# Smart Healthcare - Cybersecurity Perspectives

**Fulbright Lecture 2023 – KL Deemed University**

**Guntur, India, 1-31 July 2023**

**Homepage**

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

# Outline

- Smart Healthcare – Introduction
- Smart Healthcare – Challenges
- Selected Cybersecurity Solutions for IoT/CPS
- Drawbacks of Existing Cybersecurity Solutions
- Security by Design (SbD) Principle
- Security by Design (SbD) Example Solutions
- Trustworthy Pharmaceutical Supply Chain
- Is PUF the Solution of Every Cybersecurity Problems?
- Is Blockchain the Solution of Every Cybersecurity Problems?
- Conclusions and Future Directions

# Smart Healthcare – Introduction

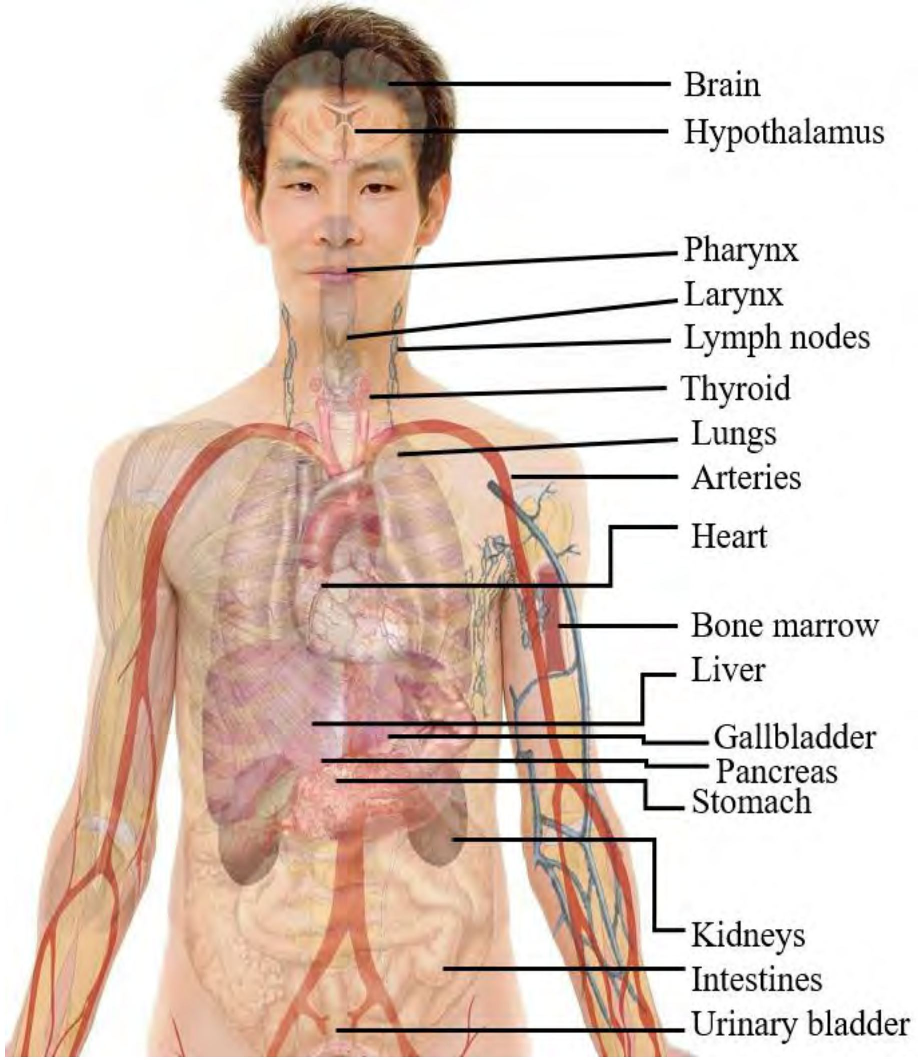
# Human Body and Health

## Human Body

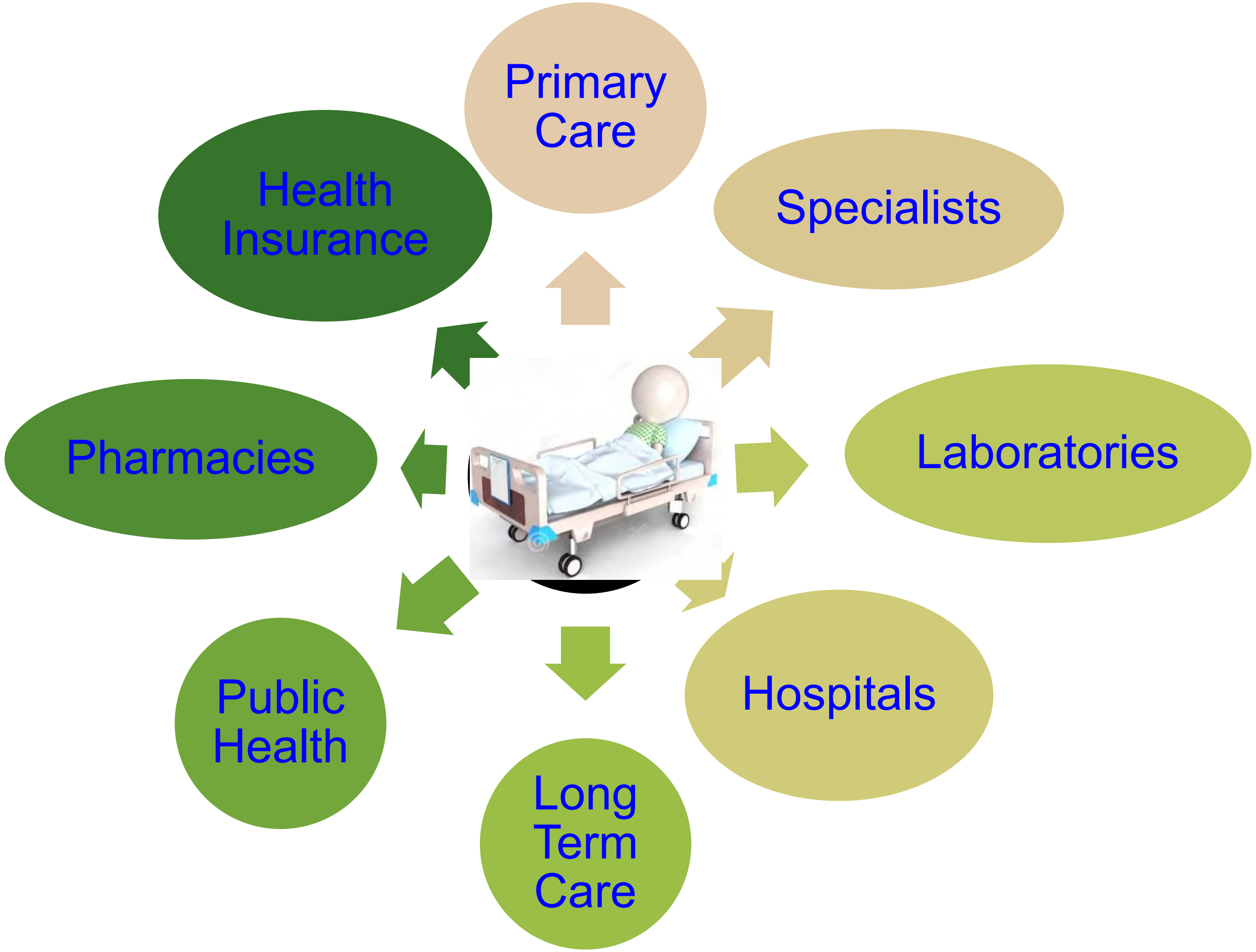
- From an engineering perspective - Human body can be defined as a combination of multi-disciplinary subsystems (electrical, mechanical, chemical …).

## Health

- Human health is a state of complete physical, mental and social well-being.



# Traditional Healthcare



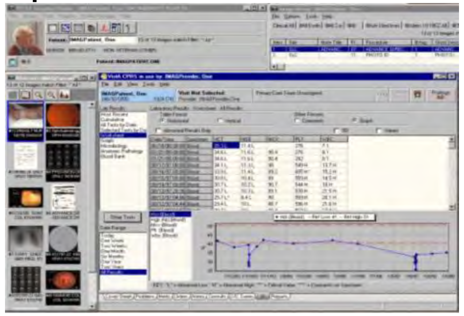

- Physical presence needed
- Deals with many stakeholders
- Stakeholders may not interact
- May not be personalized
- Not much active feedback
- Less effective follow-up from physicians

# Healthcare → Smart Healthcare

Healthcare

eHealth → Telemedicine → mHealth → cHealth → sHealth

**eHealth:** The use of information and communication technologies (ICT) to improve healthcare services.



**Telemedicine:** Telemedicine is the use of telecommunication and information technology to provide clinical healthcare from a distance.

**mHealth:** Healthcare supported by *mobile devices* that uses mobile telecommunications and multimedia technologies for the delivery of healthcare services and health information.

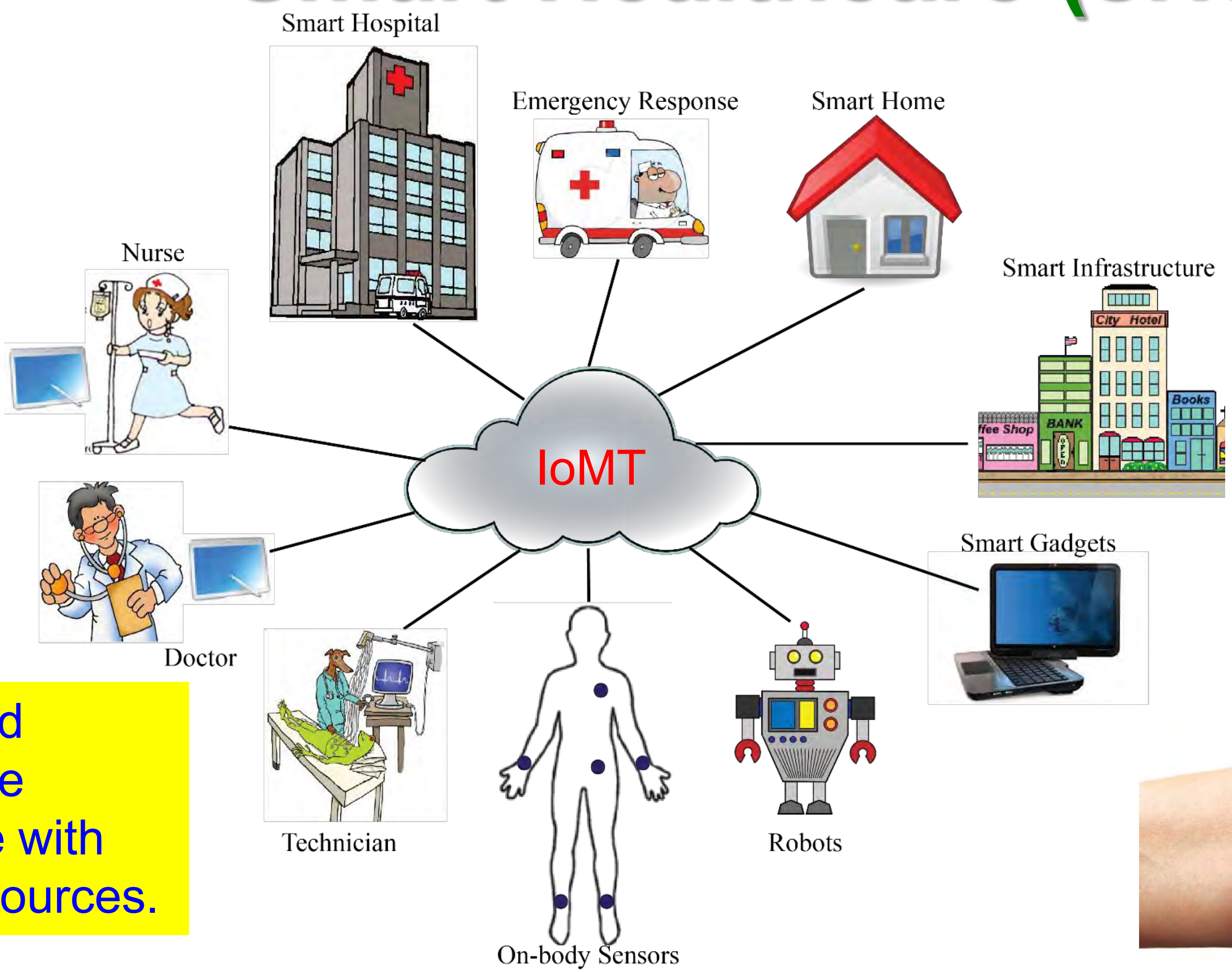
**cHealth**


**sHealth**


Embedded Skin Patches

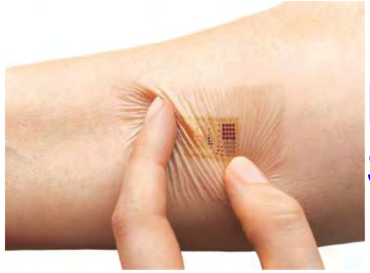
Source: **S. P. Mohanty**, "Smart Healthcare: From Healthcare to Smart Healthcare", ICCE 2020 Panel, Jan 2020.

# Smart Healthcare (sHealth)




Fitness Trackers

Headband with Embedded Neurosensors



Embedded Skin Patches

Quality and sustainable healthcare with limited resources.

Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 7, Issue 1, January 2018, pp. 18-28.

# What is Smart Healthcare?

Smart Healthcare ←
Conventional Healthcare
+ Body sensors
+ Smart Technologies
+ Information & Communication Technology (ICT)
+ AI/ML

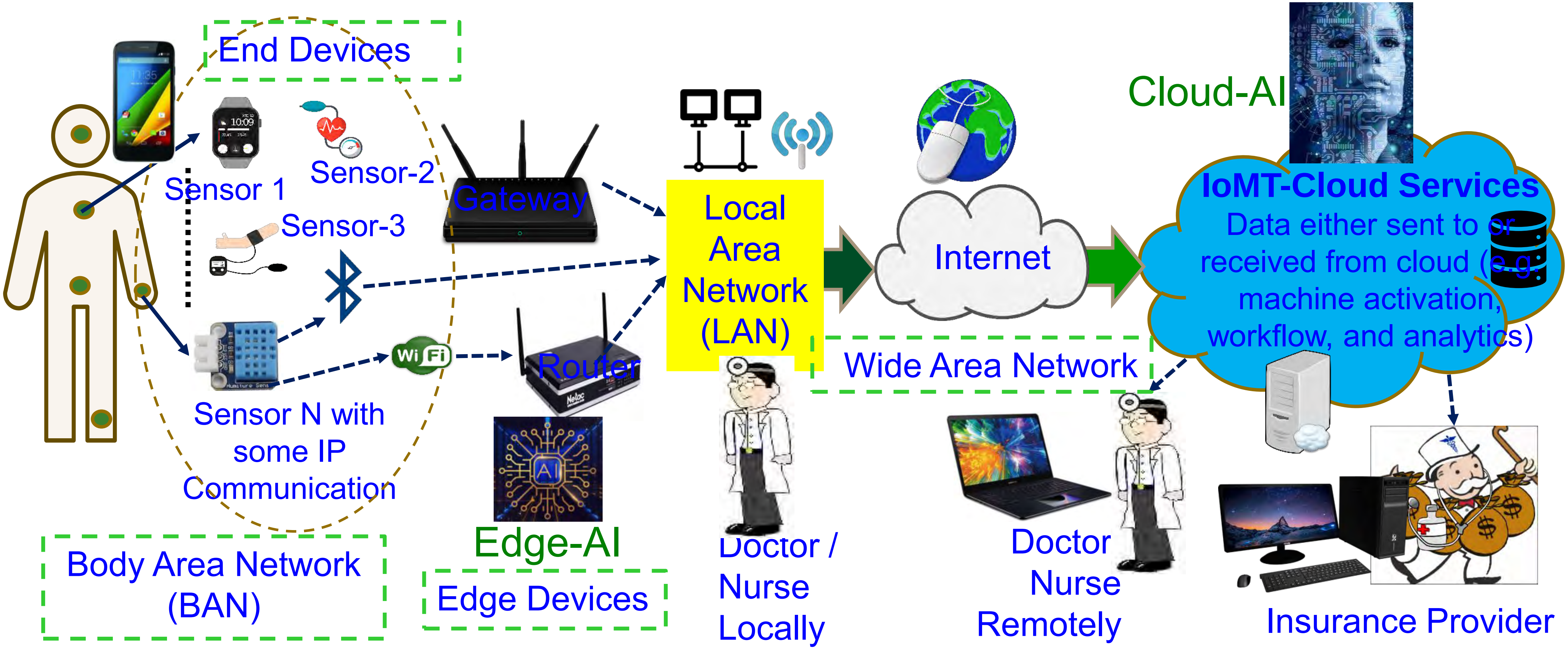
Internet of Medical Things (IoMT)

Internet of Health Things (IoHT)

Healthcare Cyber-Physical Systems (H-CPS)

Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care", *IEEE Consumer Electronics Magazine (MCE)*, Volume 7, Issue 1, January 2018, pp. 18-28.

# Smart Healthcare – Healthcare CPS

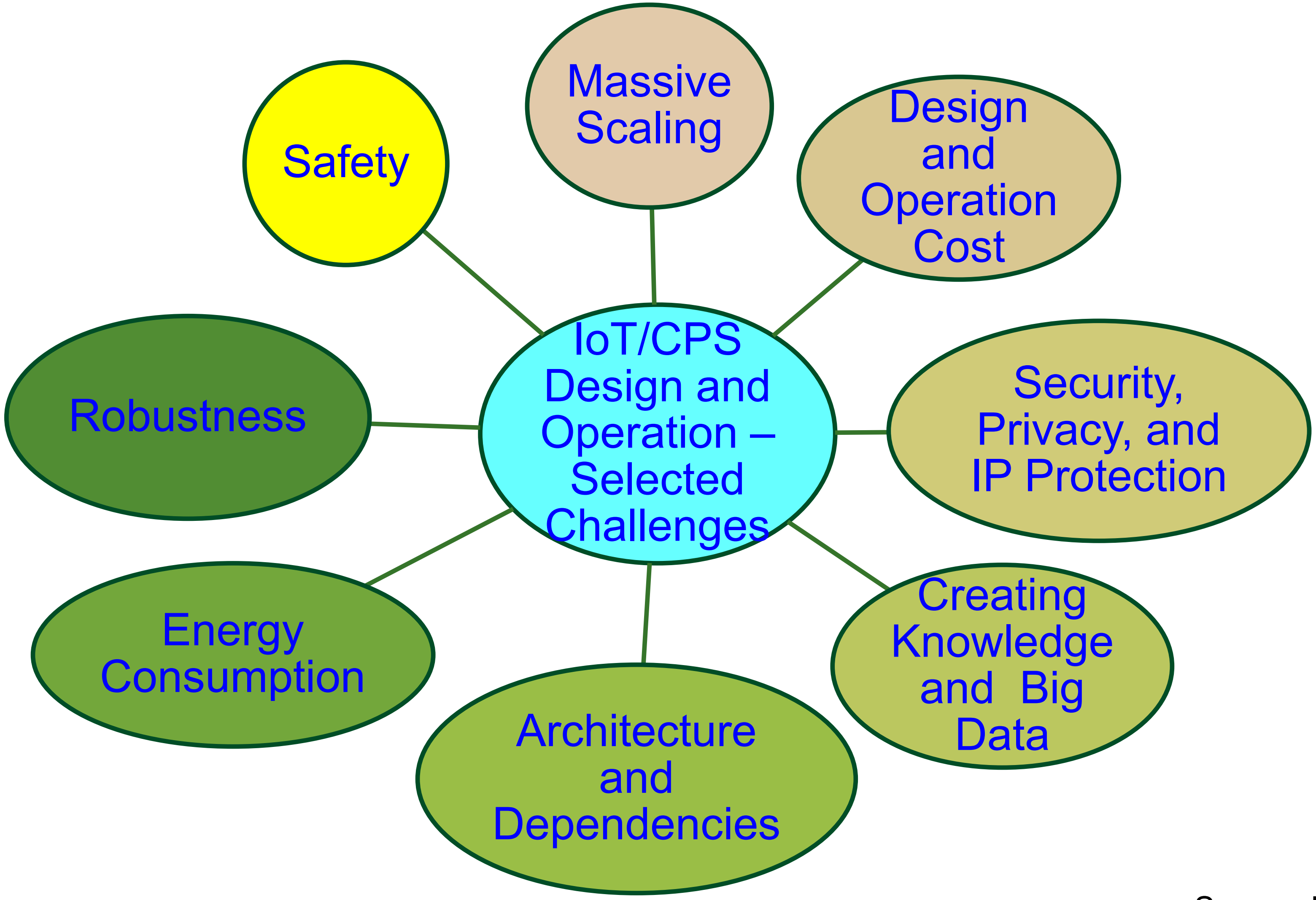



Frost and Sullivan predicts smart healthcare market value to reach US$348.5 billion by 2025.

Source: S. P. Mohanty, Secure IoT by Design, Keynote, 4th IFIP International Internet of Things Conference (IFIP-IoT), 2021, Amsterdam, Netherlands, 5th November 2021.

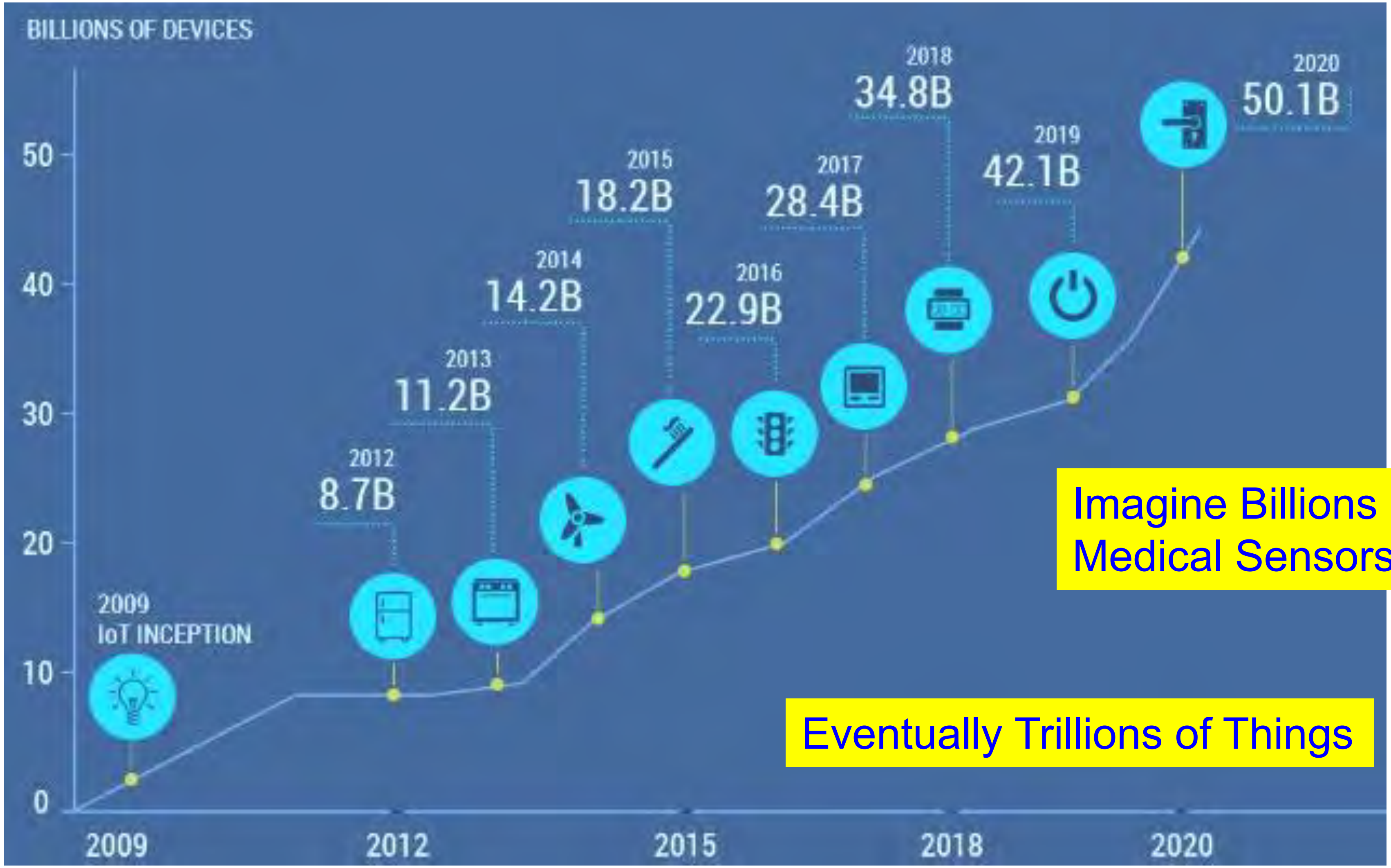
# Smart Healthcare – Some Challenges

# IoT/CPS – Selected Challenges




Source: Mohanty ICIT 2017 Keynote

# Massive Growth of Sensors/Things




Imagine Billions of user with Medical Sensors!

Eventually Trillions of Things

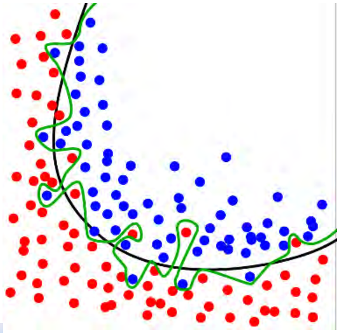
Source: https://www.linkedin.com/pulse/history-iot-industrial-internet-sensors-data-lakes-0-downtime

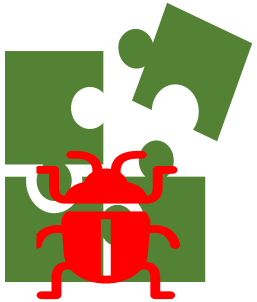
# Challenges of Data in IoT/CPS are Multifold

# AI/ML Modeling Challenges


Machine Learning Issues

- High Energy Requirements
- High Computational Resource Requirements
- Large Amount of Data Requirements
- Underfitting and Overfitting Issue
- Class Imbalance Issue
- Fake Data Issue
- Attack on Training Process

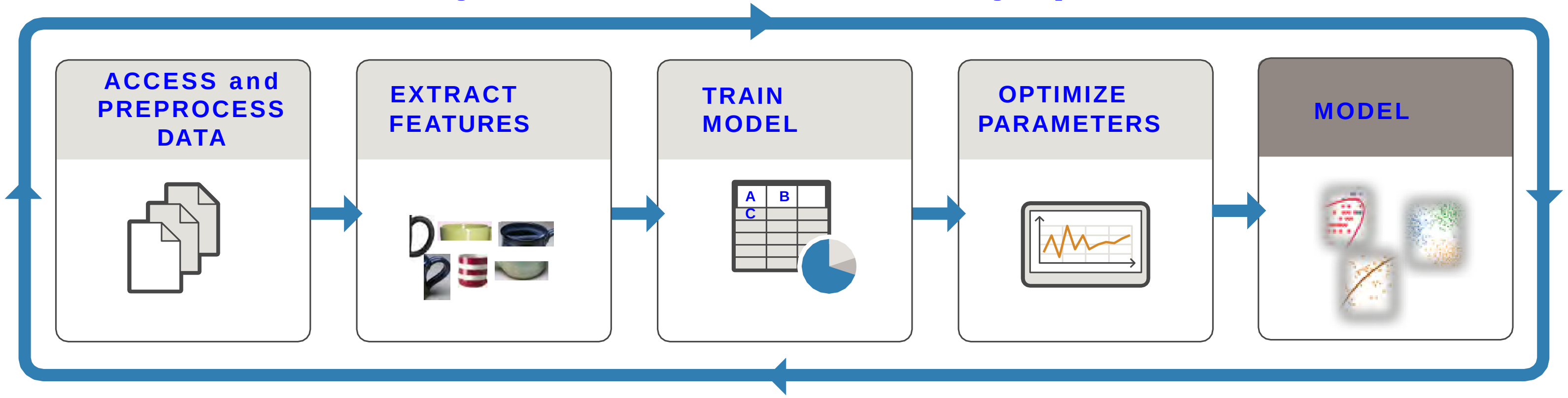




Source: Mohanty ISCT Keynote 2019

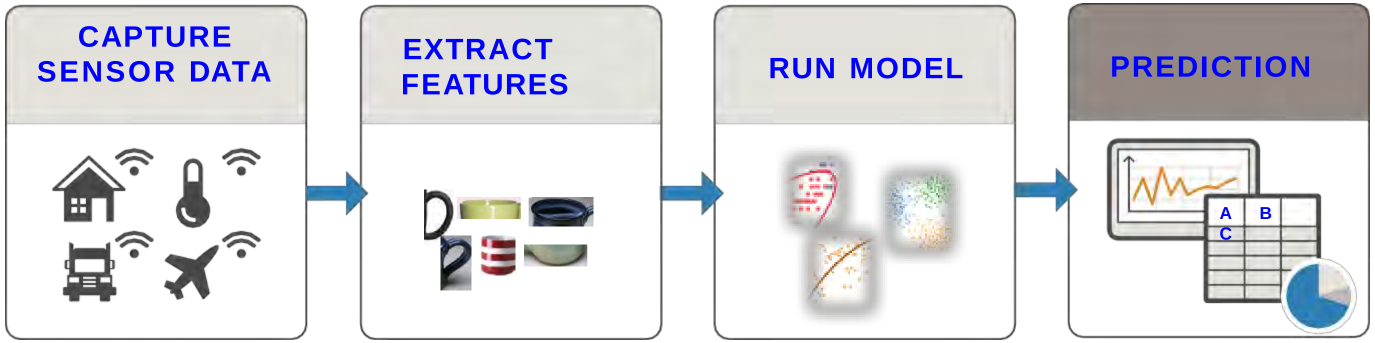
# Deep Neural Network (DNN) - Resource and Energy Costs

**TRAIN: Iterate until you achieve satisfactory performance.**




Needs Significant:
- ➢ Computational Resource
- ➢ Computation Energy

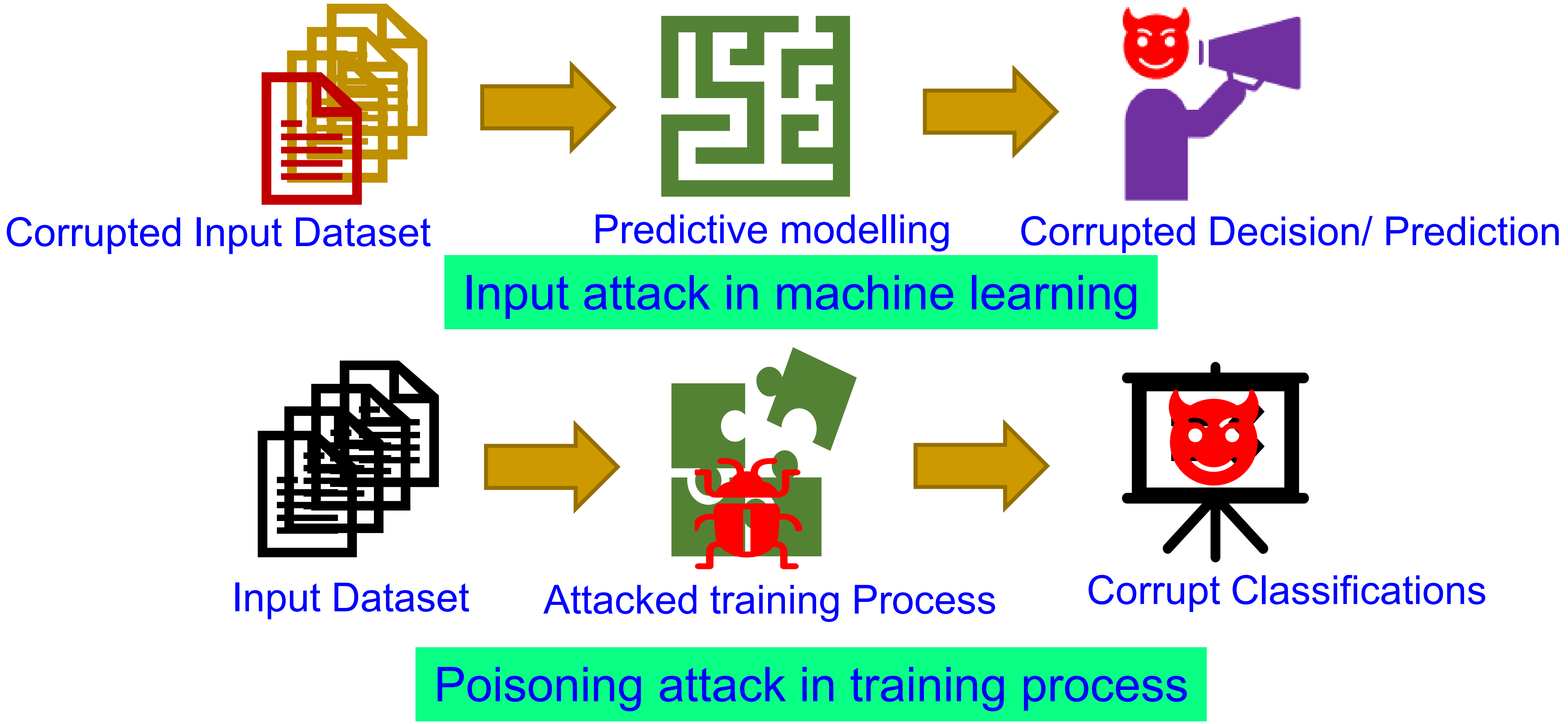
**PREDICT: Integrate trained models into applications.**




