

Sustainable Healthcare Cyber-Physical Systems

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

Nirma University, Ahmadabad, India - 25 Nov 2024



Homepage:
www.smohanty.org

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

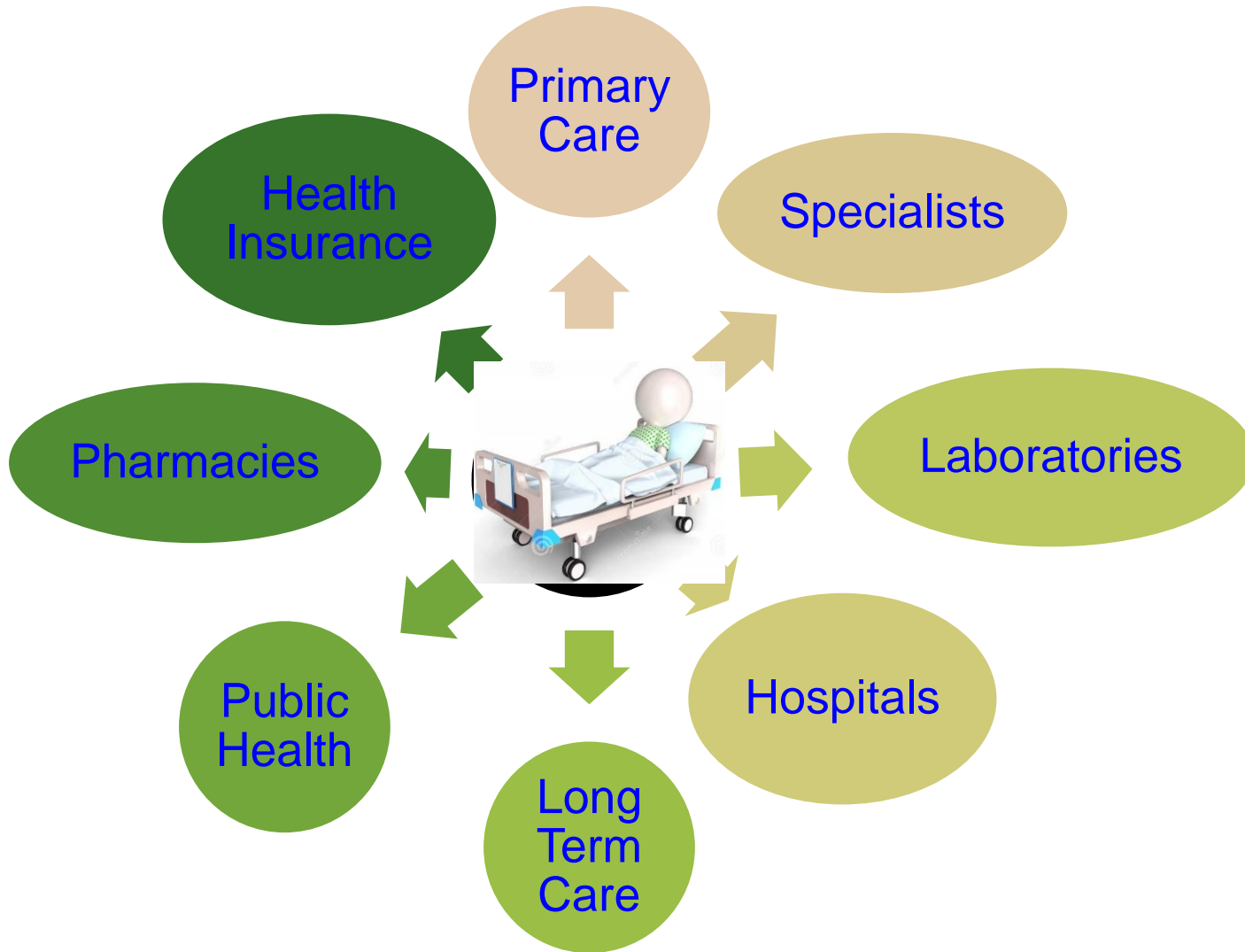


Outline

- Smart Healthcare – Broad Introduction
- Smart Healthcare – Challenges Against Sustainability
- Selected Cybersecurity Solutions for IoT/CPS
- Drawbacks of Existing Cybersecurity Solutions of IoMT/H-CPS
- Security by Design (SbD) Principle
- Security by Design (SbD) Example Solutions
- Trustworthy Pharmaceutical Supply Chain
- Trustworthy Medical Prescription
- Conclusion

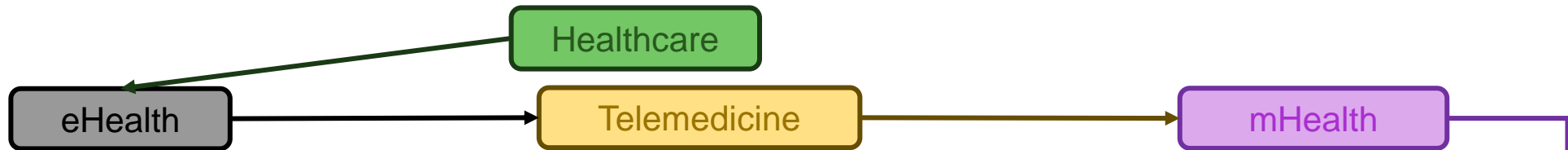
Smart Healthcare – Broad Introduction

Traditional Healthcare

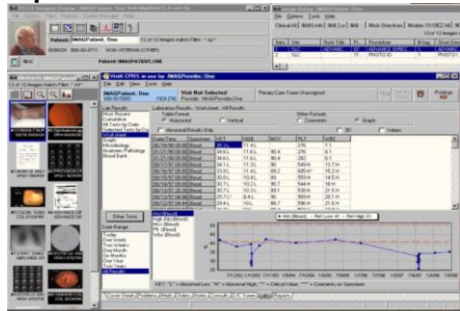


- Physical presence needed
- Deals with many stakeholders
- Stakeholders may not interact
- May not be personalized
- Not much active feedback
- Less effective follow-up from physicians

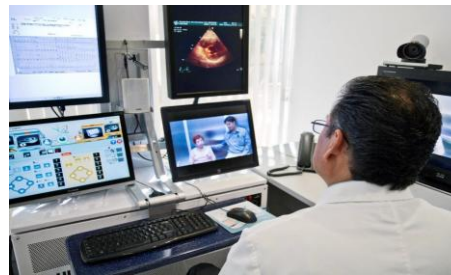
Healthcare → Smart Healthcare



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



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



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

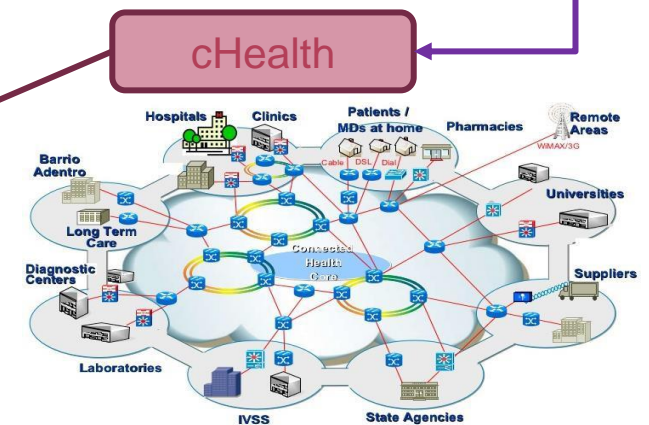


Embedded Skin Patches

Thync's - UltrasoVibeund

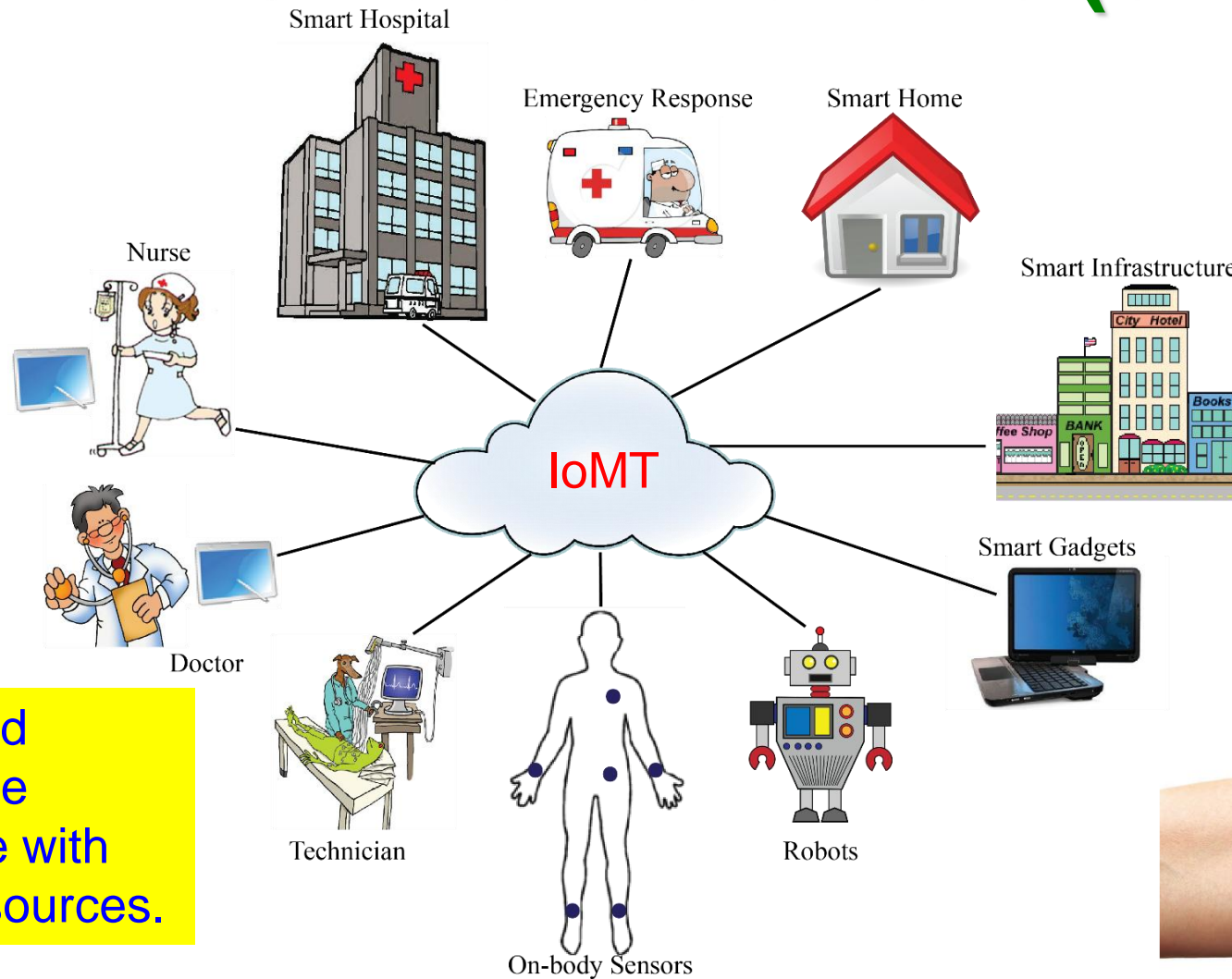
Muse - EEG

sHealth



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

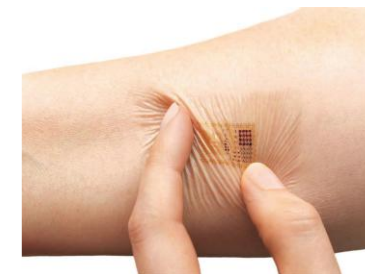
Smart Healthcare (sHealth)



Fitness Trackers



Headband with Embedded Neurosensors

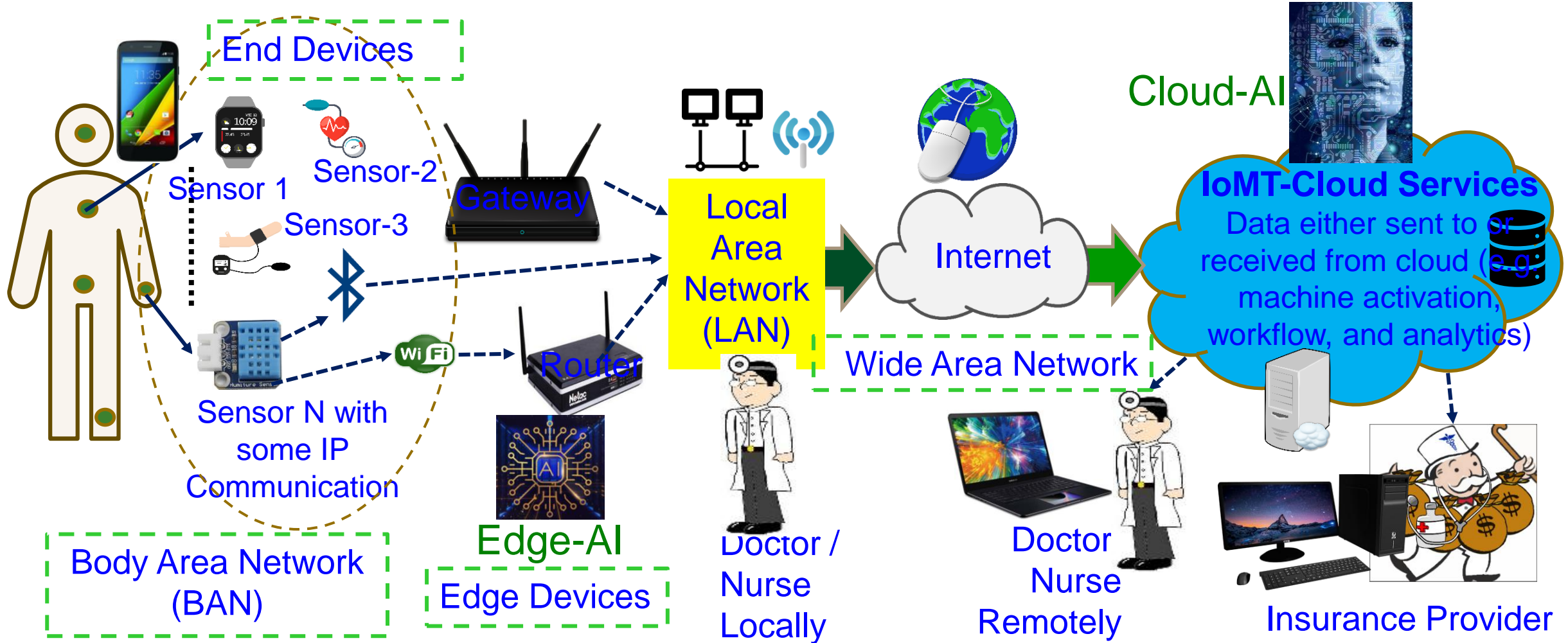


Embedded Skin Patches

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.

Smart Healthcare – Healthcare CPS

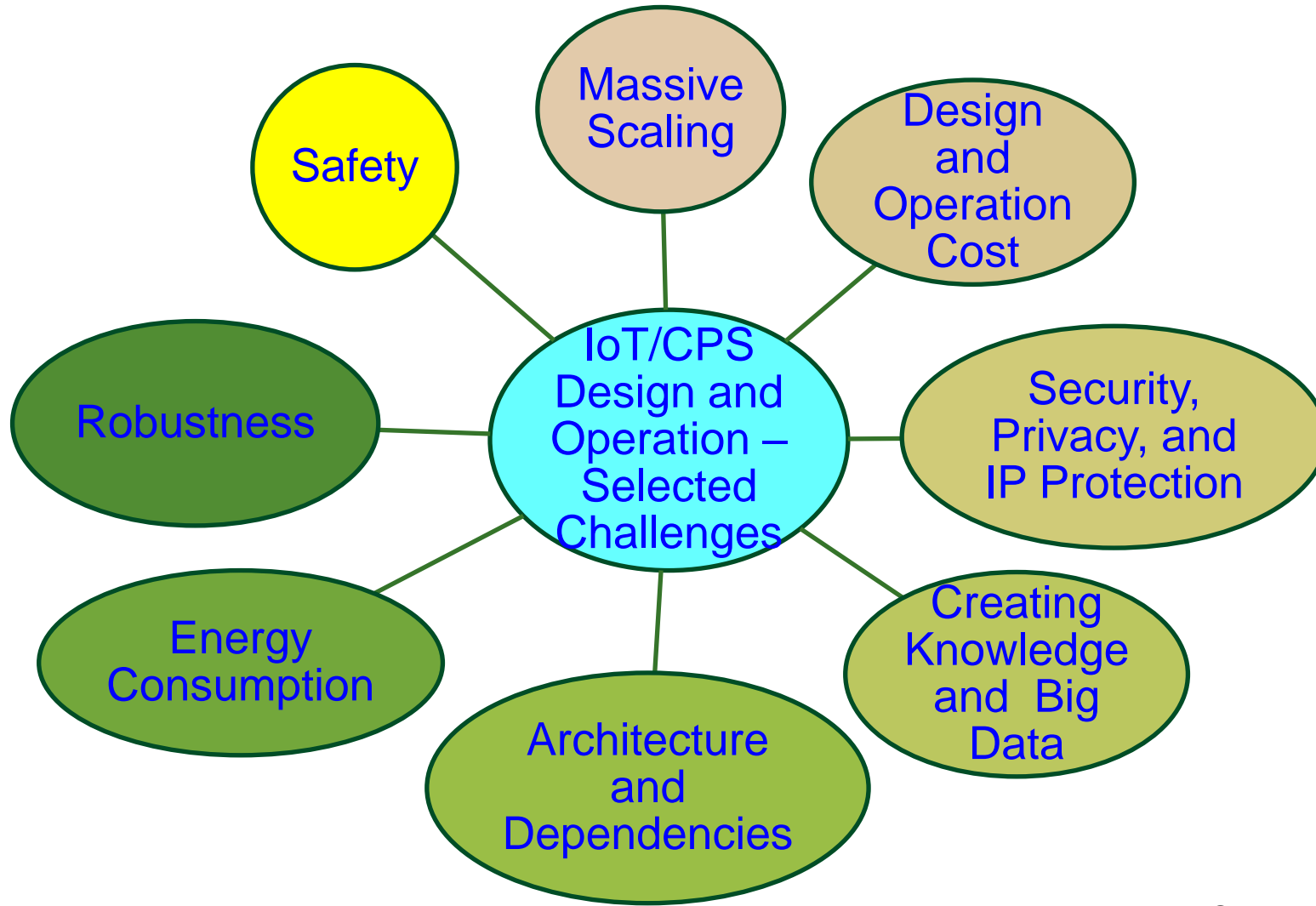


Frost and Sullivan predicts smart healthcare market value to reach US\$348.5 billion by 2025.

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

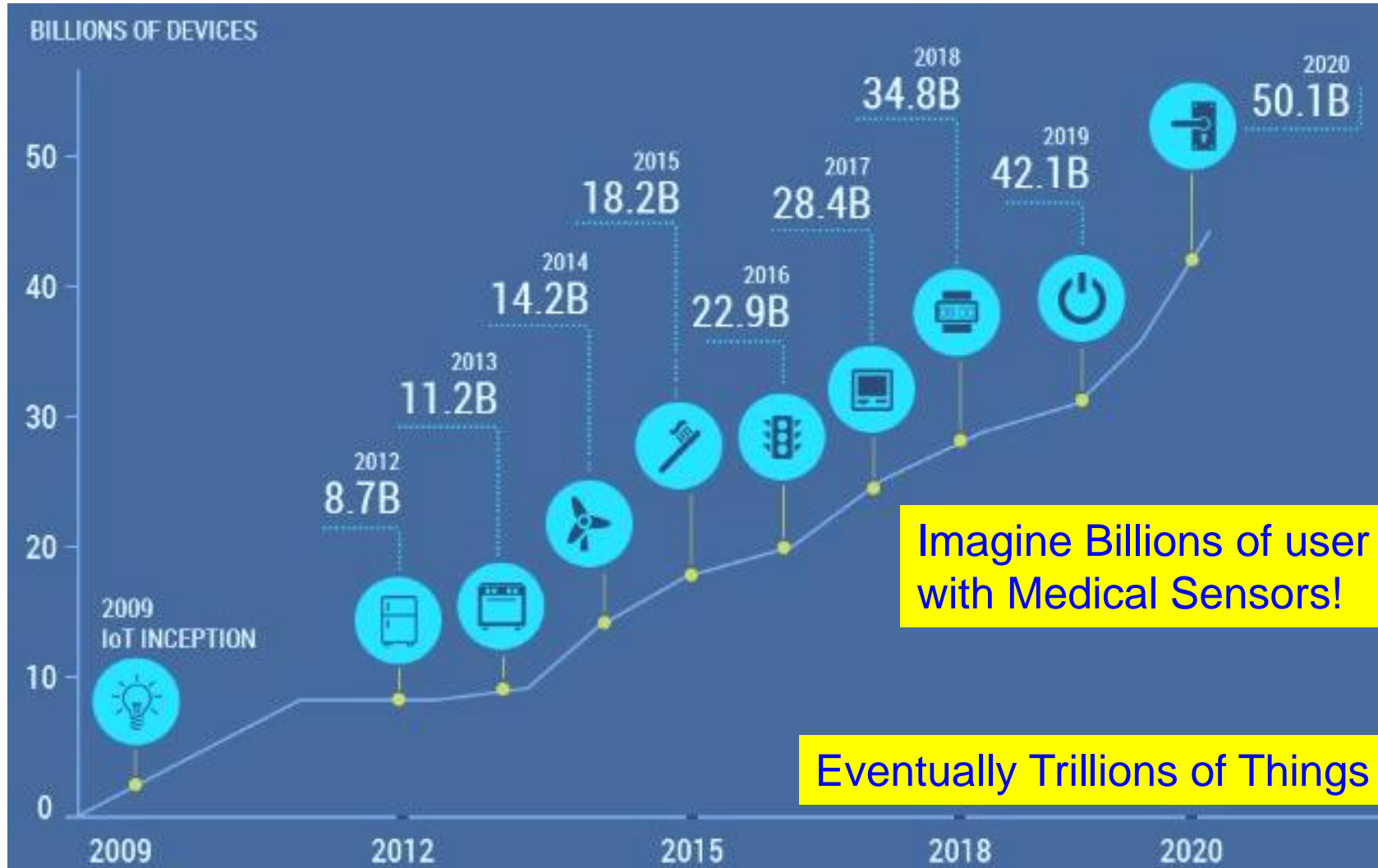
Smart Healthcare – Challenges Against Sustainability

CPS – Sustainability Challenges

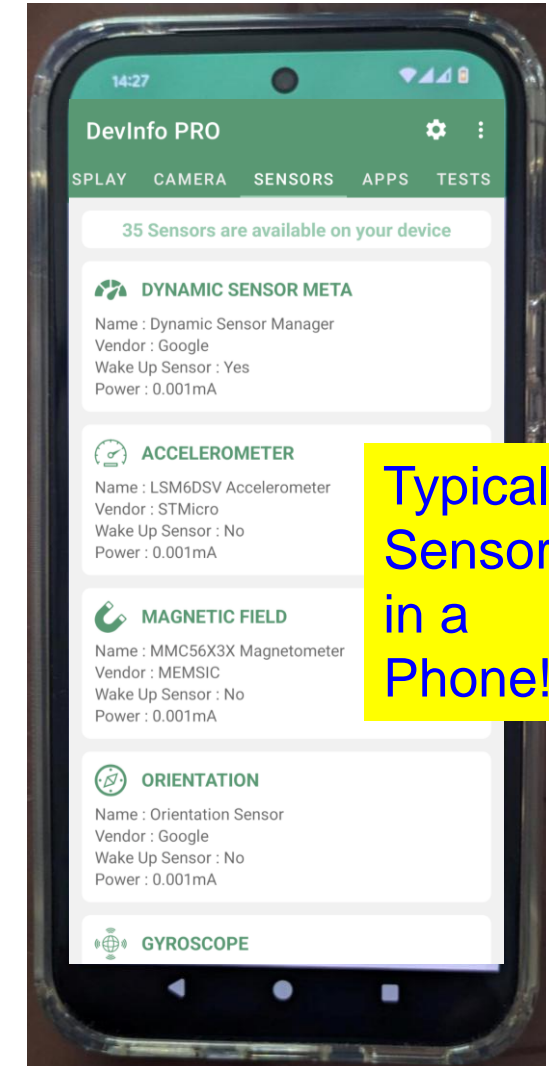


Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things



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



Challenges of Data in IoT/CPS are Multifold



AI/ML Modeling Challenges



Machine Learning Issues

High Energy Requirements

High Computational Resource Requirements

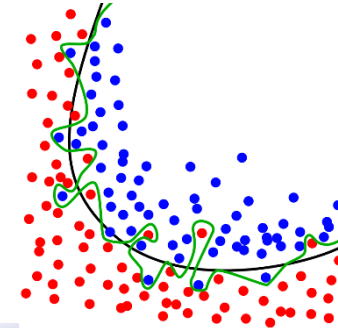
Large Amount of Data Requirements

Underfitting and Overfitting Issue

Class Imbalance Issue

Fake Data Issue

Attack on Training Process



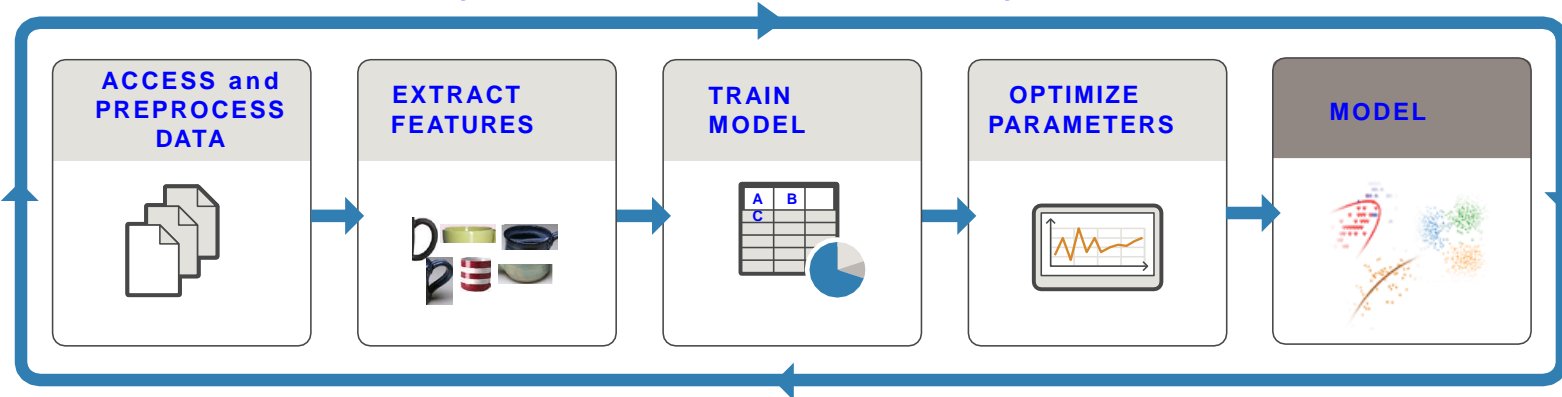
Source: Mohanty ISCT Keynote 2019

Deep Neural Network (DNN) - Resource and Energy Costs

TRAIN: Iterate until you achieve satisfactory performance.

Needs Significant:

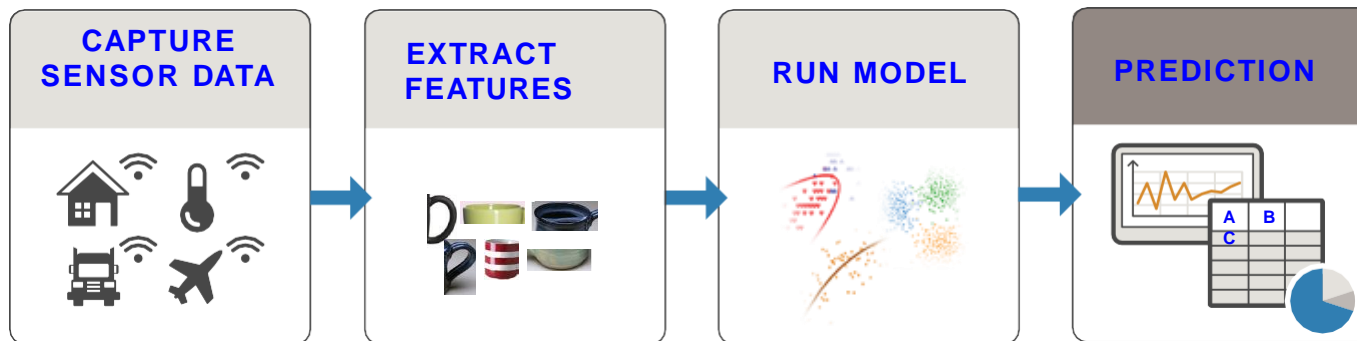
- Computational Resource
- Computation Energy



Limited Computational Capability
Limited Battery Life



PREDICT: Integrate trained models into applications.



