Cybersecurity Perspectives of Smart Healthcare

Electronics and ICT Academy
MNIT Jaipur
25 Jul - 05 Aug 2022

Saraju P. Mohanty
University of North Texas, USA.
Email: saraju.mohanty@unt.edu
More Info: http://www.smohanty.org

Outline

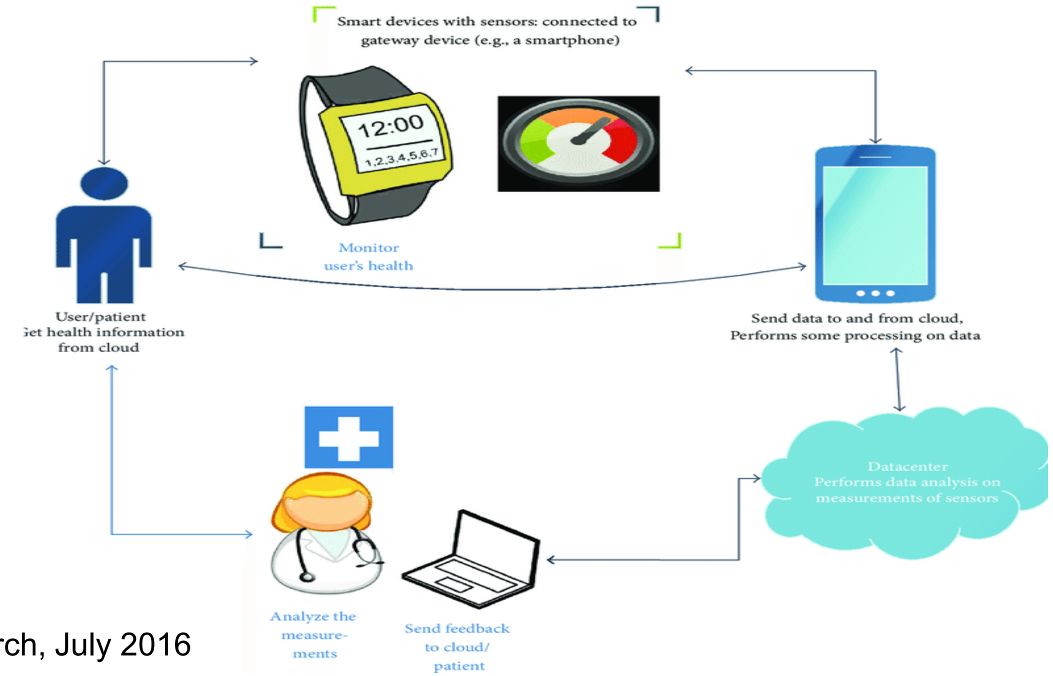
- Smart Healthcare – Introduction
- Smart Healthcare – Challenges
- Security and Privacy by Design in Smart Healthcare
- Blockchain in Smart Healthcare
- PUF based Cybersecurity in Smart Healthcare
- Conclusions and Future Directions

Smart Healthcare – Introduction

Smart Healthcare - IoMT

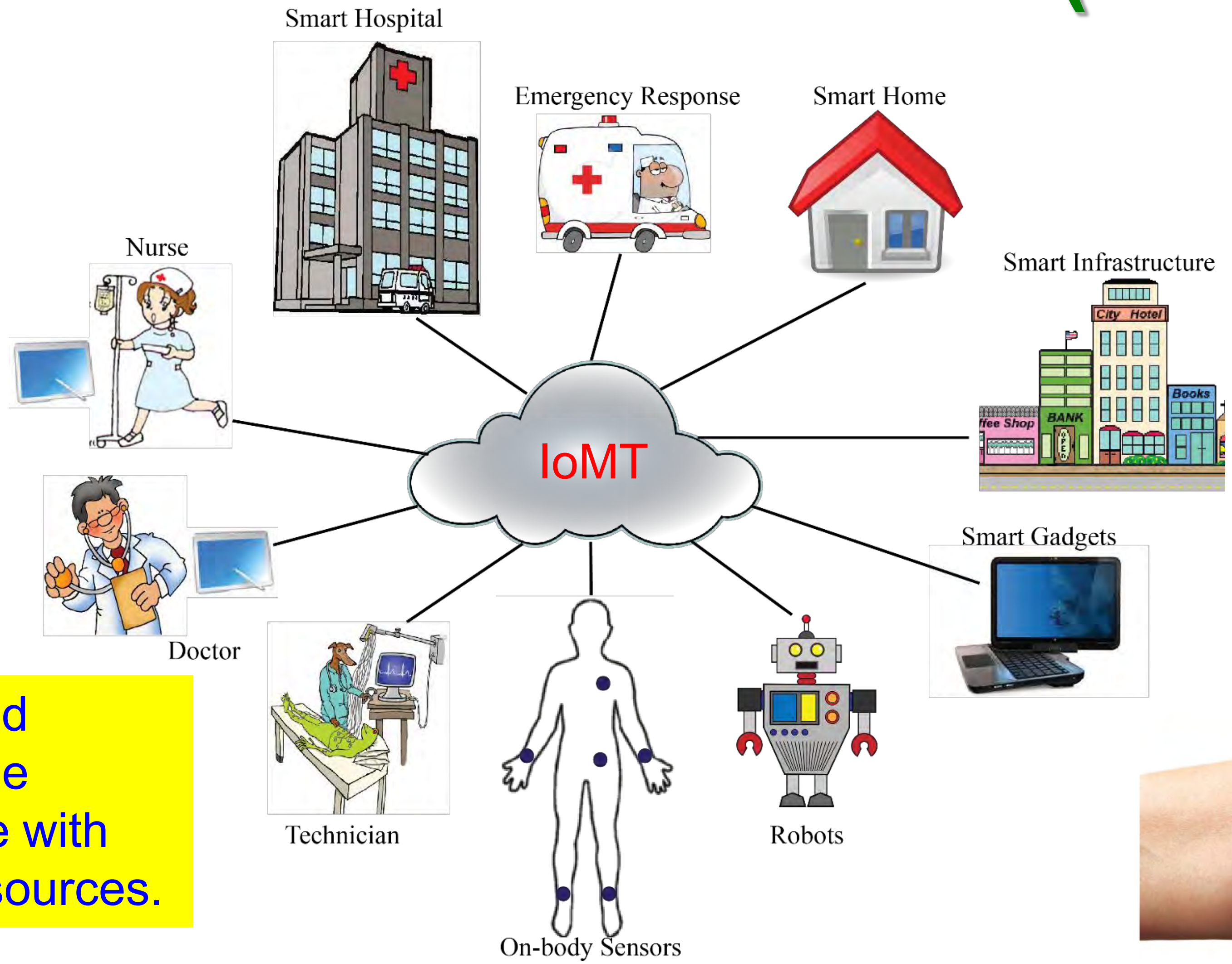
- The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks.
- Medical devices equipped with Wi-Fi allow the machine-to-machine communication that is the basis of IoMT.

Smart Healthcare is defined by the technology that leads to better diagnostic tools, better treatment for patients, and devices that improves the quality of life for anyone and everyone.



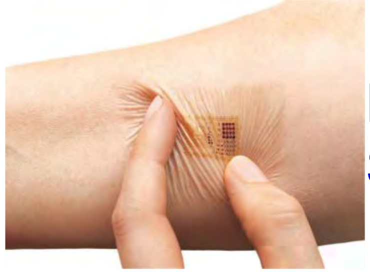
Dimitrov 2016, Healthcare Informatics Research, July 2016

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

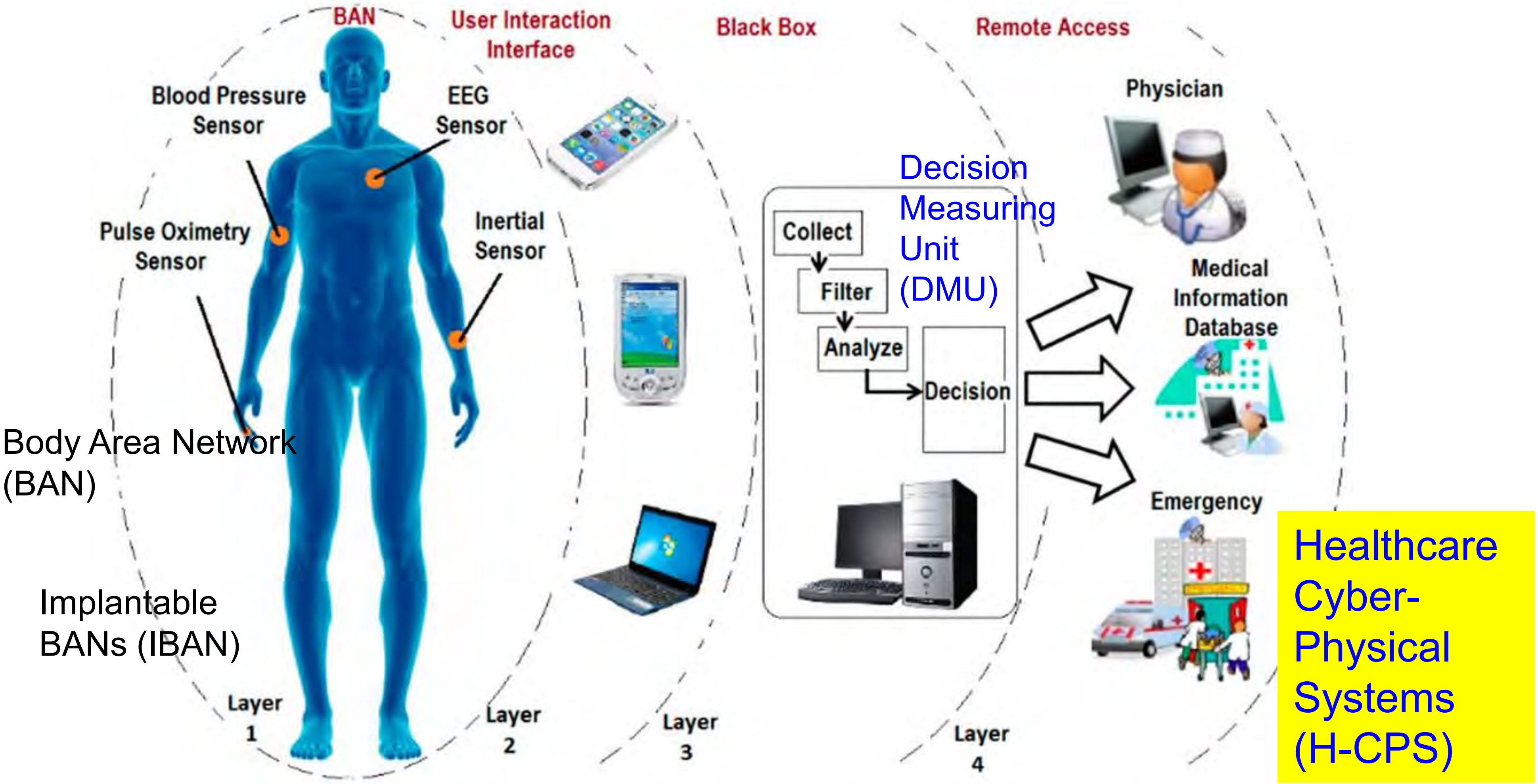
Internet of Medical Things (IoMT)

Internet of Health Things (IoHT)

Healthcare Cyber-Physical Systems (H-CPS)

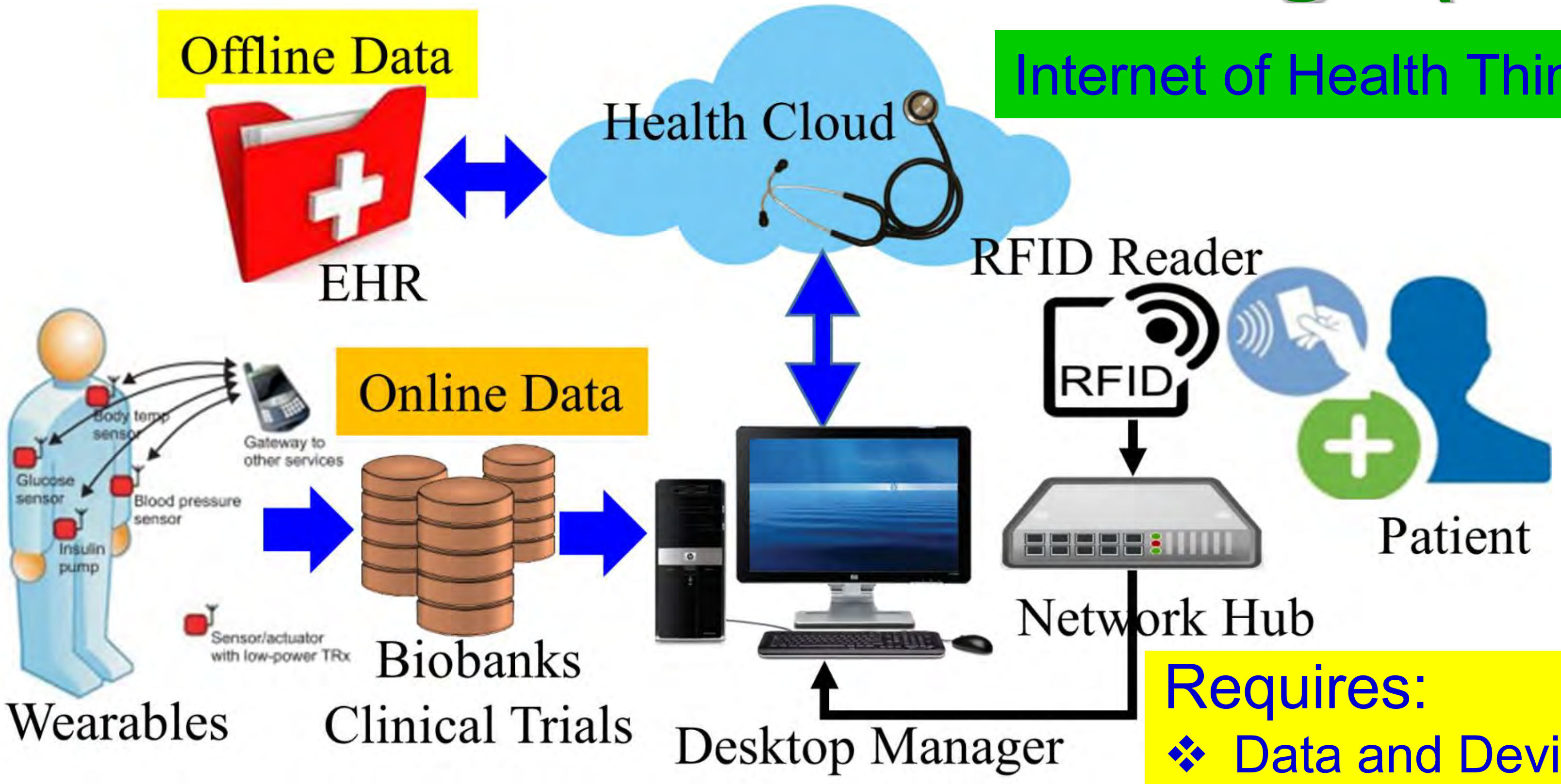
Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, *IEEE Consumer Electronics Magazine (MCE)*, Volume 7, Issue 1, January 2018, pp. 18-28.

Smart Healthcare - 4-Layer Architecture



Source: M. Ghamari, B. Janko, R.S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments", *Sensors*, 2016. 16(6): p. 831.

Internet of Medical Things (IoMT)



Internet of Health Things (IoHT)

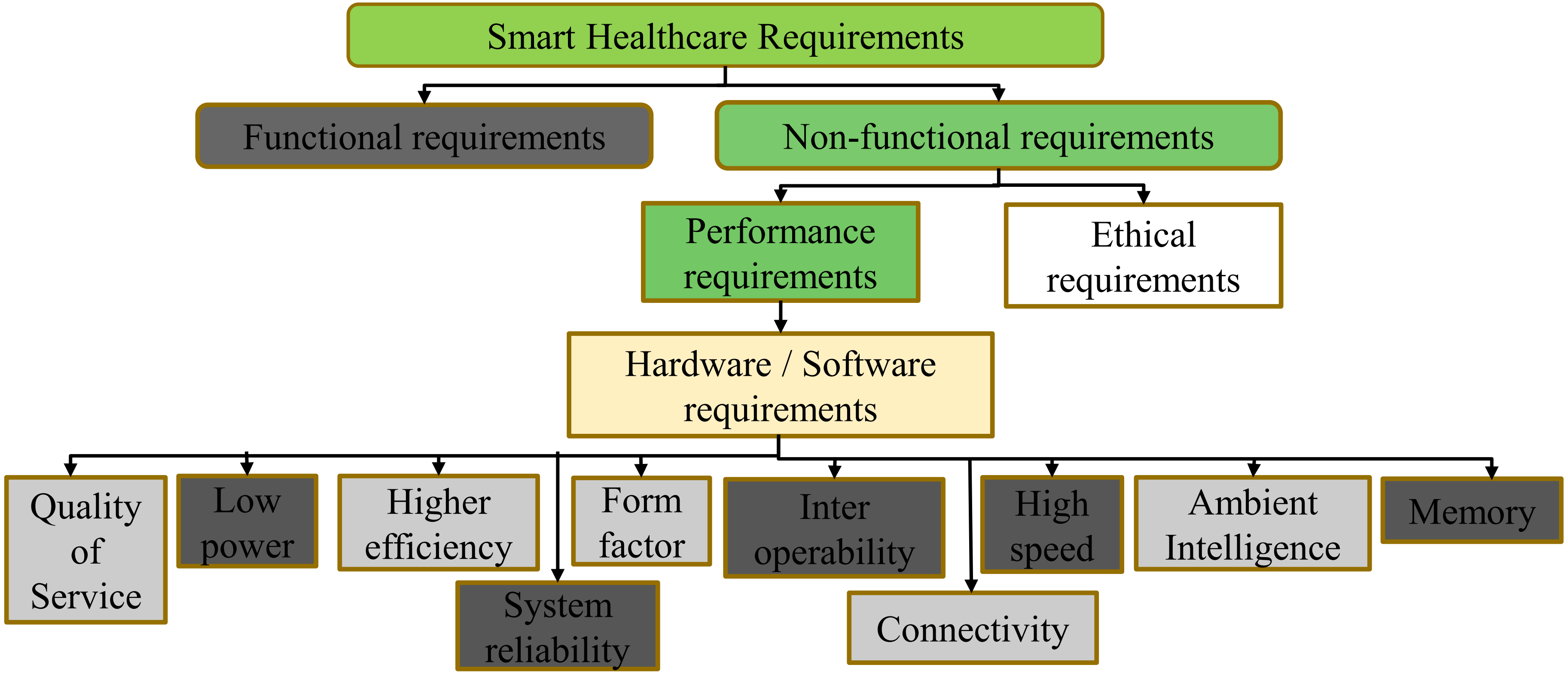
Requires:
- ❖ Data and Device Security
- ❖ Data Privacy

IoMT is a collection of medical sensors, devices, healthcare database, and applications that connected through Internet.

Source: http://www.icemiller.com/ice-on-fire-insights/publications/the-internet-of-health-things-privacy-and-security/
Source: http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

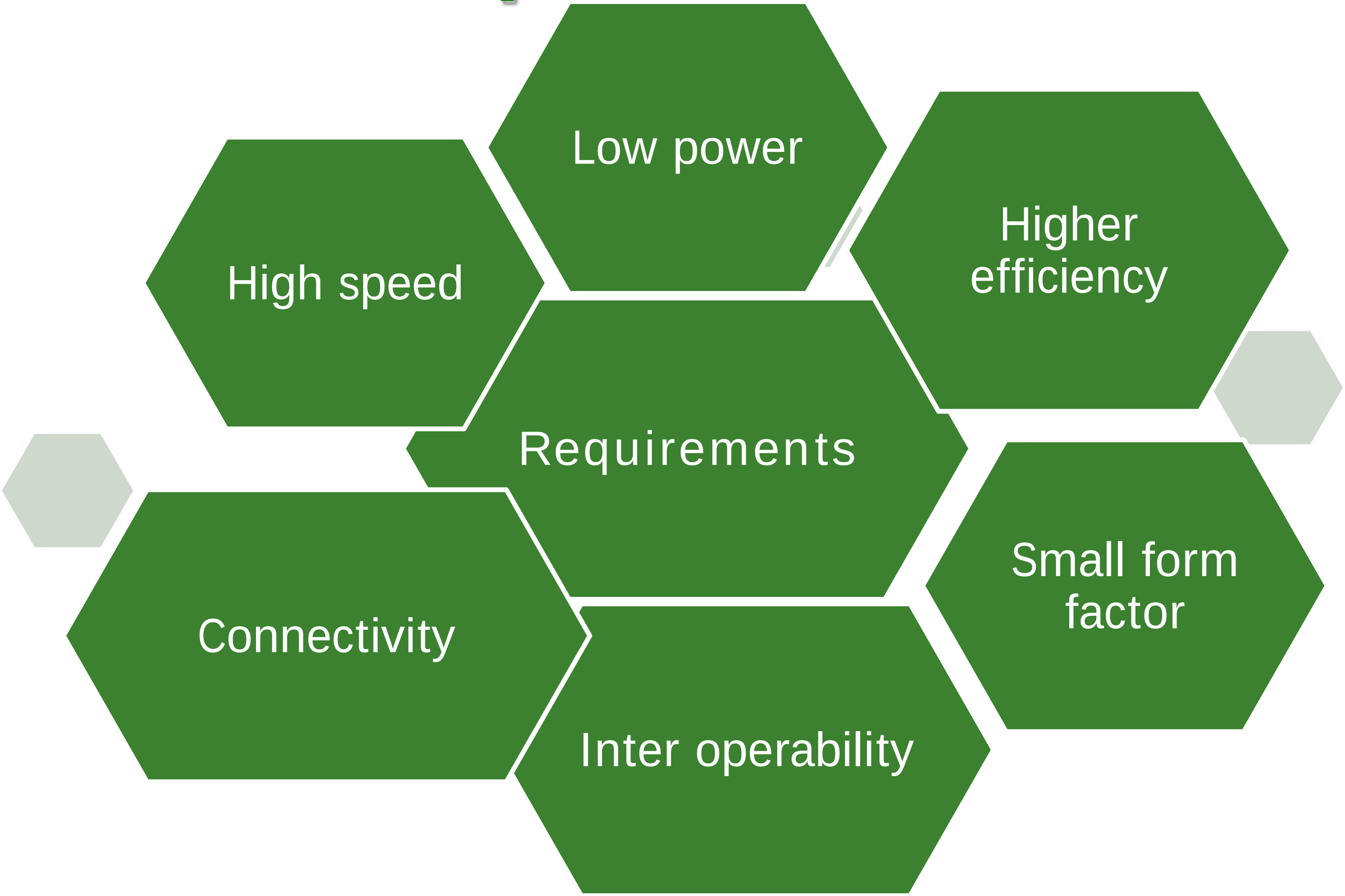
Smart Healthcare – Some Challenges

Smart Healthcare – Requirements

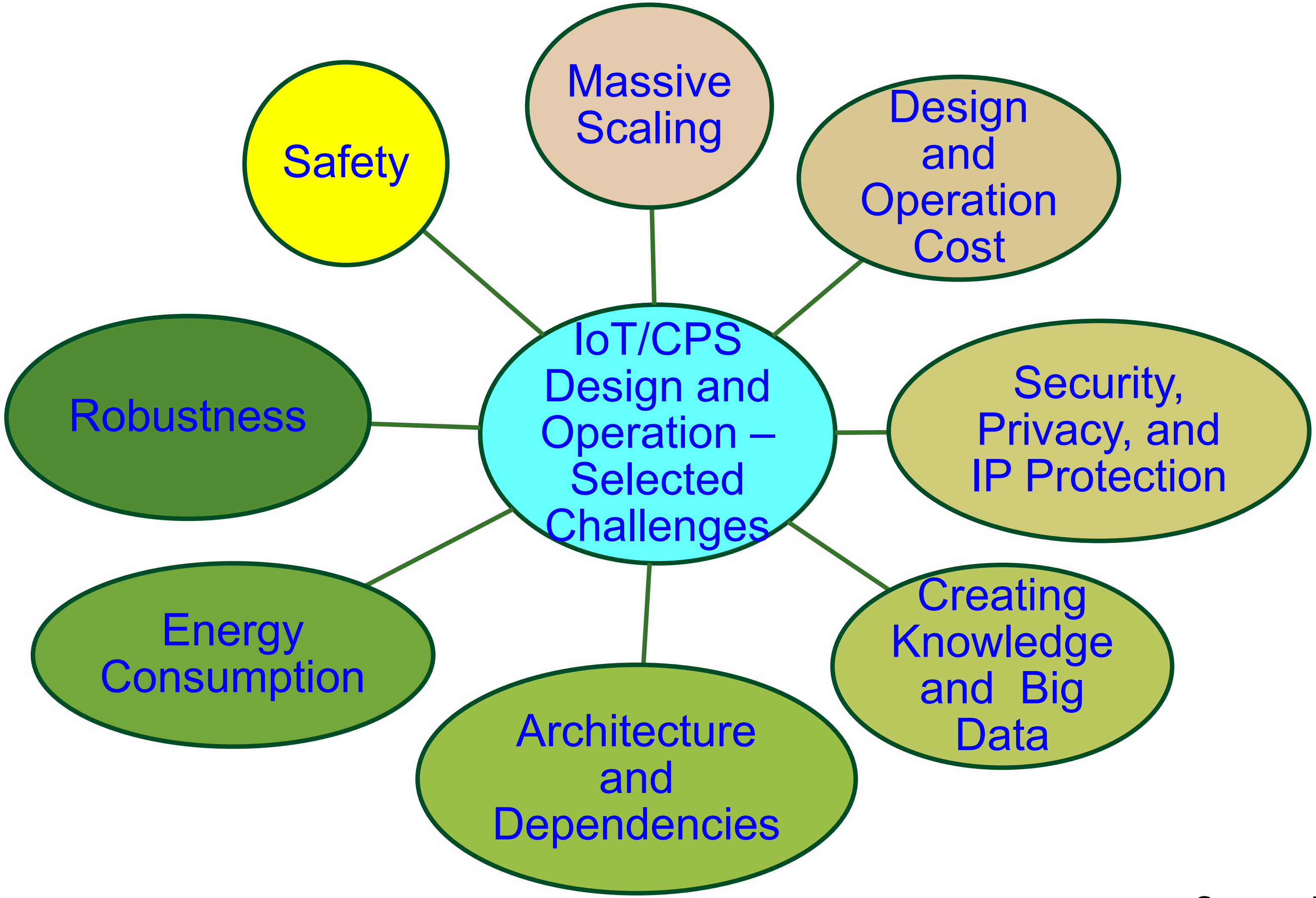


Source: P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, “Everything You Wanted to Know about Smart Health Care”, IEEE Consumer Electronics Magazine (CEM), Volume 7, Issue 1, January 2018, pp. 18-28.

Smart Healthcare Architecture – Requirements

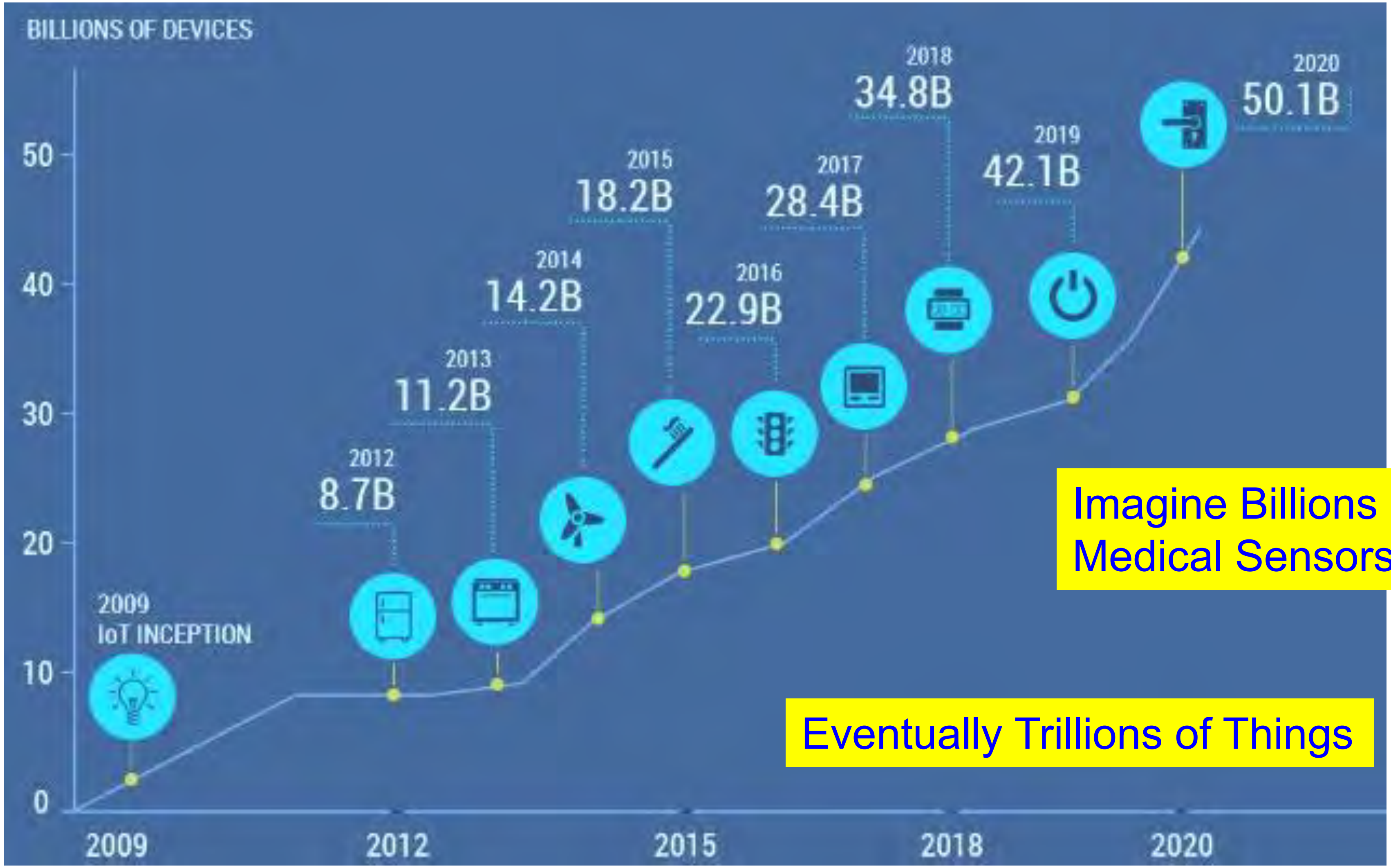


IoT/CPS – Selected Challenges



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

Smart Healthcare – Personalization and Autonomy

Personalization

	Provides input	Receive outputs
Set goals/ standard	User/Patient Healthcare provider Vendor	User/Patient
Collect & store data	Sensor User/Patient	User/Patient Healthcare provider Vendor
Report results	Stored data Goal/ target/ norm Data from comparison group	User/Patient Healthcare provider Specified others
Provide feedbacks	Results User/ Patient preferences User/ Patient characteristics User History	User/ Patient

Autonomy

Source: H. Zhu, C. K. Wu, C. H. KOO, Y. T. Tsang, Y.Liu, H. R. Chi, and K. F. Tsang, "Smart Healthcare in the Era of Internet-of-Things", IEEE Consumer Electronics Magazine, 2019, Accepted.

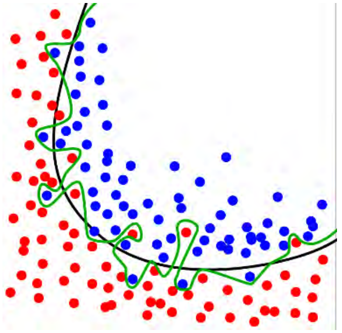
Smart Healthcare – Data Quality

Source: H. Zhu, C. K. Wu, C. H. KOO, Y. T. Tsang, Y.Liu, H. R. Chi, and K. F. Tsang, "Smart Healthcare in the Era of Internet-of-Things", *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 26-30, Sep 2019.

Machine Learning Challenges

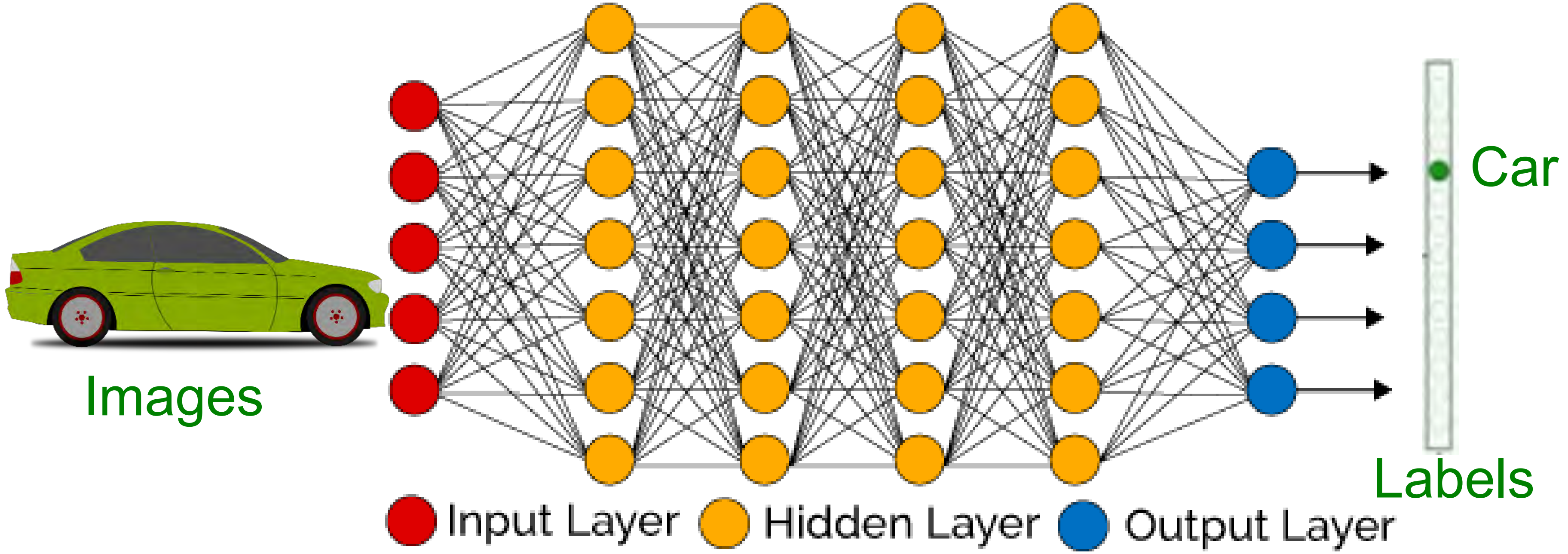
- High Energy Requirements
- High Computational Resource Requirements
- Large Amount of Data Requirements
- Underfitting/Overfitting Issue
- Class Imbalance Issue
- Fake Data Issue

Machine Learning Issues



Source: Mohanty ISCT Keynote 2019

DNN Training - Energy Issue

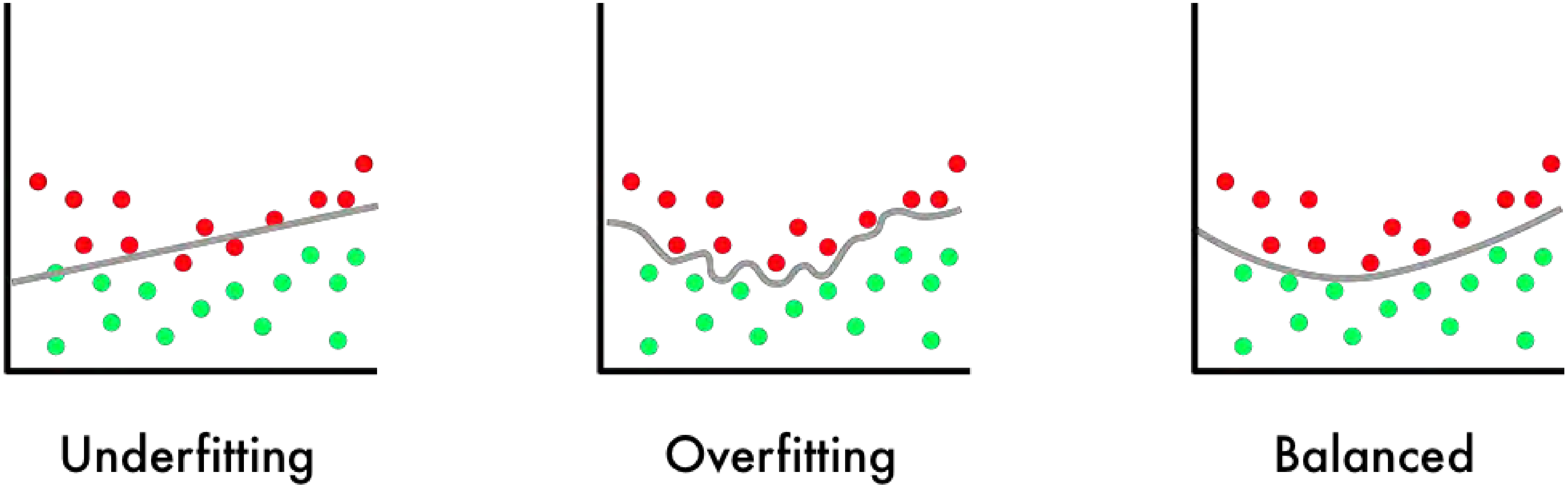


- DNN considers many training parameters, such as the size, the learning rate, and initial weights.
- High computational resource and time: For sweeping through the parameter space for optimal parameters.
- DNN needs: Multicore processors and batch processing.
- DNN training happens mostly in cloud not at edge or fog.

Source: Mohanty iSES 2018 Keynote

DNNs are not Always Smart

DNN: Underfitting and Overfitting Issues



Source: https://medium.freecodecamp.org/deep-learning-for-developers-tools-you-can-use-to-code-neural-networks-on-day-1-34c4435ae6b

DNN - Class Imbalance Issue

- Class imbalance is a classification problems where the classes are not represented equally.
- Solutions: Use Precision, Recall, F-measure metrics

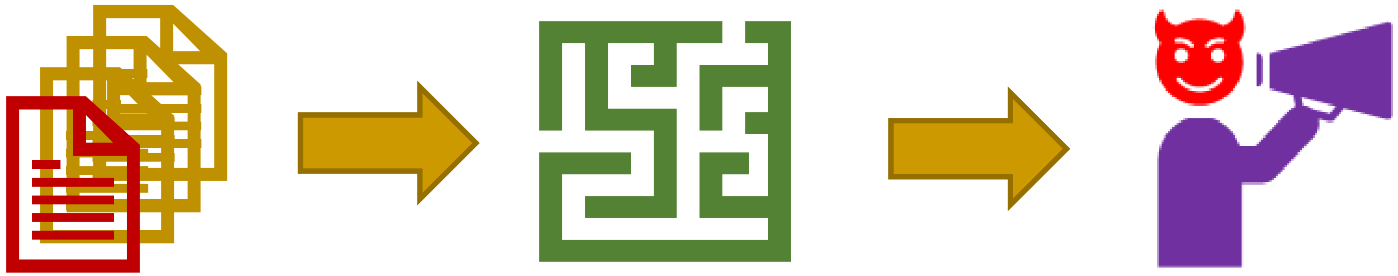
  Not only RMSE like accuracy metrics

AI/ML - Vulnerability

- Key vulnerabilities of machine learning systems
  - ML models often derived from fixed datasets
  - Assumption of similar distribution between training and real-world data
  - Coverage issues for complex use cases
  - Need large datasets, extensive data annotation, testing
- Strong adversaries against ML systems
  - ML algorithms established and public
  - Attacker can leverage ML knowledge for Adversarial Machine Learning (AML)
    - Reverse engineering model parameters, test data – Financial incentives
    - Tampering with the trained model – compromise security

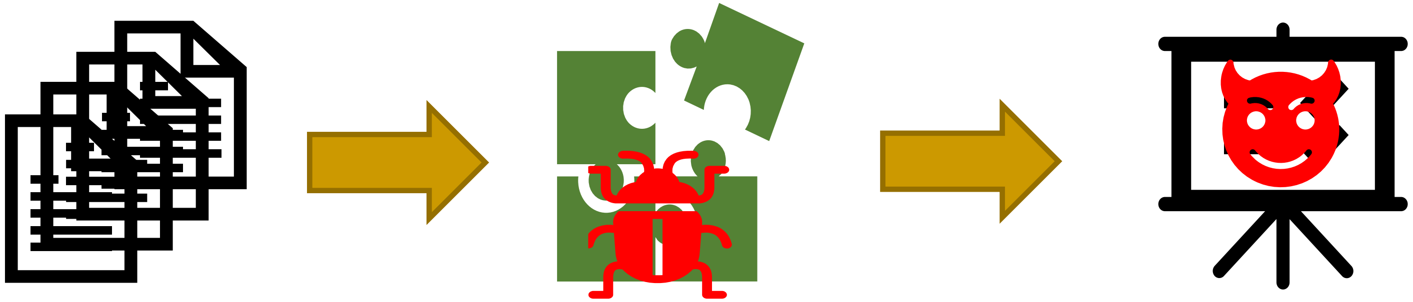
Source: Sandip Kundu ISVLSI 2019 Keynote.

AI/ML – Cybersecurity Issue



Corrupted Input Dataset — Predictive modelling — Corrupted Decision/ Prediction

Input attack in machine learning

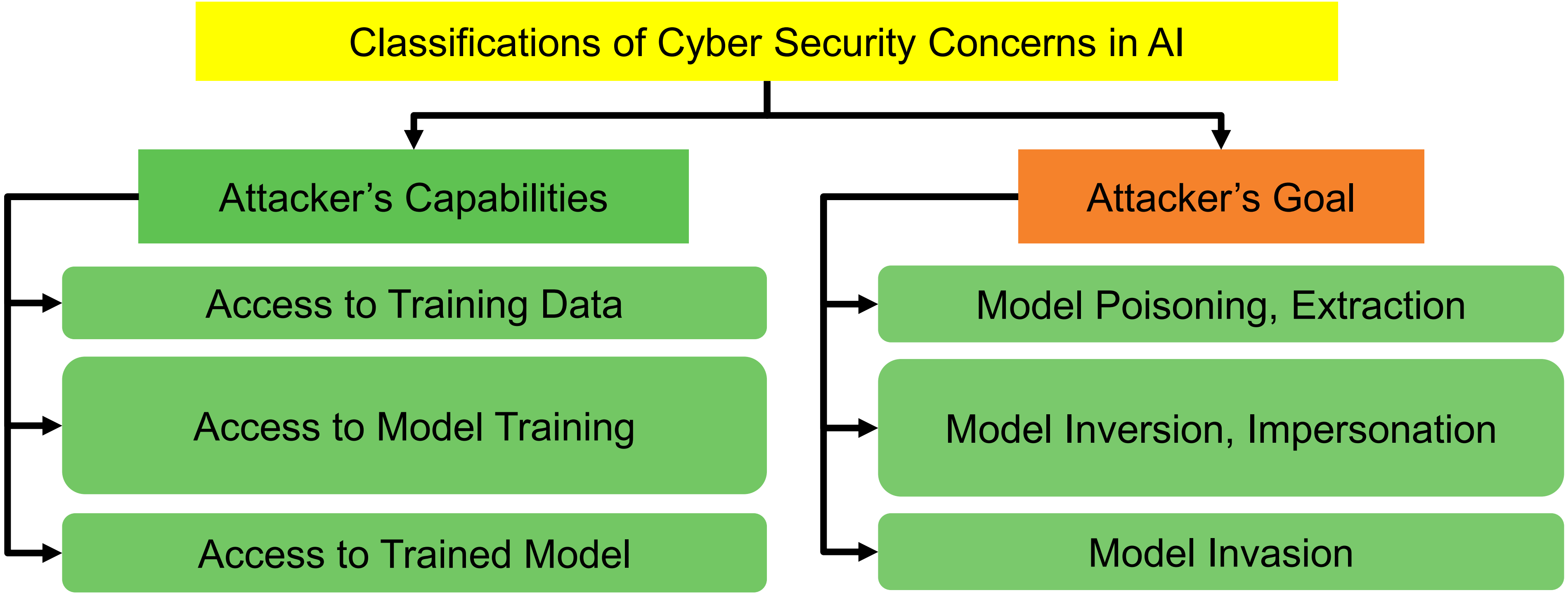


Input Dataset — Attacked training Process — Corrupt Classifications

Poisoning attack in training process

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.

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.

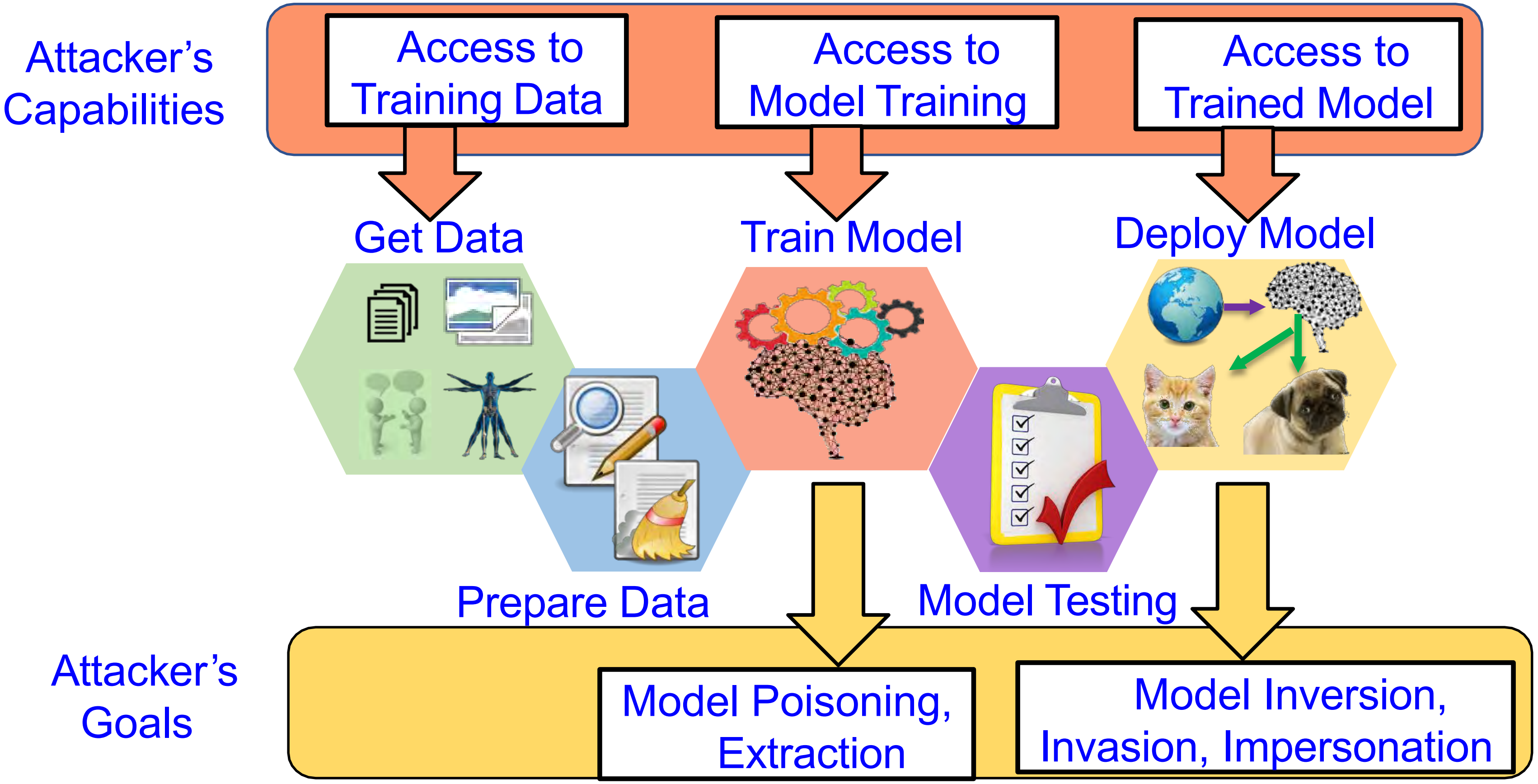
AI/ML Models - Classification of Security and Privacy Concerns

- Attacker's Goals
  - extract model parameters (model extraction)
  - extract private data (model inversion)
  - compromise model to produce false positives/negatives
- (model poisoning)
  - produce adversary selected outputs
- (model evasion)
  - render model unusable

- Attacker's Capabilities
  - access to Black-box ML model
  - access to White-box ML model
  - manipulate training data to
- introduce vulnerability
  - access to query to ML model
  - access to query to ML model with confidence values
  - access to training for building model
  - find and exploit vulnerability during
- classification

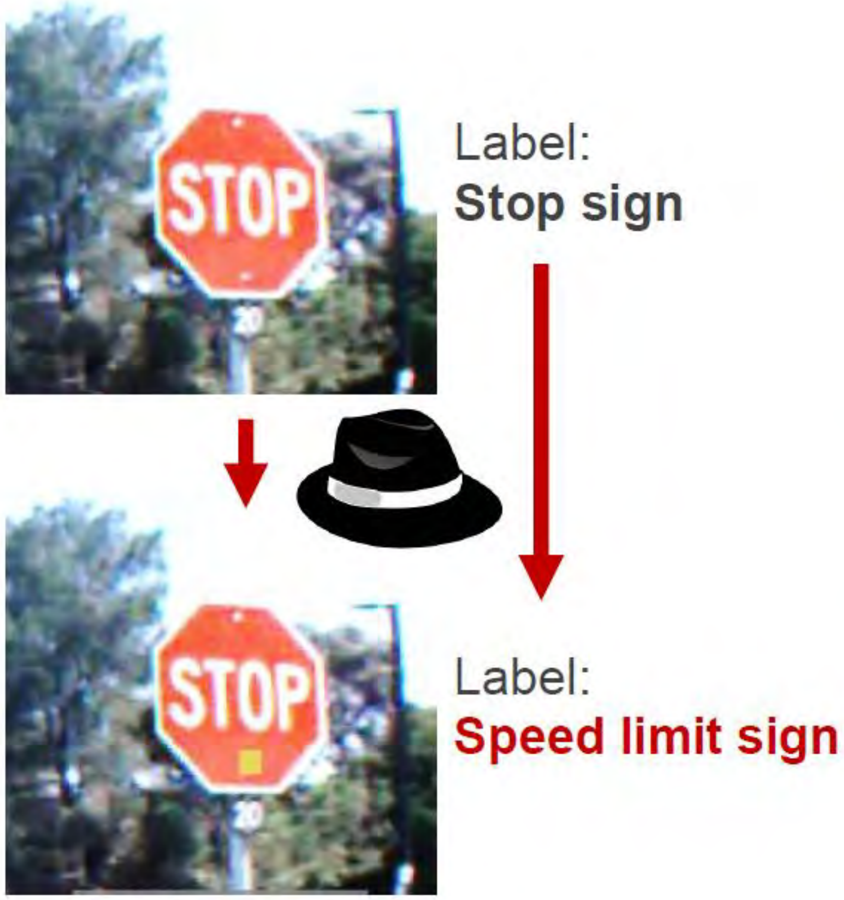
Source: Sandip Kundu ISVLSI 2019 Keynote.

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

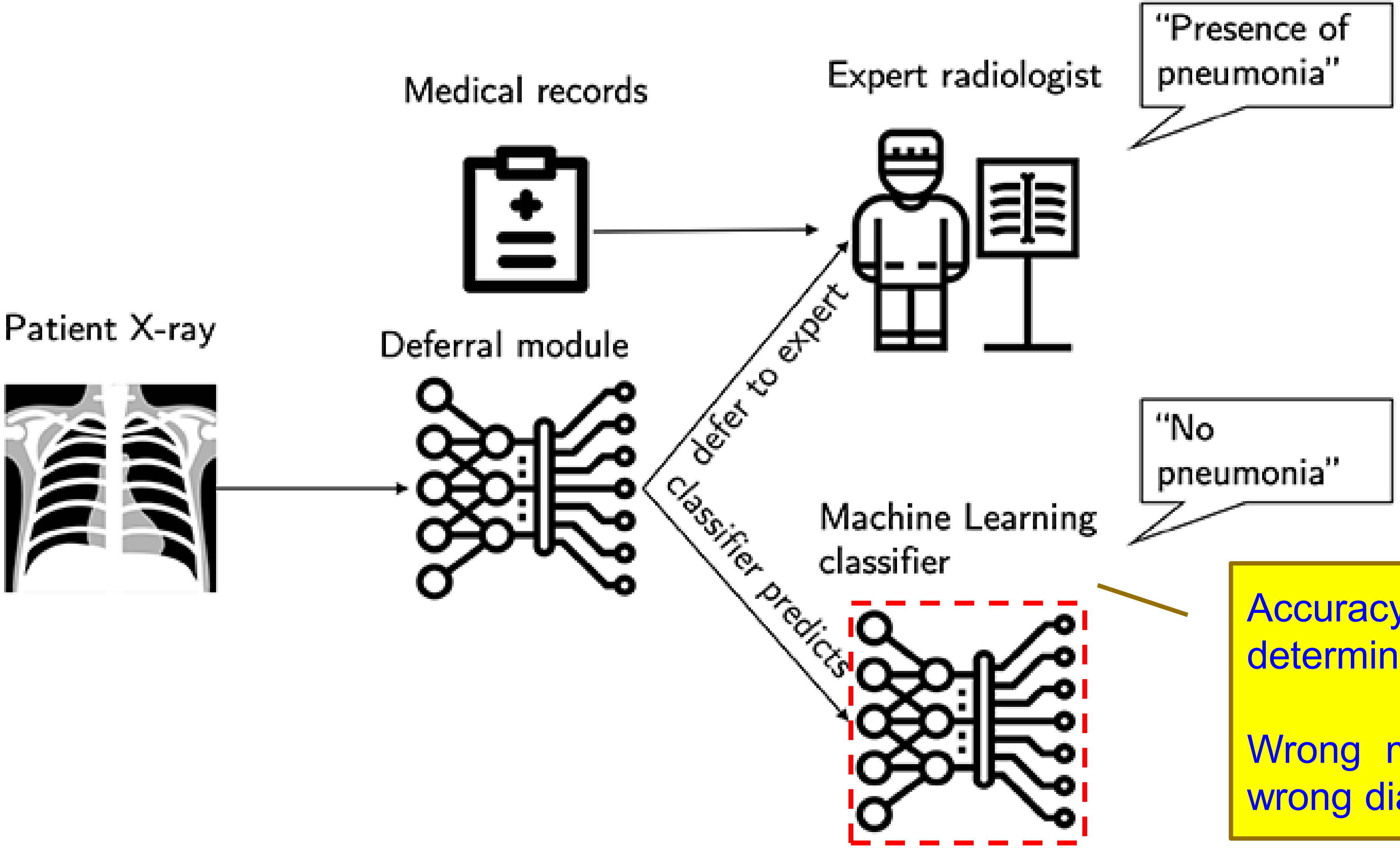
AI Security - Trojans in Artificial Intelligence (TrojAI)



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

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

Wrong ML Model → Wrong Diagnosis



Accuracy is important determine pneumonia

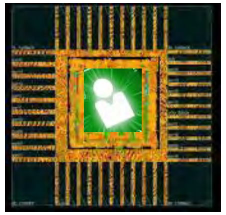
Wrong model can lead to wrong diagnosis altogether

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

Attacks on IoT Devices

Security, Privacy, and IP Rights

Hardware Trojan



System Security

Data Security

System Privacy

Data Privacy

Counterfeit Hardware (IP Rights Violation)

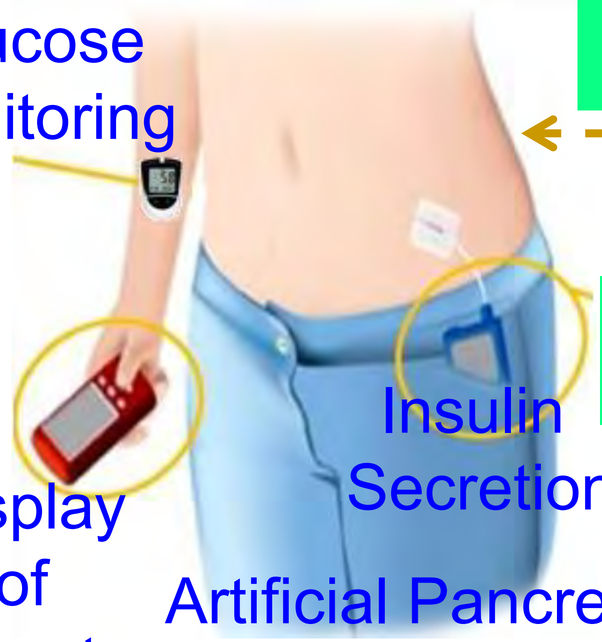
Data Ownership

Source: Mohanty ICIT 2017 Keynote

July 2017

IoMT Example - Our Intelligent Non-Invasive Glucose Monitoring with Insulin Control Device

Continuous Glucose Monitoring



Display of Parameters

Insulin Secretion

Artificial Pancreases System (APS)

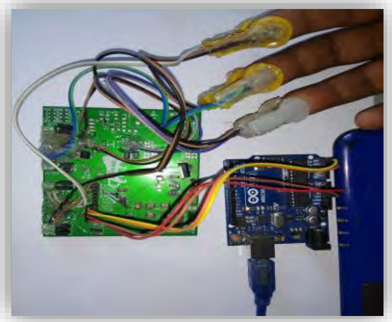
Privacy-Assured Health Data Storage

Security-Assured System

Cloud Storage

Hospital

Doctor



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.

Smart Healthcare - Cybersecurity and Privacy Issue

Selected Smart Healthcare Security/Privacy Challenges

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

Impersonation Attacks

Eavesdropping Attacks

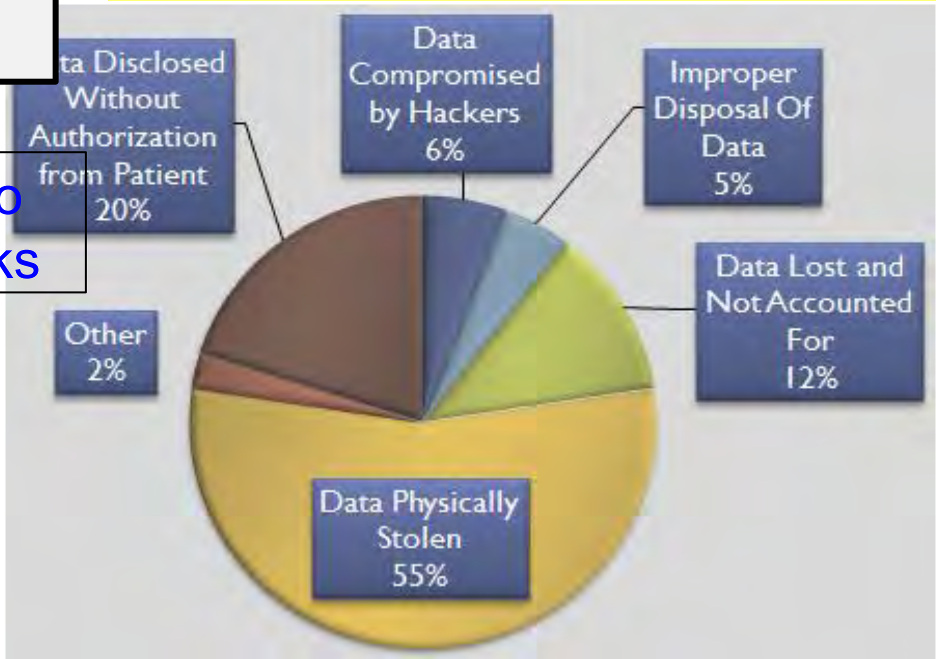
Smart Healthcare

Reverse Engineering Attacks

Radio Attacks

HIPAA
Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types



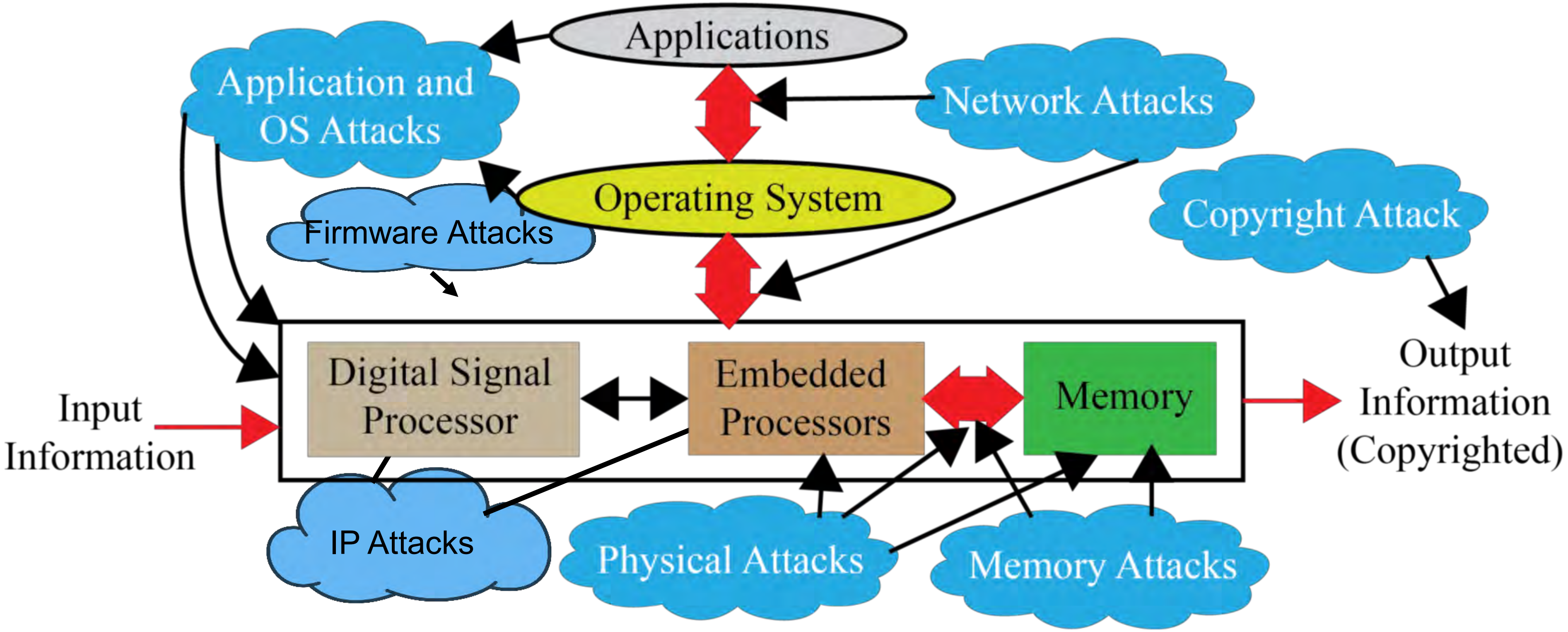
Smart Healthcare - Security Challenges

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.

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



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

Source: Mohanty ZINC 2018 Keynote

IoMT/H-CPS Security Issue is Real and Scary

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

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

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

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

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

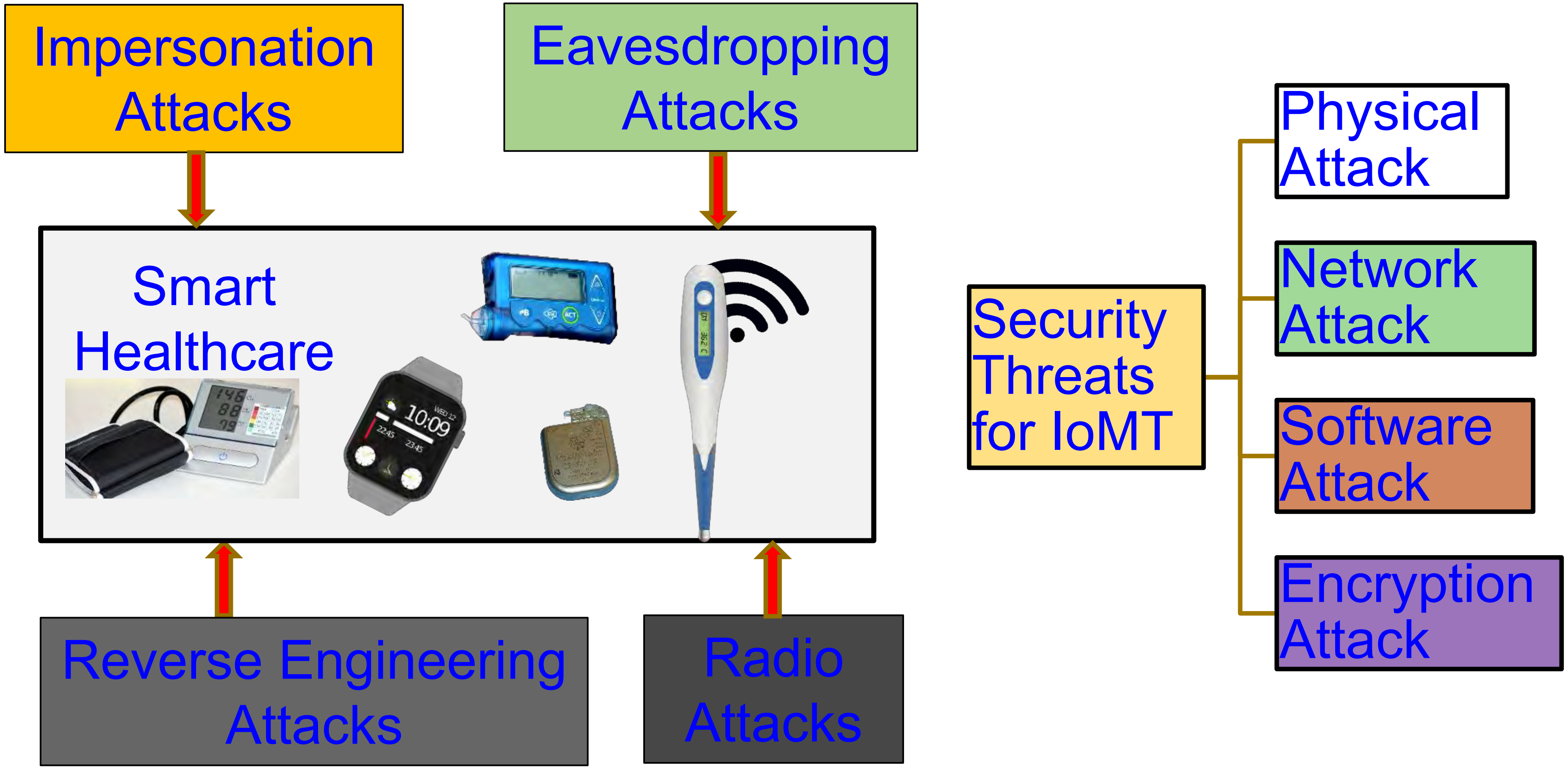
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

Implantable Medical Devices - Attacks

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

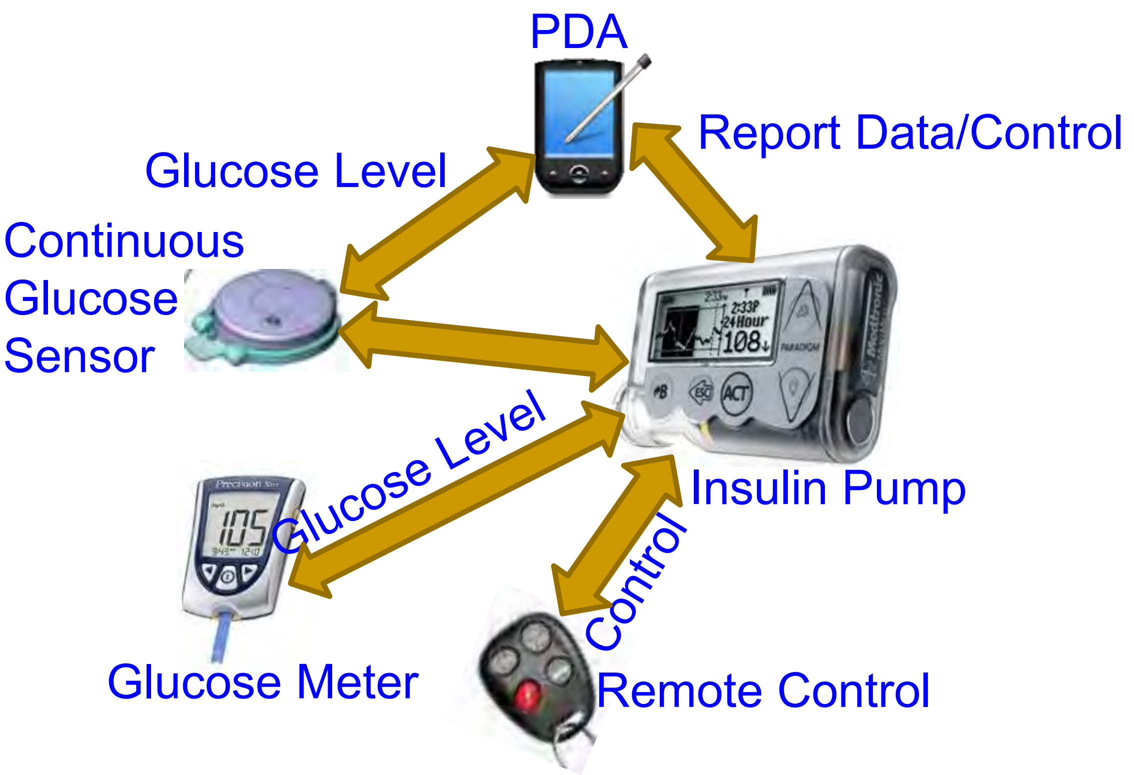
Source: Emily Waltz, Can "Internet-of-Body" Thwart Cyber Attacks on Implanted Medical Devices?, *IEEE Spectrum*, 28 Mar 2019, https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices.amp.html.

IoMT Security – Selected Attacks

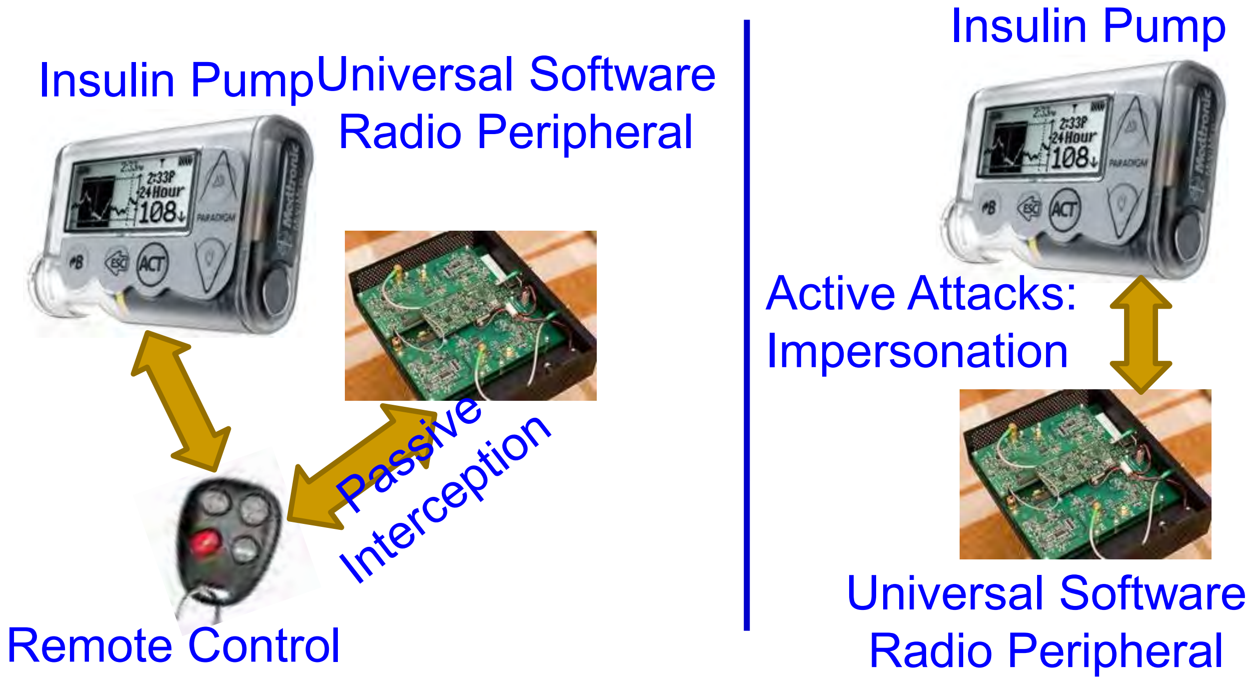


Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Specific Attack Example



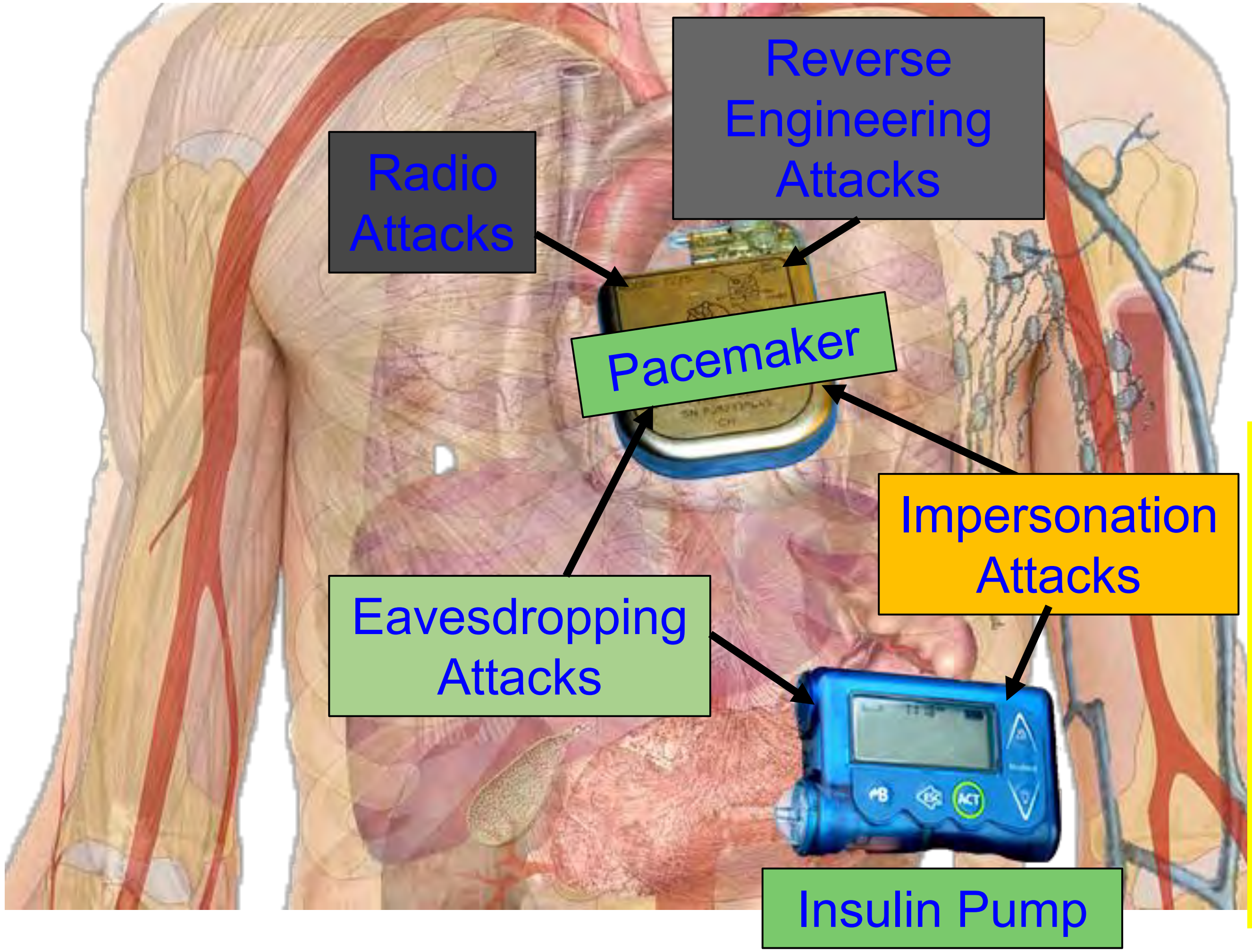
(a) Insulin Delivery System



(b) Security Attacks: Passive and Active

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 Security Measures is Hard



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

Implantable and Wearable Medical Devices (IWMDs) -- Battery Characteristics:
→ Longer life
→ Safer
→ Smaller size
→ Smaller weight

Pacemaker Battery Life - 10 years

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

AI can be fooled by fake data

AI can create fake data (Deepfake)

Authentic Fake

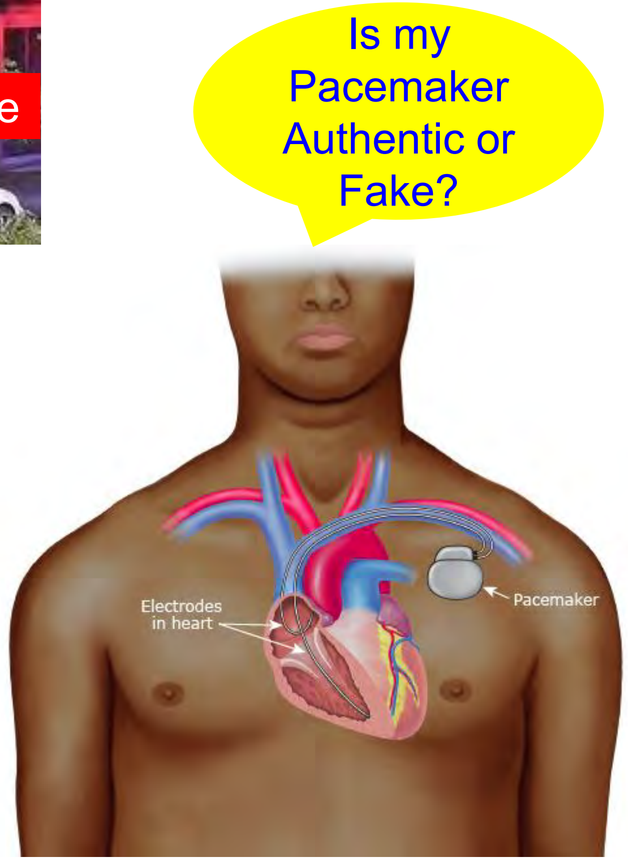
An implantable medical device

Authentic Fake

A plug-in for car-engine computers

Fake is Cheap – Why not Buy?

Source: https://www.quora.com

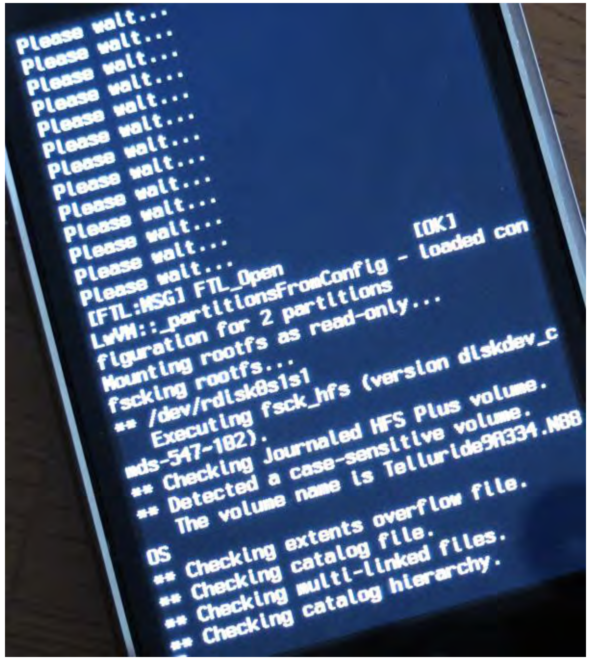


Source: https://nypost.com/

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

Firmware Reverse Engineering – Security Threat for Embedded System

Extract, modify, or reprogram code

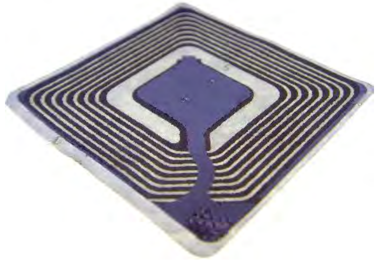


OS exploitation, Device jailbreaking

Source: http://jcjc-dev.com/

Source: http://grandideastudio.com/wp-content/uploads/current_state_of_hh_slides.pdf

RFID Security - Attacks



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

Numerous Applications

Source: Khattab 2017: Springer 2017 RFID Security

NFC Security - Attacks

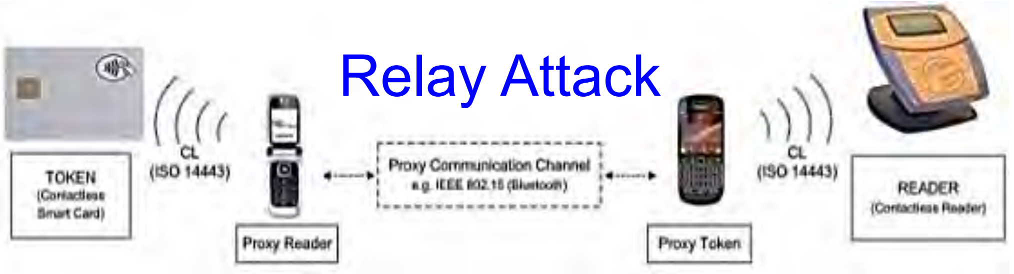
Selected NFC Attacks
- Eavesdropping
- Data Modification
- Relay Attacks
- Data Corruption
- Spoofing
- Interception Attacks
- Theft

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

Eavesdropping

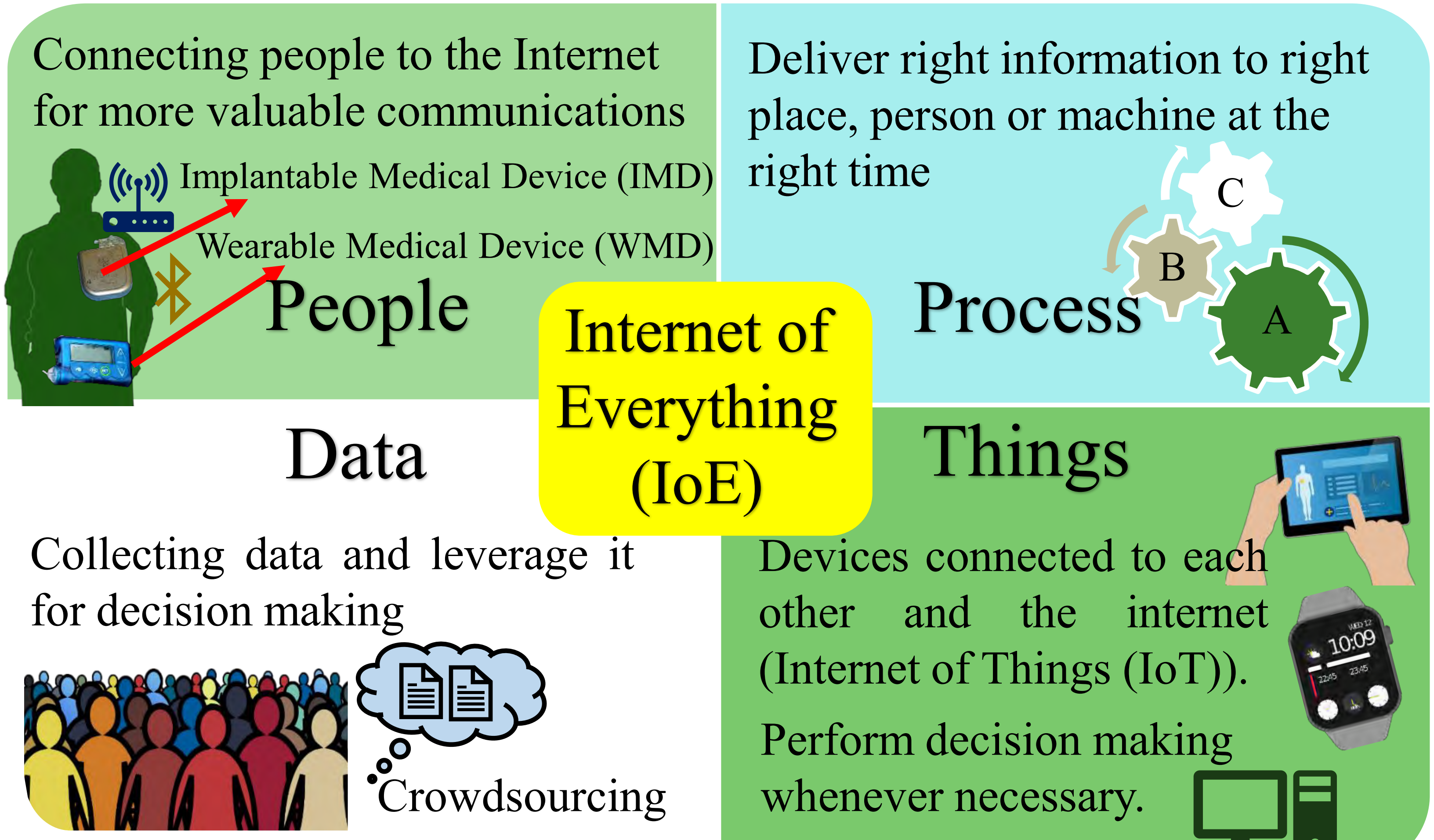
Source: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

Relay Attack



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

Users are Integral Part: For Them and By Them

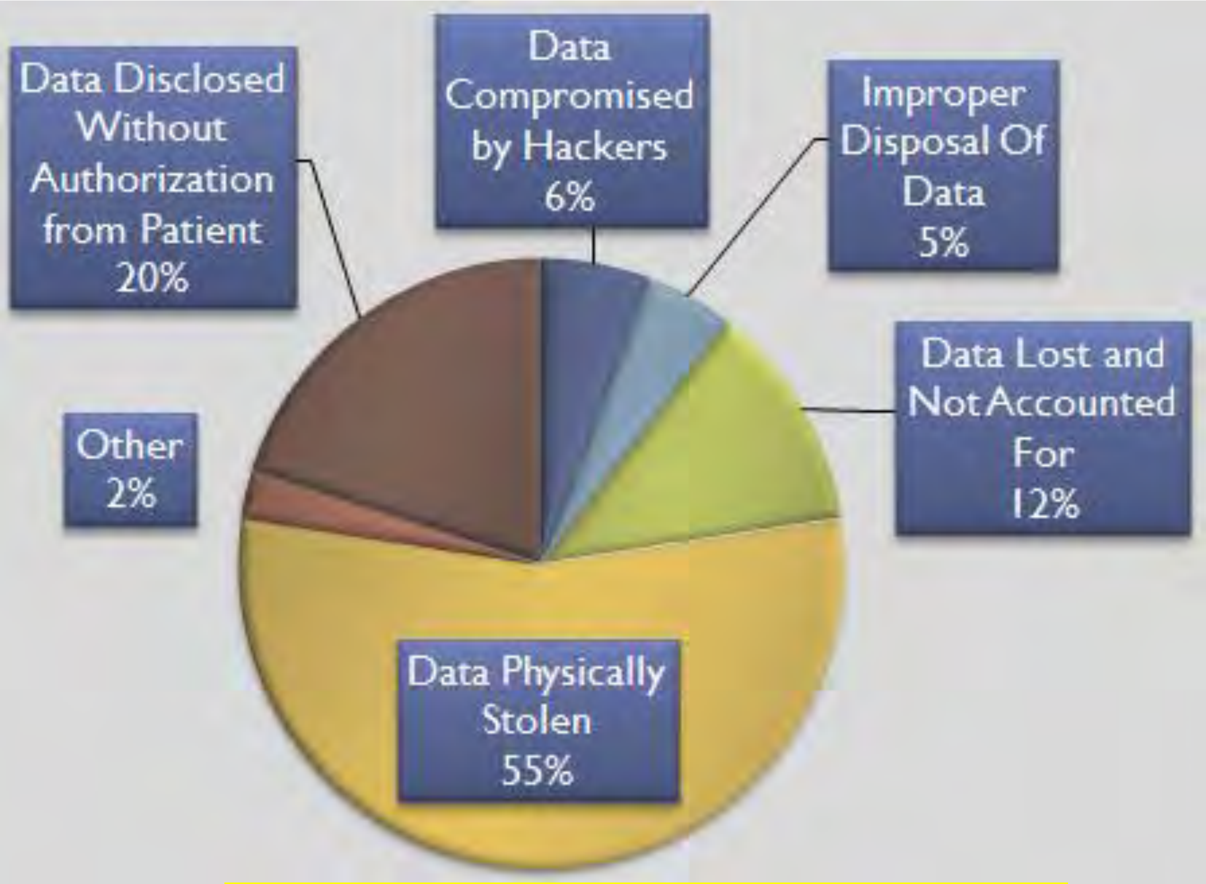


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8--16.