Needs:
- ➢ Computational Resource
- ➢ Computation Energy

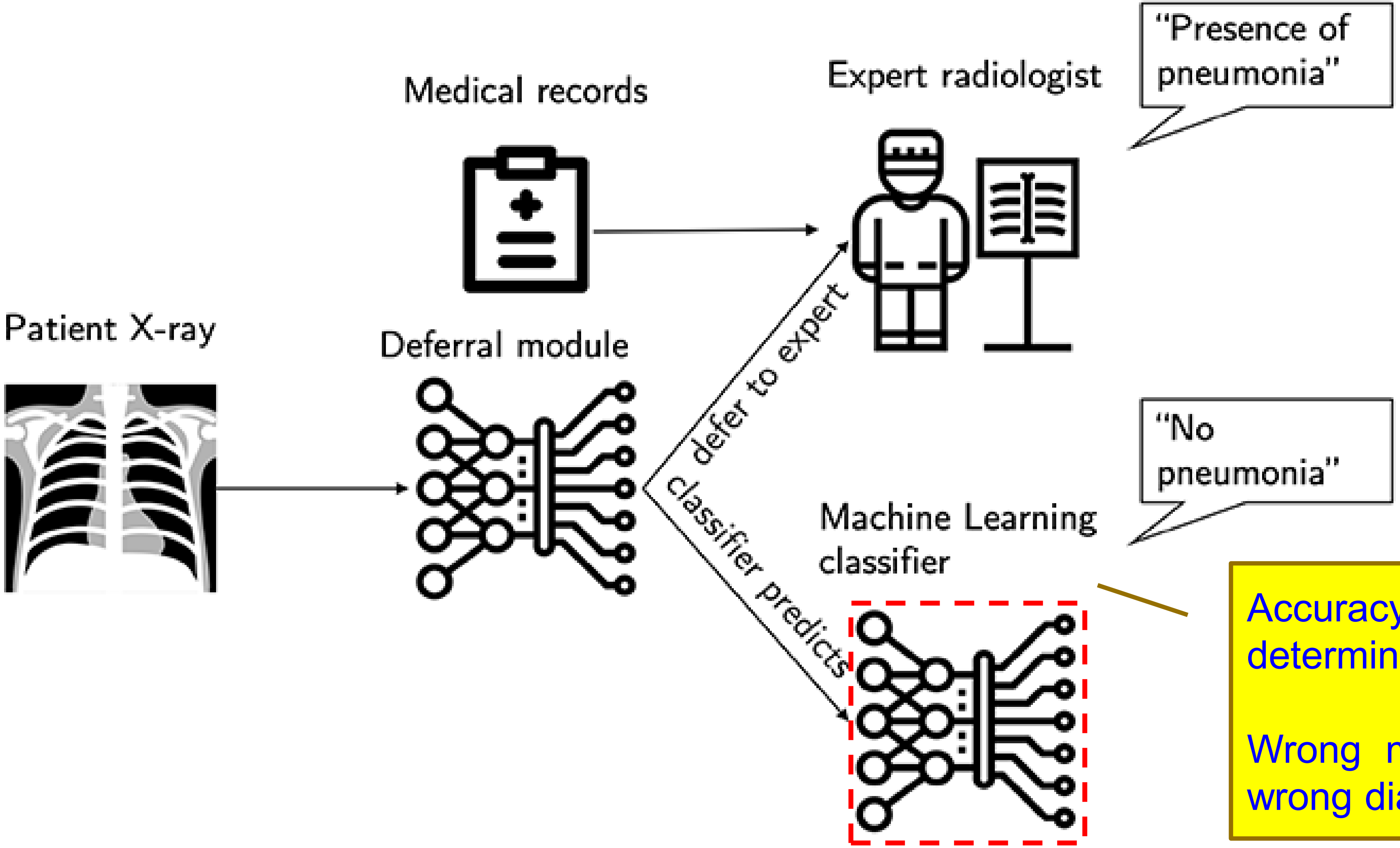
Source: https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html

# AI/ML – Cybersecurity Issue




Source: D. Puthal, and **S. P. Mohanty**, "Cybersecurity Issues in AI", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 4, July 2021, pp. 33--35.

# 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

# Smart Healthcare - Security Challenges

**Selected Smart Healthcare Security/Privacy Challenges**

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

Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 7, Issue 1, January 2018, pp. 18-28.

# 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

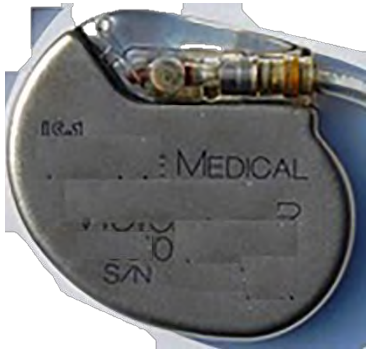
- FDA Issues Recall For Medtronic mHealth Devices Over Hacking Concerns:

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

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

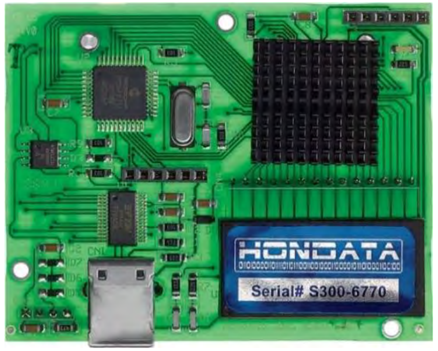
AI can be fooled by fake data

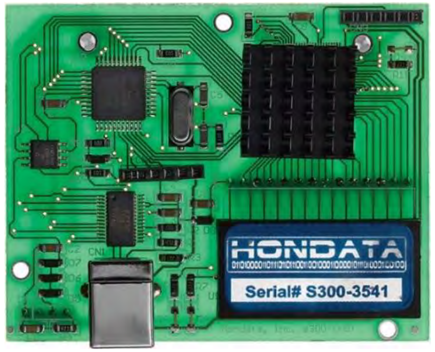
AI can create fake data (Deepfake)


Authentic Fake

An implantable medical device

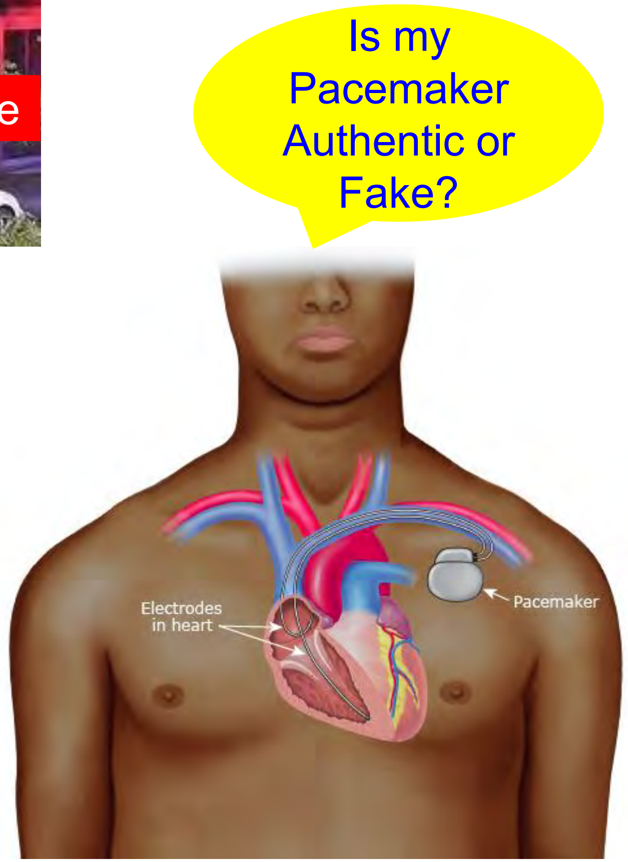



Authentic Fake

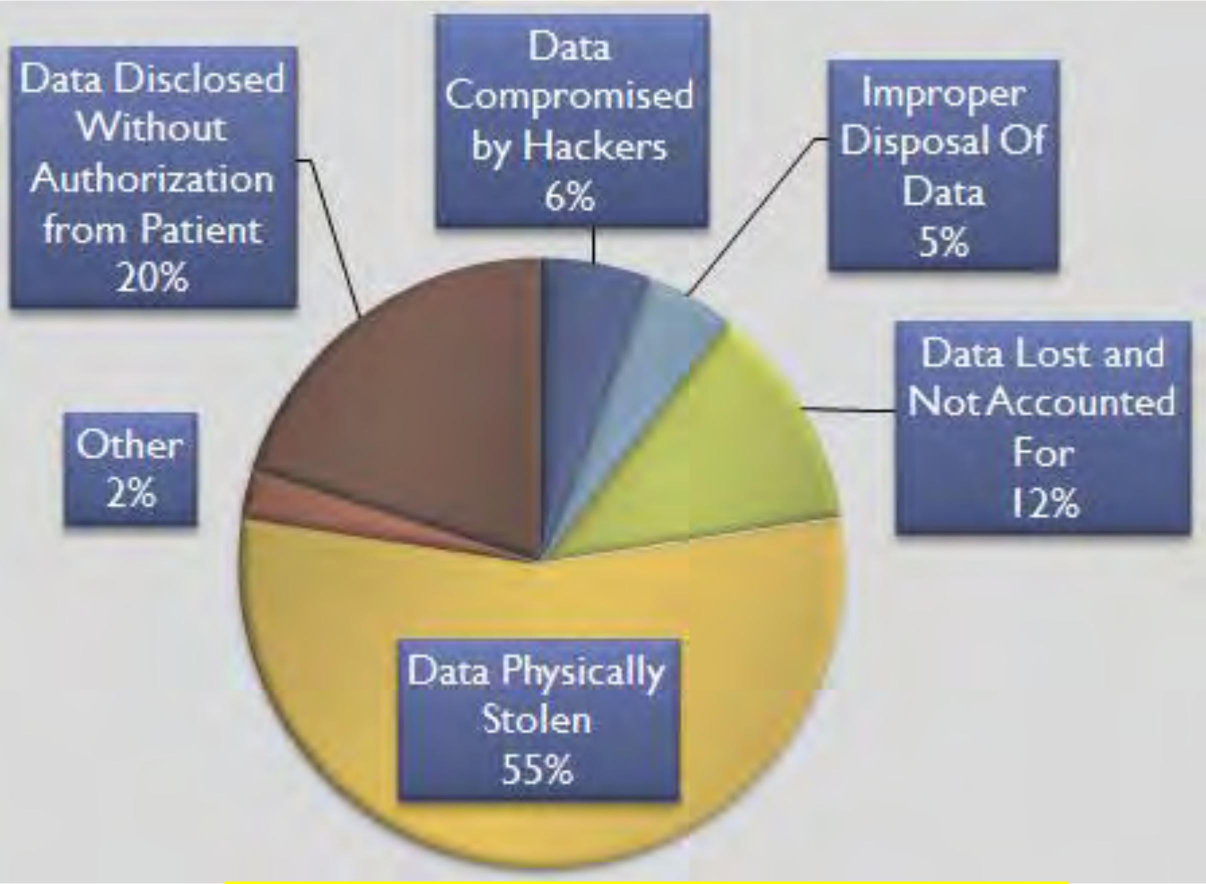
A plug-in for car-engine computers

# Fake is Cheap – Why not Buy?



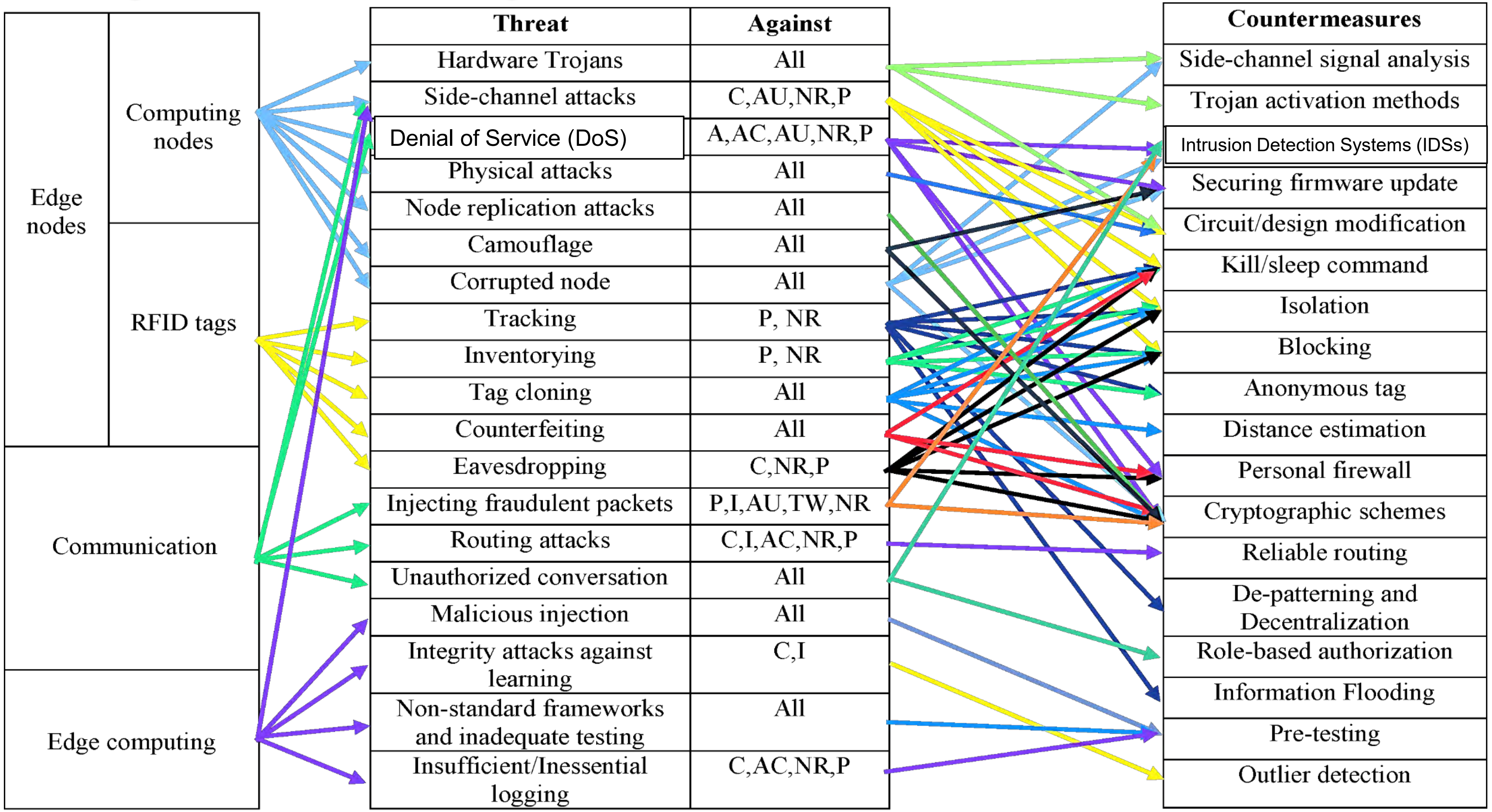
# Health Insurance Portability and Accountability Act (HIPPA)




HIPPA Privacy Violation by Types

# Cybrsecurity Solution for IoT/CPS

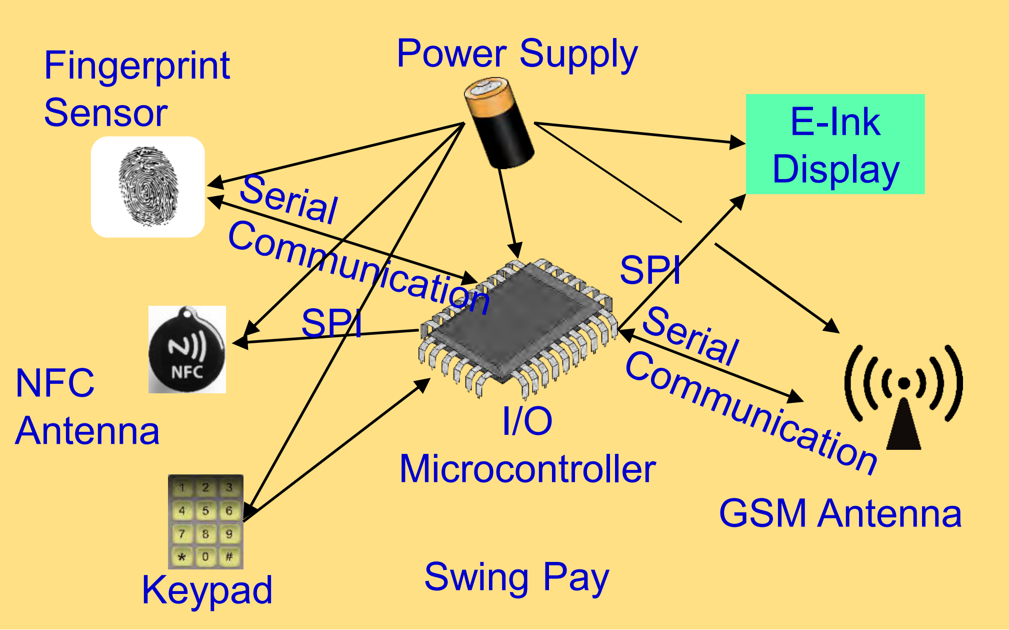
# IoT Cybersecurity - Attacks and Countermeasures

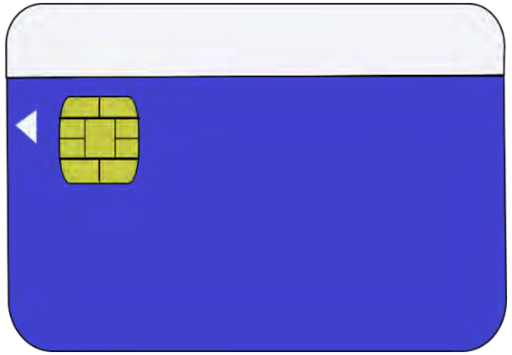


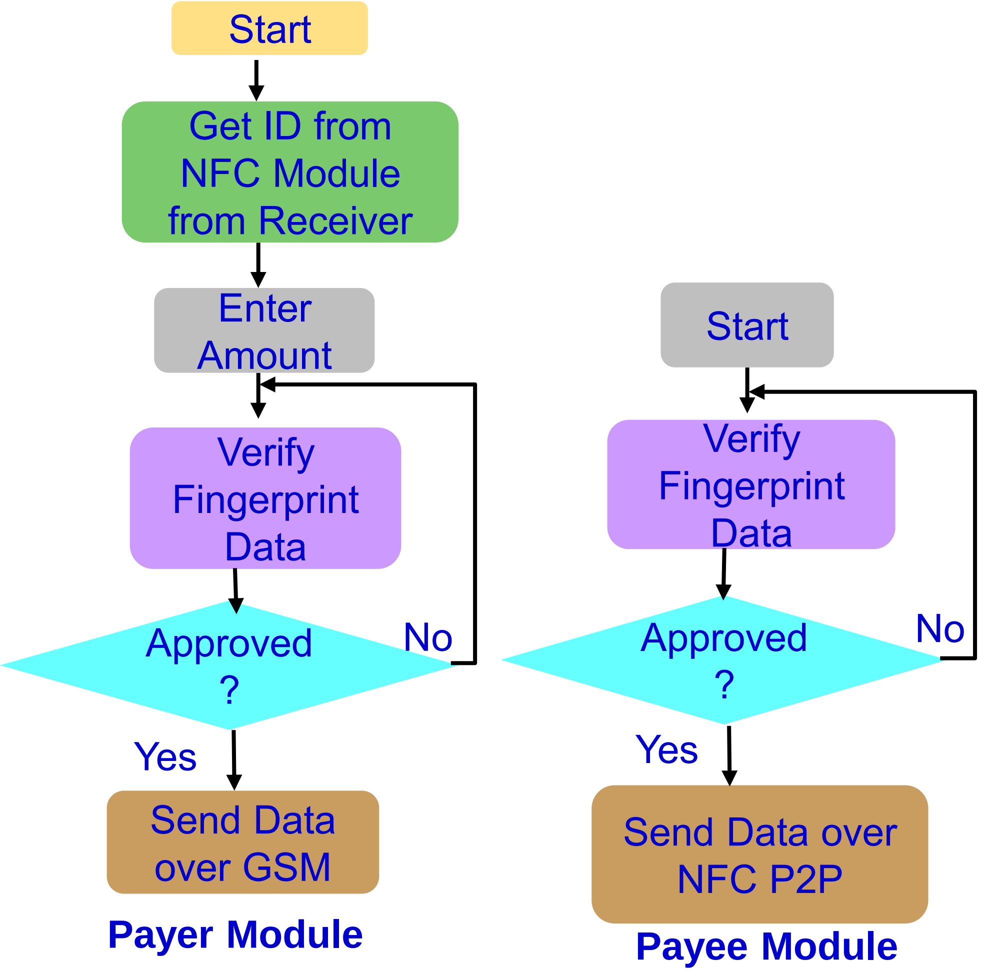

C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

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.

# Our Swing-Pay - NFC Cybersecurity Solution





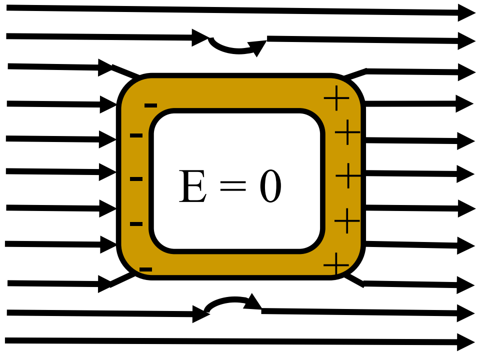

Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

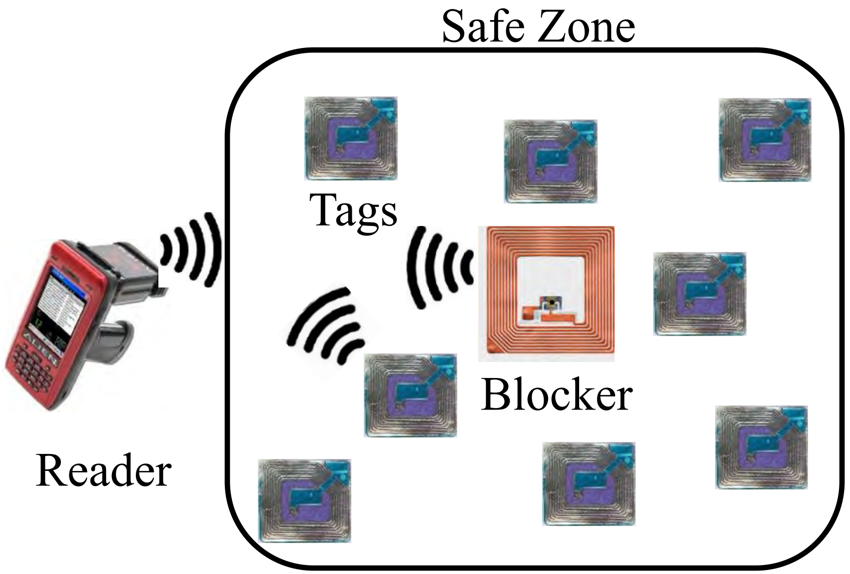
# RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

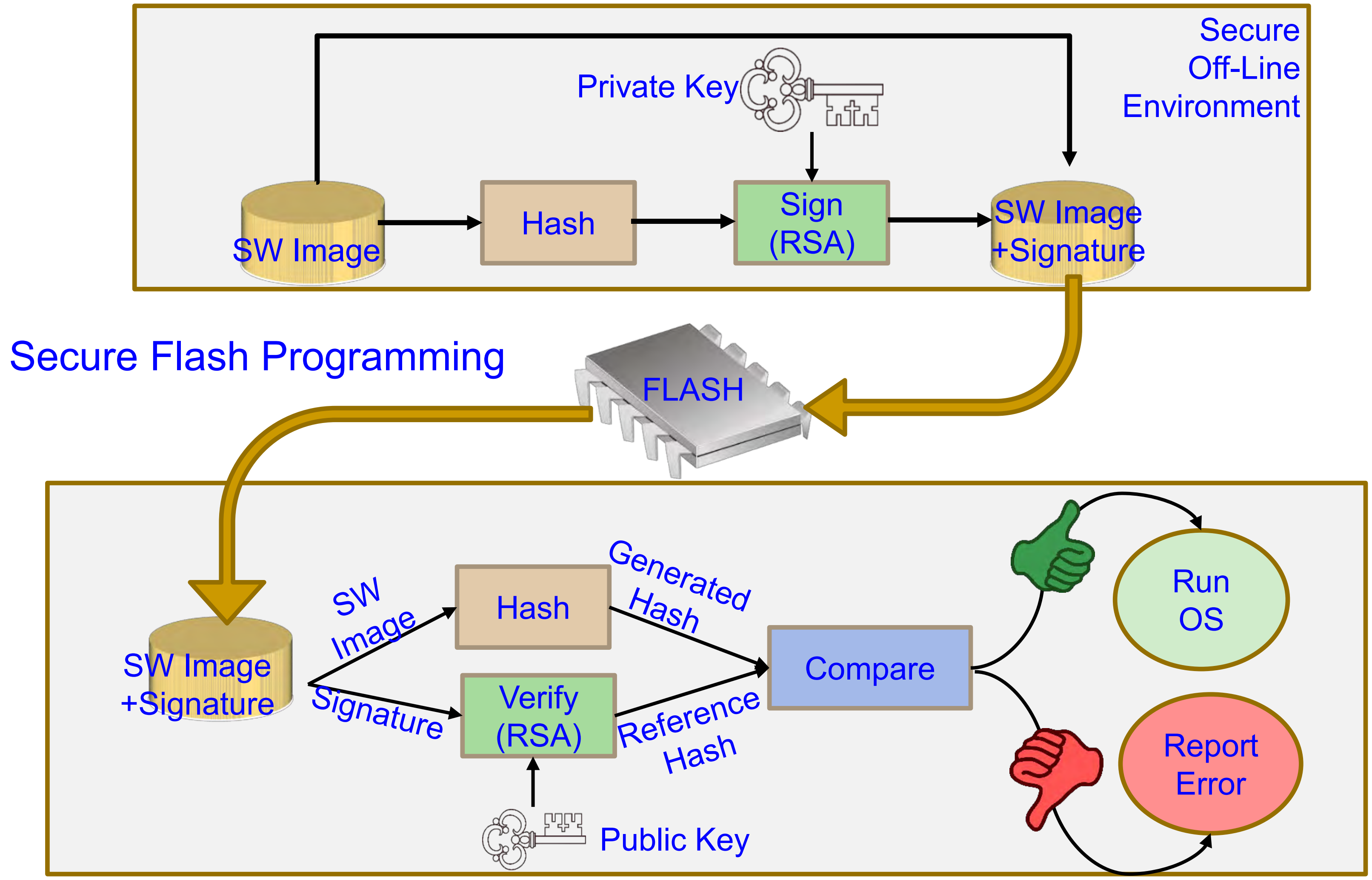



Blocker Tags

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

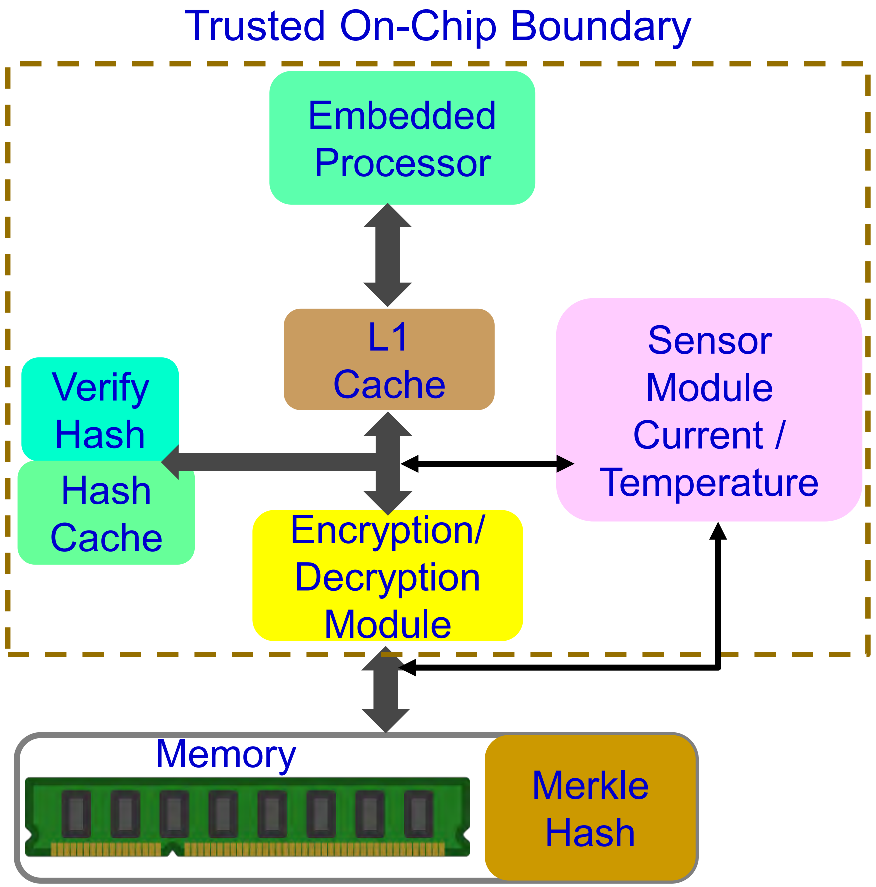
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

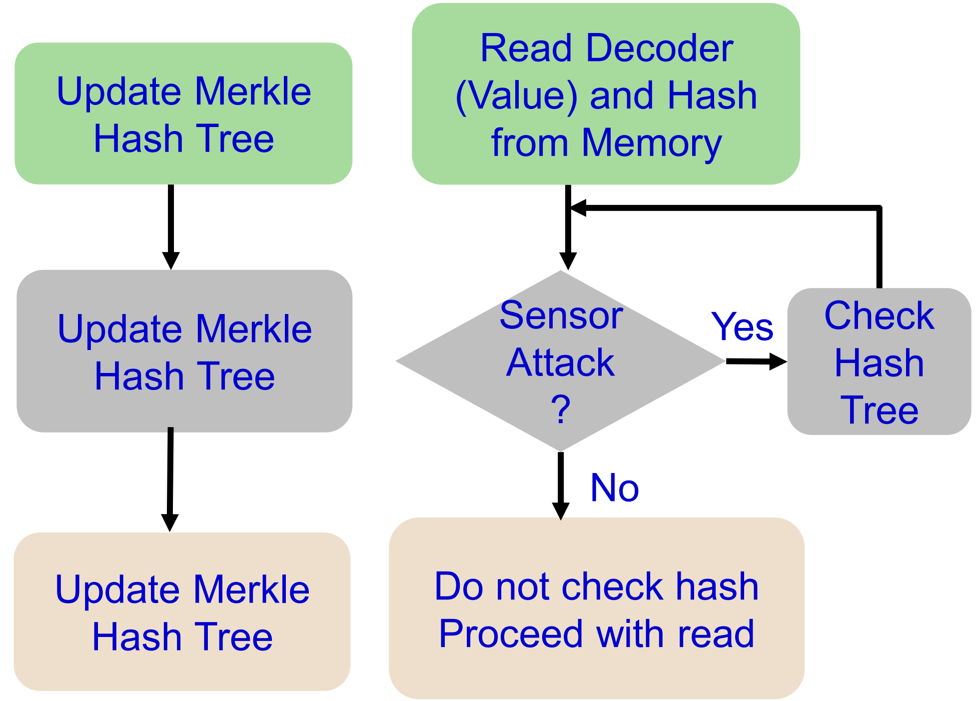
Some performance penalty due to increase in latency!