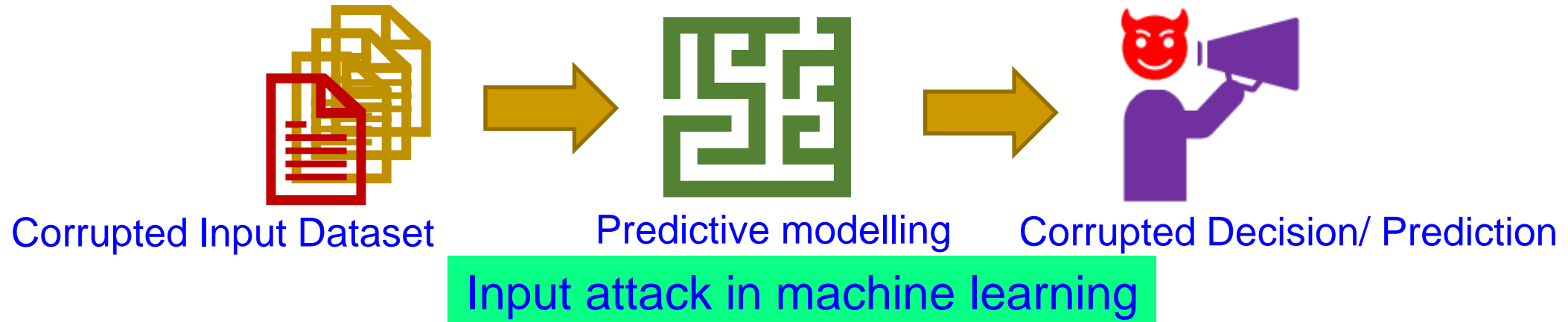
Needs:

- Computational Resource
- Computation Energy



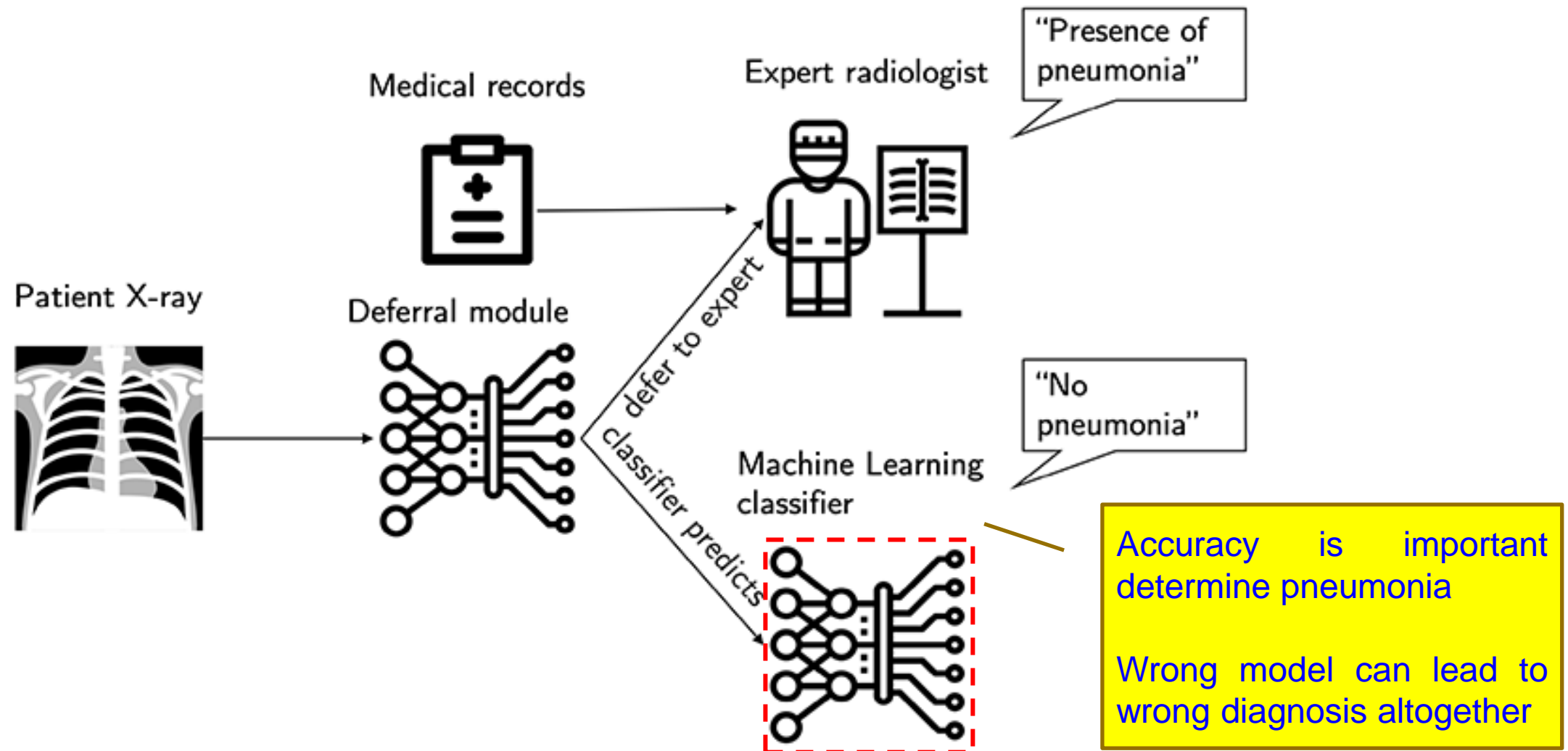
Source: <https://www.mathworks.com/campaigns/offers/mastering-machine-learning-with-matlab.html>

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



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

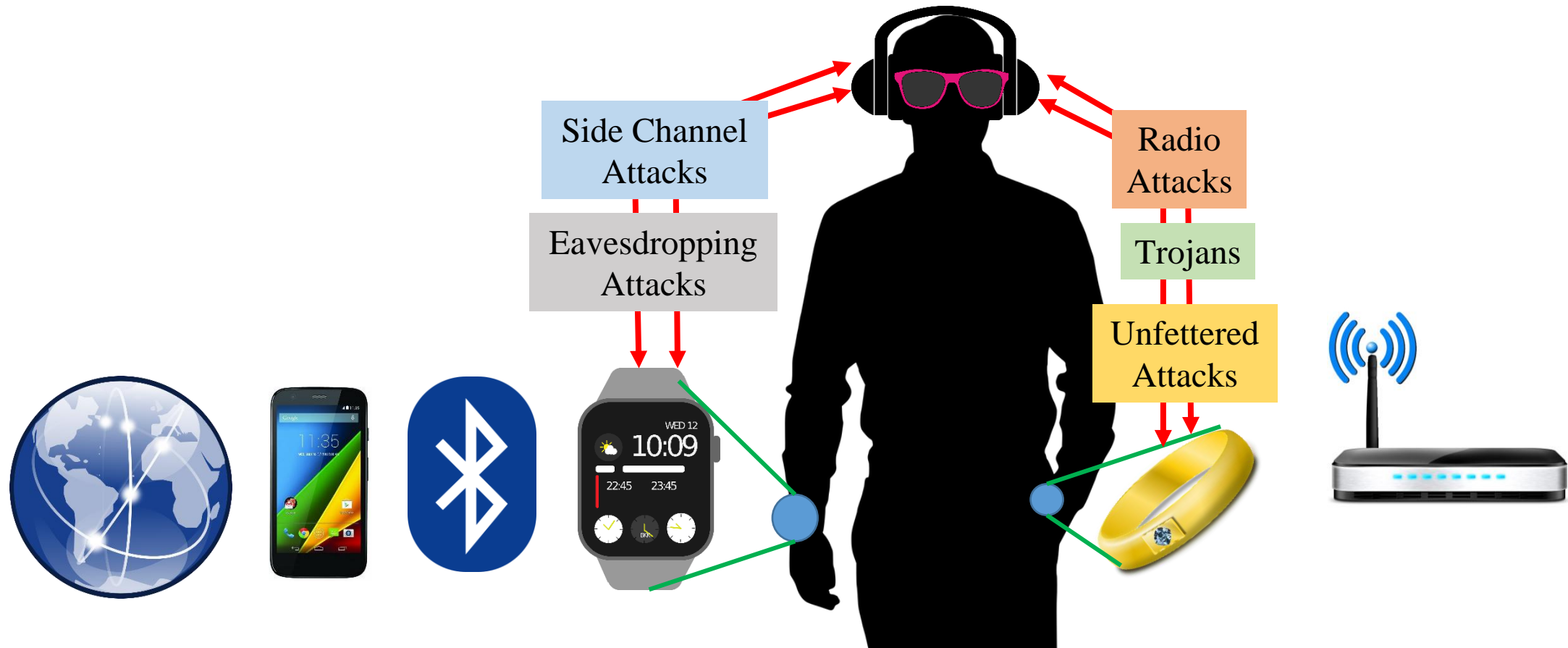
Location Privacy

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.

Attacks on Wearable Devices



Implantable Medical Devices - Attacks



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

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

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

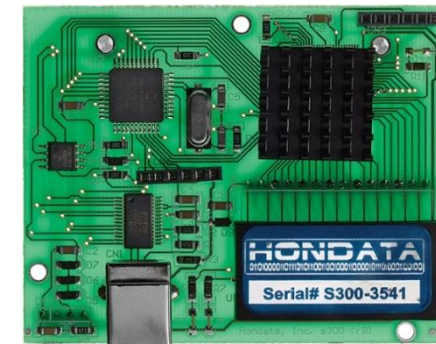


Fake

An implantable medical device



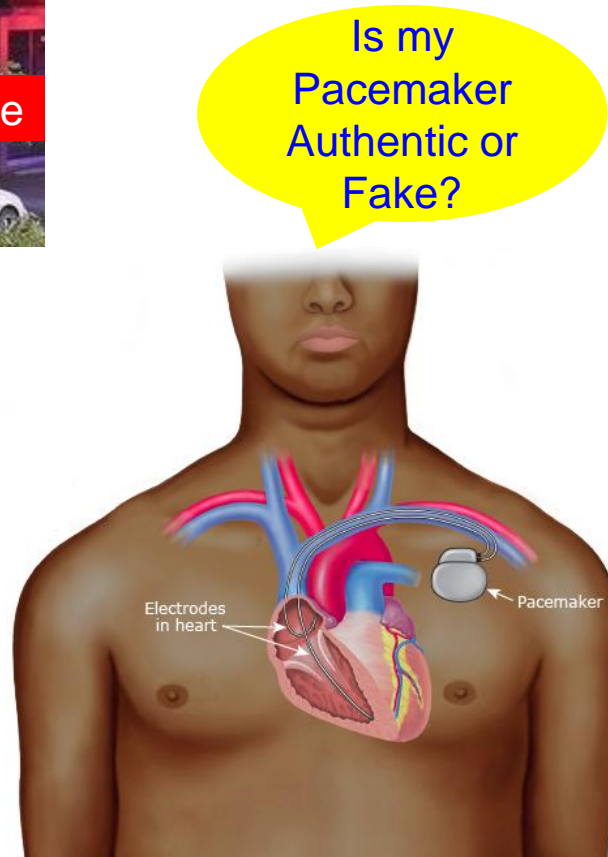
Authentic



Fake

A plug-in for car-engine computers

Fake is Cheap – Why not Buy?



International Pharmaceutical Students' Federation
Asia Pacific Regional Office

THE NEGATIVE IMPACTS OF FAKE MEDICINE

- Increased mortality and morbidity
- Development of drug resistance
- Increase the chance of adverse effects
- Loss of confidence in health systems and health workers
- Undermining of drug research and development
- Crowding out of legitimate drug manufacturers
- Decreased willingness of patients to accept treatment
- Economic loss for patients and health systems

Source: <https://apro.ipsof.org/>

Electronic Health Records (EHR's)

- Electronic Health Record (EHR) is an electronic version of patient medical history maintained by the provider
- Contains demographics, progress notes, problems, medications, and other administrative information

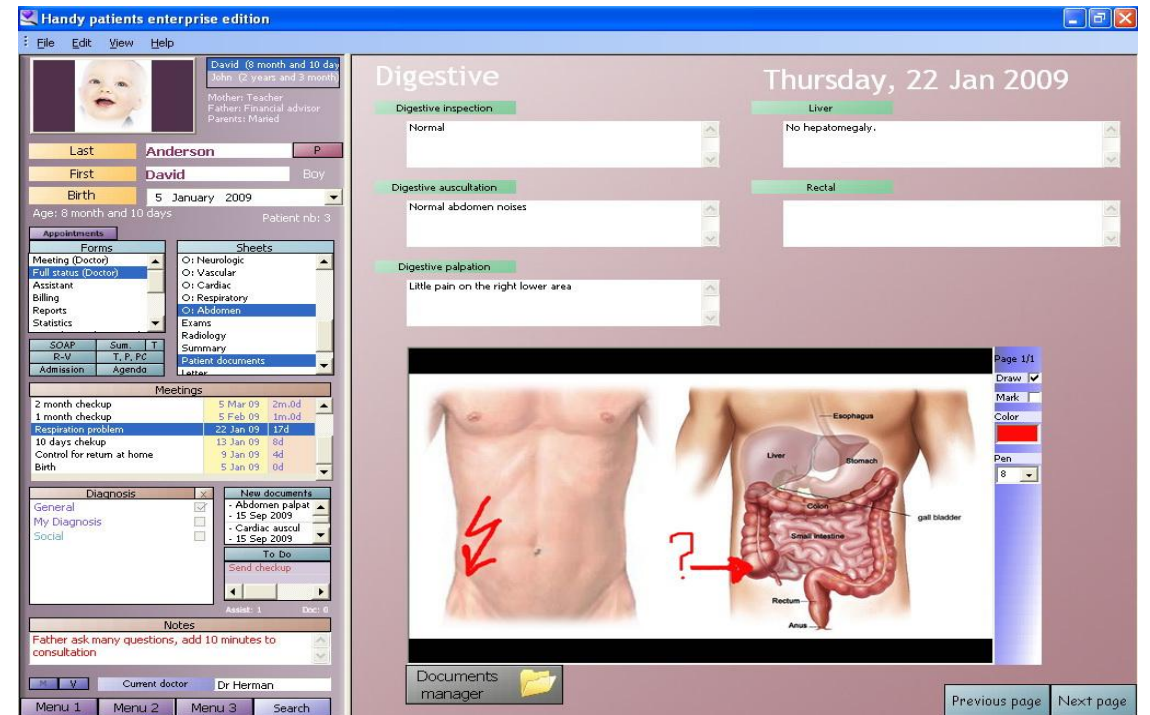
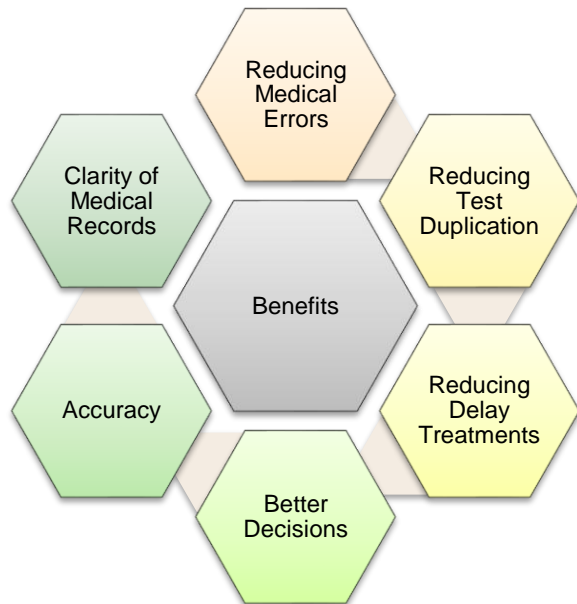
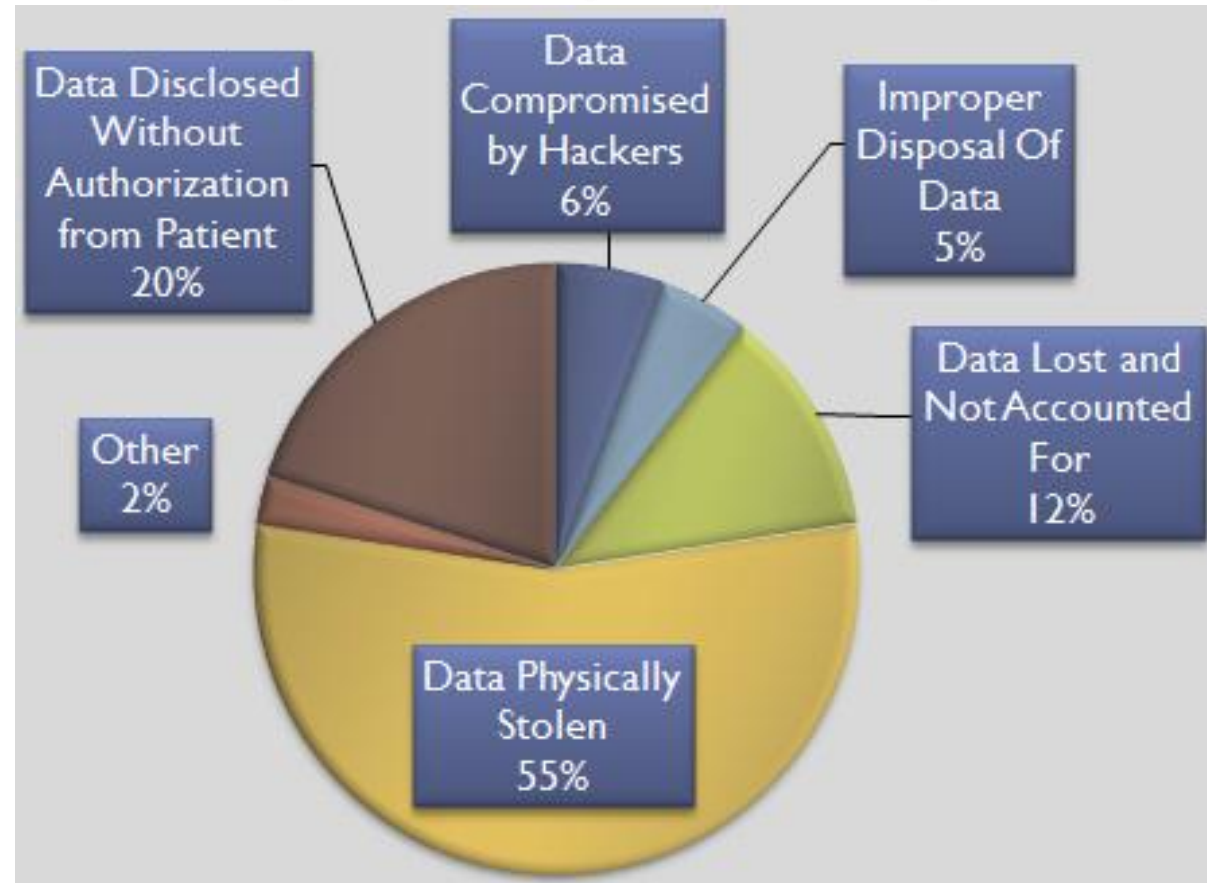


Image Source: DaCarpenter, An electronic medical record example, Handy patients electronic medical record (free open-source version)

Health Insurance Portability and Accountability Act (HIPAA)

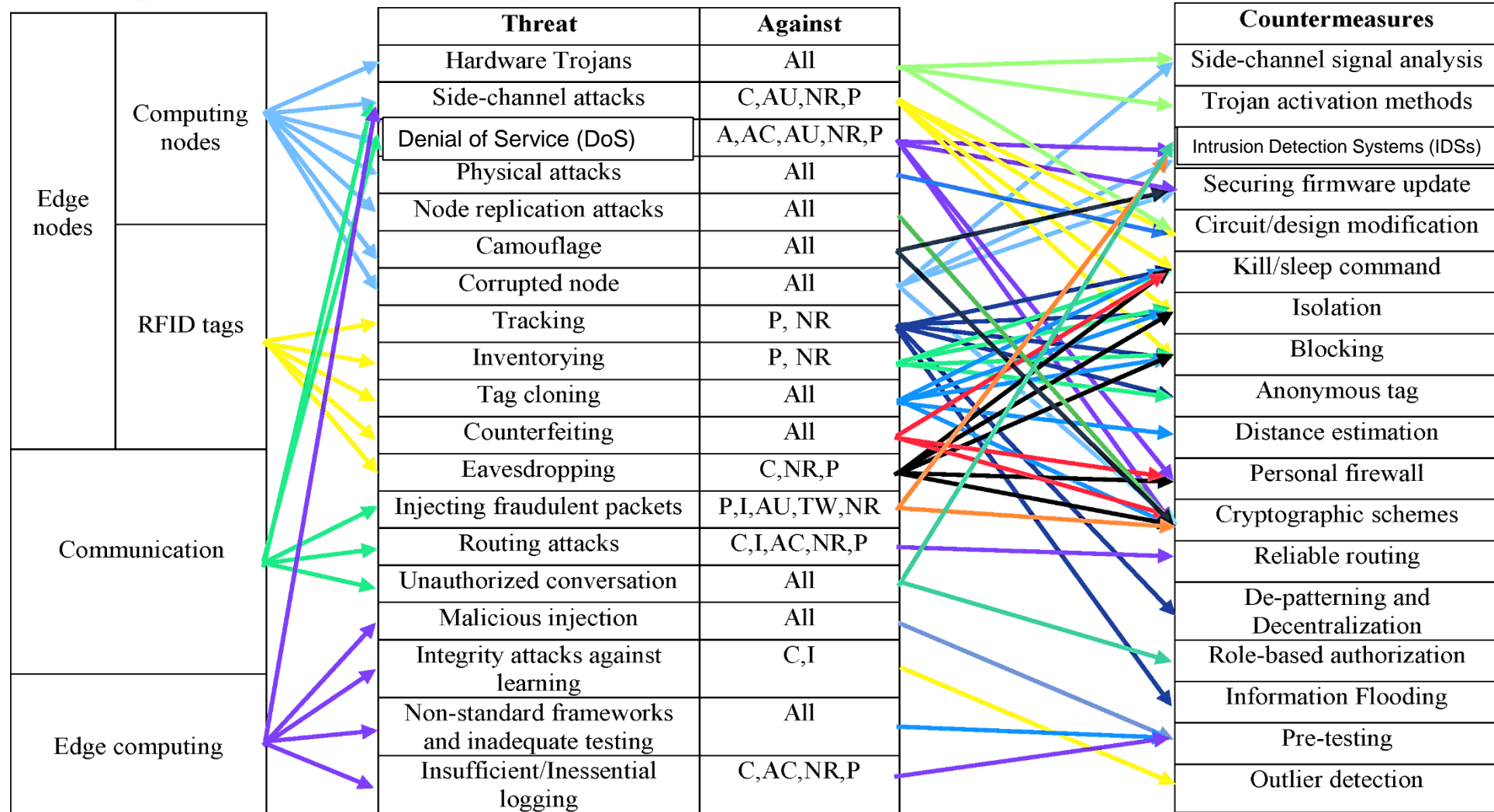


HIPPA Privacy Violation by Types

Cybrsecurity Solution for IoT/CPS



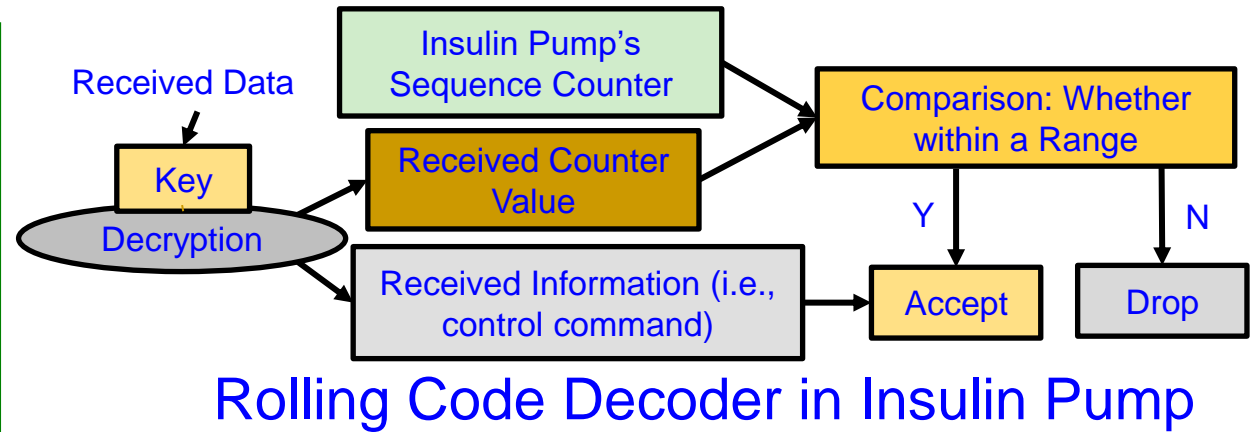
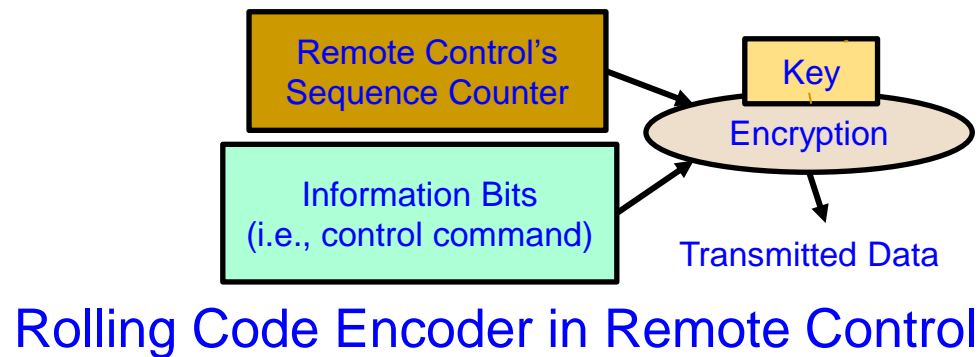
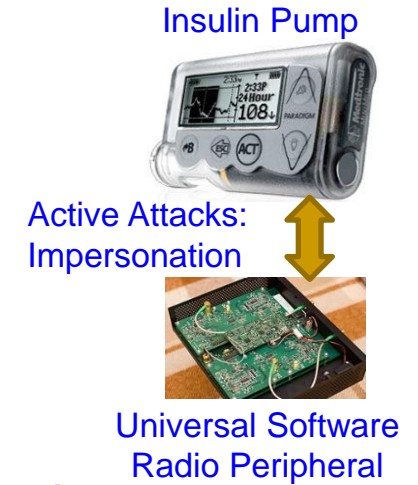
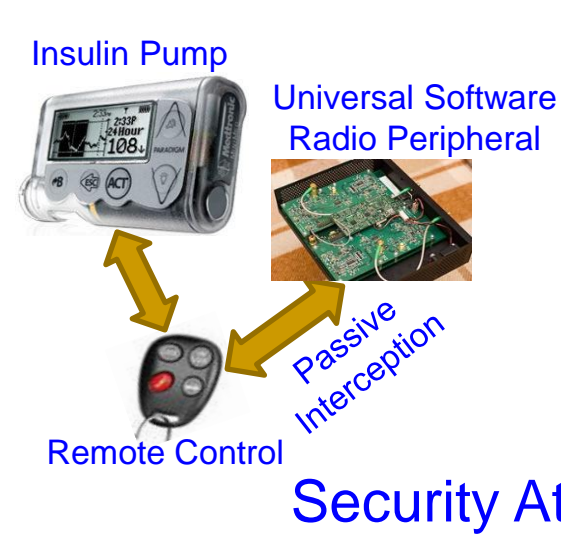
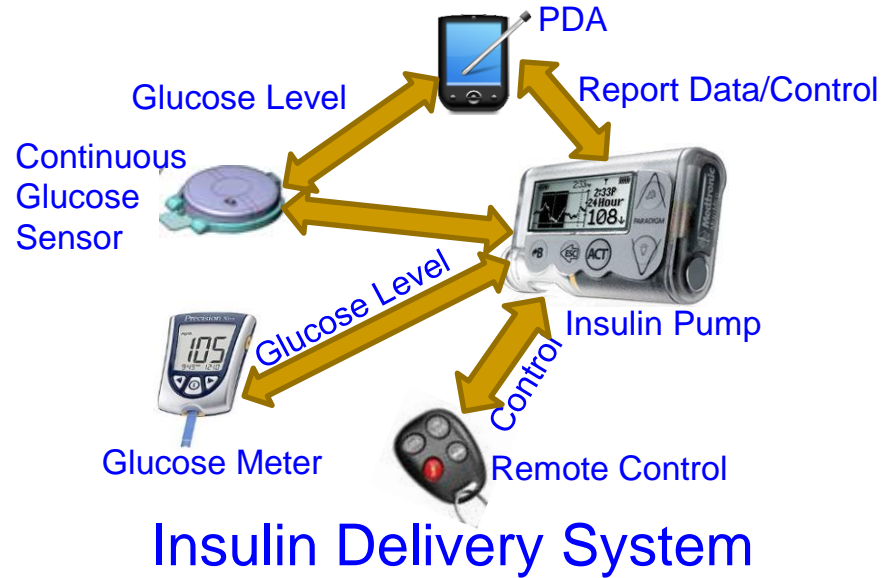
IoT Cybersecurity - Attacks and Countermeasures