Health Insurance Portability and Accountability Act (HIPPA)

HIPAA

Health Insurance Portability and Accountability Act

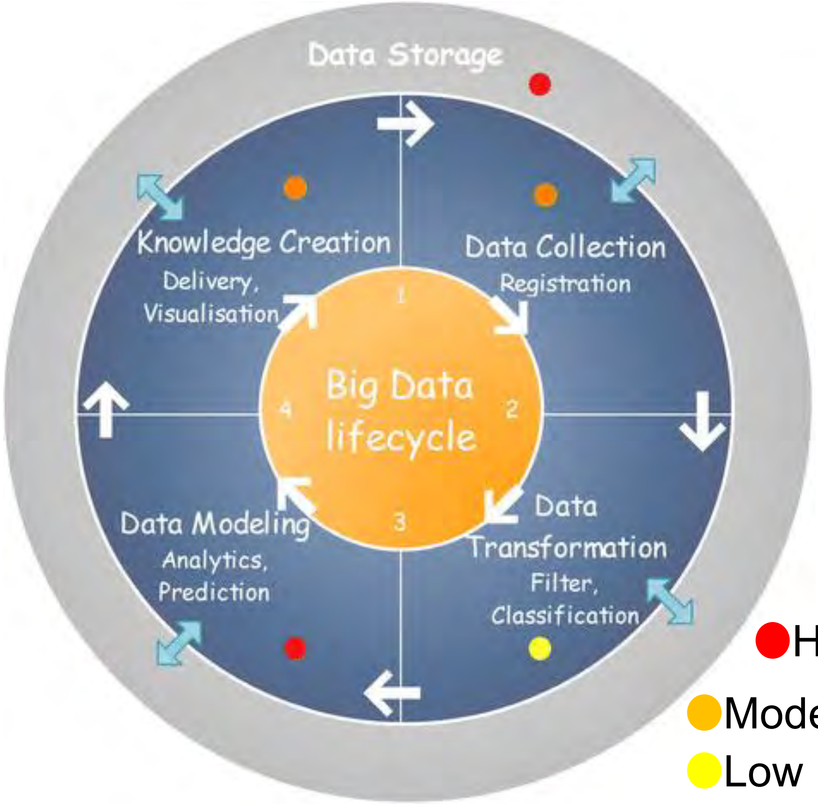


HIPPA Privacy Violation by Types

Smart Healthcare - Privacy Issue

Privacy

- Untraceability
- Unlinkability
- Unobservability
- Anonymity
- Pseudonymity



High Risk
Moderate Risk
Low Risk

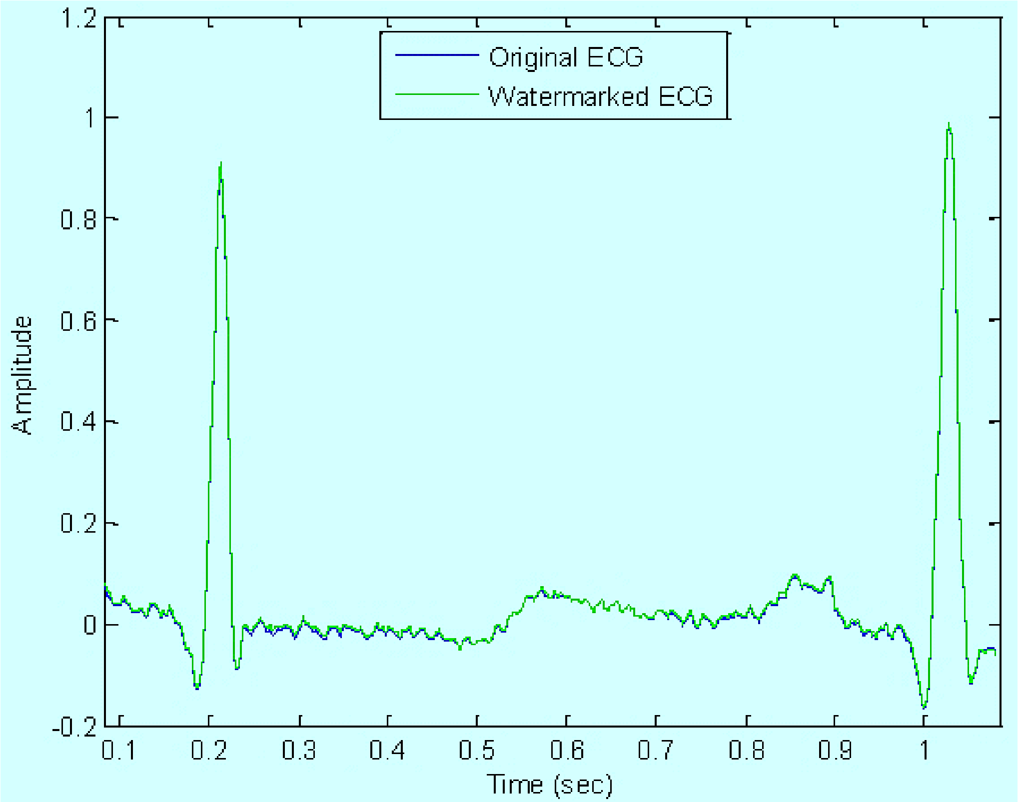
Smart Healthcare Security /Privacy Methods

- Authentication
- Data Encryption
- Data/Signal Watermarking
- Data Masking
- Access Control
- Monitoring and Auditing
- De-identification
- Hybrid Execution Model
- Identity-based Anonymization

Source: Abouelmehdi et al., Springer BigData 2018 Dec

Smart Healthcare Security – Medical Data Authentication

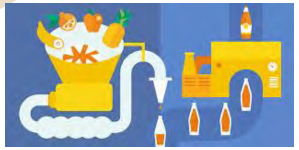
- Physiological signals like the electrocardiogram (EKG) are obtained from patients, transmitted to the cloud, and can also stored in a cloud repository.
- With increasing adoption of electronic medical records and cloud-based software-as-service (SaaS), advanced security measures are necessary.
- Protection from unauthorized access to Protected Health Information (PHI) also protects from identity theft schemes.
- From an economic stand-point, it is important to safeguard the healthcare and insurance system from fraudulent claims.



Source: Tseng 2014, Tseng Sensors Feb 2014

Reliable Supply Chain: Food Supply Chain: Farm → Dinning

How to ensure quality food through legitimate supply chain?



Farming & Growing

Processing

Transportation

Trading

Retails Service of Food

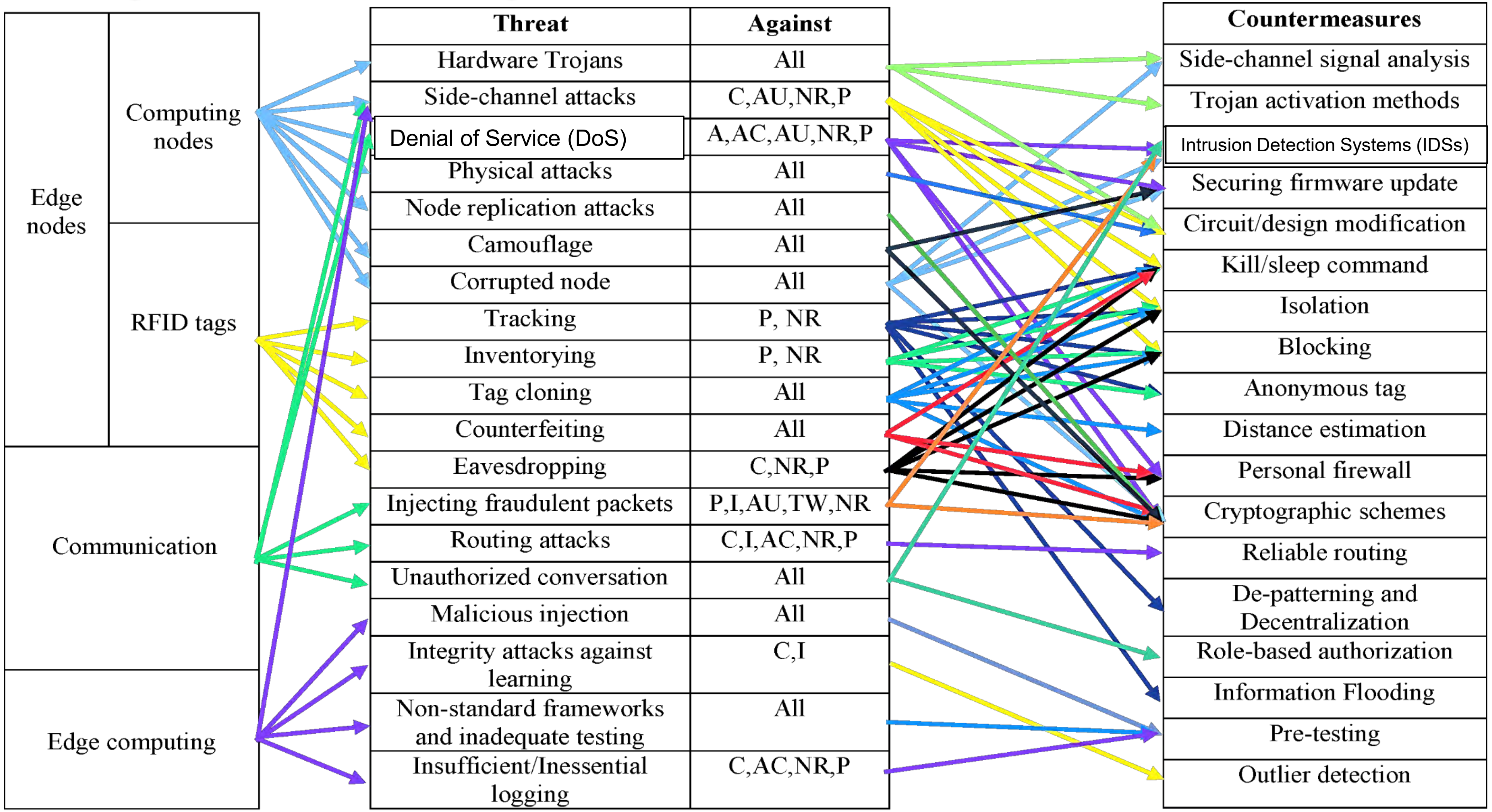
Consumption By Users

Similarly, Pharmaceutical Supply Chain

Source: A. M. Joshi, U. P. Shukla, and S. P. Mohanty, "Smart Healthcare for Diabetes: A COVID-19 Perspective", *arXiv Quantitative Biology*, arXiv:2008.11153, August 2020, 18-pages.

Cybrsecurity Solution for IoT/CPS

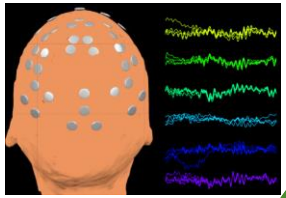
IoT Cybersecurity - Attacks and Countermeasures



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

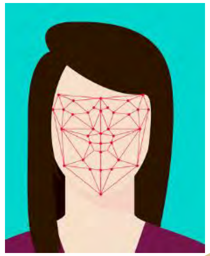
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

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



Finger Vein

Facial Recognition



Fingerprint

Electroencephalography (EEG)

Security Methods (Authentication)

Personal Identification Number (PIN)

Electrocardiography (ECG)

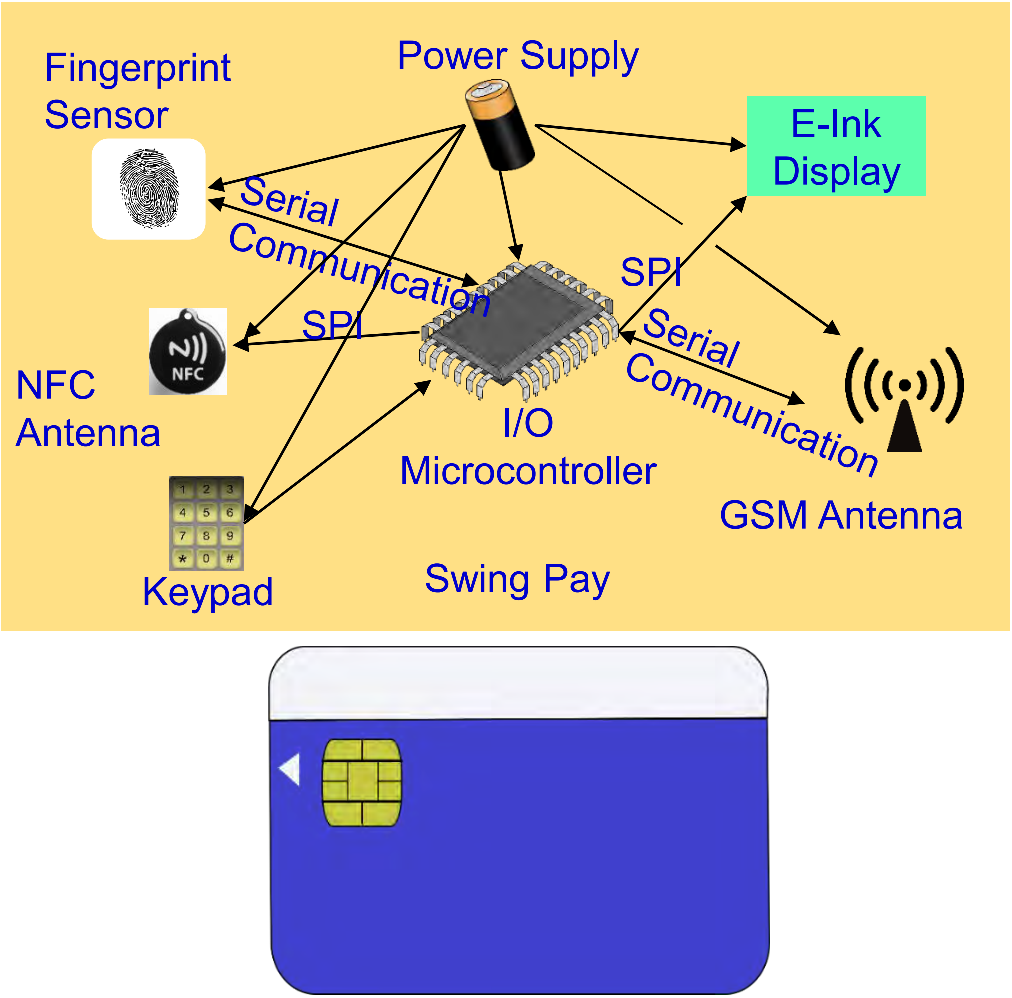
Password

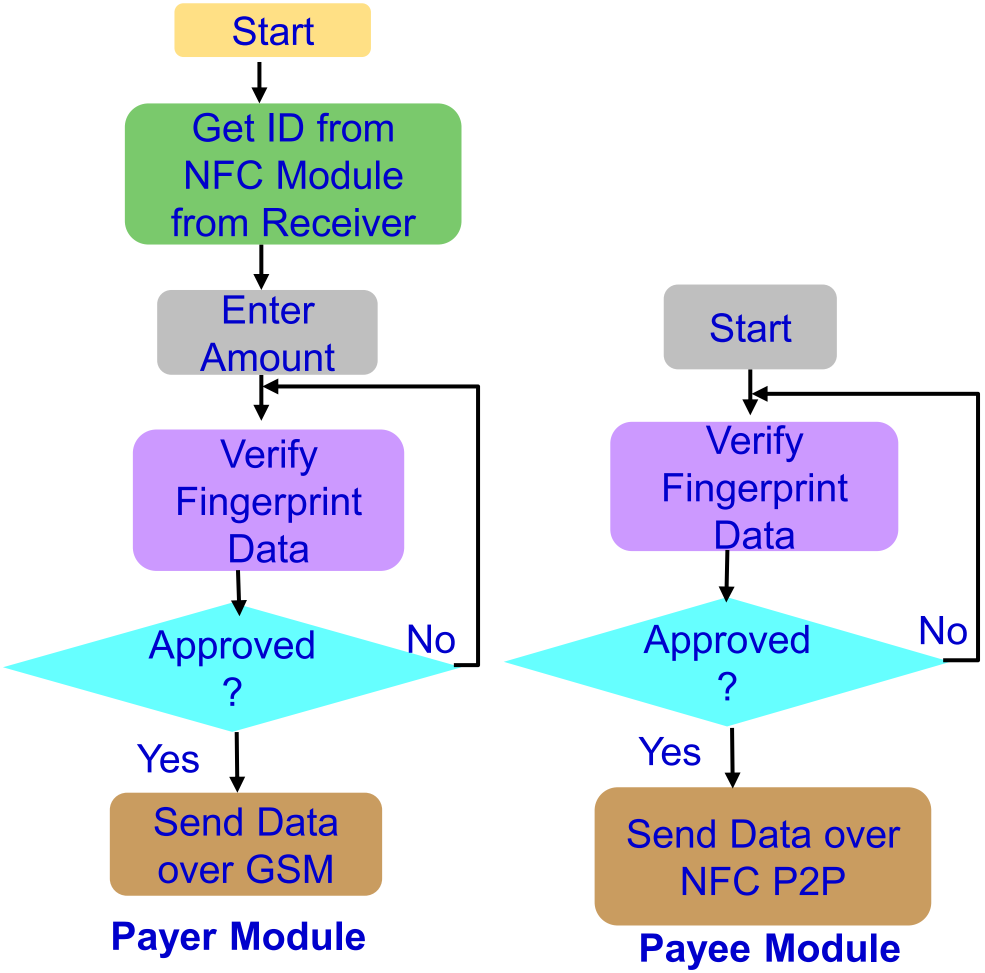
Online Signature

Touch-Screen Pattern

Source: Mohanty ISCT 2019 Keynote

Our Swing-Pay: NFC Cybersecurity Solution





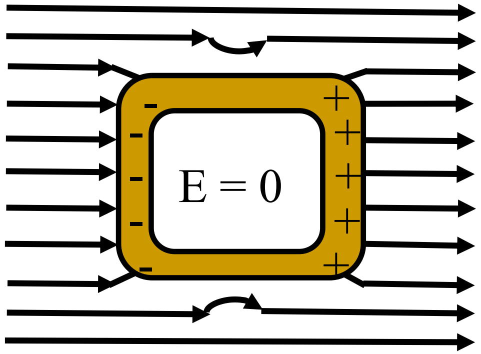
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

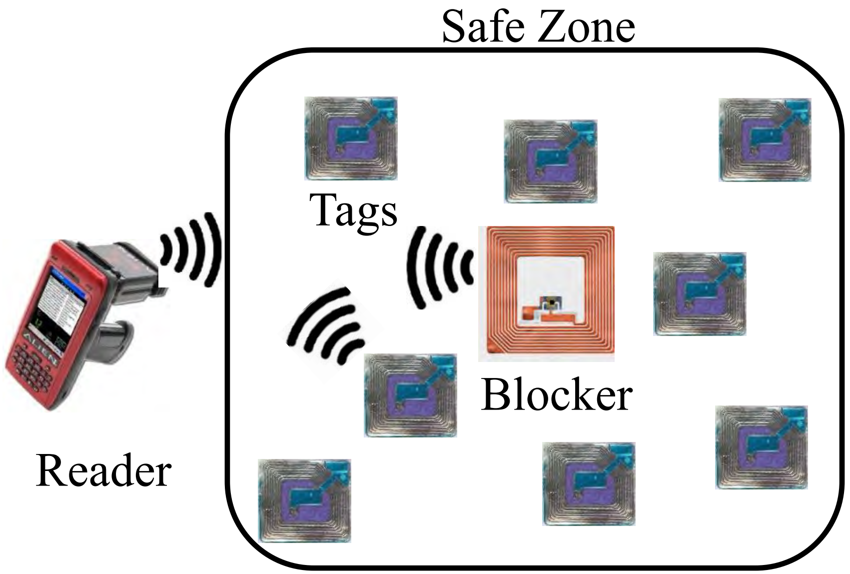
RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

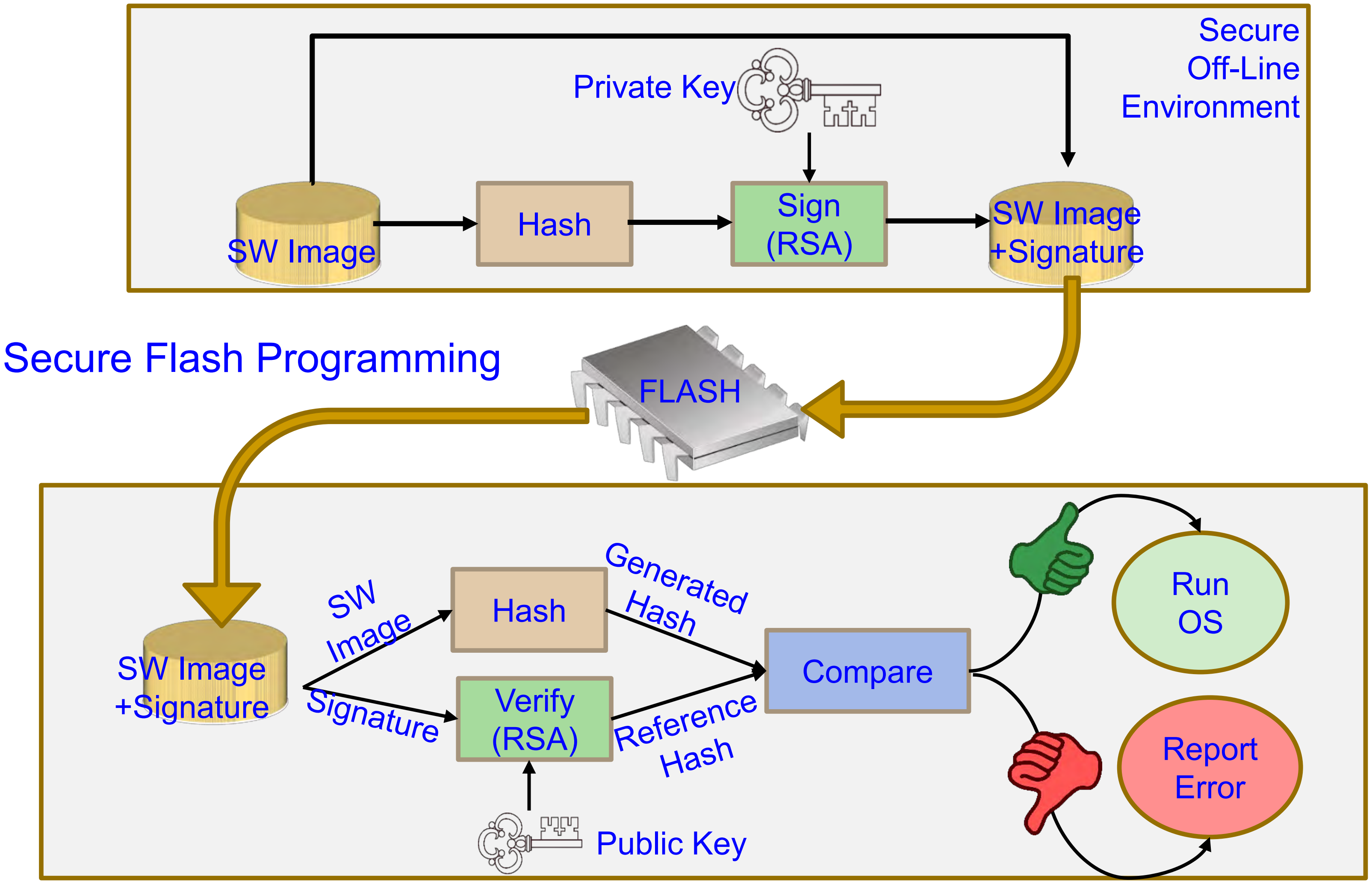




Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution



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

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

Nonvolatile / Harddrive Storage

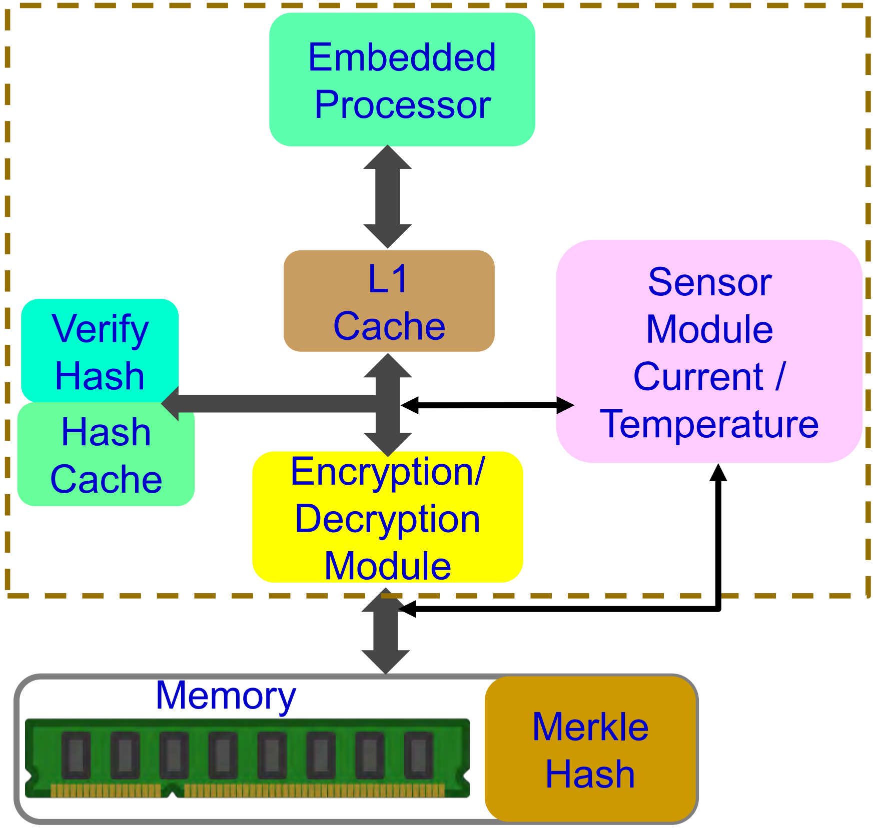
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

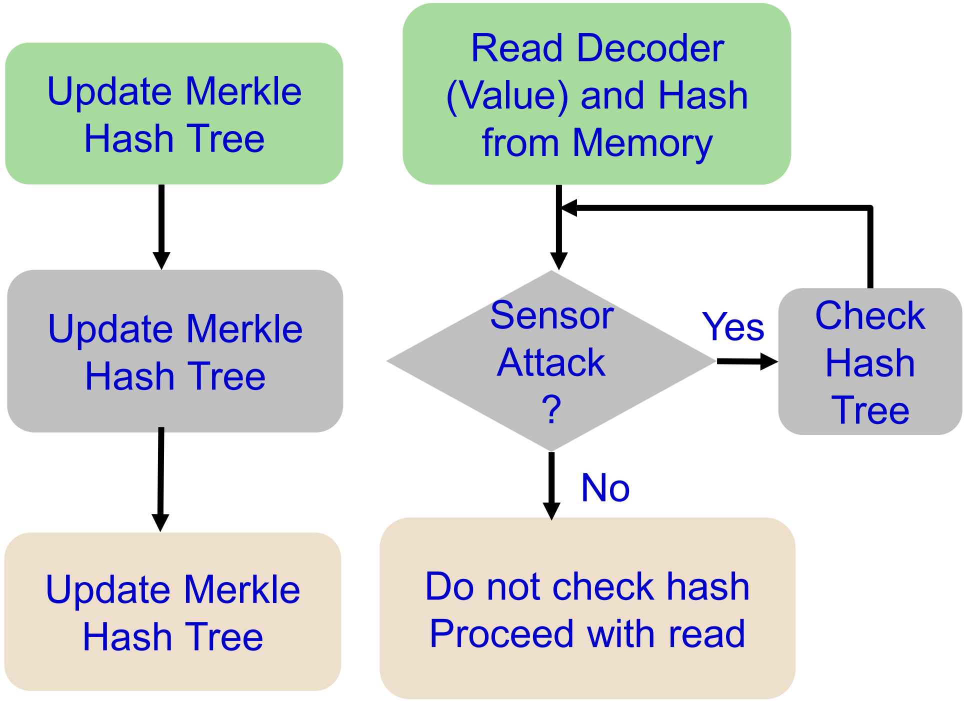
Some performance penalty due to increase in latency!

Embedded Memory Security

Trusted On-Chip Boundary



On-Chip/On-Board Memory Protection



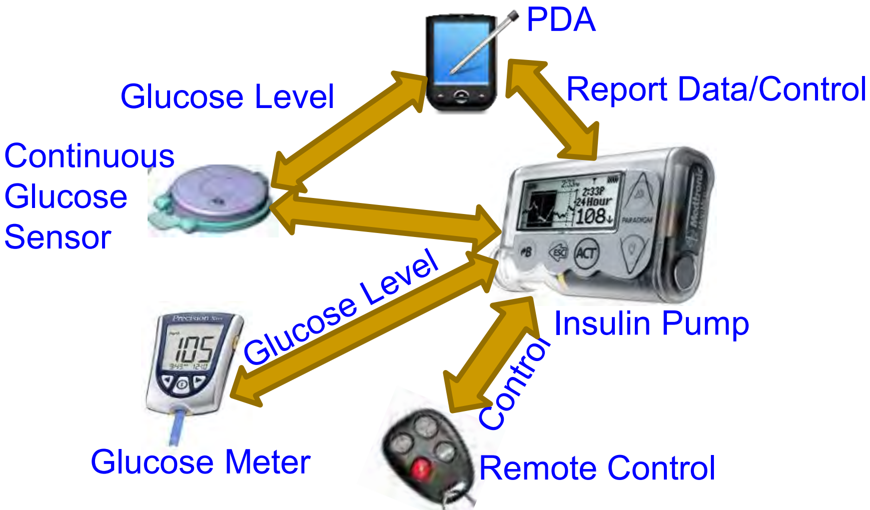
Write Operation

Read Operation

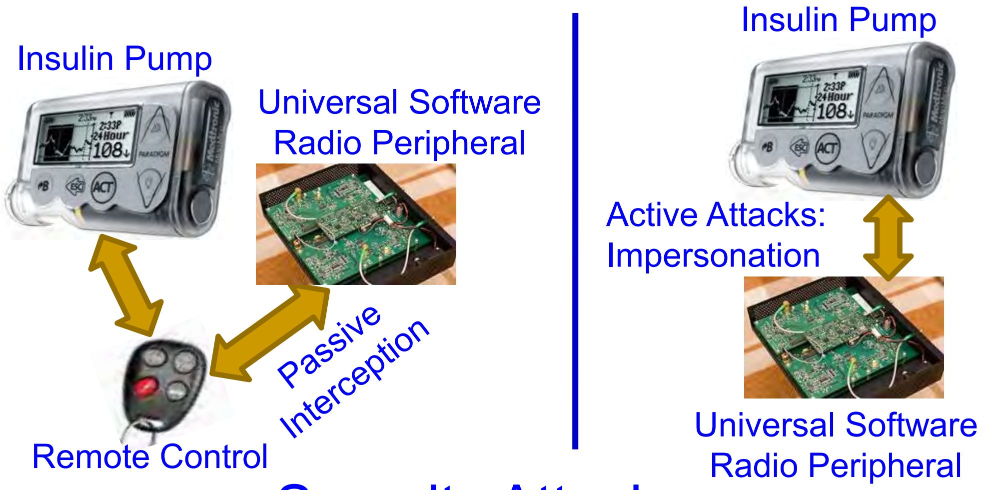
Memory integrity verification with 85% energy savings with minimal performance overhead.

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.

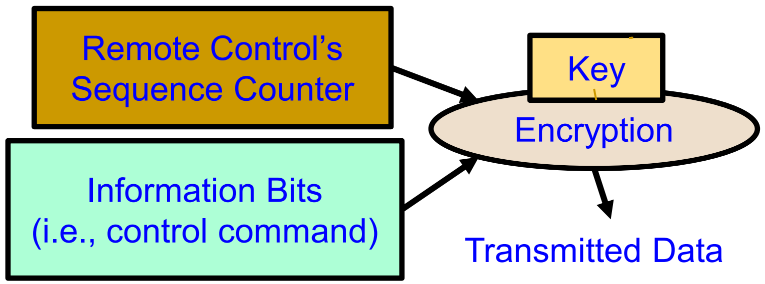
Smart Healthcare Cybersecurity



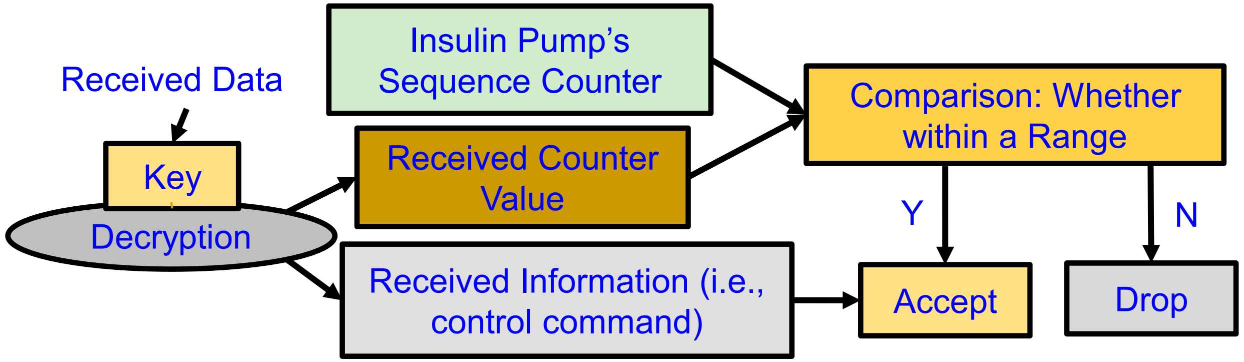
Insulin Delivery System



Security Attacks



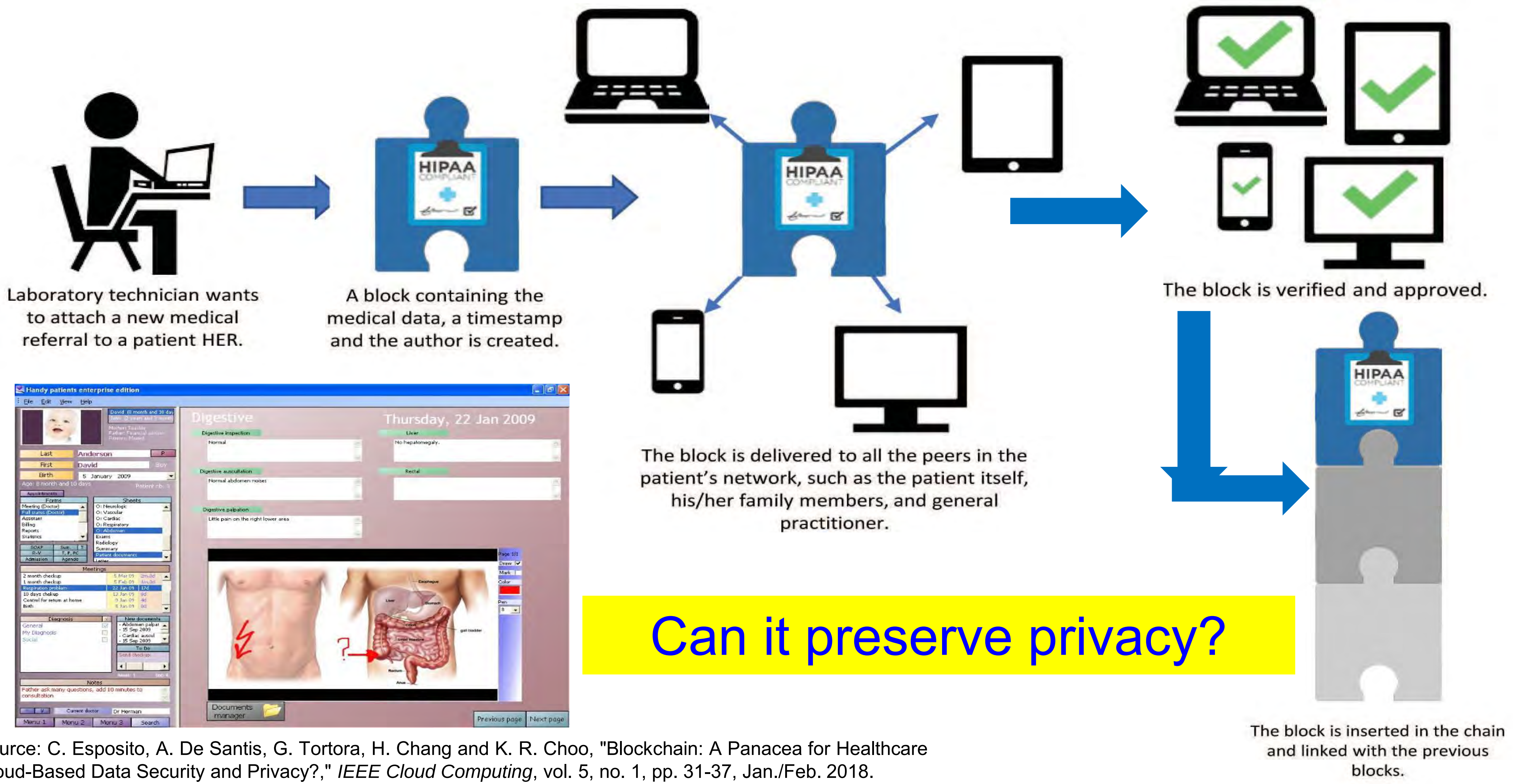
Rolling Code Encoder in Remote Control



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

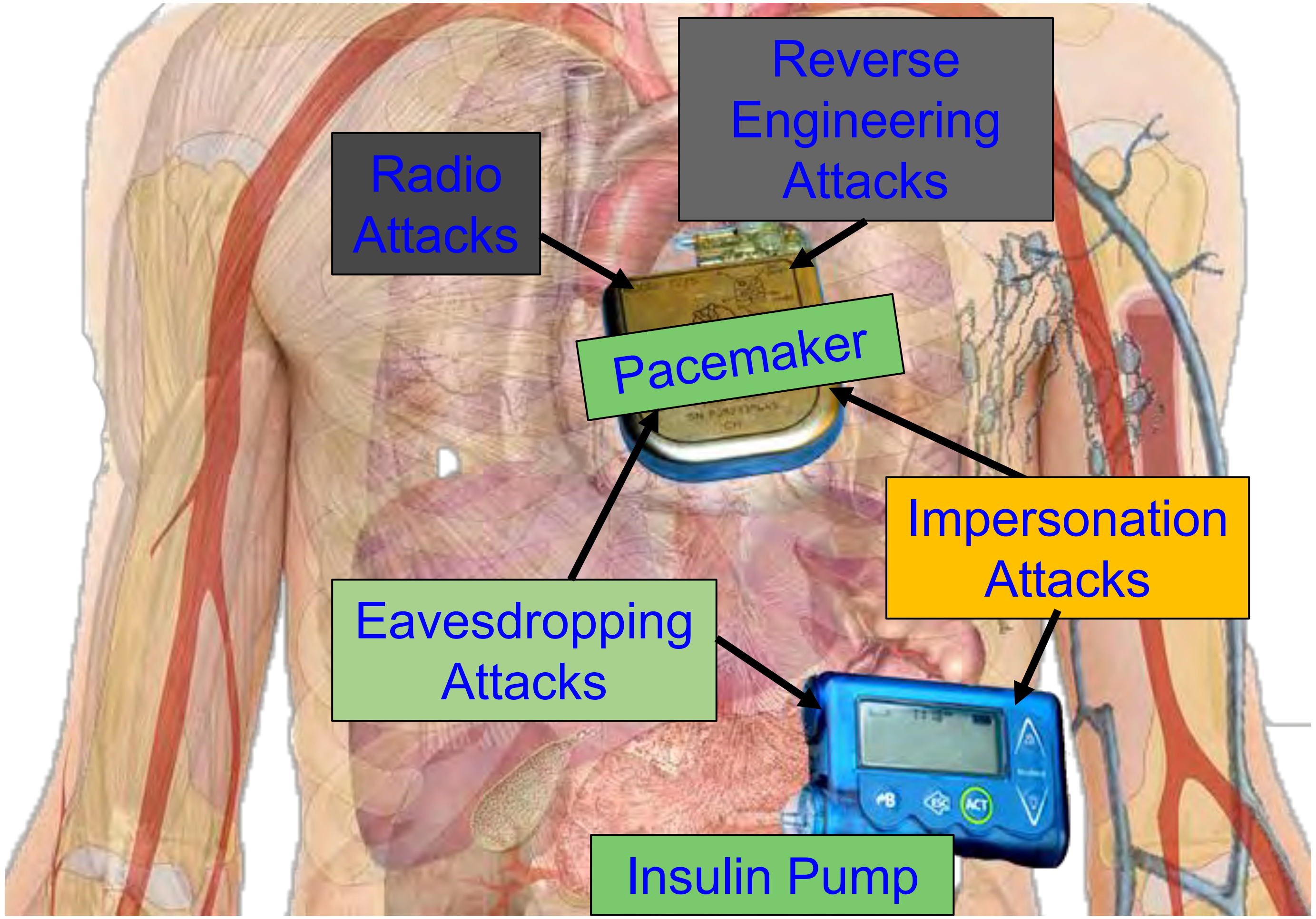
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

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.

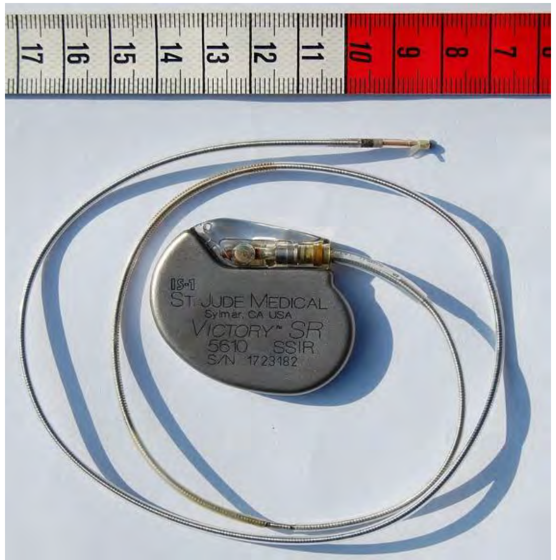
Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard



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



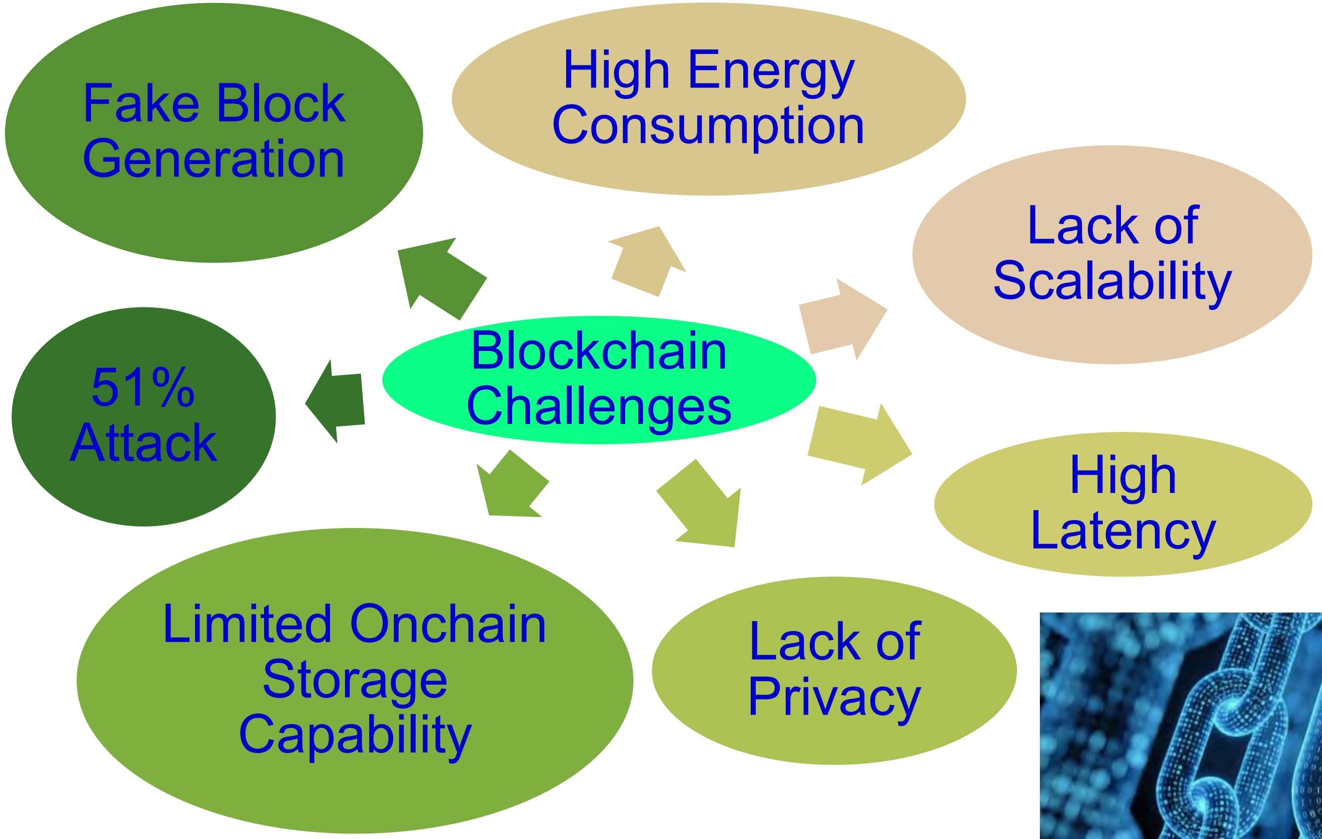
Pacemaker
Battery Life
- 10 years

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.

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

Blockchain Energy Need is Huge

Energy consumption for each bitcoin transaction

80,000X

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.

Blockchain has Serious Privacy Issue

	Bitcoin	Dash	Monero	Verge	PIVX	Zcash
Origin	-	Bitcoin	Bytecoin	Bitcoin	Dash	Bitcoin
Release	January 2009	January 2014	April 2014	October 2014	February 2016	October 2016
Consensus Algorithm	PoW	PoW	PoW	PoW	PoS	PoW
Hardware Mineable	Yes	Yes	Yes	Yes	No	Yes
Block Time	600 sec.	150 sec.	120 sec.	30 sec.	60 sec.	150 sec.
Rich List	Yes	Yes	No	Yes	Yes	No
Master Node	No	Yes	No	No	Yes	No
Sender Address Hidden	No	Yes	Yes	No	Yes	Yes
Receiver Address Hidden	No	Yes	Yes	No	Yes	Yes
Sent Amount Hidden	No	No	Yes	No	No	Yes
IP Addresses Hidden	No	No	No	Yes	No	No
Privacy	No	No	Yes	No	No	Yes
Untraceability	No	No	Yes	No	No	Yes
Fungibility	No	No	Yes	No	No	Yes

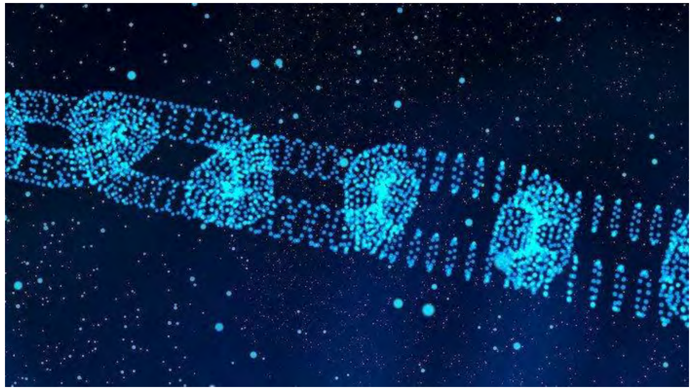
Source: J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 20-25, September 2019.

Smart Contracts - Vulnerabilities

Vulnerability	Cause	Level
Call to unknown	The called function does not exist	Contract's source code
Out-of-gas send	Fallback of the callee is executed	Contract's source code
Exception disorder	Exception handling irregularity	Contract's source code
Type casts	Contract execution type-check error	Contract's source code
Reentrance flaw	Function reentered before exit	Contract's source code
Field disclosure	Private value published by miner	Contract's source code
Immutable bug	Contract altering after deployment	Ethereum virtual machine bytecode
Ether lost	Ether sent to orphan address	Ethereum virtual machine bytecode
Unpredicted state	Contract state change before call	Blockchain Mechanism
Randomness bug	Seed biased by malicious miner	Blockchain mechanism
Time-stamp failure	Malicious miner alters time stamp	Blockchain mechanism

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?



Information of the System that may need a blockchain?

Blockchain provides historical consistent data storage	Does system need permanent shared data storage?	No
Blockchain is used when multiple entities are giving data	Are there multiple data contributors to system?	No
Blockchain does not allow data modification after storage	Does the application modify data after storage?	No
Blockchain does not provide data privacy, even if it is in an encrypted format	Is data privacy required?	No
Blockchain is not required, if there are no trust issues in a system	Does the system work in an untrusted environment?	No
Blockchain is not suitable solution if auditing in real-time	Does the system need tamperproof data storage?	No

Each "Yes" leads to the next question; each "No" leads to: Blockchain is not needed

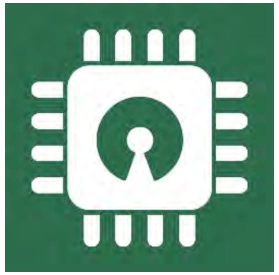
Yes → Your system needs the blockchain

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.

Cybersecurity Attacks – Software Vs Hardware Based

Software Based

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



Hardware Based

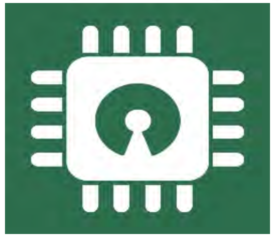
- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
  - Hardware backdoors (e.g. Trojan)
  - Inducing faults
  - Electronic system tampering/ jailbreaking
  - Eavesdropping for protected memory
  - Side channel attack
  - Hardware counterfeiting

Source: Mohanty ICCE Panel 2018

Cybersecurity Solutions – Software Vs Hardware Based

Software Based

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

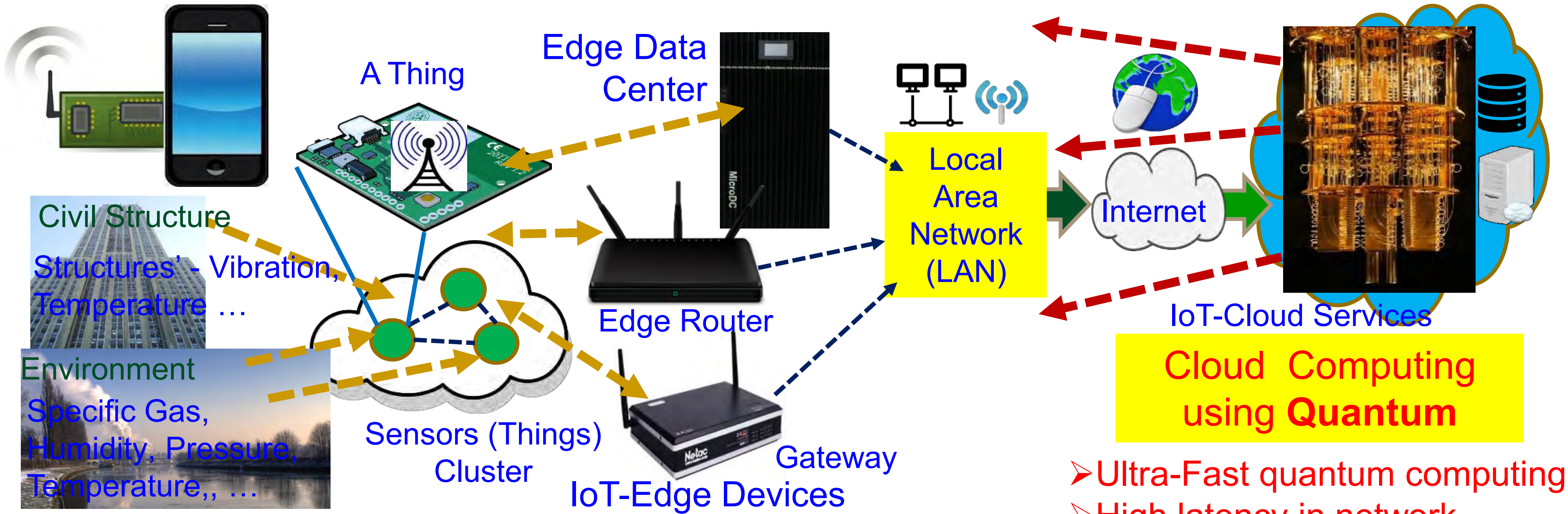


Hardware Based

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

Source: Mohanty ICCE Panel 2018

Cybersecurity Nightmare ← Quantum Computing



In-Sensor/End-Device Computing

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

Edge Computing

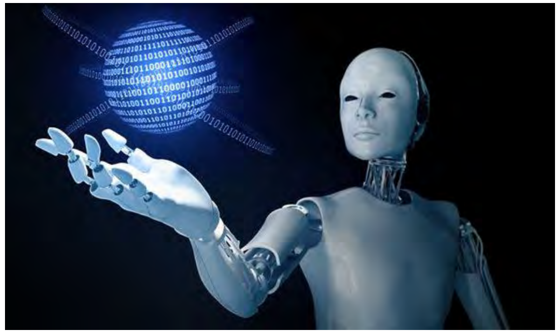
- Less computational resource
- Minimal latency in network
- Lightweight security

Cloud Computing using Quantum

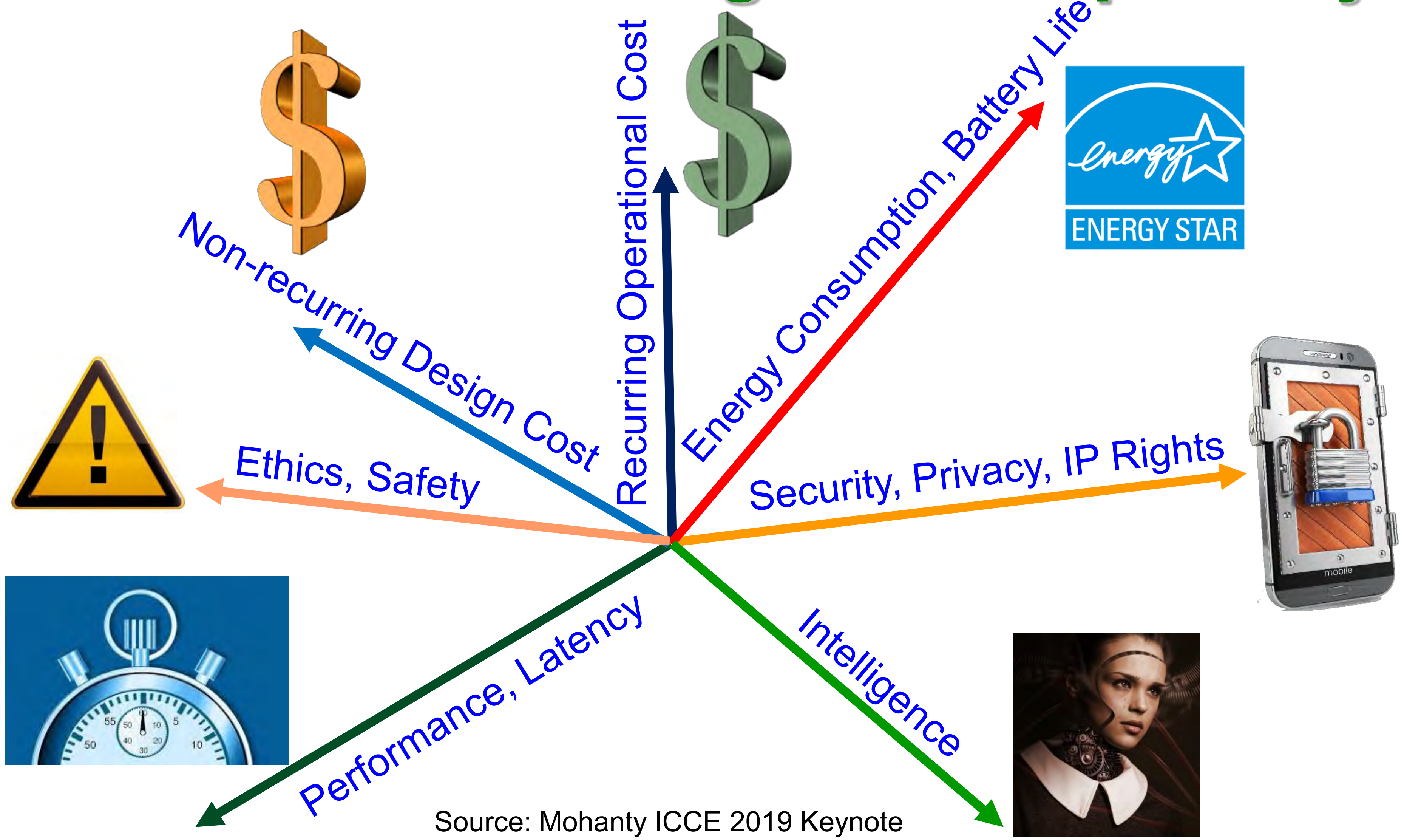
- Ultra-Fast quantum computing resources
- High latency in network
- Breaks every encryption in no time

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

Security-by-Design (SbD) – The Principle



IoT/CPS Design – Multiple Objectives



Smart Cities
Vs
Smart Villages

Source: Mohanty ICCE 2019 Keynote

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

1995
Privacy by Design (PbD)

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

2018
General Data Protection Regulation (GDPR)

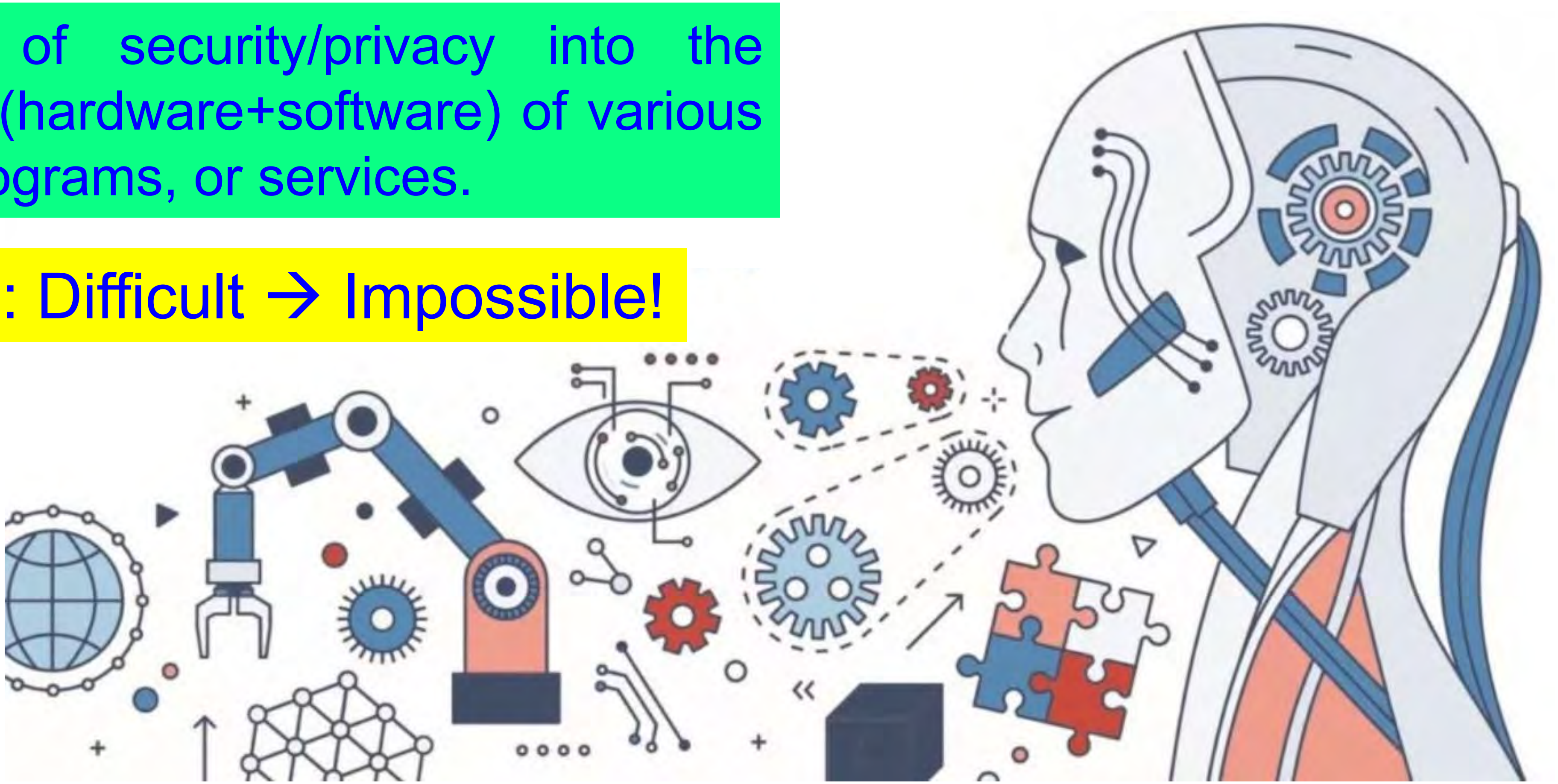
- GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

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

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

Retrofitting: Difficult → Impossible!



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

Security by Design (SbD) 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.

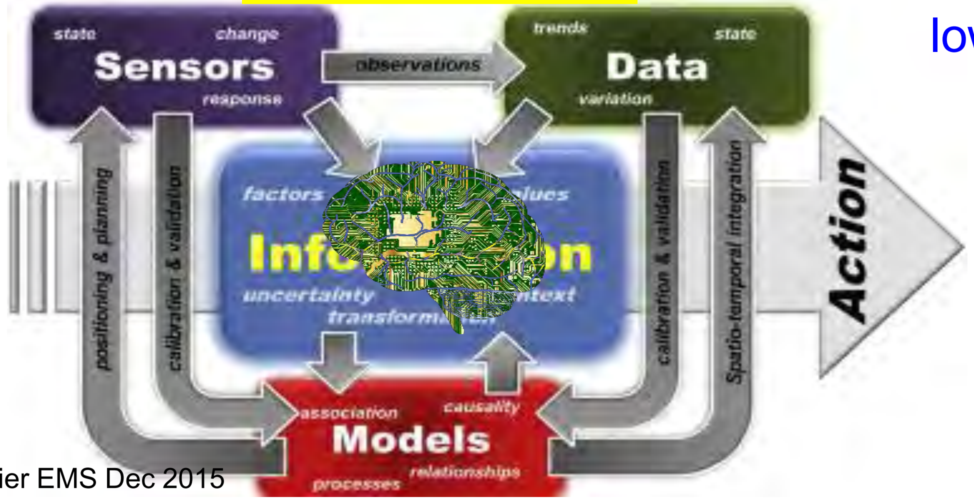
Cybersecurity

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



Source: Reis, et al. Elsevier EMS Dec 2015

Accurate sensing, analytics, and fast actuation.

Source: Mohanty iSES 2018 Keynote

Hardware-Assisted Security (HAS)

- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
  - Software based security approaches that rely on some form of encryption can’t be full proof as breaking them is just matter of time.
  - It is projected that quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security (HAS): Security/Protection provided by the hardware: for information being processed by an electronic system, for hardware itself, and/or for the system.

Hardware-Assisted Security (HAS)

- Hardware-Assisted Security: Security provided by hardware for:
  (1) information being processed,
  (2) hardware itself,
  (3) overall system
- Additional hardware components used for cybersecurity.
- Hardware design modification is performed.
- System design modification is performed.

Privacy by Design (PbD)

Security/Secure by Design (SbD)

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

Bluetooth Hardware Security

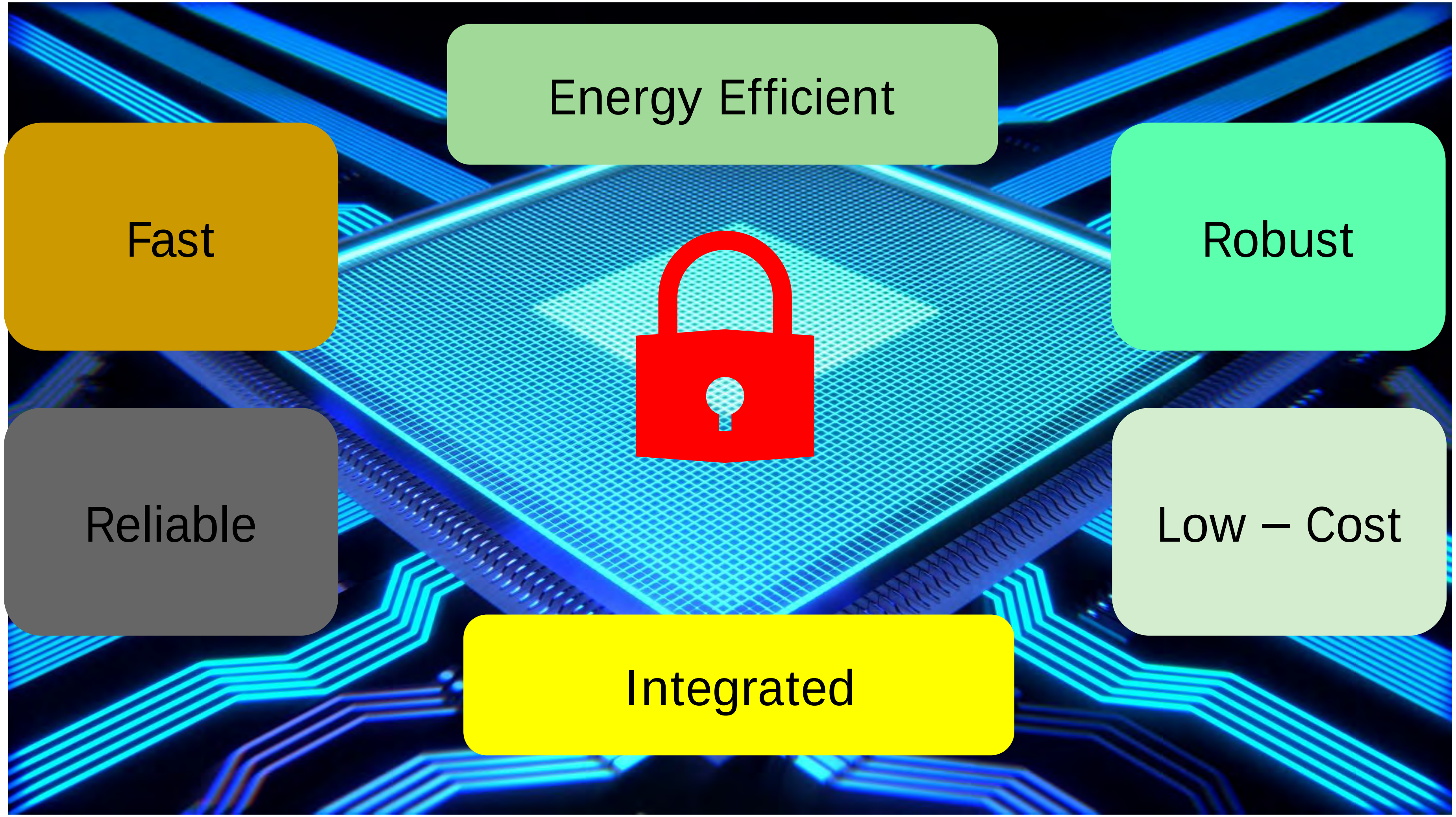
Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

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

Hardware Assisted Security (HAS)



Secure SoC Design: Alternatives

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

Secure SoC - Alternatives

- Development of hardware amenable algorithms.
- Building efficient VLSI architectures.
- Hardware-software co-design for security, power, and performance tradeoffs.
- SoC design for cybersecurity, power, and performance tradeoffs.

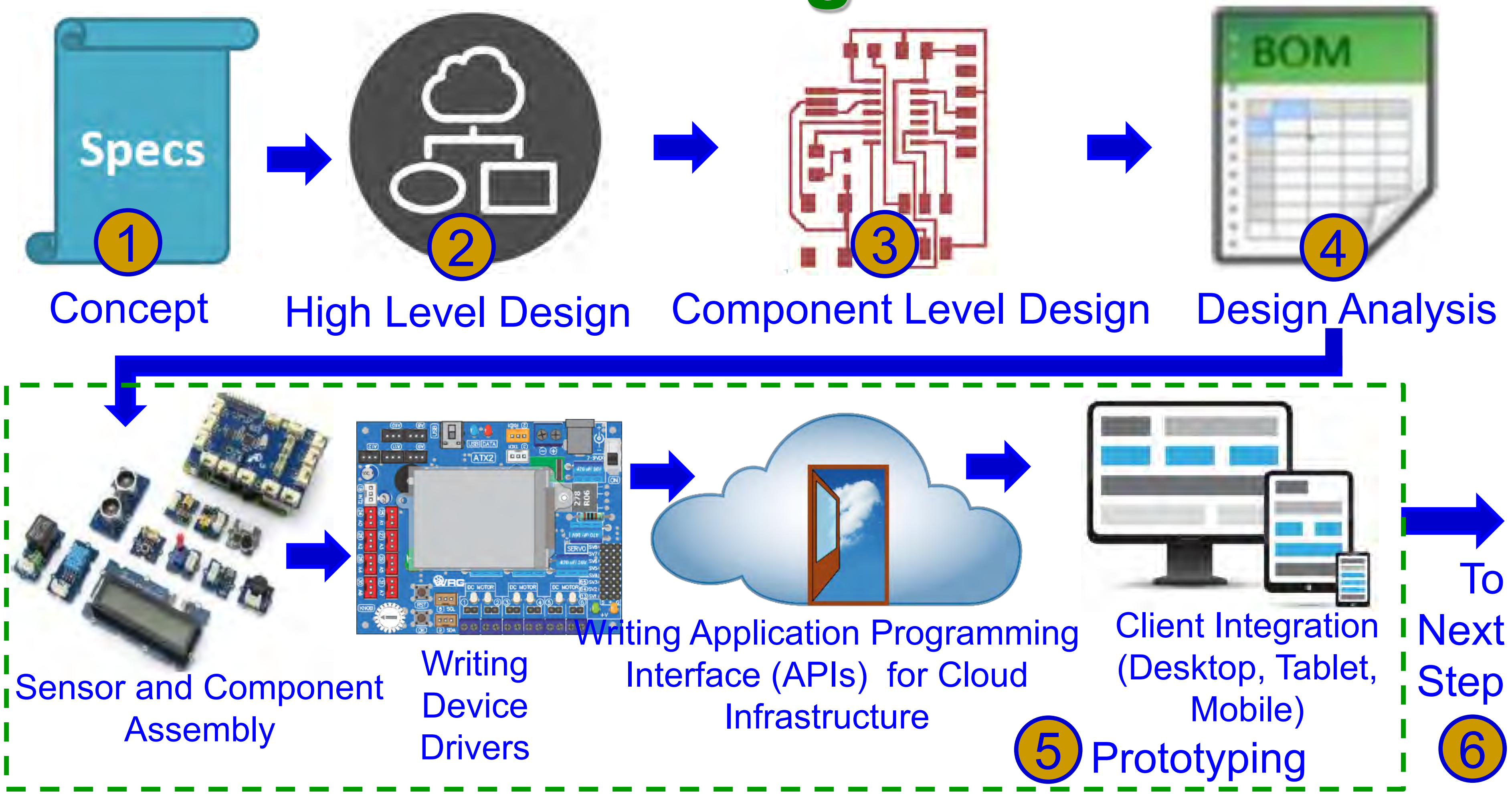
Secure SoC: Different Design Alternatives

- New CMOS sensor with security.
- New data converters with security.
- Independent security and AI processing cores.
- New instruction set architecture for RISC to support security at micro-architecture level.

Trustworthy Electronic System

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

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%20%20IoT%20Solution%20-%20Shivakumar%20Mathapathi.pdf

IoT – Design Flow

6 Field Testing

7 Release of Beta Version

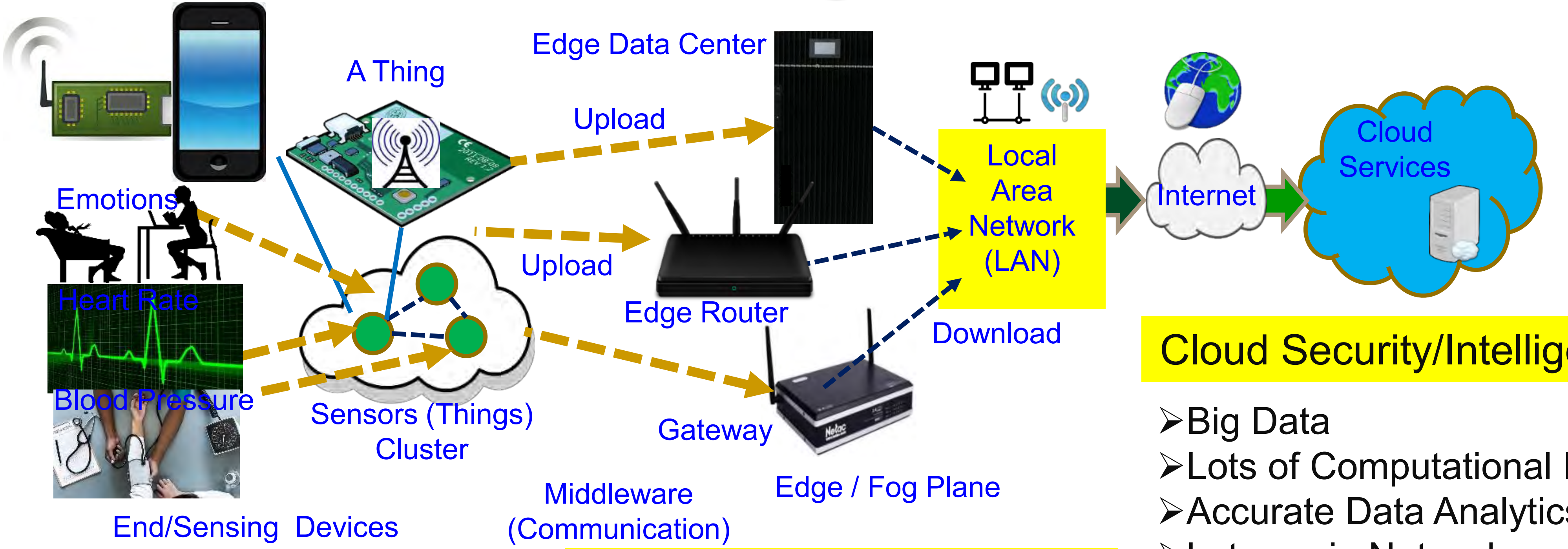
8 Production

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



Cloud Security/Intelligence

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

End Security/Intelligence

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

Edge Security/Intelligence

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

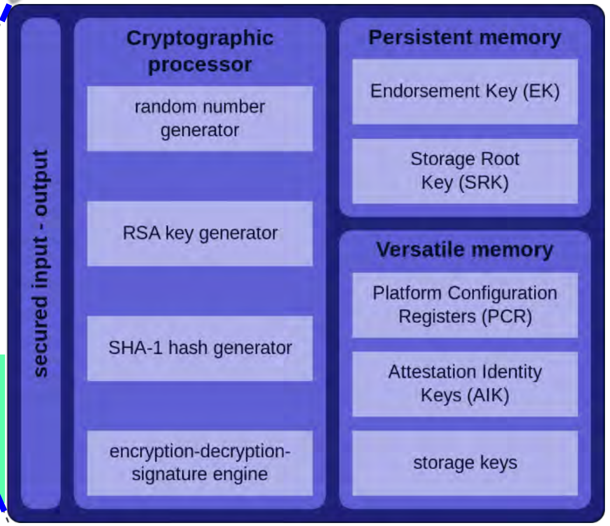
Heavy-Duty ML is more suitable for smart cities

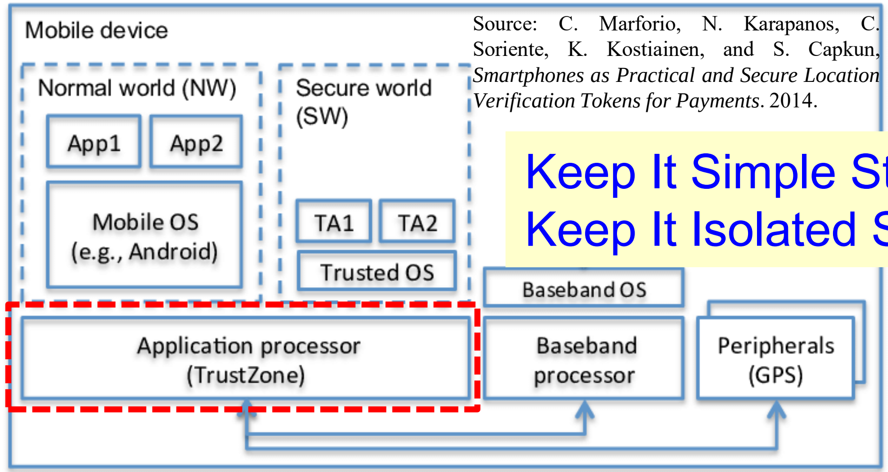
TinyML at End and/or Edge is key for smart villages.

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

Hardware Security Module (HSM)

Trusted Platform Module (TPM)





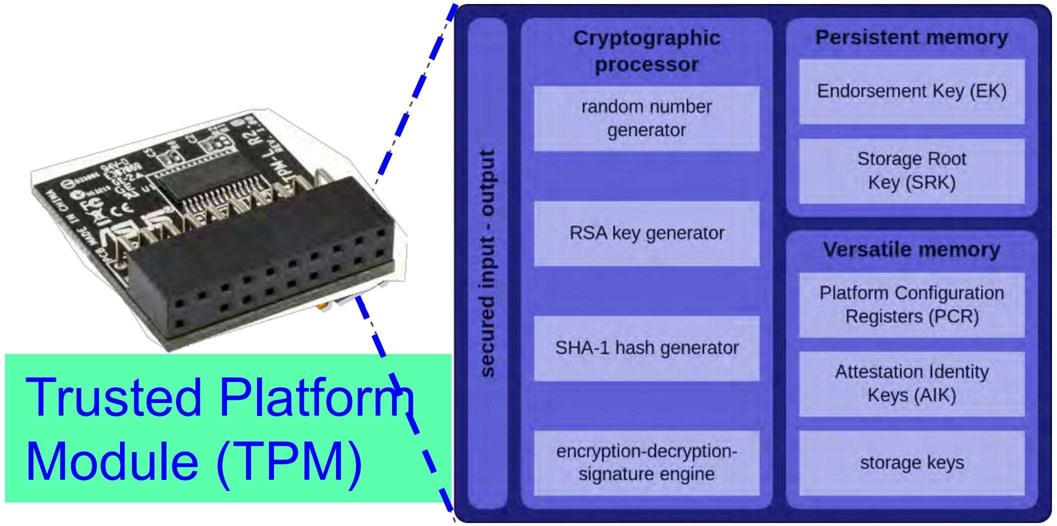
Source: C. Marforio, N. Karapanos, C. Soriente, K. Kostiainen, and S. Capkun, *Smartphones as Practical and Secure Location Verification Tokens for Payments*. 2014.

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

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

PUF versus TPM



Trusted Platform Module (TPM)

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

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

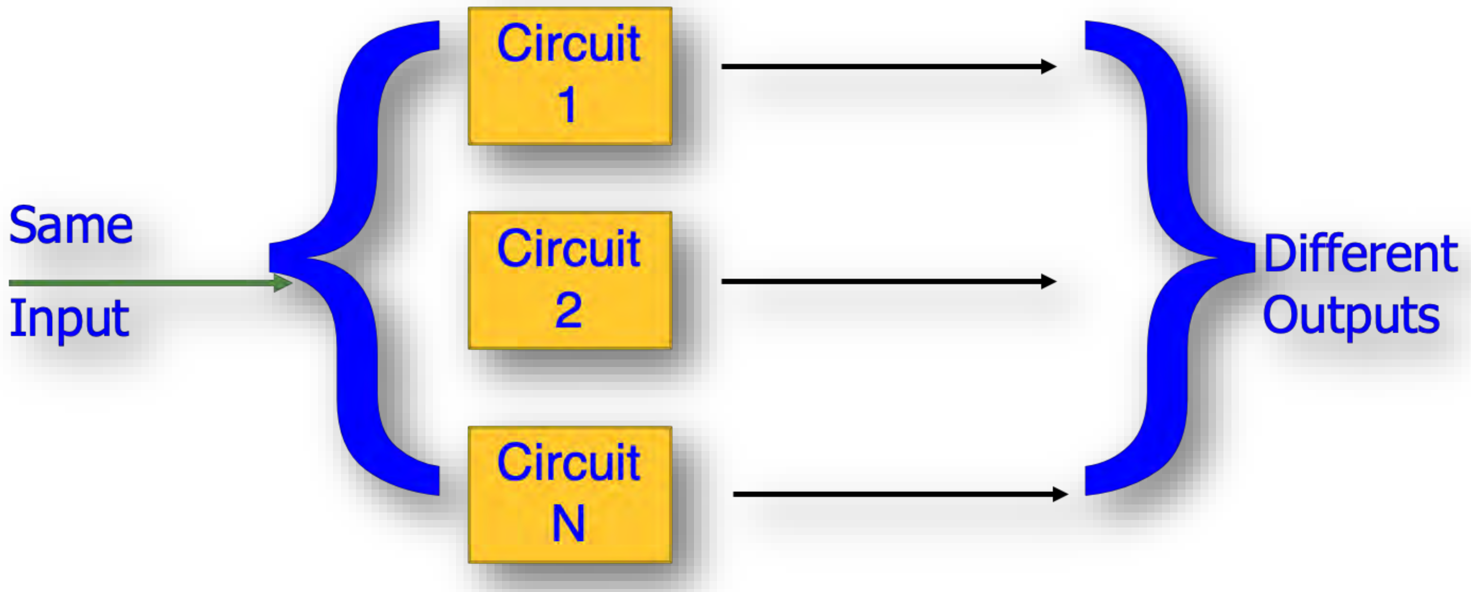
PUF:
1) Based on a physical system
2) Generates random output values

Why PUFs?

