Cyberfortifying CPS through Security-by-Design

Keynote – IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics (SaTC 2025)
https://satcconf.com/

Dayton, Ohio – 25 Feb 2025

Homepage:
www.smohanty.org

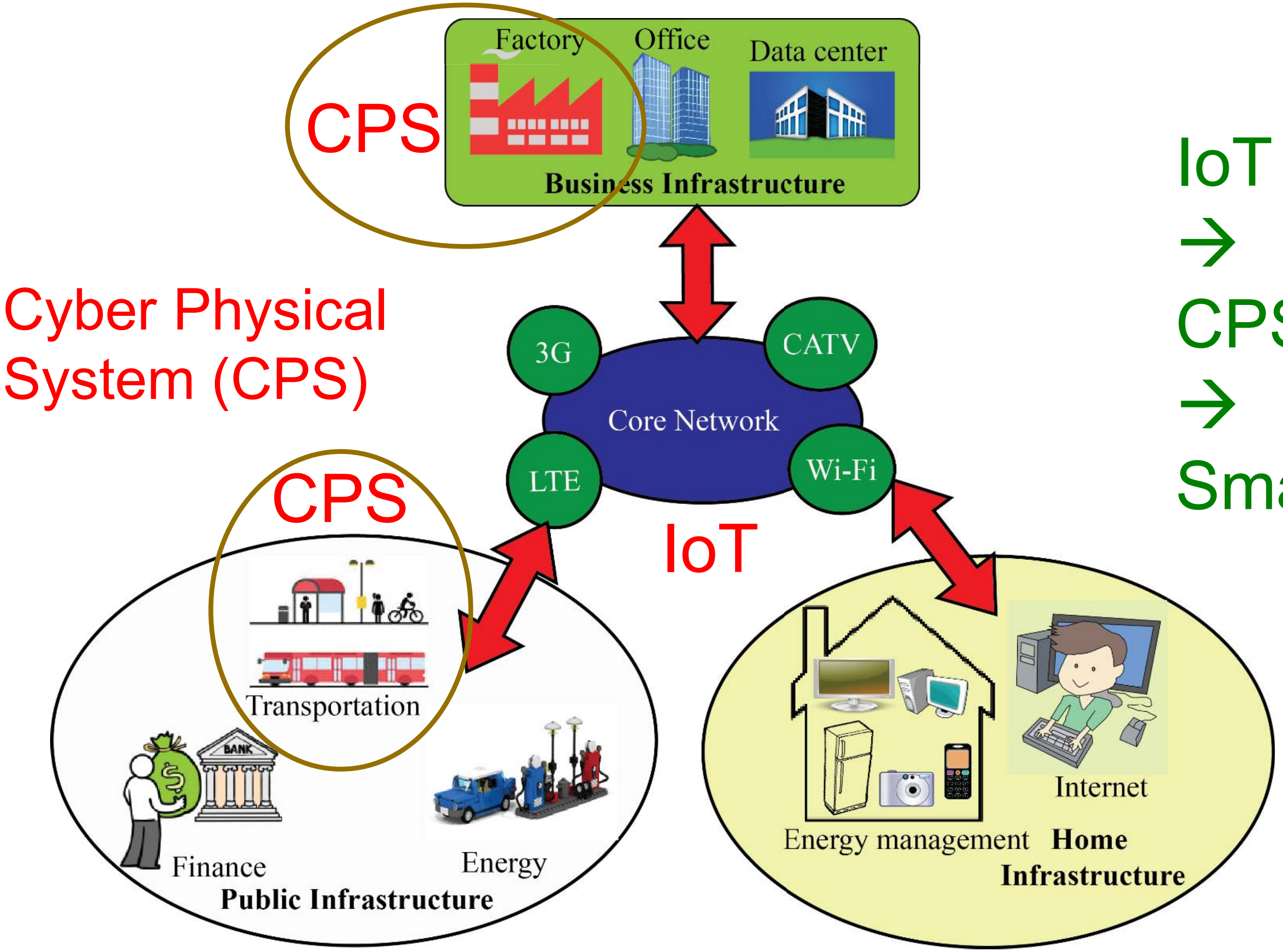
Prof./Dr. Saraju Mohanty
University of North Texas, USA.

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
- Is Physical Unclonable Function (PUF) a Solution for All Cybersecurity Problems?
- Is Blockchain a Solution for All Cybersecurity Problems?
- Conclusion

The Big Picture

IoT → CPS → Smart Cities or Smart Villages

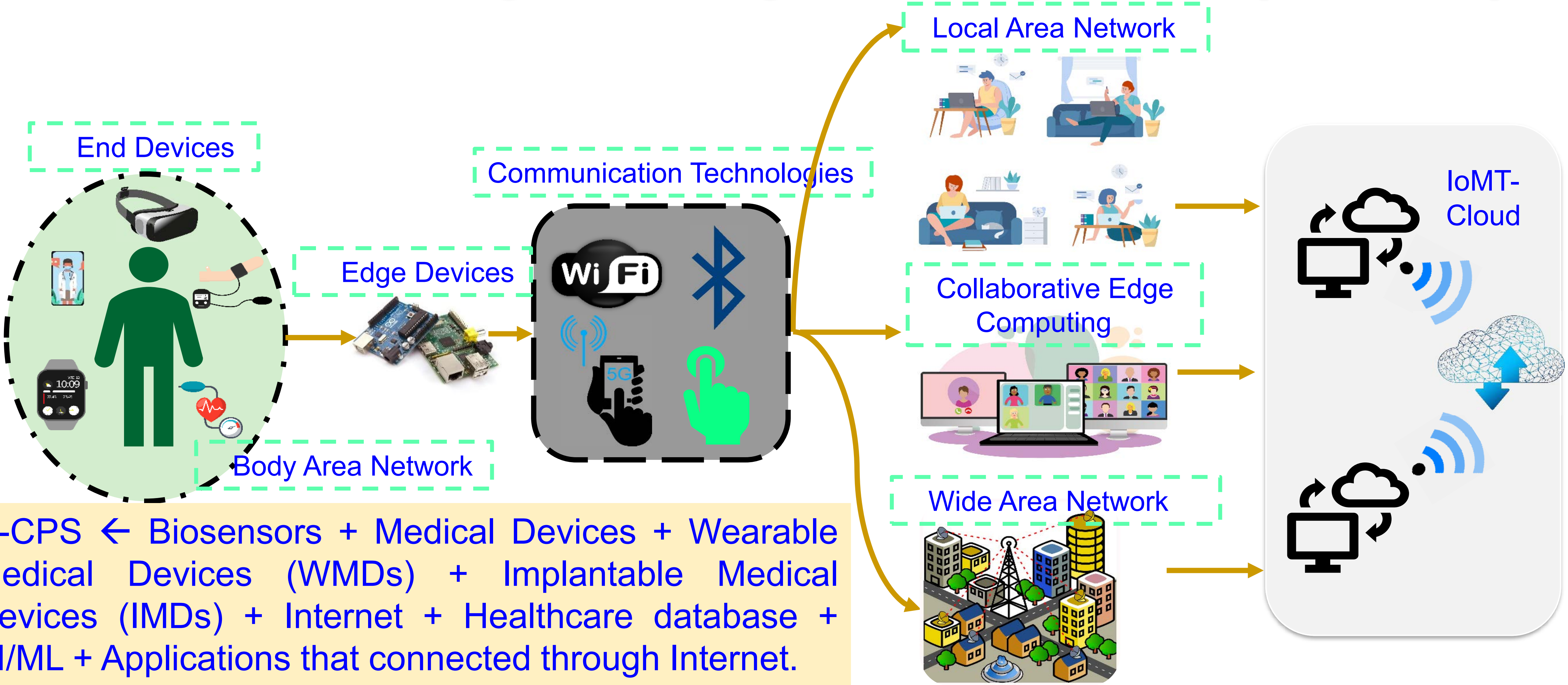


IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

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.

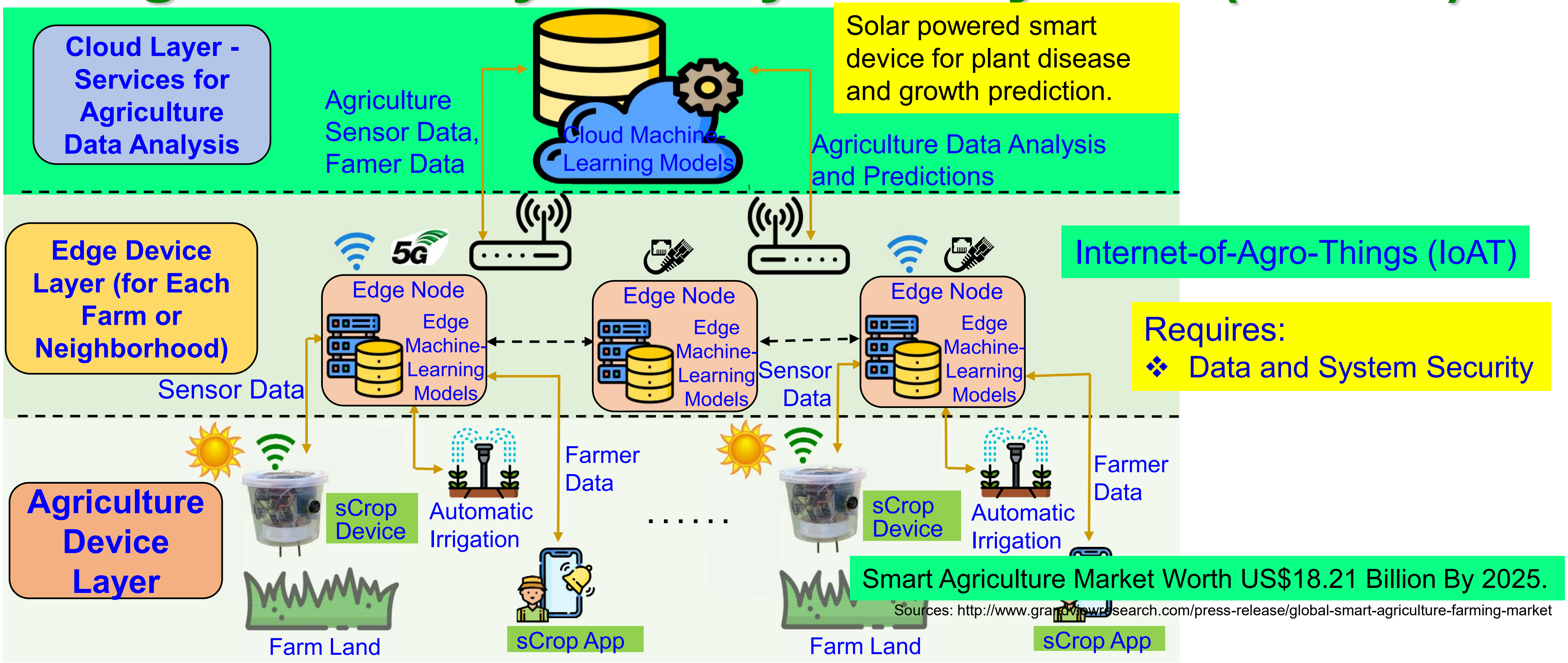
Healthcare Cyber-Physical System (H-CPS)



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

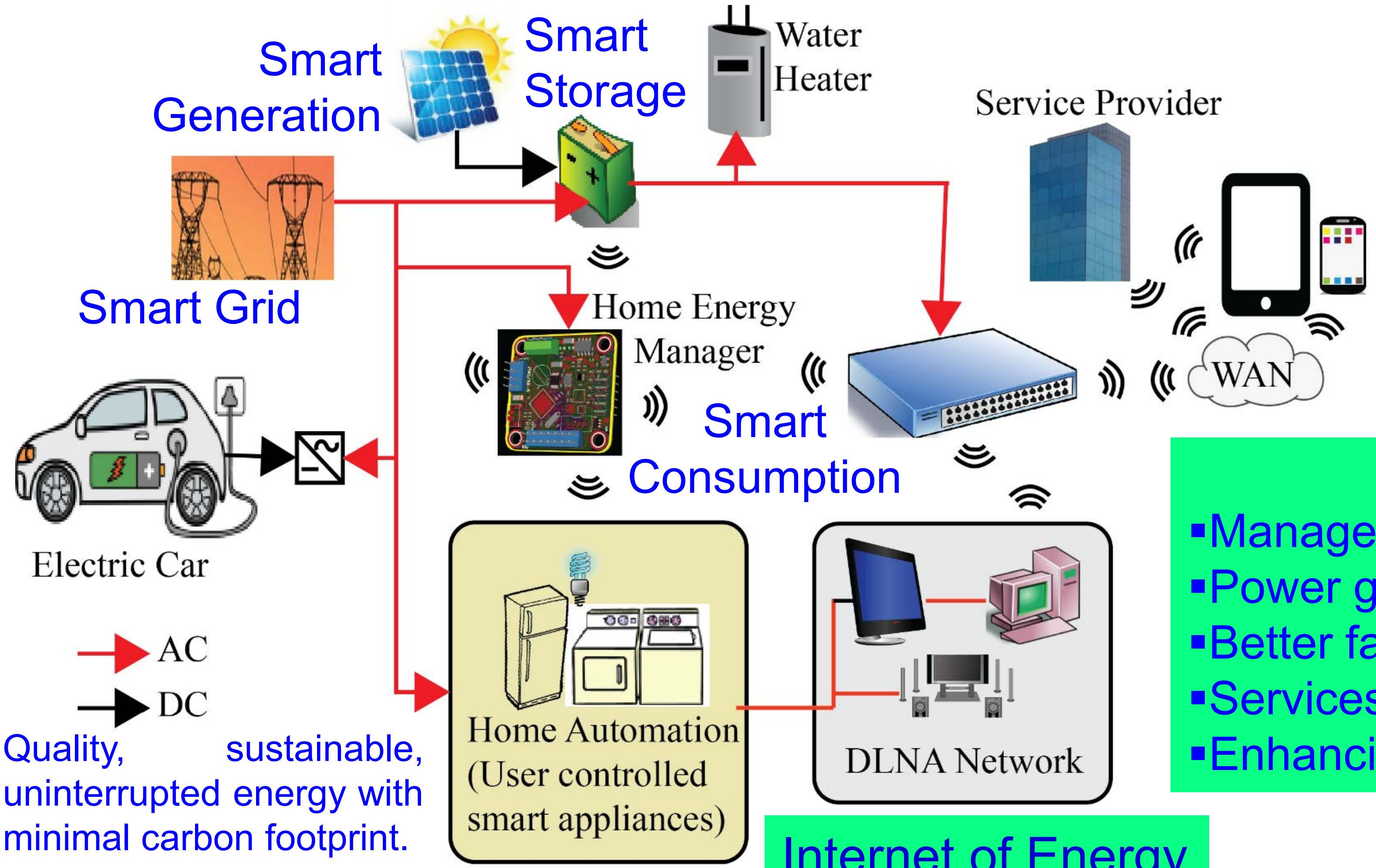
Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

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.

Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Internet of Energy

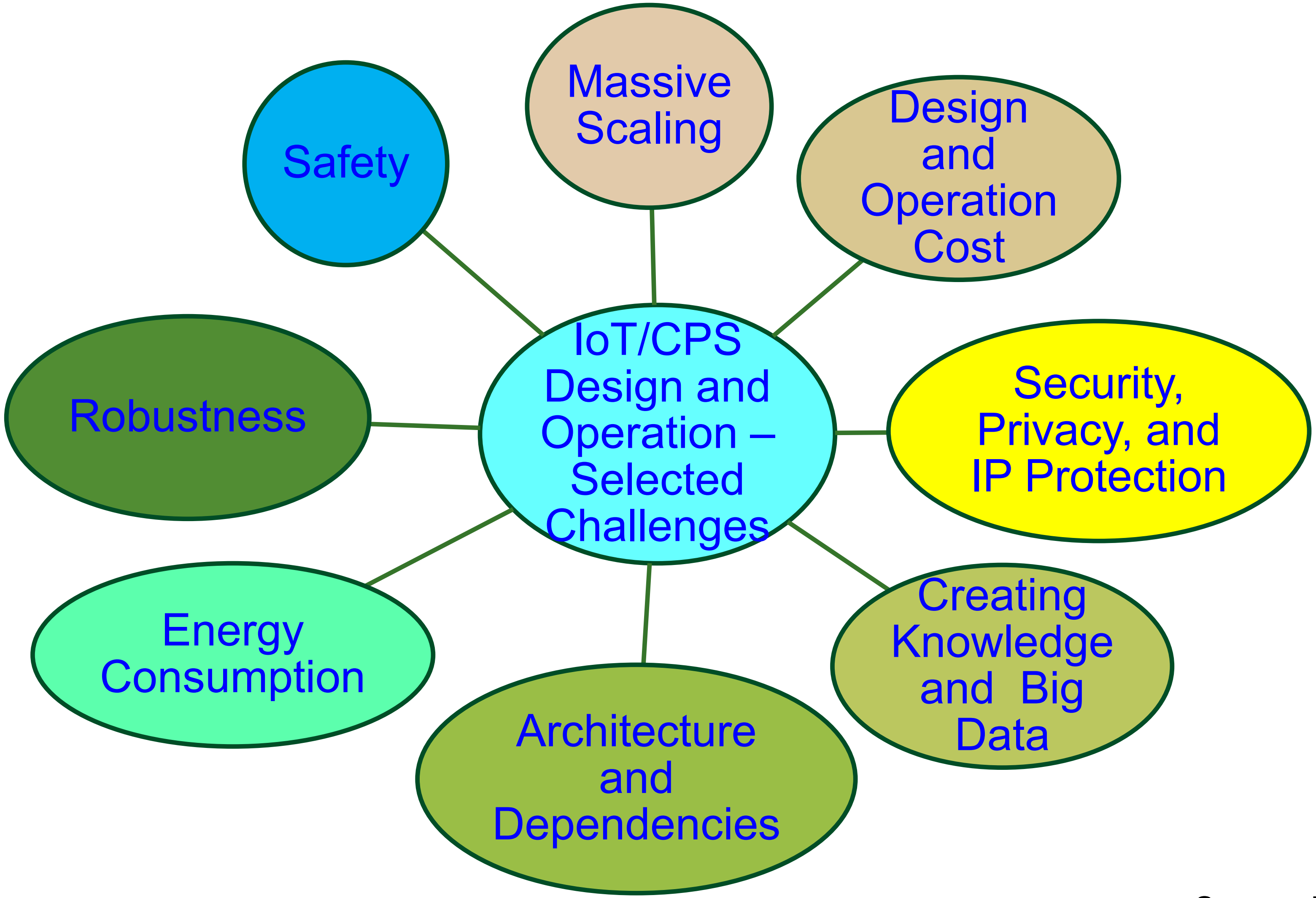
Requires:
- ❖ Data, Device, and System Security

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.