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

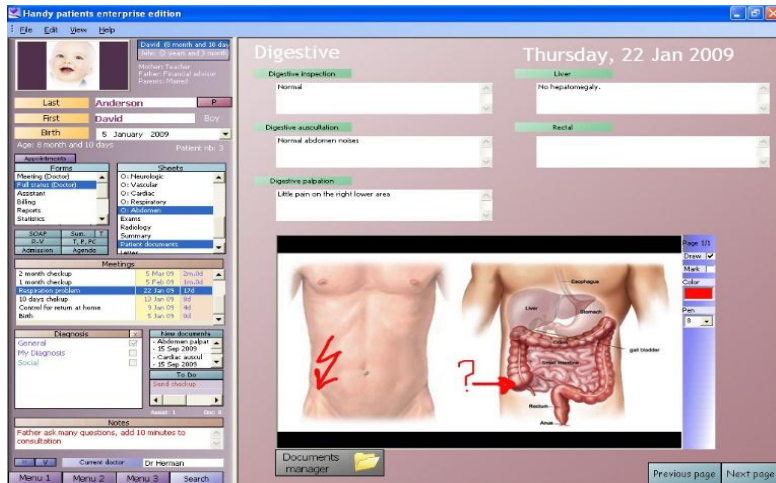
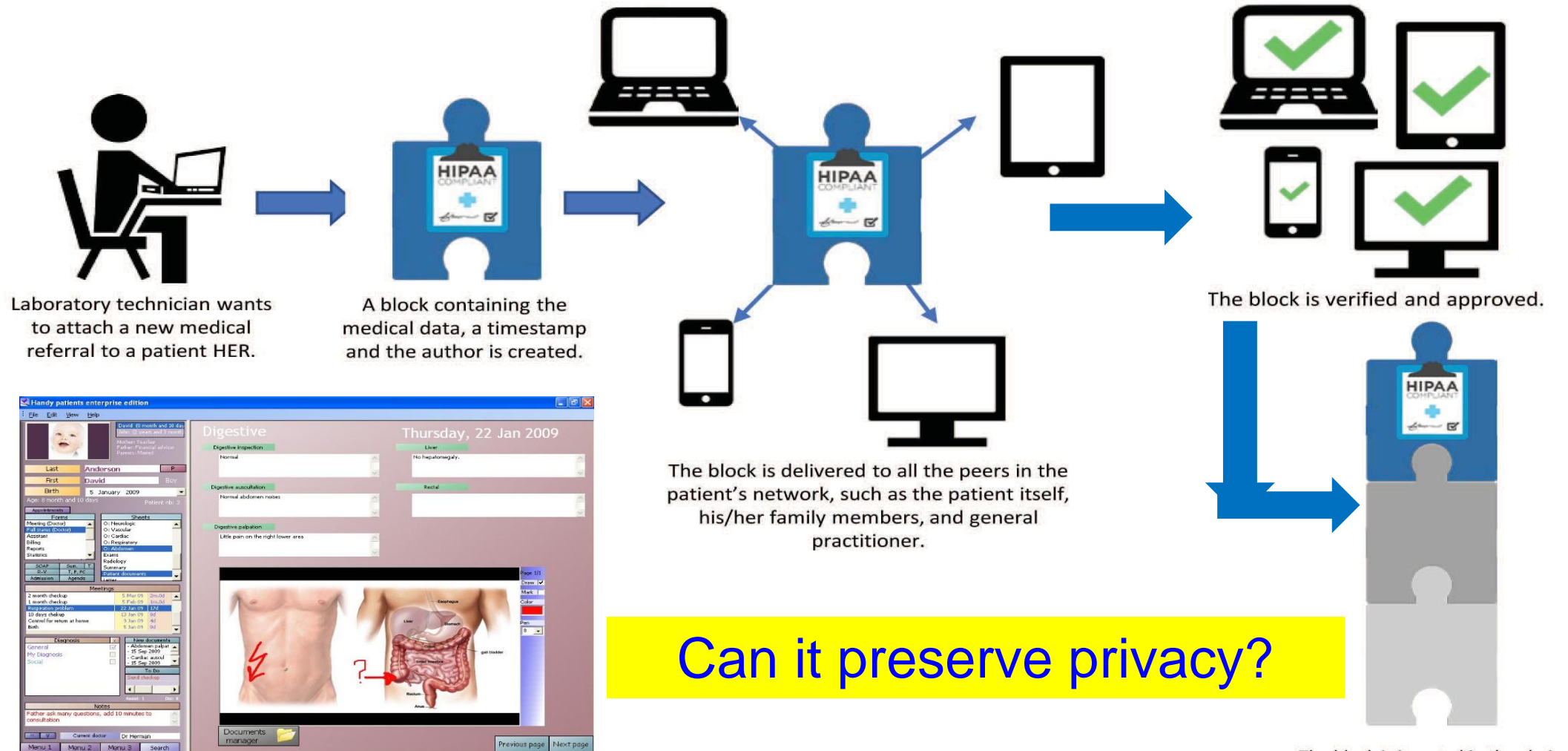
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

Smart Healthcare Cybersecurity



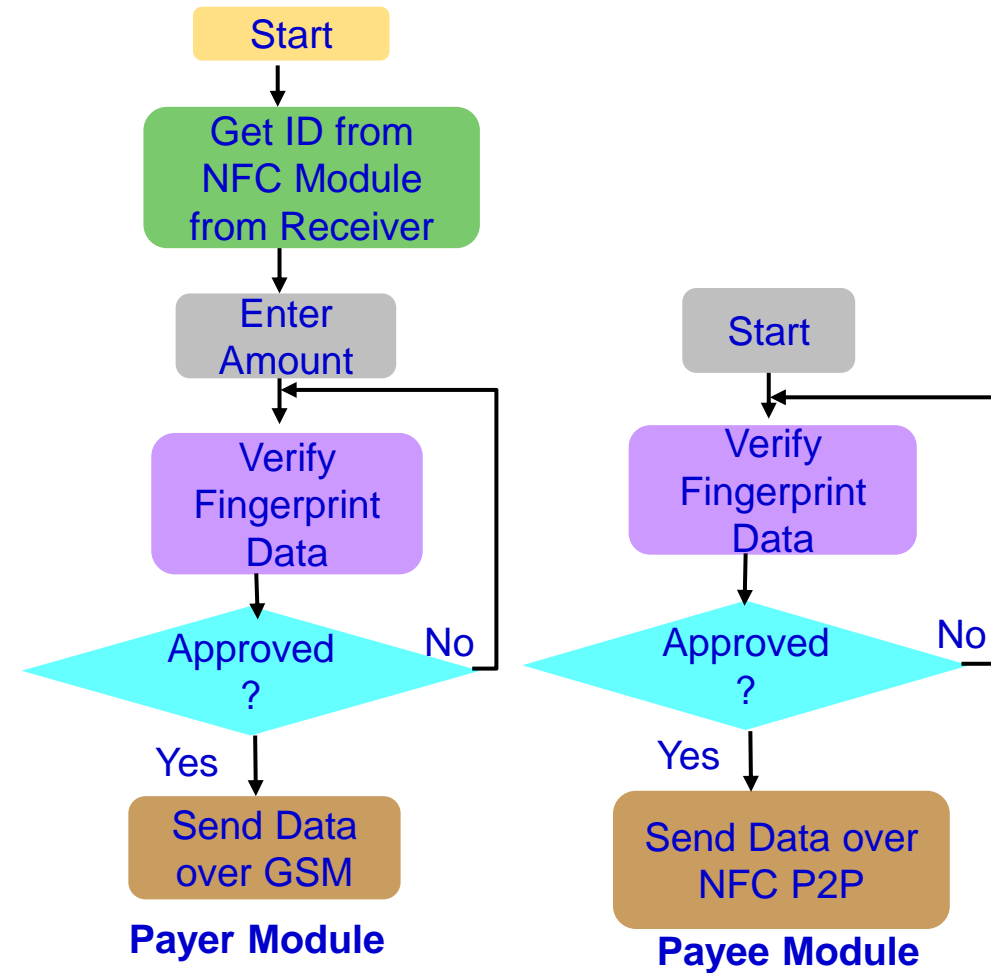
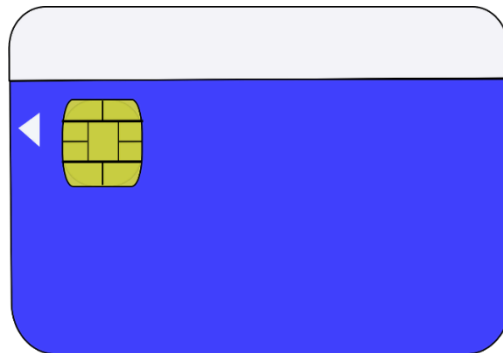
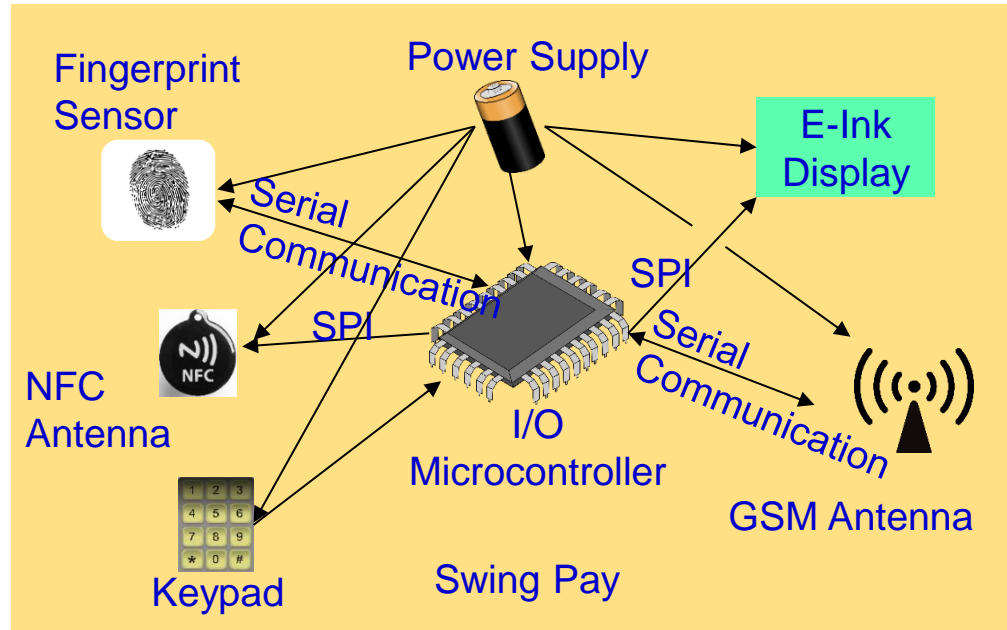
Source: Li and Jha 2011: HEALTH 2011

Blockchain in Smart Healthcare



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.

Our Swing-Pay - NFC Cybersecurity Solution



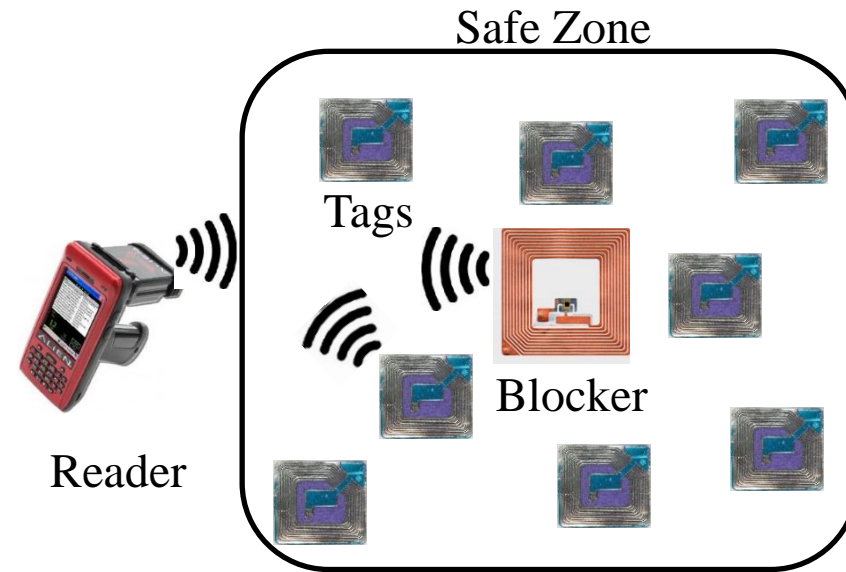
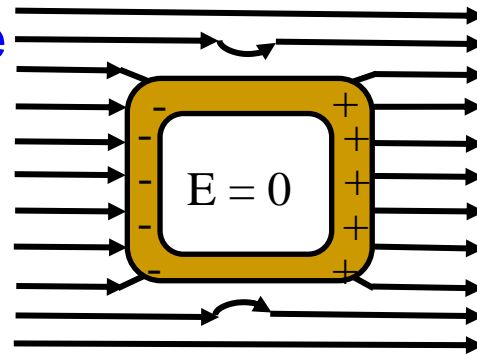
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

RFID Cybersecurity - Solutions

Selected RFID Security Methods



Faraday Cage



Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Drawbacks of Existing Cybersecurity Solutions



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

IT Cybersecurity

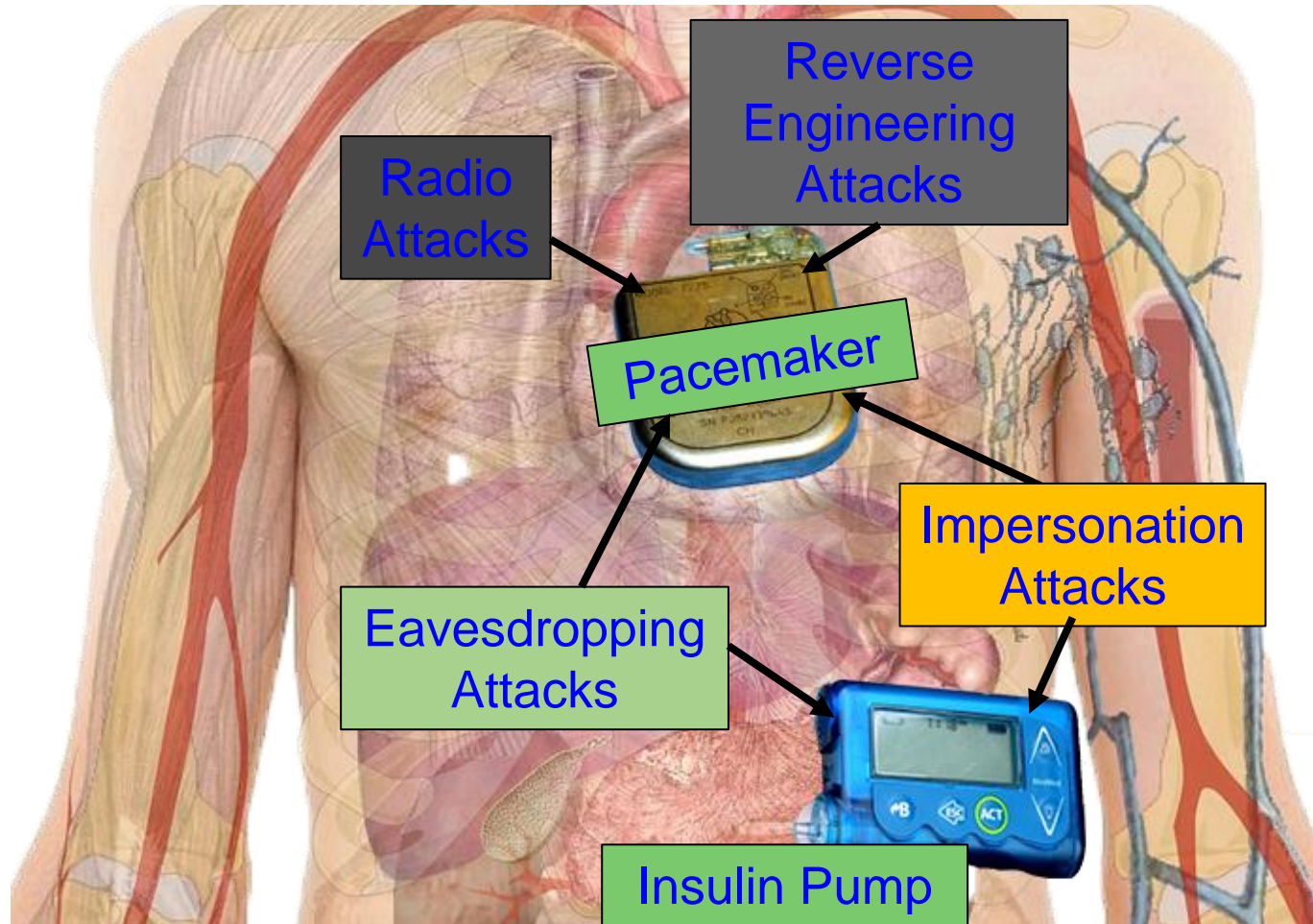
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

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

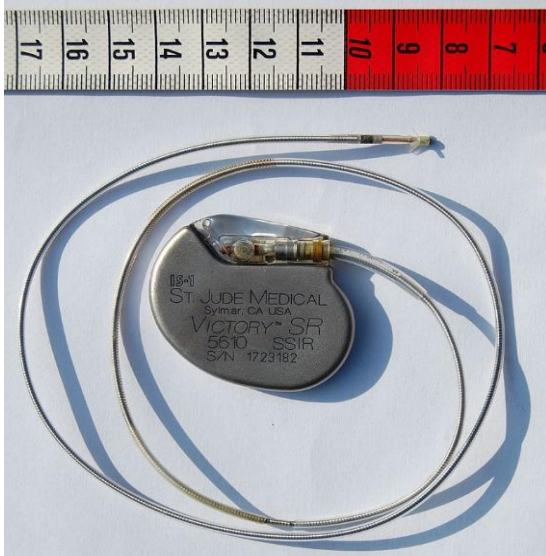


Collectively (WMD+IMD):
Implantable and Wearable
Medical Devices (IWMDs)

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-Lopez, 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

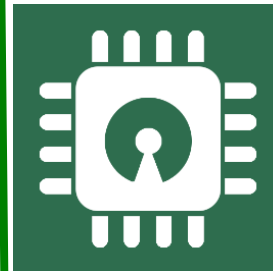
Software Based

- 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

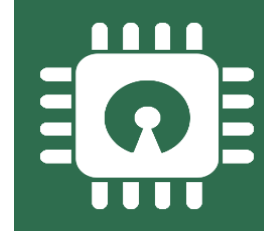
Cybersecurity Solutions – Software Vs Hardware Based

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

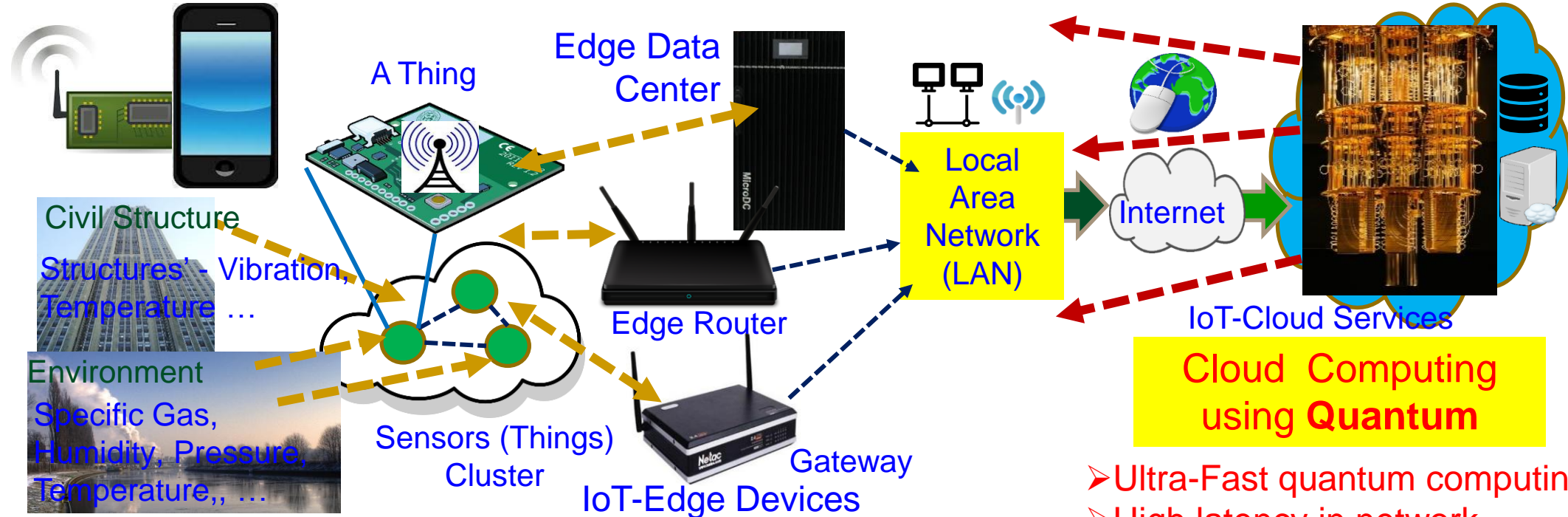
Source: Mohanty ICCE Panel 2018



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



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.

CPS Design - Multiple Objectives for Sustainability



Smart Cities
Vs
Smart Villages

Source: Mohanty ICCE 2019 Keynote

Privacy by Design (PbD) → General Data Protection Regulation (GDPR)

1995

Privacy by Design (PbD)

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



2018

General Data Protection Regulation (GDPR)

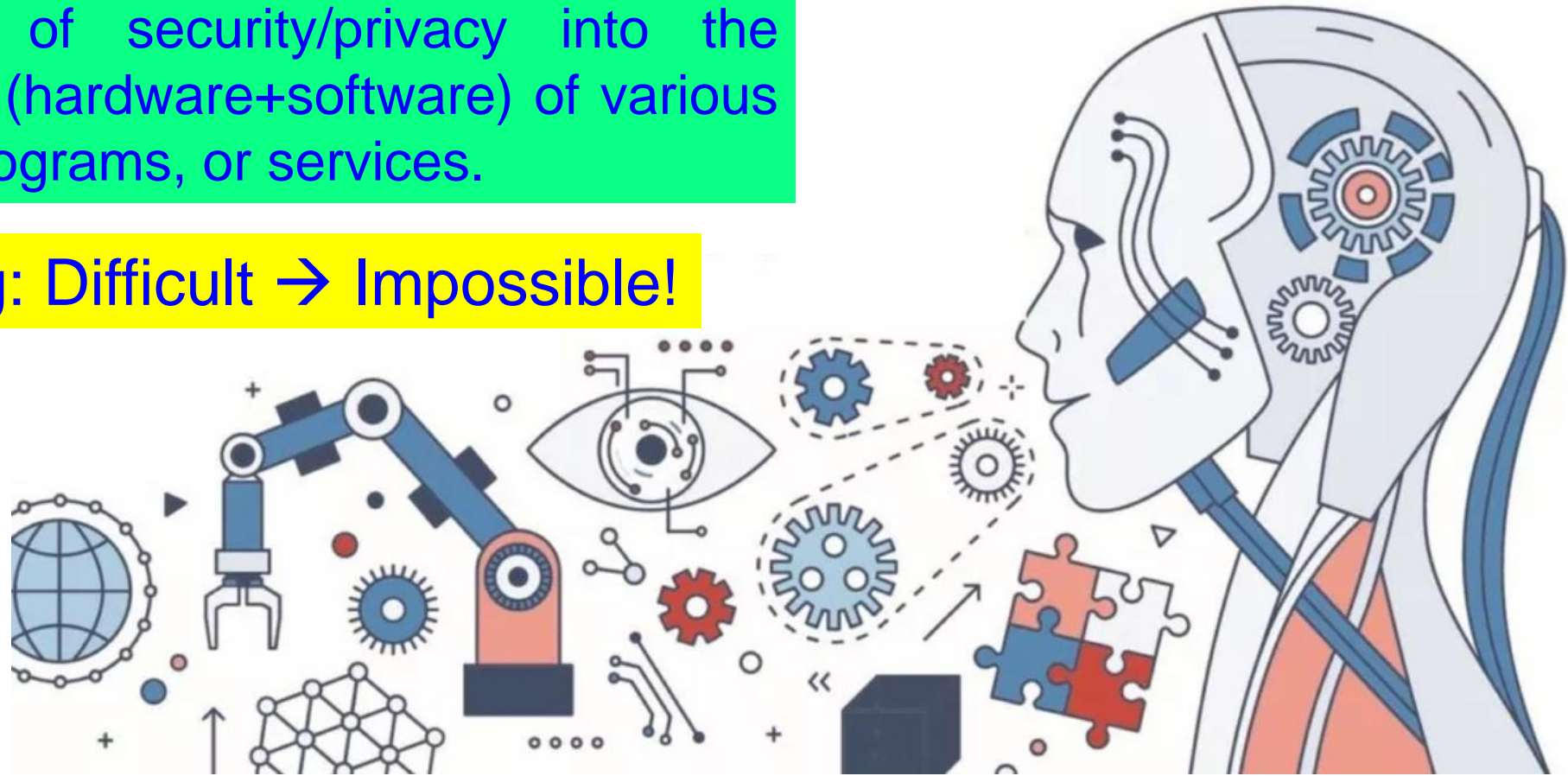
- ❖ GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

Security by Design (SbD)

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

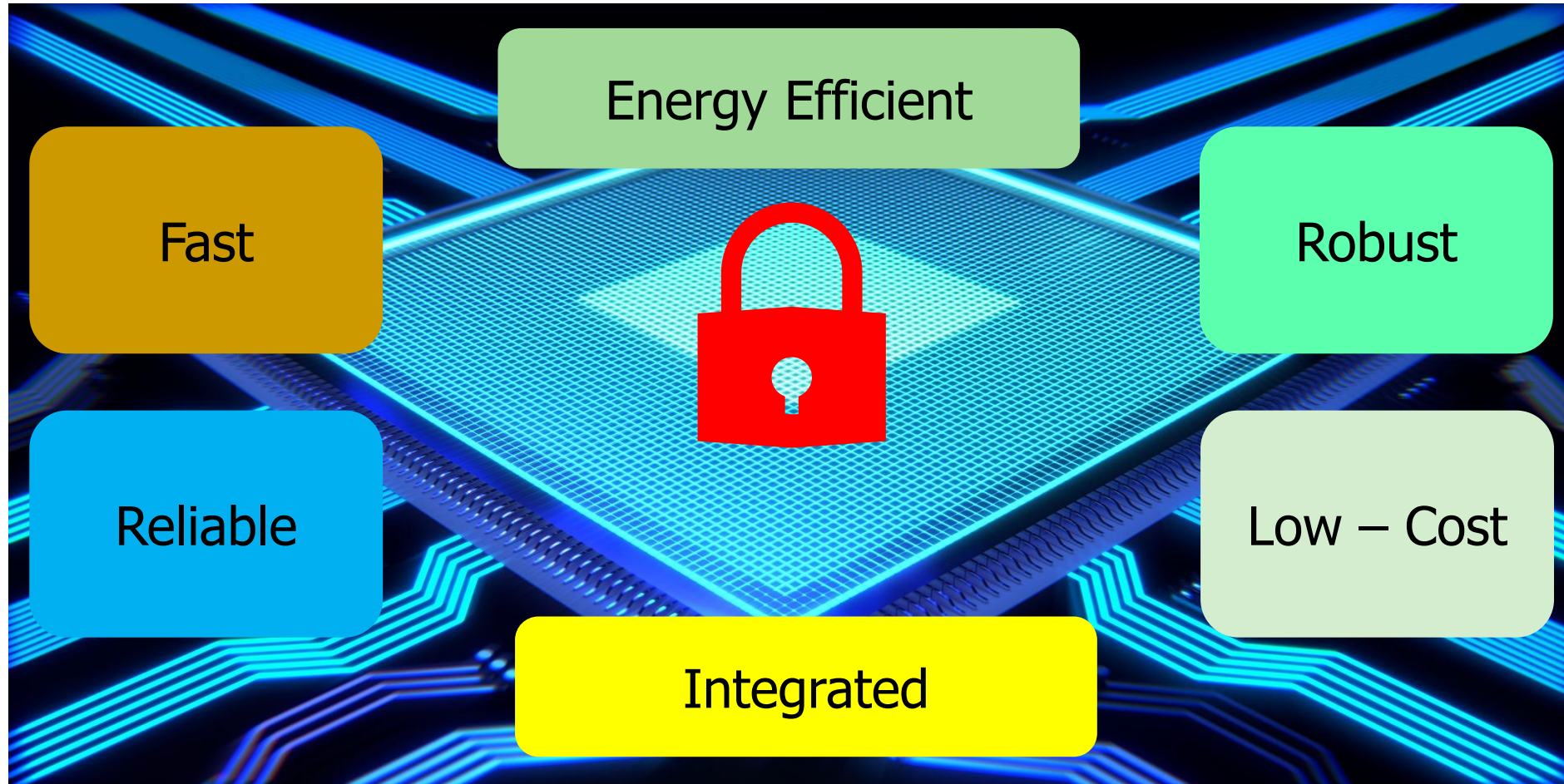
End-to-End Security/Privacy - Lifecycle Protection

Visibility and Transparency

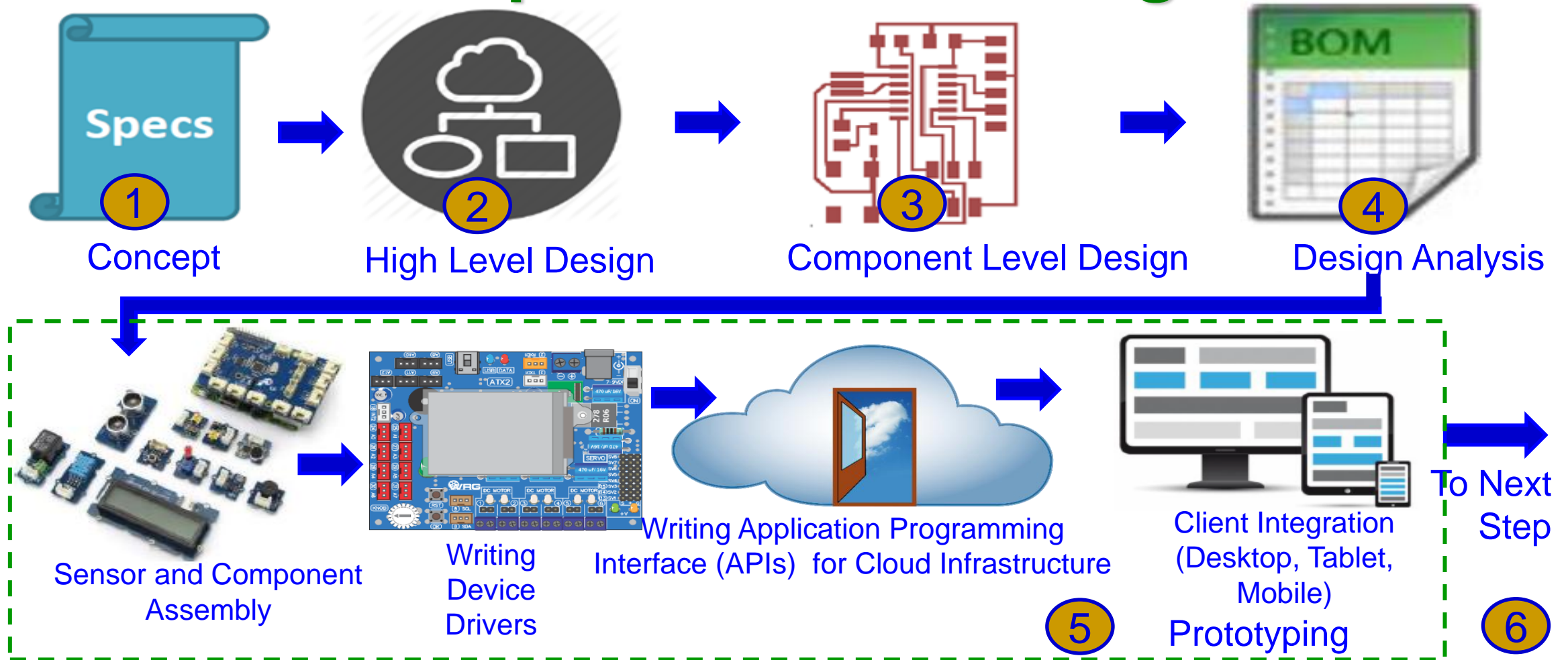
Respect for Users

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

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



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>

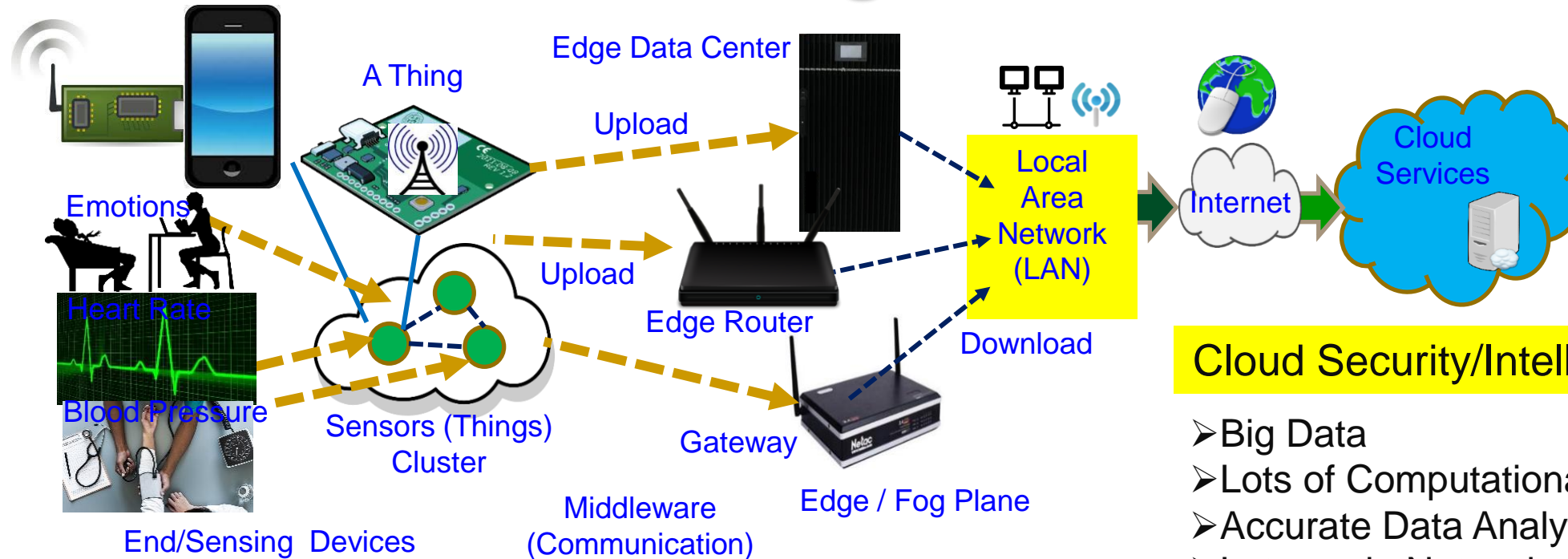
SbD Principle – IoT/CPS Design Flow



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%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

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

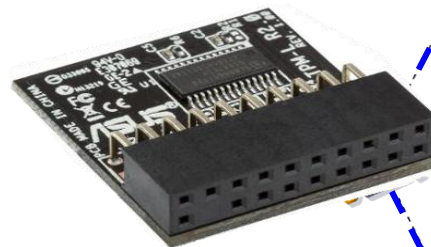
TinyML at End and/or Edge is key for smart villages.