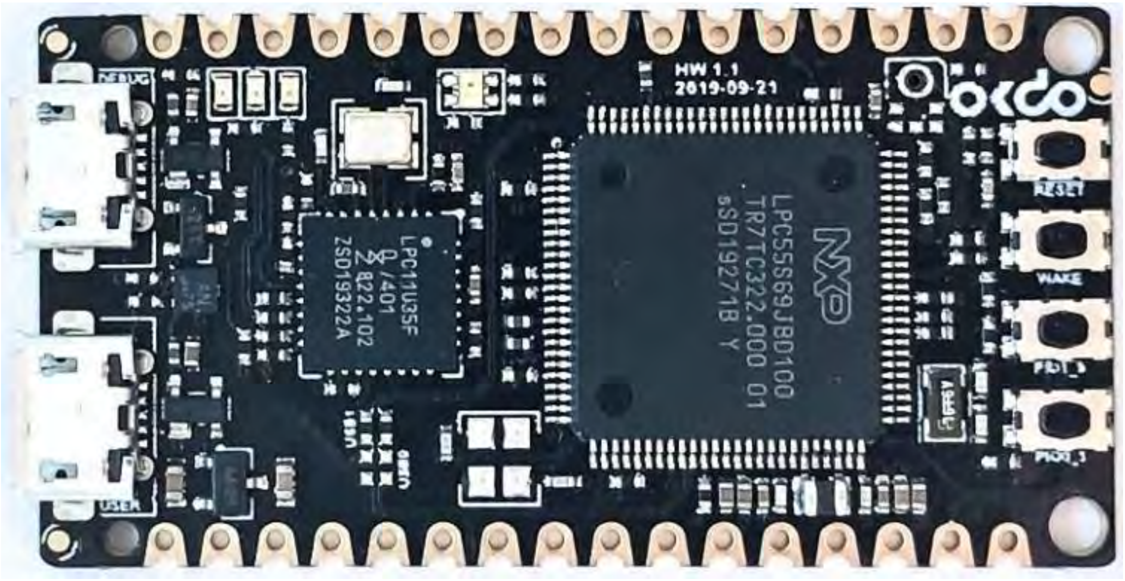
- Hardware-assisted security.
- Key not stored in memory.
- Not possible to generate the same key on another module.
- Robust and low power consuming.
- Can use different architectures with different designs.

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.

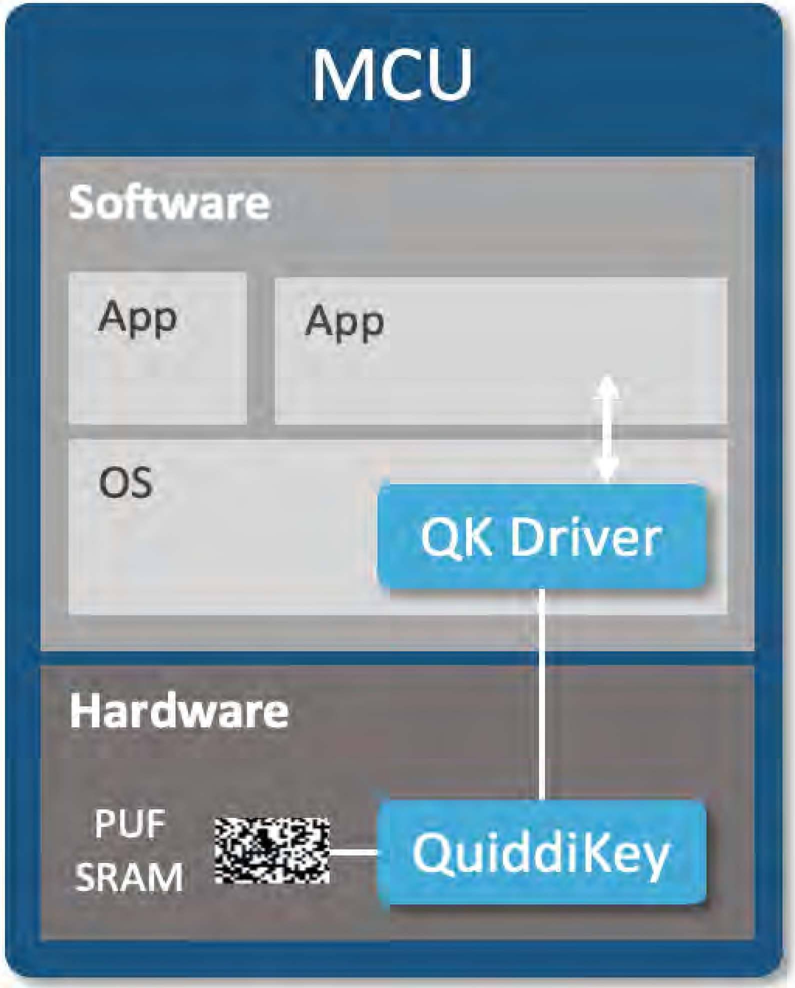


PUF Hardware Modules



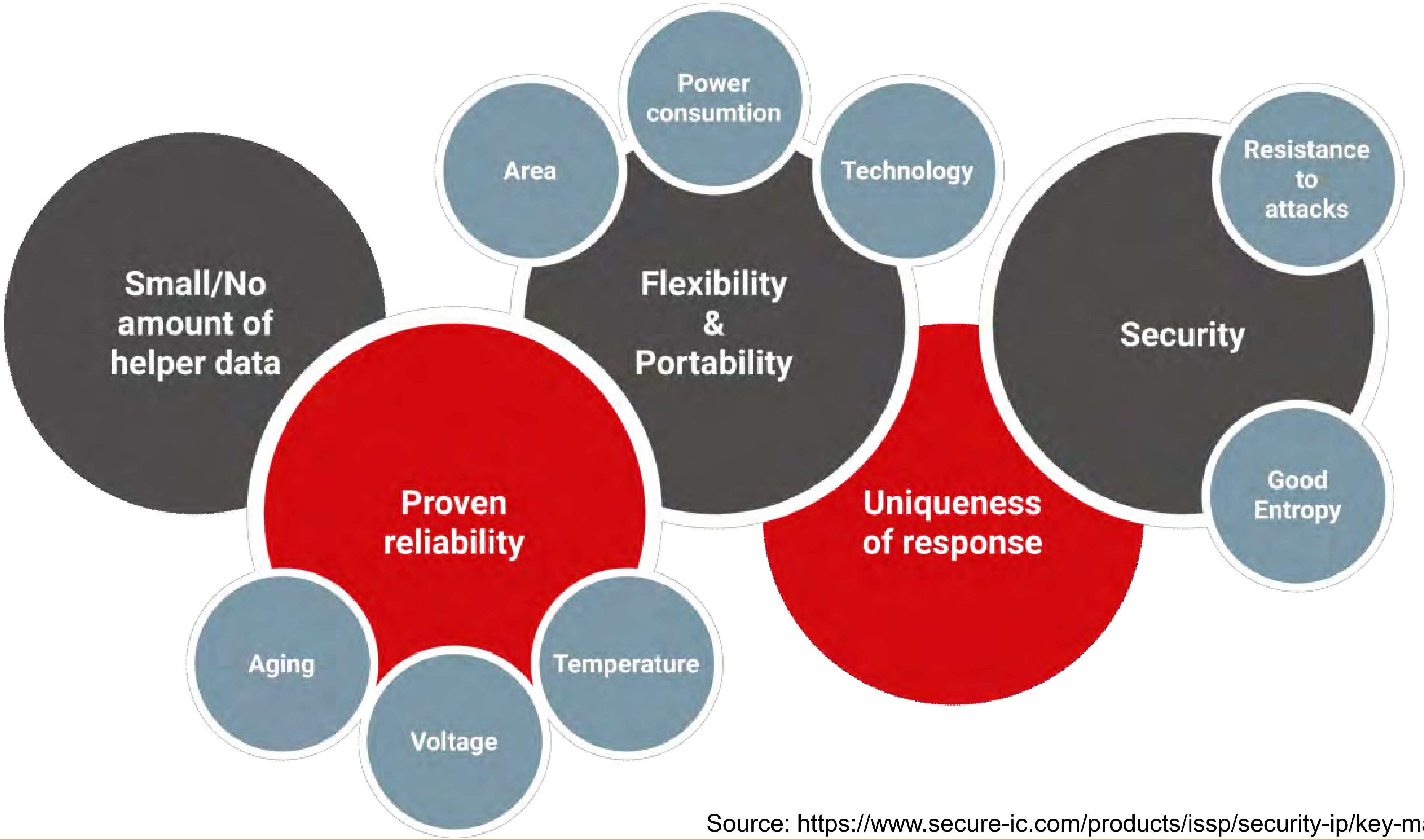
Source: https://asvin.io/physically-unclonable-function-setup/

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



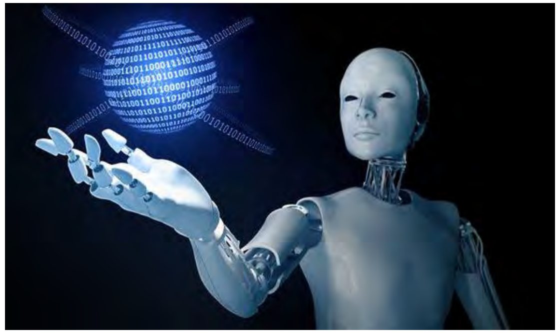
Source: https://www.intrinsic-id.com/products/quiddikey/

PUF: Advantages

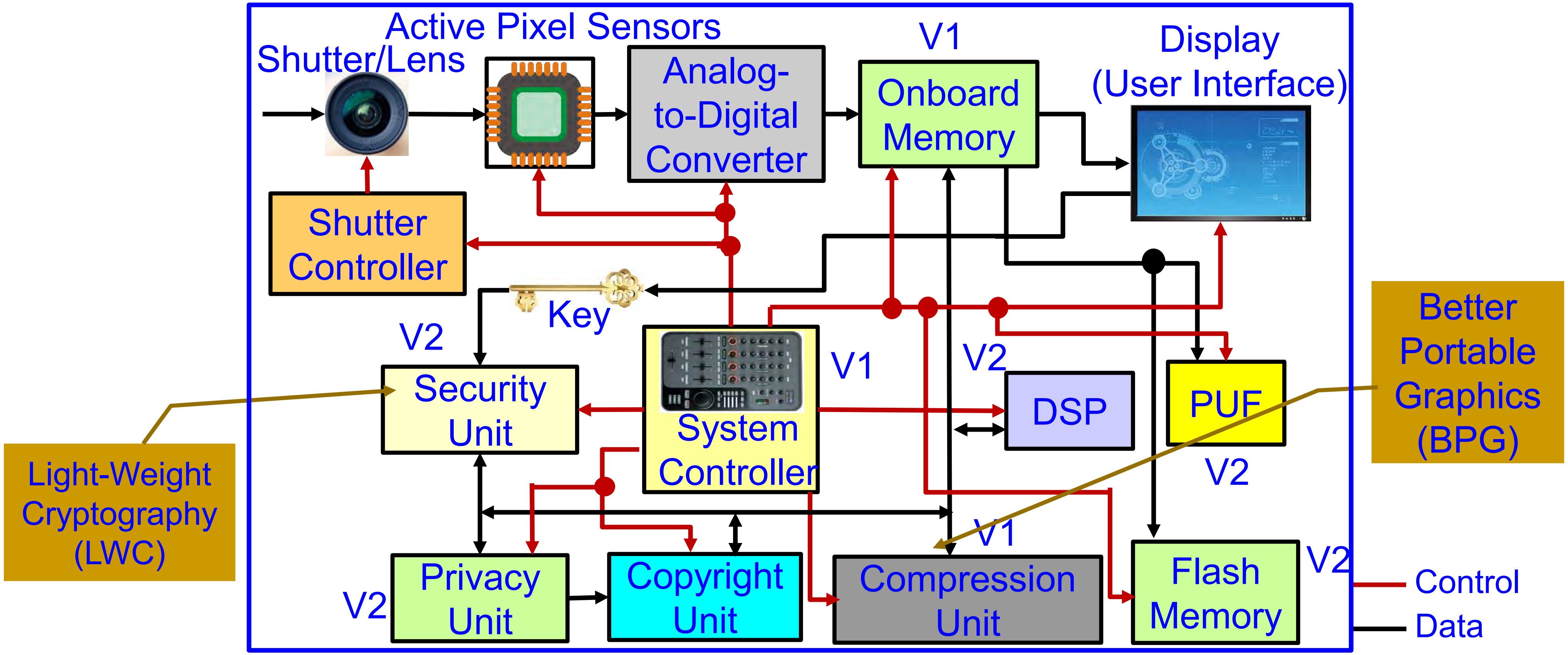


Source: https://www.secure-ic.com/products/issp/security-ip/key-management/puf-ip/

Security-by-Design (SbD) – Specific Examples



Secure Digital Camera (SDC) – My Invention

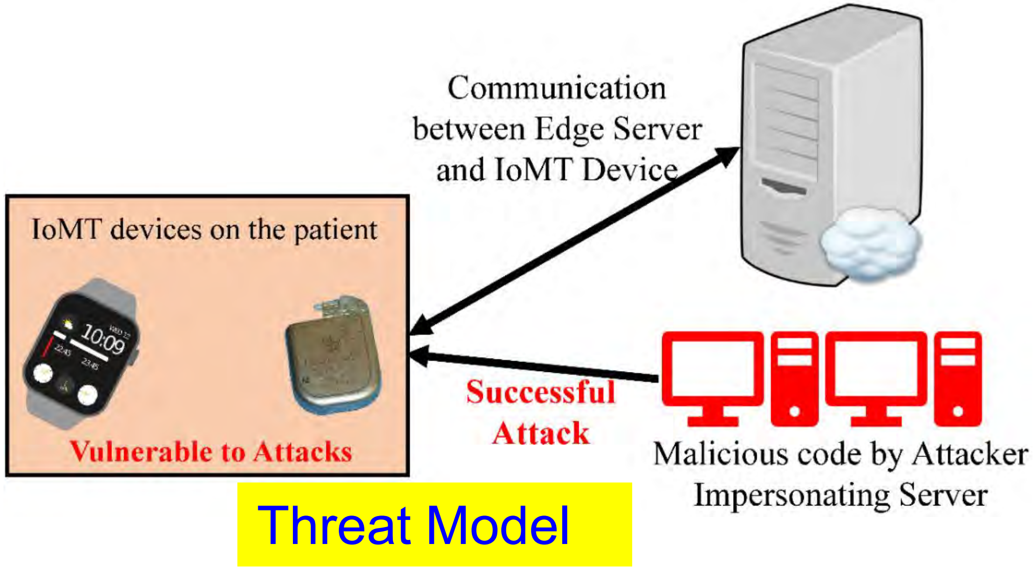


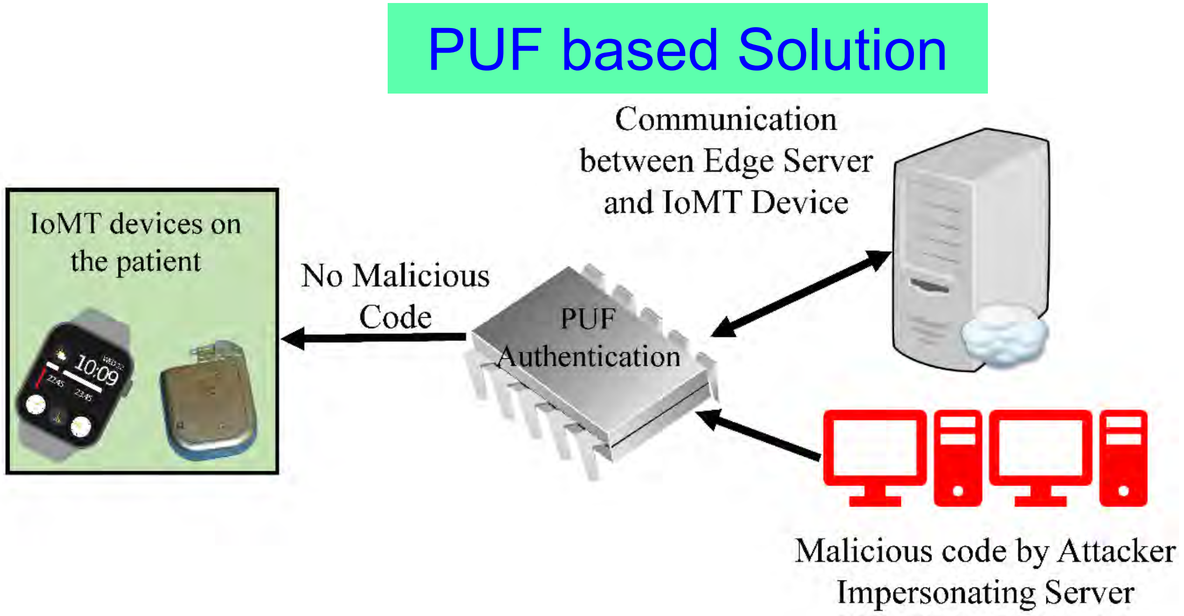
Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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

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

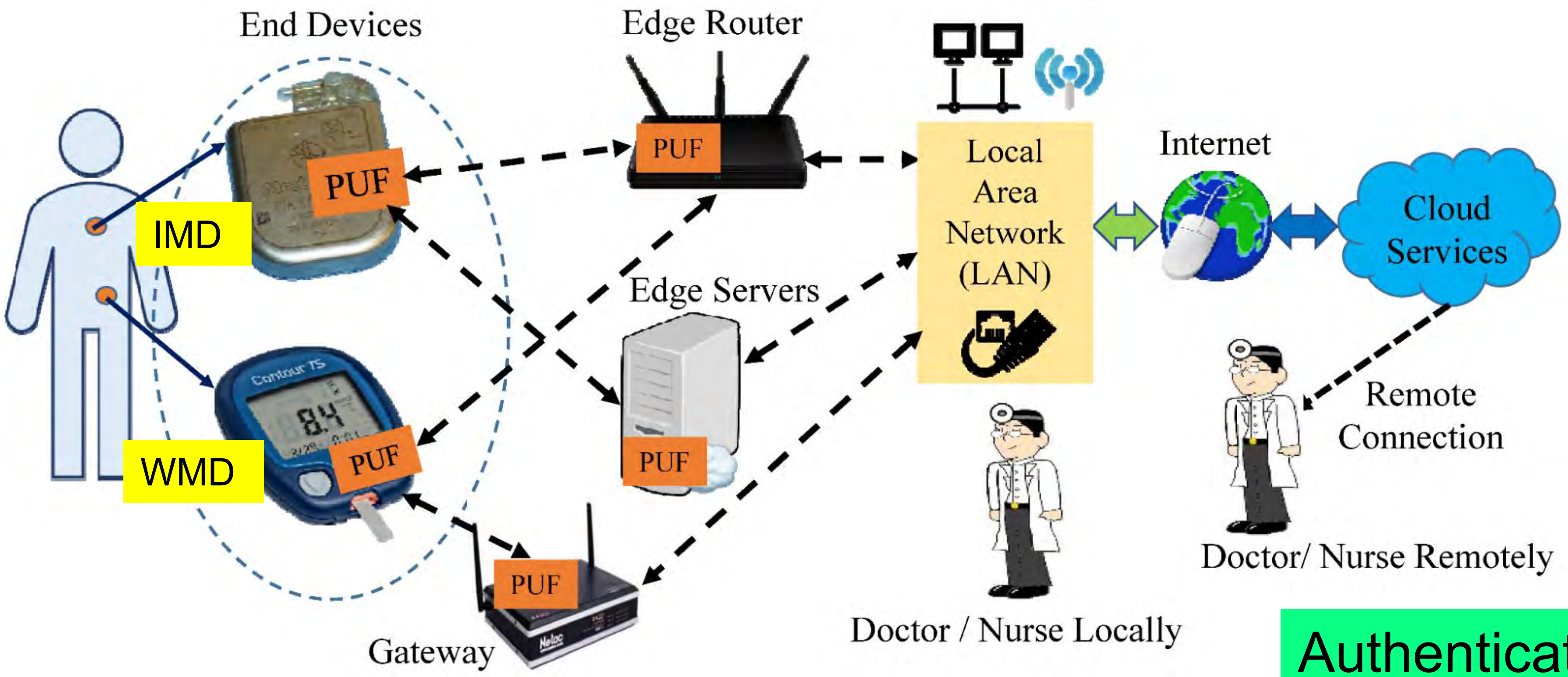
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS





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

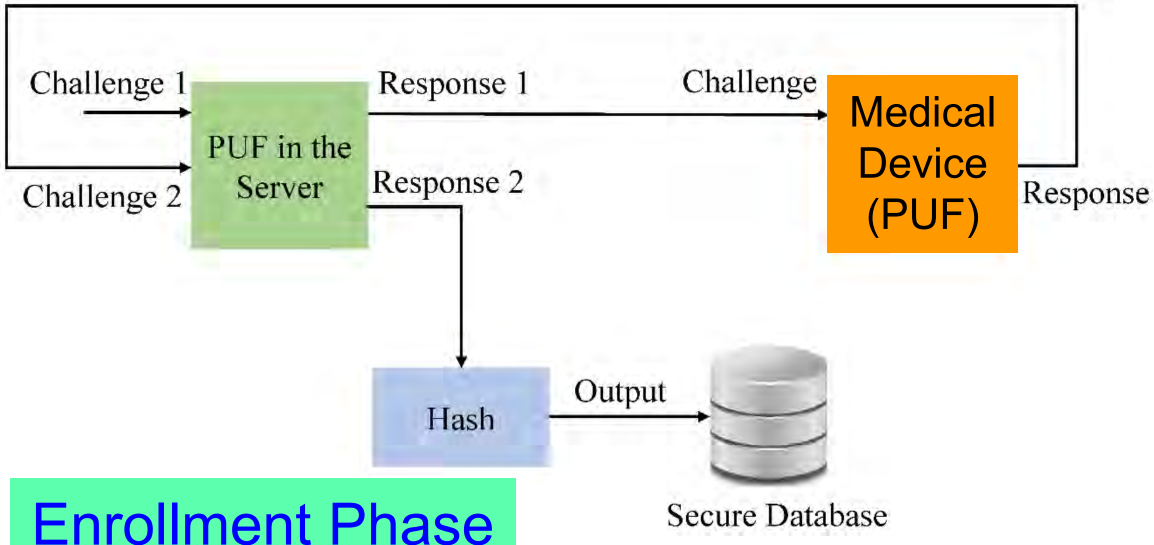
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

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

IoMT Security – Our Proposed PMsec

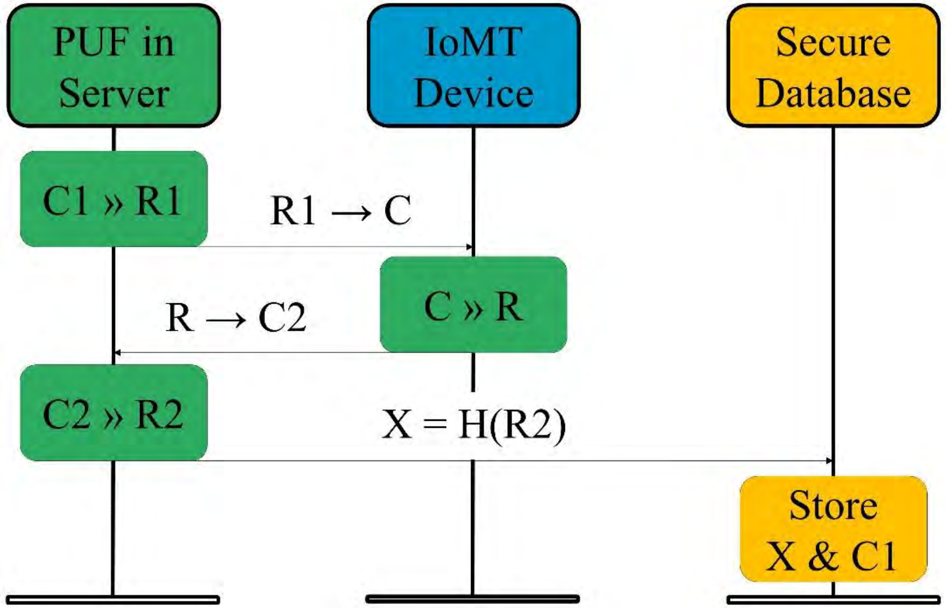


Enrollment Phase

At the Doctor

- When a new IoMT-Device comes for an User

Device Registration Procedure

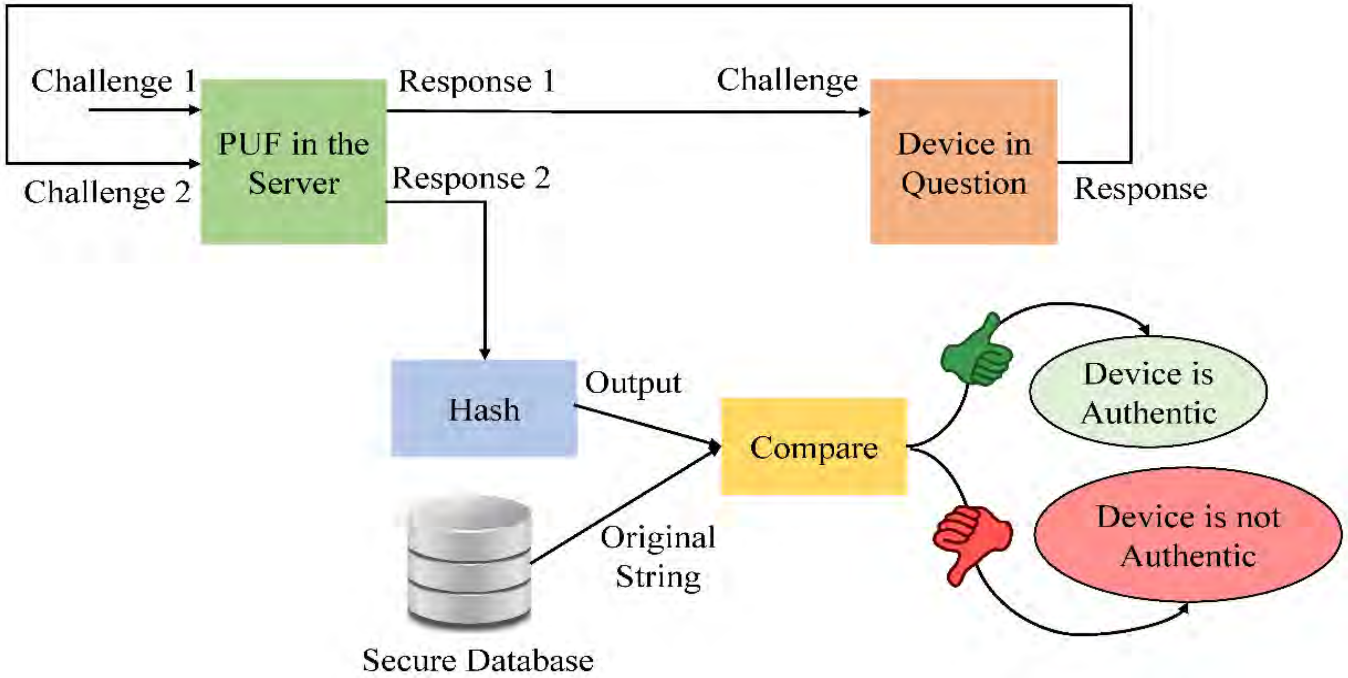


PUF Security Full Proof:

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

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

IoMT Security – Our Proposed PMsec

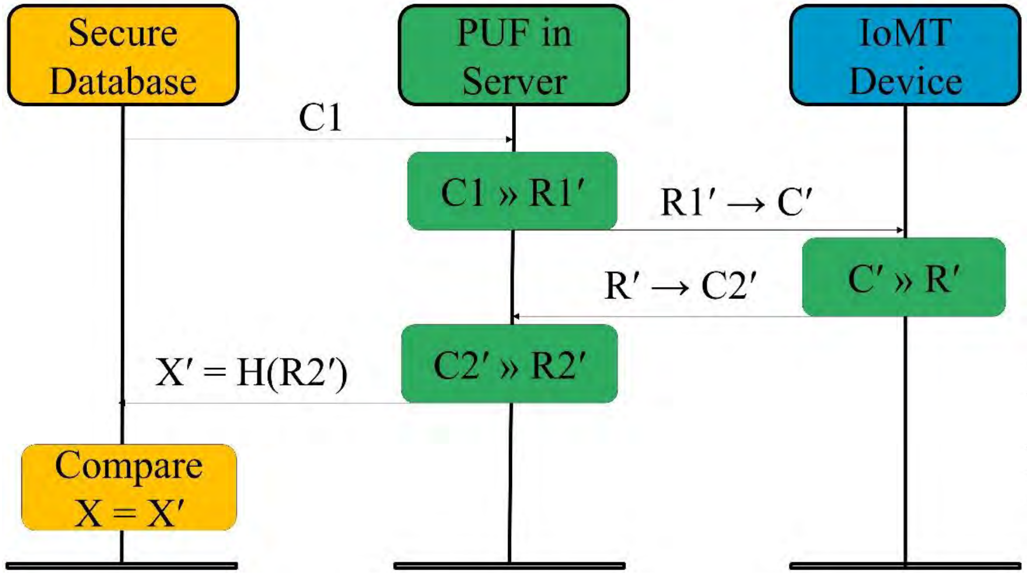


Authentication Phase

At the Doctor

- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



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

IoMT Security – Our PMsec in Action

```
------------Enrollment Phase------------
Generating the Keys
Sending the keys to the Client
Receiving the Keys from the client
Saving the database
>>>
```

Output from IoMT-Server during Enrollment

Output from the IoMT-Device

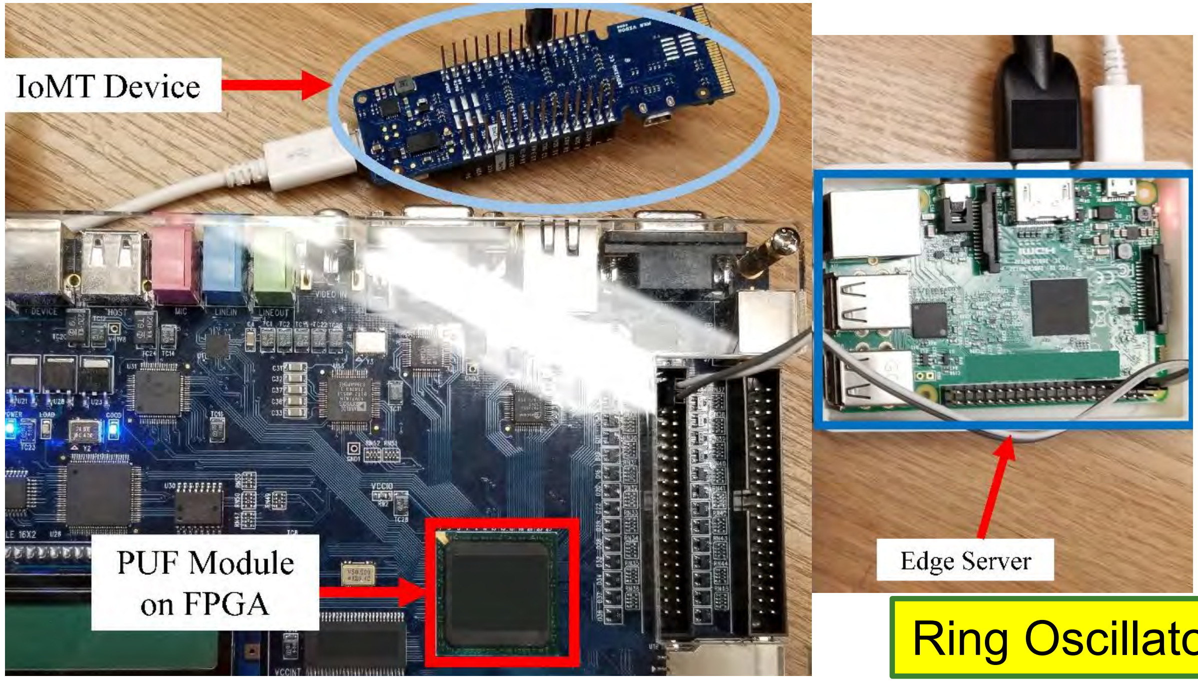
```
COM4
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 1011100001011100101111000101111000101101001101110010100101000011
Sending key for authentication
```

```
>>>
Hello
------------Authentication Phase------------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  1011100001011100101111000101111000101101001101110010100101000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>>
```

Output from IoMT-Server during Authentication

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

IoMT Security – Our Proposed PMsec



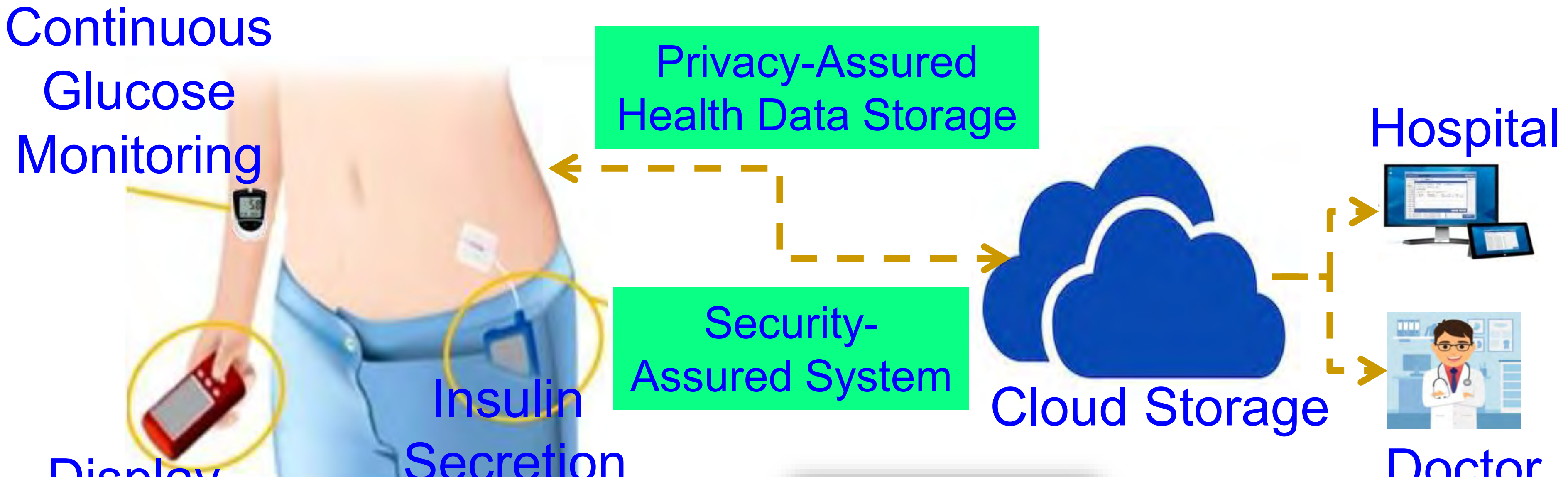
Average Power Overhead – 200 μW

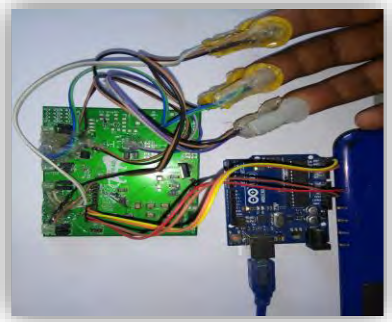
Ring Oscillator PUF – 64-bit, 128-bit, …

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

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

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

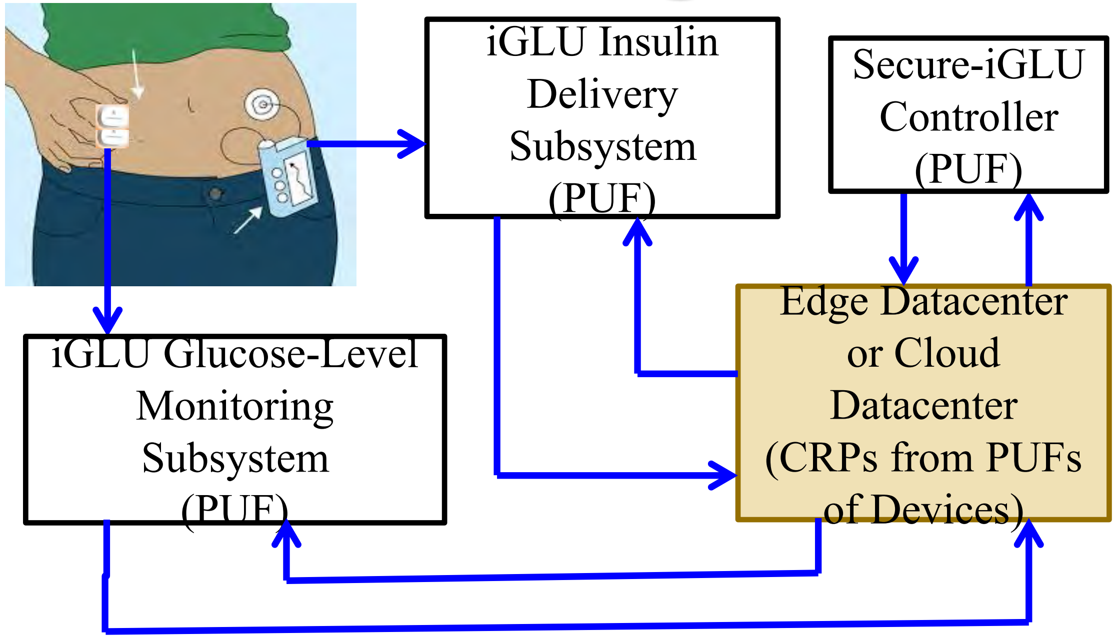




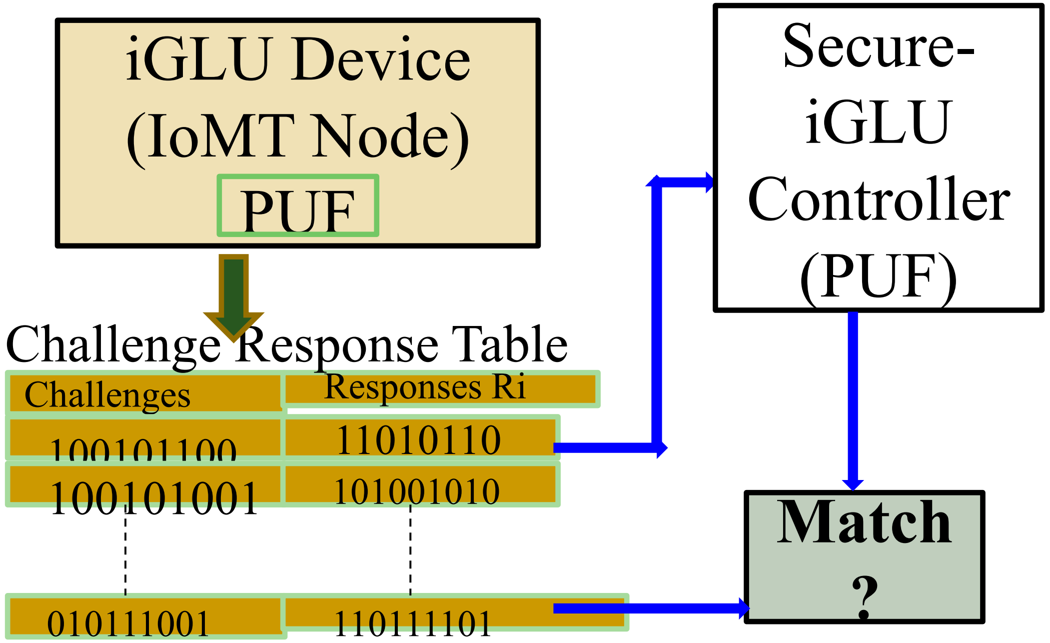
Near Infrared (NIR) based Noninvasive, Accurate, Continuous Glucose Monitoring

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

Secure-iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery



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

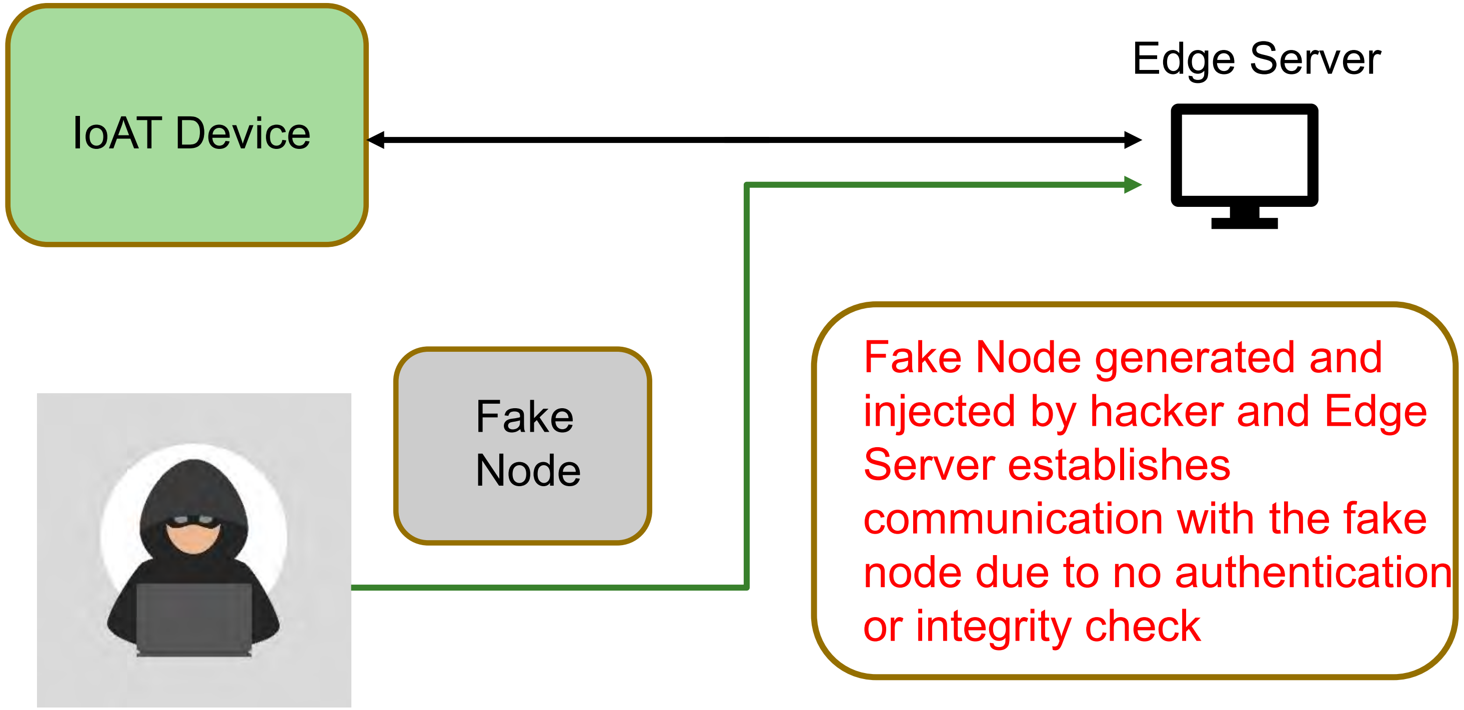


Source: A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

Smart Agriculture Cybersecurity - Solutions

- Developing a cloud centric network model
- Using Intrusion detection systems
- Blockchain based solutions for data and device integrity
- Physical countermeasures
  - Machine learning based countermeasures
- Constant security analysis

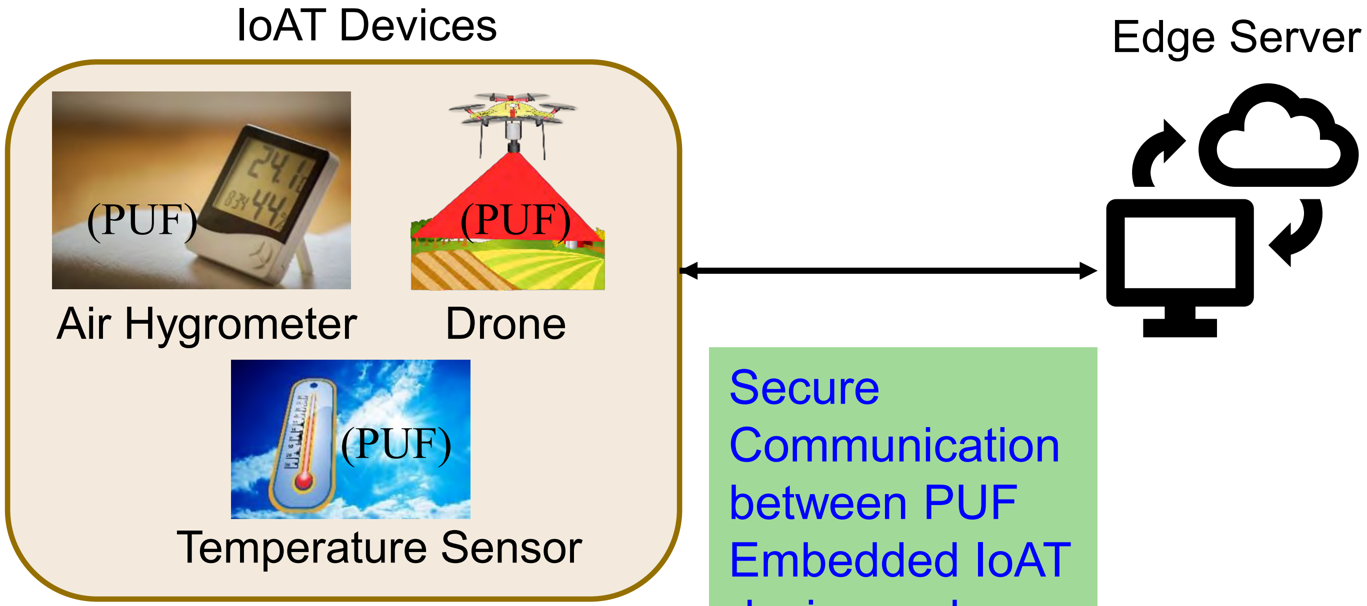
Smart Agriculture - Threat Model



Malicious Node Generation and replacement

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

Secure Design Approach for Robust IoAT

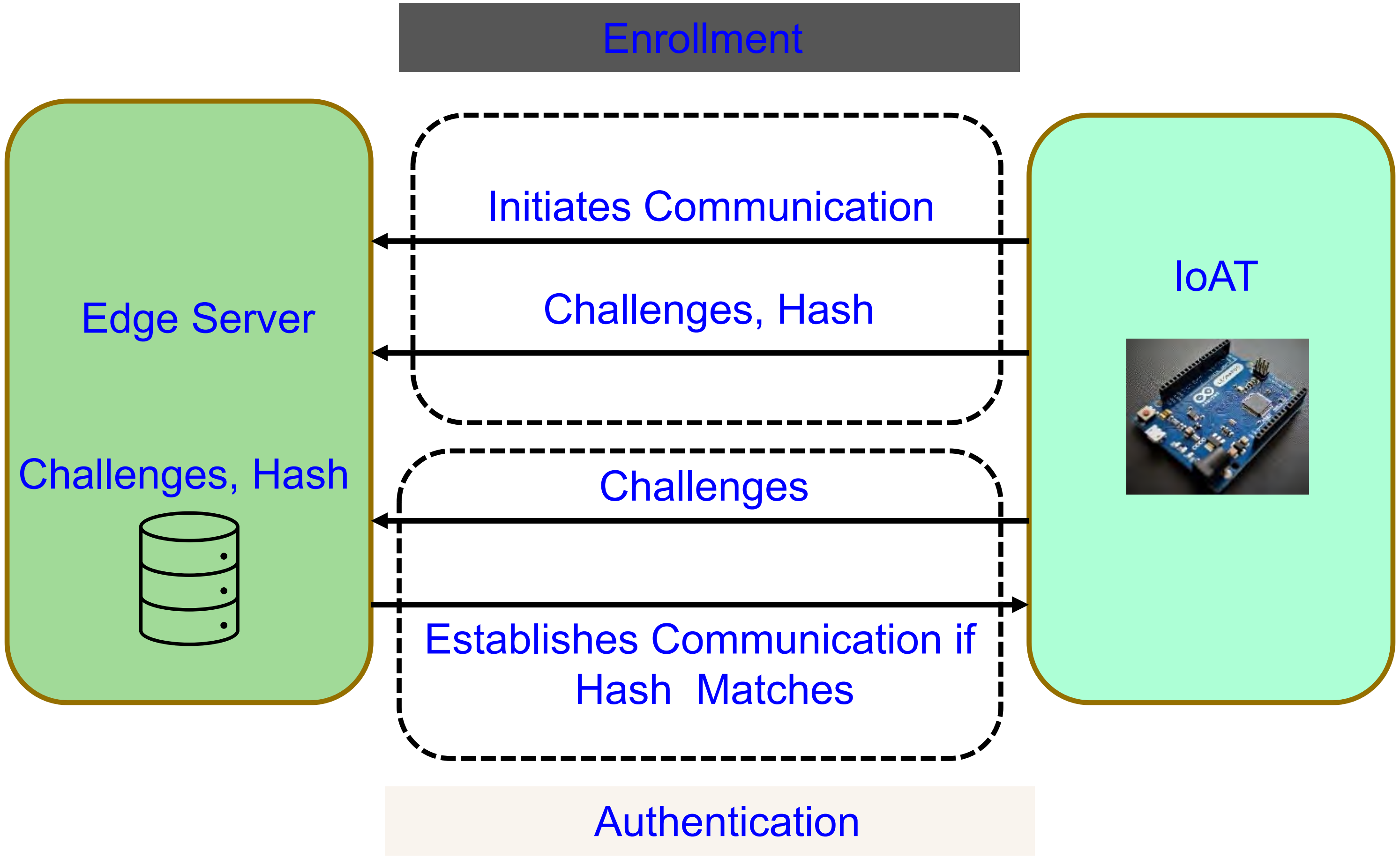


Secure Communication between PUF Embedded IoAT device and Edge Server

Edge Server authenticates the devices using the PUF key of each electronic device which is the fingerprint for that device

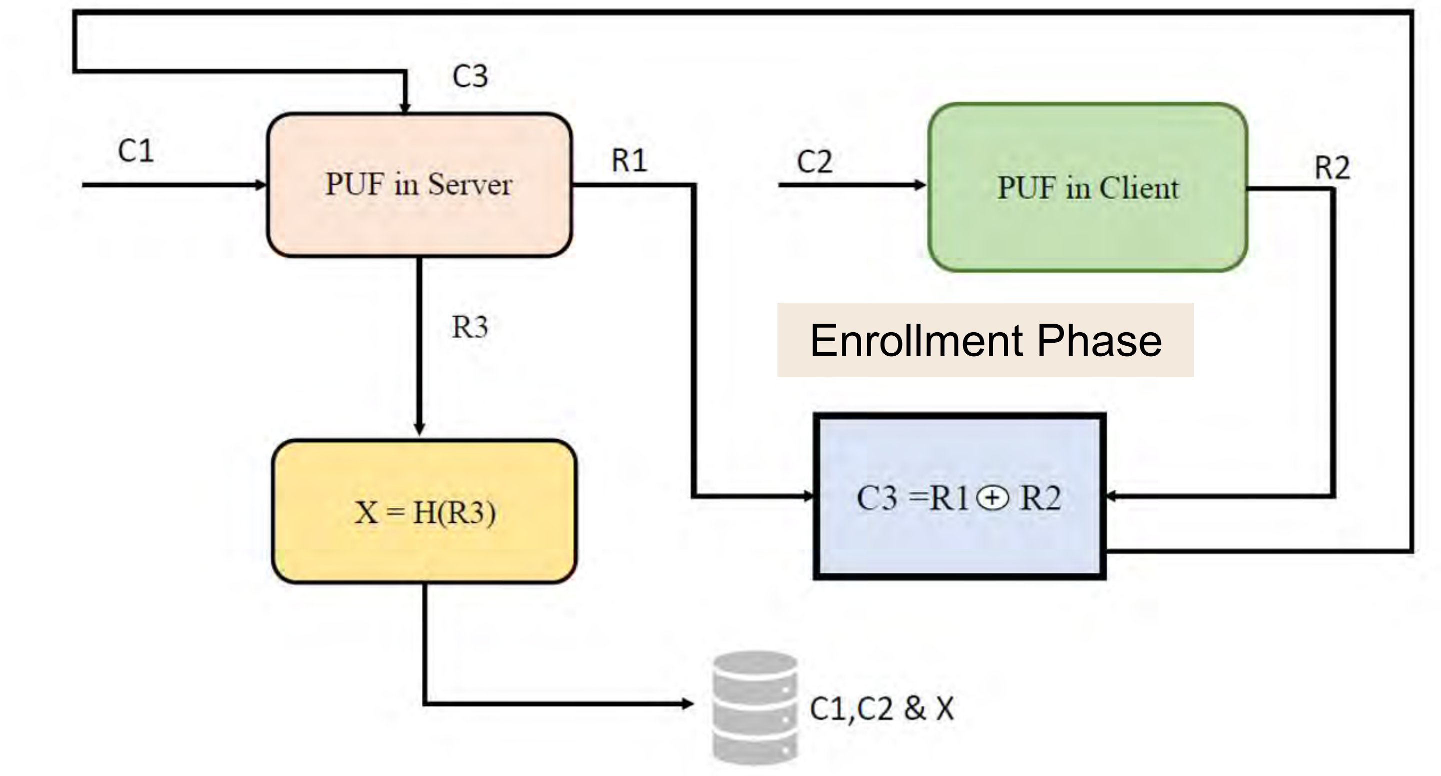
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Authentication Process for IoAT



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

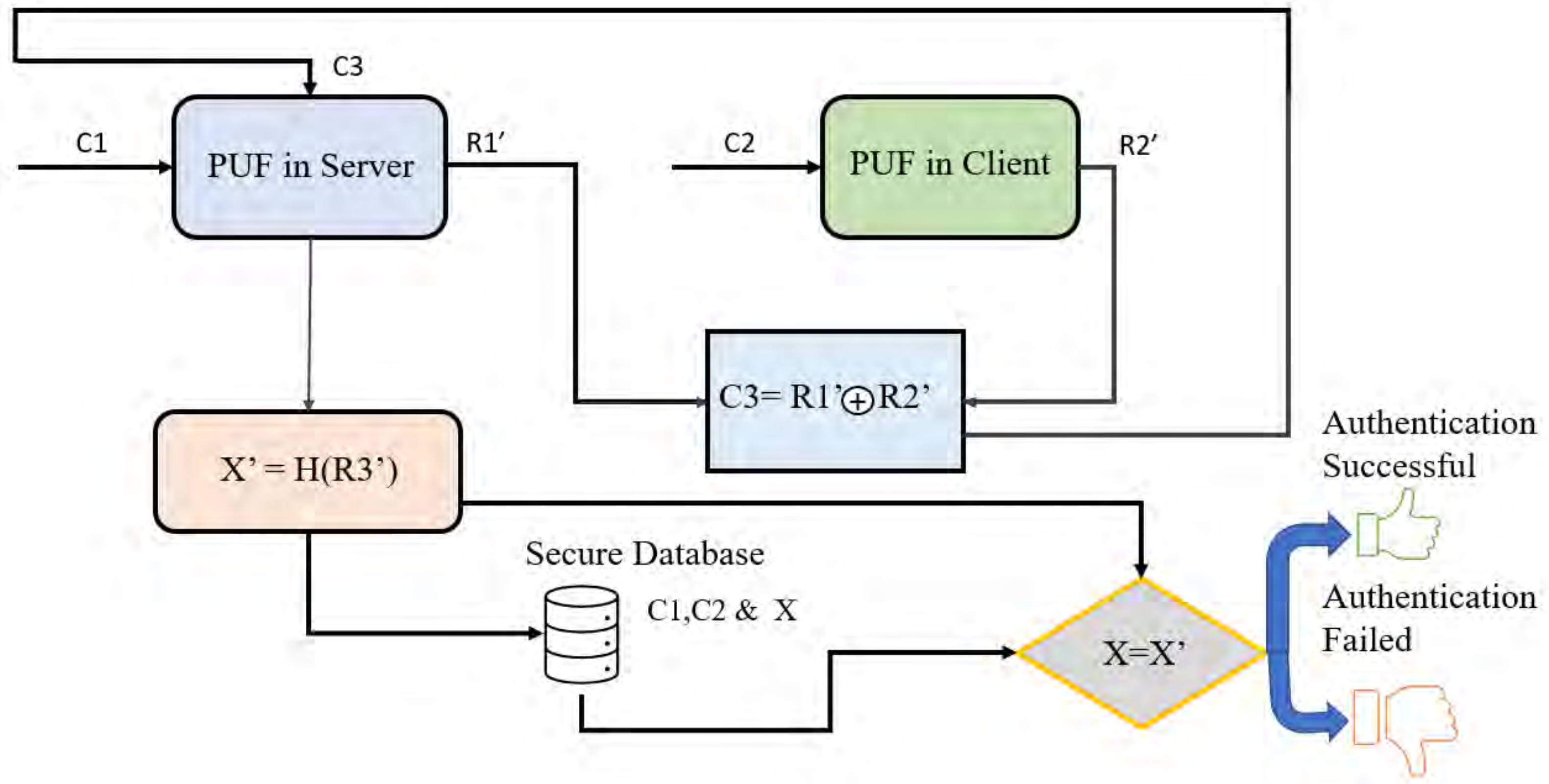
Enrollment Phase of the Proposed Security Protocol



C1 => R1
C2 => R2
C3 = R1 XOR R2
C3 => R3
X = H(R3)
X, C1,C2 are stored in Database

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

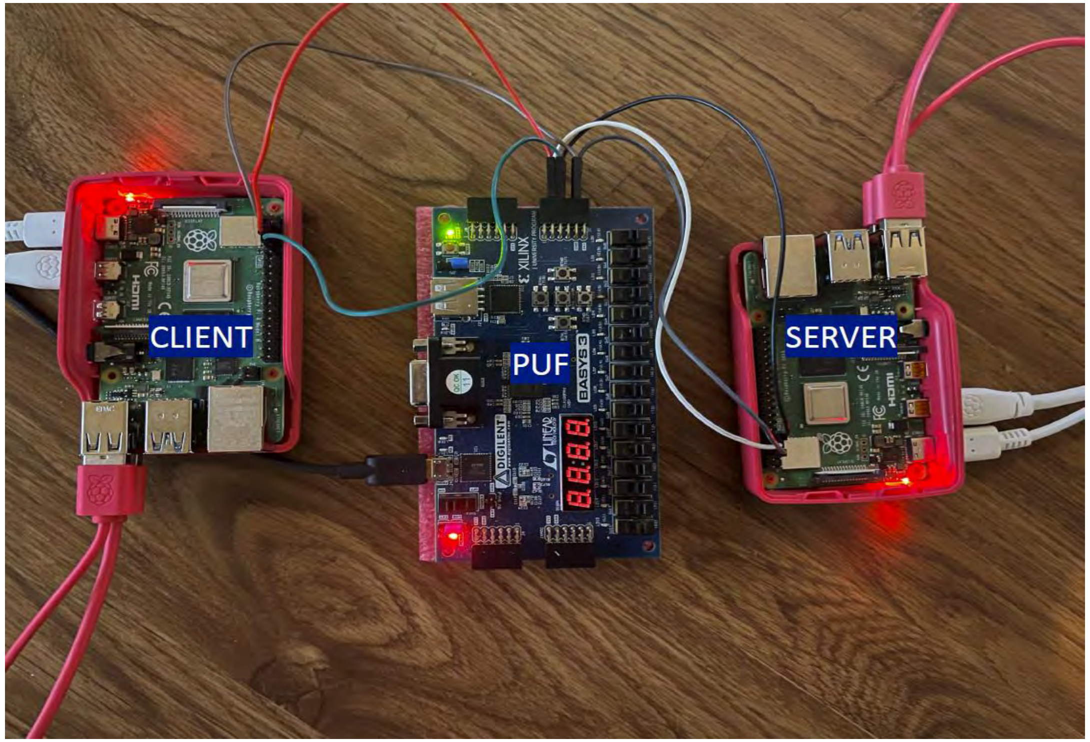
Authentication Phase of the Proposed Security Protocol



Only C1 and C2 are retrieved and given as inputs to the PUF module. The final Hash value X is compared with the stored hash value X to authenticate the device

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

Prototype of the Proposed Security Scheme



Parameter	Value
Hamming Distance	48%
Randomness	41.07%
Time Taken to Authenticate the Device in Seconds	0.16 to 2.93 Seconds
FPGA	Basys 3, Artix-7

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

Experimental Results

```
Python 3.7.3 (/usr/bin/python3)
>>> %Run server1pufauthenticatio.py
 The Server Challenge input
 [39, 33, 33, 81, 83, 82, 62, 61]
 The Server PUF Key
 1100111100000111000001110000011100000111000001110000011100000111
 Client PUF Key
 1001001110010011100100111001001110010011100100111001001110010011
 The XOR Output of Client and Server key
 0101110010010100100101001001010010010100100101001001010010010100
 The XOR ed Challenge input to Server
 [92, 148, 148, 148, 148, 148, 148, 148]
 The Response output from Server
 1000101010111100101111001011110010111100101111001011110010111100
 The Hash Output
 ed7f6d9edc9a6e8437f1fe386cfc2fa80815fb79a3fcb00debf96d1e843e5fa3
 Device Authenticated
 Time taken to Authenticate the Device in seconds
 2.9331398010253906
```

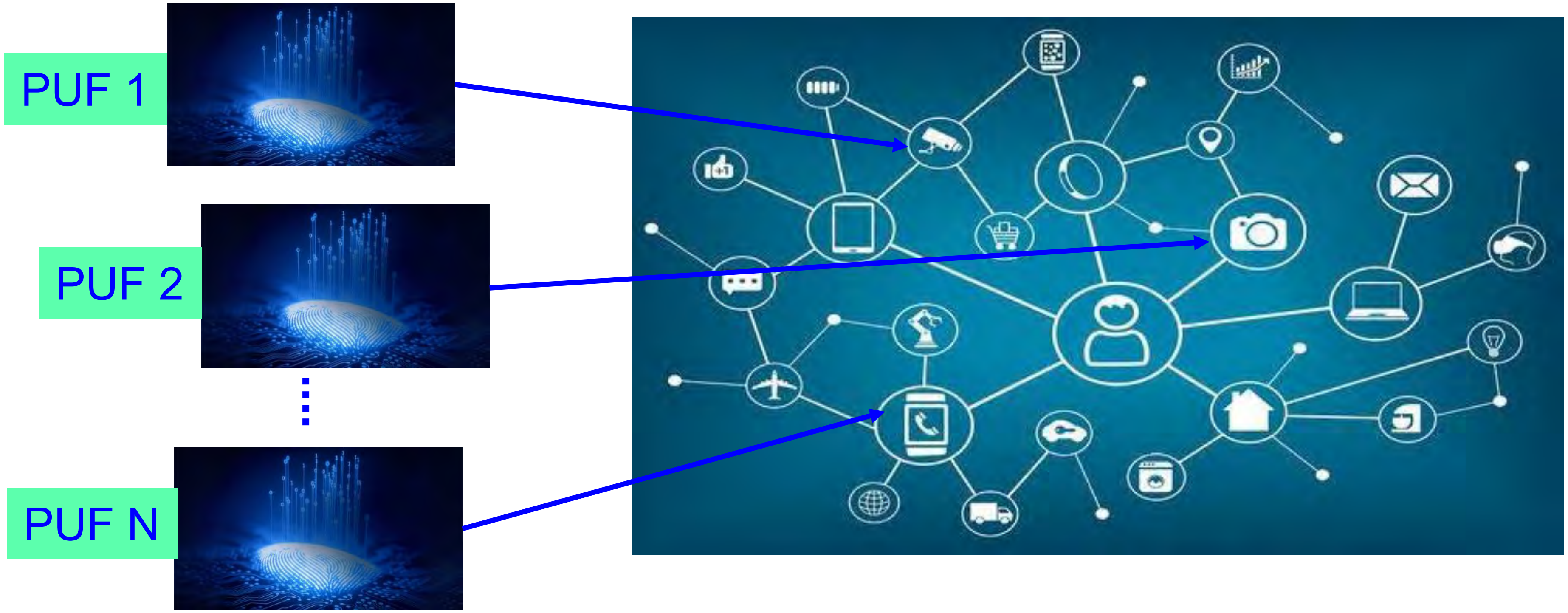
Server Output

```
Python 3.7.3 (/usr/bin/python3)
>>> %Run client_puf.py
 The Client Challenge input
 [66, 52, 17, 7, 2, 24, 89, 6]
 The Client PUF Key
 1001000110010011100100111001001110010011100100111001001110010011
 Time taken to Generate the key at Client in seconds
 0.07773900032043457
```

Client Output

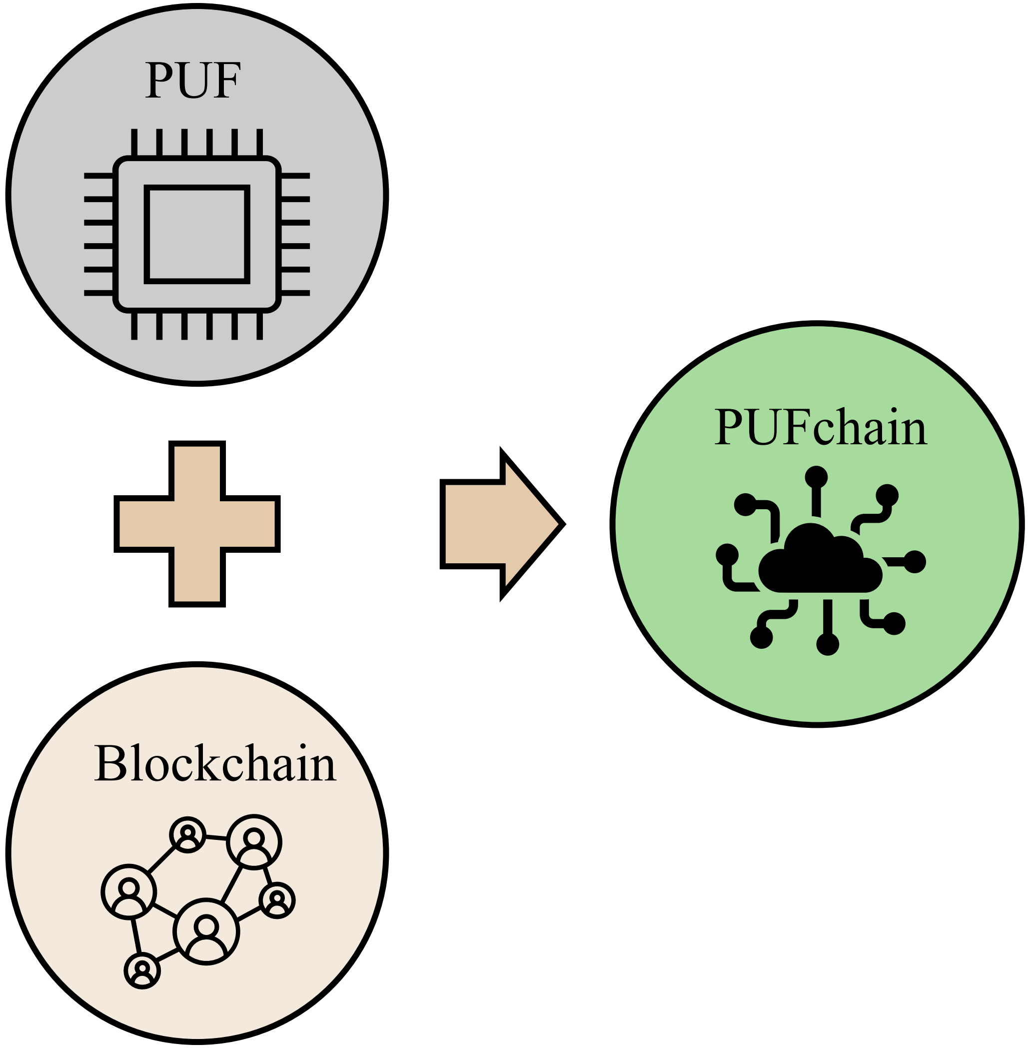
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture," in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

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



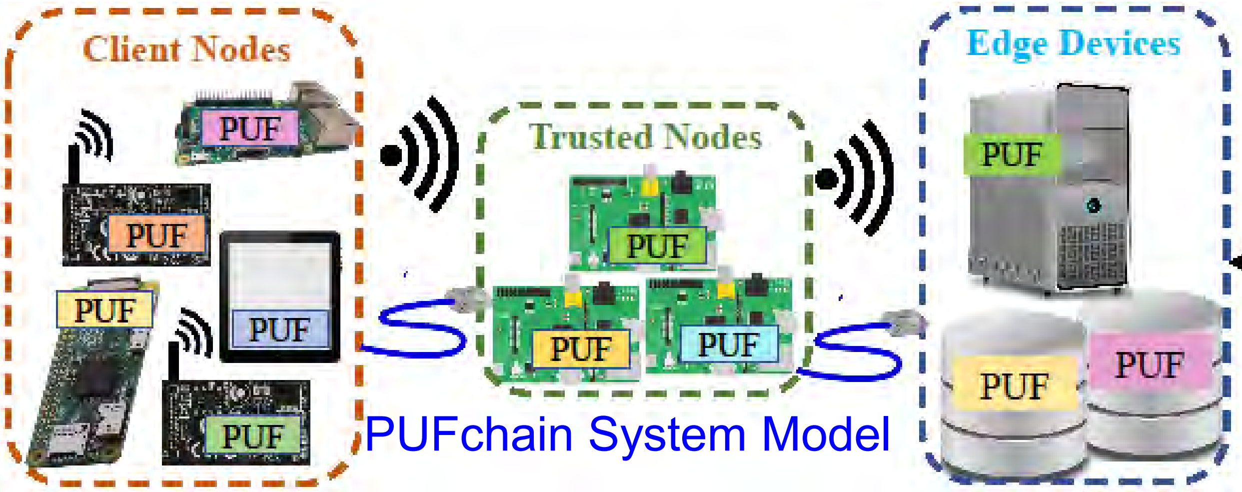
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain – Another Way

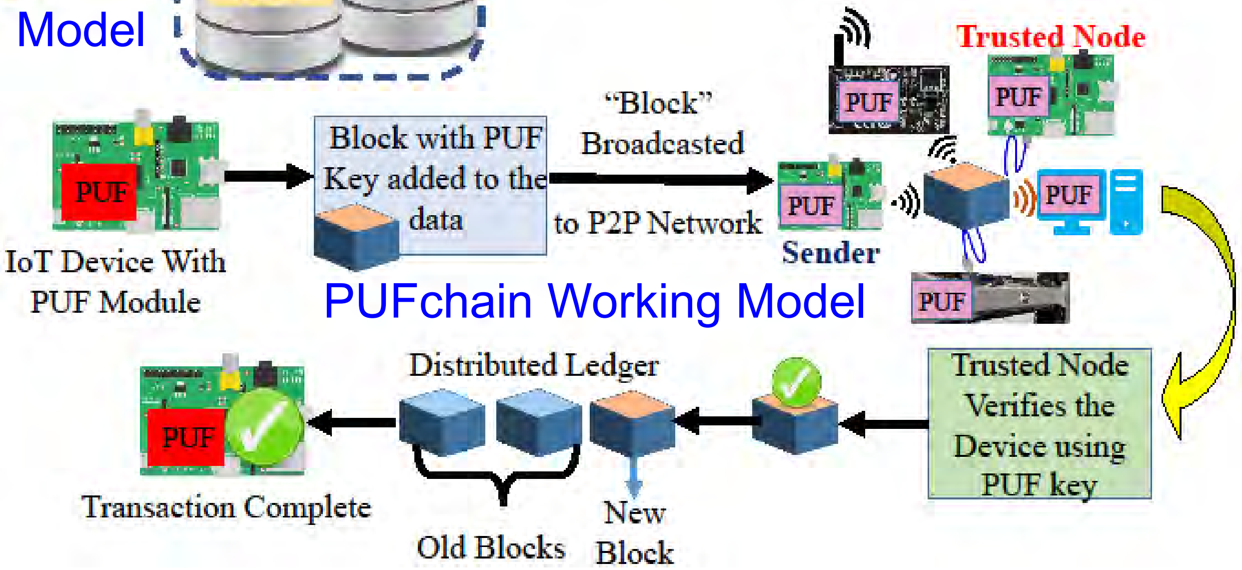


Blockchain Technology is integrated with Physically Unclonable Functions as PUFchain by storing the PUF Key into immutable Blockchain

PUFchain: Our Hardware-Assisted Scalable Blockchain



Can provide:
Device, System, and
Data Security

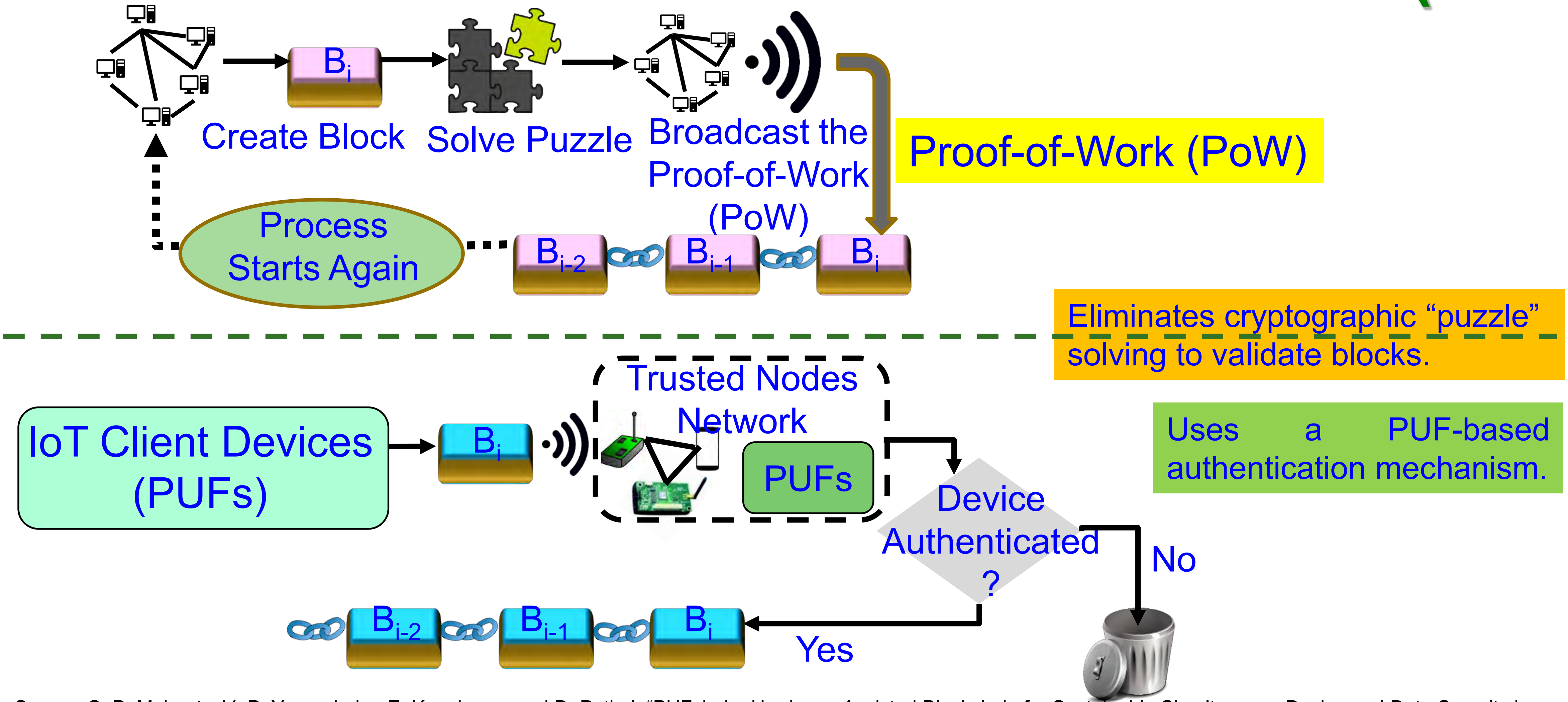


PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode

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

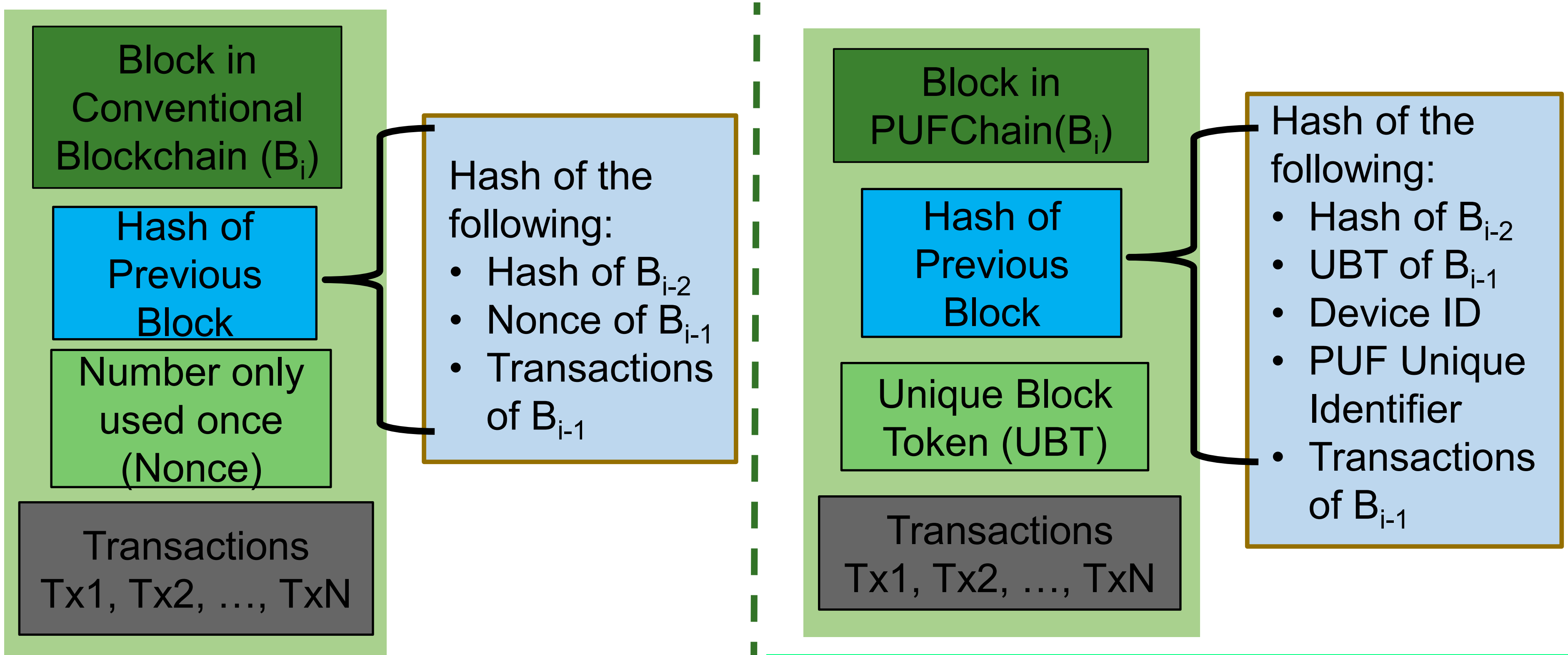
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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