How Cloud storage changes this scenario?

# Embedded Memory Security




On-Chip/On-Board Memory Protection



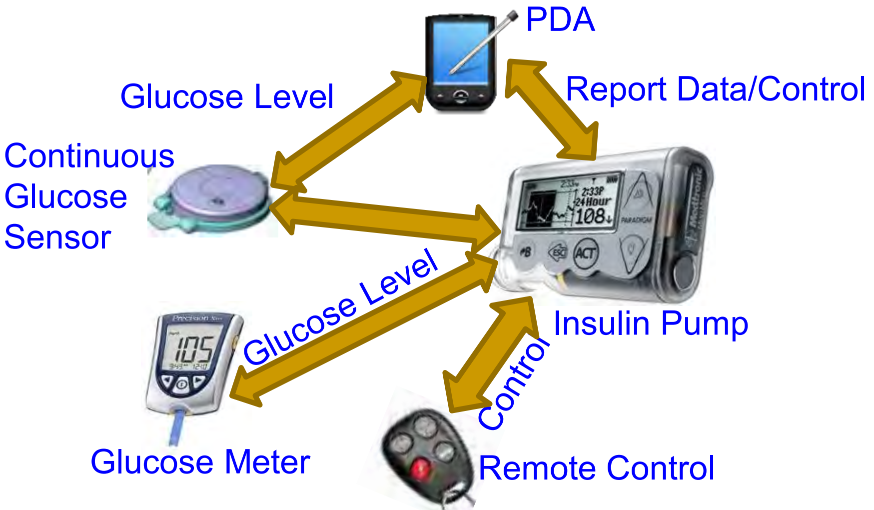

Write Operation

Read Operation

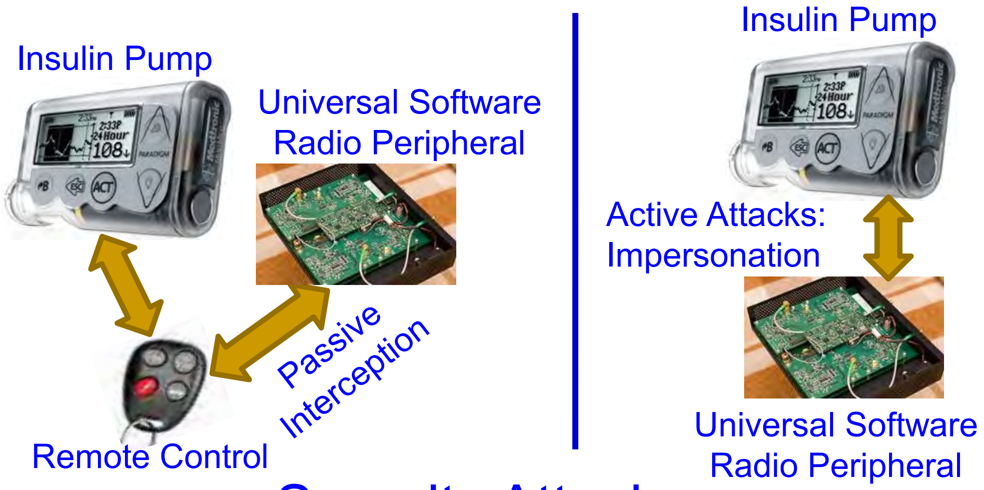
Memory integrity verification with 85% energy savings with minimal performance overhead.

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.

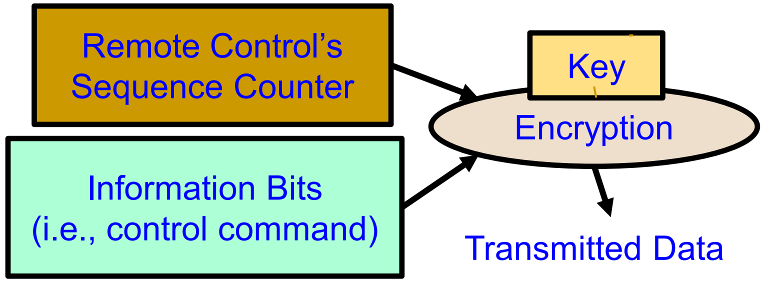
# Smart Healthcare Cybersecurity



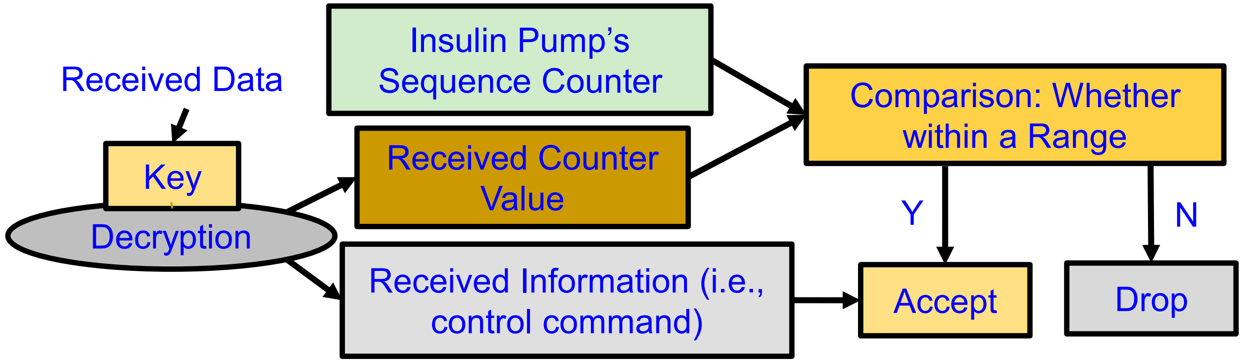

Insulin Delivery System




Security Attacks



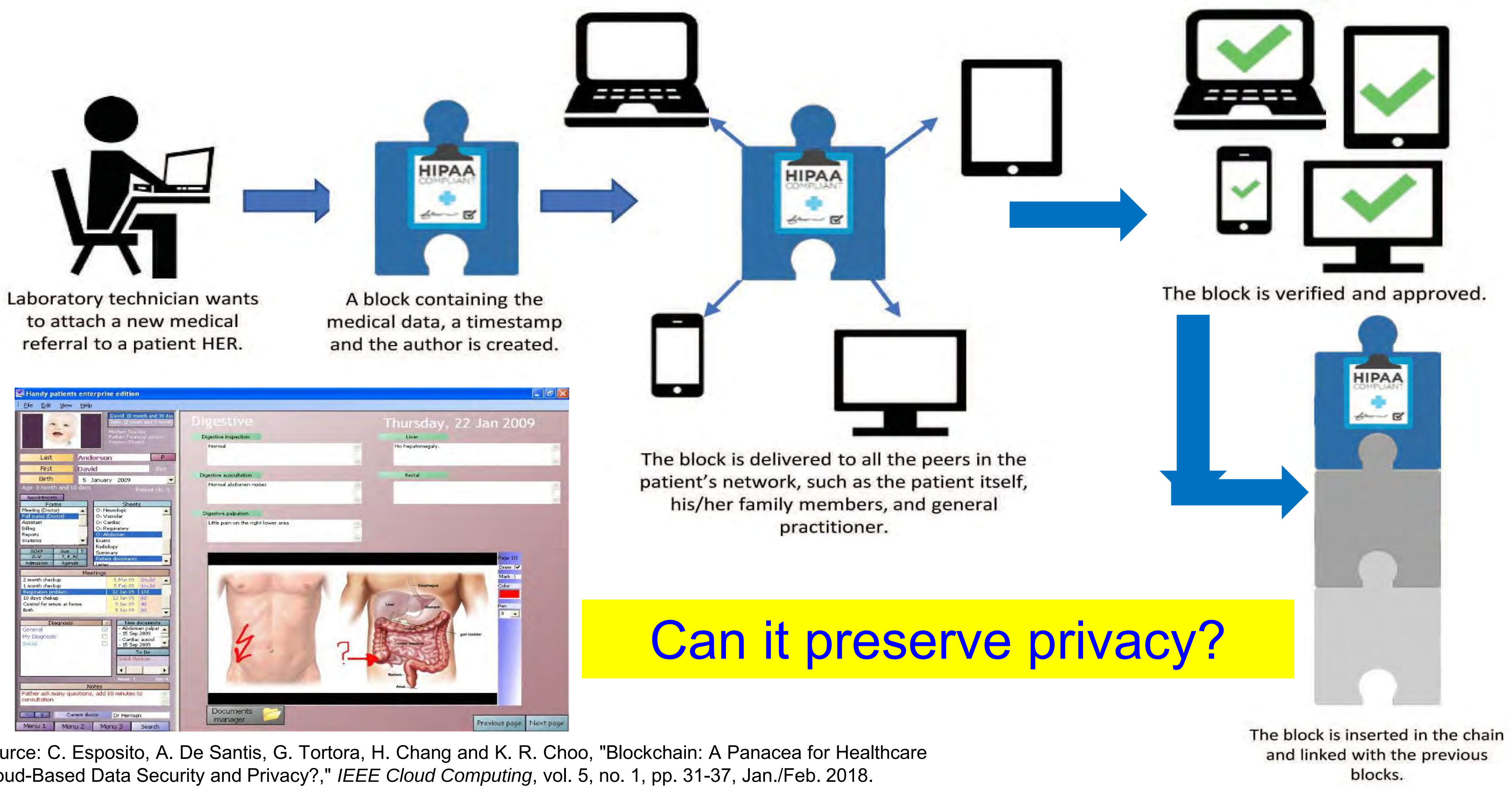

Rolling Code Encoder in Remote Control




Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

# 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.

# Drawbacks of Existing Cybersecurity Solutions

# IoT/CPS Cybersecurity Solutions – Advantages and Disadvantages

**Analysis of selected approaches to security and privacy issues in CE.**

| Category | Current Approaches | Advantages | Disadvantages |
|---|---|---|---|
| Confidentiality | Symmetric key cryptography | Low computation overhead | Key distribution problem |
| | Asymmetric key cryptography | Good for key distribution | High computation overhead |
| Integrity | Message authentication codes | Verification of message contents | Additional computation overhead |
| Availability | Signature-based authentication | Avoids unnecessary signature computations | Requires additional infrastructure and rekeying scheme |
| Authentication | Physically unclonable functions (PUFs) | High speed | Additional implementation challenges |
| | Message authentication codes | Verification of sender | Computation overhead |
| Nonrepudiation | Digital signatures | Link message to sender | Difficult in pseudonymous systems |
| Identity privacy | Pseudonym | Disguise true identity | Vulnerable to pattern analysis |
| | Attribute-based credentials | Restrict access to information based on shared secrets | Require shared secrets with all desired services |
| Information privacy | Differential privacy | Limit privacy exposure of any single data record | True user-level privacy still chal-lenging |
| | Public-key cryptography | Integratable with hardware | Computationally intensive |
| Location privacy | Location cloaking | Personalized privacy | Requires additional infrastructure |
| Usage privacy | Differential privacy | Limit privacy exposure of any single data record | Recurrent/time-series data challenging to keep private |

Source: D. A. Hahn, A. Munir, and S. P. Mohanty, “Security and Privacy Issues in Contemporary Consumer Electronics”, *IEEE Consumer Electronics Magazine*, Vol 8, No. 1, Jan 2019, pp. 95--99.

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

## IT Cybersecurity

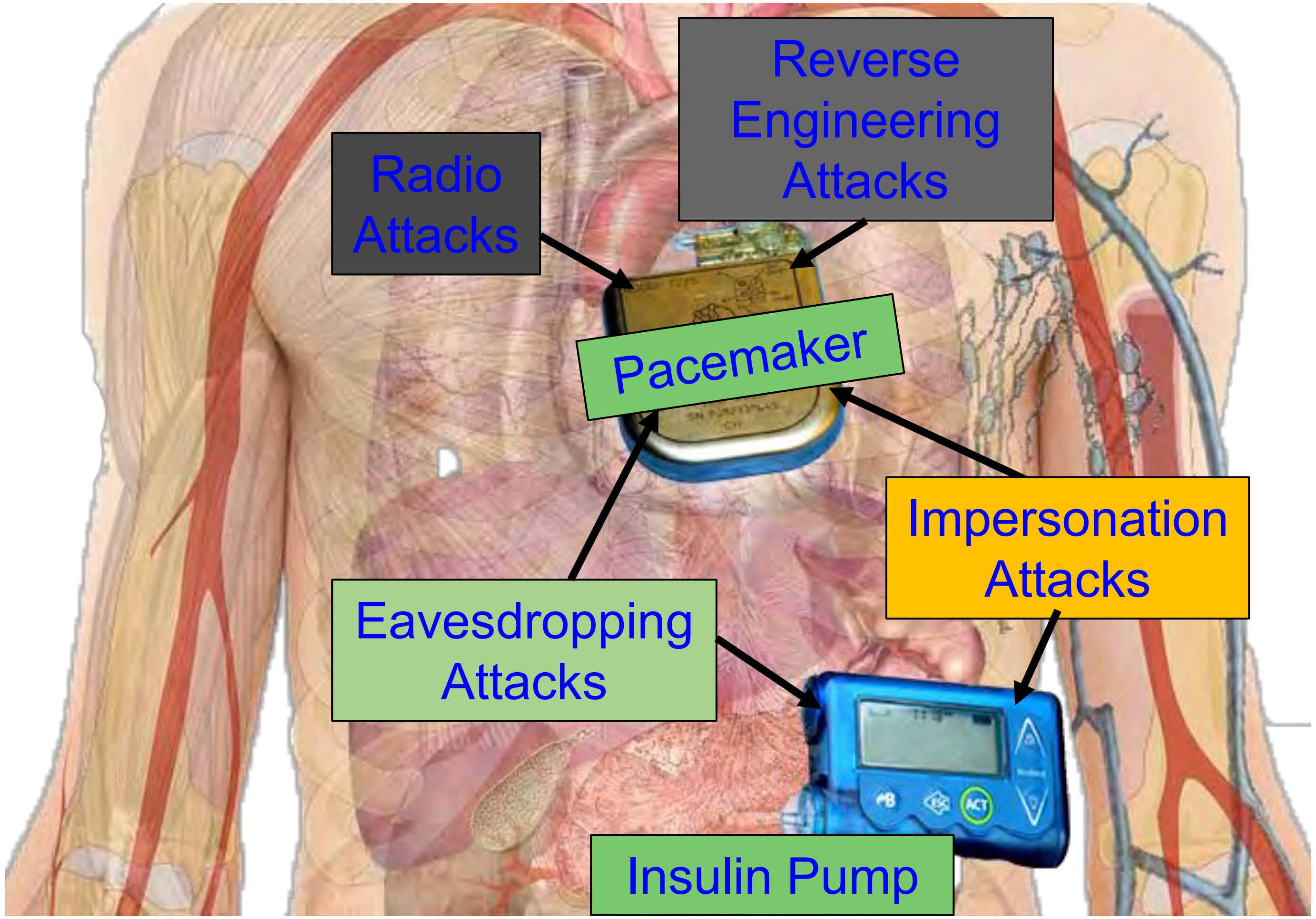
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

## IoT Cybersecurity

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

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

# Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard

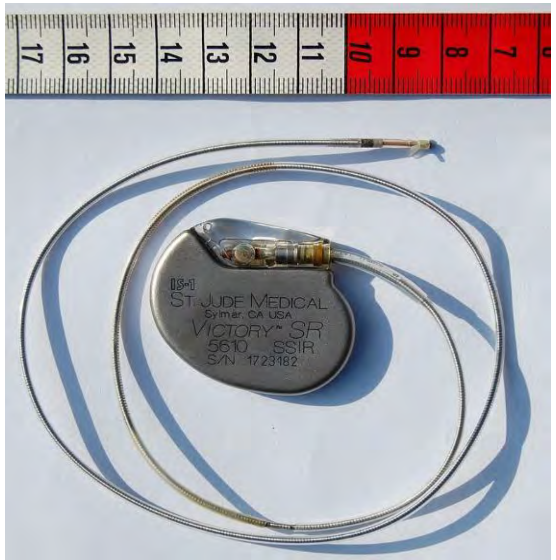



Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs):

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

# H-CPS Cybersecurity Measures is Hard - Energy Constrained




Pacemaker
Battery Life
- 10 years


Neurostimulator
Battery Life
- 8 years

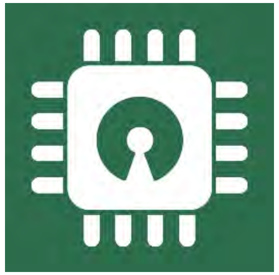
- Implantable Medical Devices (IMDs) have integrated battery to provide energy to all their functions → Limited Battery Life depending on functions
- Higher battery/energy usage → Lower IMD lifetime
- Battery/IMD replacement → Needs surgical risky procedures

Source: C. Camara, P. Peris-Lopeza, and J. E.Tapiadora, "Security and privacy issues in implantable medical devices: A comprehensive survey", *Elsevier Journal of Biomedical Informatics*, Volume 55, June 2015, Pages 272-289.

# Cybersecurity Attacks – Software Vs Hardware Based

## Software Based

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



## Hardware Based

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

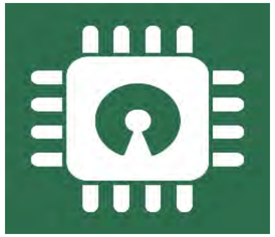
Source: Mohanty ICCE Panel 2018

# Cybersecurity Solutions – Software Vs Hardware Based

**Software Based**

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

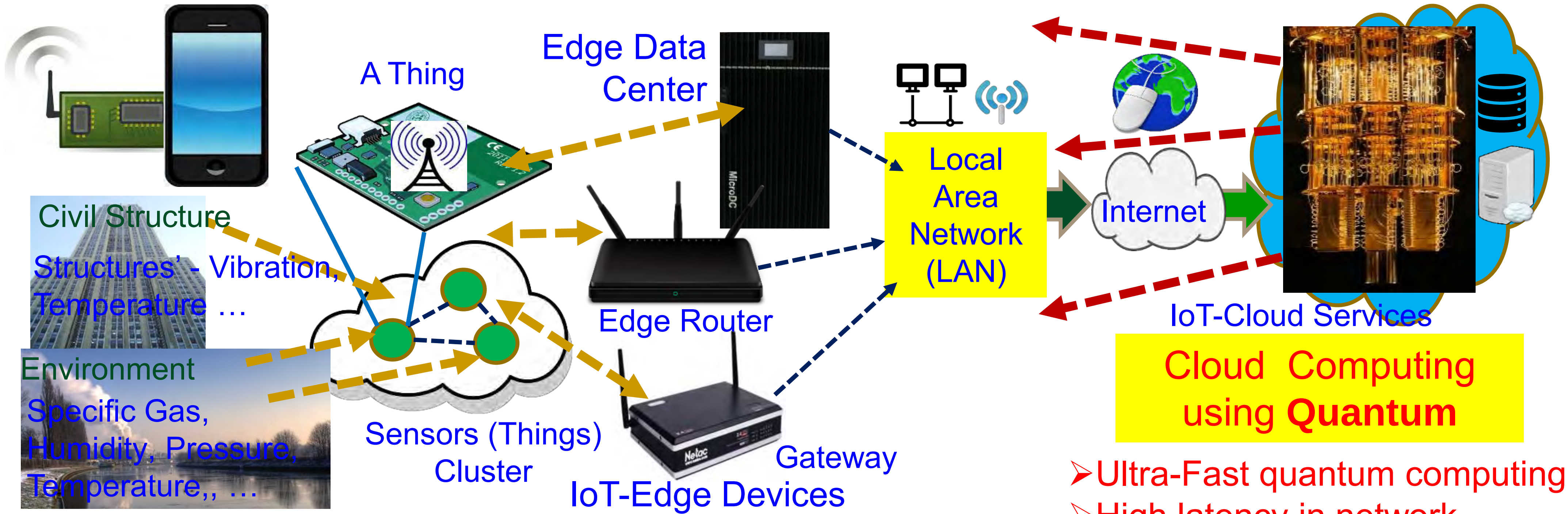
Source: Mohanty ICCE Panel 2018



**Hardware Based**

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

# Cybersecurity Nightmare ← Quantum Computing




IoT-End Devices

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

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

**Edge Computing**

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

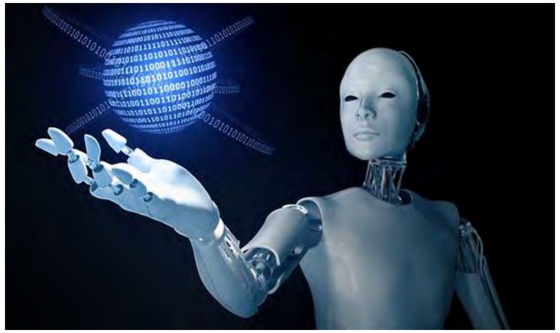
**Cloud Computing using Quantum**

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

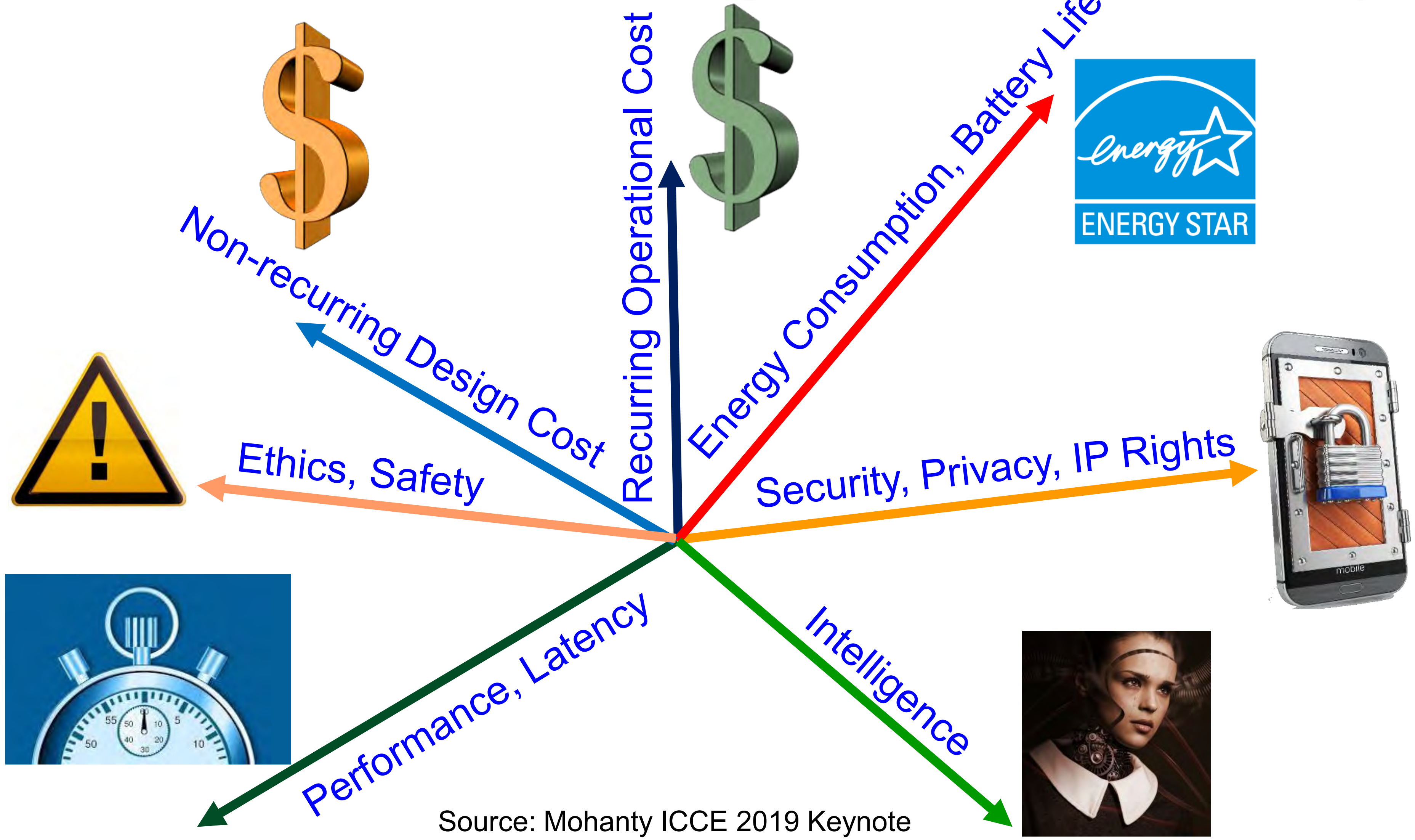
A quantum computer could break a 2048-bit RSA encryption in 8 hours.

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





# IoT/CPS Design – Multiple Objectives



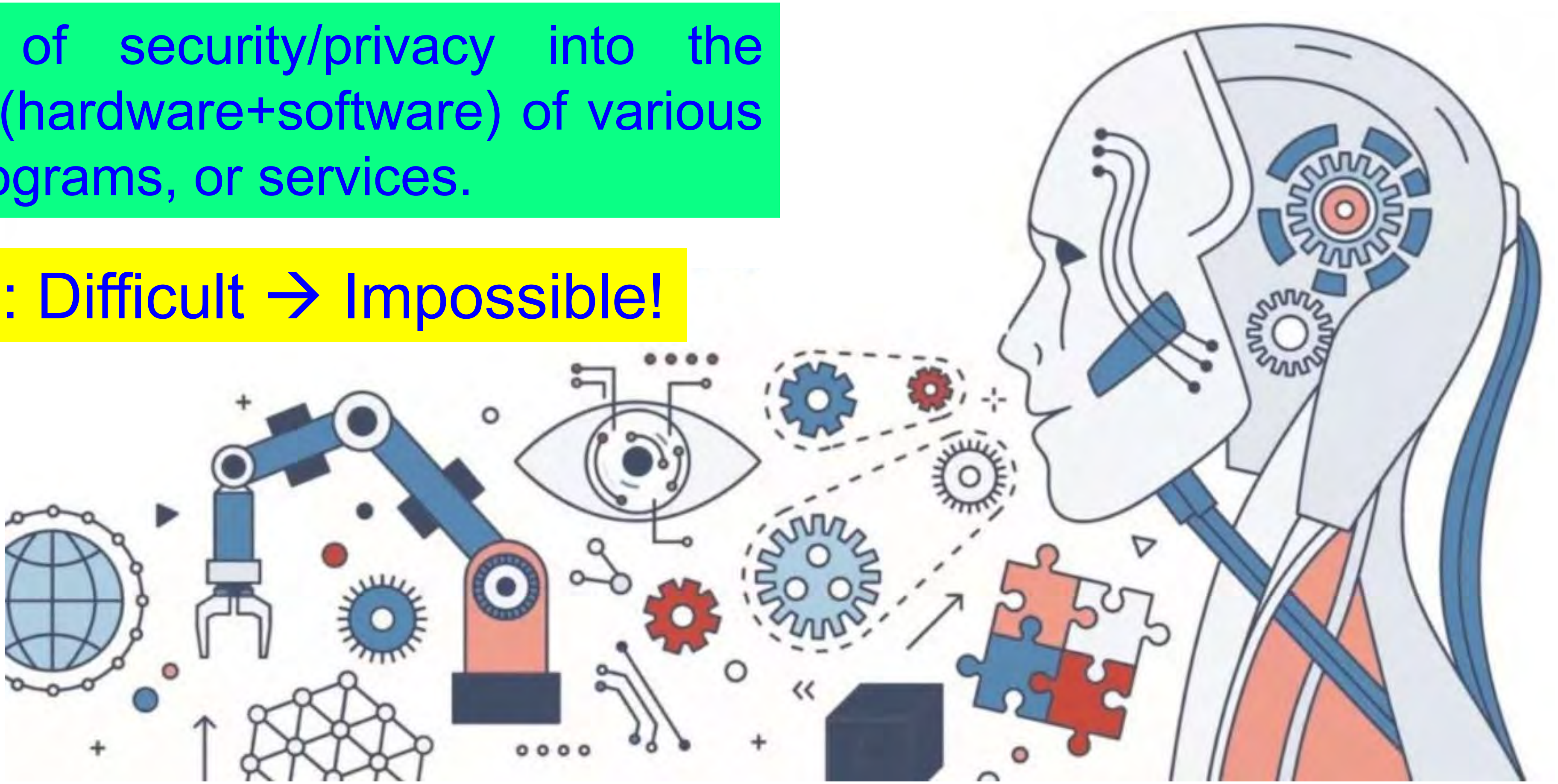

Source: Mohanty ICCE 2019 Keynote

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) and/or Privacy by Design (PbD)

7 Fundamental Principles

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

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

# CEI Tradeoffs for Smart Electronic Systems


Security of systems and data.

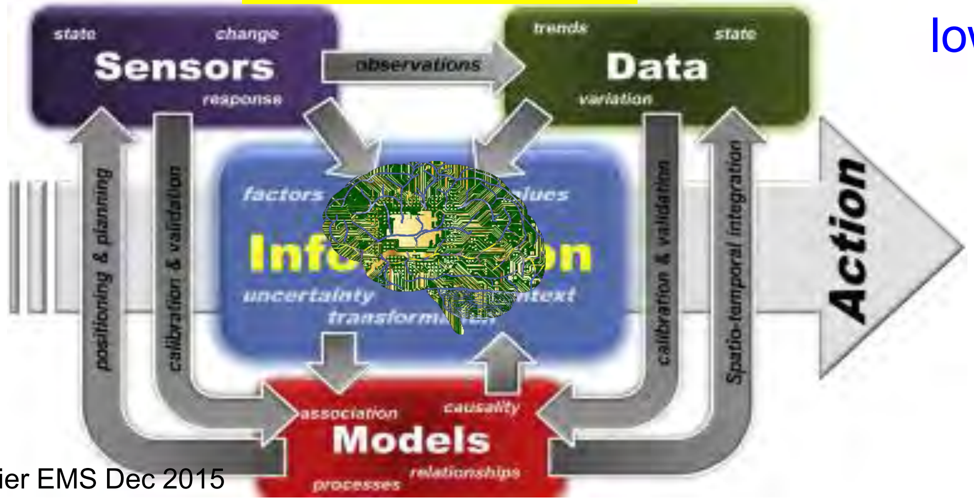
Cybersecurity

Energy


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

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

Intelligence




Accurate sensing, analytics, and fast actuation.