Hardware Cybersecurity Primitives

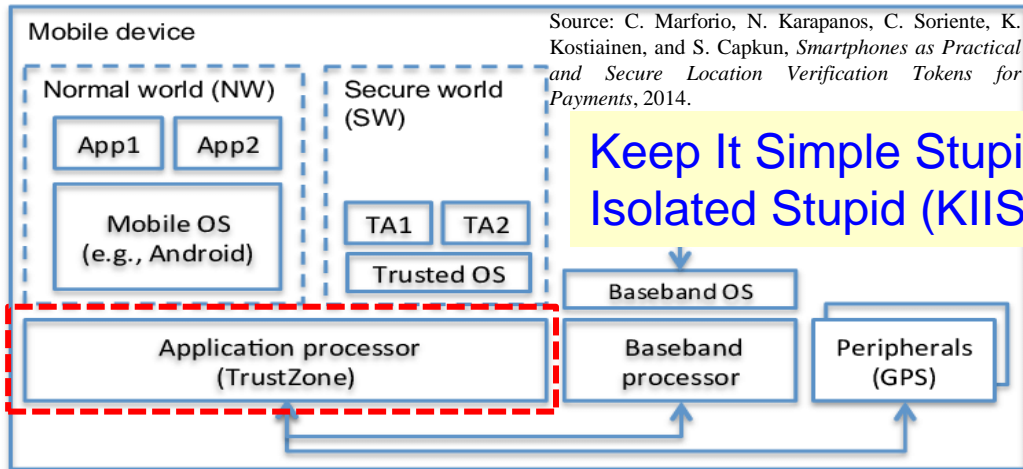
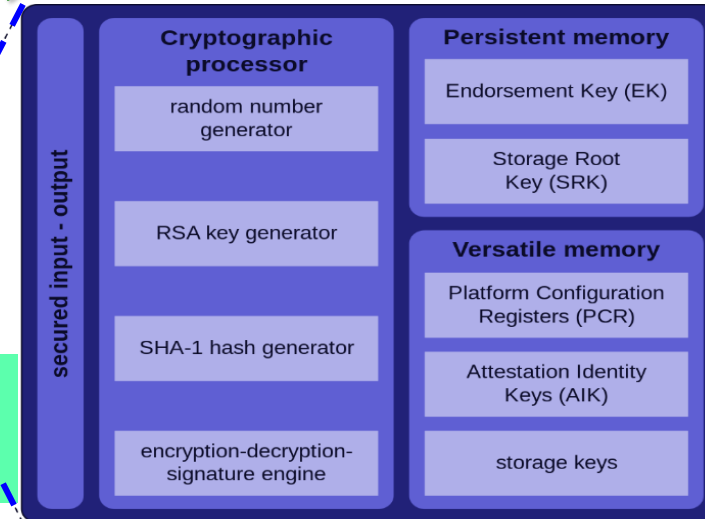
– HSM, TrustZone, TPM, and PUF



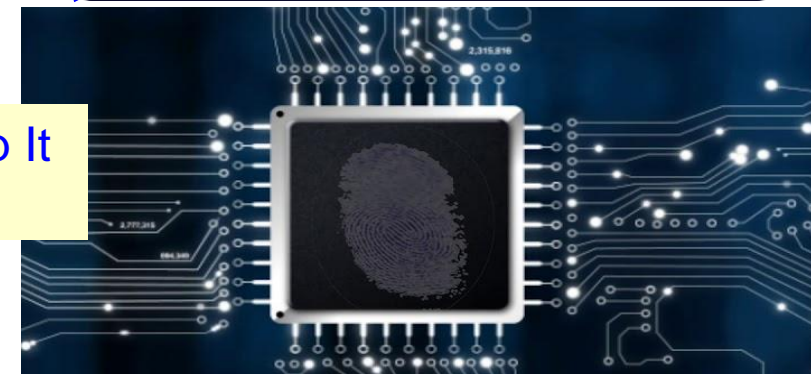
Hardware Security Module (HSM)



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.

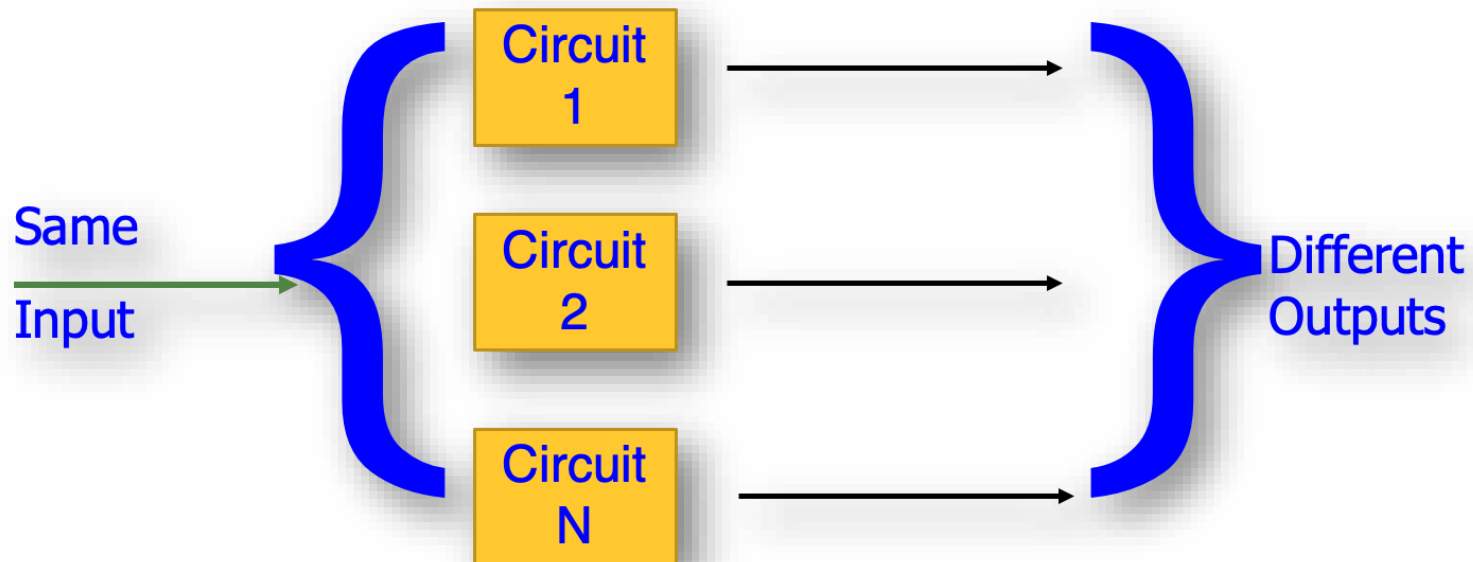


Physical Unclonable Functions (PUF)

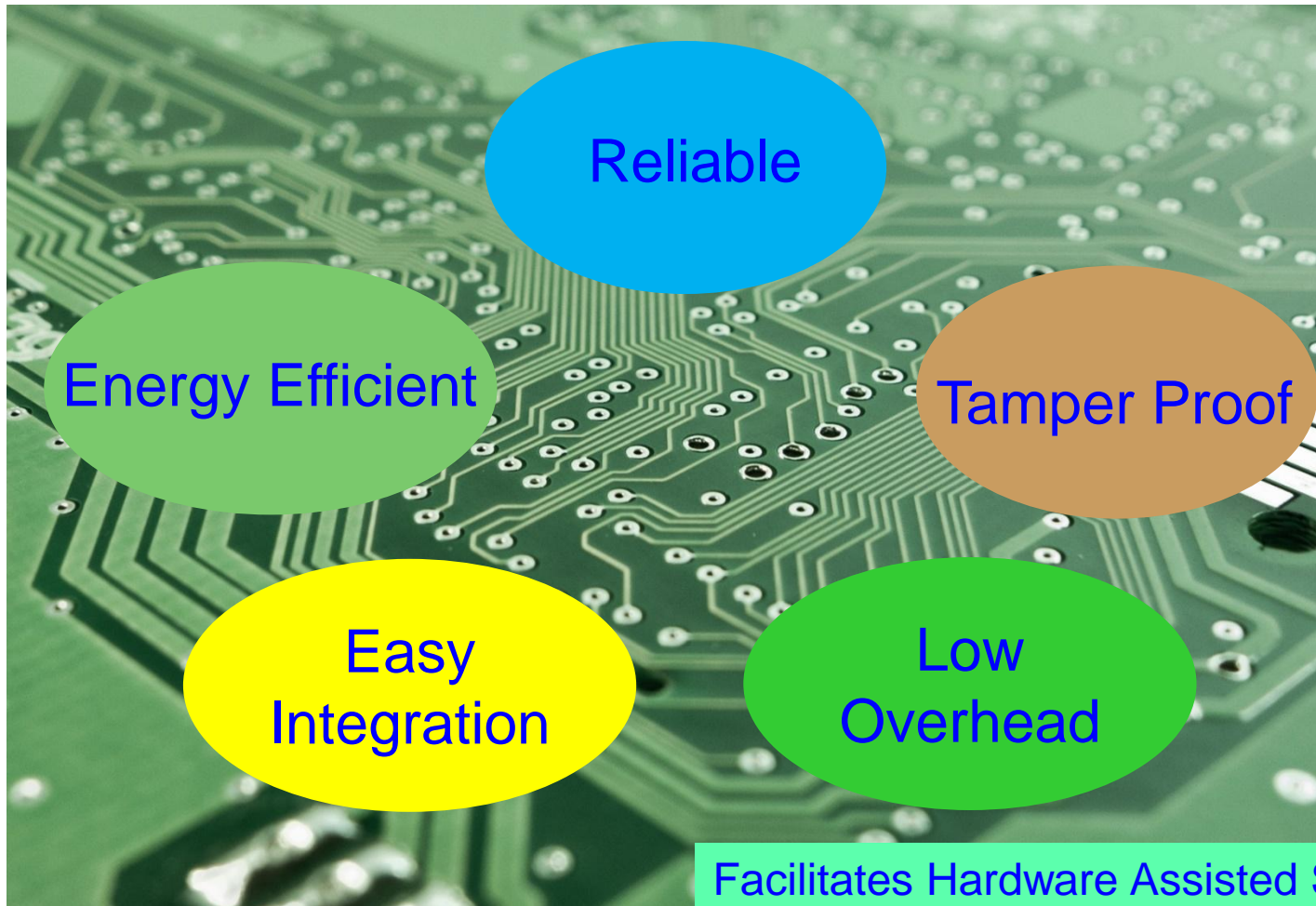
Source: Electric Power Research Institute (EPRI)

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.



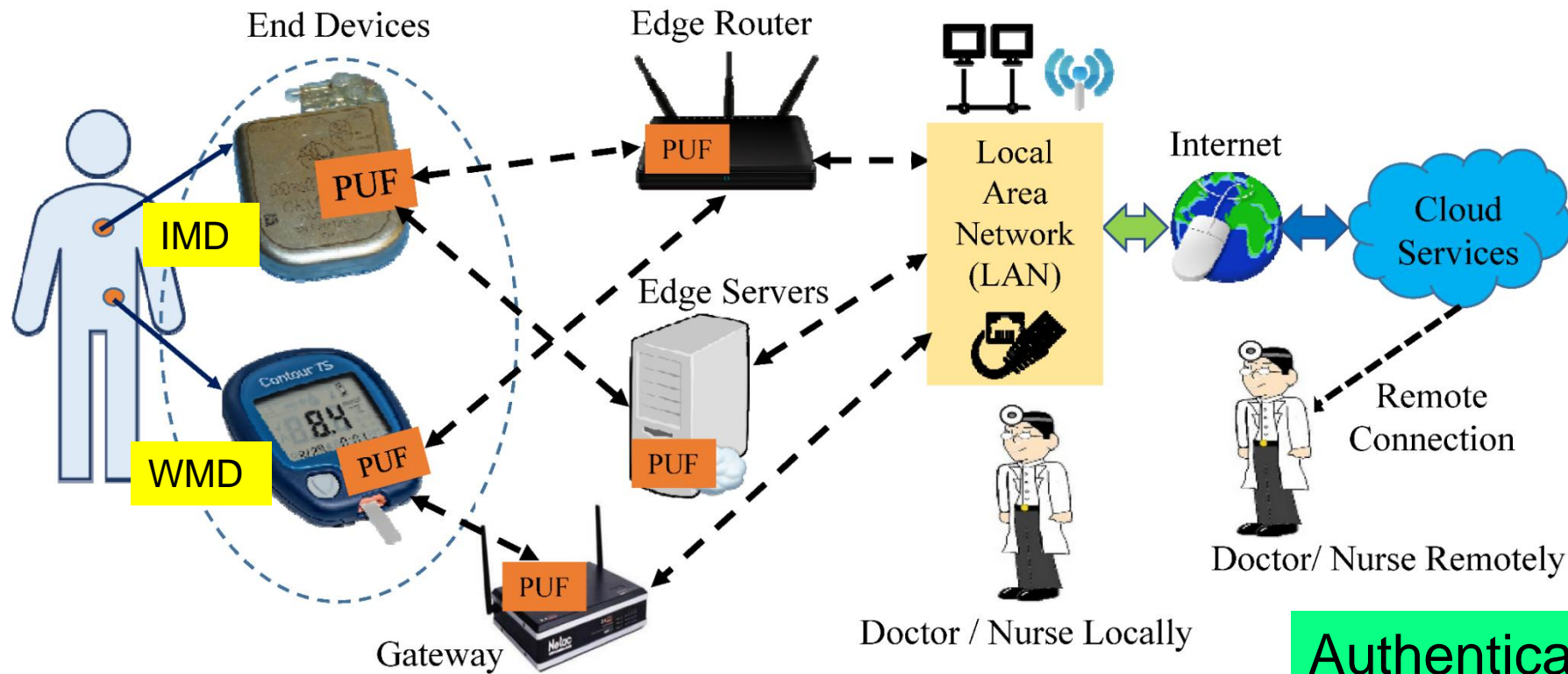
Physical Unclonable Function (PUF): Advantages



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

- 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

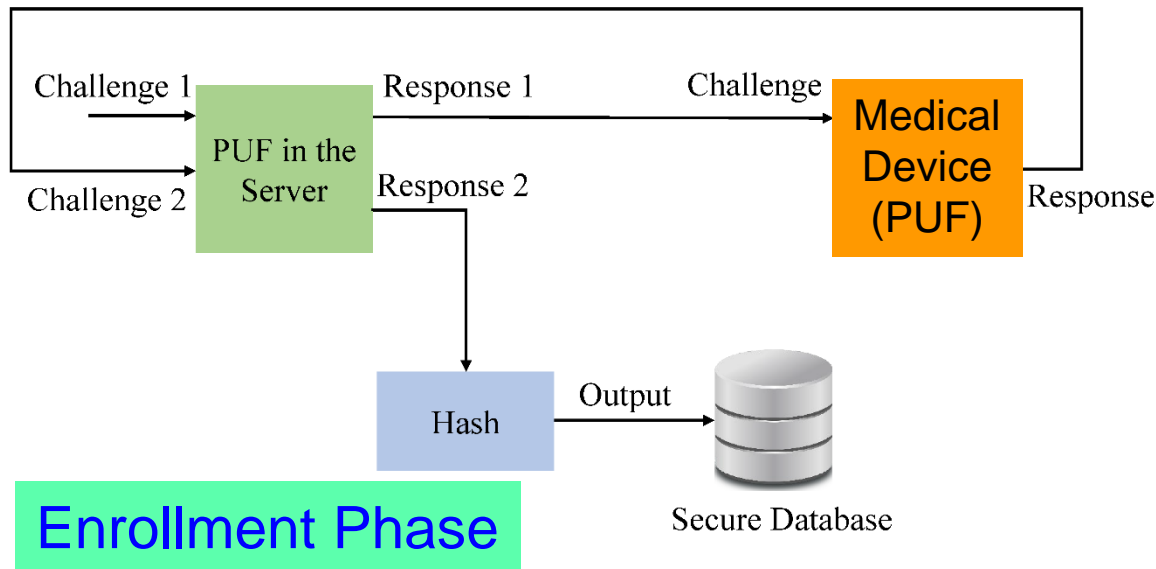
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μ 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



PUF Security Full Proof:

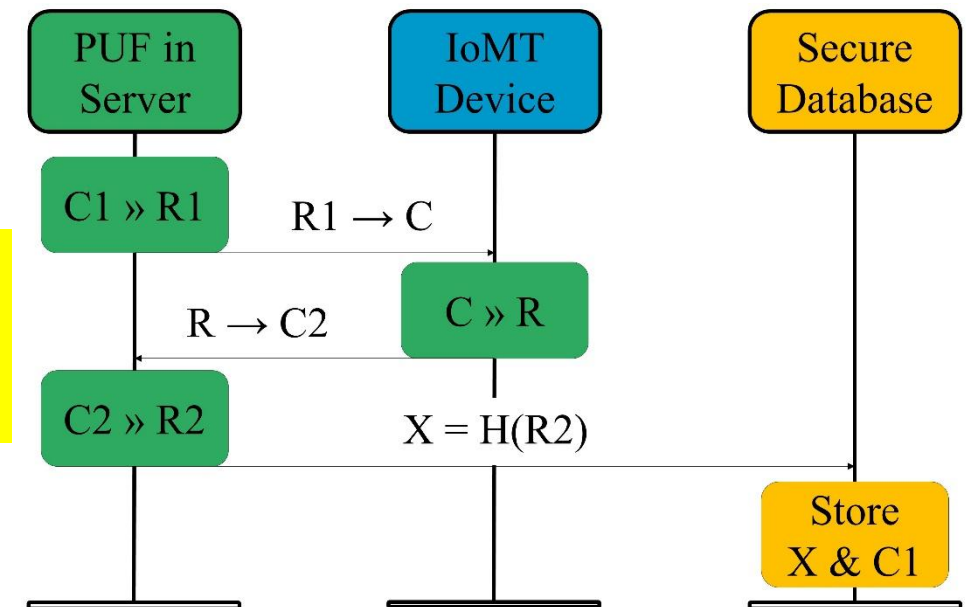
- Only server PUF Challenges are stored, not Responses
- Impossible to generate Responses without PUF

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.

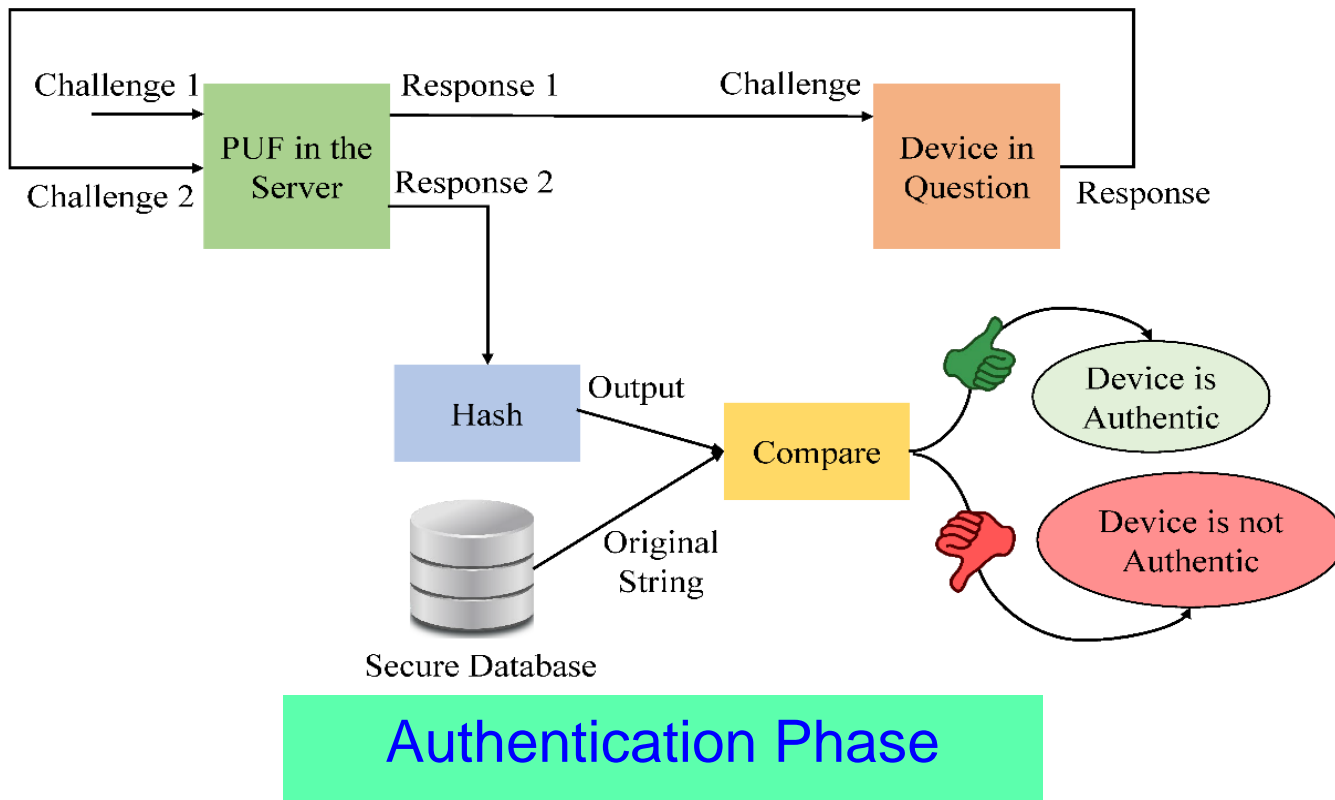
At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

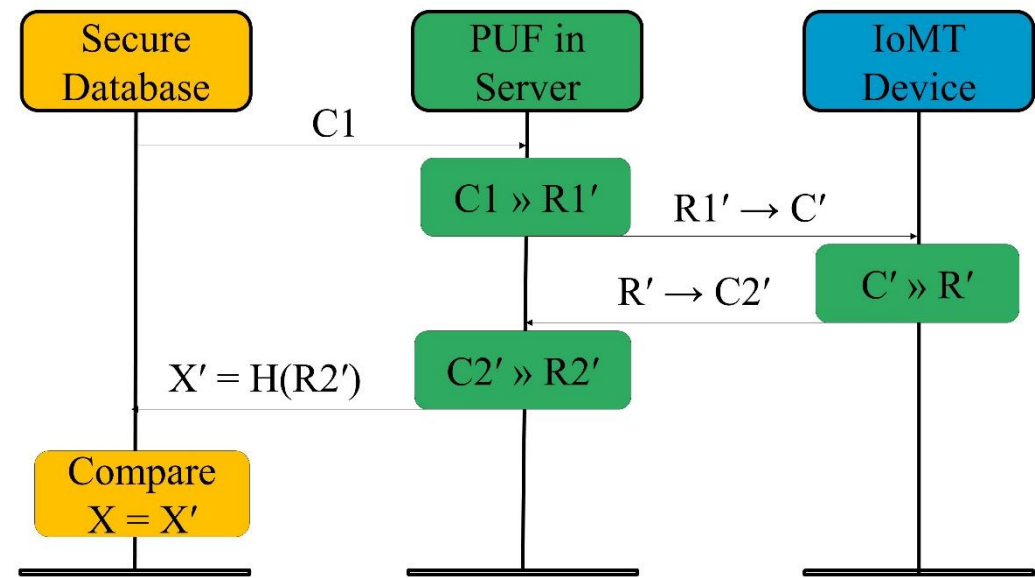


IoMT Security – Our Proposed PMsec



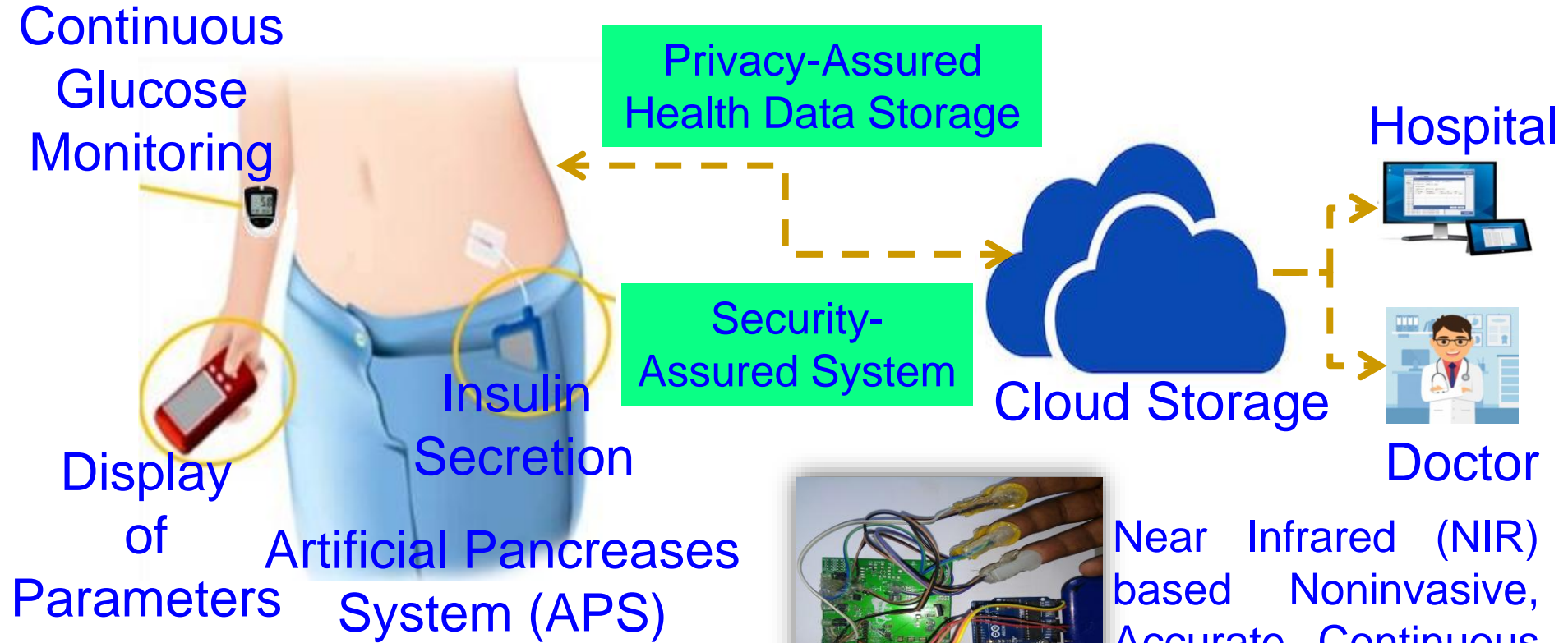
At the Doctor
 ➤ When doctor needs to access an existing IoMT-device

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.