Challenges in IoT/CPS Design

IoT/CPS – Selected Challenges

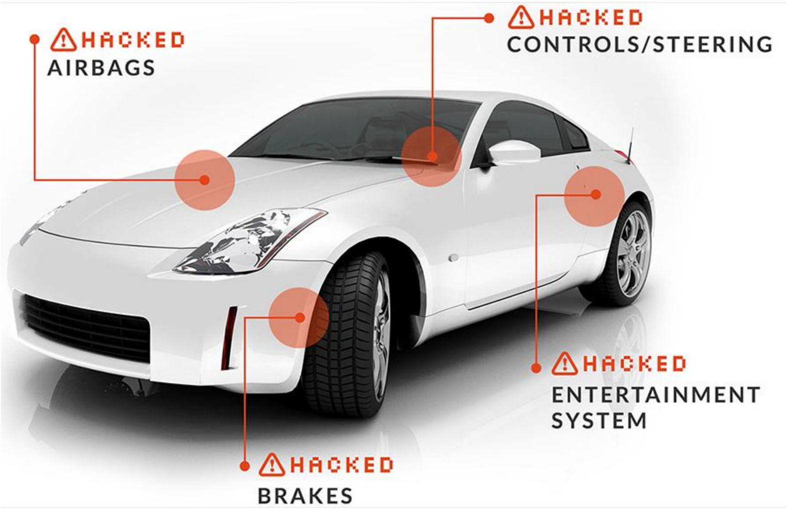


Source: Mohanty ICIT 2017 Keynote

Cybersecurity Challenges - System

Power Grid Attack

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



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

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

Smart Healthcare - 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

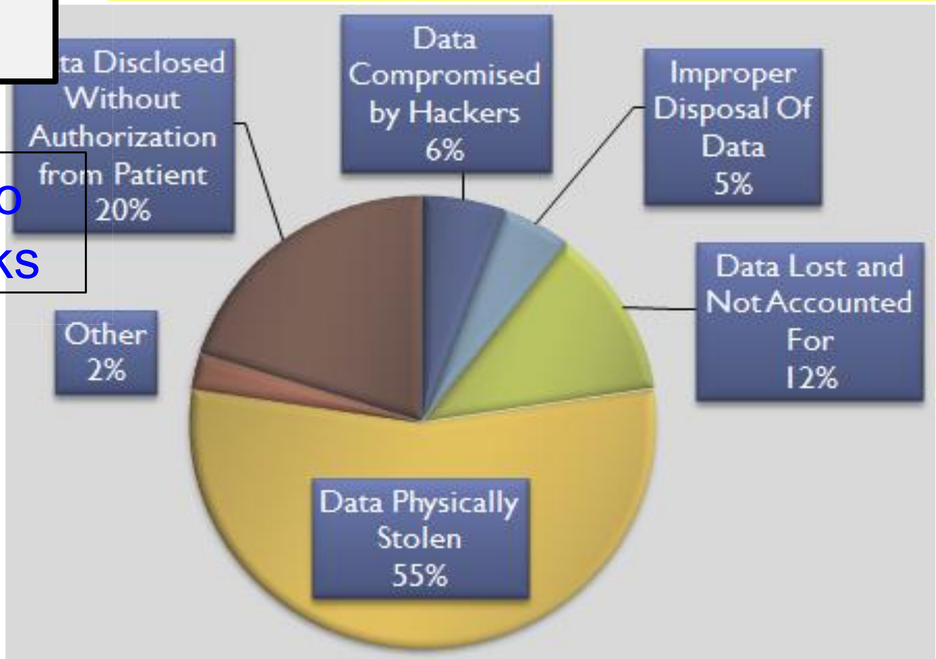
Reverse Engineering Attacks

Radio Attacks

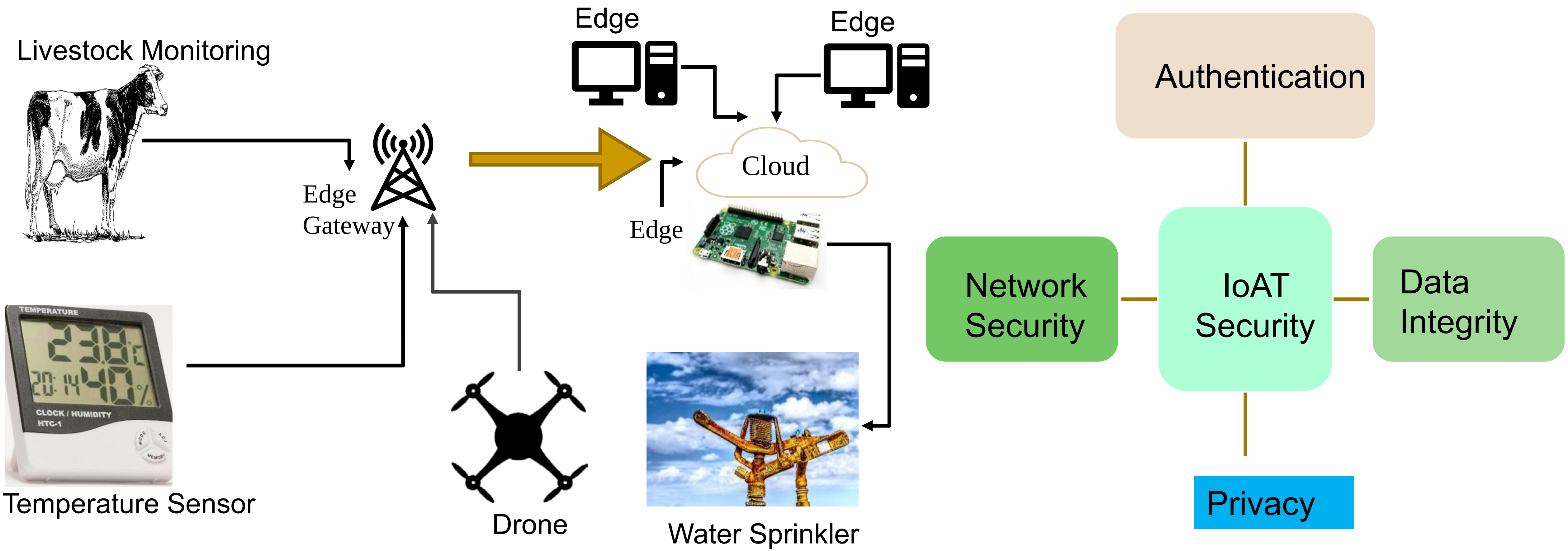
HIPAA

Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types

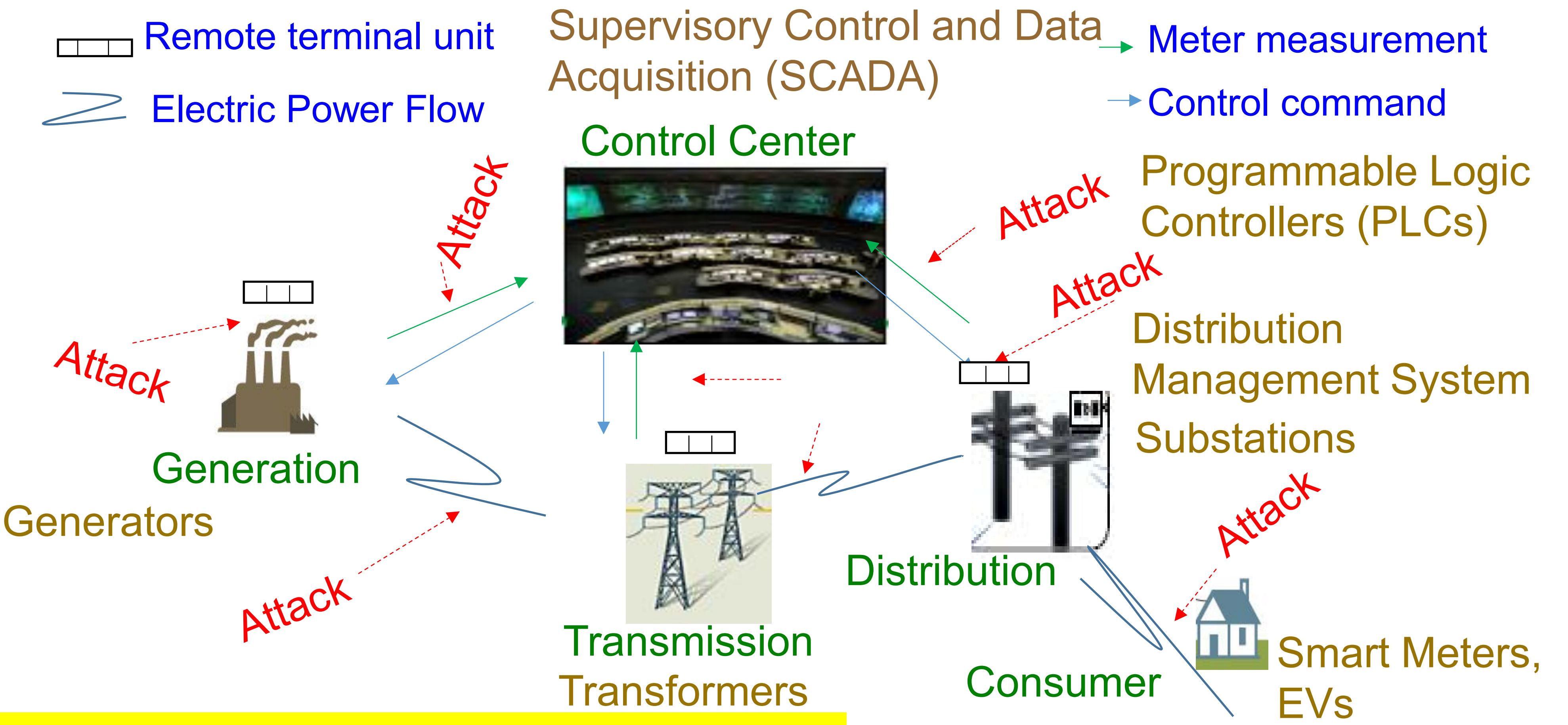


Internet of Agro-Things (IoAT) - Cybersecurity Issue



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.

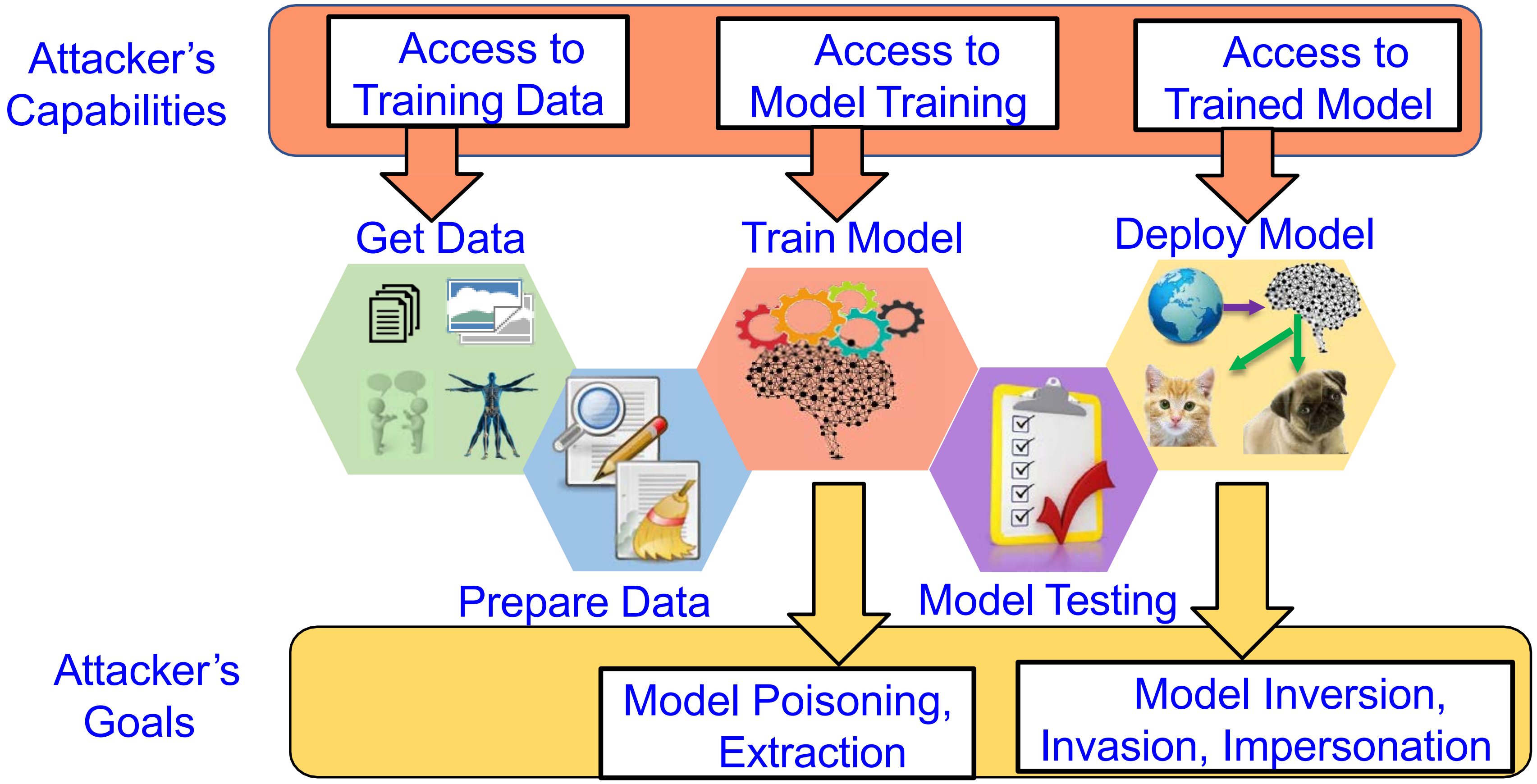
Smart Grid - Vulnerability



ICT components of smart grid is cyber vulnerable.

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

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

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

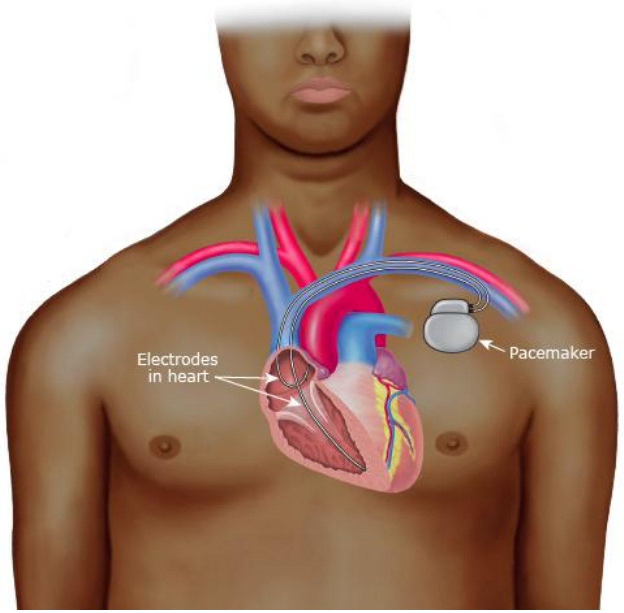
A plug-in for car-engine computers

Fake is Cheap – Why not Buy?

Source: https://www.quora.com

Source: https://nypost.com/

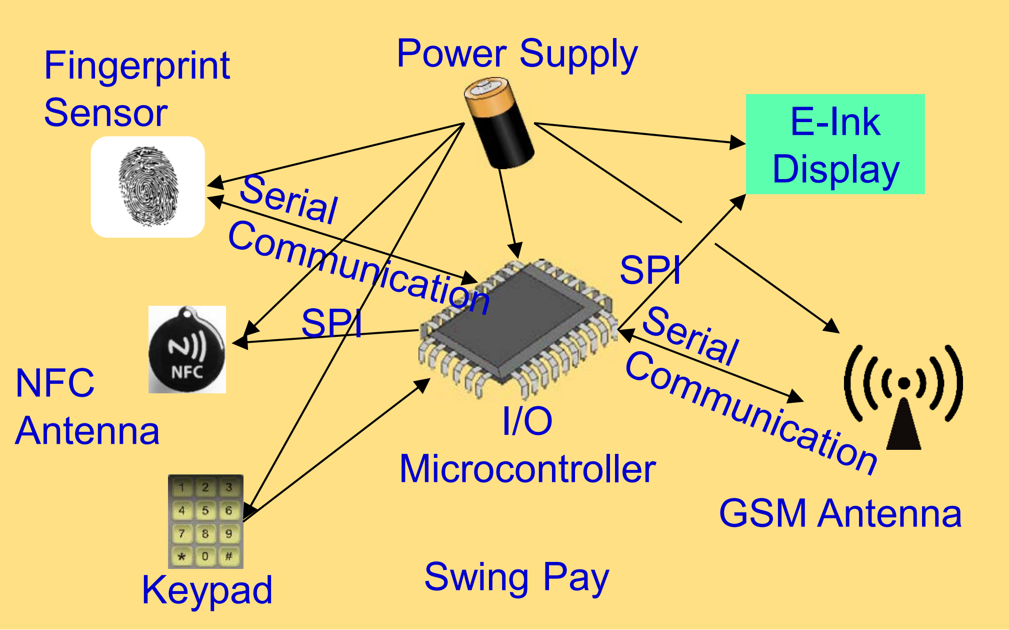
Is my Pacemaker Authentic or Fake?