Source: Reis, et al. Elsevier EMS Dec 2015

Source: Mohanty iSES 2018 Keynote

# 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

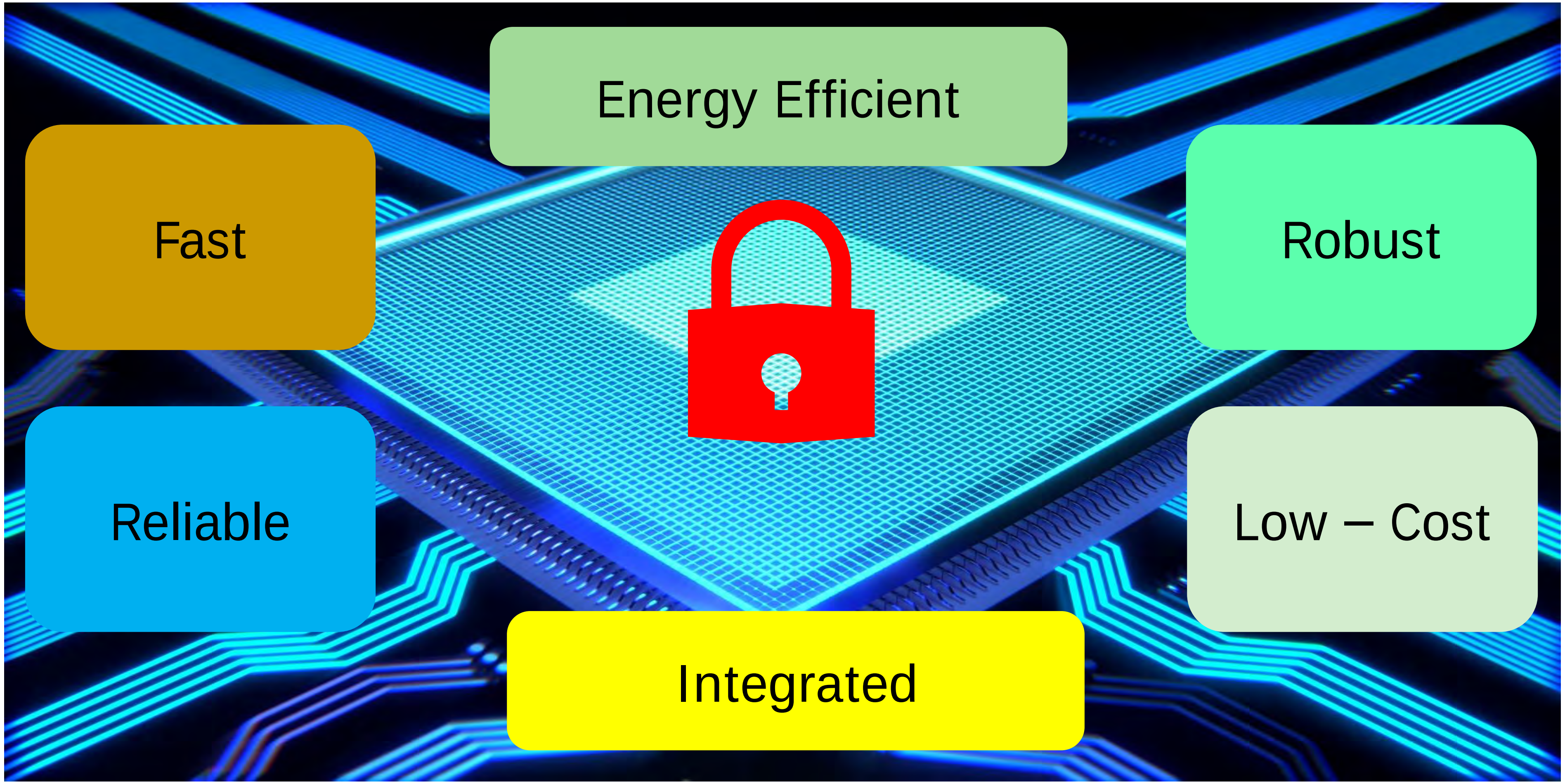
Memory Protection

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..

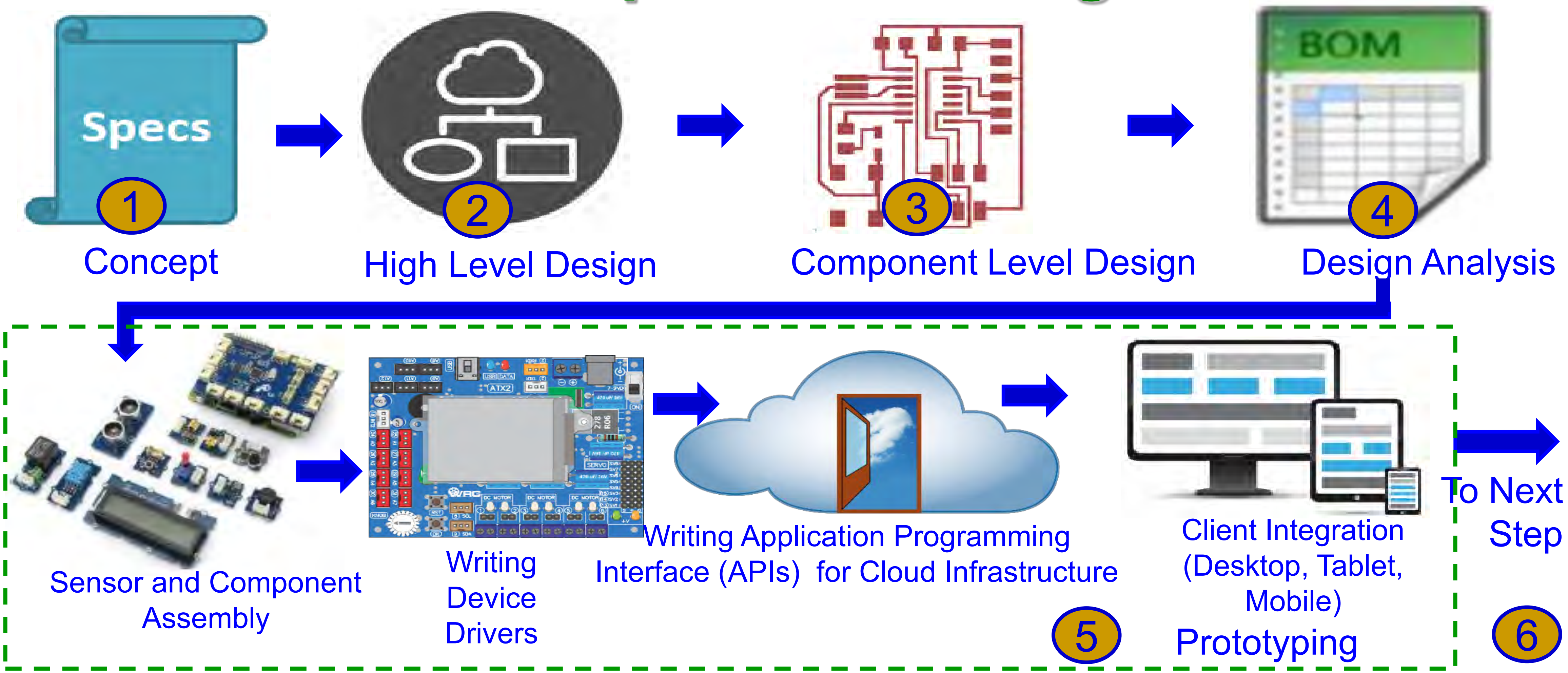
# Hardware Assisted Security (HAS) or Security-by-Design (SbD) - Advantages



# 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.

# SbD Principle - IoT 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%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

# SbD Principle- IoT Design Flow

6 Field Testing


7 Release of Beta Version

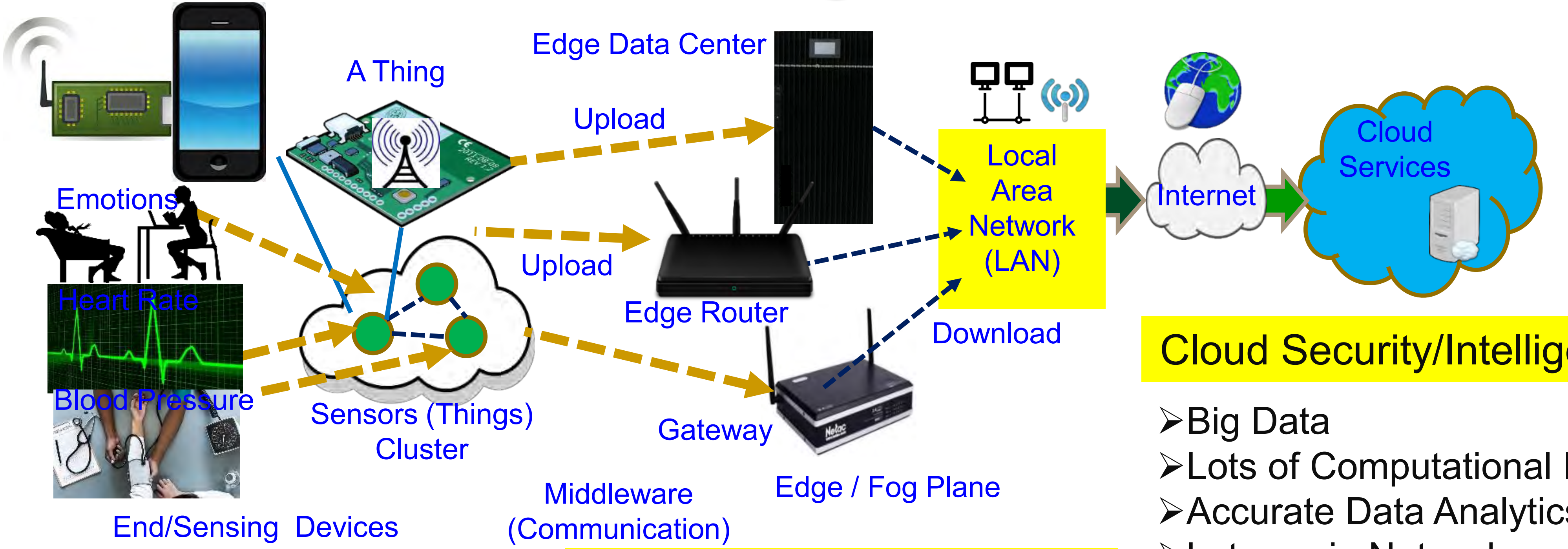
8 Production

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

# 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

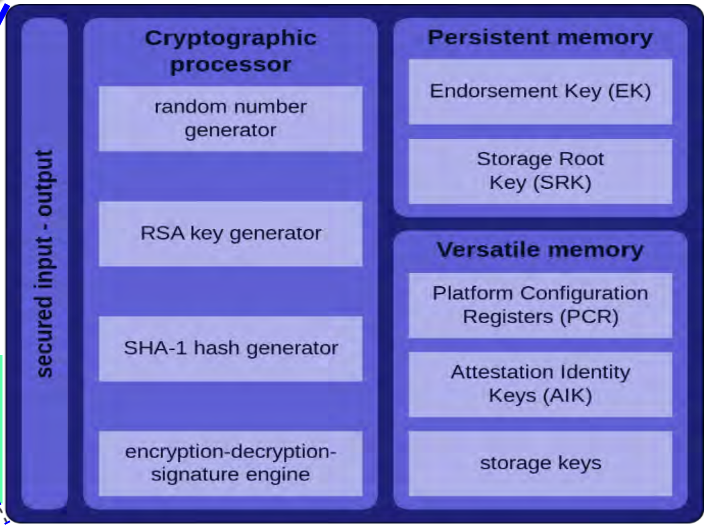
- Big Data
- Lots of Computational Resource
- Accurate Data Analytics
- Latency in Network
- Energy Overhead in Communications

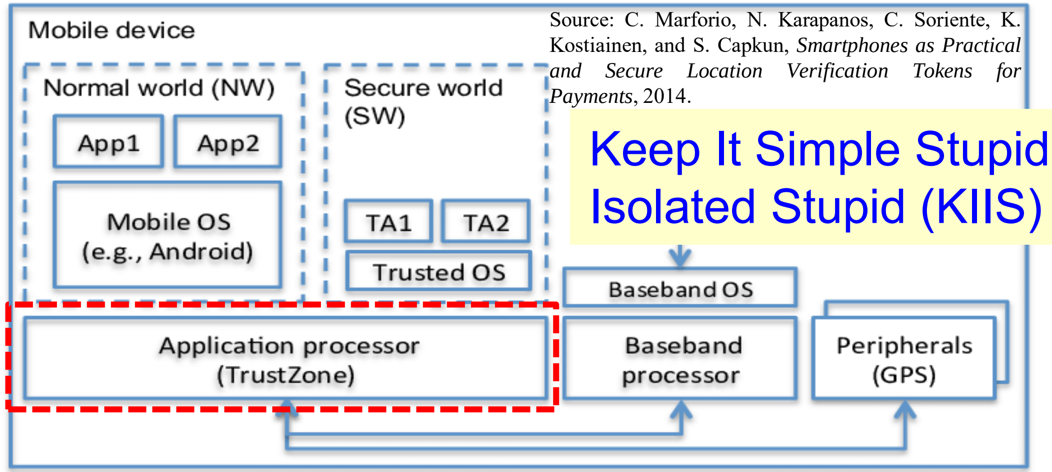
Heavy-Duty ML is more suitable for smart cities

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

Hardware Security Module (HSM)

Trusted Platform Module (TPM)




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

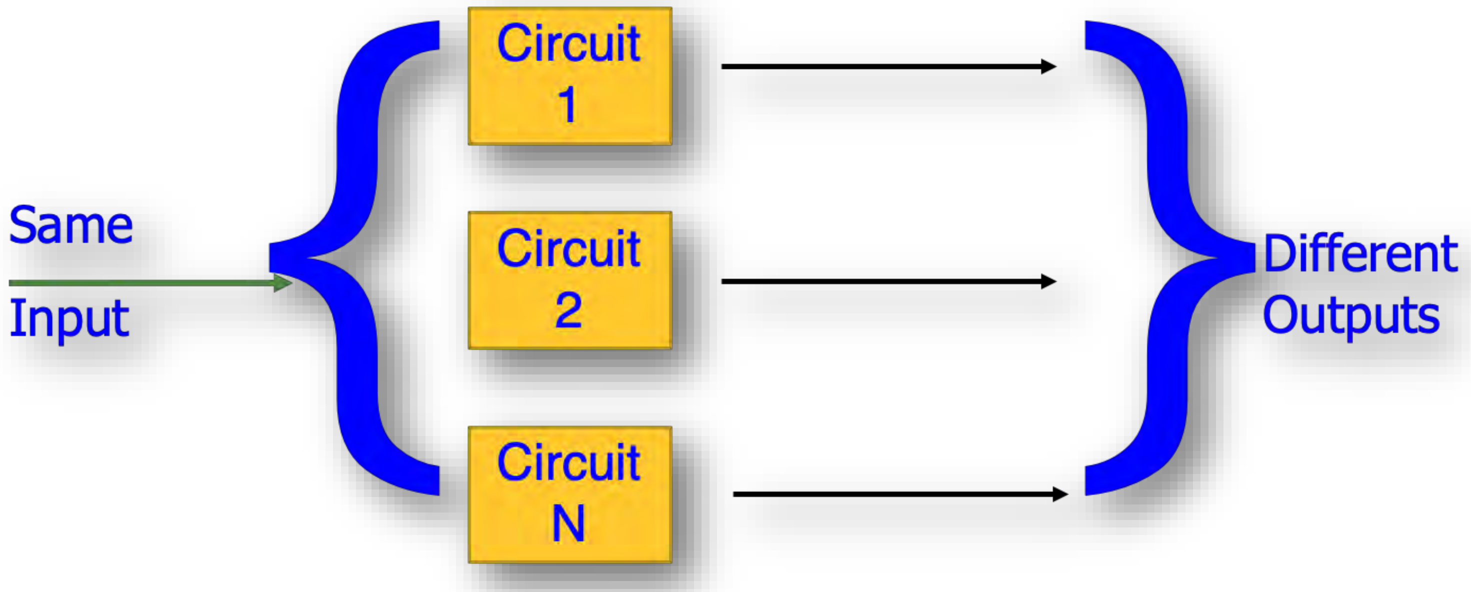
Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)

Physical Unclonable Functions (PUF)

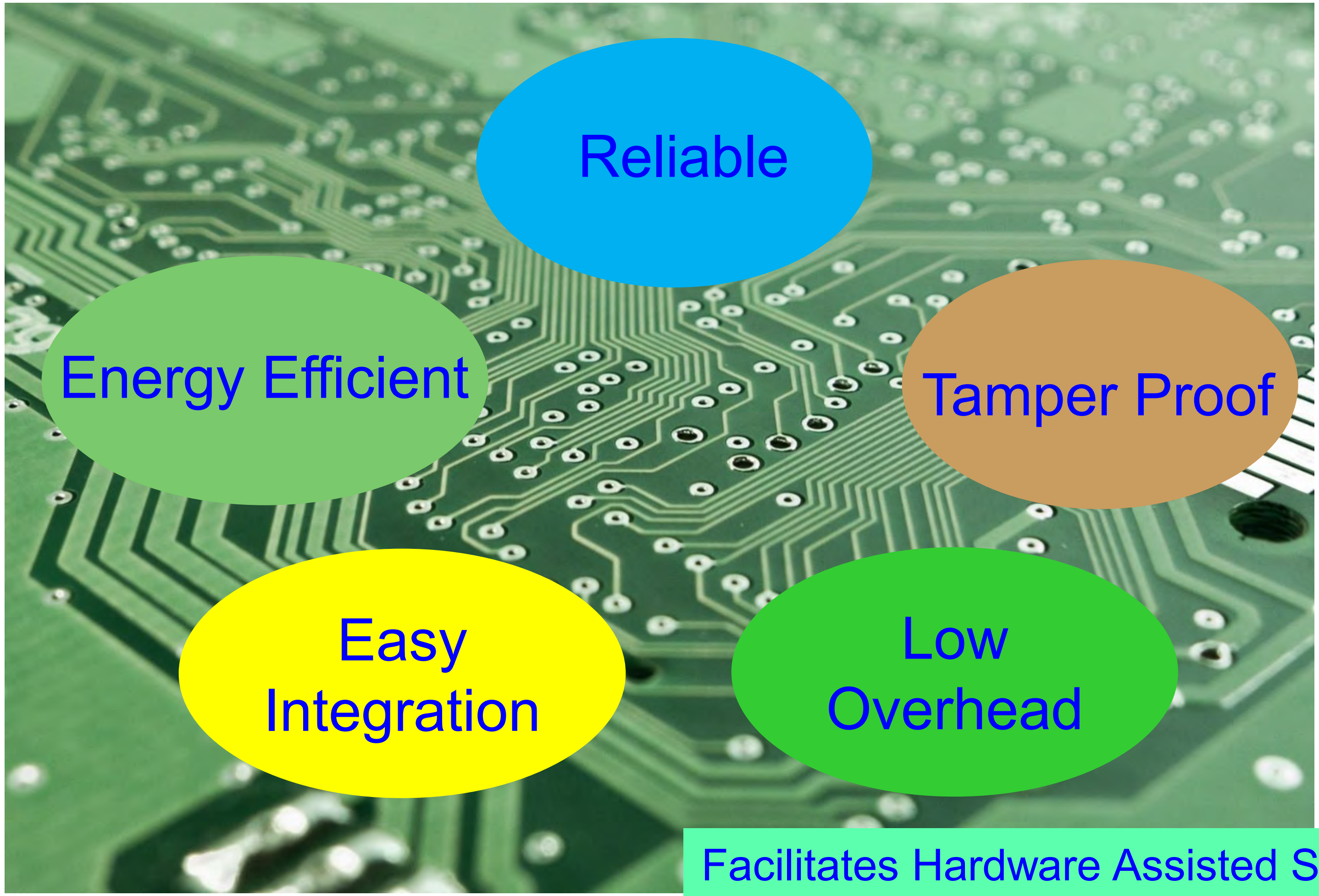
Source: Electric Power Research Institute (EPRI)

# Physical Unclonable Functions (PUF)

- Uses manufacturing variations for generating unique set of keys for cryptographic applications.
- Input of PUF is a challenge and output from PUF is response.



# PUF: Advantages

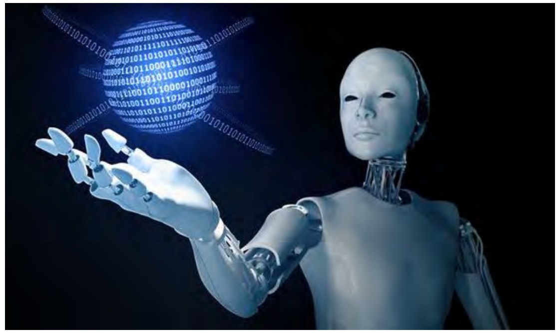



- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device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

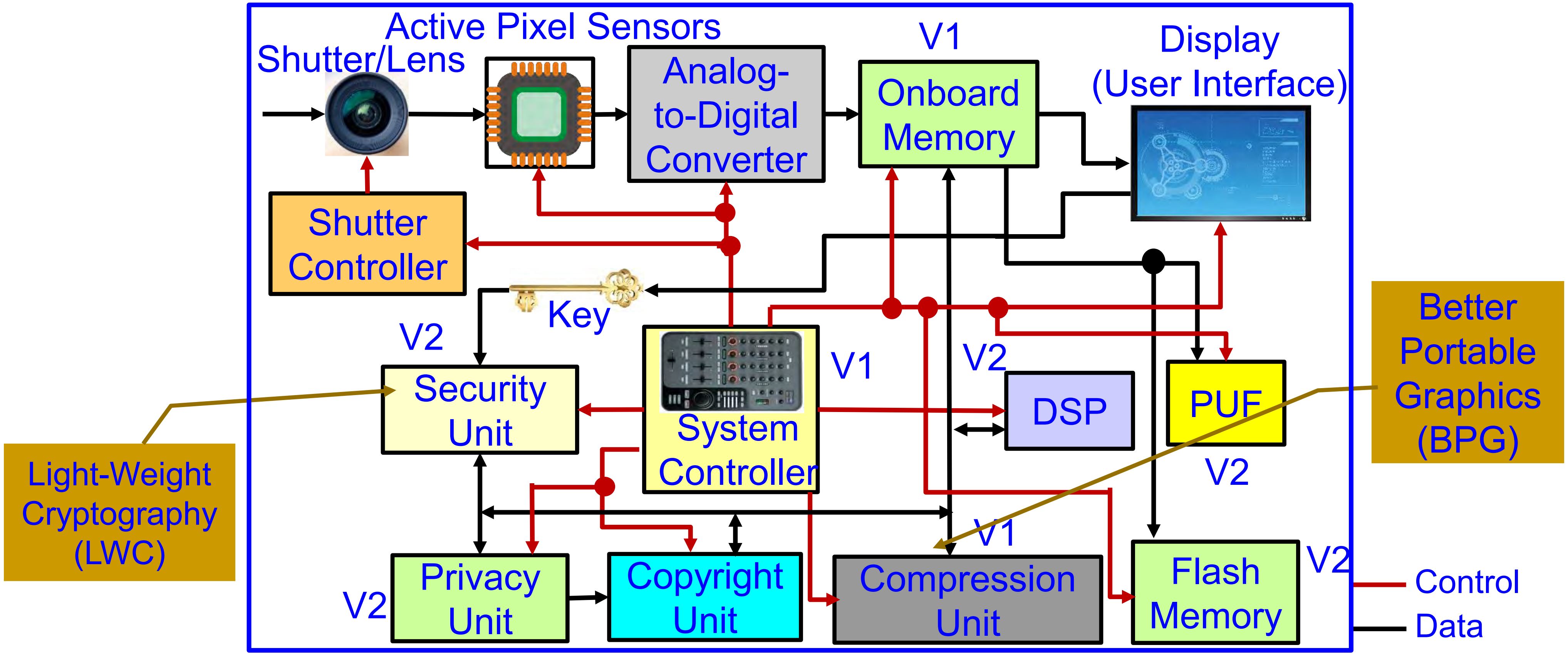
Facilitates Hardware Assisted Security (HAS) or Security-by-Design (SbD).

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





# Secure Digital Camera (SDC) – My Invention

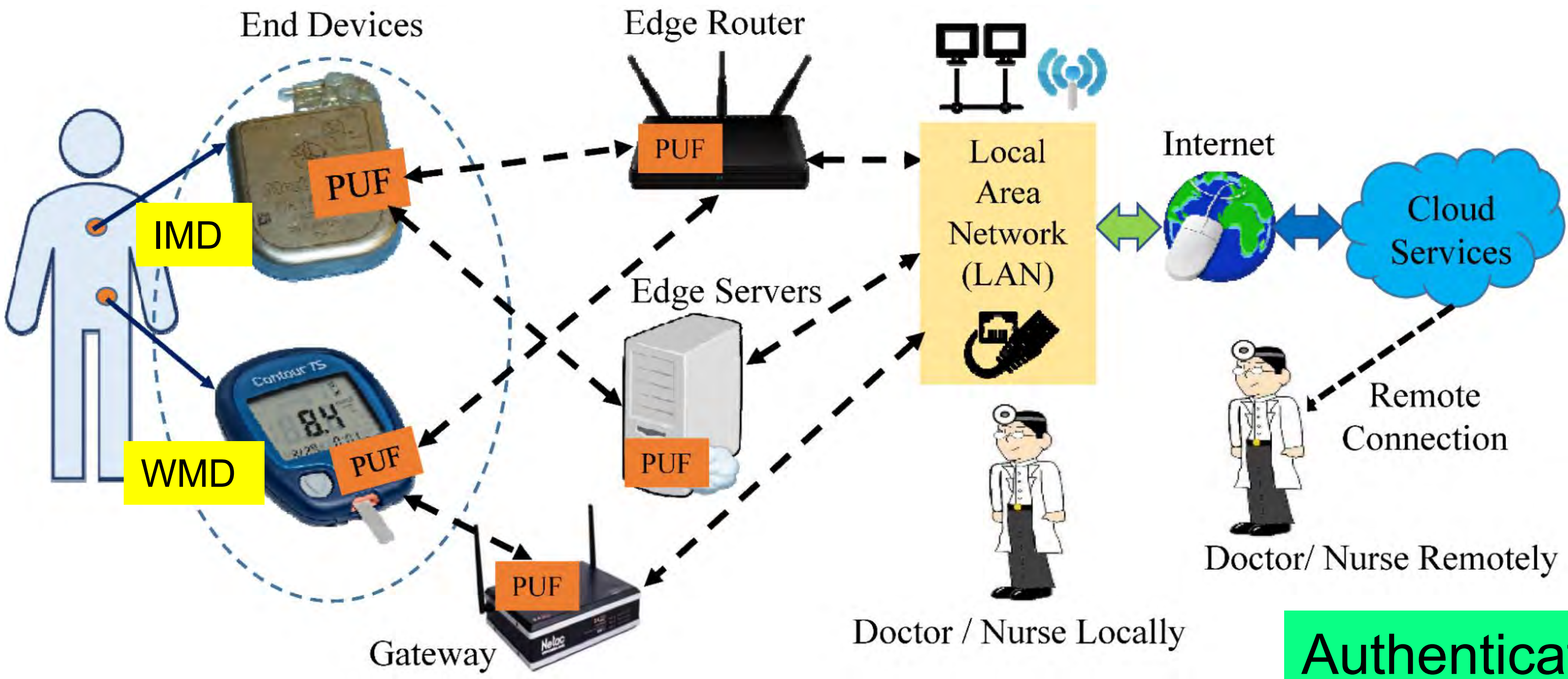



Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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.

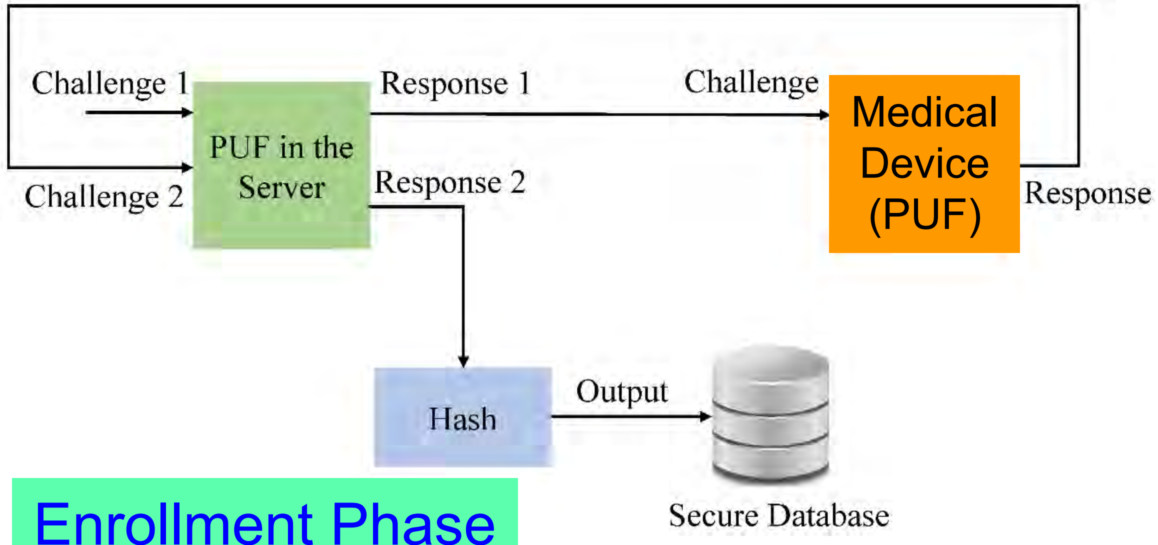
# PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS




Authenticates Time - 1 sec
Power Consumption - 200 $\mu$W

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

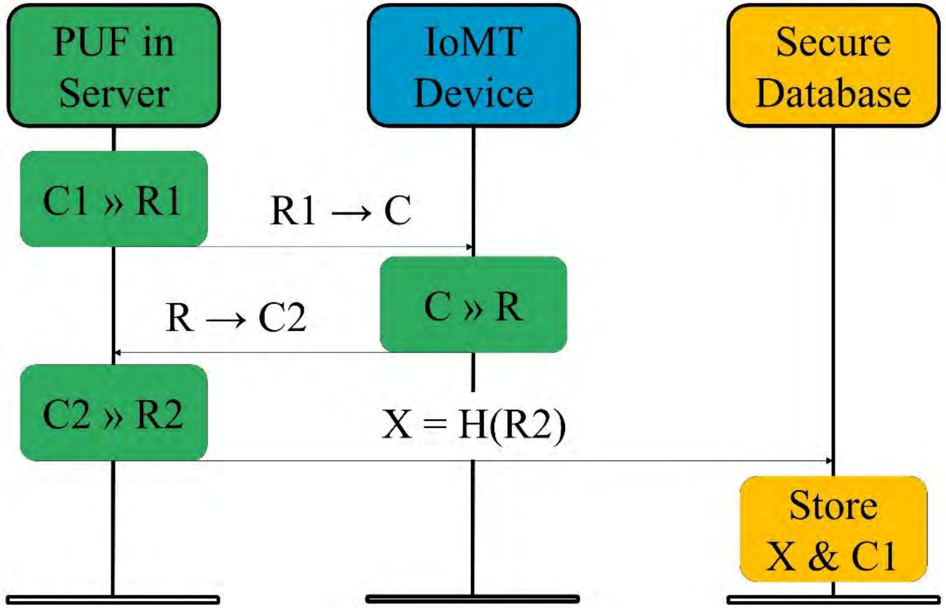



Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

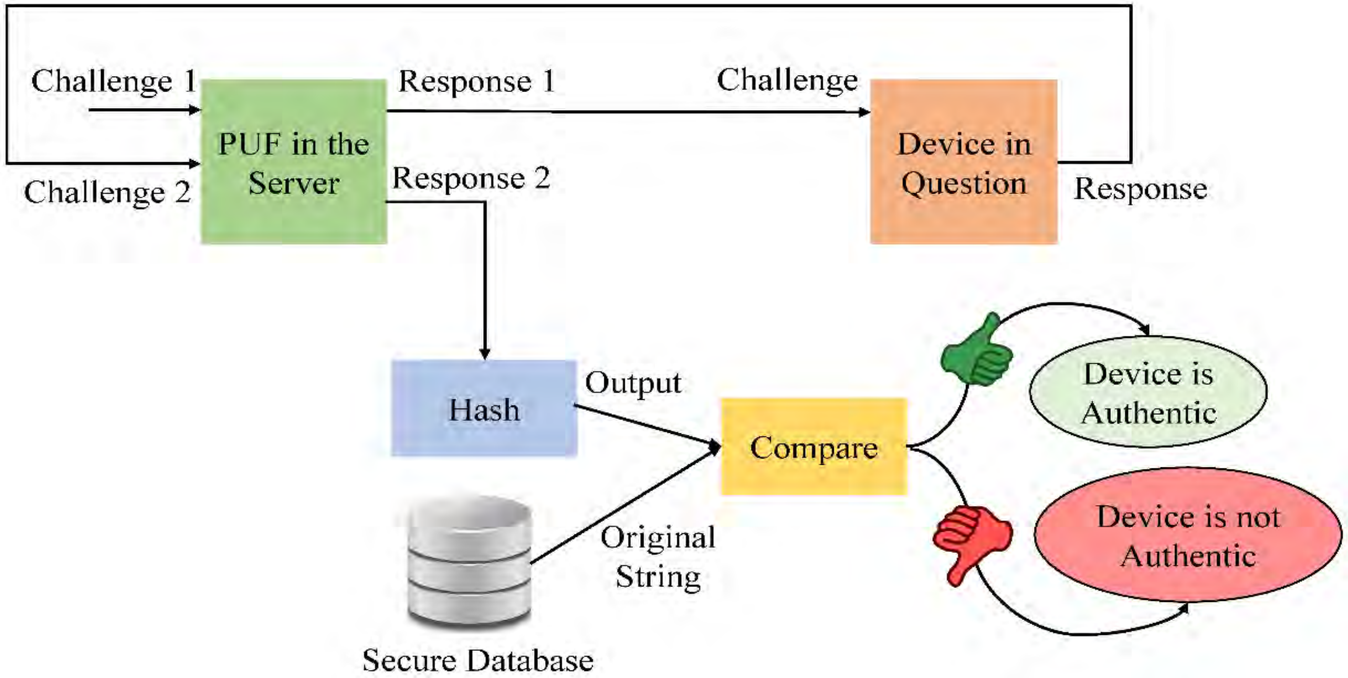



PUF Security Full Proof:

