Security by Design for IoT-Enabled Systems

Keynote – International Conference on Security, Privacy and Data Analytics (ISPDA-2021)

13-15 December 2021

Saraju P. Mohanty

University of North Texas, USA.

Email: saraju.mohanty@unt.edu Website: http://www.smohanty.org

The Big Picture

Issues Challenging City Sustainability

Pollution

Water Crisis

Energy Crisis

Traffic

Smart City Technology - As a Solution

- Smart Cities: For effective management of limited resource to serve largest possible population to improve:
  - ❑ Livability
  - ❑ Workability
  - ❑ Sustainability

At Different Levels:
- ➢ Smart Village
- ➢ Smart State
- ➢ Smart Country

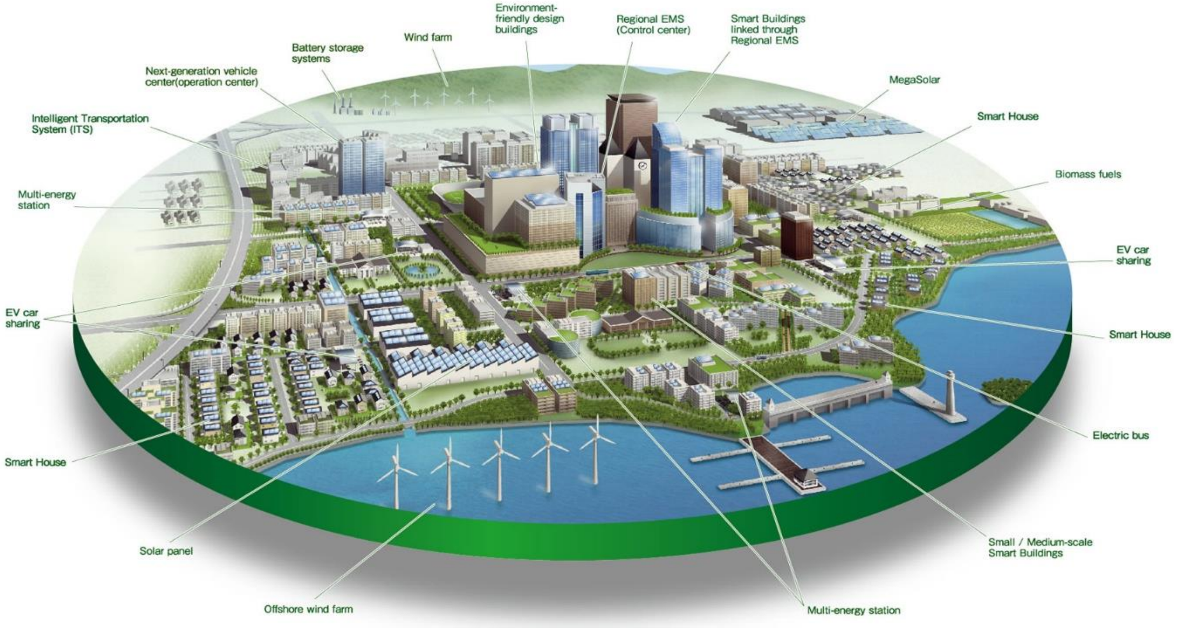
A GUIDE TO THE CE INNERVERSE
IEEE Consumer Electronics MAGAZINE
VOL. 5, NO. 3, July 2016
City Smarts
Devices, Infrastructure, and People In an Urban Environment
SMART CITY
IEEE

July 2016

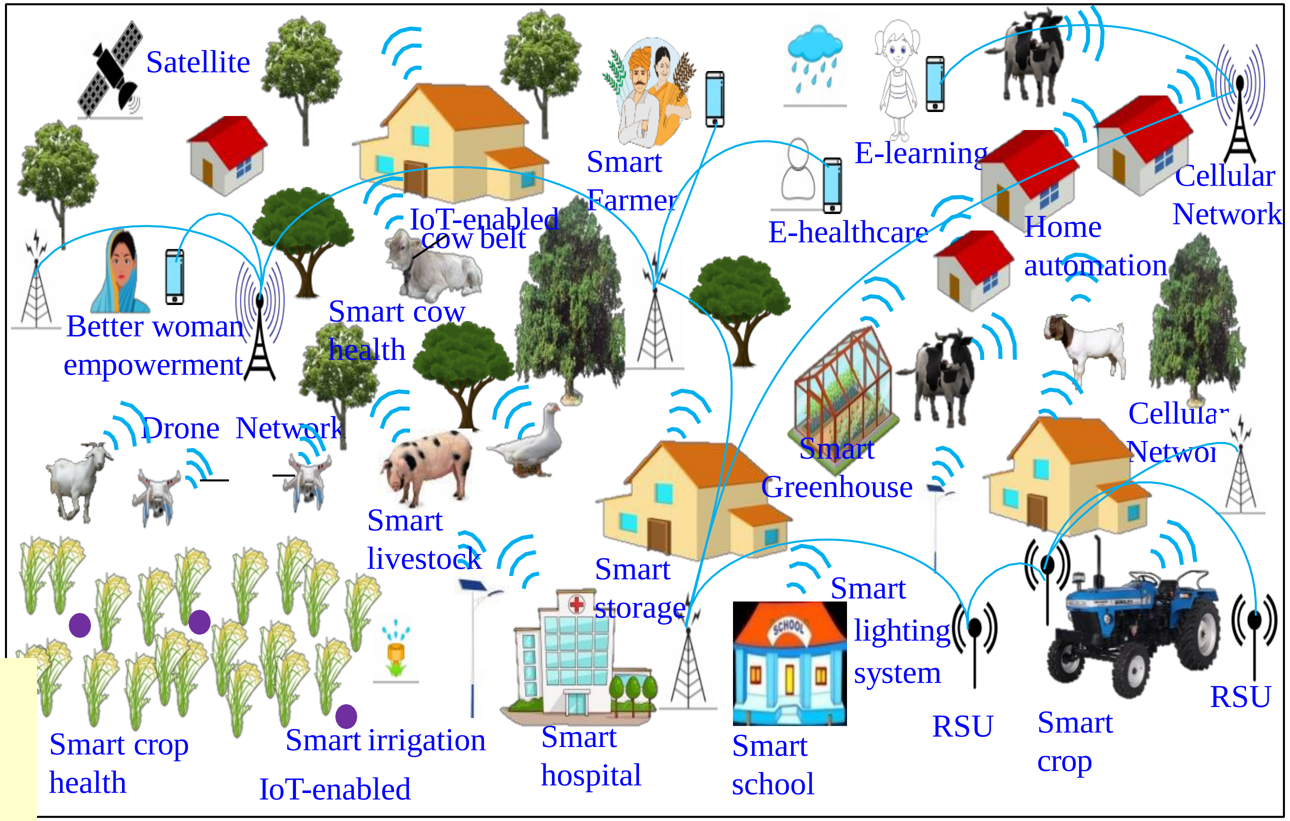
➢ Year 2050: 70% of world population will be urban

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

Smart Cities Vs Smart Villages


Environment-friendly design buildings
Regional EMS (Control center)
Smart Buildings linked through Regional EMS
Wind farm
Battery storage systems
Next-generation vehicle center(operation center)
MegaSolar
Intelligent Transportation System (ITS)
Smart House
Multi-energy station
Biomass fuels
EV car sharing
EV car sharing
Smart House
Electric bus
Smart House
Solar panel
Small / Medium-scale Smart Buildings
Offshore wind farm
Multi-energy station

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



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

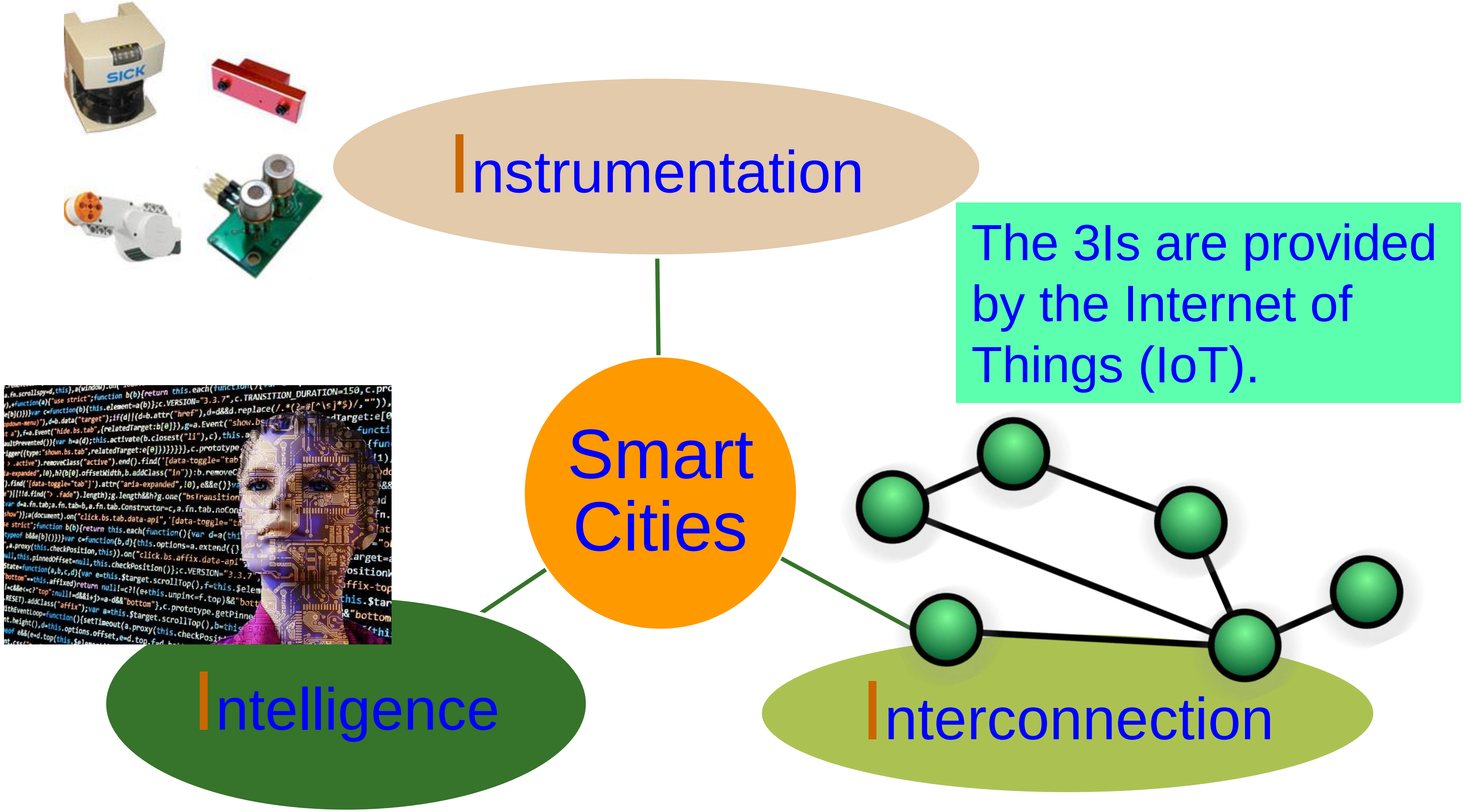
Smart Cities

CPS Types - More
Design Cost - High
Operation Cost – High
Energy Requirement - High

Smart Villages

CPS Types - Less
Design Cost - Low
Operation Cost – Low
Energy Requirement - Low

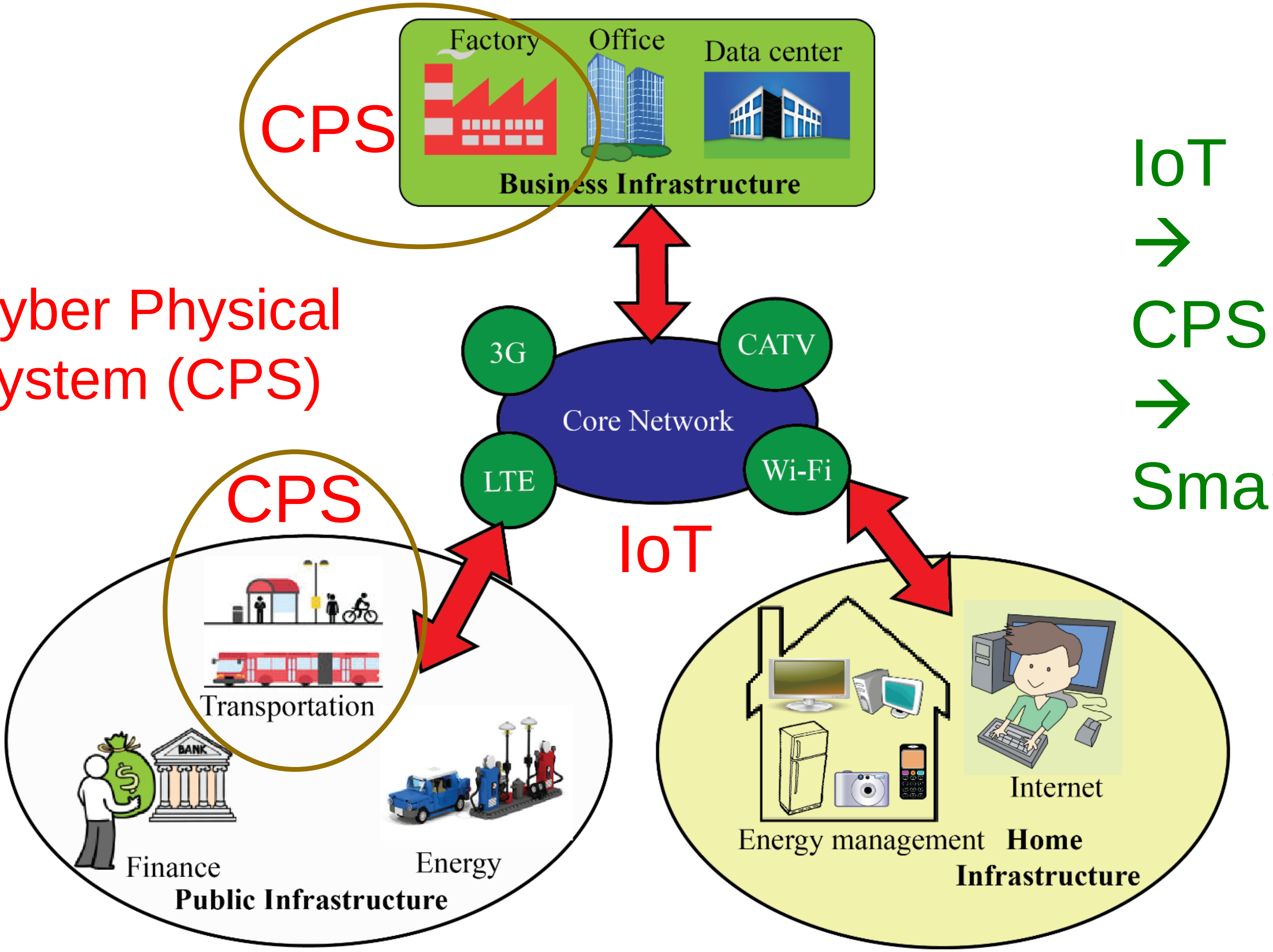
Smart Cities or Smart Villages - 3 Is



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

Source: Mohanty ISC2 2019 Keynote

IoT → CPS → Smart Cities or Smart Villages



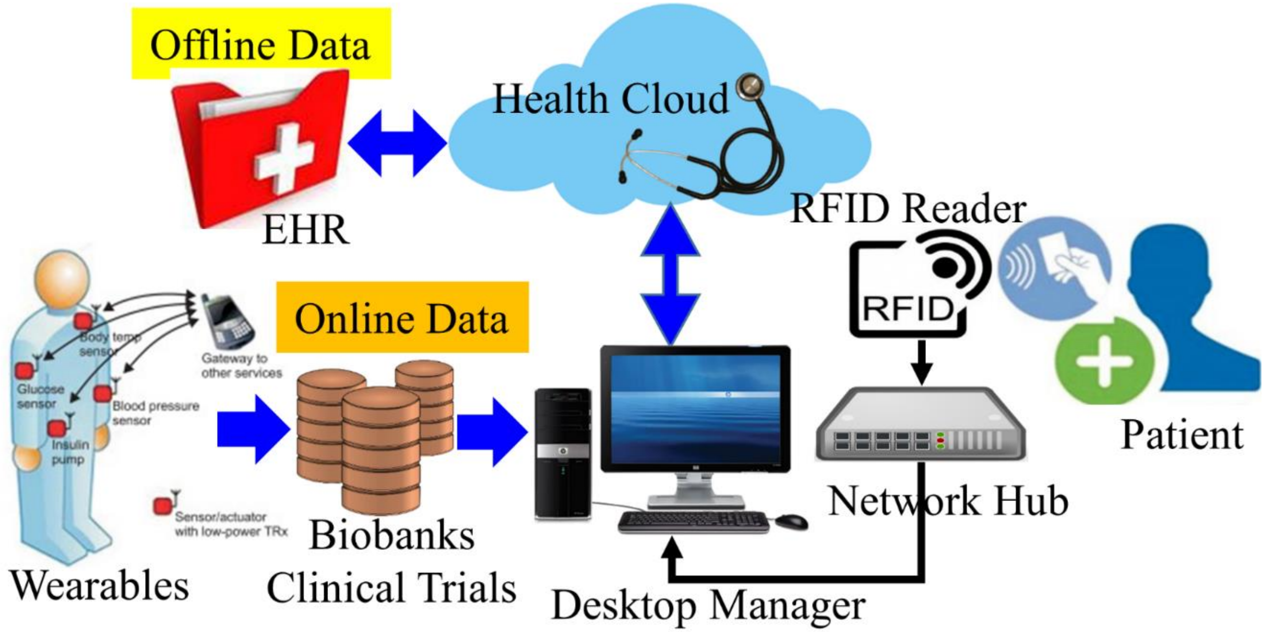
Cyber Physical System (CPS)

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

IoT is the backbone

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

Healthcare Cyber-Physical System (H-CPS)



Internet-of-Medical-Things (IoMT)

OR

Internet-of-Health-Things (IoHT)

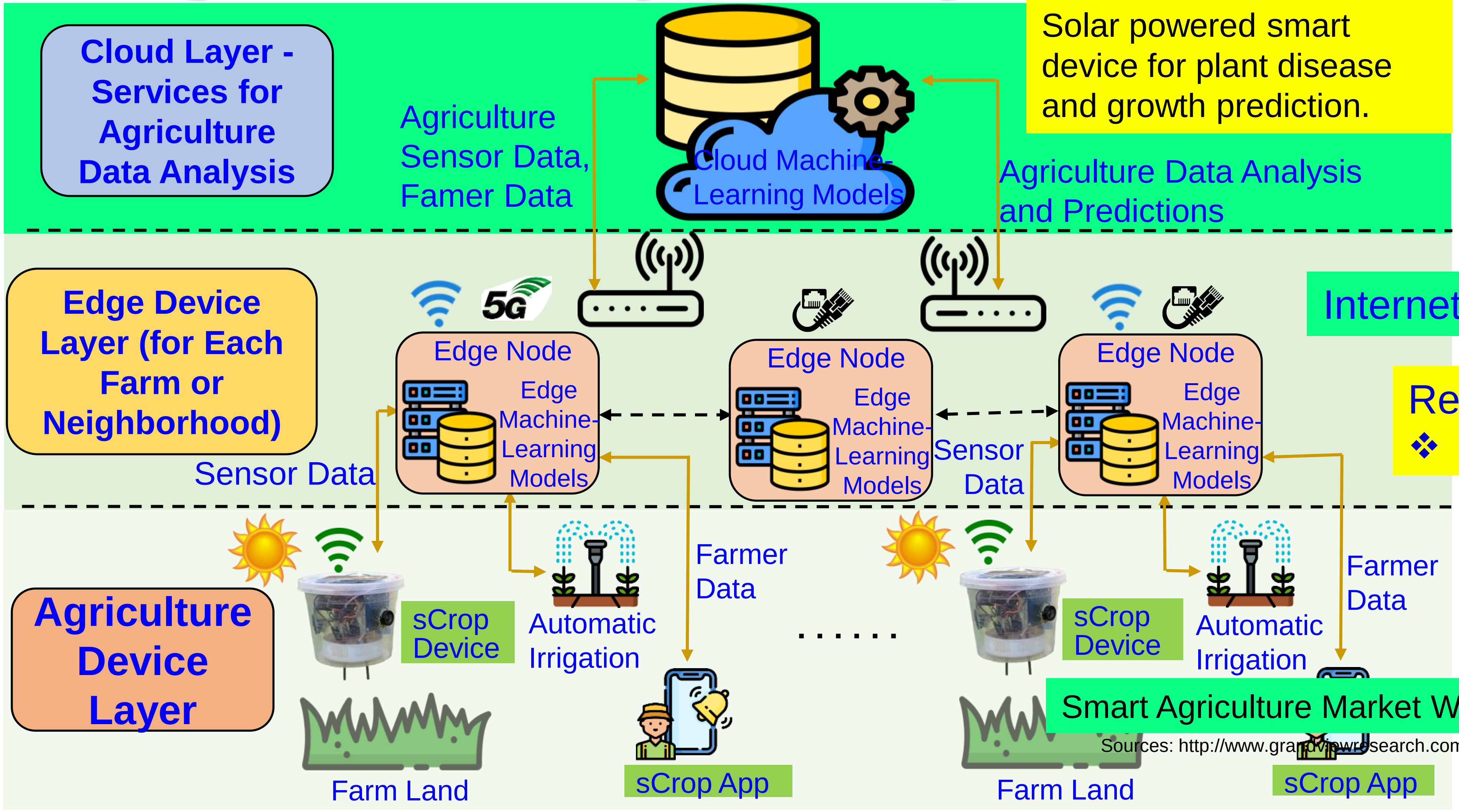
H-CPS ← Biosensors + Medical Devices + Wearable Medical Devices (WMDs) + Implantable Medical Devices (IMDs) + Internet + Healthcare database + AI/ML + Applications that connected through Internet.

Requires:

- ❖ Data and Device Security
- ❖ Data Privacy

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

Agriculture Cyber-Physical System (A-CPS)



Cloud Layer - Services for Agriculture Data Analysis
Agriculture Sensor Data, Famer Data
Cloud Machine-Learning Models
Agriculture Data Analysis and Predictions
5G
Edge Device Layer (for Each Farm or Neighborhood)
Edge Node
Edge Machine-Learning Models
Edge Node
Edge Machine-Learning Models
Edge Node
Edge Machine-Learning Models
Sensor Data
Sensor Data
Agriculture Device Layer
sCrop Device
Automatic Irrigation
Farmer Data
sCrop App
Farm Land
....
sCrop Device
Automatic Irrigation
Farmer Data
sCrop App
Farm Land

Solar powered smart device for plant disease and growth prediction.

Internet-of-Agro-Things (IoAT)

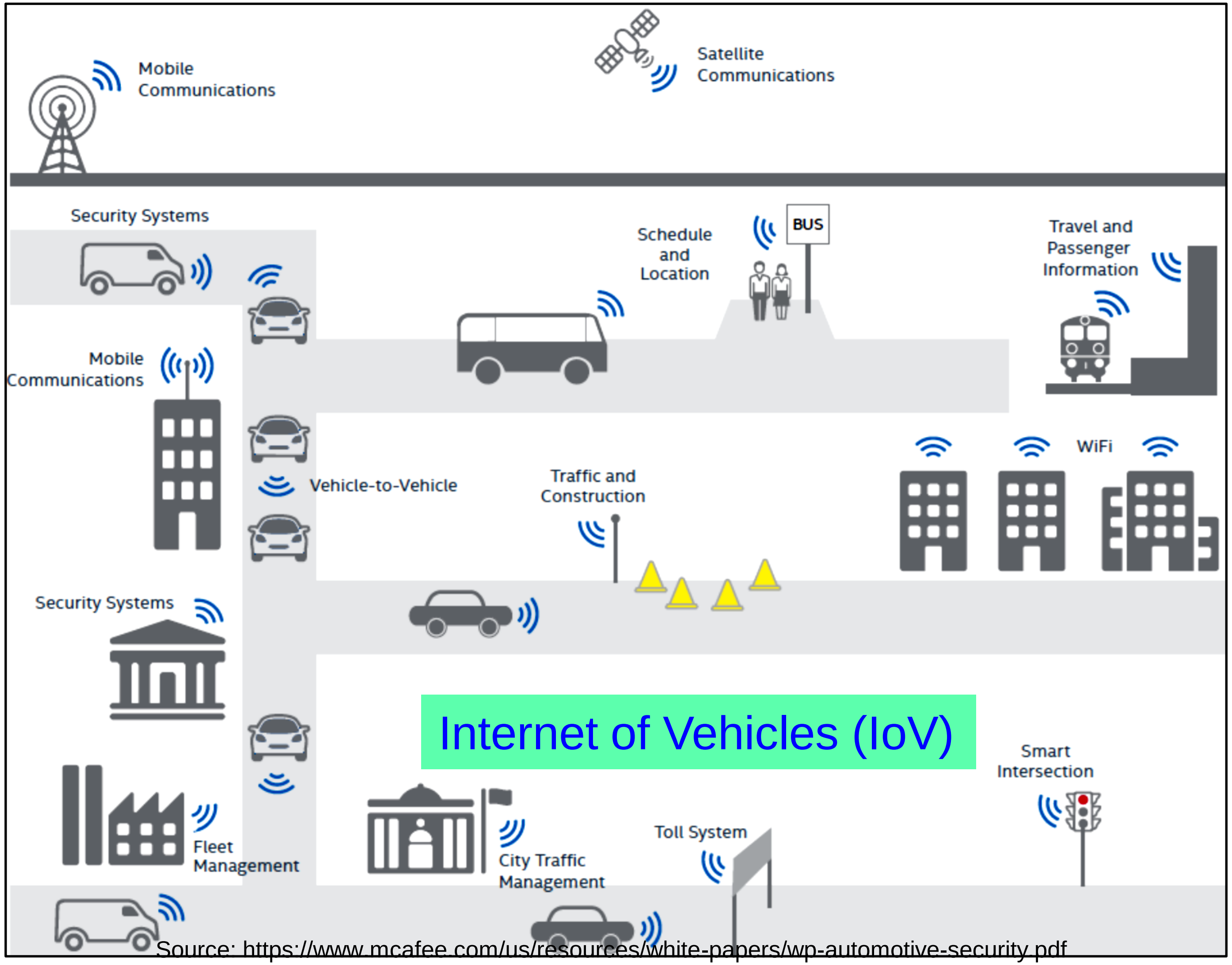
Requires:
❖ Data and System Security

Smart Agriculture Market Worth US$18.21 Billion By 2025.

Sources: http://www.grandviewresearch.com/press-release/global-smart-agriculture-farming-market

Source: V. Udutalapally, S. P. Mohanty, V. Pallagani, and V. Khandelwal, “sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture”, *IEEE Sensors Journal*, Vol. 21, No. 16, August 2021, pp. 17525--17538, DOI: 10.1109/JSEN.2020.3032438.

Transportation Cyber-Physical System (T-CPS)



Internet of Vehicles (IoV)

Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

IoT Role Includes:

- Traffic management
- Real-time vehicle tracking
- Vehicle-to-Vehicle communication
- Scheduling of train, aircraft
- Automatic payment/ticket system
- Automatic toll collection

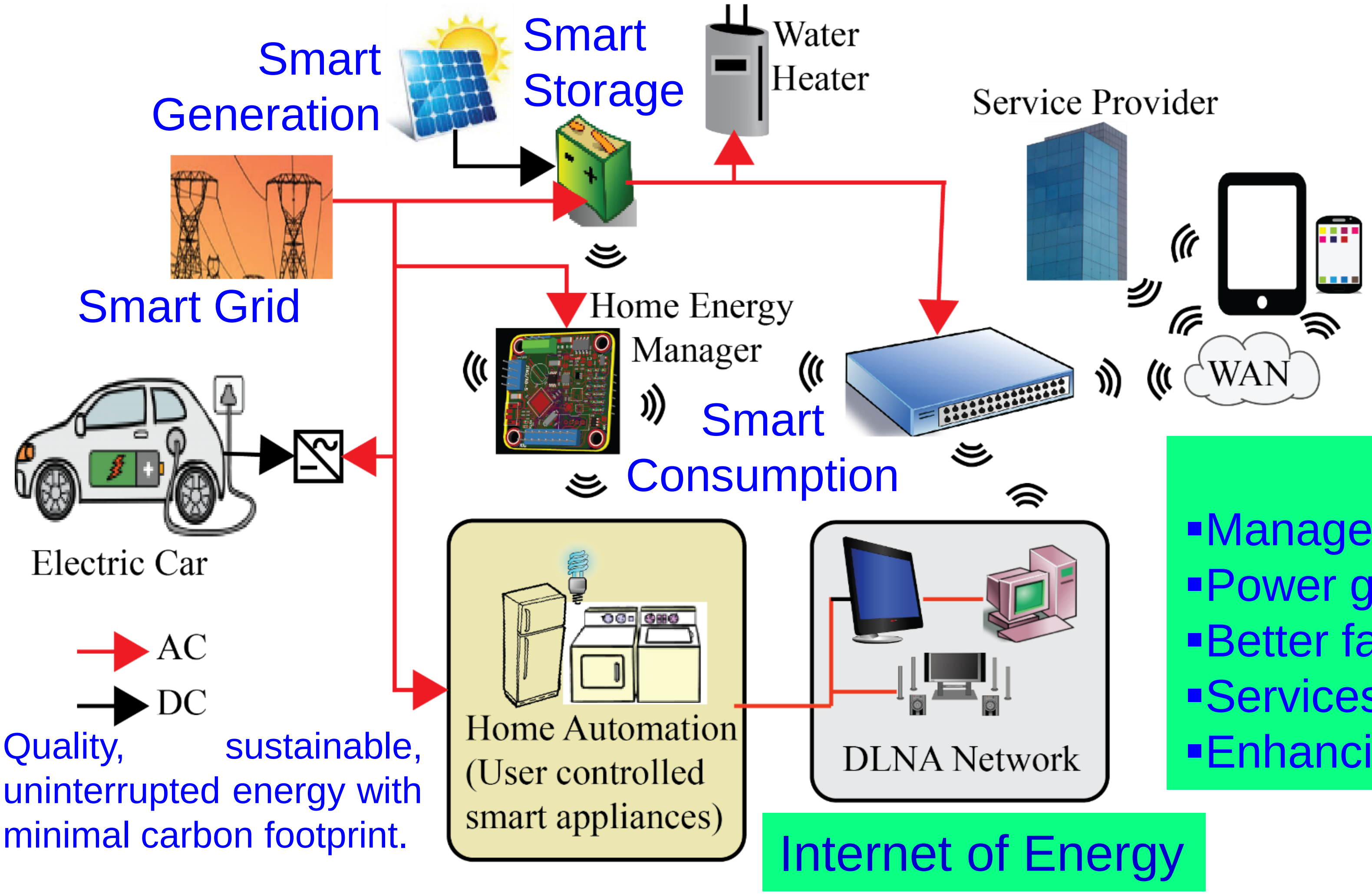
Requires:

- ❖ Data, Device, and System Security
- ❖ Location Privacy

"The global market of IoT based connected cars is expected to reach $46 Billion by 2020."

Source: Datta 2017, CE Magazine Oct 2017

Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Internet of Energy

Requires:

- ❖ Data, Device, and System Security

IoT Role:

- ▪Management of energy usage
- ▪Power generation dispatch for solar, wind, etc.
- ▪Better fault-tolerance of the grid
- ▪Services for plug-in electric vehicles (PEV)
- ▪Enhancing consumer relationships

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

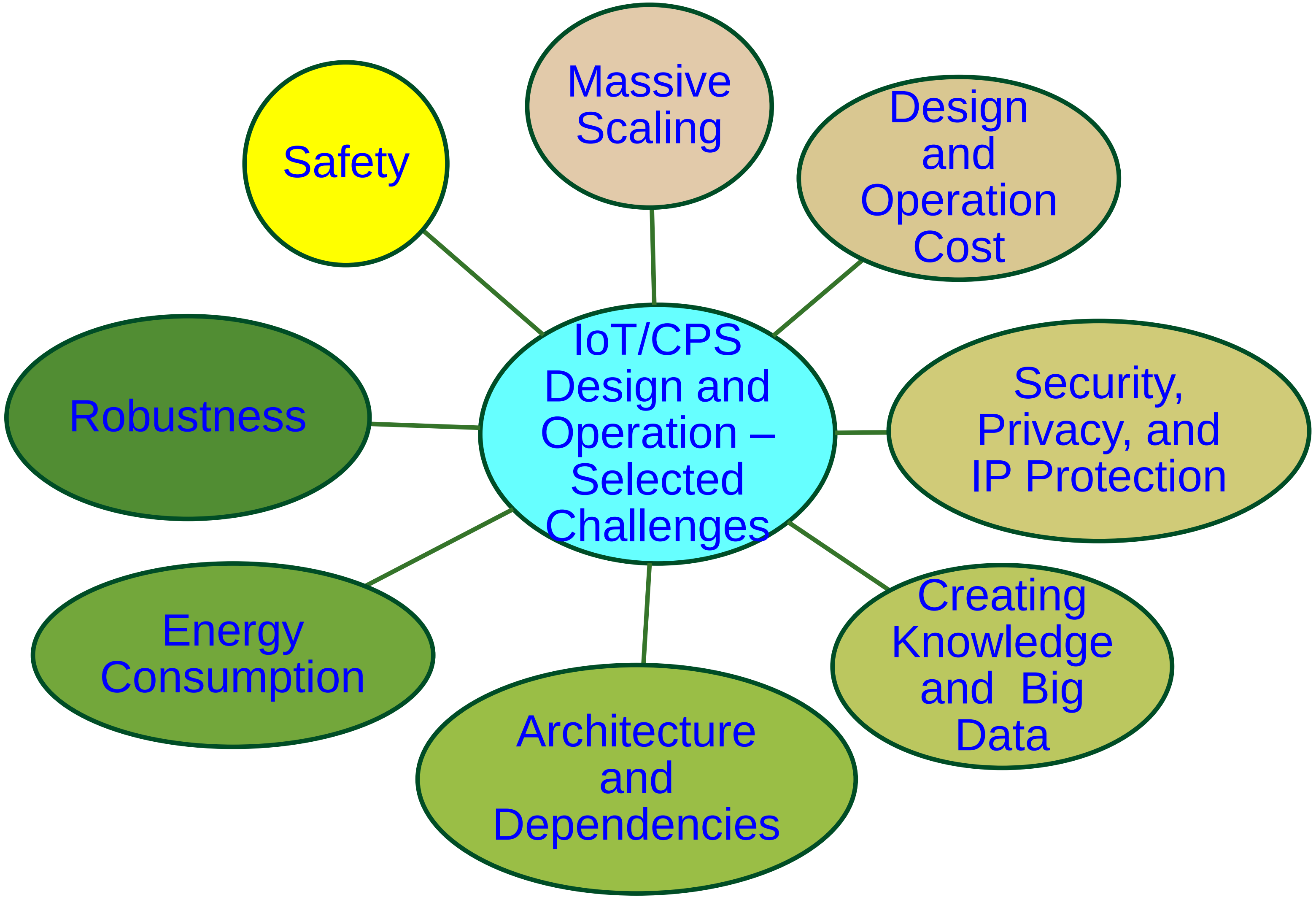
Services in Smart Cities and Smart Village

In Smart Cities	In Smart Village	Communication Type	Energy Source	Feasibility
Waste Management	Waste Management	WiFi, Sigfox, Neul, LoRaWAN	Battery Powered and Energy Harvesting	Feasible but smart containers adds in cost
Air Quality Monitoring	Smart Weather and Irrigation	BLE, ZigBee, 6LoWPAN, WiFi, Cellular, Sigfox, LoRaWAN	Solar Panels, Battery Power and Energy Harvesting	Feasible
Smart Surveillance	NA	BLE, WiFi, ZigBee, Cellular, Sigfox, LoRaWAN	Battery Power and Energy Harvesting	Feasible but additional sensors needed
Smart Energy	Smart Energy	ZigBee, Z-Wave, 6LoWPAN, Sigfox, LoRaWAN	PowerGrid, Solar Power, Wind Power, Energy Harvesting	Feasible
Smart Lighting	Smart Lighting	WiFi, ZigBee, Z-Wave, Sigfox, LoRaWAN	Power Grid, Solar Power, Energy Harvesting	Feasible
Smart Healthcare	Smart Healthcare	BLE, Bluetooth, WiFi, Cellular, Sigfox	Power Grid, Battery Power, and Energy Harvesting	Feasible
Smart Education	Smart Education	LR-WPAN, WiFi and Ethernet	Power Grid, Battery Power, and Energy Harvesting	Feasible
Smart Parking	NA	Z-Wave, WiFi, Cellular, Sigfox, LoRaWAN	Power Grid, Solar Power, Energy Harvesting	Feasible
Structural Health Monitoring	NA	BLE, WiFi, ZigBee, 6LoW-PAN, Sigfox	Power Grid, Solar Power, Battery Power, Energy Harvesting	Energy harvesting can be useful for power specs
Noise Monitoring	NA	6LoWPAN, WiFi, Cellular	Battery Power, Energy Harvesting, and Energy Scavenging	Sound pattern identification is a bottleneck
NA	Smart Farming	BLE, Bluetooth, WiFi, 6LoW-PAN, Sigfox, LoRaWAN	Power Grid, Battery Power and Energy Harvesting	Feasible
NA	Smart Diary	Bluetooth, WiFi, ZigBee, 6LoWPAN, LoRaWAN	Power Grid, Battery Power and Energy Harvesting	Feasible

Source: S. K. Ram, B. B. Das, K. K. Mahapatra, S. P. Mohanty, and U. Choppali, “Energy Perspectives in IoT Driven Smart Villages and Smart Cities”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 19-28, DOI: 10.1109/MCE.2020.3023293.