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

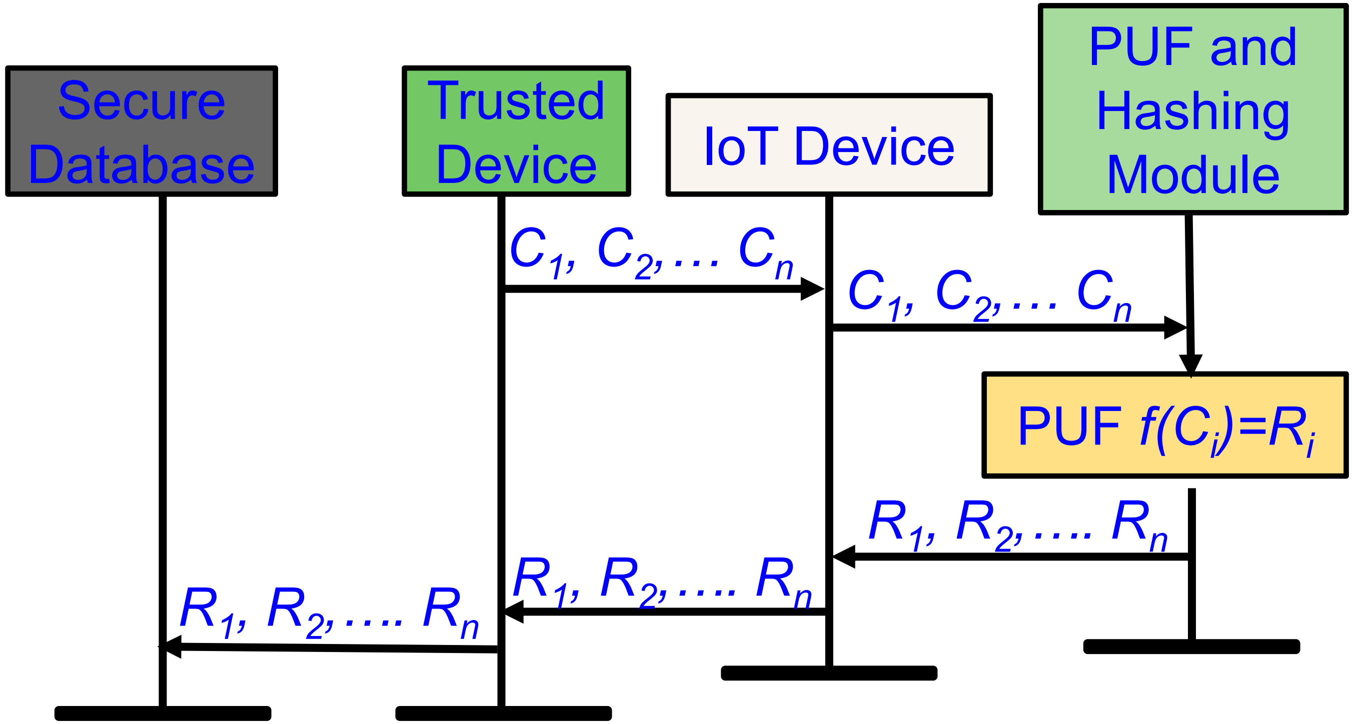
PUFchain: Proposed New Block Structure



Conventional Block Structure

Proposed Block Structure for PUFchain

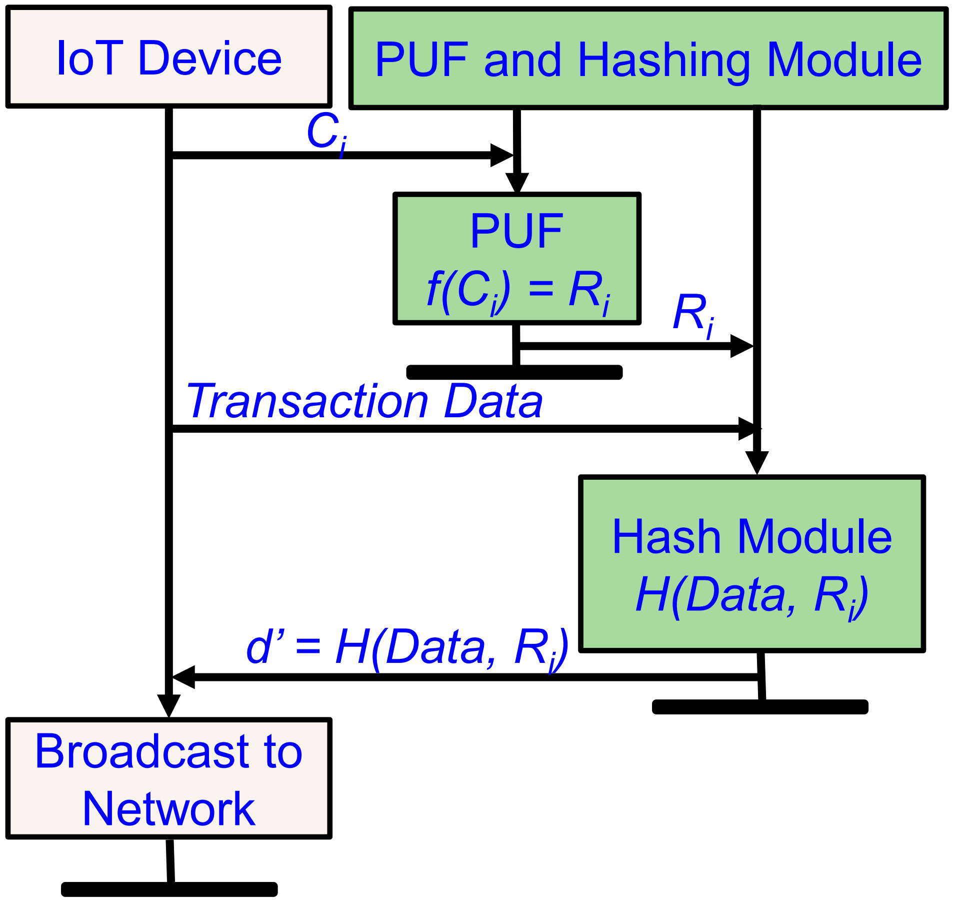
PUFchain: Device Enrollment Steps



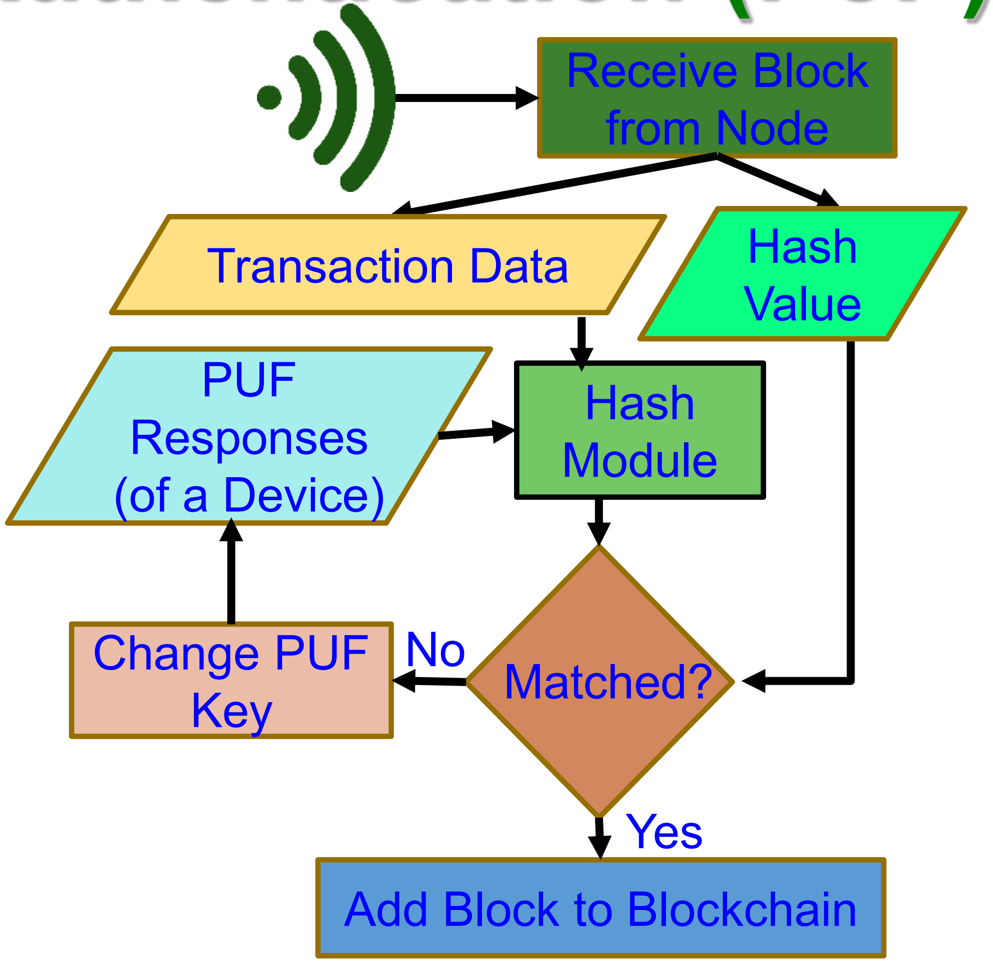
Device Enrollment Steps

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

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



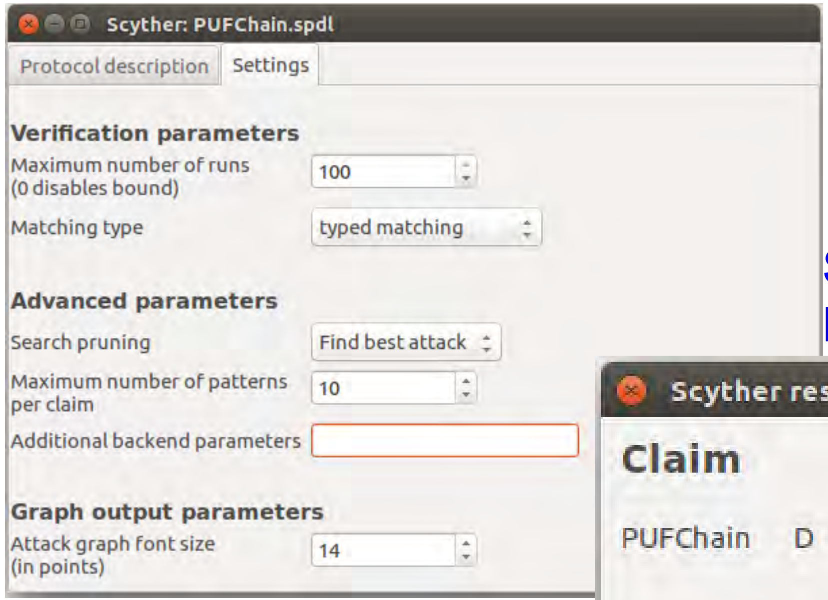
Steps for Transactions Initiation



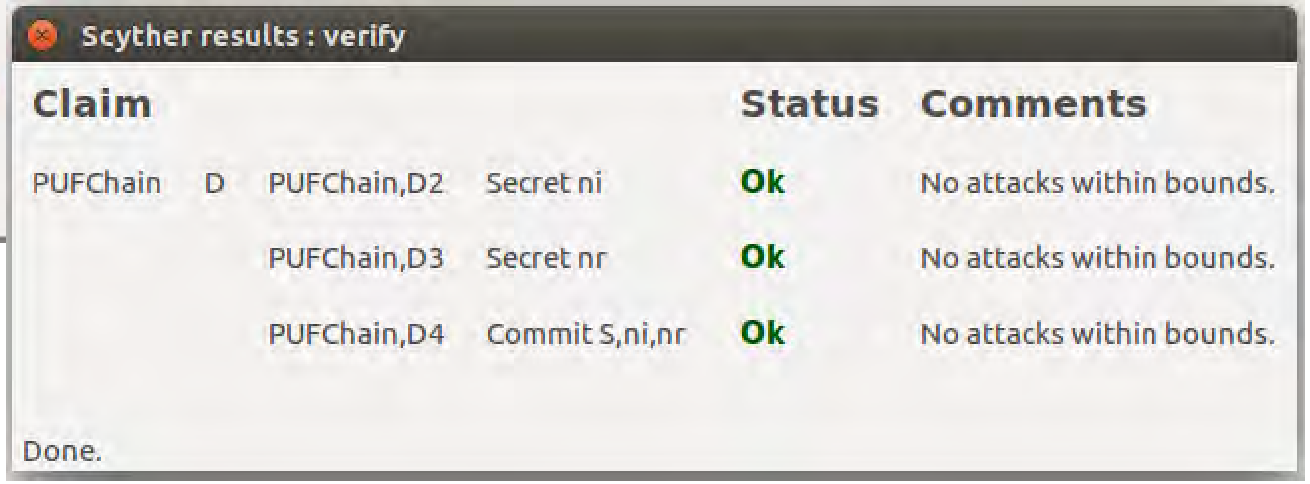
Steps for Device Authentication

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

PUFchain Security Validation



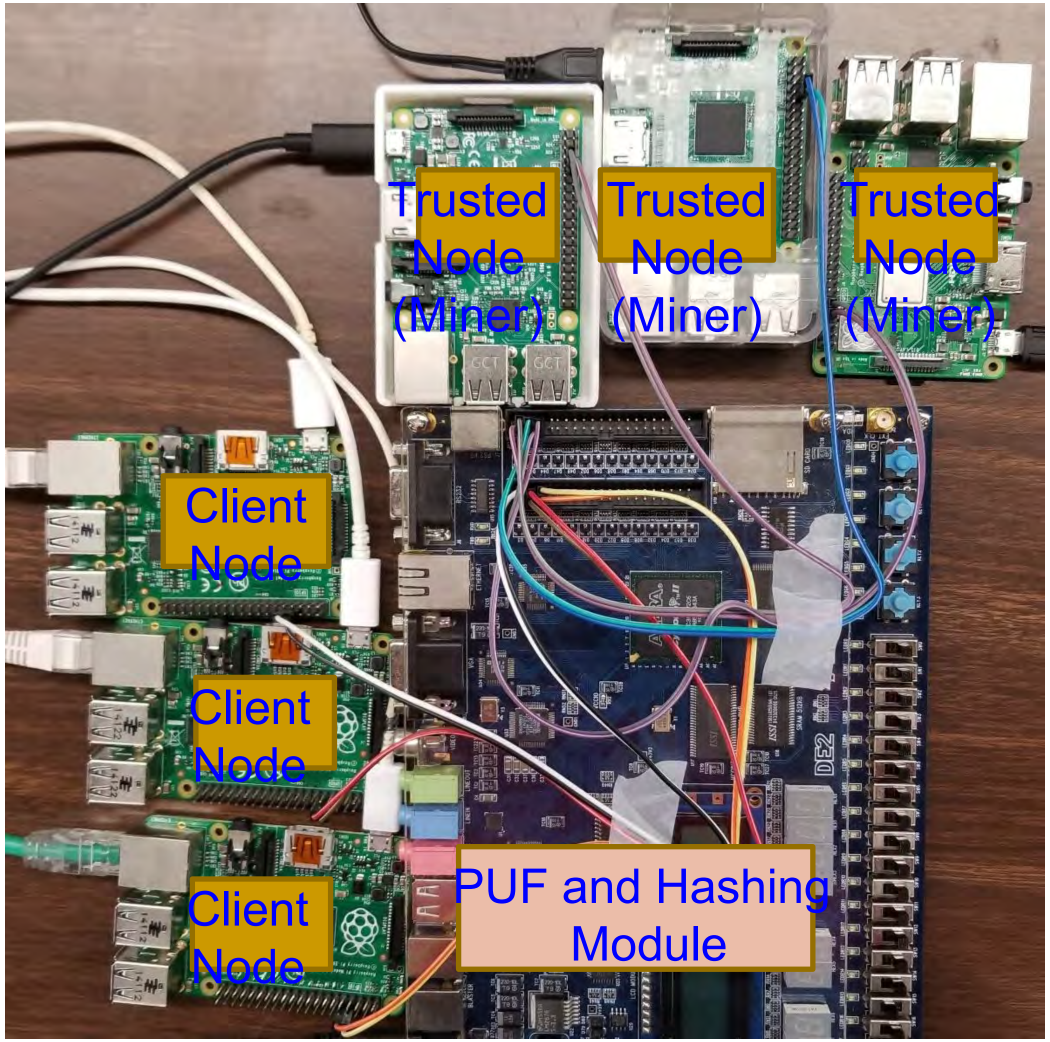
S - the source of the block
D - the miner or authenticator node in the networks



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

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

Our PoP is 1000X Faster than PoW

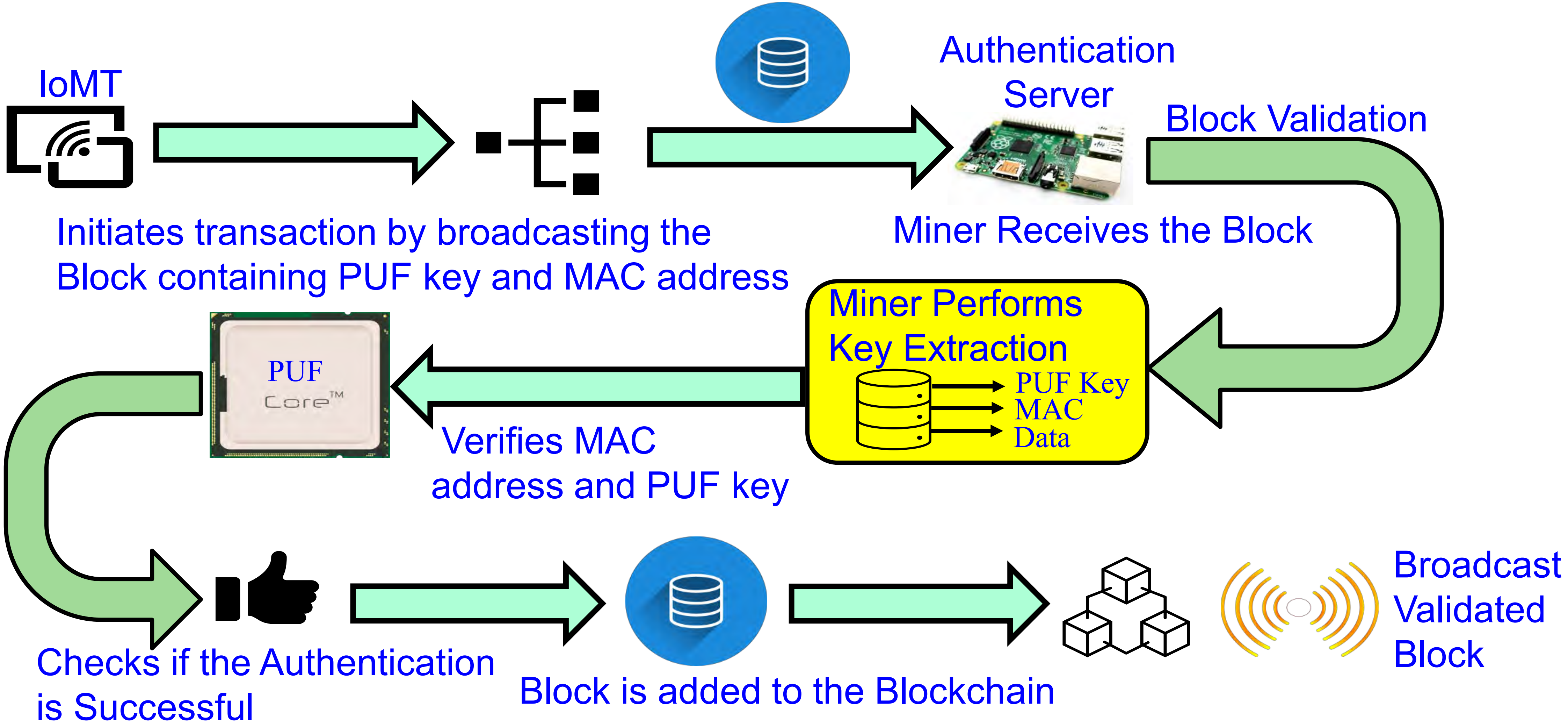


PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

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

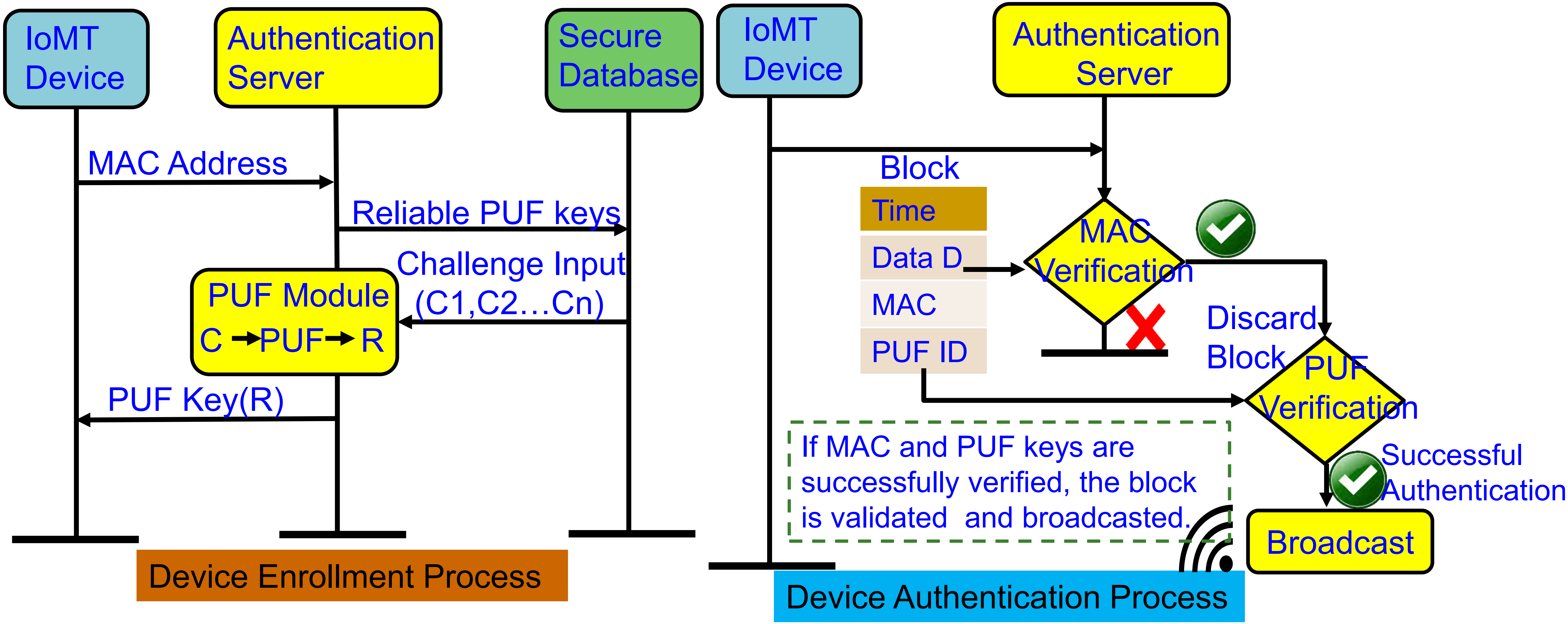
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



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

PUFchain 2.0: PUF Integrated Blockchain …



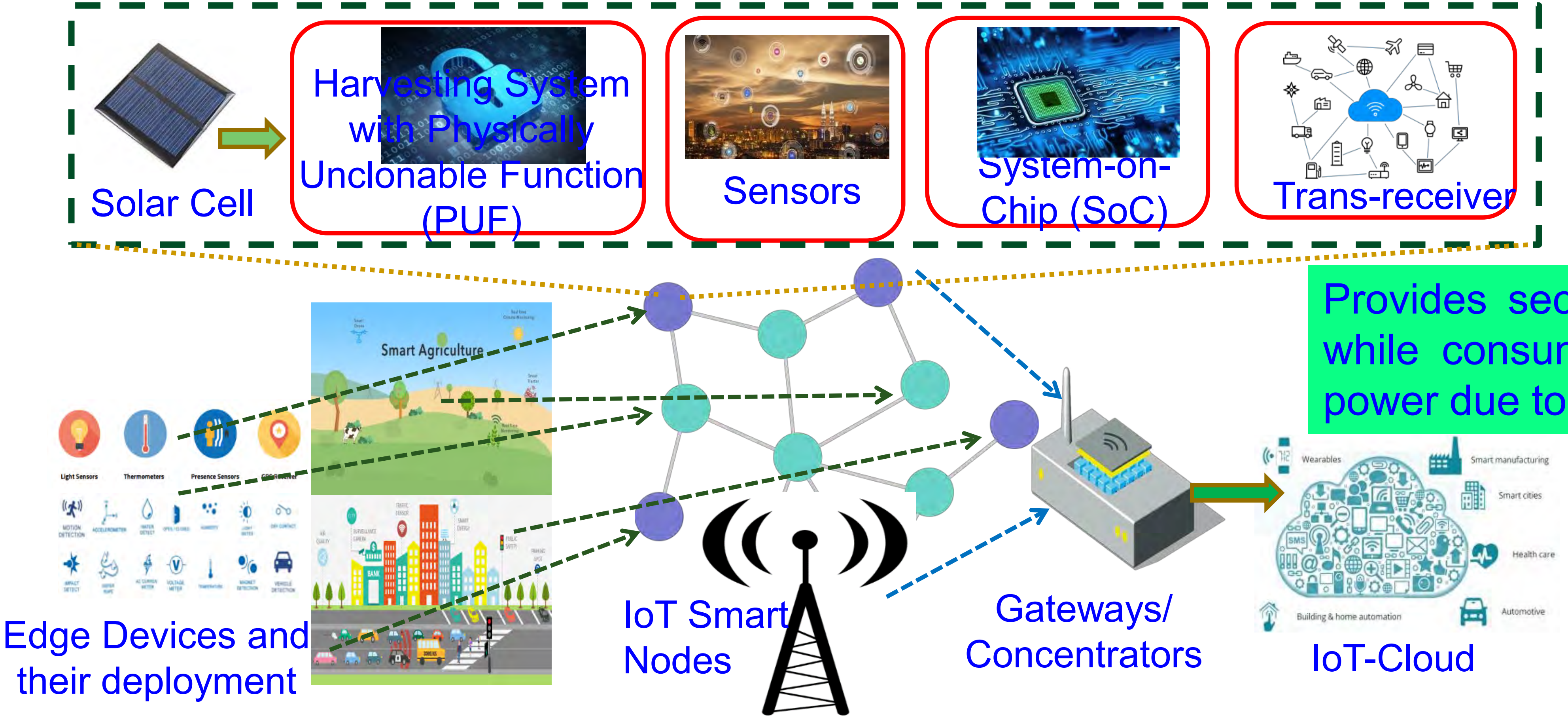
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

PUFchain 2.0: PUF Integrated Blockchain …

Parameters	PMsec [35]	PUFchain [21]	PUF based IoT Authentication [14]	PUFchain 2.0 [This Paper]
Application	IoMT	IoT	IoT	Smart Healthcare
Prototyped Hardware	FPGA, 32-bit Micro-controller based board	Altera DE-2, Single Board Computer	Coretex-M4 based STM32F4 MCU	Xilinx Artix -7 Basys3 FPGA and Single Board Computers
Blockchain Type	-	Private	-	Permission ed
Security Mechanism	PUF Key Verification	PUF key verification	PUF Key verification	MAC Address and PUF key verification
PUF Keys at Client	Serial PUF keys	Serial PUF keys	Serial PUF	Edge assigned PUF keys
PUF Circuit Design	Hybrid Oscillator Arbiter PUF	Ring oscillators	RC PUF, PHY PUF, Flash and PDRO PUF	Arbiter elements with Multiplexers and D-Flip Flop
Randomness	44%	47%	-	41.8%
Reliability	0.85%(FinFET)	1.25%	-	75% of the keys are reliable
Consensus Mechanism	-	Proof of PUF Enabled Authentication	-	Proof of PUF Enabled Authentication
Security Levels	Single level Authentication	Single Level Authentication	Single level Authentication	Two level Authentication
Blockchain Transaction Time(Client)	-	46.5 ms(Raspberry pi 3)	-	309 ms(Client 1), 314 ms(Client 2)
Blockchain Transaction Time(Miner)	-	120.03 ms(Raspberry pi 3)	-	3600 ms

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.

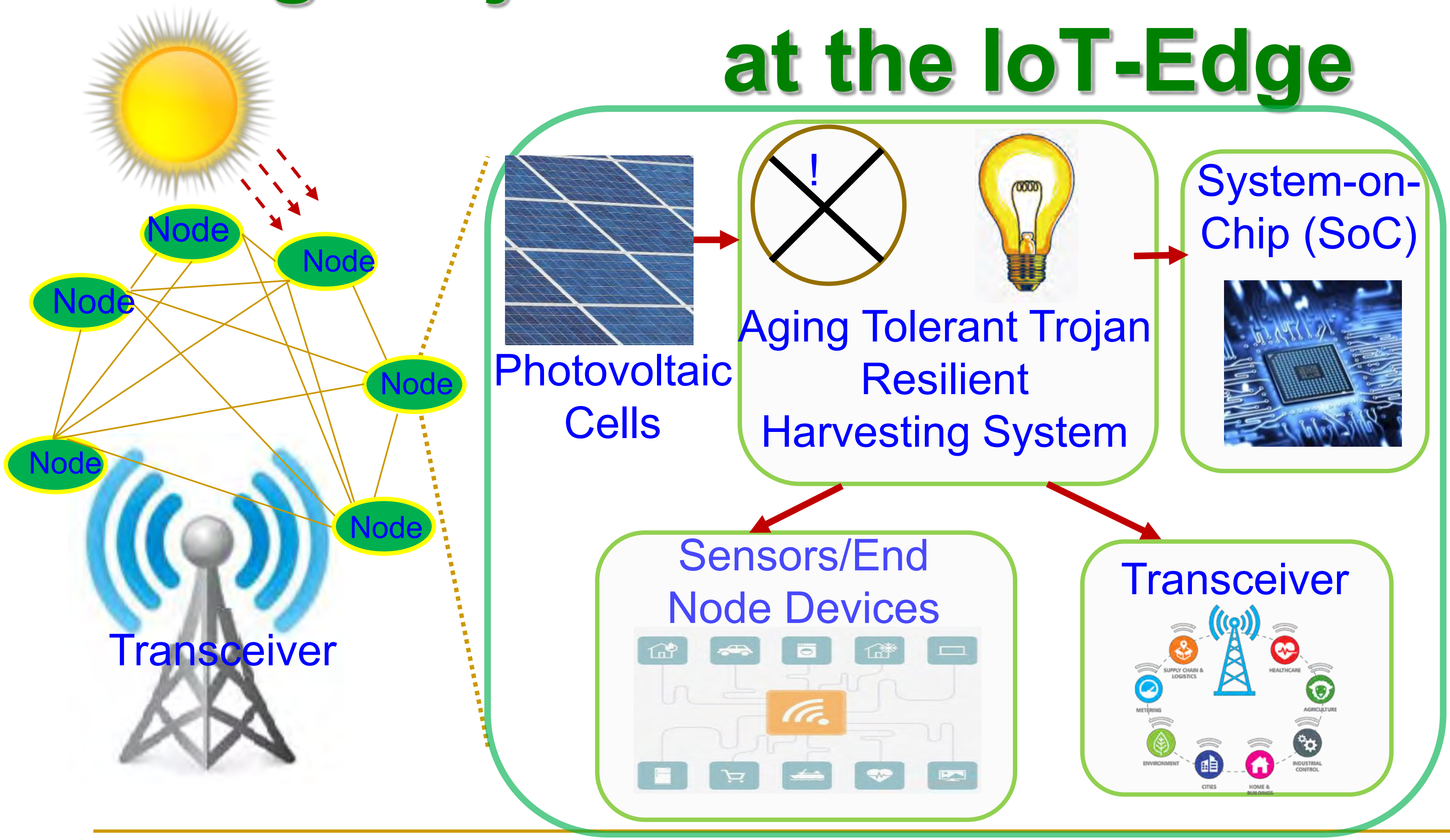
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge



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

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

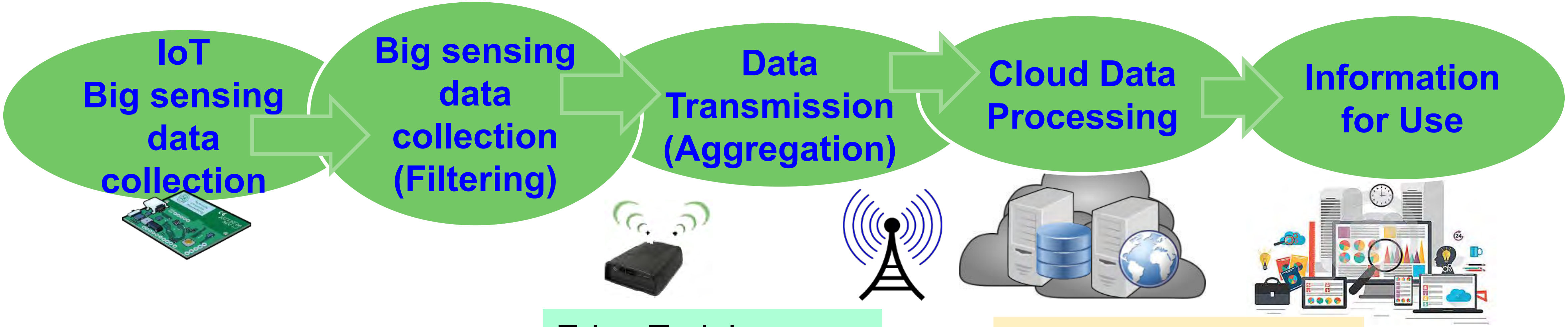
Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge



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

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, “Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT”, arXiv Computer Science, arXiv:2103.05615, March 2021, 24-pages.

Data Quality Assurance in IoT/CPS



Edge Training:
- ➢ Data Signature
- ➢ Model Signature

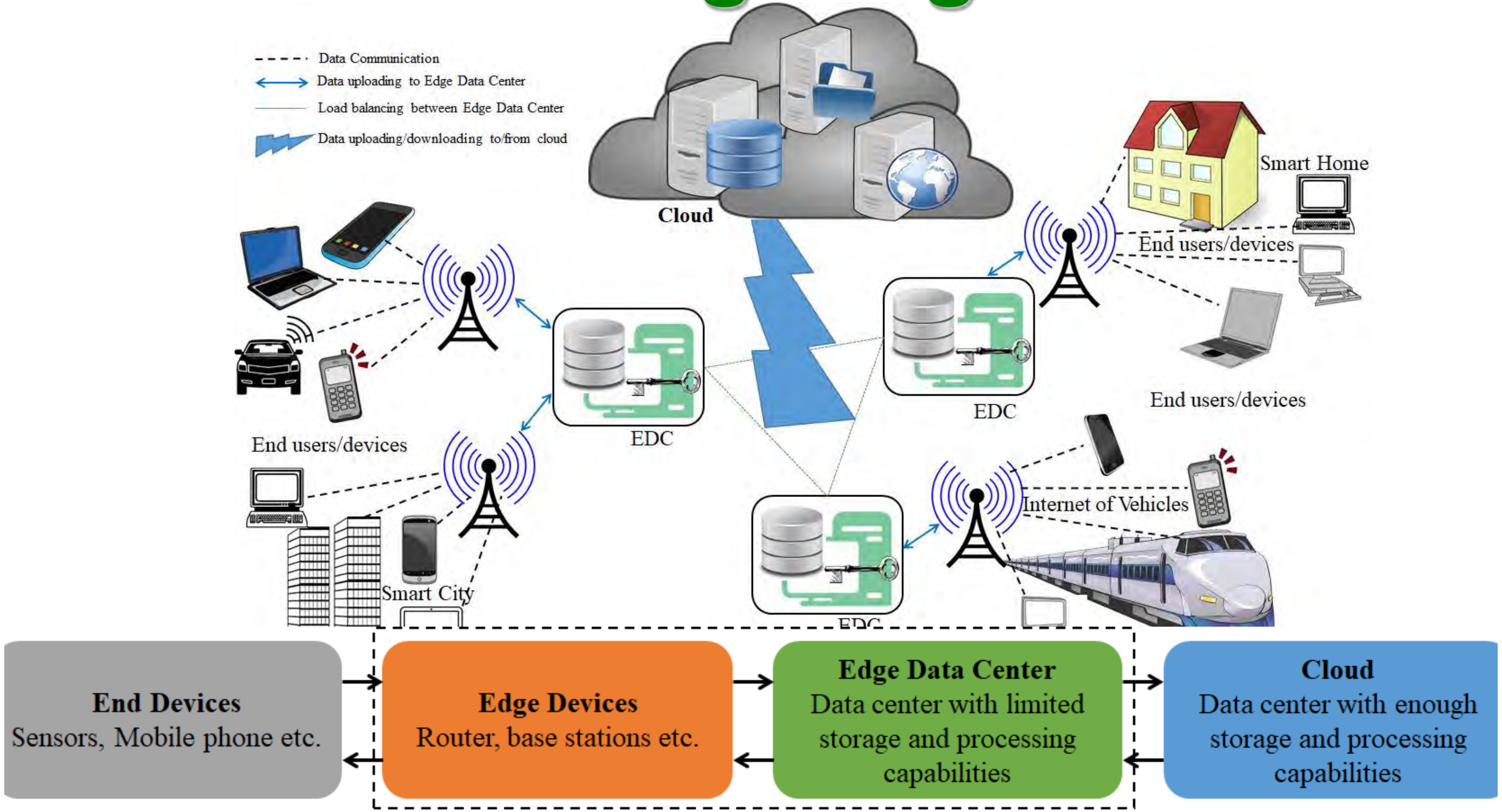
Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

Secure data curation a solution for fake data?

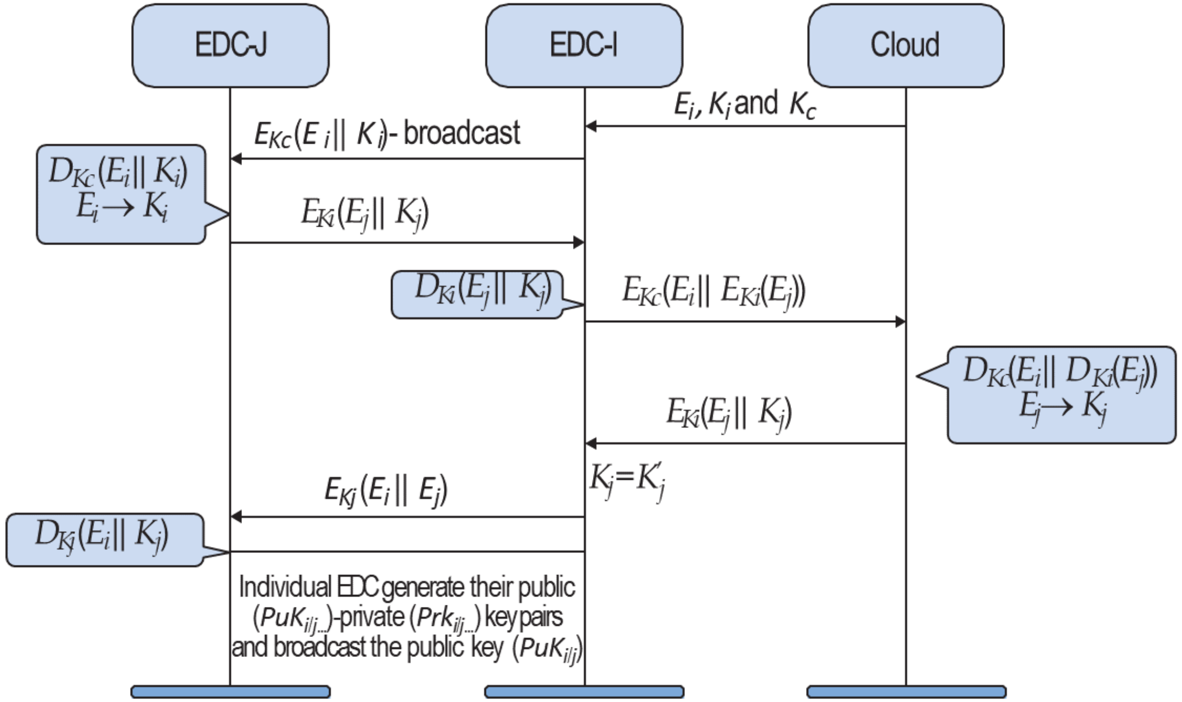
Source: C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, “Big-Sensing-Data Curation for the Cloud is Coming”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 6, Issue 4, October 2017, pp. 48--56.

Data and Security Should be Distributed using Edge Datacenter



Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Magazine*, Volume 56, Issue 5, May 2018, pp. 60--65.

Our Proposed Secure Edge Datacenter



Secure edge datacenter –

- Balances load among the EDCs
- Authenticates EDCs

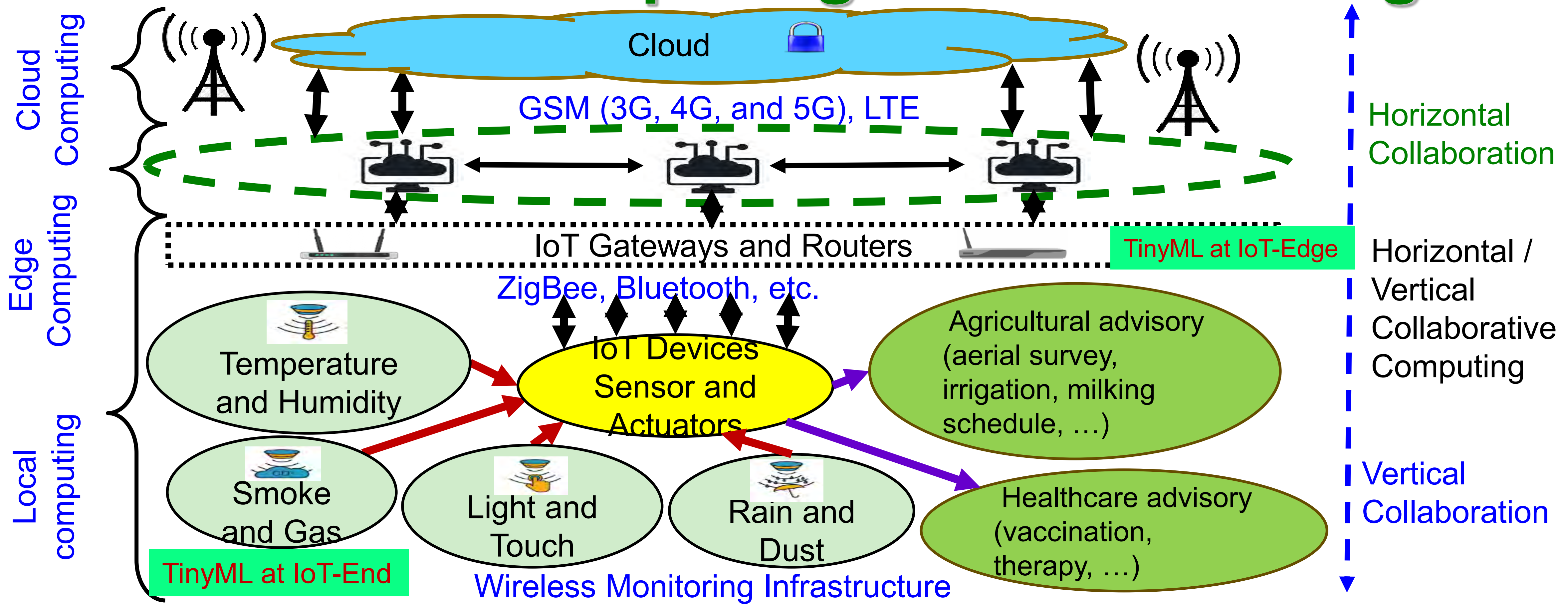
Algorithm 1: Load Balancing Technique

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

Response time of the destination EDC has reduced by 20-30% using the proposed allocation approach.

Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Magazine*, Volume 56, Issue 5, May 2018, pp. 60--65.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



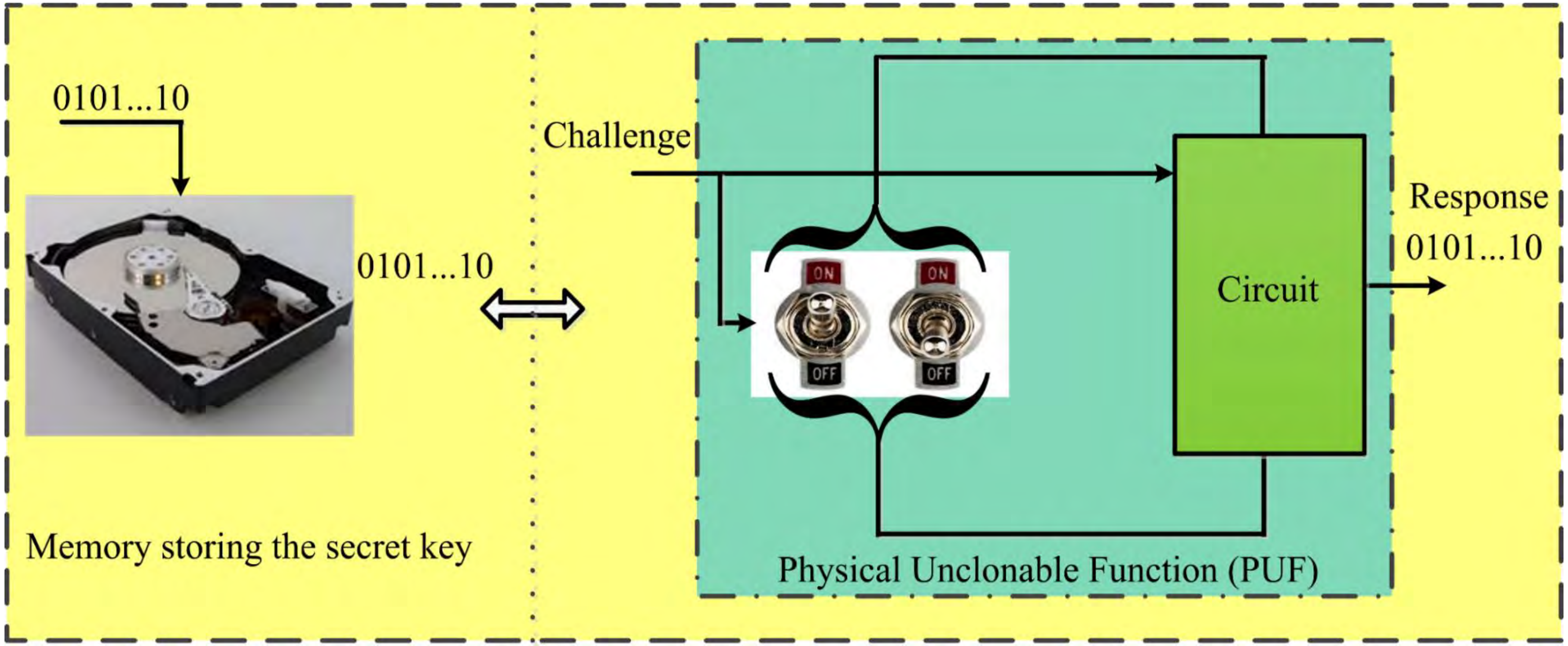
Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, "Collaborative Edge Computing for Smart Villages", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

Physical Unclonable Function – Broad Overview

Lock and Key

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

PUFs Don’t Store Keys

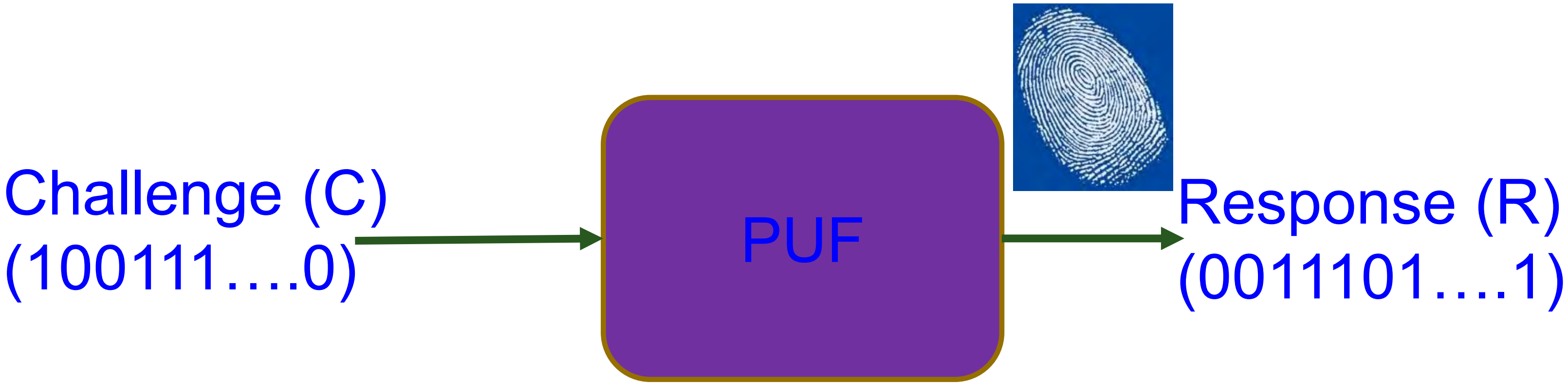


Source: S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything You Wanted to Know about PUFs”, *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

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

Physical Unclonable Functions (PUFs) - Principle

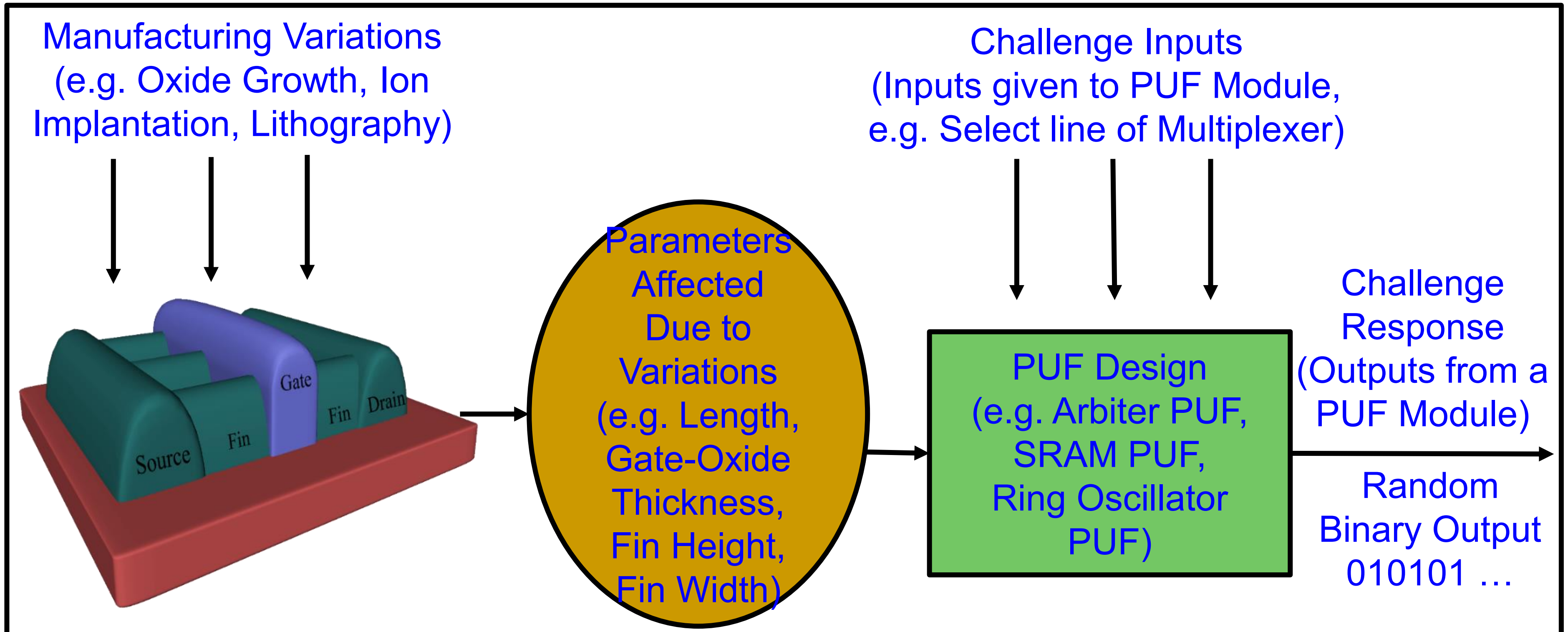
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

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

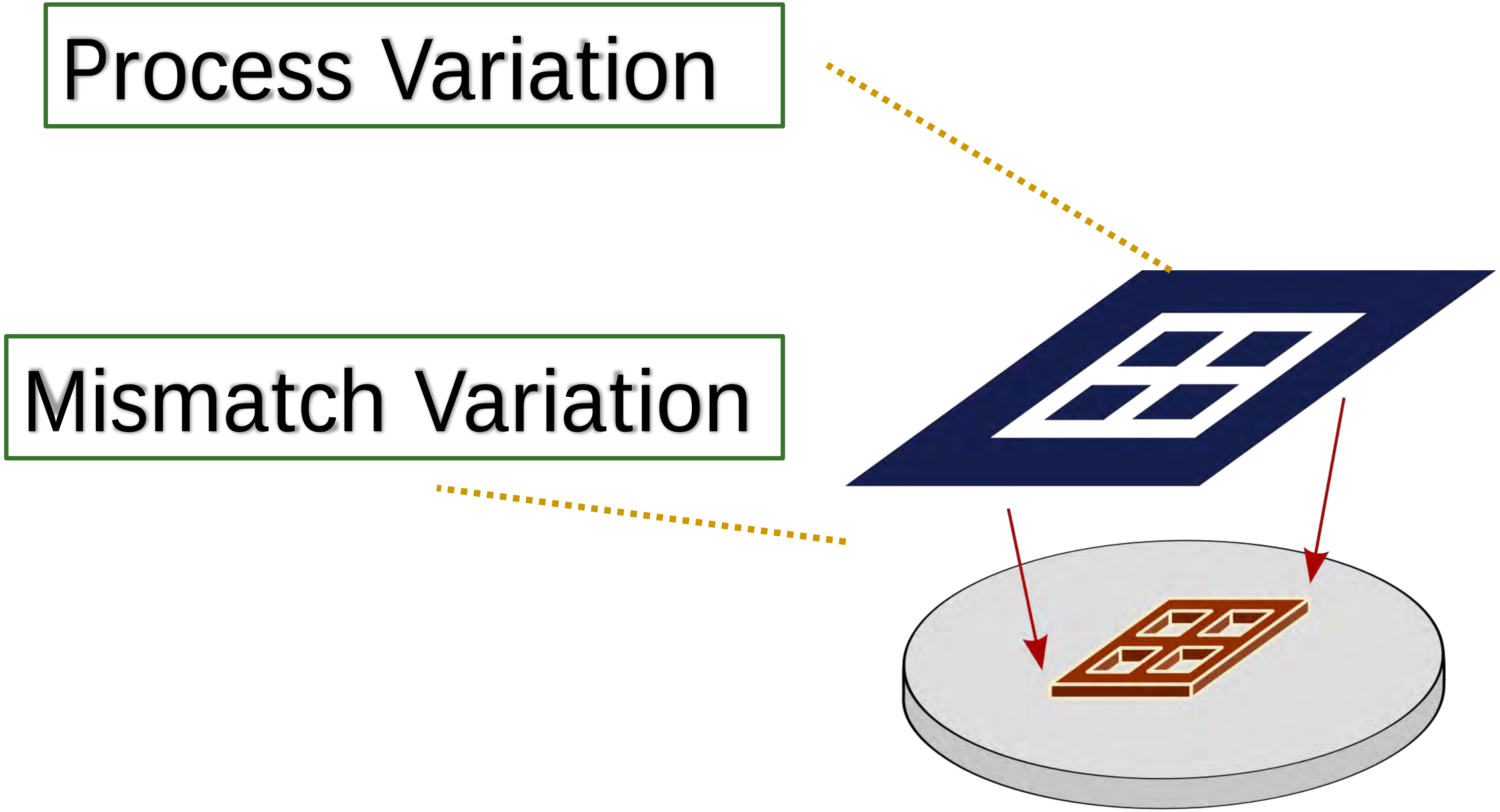
PUF - Principle



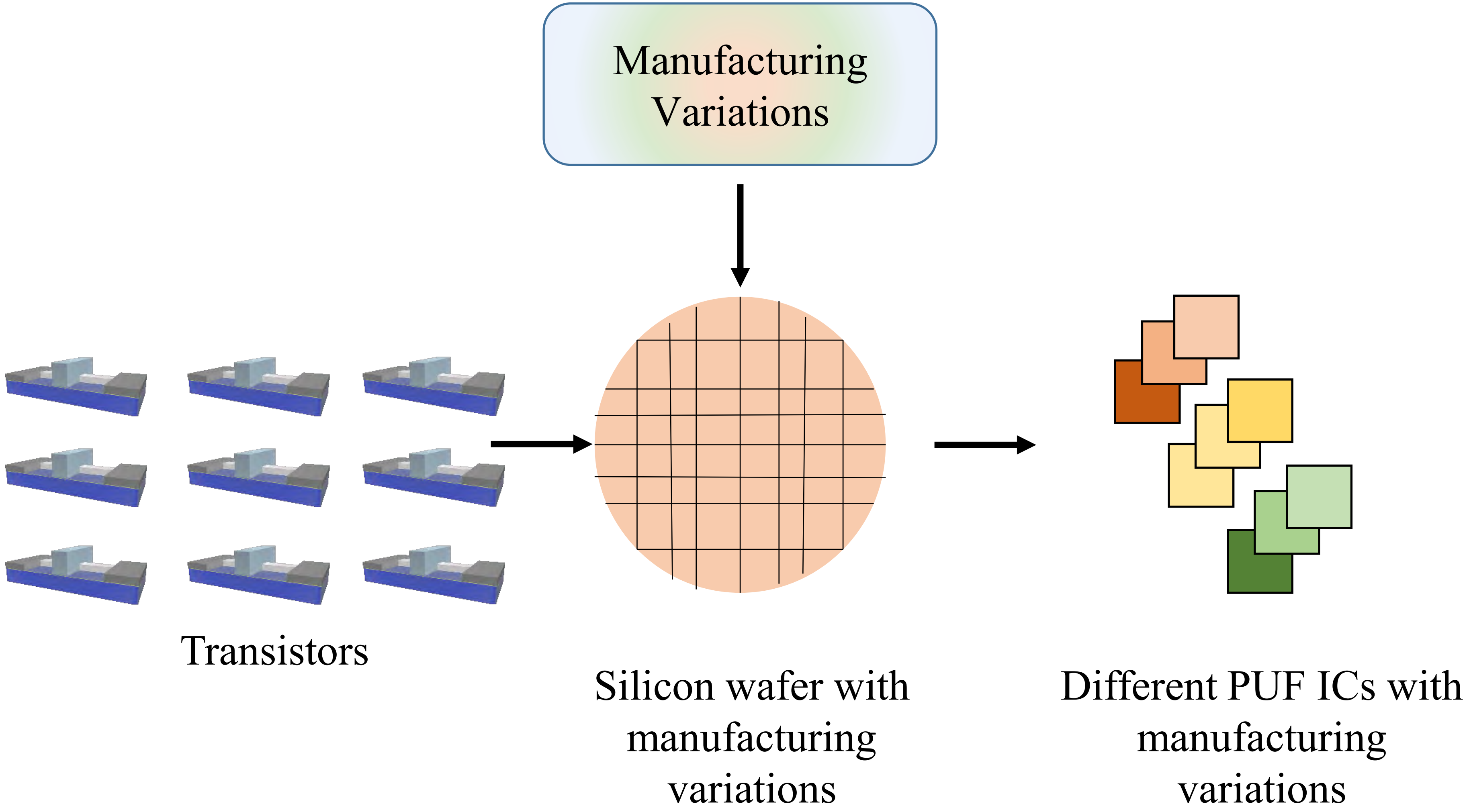
Silicon manufacturing process variations are turned into a feature rather than a problem.

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

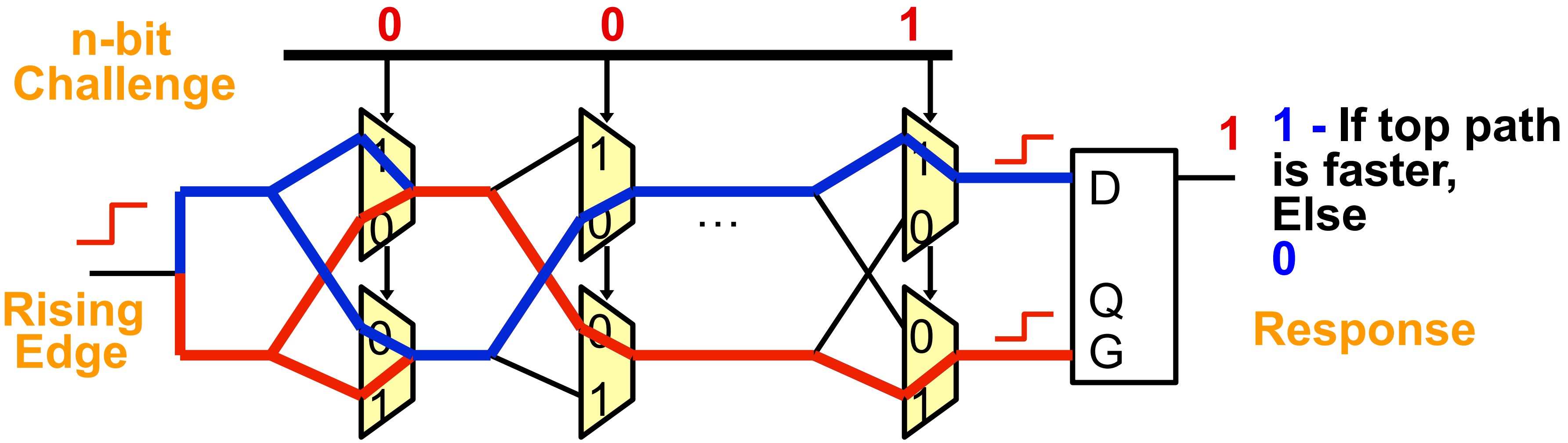
How PUF Works?



How PUFs Work?



Principle of Generating Random Response using PUF

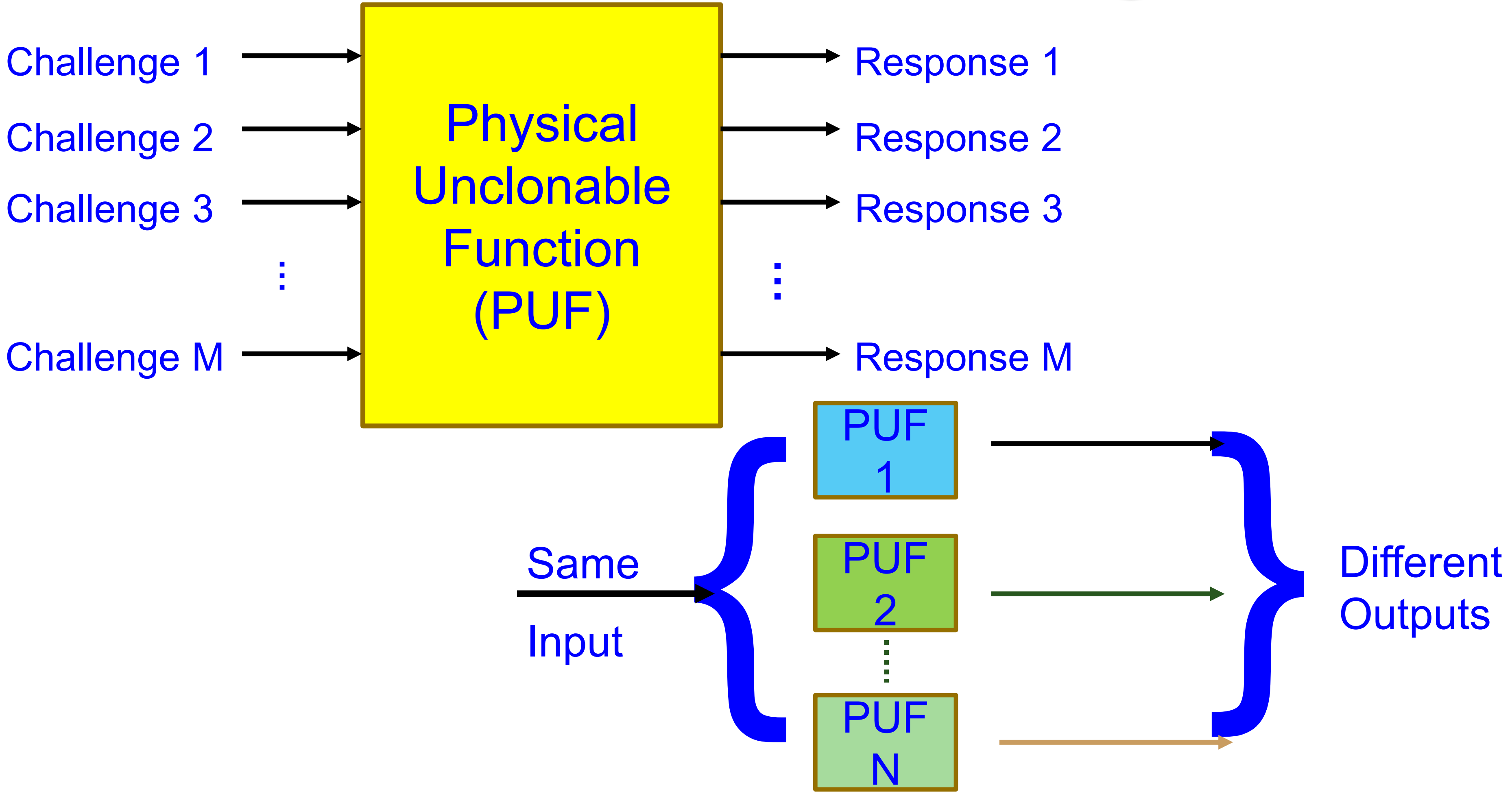


Compare two paths with an identical delay in design

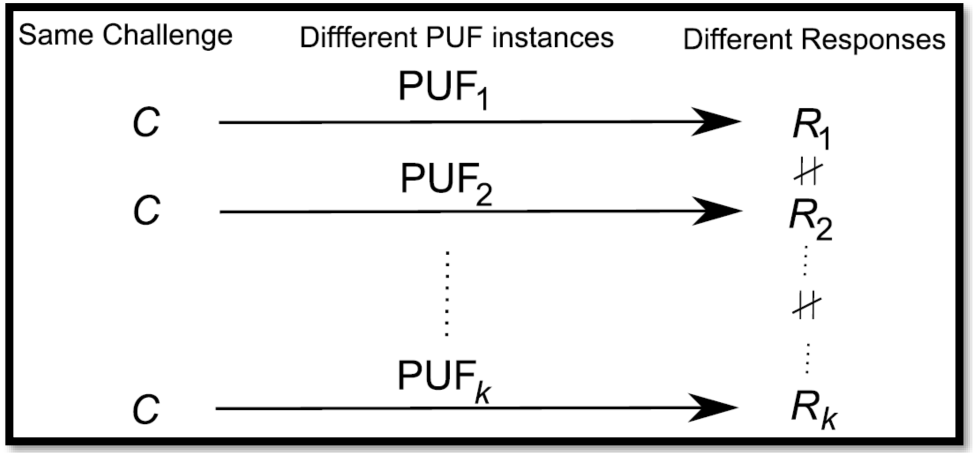
- Random process variation determines which path is faster
- An arbiter outputs 1-bit digital response

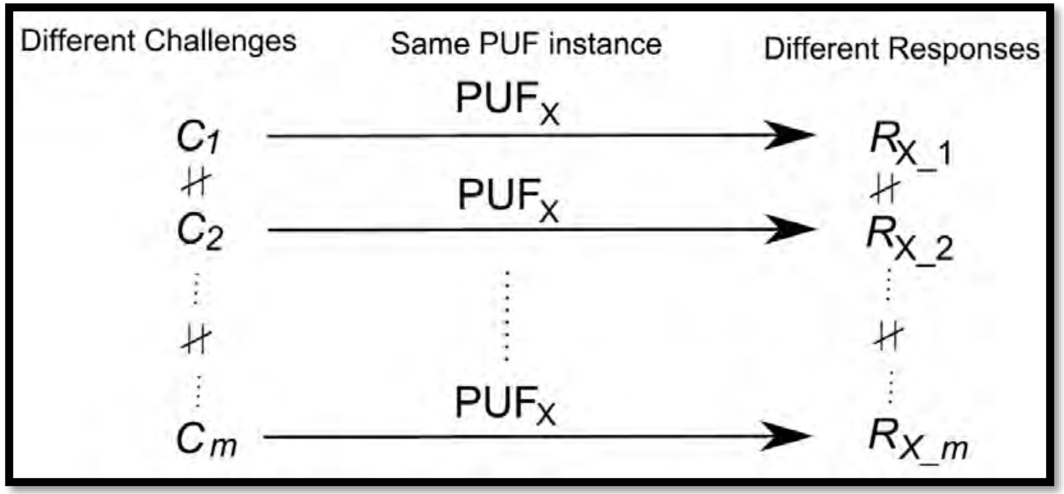
Source: Srini Devadas, Physical Unclonable Functions (PUFs) and Secure Processors, *Cryptographic Hardware and Embedded Systems*, 2009.

Principle of Generating Multiple Random Response using PUF



Principle of Generating Multiple Random Response using PUF





PUF Response is *not* Same as Encryption

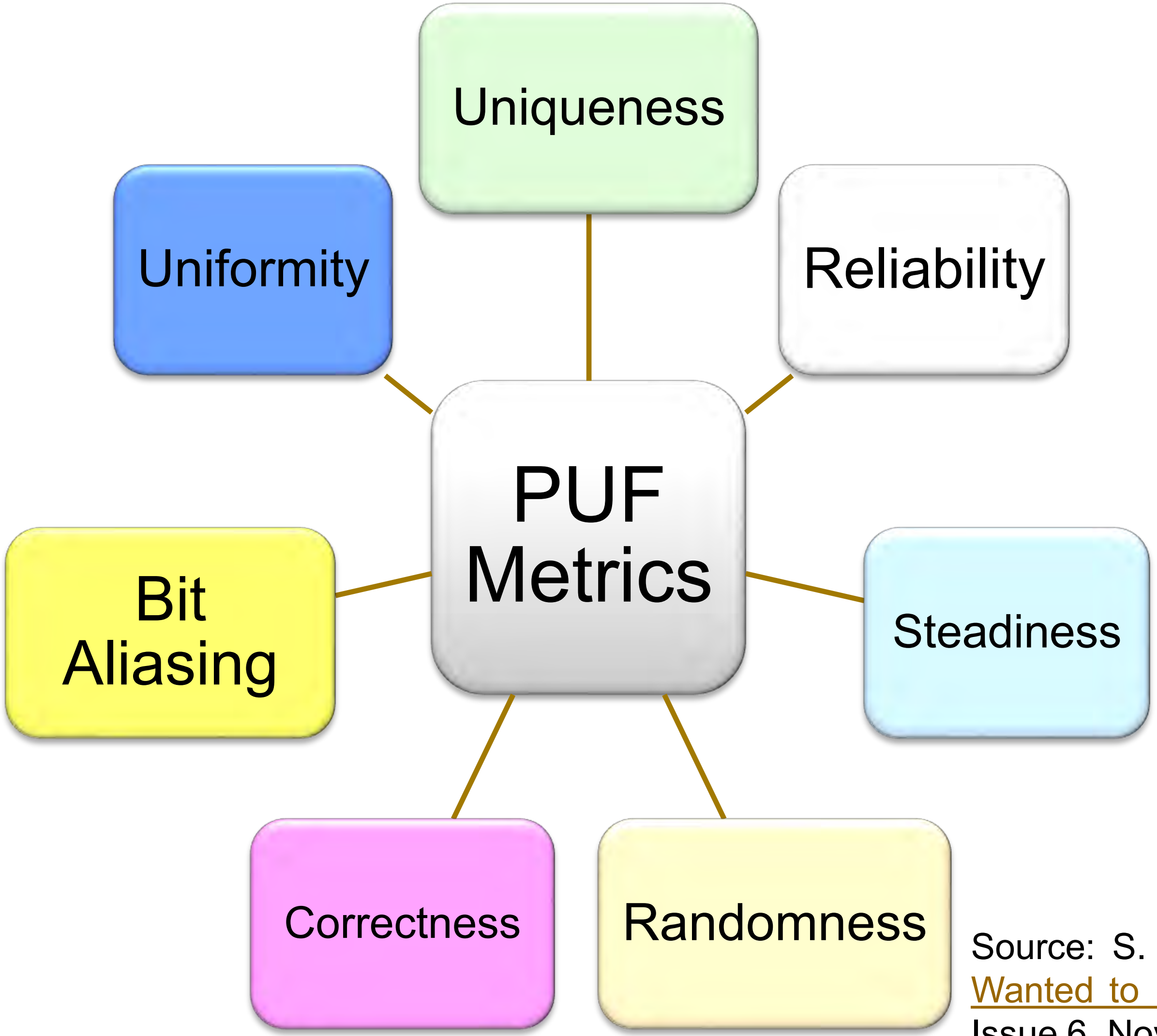
PUF vs Encryption

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

Performance Metrics …

Can any circuit become PUF?

PUF - Performance Metrics



AKA - Figure of Merits

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

Performance Metrics …

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

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

Performance Metrics …

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

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

More Performance Metrics …

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

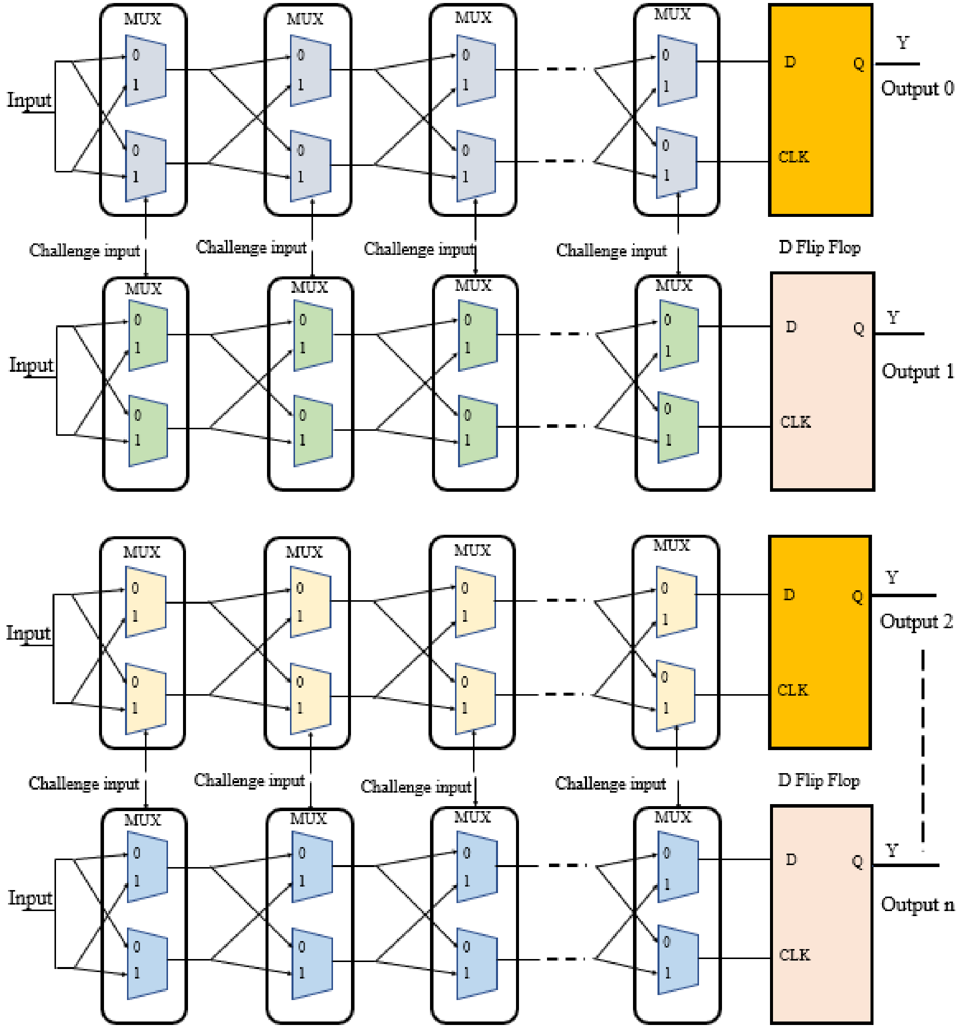
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

More Performance Metrics …

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

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

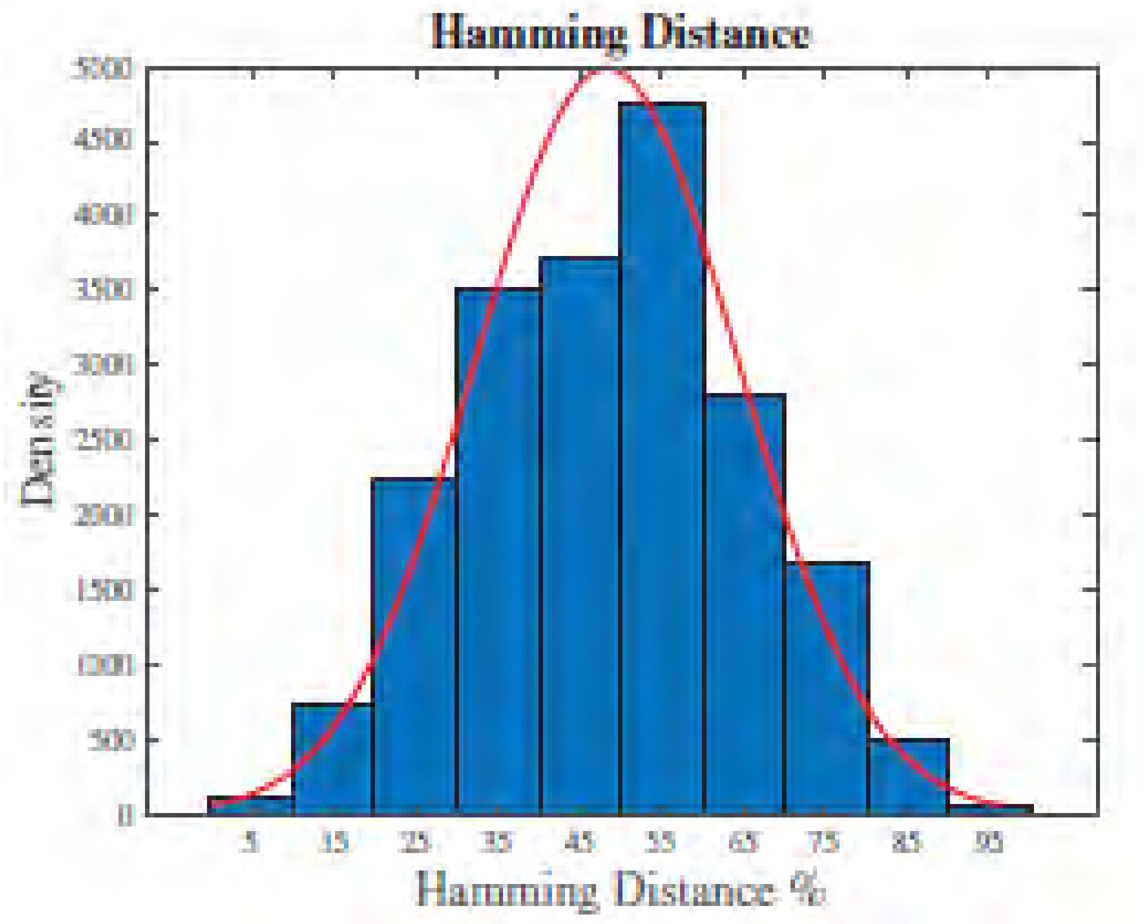
Arbiter PUF Design

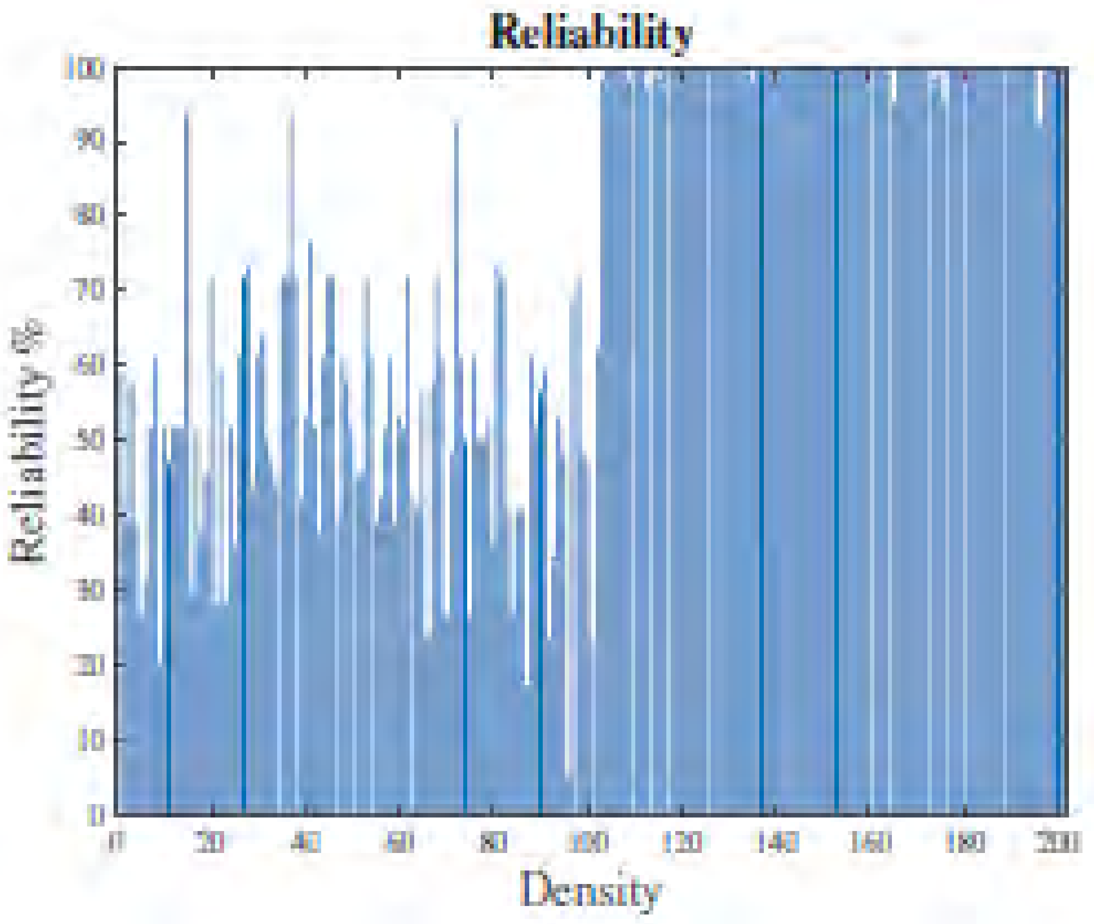


Strong PUF module which can be used for cryptographic purposes due to large number of CRP's.