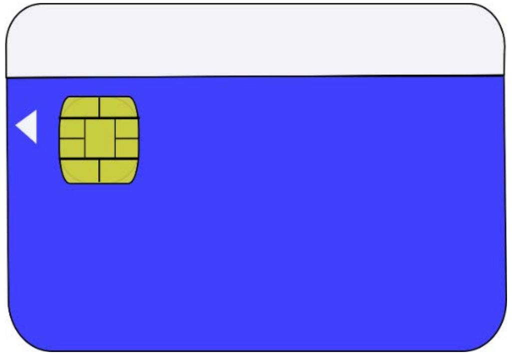


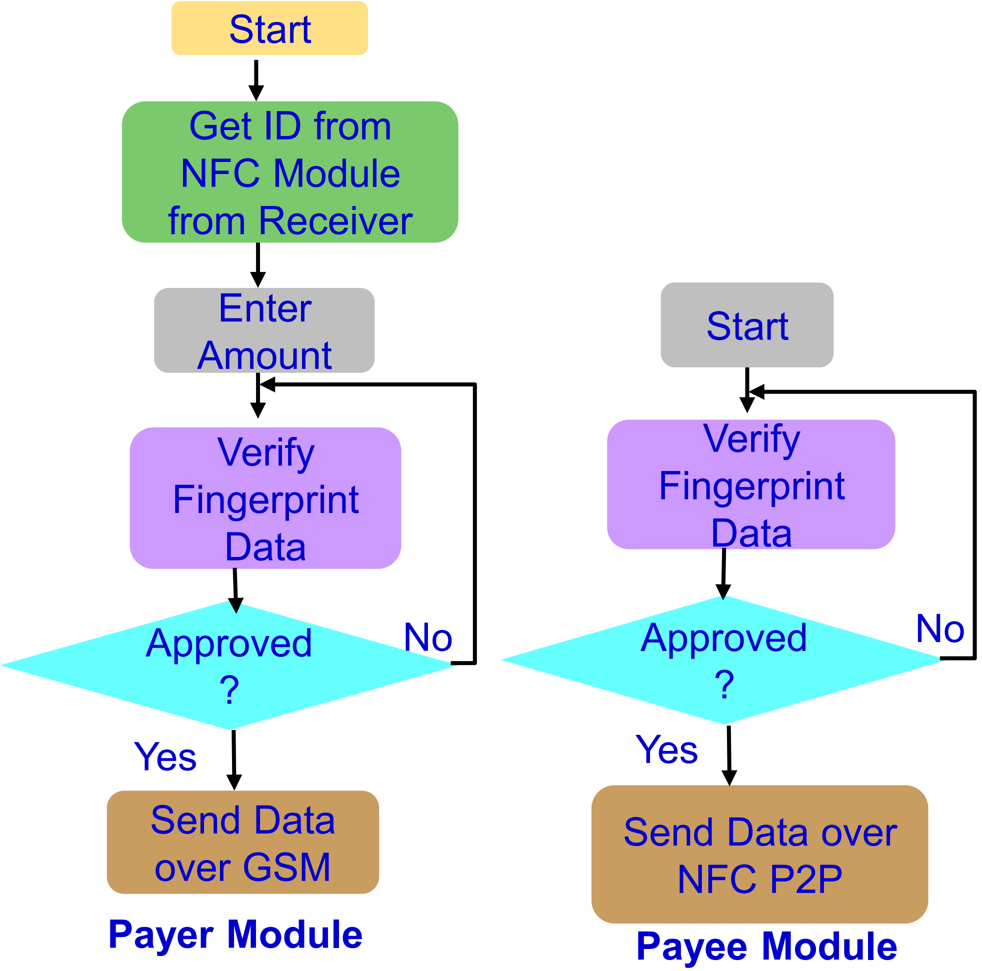
Source: https://apro.ipsf.org/

Cybersecurity Solution for IoT/CPS

Our Swing-Pay: NFC Cybersecurity Solution







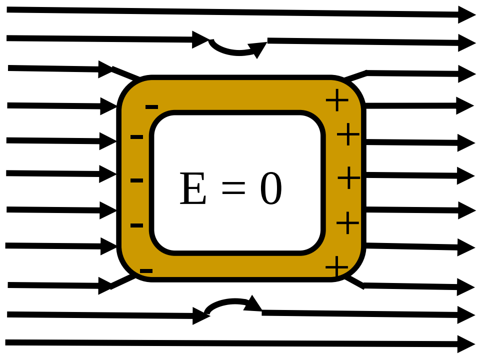
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

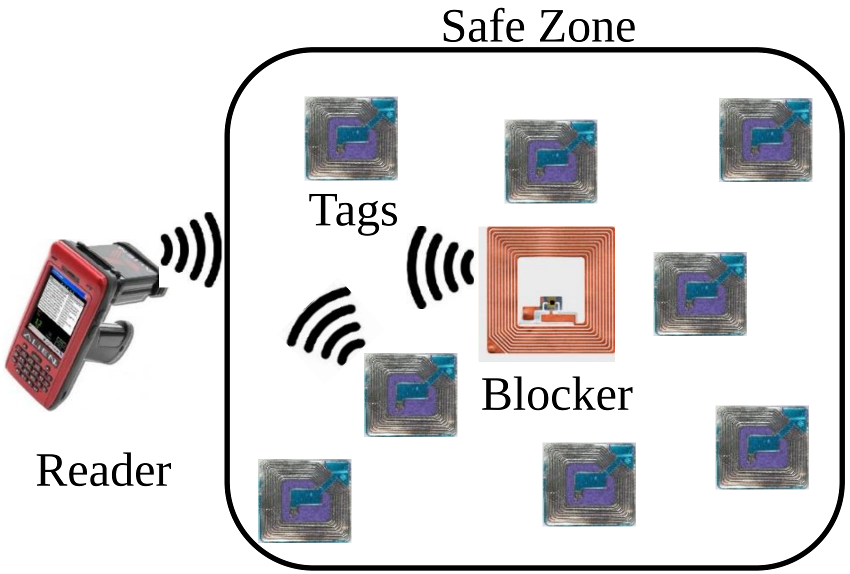
RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

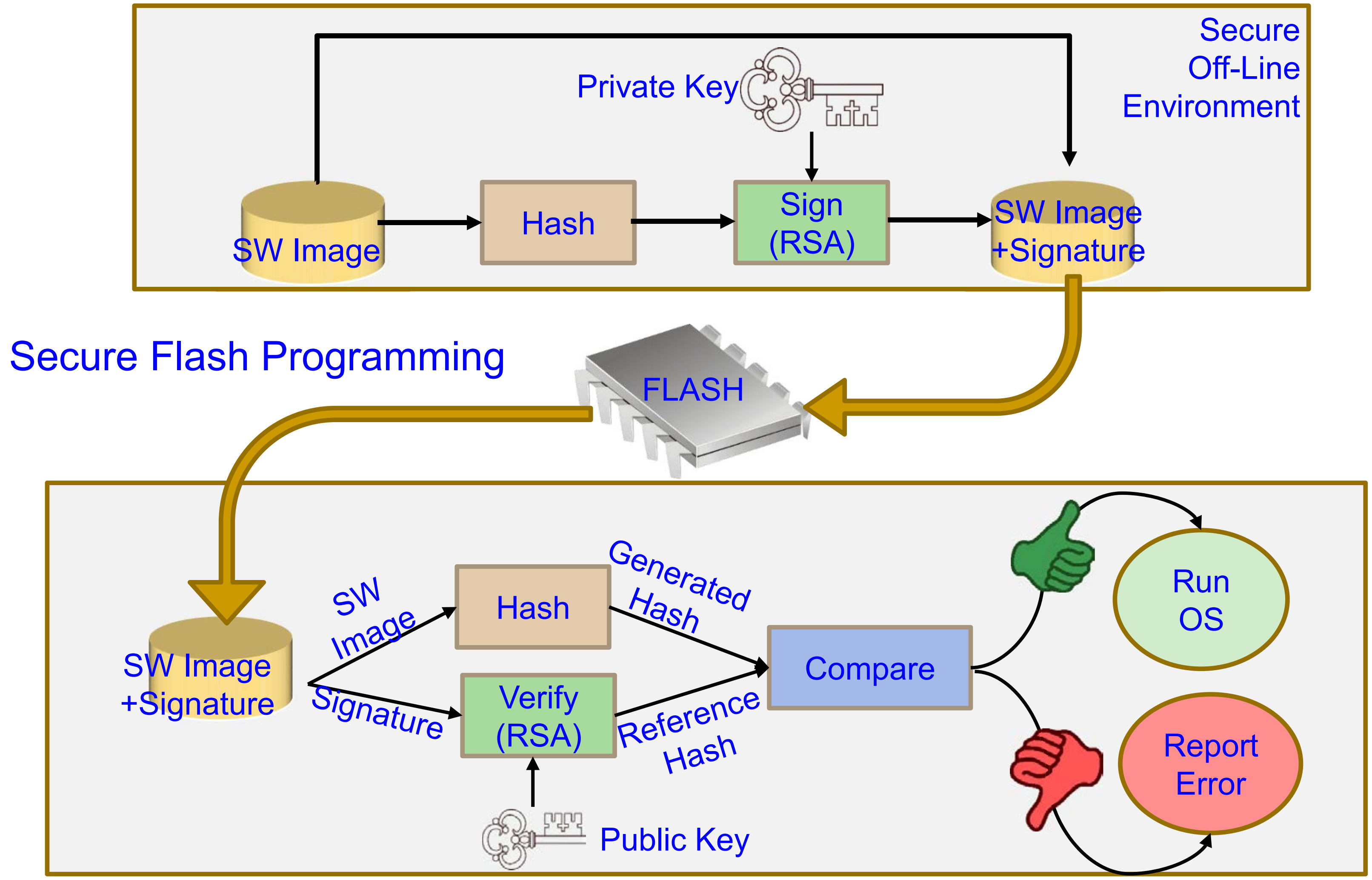




Blocker Tags

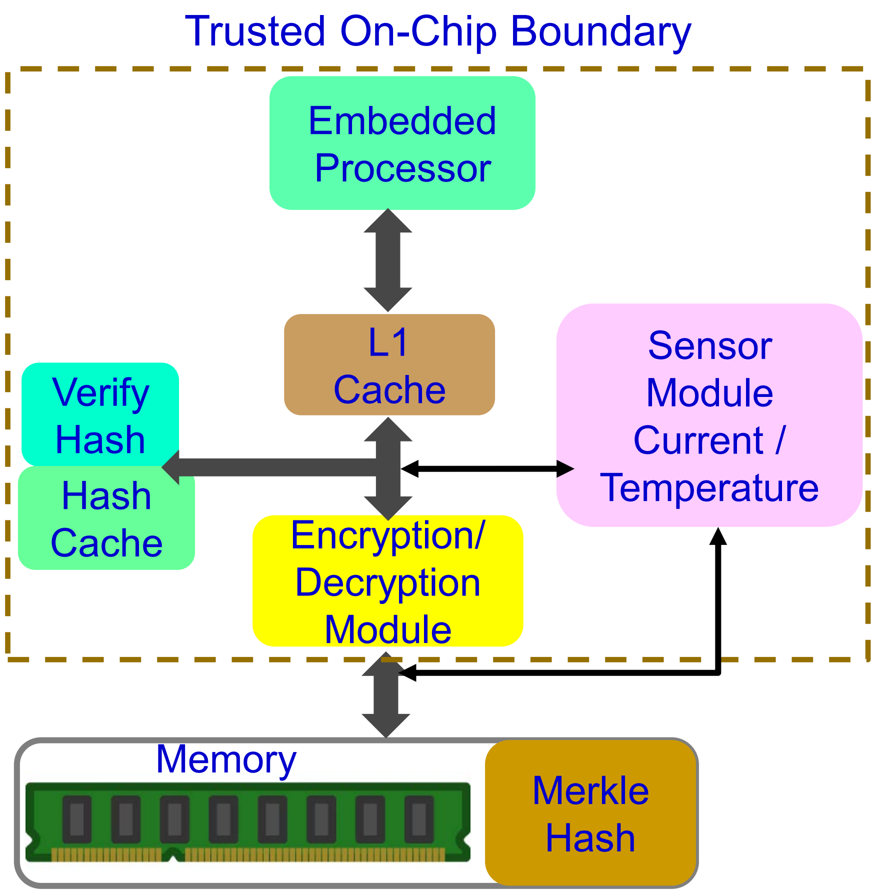
Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution

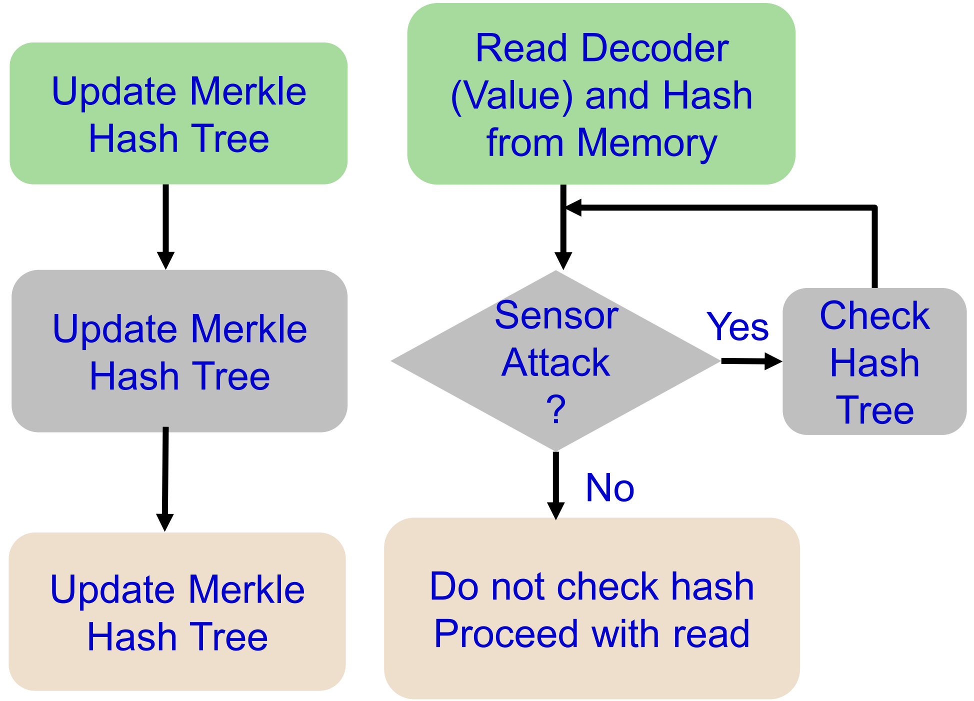


Source: https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

Embedded Memory Security



On-Chip/On-Board Memory Protection



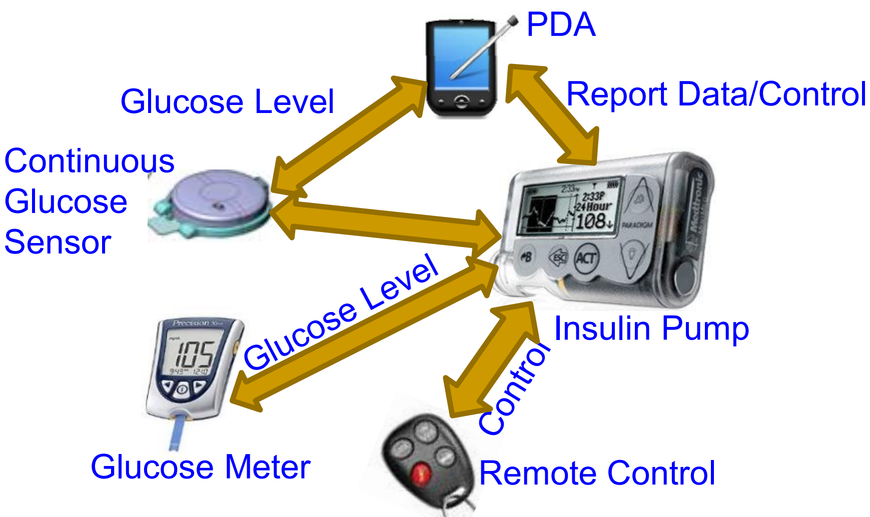
Write Operation

Read Operation

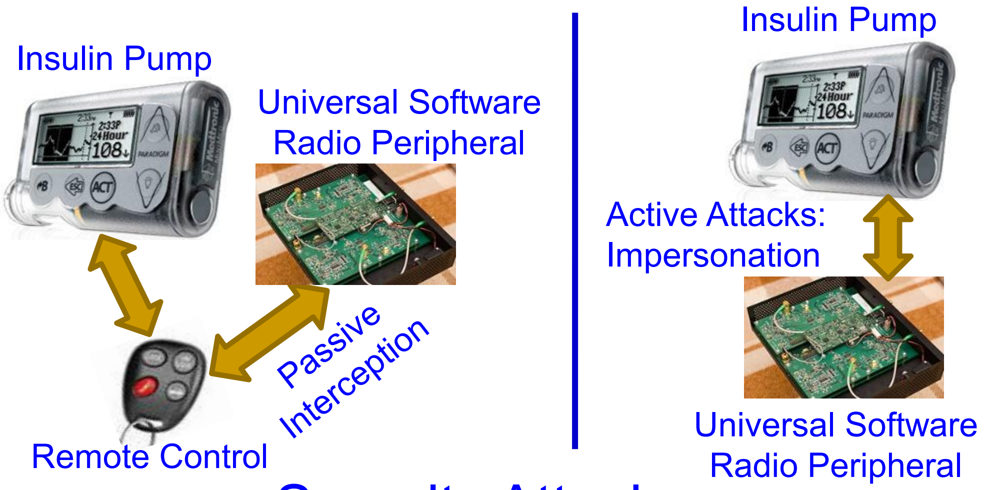
Memory integrity verification with 85% energy savings with minimal performance overhead.

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.

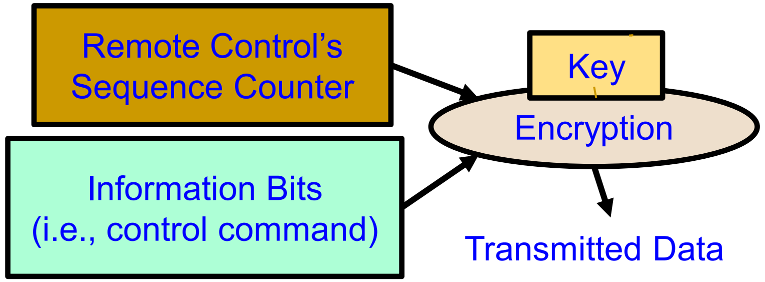
Smart Healthcare Cybersecurity



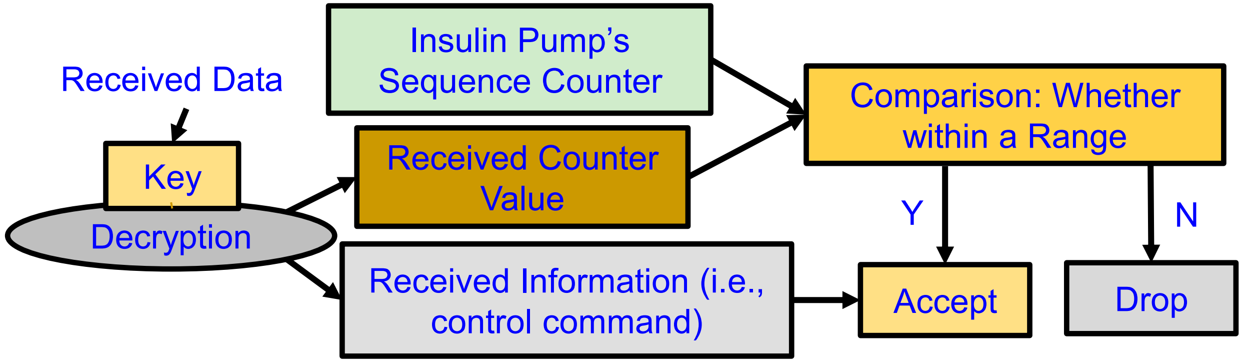
Insulin Delivery System



Security Attacks



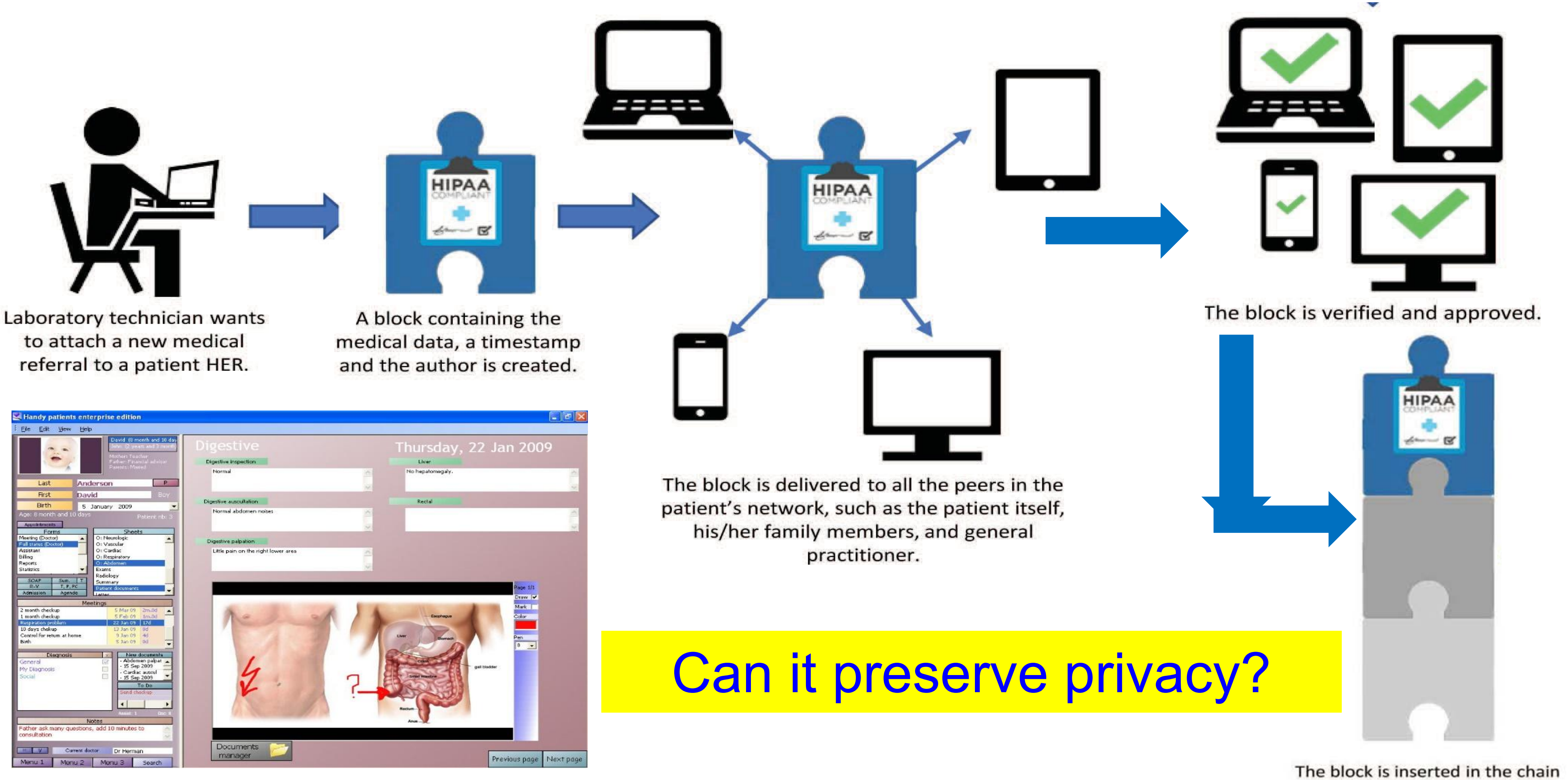
Rolling Code Encoder in Remote Control



Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Blockchain in Smart Healthcare