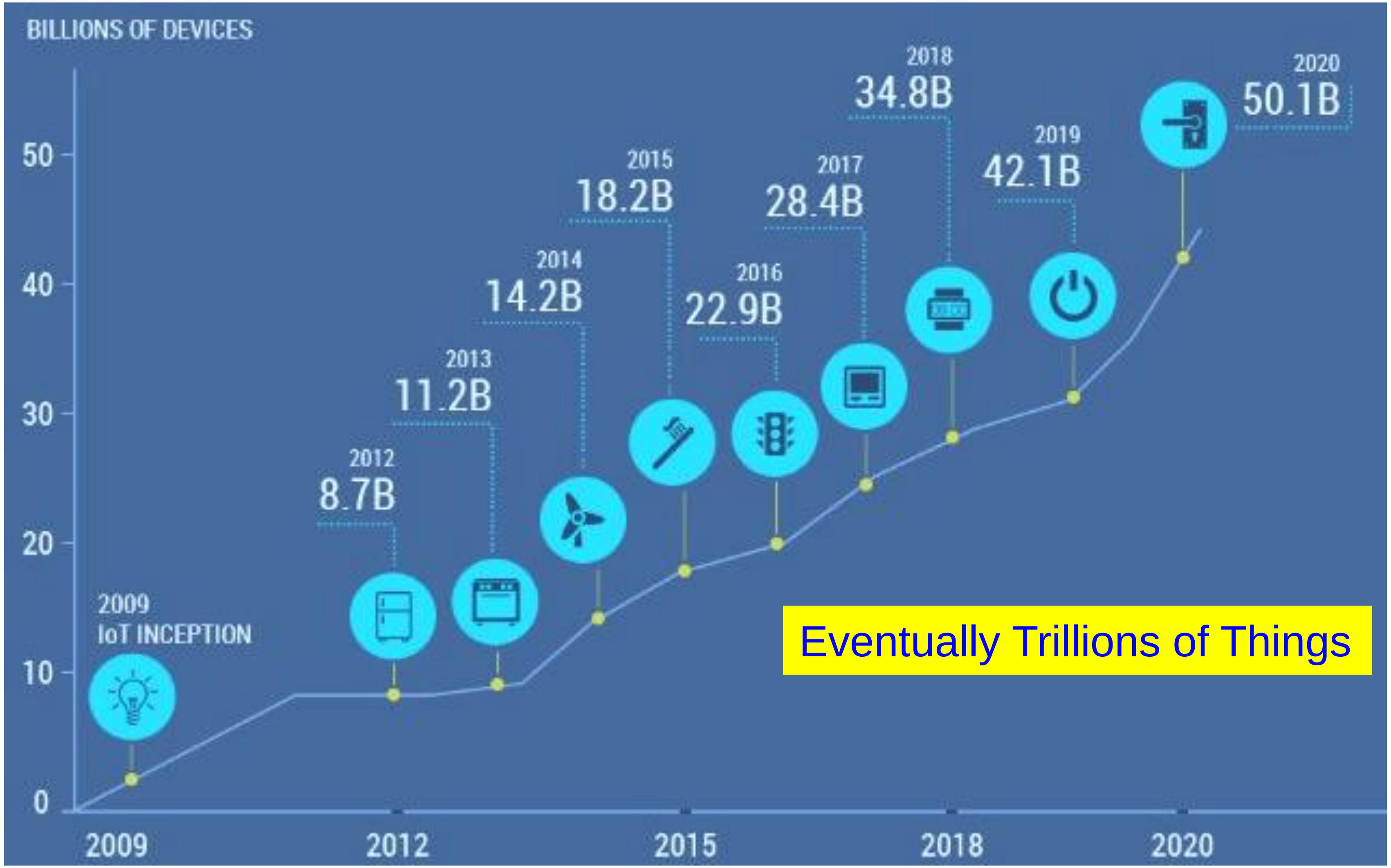
Challenges in IoT/CPS Design

IoT/CPS – Selected Challenges


Safety
Massive Scaling
Design and Operation Cost
Robustness
IoT/CPS Design and Operation – Selected Challenges
Security, Privacy, and IP Protection
Energy Consumption
Architecture and Dependencies
Creating Knowledge and Big Data

Source: Mohanty ICIT 2017 Keynote

Massive Growth of Sensors/Things

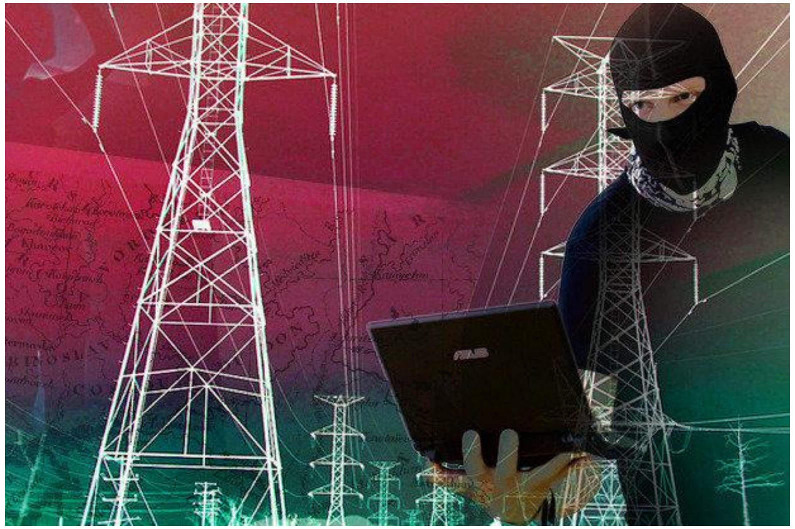


Eventually Trillions of Things

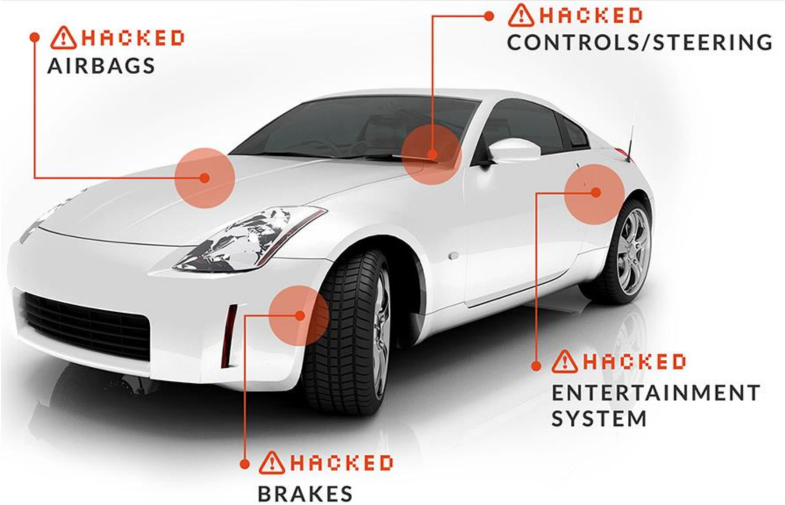
Source: https://www.linkedin.com/pulse/history-iot-industrial-internet-sensors-data-lakes-0-downtime

Cybersecurity Challenges - System

Power Grid Attack



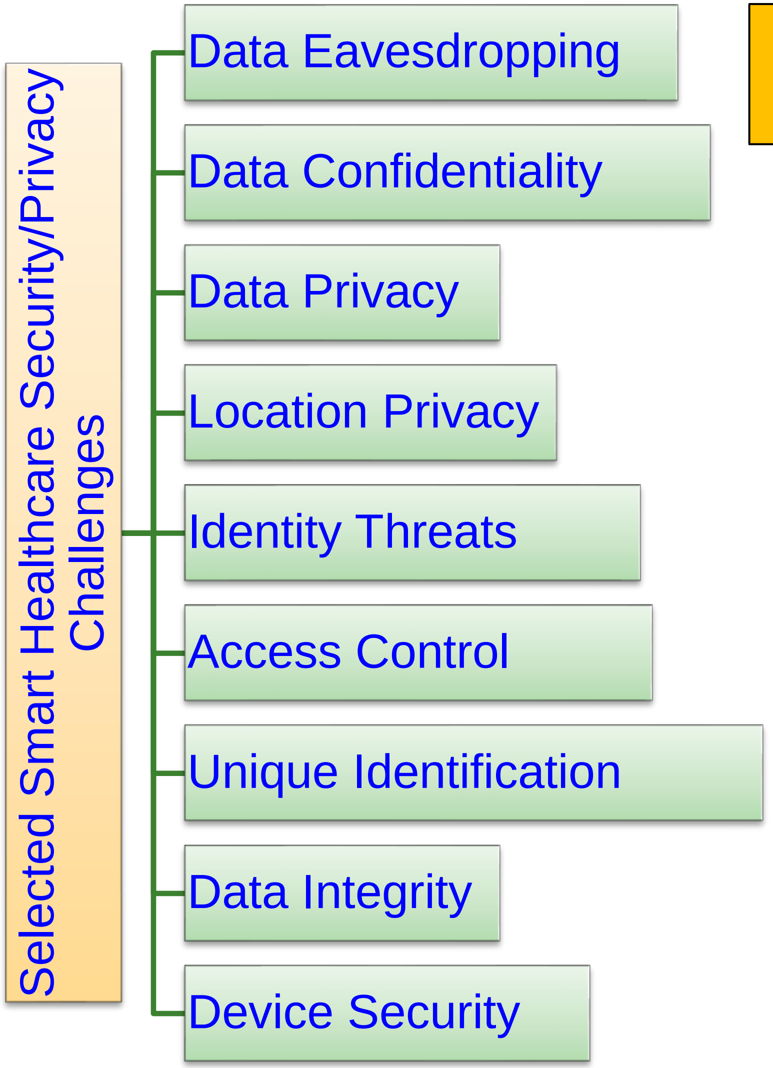
Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html



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

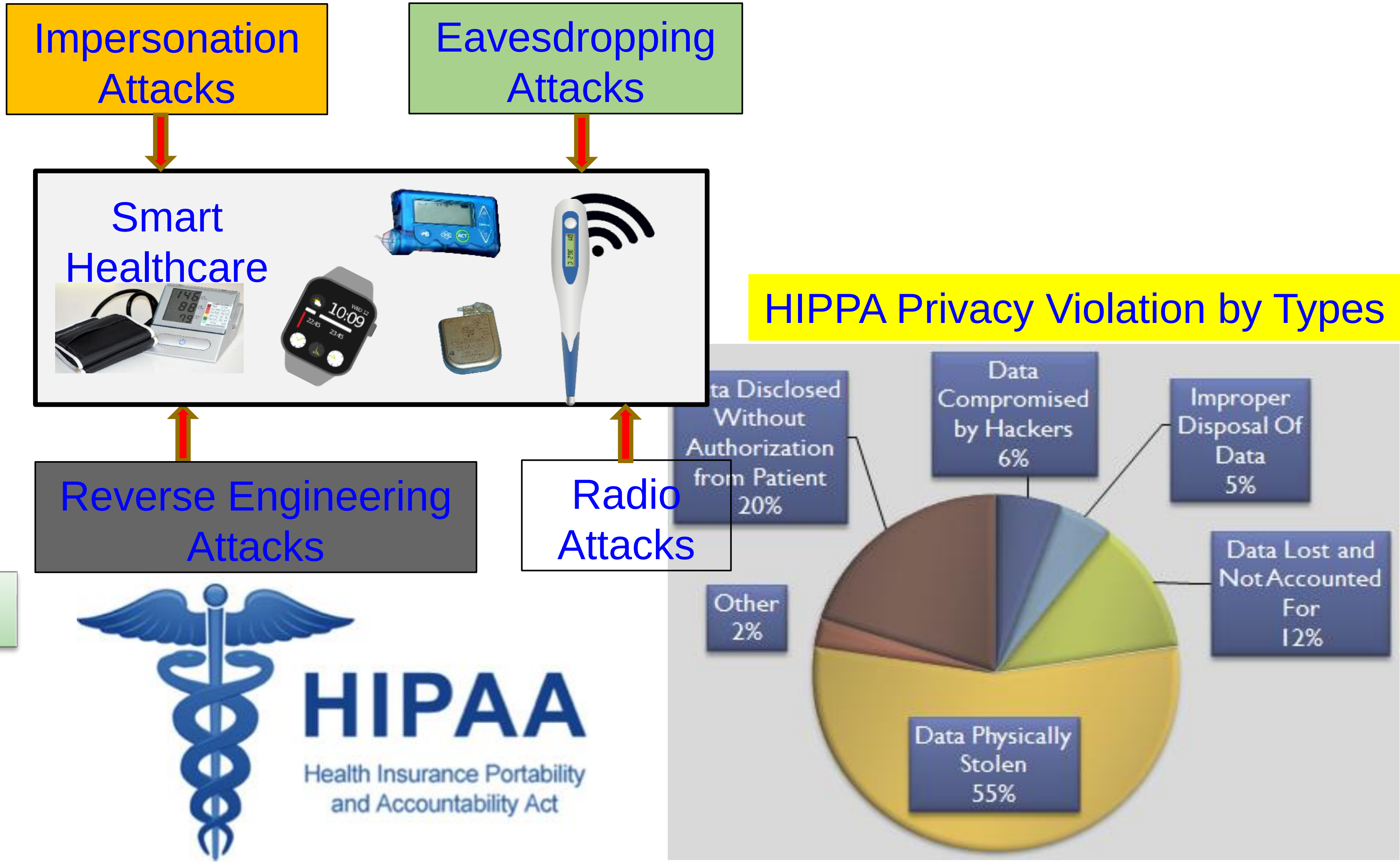
Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Smart Healthcare - Cybersecurity and Privacy Issue



Selected Smart Healthcare Security/Privacy Challenges

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



Impersonation Attacks

Eavesdropping Attacks

Smart Healthcare

Reverse Engineering Attacks

Radio Attacks

HIPAA

Health Insurance Portability and Accountability Act

HIPPA Privacy Violation by Types

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:

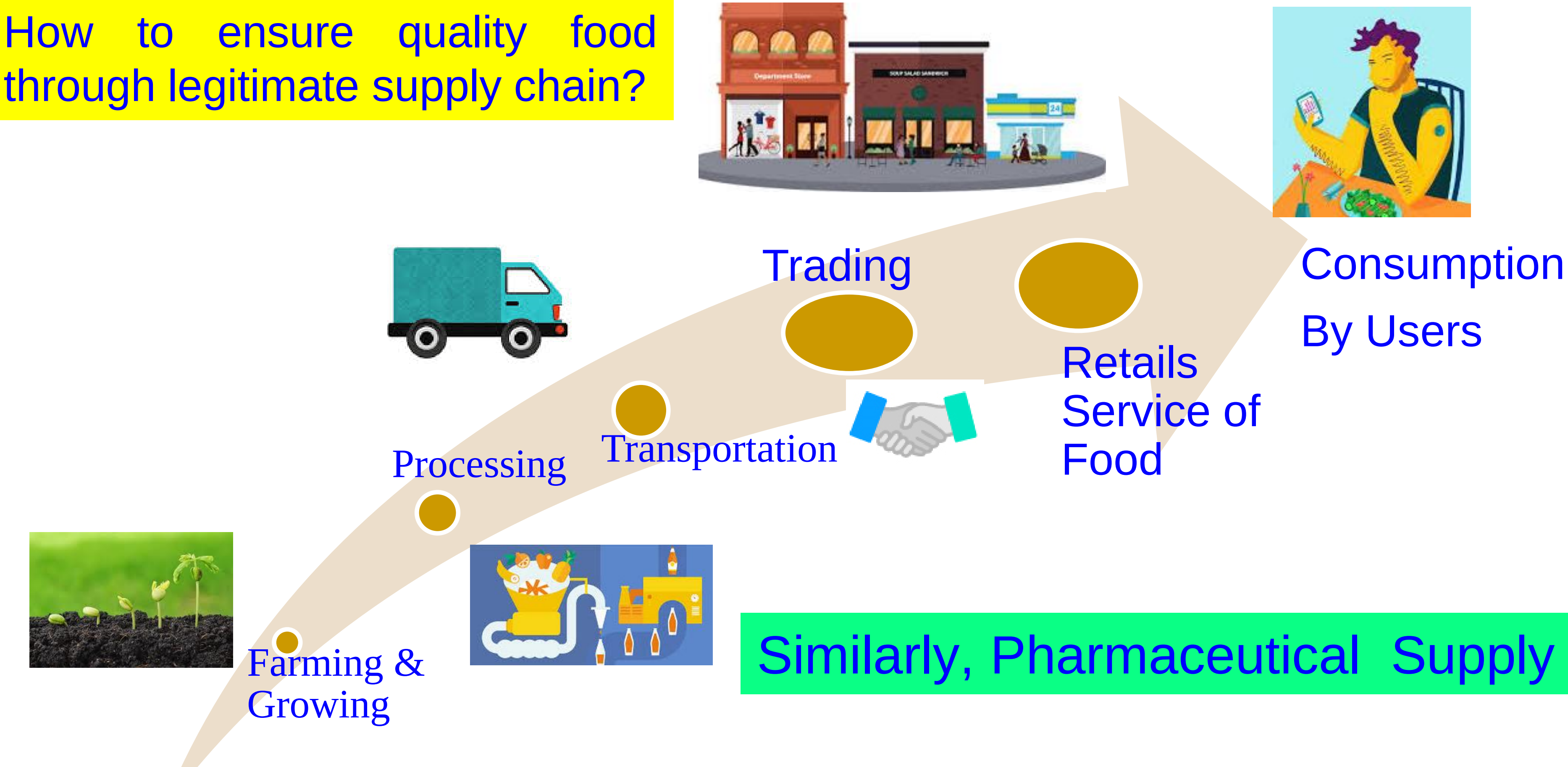
https://www.cnn.com/2019/10/02/health/fda-medical-devices-hackers-trnd/index.html

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

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

Reliable Supply Chain: Food Supply Chain: Farm → Dinning

How to ensure quality food through legitimate supply chain?

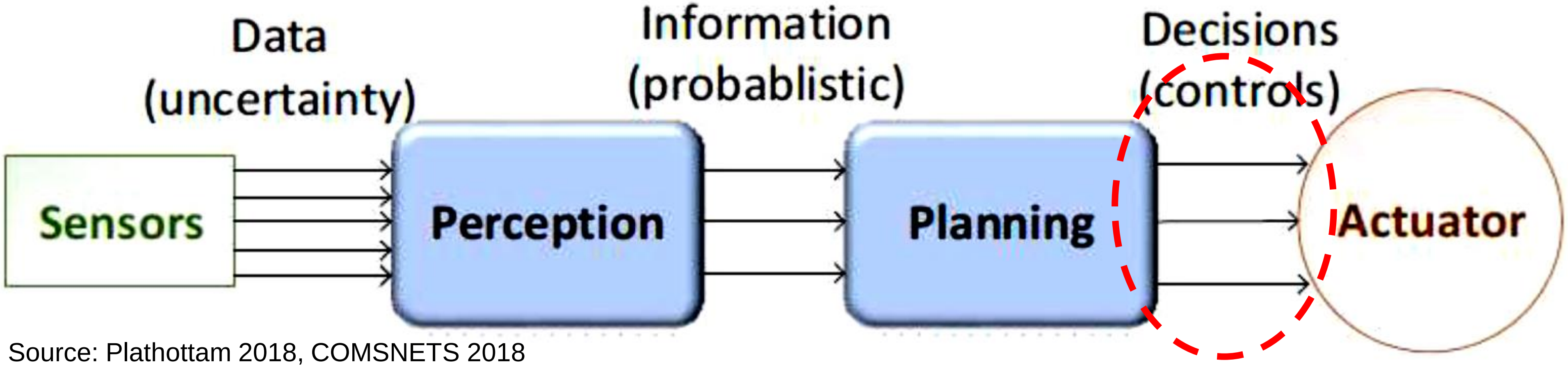


Similarly, Pharmaceutical Supply Chain

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.

Smart Car – Modification of Input Signal of Control Can be Dangerous

- ➢Typically vehicles are controlled by human drivers
- ➢Designing an Autonomous Vehicle (AV) requires decision chains.
- ➢AV actuators controlled by algorithms.
- ➢Decision chain involves sensor data, perception, planning and actuation.
- ➢Perception transforms sensory data to useful information.
- ➢Planning involves decision making.



Source: Plathottam 2018, COMSNETS 2018

Smart Grid Attacks can be Catastrophic

Threats	Vulnerabilities
Security group knowledge	Management deficiencies of network access rules Inaccurate critical assests documentation
Information leakage	Unencrypted services in IT Weak protection credentials
Access point	Improper access point Remote access deficiency Firewall filtering deficiency
Unpatched System	Unpatched operating system Unpatched third party application
Weak cyber security	Buffer overflow in control system services SQL injection vulnerability

Source of Threats

- Phishers
- Nation
- Hacker
- Insider
- Terrorist
- Spammers
- Spyware / Malware authors

Attacks

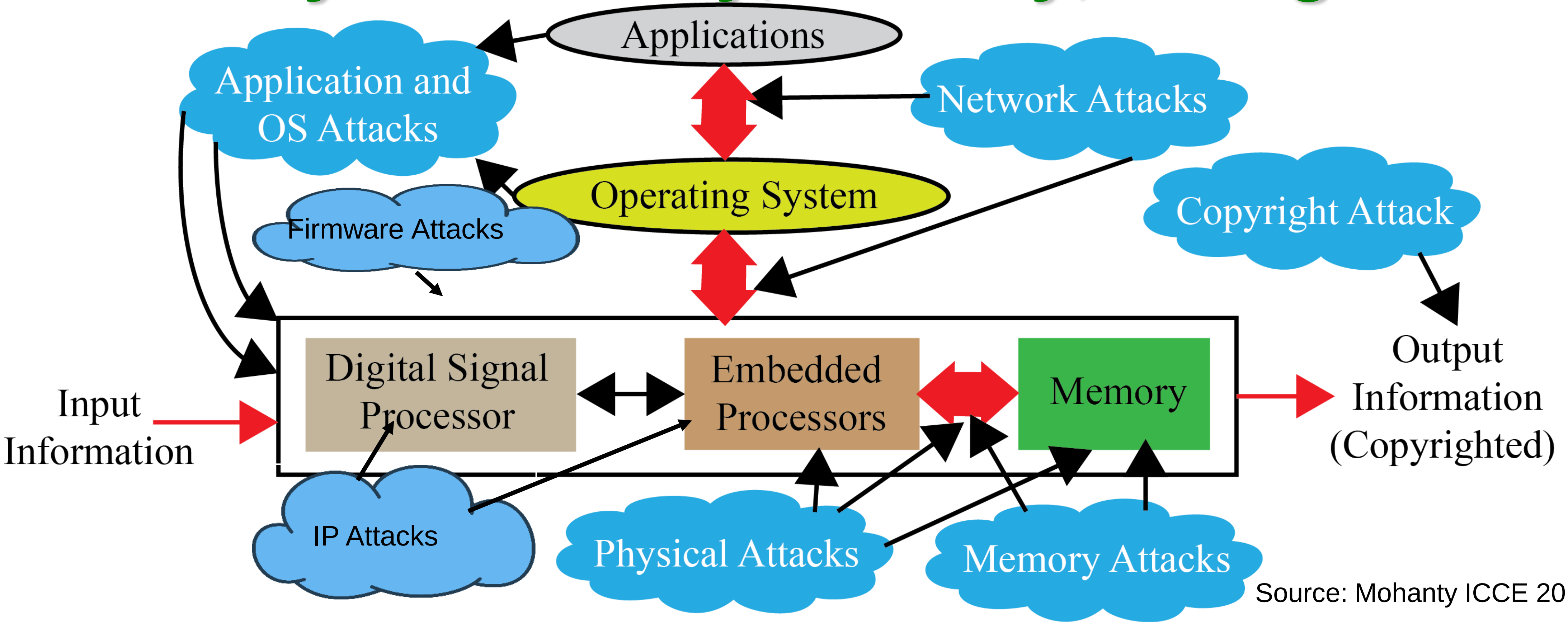
- Stuxnet
- Night Dragon
- Virus
- Denial of service
- Trojan horse
- Worm
- Zero day exploit
- Logical bomb
- Phishing
- Distributed DoS
- False data Injection

Impacts

- Ukraine power attack, 2015
- Stuxnet attack in Iran, 2010
- Browns Ferry plant, Alabama 2006
- Emergency shut down of Hatch Nuclear Power Plant, 2008
- Slammer attack at Davis-Besse power plant, 2001
- Attacks at South Korea NPP, 2015

Source: R. K. Kaur, L. K. Singh and B. Pandey, "Security Analysis of Smart Grids: Successes and Challenges," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 10-15, Mar 2019.

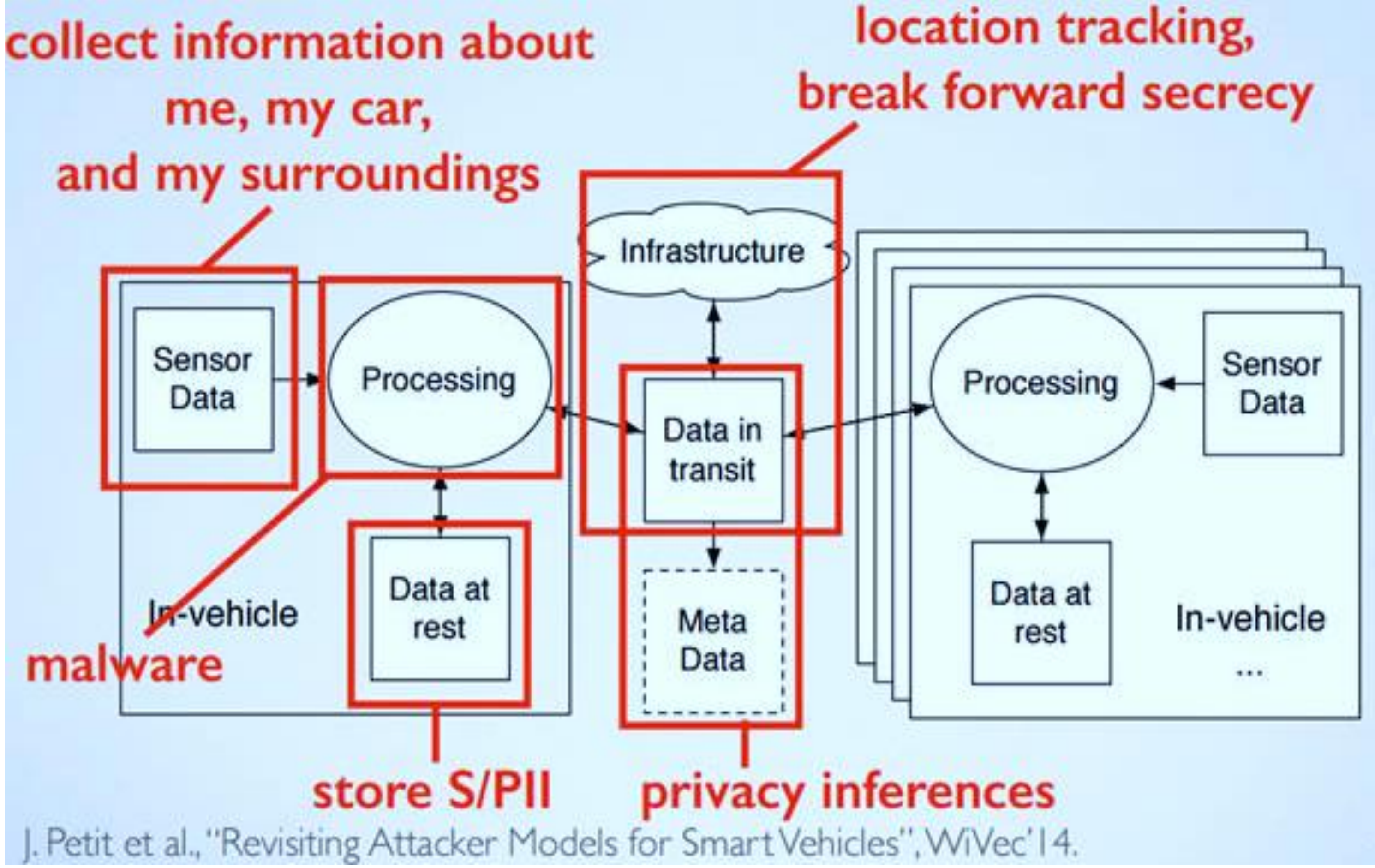
Selected Attacks on an Electronic Device – Cybersecurity, Privacy, IP Rights

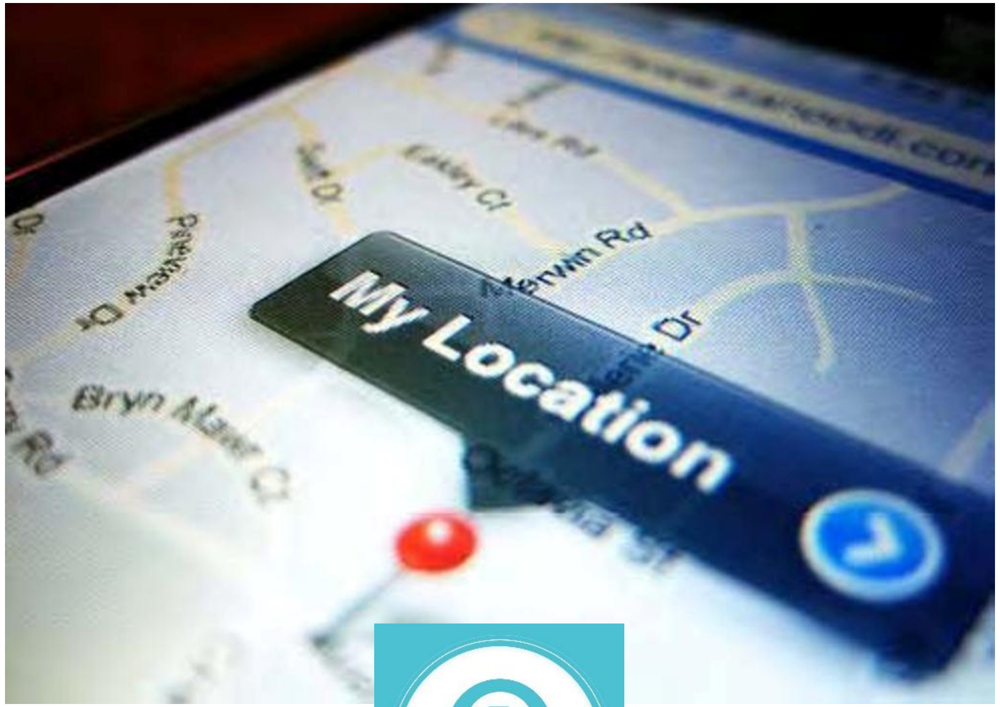


Source: Mohanty ICCE 2018 Keynote

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

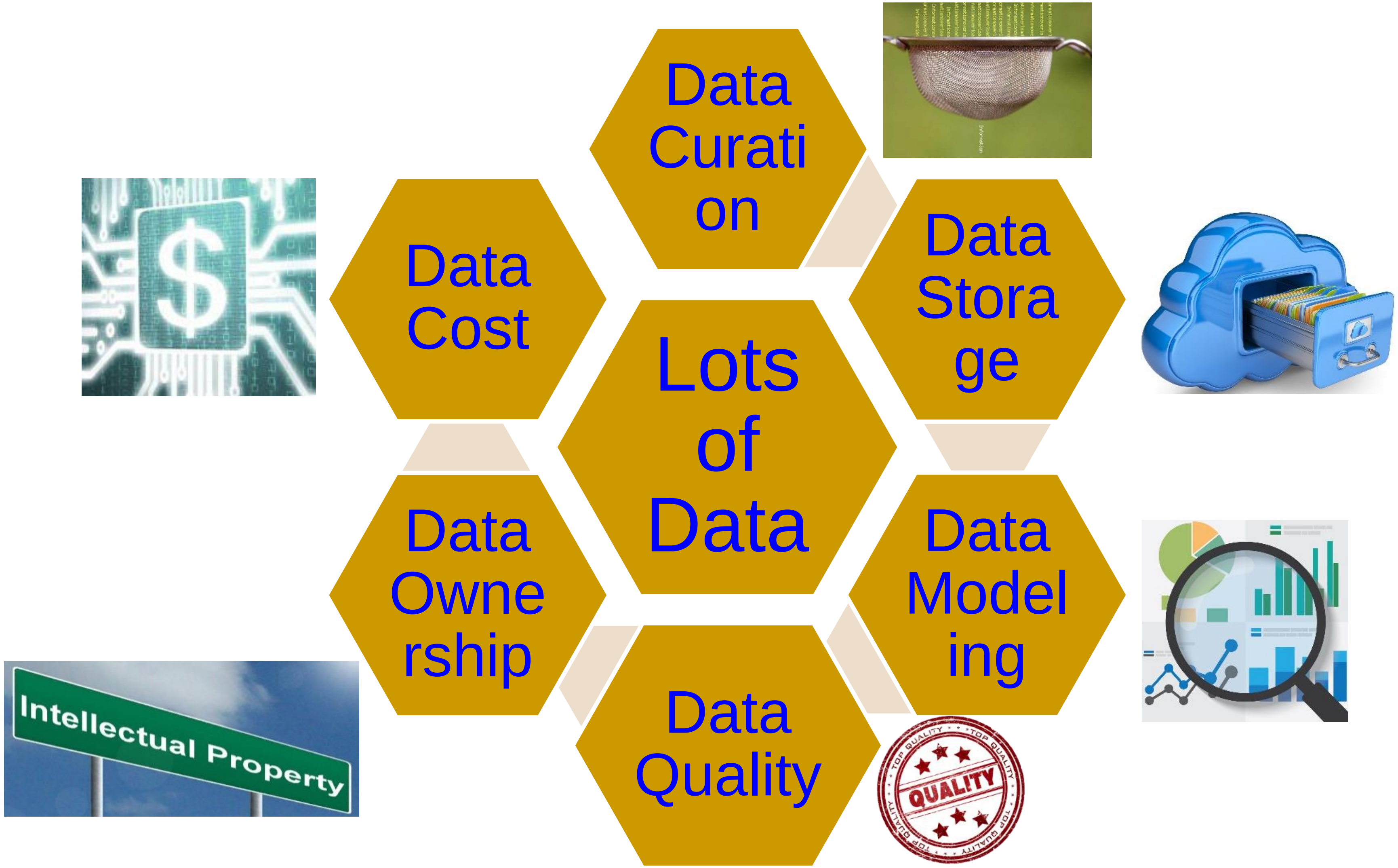
Privacy Challenge – System, Location





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

Challenges of Data in IoT/CPS are Multifold



Lots of Data

Data Curation

Data Storage

Data Modeling

Data Quality

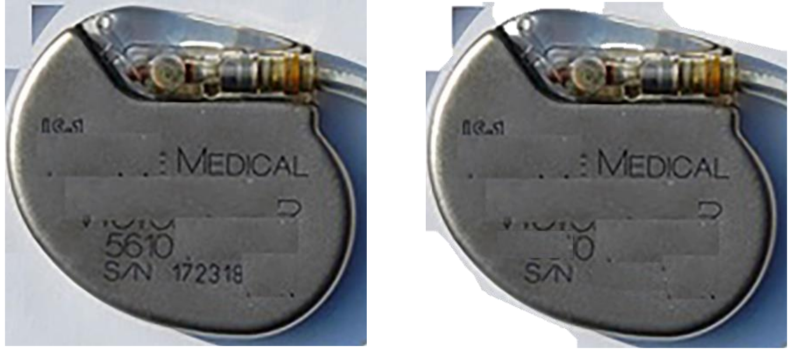
Data Ownership

Data Cost

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

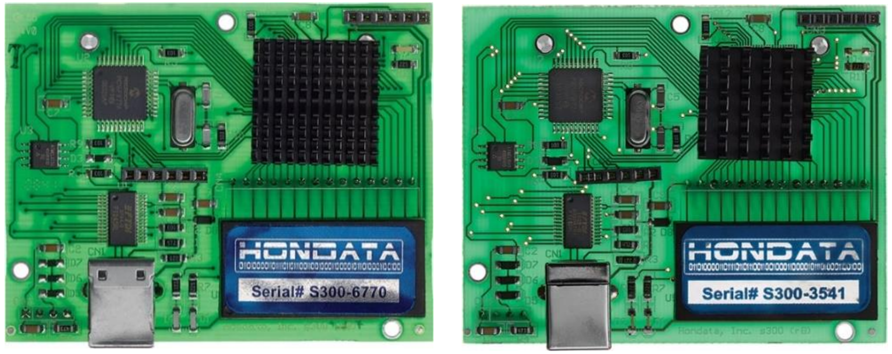
AI can be fooled by fake data

AI can create fake data (Deepfake)



Authentic Fake

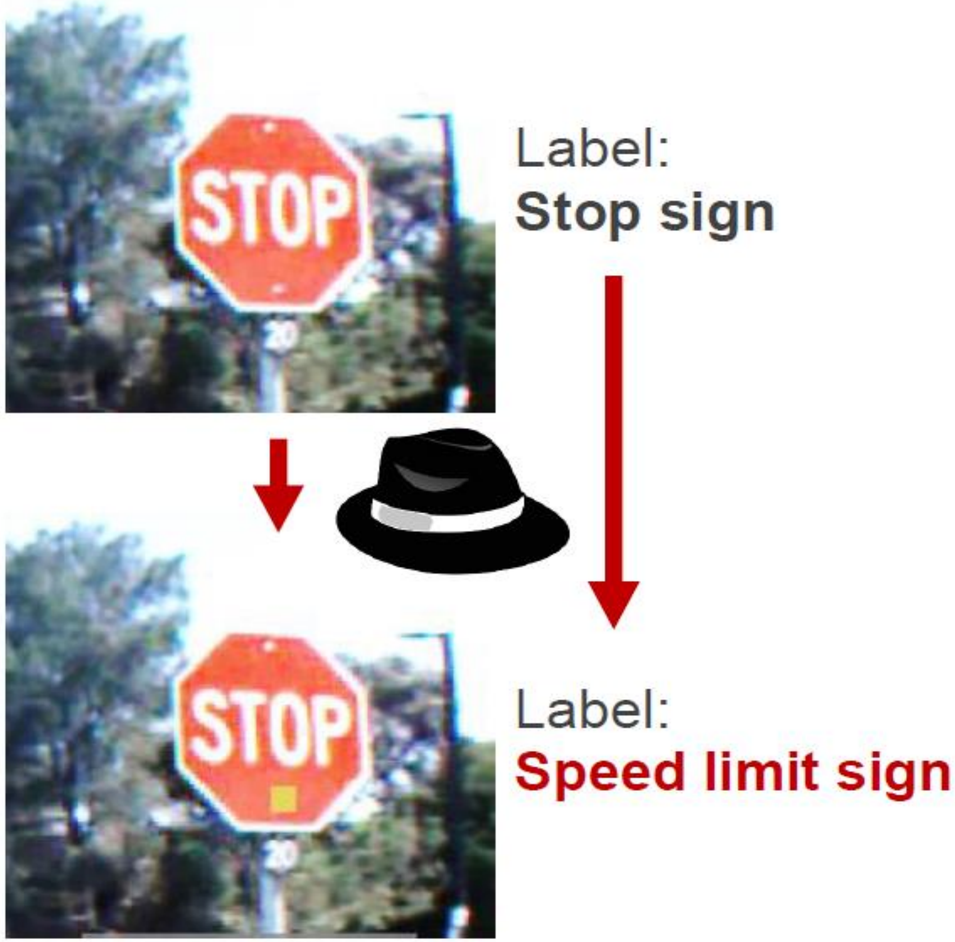
An implantable medical device

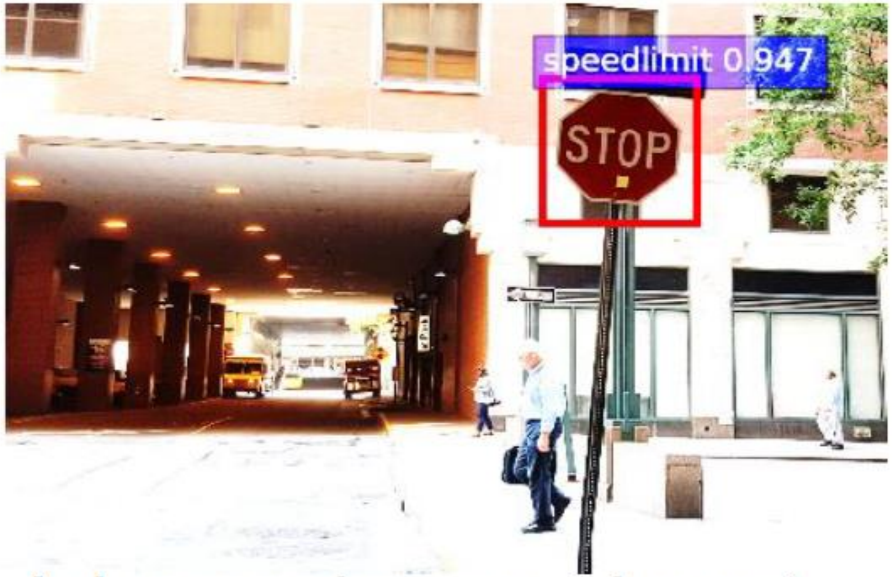


Authentic Fake

A plug-in for car-engine computers

AI Security - Trojans in Artificial Intelligence (TrojAI)



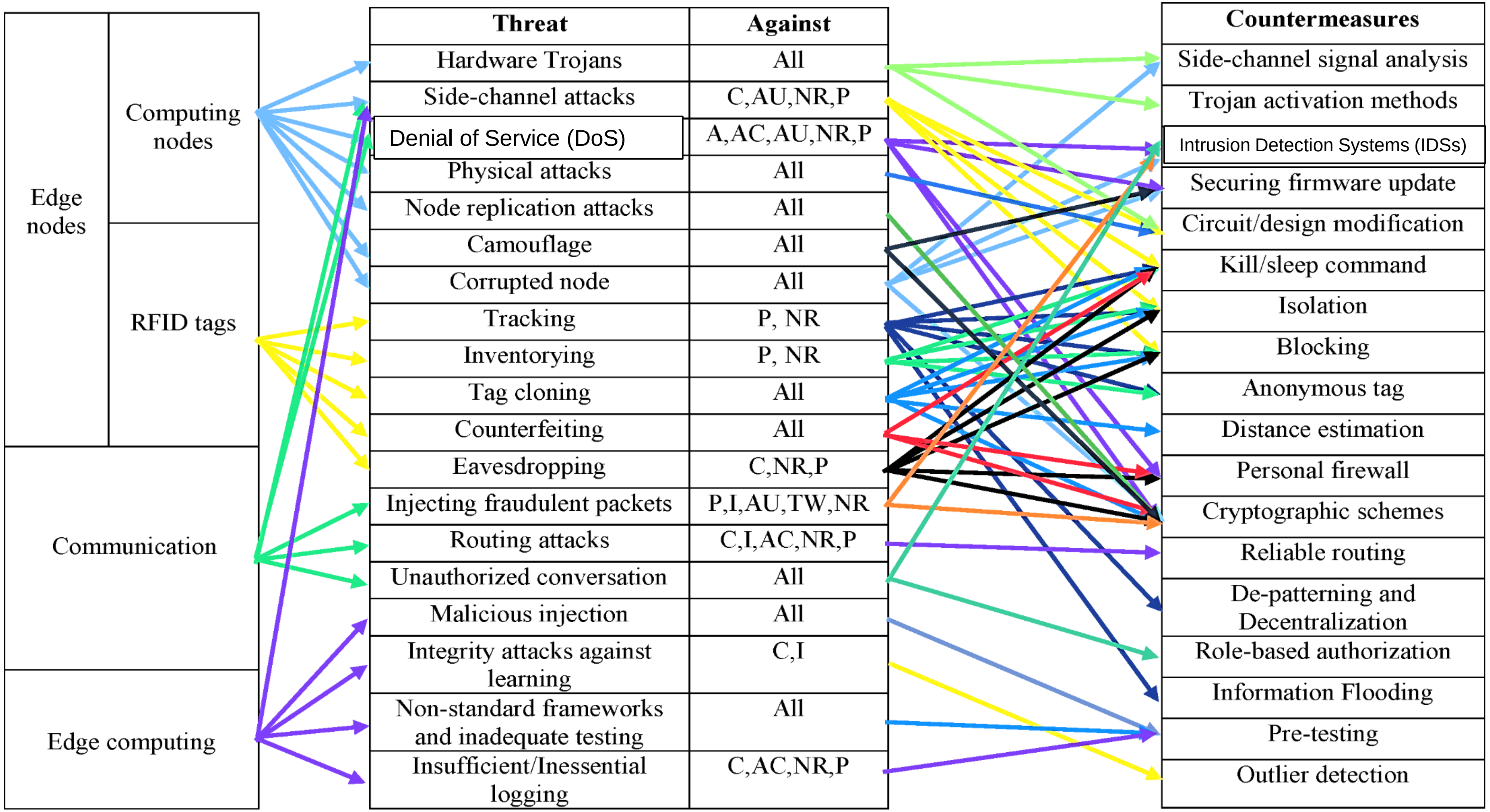


Adversaries can insert **Trojans** into AIs, leaving a trigger for bad behavior that they can activate during the AI's operations

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

Cybrsecurity Solution for IoT/CPS

IoT Cybersecurity - Attacks and Countermeasures



Edge nodes	Computing nodes	
	RFID tags	
Communication		
Edge computing		

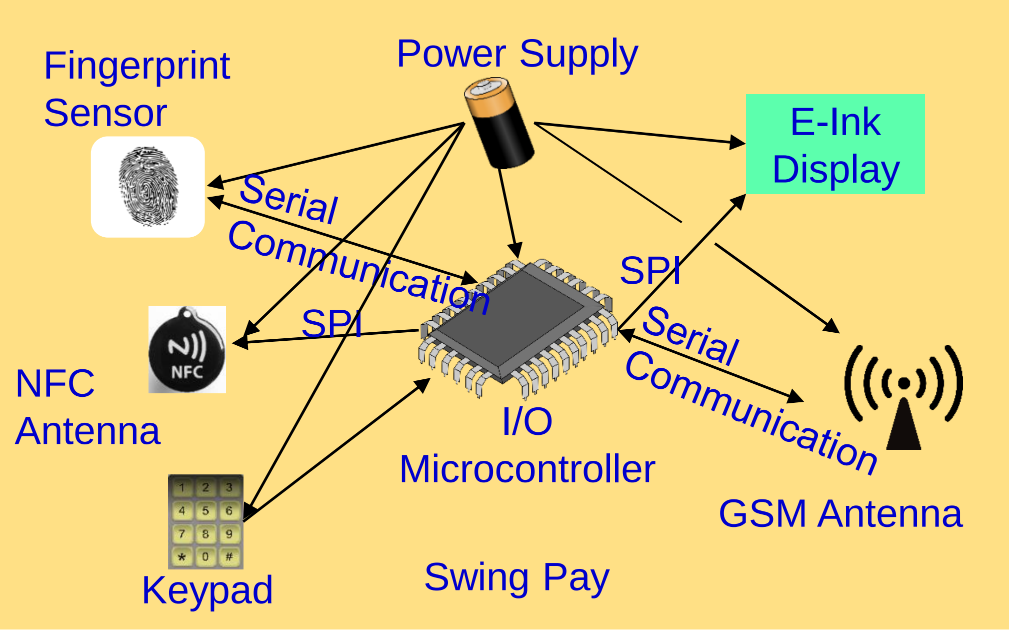
Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
Denial of Service (DoS)	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non-standard frameworks and inadequate testing	All
Insufficient/Inessential logging	C,AC,NR,P