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

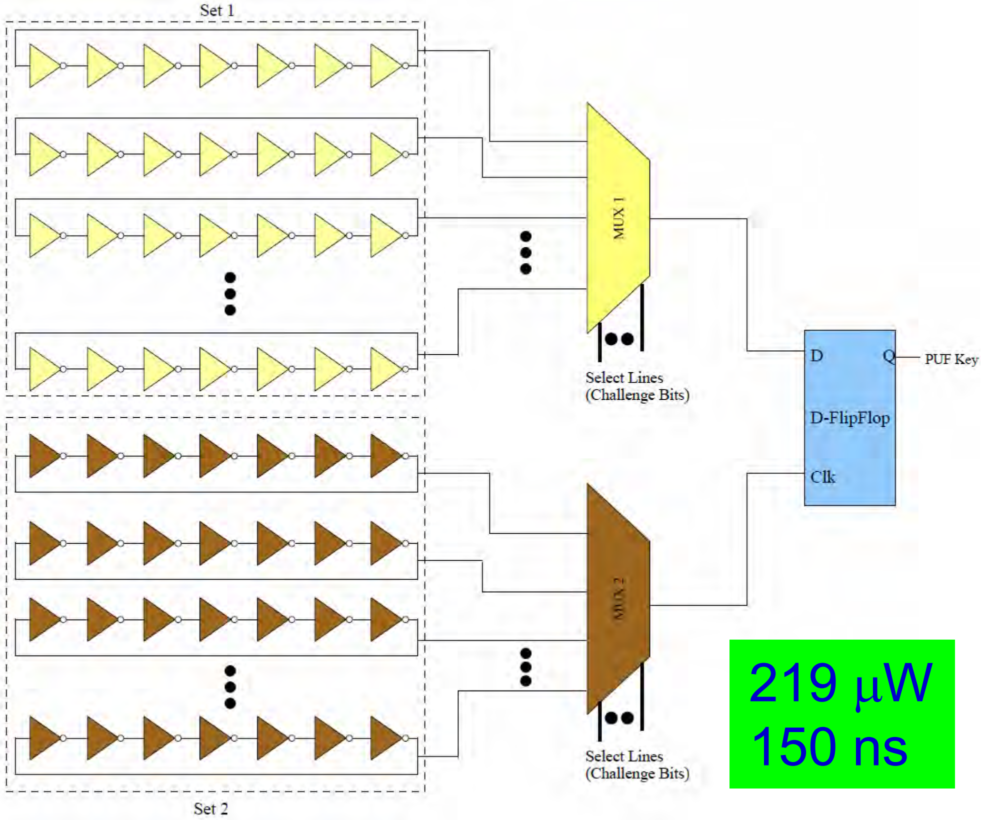
Arbiter PUF Metrics





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

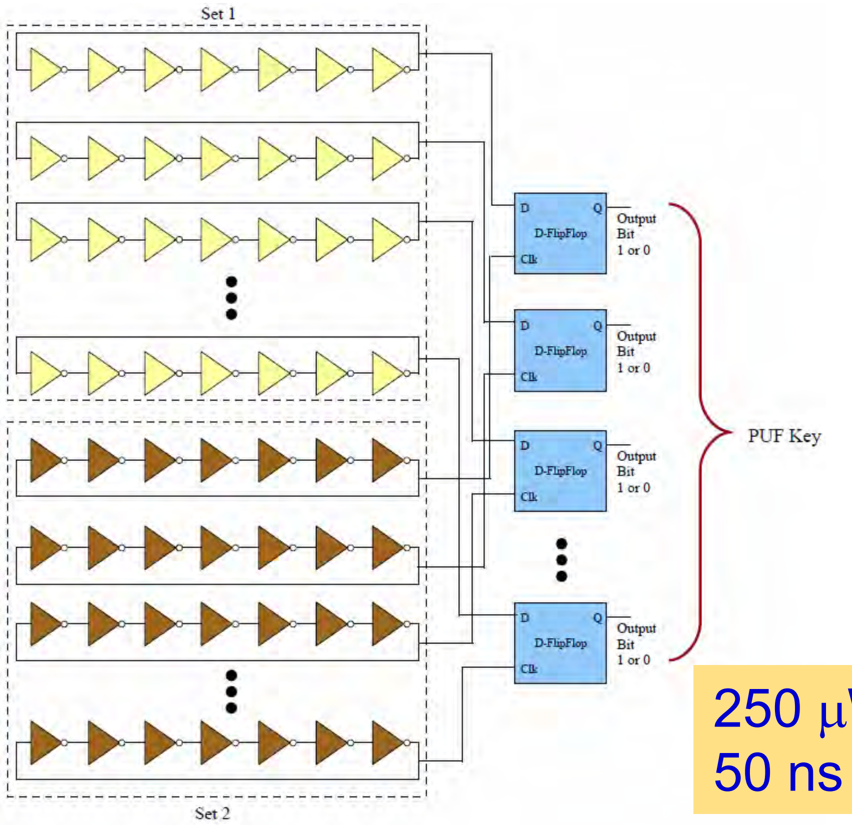
We Have Design a Variety of PUFs - FinFET based



219 μW
150 ns

Power Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS



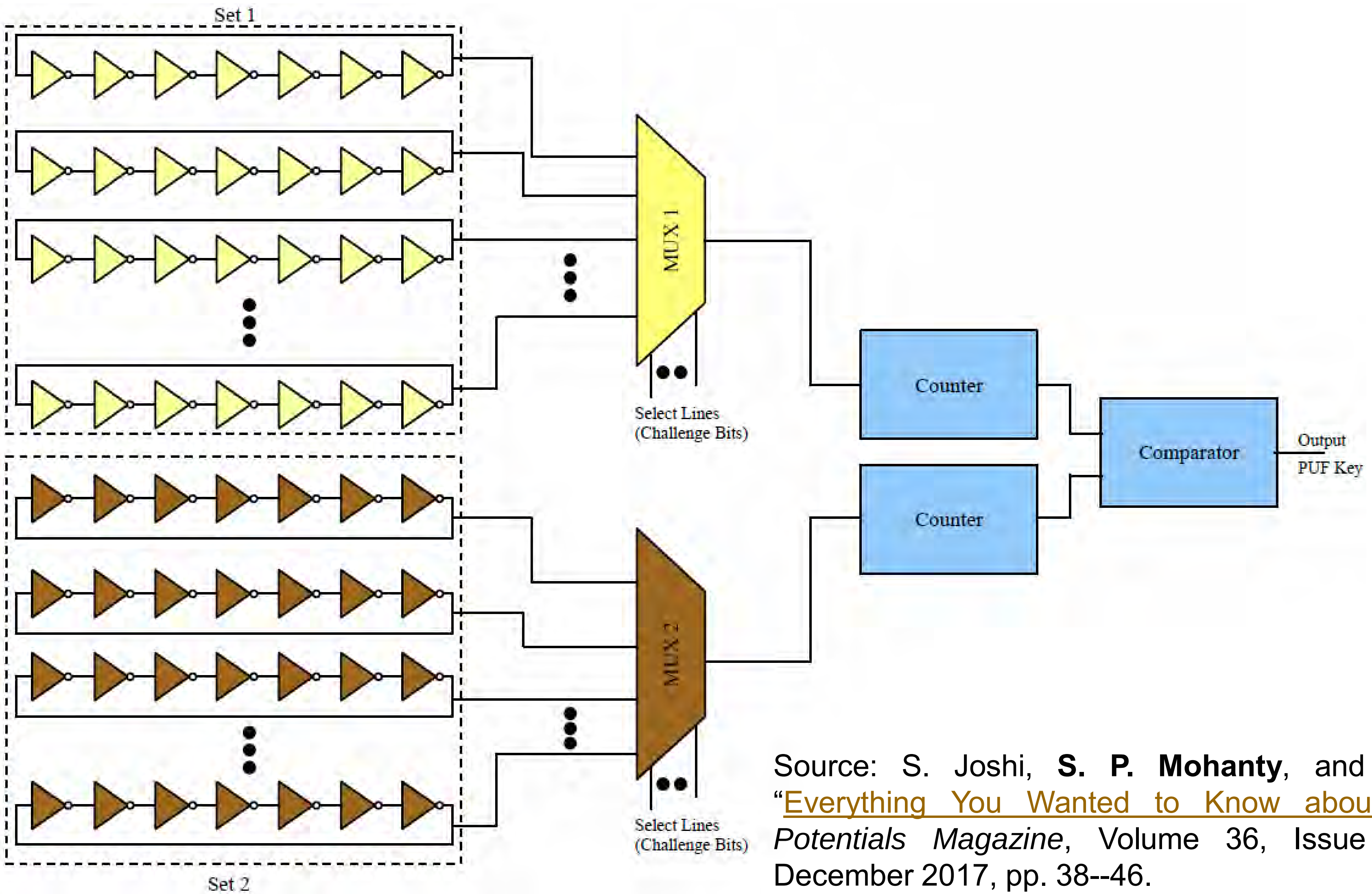
250 μW
50 ns

Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Transportation and Energy CPS

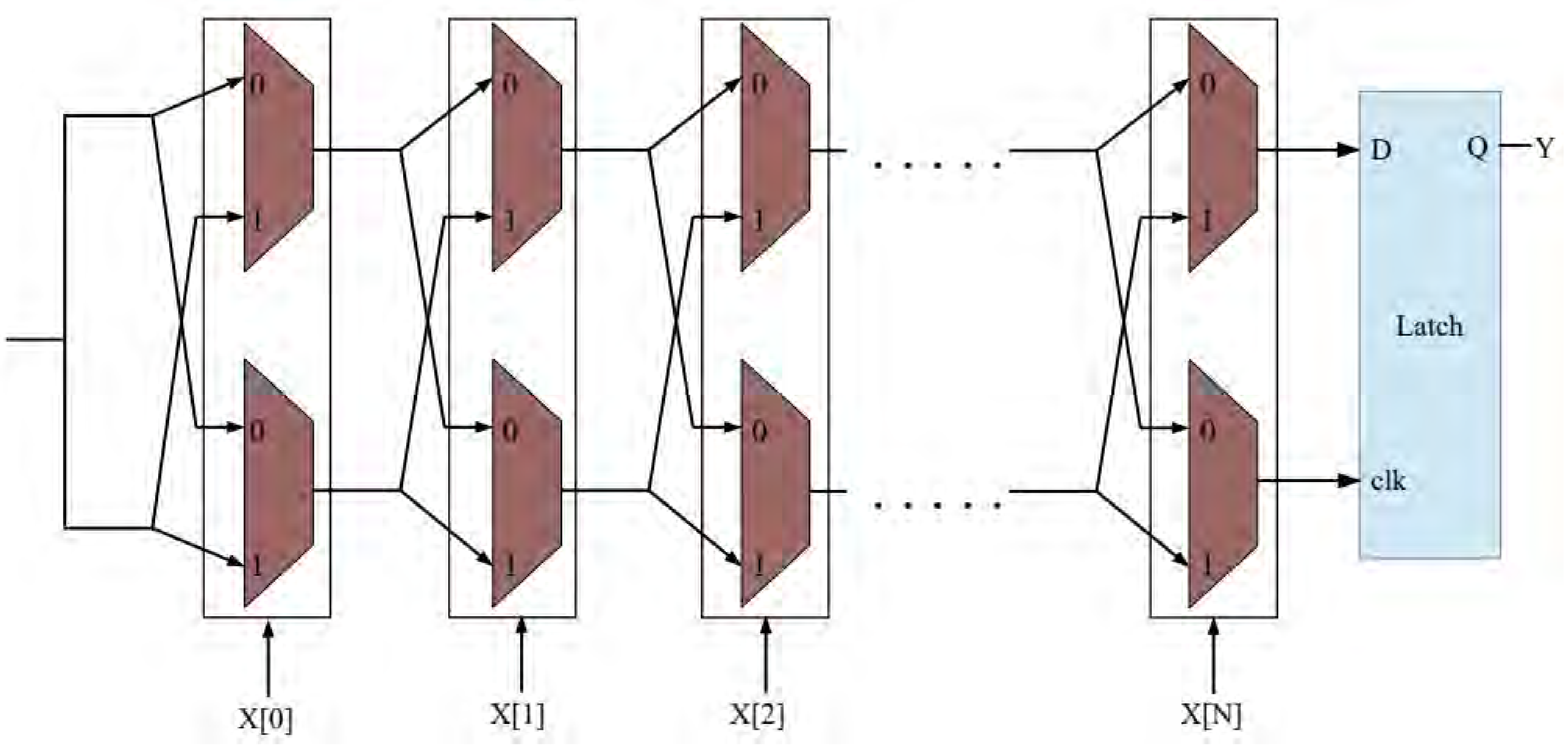
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT", *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3,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

Conventional Ring Oscillator PUF



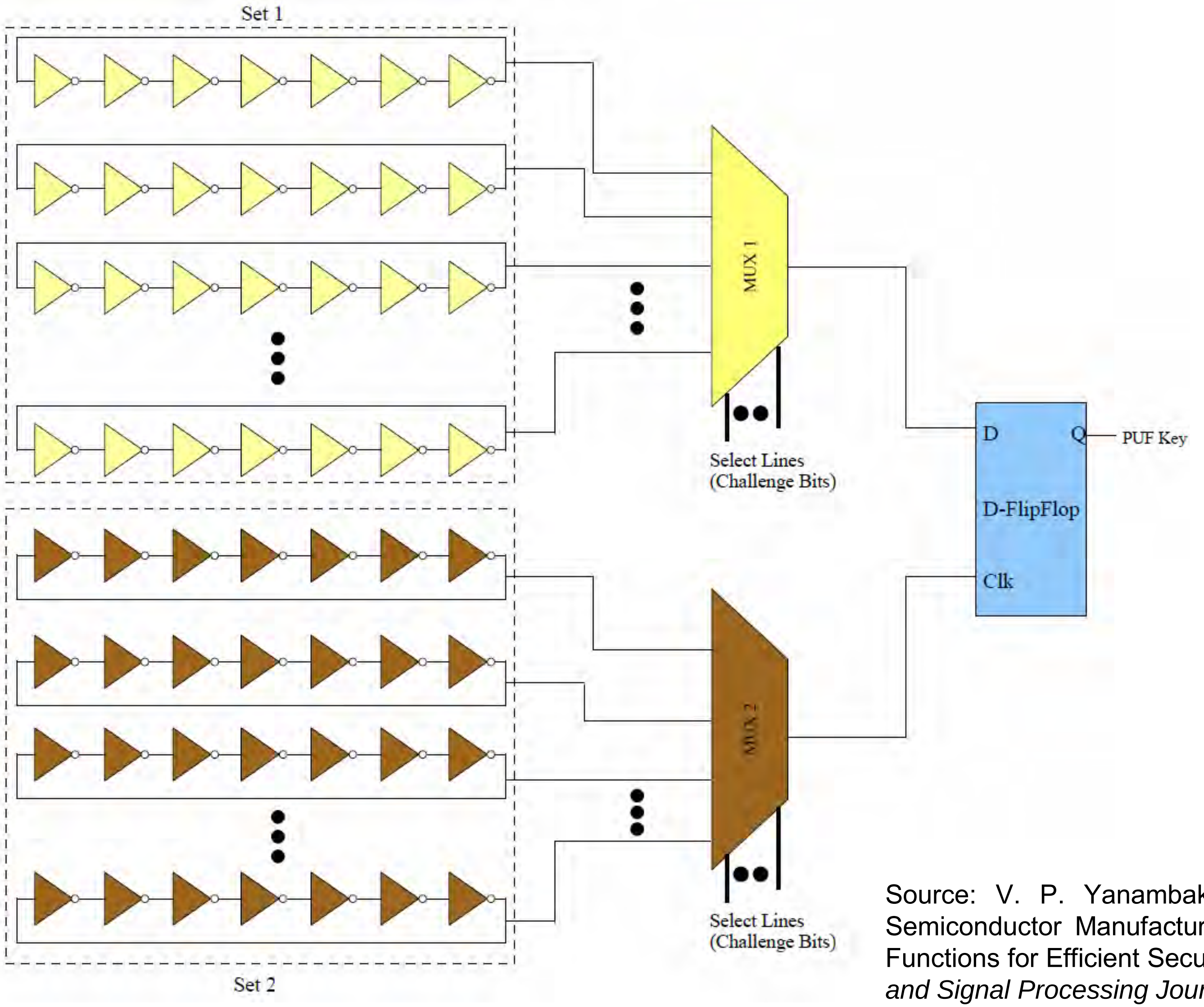
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Conventional Arbiter PUF



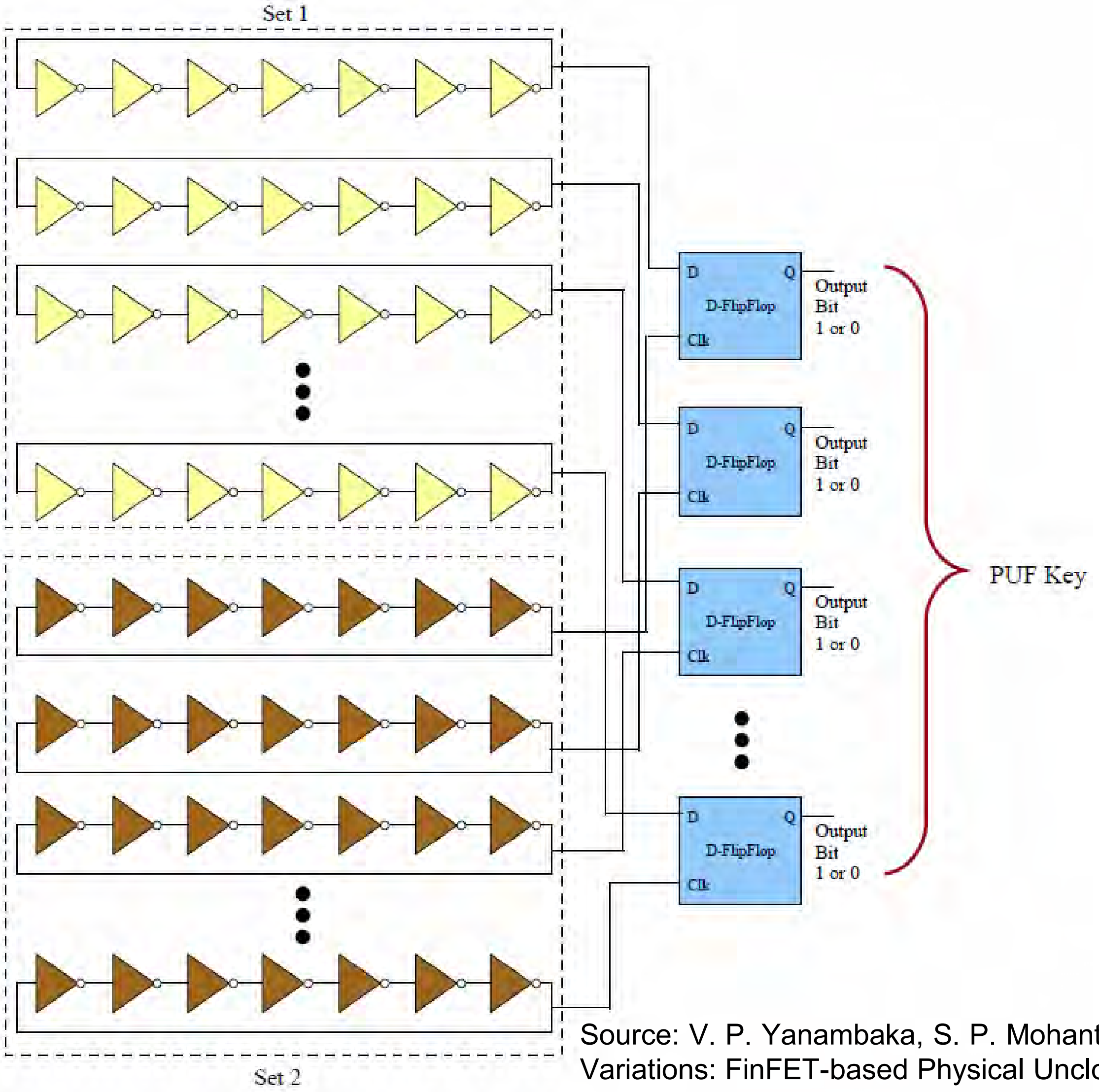
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Power Optimized Hybrid Oscillator Arbiter PUF



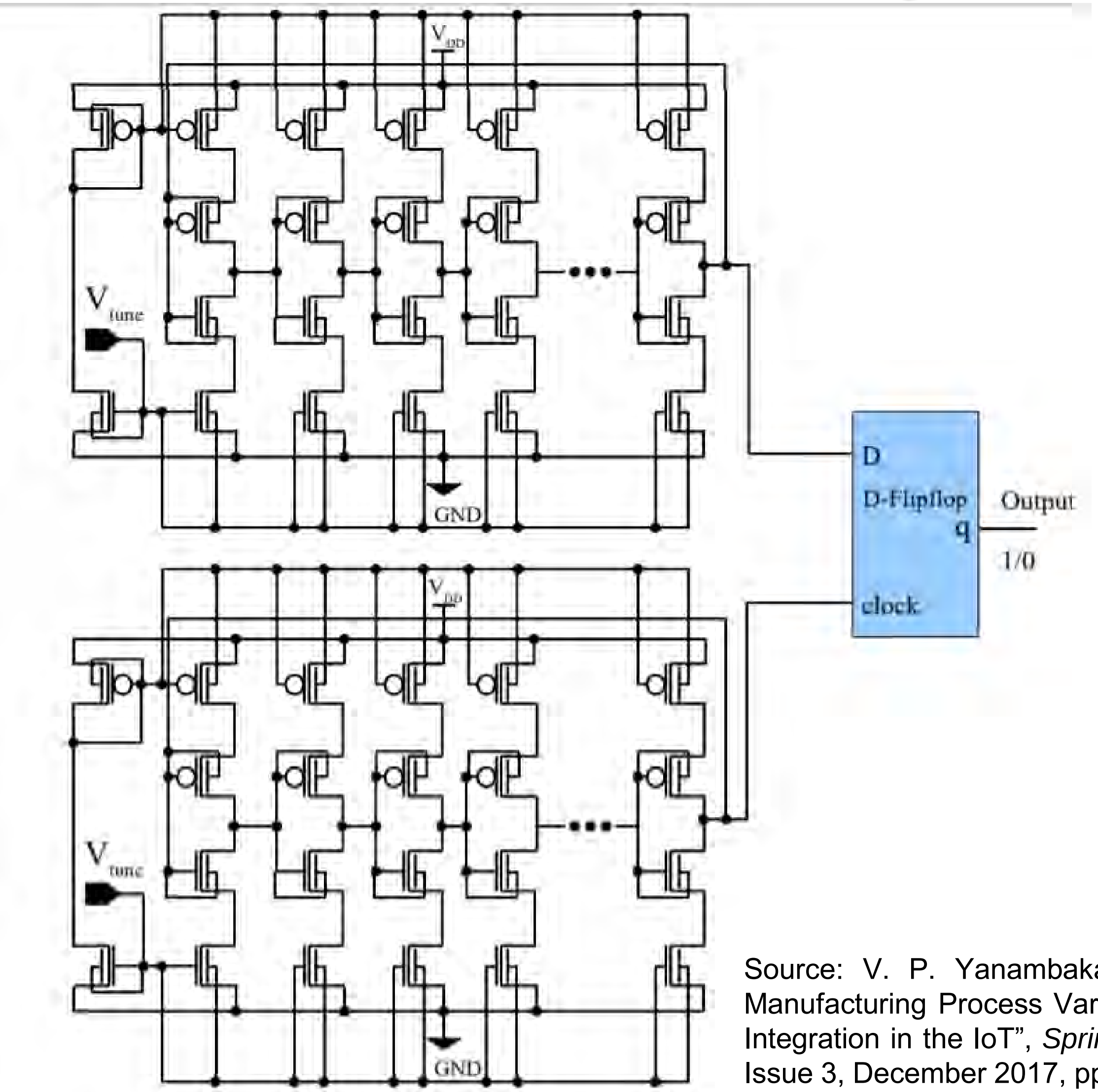
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3,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

Speed Optimized Hybrid Oscillator Arbiter PUF



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

FinFET – Based One Bit Hybrid Oscillator Arbiter PUF



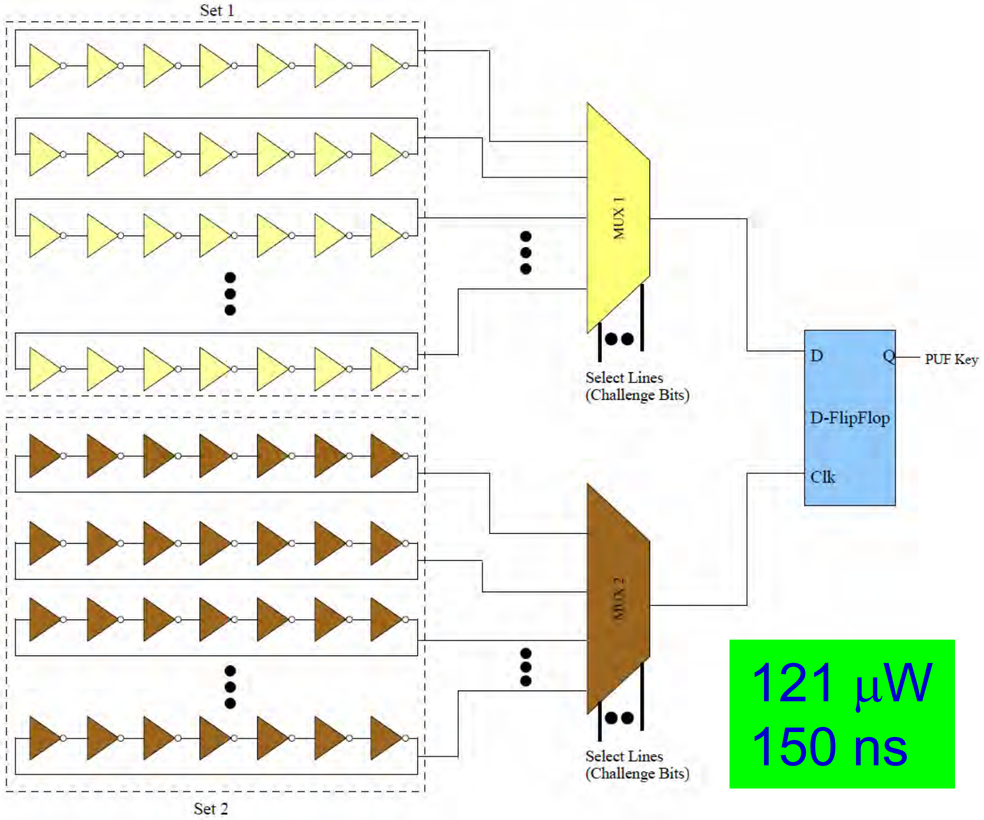
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT", *Springer Analog Integrated Circuits and Signal Processing Journal*, Volume 93, Issue 3,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

Simulation Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [1] (Power Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	285.5 µW	50.9	0.79
Yanambaka et al. [1] (Speed Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	310.8 µW	50.0	0.79
Yanambaka et al. [2] (Power Optimized)	32 nm FinFET	Ring Oscillator Multi-Key Generation PUF	175.5 µW	48.3	50
Yanambaka et al. [2] (Power Optimized)	32 nm FinFET	Ring Oscillator Multi-Key Generation PUF	251 µW	50.1	48.7

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

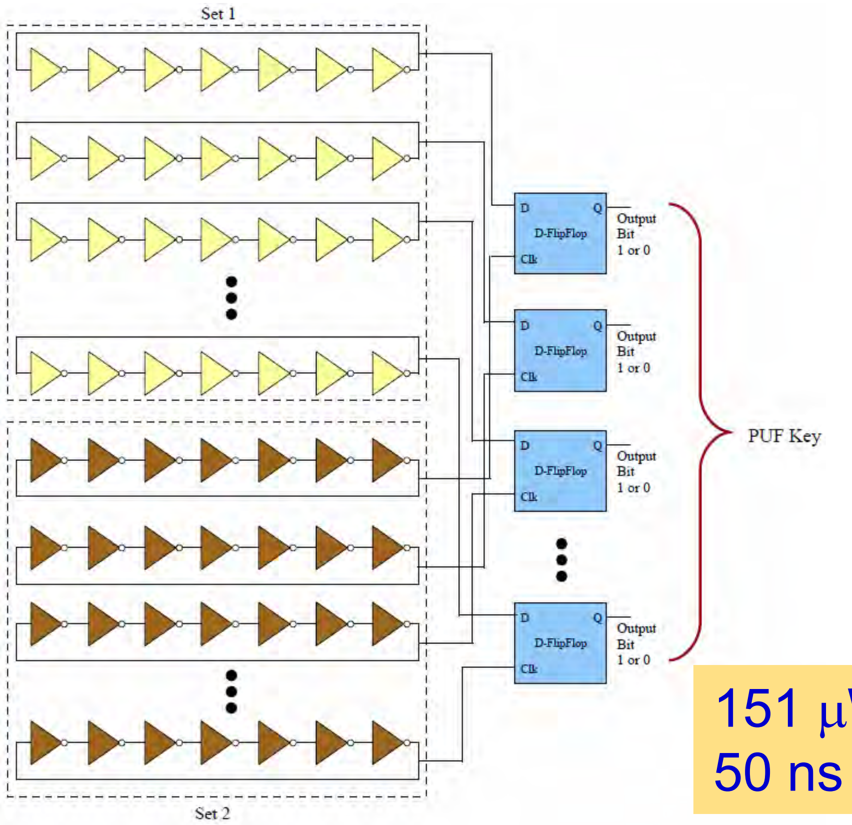
We Have Design a Variety of PUFs - DLFET Based



121 µW
150 ns

Power Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS



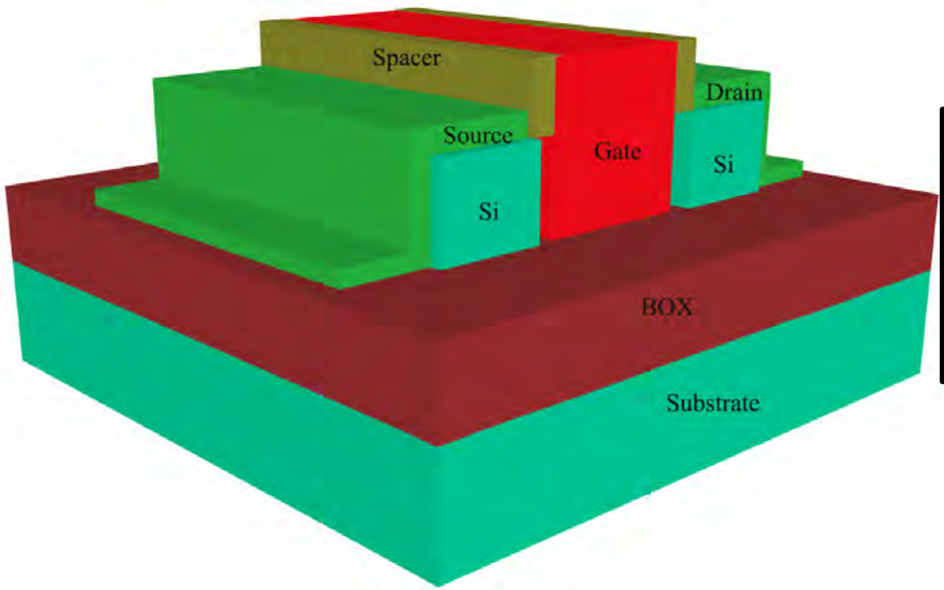
151 µW
50 ns

Speed Optimized Hybrid Oscillator Arbiter PUF

Suitable for Transportation and Energy CPS

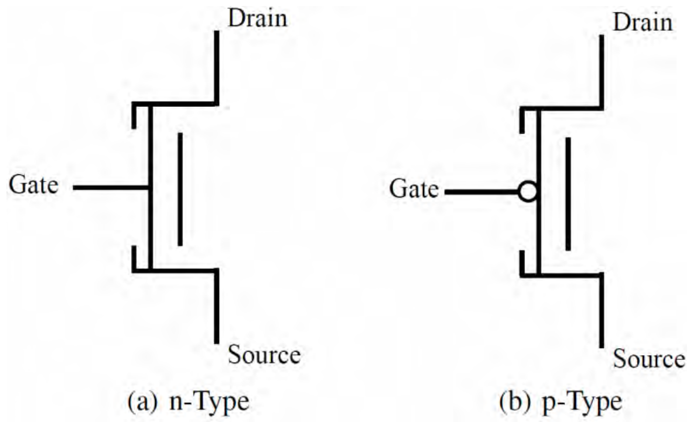
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor



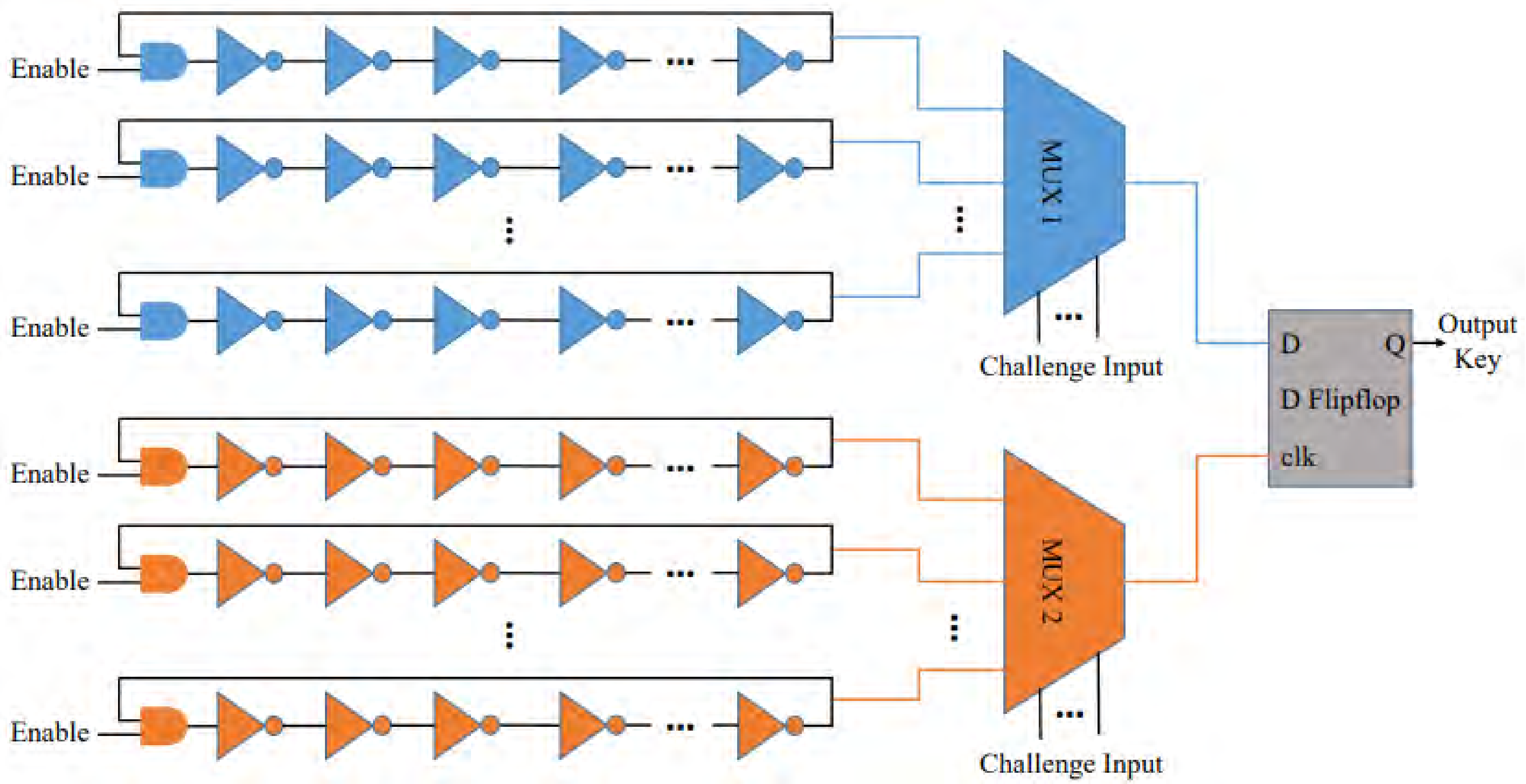
Structure of Dopingless FET

Symbols of n-type and p-type Dopingless FET



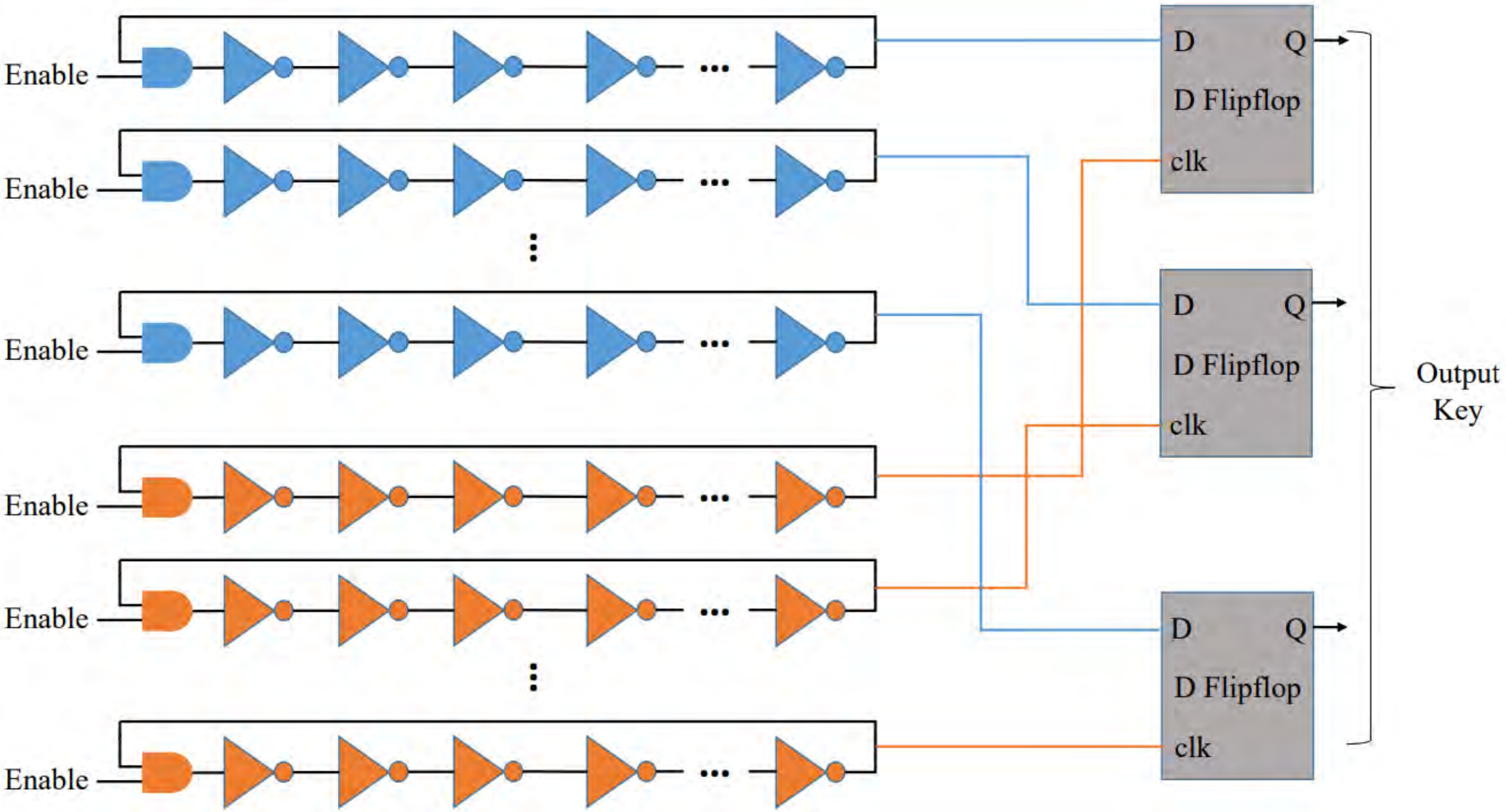
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

DLFET Based Power Optimized Hybrid Oscillator Arbiter PUF



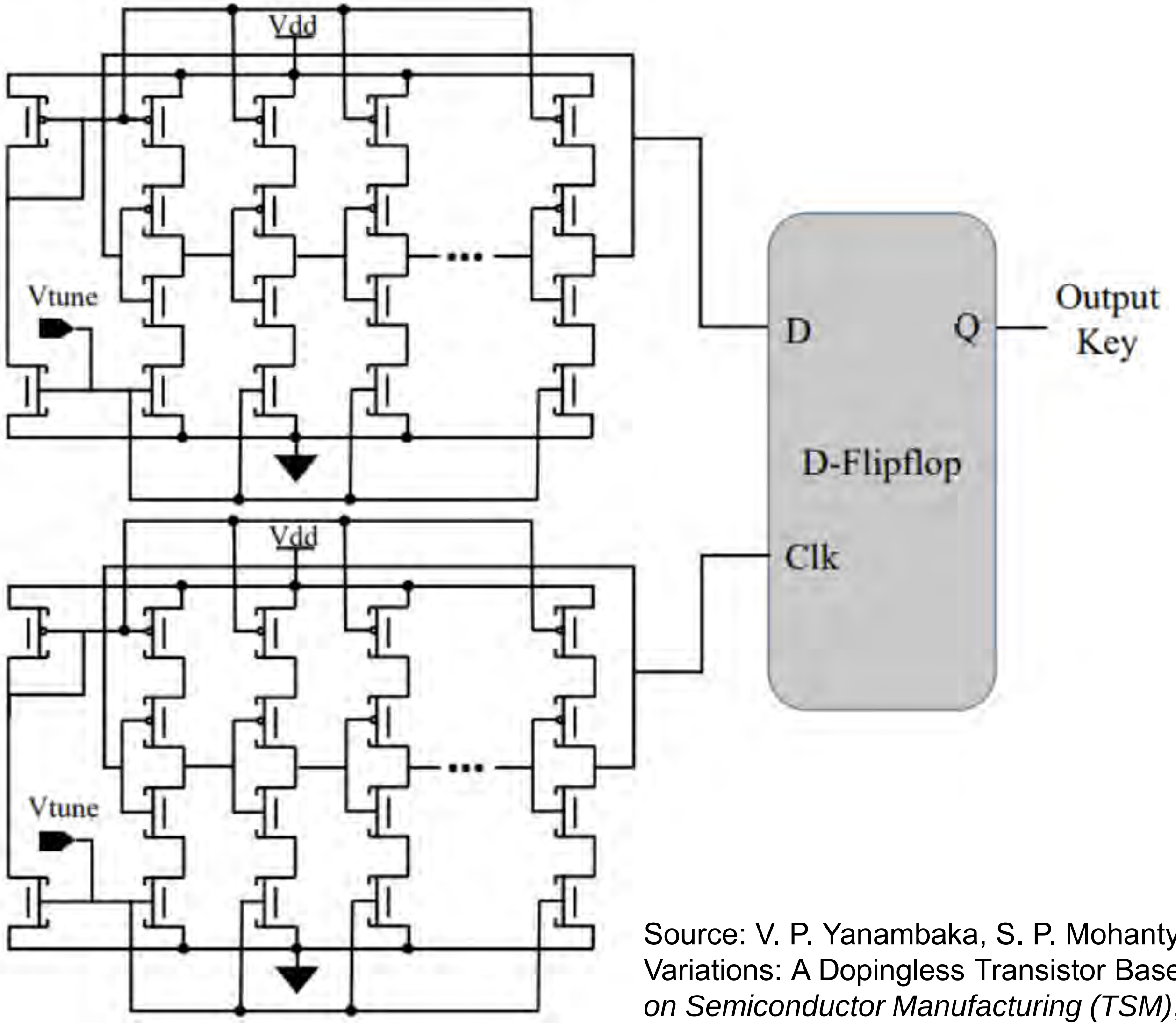
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

DLFET Based Speed Optimized Hybrid Oscillator Arbiter PUF



Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor Device Parameters



Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Dopingless Transistor Device Parameters

Parameters	Dopingless FET
Silicon Film Thickness (T_{si})	10 nm
Effective Oxide Thickness (EOT)	1 nm
Gate Length (L_g)	20 nm
Width (W)	1 μm
Source/Drain extension	10 nm
Metal work function/doping for source/drain	3.9 eV (Hafnium)
Metal work function/doping for gate	4.66 eV (TiN)
Doping	$10^{15}/cm^3$

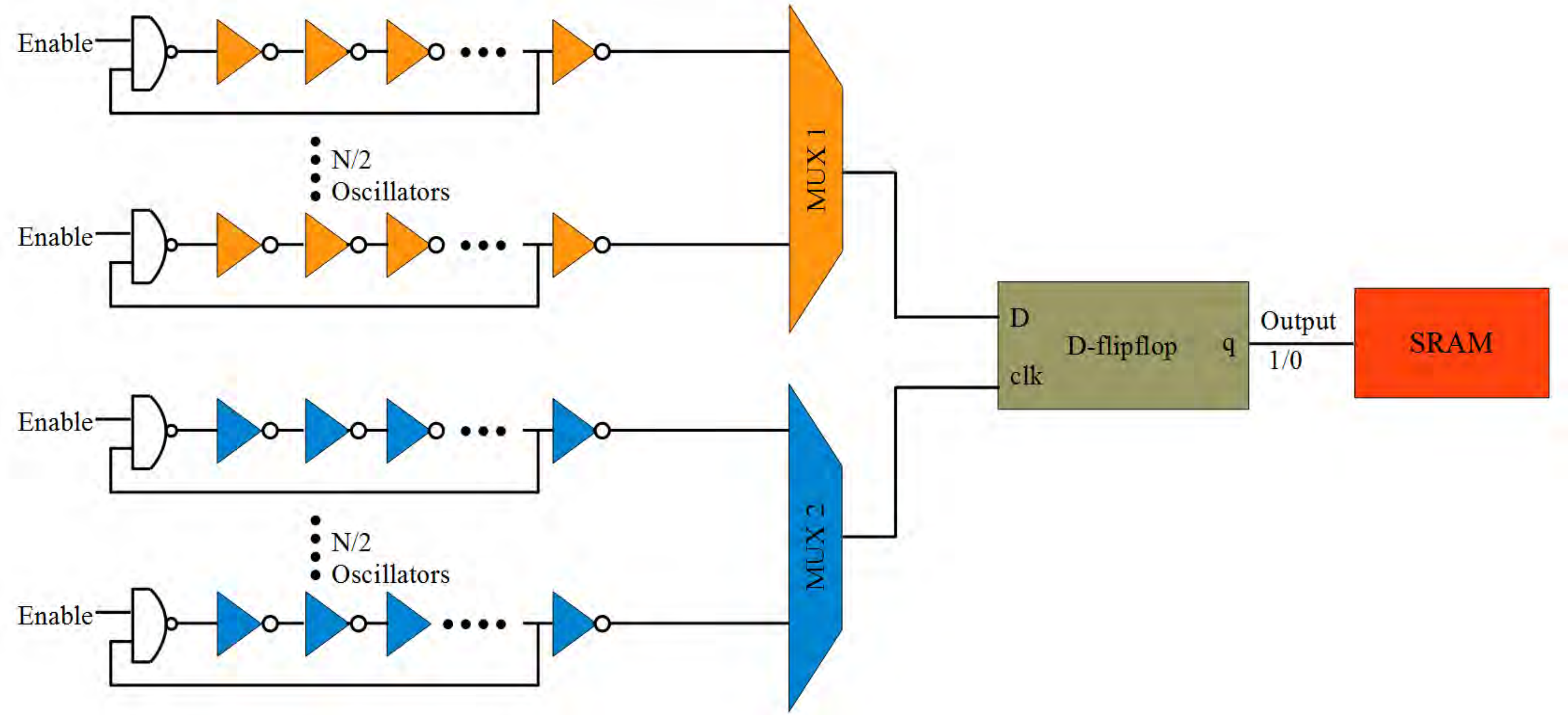
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Simulation Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [3] (Power Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	121.3 µW	50.0	1.9
Yanambaka et al. [3] (Speed Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	310.8 µW	50.0	1.5
Yanambaka et al. [4] (Power Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter PUF	143.3 µW	47.0	1.25
Yanambaka et al. [4] (Speed Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter PUF	167.5 µW	48.0	2.1

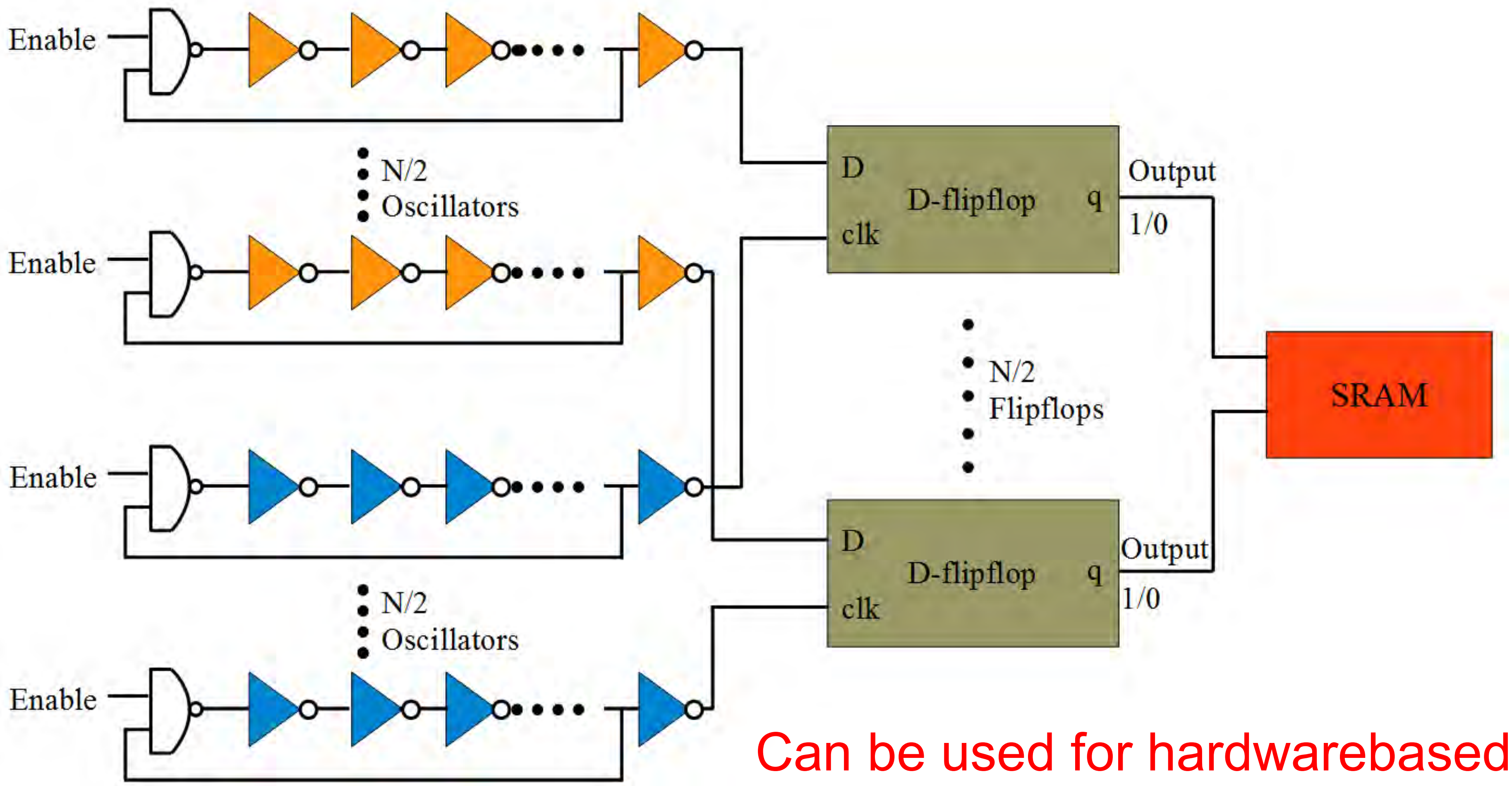
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Multikey Generating PUF



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, and J. Singh, "Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function", in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 200--205.

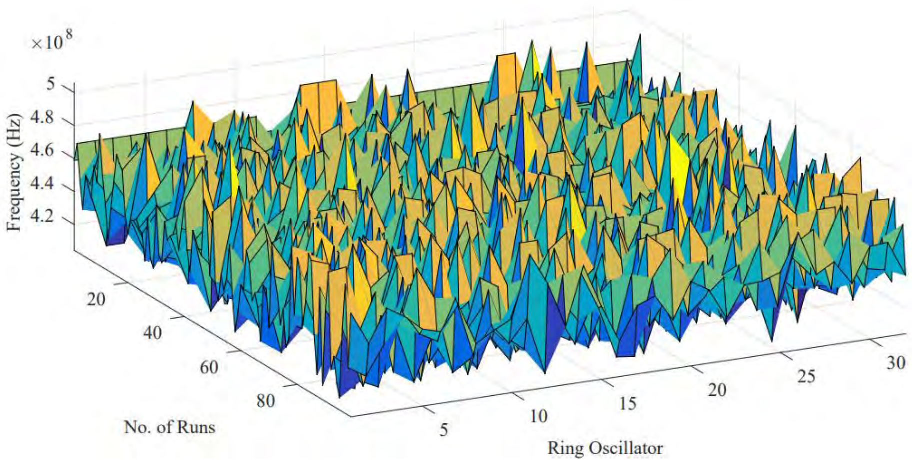
Multikey Generating PUF



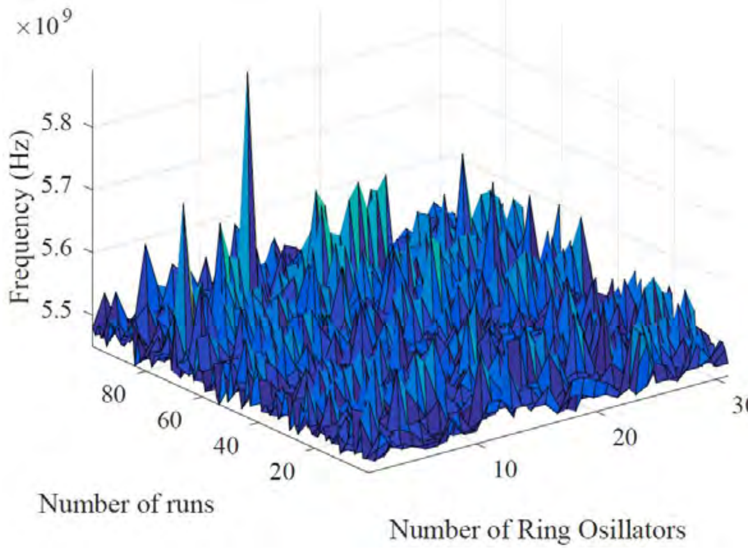
Can be used for hardwarebased OTP generation.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, and J. Singh, "Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function", in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 200--205.

Frequencies of Different Ring Oscillators



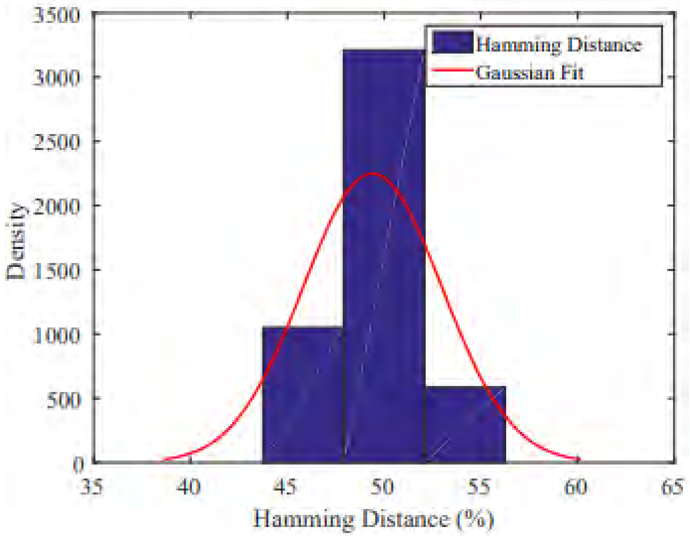
FinFET Based Ring Oscillators



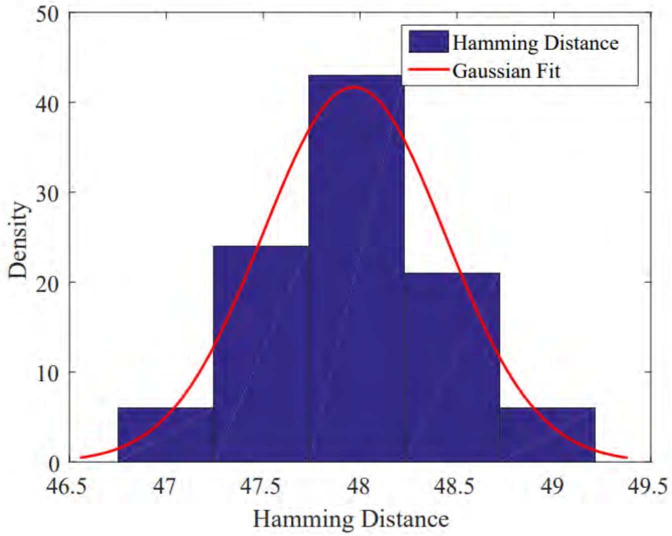
DLFET Based Ring Oscillators

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

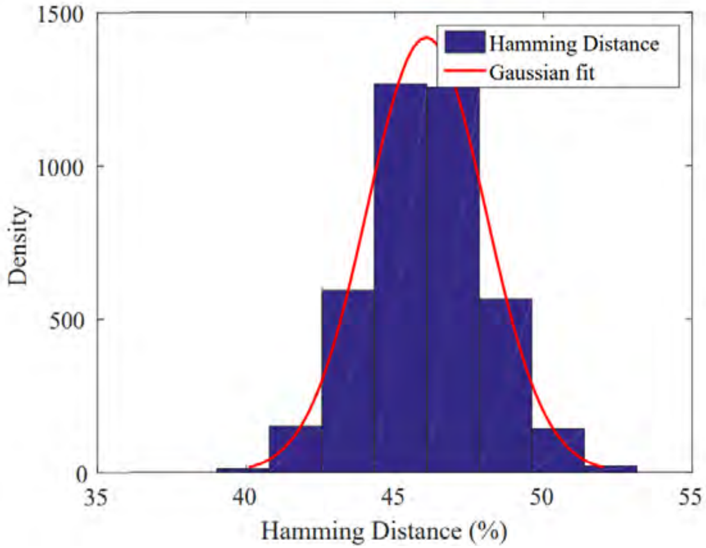
Uniqueness of Power-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



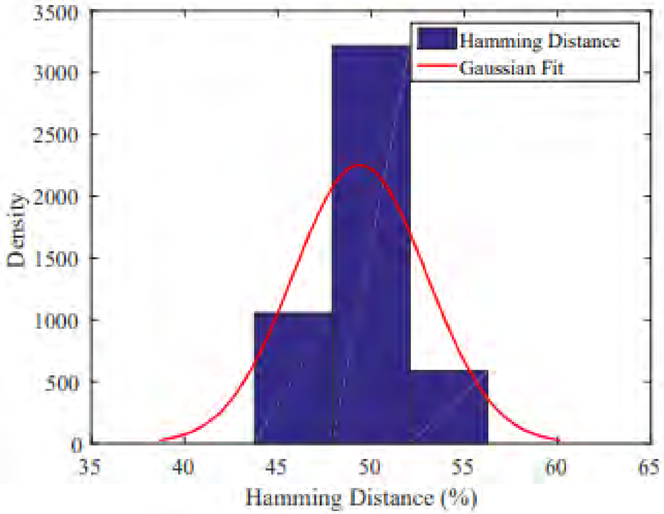
DLFET Based Hybrid Oscillator Arbiter PUF



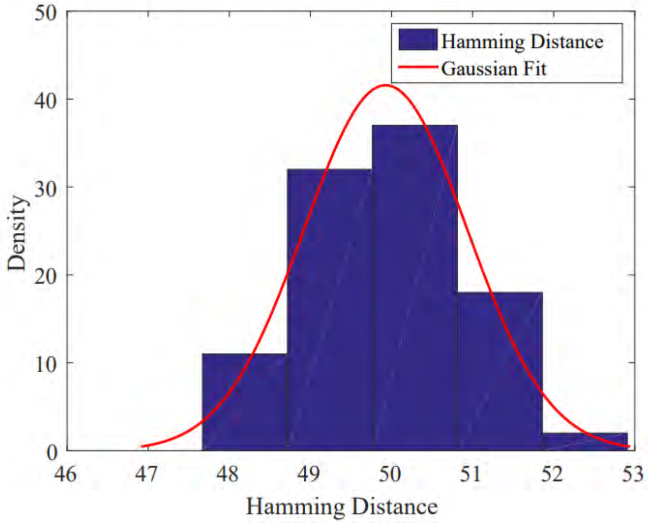
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

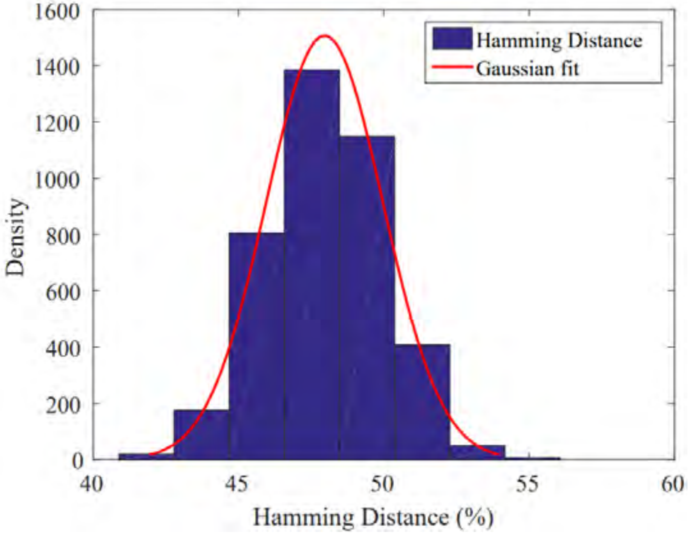
Uniqueness of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



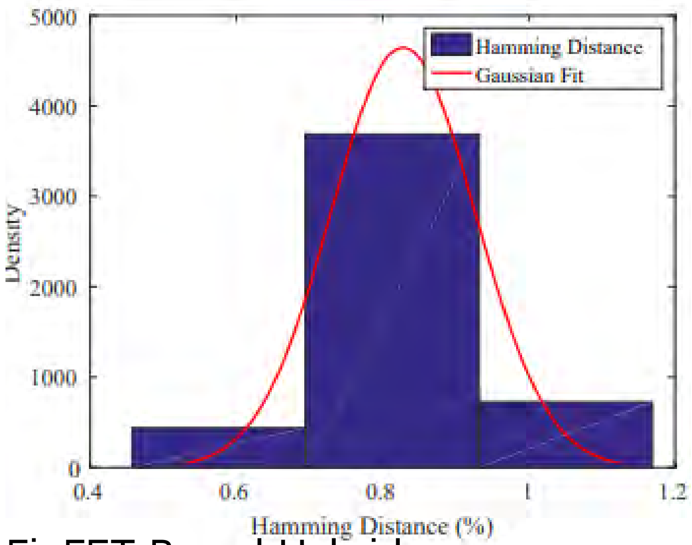
DLFET Based Hybrid Oscillator Arbiter PUF



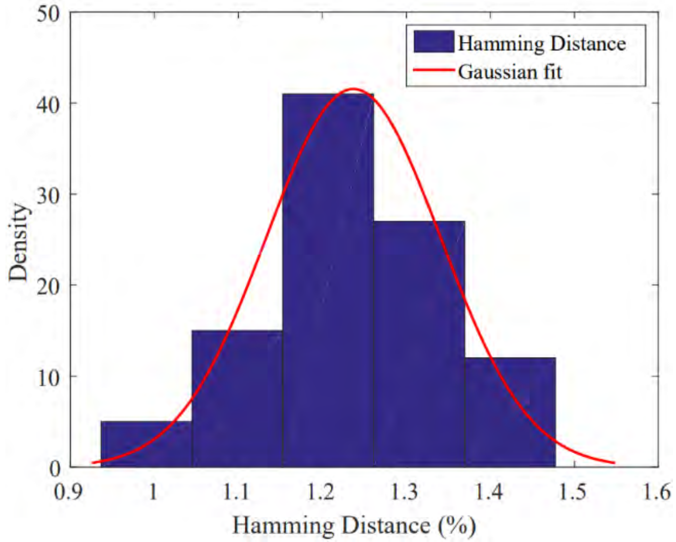
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

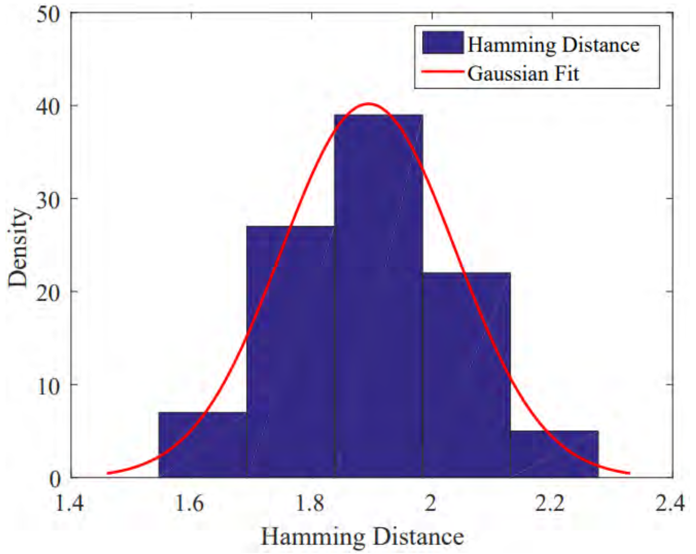
Reliability of Power-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



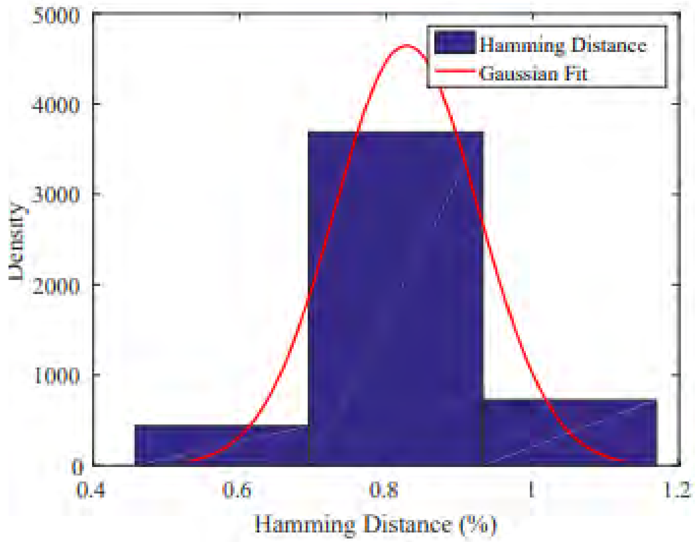
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF



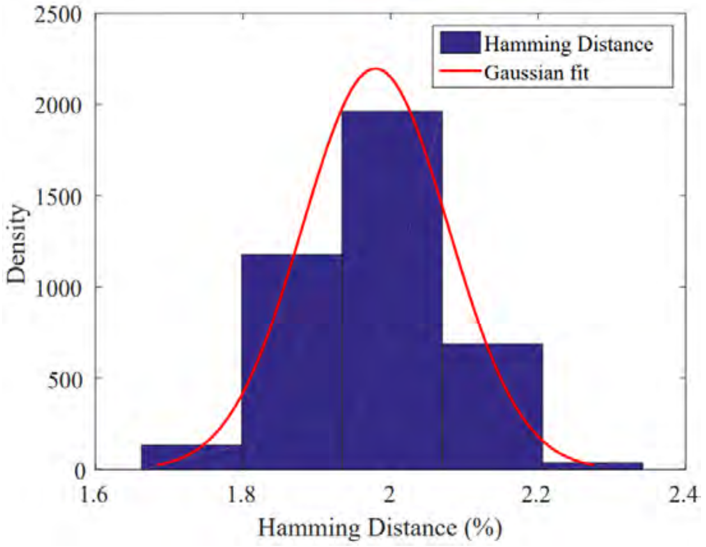
DLFET Based Hybrid Oscillator Arbiter PUF

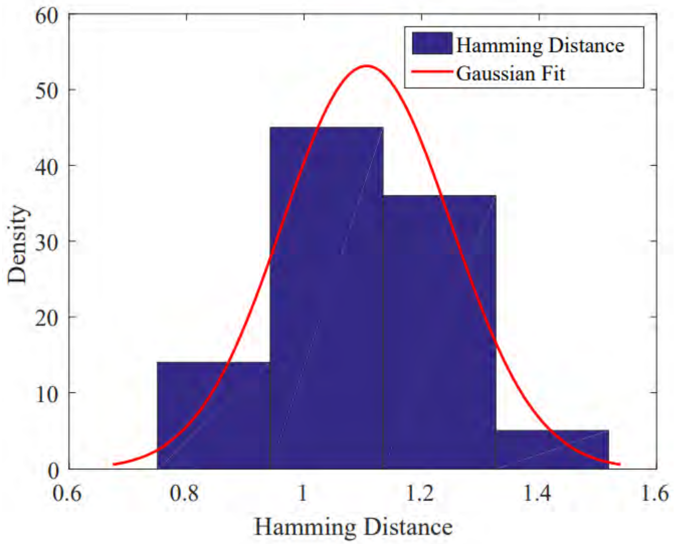
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Reliability of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



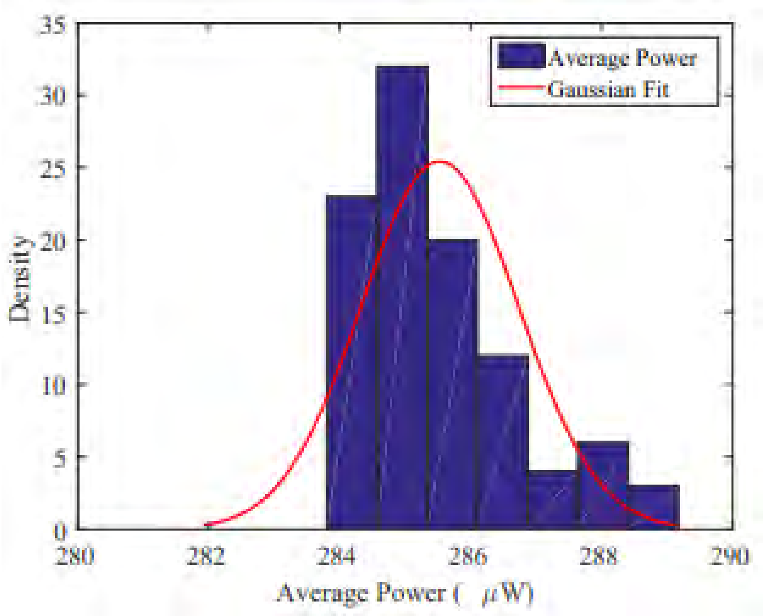


DLFET Based Hybrid Oscillator Arbiter PUF

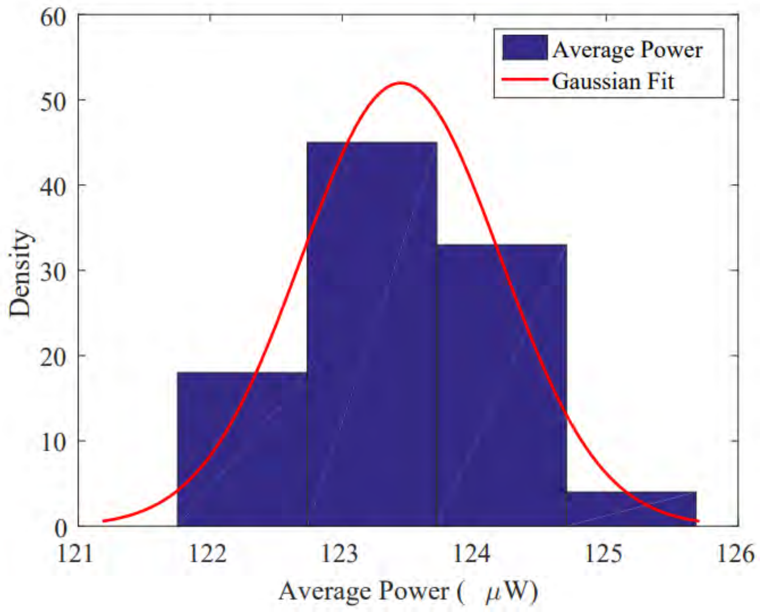
DLFET Based Reconfigurable Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Average Power of Power-Optimized PUF



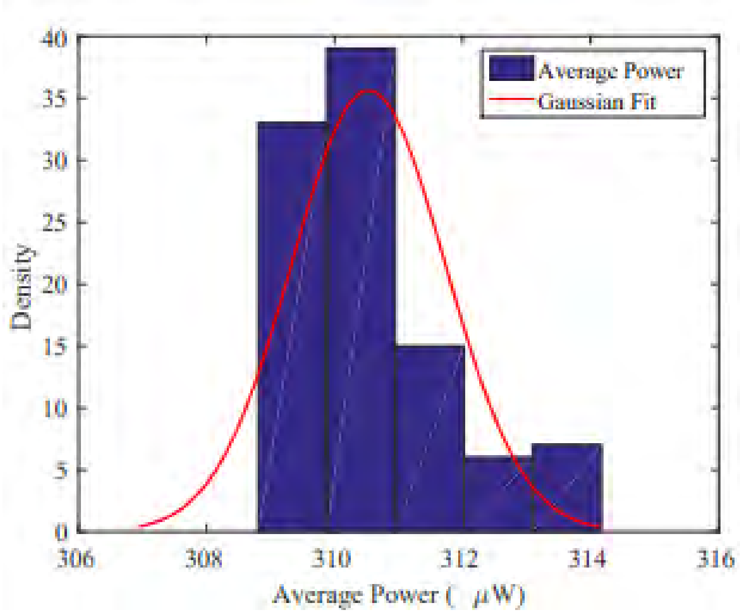
FinFET Based Hybrid Oscillator Arbiter PUF



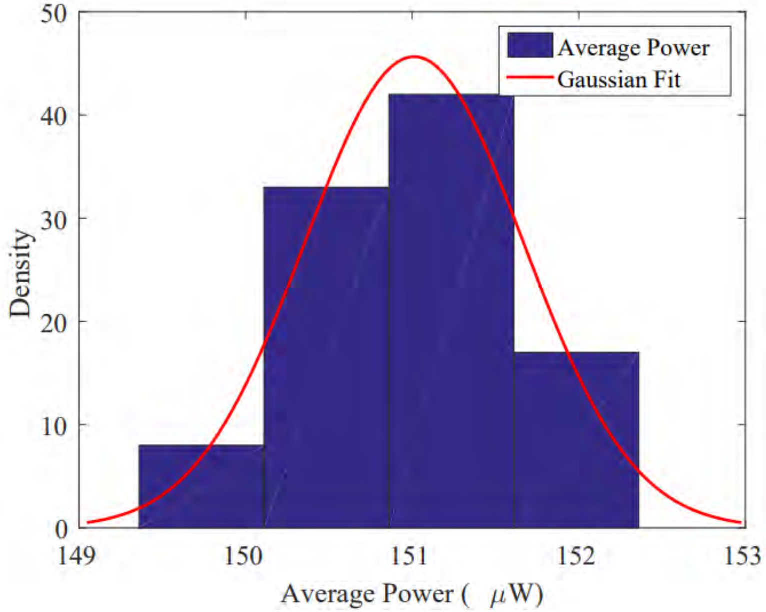
DLFET Based Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Average Power of Speed-Optimized PUF



FinFET Based Hybrid Oscillator Arbiter PUF



DLFET Based Hybrid Oscillator Arbiter PUF

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security", *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Randomness of Hybrid Oscillator Arbiter PUF

	Power Optimized PUF	Speed Optimized PUF
32nm FinFET Based Hybrid Oscillator Arbiter PUF	42	42
DLFET Based Hybrid Oscillator Arbiter PUF	47.5	51.3
DLFET Based Reconfigurable PUF	48	46

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Time to Generate Keys

	Power Optimized PUF	Speed Optimized PUF
32nm FinFET Based Hybrid Oscillator Arbiter PUF	150 ns	50 ns
DLFET Based Hybrid Oscillator Arbiter PUF	150 ns	50 ns
DLFET Based Reconfigurable PUF	200 ns	100 ns

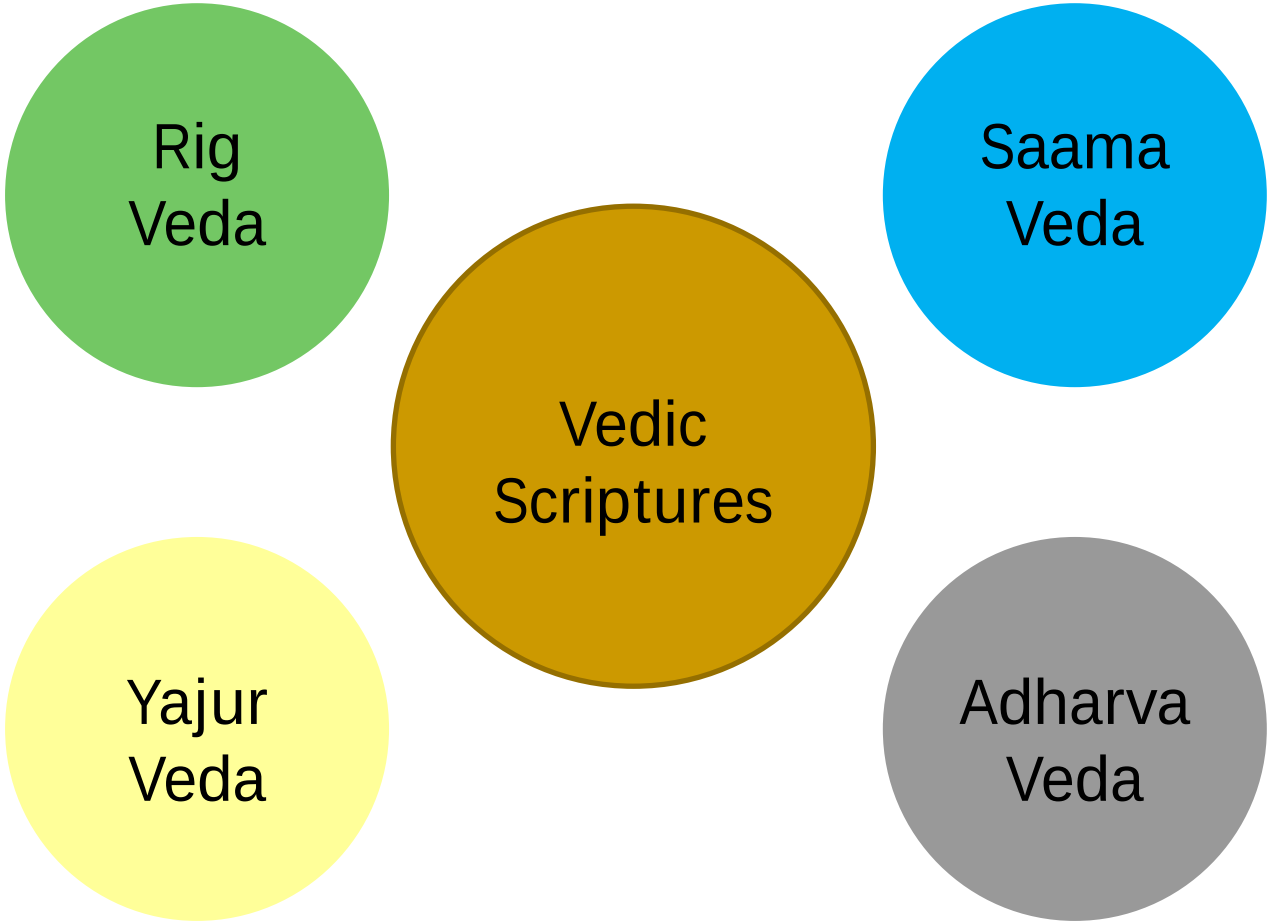
Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

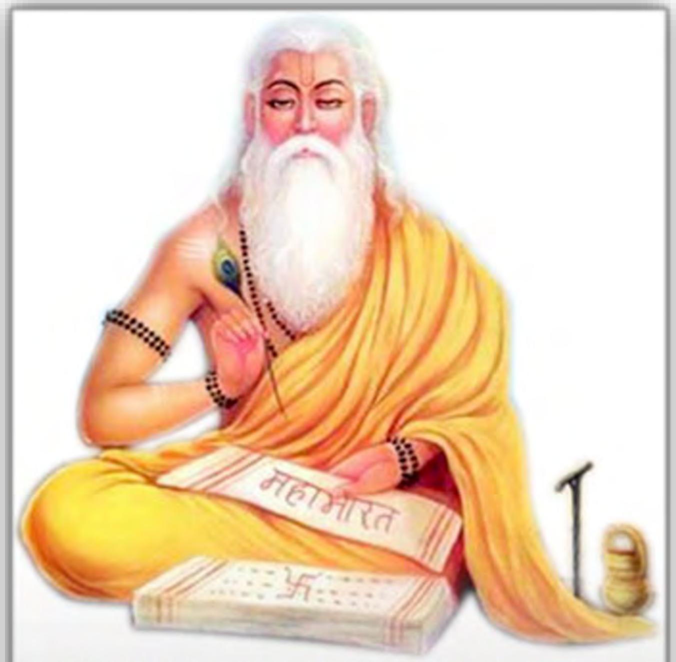
Comparison of Results

Research Work	Technology	Architecture Used	Power Consumption	Uniqueness (%)	Reliability (%)
Yanambaka et al. [1] (Power Optimized)	32 nm FinFET	Current Starved VCO Hybrid Oscillator Arbiter PUF	285.5 µW	50.9	0.79
Yanambaka et al. [3] (Power Optimized)	10 nm Dopingless FET	Current Starved VCO Hybrid Oscillator Arbiter PUF	121.3 µW	50.0	1.9
Yanambaka et al. [4] (Power Optimized)	10 nm Dopingless FET	ReconfigurableHybrid Oscillator Arbiter PUF	143.3 µW	47.0	1.25
S. R. Sahoo, et al. [5]	90 nm CMOS	Ring Oscillator	-	45.78	-
Maiti, et al. [6]	90nm CMOS	Ring Oscillator	-	47.31	0.86
Cherkaoui, et al. [7]	350 nm CMOS	Transient Effect Ring Oscillator	-	49.7	0.6

Source: V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, *IEEE Transactions on Semiconductor Manufacturing (TSM)*, Volume 31, Issue 2, May 2018, pp. 285--294.

Vedas – Ancient Indian Scriptures





Credit by: www.hindufaqs.com

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Vedic Chanting

- Vedas were passed down through generations using mnemonic techniques.
- To ensure their integrity, two aspects were added to Vedas
  - Tones
    - Udaatta, Anudaatta, Svarita, Deergha Svarita
  - Pathas
    - Pada, Krama, etc.,

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

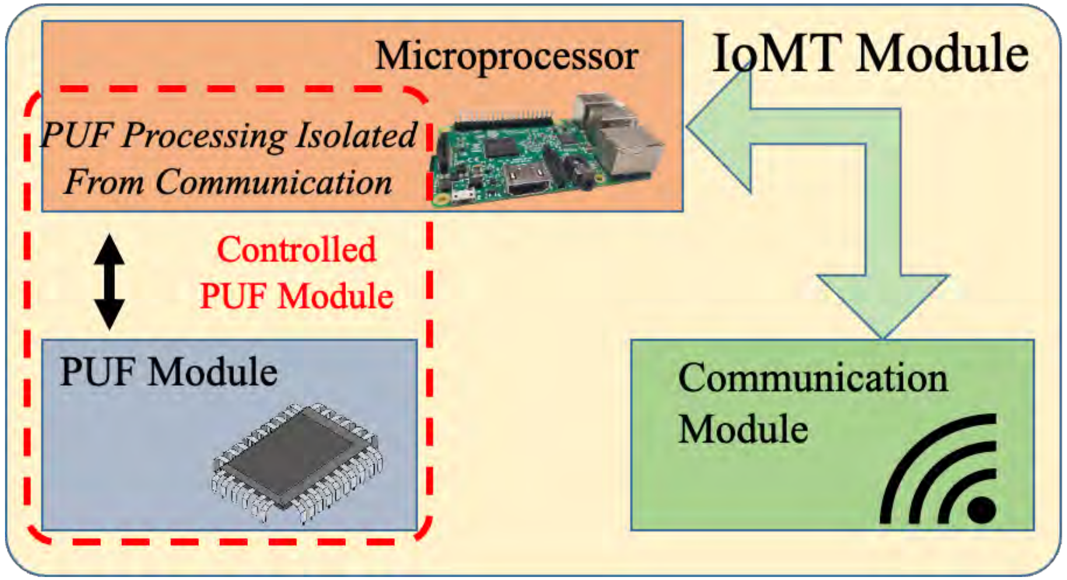
Why Veda for PUF?

- The key length increases significantly
- Number of keys around the ideal value increases significantly.
  - Keys around 54 % uniqueness decreased and 50 % increased.
  - Number of keys with randomness around 48 % increased significantly.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Proposed Veda – PUF Architecture

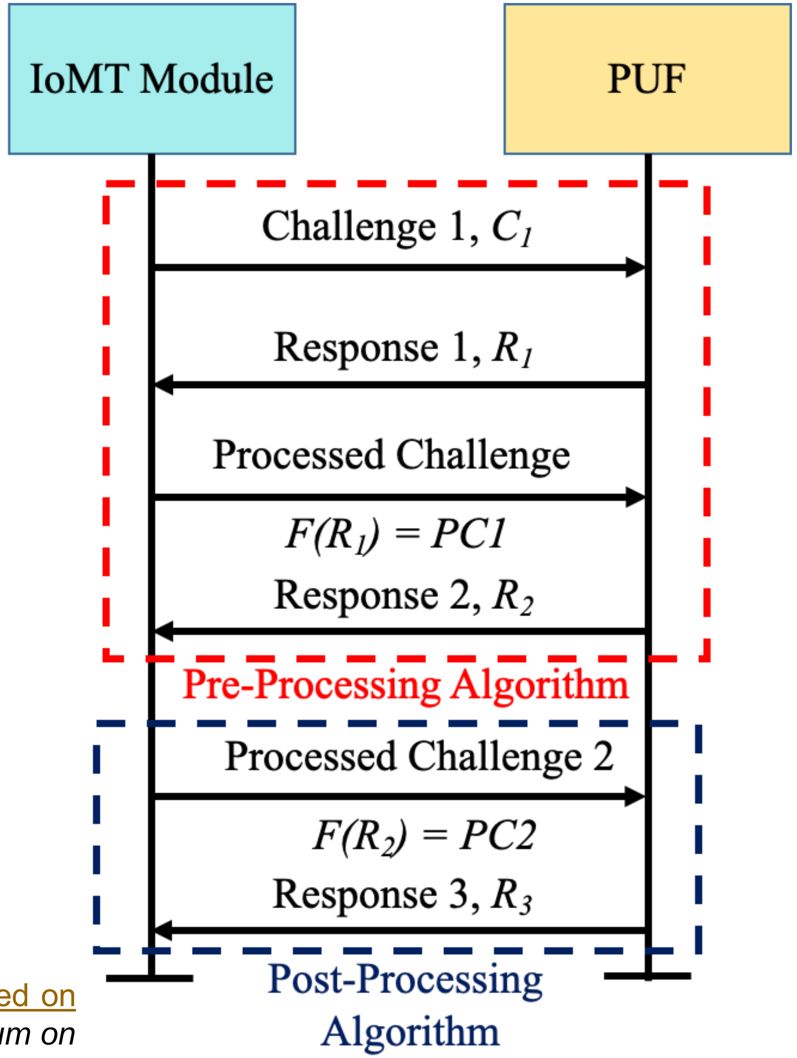
- Veda – PUF is a controlled PUF.
- Challenges and Responses are processed in the PUF.
- Communication module is isolated from the PUF.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Proposed Controller Algorithm for Veda – PUF

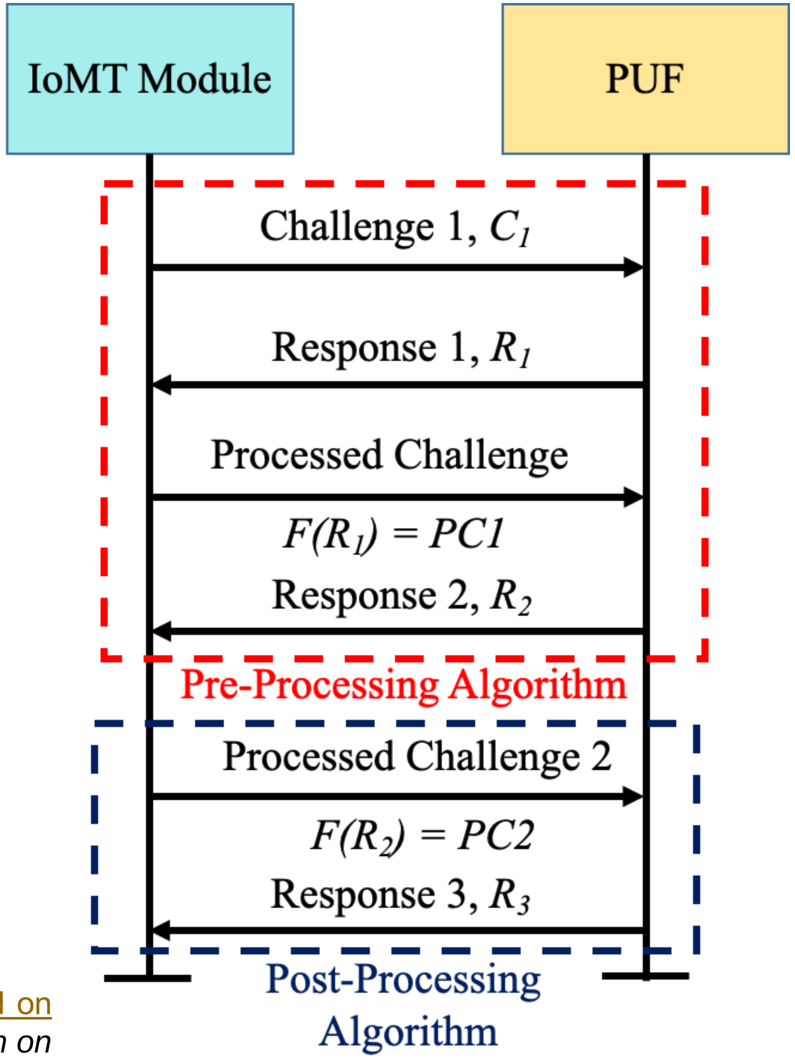
- Pre – Processing Algorithm
  - The first stage in key generation.
  - Generate the first response for a challenge and process it for the second stage.
- Post – Processing Algorithm
  - Generates the final response with increased key length.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

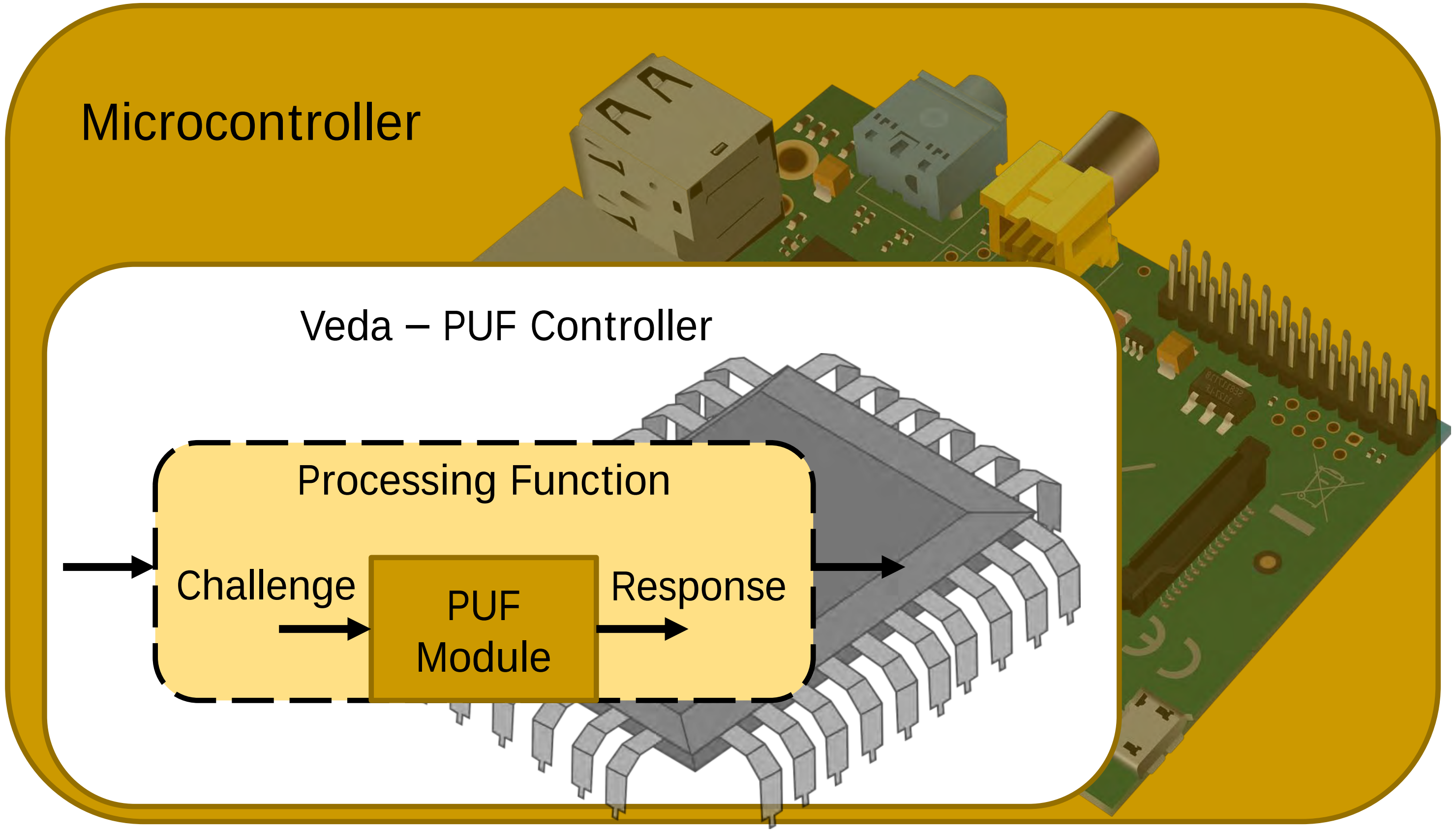
Key Processing Function Veda – PUF

- Considering the following binary key:
  - b1, b2,…. bn
- Ghana Paatha formula is used for the bits b1 -> bn-1.
- Jata Paatha formula is used for the last two bits.