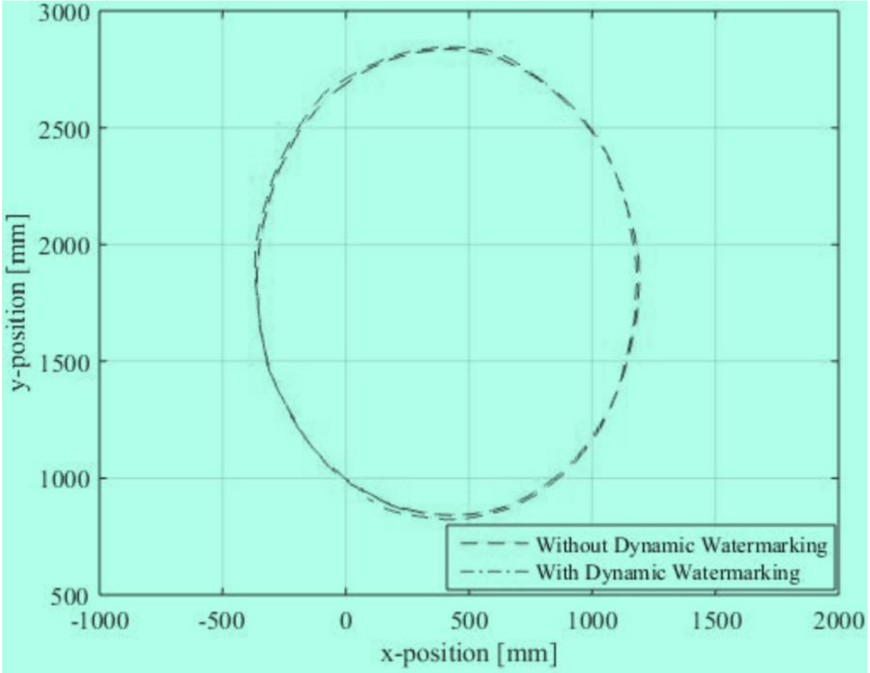


Can it preserve privacy?

Source: C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.

Autonomous Car Cybersecurity – Collision Avoidance

- Attack: Feeding of malicious sensor measurements to the control and the collision avoidance module. Such an attack on a position sensor can result in collisions between the vehicles.
- Solutions: "**Dynamic Watermarking**" of signals to detect and stop such attacks on cyber-physical systems.
- Idea: Superimpose each actuator *i* a random signal $e_i[t]$ (watermark) on control policy-specified input.



Source: Ko 2016, CPS-Sec 2016

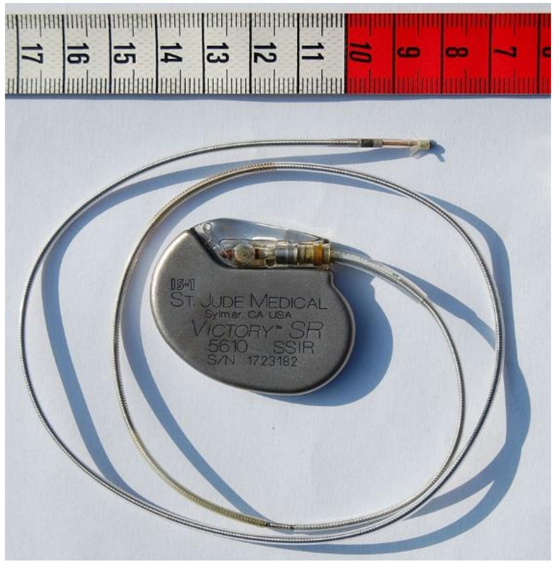
Drawbacks of Existing Cybersecurity Solutions

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

IT Cybersecurity	IoT Cybersecurity
IT infrastructure may be well protected rooms	IoT may be deployed in open hostile environments
Limited variety of IT network devices	Significantly large variety of IoT devices
Millions of IT devices	Billions of IoT devices
Significant computational power to run heavy-duty security solutions	May not have computational power to run security solutions
IT security breach can be costly	IoT security breach (e.g. in a IoMT device like pacemaker, insulin pump) can be life threatening

Incorporation of Cybersecurity of Electronic Systems, IoT, CPS, needs Energy, and hence affects Performance.

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

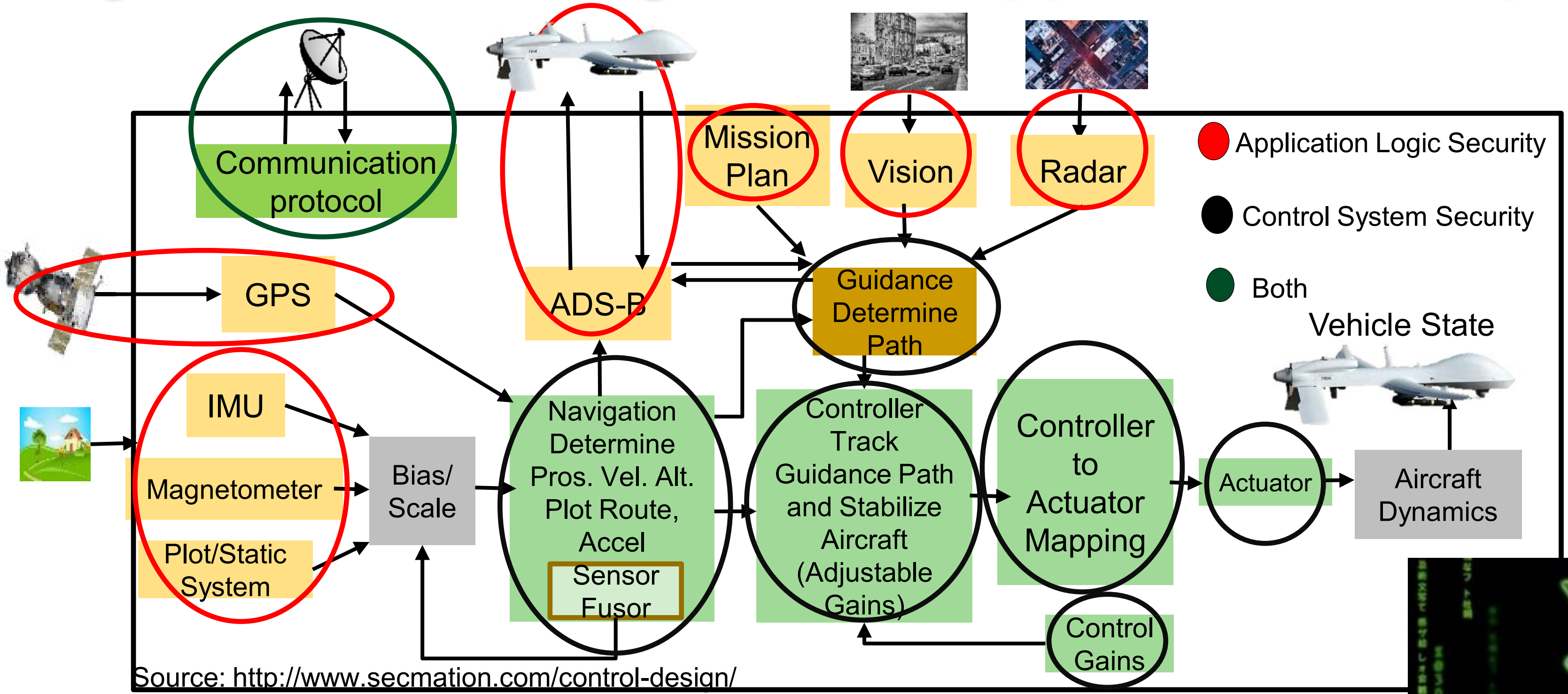
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

- 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

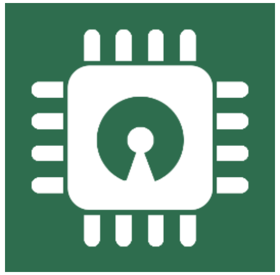
Smart Grid – Security Solution Constraints
- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

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

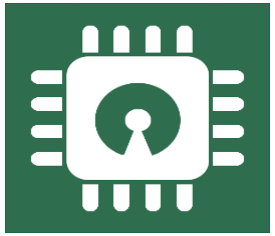
Source: Mohanty ICCE Panel 2018

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 to run
- Can’t stop hardware reverse engineering

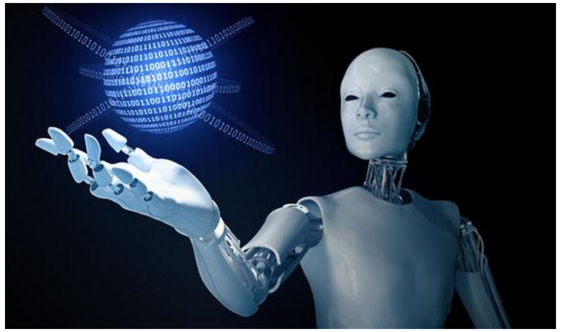
Source: Mohanty ICCE Panel 2018



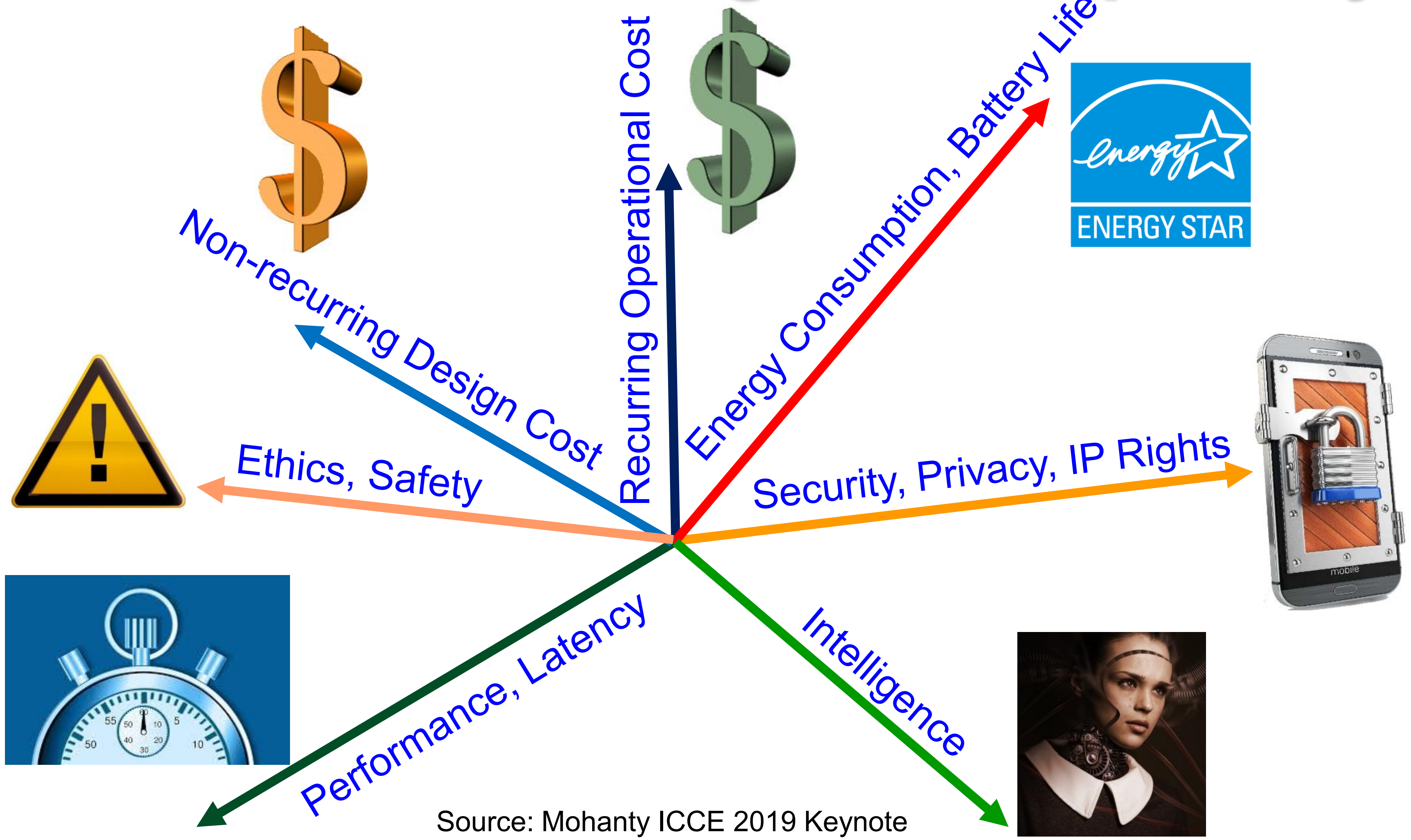
Hardware Based

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

Security-by-Design (SbD) – The Principle



IoT/CPS Design – Multiple Objectives



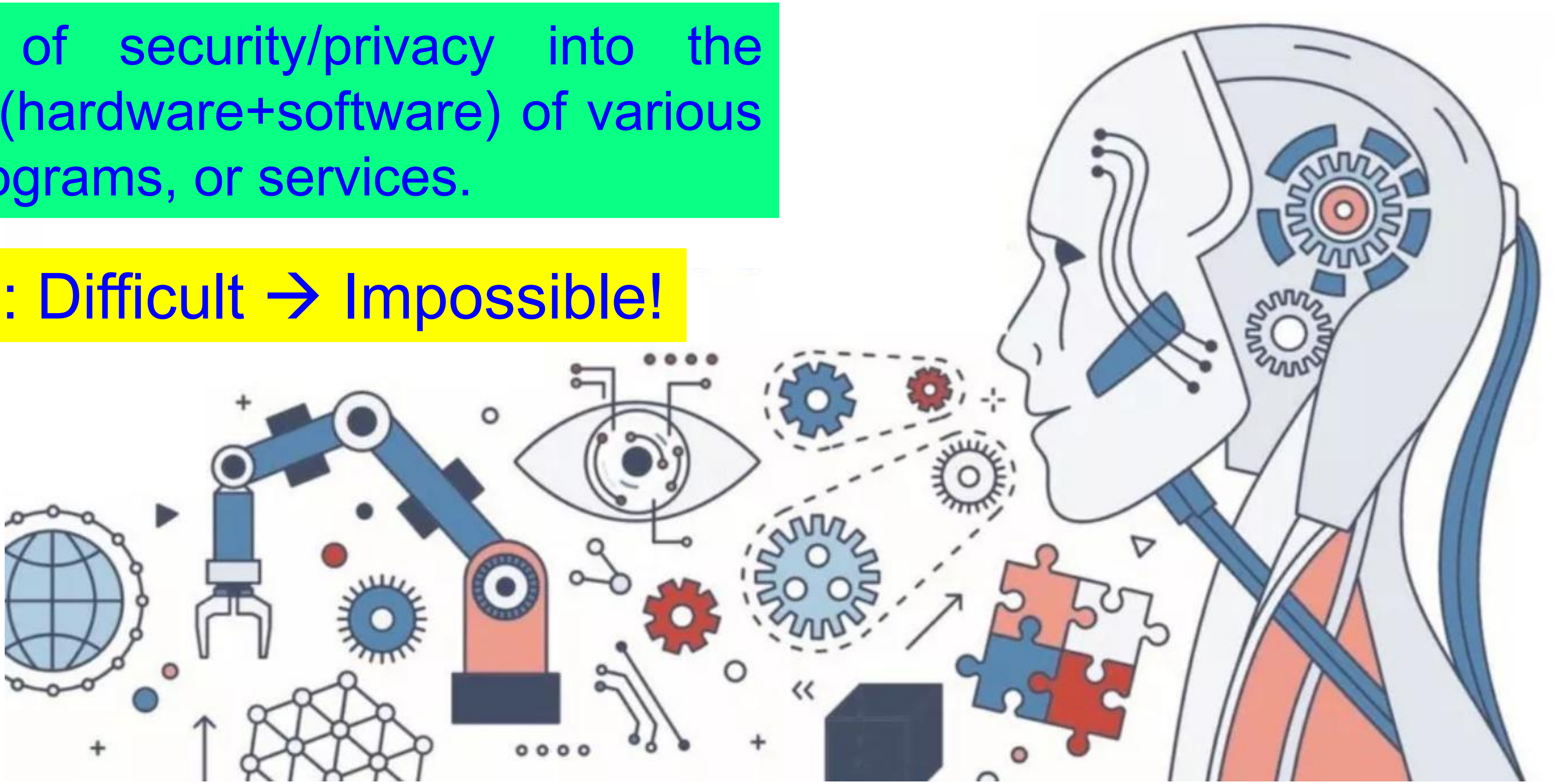
Source: Mohanty ICCE 2019 Keynote

Smart Cities
Vs
Smart Villages

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/

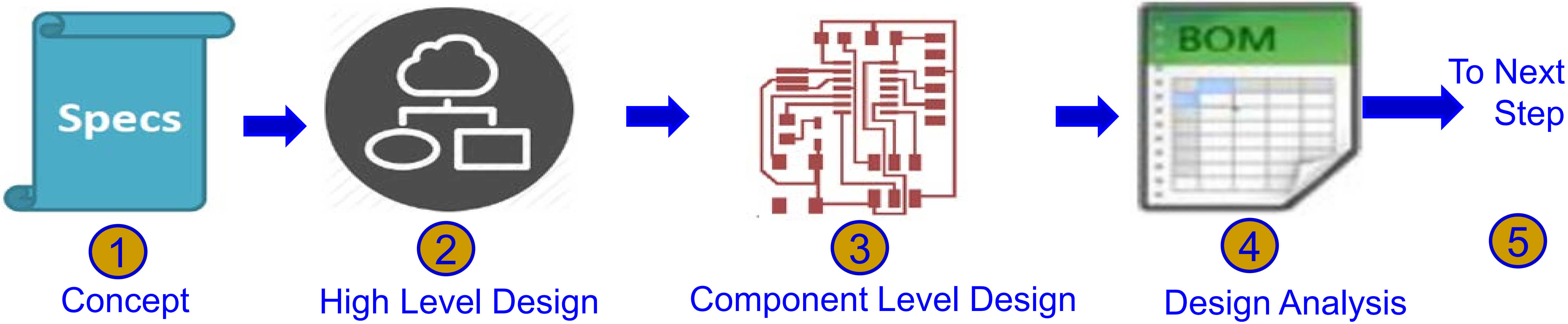
Security by Design (SbD)

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

SbD Principle – IoT/CPS Design Flow …



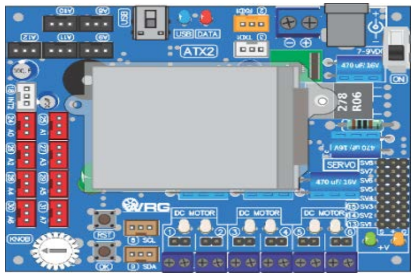
How to integrate cybersecurity and privacy at every stage of design flow?