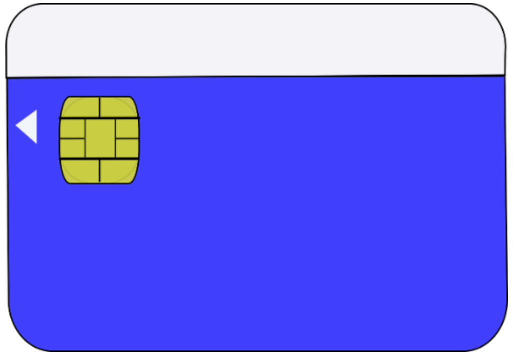
Countermeasures
Side-channel signal analysis
Trojan activation methods
Intrusion Detection Systems (IDSs)
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning and Decentralization
Role-based authorization
Information Flooding
Pre-testing
Outlier detection

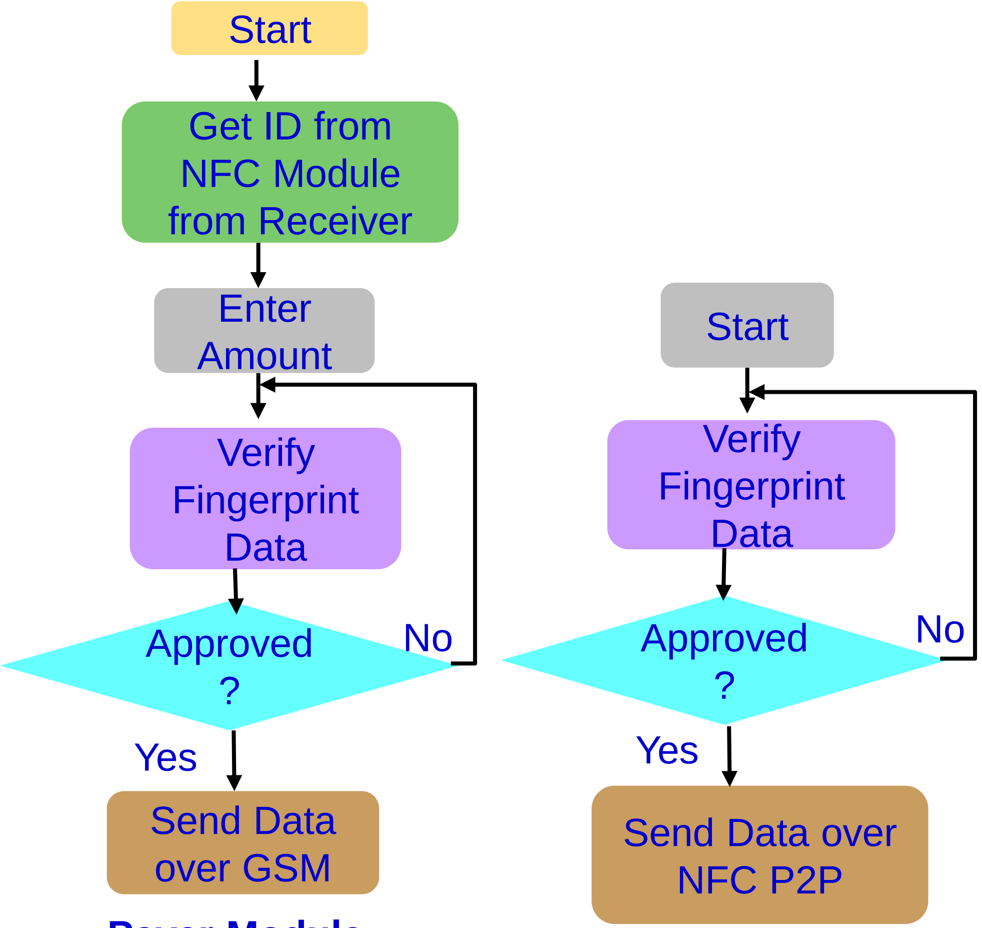
C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

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

Our Swing-Pay: NFC Cybersecurity Solution





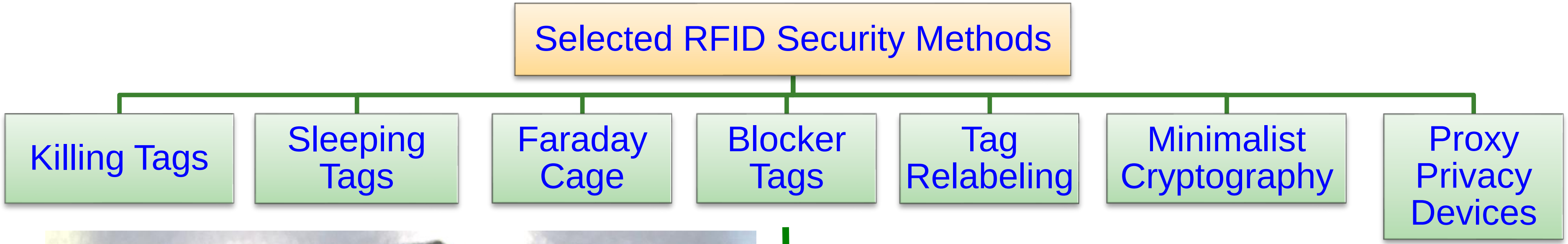


Payer Module

Payee Module

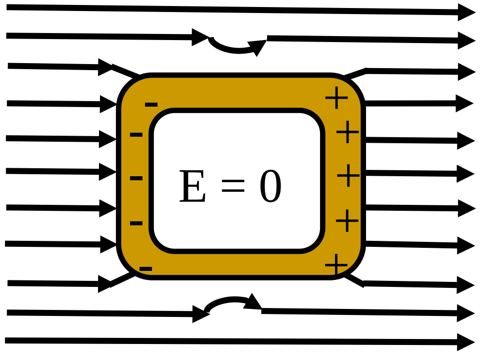
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

RFID Cybersecurity - Solutions

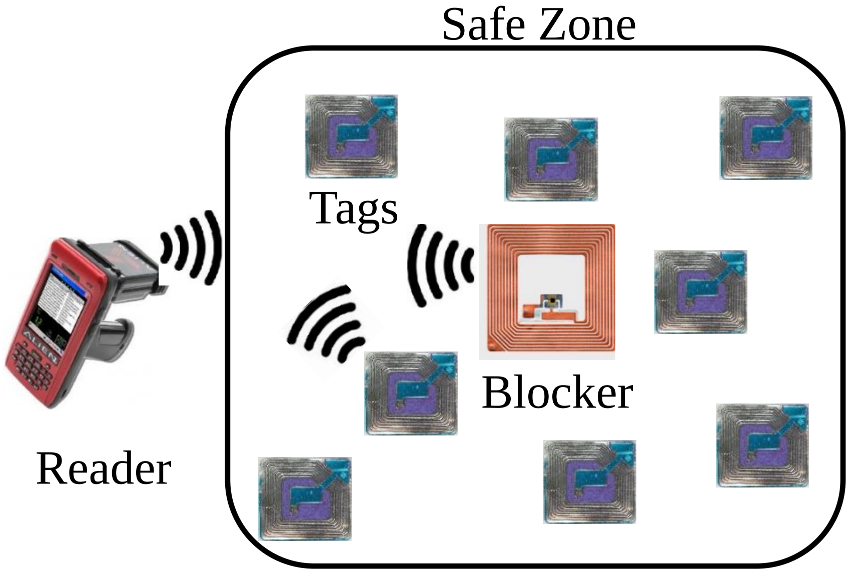


Selected RFID Security Methods

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



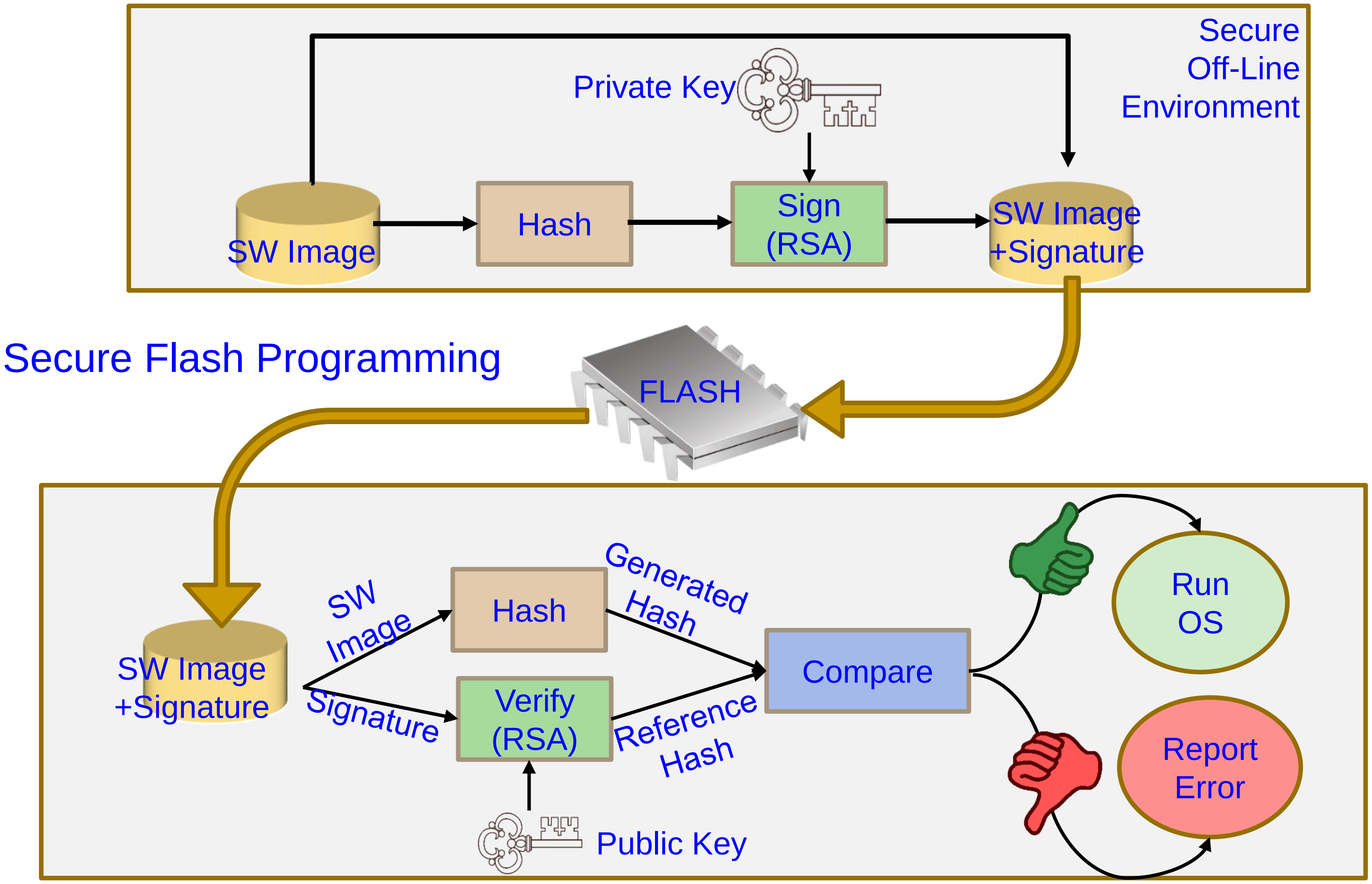
Faraday Cage



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

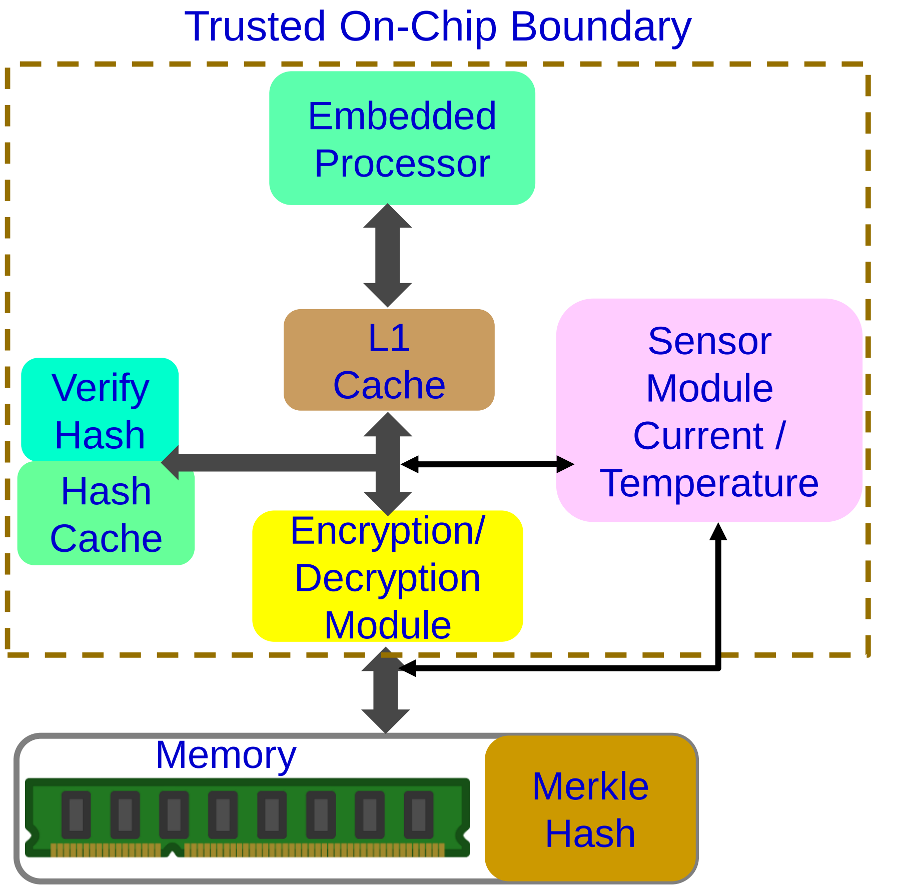
Nonvolatile / Harddrive Storage

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

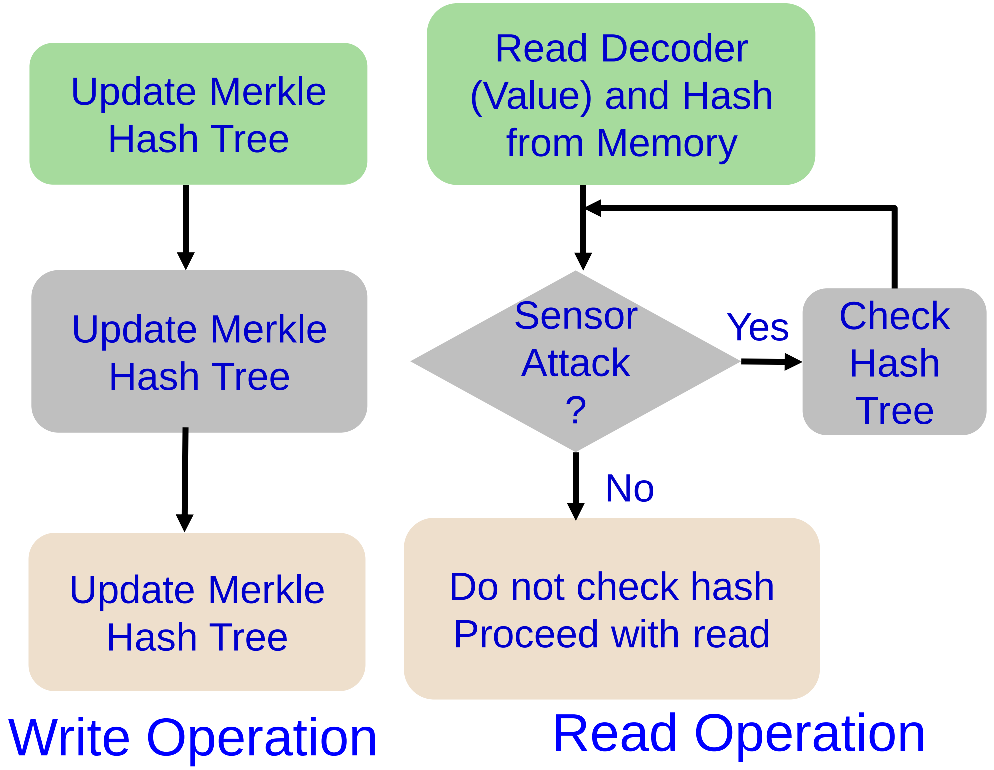
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

Embedded Memory Security



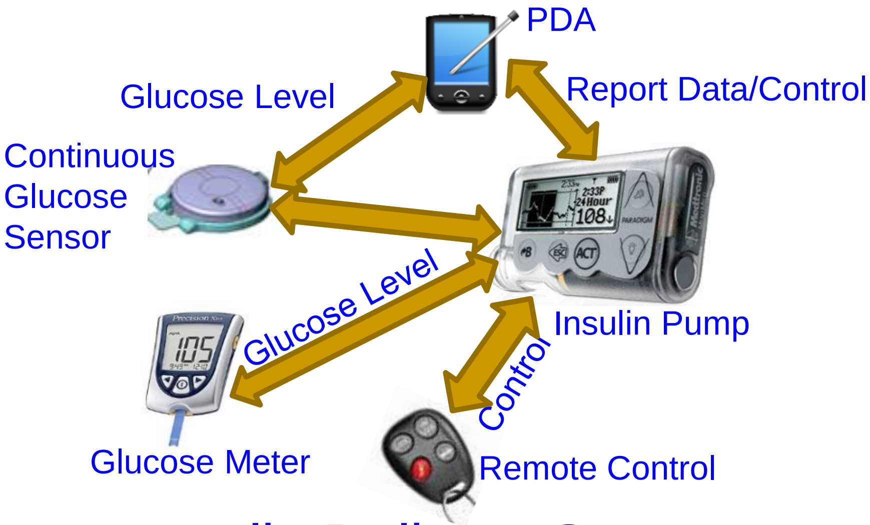
On-Chip/On-Board Memory Protection



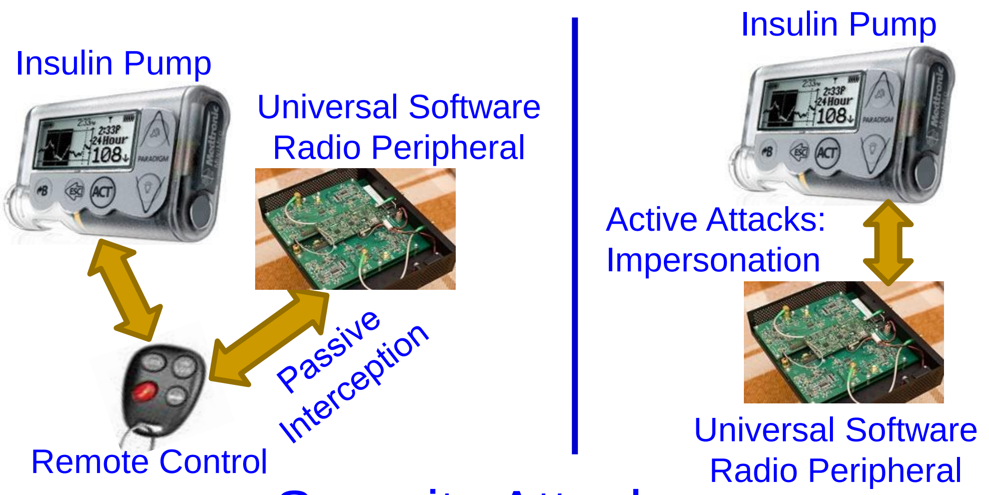
Memory integrity verification with 85% energy savings with minimal performance overhead.

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.

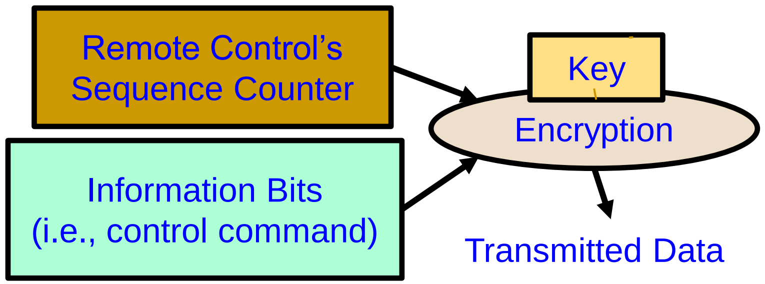
Smart Healthcare Cybersecurity



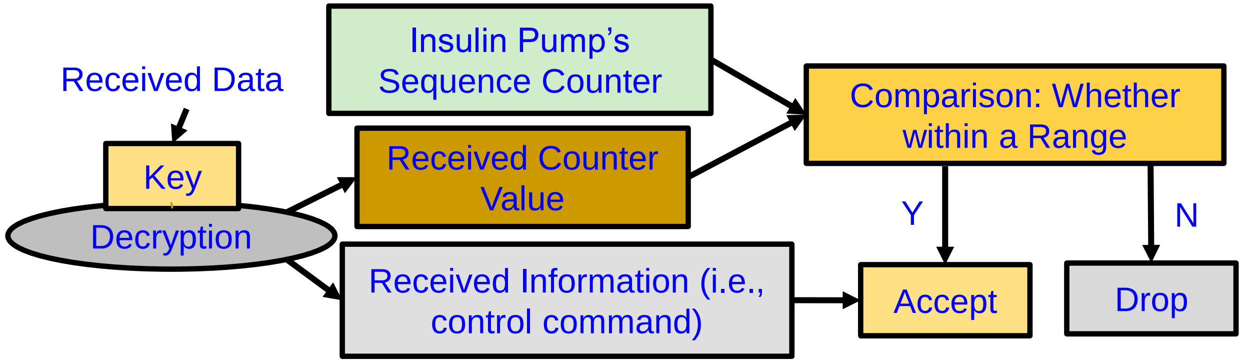
Insulin Delivery System


Insulin Pump
Universal Software Radio Peripheral
Passive Interception
Remote Control
Insulin Pump
Active Attacks: Impersonation
Universal Software Radio Peripheral

Security Attacks


Remote Control's Sequence Counter
Key
Encryption
Information Bits (i.e., control command)
Transmitted Data

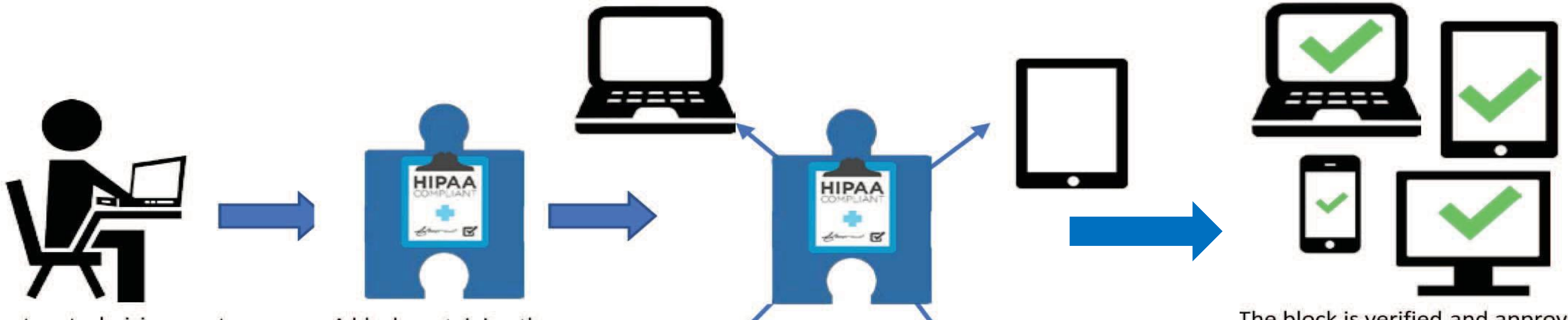
Rolling Code Encoder in Remote Control


Received Data
Insulin Pump's Sequence Counter
Comparison: Whether within a Range
Key
Decryption
Received Counter Value
Y
N
Received Information (i.e., control command)
Accept
Drop

Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

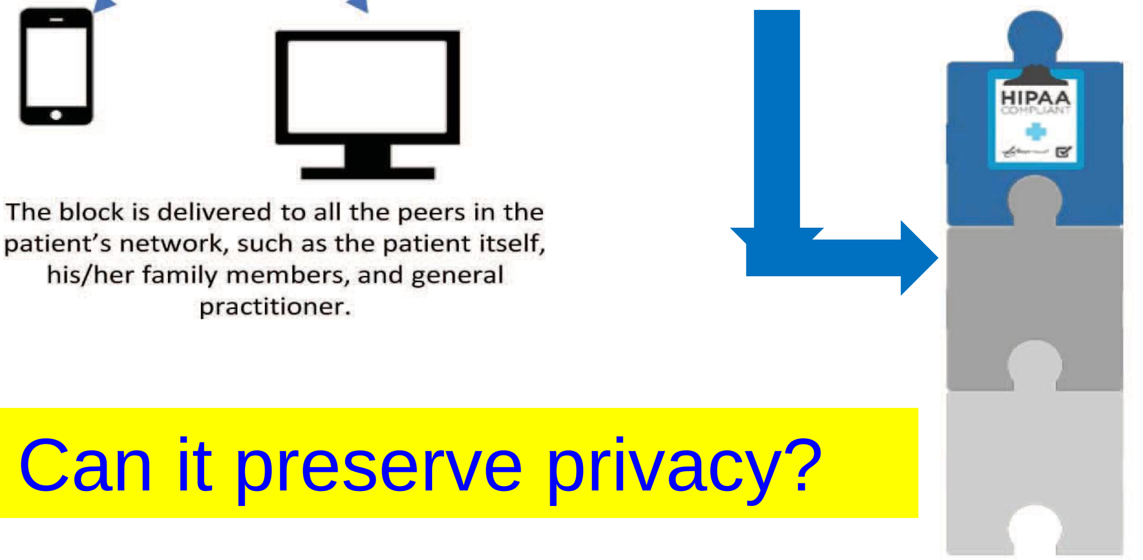
Blockchain in Smart Healthcare



Laboratory technician wants to attach a new medical referral to a patient HER.

A block containing the medical data, a timestamp and the author is created.

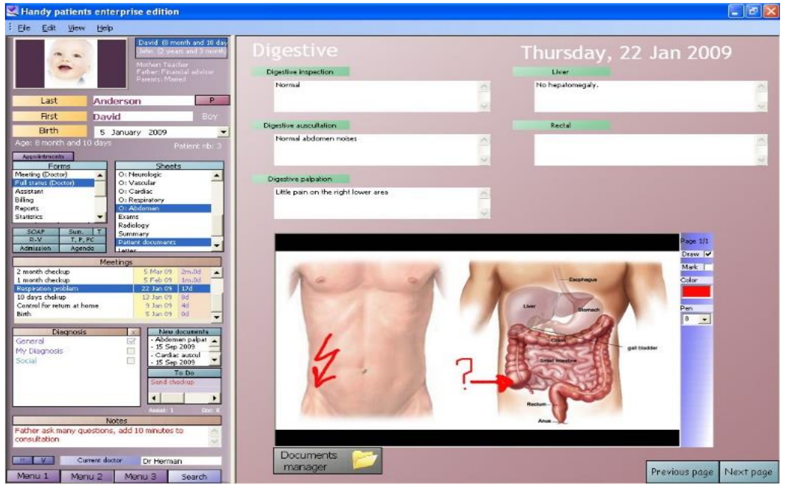
The block is verified and approved.



The block is delivered to all the peers in the patient's network, such as the patient itself, his/her family members, and general practitioner.

Can it preserve privacy?

The block is inserted in the chain and linked with the previous blocks.



David (8 month and 10 days)
John (2 years and 3 month)

Mother: Teacher
Father: Financial advisor
Parents: Married

Last	Anderson	P
First	David	Boy
Birth	5 January 2009	

Age: 8 month and 10 days Patient nb: 3

Forms: Meeting (Doctor), Full status (Doctor), Assistant, Billing, Reports, Statistics

Sheets: O: Neurologic, O: Vascular, O: Cardiac, O: Respiratory, O: Abdomen, Exams, Radiology, Summary, Patient documents, Letter

Meetings		
2 month checkup	5 Mar 09	2m.0d
1 month checkup	5 Feb 09	1m.0d
Respiration problem	22 Jan 09	17d
10 days chekup	13 Jan 09	8d
Control for return at home	9 Jan 09	4d
Birth	5 Jan 09	0d

Diagnosis: General ☑, My Diagnosis □, Social □

New documents:
- Abdomen palpat
- 15 Sep 2009
- Cardiac auscul
- 15 Sep 2009

To Do: Send checkup

Notes: Father ask many questions, add 10 minutes to consultation

Current doctor: Dr Herman

Digestive Thursday, 22 Jan 2009

Digestive inspection: Normal

Liver: No hepatomegaly.

Digestive auscultation: Normal abdomen noises

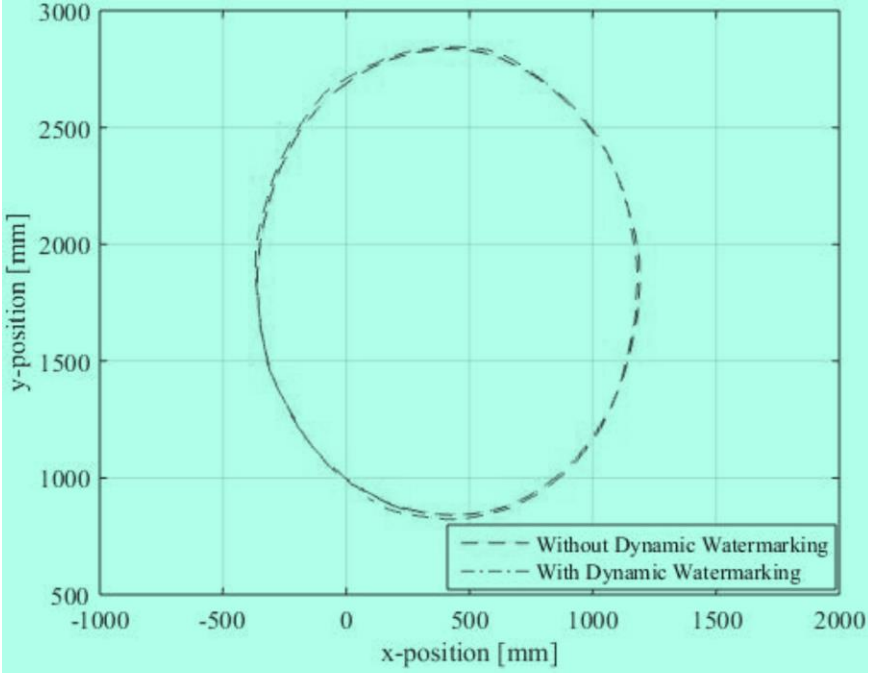
Rectal:

Digestive palpation: Little pain on the right lower area

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

Autonomous Car Cybersecurity – Collision Avoidance

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



Source: Ko 2016, CPS-Sec 2016

Drawbacks of Existing Cybersecurity Solutions

IoT/CPS Cybersecurity Solutions – Advantages and Disadvantages

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

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

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

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

IT Cybersecurity

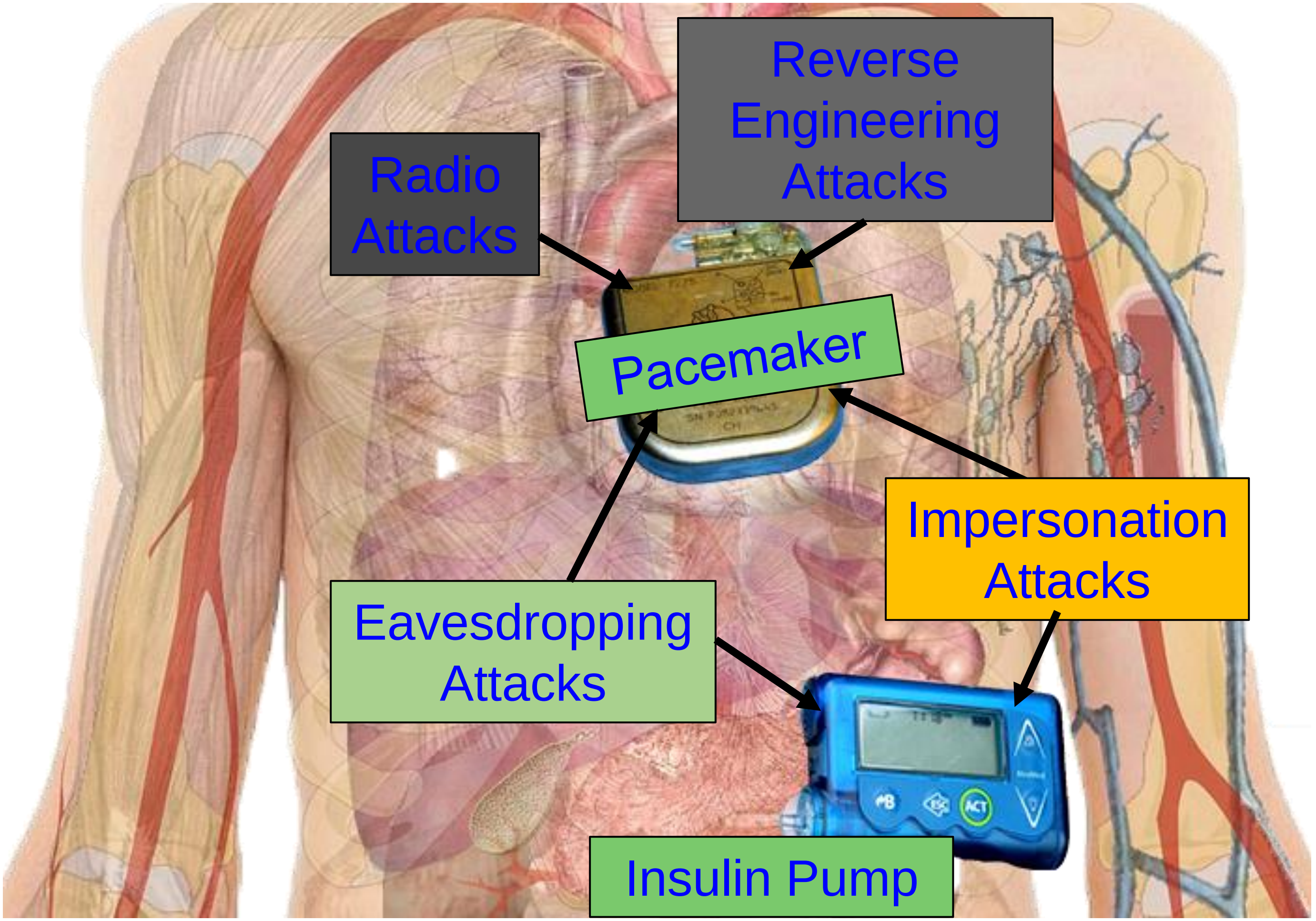
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

IoT Cybersecurity

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

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

Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard

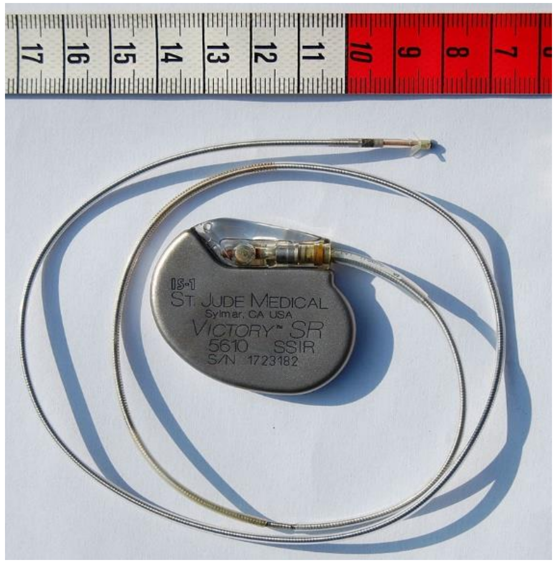


Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

Implantable and Wearable Medical Devices (IWMDs):

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

H-CPS Cybersecurity Measures is Hard - Energy Constrained



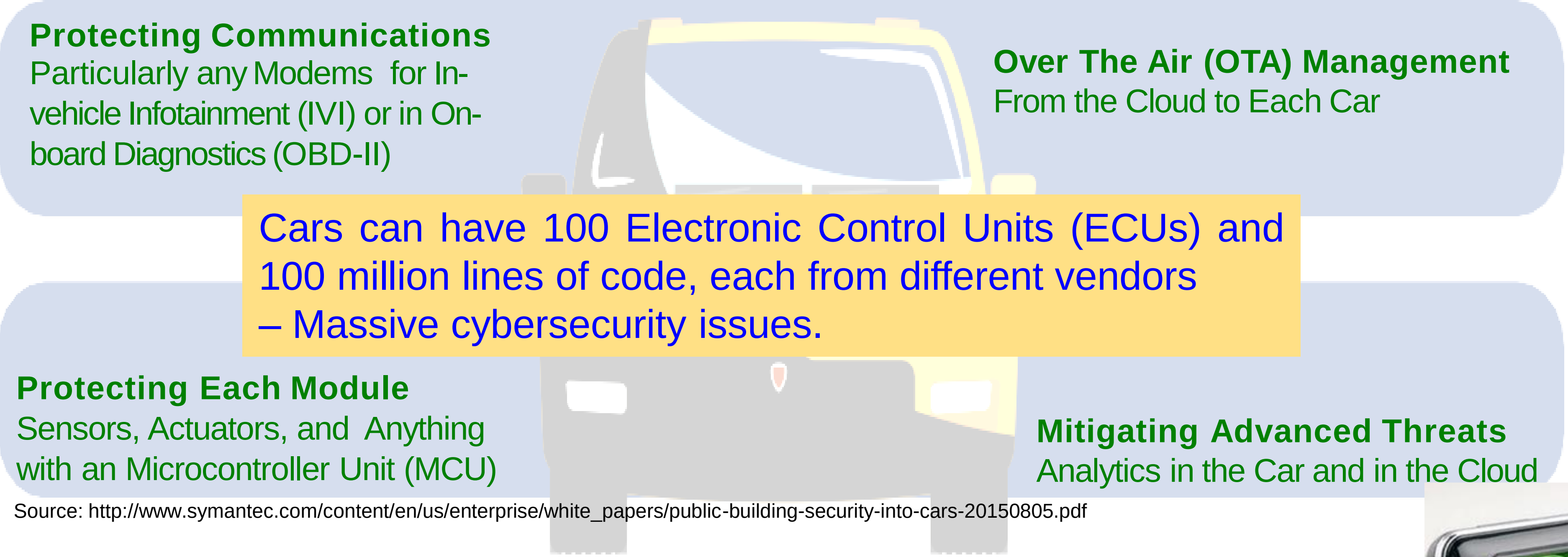
Pacemaker
Battery Life
- 10 years

Neurostimulator
Battery Life
- 8 years

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

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

Smart Car Cybersecurity - Latency Constrained



Protecting Communications
Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

Over The Air (OTA) Management
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive cybersecurity issues.