- 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

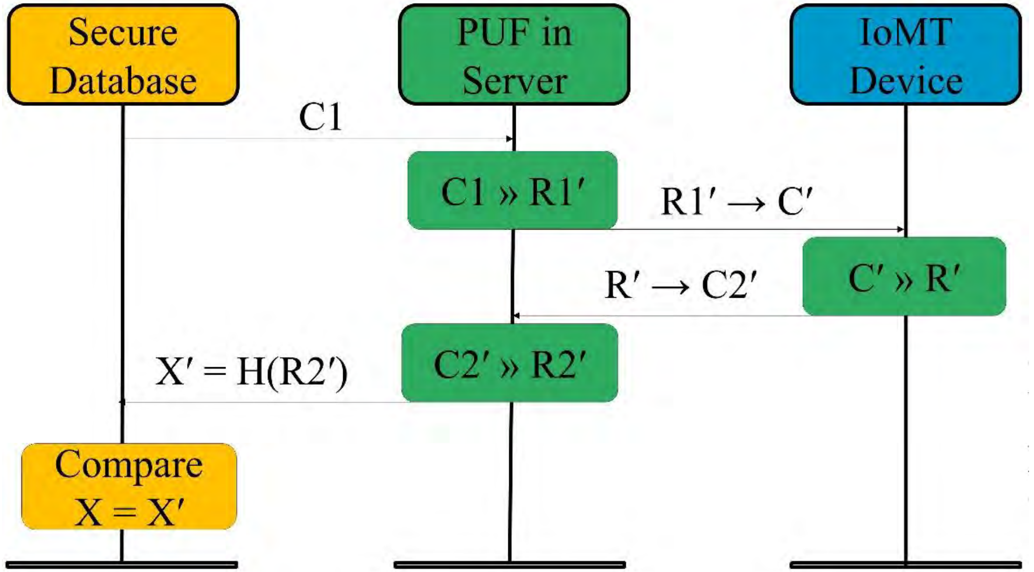



Authentication Phase

At the Doctor

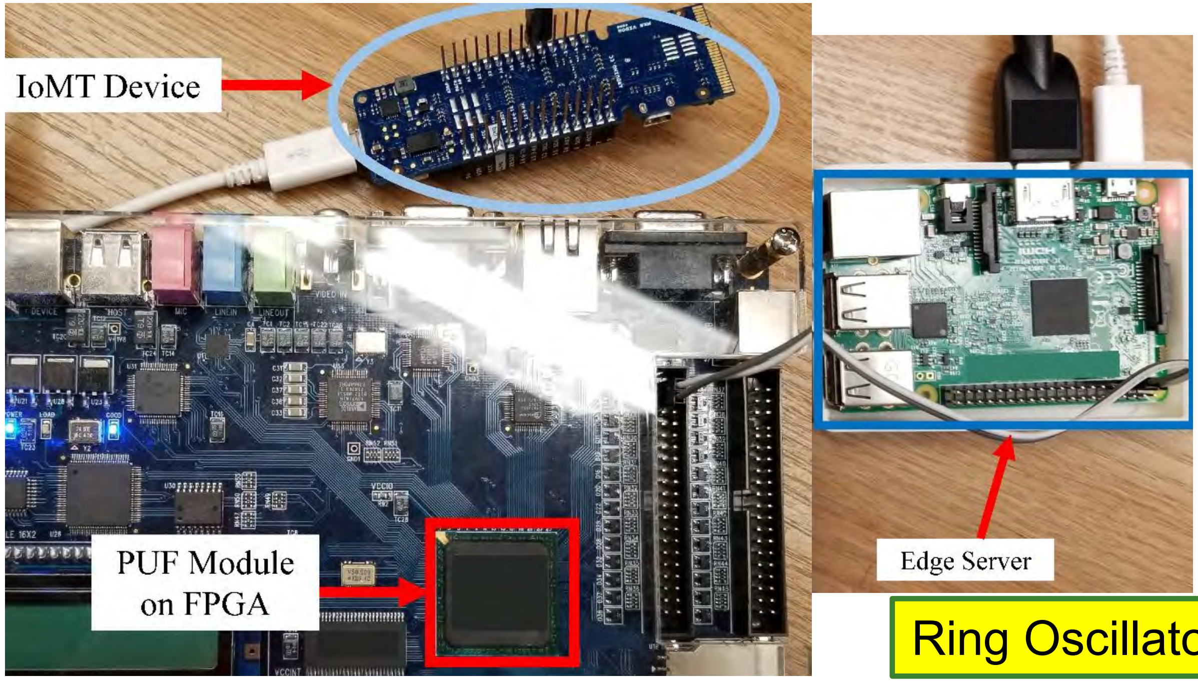
- When doctor needs to access an existing IoMT-device

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



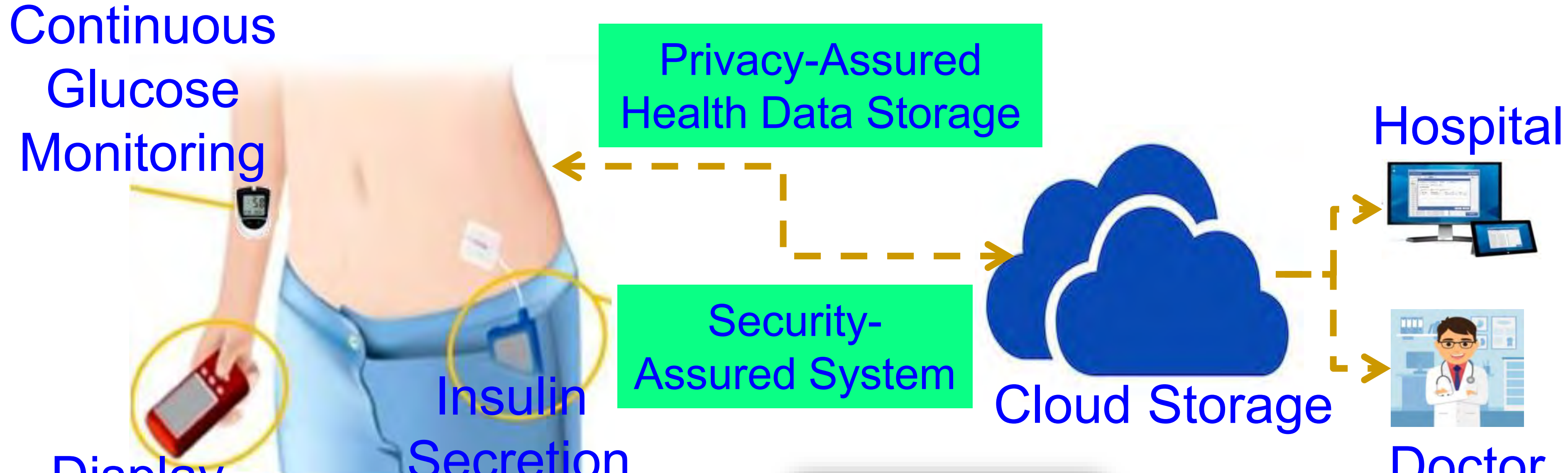

Average Power Overhead – 200 μW

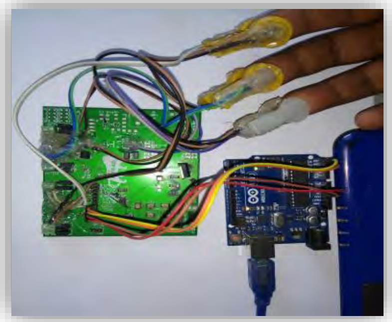
Ring Oscillator PUF – 64-bit, 128-bit, …

| 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.

# Secure-iGLU - Our Intelligent Non-Invasive Glucose Monitoring with Insulin Control Device



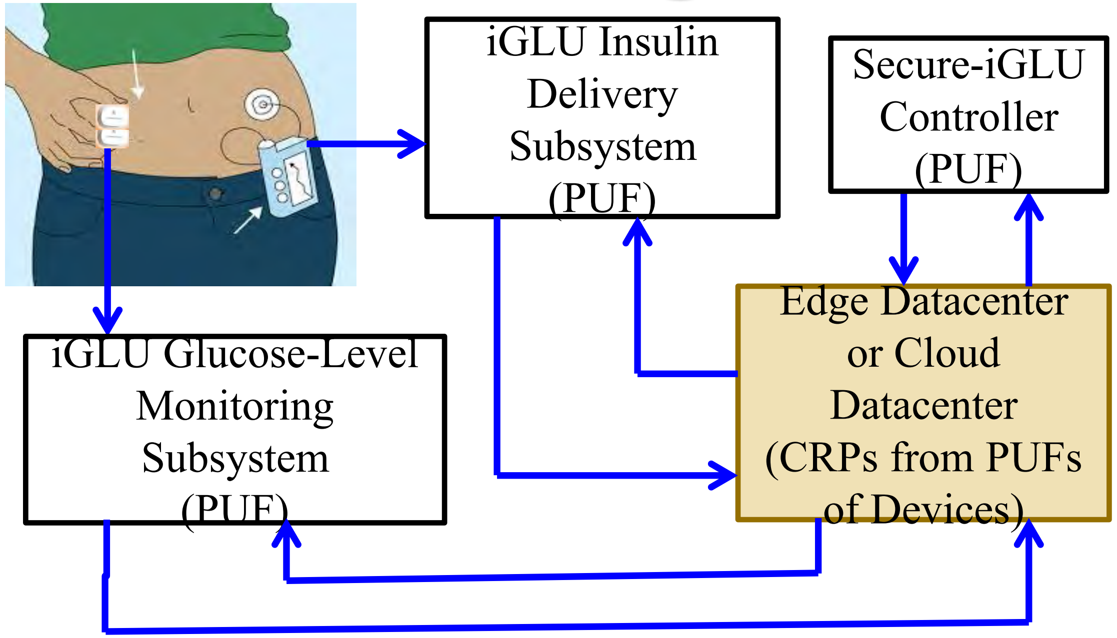



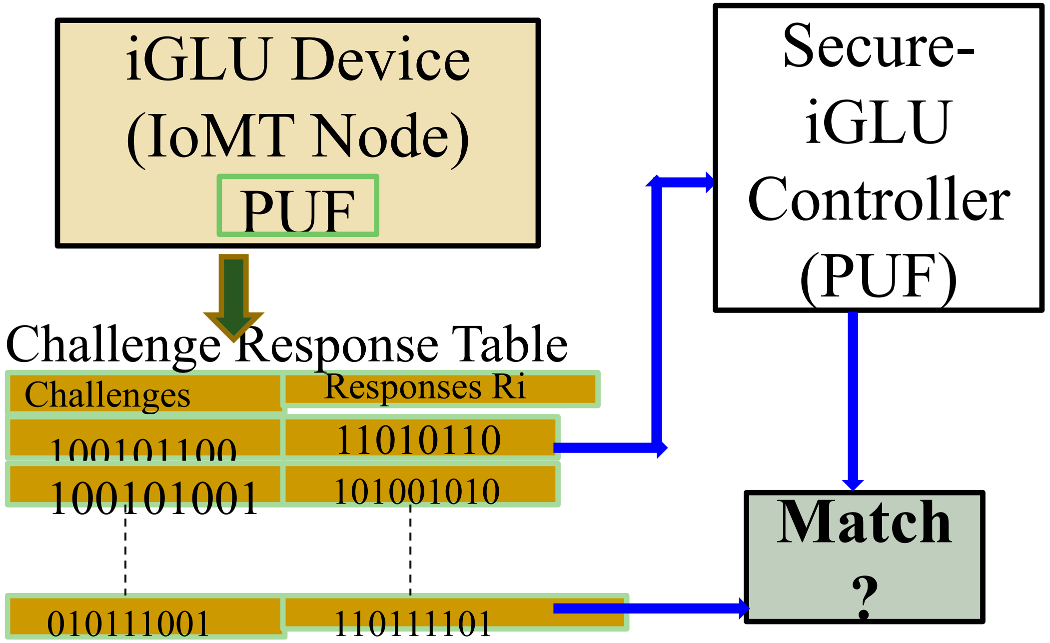
Near Infrared (NIR) based Noninvasive, Accurate, Continuous Glucose Monitoring

Smart Healthcare (H-CPS)
→ Security, Privacy, …

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

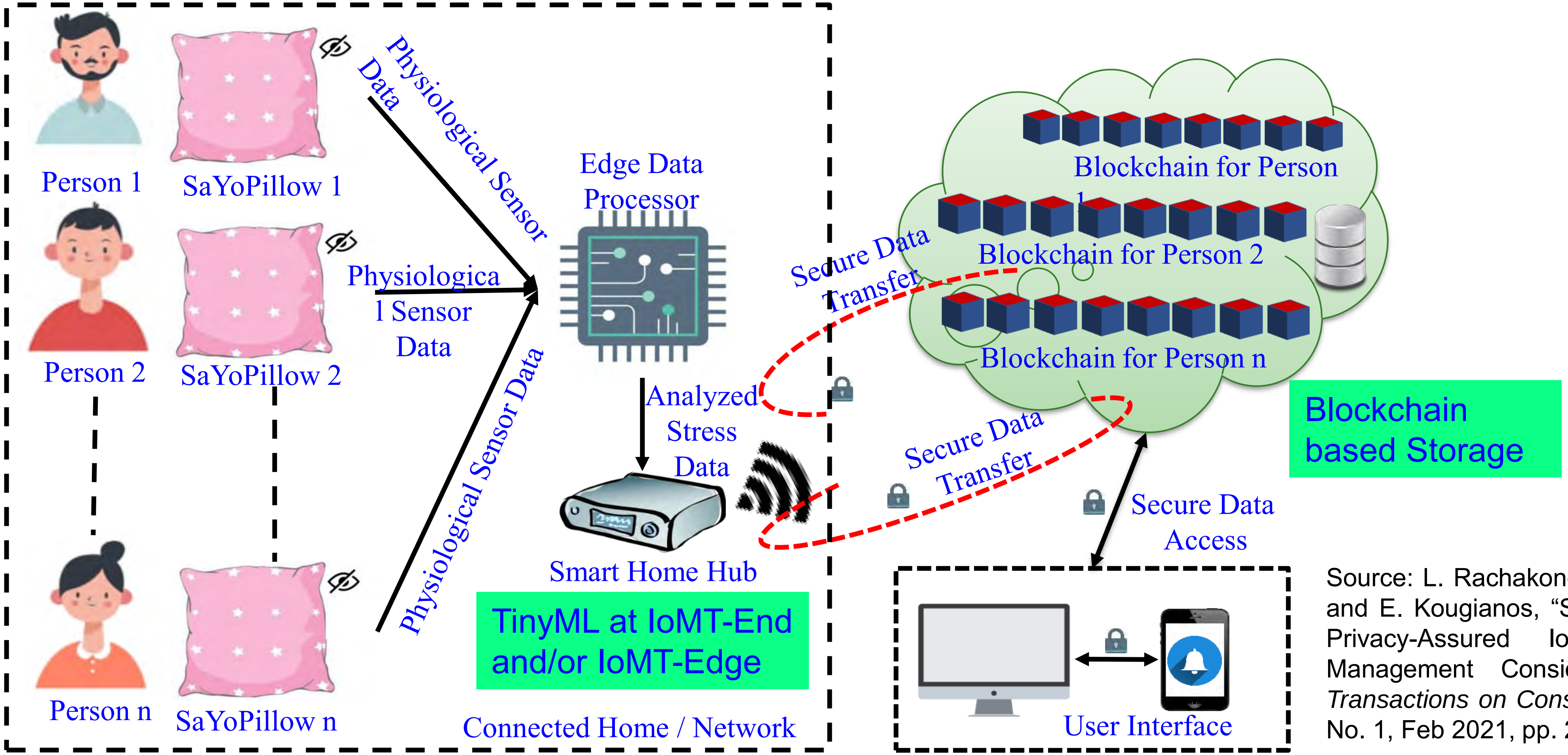



Arbiter PUF – 64-bit, 128-bit, 256 bit …

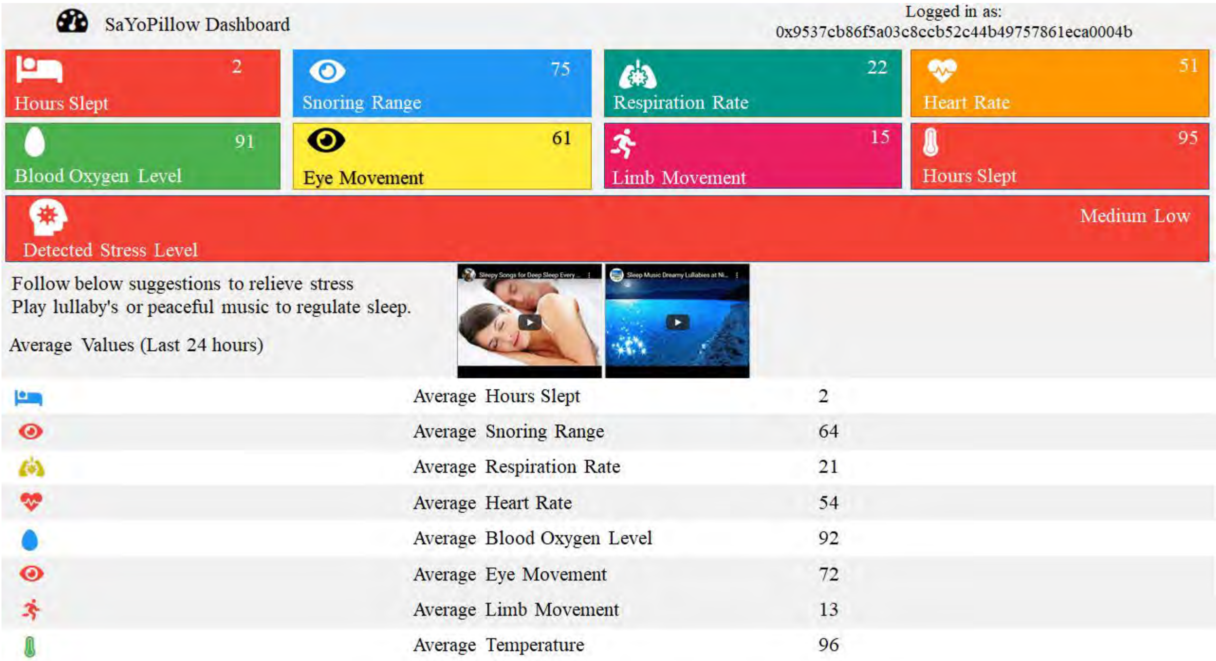
Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

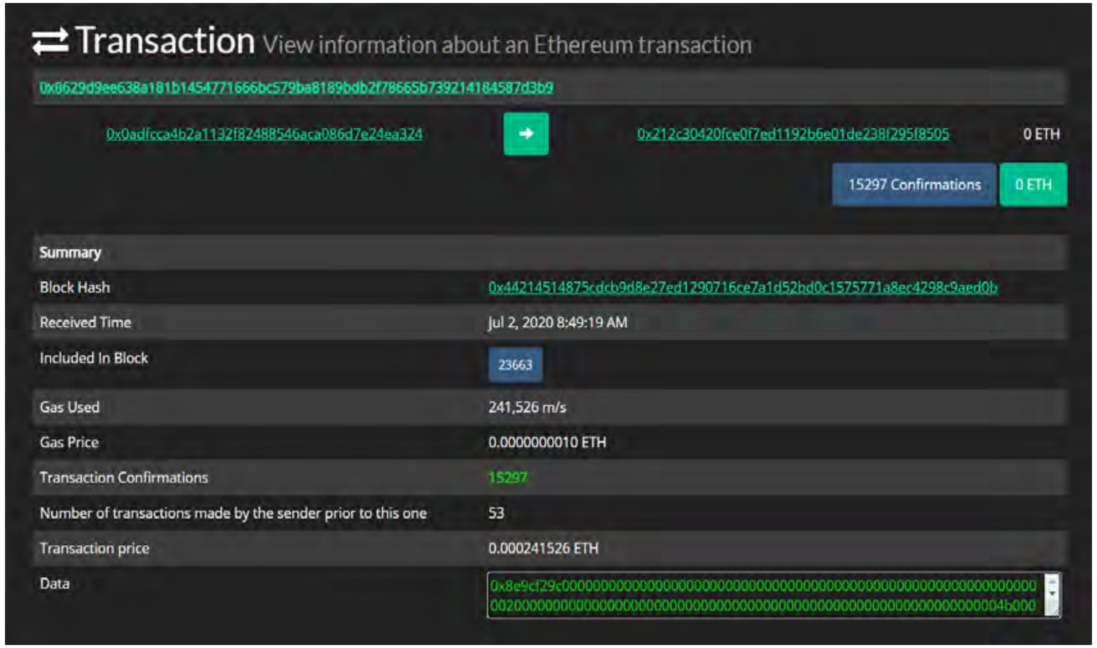
# Our Smart-Yoga Pillow (SaYoPillow) with TinyML and Blockchain based Security

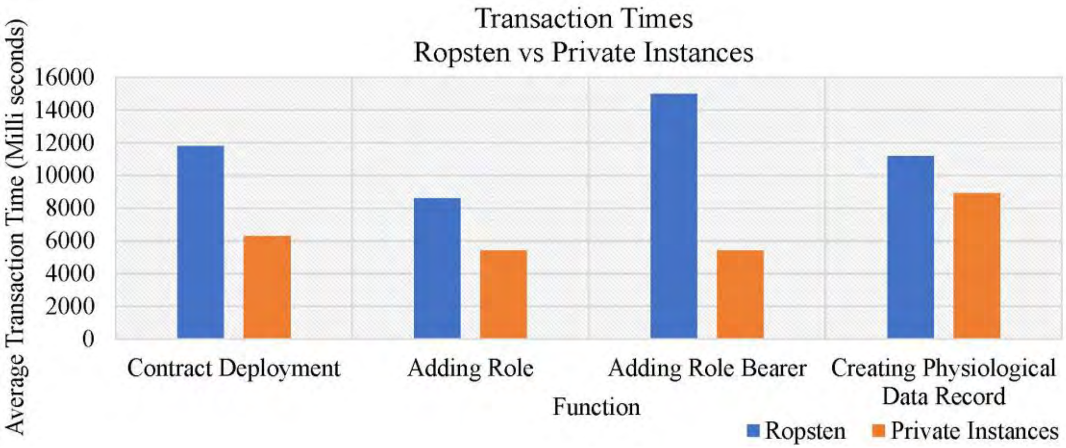



Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habit", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

# SaYoPillow: Blockchain Results



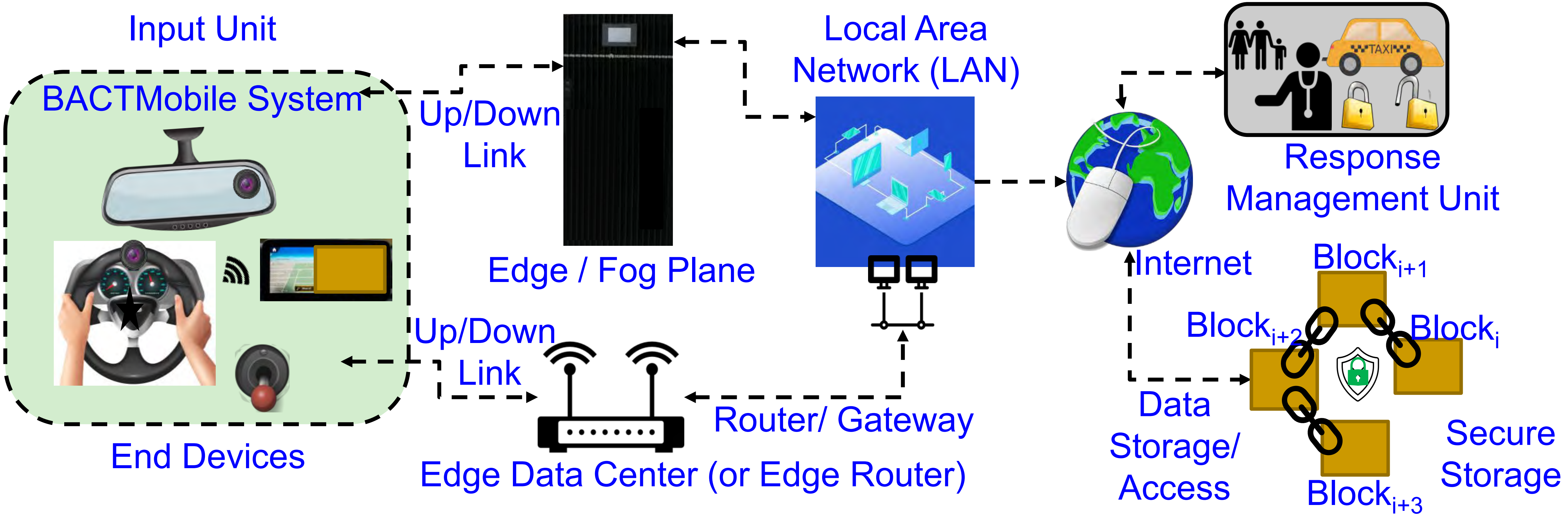




**Transaction times of Private Ethereum in SaYoPillow is 2X faster in operations as compared to public ethereum test network Ropsten, as it is impacted by network congestion.**

Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

# Our Smart Blood Alcohol Concentration Tracking Mechanism in Healthcare CPS - BACTmobile

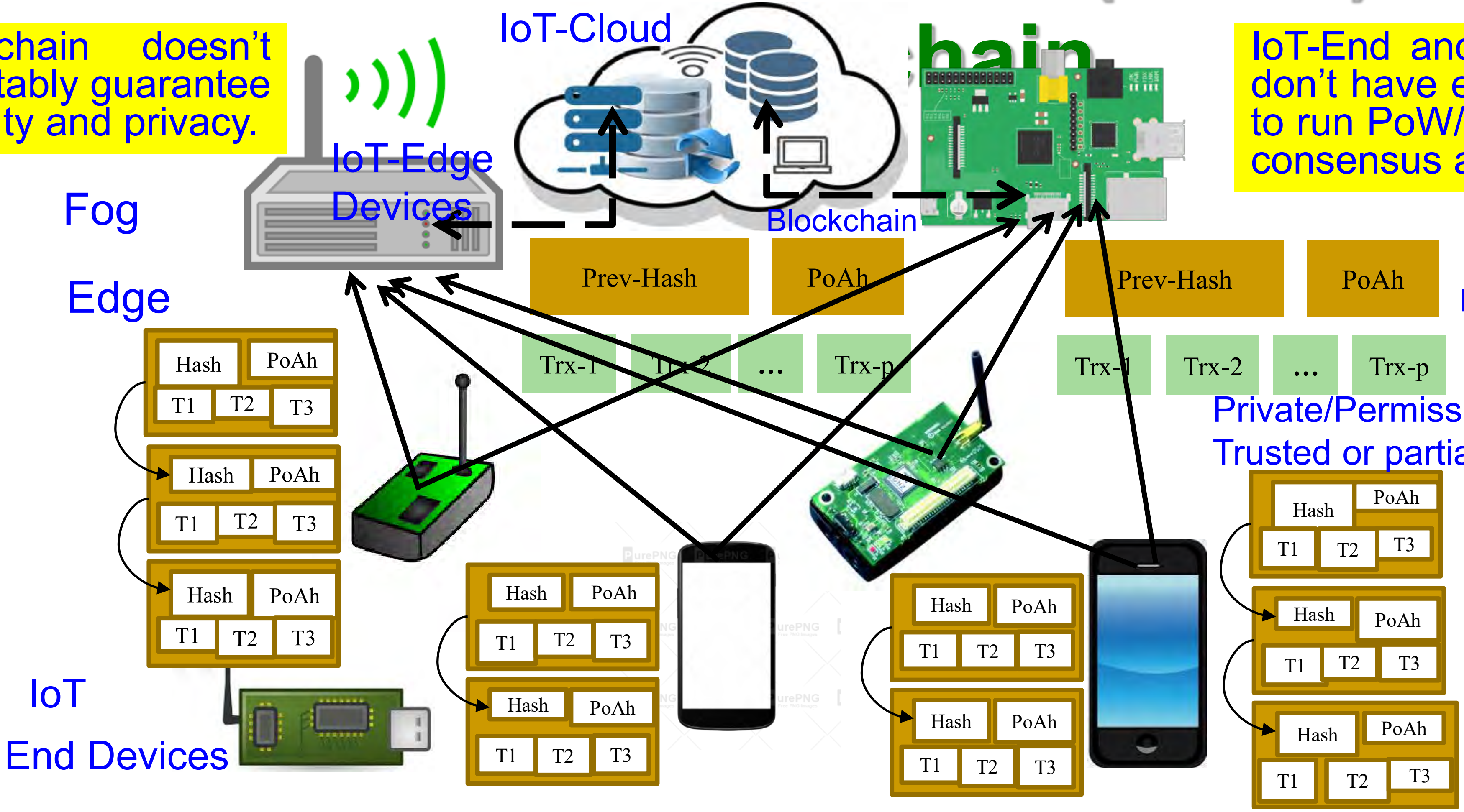



Source: L. Rachakonda, A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "BACTmobile: A Smart Blood Alcohol Concentration Tracking Mechanism for Smart Vehicles in Healthcare CPS Framework", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 236, 24-pages, DOI: https://doi.org/10.1007/s42979-022-01142-9.