Source: http://events.linuxfoundation.org/sites/events/files/slides/Design%20-%20End-to-End%20%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

SbD Principle – IoT/CPS Design Flow …

From Previous Step 4

Sensor and Component Assembly



Writing Device Drivers

Writing Application Programming Interface (APIs) for Cloud Infrastructure

Client Integration (Desktop, Tablet, Mobile)

To Next Step 6

5 Prototyping

How to integrate cybersecurity and privacy at every stage of design flow?

Source: http://events.linuxfoundation.org/sites/events/files/slides/Design%20-%20End-to-End%20%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

SbD Principle – IoT/CPS Design Flow

From Previous Step

5

6 Field Testing

7 Release of Beta Version

8 Production

9 Release and Documentation

How to validate and document cybersecurity and privacy features at every stage of production?

Source: http://events.linuxfoundation.org/sites/events/files/slides/Design%20-%20End-to-End%20%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

A Specific SbD Approach: 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

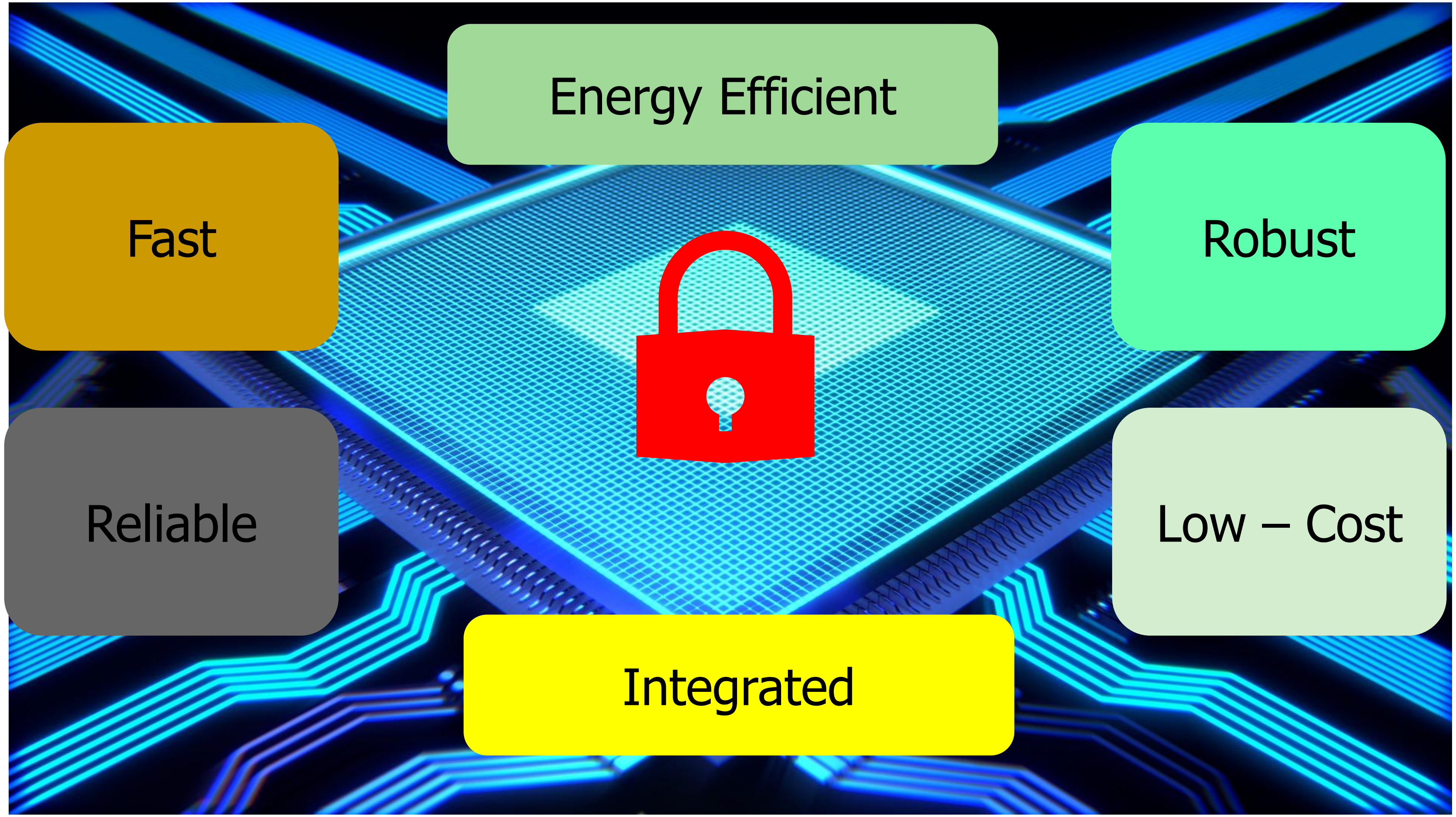
Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

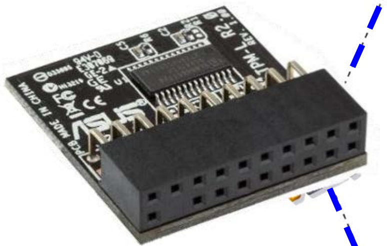
Source: E. Kougianos, S. P. Mohanty, and R. N. Mahapatra, "Hardware Assisted Watermarking for Multimedia", Special Issue on Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia, Elsevier International Journal on Computers and Electrical Engineering, Vol 35, No. 2, Mar 2009,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

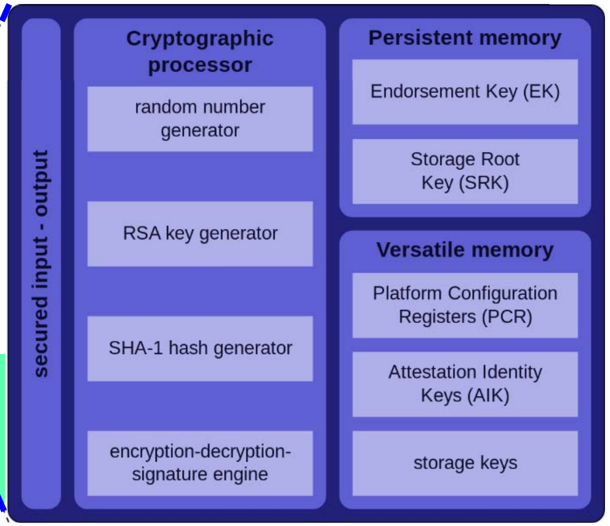
SbD/HAS - Advantages



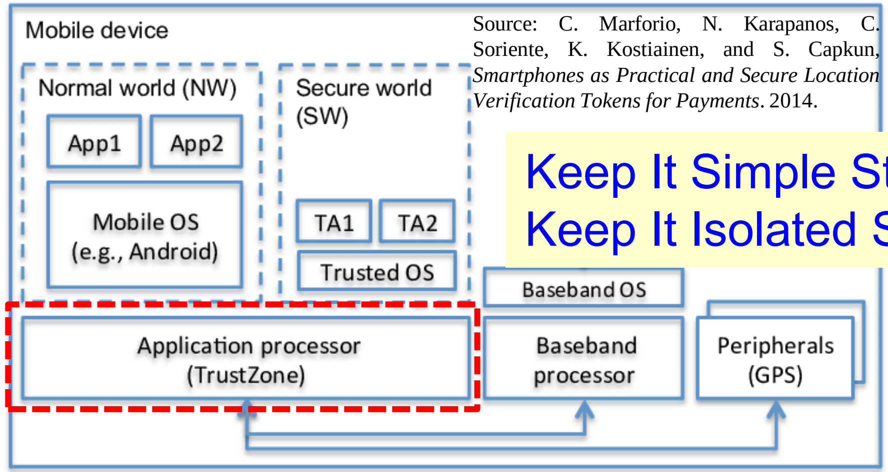
SbD/HAS Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



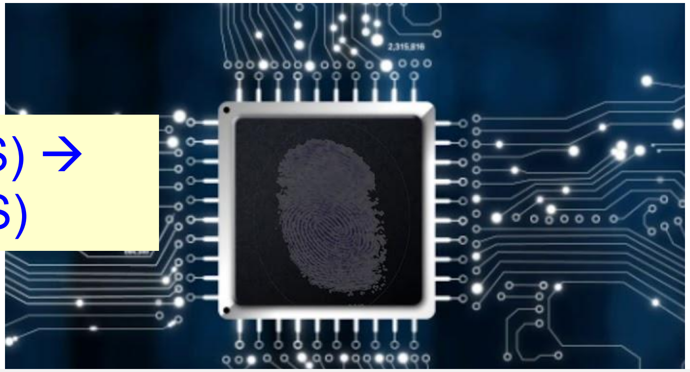


Trusted Platform Module (TPM)



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

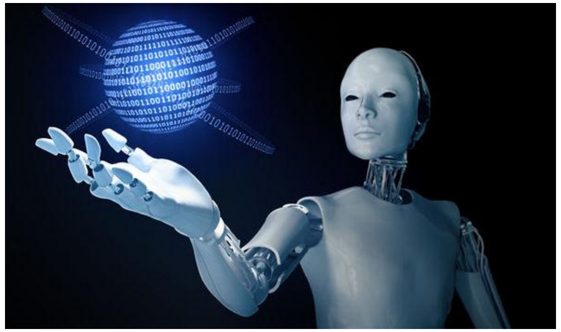
Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)



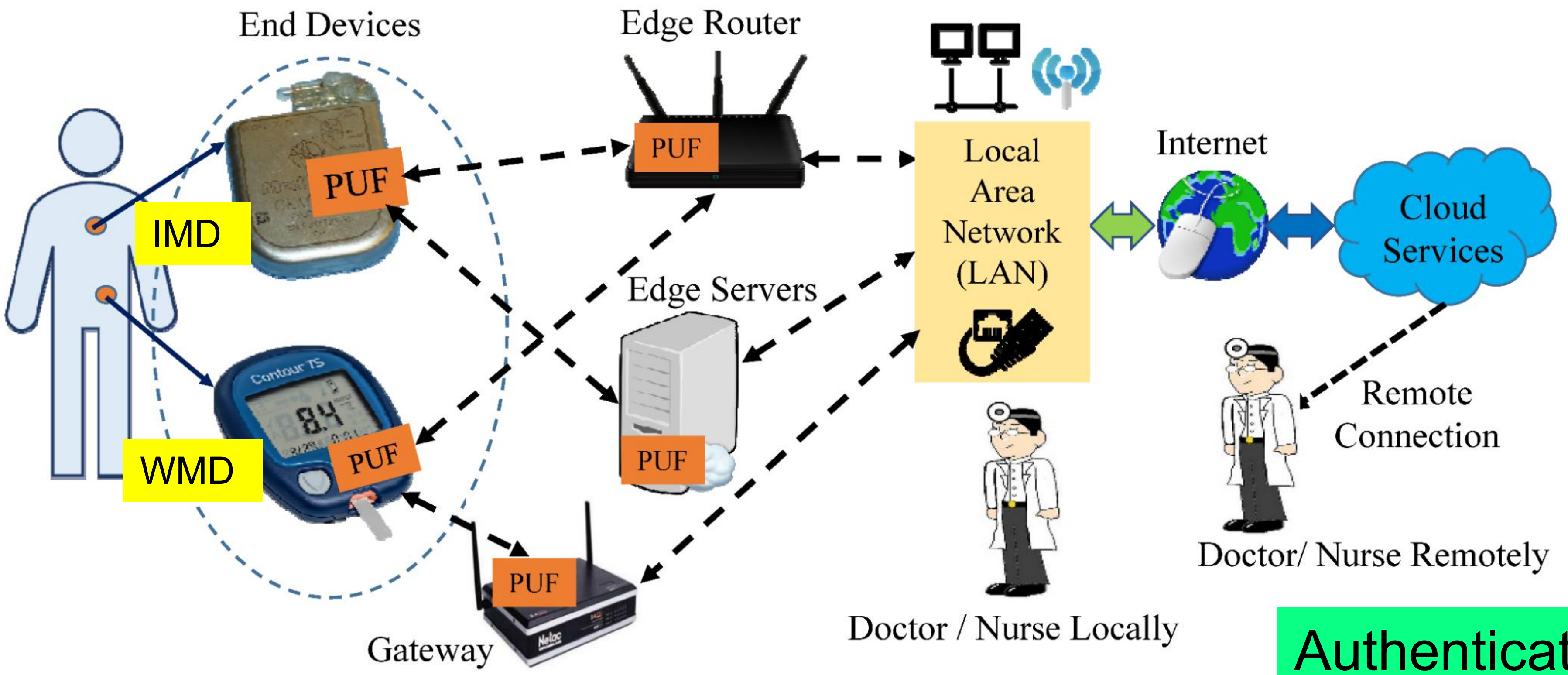
Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

Security-by-Design (SbD) – Specific Examples



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

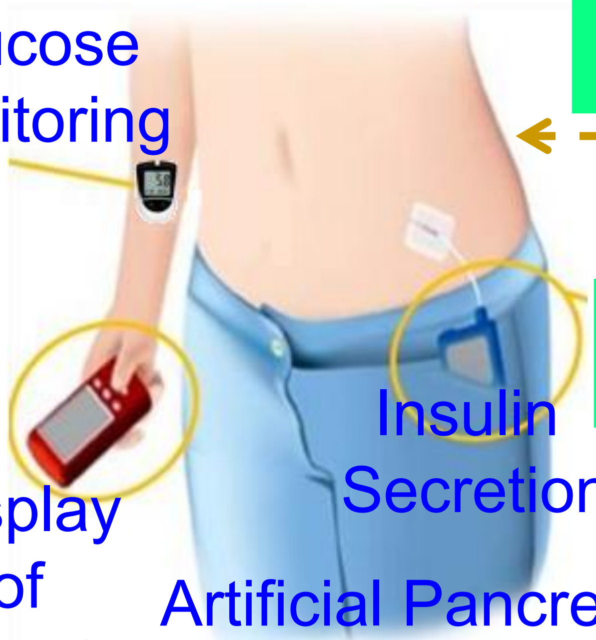


Authenticates Time - 1 sec
Power Consumption - 200 μW

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.