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

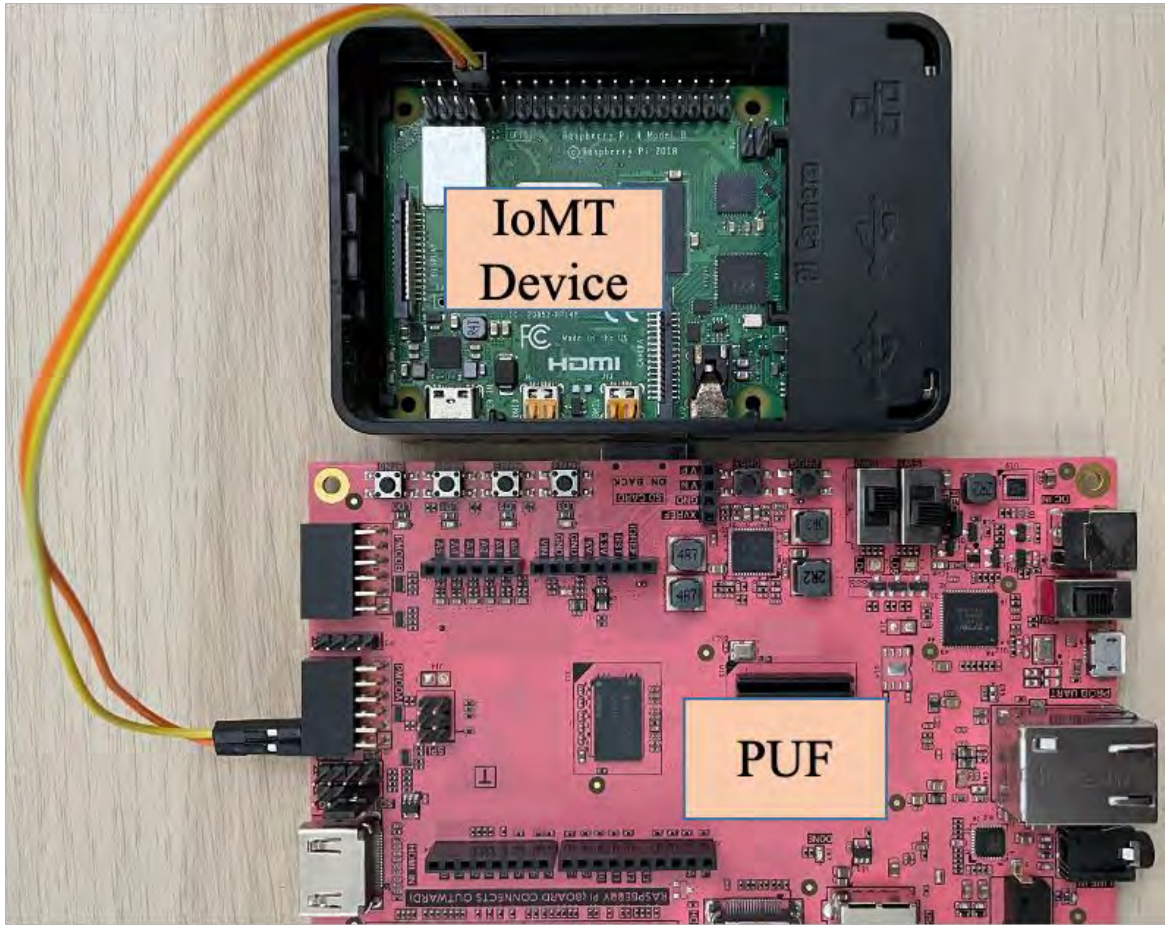
Veda-PUF Circuits



Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

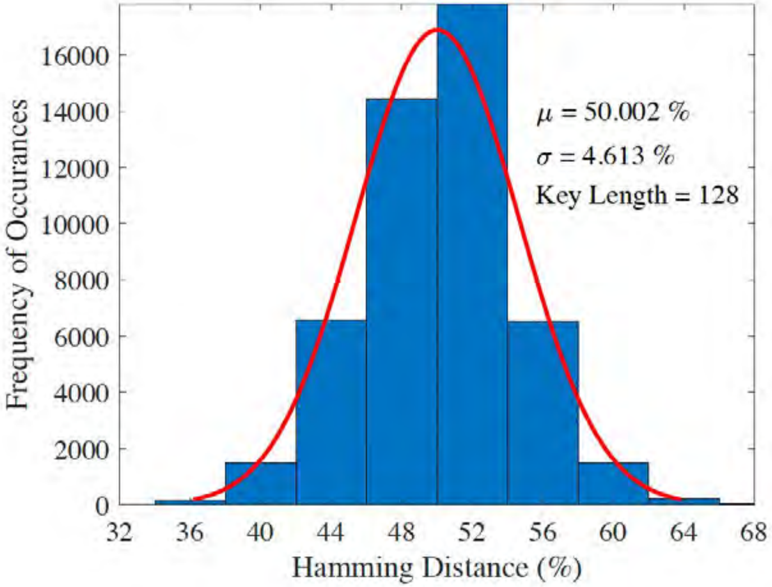
Experimental Setup

- Initial Considerations:
  - Initial challenge length is 128 – bits.
  - 1000 keys were generated.
  - Raspberry Pi– Key Generation IoMT device.
  - FPGA – PUF.

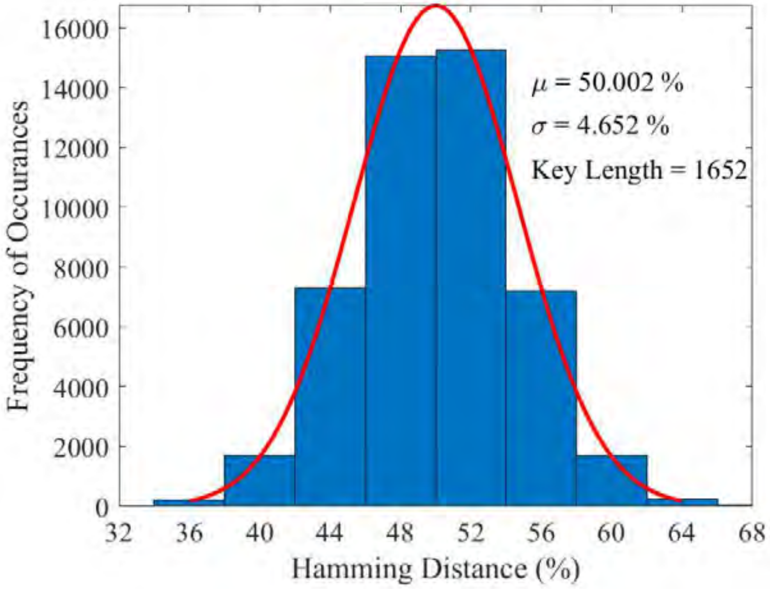


Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

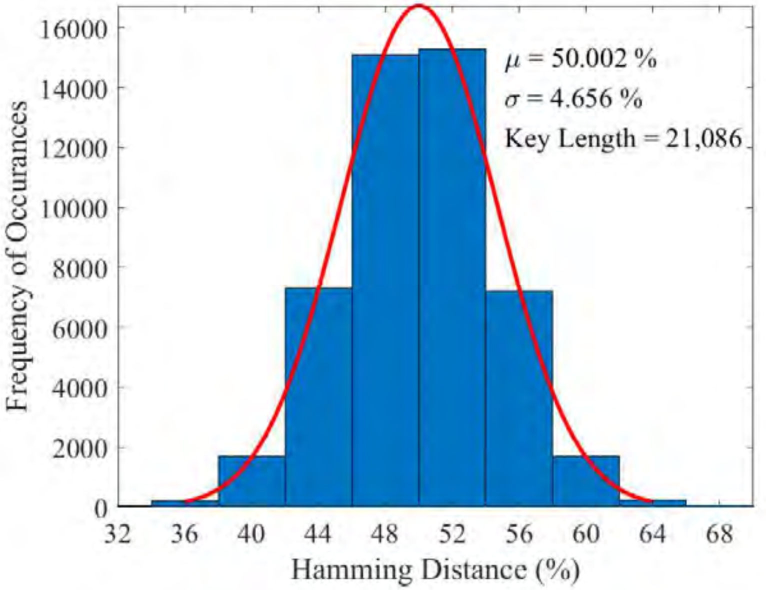
Characterization - Uniqueness



(a) Uniqueness of Original Keys



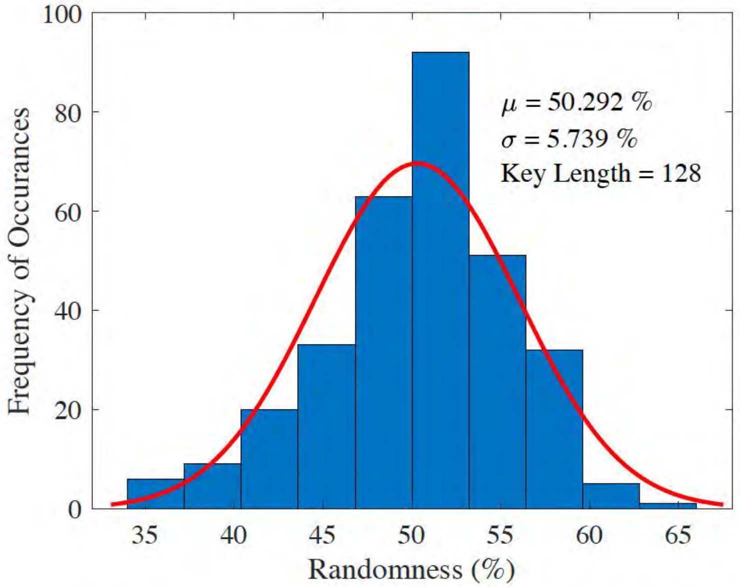
(b) Uniqueness of Processed Keys



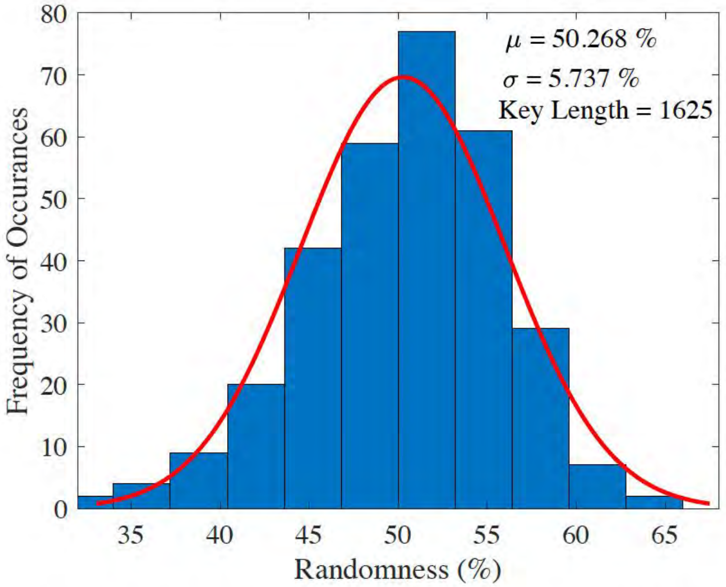
(c) Uniqueness of Keys Processed a Second Time

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

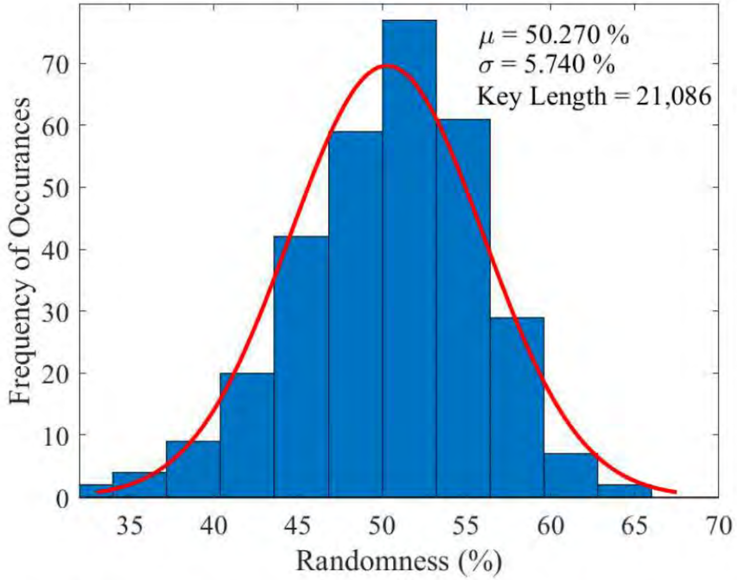
Characterization - Randomness



(a) Randomness of Original Keys



(b) Randomness of Processed Keys



(c) Randomness of Keys Processed a Second Time

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Reliability and Power Consumption

PUF Characteristic	Original Key	Processed Key
Uniqueness		
Mean	50.002 %	50.002 %
Standard Deviation	4.613 %	4.656 %
Reliability		
Mean	99.9 %	99.9 %
Standard Deviation	0 %	0 %
Randomness		
Mean	50.292 %	50.270 %
Standard Deviation	5.739 %	5.740 %
Power Consumption	3.1 W	3.25 W

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Veda-PUF: Conclusion and Future Research

- Key length increased significantly preserving the integrity.
  - 128 – bit key length increased to around 2.1 Kbits
- The number of keys at the ideal uniqueness and ideal randomness increased.
- Develop a machine learning resistant algorithm based on the Veda – PUF Architecture.

Source: V. P. Yanambaka, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT", in *Proceedings of the 7th IEEE International Symposium on Smart Electronic Systems (iSES)*, 2021, pp. 400--405, DOI: https://doi.org/10.1109/iSES52644.2021.00097.

Physical Unclonable Function
- Challenges and Research

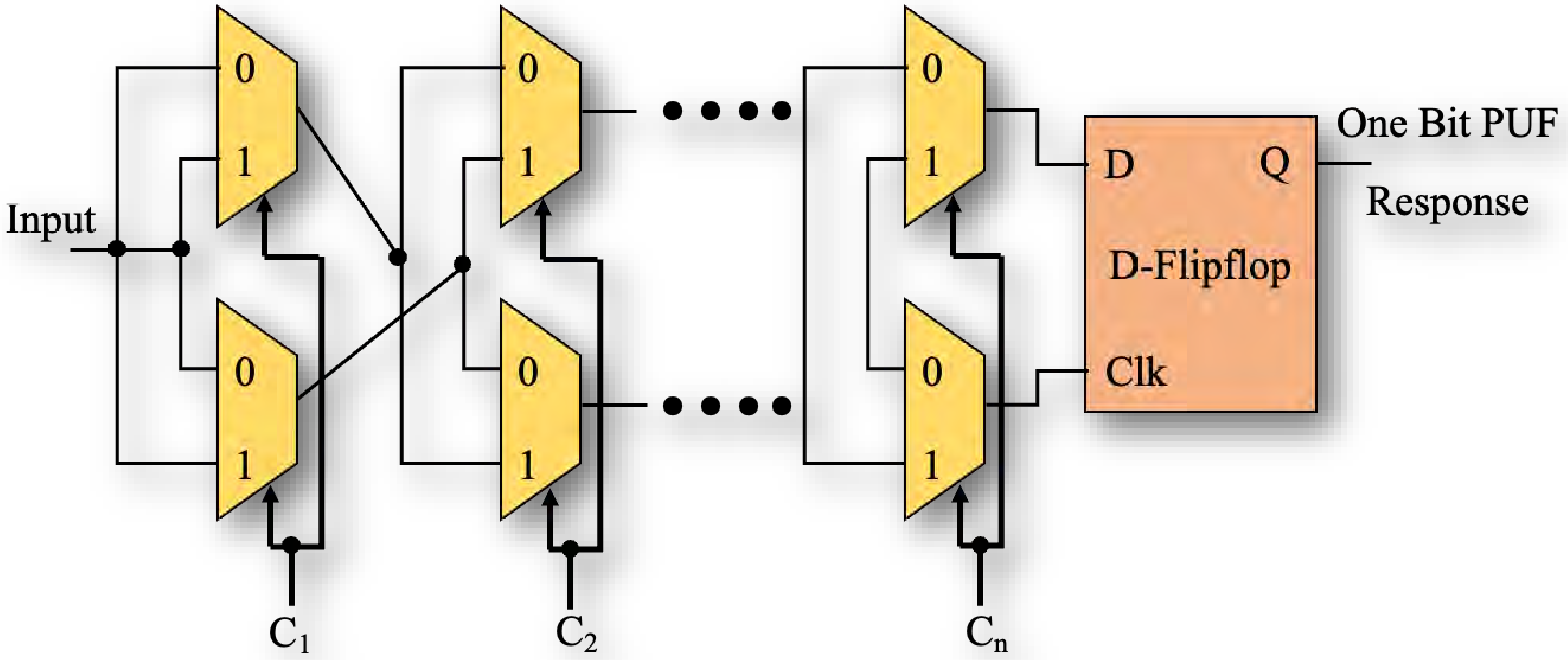
If PUF is So Great, Why Isn't Everyone Using It?

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

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

PUF Limitations – Larger Key Needs Large ICs

- Larger key requires larger chip circuit.



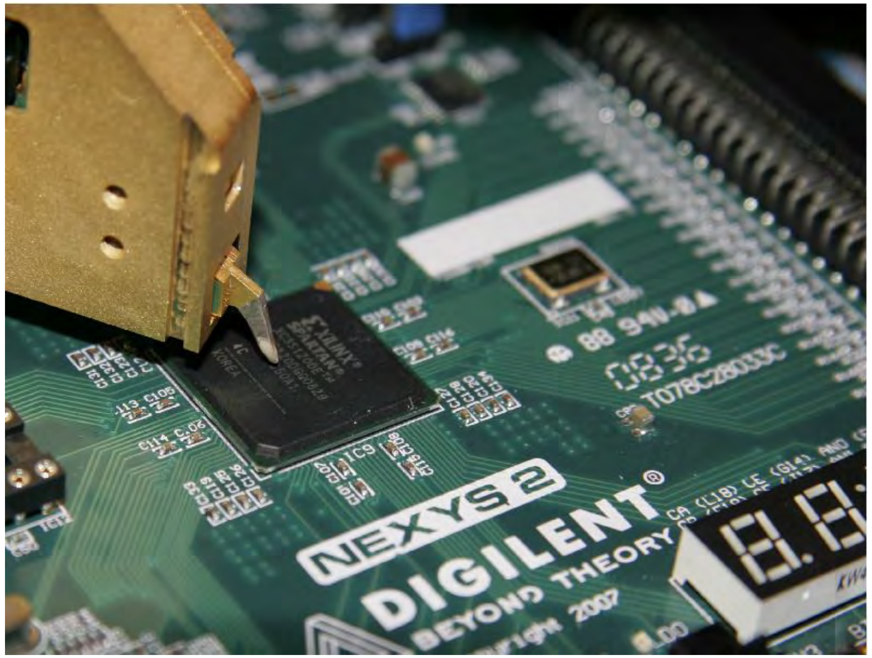
1 – Bit Arbiter PUF Architecture

PUF - Side Channel Leakage

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

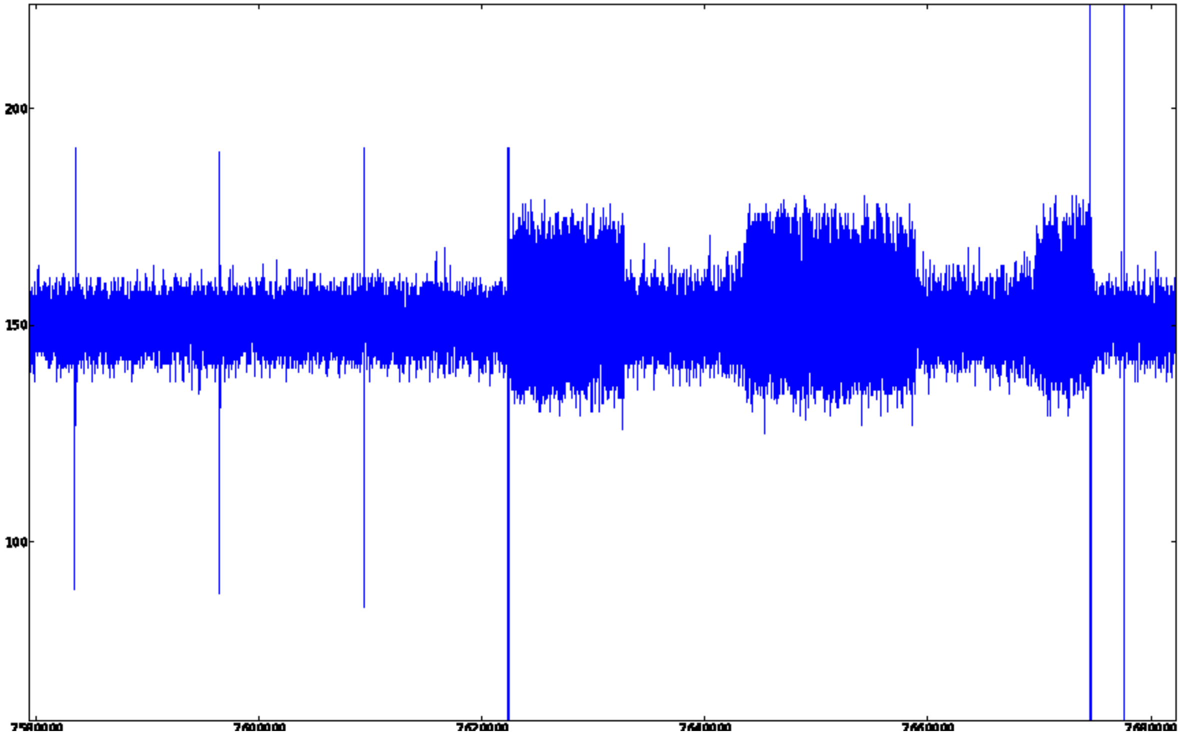
PUF - Side Channel Leakage

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



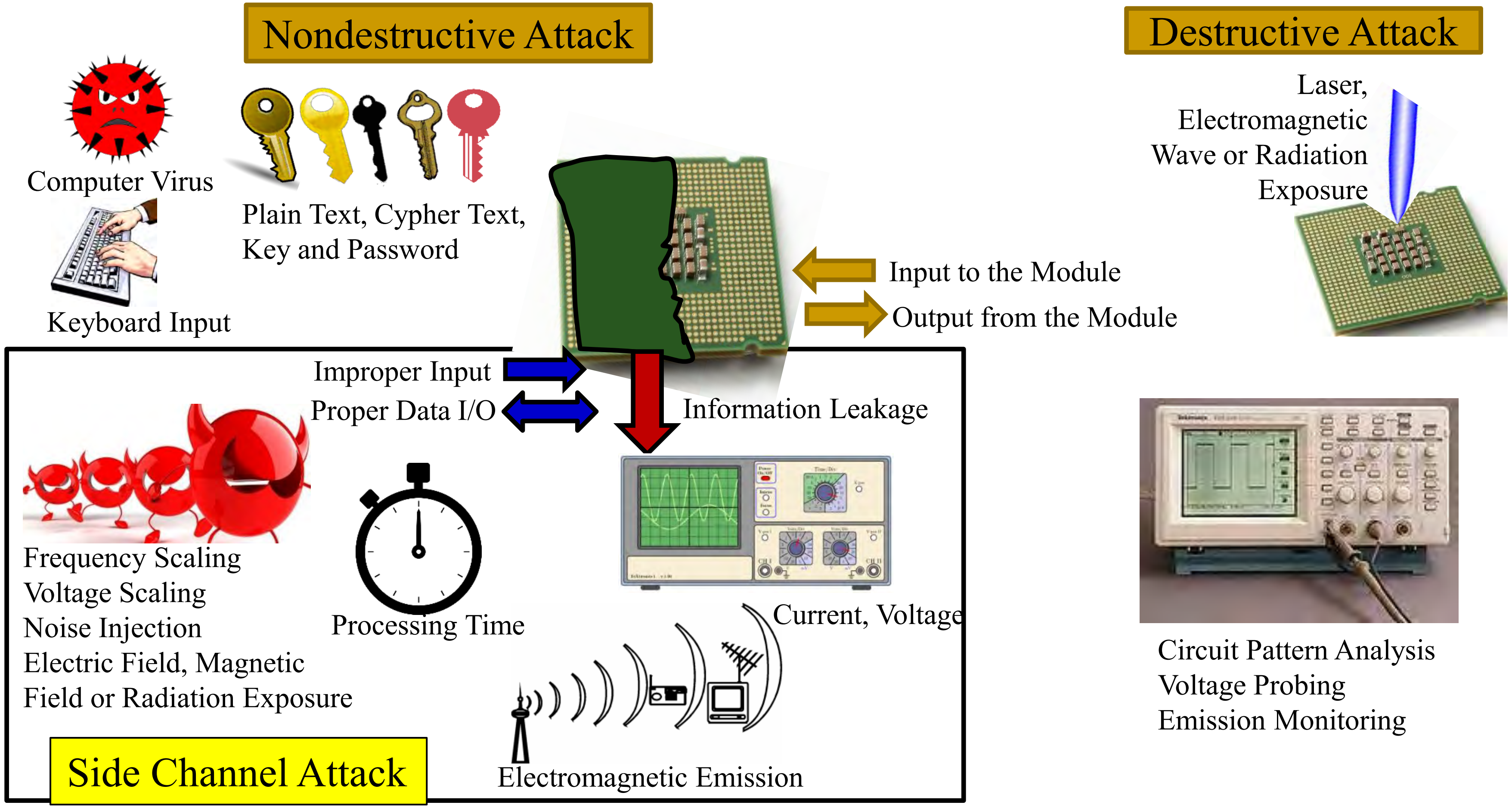
Langer ICR HH 150 probe over Xilinx Spartan3E-1200 FPGA

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



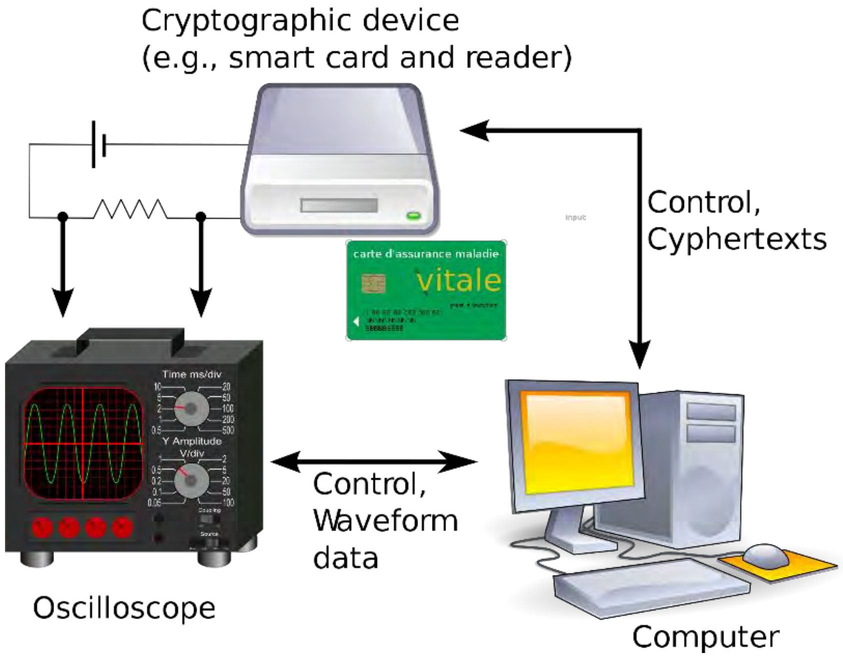
Magnification of the last part of the complete trace. Three trigger signals can be identified: (1) between oscillator phase and error correction phase, (2) between error correction and hashing, and (3) at the end of hashing.

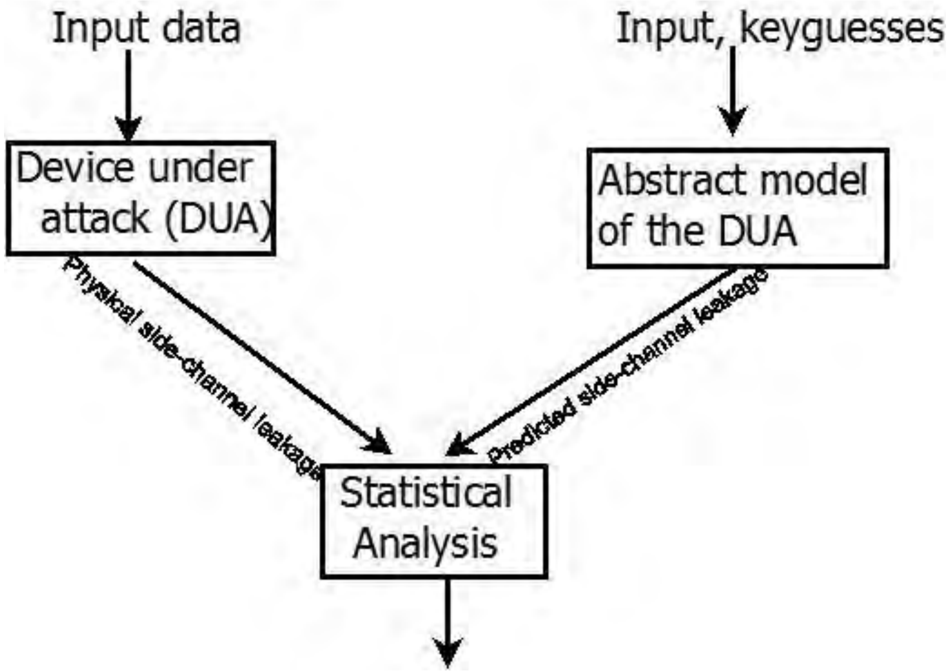
Side Channel Attacks



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

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





Decision on key guess

Side Channel Attacks - Correlation Power Analysis (CPA)

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

Differential Power Analysis (DPA)
- ❖ Attacks using relationship between data and power.
- ❖ Looks at difference of category averages for all key guess.
- ❖ Requires more power traces than CPA.
- ❖ Slower and less efficient than CPA.

Correlation Power Analysis (CPA)
- ❖ Attacks using relationship between data and power.
- ❖ Looks at correlation between all key guesses.
- ❖ Requires less power traces than DPA.
- ❖ Faster, more accurate than DPA.

Source: Zhang and Shi ITNG 2011

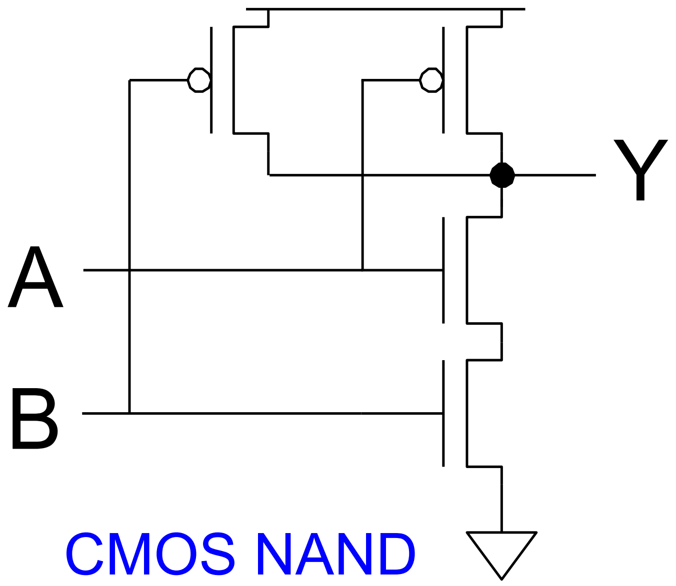
Differential Power Analysis (DPA) Attack Countermeasures

- DPA Attack Countermeasures
  - Hardware Measures
    - Power Randomization
    - Power Process Interrupts
    - Detached Power Supplies
    - Nondeterministic Execution
  - Software Measures
    - Desynchronization
    - Software Balancing
    - The Duplication Method
    - Random Masking
    - Secret-Sharing

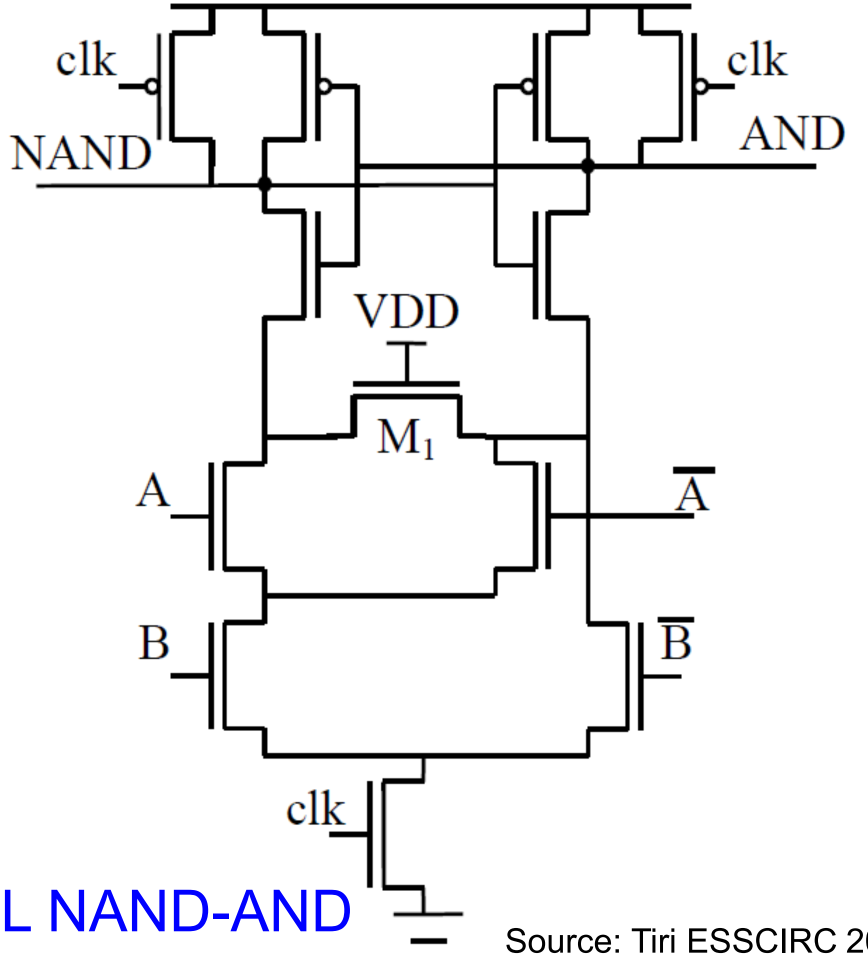
Selected DPA and Correlation Power Analysis (CPA) Attack Resilience Methods

- DPA and CPA Attack Resilience Methods
  - Sense Amplifier Basic Logic (SABL)
  - Wave Dynamic Differential Logic (WDDL)
  - Two-Spacer Alternating Dual Rail Circuit
  - Dynamic Voltage & Frequency Switching Approach
  - Random Switching Logic (RSL)
  - Return To Zero Protocols (RTZ)
  - Masked Dual-Rail Pre-charged Logic (MDPL)

DPA Resilience Hardware: Sense Amplifier Basic Logic (SABL)



CMOS NAND

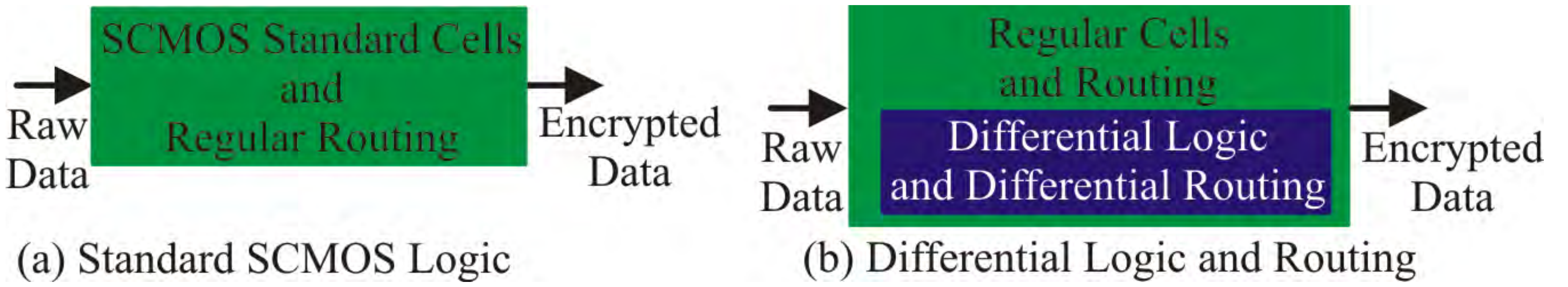


SABL NAND-AND

Source: Tiri ESSCIRC 2002

DPA Resilience Hardware: Differential Logic and Routing

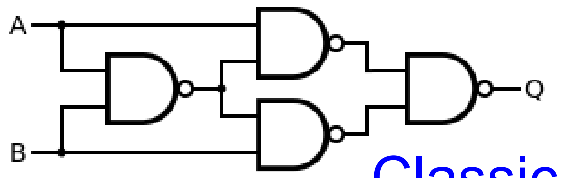
- Develop logic styles and routing techniques such that power consumption per cycle is constant and capacitance charged at a node is constant.



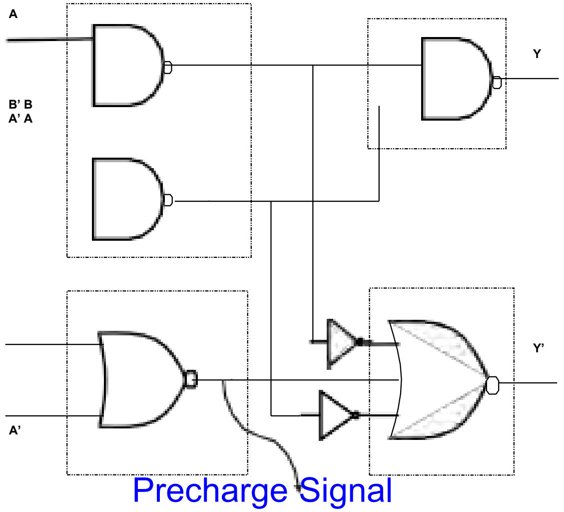
Vulnerable to side channel attack.

May abstract switching activity and reduce information leaking.

DPA Resilience Hardware: Differential Logic and Routing

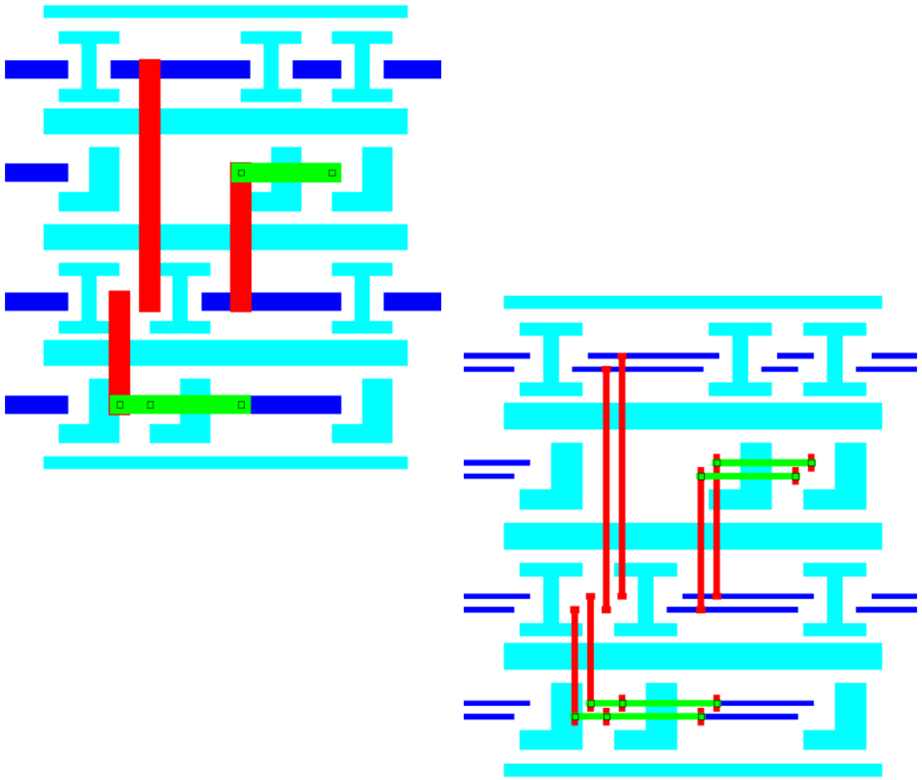


Classic XOR



Reduced Complementary Dynamic and Differential Logic (RCDDL) XOR

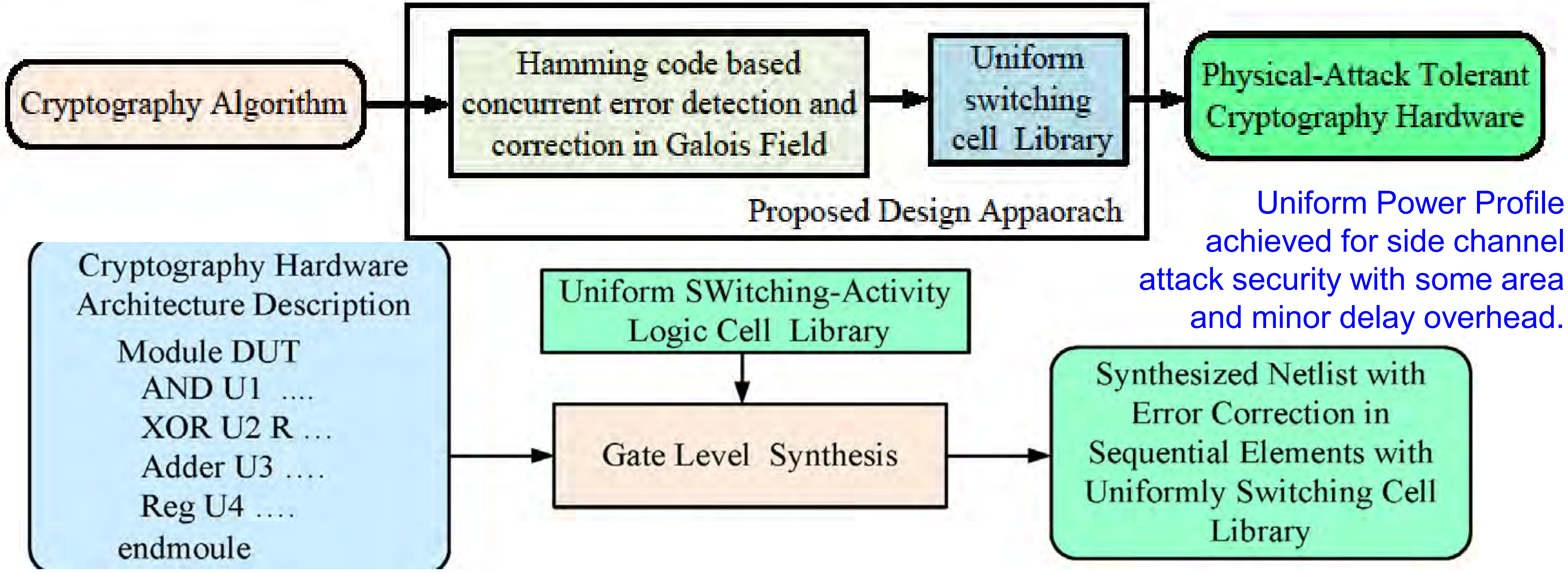
Source: Rammohan VLSID 2008



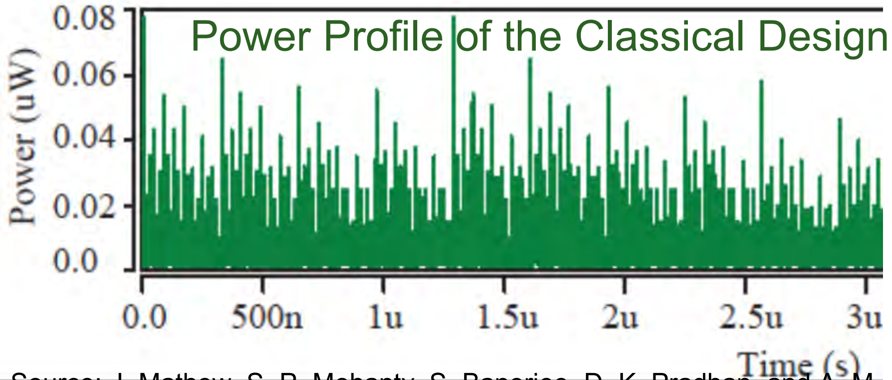
Differential Routing

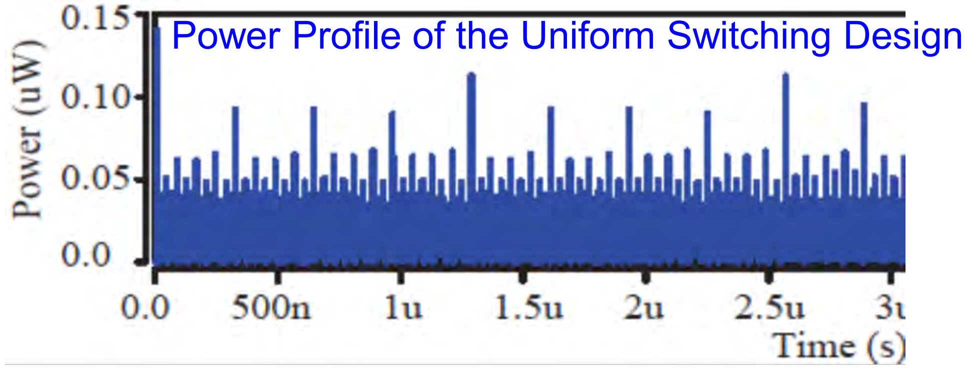
Source: Schaumont IWLS 2005

Our SdD: Approach for DPA Resilience Hardware



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





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

PUF – Trojan Issue

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

Provide backdoor to adversary.
Chip fails during critical needs.

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

PUF – Machine Learning Attack

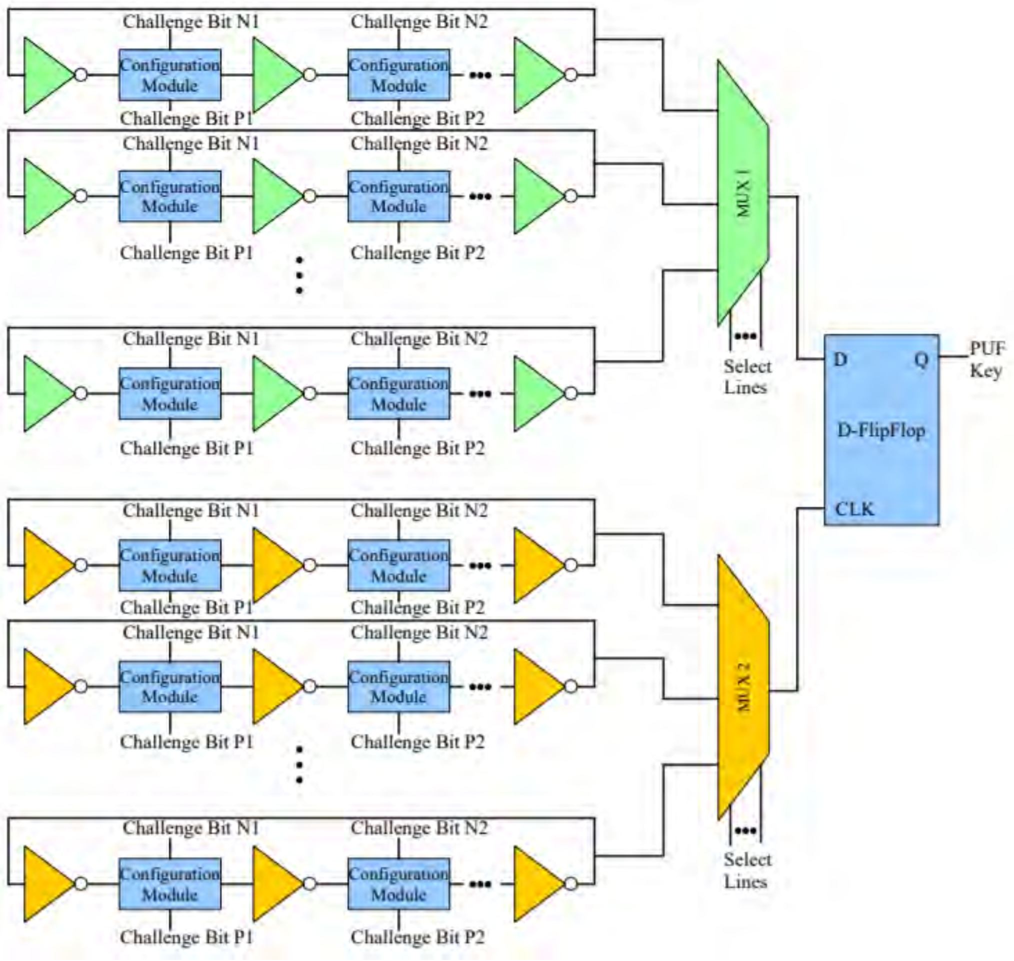
- One types of non-invasive attacks is machine learning (ML) attacks.
- ML attacks are possible for PUFs as the pre- and post-processing methods ignore the effect of correlations between PUF outputs.
- Many ML algorithms are available against known families of PUFs.

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

Why Reconfigurability?

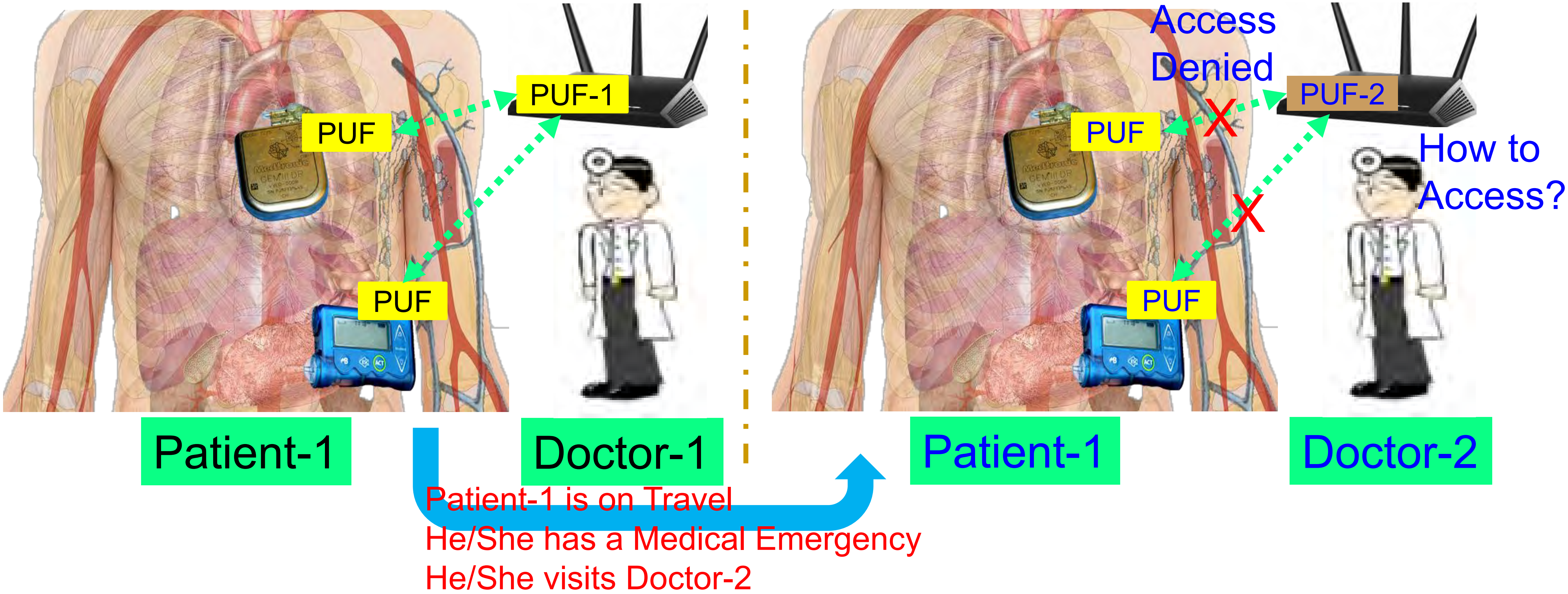
- Increased robustness.
- More Challenge Response Pairs.
- Lower chip area.

Reconfigurable Power Optimized Hybrid Oscillator Arbiter PUF



How to implement?

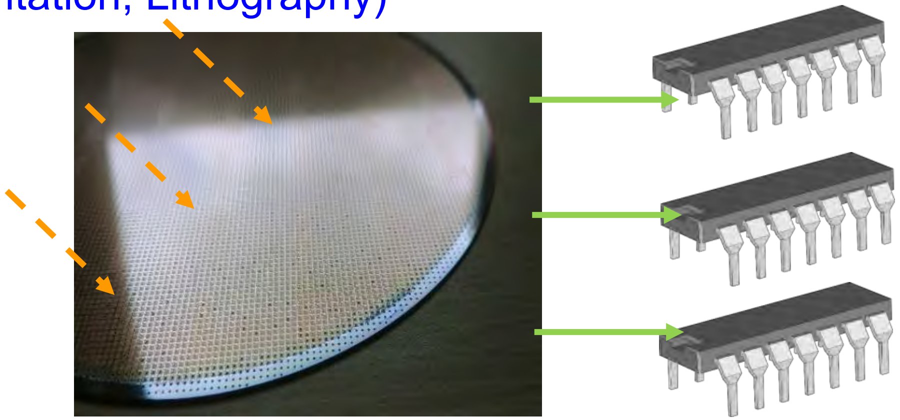
PUF based Cybersecurity in Smart Healthcare - Doctor's Dilemma



IC for PUF – Variability versus Variability-Aware Design

Variability → Randomness for PUF

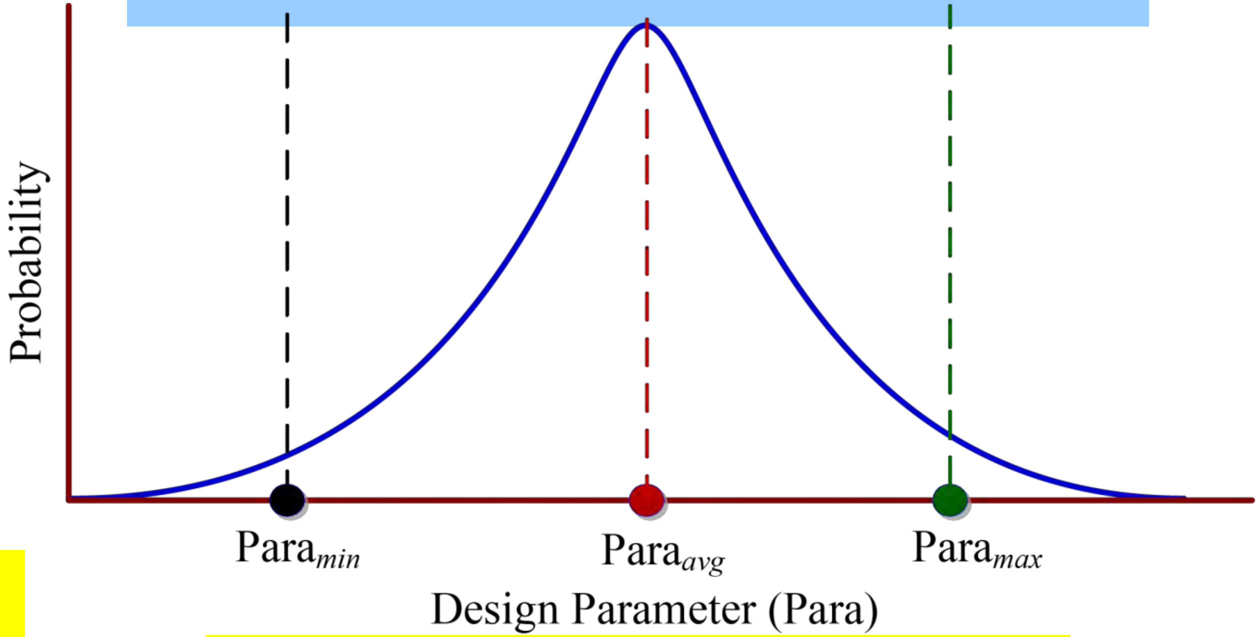
Manufacturing Variations (e.g. Oxide Growth, Ion Implantation, Lithography)



Variability Features → Randomness → PUF

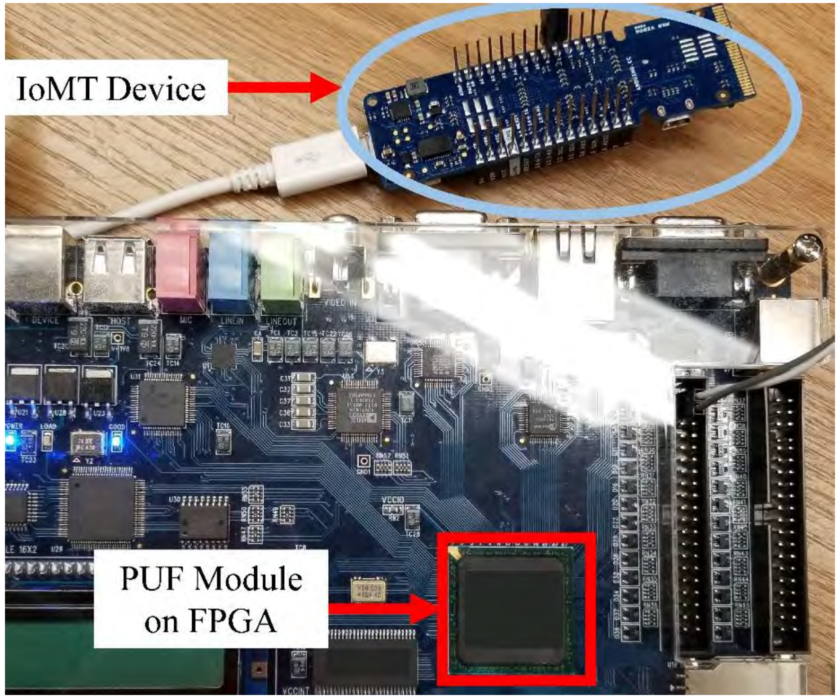
Is it not case of Conflicting Objectives?
How to have a Robust-IC design that functions as a PUF?

Variability-Aware Design → Robust Hardware



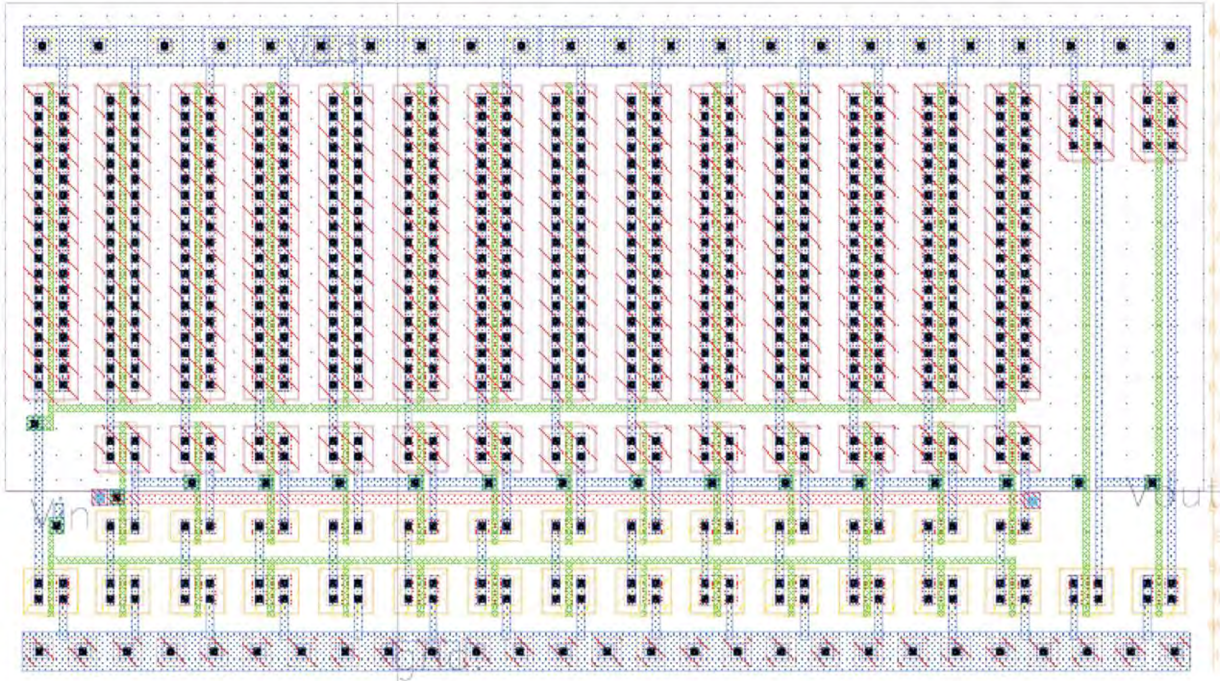
Optimize (μ+nσ) to reduce variability for Robust Design

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

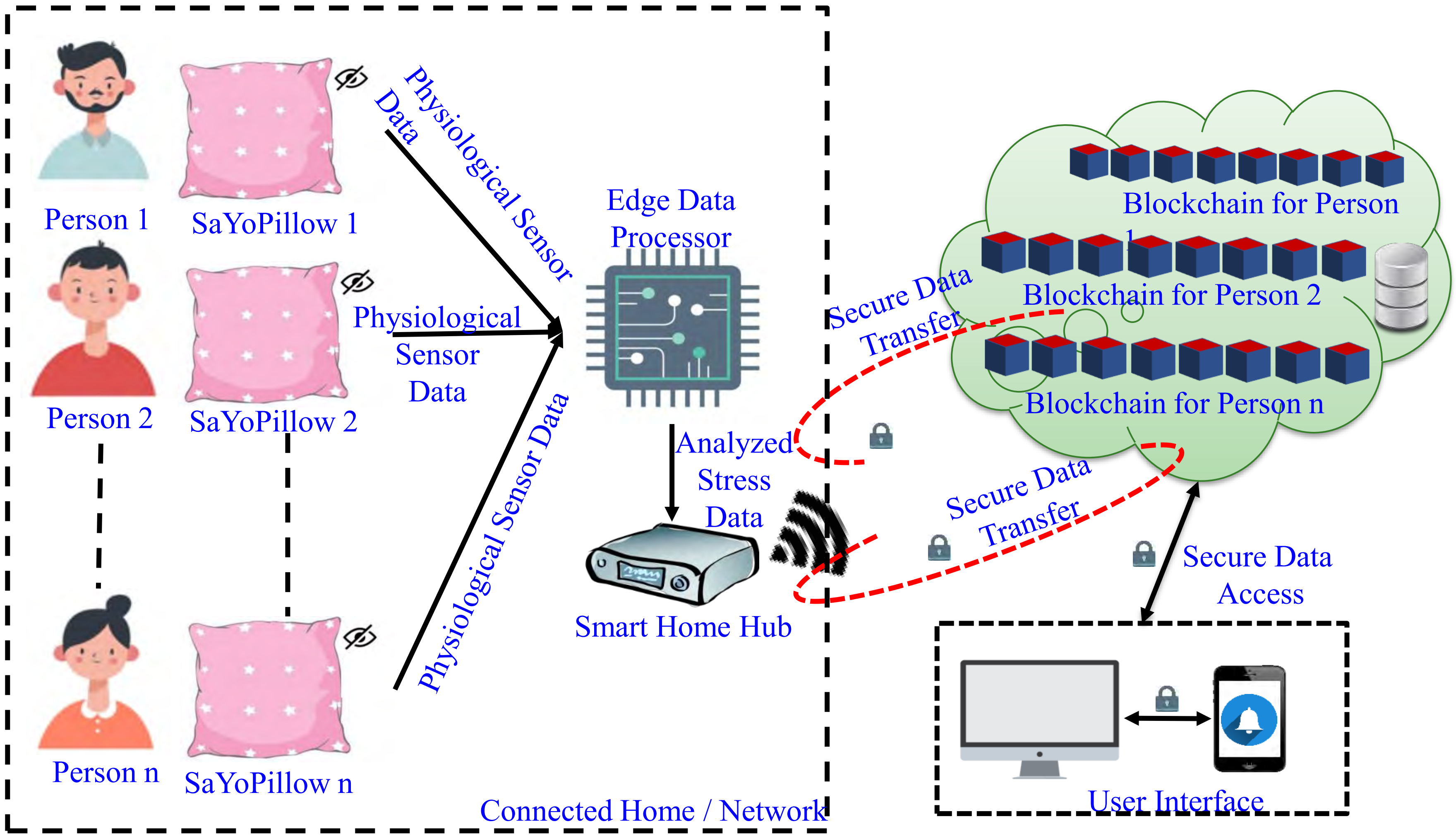
Blockchain in Smart Healthcare

Traditional Versus Blockchain EHR

	Health Information Exchange (HIE) Pain Points	Blockchain Opportunities
	Establishing a Trust Network depends on the HIE as an intermediary to establish point-to-point sharing and "book-keeping" of what data was exchanged.	**Disintermediation of Trust** likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
	Cost Per Transaction, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	**Reduced Transaction Costs** due to disintermediation, as well as near-real time processing, would make the system more efficient.
	Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	**Distributed framework for patient digital identities,** which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
	Varying Data Standards reduce interoperability because records are not compatible between systems.	**Shared data** enables near real-time updates across the network to all parties.
	Limited Access to Population Health Data, as HIE is one of the few sources of integrated records.	**Distributed, secure access** to patient longitudinal health data across the distributed ledger.
	Inconsistent Rules and Permissions inhibit the right health organization from accessing the right patient data at the right time.	**Smart Contracts** create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

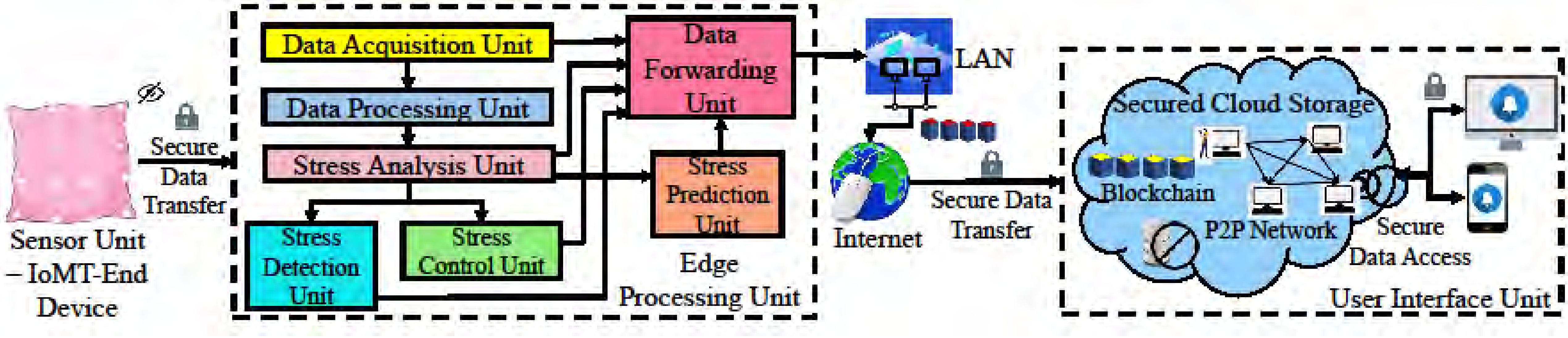
Source: Exploring the Use of Blockchain for EHRs, Healthcare Big Data, https://healthitanalytics.com/features/exploring-the-use-of-blockchain-for-ehrs-healthcare-big-data

Our Smart-Yoga Pillow (SaYoPillow)



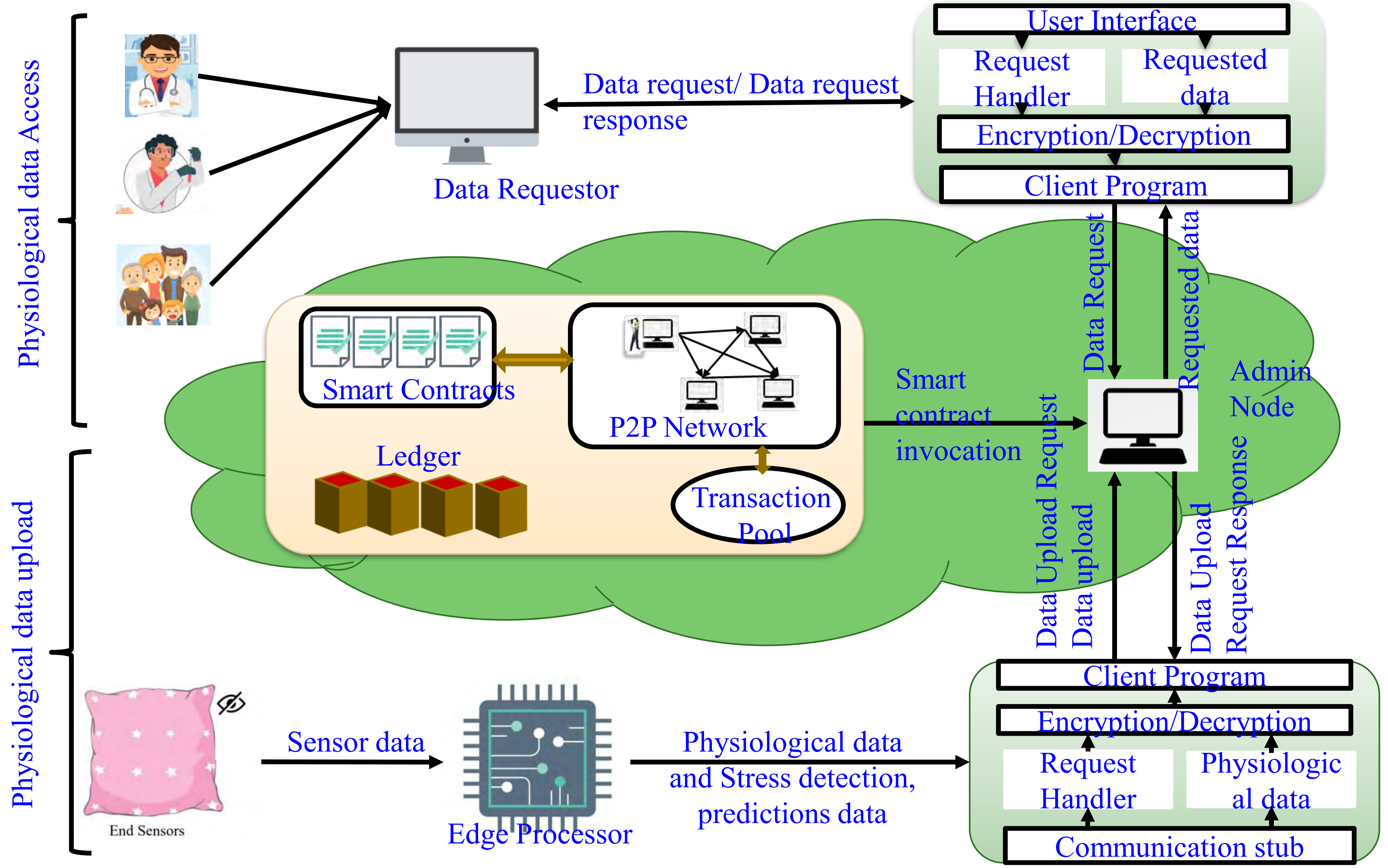
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, “SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits”, *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

Our Smart-Yoga Pillow SaYoPillow – Architectural Details



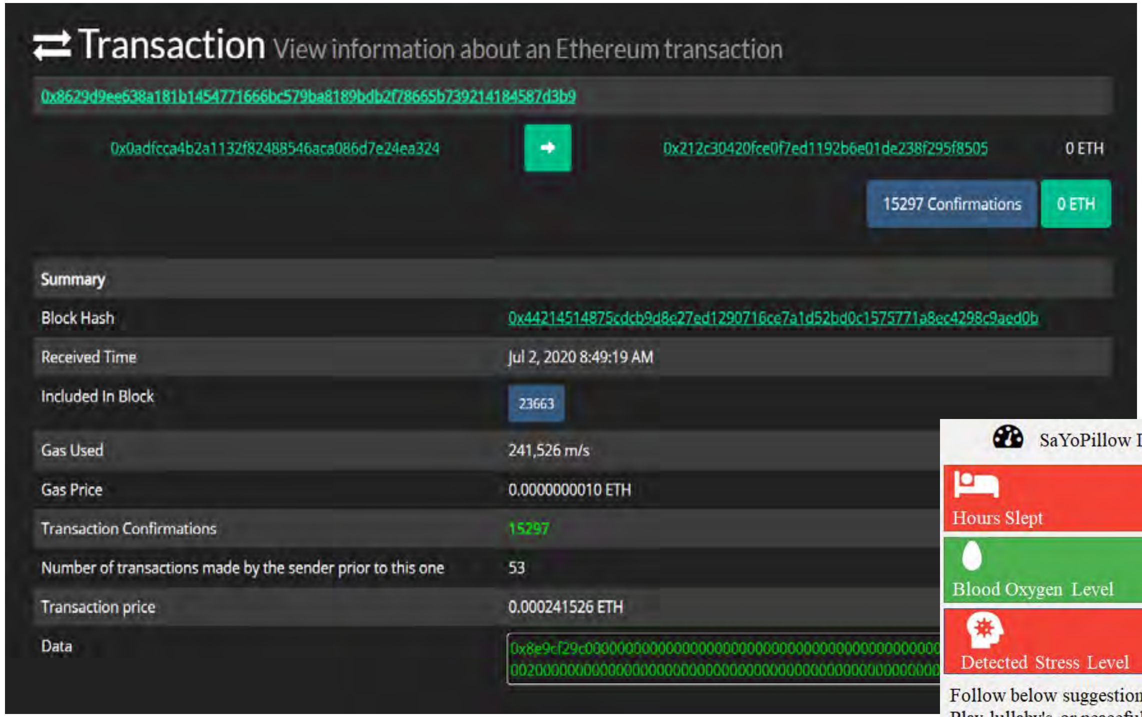
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

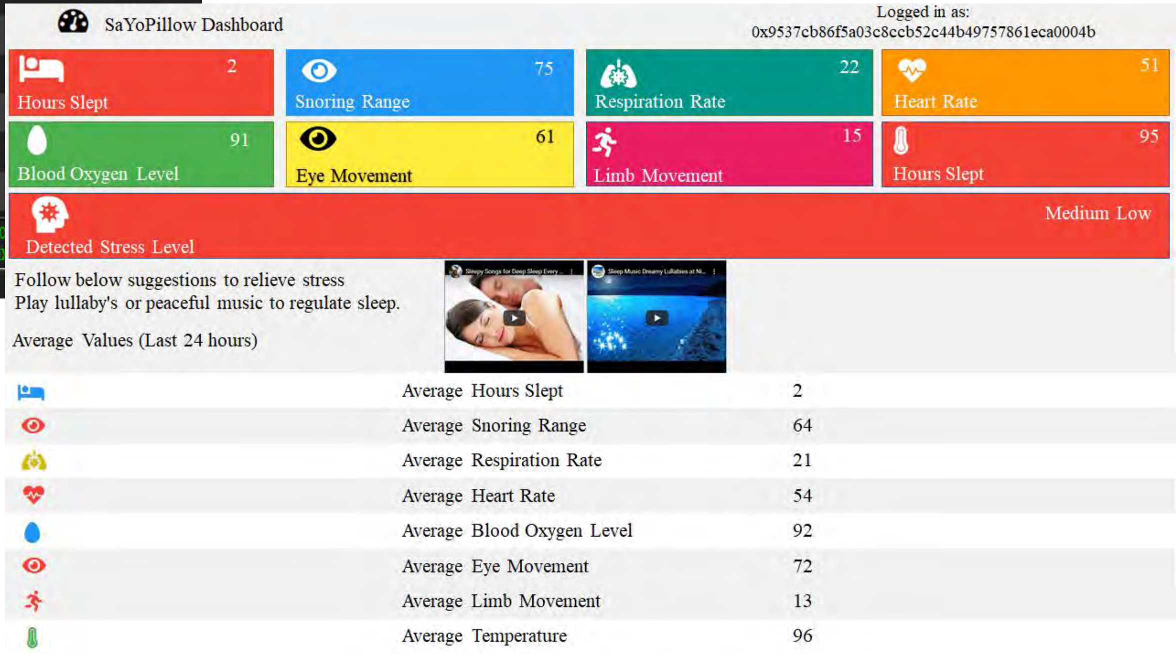
SaYoPillow: Blockchain Details



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.