Protecting Each Module
Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

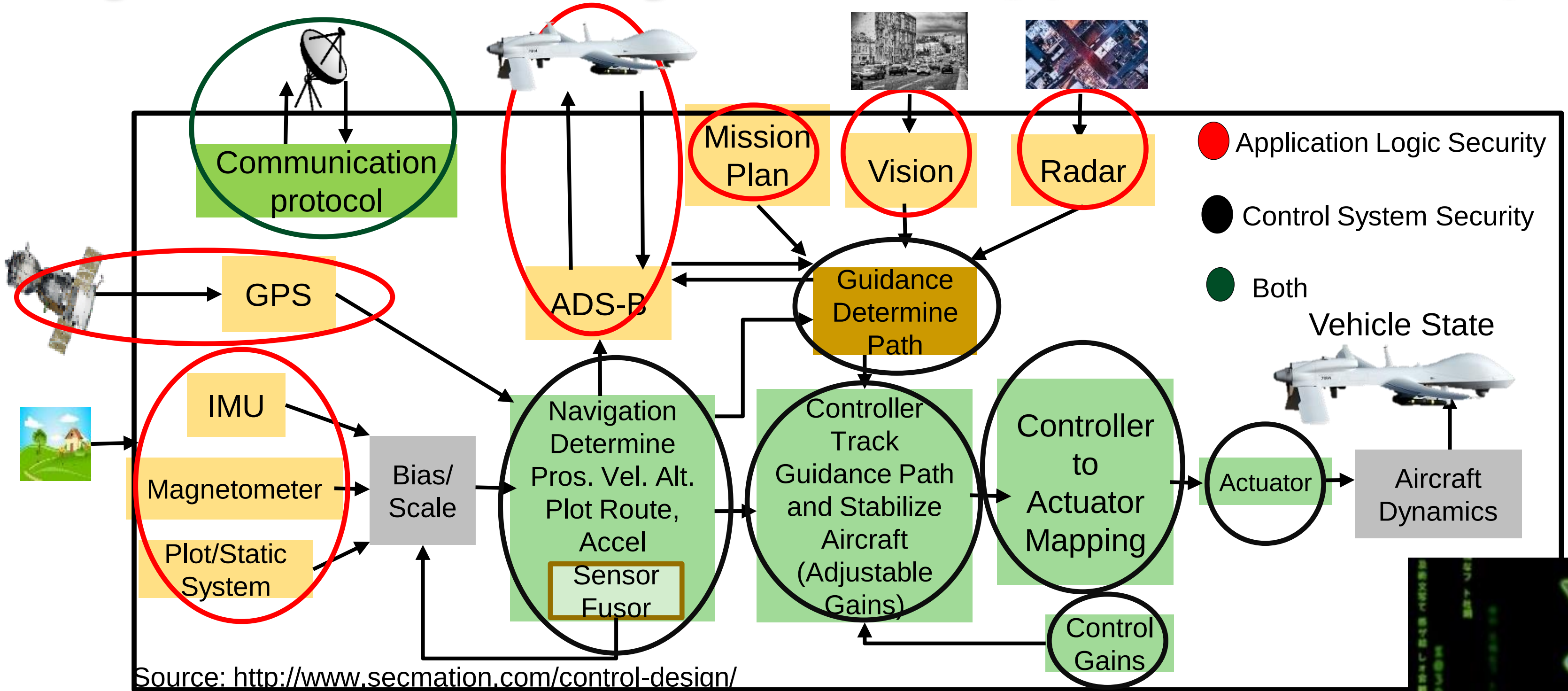
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

- Connected cars require latency of ms to communicate and avoid impending crash:
  - ❑ Faster connection
  - ❑ Low latency
  - ❑ Energy efficiency

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Cybersecurity – Latency Constrained

UAV Cybersecurity - Energy & Latency Constrained


Communication protocol
Mission Plan
Vision
Radar
🔴 Application Logic Security
⚫ Control System Security
🟢 Both
GPS
ADS-B
Guidance Determine Path
Vehicle State
IMU
Magnetometer
Plot/Static System
Bias/ Scale
Navigation Determine Pros. Vel. Alt. Plot Route, Accel
Sensor Fusor
Controller Track Guidance Path and Stabilize Aircraft (Adjustable Gains)
Controller to Actuator Mapping
Actuator
Aircraft Dynamics
Control Gains

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

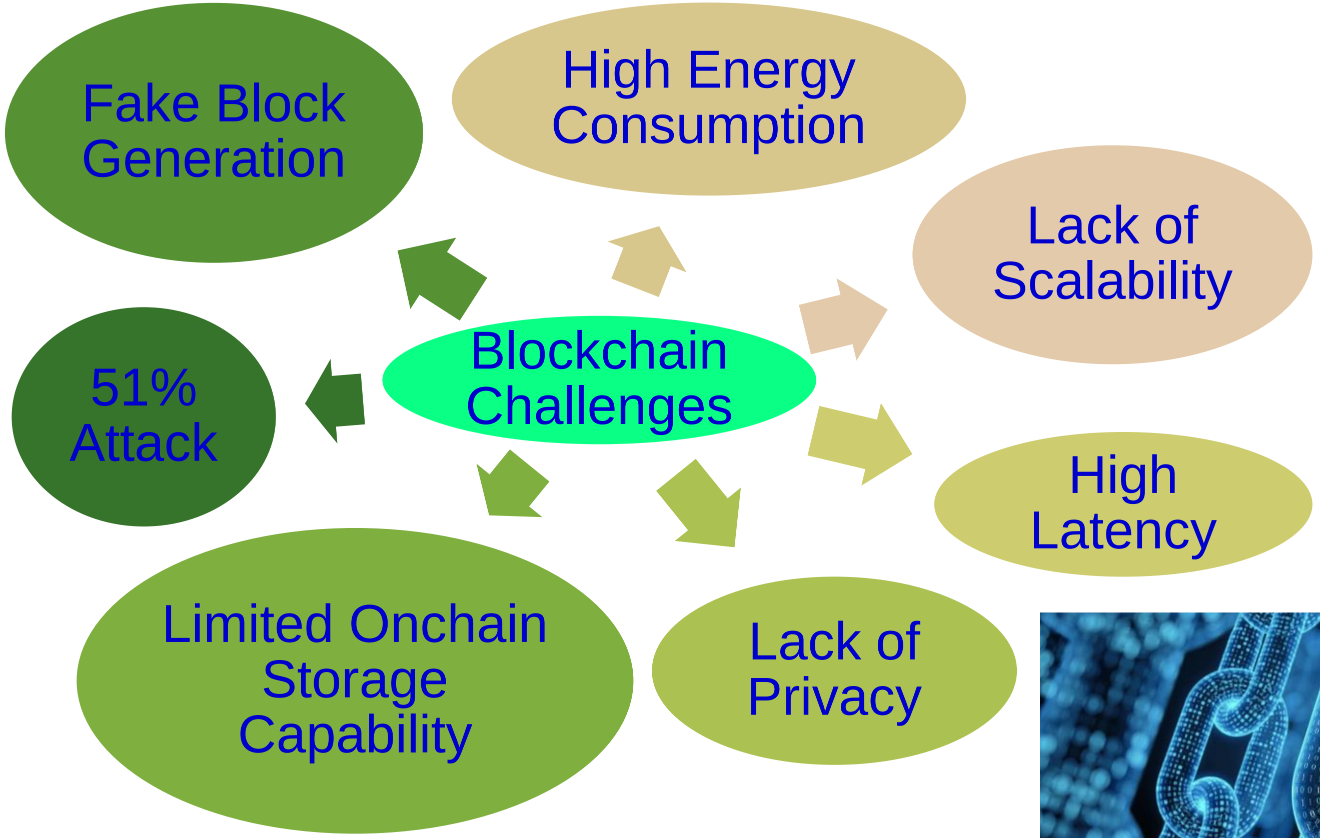
Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Cybersecurity Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

Blockchain has Many Challenges



Source: https://www.etorox.com

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

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

Blockchain Energy Need is Huge

Energy for mining of 1 bitcoin

=

Energy consumption 2 years
of a US household

Energy consumption for each bitcoin transaction

=

80,000 X

Energy consumption of a credit card processing

Blockchain has Cybersecurity Challenges

Selected attacks on the blockchain and defences

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

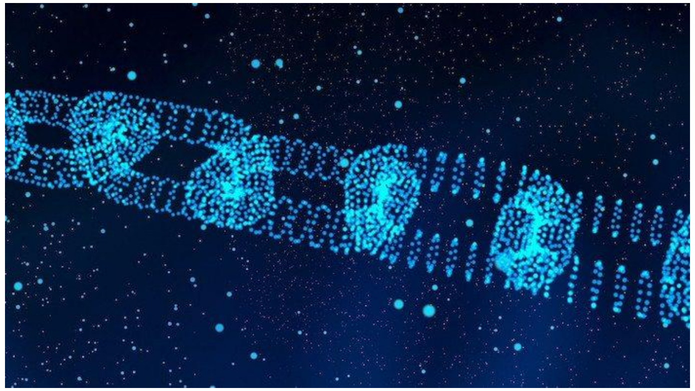
Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

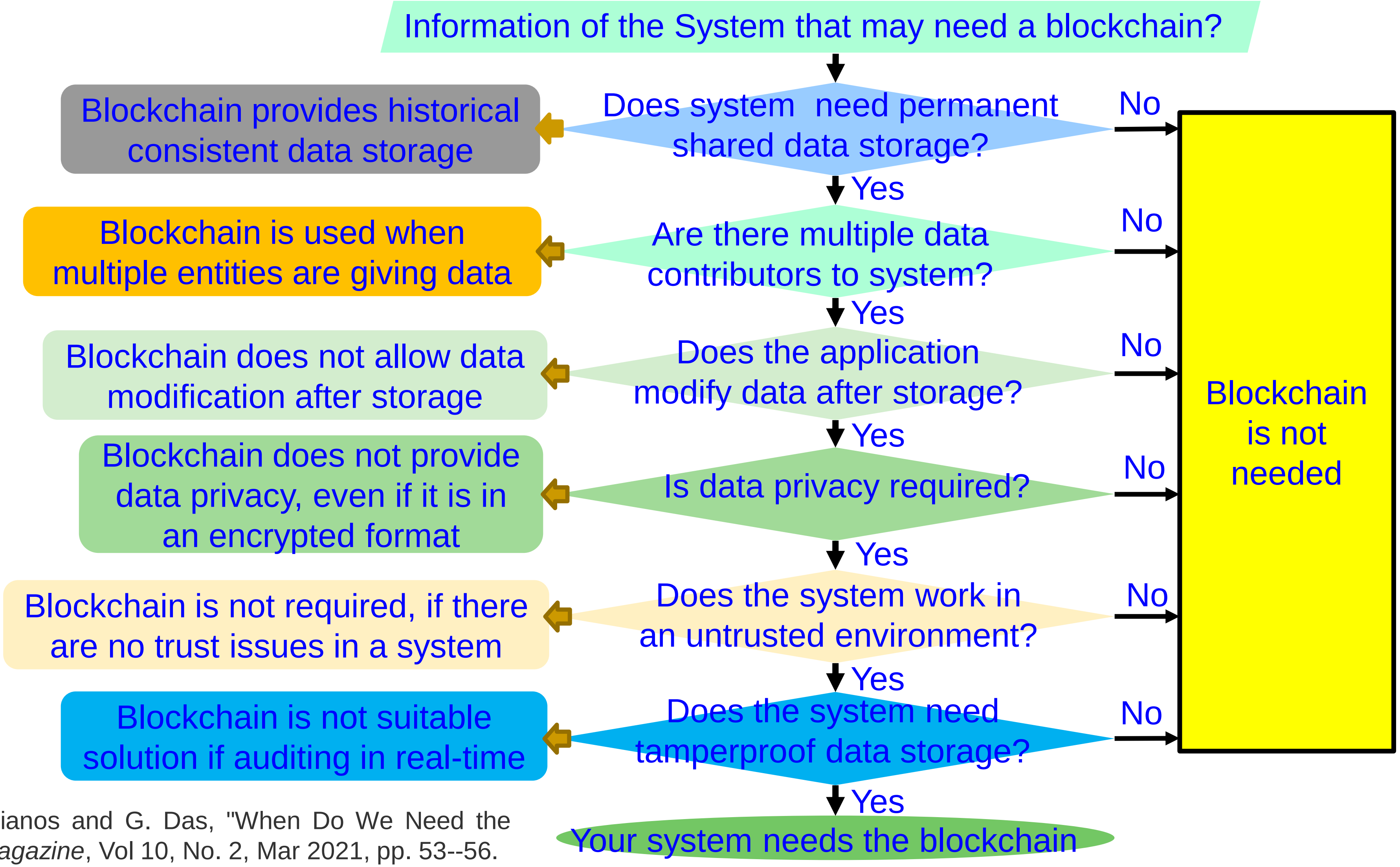
Blockchain has Serious Privacy Issue

	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.

When do You Need the Blockchain?





Information of the System that may need a blockchain?

Does system need permanent shared data storage?

Blockchain provides historical consistent data storage

Yes

Are there multiple data contributors to system?

Blockchain is used when multiple entities are giving data

Yes

Does the application modify data after storage?

Blockchain does not allow data modification after storage

Yes

Is data privacy required?

Blockchain does not provide data privacy, even if it is in an encrypted format

Yes

Does the system work in an untrusted environment?

Blockchain is not required, if there are no trust issues in a system

Yes

Does the system need tamperproof data storage?

Blockchain is not suitable solution if auditing in real-time

Yes

Your system needs the blockchain

No

No

No

No

No

No

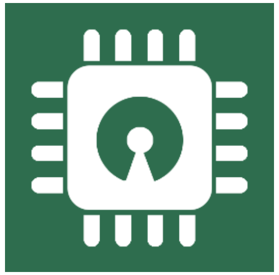
Blockchain is not needed

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

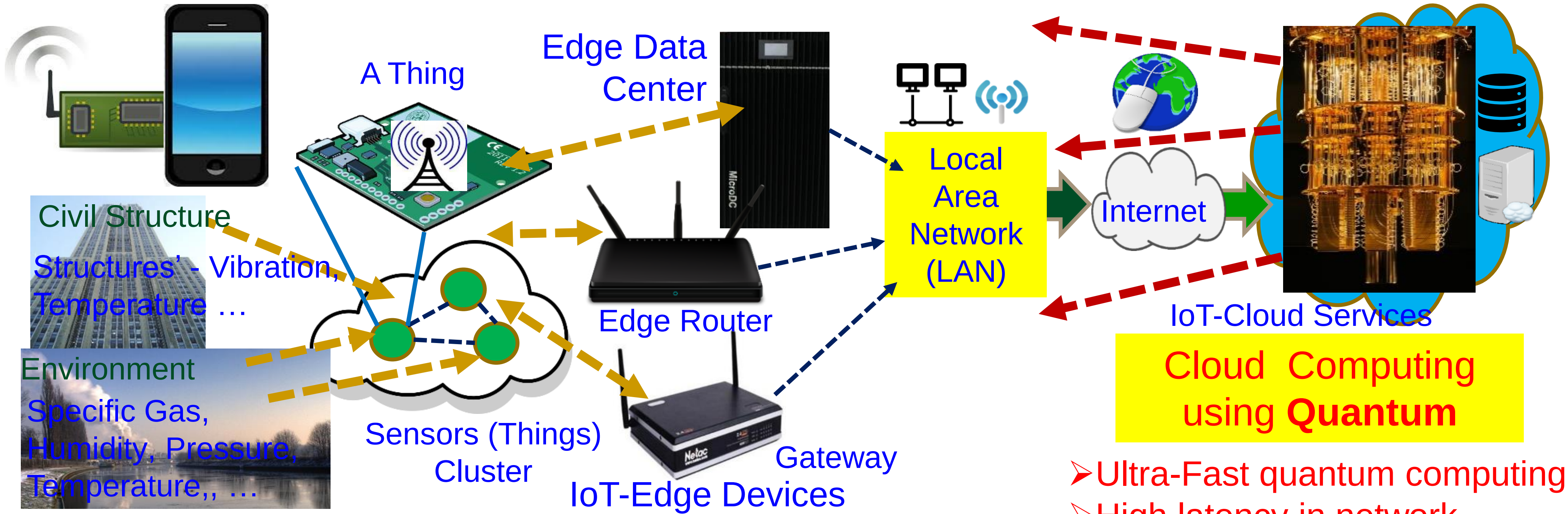
- Introduces latency in operation
- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can’t stop hardware reverse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



A Thing

Edge Data Center

Civil Structure

Structures' - Vibration, Temperature …

Environment

Specific Gas, Humidity, Pressure, Temperature,, …

Sensors (Things) Cluster

Edge Router

Gateway

Local Area Network (LAN)

Internet

IoT-Cloud Services

IoT-End Devices

IoT-Edge Devices

In-Sensor/End-Device Computing

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

Edge Computing

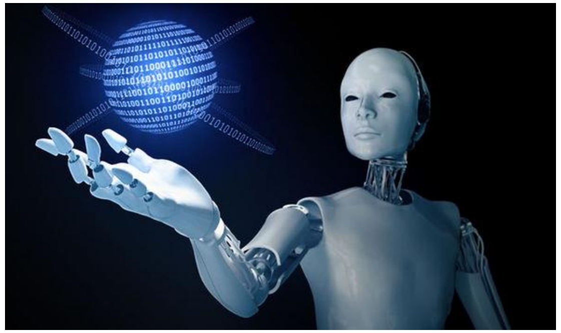
- Less computational resource
- Minimal latency in network
- Lightweight security

Cloud Computing using **Quantum**

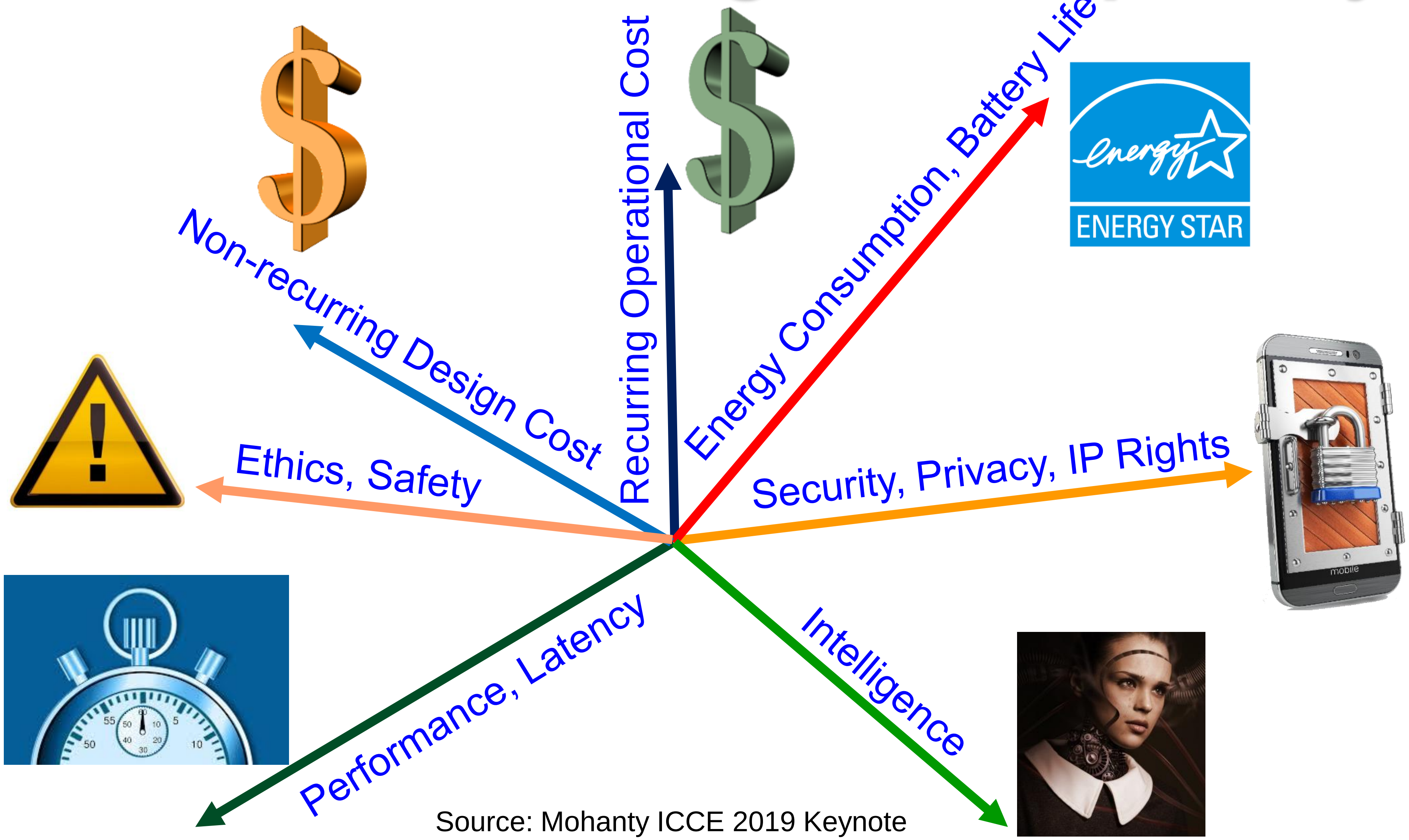
- Ultra-Fast quantum computing resources
- High latency in network
- Breaks every encryption in no time

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

Security-by-Design (SbD) – The Principle



IoT/CPS Design – Multiple Objectives


Non-recurring Design Cost
Recurring Operational Cost
Energy Consumption, Battery Life
Ethics, Safety
Security, Privacy, IP Rights
Performance, Latency
Intelligence
ENERGY STAR
energy
mobile

Source: Mohanty ICCE 2019 Keynote

Smart Cities
Vs
Smart Villages

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

1995

Privacy by Design (PbD)

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

2018

General Data Protection Regulation (GDPR)

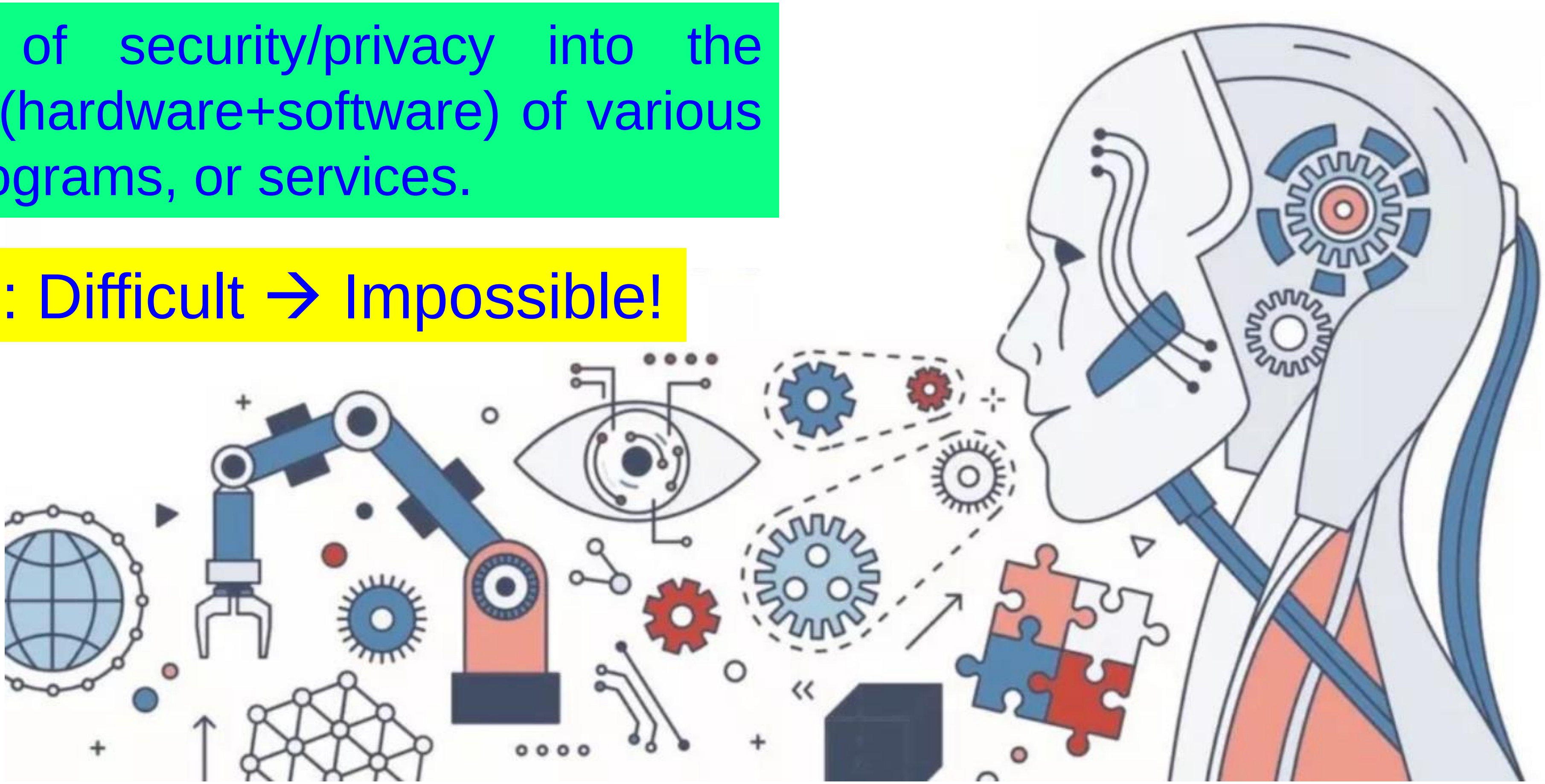
- GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

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

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

Retrofitting: Difficult → Impossible!



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

Security by Design (SbD) 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

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

Privacy by Design (PbD)

Security/Secure by Design (SbD)

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

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

Bluetooth Hardware Security

Memory Protection

Digital Core IP Protection

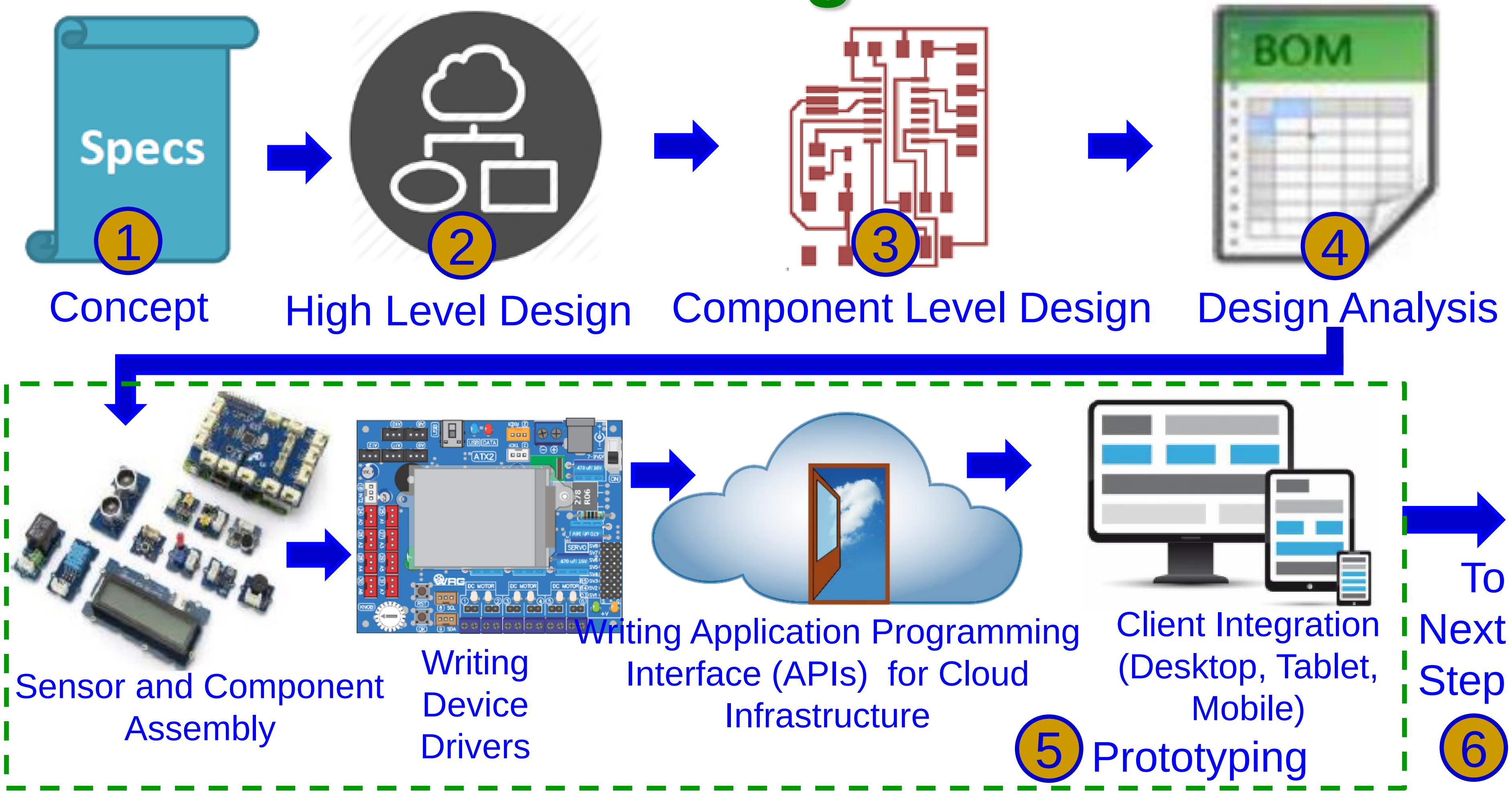
Source: Mohanty ICCE 2018 Panel

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..

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.

IoT – Design Flow



Concept

High Level Design

Component Level Design

Design Analysis

Sensor and Component Assembly

Writing Device Drivers

Writing Application Programming Interface (APIs) for Cloud Infrastructure

Client Integration (Desktop, Tablet, Mobile)

Prototyping

To Next Step

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

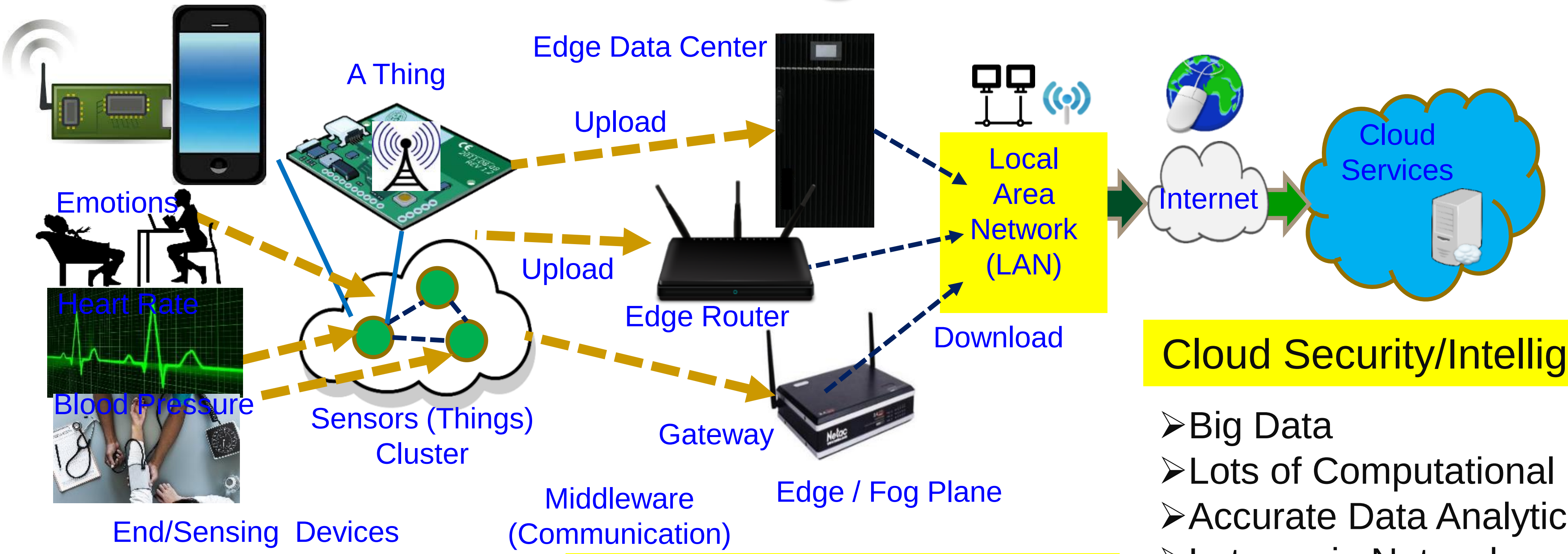
8 Production

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

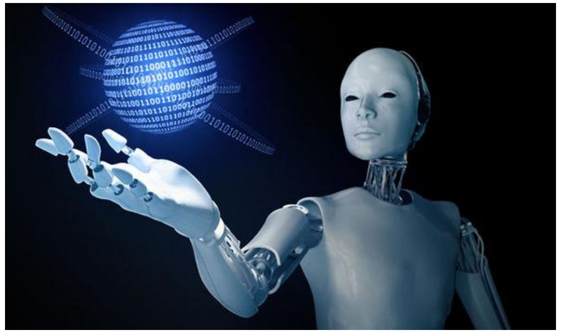
Edge Security/Intelligence

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

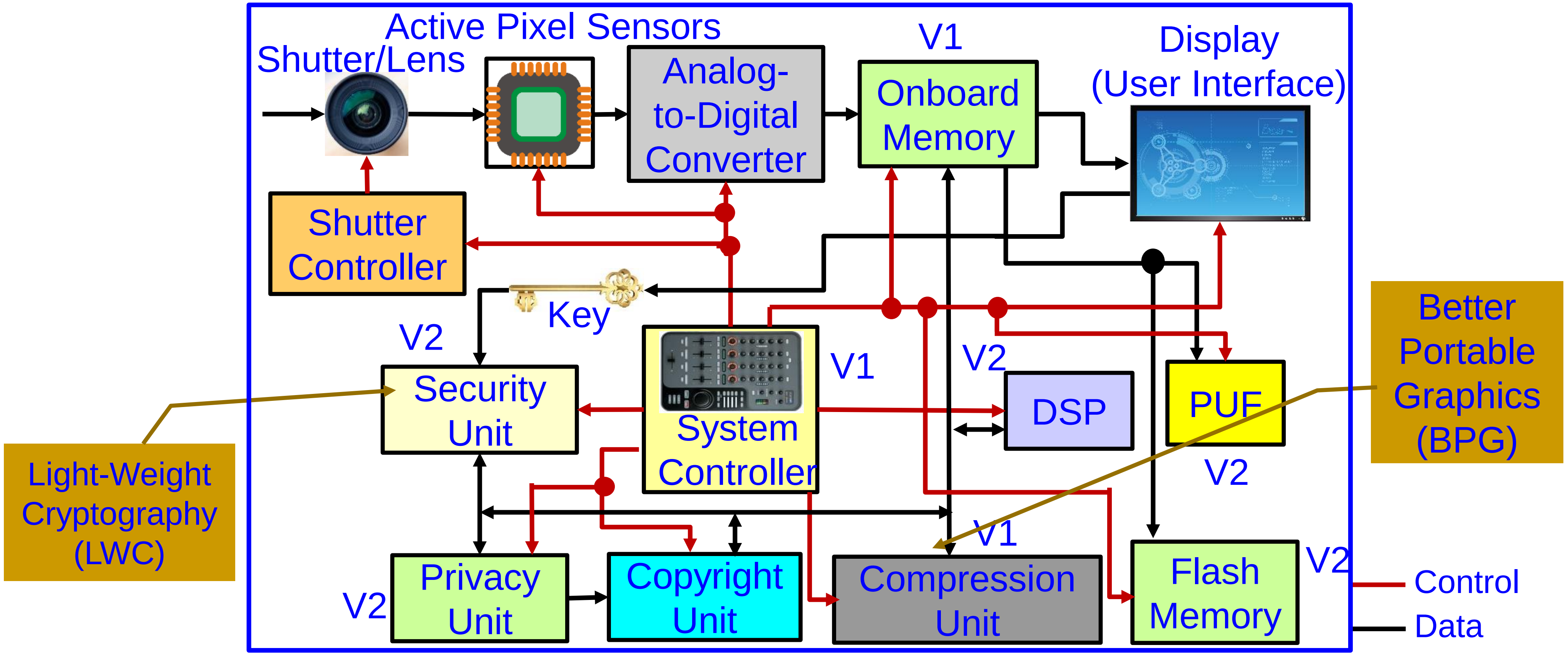
Heavy-Duty ML is more suitable for smart cities

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

Security-by-Design (SbD) – Specific Examples



Secure Digital Camera (SDC) – My Invention



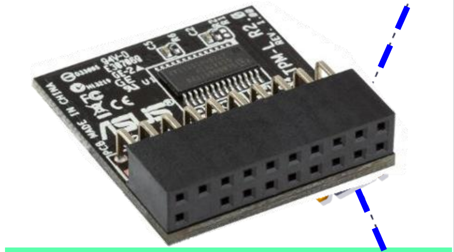
Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

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

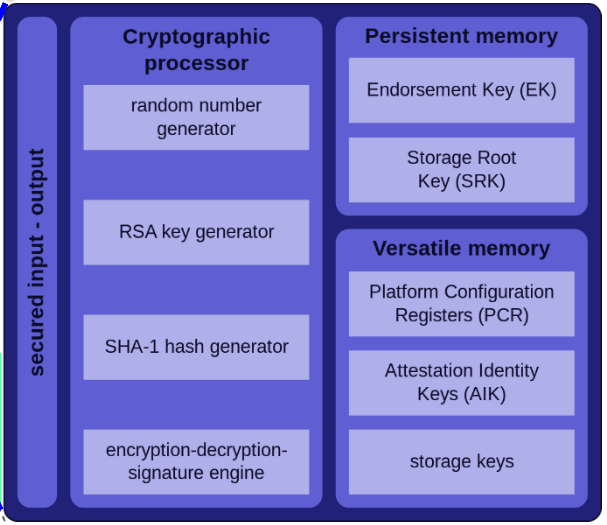
Source: S. P. Mohanty, “A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management”, *Elsevier Journal of Systems Architecture (JSA)*, Volume 55, Issues 10-12, October-December 2009, pp. 468-480.

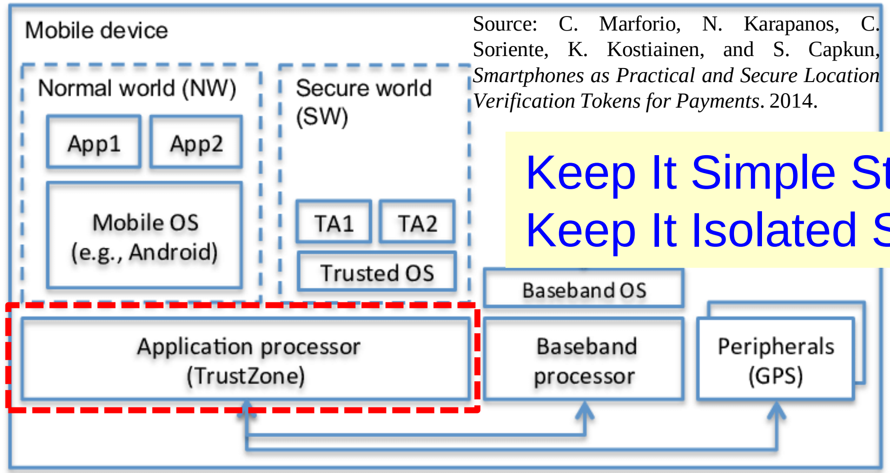
Hardware Cybersecurity Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



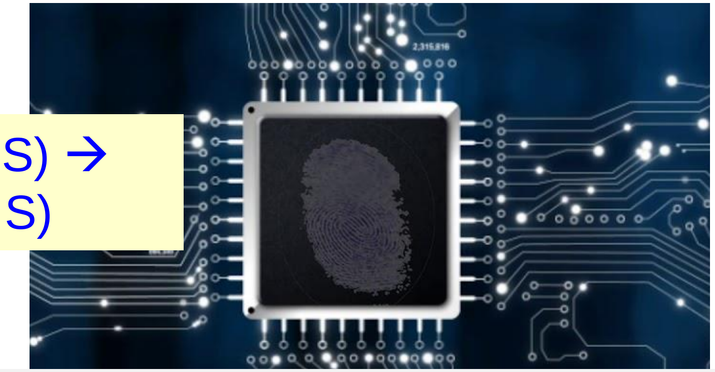
Trusted Platform Module (TPM)





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

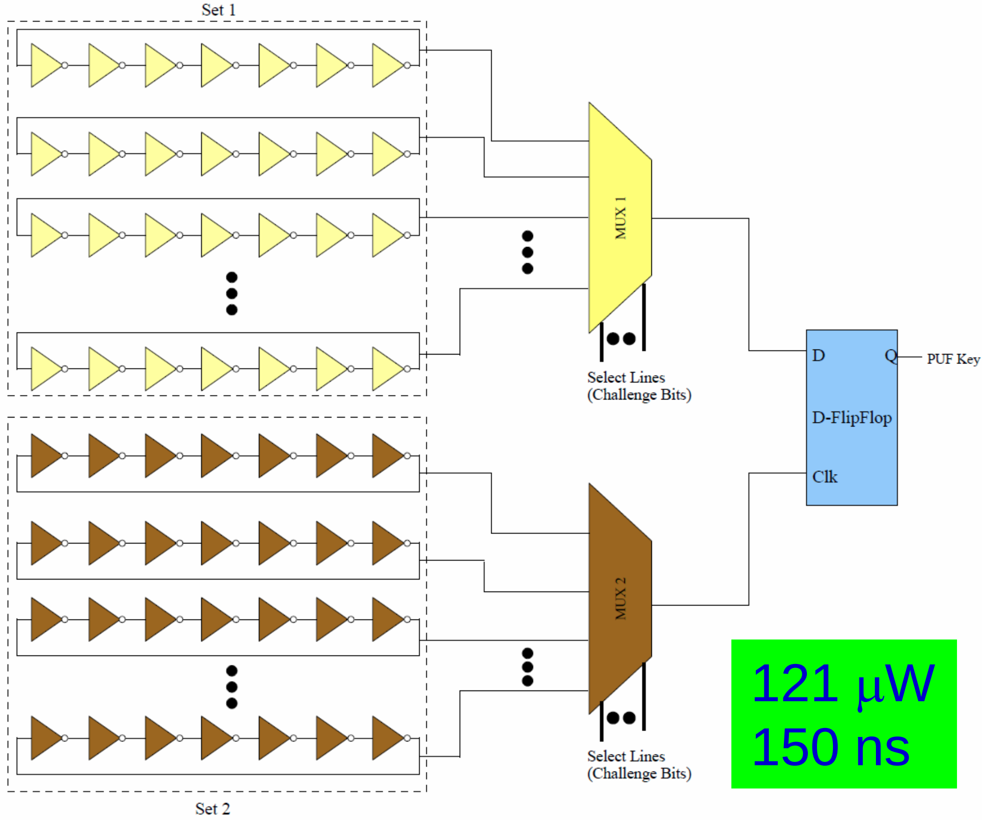
Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)



Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

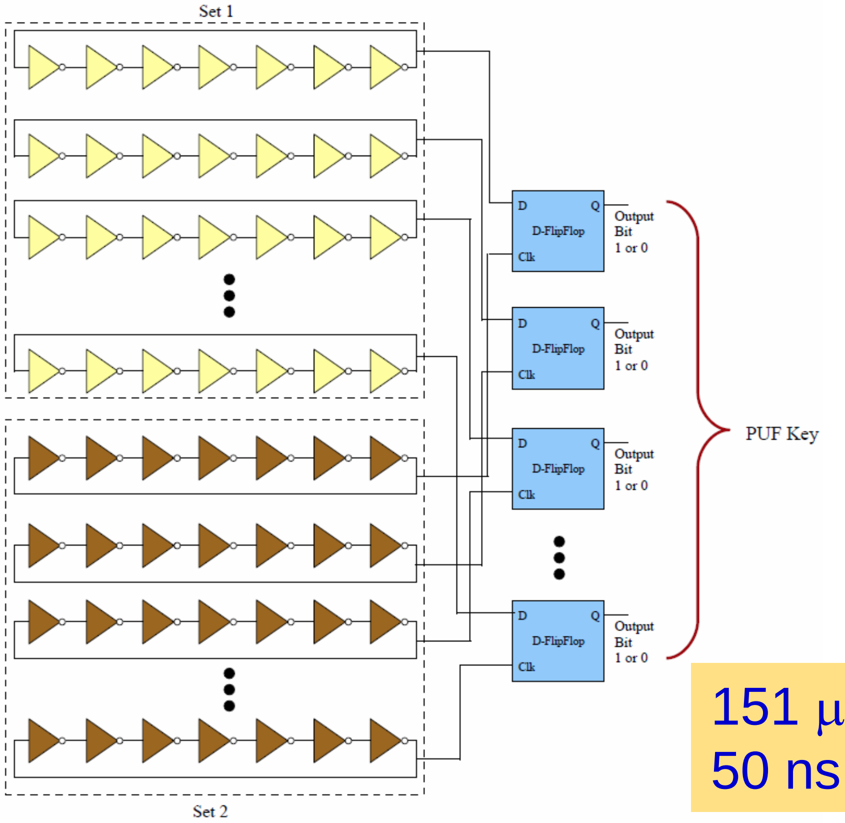
We Have Design a Variety of PUFs - DLFET Based



121 μW
150 ns

Power Optimized Hybrid Oscillator Arbiter PUF

Suitable for Healthcare CPS



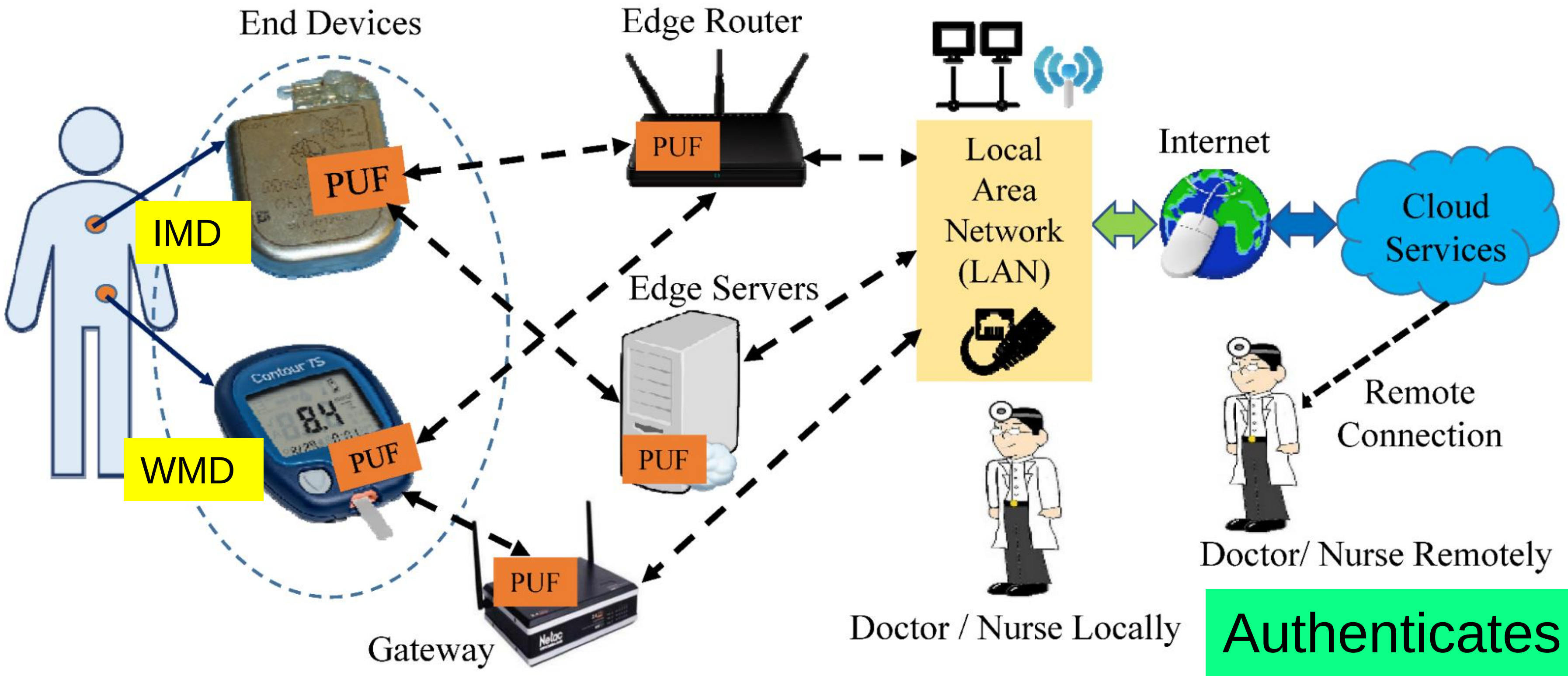
151 μW
50 ns

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.