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

Continuous Glucose Monitoring



Privacy-Assured Health Data Storage

Security-Assured System

Cloud Storage

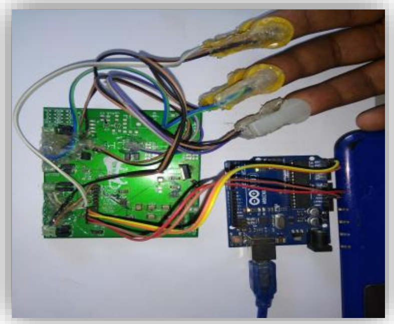
Hospital

Doctor

Display of Parameters

Insulin Secretion

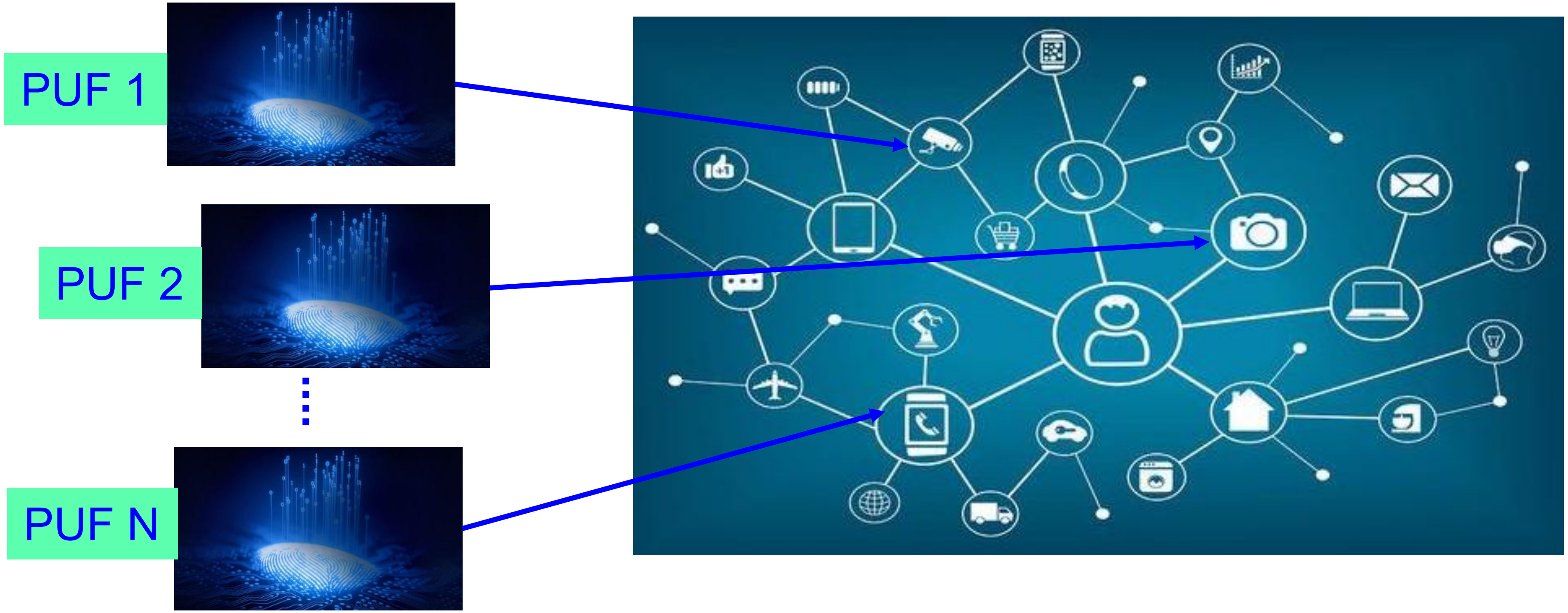
Artificial Pancreases System (APS)



Near Infrared (NIR) based Noninvasive, Accurate, Continuous Glucose Monitoring

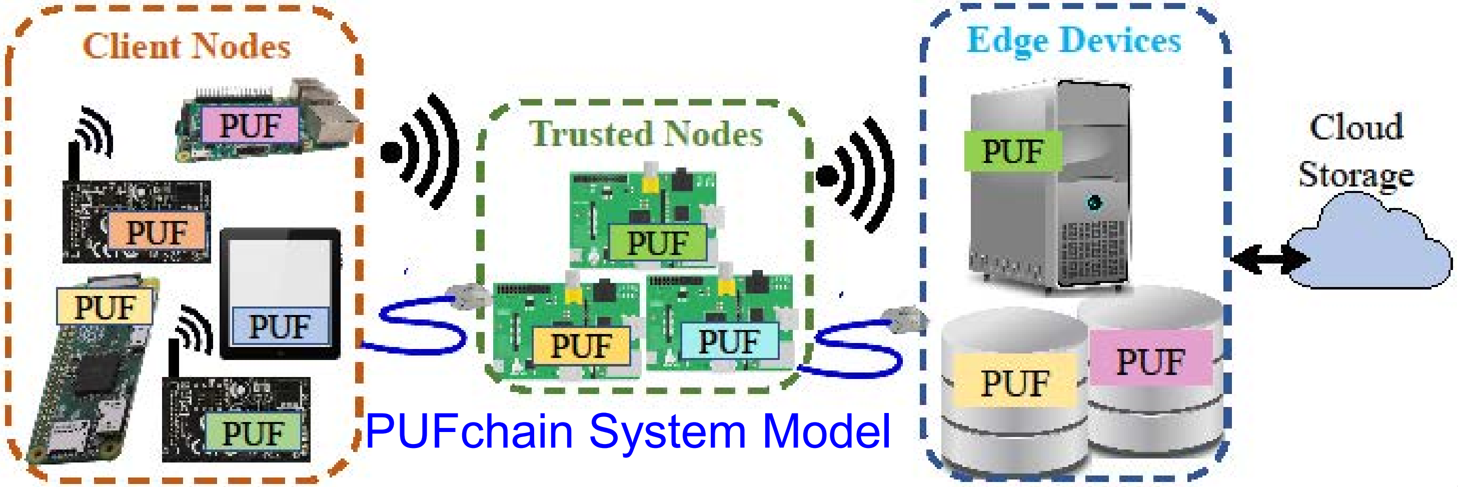
P. Jain, A. M. Joshi, and S. P. Mohanty, “iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare”, *IEEE Consumer Electronics Magazine (MCE),* Vol. 9, No. 1, January 2020, pp. 35–42.

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



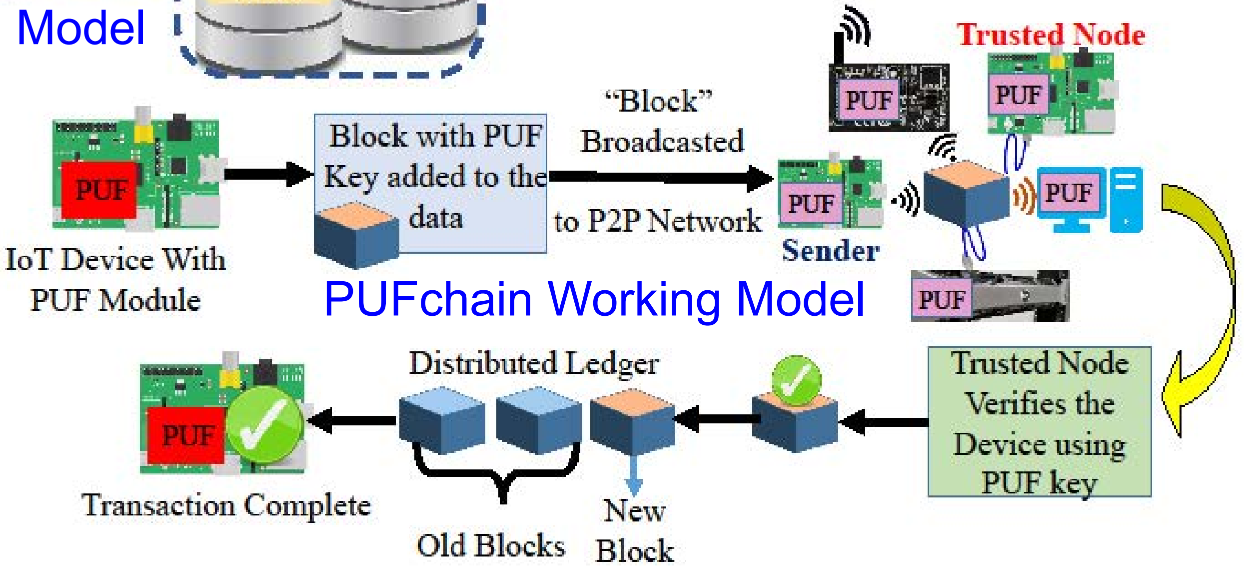
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security



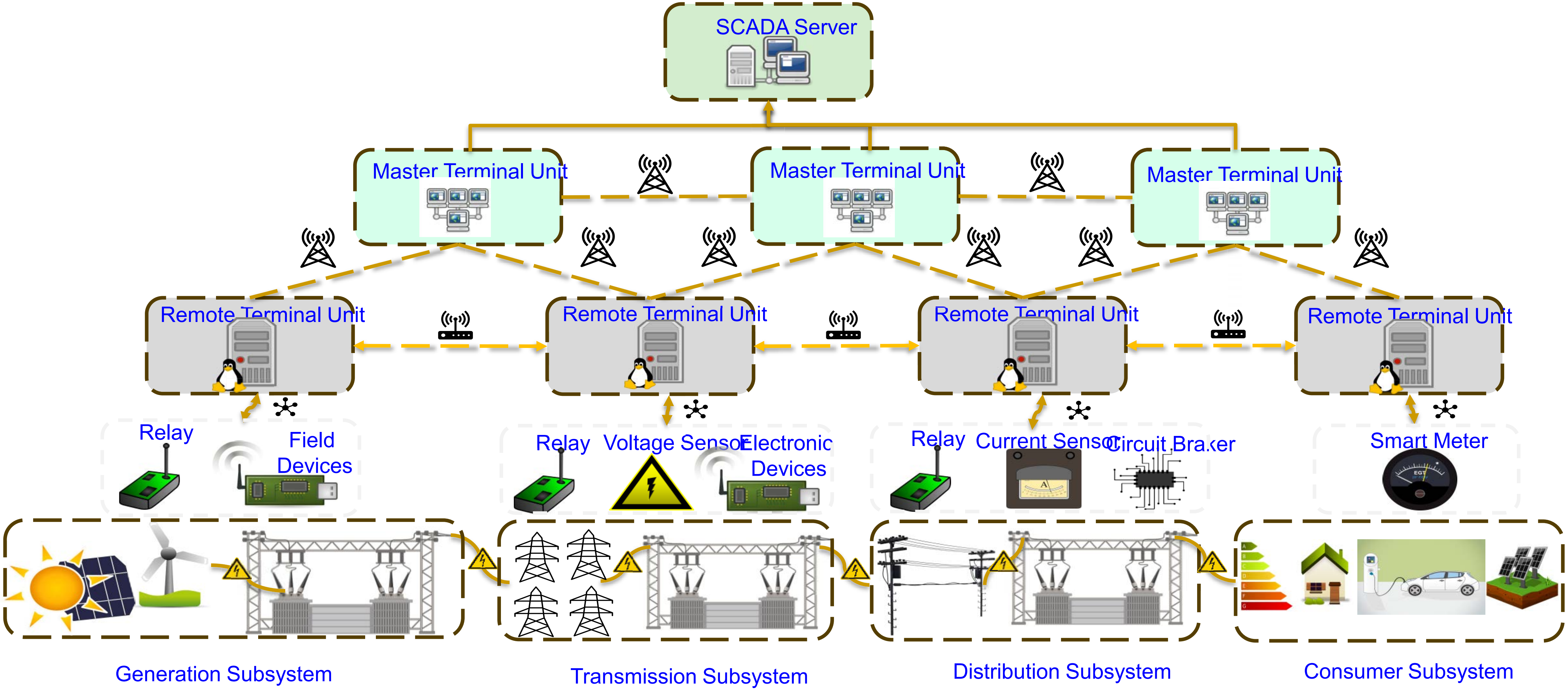
PUFchain Working Model

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

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

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

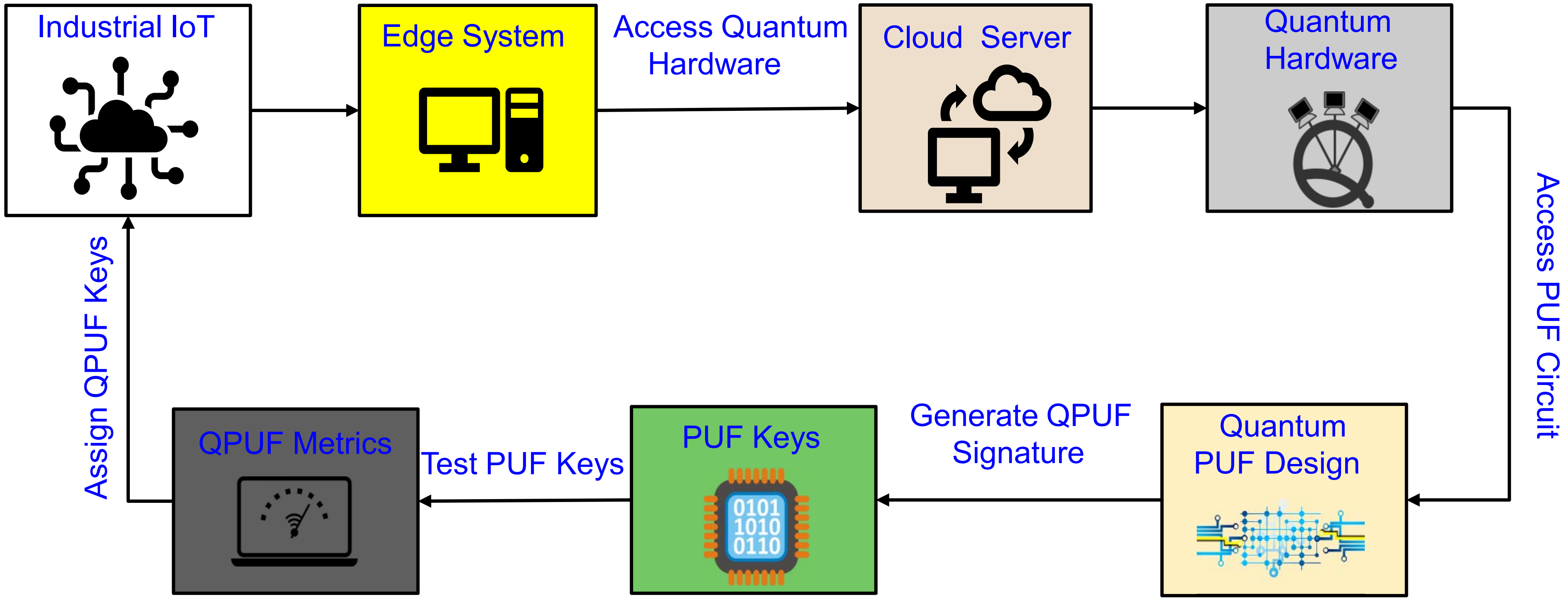
Smart Grid Cybersecurity



Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, C. Pan, and E. Kougianos, "QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems", *arXiv Quantum Physics*, arXiv:2410.12702, Oct 2024, 26-pages.

Serial/Wireless Wide Area Network Wireless Connection/LAN

Our QPUF: Quantum PUF for SbD of Industrial IoT

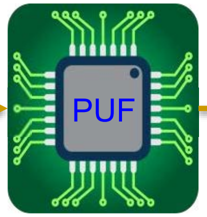


Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, C. Pan, and E. Kougianos, "QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2023, pp. 296--301, DOI: https://doi.org/10.1109/iSES58672.2023.00067.

Our QPUF 2.0 …

IC

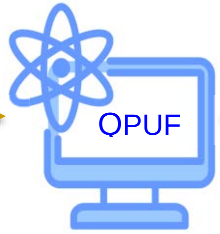
Challenge (C) → Response (R)



C	R
101101011	101001010
111001010	001101011
101001000	110110100
000101110	101110010

Quantum Computer

Initialization (I) → Response (R)

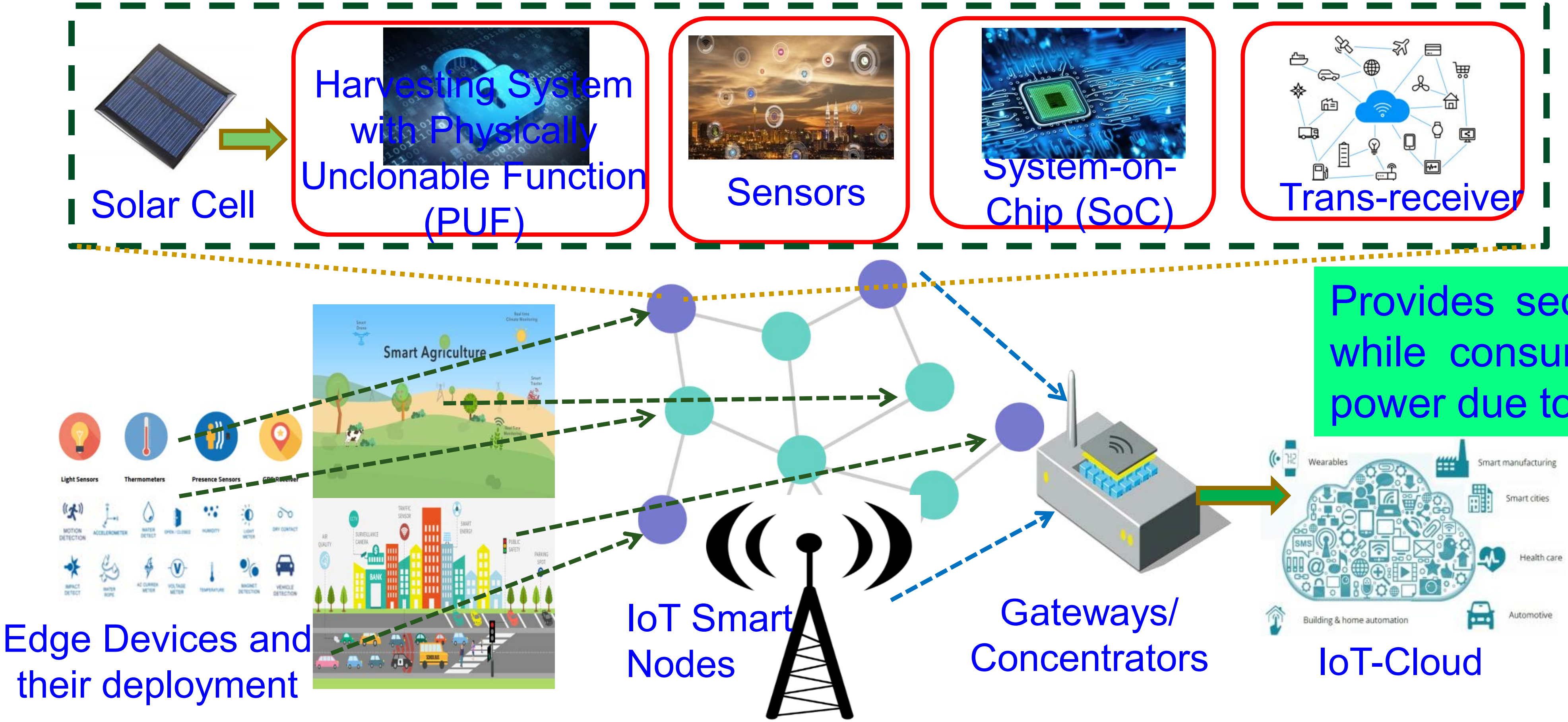


I→(Angle, Quantum State (0|1)) R→1010010

$$I1 \rightarrow \left(\frac{\pi}{2},0\right) \left(\frac{\pi}{2},1\right) \left(\frac{\pi}{2},0\right) \left(\frac{\pi}{2},1\right) \rightarrow R1 \quad I2 \rightarrow \left(\frac{\pi}{5},1\right) \left(\frac{\pi}{5},1\right) \left(\frac{\pi}{5},0\right) \left(\frac{\pi}{5},0\right) \rightarrow R2 \;\text{--------}\; In \rightarrow \left(\frac{\pi}{4},1\right) \left(\frac{\pi}{4},0\right) \left(\frac{\pi}{4},1\right) \left(\frac{\pi}{4},0\right) \rightarrow Rn$$

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, C. Pan, and E. Kougianos, "QPUF 2.0: Exploring Quantum Physical Unclonable Functions for Security-by-Design of Energy Cyber-Physical Systems", *arXiv Quantum Physics*, arXiv:2410.12702, Oct 2024, 26-pages.