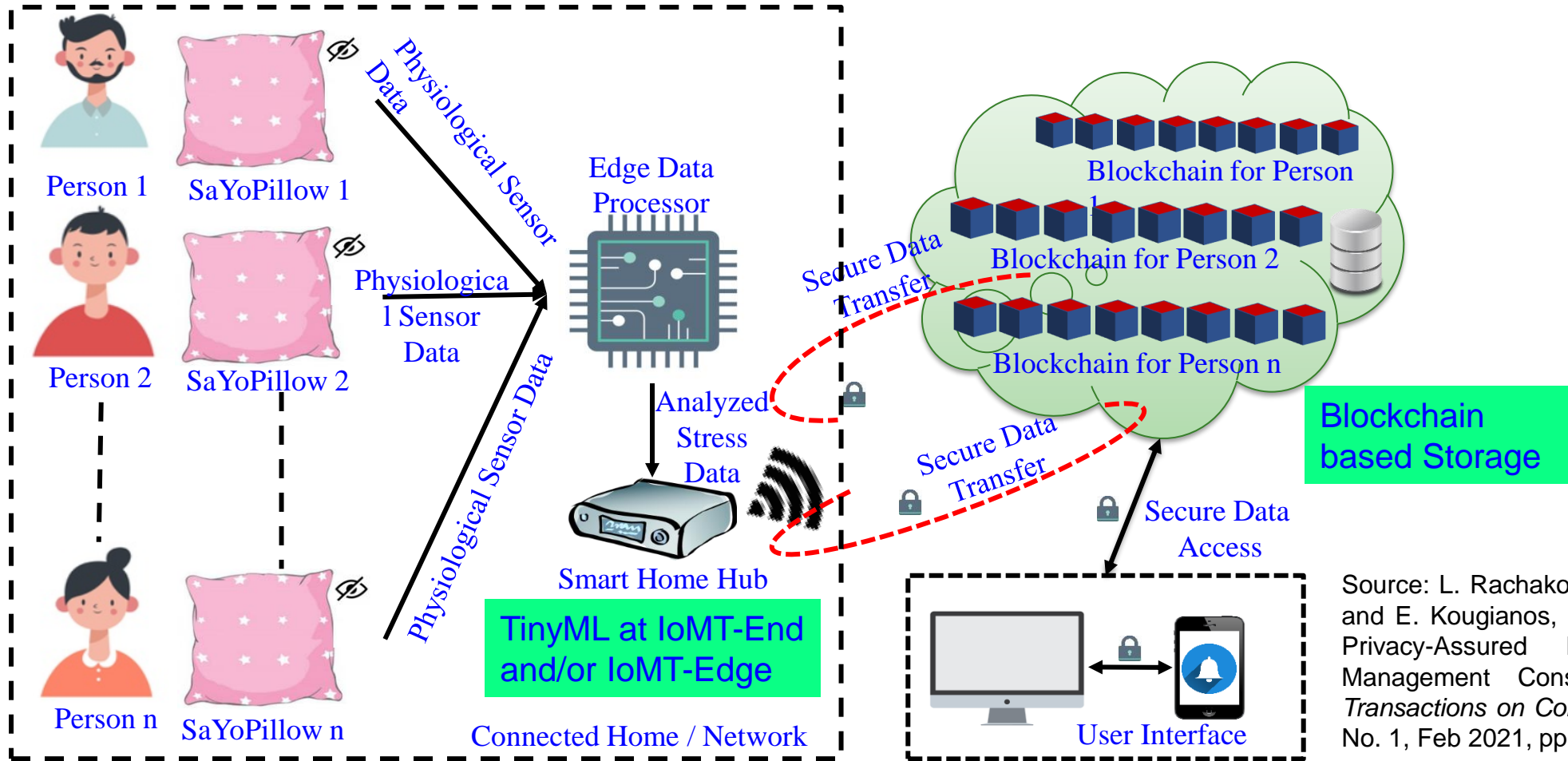
Secure-iGLU - Our Intelligent Non-Invasive Glucose Monitoring with Insulin Control Device



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

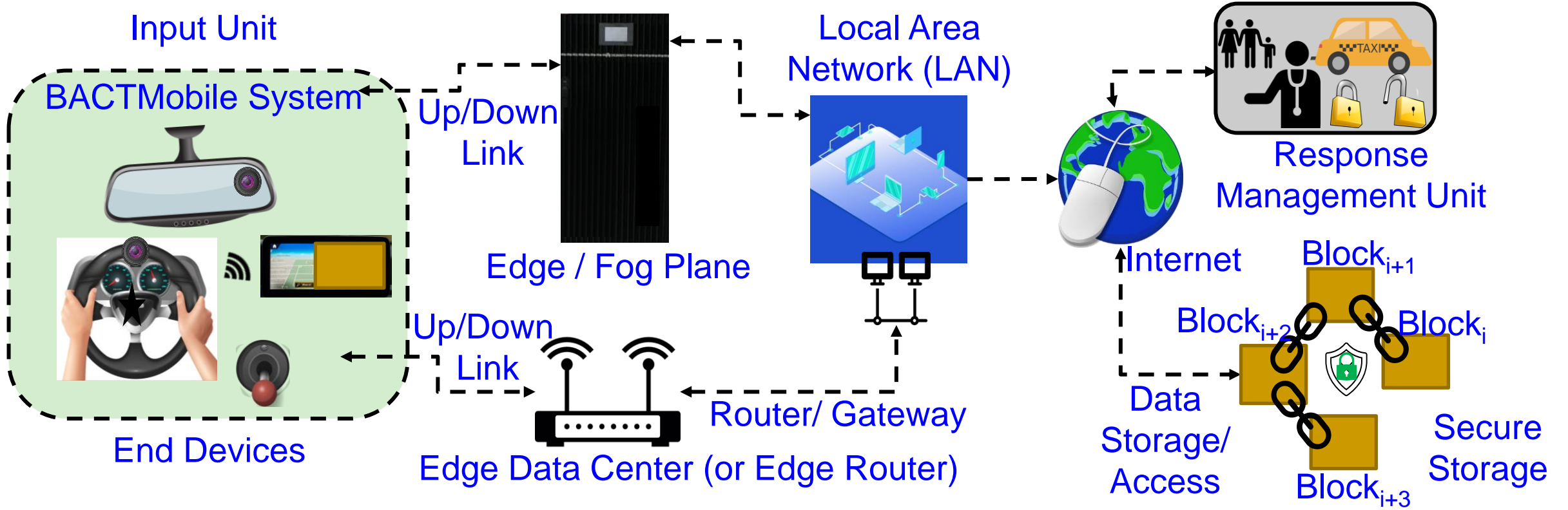
P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 1, January 2020, pp. 35–42.

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



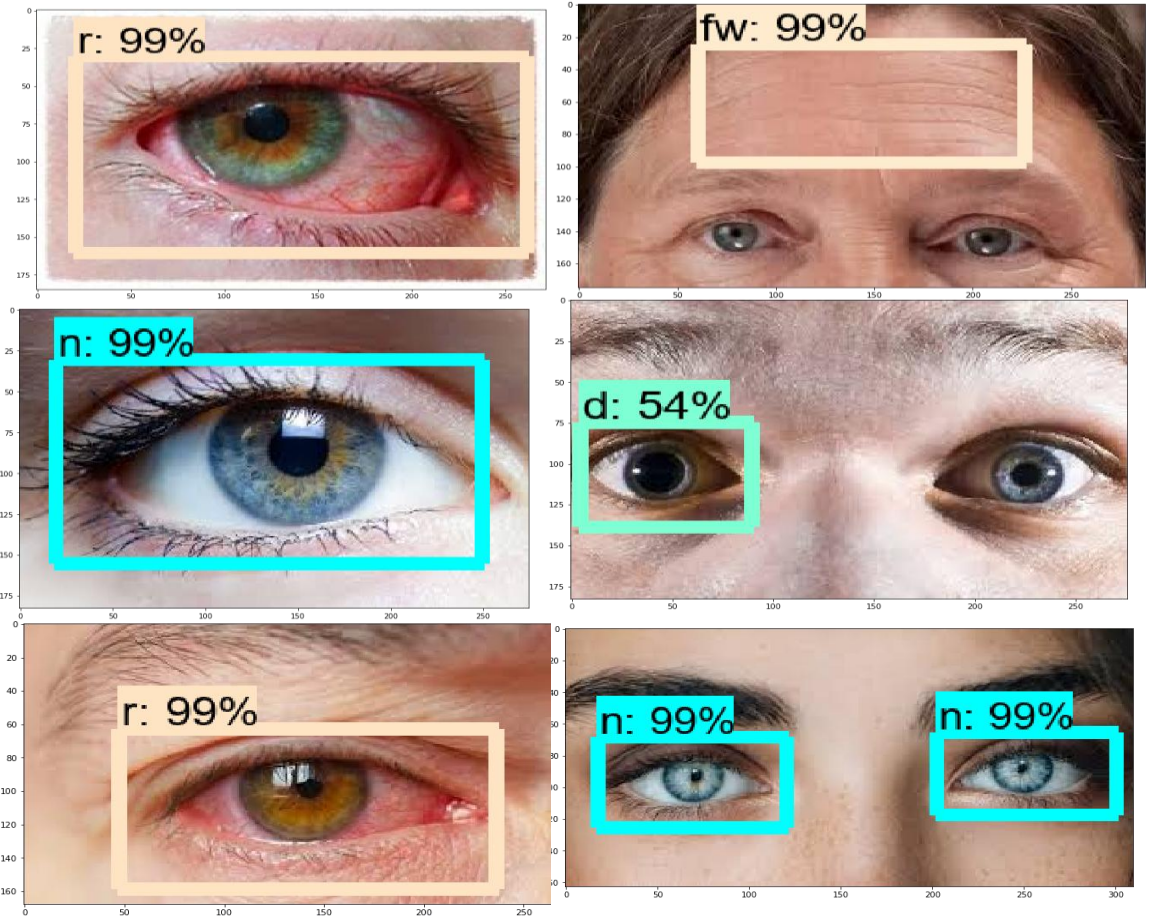
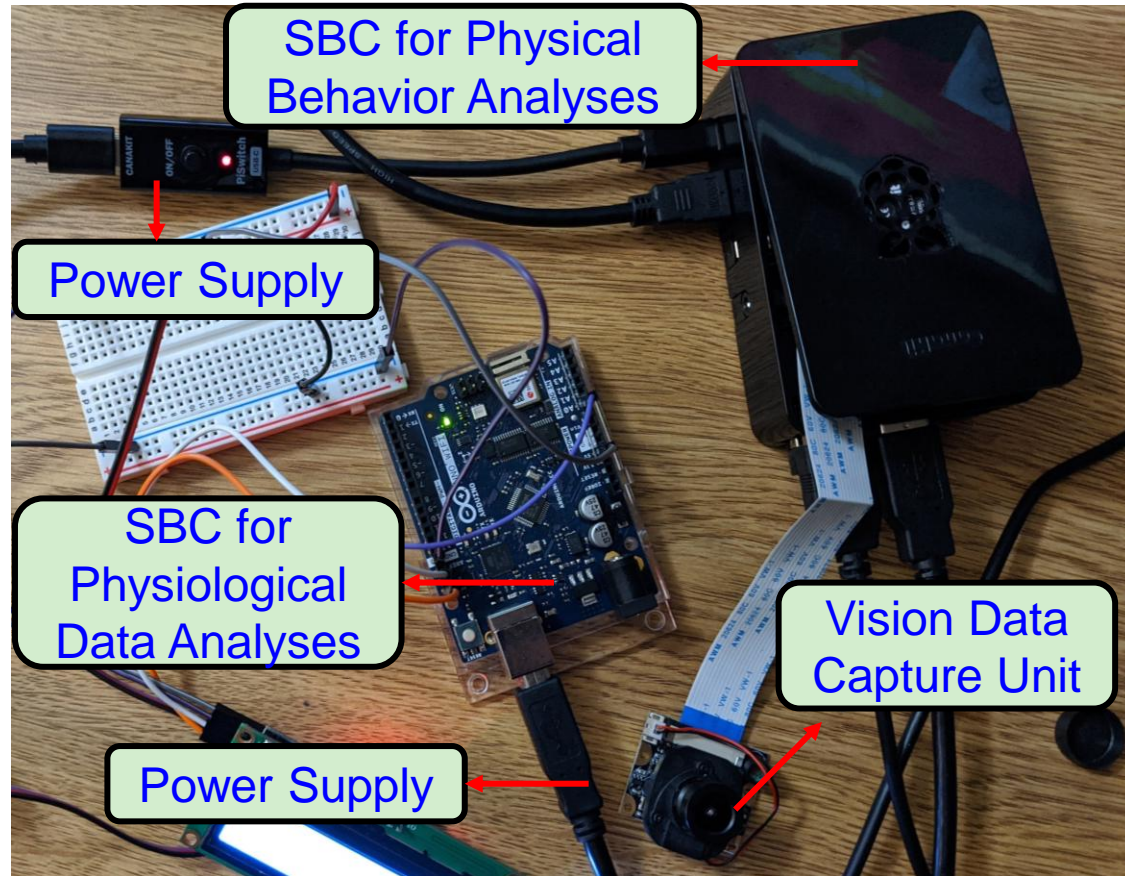
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habit", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

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



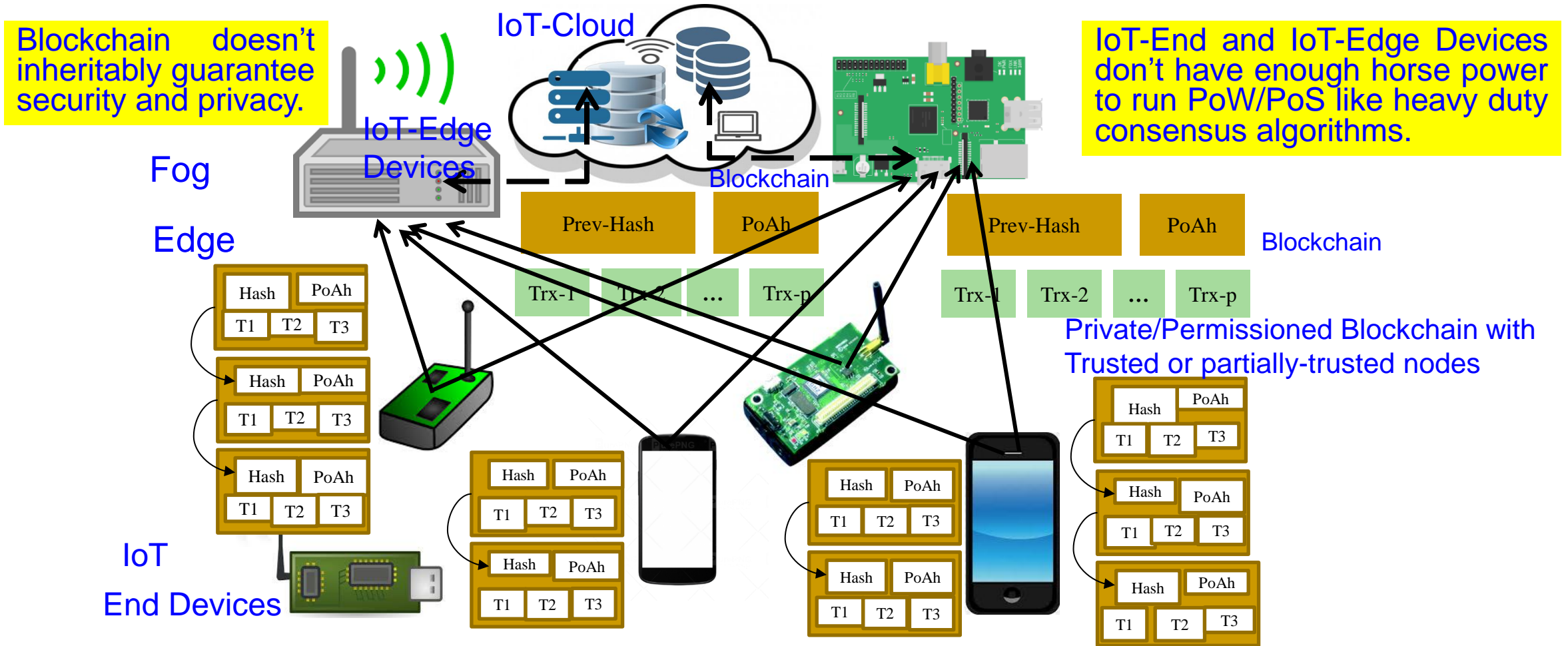
Source: L. Rachakonda, A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "BACTmobile: A Smart Blood Alcohol Concentration Tracking Mechanism for Smart Vehicles in Healthcare CPS Framework", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 236, 24-pages, DOI: <https://doi.org/10.1007/s42979-022-01142-9>.

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



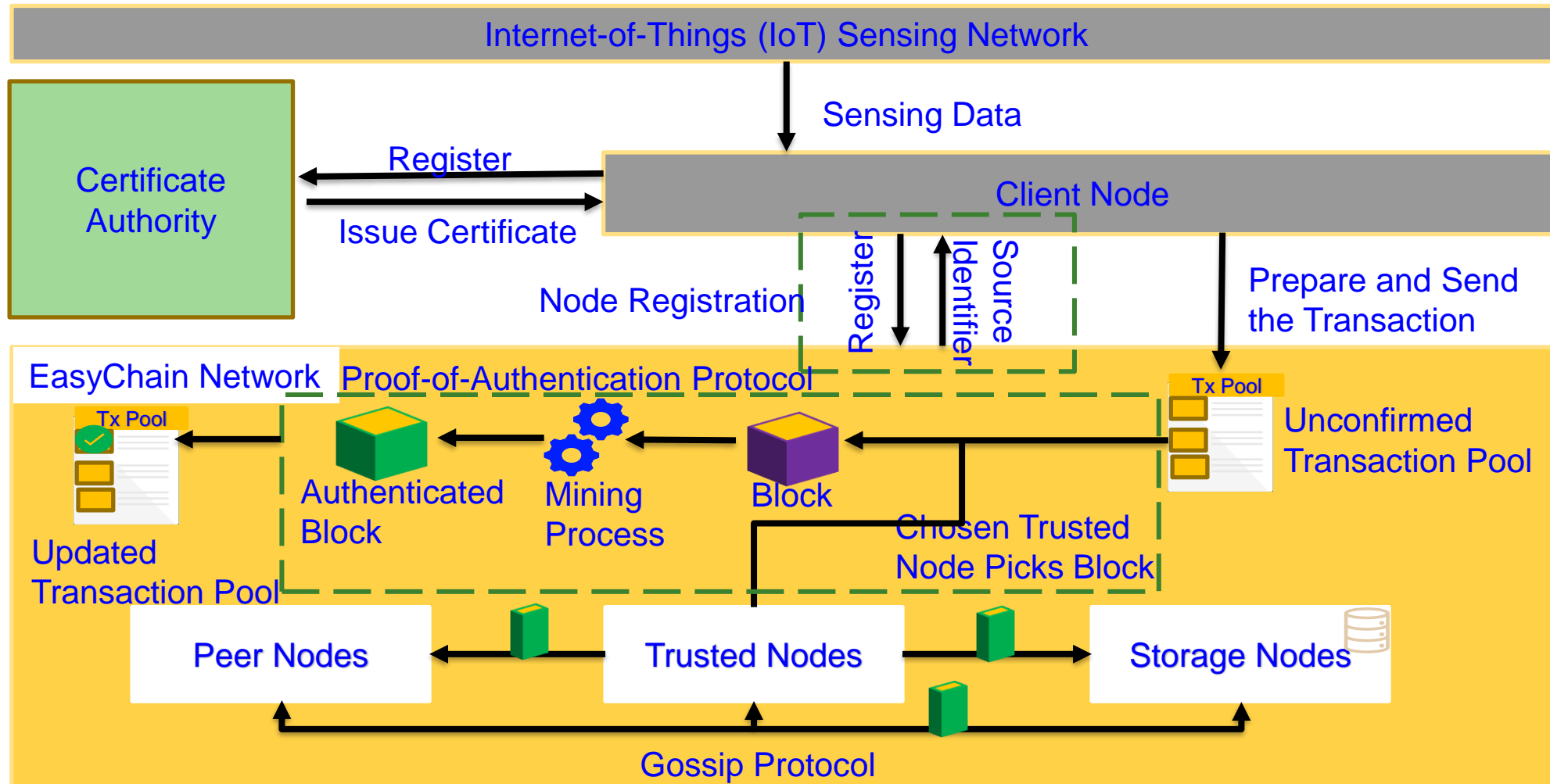
Source: L. Rachakonda, A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "BACTmobile: A Smart Blood Alcohol Concentration Tracking Mechanism for Smart Vehicles in Healthcare CPS Framework", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 236, 24-pages, DOI: <https://doi.org/10.1007/s42979-022-01142-9>.

IoT-Friendly Blockchain – Our EasyChain



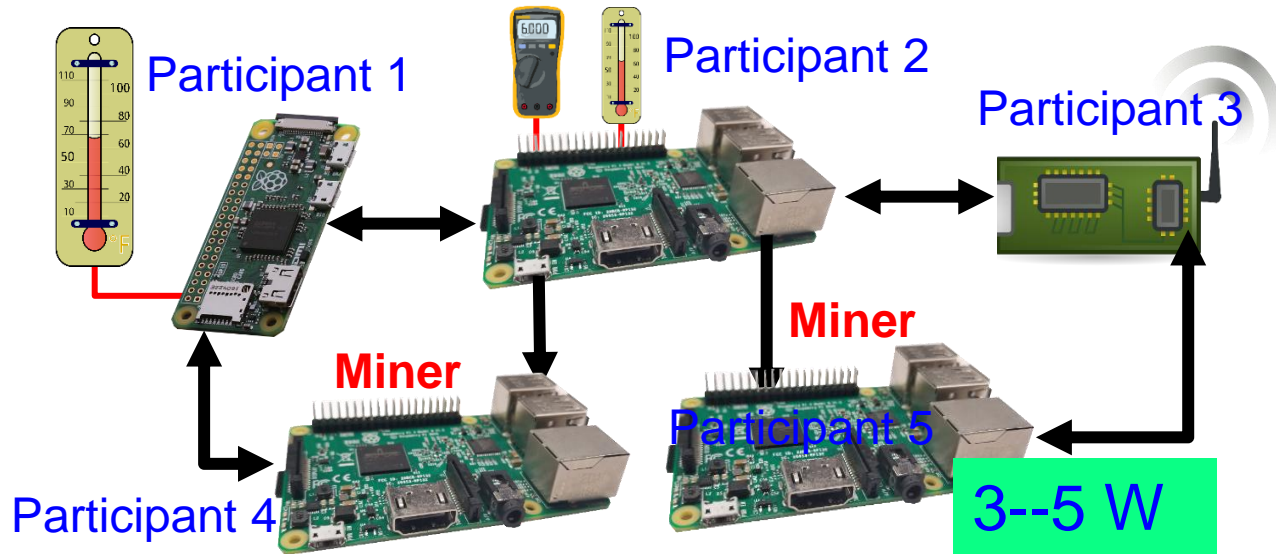
Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

Our EasyChain: Architectural Overview



Source: A. K. Bapatla, D. Puthal, **S. P. Mohanty**, V. P. Yanambaka, and E. Kougianos, "EasyChain: An IoT-Friendly Blockchain for Robust and Energy-Efficient Authentication", *Frontiers in Blockchain*, Vol. 6, No. 1194883, Aug 2023, pp. 1--19, DOI: <https://doi.org/10.3389/fbloc.2023.1194883>.

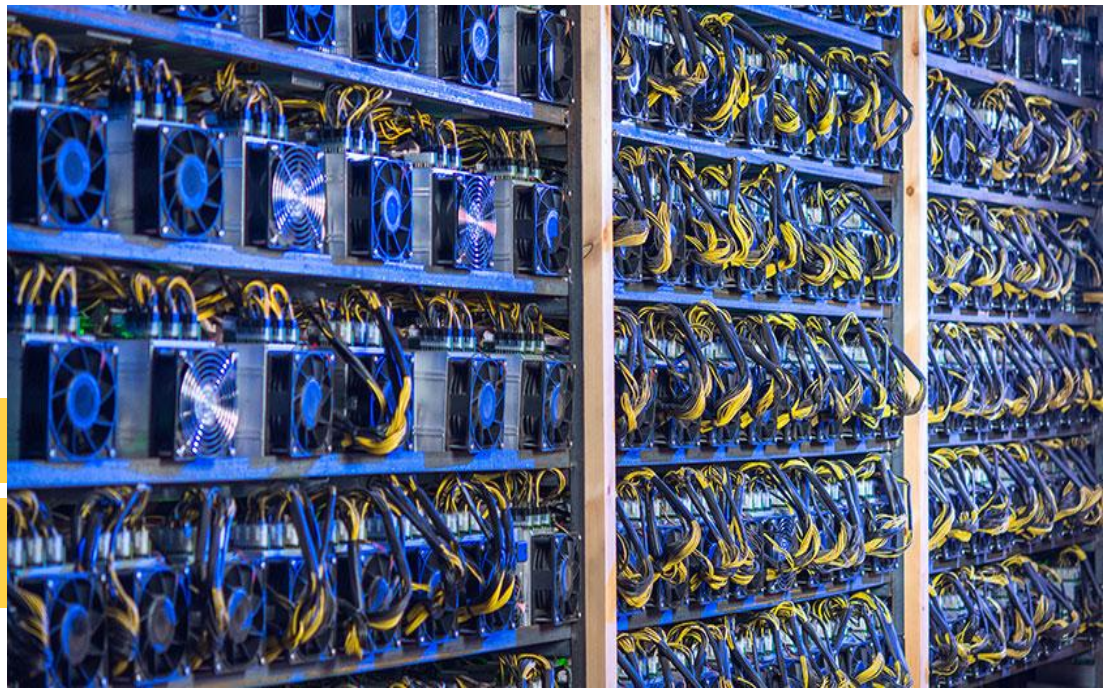
Our EasyChain with PoAh Runs in Resource Constrained Environment



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

Blockchain using PoW Needs Significant Resource

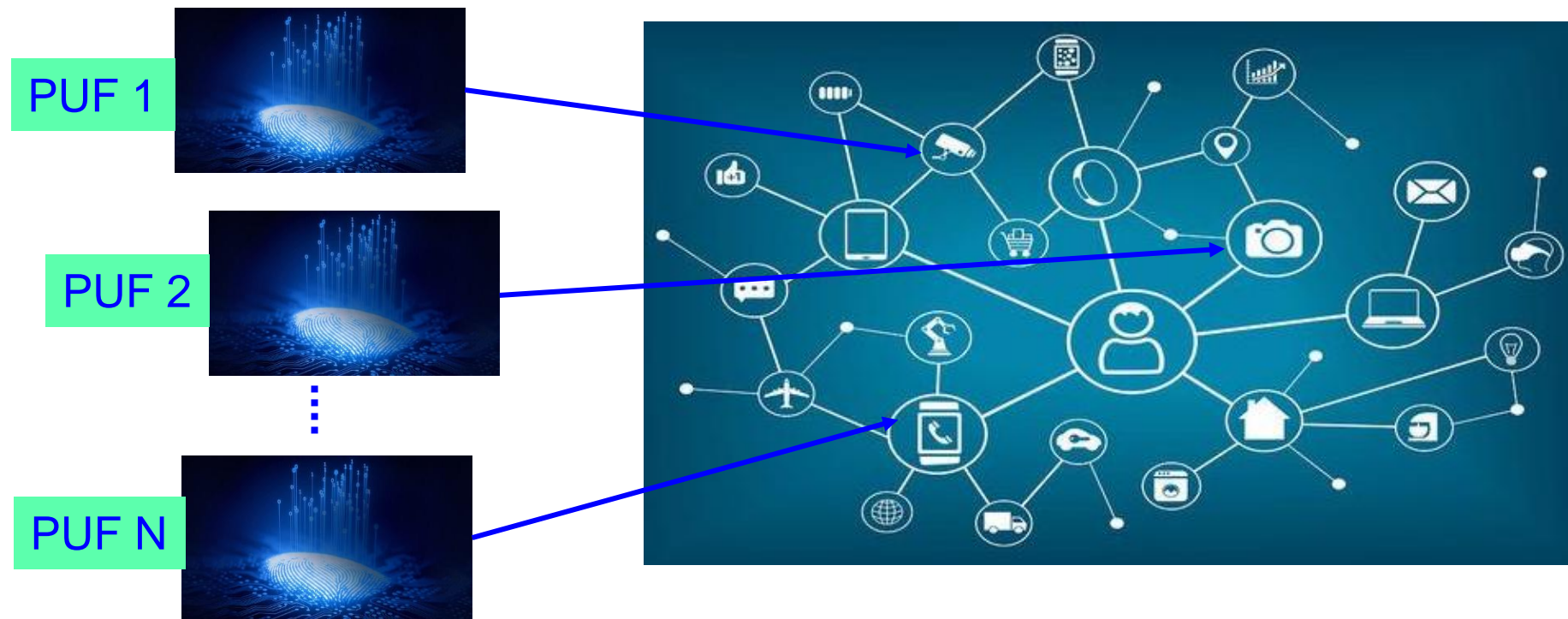
500,0000 W



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](https://arxiv.org/abs/2001.07297), January 2020, 26-pages.