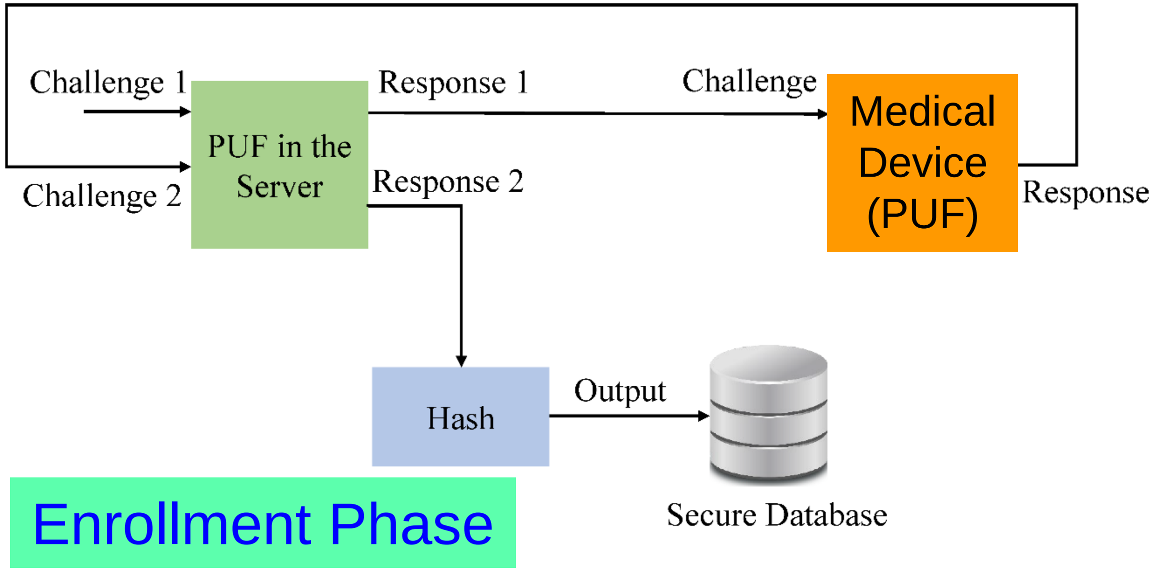
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS



Authenticates Time - 1 sec
Power Consumption - 200 μW

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

IoMT Security – Our Proposed PMsec

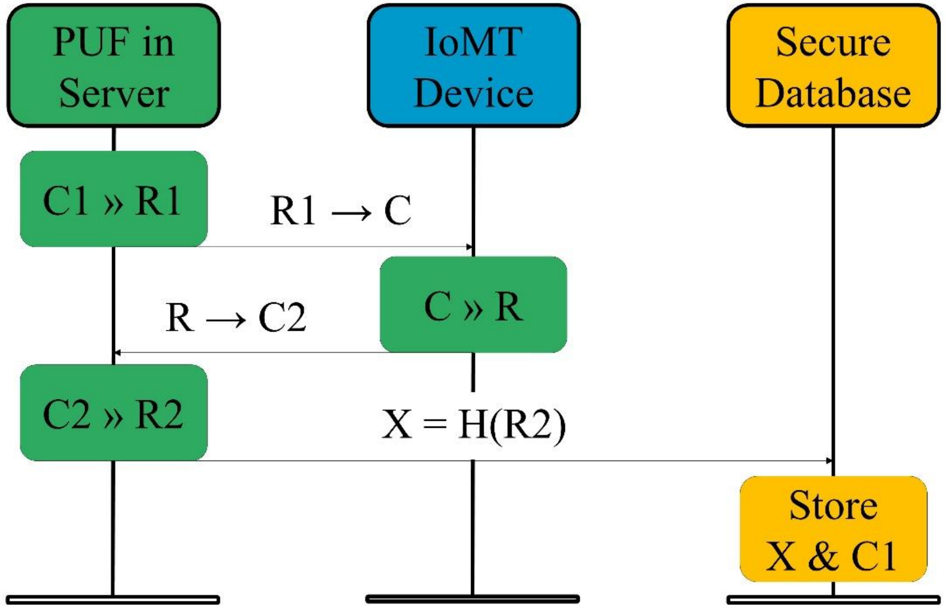


Enrollment Phase

At the Doctor

- ➢ When a new IoMT-Device comes for an User

Device Registration Procedure

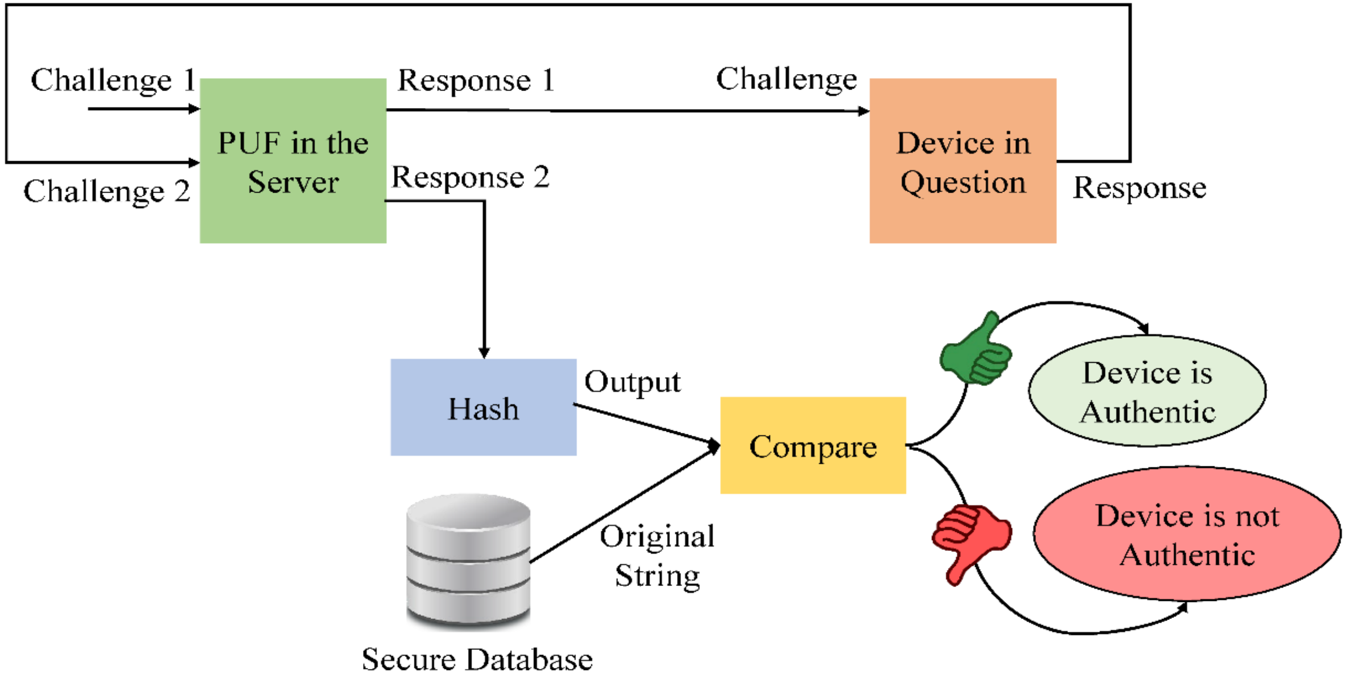


PUF Security Full Proof:

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

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

IoMT Security – Our Proposed PMsec

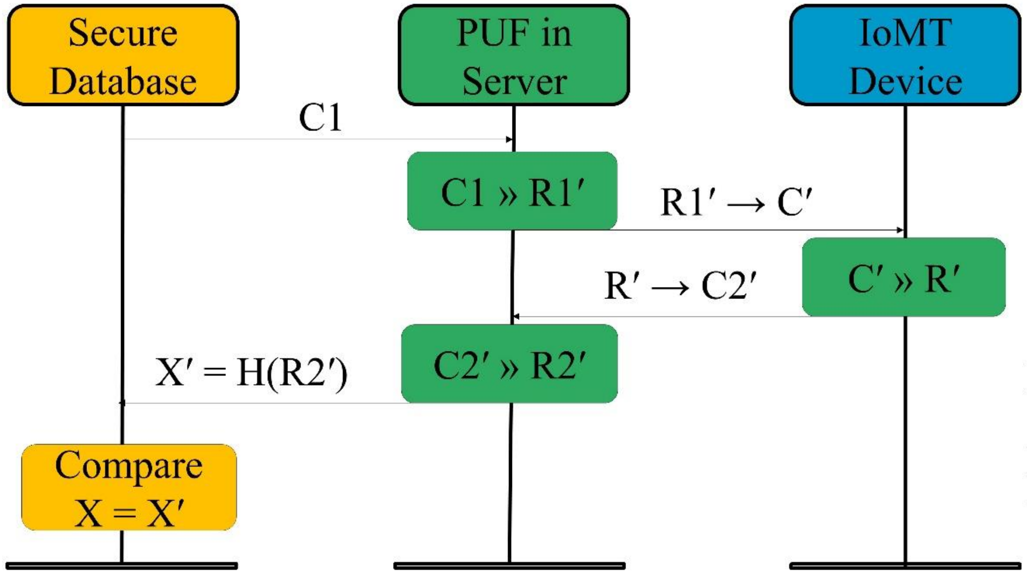


Authentication Phase

At the Doctor

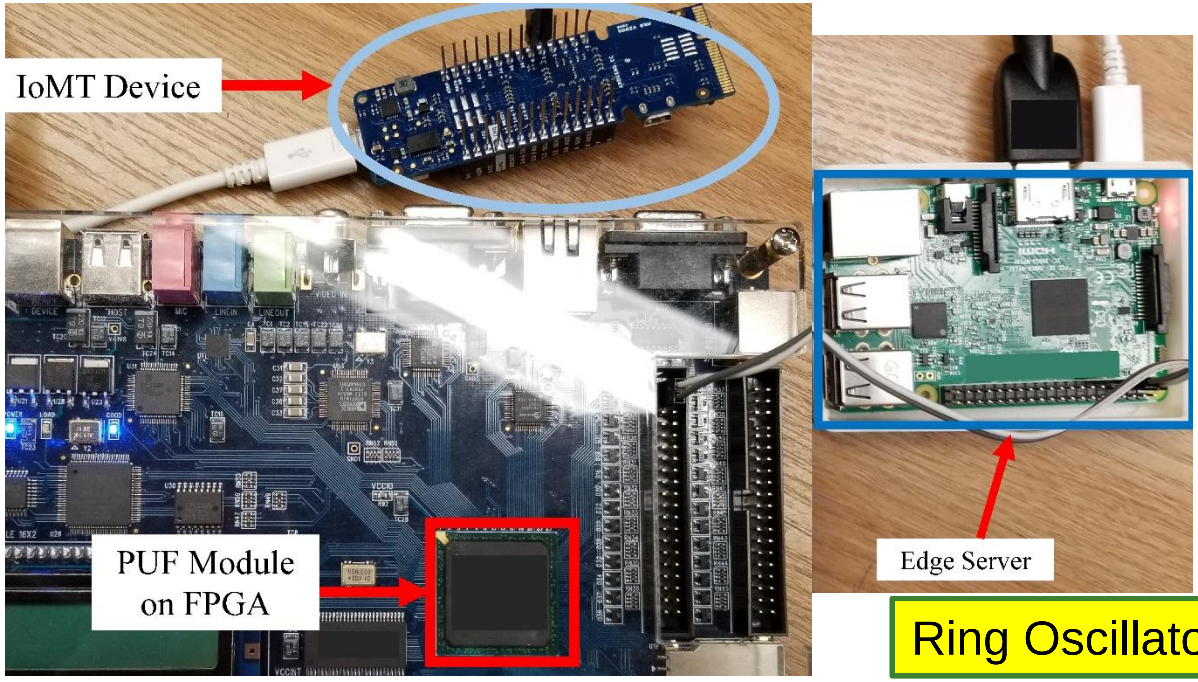
- When doctor needs to access an existing IoMT-device

Device Authentication Procedure



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

IoMT Security – Our Proposed PMsec



Average Power Overhead – 200 μW

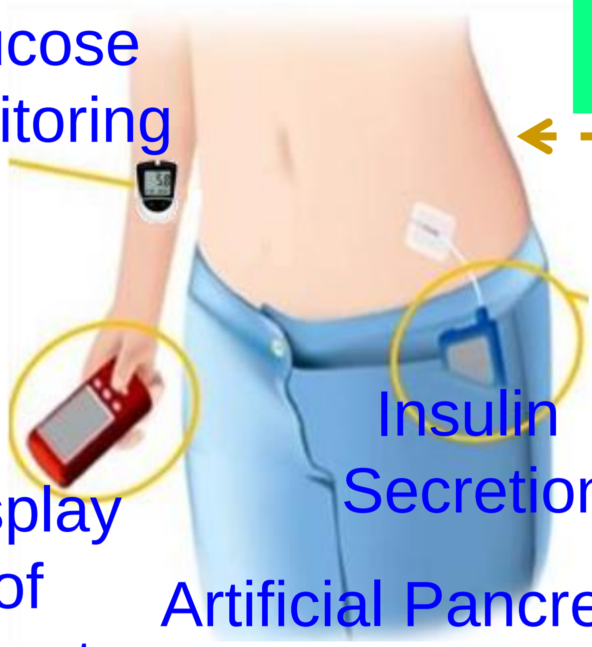
Ring Oscillator PUF – 64-bit, 128-bit, …

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

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

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

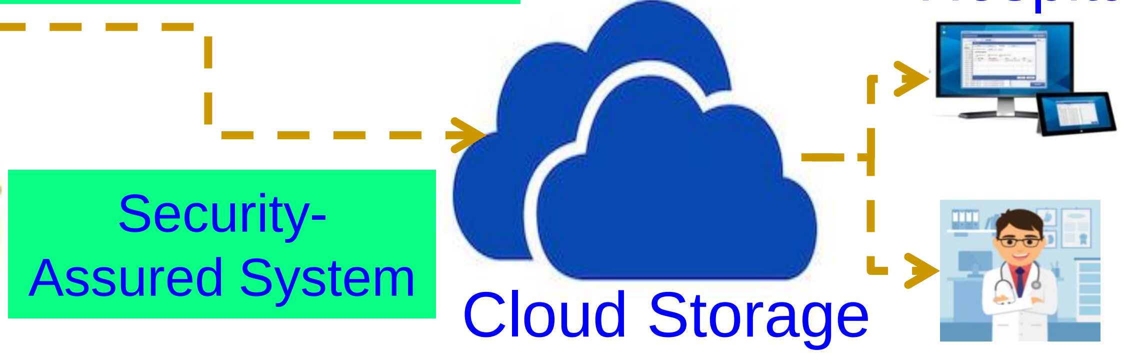
Continuous Glucose Monitoring



Display of Parameters

Insulin Secretion

Artificial Pancreases System (APS)



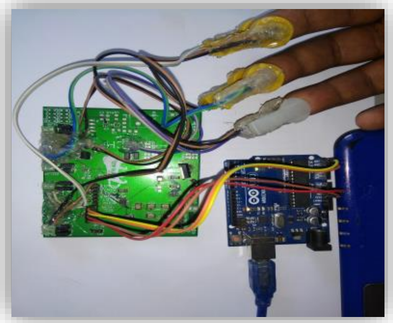
Privacy-Assured Health Data Storage

Security-Assured System

Cloud Storage

Hospital

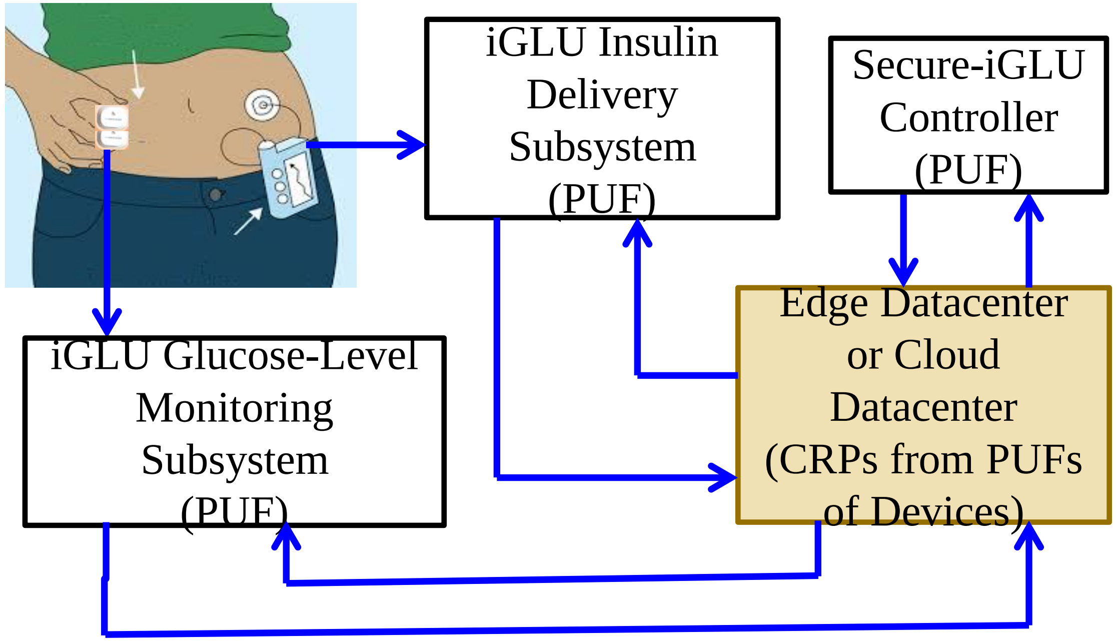
Doctor



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

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



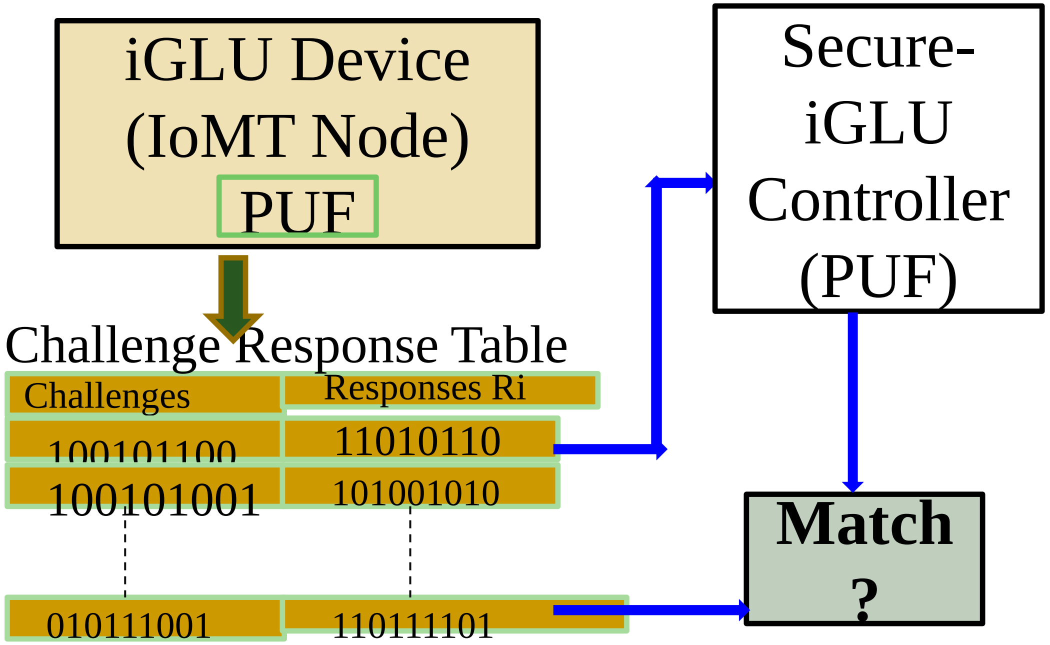
iGLU Insulin Delivery Subsystem (PUF)

Secure-iGLU Controller (PUF)

Edge Datacenter or Cloud Datacenter (CRPs from PUFs of Devices)

iGLU Glucose-Level Monitoring Subsystem (PUF)

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



iGLU Device (IoMT Node)

PUF

Challenge Response Table

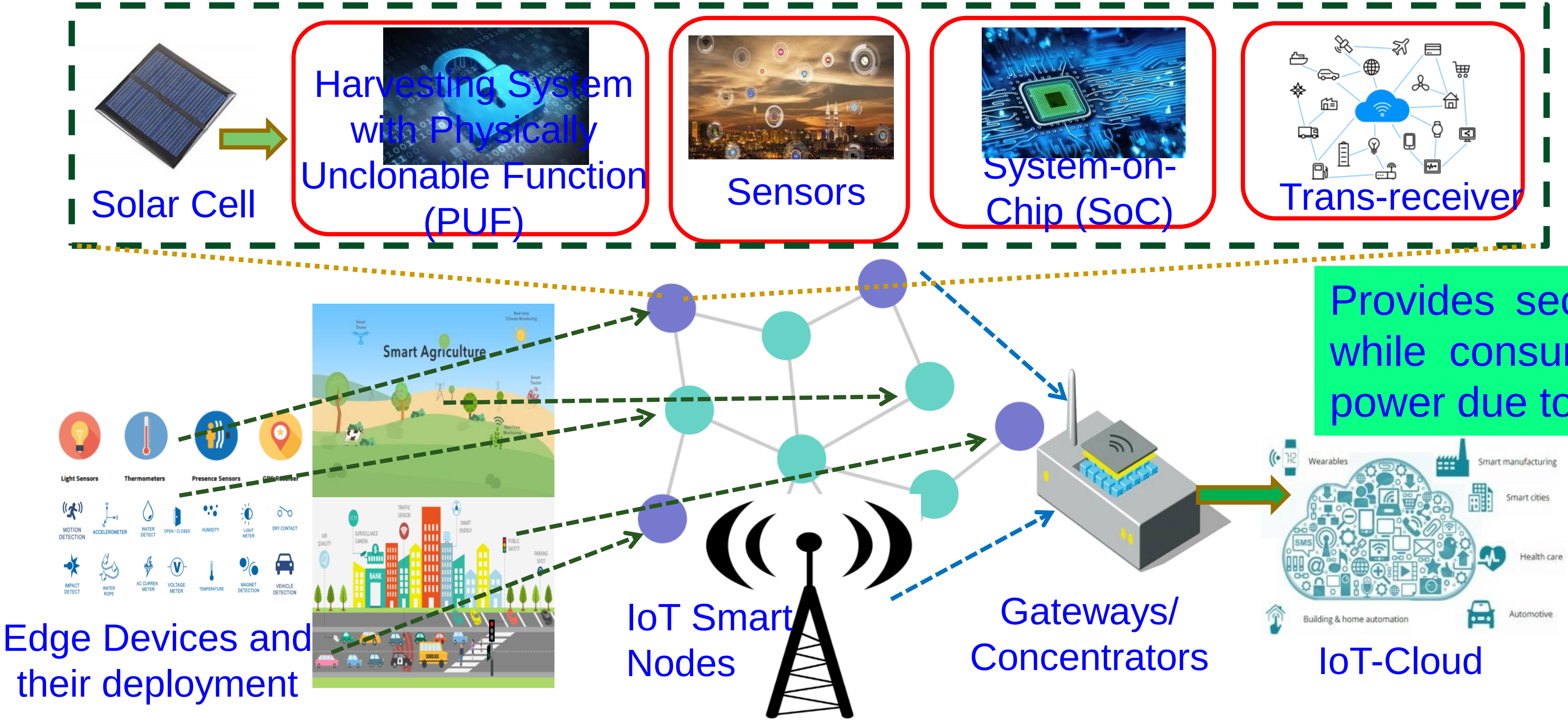
Challenges	Responses Ri
100101100	11010110
100101001	101001010
⋮	⋮
010111001	110111101

Secure-iGLU Controller (PUF)

Match ?

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

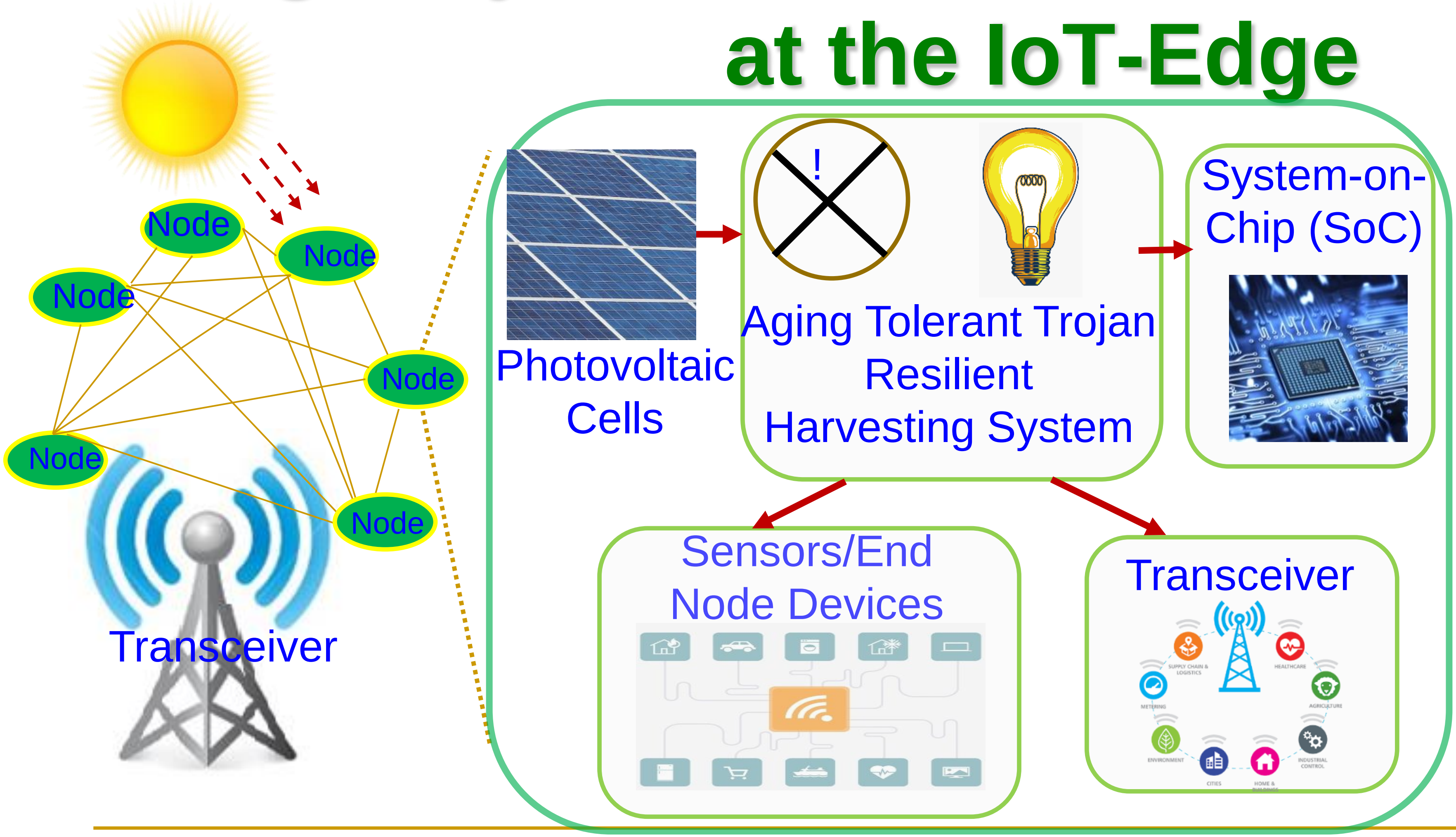
Our SbD: Eternal-Thing: Combines Security and Energy Harvesting at the IoT-Edge



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



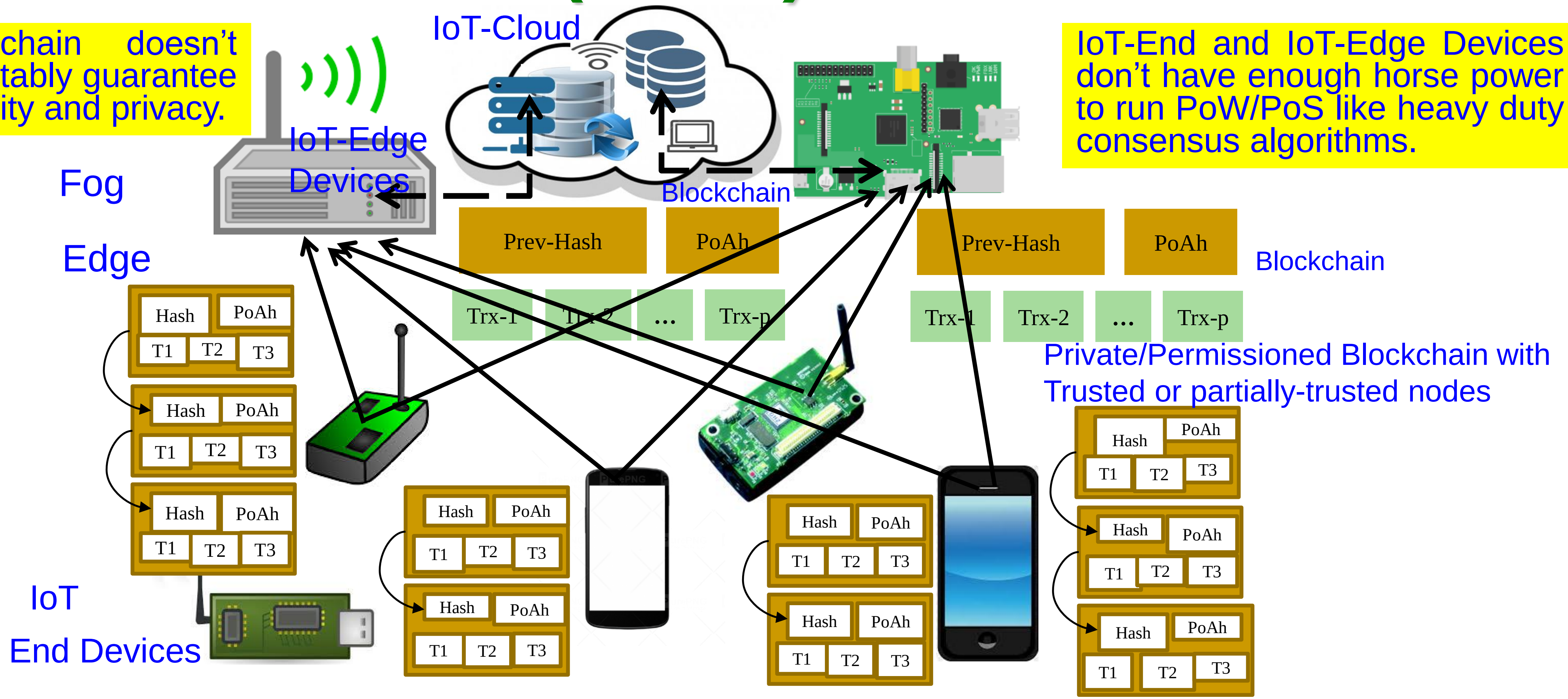
Provides security against analog-Trojan while consuming only 22 µW power due to harvesting.

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.

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

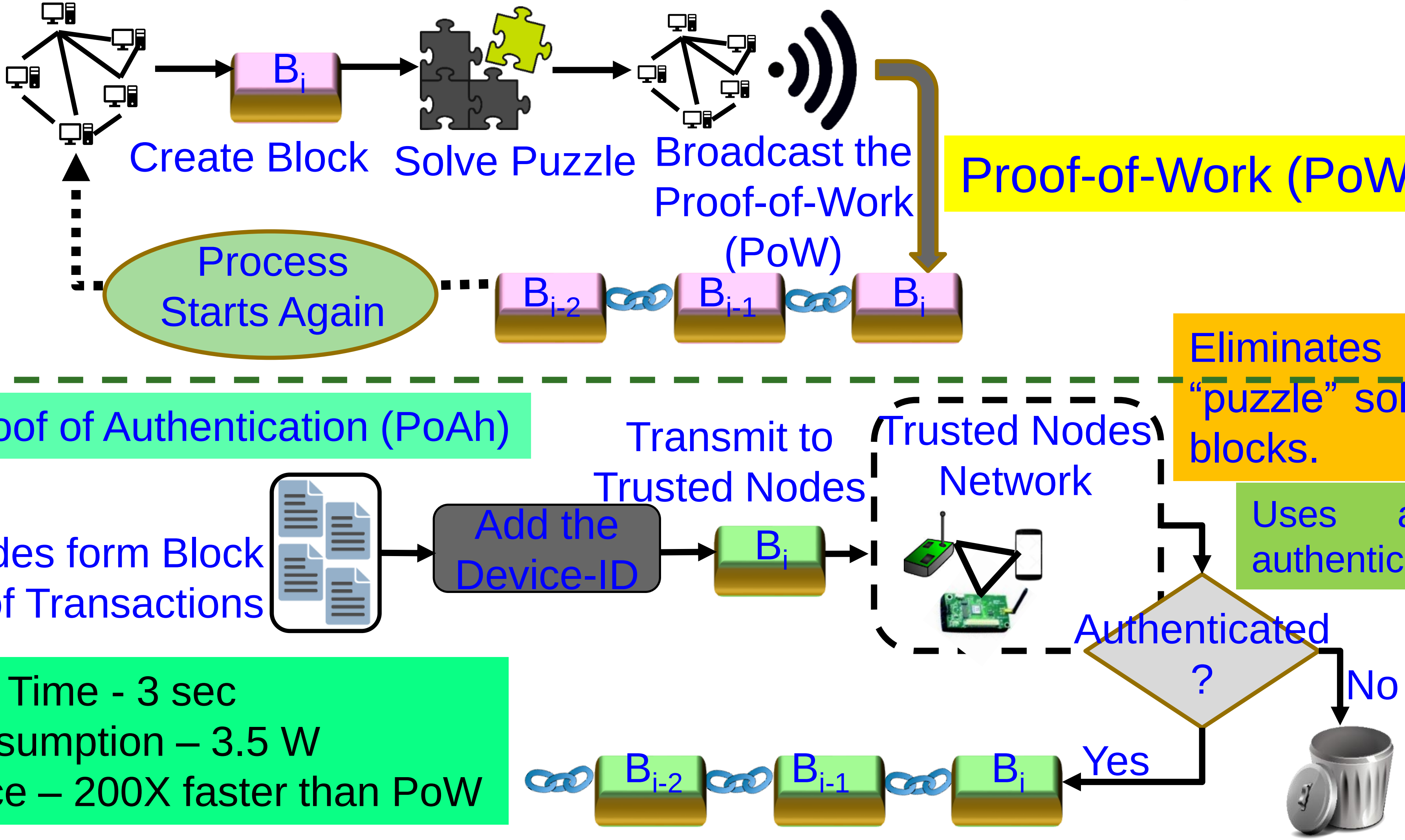
Blockchain doesn't inheritably guarantee security and privacy.

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



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

Our Proof-of-Authentication (PoAh)



Create Block B_i

Solve Puzzle

Broadcast the Proof-of-Work (PoW)

Process Starts Again

B_{i-2} B_{i-1} B_i

Proof-of-Work (PoW)

Eliminates cryptographic "puzzle" solving to validate blocks.

Proof of Authentication (PoAh)

Nodes form Block of Transactions

Add the Device-ID

Transmit to Trusted Nodes B_i

Trusted Nodes Network

Authenticated ?