# IoT-Friendly Blockchain – EasyChain: Our Proof-of-Authentication (PoAh) based Blockchain

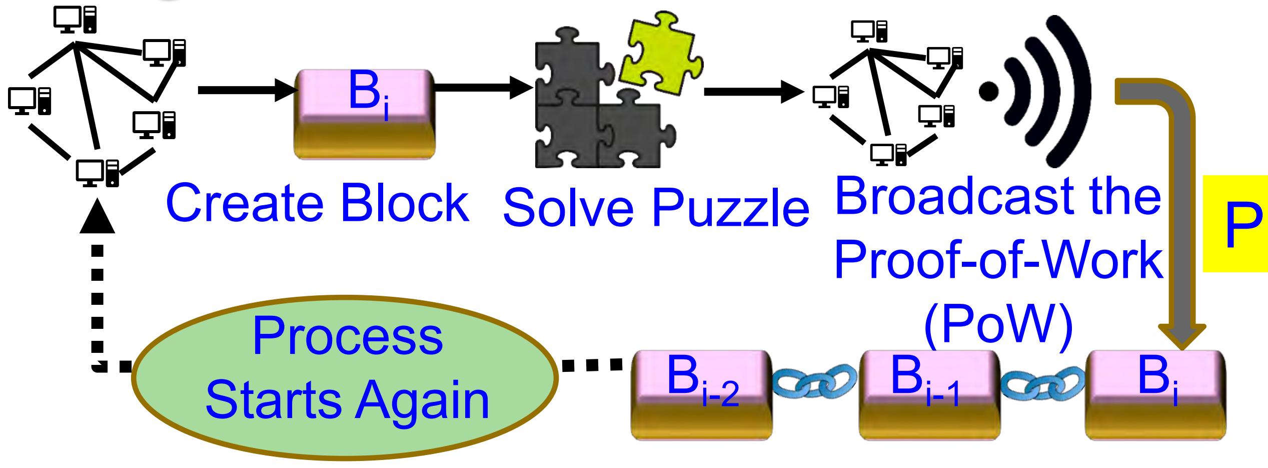
Blockchain doesn't inheritably guarantee security and privacy.

IoT-End and IoT-Edge Devices don't have enough horse power to run PoW/PoS like heavy duty consensus algorithms.




Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

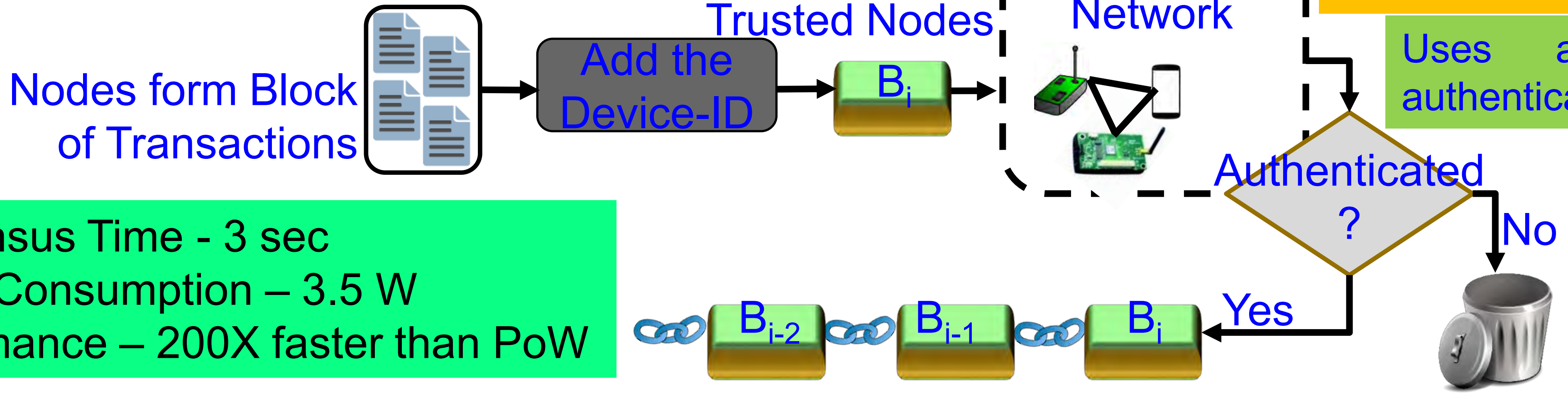
# Our EasyChain: Proof-of-Authentication (PoAh)




Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.

Proof of Authentication (PoAh)

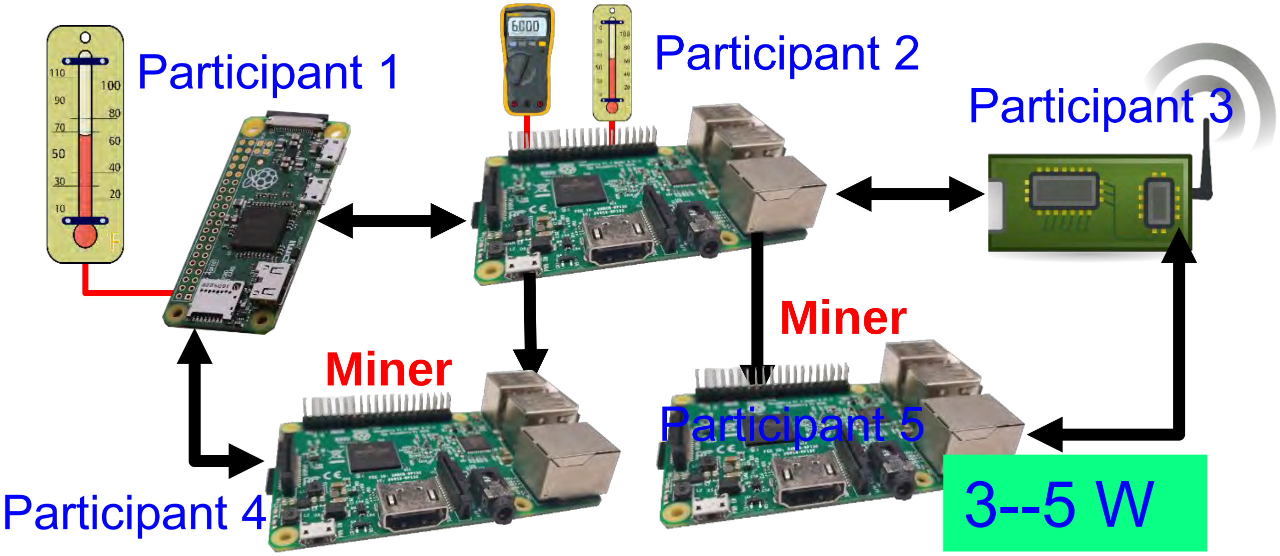



Uses a cryptographic authentication mechanism.

Consensus Time - 3 sec
Power Consumption – 3.5 W
Performance – 200X faster than PoW

Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

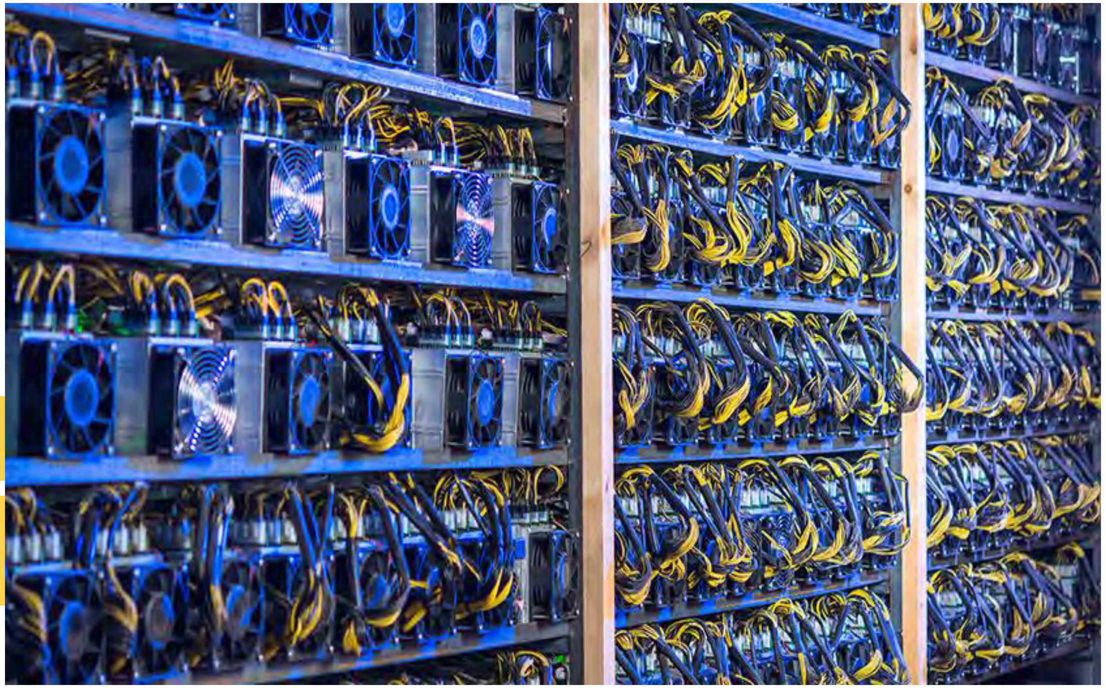
# Our EasyChain with PoAh Runs in Resource Constrained Environment




Our PoAh-Chain Runs even in IoT-end devices.

Blockchain using PoW Needs Significant Resource

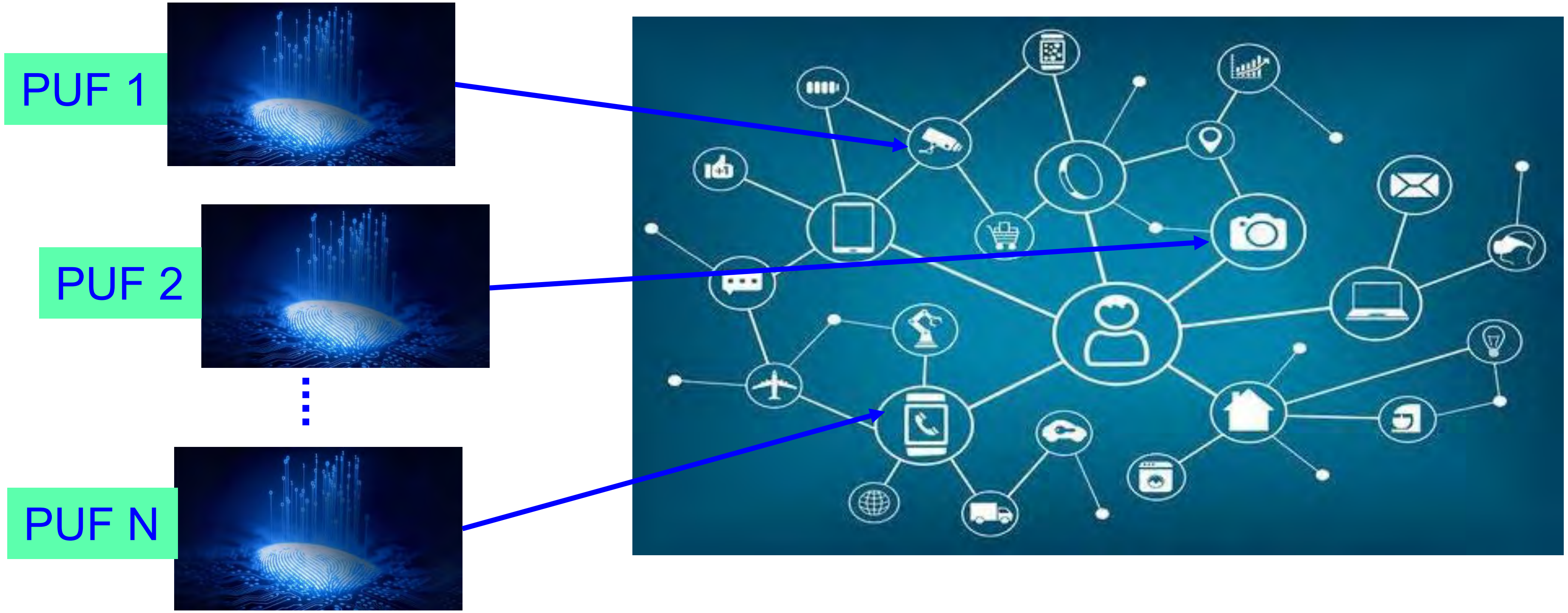
500,0000 W



Source: D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, “PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks”, *arXiv Computer Science*, arXiv:2001.07297, January 2020, 26-pages.

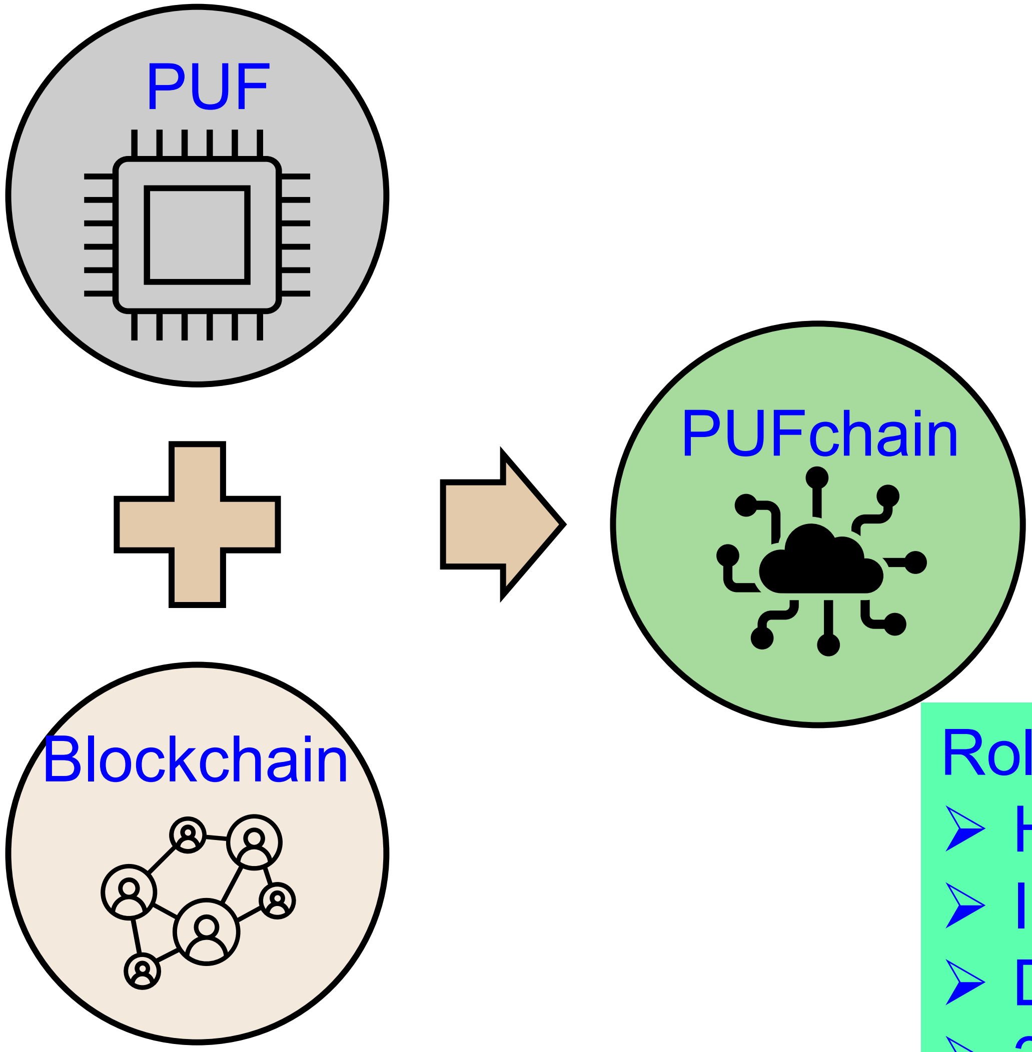
Source: https://www.iea.org/newsroom/news/2019/july/bitcoin-energy-use-mined-the-gap.html

# 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



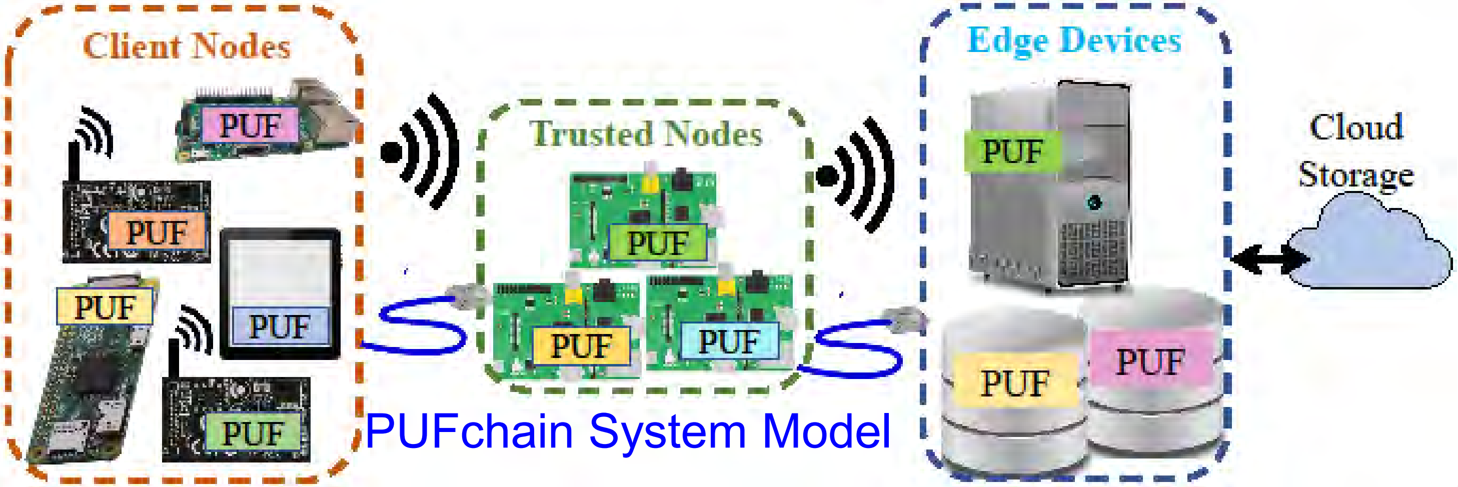

Blockchain Technology is integrated with Physically Unclonable Functions as PUFchain by storing the PUF Key into immutable Blockchain

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

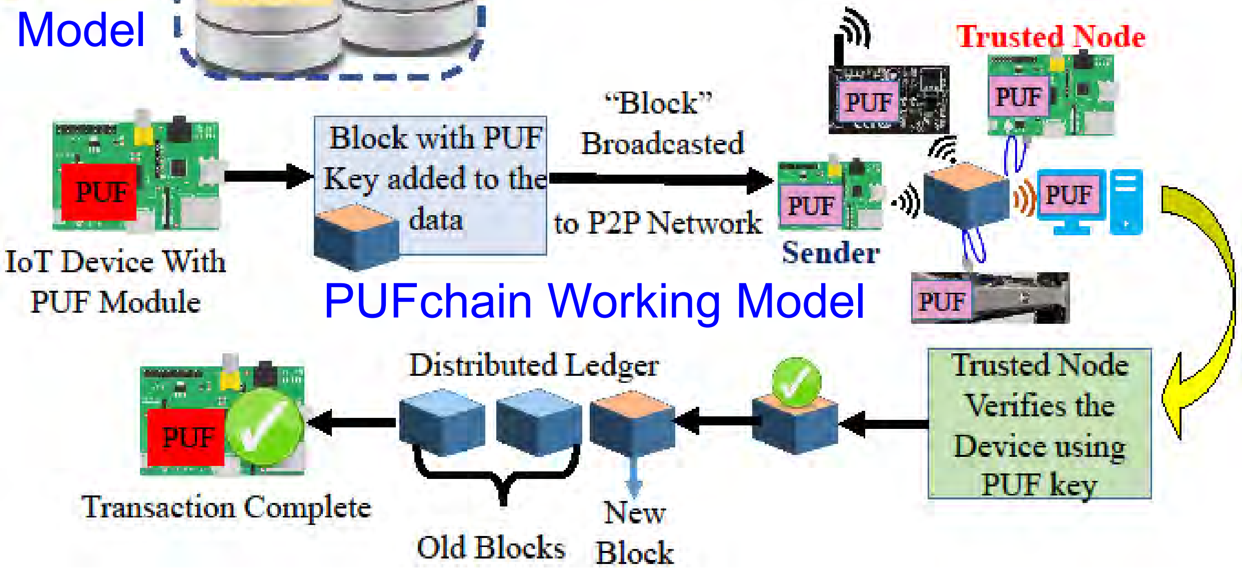
# Our PUFchain – 3 Variants

| 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




Can provide:
Device, System, and
Data Security

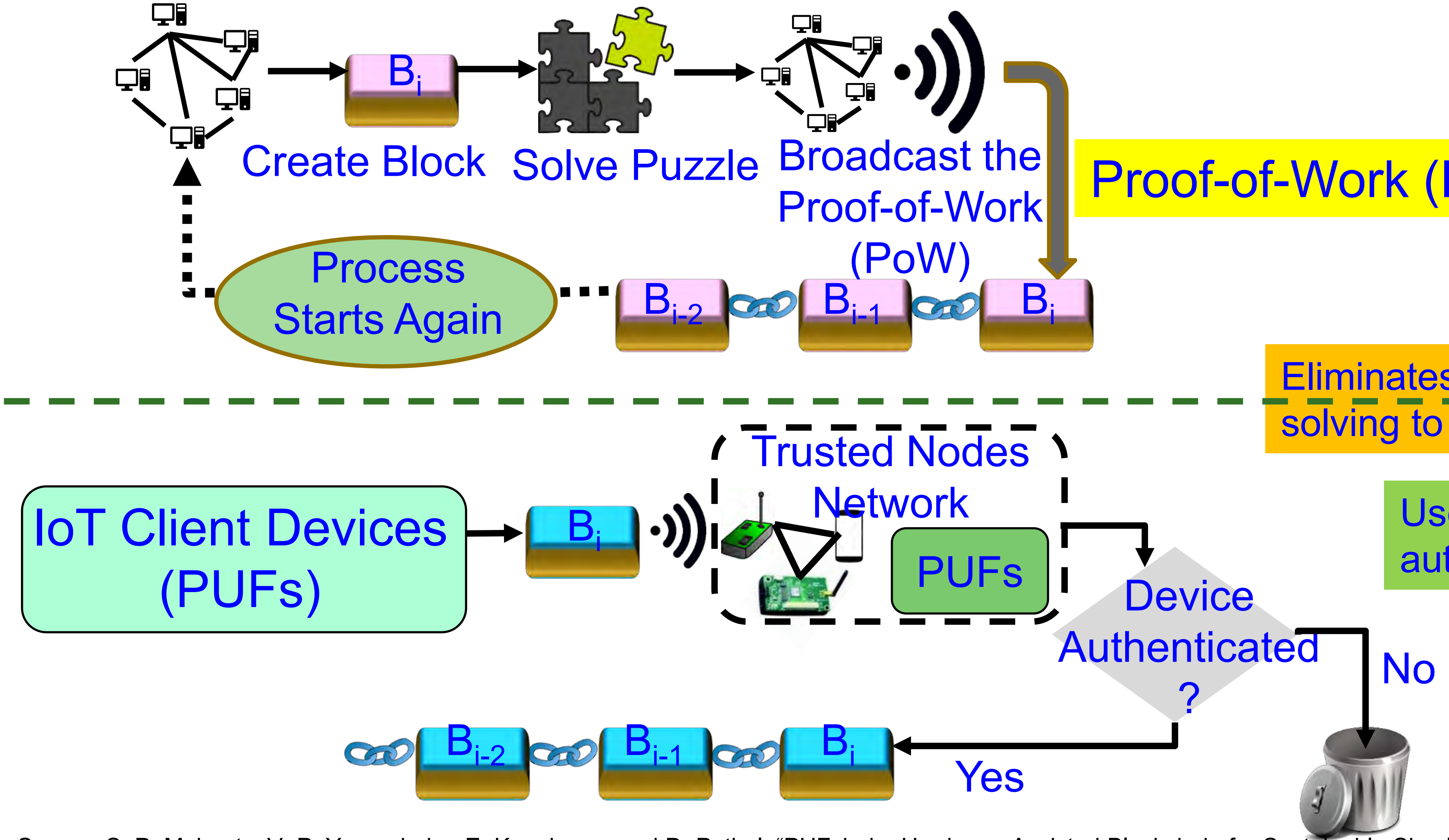



PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode

- ✓ 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)



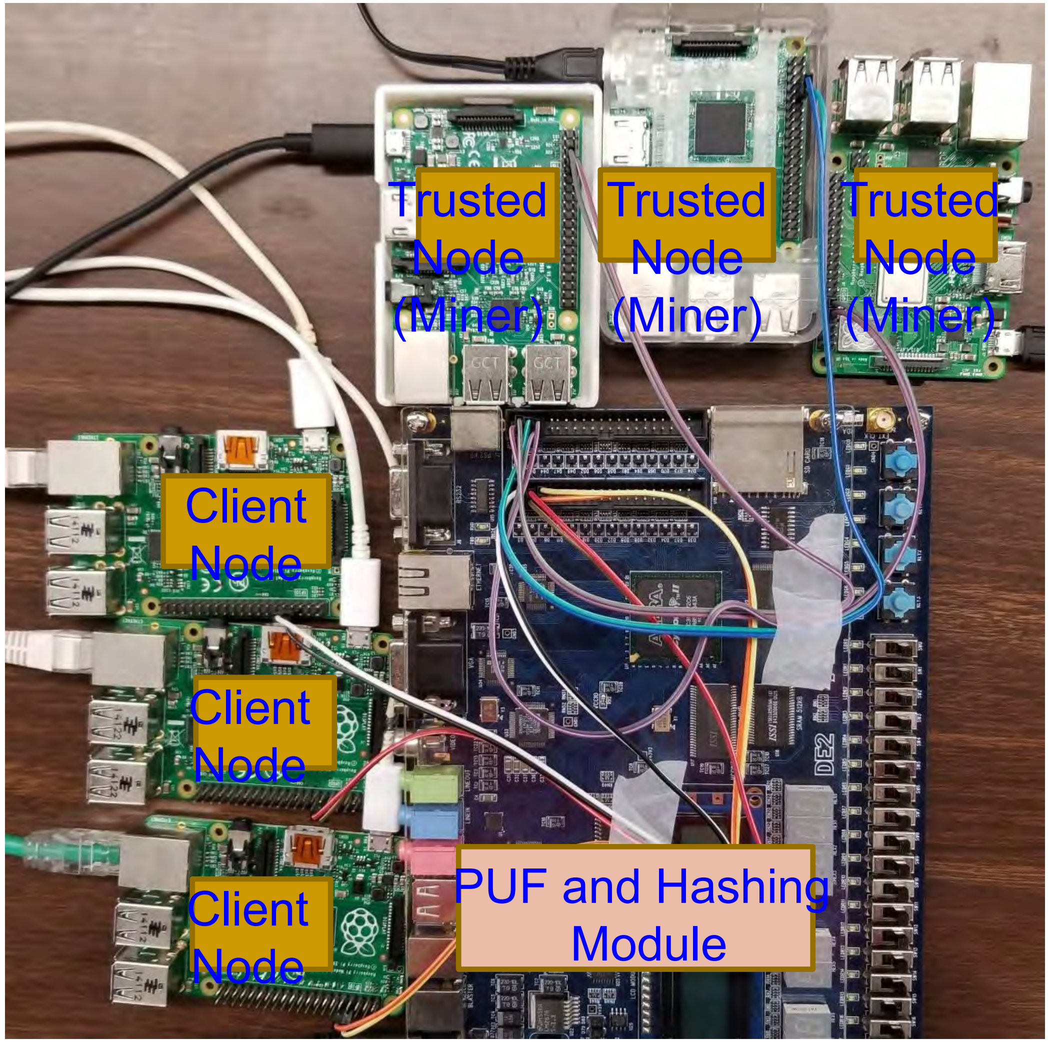

Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.

Uses a PUF-based authentication mechanism.