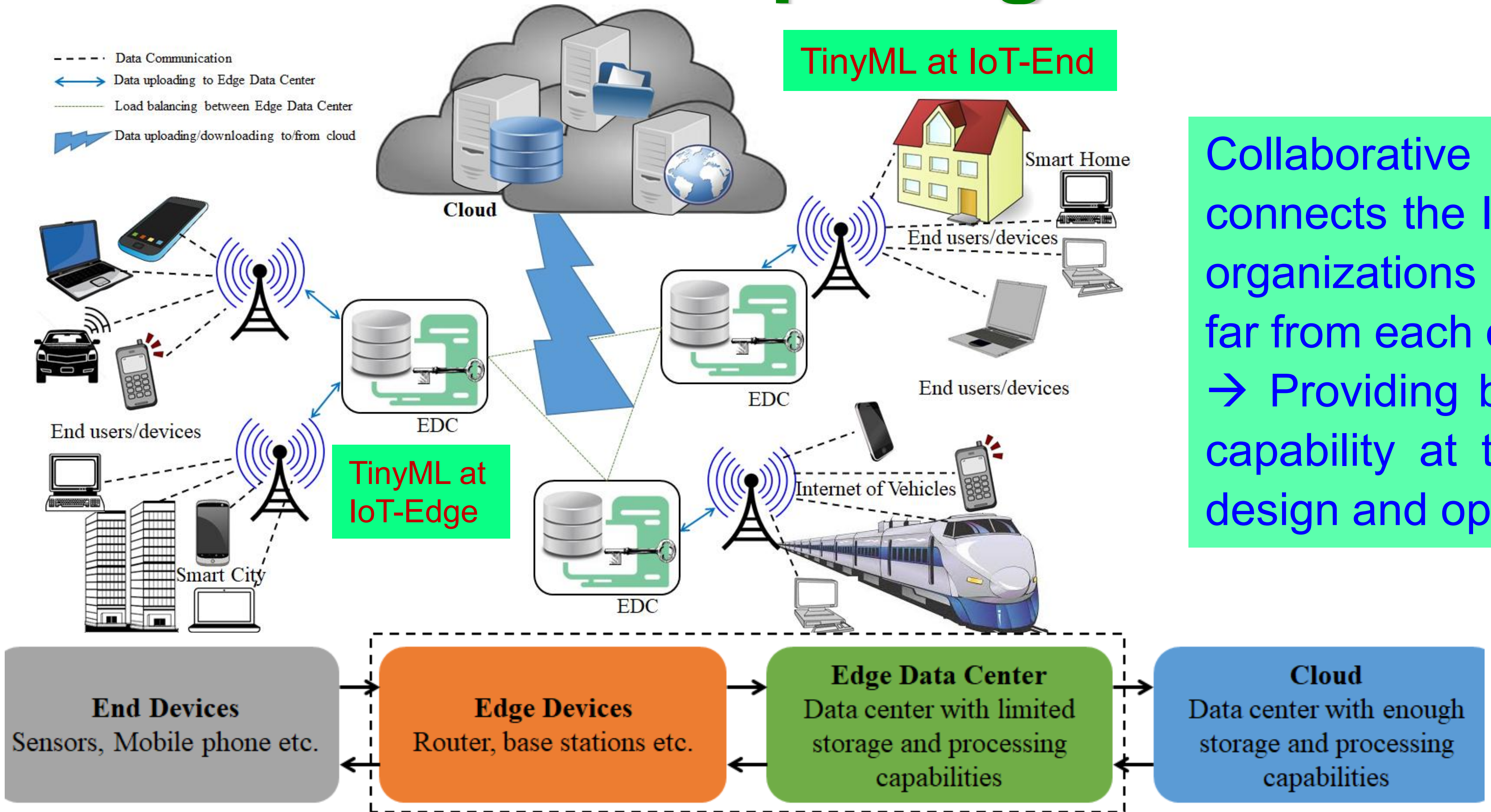
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge



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, DOI: https://doi.org/10.1109/TSUSC.2020.2987616.

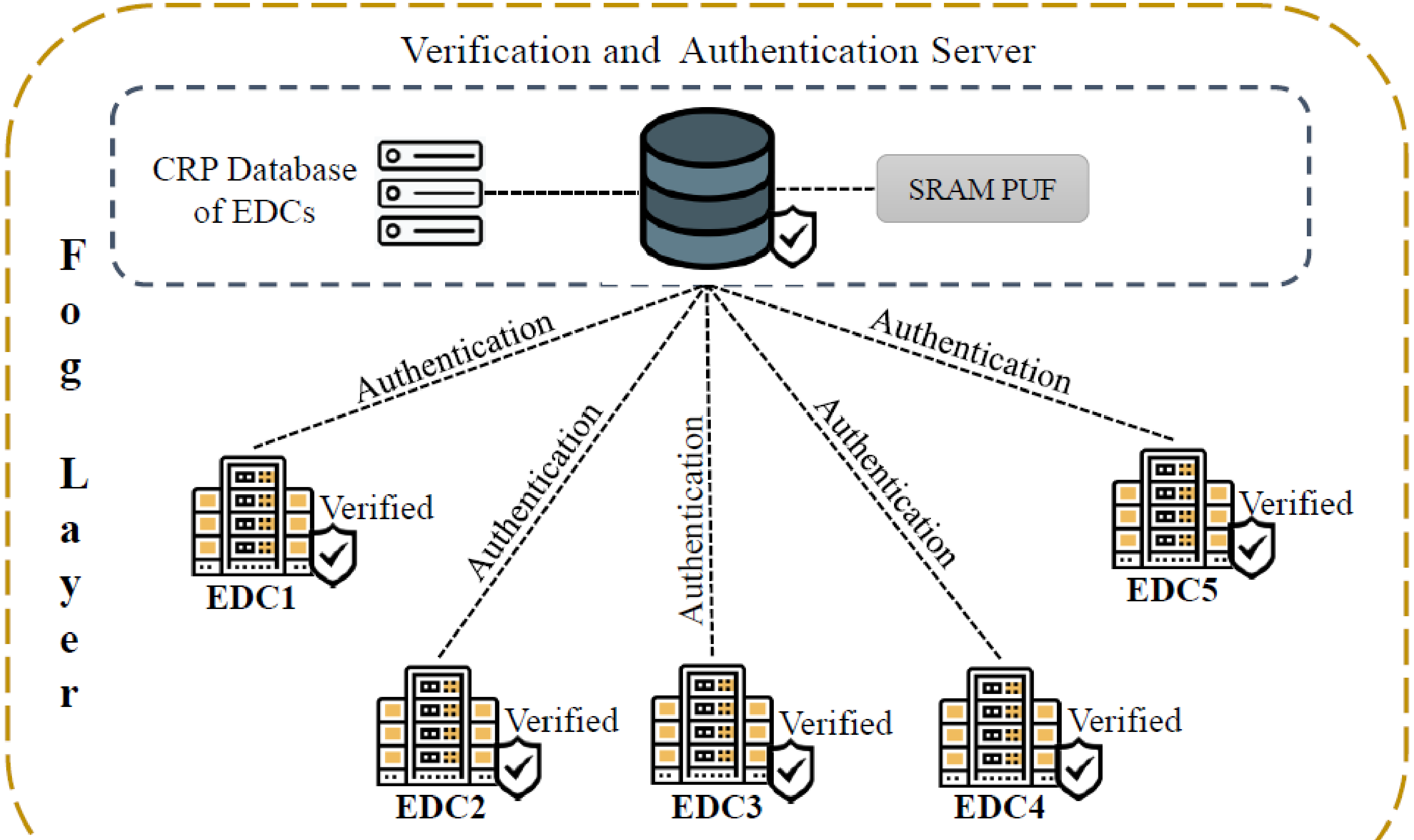
Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



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, DOI: https://doi.org/10.1109/MCOM.2018.1700795.

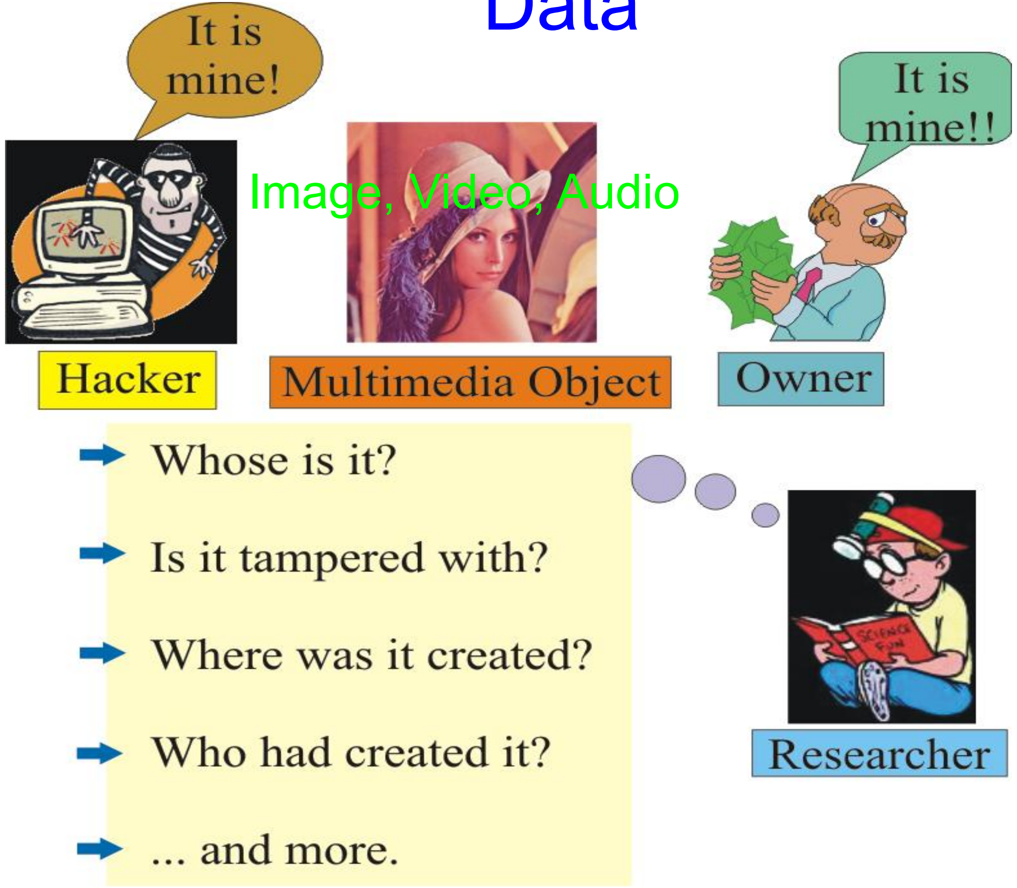
Our Fortified-Edge: PUF based Authentication in Collaborative Edge Computing



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.

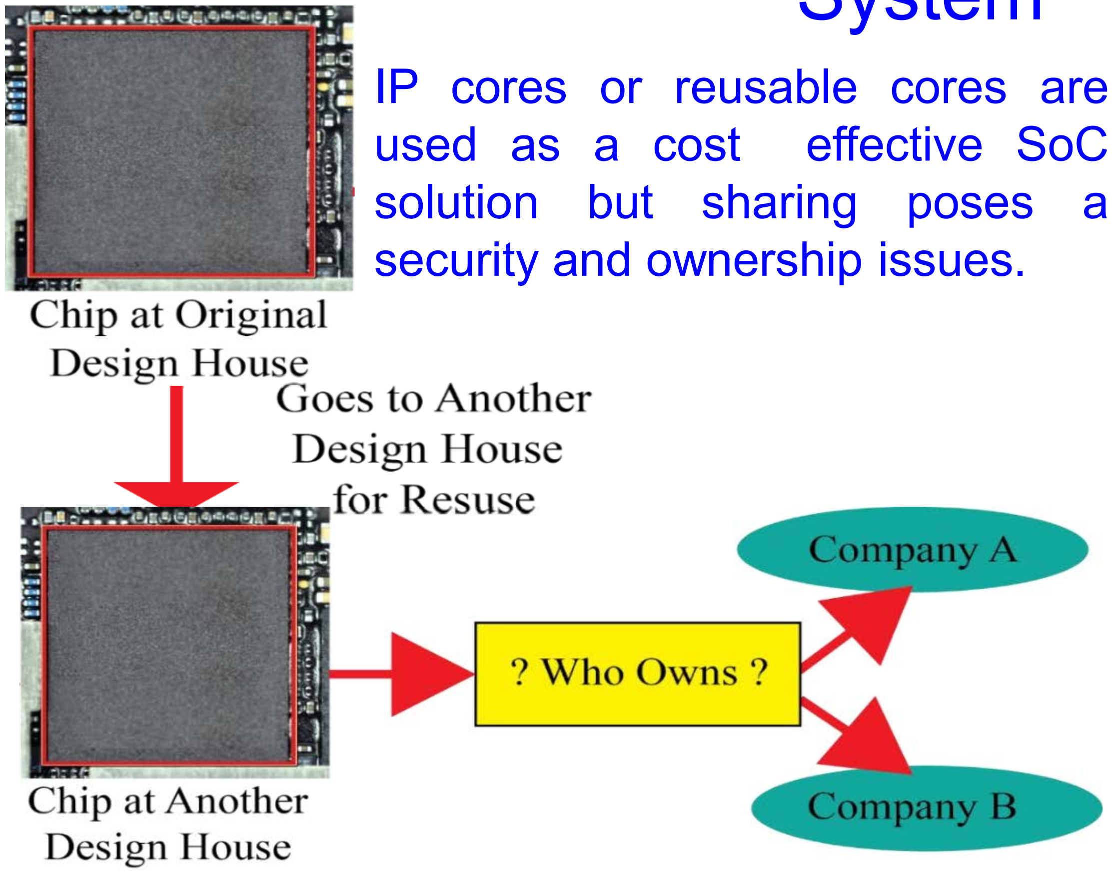
Data and System Authentication and Ownership Protection – My 20 Years of Experiences

Data



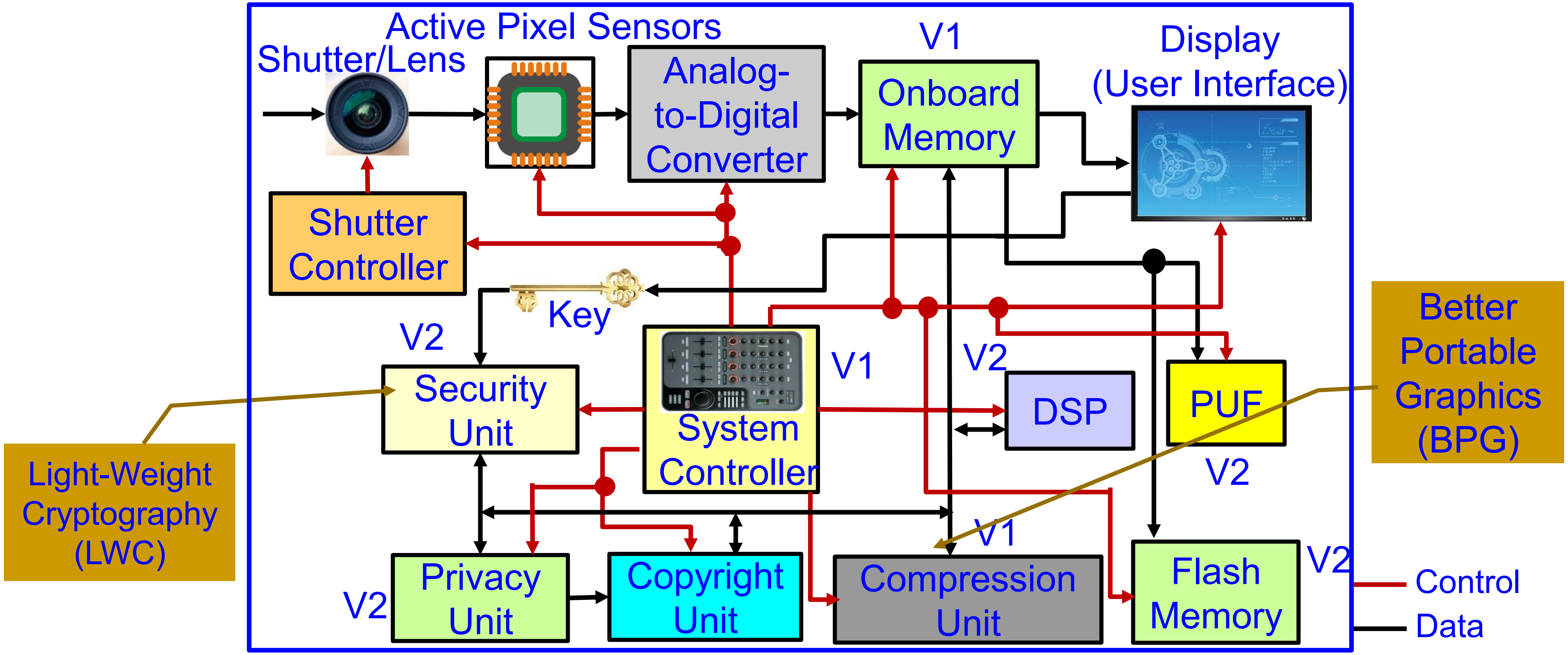
System

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.

Secure Digital Camera (SDC) – My Invention

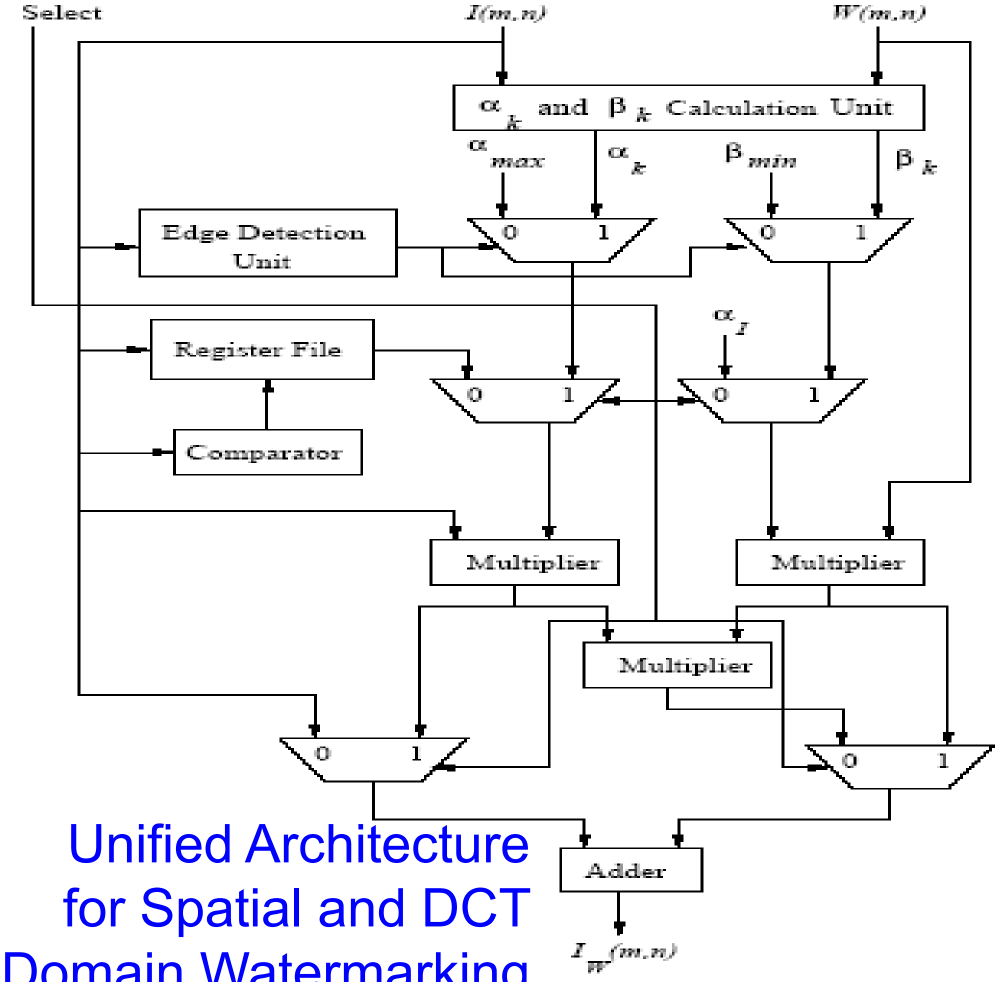


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

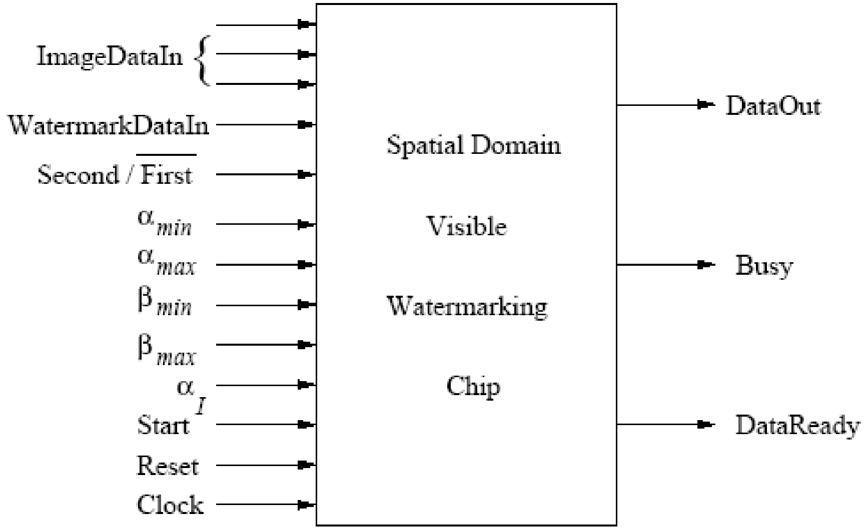
Security and/or Privacy by Design (SbD and/or PbD)

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.