SaYoPillow: Prototyping

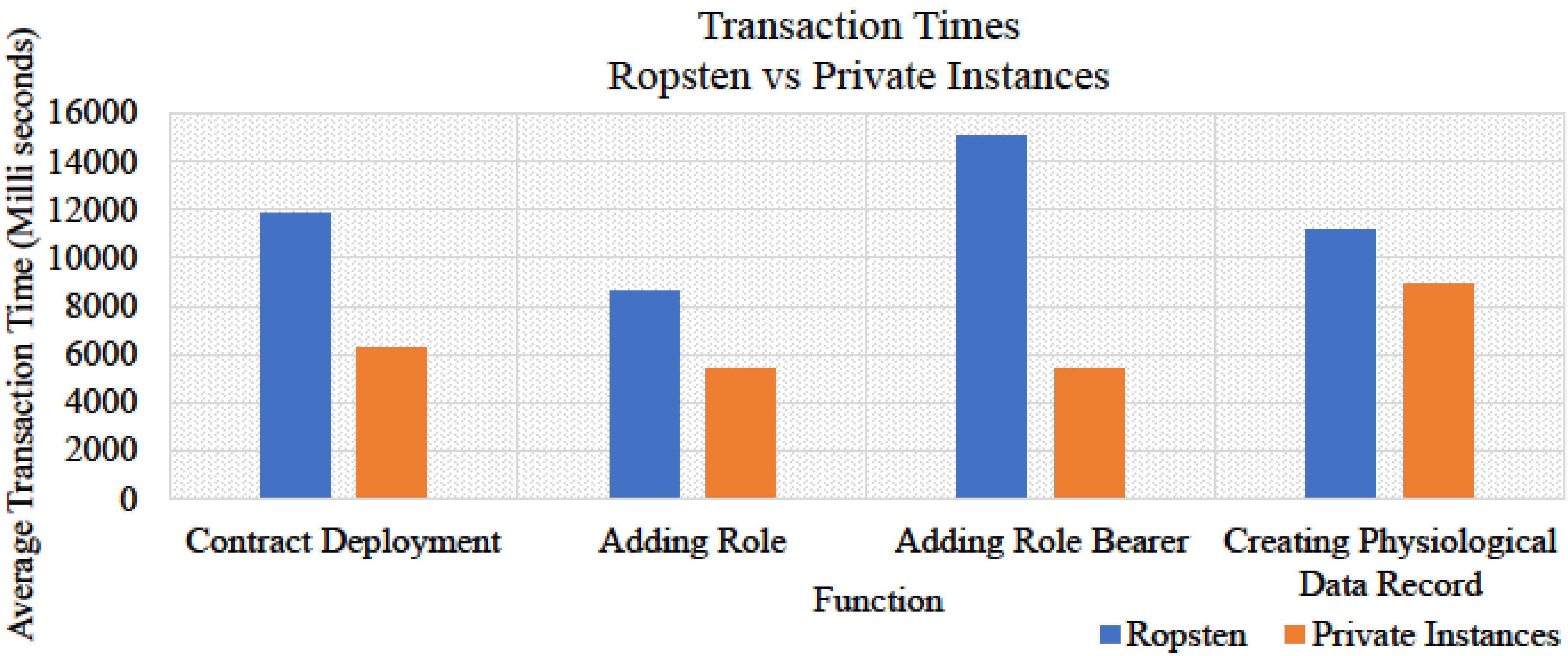




Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

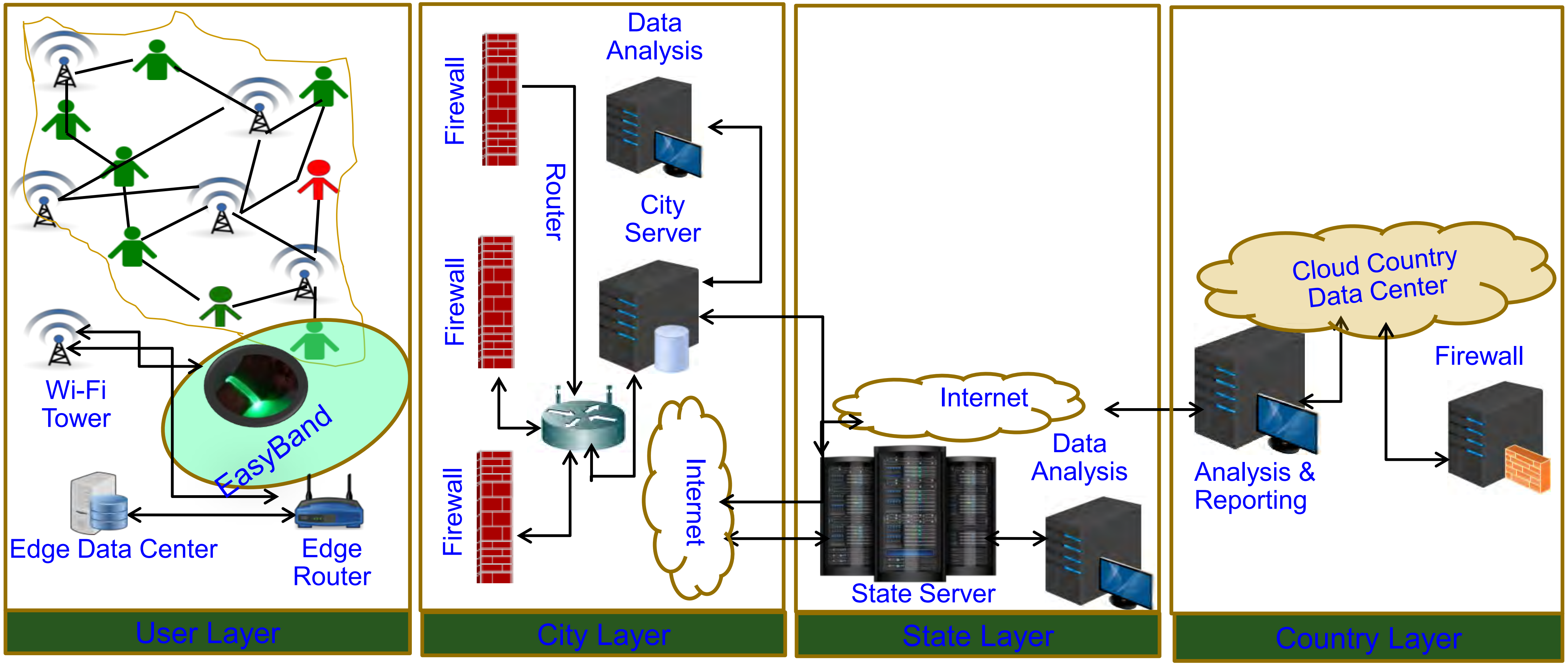
SaYoPillow: Prototyping

Network	Contract Deployment: Min, Max and Avg TT (secs)	Adding Role: Min, Max and Avg TT (secs)	Adding Role Bearer: Min, Max and Avg TT (secs)	Creating Data Record: Min Max and Avg TT (secs)
Ropsten	3.29 | 26.75 | 11.8	1.2 | 18.4 | 8.6	1.4 | 35 | 15	1.5 | 38.2 | 11.2
SaYoPillow	3.2 | 13.5 | 6.3	1.4 | 10.7 | 5.4	1.5 | 14.2 | 5.4	2.2 | 11.5 | 8.9



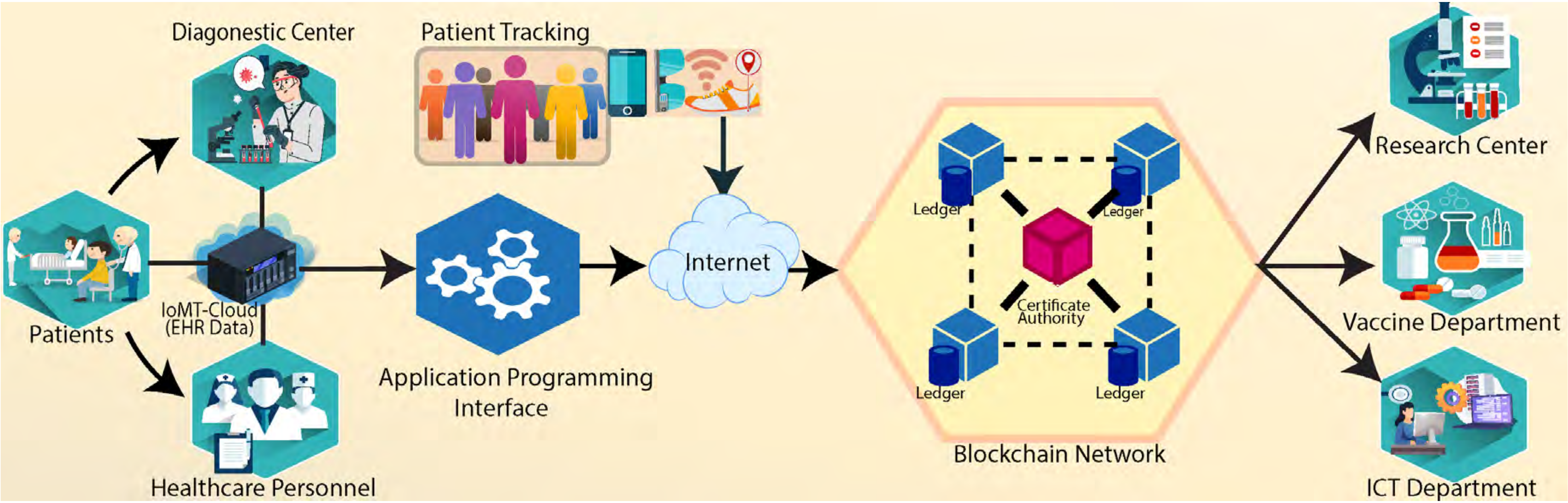
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

EasyBand in Healthcare CPS (H-CPS)



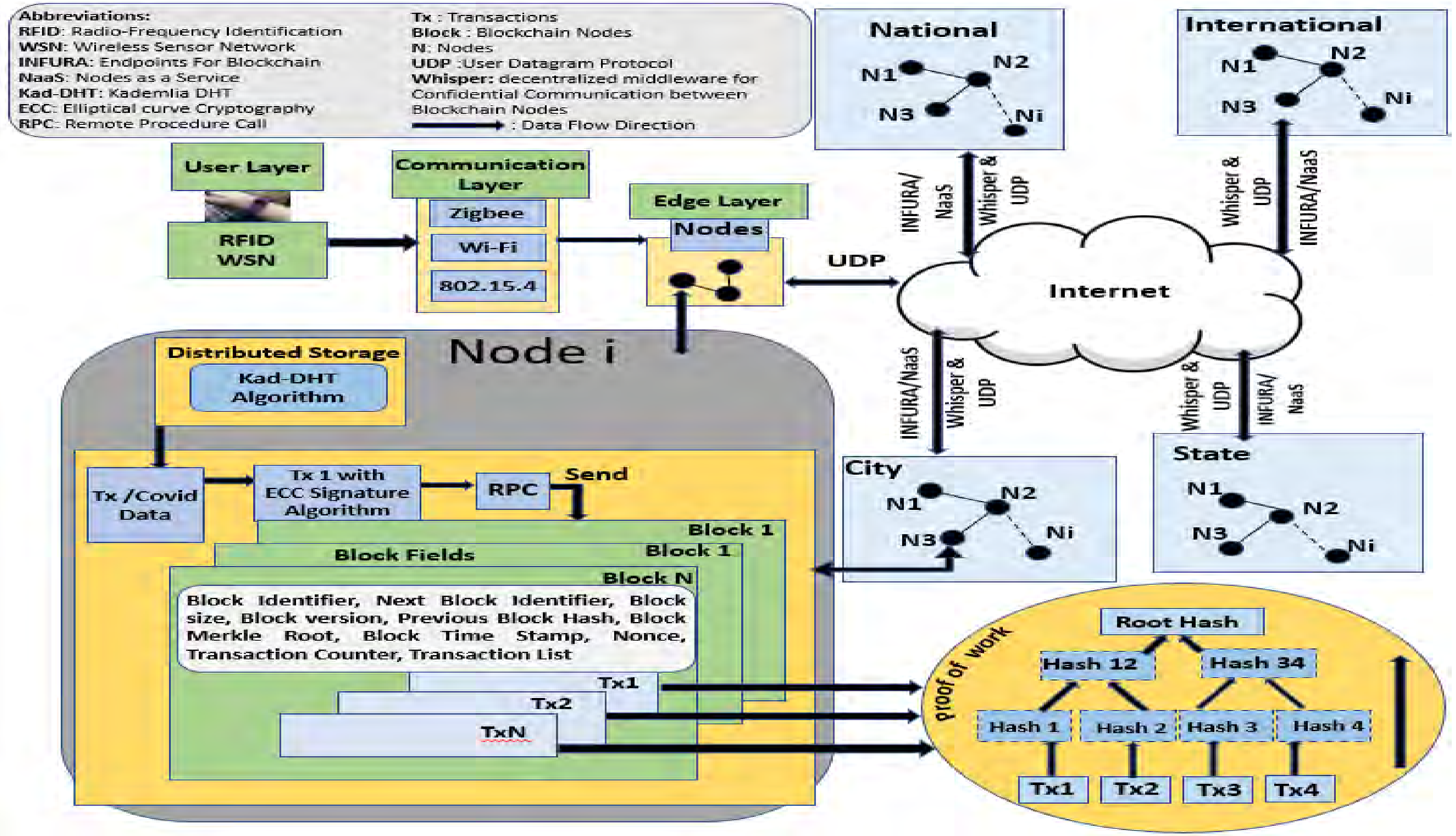
Source: A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi and G. Das, "EasyBand: A Wearable for Safety-Aware Mobility During Pandemic Outbreak," *IEEE Consumer Electronics Magazine*, vol. 9, no. 5, pp. 57-61, 1 Sept. 2020, doi: 10.1109/MCE.2020.2992034..

GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data



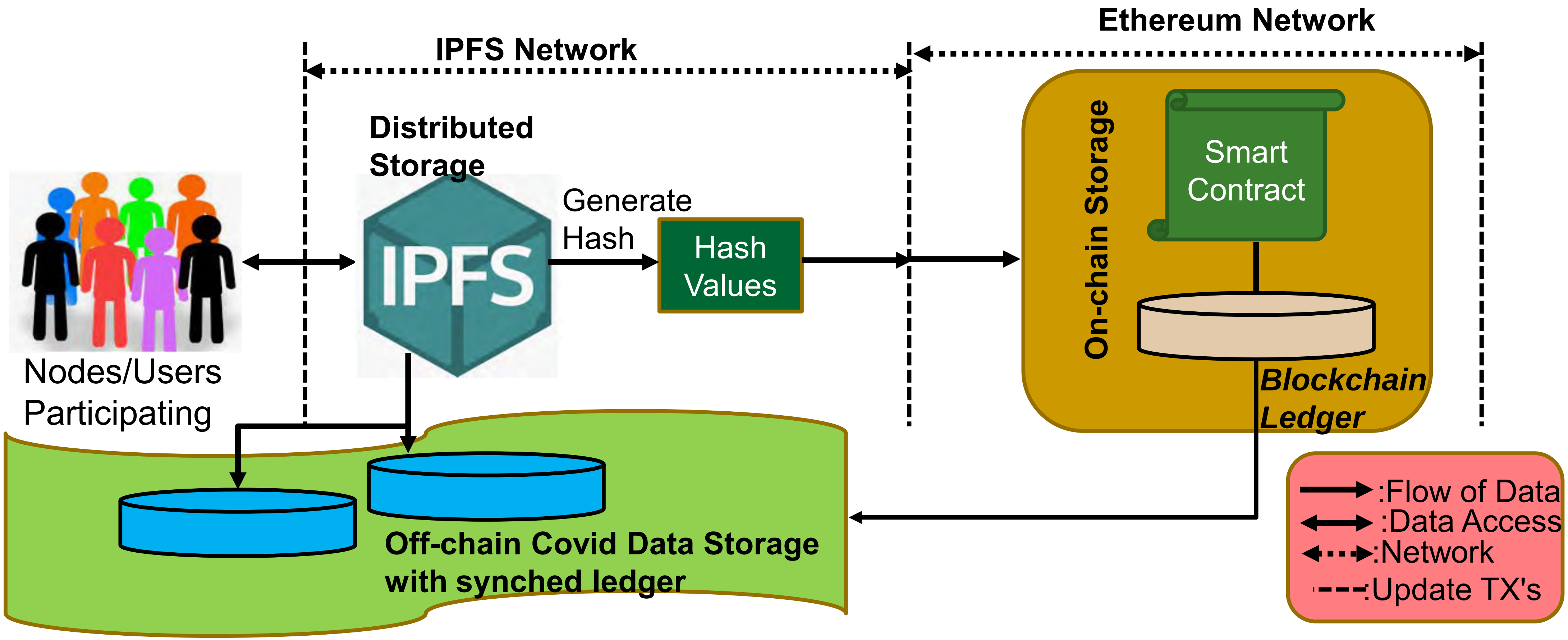
Source: S. Biswas, F. Li, Z. Latif, K. Sharif, A. K. Bairagi and S. P. Mohanty, "GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data - A COVID-19 Perspective," *IEEE Consumer Electronics Magazine*, doi: 10.1109/MCE.2021.3074688.

CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, Springer Nature Computer Science (SN-CS), Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS

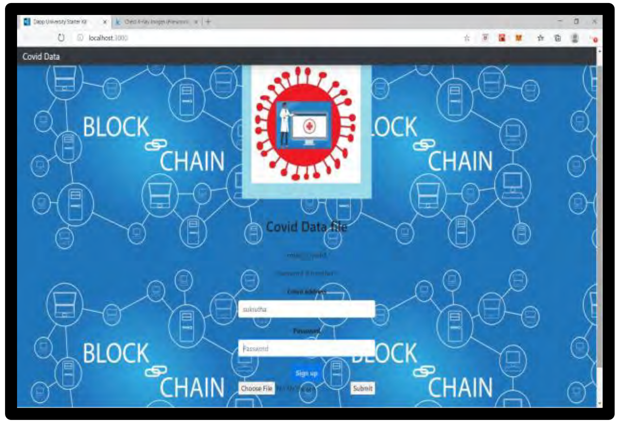


Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks", Springer Nature Computer Science (SN-CS), Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

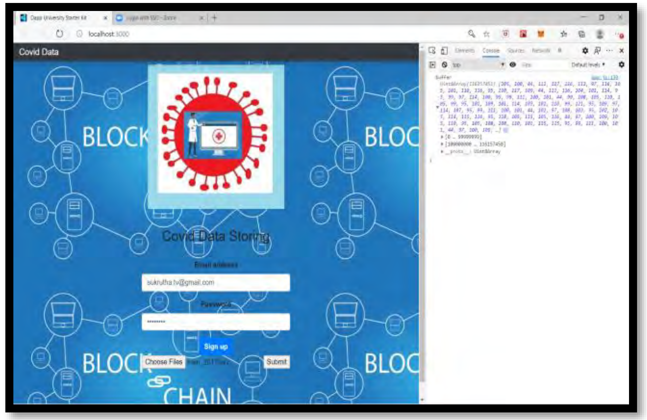
CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS

- From the front-end, Covid file is submitted to the IPFS and store it.
- Once the file is stored, the hash of the file is returned to the browser console.
- The hash generated from IPFS is stored on the blockchain, instead of the actual file.

1. User Interface

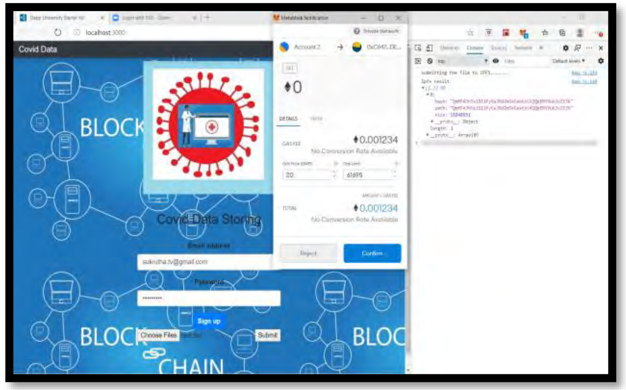


2. File Converted to Buffer



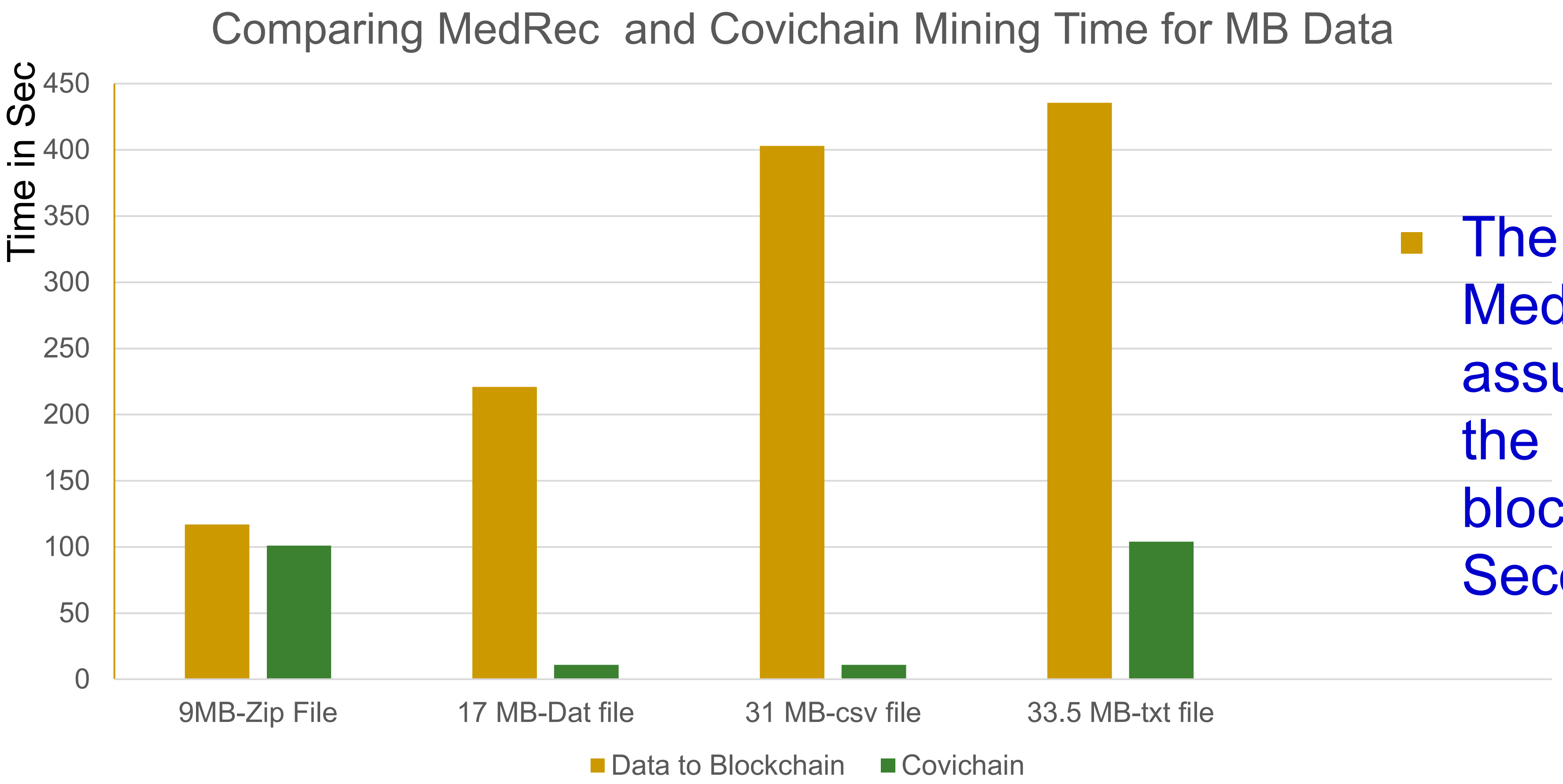
3. IPFS returning Hash

4. Confirming Metamask



Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, Springer Nature Computer Science (SN-CS), Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



- The times for data in MedRec are calculated assuming the mining time of the conventional Ethereum blockchain to be 13 Seconds for 1MB Data.

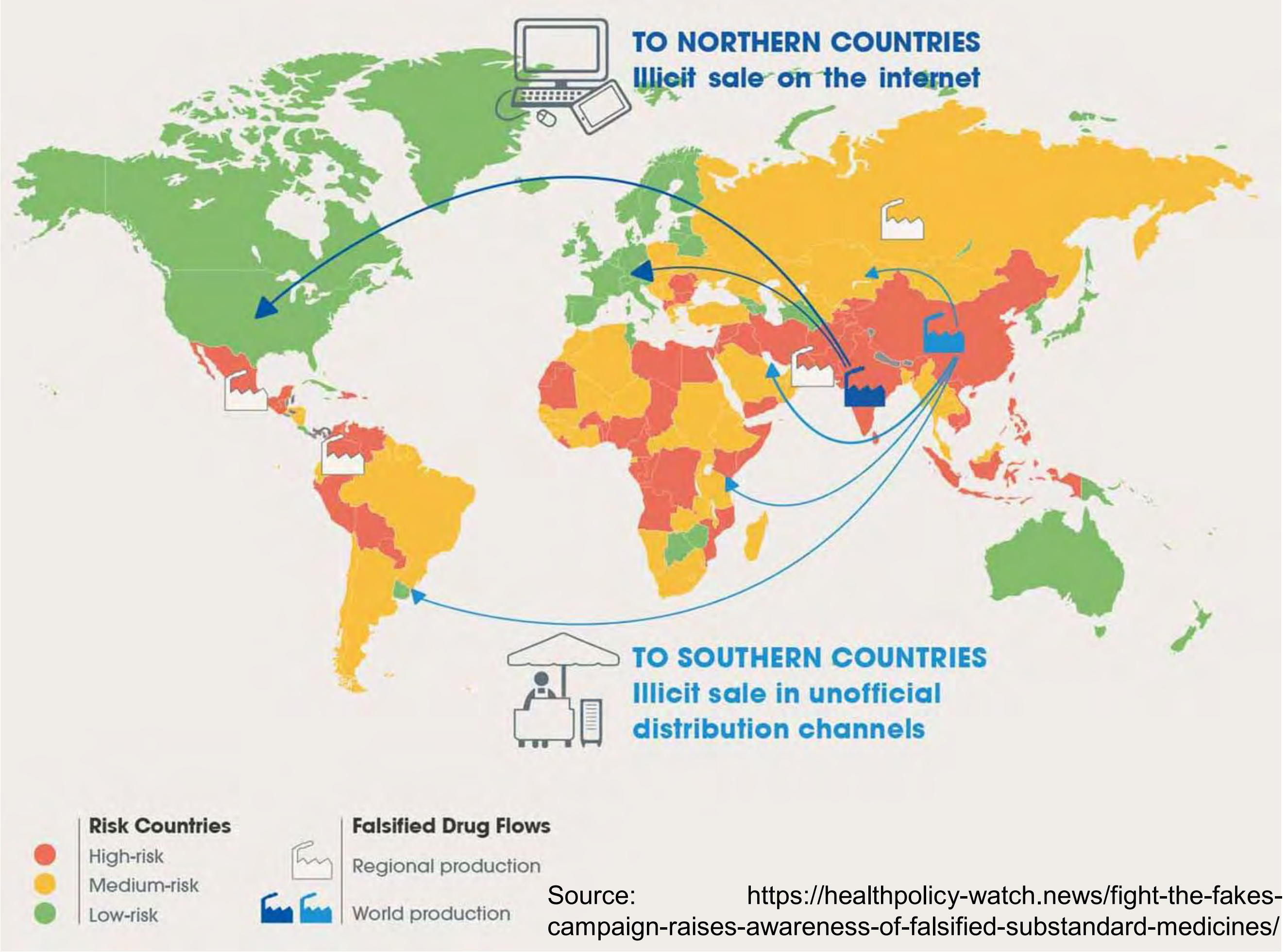
Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks", Springer Nature Computer Science (SN-CS), Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

Fake Medicine or Vaccine - 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/

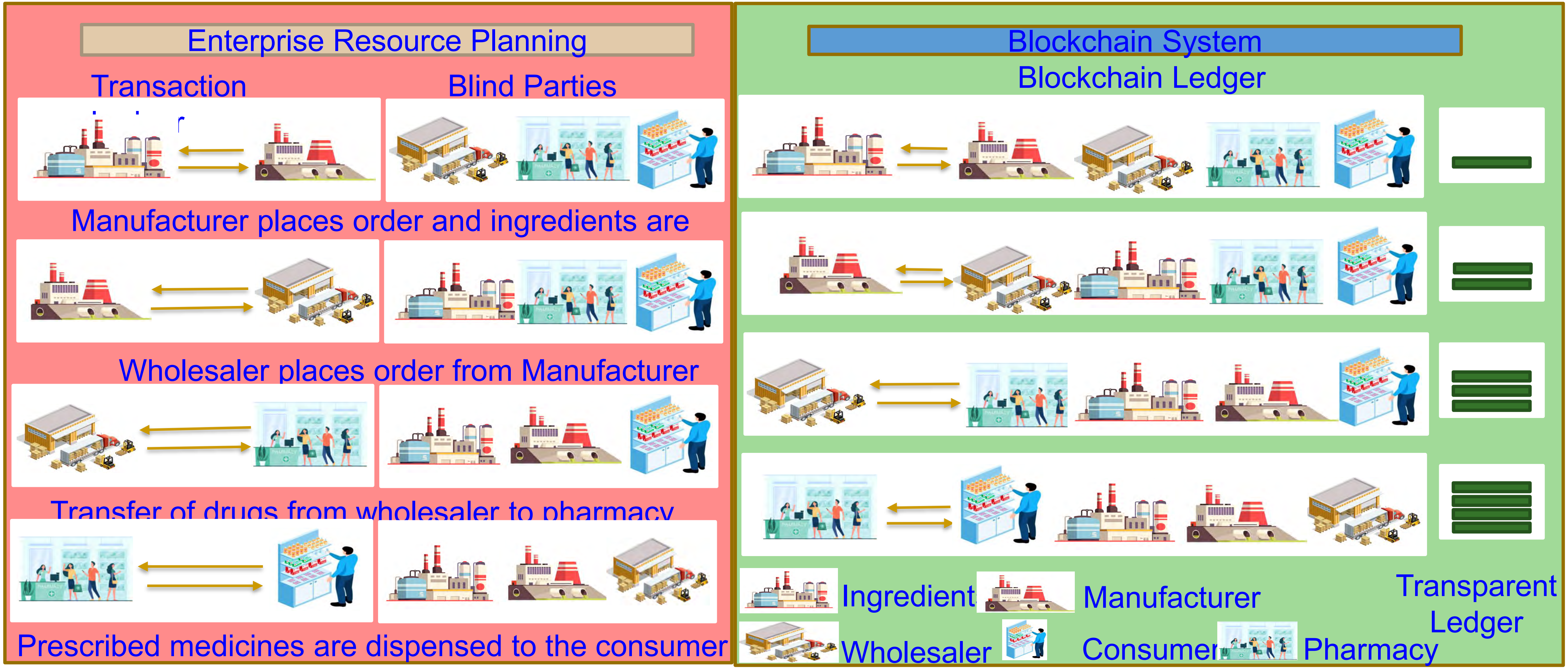


Source: https://healthpolicy-watch.news/fight-the-fakes-campaign-raises-awareness-of-falsified-substandard-medicines/

PharmaChain - Counterfeit Free Pharmaceutical …

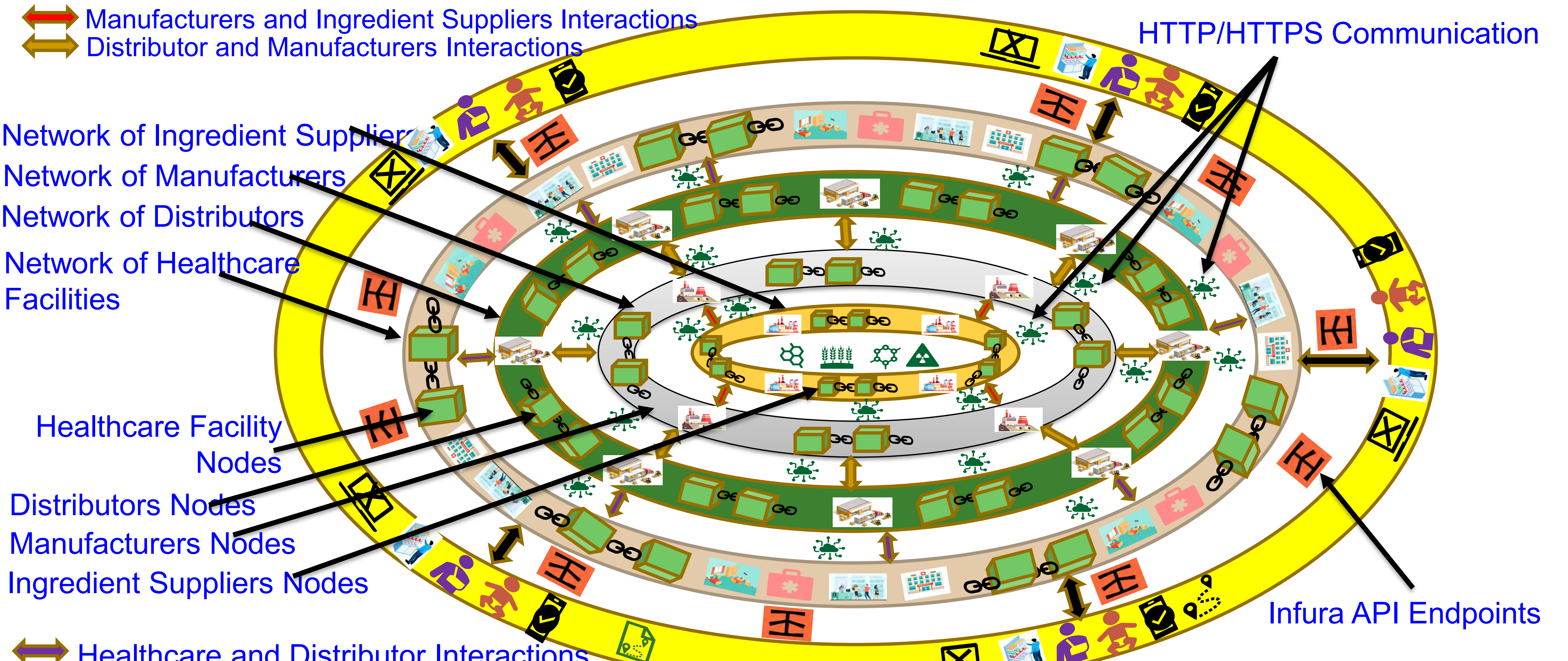
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: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

PharmaChain - Counterfeit Free Pharmaceutical …



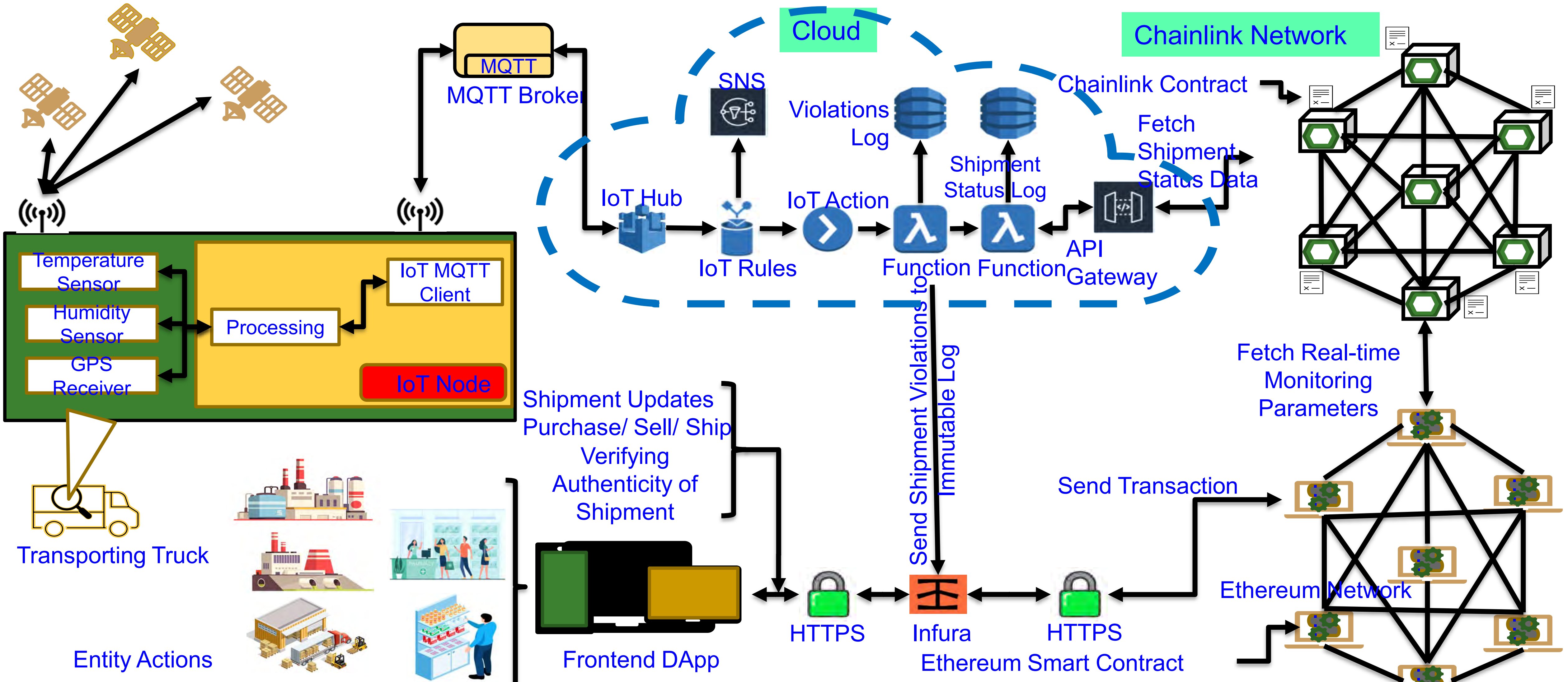
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: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

PharmaChain - Counterfeit Free Pharmaceutical …



Sou… , 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 - Counterfeit Free Pharmaceutical …

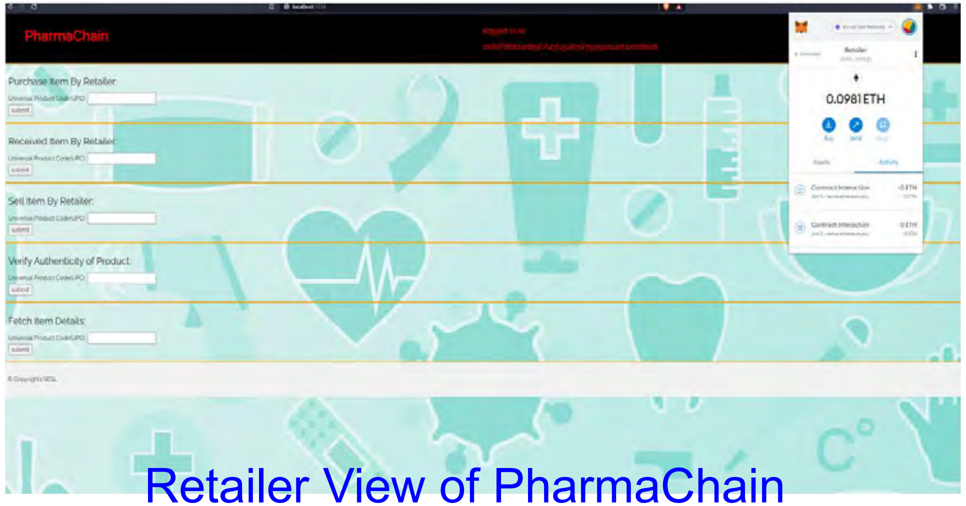


Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: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

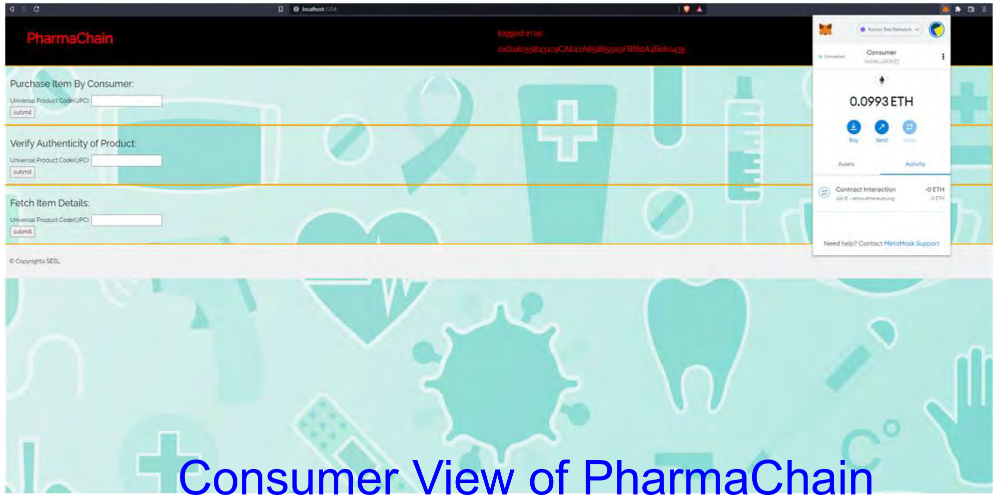
PharmaChain - Counterfeit Free Pharmaceutical …

Manufacturer View of PharmaChain

Distributor View of PharmaChain



Retailer View of PharmaChain



Consumer View 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 - Counterfeit Free Pharmaceutical …

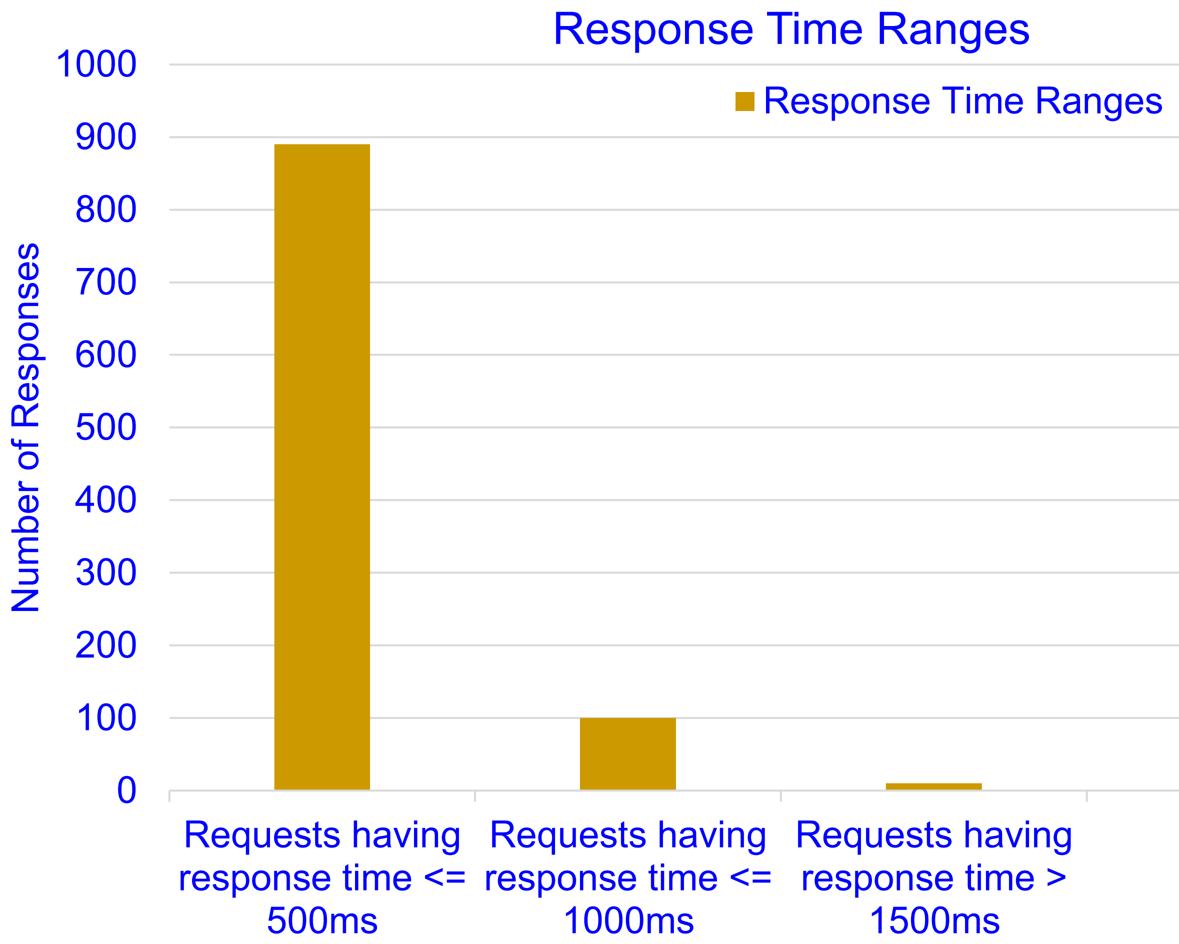
Parameter	Subramanian et.al. [30]	Bocek et.al. [31]	Kumar et.al. [32]	Huang et.al. [33]	Alhoori et.al. [35]	Our Solution
Blockchain Platform	New Economic Movement (NEM)	Ethereum	-	Bitcoin	Ethereum	Ethereum
Business Functions	Smart Contracts	Smart Contracts	-	UTXO Scripts	Smart Contracts	Smart Contracts
Consensus Mechanism	PoI	PoW	-	PoW	PoW	PoA
Data Integration from IoT	Cloud Functions	Centralized Database	[×]	[×]	Cloud Functions	Oracles
Transactions Re-playable	[×]	[×]	[×]	[×]	[×]	[✓]
IoT Integration	[✓]	[✓]	[×]	[×]	[✓]	[✓]
Scalability Analysis	[×]	[×]	[×]	[×]	[✓]	[✓]
Cost Analysis	[×]	[×]	[×]	[×]	[×]	[✓]
Security Analysis	[×]	[×]	[×]	[✓]	[×]	[✓]
User Friendly Interface	[✓]	[×]	[×]	[×]	[✓]	[✓]
Access Control Mechanism	[×]	[×]	[×]	[×]	[✓]	[✓]
Real-time Decision Support Tools	[×]	[×]	[×]	[×]	[✓]	[✓]
Throughput	Highest	Less	-	Least	Less	Higher

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 - Counterfeit Free Pharmaceutical …

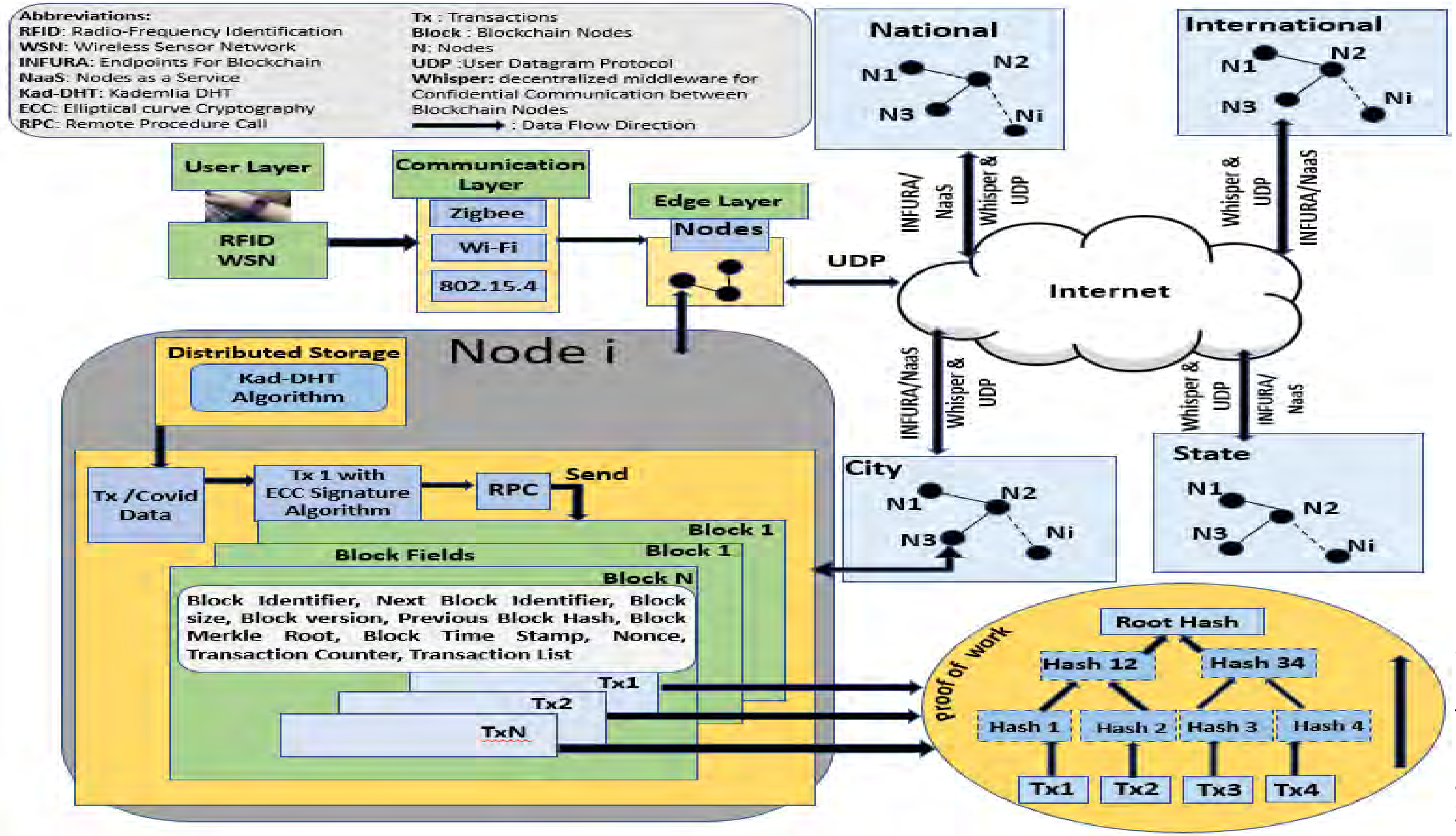
Load Testing in Proposed PharmaChain

Parameters	**Value**
Number of Oracle Requests sent	1000
Load Duration	2 Seconds
Failed Requests	0
Percentage of Error	0%
Average Response Time(ms)	285.196 ms
Minimum Response Time(ms)	78 ms
Maximum Response Time(ms)	1960 ms
Throughput (Requests/Sec)	16.66



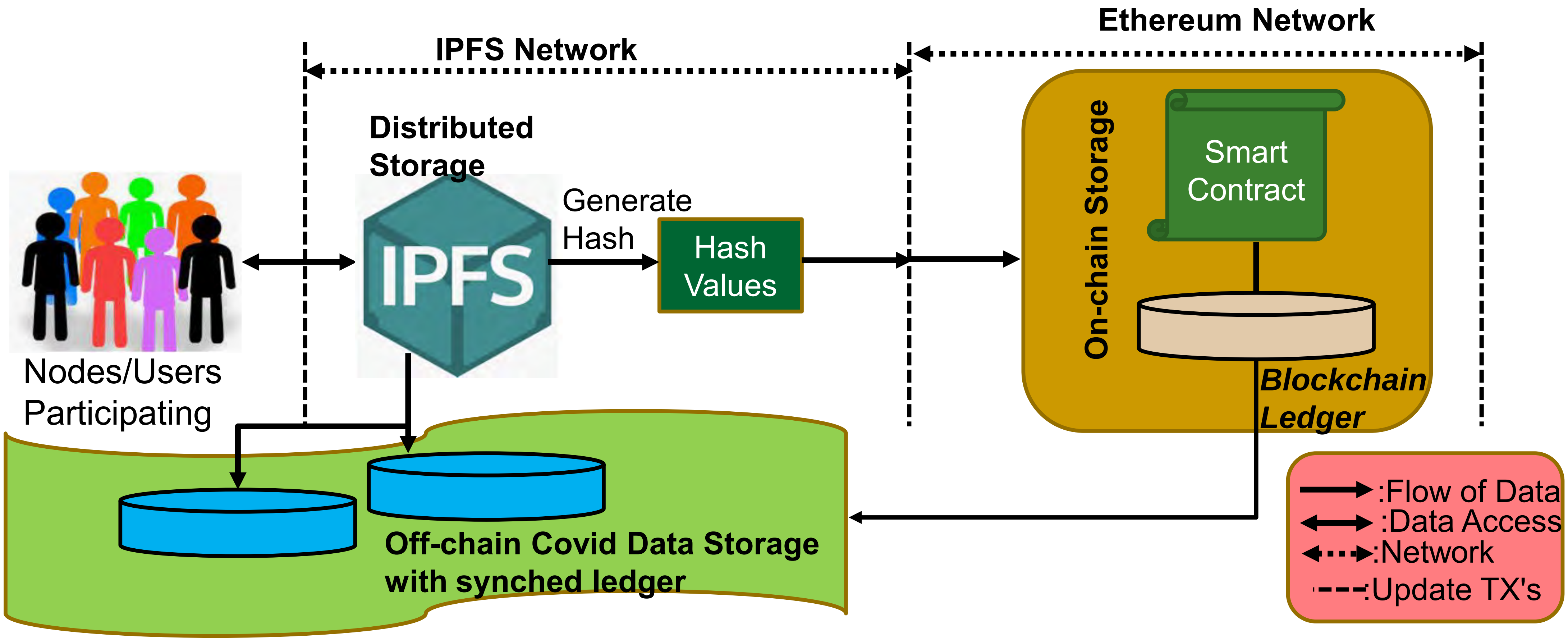
Source: A. K. Bapatla, **S. P. Mohanty**, E. Kougianos, D. Puthal, and A. Bapatla, "PharmaChain: A Blockchain to Ensure Counterfeit-Free Pharmaceutical Supply Chain", *IET Networks*, Vol. XX, No. YY, ZZ 2022, pp. Accepted on 24 June 2022, DOI: https://doi.org/10.1049/ntw2.12041. (Dataset for Research: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

CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, *Springer Nature Computer Science (SN-CS)*, Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS

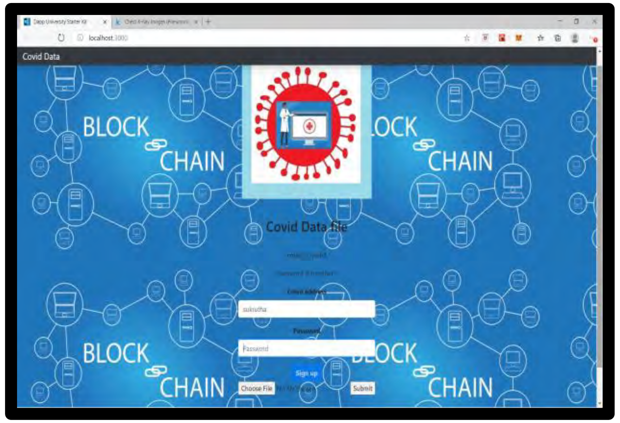


Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks", *Springer Nature Computer Science (SN-CS)*, Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

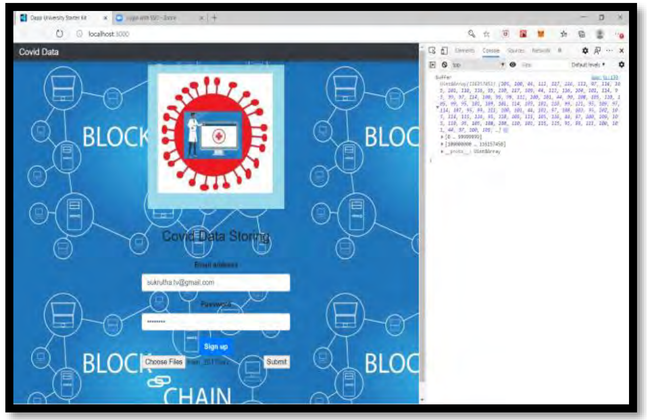
CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS

- From the front-end, Covid file is submitted to the IPFS and store it.
- Once the file is stored, the hash of the file is returned to the browser console.
- The hash generated from IPFS is stored on the blockchain, instead of the actual file.

1. User Interface

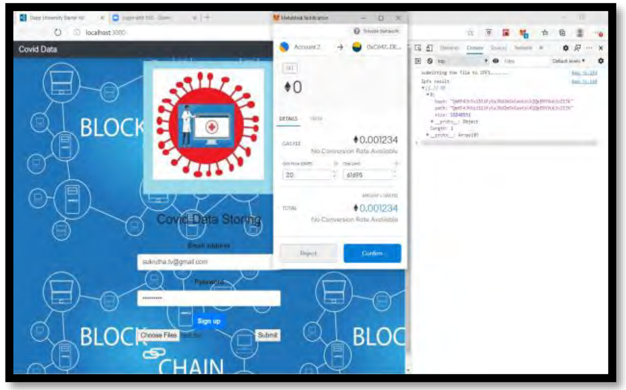


2. File Converted to Buffer



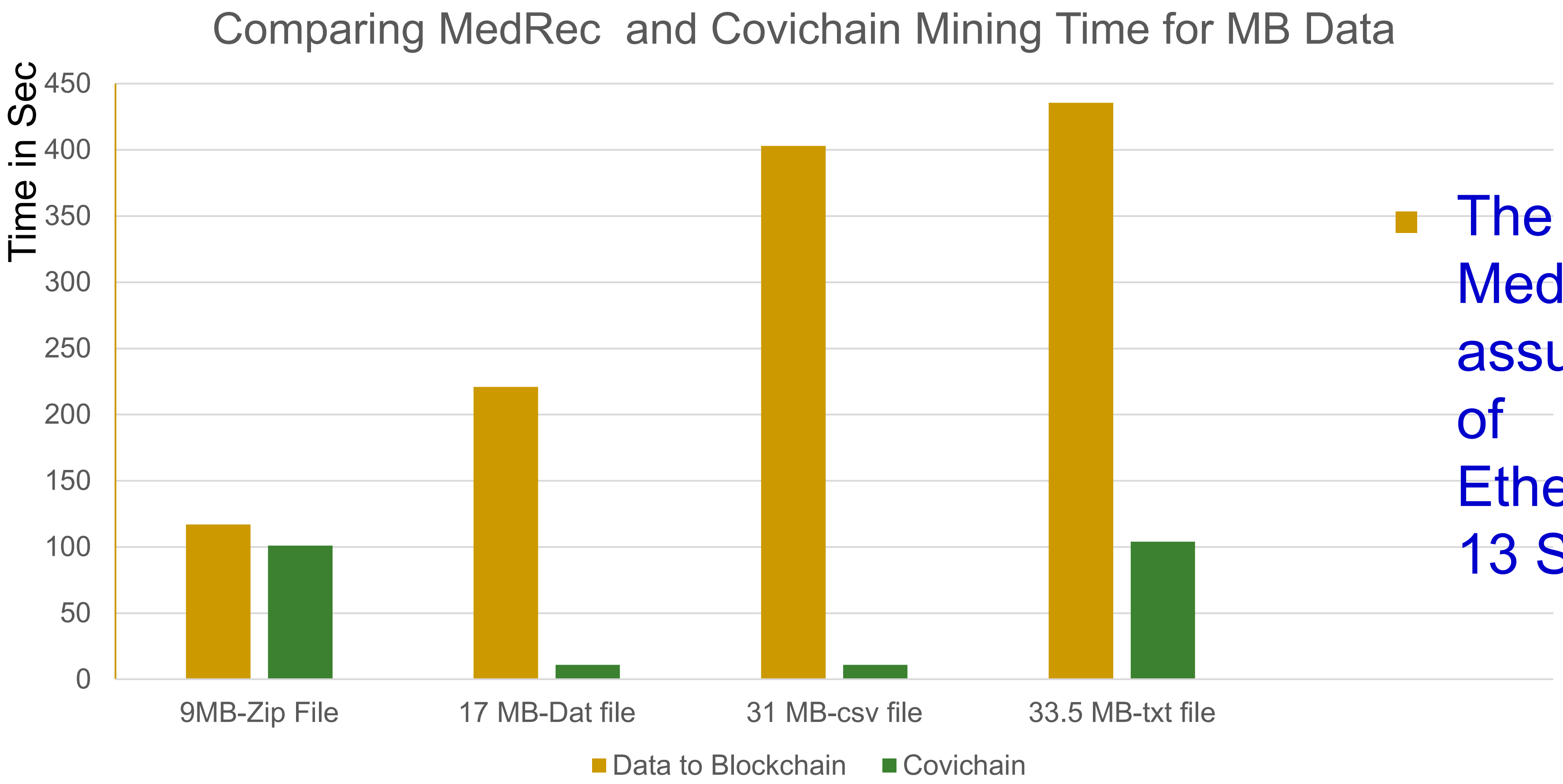
3. IPFS returning Hash

4. Confirming Metamask



Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, *Springer Nature Computer Science (SN-CS)*,Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

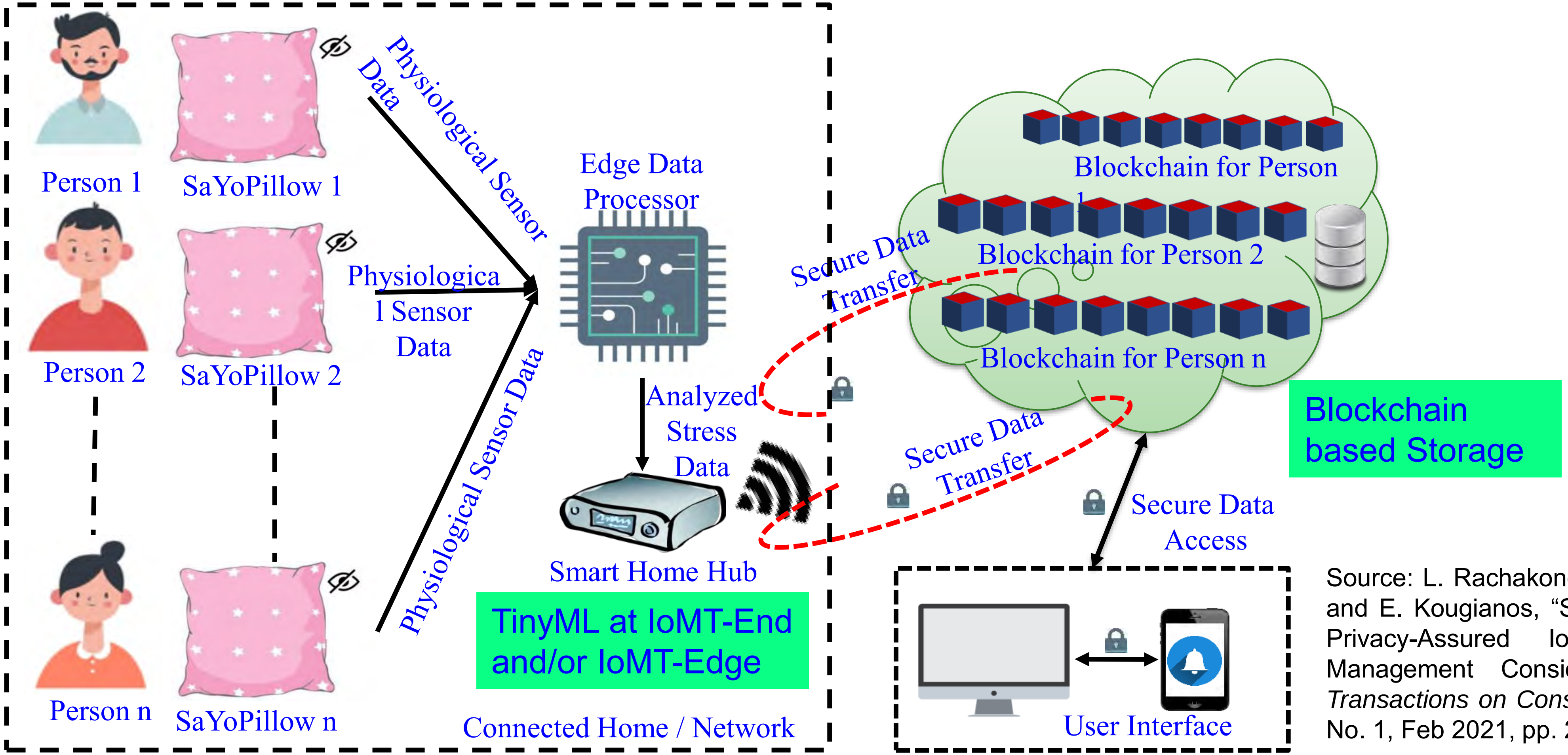
CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



- The time for data in MedRec are calculated assuming the mining time of the conventional Ethereum blockchain to be 13 Seconds for 1MB Data.

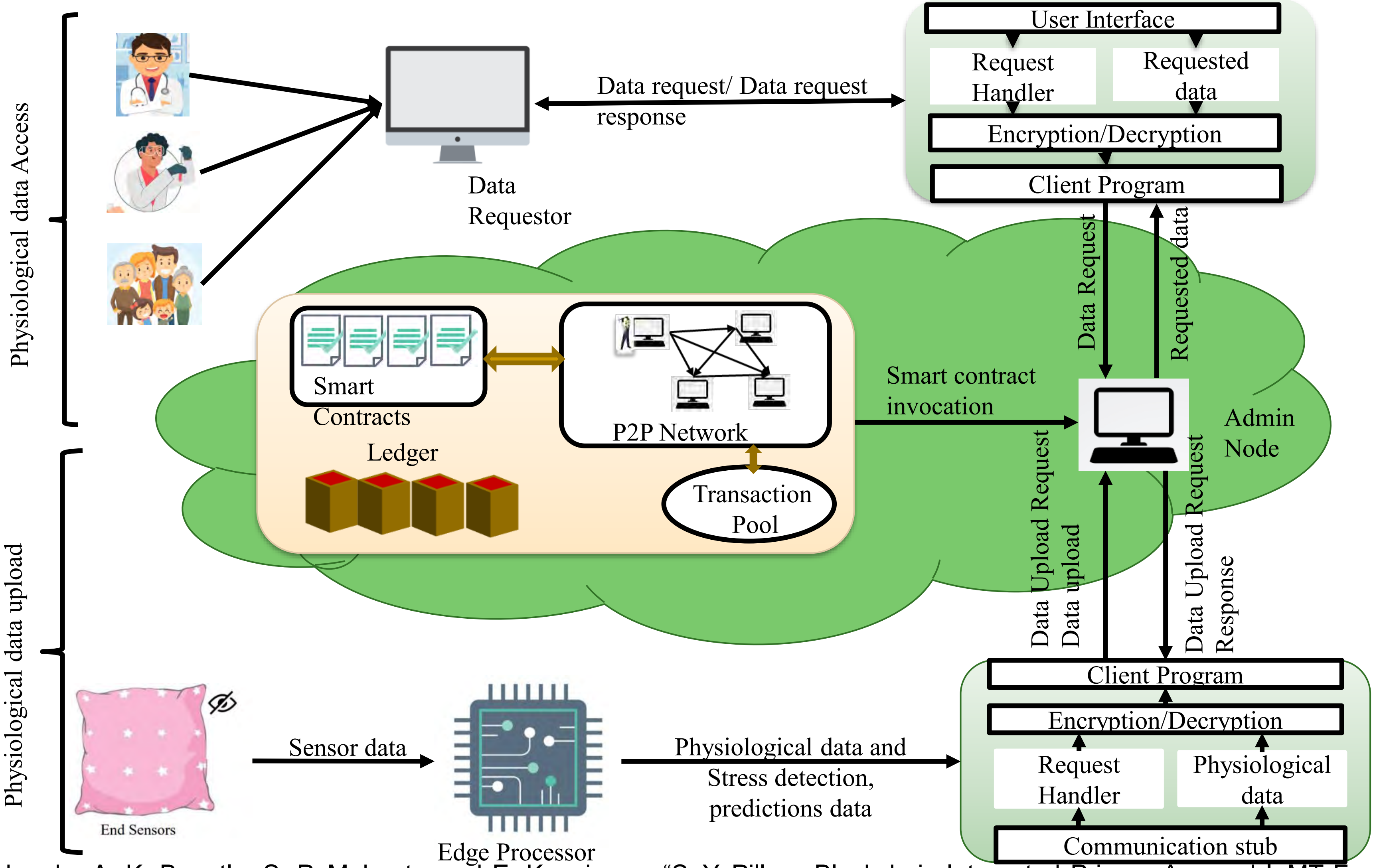
Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, *Springer Nature Computer Science (SN-CS)*, Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

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



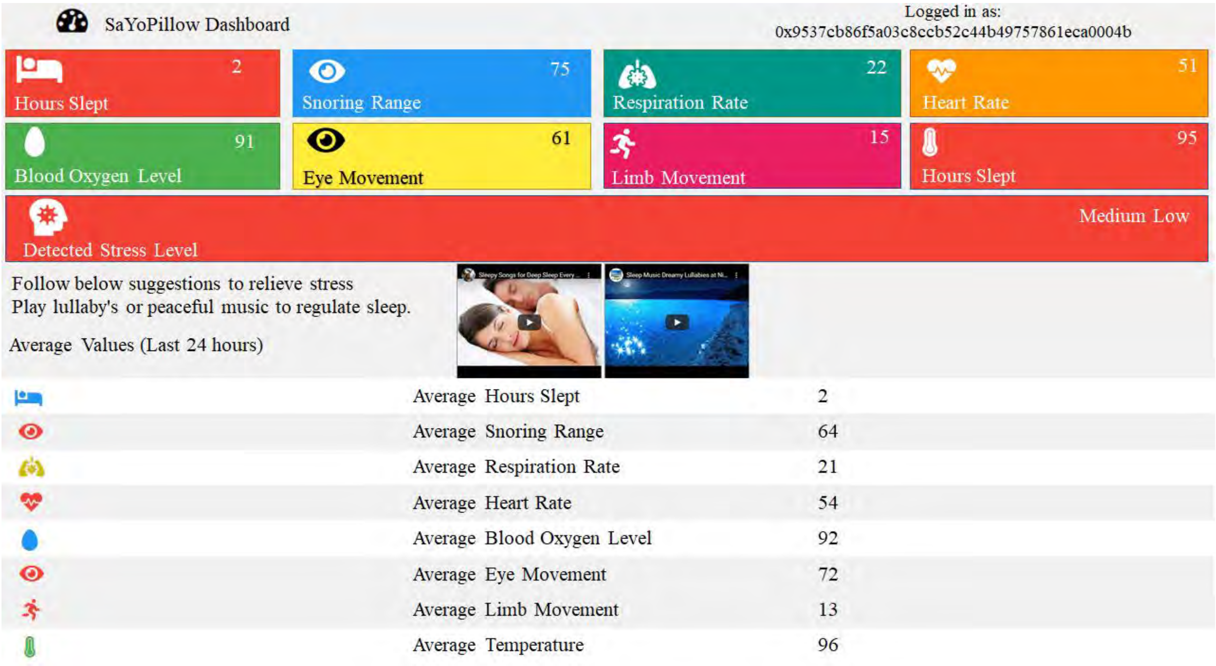
Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habit", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

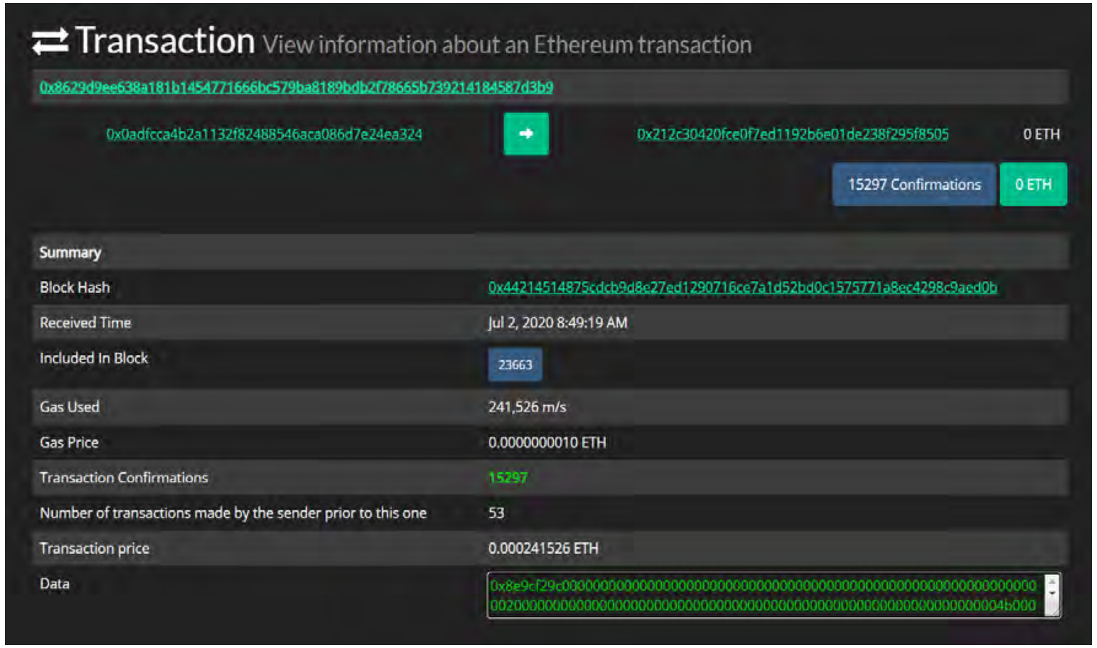
SaYoPillow: Blockchain Details

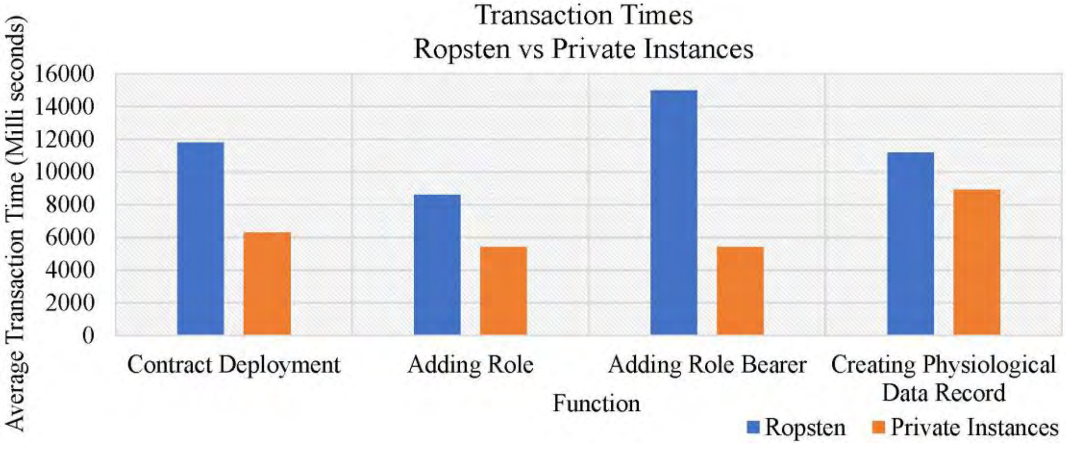


Source: L. Rachakonda, A. K. Bapatla, S. P. Mohanty, and E. Kougianos, "SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habit", *IEEE Transactions on Consumer Electronics (TCE)*, Vol. 67, No. 1, Feb 2021, pp. 20-29.

SaYoPillow: Blockchain Results







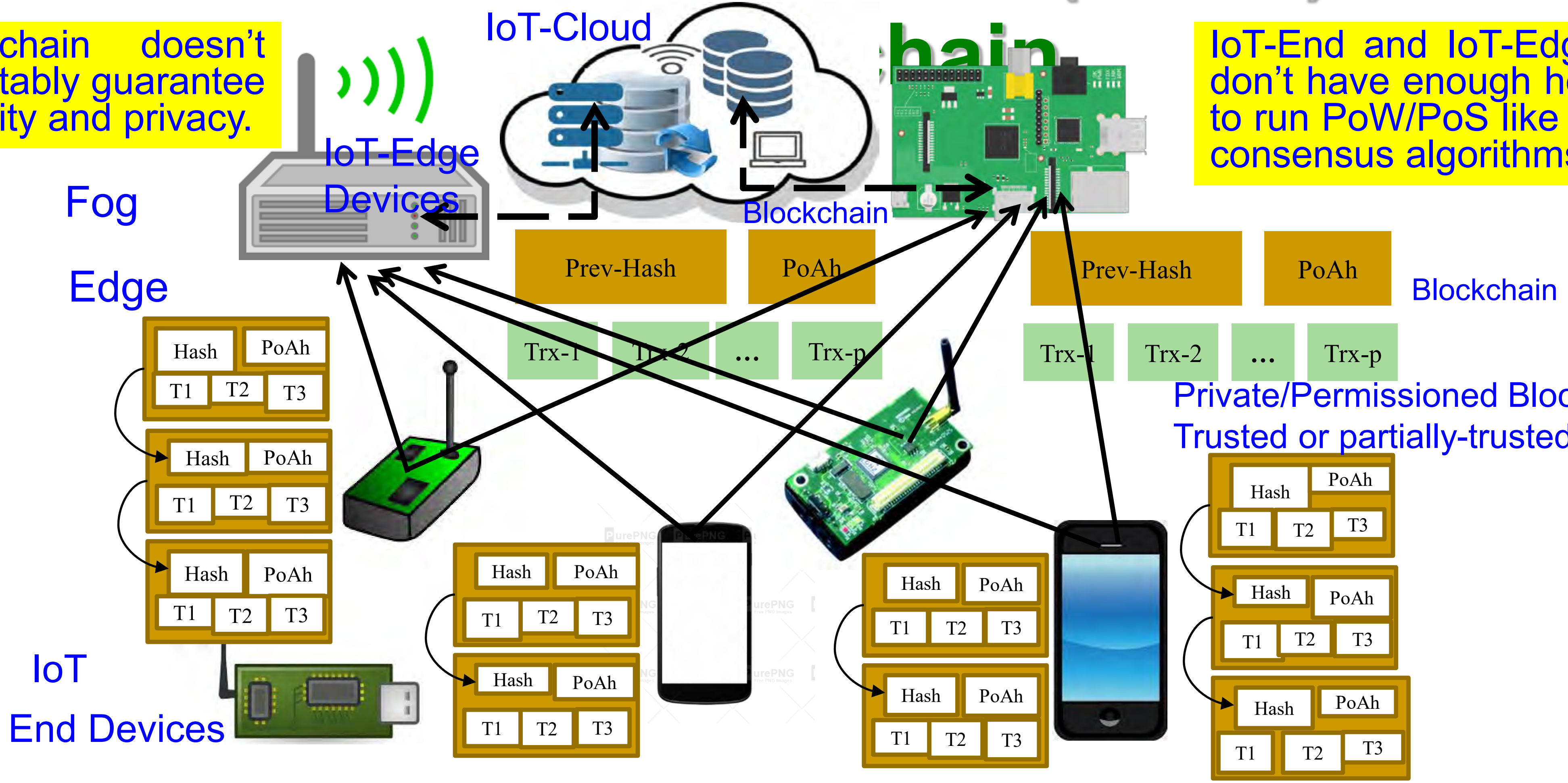
Transaction times of Private Ethereum in SaYoPillow is 2X faster in operations as compared to public ethereum test network Ropsten, as it is impacted by network congestion.

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.

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

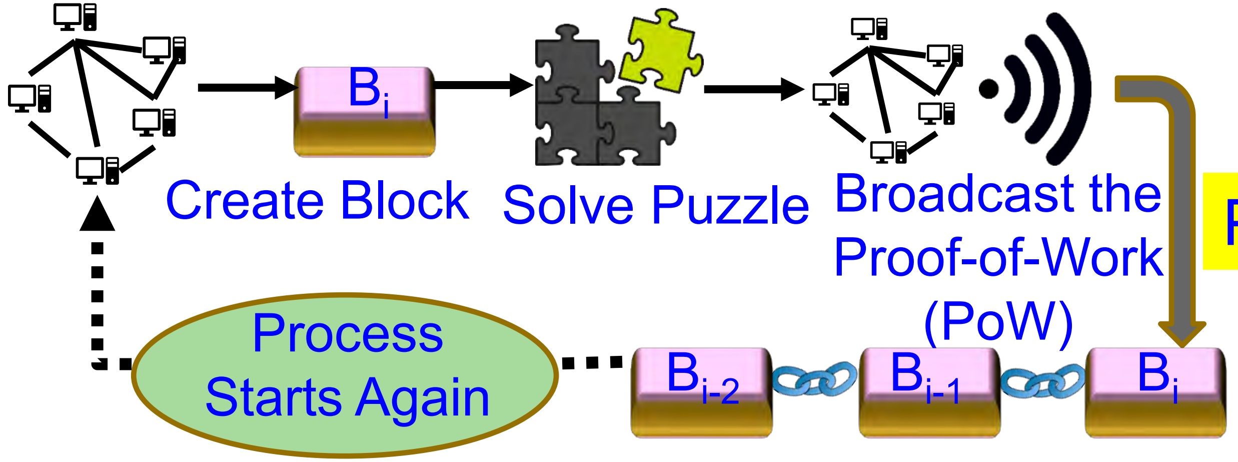
Blockchain doesn't inheritably guarantee security and privacy.

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.

EasyChain: Our Proof-of-Authentication (PoAh)

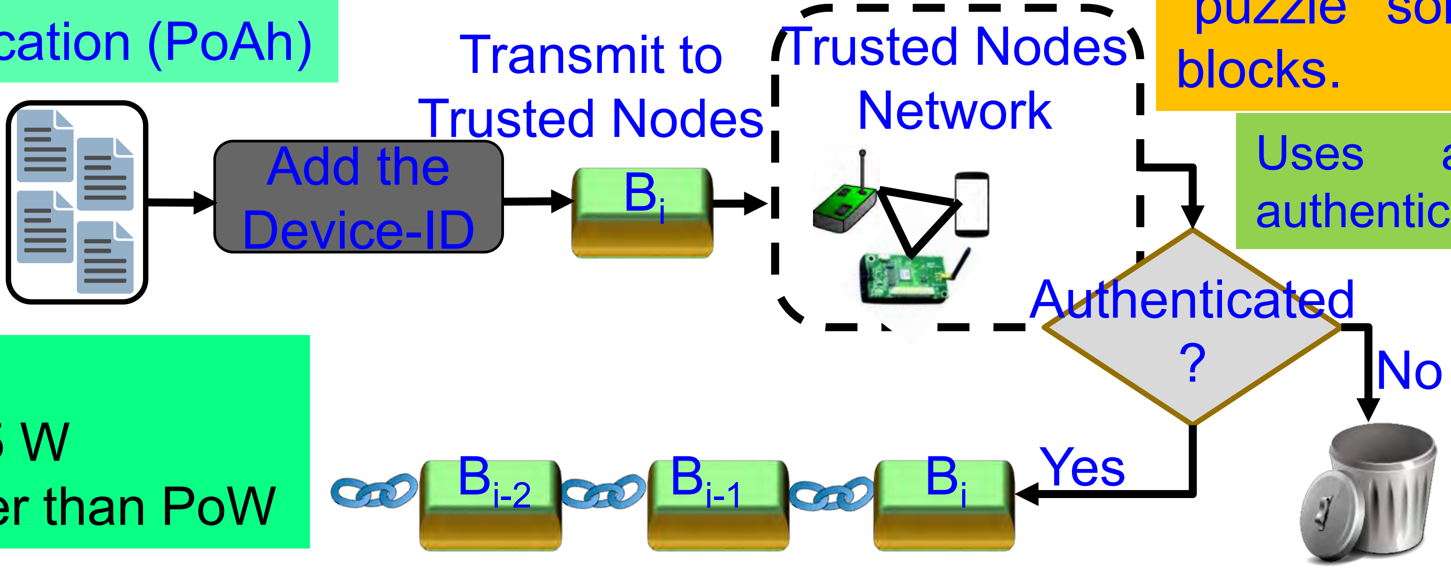


Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.

Proof of Authentication (PoAh)

Nodes form Block of Transactions

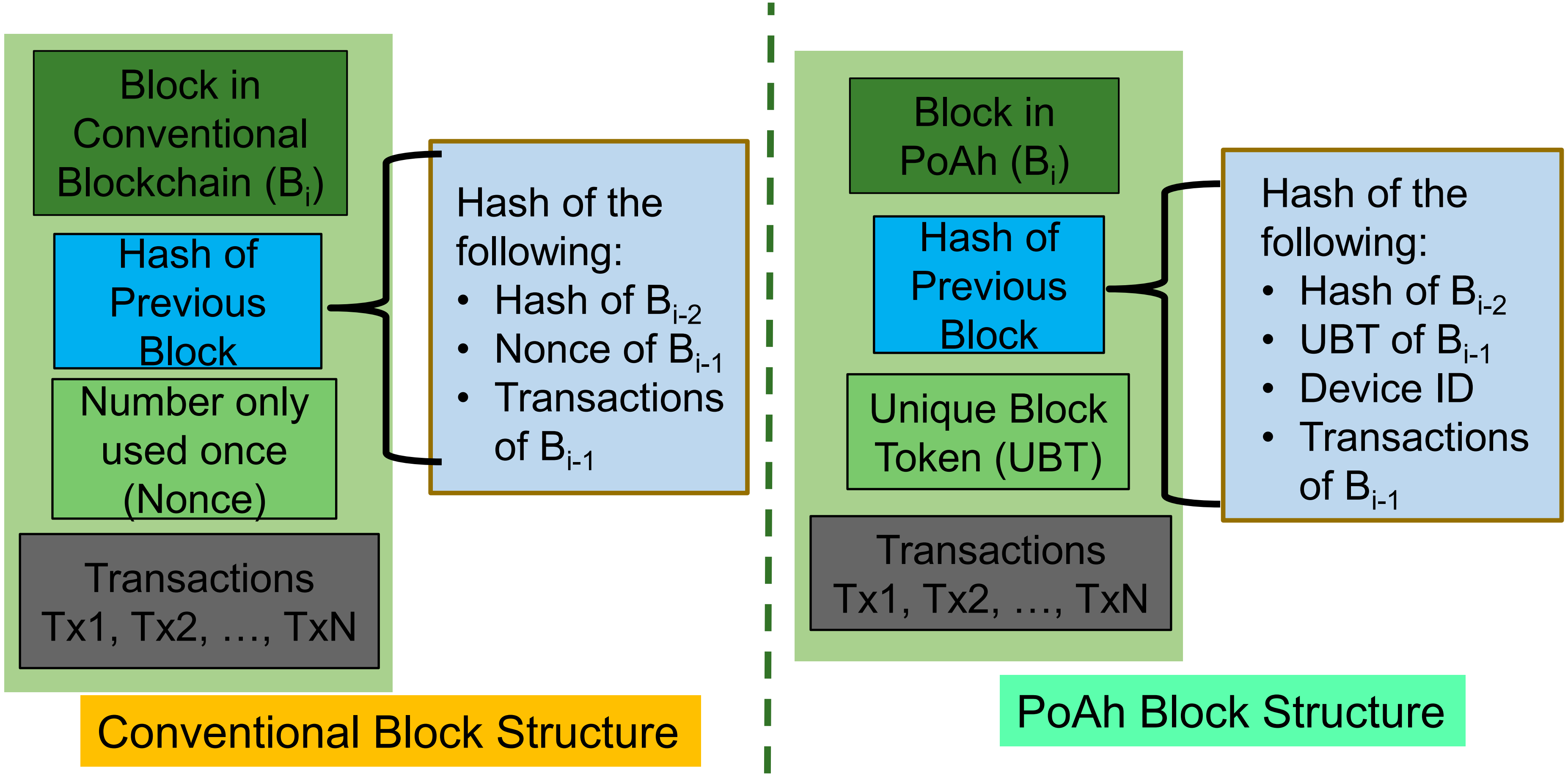


Uses a cryptographic authentication mechanism.