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

# PUFchain: Our PoP is 1000X Faster than PoW

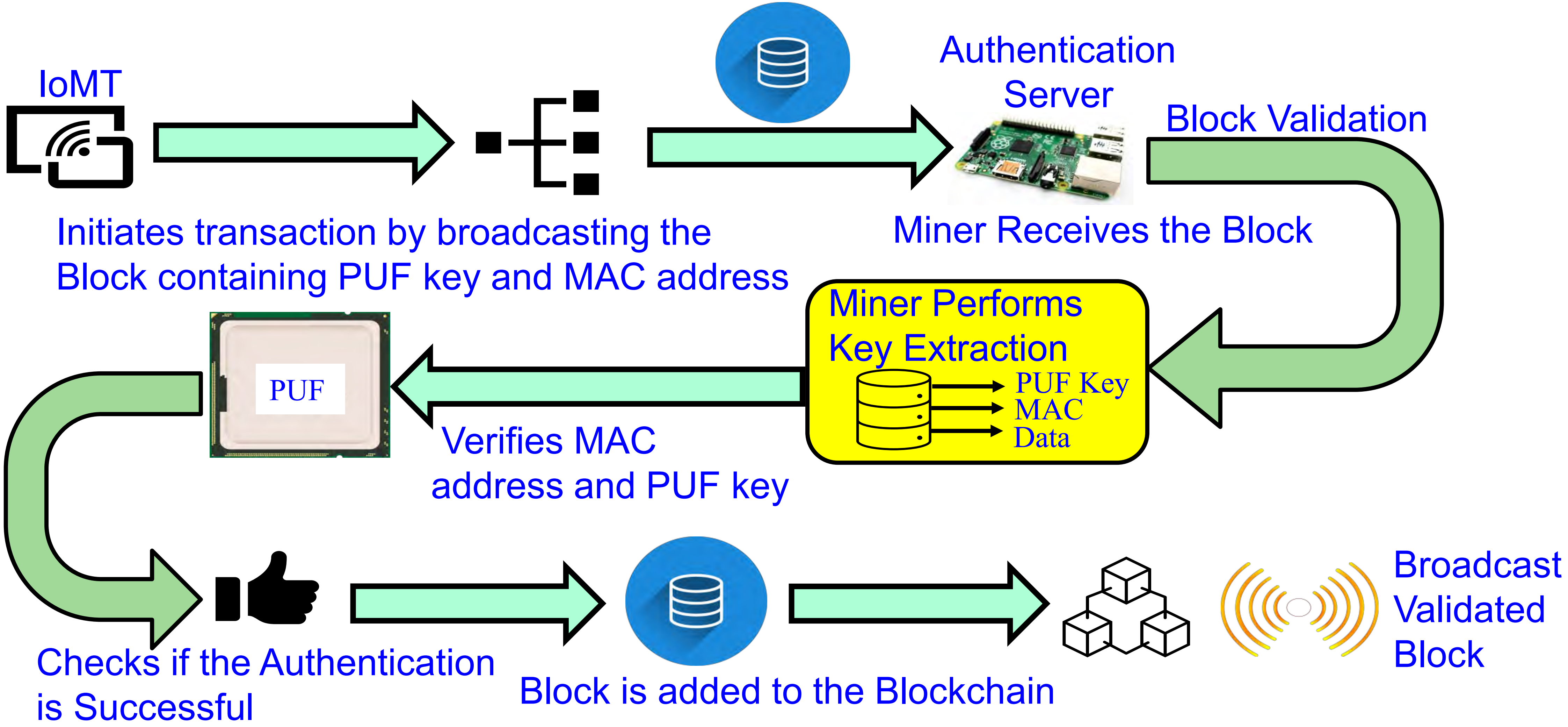



| | | |
|---|---|---|
| PoW - 10 min in cloud | PoAh – 950ms in Raspberry Pi | PoP - 192ms in Raspberry Pi |
| High Power | 3 W Power | 5 W Power |

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

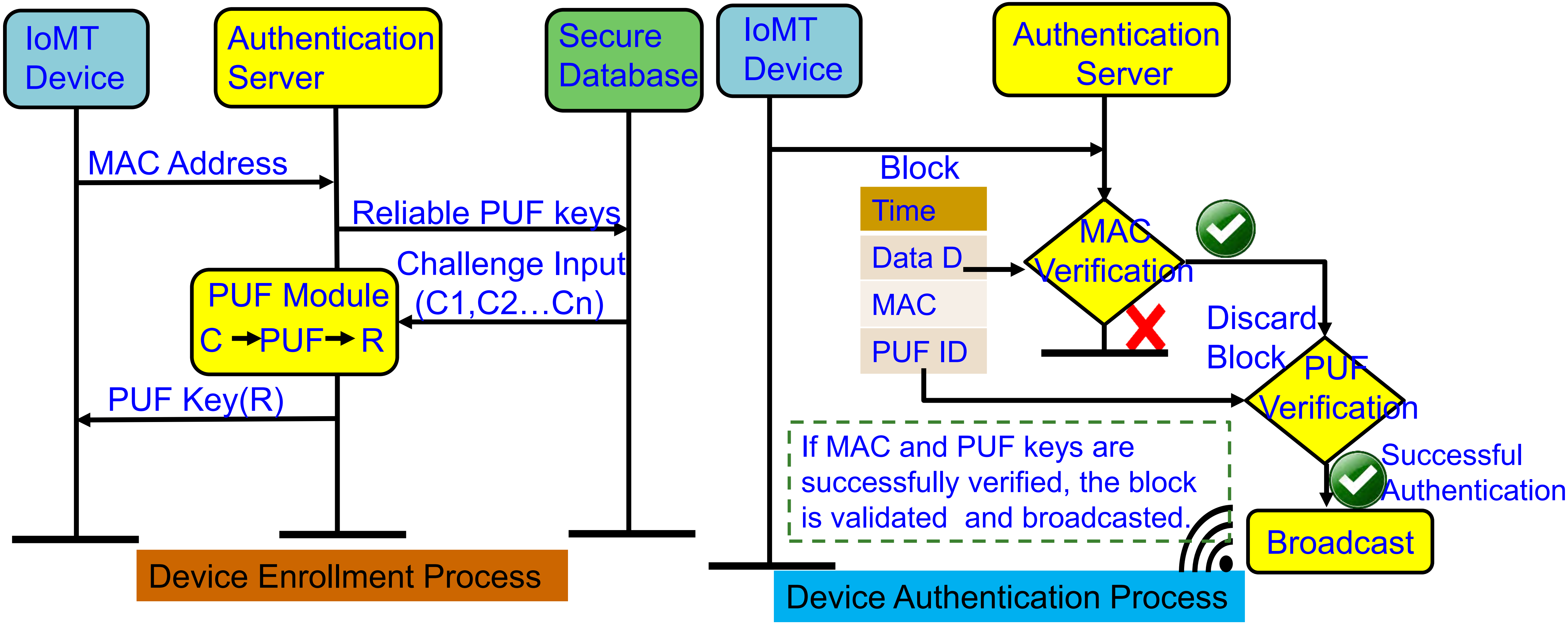
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

# PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



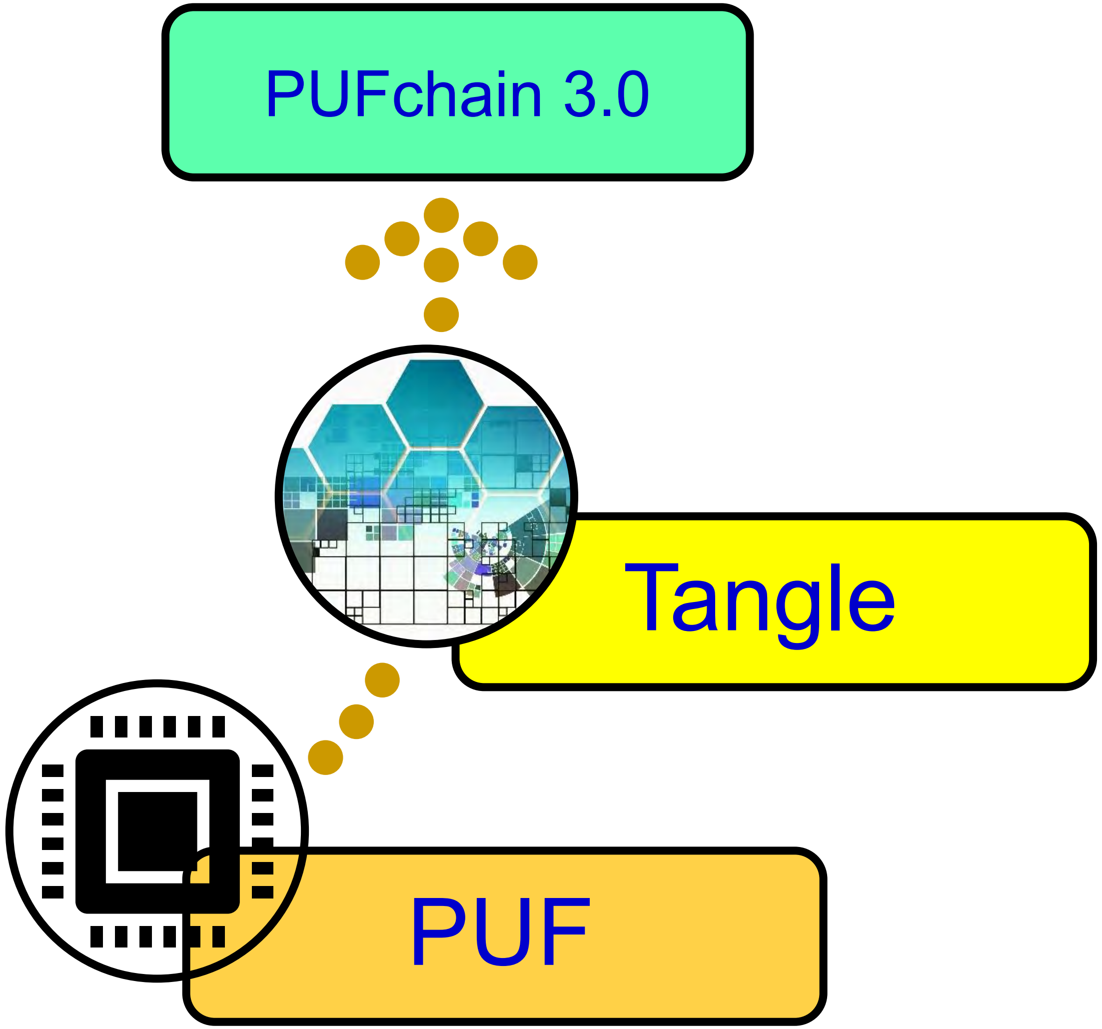

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

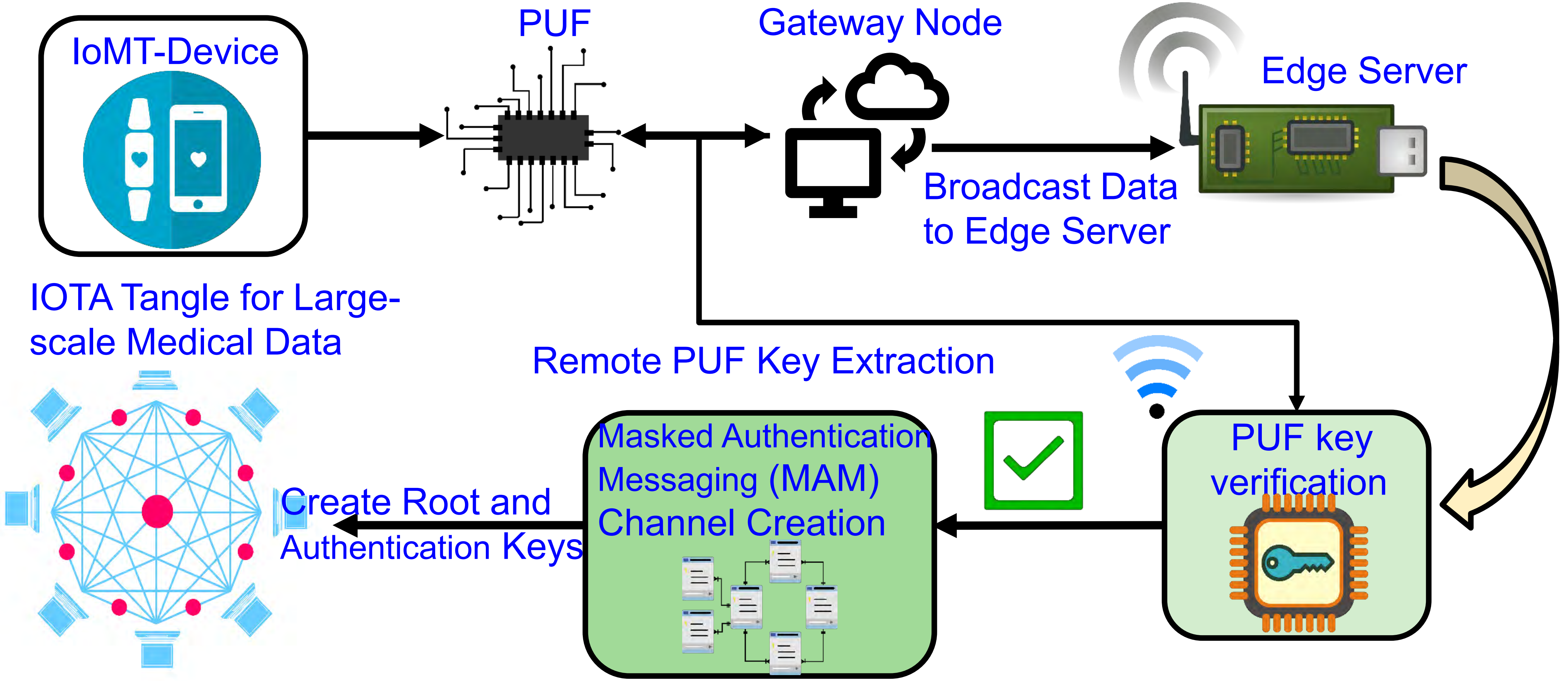
# PUFchain 3.0 - Conceptual Idea




- 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.

# PUFchain 3.0: Comparative Analysis

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

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

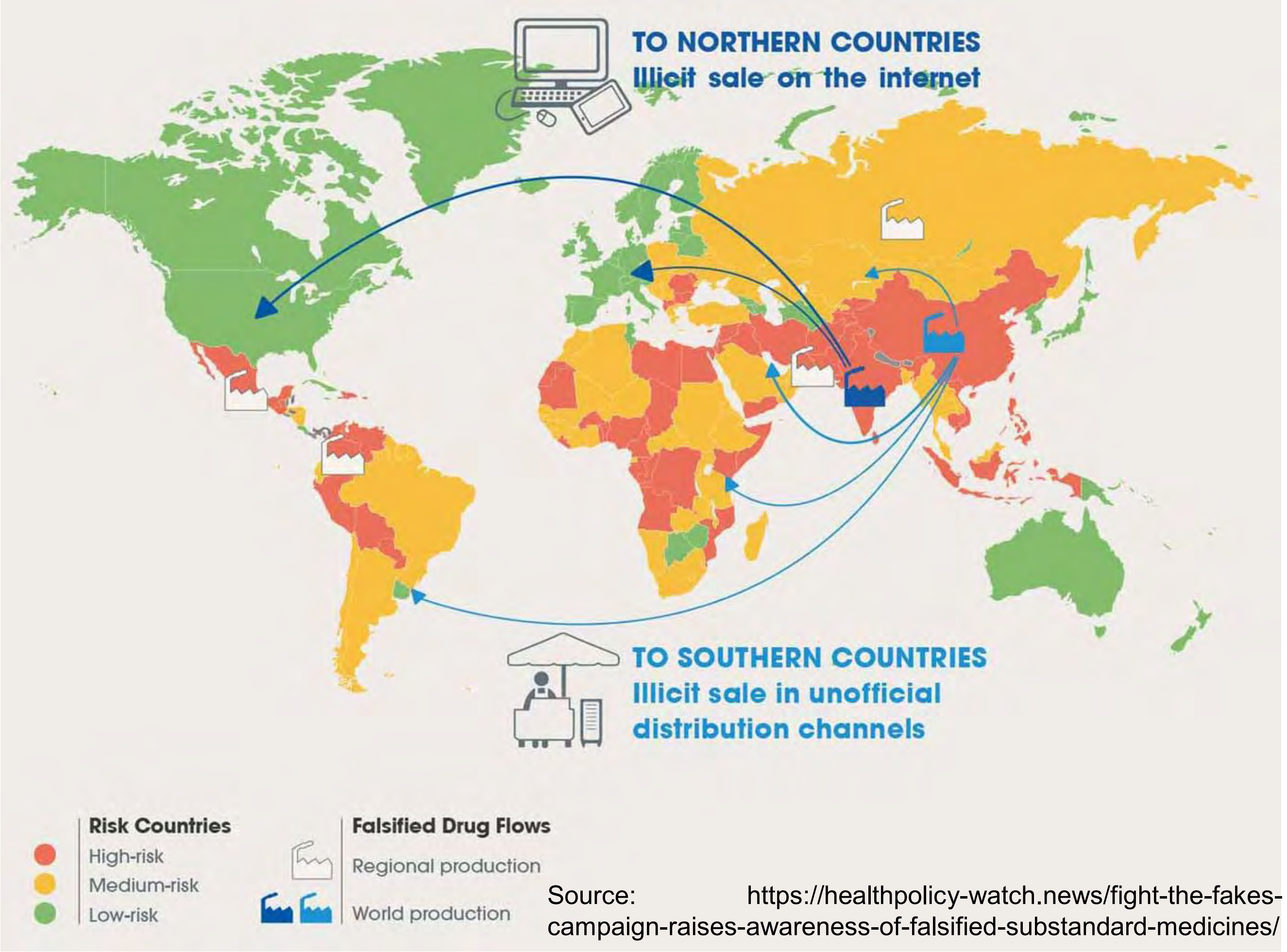
# Smart Healthcare – Trustworthy Pharmaceutical Supply Chain

# Fake Medicine - Serious Global Issue

- It is estimated that close to $83 billion worth of counterfeit drugs are sold annually.
- One in 10 medical products circulating in developing countries are substandard or fake.
- In Africa: Counterfeit antimalarial drugs results in more than 120,000 deaths each year.
- USA has a closed drug distribution system intended to prevent counterfeits from entering U.S. markets, but it isn't foolproof due to many reason including illegal online pharmacy.

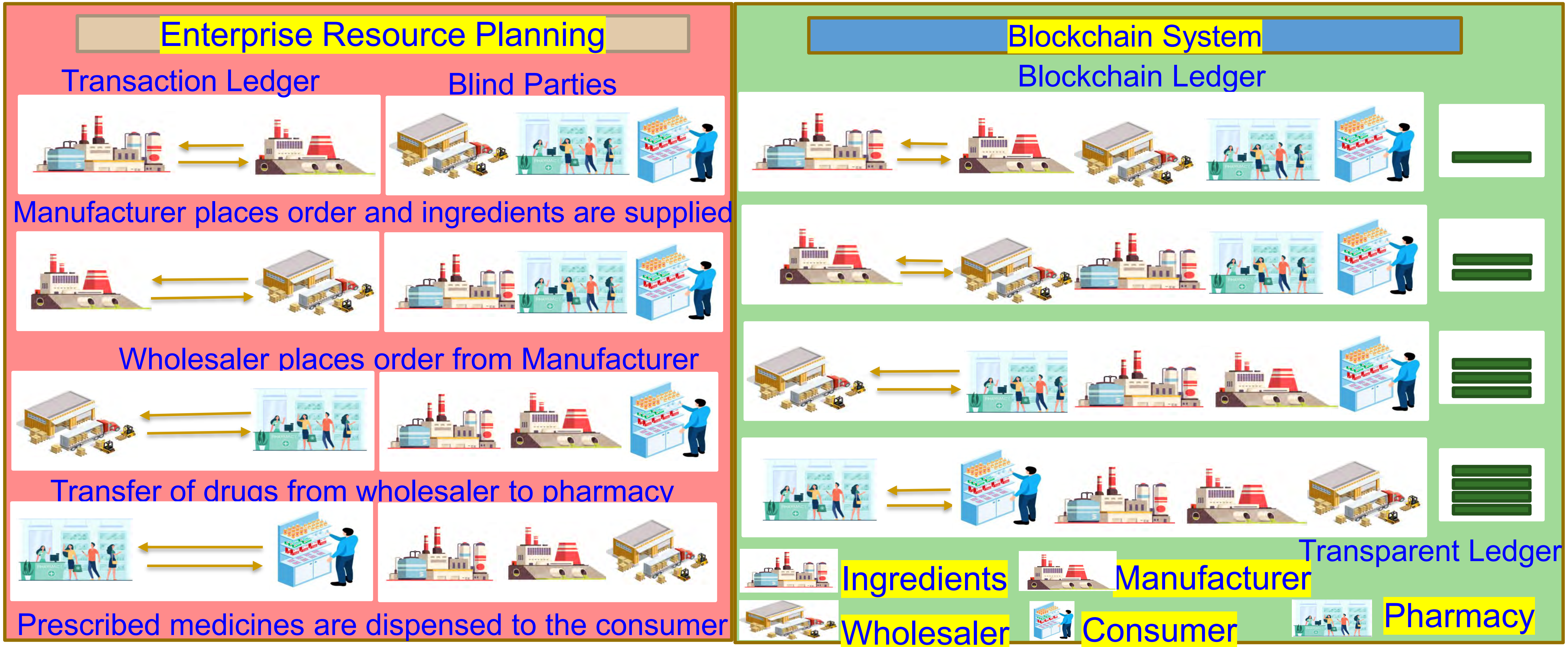
Source: https://fraud.org/fakerx/fake-drugs-and-their-risks/counterfeit-drugs-are-a-global-problem/


Source: https://allaboutpharmacovigilance.org/be-aware-of-counterfeit-medicine/



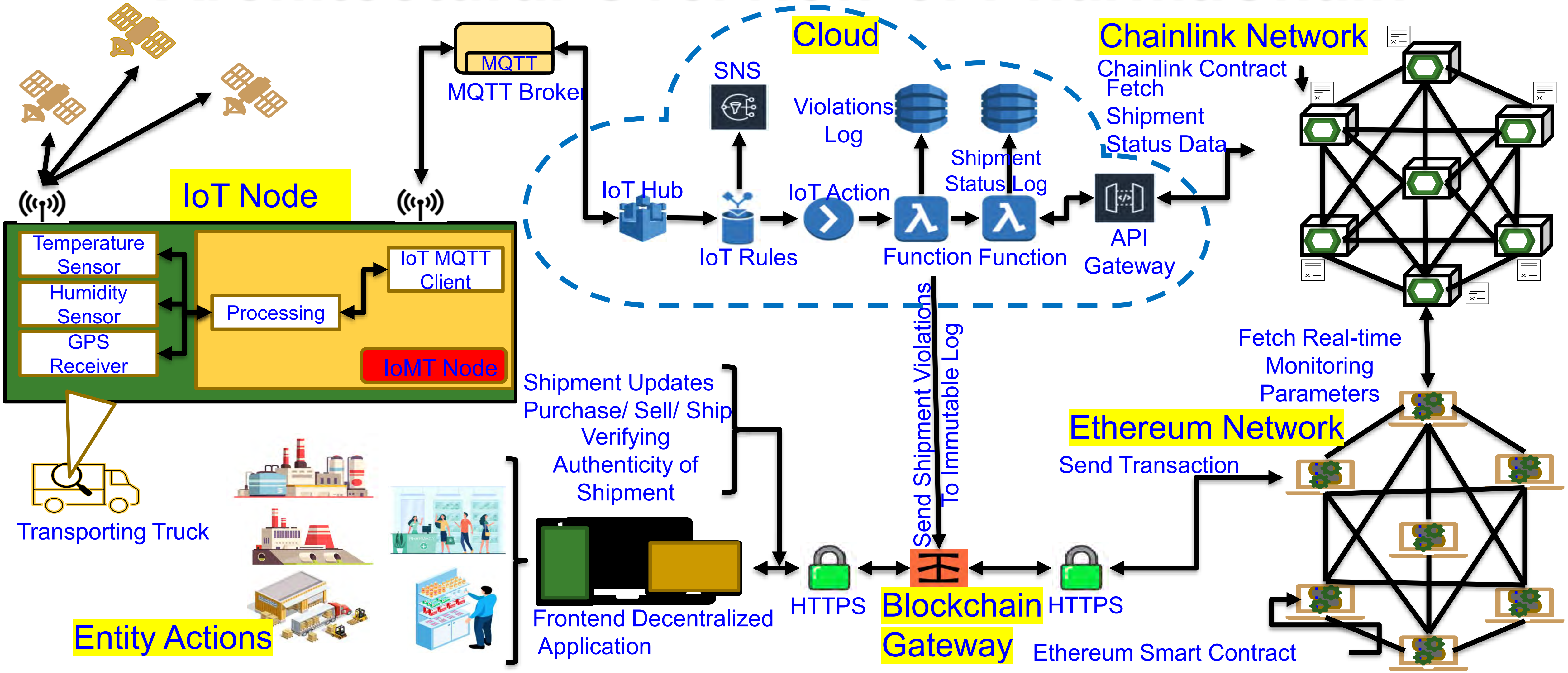

Source: https://healthpolicy-watch.news/fight-the-fakes-campaign-raises-awareness-of-falsified-substandard-medicines/

# PharmaChain - Counterfeit Free Pharmaceutical



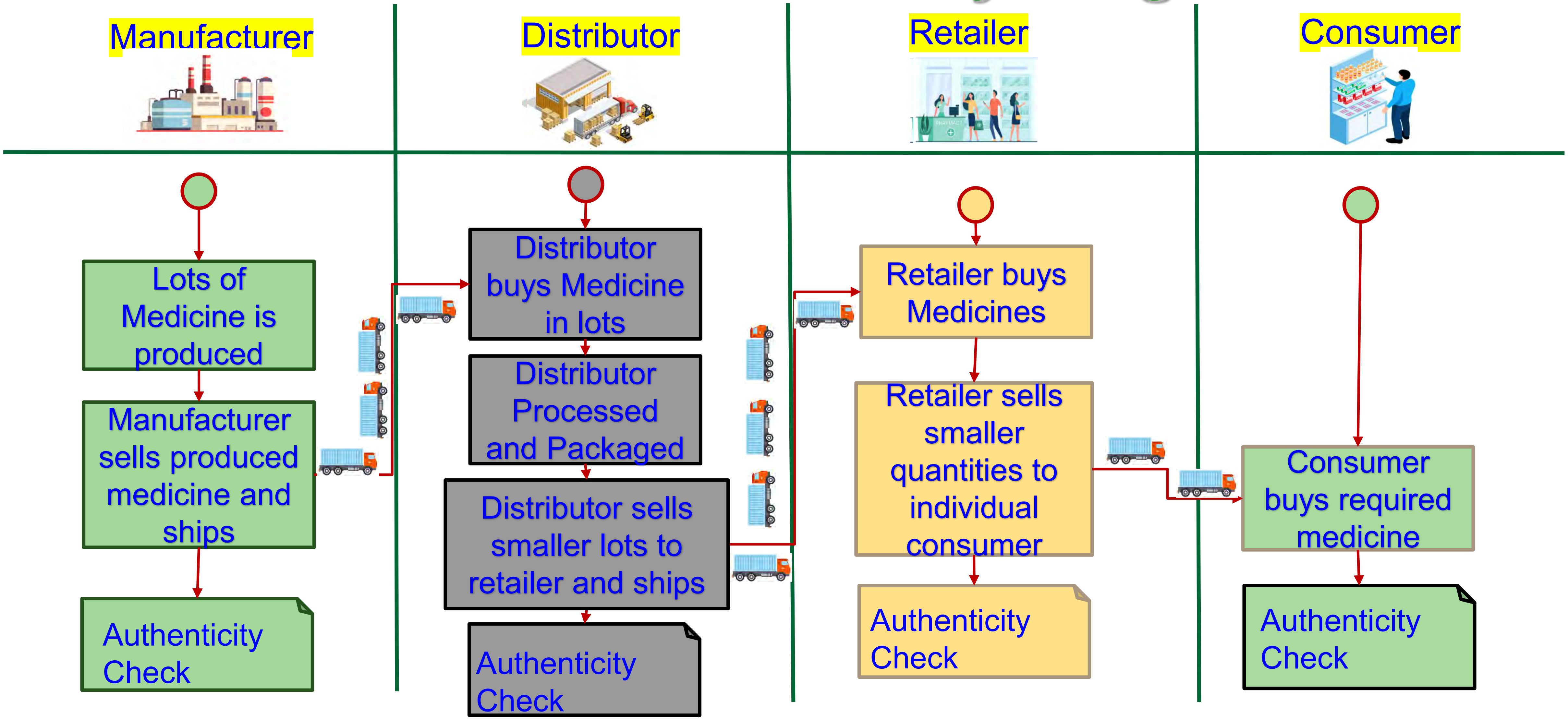

Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: GitHub)

# Architectural Overview of PharmaChain



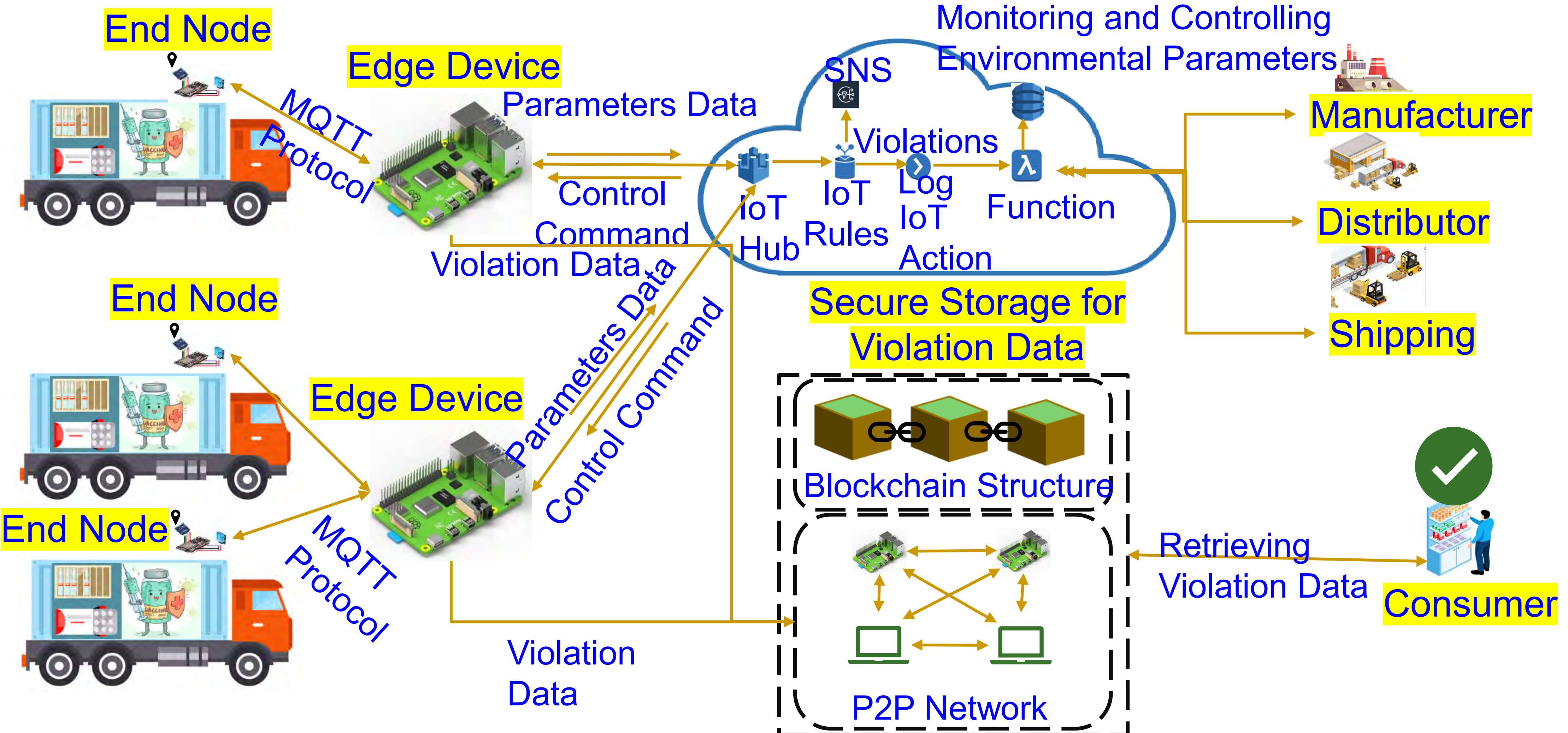

Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: GitHub)

# PharmaChain Entity Diagram




Source: Bapatla, A.K., et al.: PharmaChain: a blockchain to ensure counterfeit-free pharmaceutical supply chain. IET Netw. 1– 24 (2022). https://doi.org/10.1049/ntw2.12041

# PharmaChain 2.0 - Architecture Overview

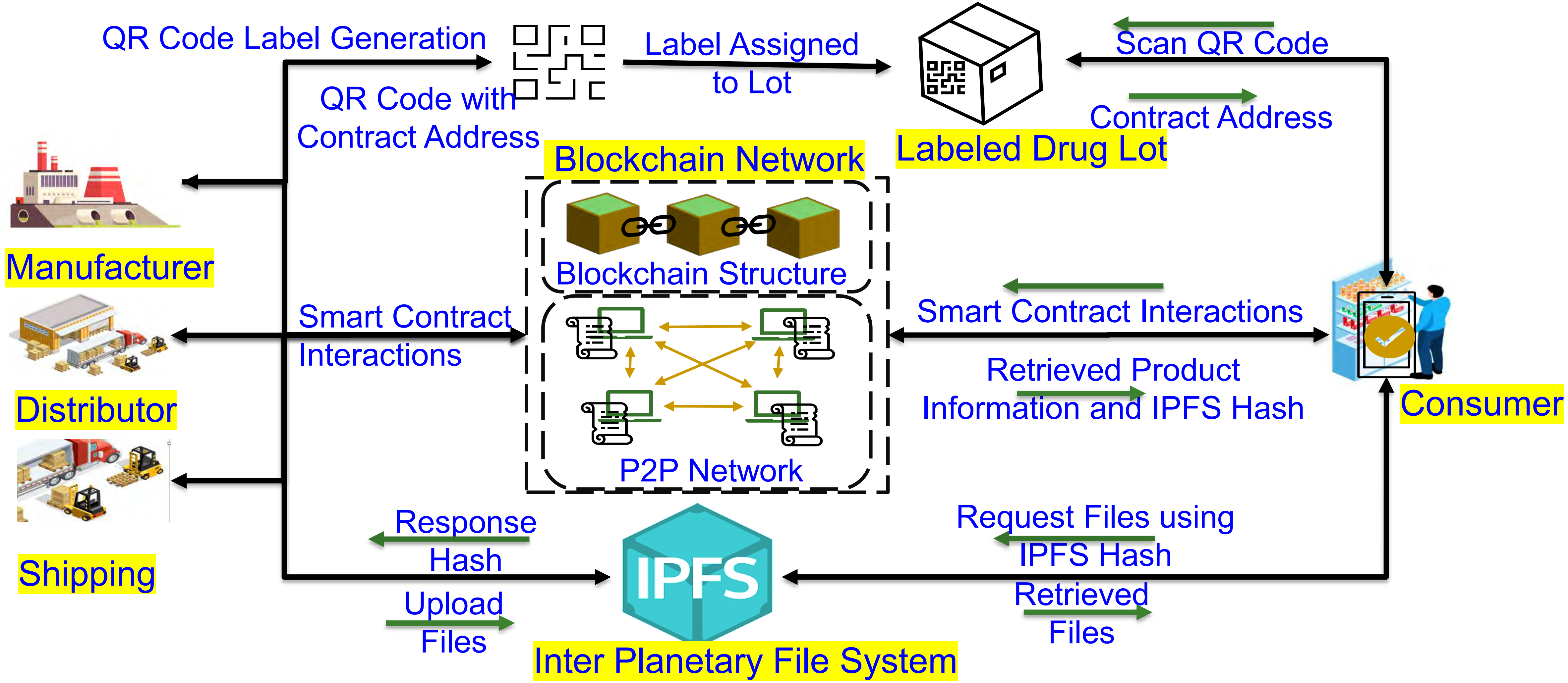



Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PharmaChain 2.0: A Blockchain Framework for Secure Remote Monitoring of Drug Environmental Parameters in Pharmaceutical Cold Supply Chain", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2022, pp. Accepted.

