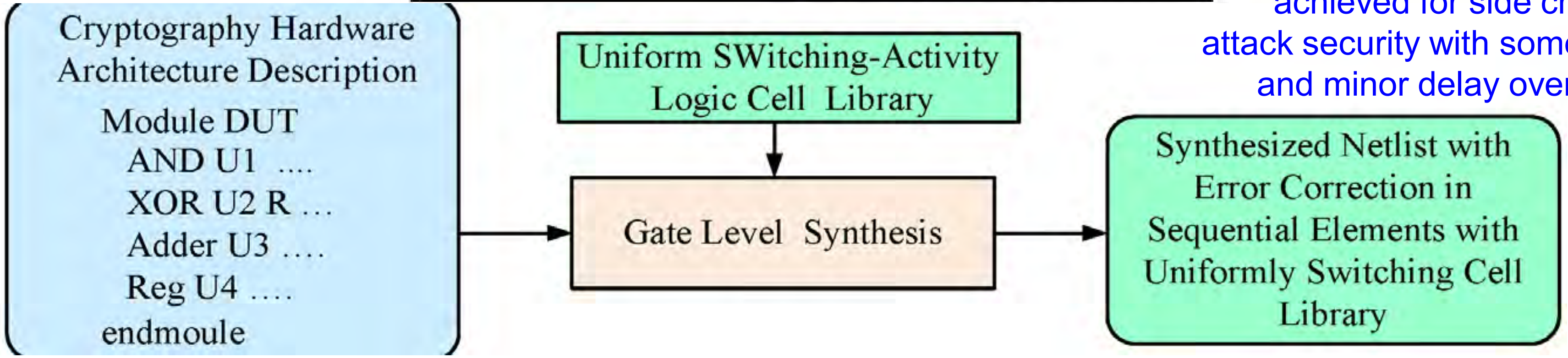

SABL NAND-AND

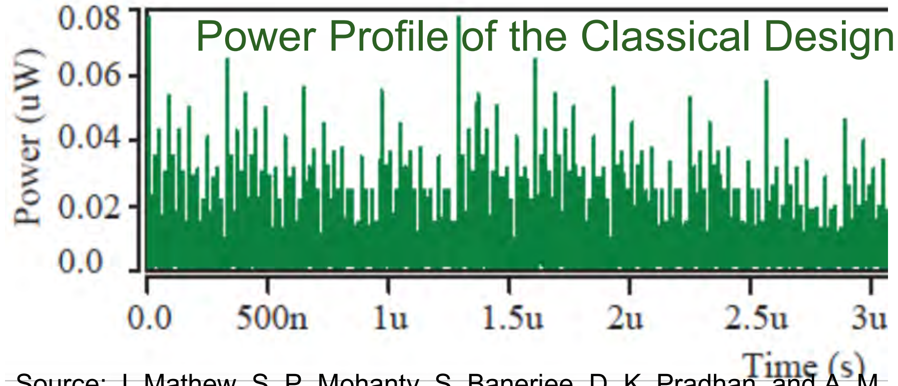
Source: Tiri ESSCIRC 2002

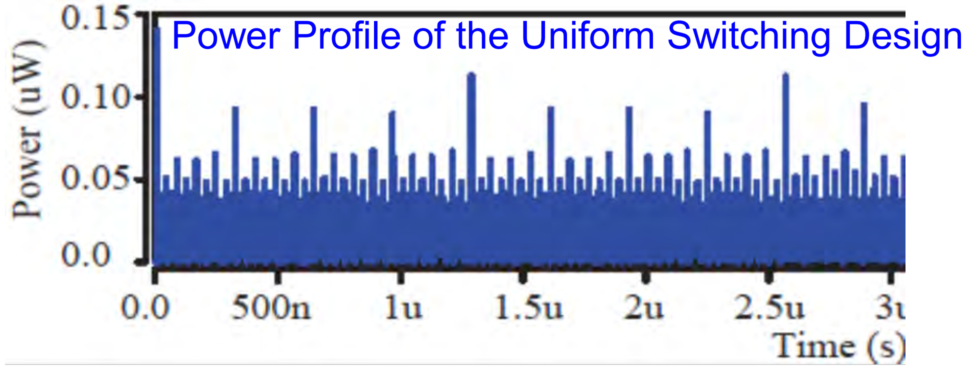
# Our SdD: Approach for DPA Resilience Hardware