No

Yes

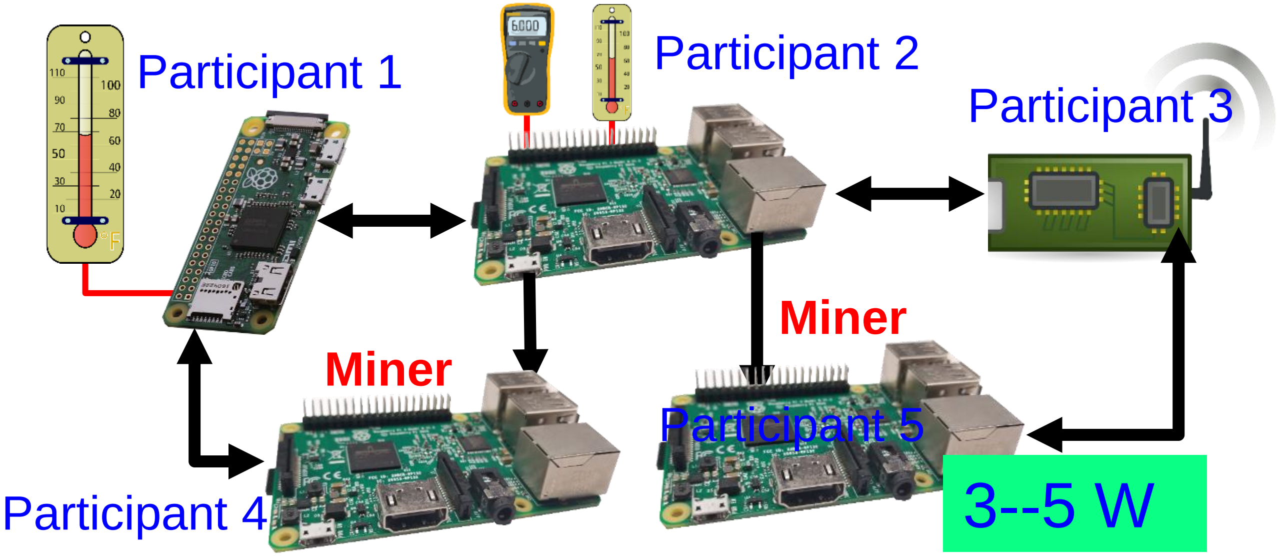
B_{i-2} B_{i-1} B_i

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 Runs in Resource Constrained Environment



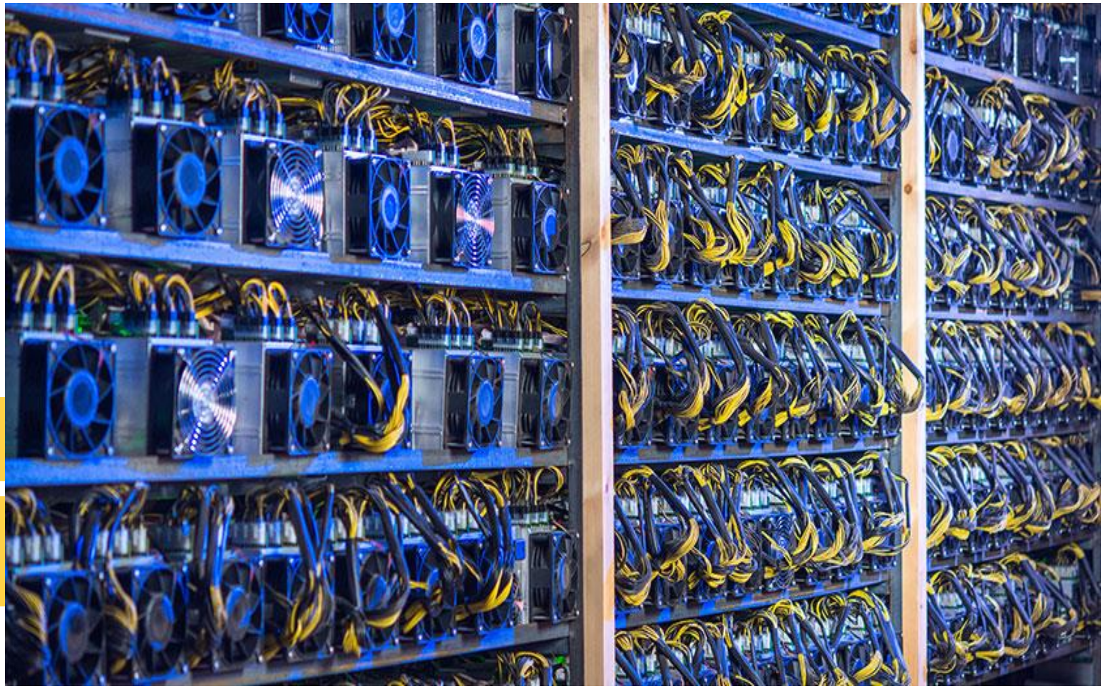
3--5 W

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

Blockchain using PoW Needs Significant Resource

500,0000 W

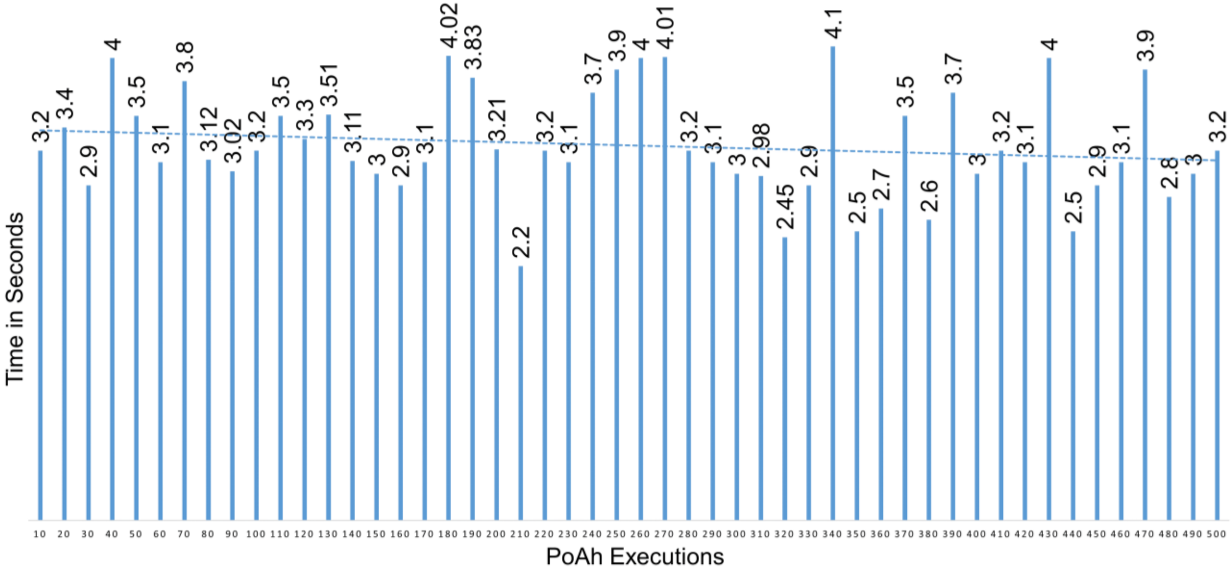
Source: D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks", *arXiv Computer Science*, arXiv:2001.07297, January 2020, 26-pages.



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

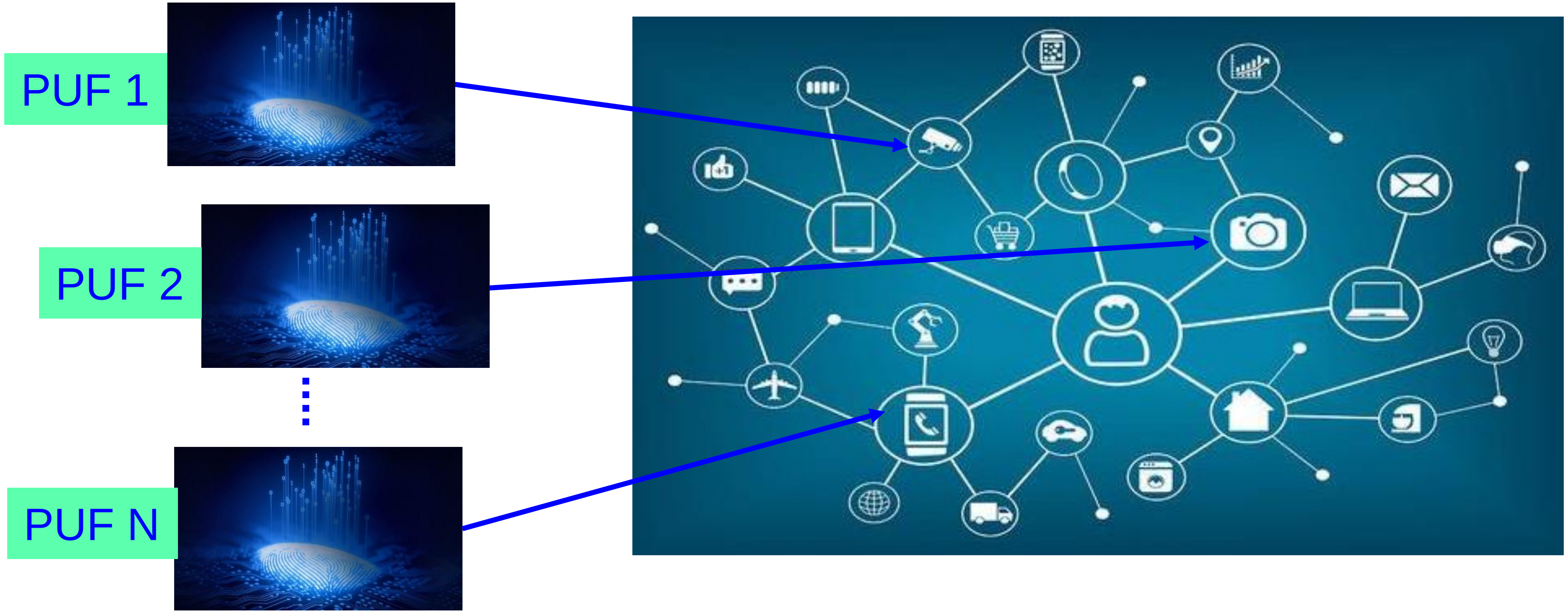
Consensus Algorithm	Blockchain Type	Prone To Attacks	Power Consumption	Time for Consensus
Proof-of-Work (PoW)	Public	Sybil, 51%	538 KWh	10 min
Proof-of-Stake (PoS)	Public	Sybil, DoS	5.5 KWh	
Proof-of-Authentication (PoAh)	Private	Not Known	3.5 W	3 sec



PoAh Execution for 100s of Nodes

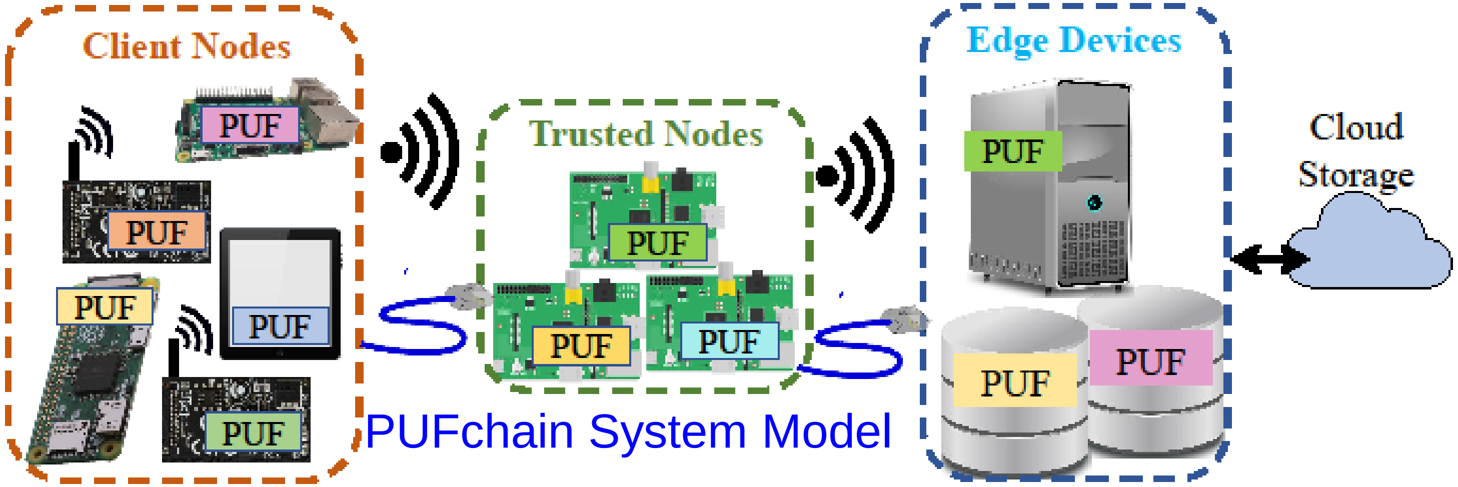
Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", in *Proc. 37th IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

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



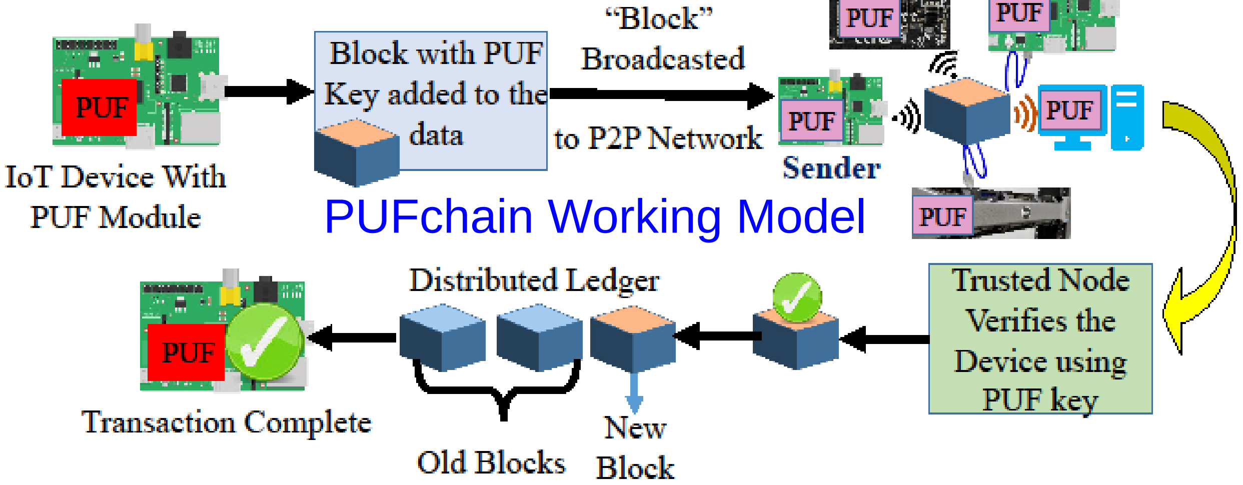
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, “PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security



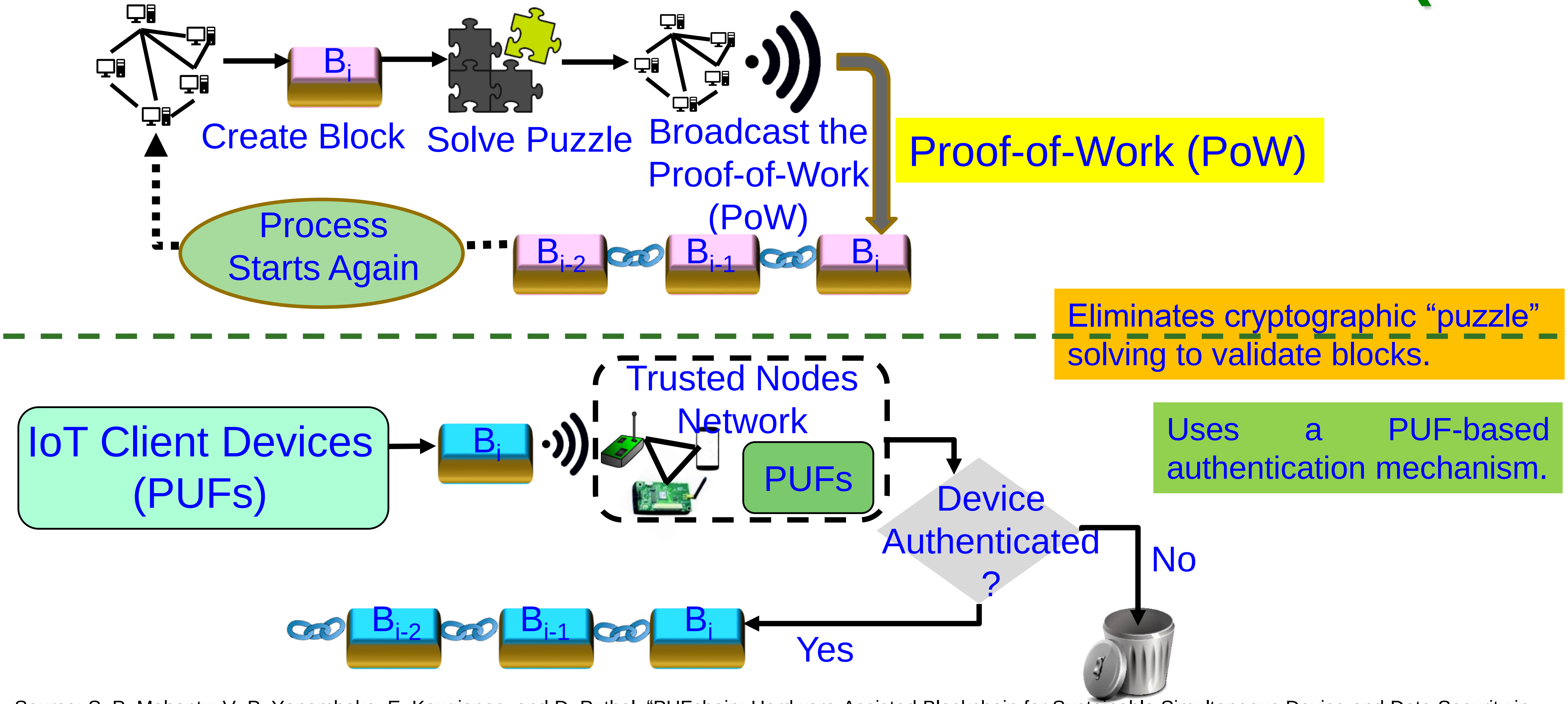
PUFchain Working Model

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

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

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

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



Create Block

Solve Puzzle

Broadcast the Proof-of-Work (PoW)

Process Starts Again

B_i

B_{i-2} B_{i-1} B_i

Proof-of-Work (PoW)

Eliminates cryptographic “puzzle” solving to validate blocks.

IoT Client Devices (PUFs)

Trusted Nodes Network

PUFs

Device Authenticated ?

No

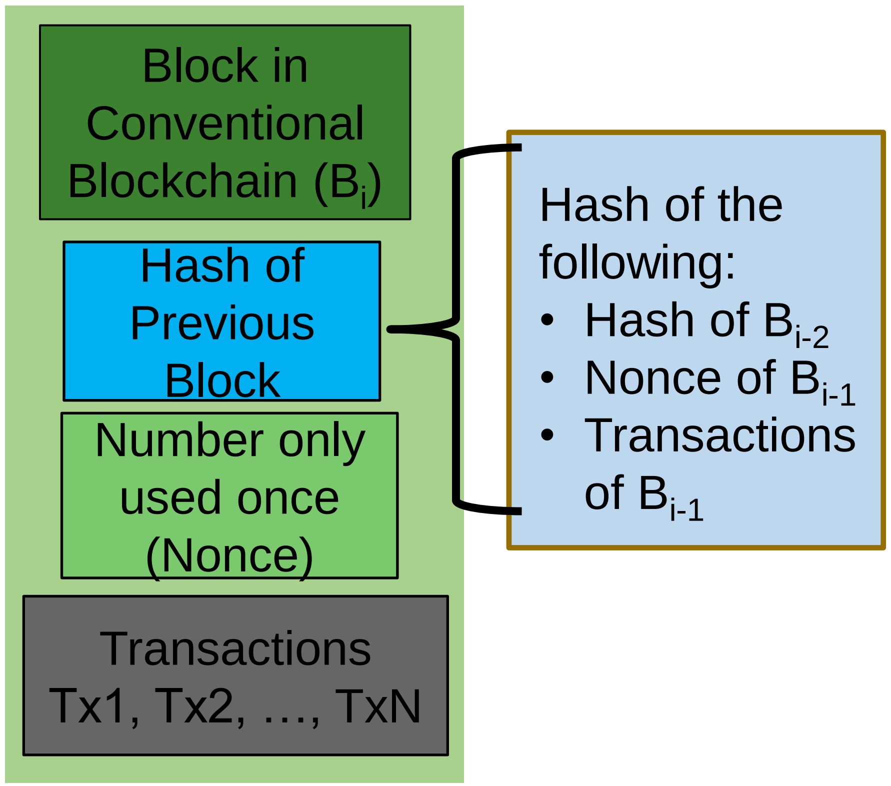
Yes

B_{i-2} B_{i-1} B_i

Uses a PUF-based authentication mechanism.

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

PUFchain: Proposed New Block Structure



Block in Conventional Blockchain (B_i)

Hash of Previous Block

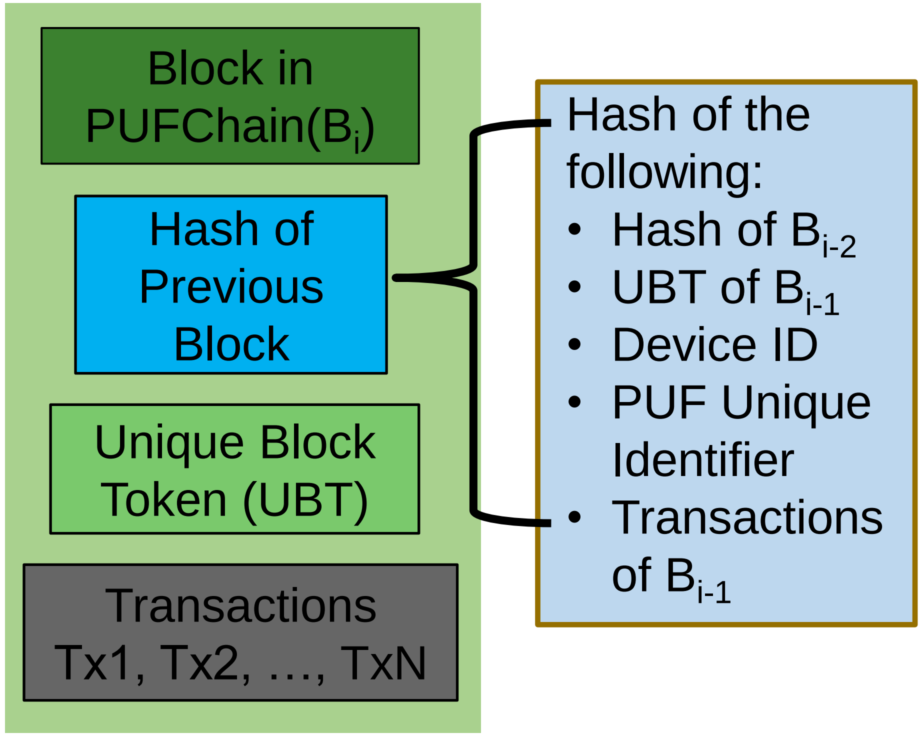
Number only used once (Nonce)

Transactions Tx1, Tx2, …, TxN

Hash of the following:

- Hash of B_{i-2}
- Nonce of B_{i-1}
- Transactions of B_{i-1}

Conventional Block Structure



Block in PUFChain(B_i)

Hash of Previous Block

Unique Block Token (UBT)

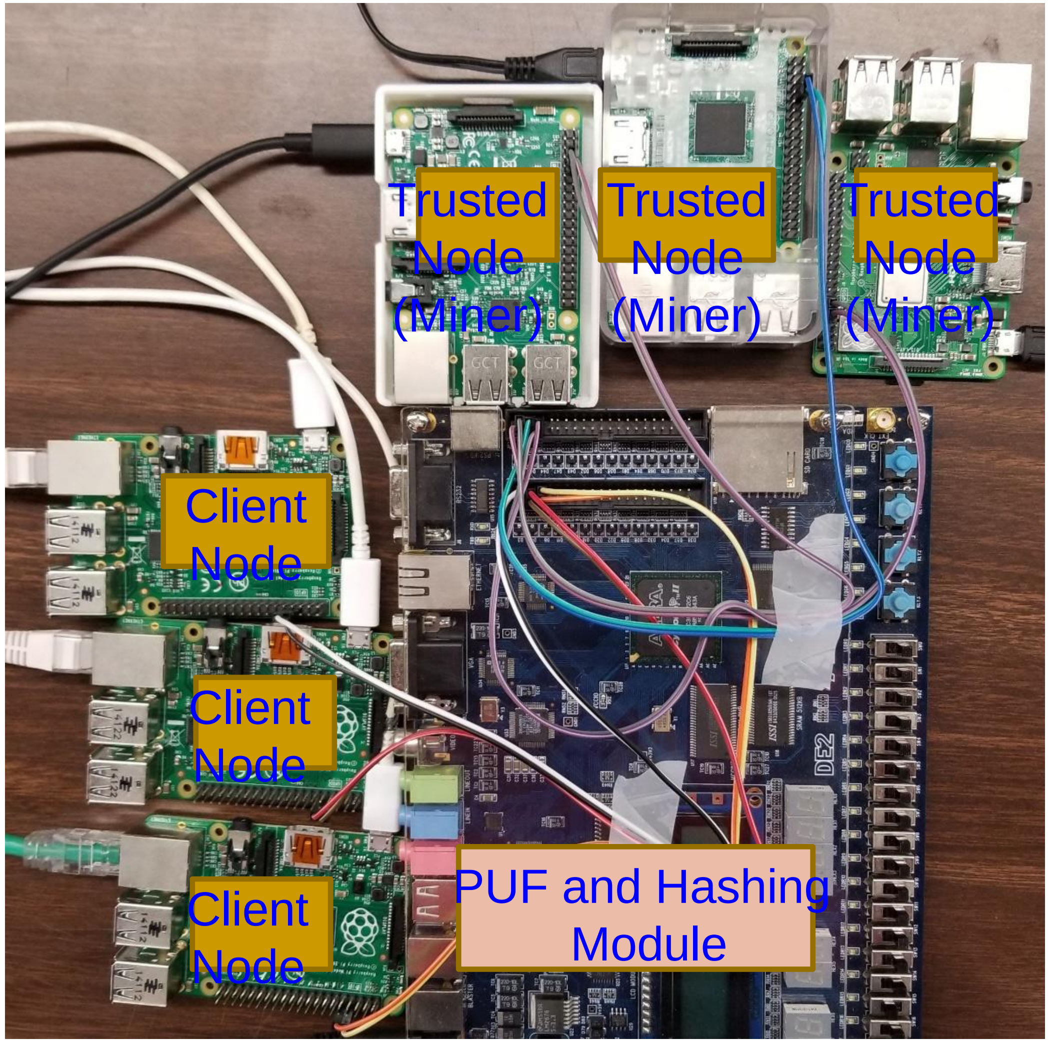
Transactions Tx1, Tx2, …, TxN

Hash of the following:

- Hash of B_{i-2}
- UBT of B_{i-1}
- Device ID
- PUF Unique Identifier
- Transactions of B_{i-1}

Proposed Block Structure for PUFchain

Our PoP is 1000X Faster than PoW



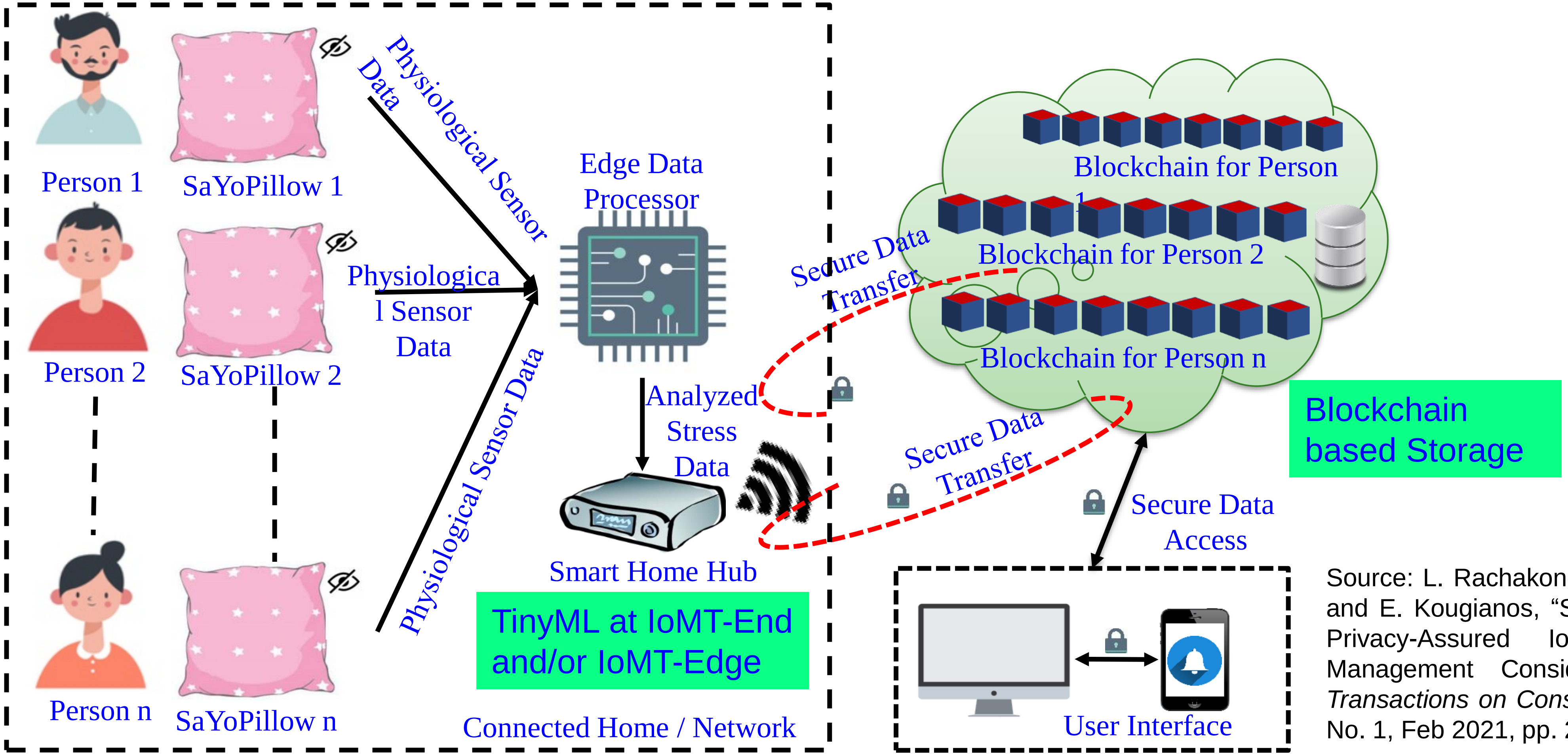
PoW - 10 min in cloud	PoAh – 950ms in Raspberry Pi	PoP - 192ms in Raspberry Pi
High Power	3 W Power	5 W Power

✓ PoP is 1,000X faster than PoW

✓ PoP is 5X faster than PoAh

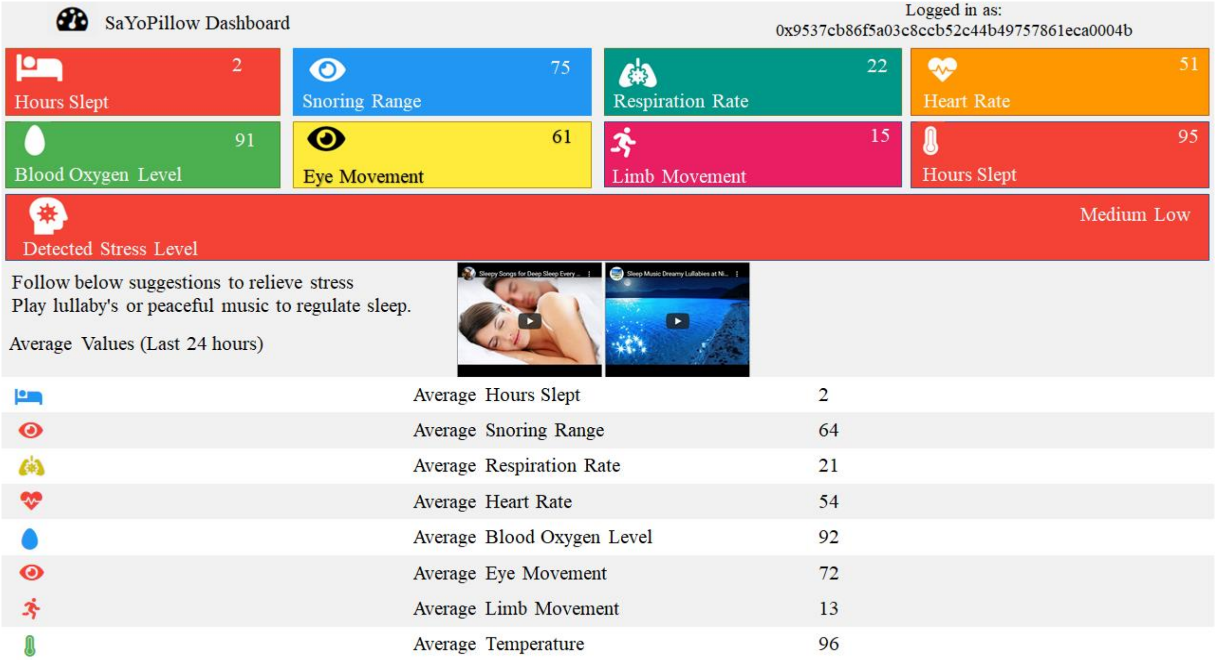
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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



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

SaYoPillow: Blockchain Results



SaYoPillow Dashboard

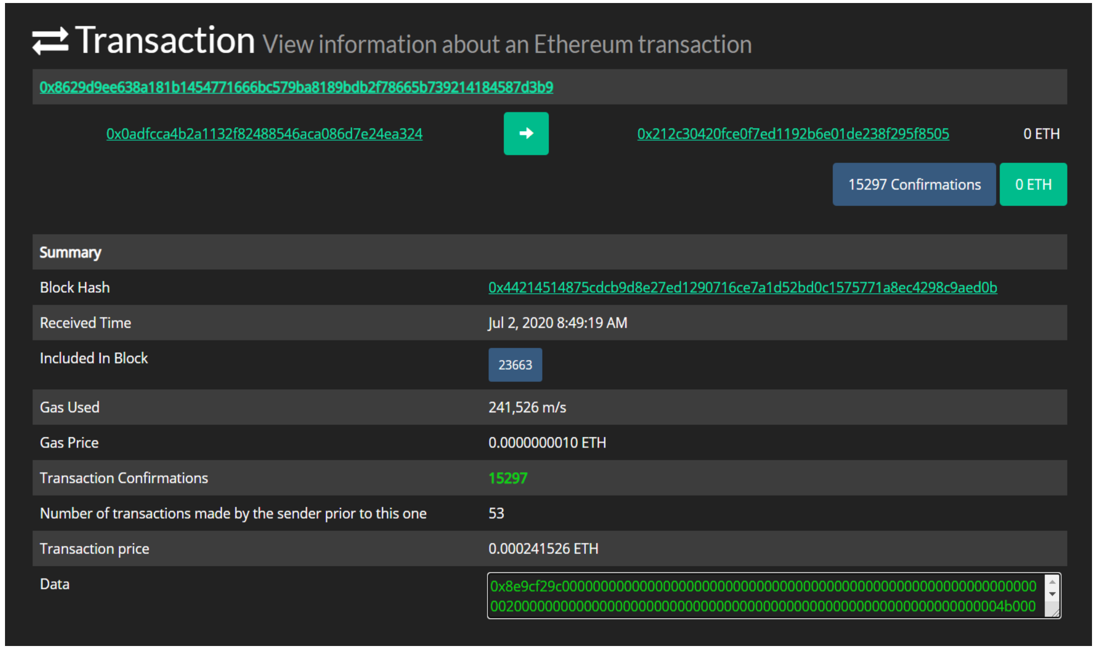
Logged in as:
0x9537cb86f5a03c8ccb52c44b49757861eca0004b

Hours Slept	2
Snoring Range	75
Respiration Rate	22
Heart Rate	51
Blood Oxygen Level	91
Eye Movement	61
Limb Movement	15
Hours Slept	95
Detected Stress Level	Medium Low

Follow below suggestions to relieve stress
Play lullaby's or peaceful music to regulate sleep.

Average Values (Last 24 hours)

Average Hours Slept	2
Average Snoring Range	64
Average Respiration Rate	21
Average Heart Rate	54
Average Blood Oxygen Level	92
Average Eye Movement	72
Average Limb Movement	13
Average Temperature	96



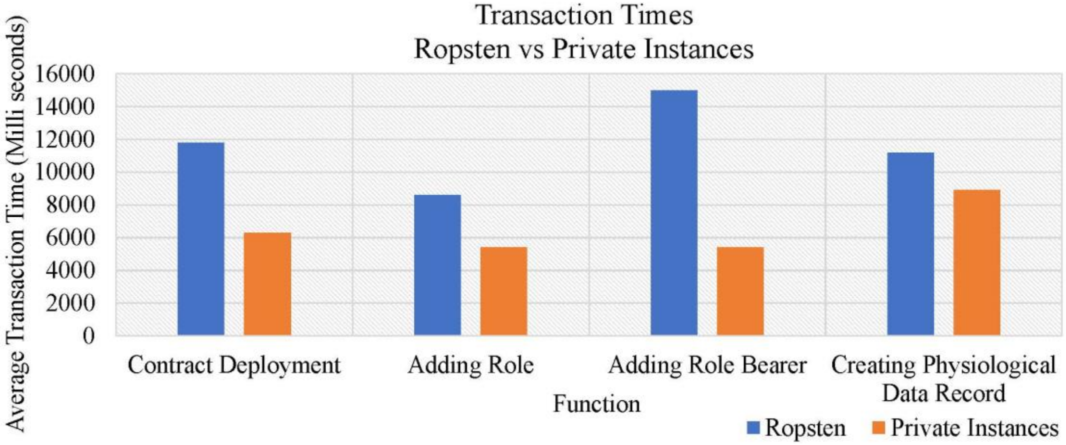
Transaction View information about an Ethereum transaction

0x8629d9ee638a181b1454771666bc579ba8189bdb2f78665b739214184587d3b9

0x0adfcca4b2a1132f82488546aca086d7e24ea324 → 0x212c30420fce0f7ed1192b6e01de238f295f8505 0 ETH

15297 Confirmations 0 ETH

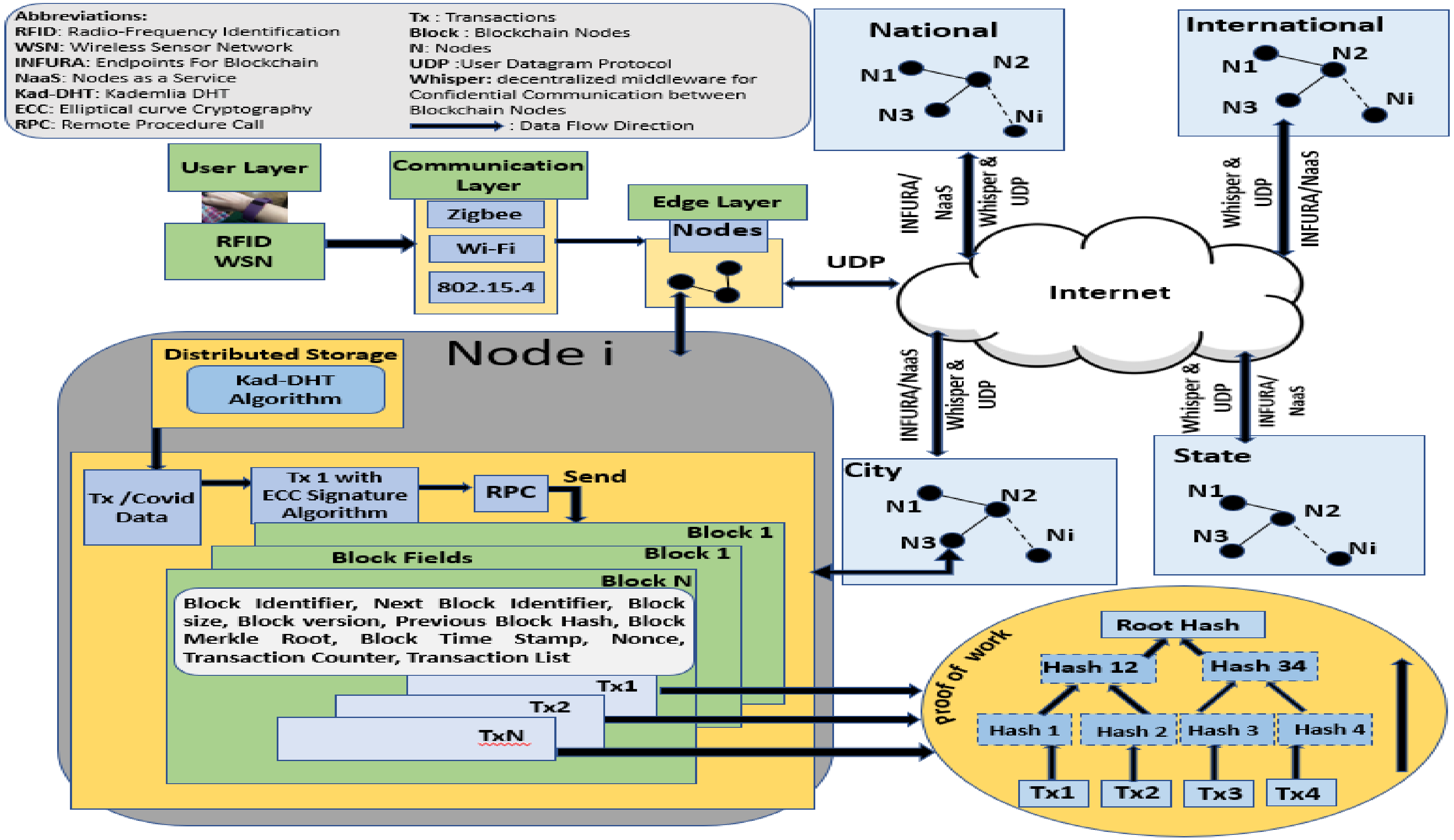
Summary	
Block Hash	0x44214514875cdcb9d8e27ed1290716ce7a1d52bd0c1575771a8ec4298c9aed0b
Received Time	Jul 2, 2020 8:49:19 AM
Included In Block	23663
Gas Used	241,526 m/s
Gas Price	0.0000000010 ETH
Transaction Confirmations	15297
Number of transactions made by the sender prior to this one	53
Transaction price	0.000241526 ETH
Data	0x8e9cf29c000000000000000000000000000000000000000000000000000000000000 002000000000000000000000000000000000000000000000000000000000000004b000



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.