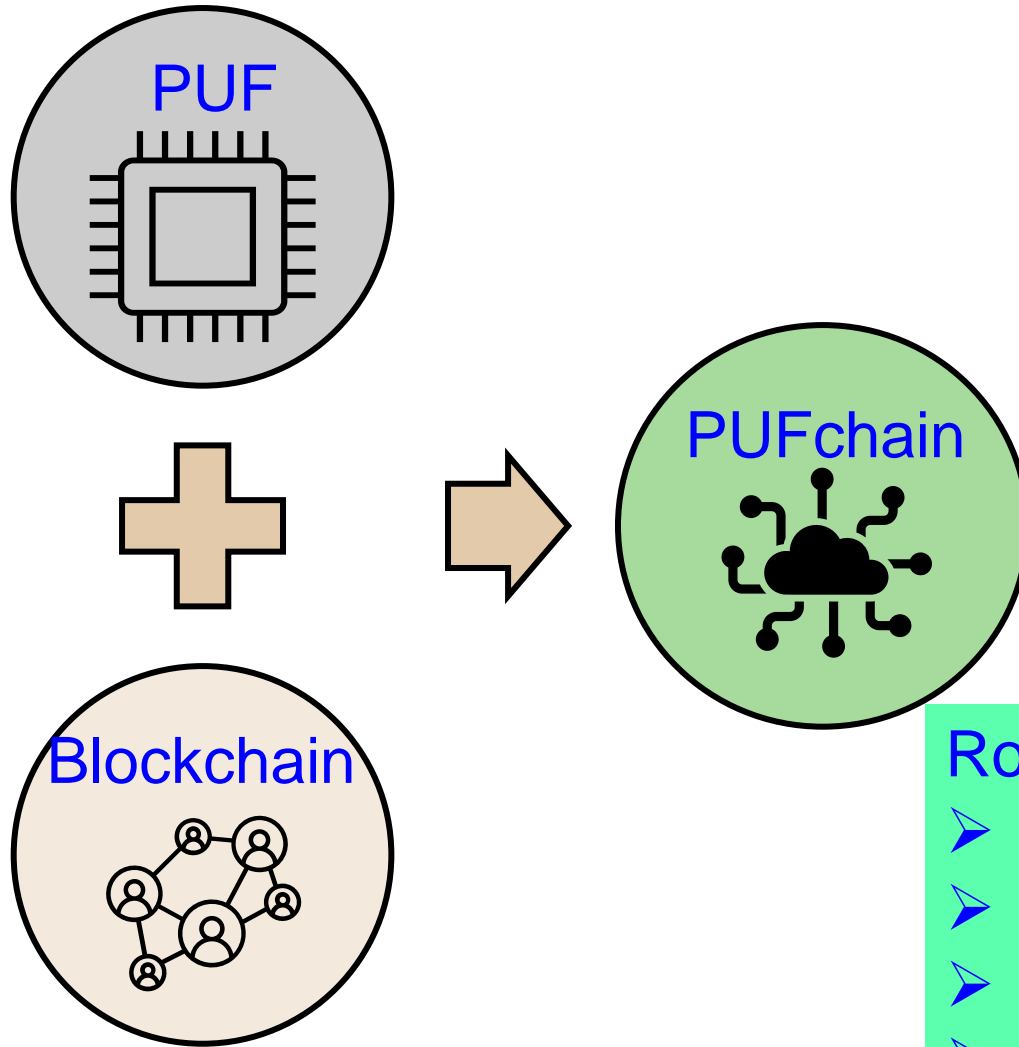
Source: <https://www.iea.org/newsroom/news/2019/july/bitcoin-energy-use-mined-the-gap.html>

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

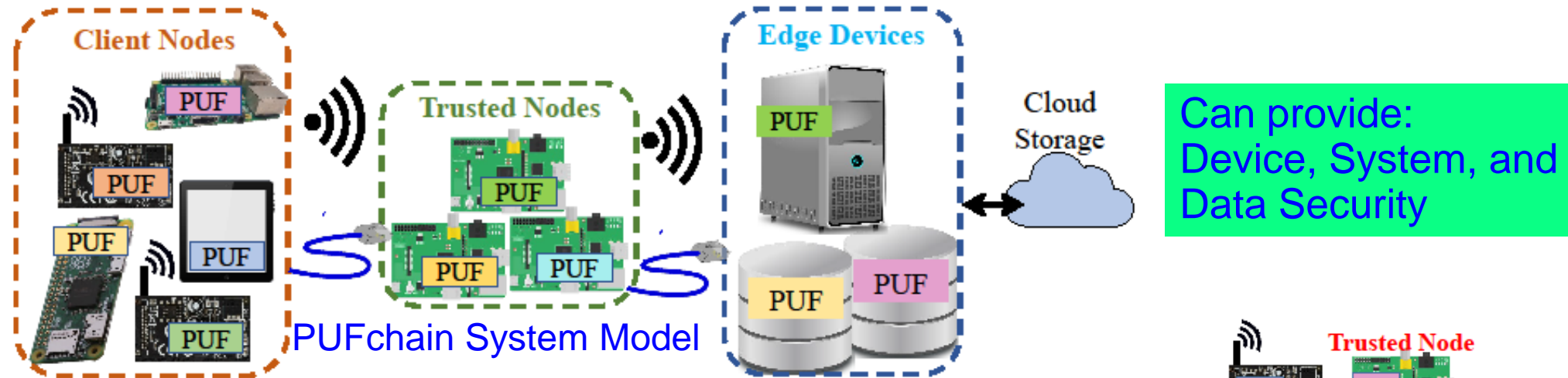


Blockchain Technology is integrated with Physically Unclonable Functions as PUFchain by storing the PUF Key into immutable Blockchain

Roles of PUF:

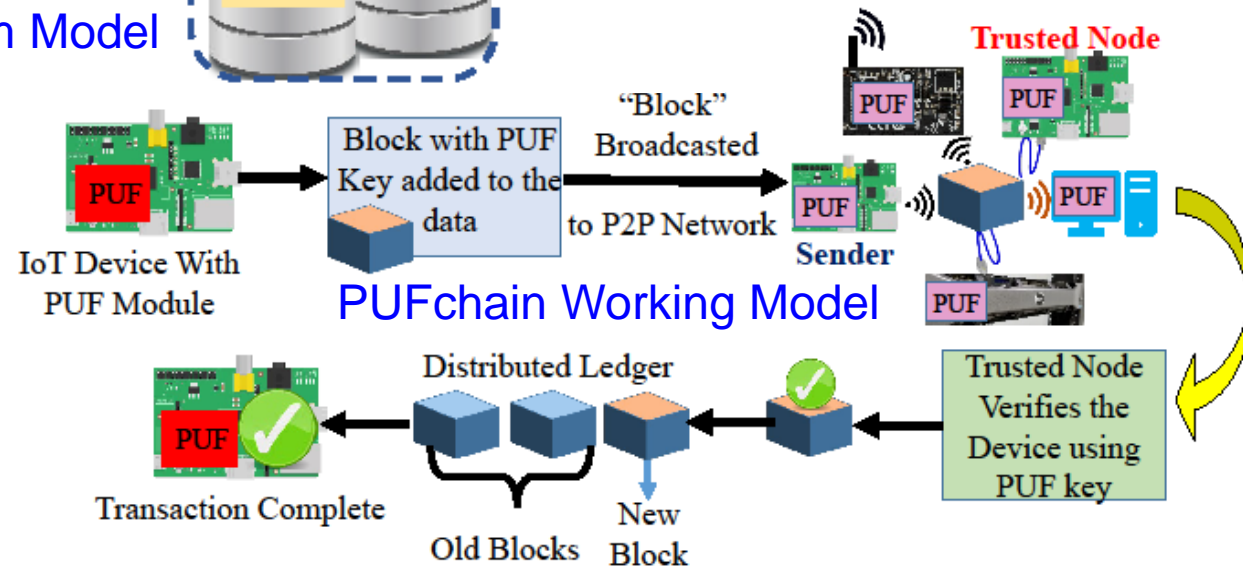
- Hardware Accelerator for Blockchain
- Independent Authentication
- Double-Layer Protection
- 3 modes: PUF, Blockchain, PUF+Blockchain

PUFchain: Our Hardware-Assisted Scalable Blockchain



Can provide:
Device, System, and
Data Security

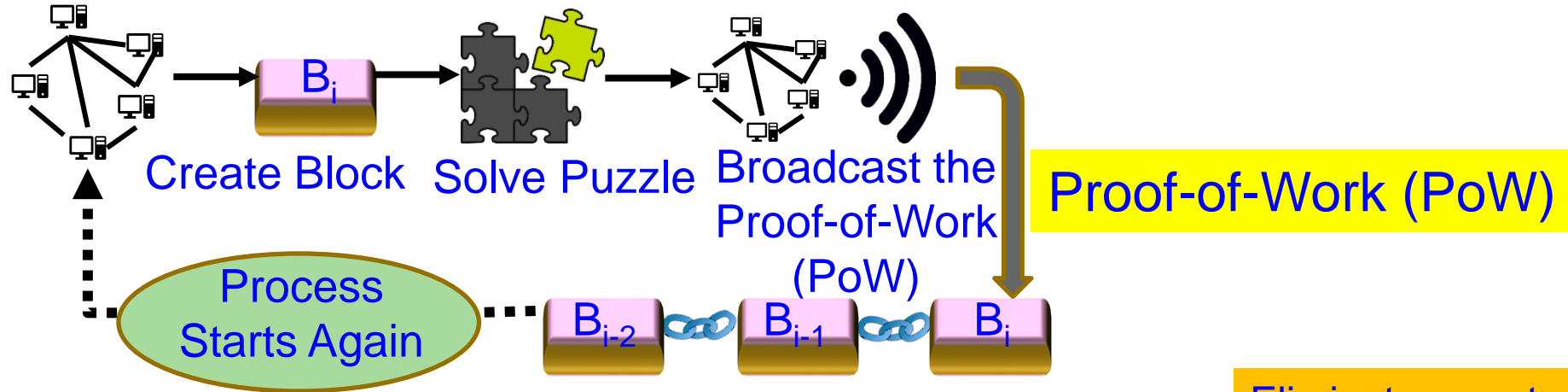
PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode



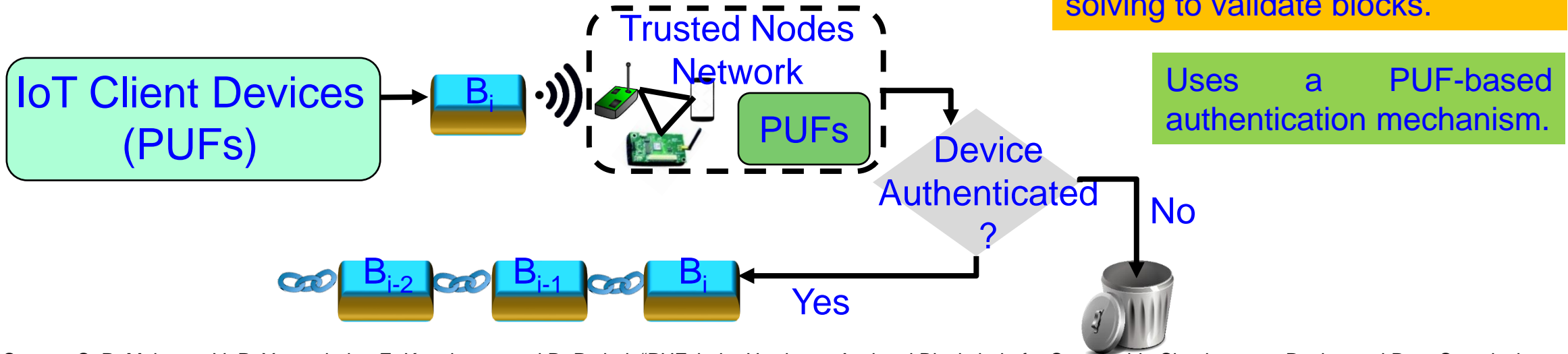
- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

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)

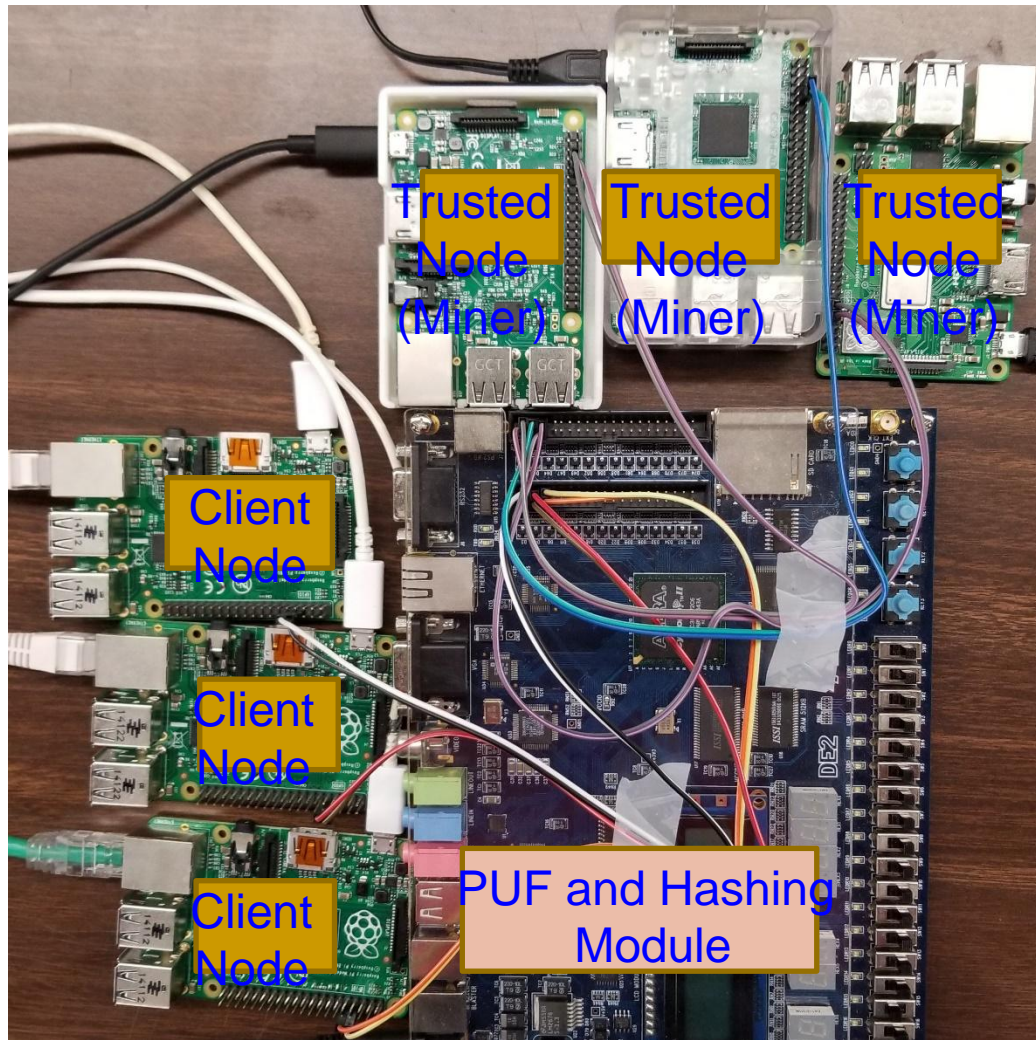


Eliminates cryptographic “puzzle” solving to validate blocks.



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

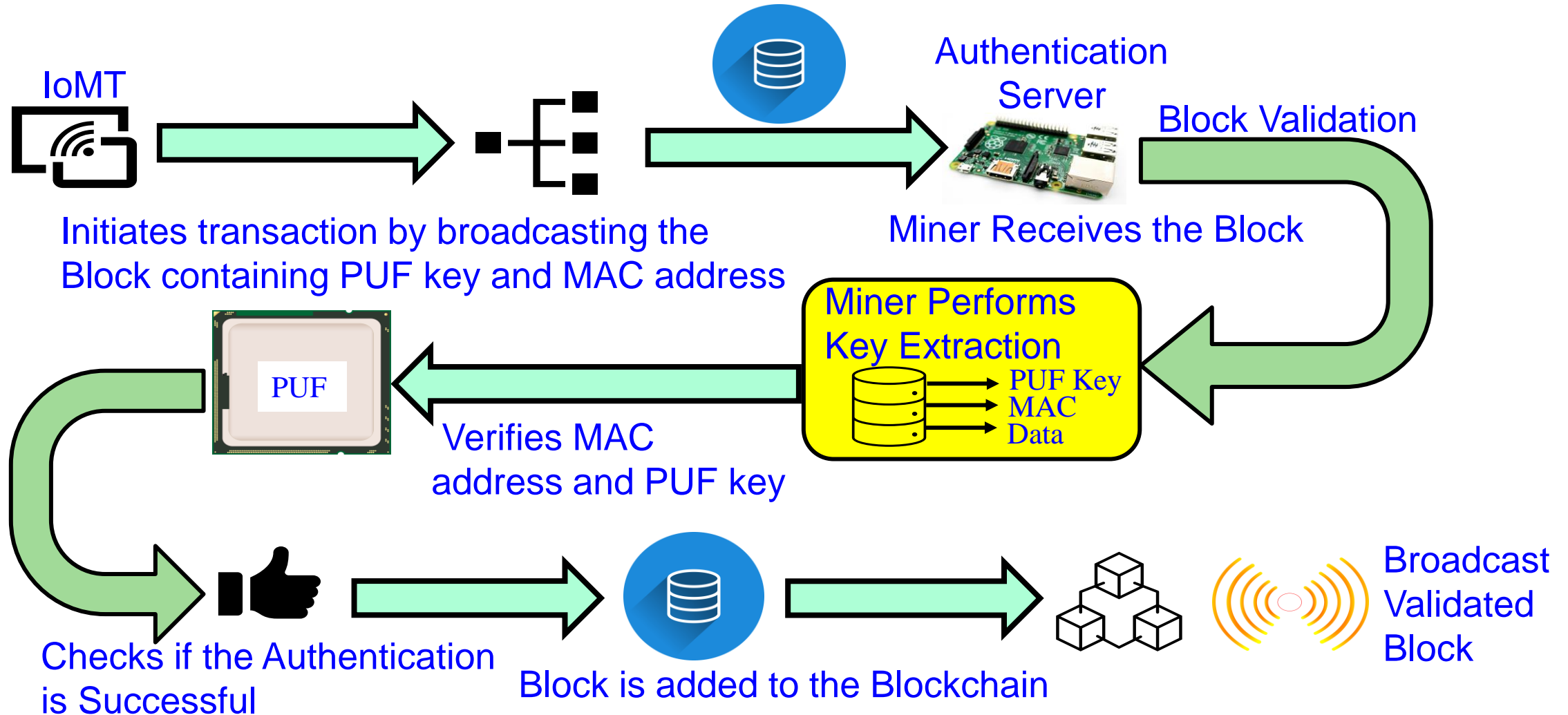


PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

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

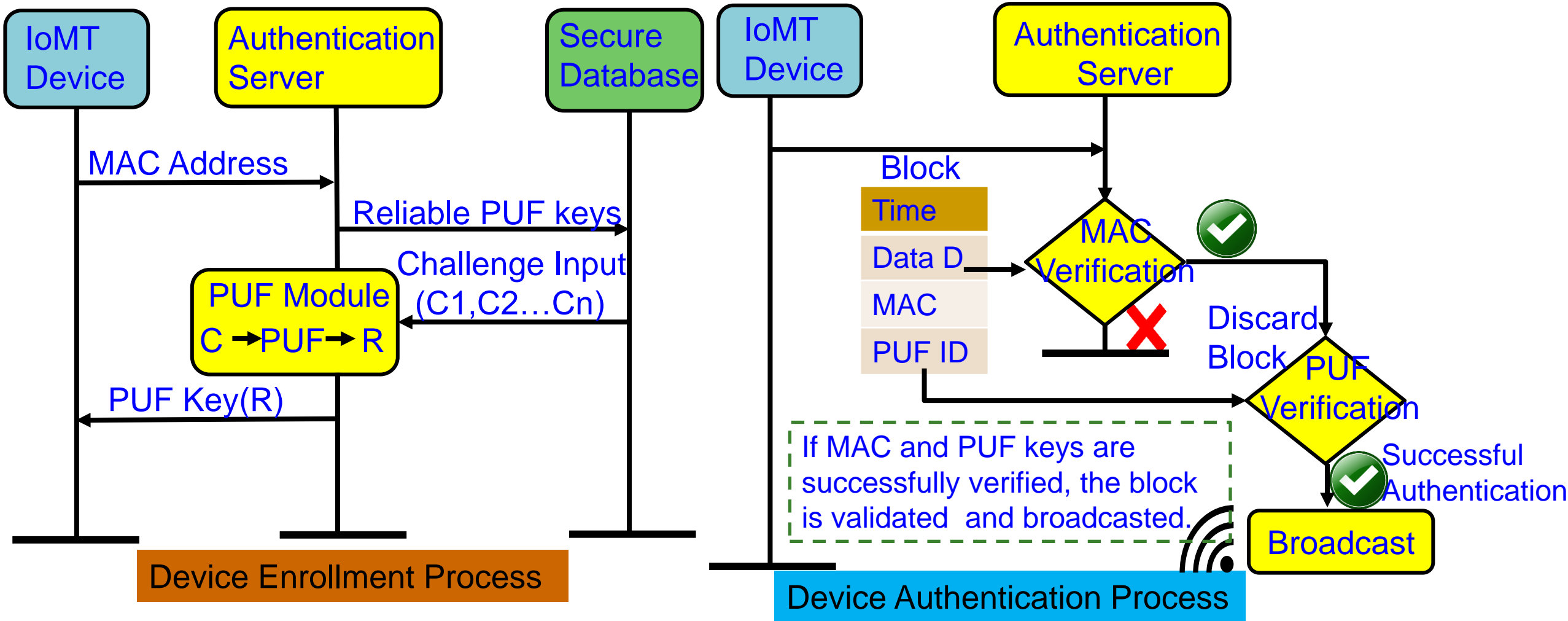
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



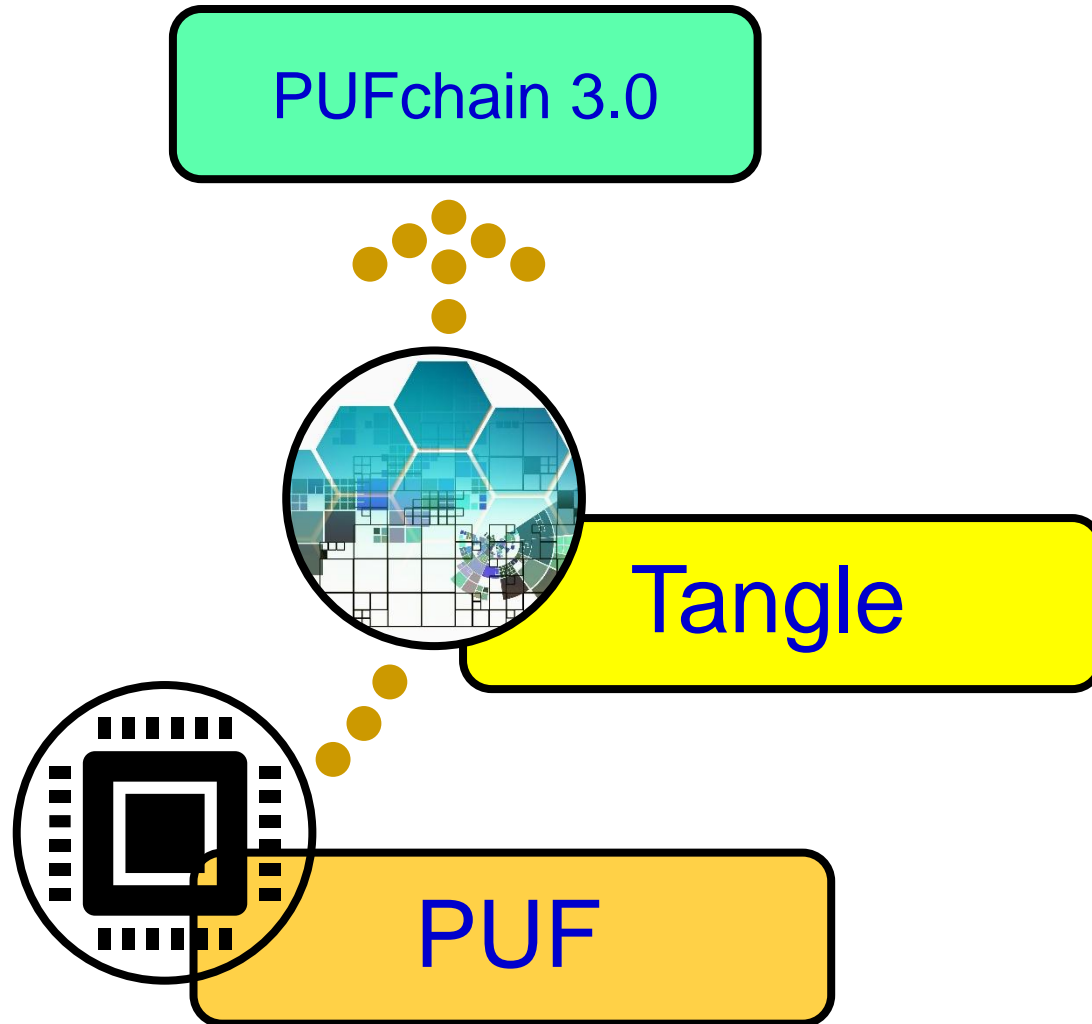
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

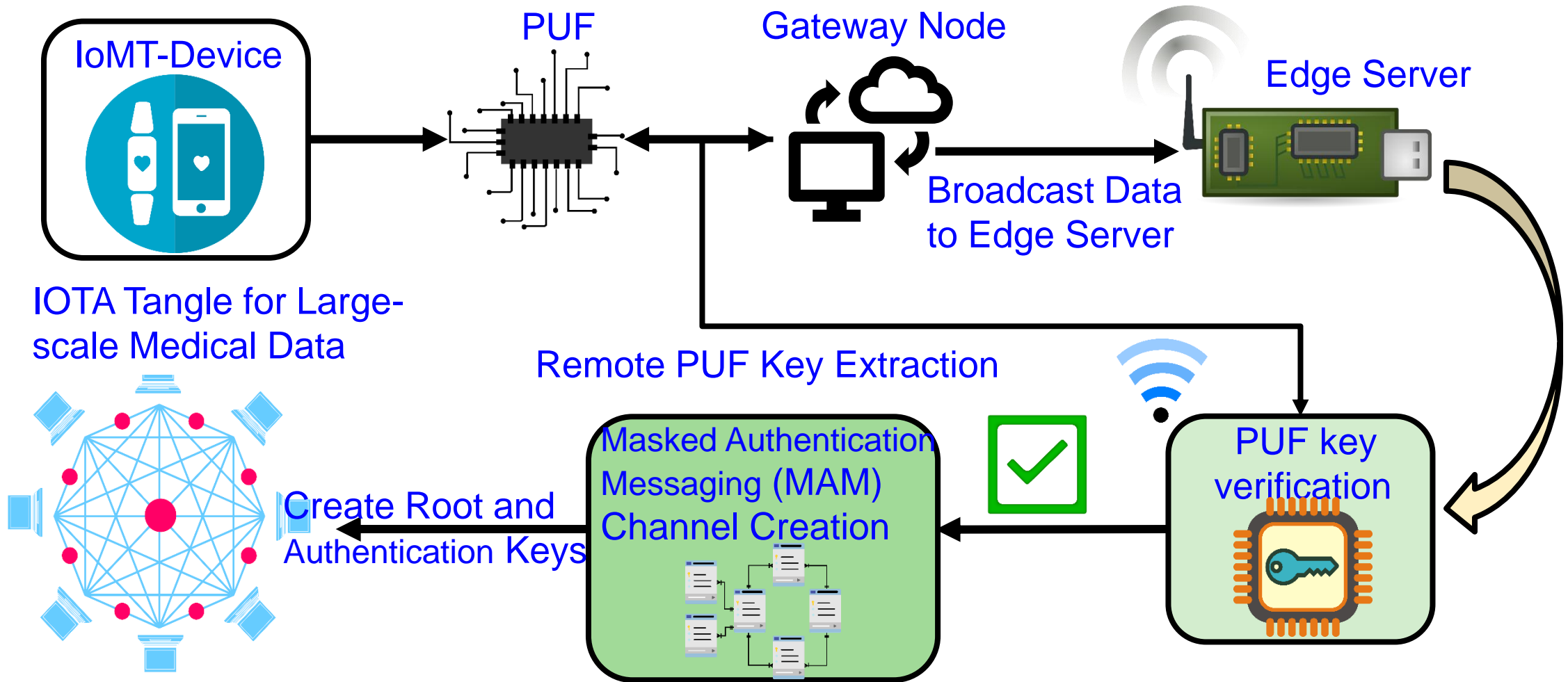
PUFchain 3.0 - Conceptual Idea



- 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](https://doi.org/10.1007/978-3-031-18872-5_2)”, 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

Counterfeits in Healthcare



The original product:

- sold in a white box with blue borders
- contains sixty (60) 500mg tablets
- divided on four (4) silver blister packs, each containing fifteen (15) tablets

The fake product:

- sold in a white box with no border
- contains sixty (60) 500mg tablets
- divided on six (6) silver with blue blister packs, each containing ten (10) tablets

Source: GA-FDD (Government Analyst – Food and Drug Department) issues warning over “fake” drug on local market,
<https://www.inewsguyana.com/ga-fdd-issues-warning-over-fake-drug-on-local-market/>

Daflon 500 is used to treat gravitational (stasis) dermatitis and dermatofibrosclerosis

Counterfeits in Healthcare



- Drug Components: Active Pharmaceutical Ingredient (API) + Excipients or inactive ingredients
- Counterfeit Drugs: Less API or no API or wrong API drugs produced in sub-standard conditions

Source: GA-FDD's (Government Analyst –Food and Drug Department's) occasional fake drugs disclosures may be tip of the iceberg, <https://www.stabroeknews.com/2019/09/06/business/ga-fdds-occasional-fake-drugs-disclosures-may-be-tip-of-the-iceberg/>