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

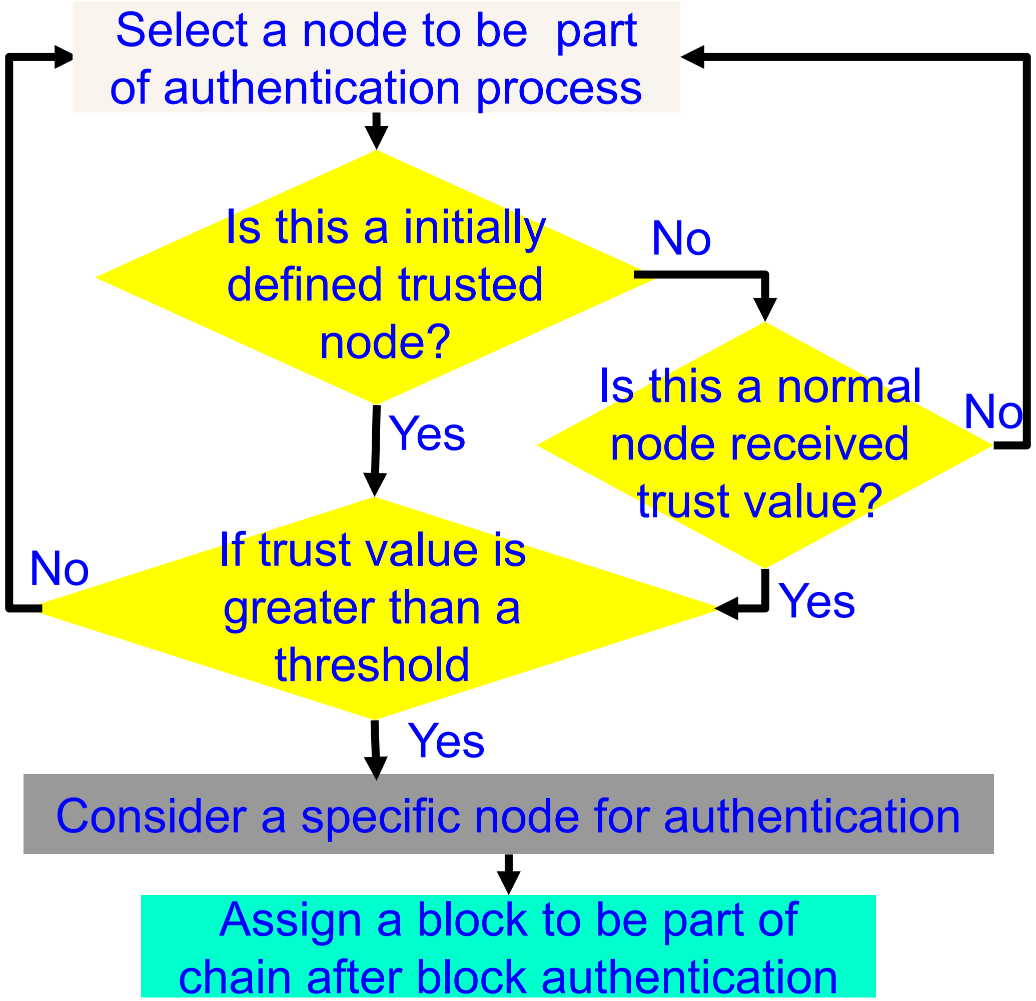
Source: D. Puthal and S. P. Mohanty, "Proof of Authentication: IoT-Friendly Blockchains", *IEEE Potentials Magazine*, Vol. 38, No. 1, January 2019, pp. 26--29.

Our PoAh-Chain: Proposed New Block Structure



Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and DataSecurity in the Internet of Everything(IoE)", arXiv Computer Science, arXiv:1909.06496, Sep 2019, 37-pages.

Our PoAh: Authentication Process

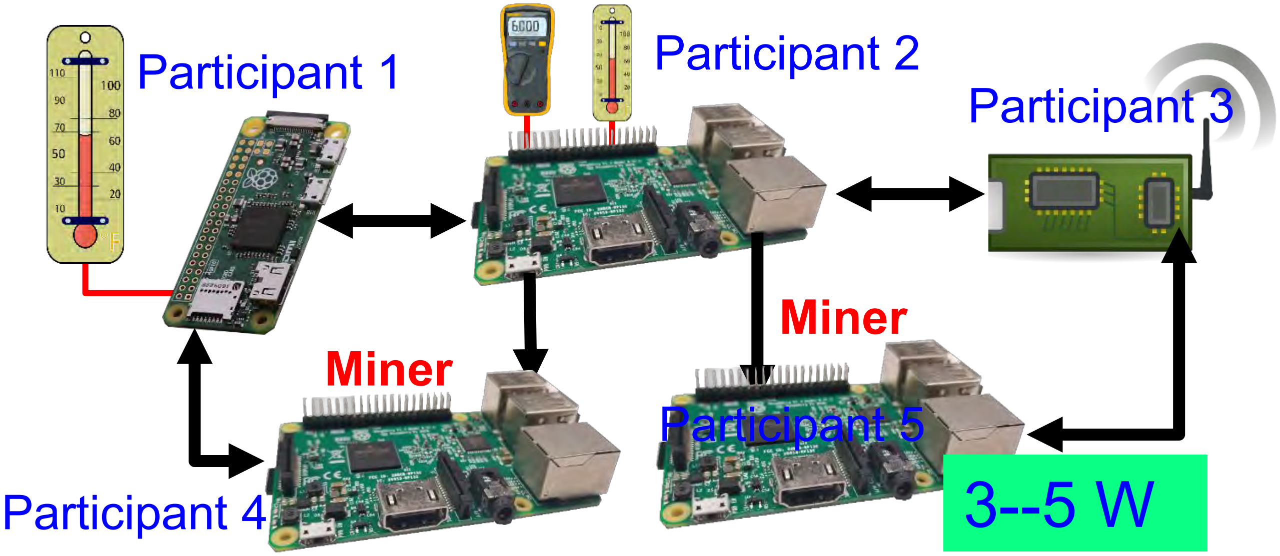


Algorithm 1: PoAh Block Authentication

Provided:
All nodes in the network follow SHA-256 Hash
Individual node has Private (PrK) and Public key (PuK)
Steps:
(1) Nodes combine transactions to form blocks
    $(Trx^+) \rightarrow$ blocks
(2) Blocks sign with own private key
    S_{PrK} (block) $\rightarrow$ broadcast
(3) Trusted node verifies signature with source public key
    V_{PuK}(block) $\rightarrow$ MAC Checking
(4) If (Authenticated)
    Block||PoAh(ID) $\rightarrow$ broadcast
    H(block) $\rightarrow$ Add blocks into chain
(5) Else
    Drop blocks
(6) GOTO (Step-1) for next block

Steps to find a Trusted Node which will Authenticate a Block.

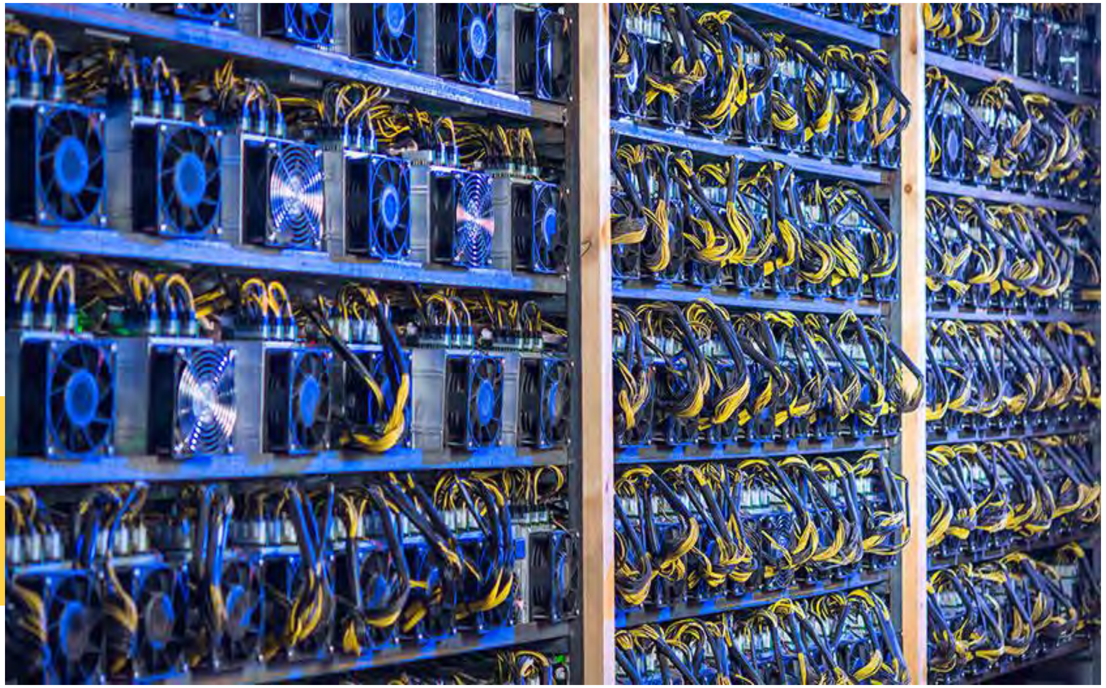
Our PoAh-Chain Runs in Resource Constrained Environment



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

Blockchain using PoW Needs Significant Resource

500,0000 W

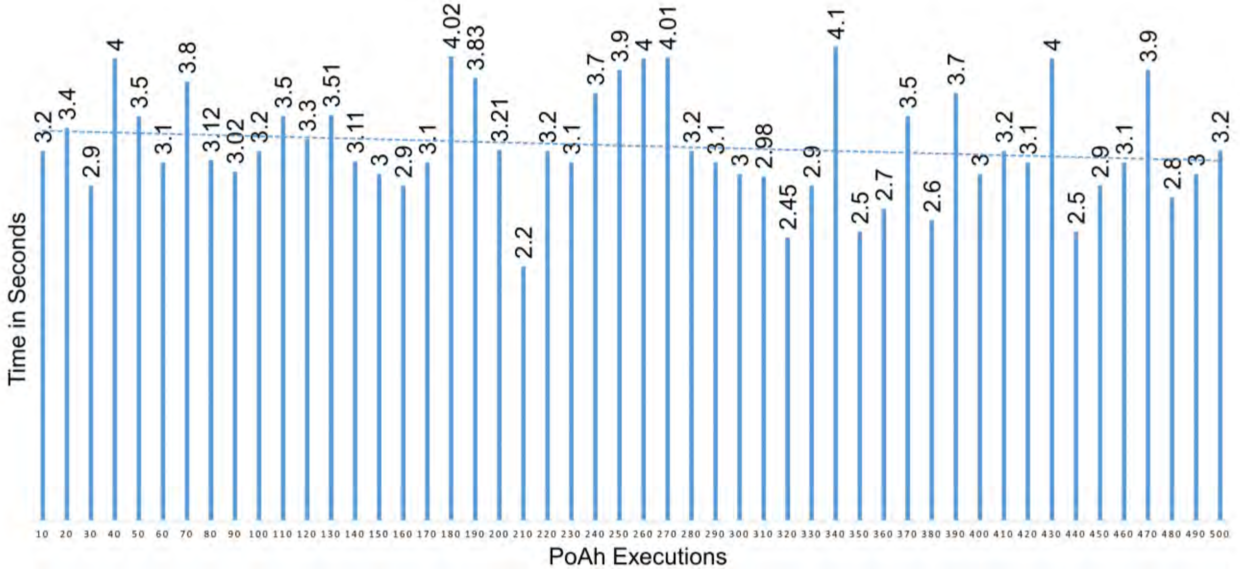


Source: D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks", *arXiv Computer Science*, arXiv:2001.07297, January 2020, 26-pages.

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

Our PoAh is 200X Faster than PoW While Consuming a Very Minimal Energy

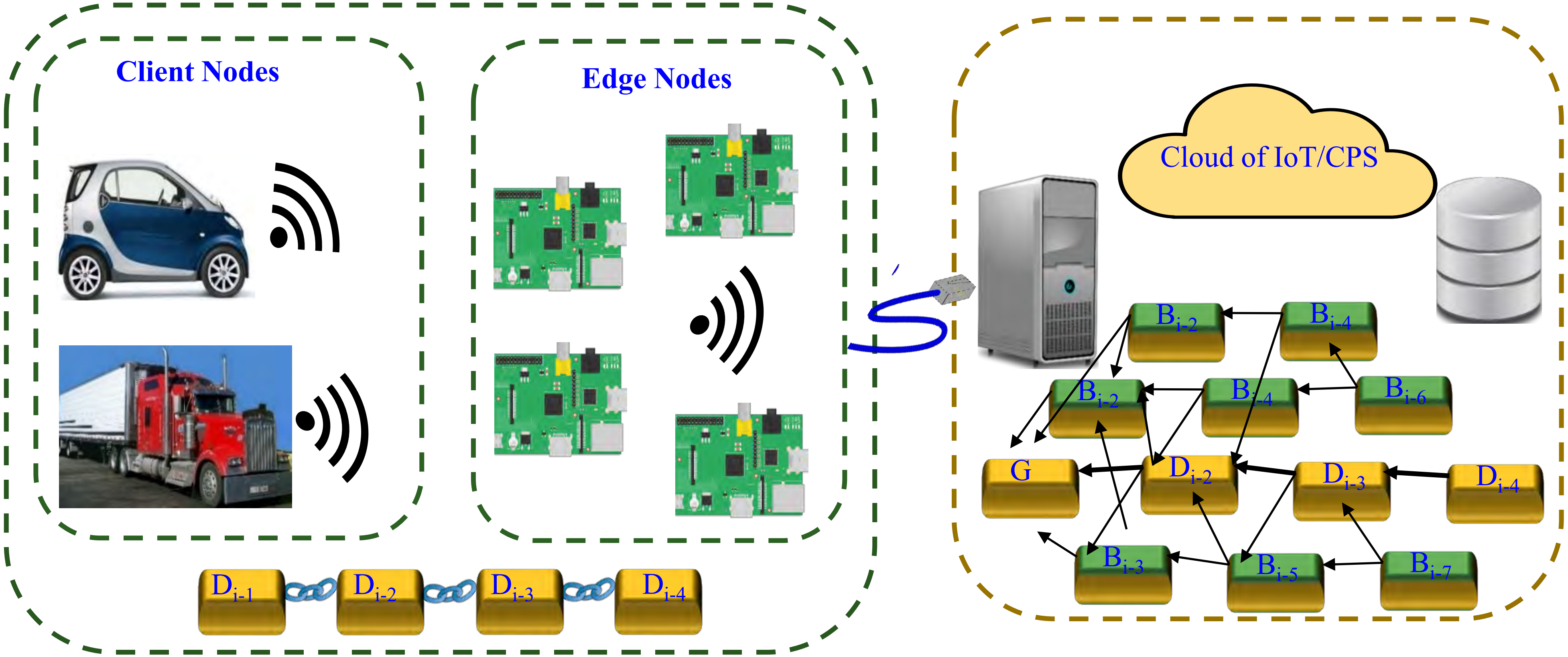
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, DoS	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



PoAh Execution for 100s of Nodes

Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

FlexiChain: Our Multi-Chain Technology to Enhance Blockchain Scalability



(a) Nodes-Chain

(b) Multi-Blockchains

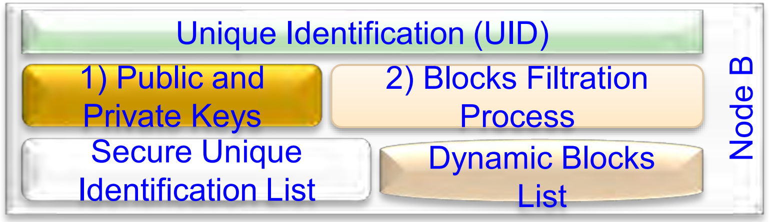
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

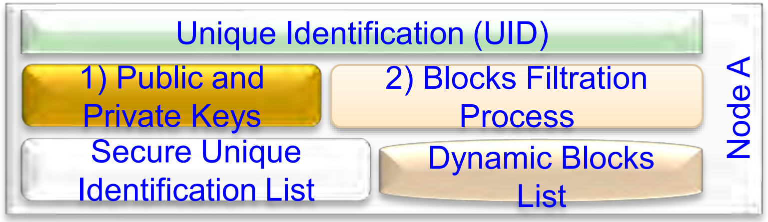
A Perspective of BC, Tangle Vs Our Multichain

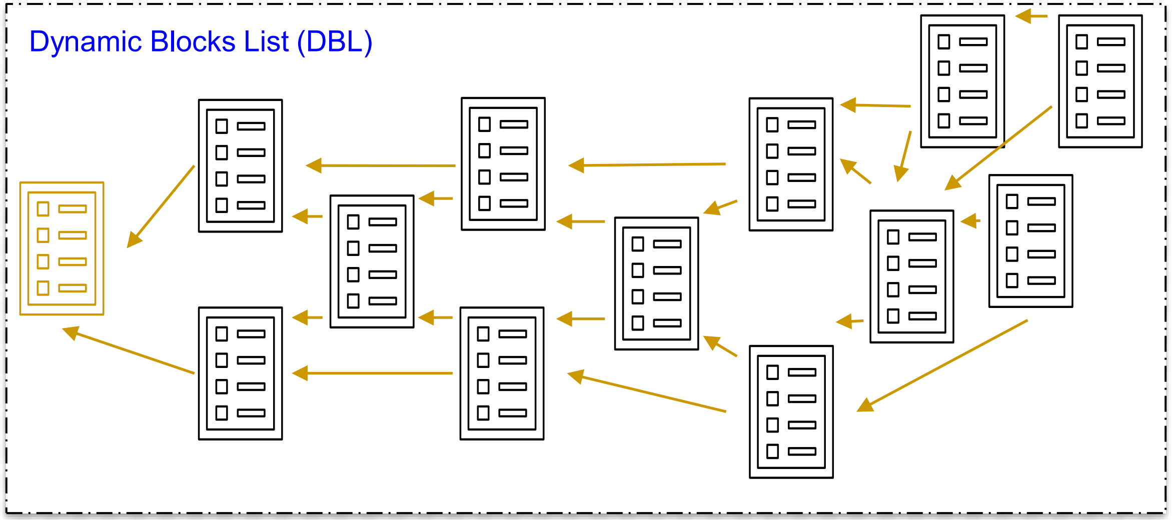
Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRA (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions hash	• DAG linked List. • Block of transactions. • Reduced block.
Validation	Mining	Authentication	Mining	Virtual Voting (witness)	Authentication
Type of validation	Miners	Trusted Nodes	Transactions	Containers	All Nodes
Ledger Requirement	Full ledger required	Full ledger required	Portion based on longest and shortest paths.	Full ledger required	Portion based on authenticators' number
Cryptography	Digital Signatures	Digital Signatures	Quantum key signature	Digital Signatures	Digital Signatures
Hash function	SHA 256	SHA 256	KECCAK-384	SHA 384	SCRYPT
Consensus	Proof of Work	Cryptographic Authentication	Proof of Work	aBFT	Predefined UID
Numeric System	Binary	Binary	Trinity	Binary	Binary
Involved Algorithms	HashCash	No	• Selection Algorithm • HashCash	No	BFP
Decentralization	Partially	Partially	Fully	Fully	Fully
Appending Requirements	Longest chain	One chain	Selection Algorithm	Full Randomness	Filtration Process
Energy Requirements	High	Low	High	Medium	Low
Node Requirements	High Resources Node	Limited Resources Node	High Resources Node	High Resources Node	Limited Resources Node
Design Purpose	Cryptocurrency	IoT applications	IoT/Cryptocurrency	Cryptocurrency	IoT/CPS applications

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446--451.

McPoRA based MultiChain -- Components







Secure Unique Identification List (SUIL)

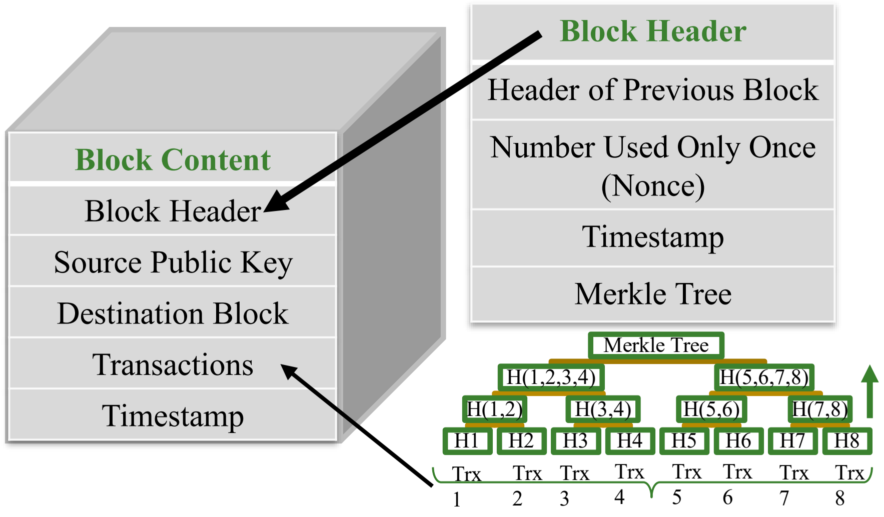
Secure IDs' file consists of all active Nodes joined the Private network.

Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique Identification (UID)

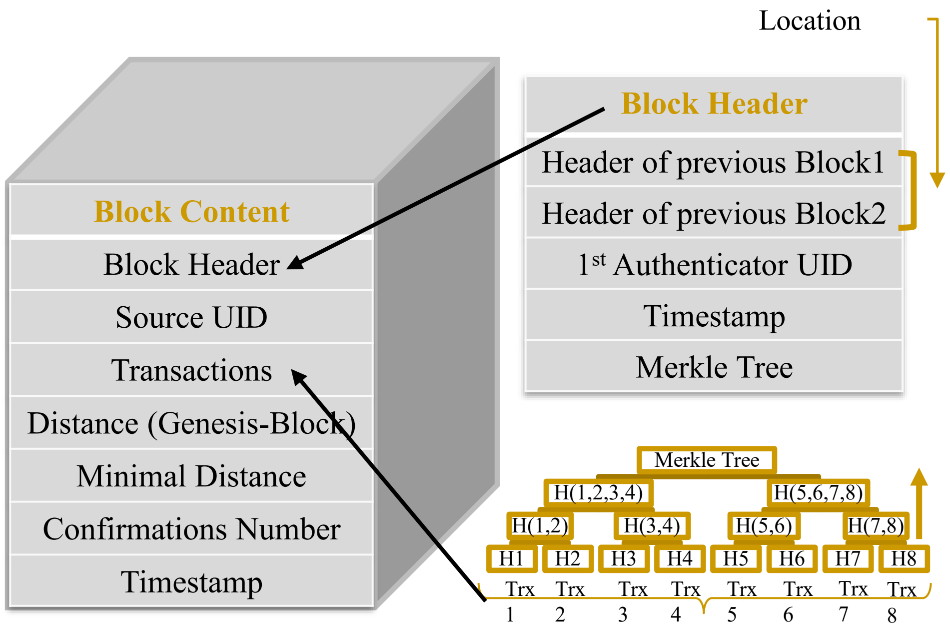
Consensus Time – 0.7 sec (Avg)
Power Consumption – 3.5 W
Performance – 4000X faster than PoW

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

Block Structure in McPoRA



(a) For Traditional Blockchain

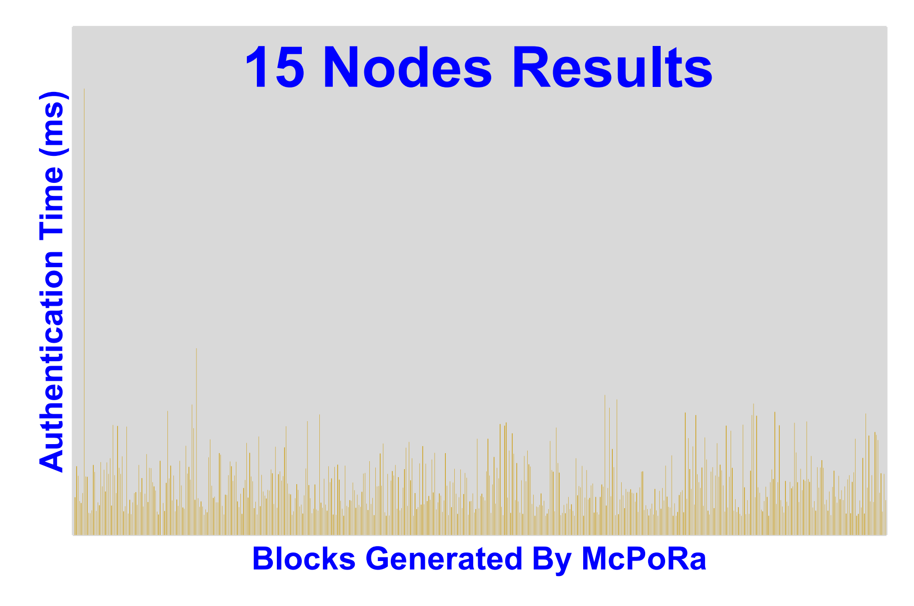


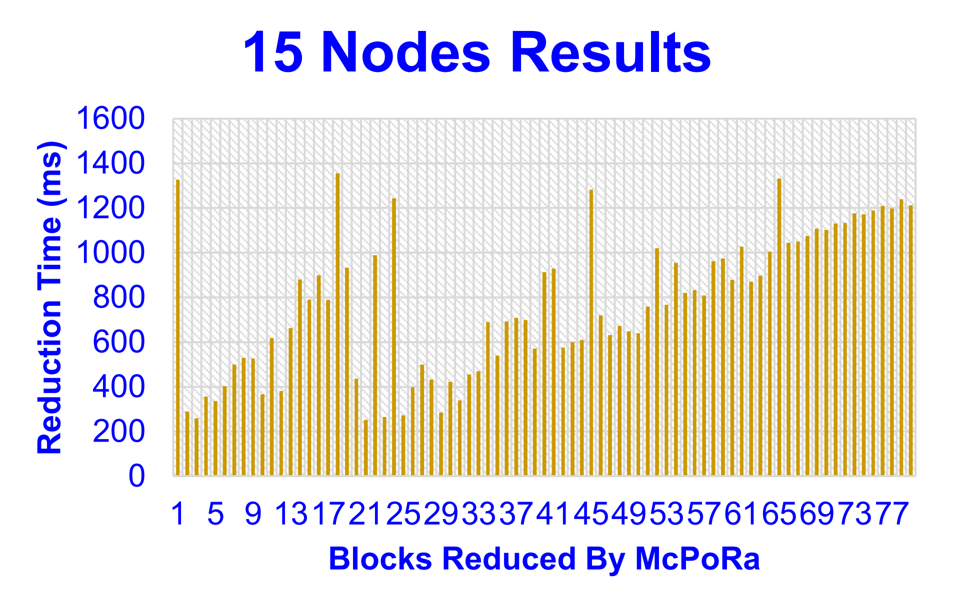
(b) For Proposed Post-Blockchain

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

McPoRA – Experimental Results

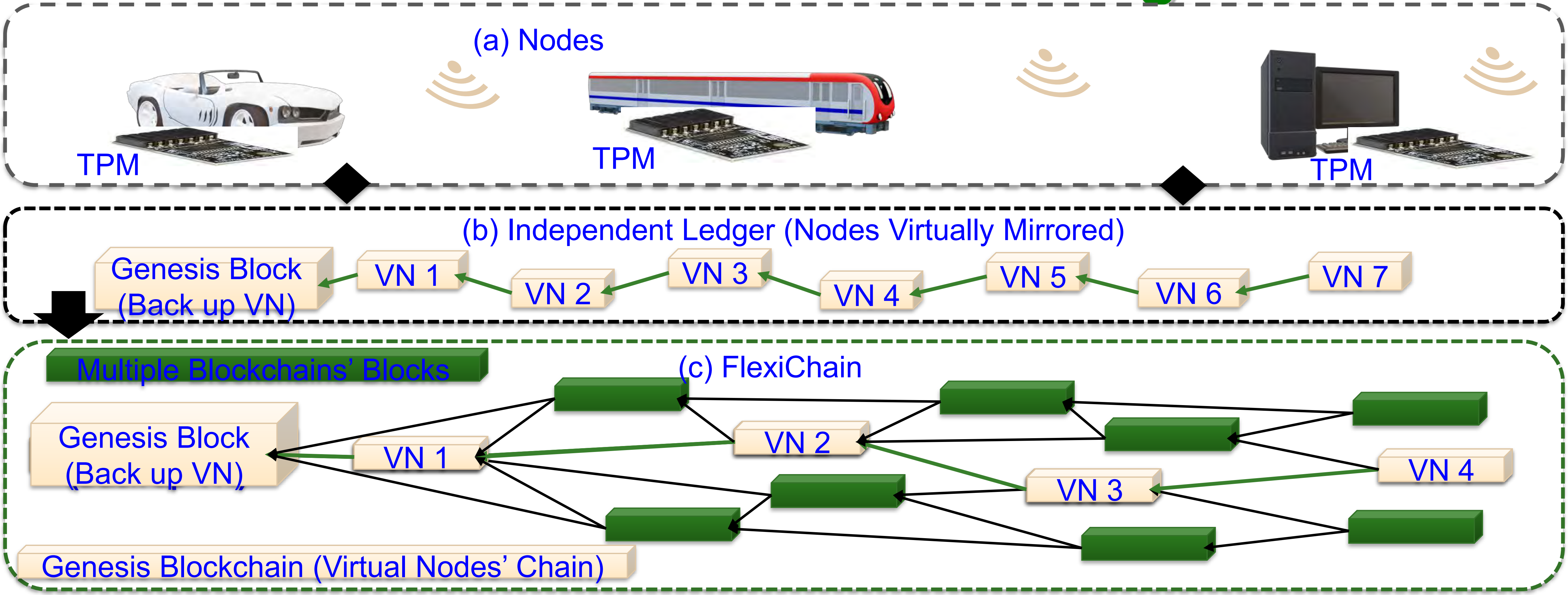
Time (ms)	Authentication (ms)	Reduction (ms)
Minimum	1.51	252.6
Maximum	35.14	1354.6
Average	3.97	772.53





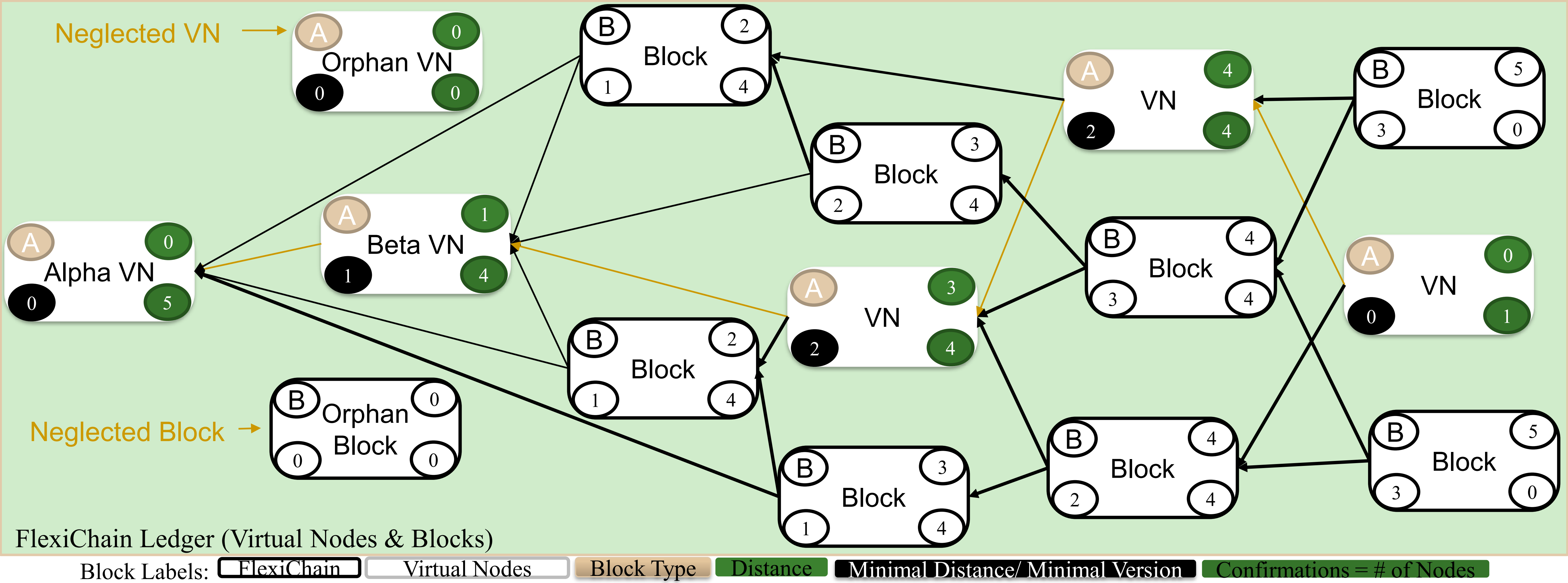
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446—451.

FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS



Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS



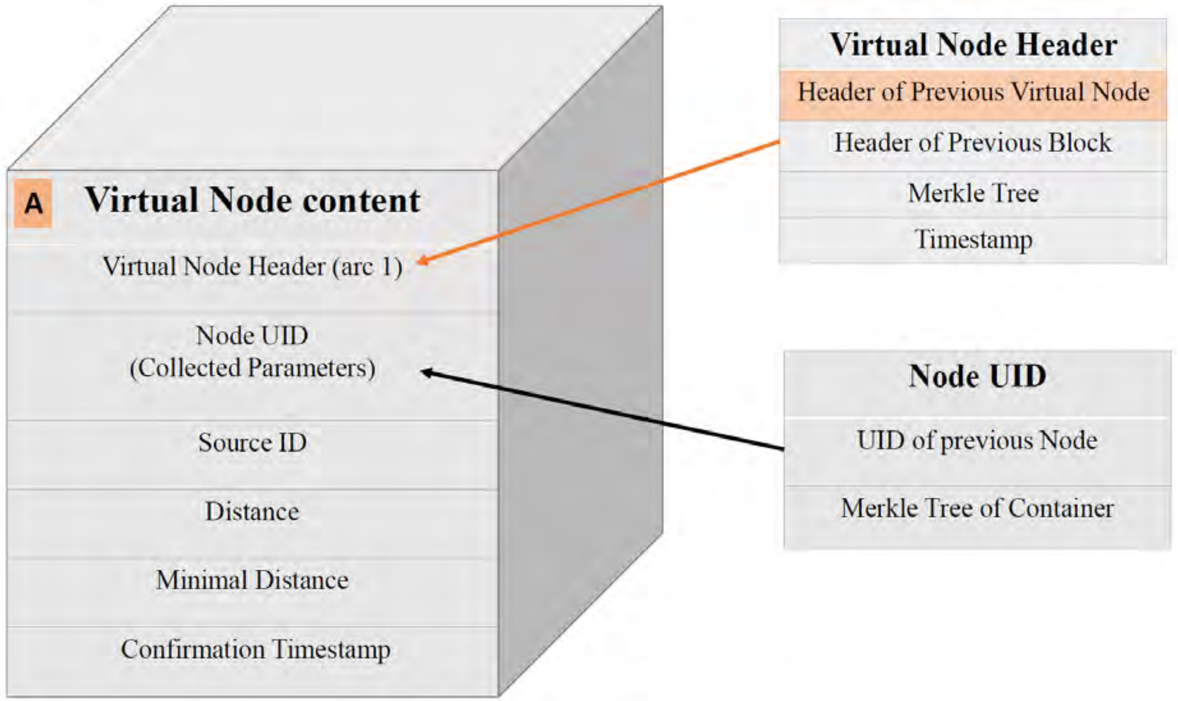
Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS

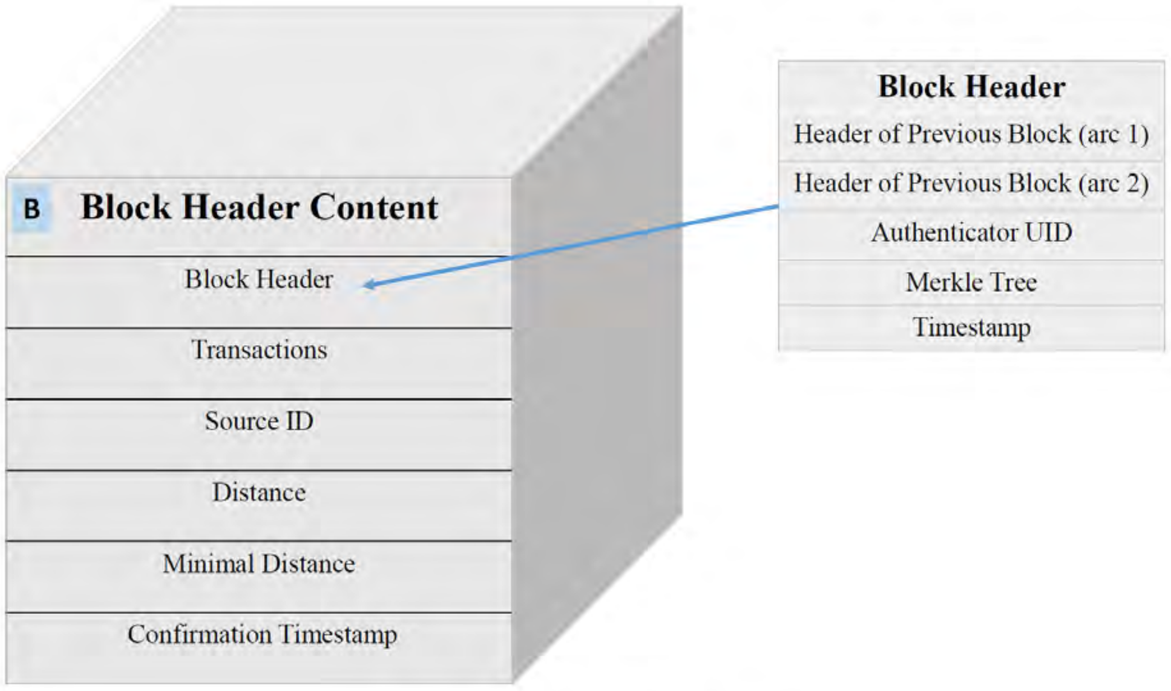
Features	Blockchain Technology (for Bitcoin) [22, 18]	Tangle Technology (for Cryptocurrency) [12, 21]	HashGraph Distributed Ledger Technology [3, 4]	McPoRa (Our Previous paper) [1]	Minerless FlexiChain Technology (current paper)
Linked Lists	– Linked list of blocks – Each block contains multiple transactions	– DAG linked list – One transaction	– DAG linked List – Container of transaction hash	– DAG linked List – Each block contains multiple transactions	– Genesis Blockchain (independent ledger) – DAG linked list
Registration	Manual	Manual	Manual	Manual	Pre-Installed or Equipped Manufacturer Trusted Modules
Type of Validation	Mining	Mining	Virtual voting (witness)	Authentication (Minerless)	Authentication (Minerless)
Validators	Miners	Transactions	Containers	All Nodes	All Virtual Nodes
Types of Nodes	– Traders – Miners	– Traders – Coordinators	– Users	– Users	– Users – Back up
Number of Chains	One Chain	One Chain	One Chain	Multi-Chain	Multi-Chain: An Identified and Integrated NodeChain
Cryptography	Digital Signatures	Quantum key signature	Digital Signatures	Digital Signatures	– Trusted modules keys – Post-Constructed Digital Signatures
Hash Function	SHA 256	KECCAK-384	SHA 384	SCRYPT	SCRYPT
Consensus	Proof of Work	Proof of Work	Asynchronous Byzantine Fault Tolerance (ABFT)	Predefined UID Authentication	Two Factor Authentication: Constructed Public ID and Constructed UID
Numeric System	Binary	Trinity	Binary	Binary	Binary
Energy Requirements	High	High	Medium	Low	Low
Node Requirements	High Resources Node	High Resources Node	High Resources Node	Limited Resources Node	Limited Resources Node
Design Purpose	Cryptocurrency	IoT Cryptocurrency	Cryptocurrency	IoT/CPS Applications	IoT/CPS Applications
Block type	One	One	One	One	Two Blocks: – MC Block – VN Block – more as needed.

Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS



(a) Block Type A



(b) Block Type B

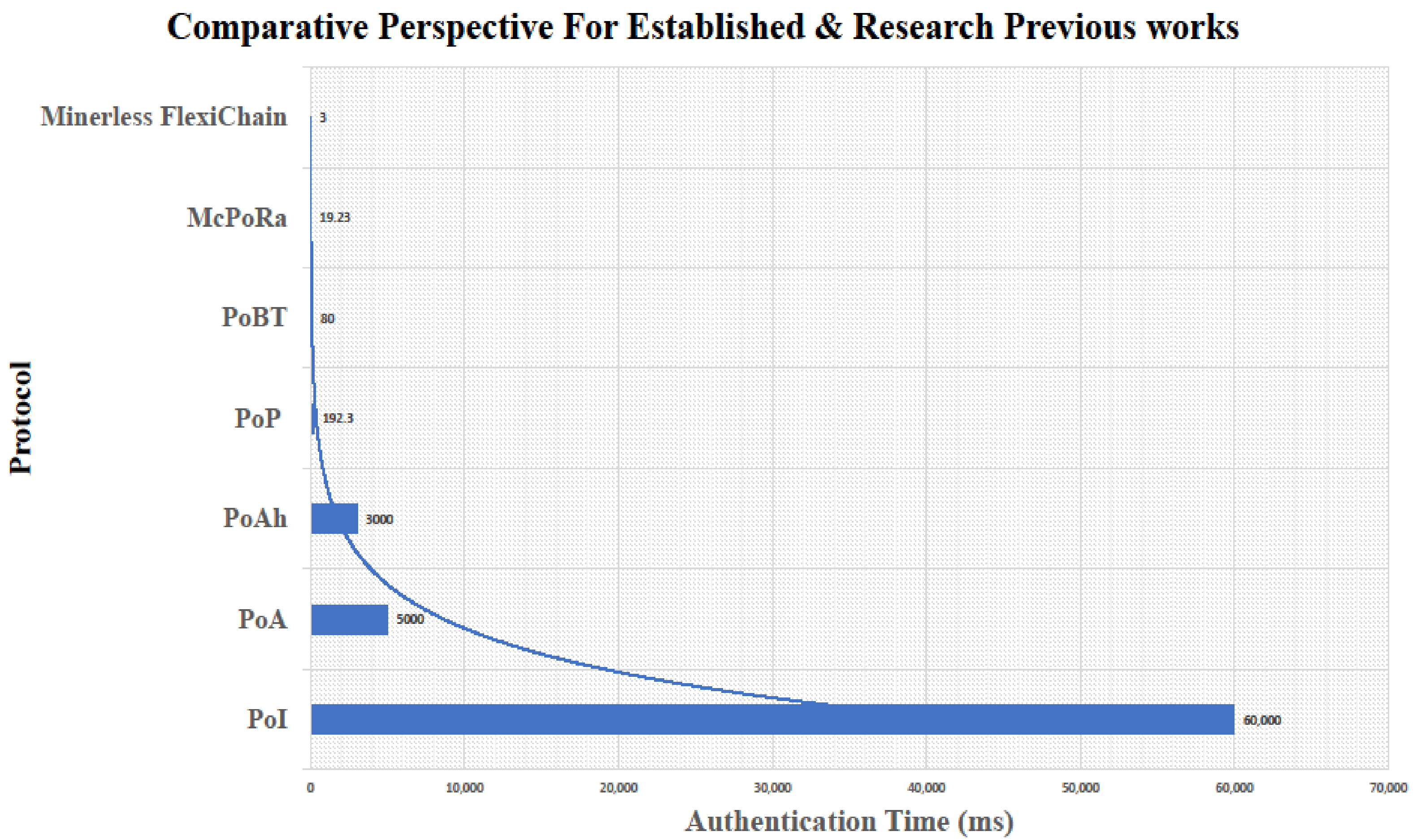
Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS

Consensus Algorithm	Registration (ms)	Authentication (ms)	Ledger	Miners	Validation	Blockchain Type	Linked List
Proof of Importance (PoI) [19]	Manual	60,000	Full	Yes	Accounts Importance	Public	Blockchain
Proof of Authority (PoA) [29]	Manual	5000	Full	Yes	PoS	Permissioned	Blockchain
Proof of Authentication (PoAh) [24]	Manual	3000	Full	Yes	Cryptographic	Private	Blockchain
Proof of PUF-Enabled Authentication (PoP) [17]	Manual	192.3	Full	Yes	Predefined PUF keys verification	Private	Blockchain
Proof of Block and Trade (PoBT) [6]	Manual	80-210	Full	Yes	Smart Contract and BFT	Private	Blockchain
McPoRA (Previous Paper) [1]	Manual	3.9-19.23 (Avg.)	Portion	No	UID verification	Private	Multichain
Minerless FlexiChain (Current Paper)	Automated 0.48 - 0.7 (Avg.)	1.23 - 3 (Avg.)	Portion	No	UID verification	Private	FlexiChain (Multiple-Integrated Conventional Blockchains)

Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

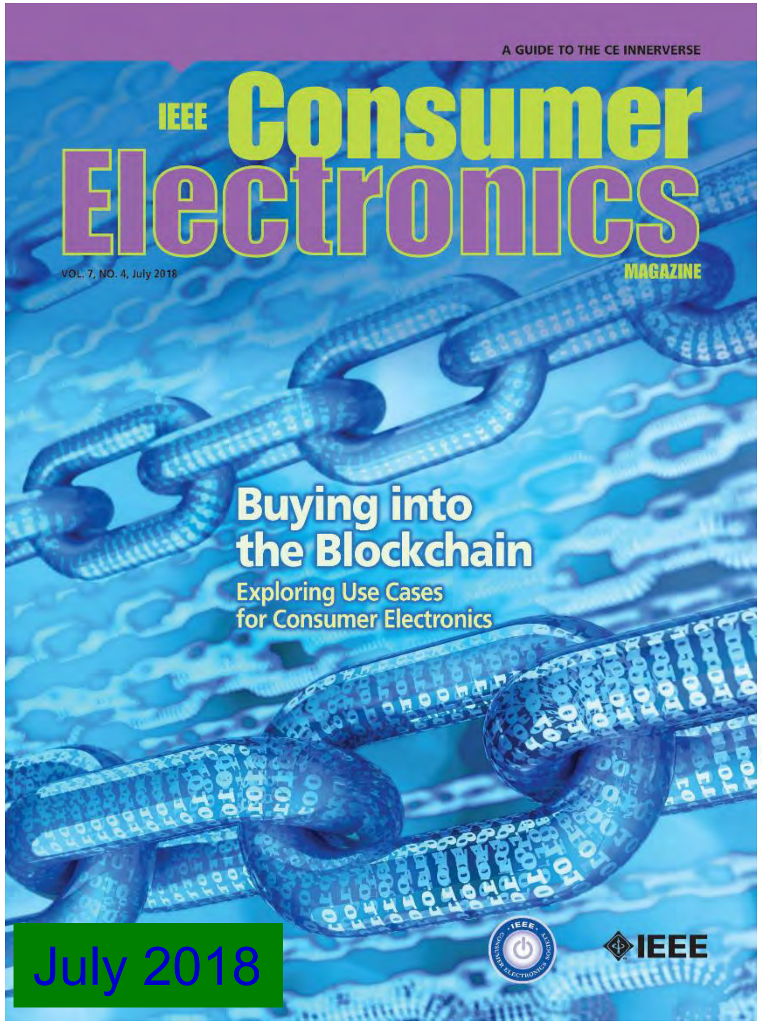
FlexiChain: A Minerless Scalable Next Generation Blockchain for Large CPS

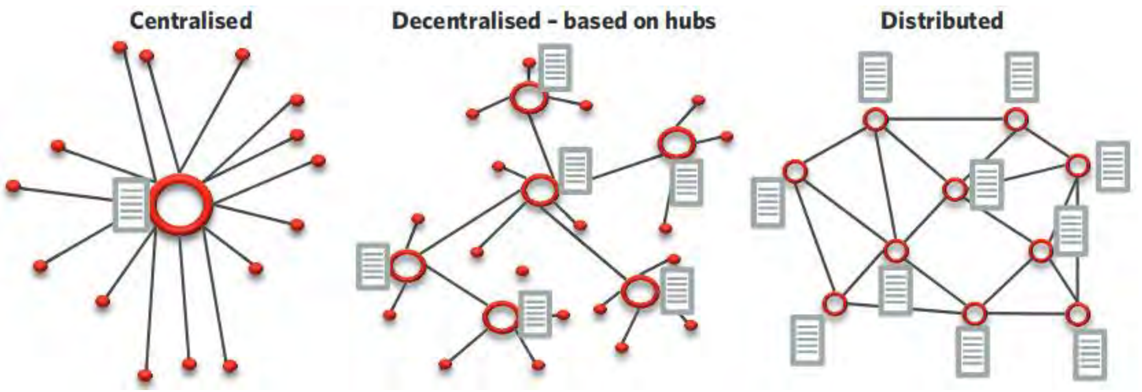


Source: A. J. Alkhodair, **S. P. Mohanty**, and E. Kougianos, "FlexiChain: A Minerless Scalable Next Generation Blockchain for Rapid Data and Device Security in Large Scale Complex Cyber-Physical Systems", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 3, May 2022, Article: 235, 13-pages, DOI: https://doi.org/10.1007/s42979-022-01139-4.

Distributed Ledger – Broad Overview

Blockchain Technology



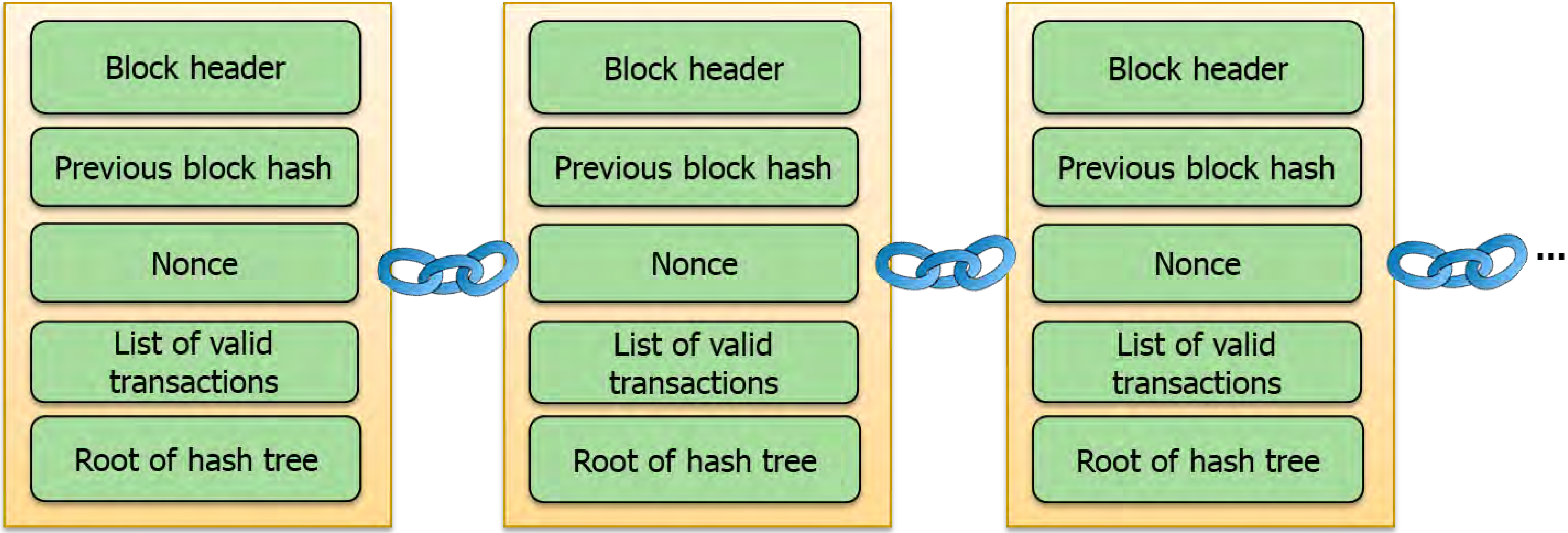


Source: https://icomalta.com/distributed-ledger-technology/

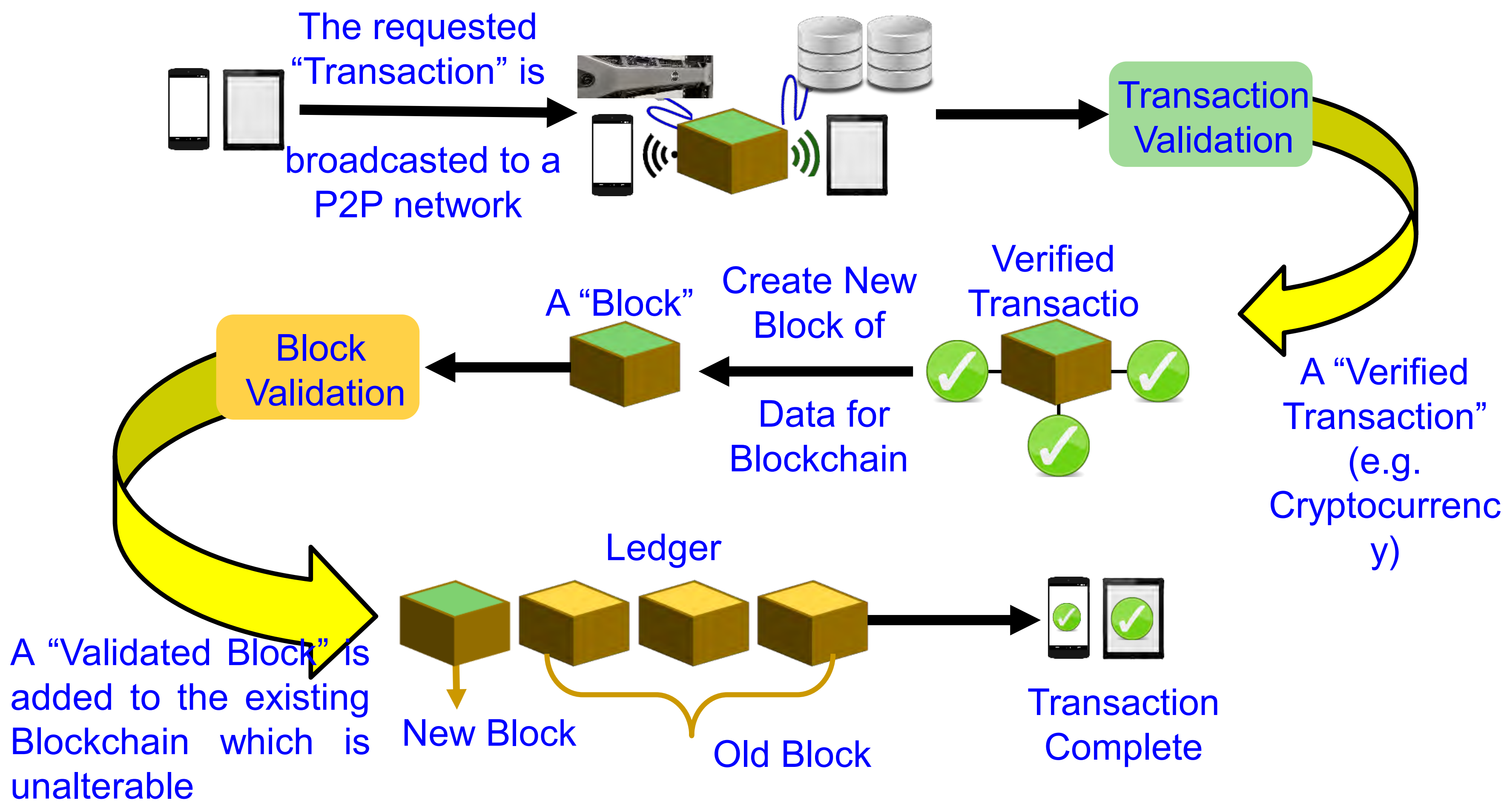
Blockchains

- Blockchain is ledger of Blocks connected by cryptographic hashes which have group of transactions.
- This ledger is typically managed by peer-to-peer network which has preset rules on validating and updating the new blocks to blockchain.
- Blockchains are considered as SbD (Secure by Design) as the Transactions once accepted into chain cannot be modified or altered in any way.
- Fully functional application of Blockchain Bitcoin is invented by Satoshi Nakamoto in 2008.
- These properties of blockchain help in managing digital assets efficiently.

Blockchain Structure



Blockchain - Working Model

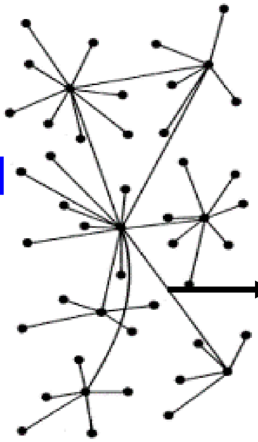


Source: Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das, "Everything you Wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Vol. 8, No. 4, pp. 6--14, 2018.

Transaction Generation

Transaction is requested by a node

Broadcasted to a P2P network of nodes



P-2-P Network

Users in same network know address of each other

It is called as input transaction: has amount to be transferred + recipient's bitcoin (BTC) address

Input Transaction

Public Key Hash of receiver: 'A' BTC address

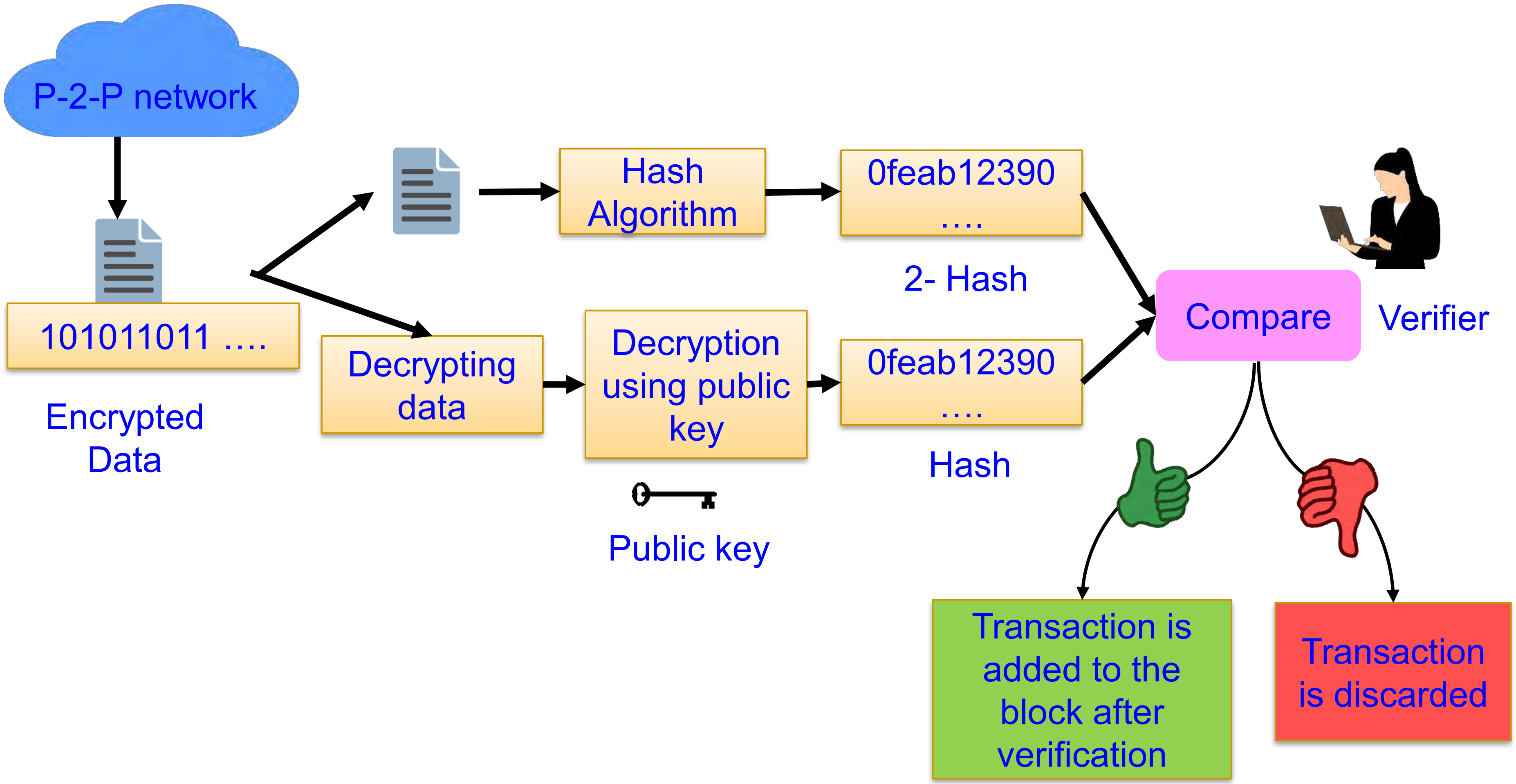
Hashing (e.g. SHA-256)

Unique Transaction identity

Sender's Private key

Digital Signature

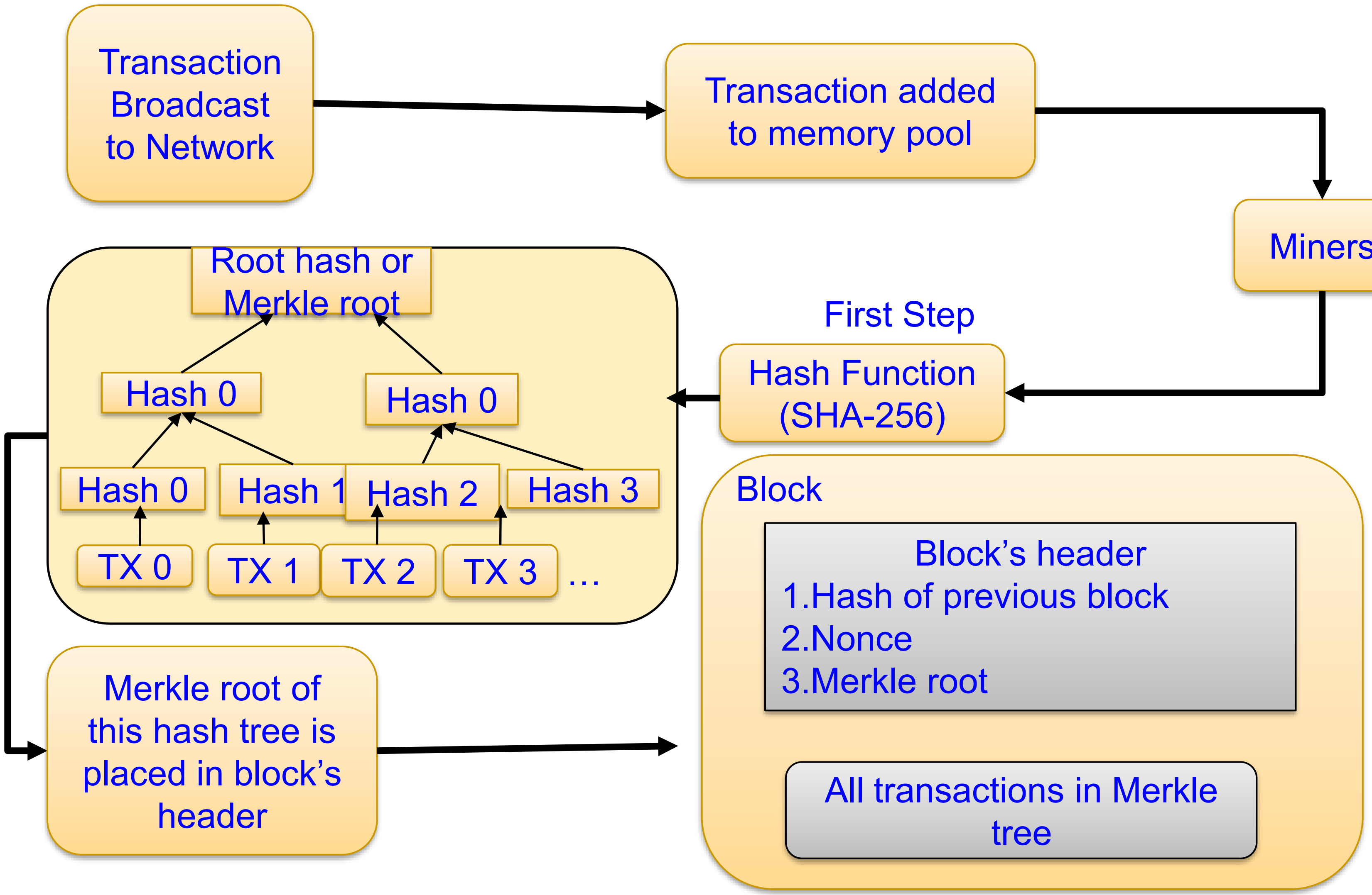
Transaction Validation



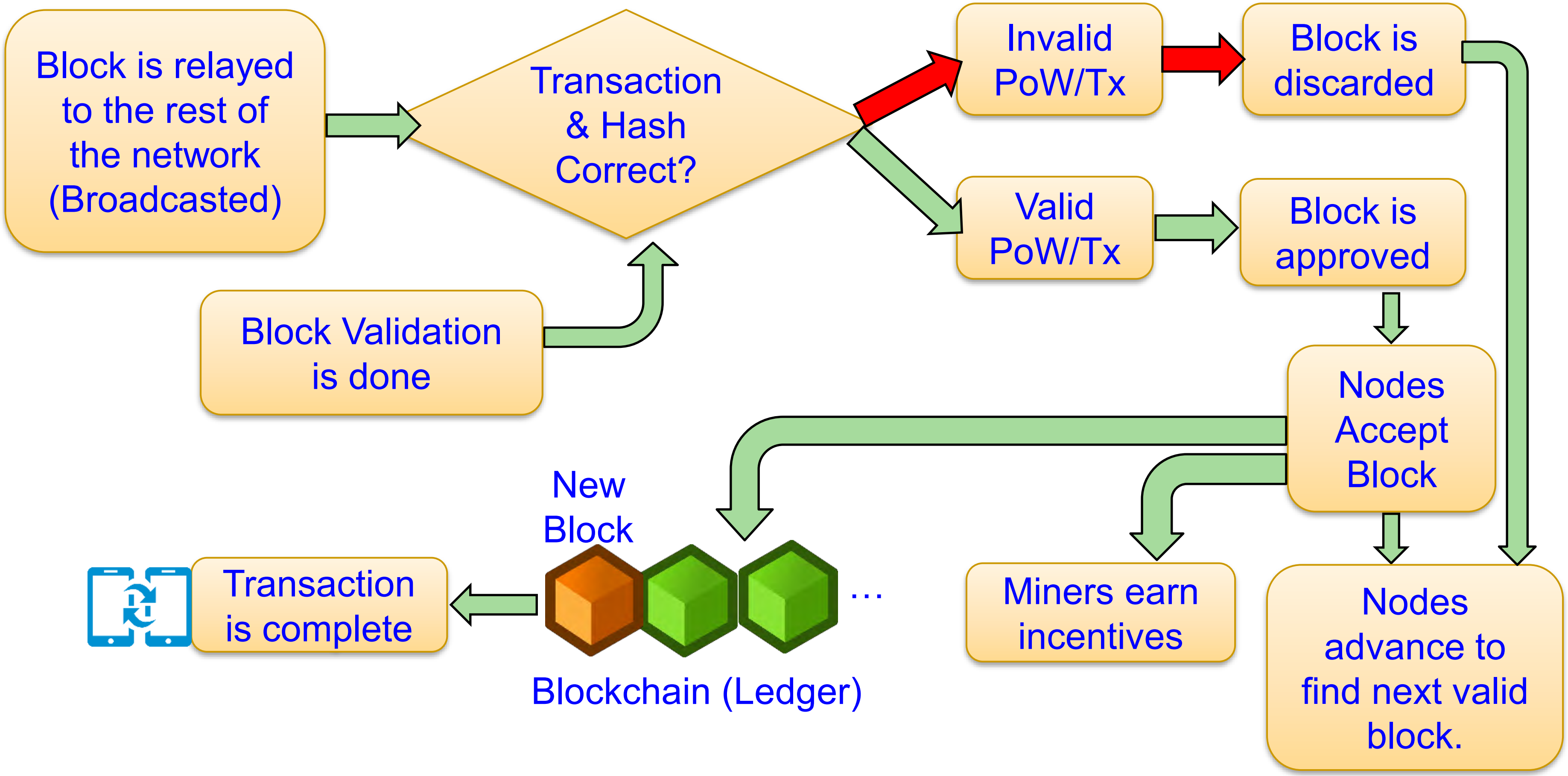
Transaction Verification

- General nodes are not required to store all the transactions
- Only block headers are stored
- To verify a transaction
  - Get the latest longest chain
  - Obtain the Merkle branch linking the transaction to block
  - If the node is accepted and block is created, transaction is verified

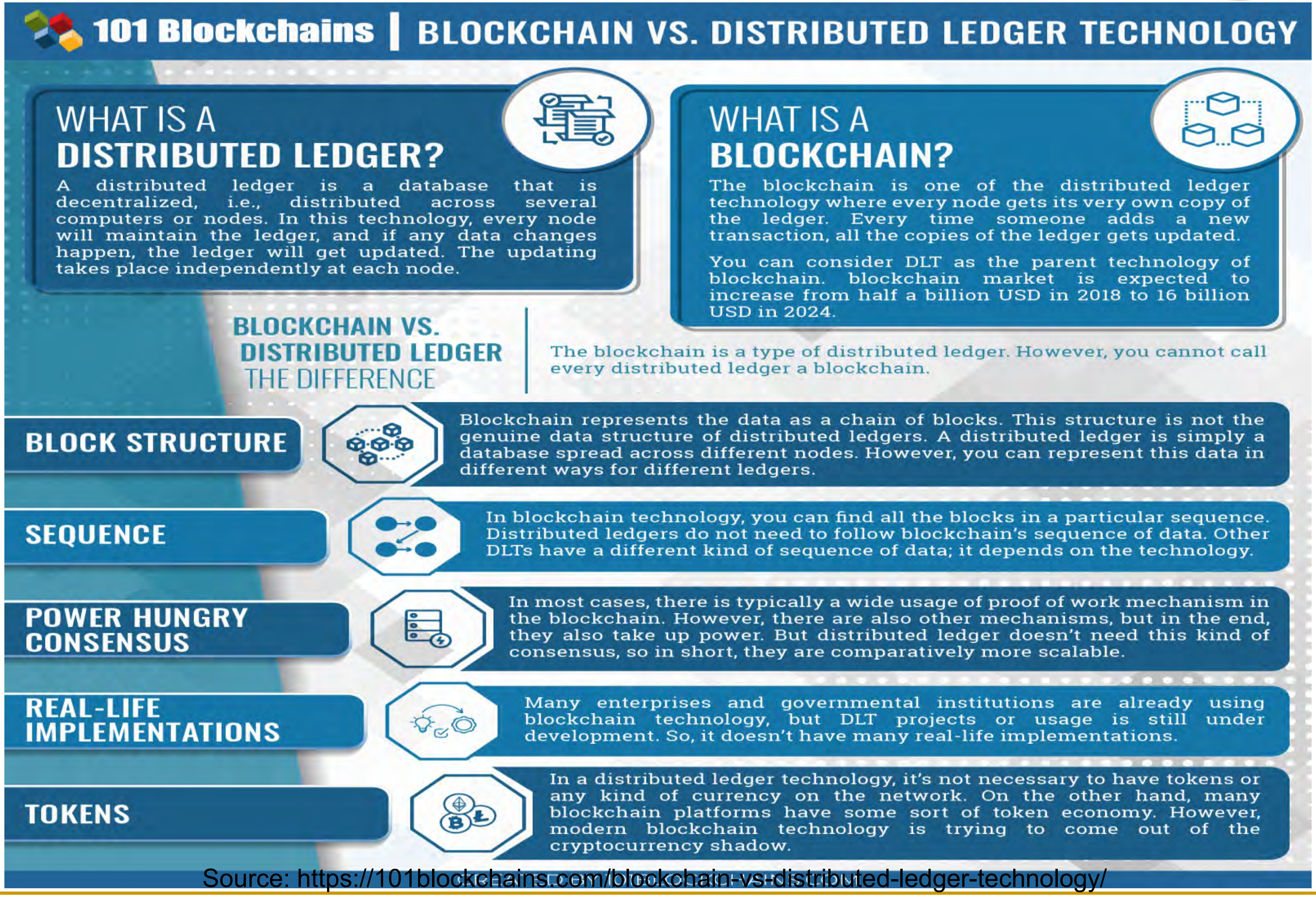
Block Generation



Block Validation



Blockchain vs. Distributed Ledger



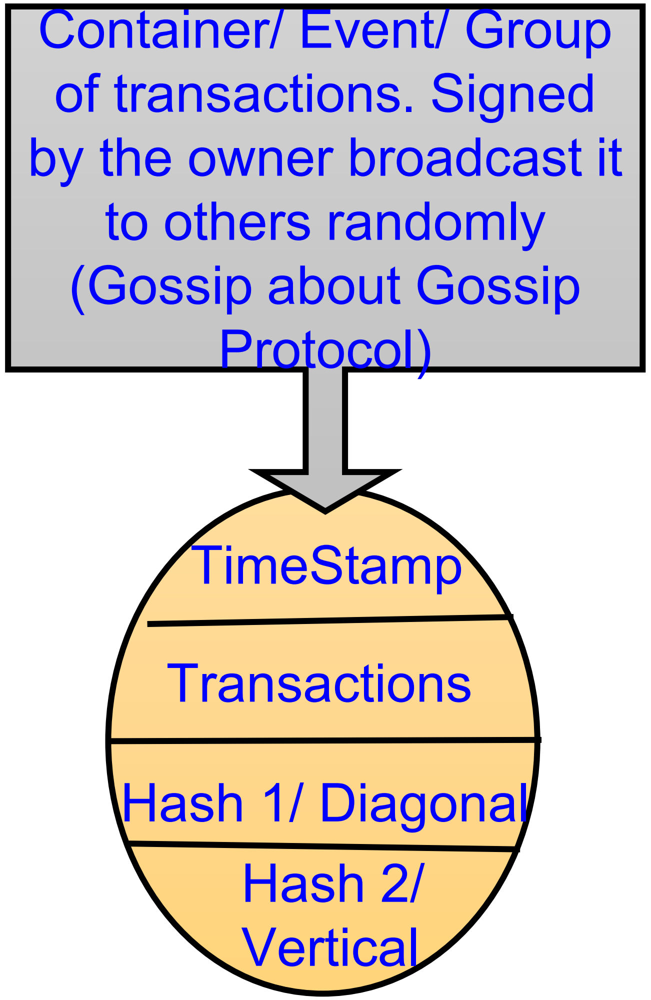
Source: https://101blockchains.com/blockchain-vs-distributed-ledger-technology/

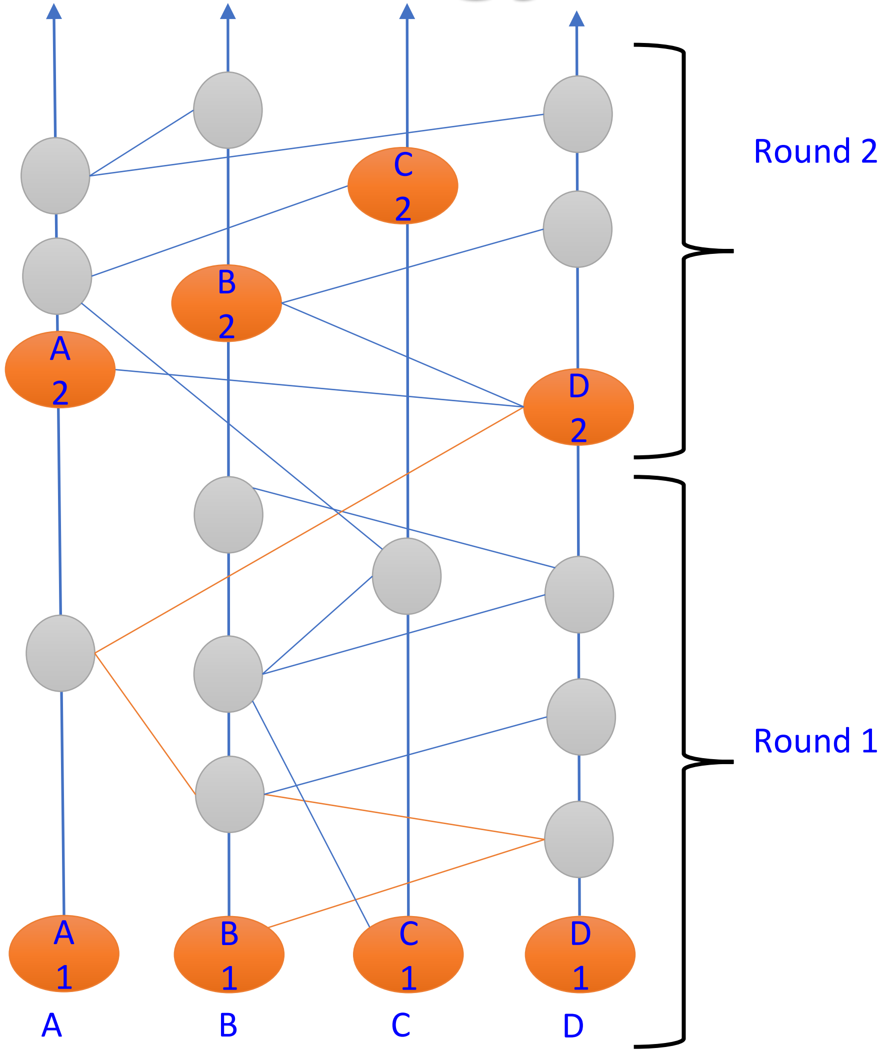
Variants of Distributed Ledger Technologies

- Distributed Ledger Technologies
  - Blockchain
  - DAG
  - DAG-bsed Blockchain
  - Hashgraph
  - Tempo
  - Sidechain
  - Holochain

Source: B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," *IEEE Access*, doi: 10.1109/ACCESS.2021.3065880.

Hashgraph Technology





Tangle Technology

- One disadvantage of blockchain-based cryptocurrencies like bitcoin: The concept of a transaction fee that is levied for all transactions occurring on the network irrespective of the transaction value.
- Transaction costs make the use of blockchain-based cryptocurrency impractical for such small payments.
- Tangle: A directed acyclic graph (DAG) structure stores the transactions occurring on the public ledger. It does not incorporate blockchain technology, thereby attempting to address the issue of transaction costs by using the Tangle storage system.

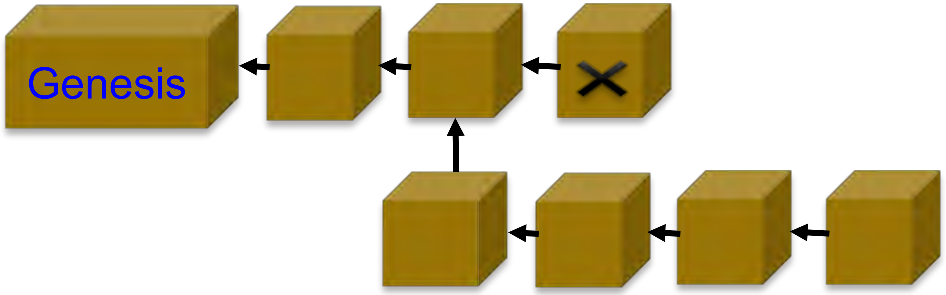
Source: https://www.investopedia.com/terms/t/tangle-cryptocurrency.asp

Tangle Technology

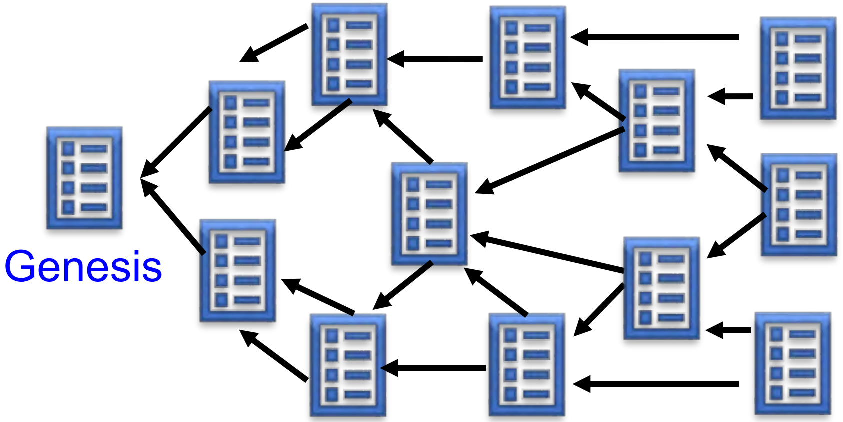
- The working mechanism of Tangle requires a new transaction to approve the previous two transactions.
- Tangle forces a transaction issuing-participant, or node, to contribute towards the agility and security of the network by making him/her approve earlier two pending transactions.
- The nodes also ensure that there are no duplicate transactions leading to double spending, and there are no conflicts among the various transactions as per the Tangle transaction history.

Source: https://www.investopedia.com/terms/t/tangle-cryptocurrency.asp

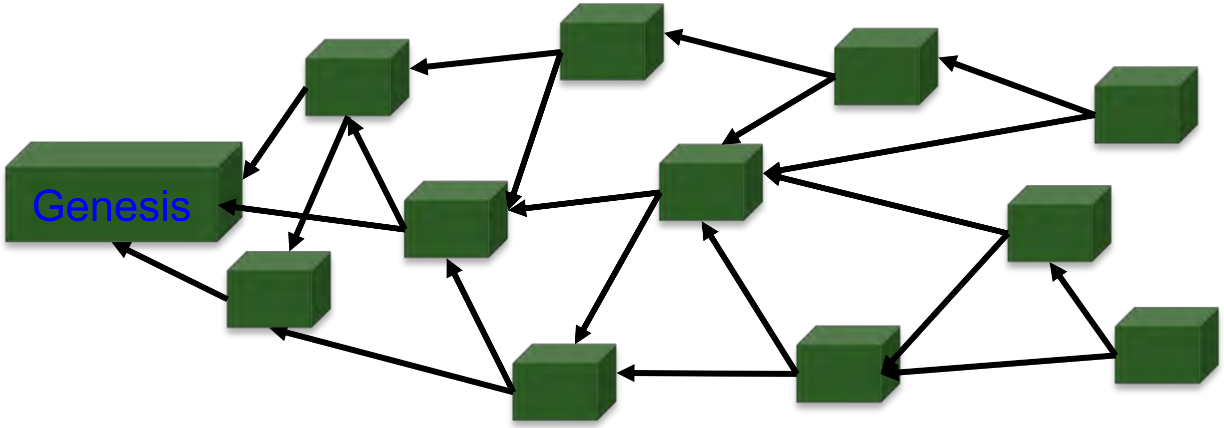
Blockchain Versus Tangle Versus FlexiChain



(a) Blockchain Technology



(b) Tangle Technology



(c) Post-Blockchain Multichain as a Directed Acyclic Graph (DAG)

Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, "McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems", *Proc. 9th IEEE-CS Annual Sympo. on VLSI (ISVLSI)*, 2020, pp. 446--451.

Blockchain Development Tools

1. Geth
2. Mist
3. Solc
4. Remix
5. Testnet
6. GanacheCLI
7. Coinbase
8. EtherScripter
9. BaaS
10. Metamask
11. Ethers.js
12. Tierion
13. Embark
14. Truffle
15. MyEtherWallet

Source: https://blockgeeks.com/guides/15-best-tools-blockchain-development/

Blockchain Platforms

1. Tezos
2. Ethereum
3. Hyperledger Fabric
4. Hyperledger Sawtooth
5. Hedera Hashgraph
6. Ripple
7. Quorum
8. Hyperledger Iroha
9. Corda
10. EOS
11. OpenChain
12. Stellar
13. Dragonchain
14. NEO

Source: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/

Blockchain Platforms

Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum	Hyperledger Sawtooth	EOS	Hyperledger Iroha	OpenChain	Stellar
Industry focus	Cross-Industry	Cross-Industry	Financial Services	Financial Services	Cross-Industry	Cross-Industry	Cross-Industry	Cross-Industry	Digital Asset Management
Ledger Type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned
Consensus Algorithm	Proof of Work	Pluggable Framework	Pluggable Framework	Probabilistic Voting	Majority Voting	Pluggable Framework	Delegated Proof-of-Stake	Chain-based Byzantine Fault Tolerant	Partionned Consensus
Smart Contract	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Governance	Ethereum Developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum Developers and JP Morgan Chase	Linux Foundation	EOSIO Core Arbitration Forum(ECAF)	Linux Foundation	CoinPrism

Source: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/

Blockchain - Application Specific Hardware

- It is a hardware assistance to speed up the transactions process and increase the network throughput.
- The accelerator could be built using an FPGA, GPU, or ASIC processors.
- These acceleration hardware could be targeting one aspect of the blockchain or contribute in the whole network.
  - For example, an ASIC could be programmed to accelerate the trust process among nodes with lowest time and power consumption.
  - Also, increases the mining process with lowest power consumption.
- Devices in market:
- BITMAIN company has many versions of hardware mining accelerators for Blockchain applications.
- KRAMBU company provides different models of accelerators using FPGA, GPU, and ASIC.

Hardware wallets

Image source: https://www.buybitcoinworldwide.com/wallets/ledger-nano-s/

Research Publishing – Best Practices

Publishing Venue – Where to Publish?

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

    OR

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

Publishing Venue – Where to Publish?

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

Publishing Venue - Magazine

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

Conference → Journal?

- Conference publishing first → corresponding journal
  OR

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

Conference → Journal: How to Do it?

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

General question on academic publishing

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

Focused discussion topics/questions

- How important is social media for researchers? Should Ph.D. students invest time in building profiles & networks social media?
  - Neutral – Publicity + Typical Negativity of social media (Privacy issues)
- How challenging do you feel it is for new Ph.D. researchers to get published? Any advice/tips?
  - Reasonable challenging for new researchers, Conference → Journals
- What are your thoughts on open-access?
  - Open access is better, but I think expensive to authors

What are the Best Practices of Publishing?

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

How important is author ordering in a publication?

- There is no fixed answer.
- In some disciplines the faculty mentor is typically the last author.
- In some cases, the primary contributor is the first author and other is made based on level of contributions to the work.

How Important It is to be a Reviewer?

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

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.