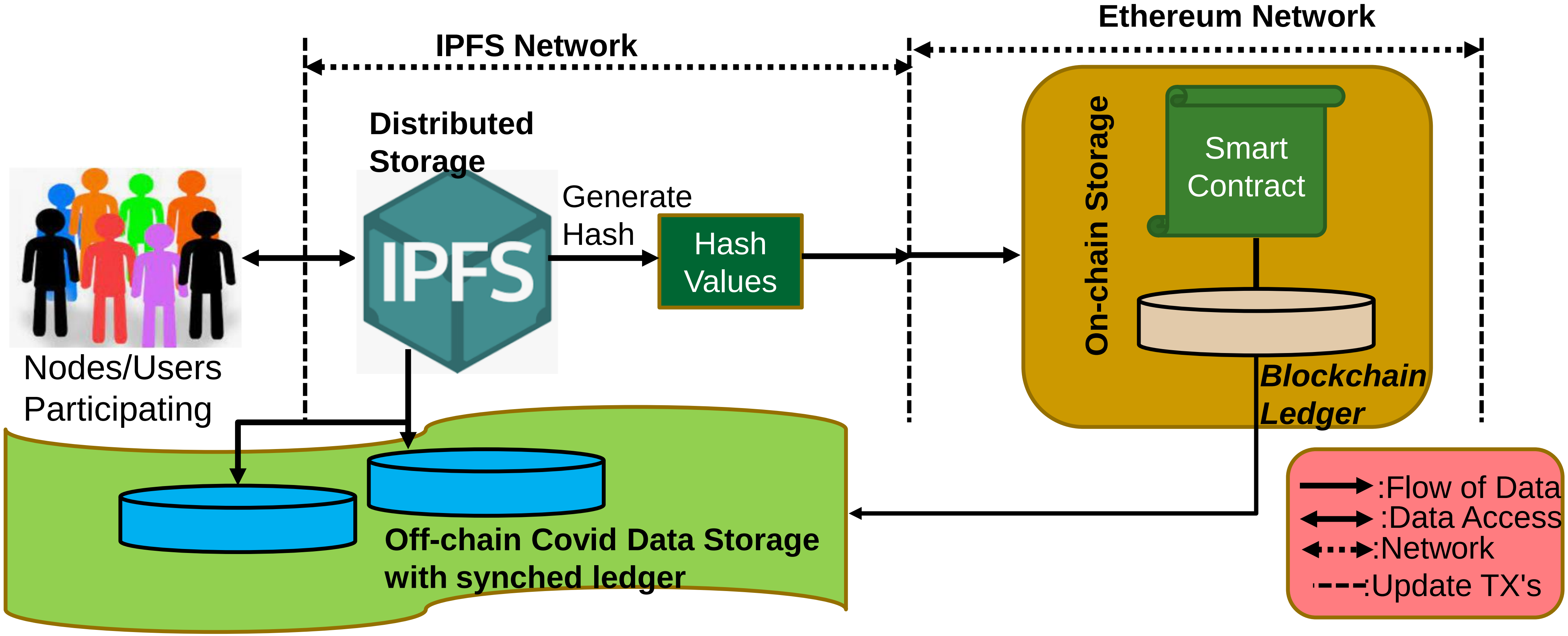
CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



Abbreviations:
RFID: Radio-Frequency Identification
WSN: Wireless Sensor Network
INFURA: Endpoints For Blockchain
NaaS: Nodes as a Service
Kad-DHT: Kademlia DHT
ECC: Elliptical curve Cryptography
RPC: Remote Procedure Call
Tx : Transactions
Block : Blockchain Nodes
N: Nodes
UDP :User Datagram Protocol
Whisper: decentralized middleware for Confidential Communication between Blockchain Nodes
→ : Data Flow Direction

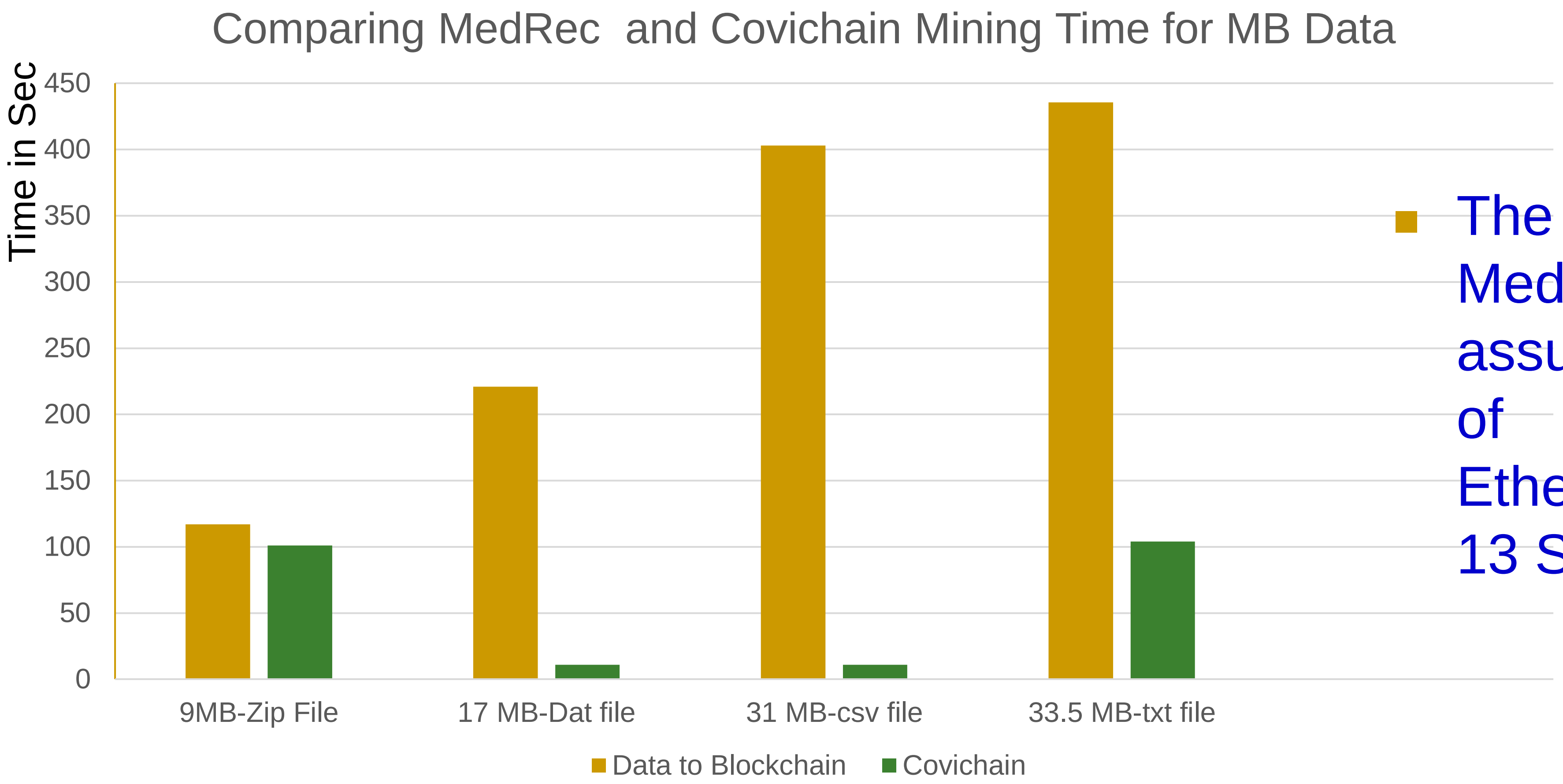
Source: S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems during Pandemic Outbreaks”, *Springer Nature Computer Science (SN-CS)*, Vol. 2, No. 2, June 2021, Article: 346, 16-pages.

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.

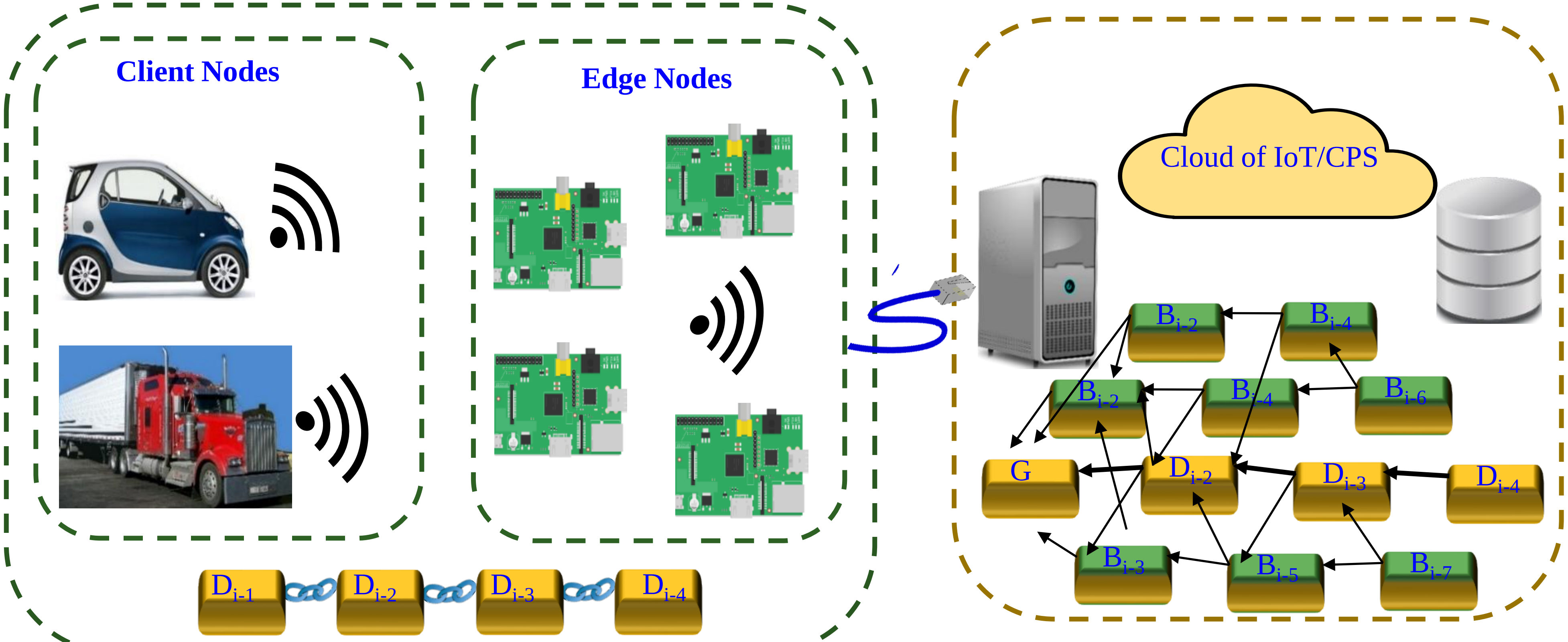
CoviChain: A Blockchain based Framework for Nonrepudiable Contact Tracing in H-CPS



- 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 Multi-Chain Technology to Enhance Blockchain Scalability



(a) Nodes-Chain (b) Multi-Blockchains

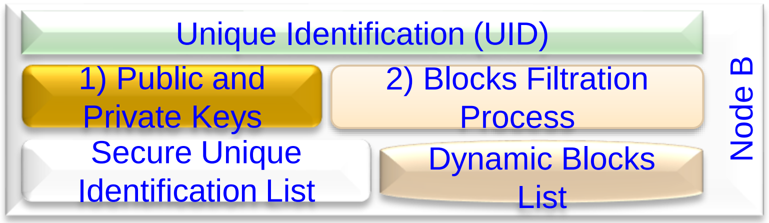
Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp.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

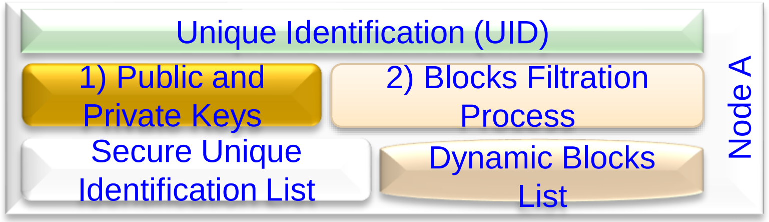
A Perspective of BC, Tangle Vs Our Multichain

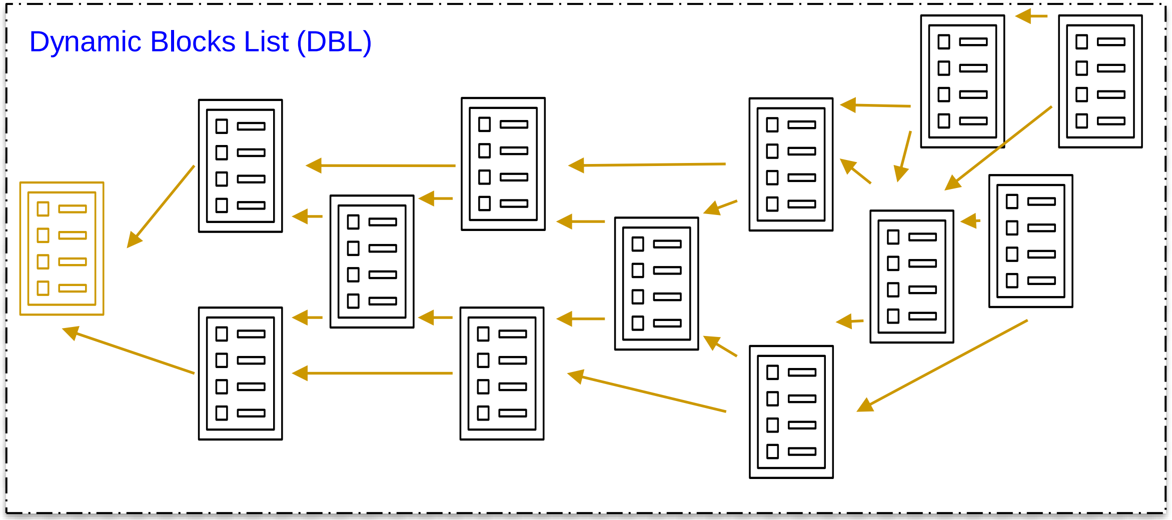
Features/Technology	Blockchain (Bitcoin)	Proof of Authentication	Tangle	HashGraph	McPoRA (current Paper)
Linked Lists	• One linked list of blocks. • Block of transactions.	• One linked list of blocks. • Block of transactions.	• DAG linked list. • One transaction.	• DAG linked List. • Container of transactions 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


Unique Identification (UID)
1) Public and Private Keys
2) Blocks Filtration Process
Secure Unique Identification List
Dynamic Blocks List
Node B


Unique Identification (UID)
1) Public and Private Keys
2) Blocks Filtration Process
Secure Unique Identification List
Dynamic Blocks List
Node A



Secure Unique Identification List (SUIL)

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

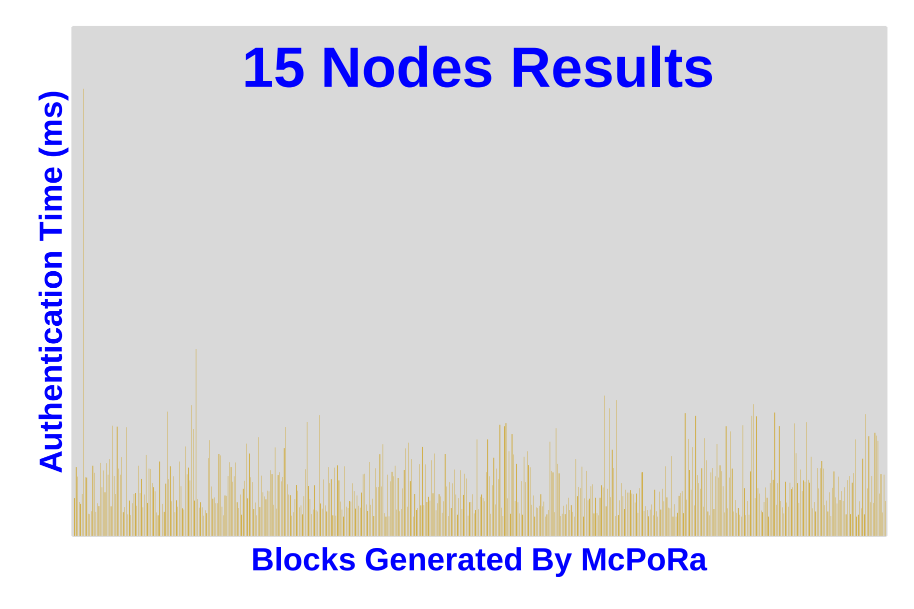
Hashed
Node A Unique Identification (UID)
Node B Unique Identification (UID)
Node C Unique Identification (UID)
Node D Unique Identification (UID)
Node E Unique Identification (UID)
Node F Unique Identification (UID)
Node G Unique Identification (UID)
Node H Unique Identification (UID)
Node I Unique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

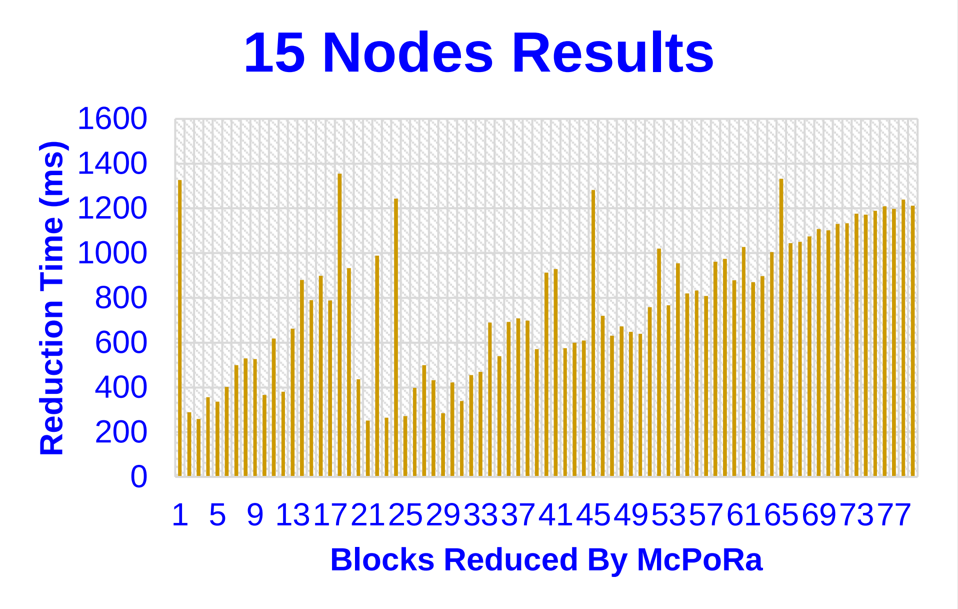
Consensus Time – 0.7 sec (Avg)
Power Consumption – 3.5 W
Performance – 4000X faster than PoW

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.

McPoRA – Experimental Results

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

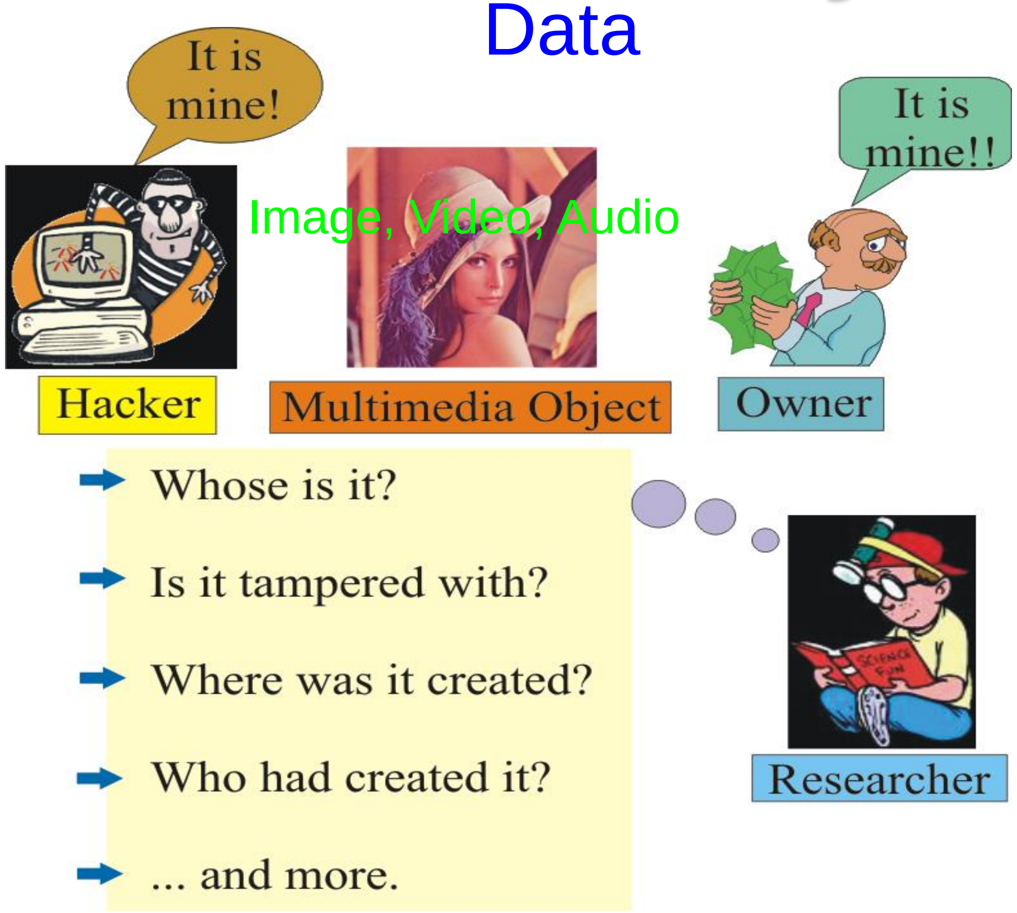




Source: A. J. Alkhodair, S. P. Mohanty, E. Kougianos, and D. Puthal, “McPoRA: A Multi-Chain Proof of Rapid Authentication for Post-Blockchain based Security in Large Scale Complex Cyber-Physical Systems”, in *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp.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

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

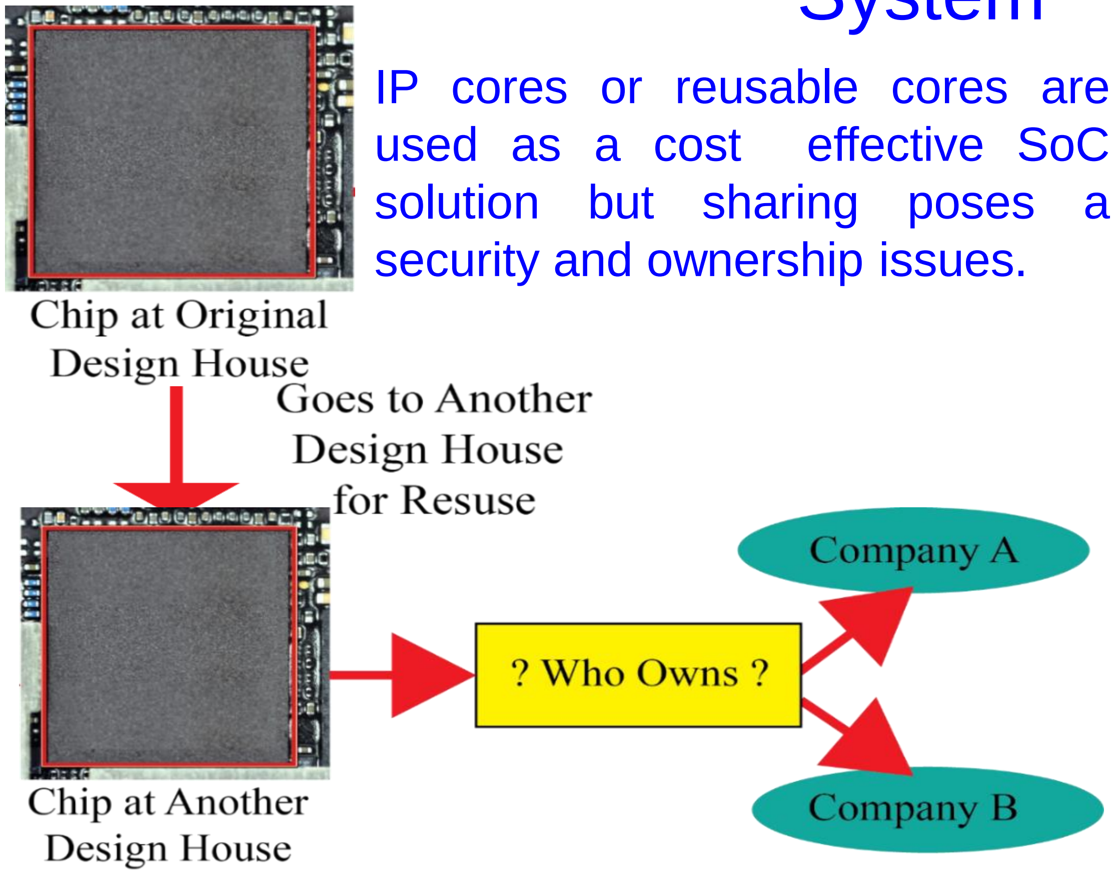
Data



- Whose is it?
- Is it tampered with?
- Where was it created?
- Who had created it?
- ... and more.

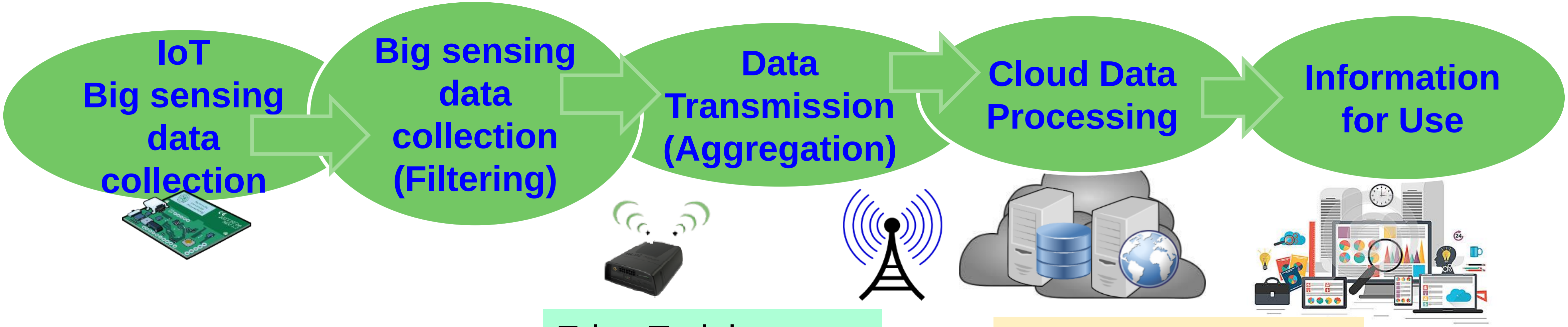
System

IP cores or reusable cores are used as a cost effective SoC solution but sharing poses a security and ownership issues.


Chip at Original Design House
Goes to Another Design House for Resuse
Chip at Another Design House
? Who Owns ?
Company A
Company B

Source: S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougianos, "Everything You Want to Know About Watermarking", *IEEE Consumer Electronics Magazine (CEM),* Volume 6, Issue 3, July 2017, pp. 83--91.

Data Quality Assurance in IoT/CPS



IoT Big sensing data collection

Big sensing data collection (Filtering)

Data Transmission (Aggregation)

Cloud Data Processing

Information for Use

Edge Training:

- Data Signature
- Model Signature

Cloud Training:

- Data Signature
- Model Signature

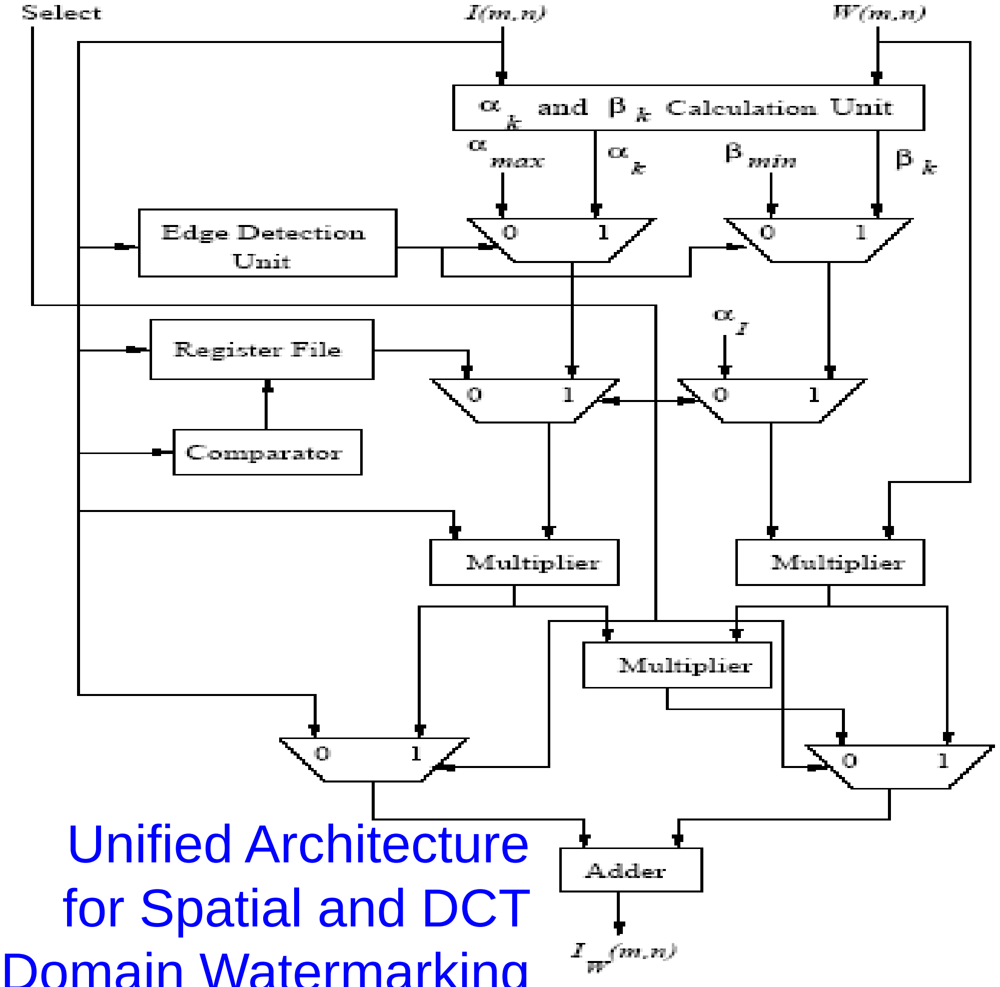
Fake Data Defense:

- Stop (Shield)
- Detect

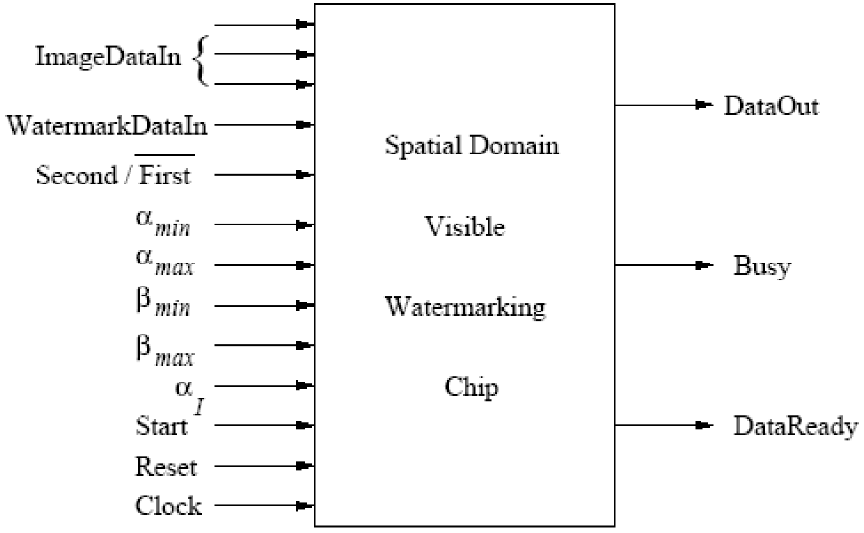
Secure data curation a solution for fake data?

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

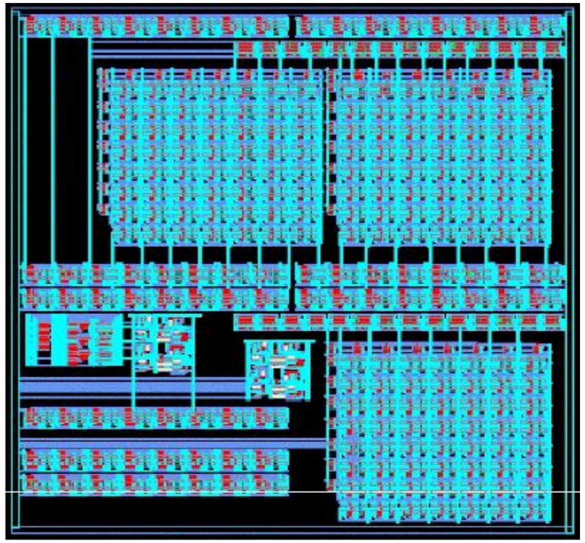
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

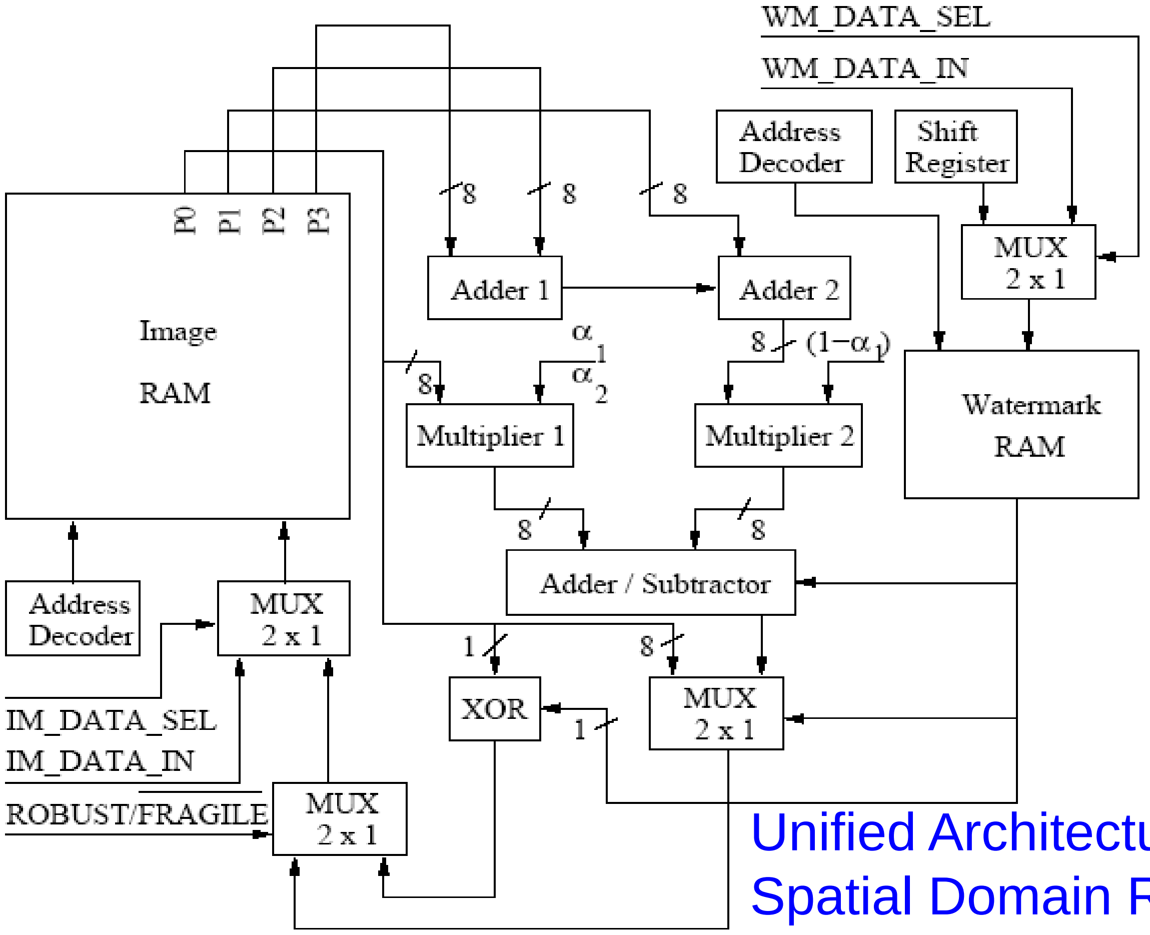
Chip Design Data

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

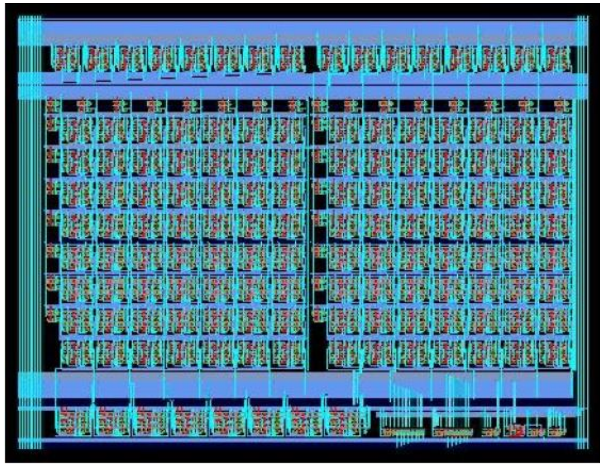
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

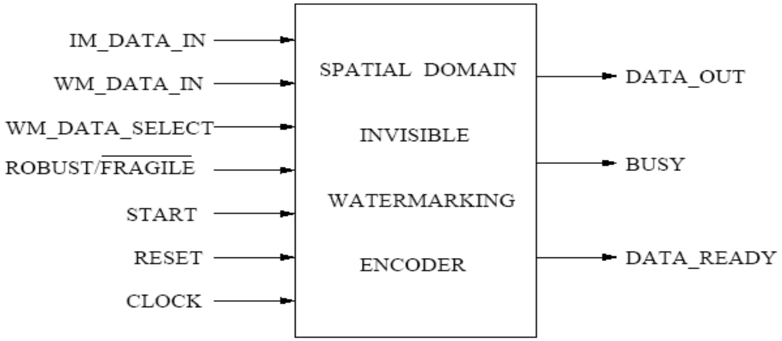
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

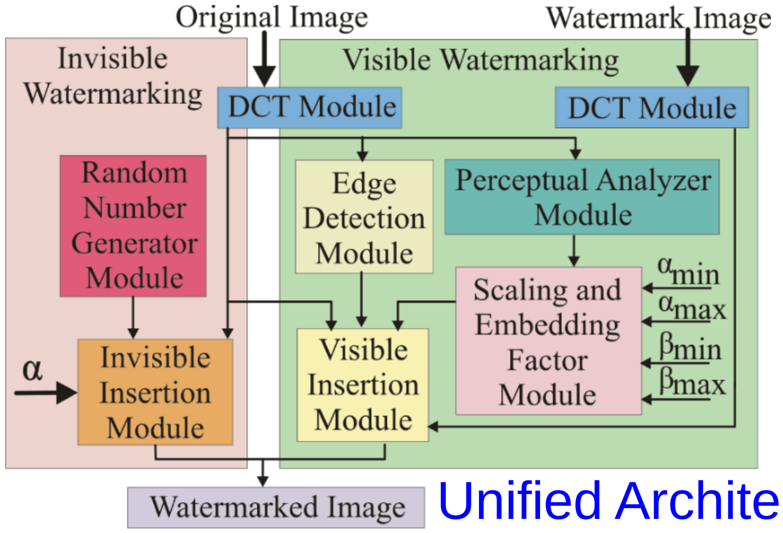
Chip Design Data

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

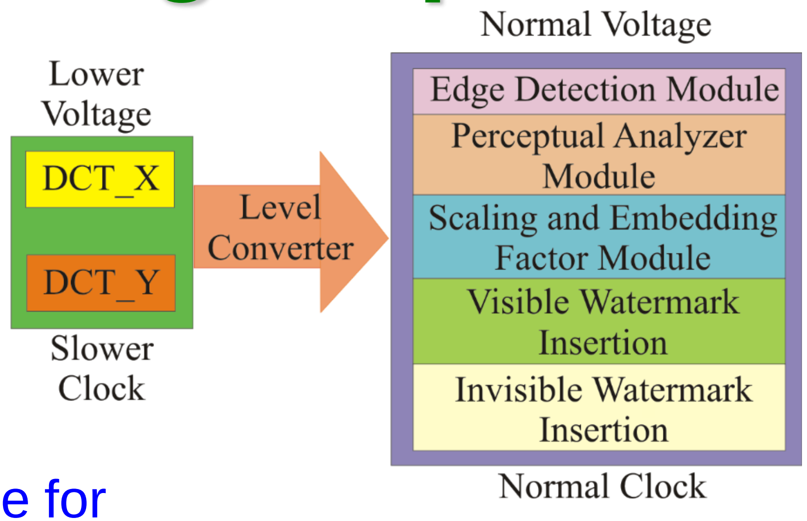
Power Consumption: 2.0 mW, Frequency: 500 MHz

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

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

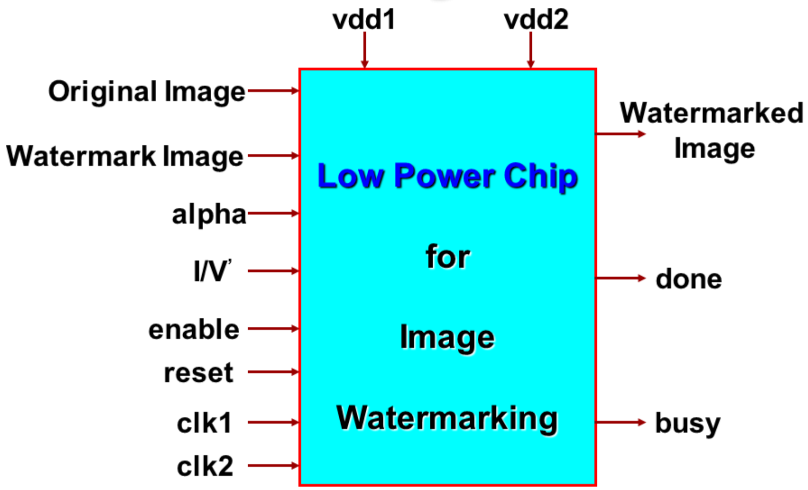


Unified Architecture for DCT Domain Watermarking

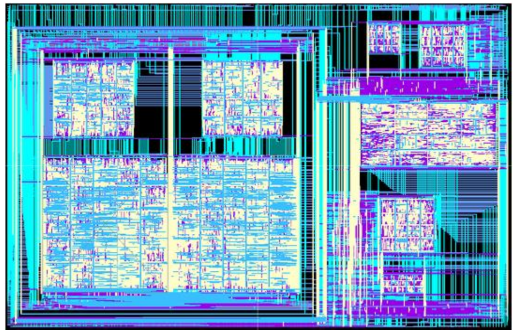


Lower Voltage
DCT_X
DCT_Y
Slower Clock
Level Converter
Normal Voltage
Edge Detection Module
Perceptual Analyzer Module
Scaling and Embedding Factor Module
Visible Watermark Insertion
Invisible Watermark Insertion
Normal Clock

DVDF Low-Power Design



Pin Diagram



Chip Layout

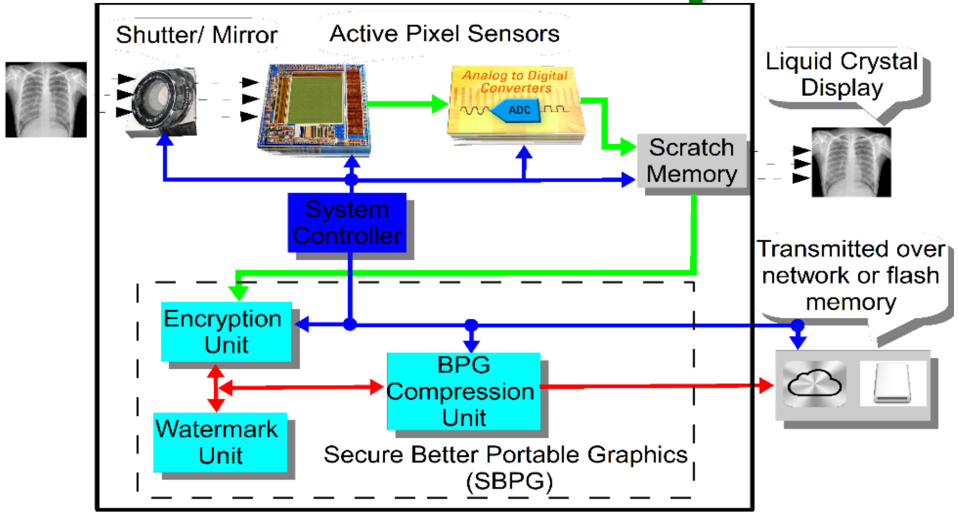
Chip Design Data

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

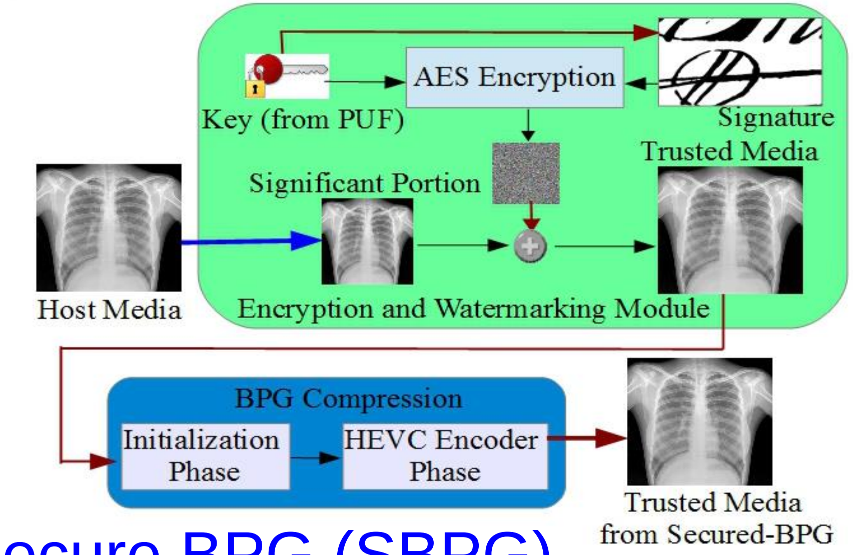
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V

Source: S. P. Mohanty, N. Ranganathan, and K. Balakrishnan, "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain", *IEEE Transactions on Circuits and Systems II (TCAS-II)*, Vol. 53, No. 5, May 2006, pp. 394-398.