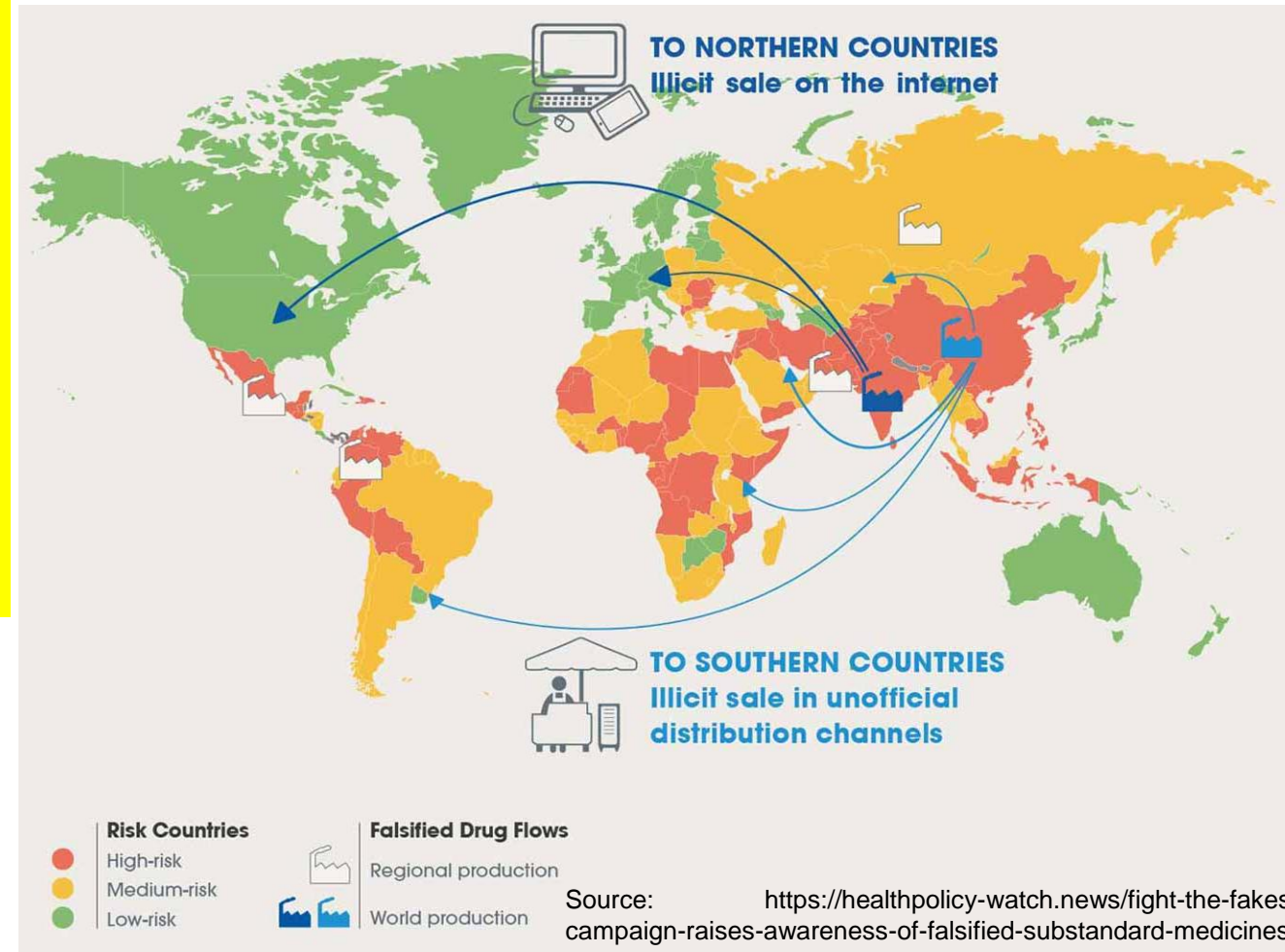
Fake Medicine - Serious Global Issue

- 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/>



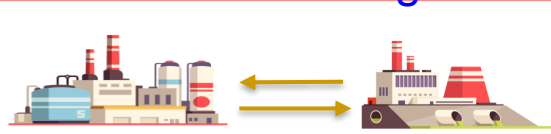
Source: <https://allaboutpharmacovigilance.org/be-aware-of-counterfeit-medicine/>



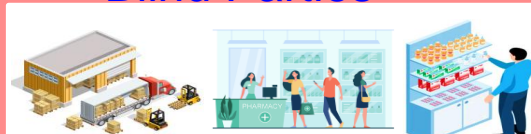
PharmaChain - Counterfeit Free Pharmaceutical

Enterprise Resource Planning

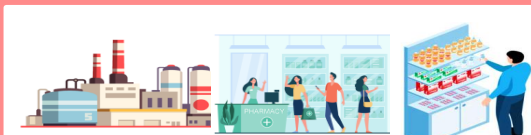
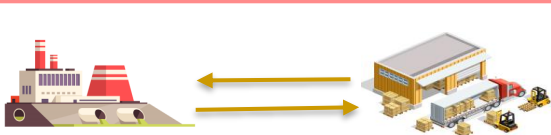
Transaction Ledger



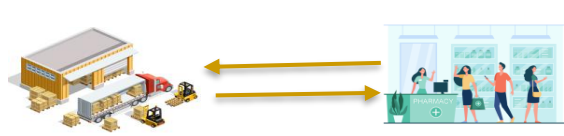
Blind Parties



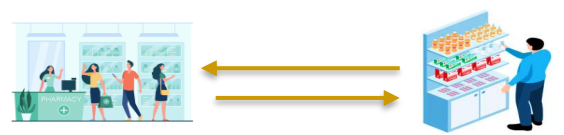
Manufacturer places order and ingredients are supplied



Wholesaler places order from Manufacturer



Transfer of drugs from wholesaler to pharmacy



Prescribed medicines are dispensed to the consumer

Blockchain System

Blockchain Ledger



Transparent Ledger

Ingredients

Manufacturer

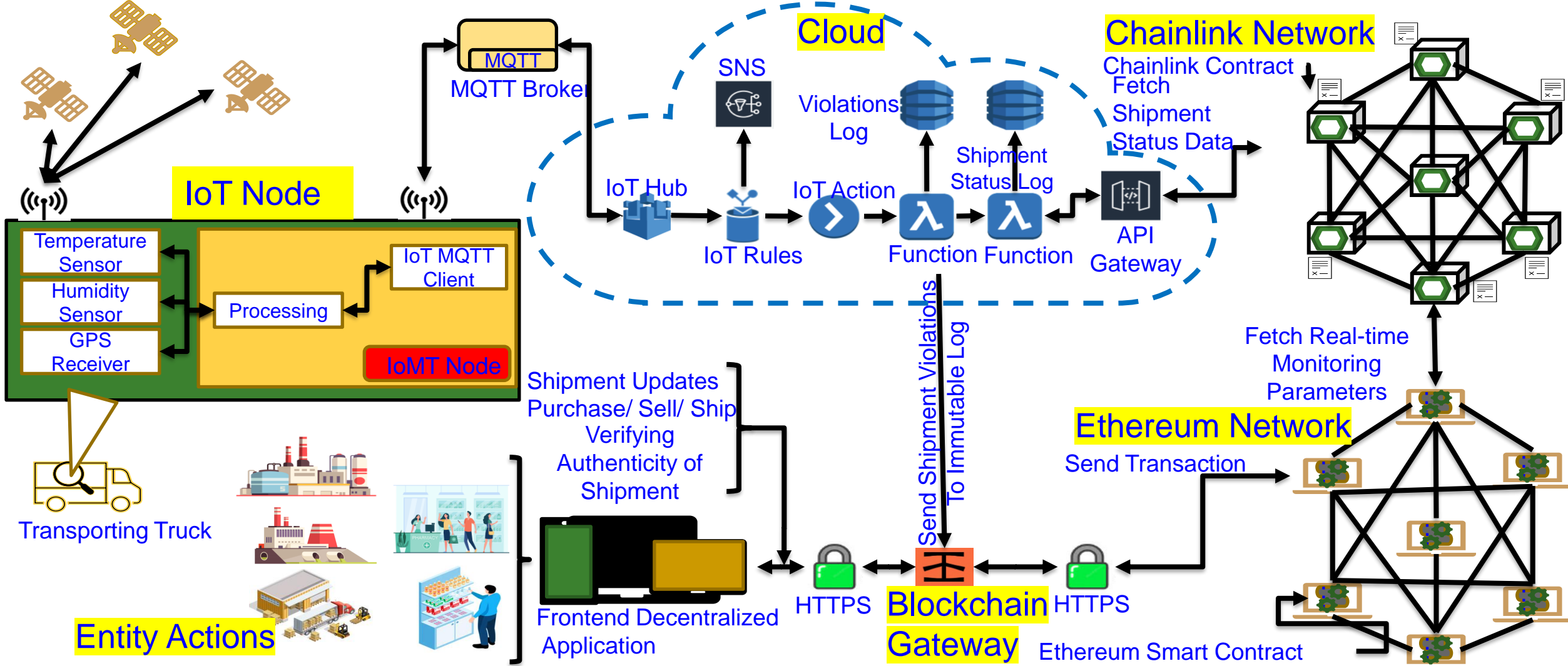
Wholesaler

Consumer

Pharmacy

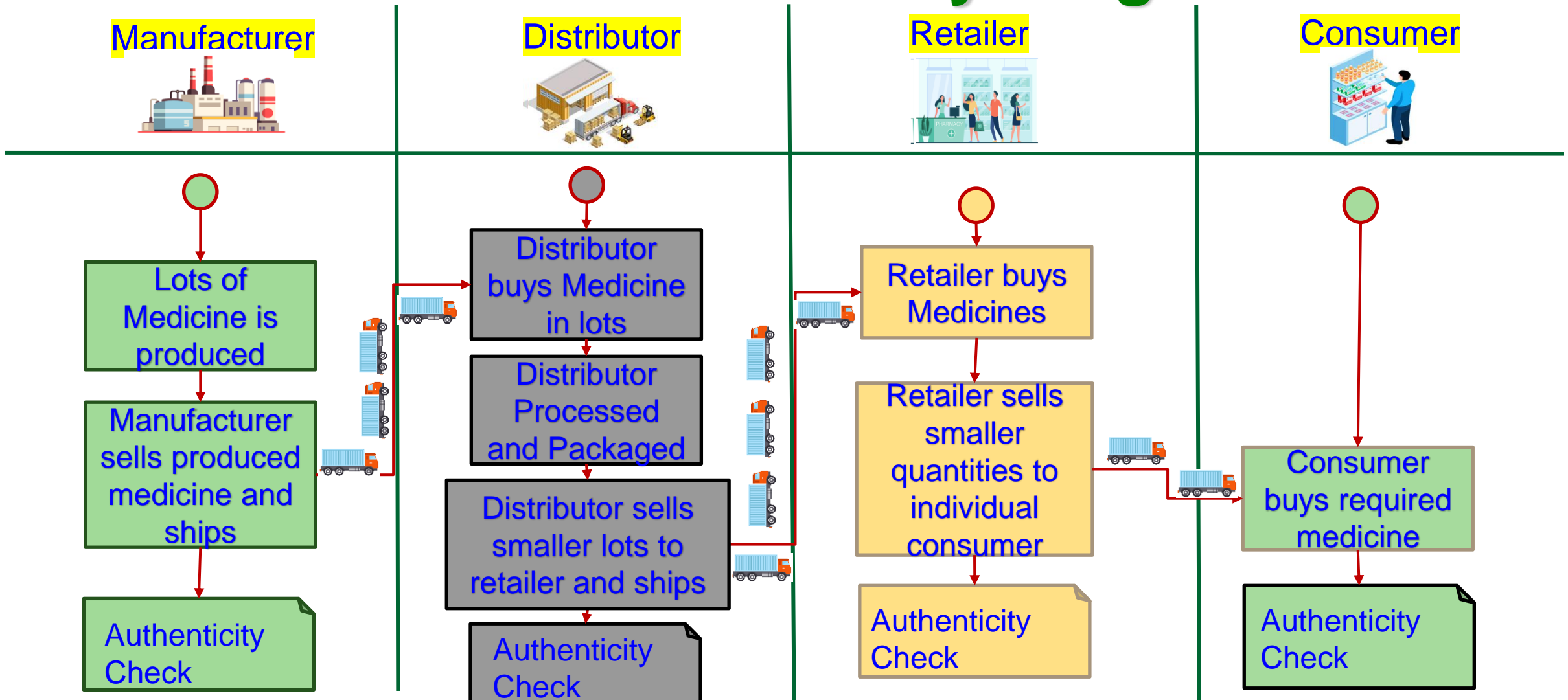
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: <https://doi.org/10.1049/ntw2.12041>. (Dataset for Research: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

Our PharmaChain: Architectural Overview



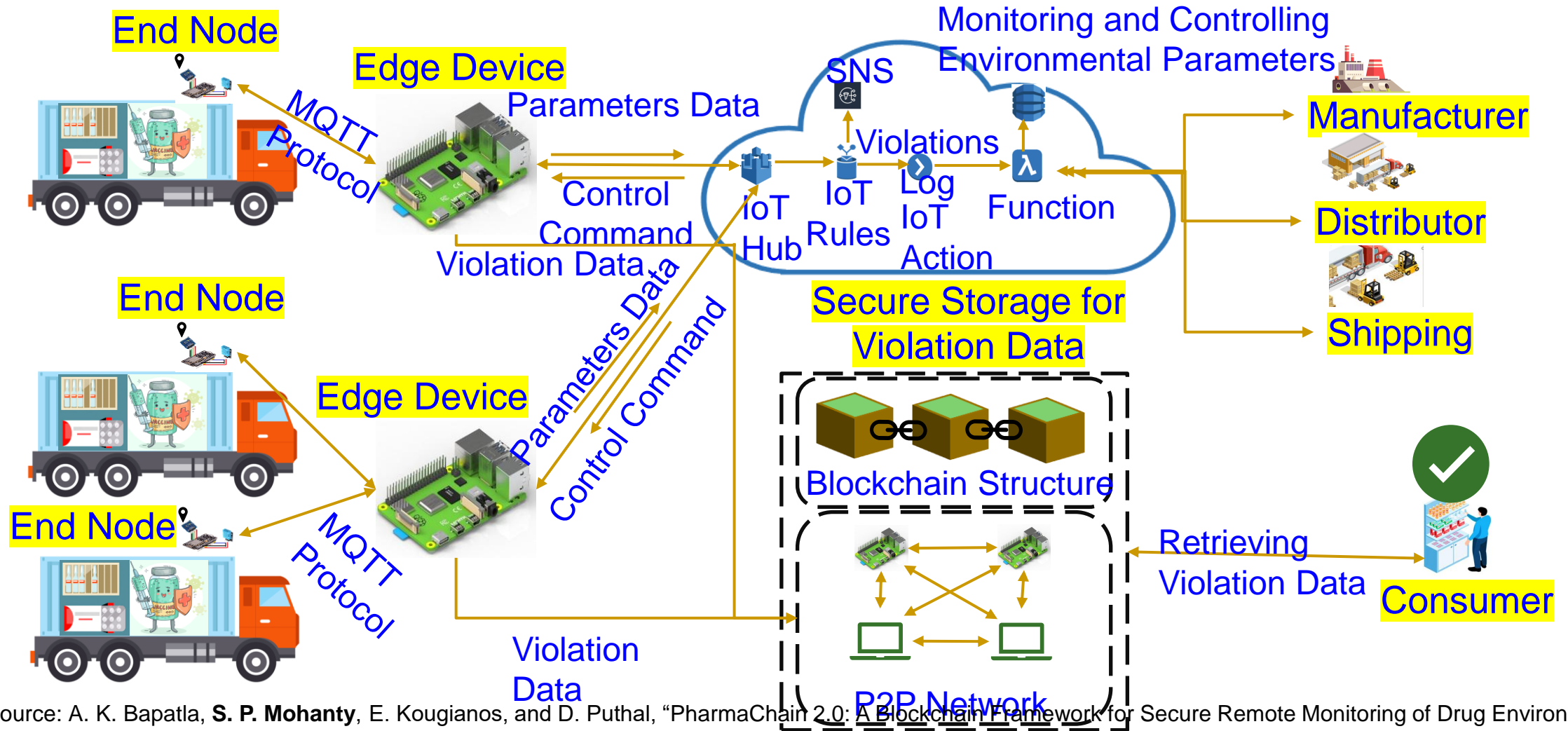
Source: A. K. Bapatla, S. P. Mohanty, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. 12, No. 2, March 2023, pp. 53--76, DOI: <https://doi.org/10.1049/ntw2.12041>. (Dataset for Research: [GitHub](#))

PharmaChain Entity Diagram



Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougioukos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. 12, No. 2, March 2023, pp. 53--76, DOI: <https://doi.org/10.1049/ntw2.12041>. (Dataset for Research: [GitHub](#))

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. 185--190, DOI: <https://doi.org/10.1109/iSES54909.2022.00046>.

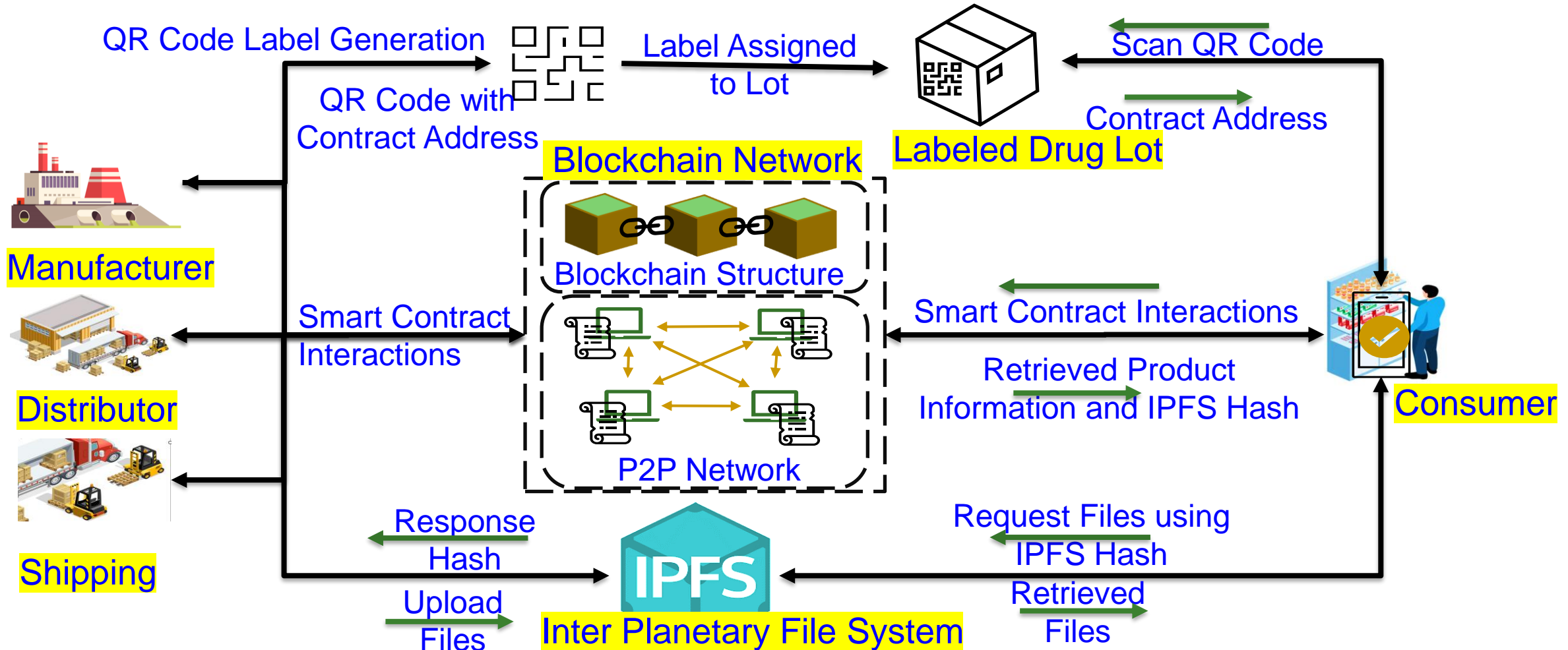
PharmaChain 2.0 - Comparative Analysis

Comparison of Proposed PharmaChain 2.0 solution with Existing Solutions

Features	Blockchain	Consensus Protocol	Openness	IoT Friendly Consensus	Average Time
CryptoCargo [15]	Ethereum	Proof-of-Work (PoW)	Public	No	43.36 sec
PharmaChain [9]	Ethereum	Proof-of-Authority (PoA)	Private	No	5.6 sec
Current Paper (PharmaChain 2.0)	PoAh Consensus Based Blockchain	Proof-of-Authentication (PoAh)	Private	Yes	322.28ms

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 3.0 - Architectural Overview



Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "PharmaChain 3.0: Efficient Tracking and Tracing of Drugs in Pharmaceutical Supply Chain using Blockchain Integrated Product Serialization Mechanism", *Springer Nature Computer Science (SN-CS)*, Vol. 5, No. 1, Jan 2024, Article: 149, 22-pages, DOI: <https://doi.org/10.1007/s42979-023-02510-9>.

PharmaChain 3.0 – The Key Idea

0x1EcbFd5Edb3747927033
Aa893416e4aD01DF0c6E

Lot Contract Address



QR Code Generated for Lot Labelling

New Lot Contract Address Converted to QR Code for Labeling

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 3.0 - Comparative Analysis

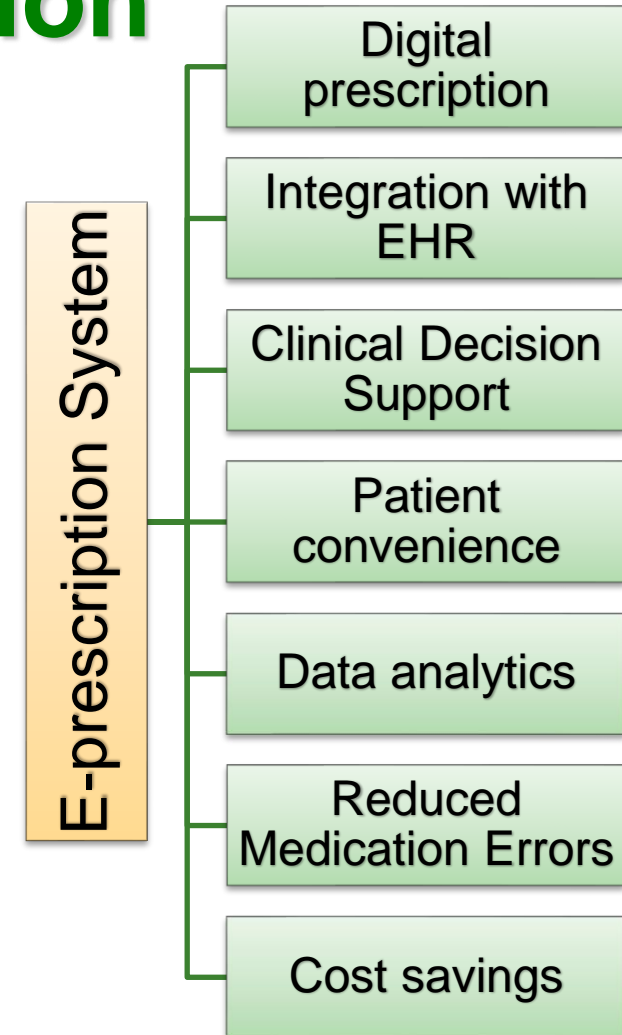
Works	Blockchain	Consensus Mechanism	Computational Needs	Openness	QR Code Integrated	Storage	Handling Large data
Crypto Cargo [11]	Ethereum	Proof-of-Work (PoW)	High	Public	No	On-Chain and Cloud	No
Kumar et.al. [9]	NA	NA	NA	NA	Yes	On-chain	No
PharmaChain [12]	Ethereum	Proof-of-Authority (PoA)	Low	Private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

Smart Healthcare – Trustworthy Medical Prescription

Electronic Prescription

- Revolutionized the way medications are prescribed, processed, and dispensed
- Digital version of prescriptions increase legibility and reduces medication errors
- Clinical Decision Support Tools – Warn potential drug interactions, suggest alternate medication, offer dosage recommendations

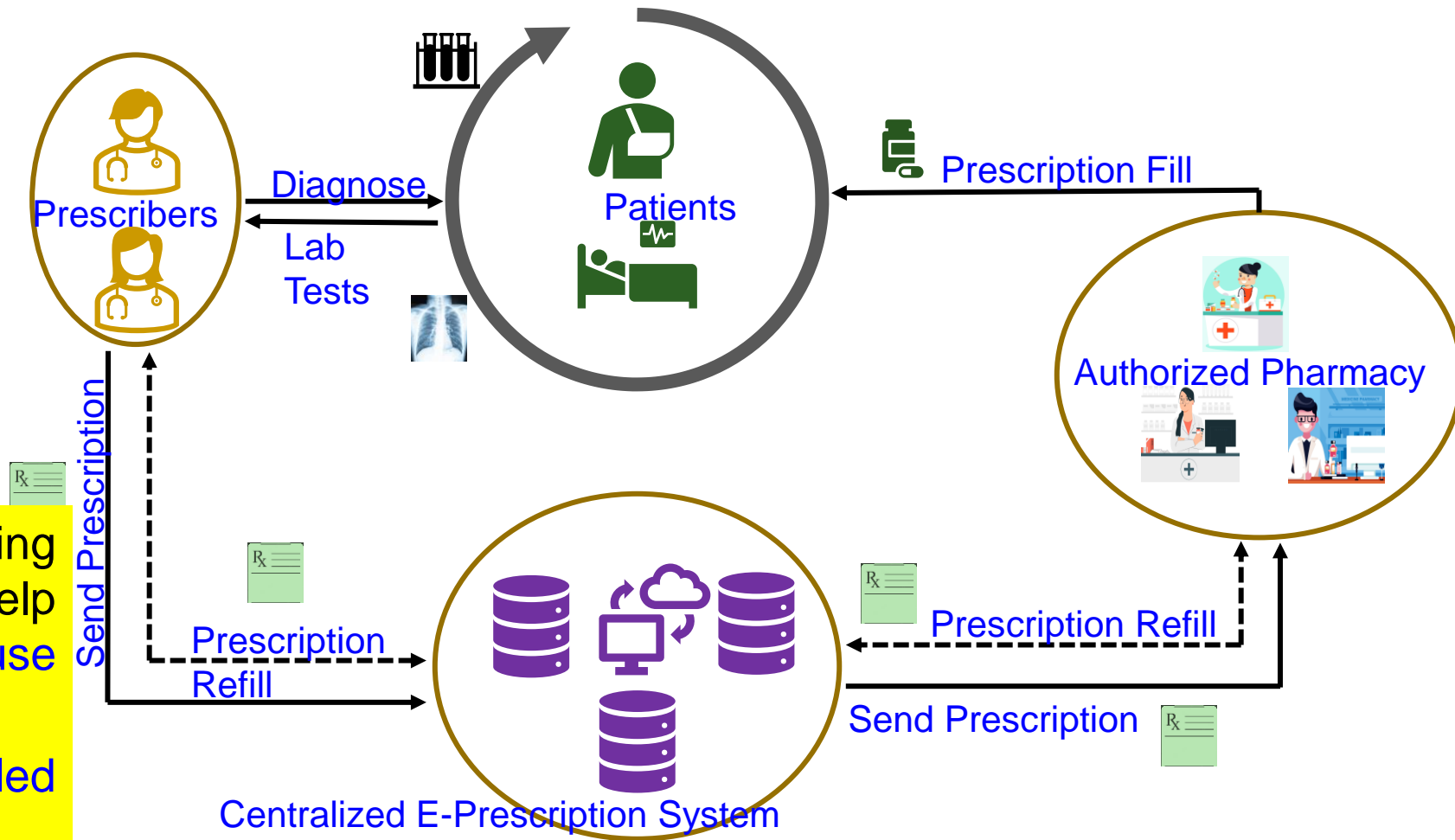
- More than 100,000 reports of medication errors (FDA)
- 40% of Americans report being involved in medical errors (Institute for Healthcare Improvement/NORC at the University of Chicago)
- 1 in 5 doses of medication provided during patient visits is administered incorrectly



Source: A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing", in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2023, pp. 283--301, DOI: https://doi.org/10.1007/978-3-031-45882-8_19.

E-Prescription System and Issues

- Single Point of Failure (SPOF)
 - Data Security
 - Privacy Concerns
 - Interoperability Concerns (PDMP)
 - System availability Issues
- Prescription Drug Monitoring Programs (PDMP) help mitigate prescription misuse and diversion
 - Oversight of controlled substance prescriptions



Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing", in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2023, pp. 283--301, DOI: https://doi.org/10.1007/978-3-031-45882-8_19.

E-Prescription is the Need of the Hour

Prescription Drug Type	Annual Abusers	% Among Rx Abusers	% Among Americans
Painkillers	9.7 million	59.5%	3.43%
Opioids Alone	9.3 million	57.1%	3.29%
Sedatives	5.9 million	36.2%	2.08%
Stimulants	4.9 million	30.1%	1.73%
Benzodiazepine Alone	4.8 million	29.4%	1.70%
All Prescription Drugs	16.3 million	100%	5.76%

Reduced Fraud and Abuse

Blockchain Immutability
Combats prescription fraud and abuse

Enhanced Security and Privacy:

Provides security and integrity of the medical data

Efficiency and Accuracy

Accuracy can be improved to reduce medication errors

Interoperability

Seamless data exchange between healthcare providers

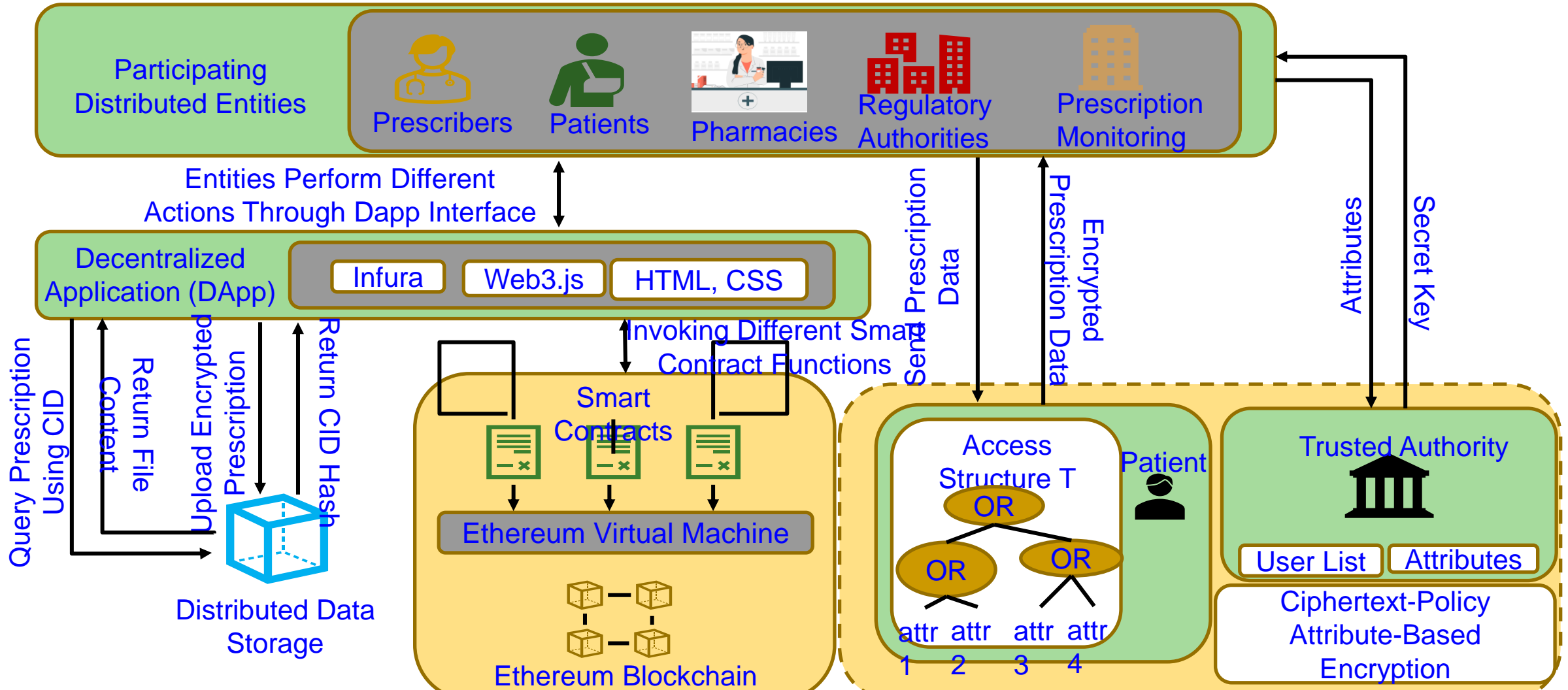
Addressing Opioid Crisis

Prevents misuse and abuse of opioids

- 16M – 6% of Americans over the age of 12 abuse prescriptions in a year.
- 2M – 12% of prescription drug abusers are addicted.