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

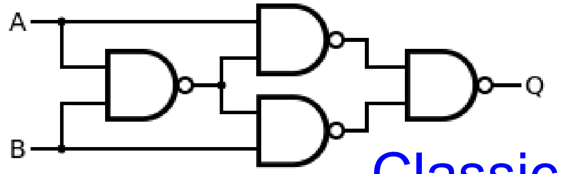


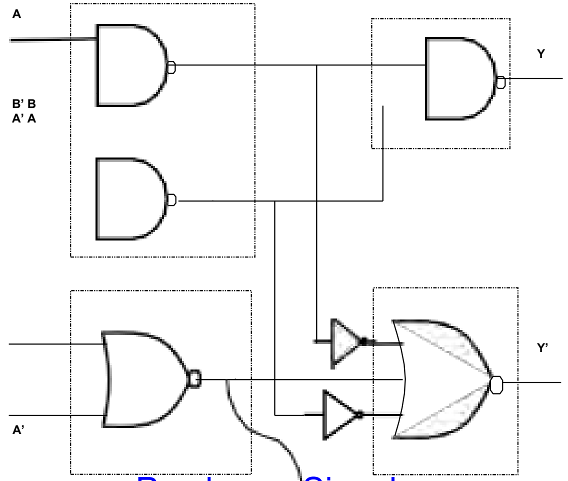




Source: J. Mathew, S. P. Mohanty, S. Banerjee, D. K. Pradhan, and A. M. Jabir, "Attack Tolerant Cryptographic Hardware Design by Combining Galois Field Error Correction and Uniform Switching Activity", *Elsevier Computers and Electrical Engineering*, Vol. 39, No. 4, May 2013, pp. 1077--1087.

# DPA Resilience Hardware: Differential Logic and Routing

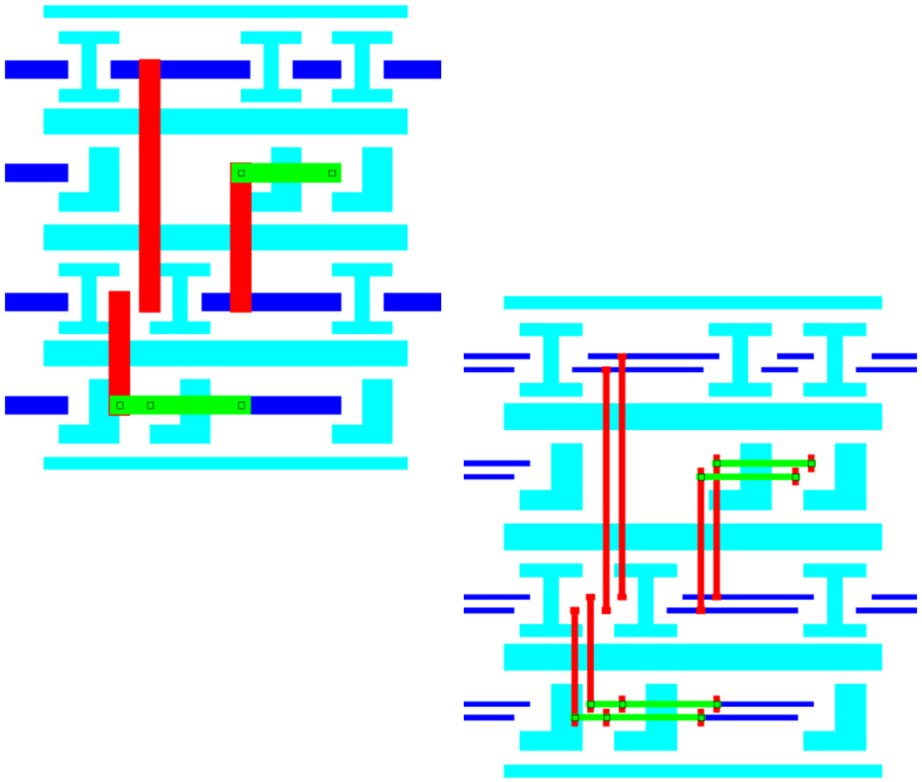



Classic XOR




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.

# Conclusion

# Conclusion

- 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.