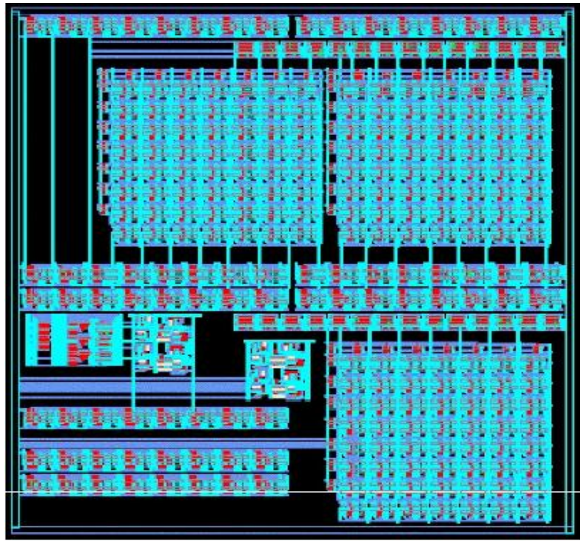
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

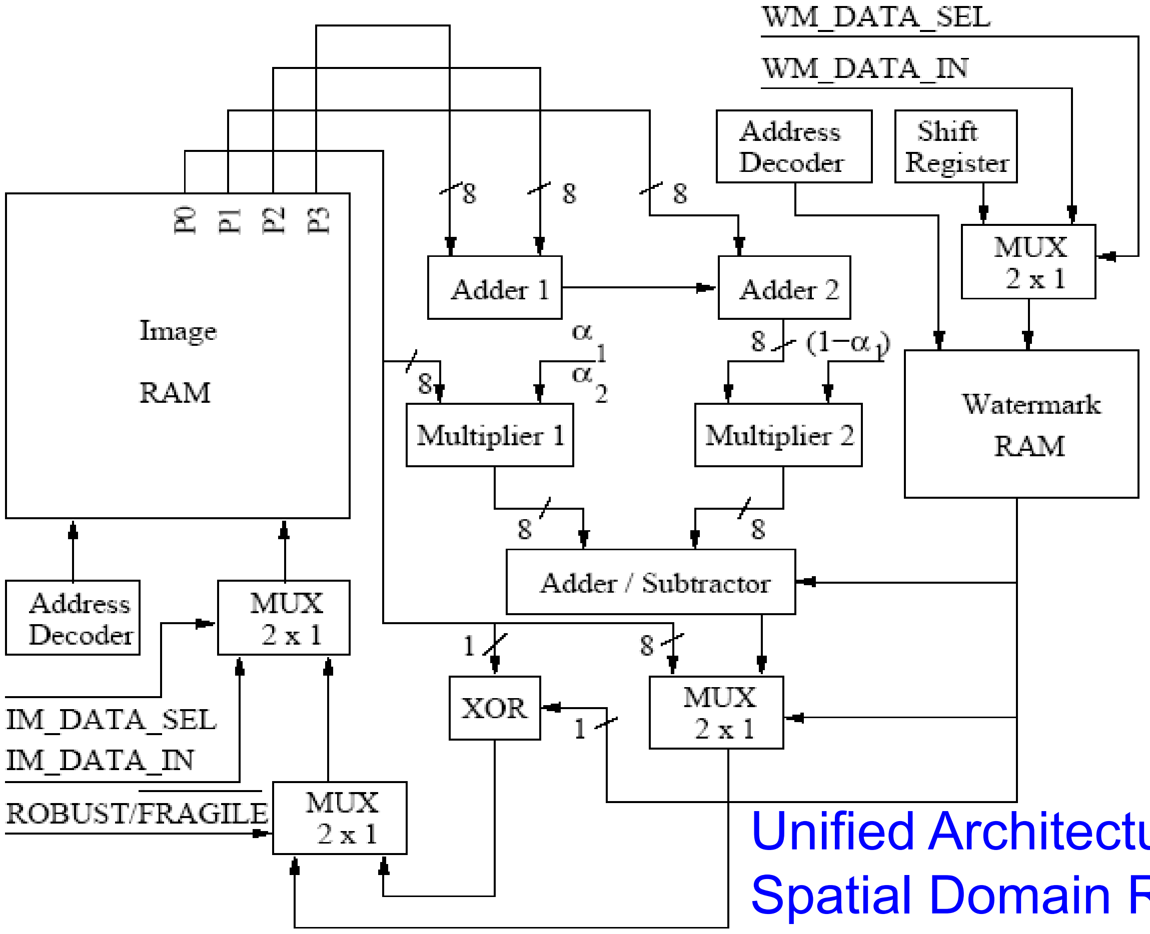
Chip Design Data

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

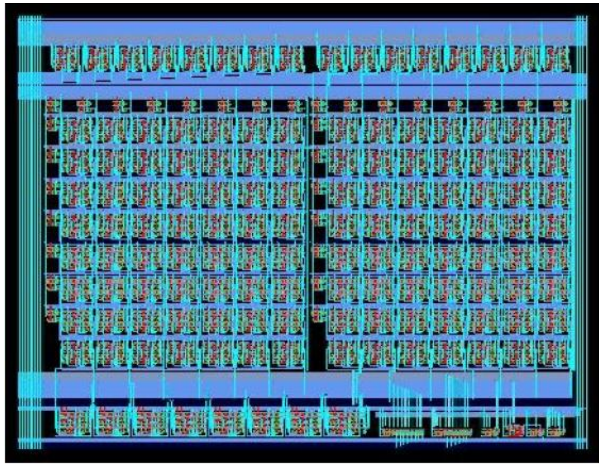
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

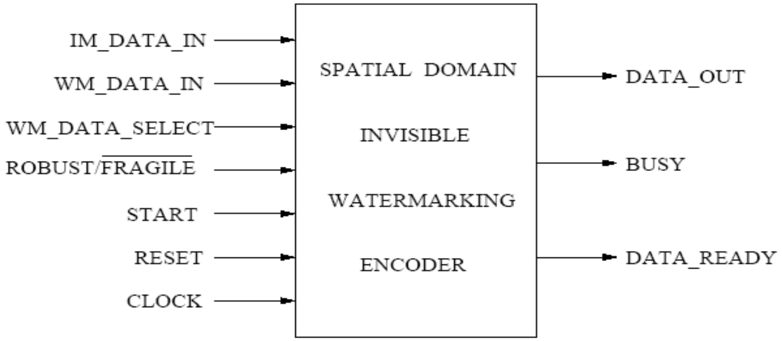
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

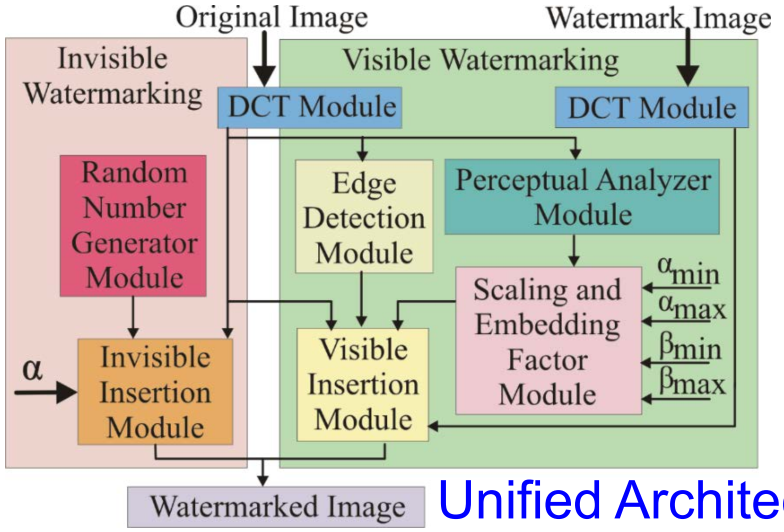
Chip Design Data

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

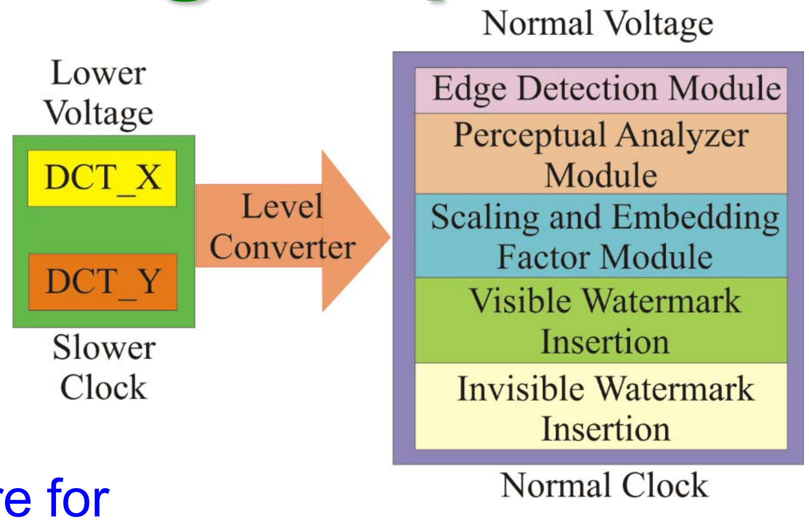
Power Consumption: 2.0 mW, Frequency: 500 MHz

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

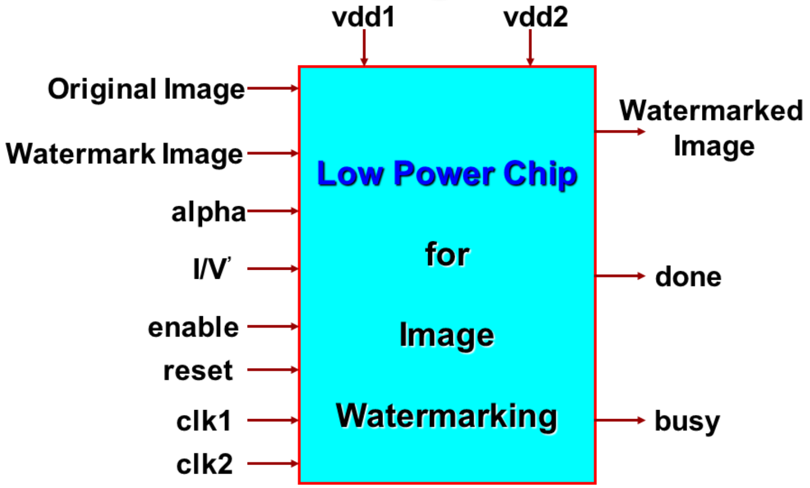
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



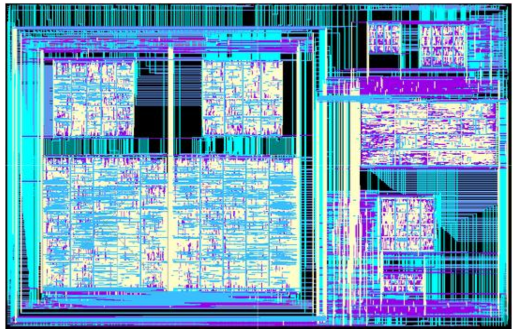
Unified Architecture for DCT Domain Watermarking



DVDF Low-Power Design



Pin Diagram



Chip Layout

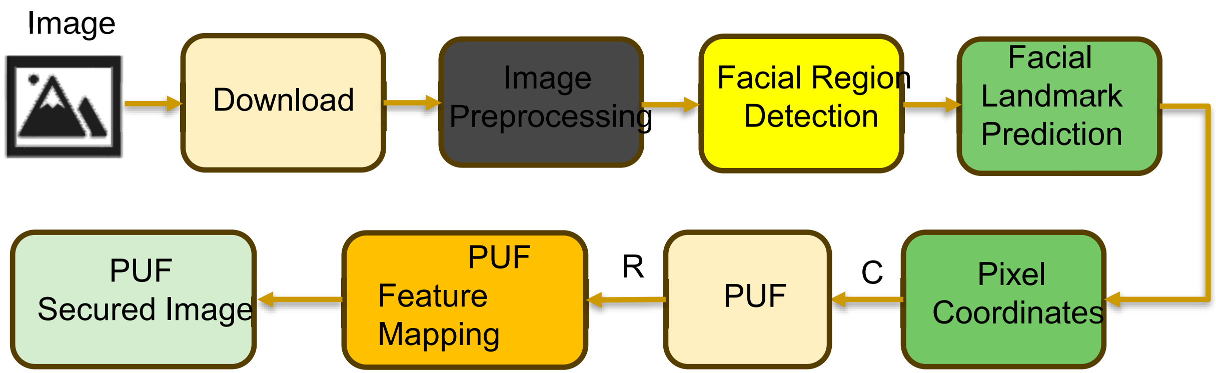
Chip Design Data

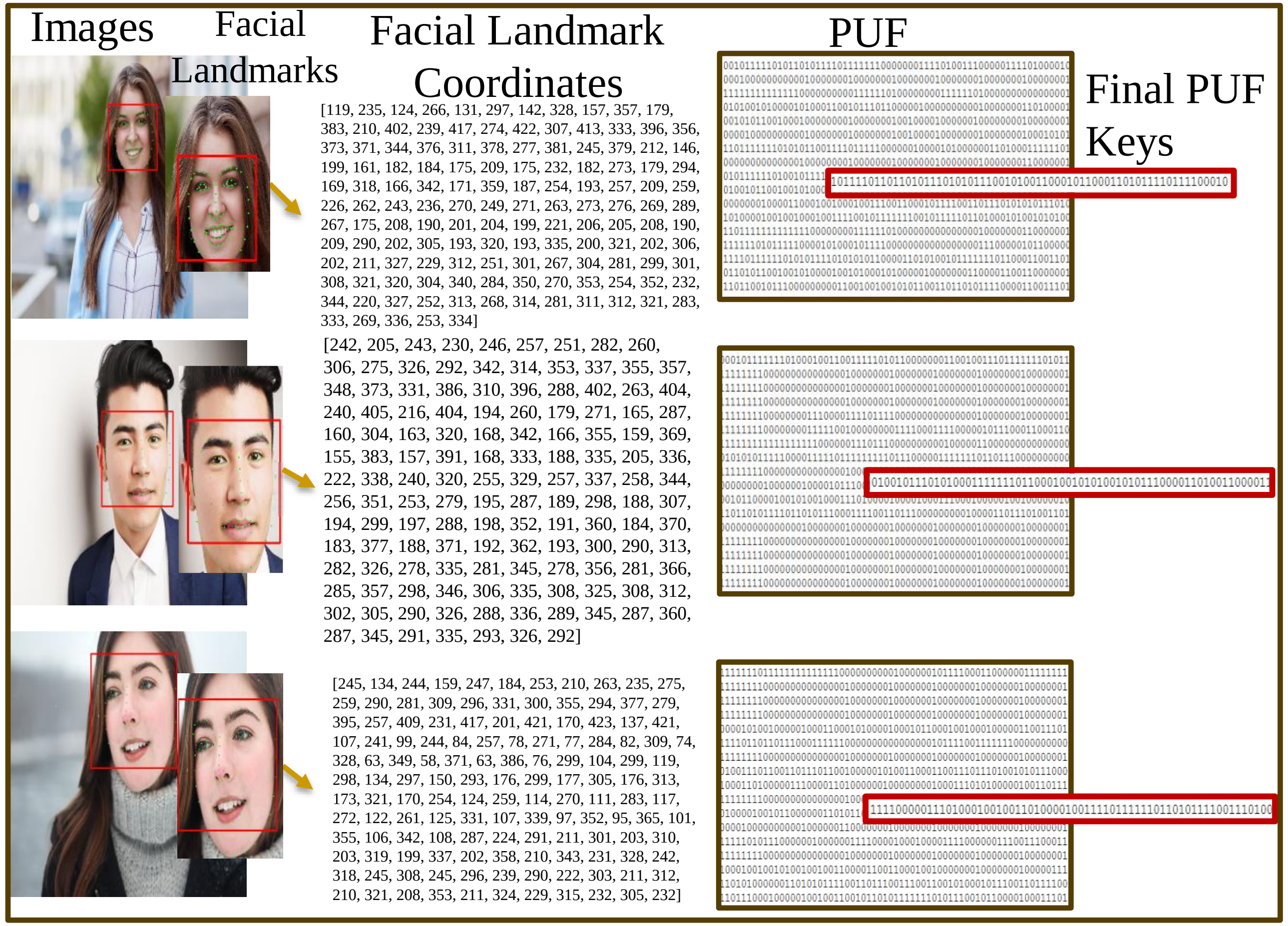
Total Area : 16.2 sq mm, No. of Transistors: 1.4 million

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.

Our PUFshield: for Deepfake Mitigation Through PUF-Based Facial Feature Attestation …





Source: V. K. V. V. Bathalapalli, V. P. Yanambaka, **S. P. Mohanty**, and E. Kougianos, "PUFshield: A Hardware-Assisted Approach for Deepfake Mitigation Through PUF-Based Facial Feature Attestation", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2024, pp. XXX--YYY, DOI: https://doi.org/10.1145/3649476.3660394.

Conclusion

Conclusion

- Cybersecurity is important problem in IoT-driven Cyber-Physical Systems (CPS) that build smart systems.
- 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, IIoT, 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): Cybersecurity provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system.

Future Directions

- Security by Design (PbD) needs significant research.
- Cybersecurity, Privacy, IP Protection of Information, Device, 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 IoT and CPS with integrated cybersecurity features can provide robust solutions.
- More research is needed for robust, low-overhead PUF design and protocols that can be integrated in any CPS.
- Cybersecurity solutions for the quantum computing era for system needs attention.