Statistics Source: <https://drugabusestatistics.org/prescription-drug-abuse-statistics/>

Our FortiRx: Architecture Overview



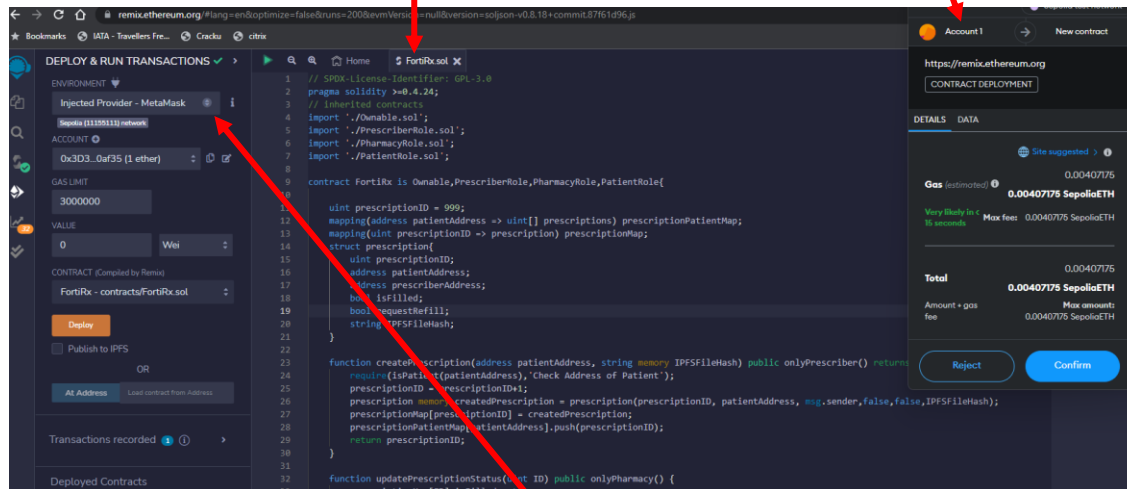
Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing", in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2023, pp. 283--301, DOI: https://doi.org/10.1007/978-3-031-45882-8_19.

FortiRx: Smart Contract Deployment

Deployment in Sepolia

Smart Contract

Wallet Transaction



Ethereum Addresses with Roles

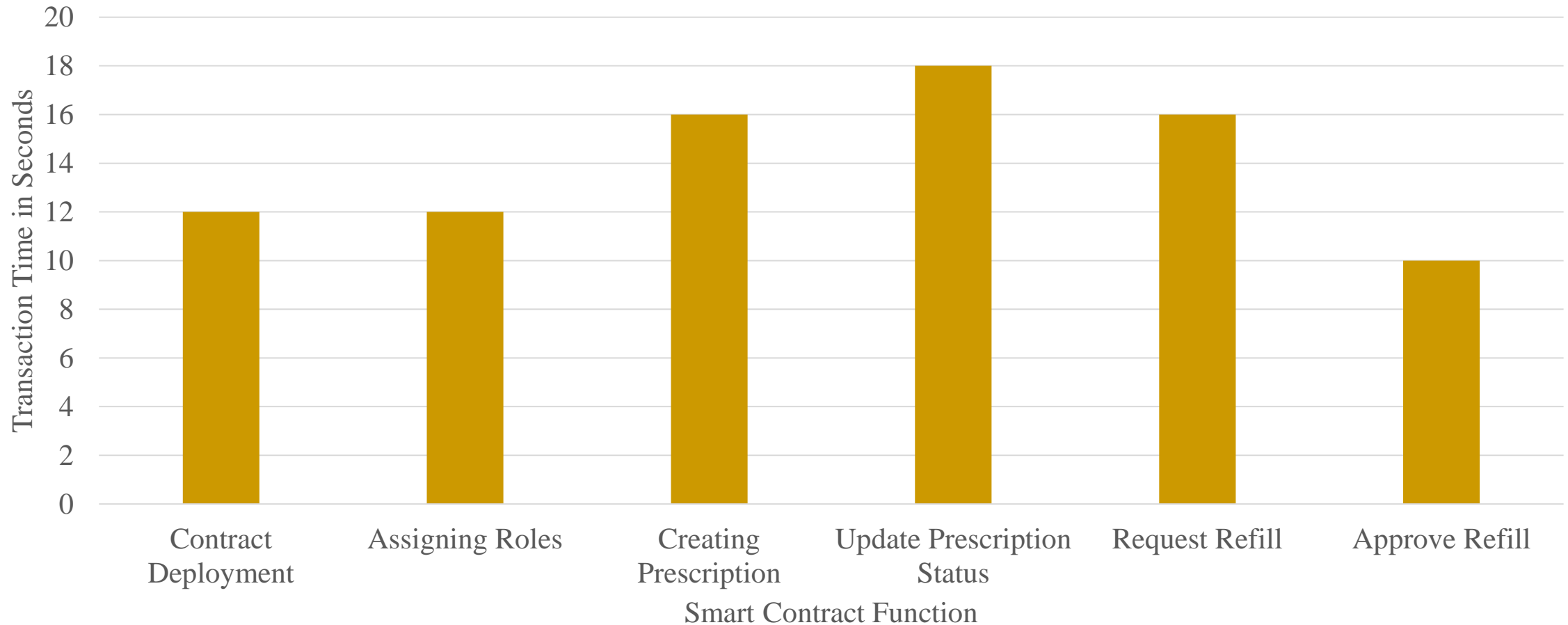
Feature	Value
Physician Account Address	0x3d352313f4f5561d0ffbfa205b52a3c3b70af35
Pharmacy Account Address	0x3D352313F4f5561D0ffbfa205B52A3c3b70af35
Patient Account Address	0x2a9884dfa7E6890FE8AA99FE2486c613C32b697a
Contract Deployment Hash	0x798d1f5ff49f9df09b9856db2646cebc2029d5cd2a45c5ef0c1b9acb9f217c6f
Prescription Content ID	Qme7Sq8gLmE875kE79QyWWFy9wqQ4yHnTEHMur511PrZff
Prescription Creation Hash	0xda5bd0ce943325696e91bfe140bd8cdd60eafda6f2a41b07221e499bfe7f1f7

Remix Environment Network Configuration

Source: A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing", in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2023, pp. 283--301, DOI: https://doi.org/10.1007/978-3-031-45882-8_19.

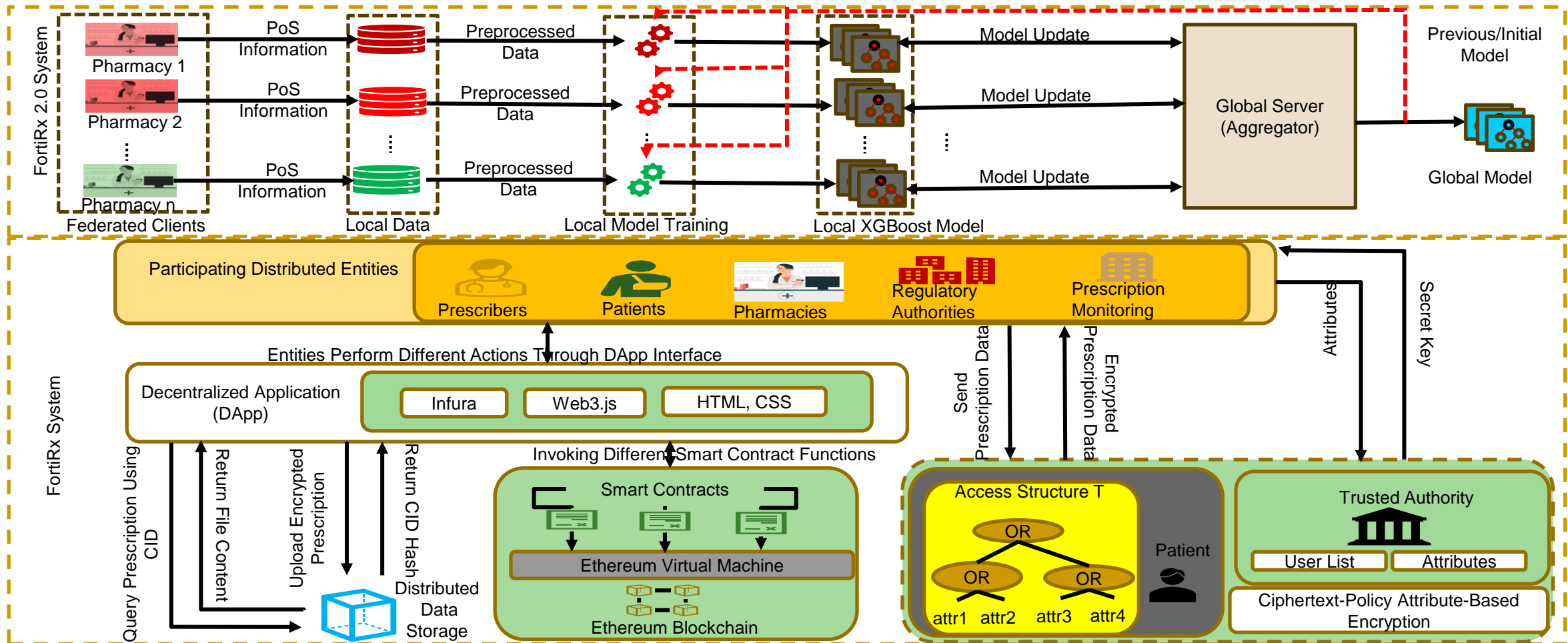
FortiRx: Transaction Confirmation Times

Smart Contract Function vs Average Transaction Time (Sec)



Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing", in *Proceedings of the IFIP International Internet of Things Conference (IFIP-IoT)*, 2023, pp. 283--301, DOI: https://doi.org/10.1007/978-3-031-45882-8_19.

Our FortiRx 2.0: Architecture



Source: A. K. Bapatla, **S. P. Mohanty**, and E. Kougianos, "FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2023, pp. 438--443, DOI: <https://doi.org/10.1109/OCIT59427.2023.10430944>.

FortiRx – A Comparative Perspective

Works	Blockchain Platform	Prescription Privacy	Data Management	Drug Demand Forecasting
Ionescu et al, SmartBlock4Health, 2022	Ethereum	Asymmetric Encryption	On-chain	✗
VigilRx, 2022	Ethereum	Role-Based Access Control	On-Chain	✗
FortiRx, 2023	Ethereum	Role-Based Access Control and CP-ABE	On-chain and off-chain	✗
FortiRx 2.0	Ethereum	Role-Based Access Control and CP-ABE	On-chain and off-chain	✓

Source: A. K. Bapatla, **S. P. Mohanty**, and E. Koungianos, “[FortiRx 2.0: Smart Privacy-Preserved Demand Forecasting of Prescription Drugs in Healthcare-CPS](https://doi.org/10.1109/OCIT59427.2023.10430944)”, in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2023, pp. 438--443, DOI: <https://doi.org/10.1109/OCIT59427.2023.10430944>.

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

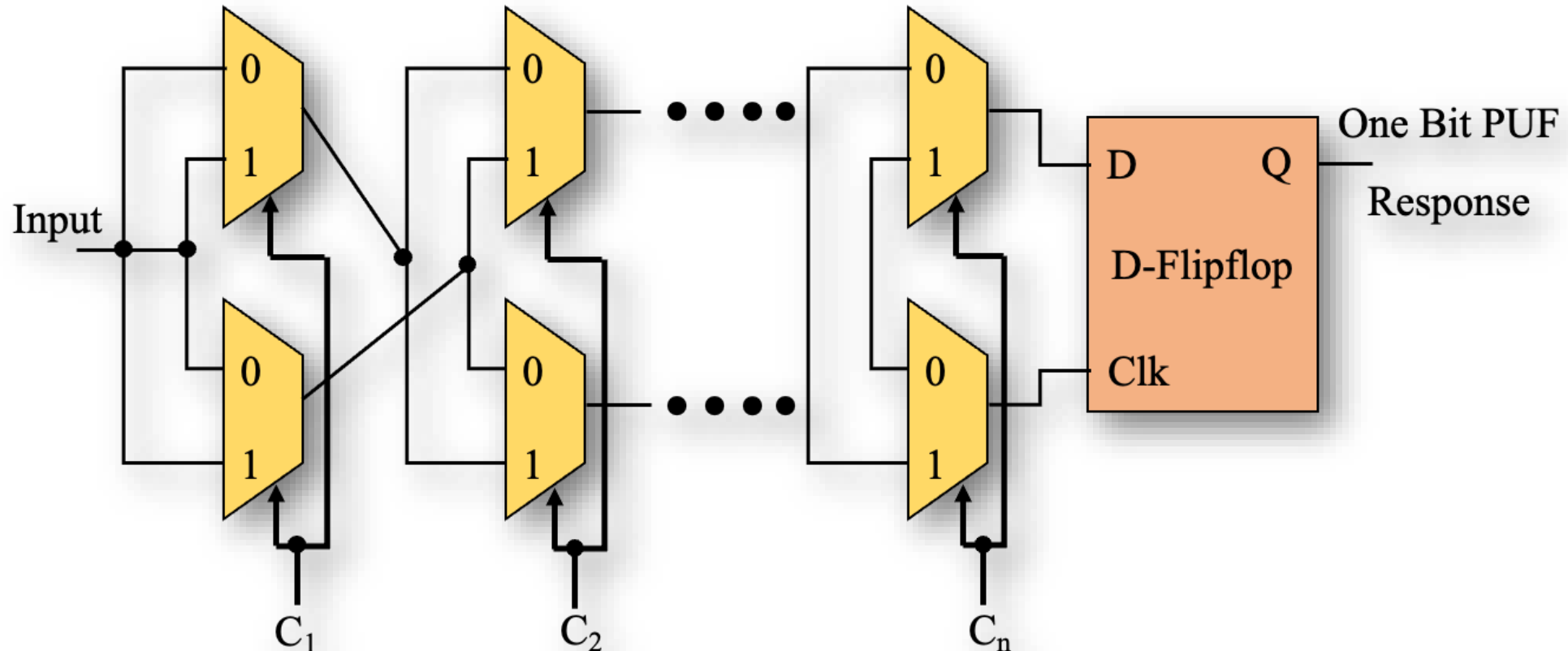
If PUF is So Great, Why Isn't Everyone Using It?

- 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>

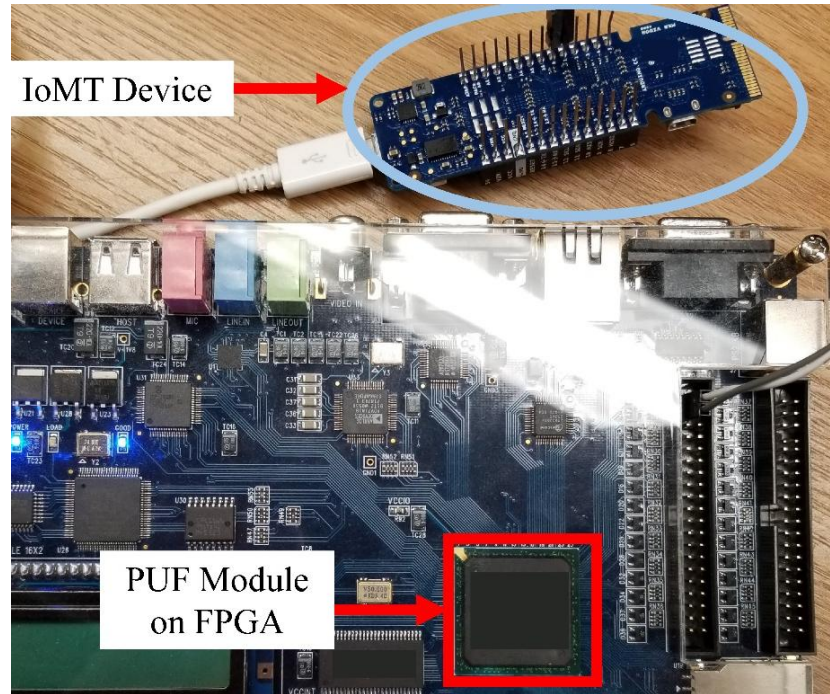
PUF Limitations – Larger Key Needs Large ICs

- Larger key requires larger chip circuit.



1 – Bit Arbiter PUF Architecture

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.

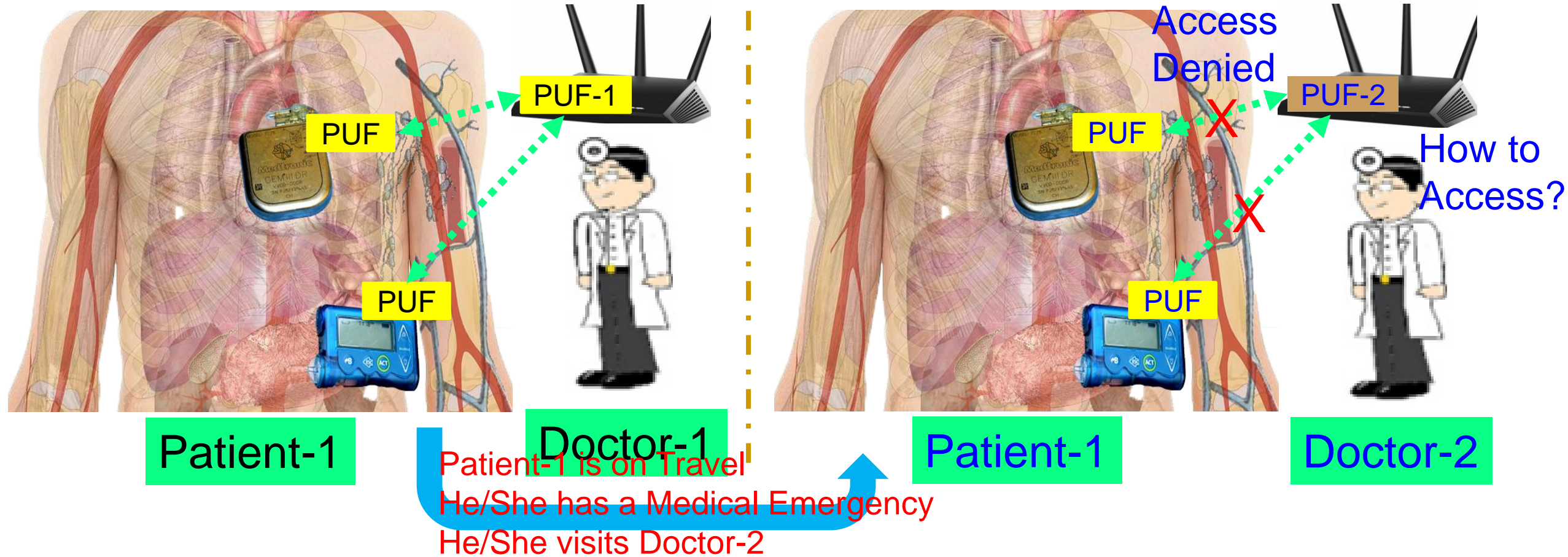
- Faster prototyping
- Lesser design effort
- Minimal skills
- Cheap
- Rely on already existing post fabrication variability



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

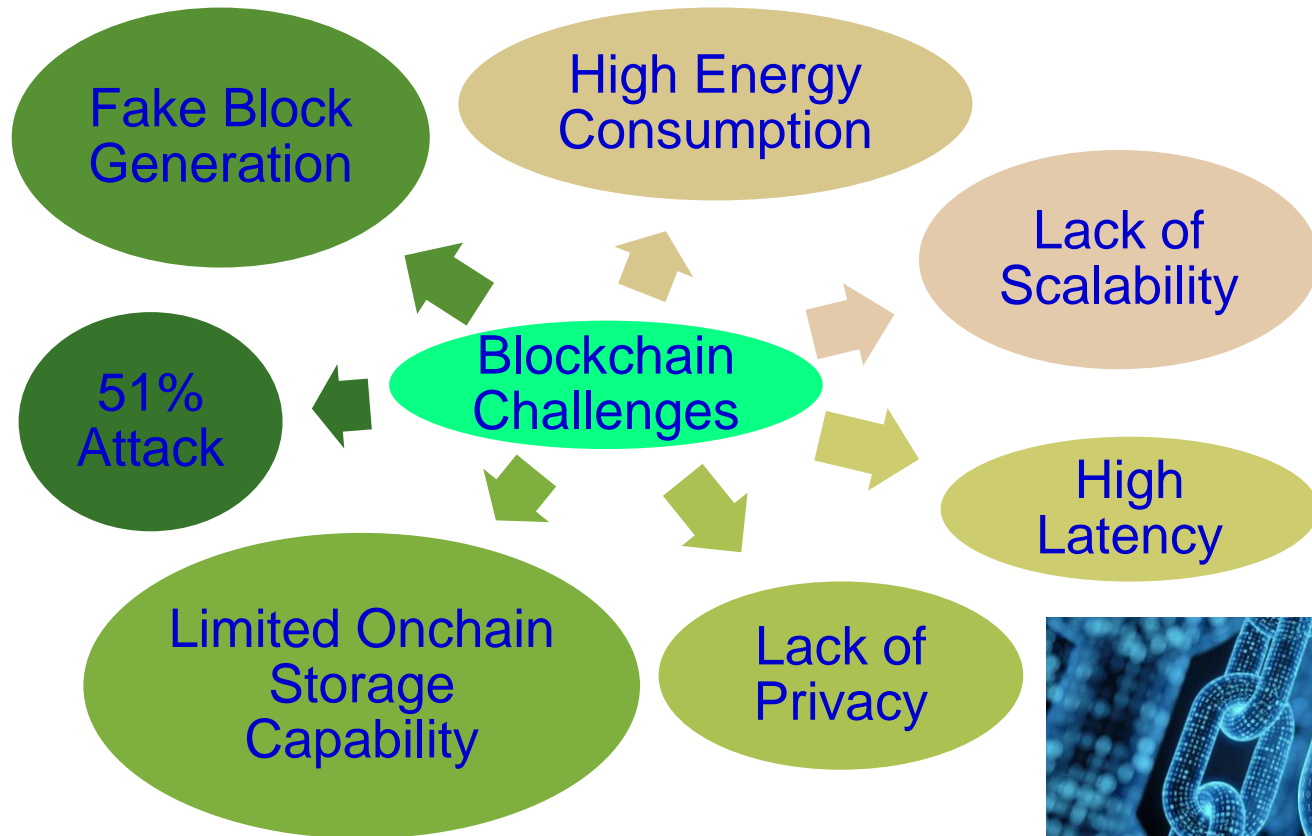
PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma



Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, "PMsec 2.0: A Security-By-Design Solution for Doctor's Dilemma Problem in Smart Healthcare", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2023, pp. 456--461, DOI: <https://doi.org/10.1109/OCIT59427.2023.10430808>.

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



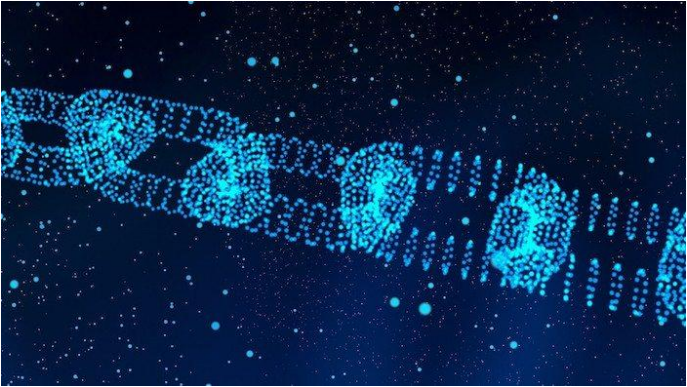
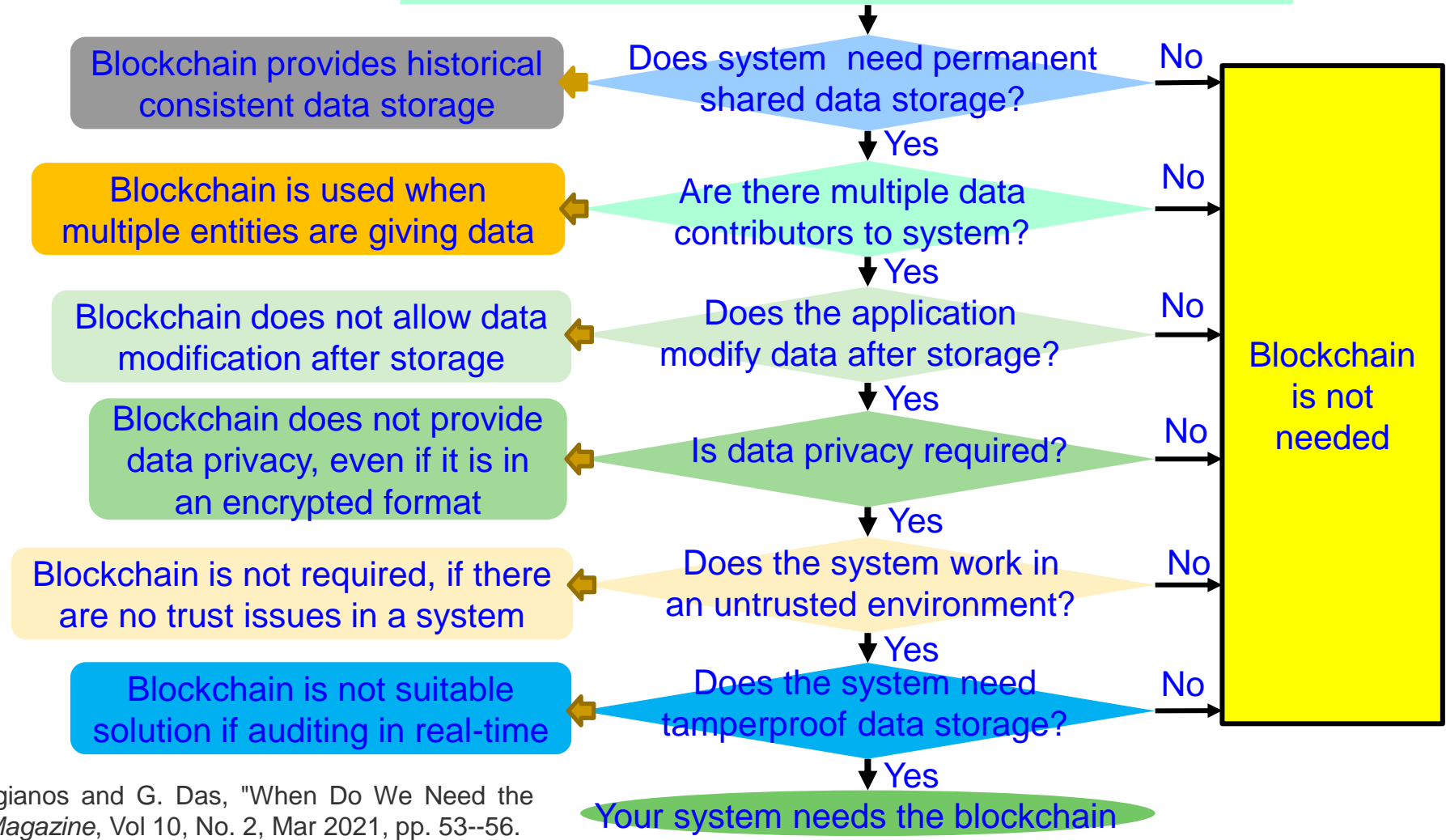
80,000 X

Energy consumption of a credit card processing



When do You Need the Blockchain?

Information of the System that may need a 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.

Conclusion and Future Research



Conclusion

- 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 has advantages but also has limitations in terms of cybersecurity; thus challenging to build sustainable healthcare.
- Cybersecurity in smart healthcare is a serious challenge as device as well as data security and privacy are important.
- Medical device security is a difficult problem due to resource and battery constraints; thus challenge for sustainable H-CPS.
- Security-by-Design is critical for IoMT/H-CPS.

Future Research

- TinyML for smart healthcare that can run at user-end (edge/sensor) needs research.
- H-CPS requires robust data, devices, along with cybersecurity and privacy assurance to be sustainable and hence needs 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.
- Trustworthy Pharmaceutical Supply Chain needs research.