# PharmaChain Versus PharmaChain 2.0

| PharmaChain | PharmaChain 2.0 |
|---|---|
| Tracking and Tracing in Pharmaceutical Supply Chain | Both Tracking & Tracing along with Monitoring and Controlling Temperature Excursions |
| Ethereum Blockchain | PoAh Consensus Based Blockchain (our EasyChain) |
| Proof-of-Authority (PoA) with less throughput compared to PoAh | Proof-of-Authentication (PoAh) with higher throughput |
| Private Blockchain with only nodes participating from Entities | Private Blockchain with only nodes participating from Entities |
| Not IoT friendly Consensus | IoT Friendly Consensus with less power and computations |
| Average transaction processing time is 5.6 sec. | Average transaction time has been improved significantly to 322.28 ms |

# PharmaChain 3.0 - Architectural Overview




Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "PharmaChain 3.0: Blockchain Integrated Efficient QR Code Mechanism for Pharmaceutical Supply Chain", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2022, pp. Accepted.

# PharmaChain 2.0 Versus PharmaChain 3.0

| PharmaChain 2.0 | PharmaChain 3.0 |
|---|---|
| Both Tracking & Tracing along with Monitoring and Controlling Temperature Excursions | Integrating QR Code Mechanism for easy Tracking and Tracing and Drug Information |
| PoAh Consensus Based Blockchain (Our EasyChain) | Ethereum Blockchain into the CPS |
| Proof-of-Authentication (PoAh) with higher throughput | Proof-of-Stake (PoS) Consensus mechanism is used with lesser throughput than PoAh |
| Private Blockchain with only nodes participating from Entities | Private Blockchain with only nodes participating from Entities |
| IoT Friendly Consensus with less power and computations. Doesn't support smart Contracts. | P2P nodes are maintained by the entities and are computationally capable. No need for IoT-Friendly Consensus |
| The average transaction time is 322.28ms | The average Transaction time is 16.2 Sec |
| Less information storage capabilities | More information can be stored |

# PharmaChain 3.0 - Comparative Analysis

| Works | Blockchain | Consensus Mechanism | Computational Needs | Openness | QR Code Integrated | Storage | Handling Large data |
|---|---|---|---|---|---|---|---|
| Crypto Cargo [11] | Ethereum | Proof-of-Work (PoW) | High | Public | No | On-Chain and Cloud | No |
| Kumar et.al. [9] | NA | NA | NA | NA | Yes | On-chain | No |
| PharmaChain [12] | Ethereum | Proof-of-Authority (PoA) | Low | Private | No | On-Chain and Cloud | No |
| PharmaChain 2.0 | Our EasyChain | Proof-of-Authentication (PoAh) | Low | Private | No | On-Chain and Cloud | No |
| Current Solution (PharmaChain 3.0) | Ethereum | Proof-of-Stake (PoS) | Low | Private | Yes | On-Chain and off-Chain | Yes |

# Is Physical Unclonable Function (PUF) the Solution for Every Cybersecurity Problem?

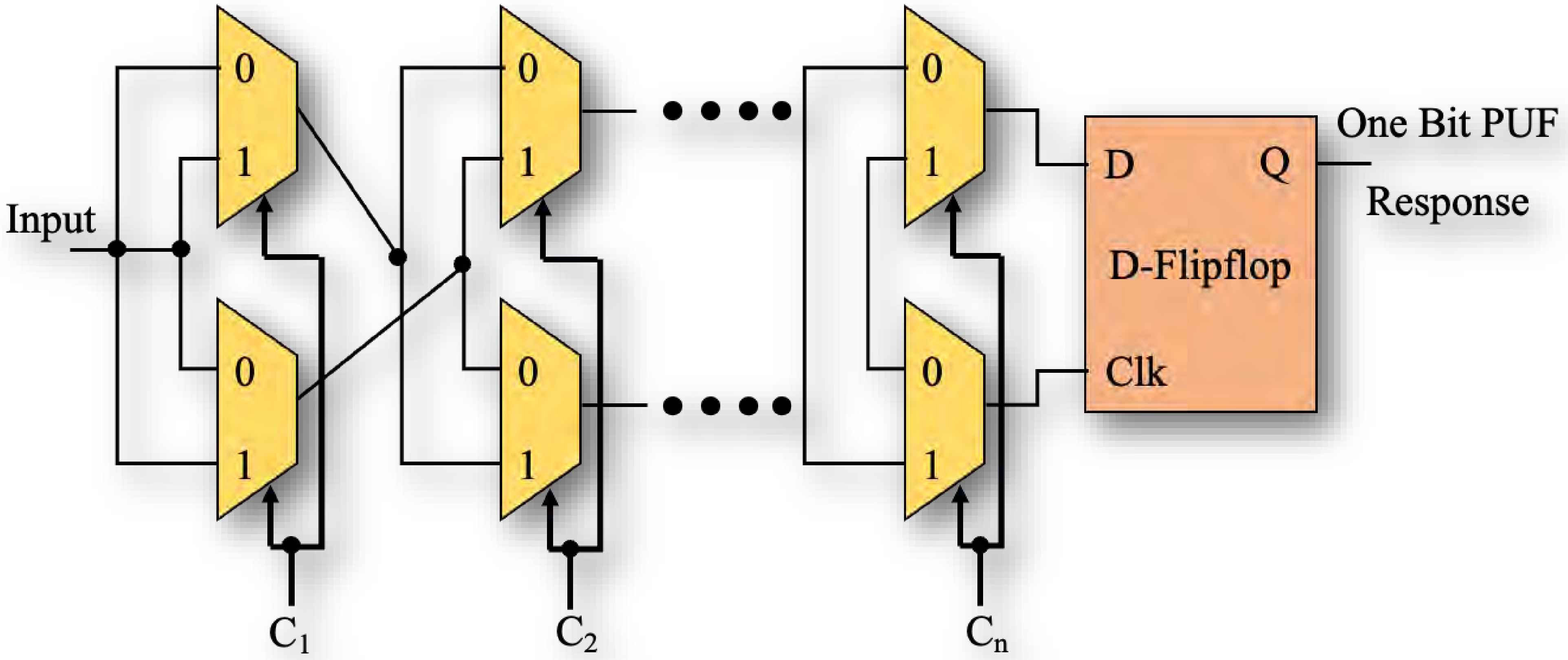
# If PUF is So Great, Why Isn't Everyone Using It?

- 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.

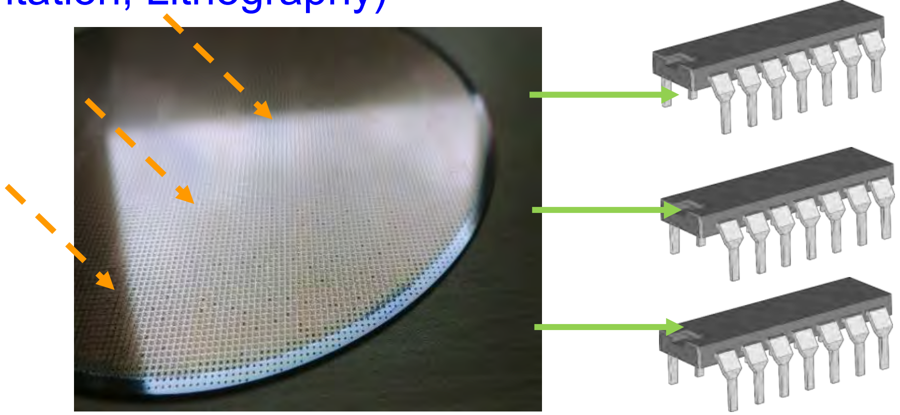



1 – Bit Arbiter PUF Architecture

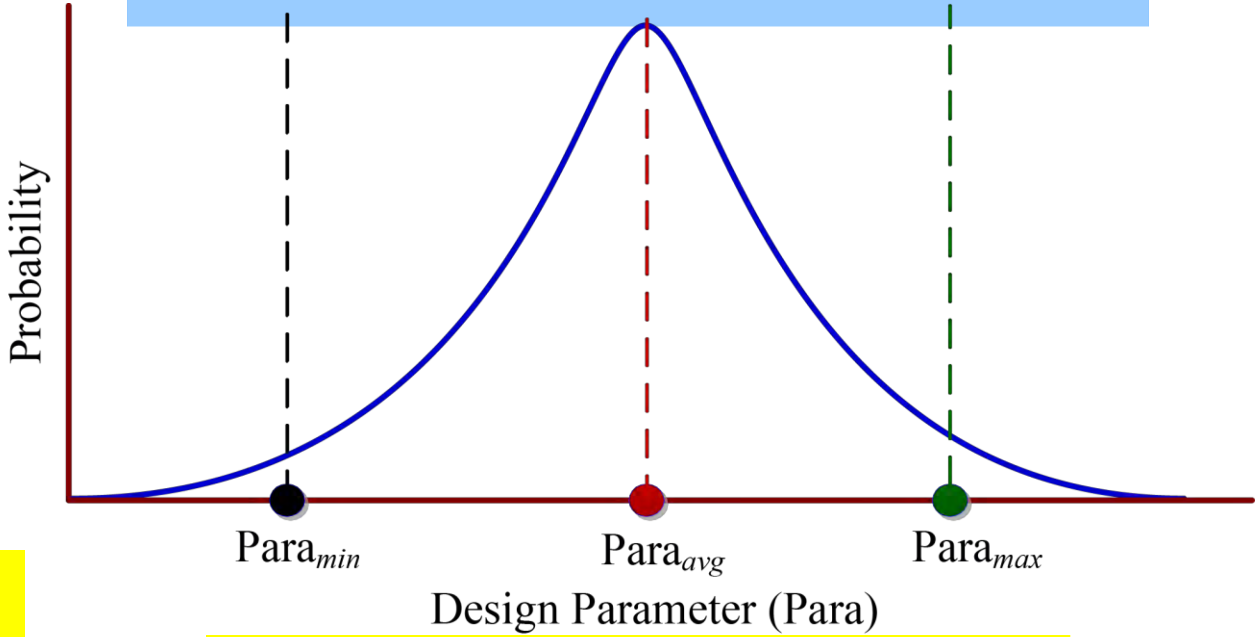
# IC for PUF – Contradictory Design Objective - Variability versus Variability-Aware Design

Variability → Randomness for PUF

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



Variability-Aware Design → Robust Hardware

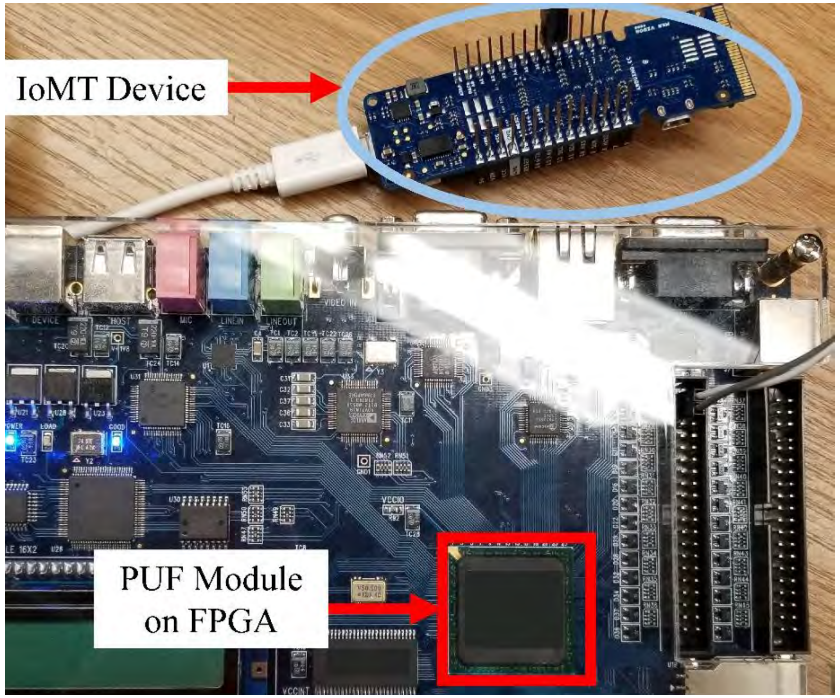



Variability Features → Randomness → PUF

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

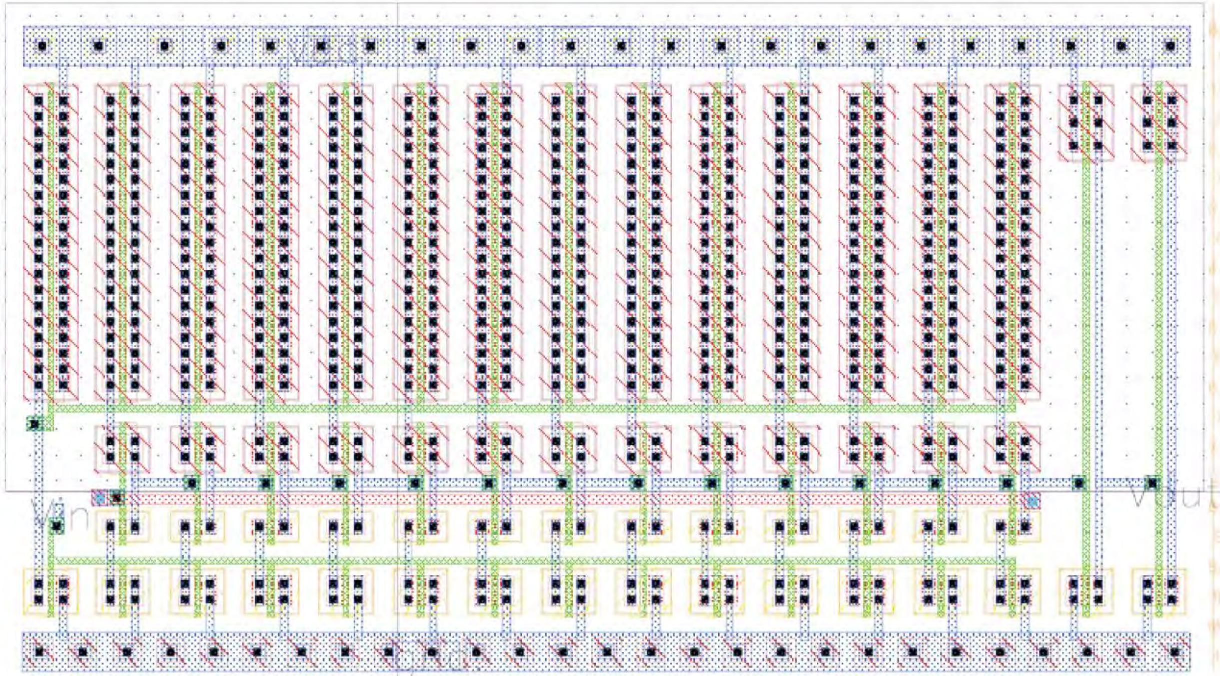
Optimize $(\mu+n\sigma)$ to reduce variability for Robust Design

# 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.

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

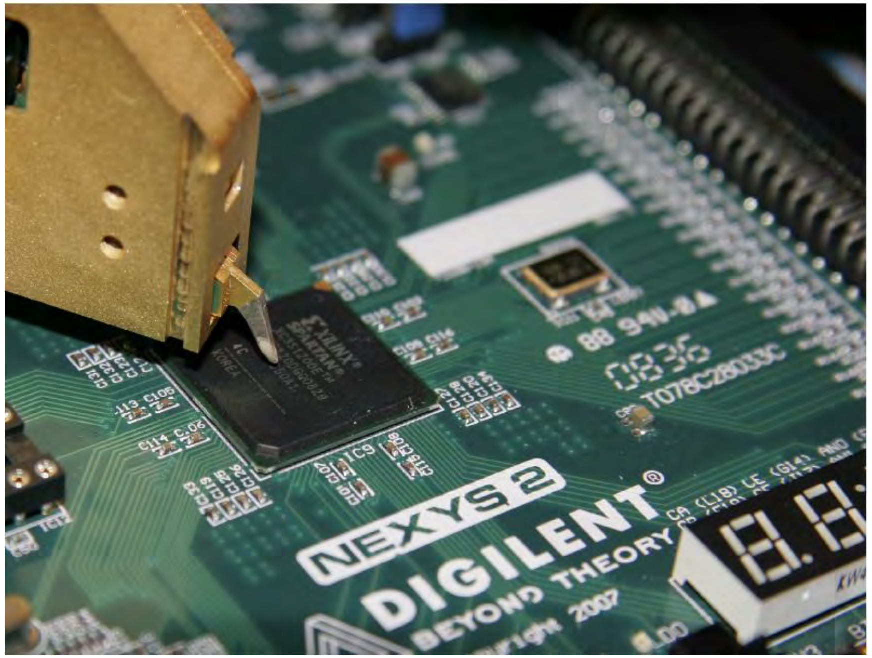


Source: **S. P. Mohanty** and E. Kougianos, "Incorporating Manufacturing Process Variation Awareness in Fast Design Optimization of Nanoscale CMOS VCOs", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 27, Issue 1, February 2014, pp. 22--31.

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

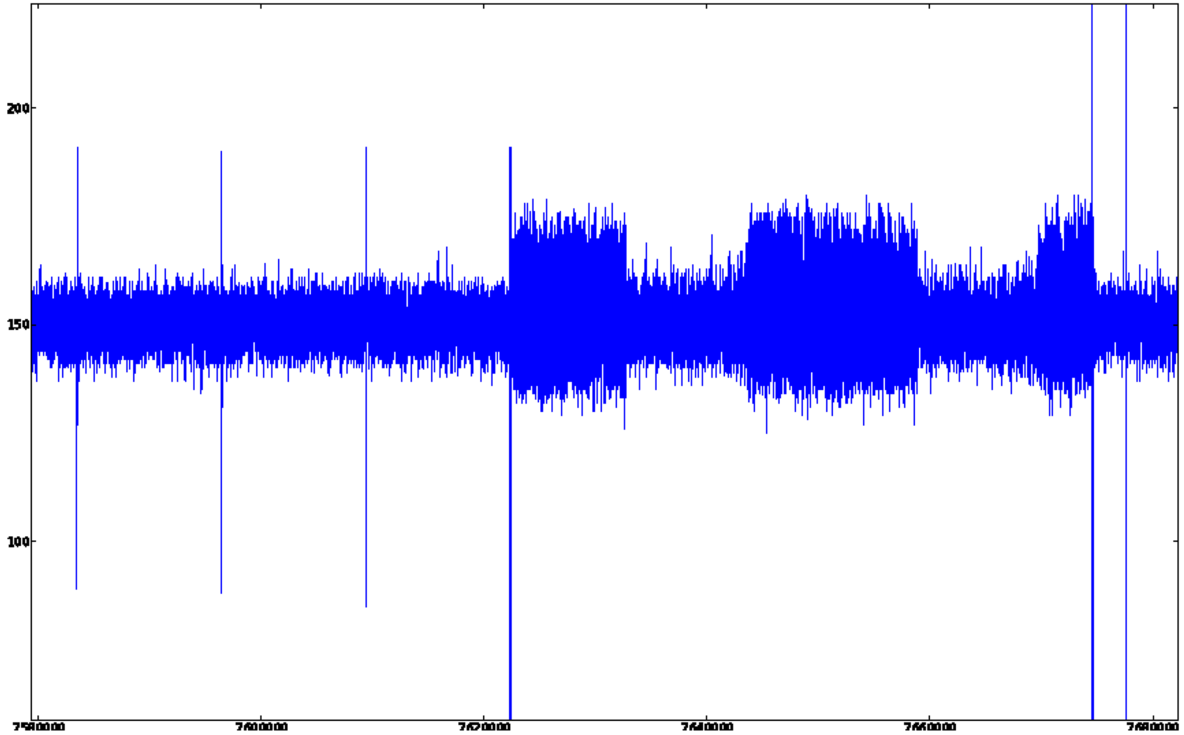
# PUF - Side Channel Leakage

- 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.

# 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.

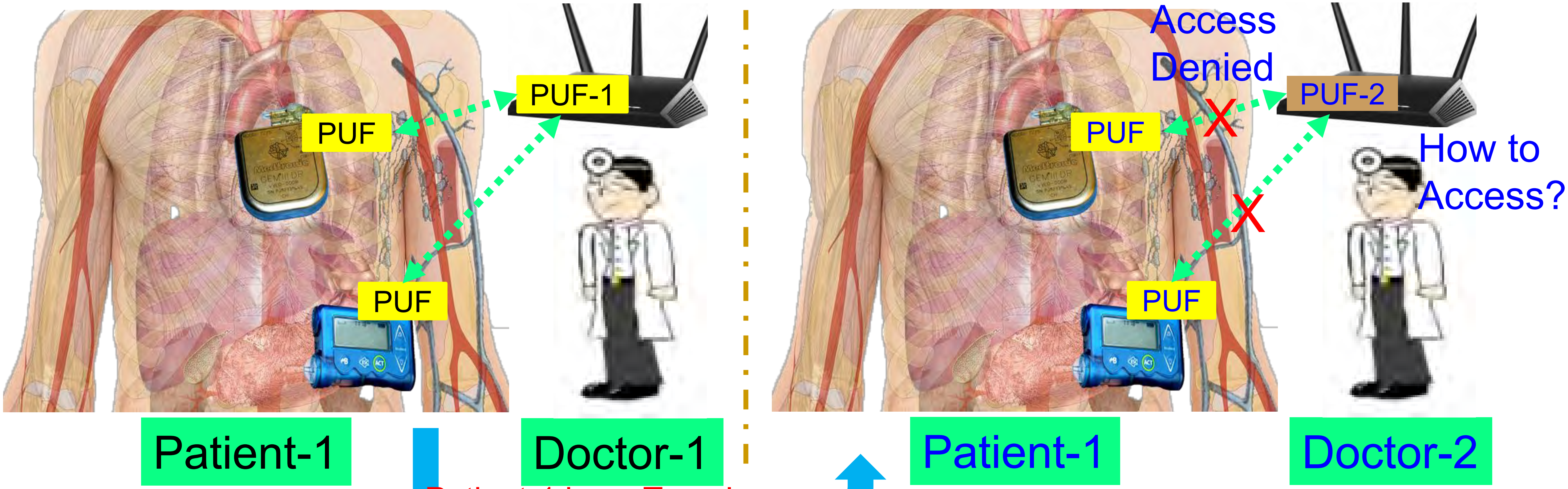
Source: Rührmair, Ulrich; van Dijk, Marten (2013). *PUFs in Security Protocols: Attack Models and Security Evaluations* (PDF), in *Proc. IEEE Symposium on Security and Privacy*, May 19–22, 2013

# 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.

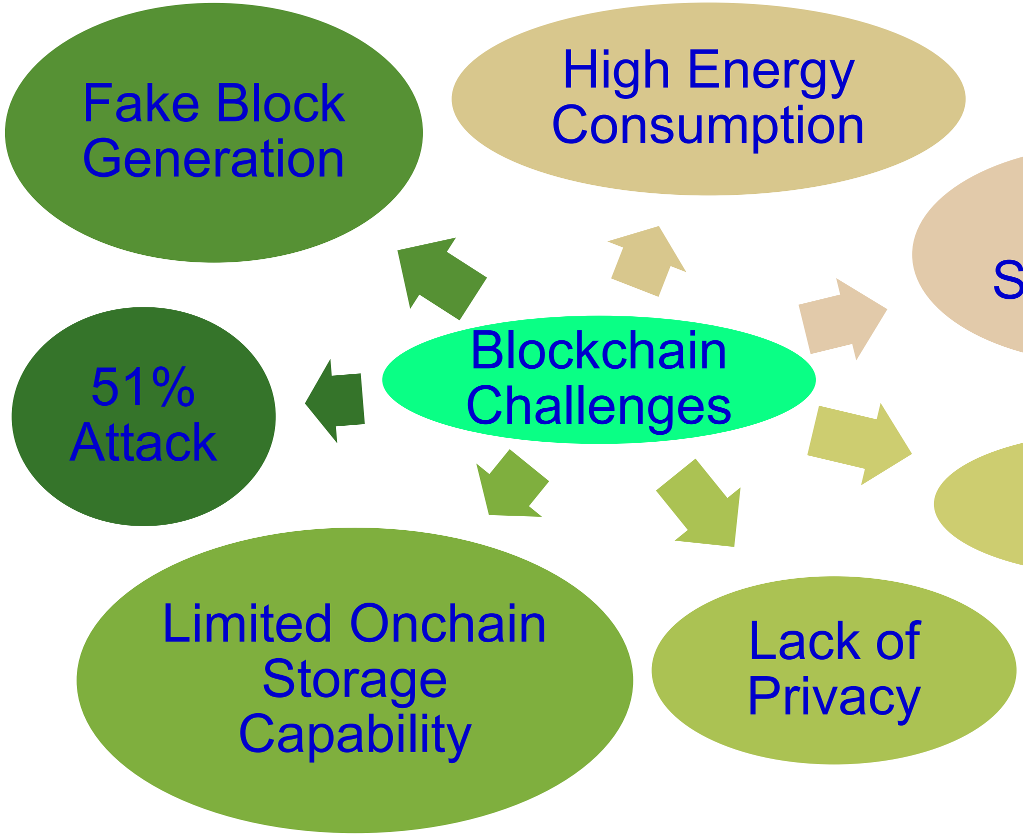
# PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma




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

# Is Blockchain the Solution for Every Cybersecurity Problem?

# Blockchain has Many Challenges




Source: https://www.etorox.com

Source: https://www.monash.edu/blockchain/news/how-do-we-know-blockchain-cant-be-hacked-or-manipulated-or-can-it

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

# Blockchain Energy Need is Huge


Energy for mining of 1 bitcoin

=

Energy consumption 2 years of a US household

Energy consumption for each bitcoin transaction

=

80,000 X

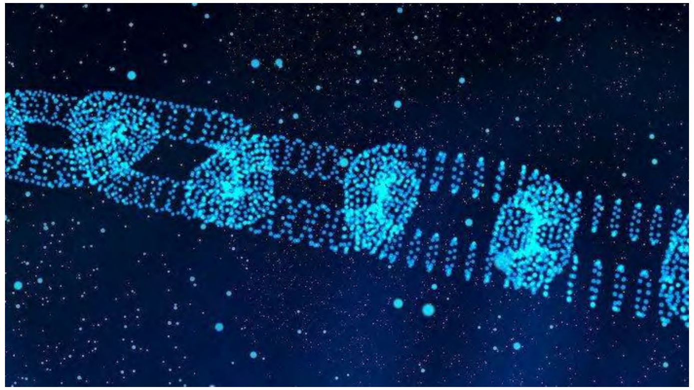
Energy consumption of a credit card processing

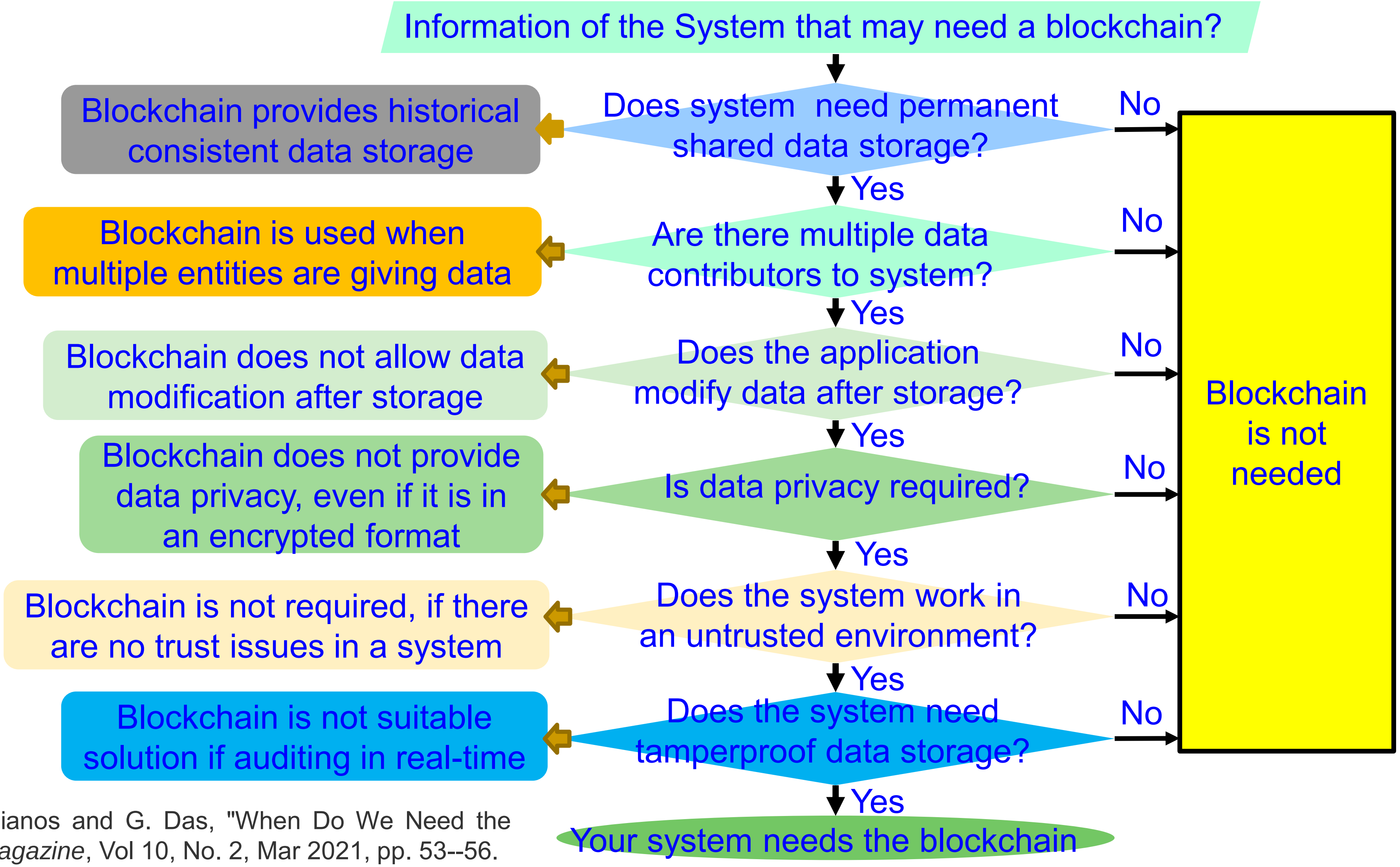
# Blockchain has Cybersecurity Challenges

| Selected attacks on the blockchain and defences | | |
|---|---|---|
| **Attacks** | Descriptions | Defence |
| **Double spending** | Many payments are made with a body of funds | Complexity of mining process |
| **Record hacking** | Blocks are modified, and fraudulent transactions are inserted | Distributed consensus |
| **51% attack** | A miner with more than half of the network's computational power dominates the verification process | Detection methods and design of incentives |
| **Identity theft** | An entity's private key is stolen | Reputation of the blockchain on identities |
| **System hacking** | The software systems that implement a blockchain are compromised | Advanced intrusion detection systems |

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

# When do You Need the Blockchain?






Source: D. Puthal, S. P. Mohanty, E. Kougianos and G. Das, "When Do We Need the Blockchain?," *IEEE Consumer Electronics Magazine*, Vol 10, No. 2, Mar 2021, pp. 53--56.

# Conclusions and Future Research

# Conclusions

- Healthcare has been evolving to Healthcare-CPS (H-CPS).
- Internet of Medical Things (IoMT) is key for smart healthcare.
- Smart healthcare can reduce cost of healthcare and give more personalized experience to the individual.
- IoMT provides advantages but also has limitations in terms of security, and privacy.
- Cybersecurity in smart healthcare is challenging as device as well as data security and privacy are important.
- Medical device security is a difficult problem as these are resource and battery constrained.
- Security-by-Design and/or Privacy-by-Design is critical for IoMT/H-CPS.

# Future Research

- ML models for smart healthcare needs research.
- Internet-of-Everything (IoE) with Human as active part need research.
- IoE will need robust data, device, and H-CPS security need more research.
- Security of IWMDs needs to have extremely minimal energy overhead to be useful and hence needs research.
- Integration of blockchain for smart healthcare need research due to energy and computational overheads associated with it.
- SbD research for IoMT/H-CPS is needed.
- PbD research for IoMT/H-CPS is needed.
- Trustworthy Pharmaceutical Supply Chain needs research.