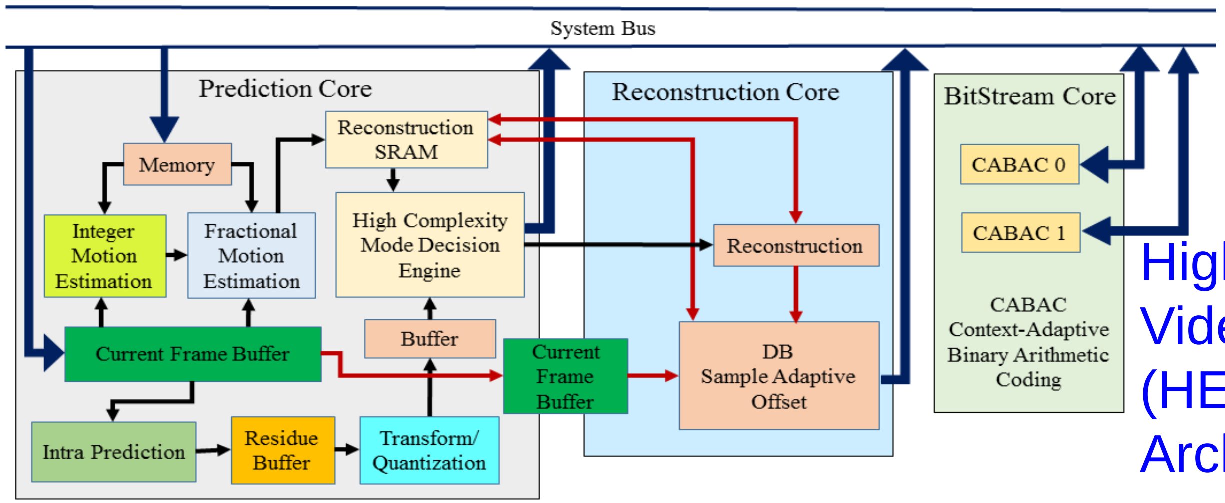
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)



High-Efficiency Video Coding (HEVC) Architecture

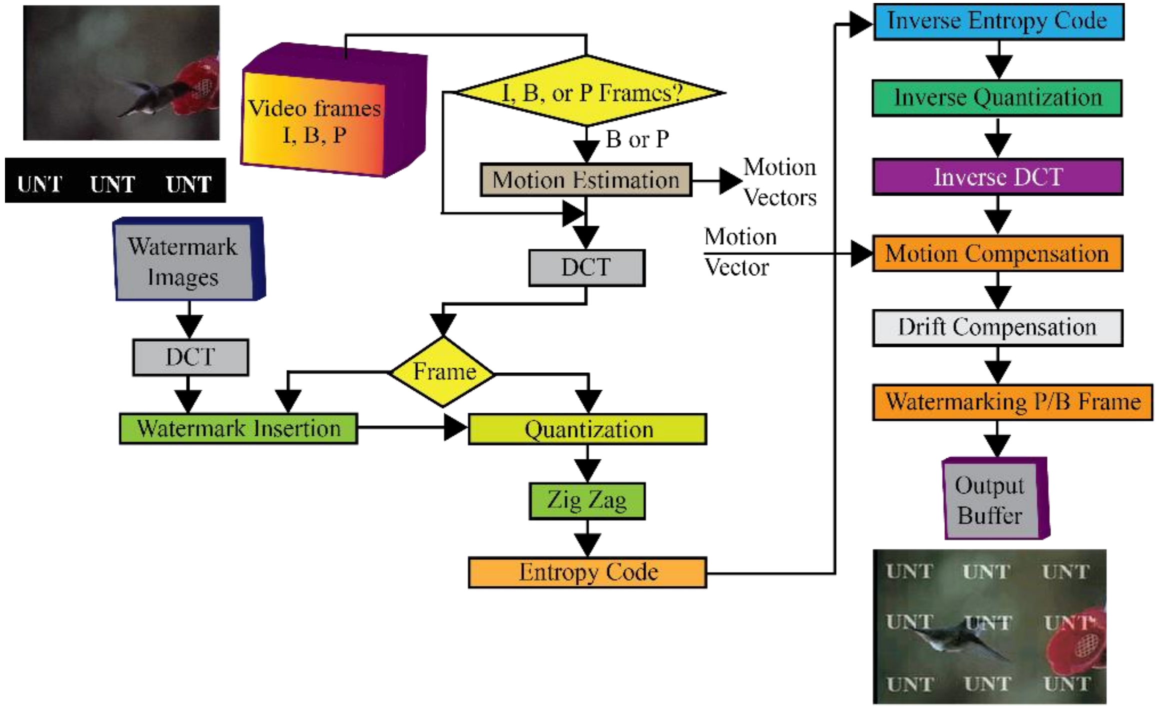
Simulink Prototyping

Throughput: 44 frames/sec

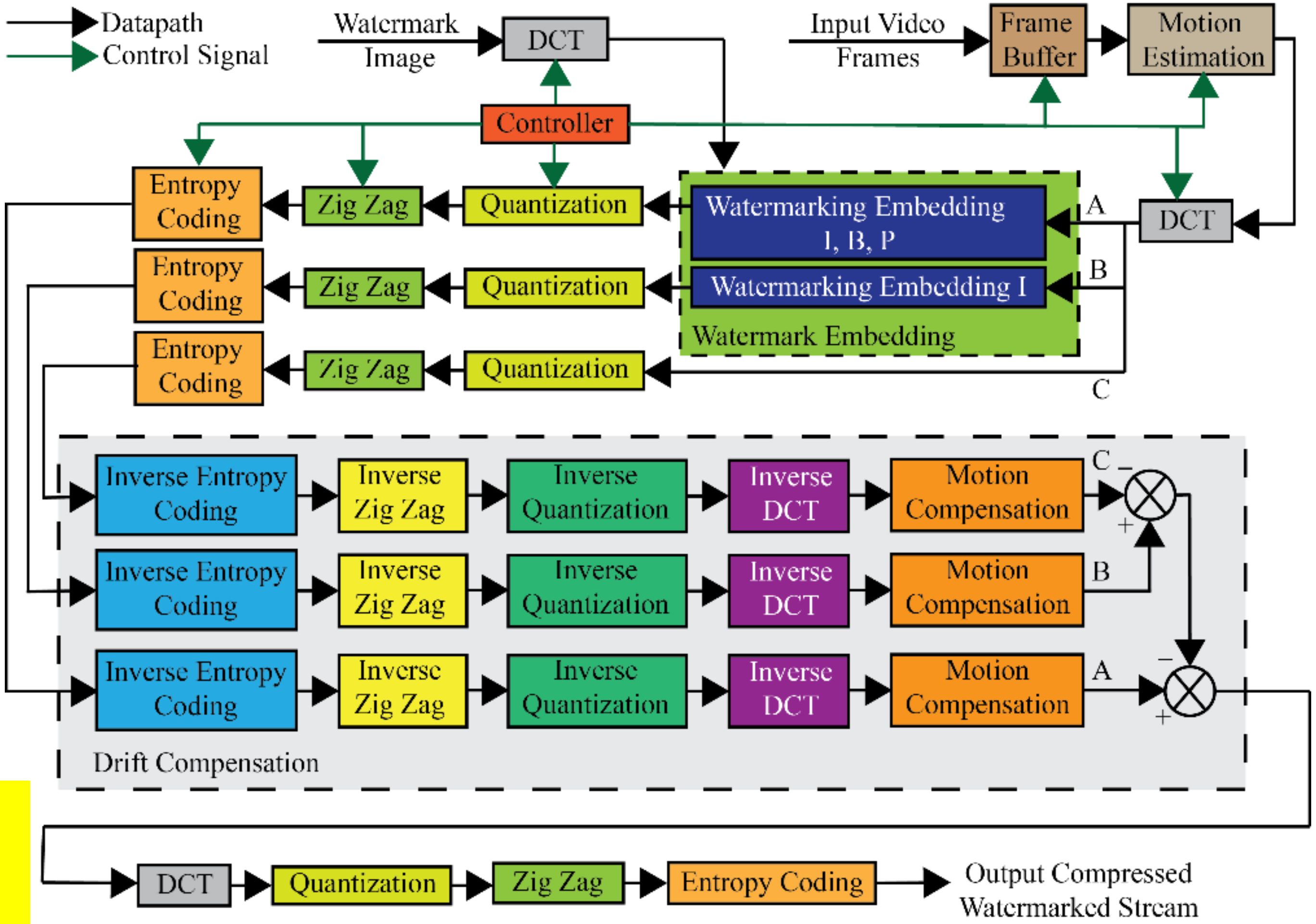
Power Dissipation: 8 nW

Source: S. P. Mohanty, E. Kougianos, and P. Guturu, "SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT (Invited Paper)", *IEEE Access Journal*, Volume 6, 2018, pp. 5939--5953.

Our Hardware for Real-Time Video Watermarking



(a) Video Watermarking Algorithm as a Flow Chart



(b) Architecture of the Video Watermrking Algorithm

FPGA based Design Data

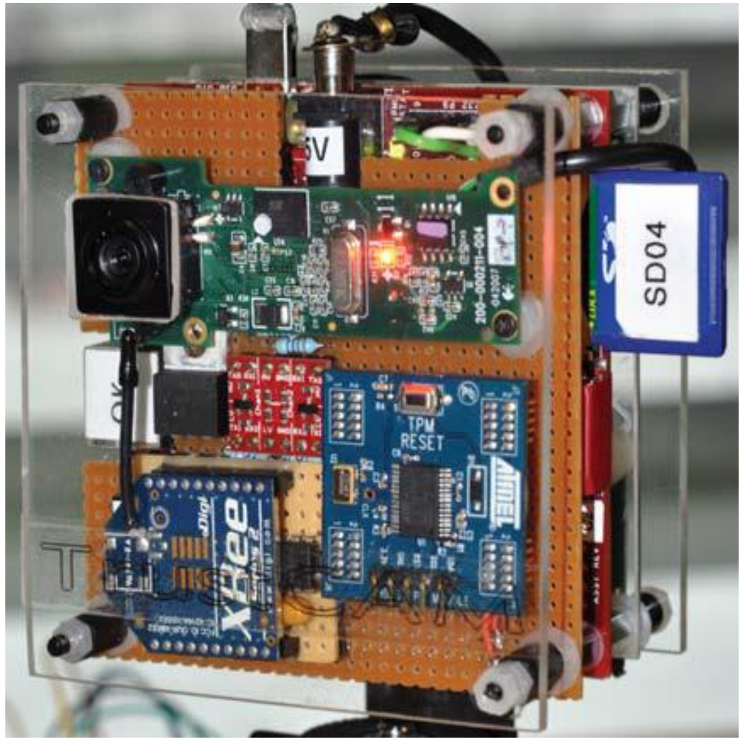
Resource: 28322 LE, 16532 Registers, 9 MUXes

Operating Frequency: 100 MHz

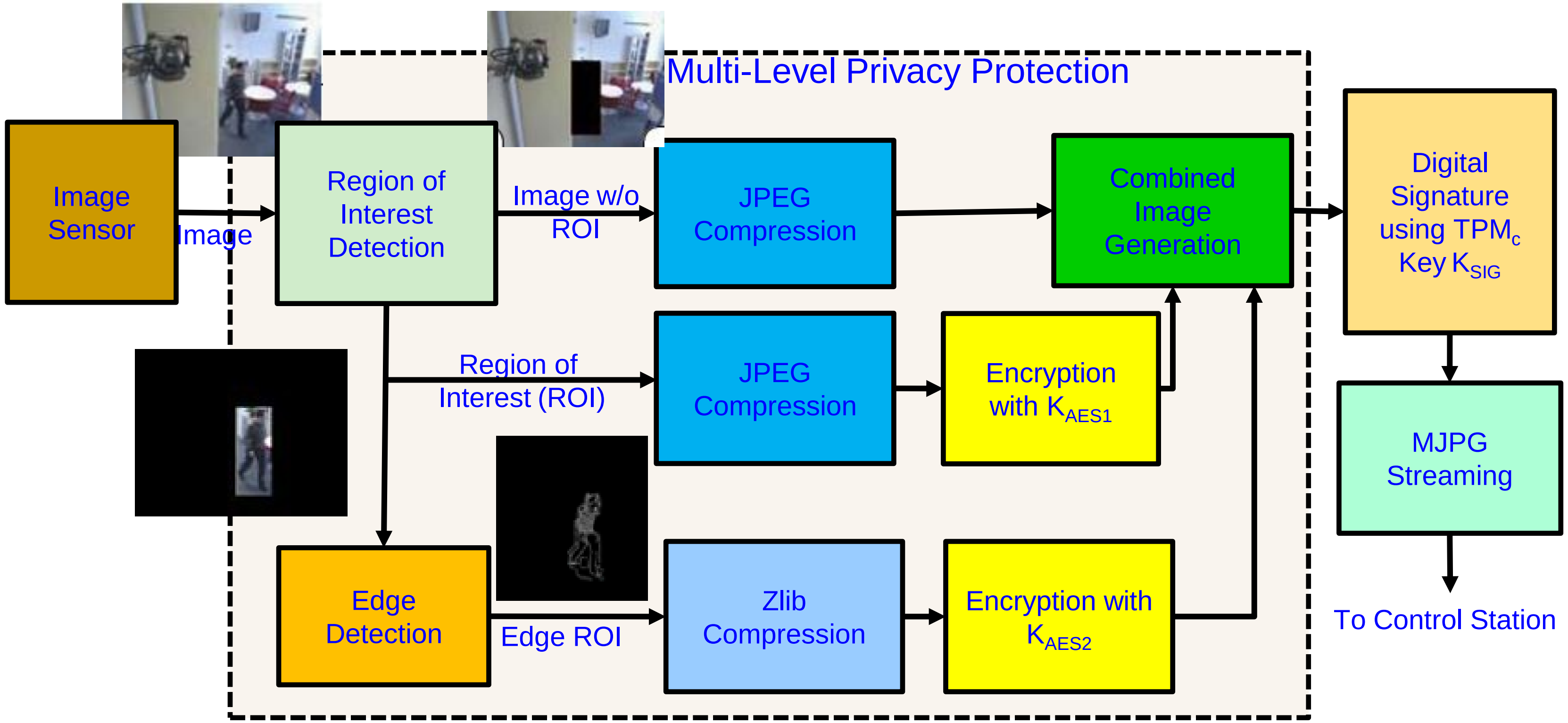
Throughput: 43 fps

Source: **S. P. Mohanty** and E. Kougianos, "Real-Time Perceptual Watermarking Architectures for Video Broadcasting", *Journal of Systems and Software*, Vol. 84, No. 5, May 2011, pp. 724--738.

My Watermarking Research Inspired - TrustCAM



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



Multi-Level Privacy Protection

Image Sensor

Image

Region of Interest Detection

Image w/o ROI

JPEG Compression

Combined Image Generation

Digital Signature using TPM$_c$ Key K$_{SIG}$

Region of Interest (ROI)

JPEG Compression

Encryption with K$_{AES1}$

MJPG Streaming

Edge Detection

Edge ROI

Zlib Compression

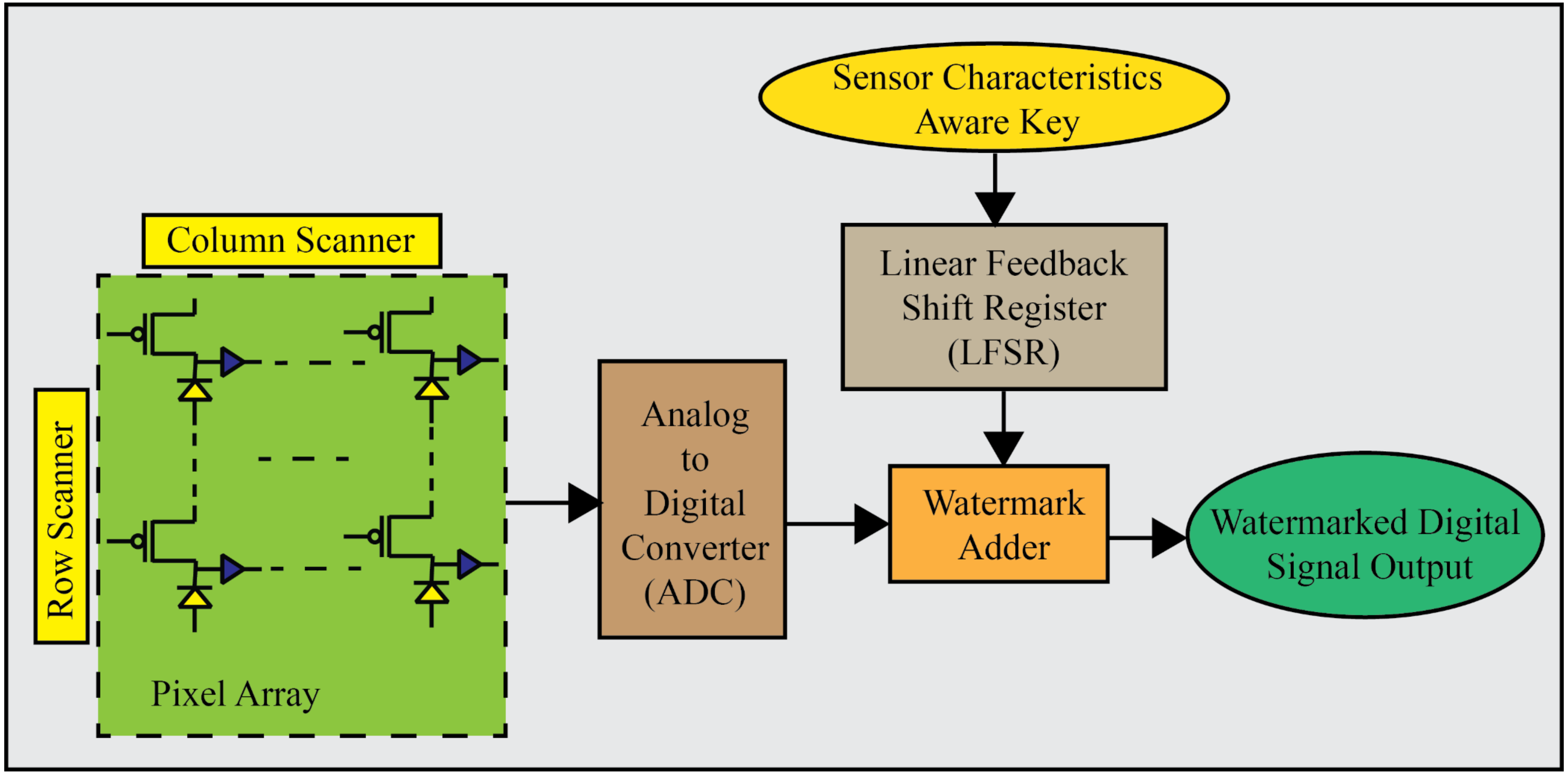
Encryption with K$_{AES2}$

To Control Station

For integrity protection, authenticity and confidentiality of image data.

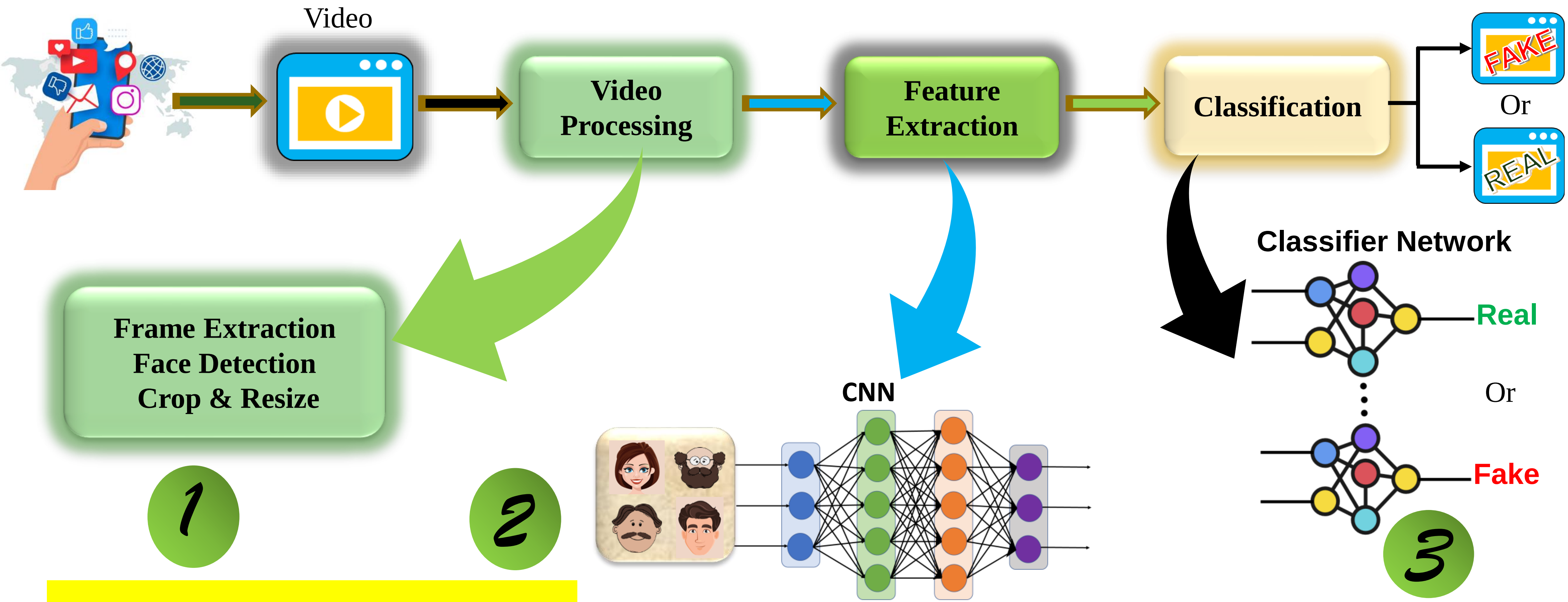
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor


Sensor Characteristics Aware Key
Column Scanner
Linear Feedback Shift Register (LFSR)
Row Scanner
Analog to Digital Converter (ADC)
Watermark Adder
Watermarked Digital Signal Output
Pixel Array

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

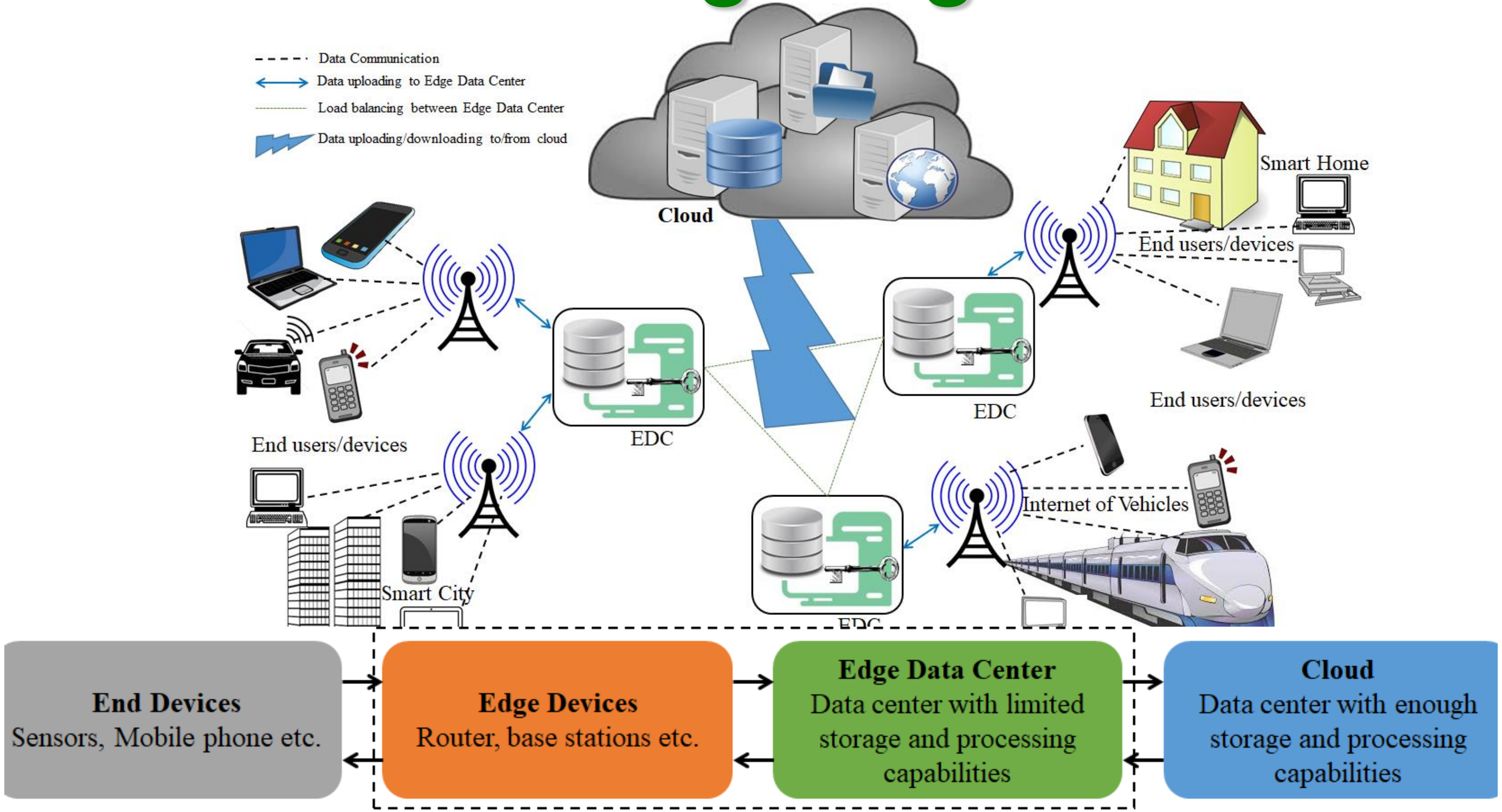
Our Deepfake Detection Method



Accuracy = 96%

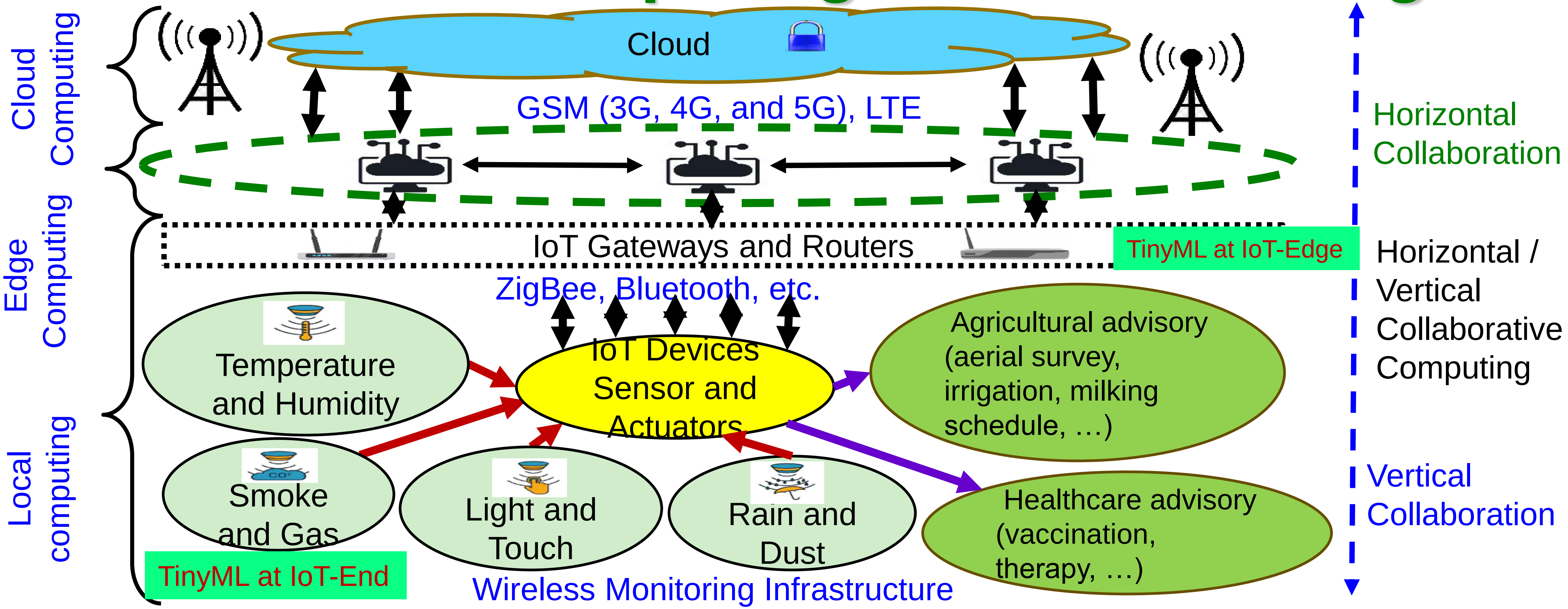
Source: A. Mitra, S. P. Mohanty, P. Corcoran, and E. Kougianos, "A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction", *Springer Nature Computer Science (SN-CS)*, Vol. 2, No. 2, Feb 2021, Article: 99, 18-pages.

Data and Security Should be Distributed using Edge Datacenter


Data Communication
Data uploading to Edge Data Center
Load balancing between Edge Data Center
Data uploading/downloading to/from cloud
Cloud
Smart Home
End users/devices
End users/devices
End users/devices
EDC
EDC
EDC
Internet of Vehicles
Smart City
End Devices
Sensors, Mobile phone etc.
Edge Devices
Router, base stations etc.
Edge Data Center
Data center with limited storage and processing capabilities
Cloud
Data center with enough storage and processing capabilities

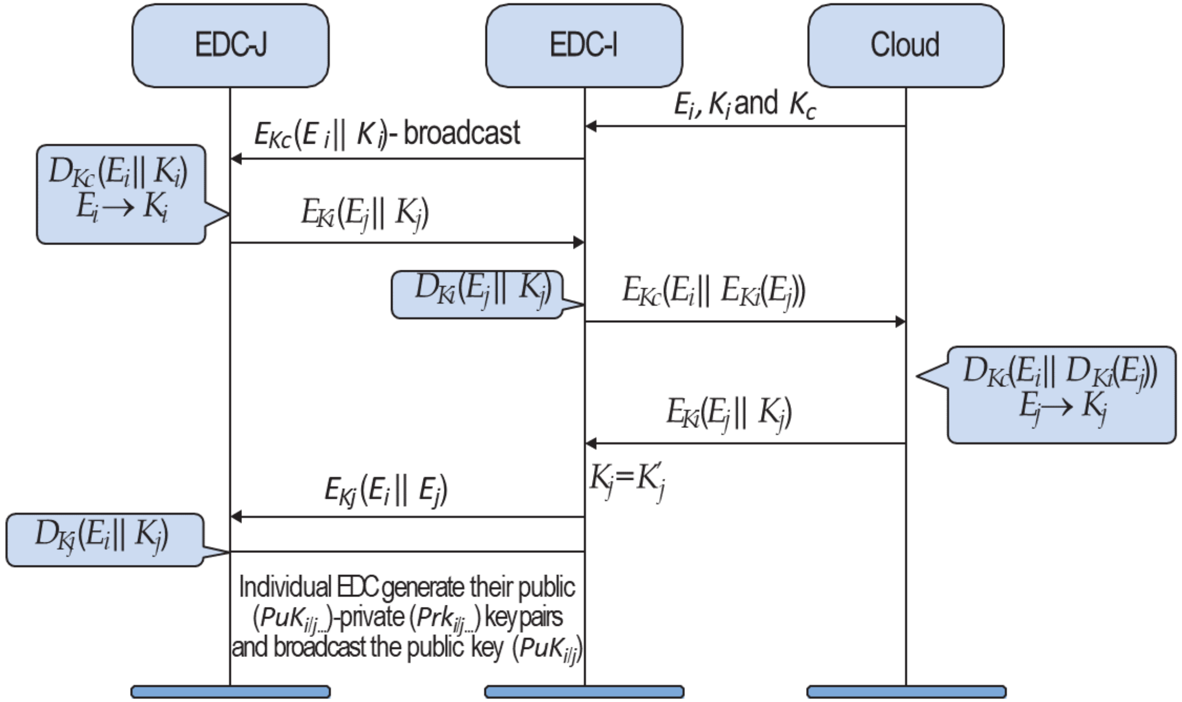
Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Magazine*, Volume 56, Issue 5, May 2018, pp. 60--65.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages


Cloud Computing
Edge Computing
Local computing
Cloud
GSM (3G, 4G, and 5G), LTE
IoT Gateways and Routers
TinyML at IoT-Edge
ZigBee, Bluetooth, etc.
Temperature and Humidity
IoT Devices Sensor and Actuators
Agricultural advisory (aerial survey, irrigation, milking schedule, …)
Smoke and Gas
CO
Light and Touch
Rain and Dust
Healthcare advisory (vaccination, therapy, …)
TinyML at IoT-End
Wireless Monitoring Infrastructure
Horizontal Collaboration
Horizontal / Vertical Collaborative Computing
Vertical Collaboration

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

Our Proposed Secure Edge Datacenter


EDC-J
EDC-I
Cloud
E_i, K_i and K_c
$E_{Kc}(E_i || K_i)$- broadcast
$D_{Kc}(E_i|| K_i)$
$E_i \rightarrow K_i$
$E_{Ki}(E_j|| K_j)$
$D_{Ki}(E_j|| K_j)$
$E_{Kc}(E_i|| E_{Ki}(E_j))$
$D_{Kc}(E_i|| D_{Ki}(E_j))$
$E_j \rightarrow K_j$
$E_{Ki}(E_j|| K_j)$
$K_j=K_j'$
$E_{Kj}(E_i|| E_j)$
$D_{Kj}(E_i|| K_j)$
Individual EDC generate their public ($PuK_{i/j...}$)-private ($Prk_{i/j...}$) key pairs and broadcast the public key ($PuK_{i/j}$)

Secure edge datacenter –

- ➢ Balances load among the EDCs
- ➢ Authenticates EDCs

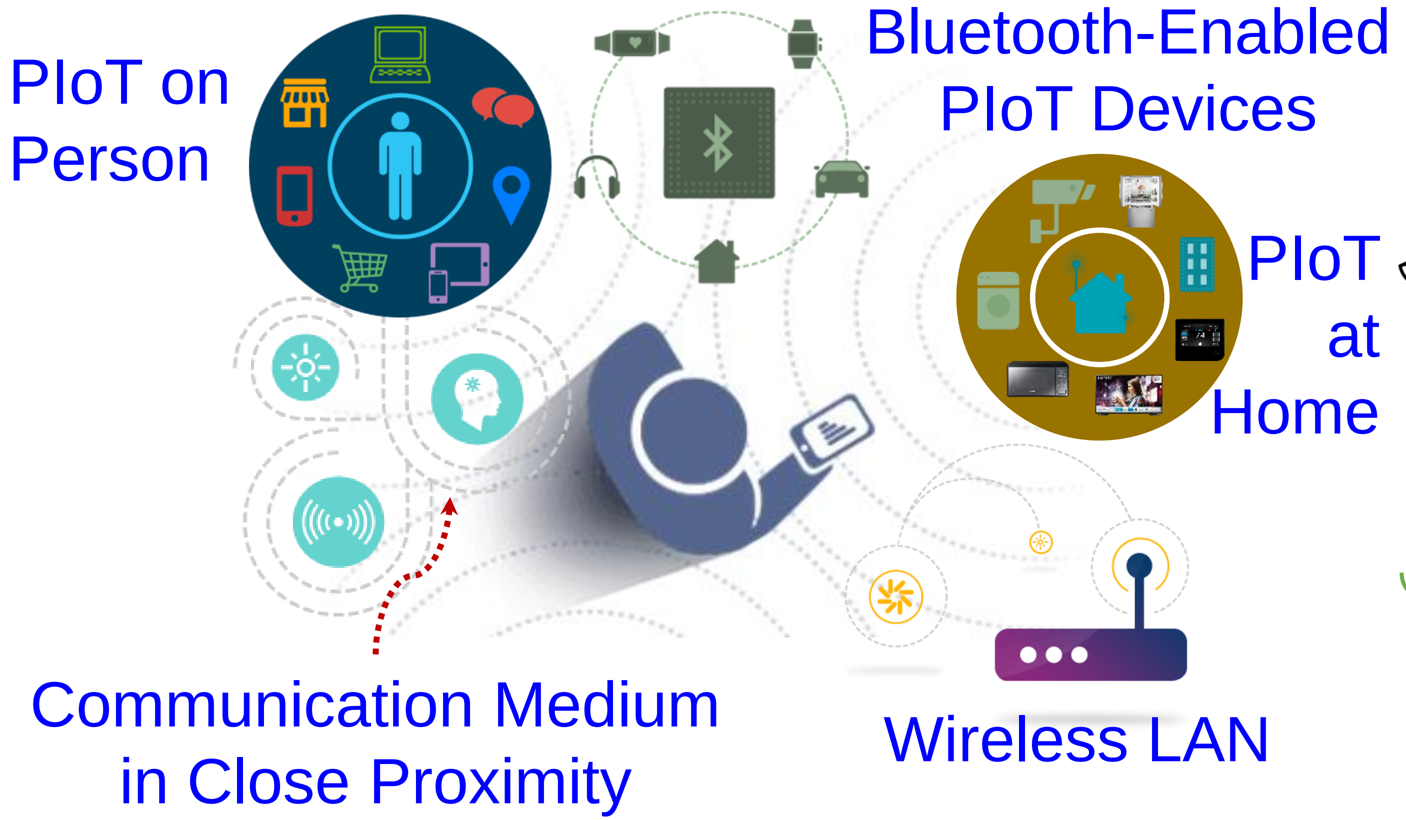
Algorithm 1: Load Balancing Technique

```
If (EDC-I is overloaded)
    EDC-I broadcast ($E_i$, $L_i$)
EDC-J (neighbor EDC) verifies:
If ($E_i$ is in database) & ($p \leq 0.6$ & $L_i << (n-m)$)
        Response $E_{Kpu_i}(E_j||K_j||p)$
EDC-I perform $D_{Kpr_i}(E_j||K_j||p)$
$k_j' \leftarrow E_j$
If ($k_j' = k_j$)
   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.

Personal IoT (PIoT) – Cybersecurity and AI?



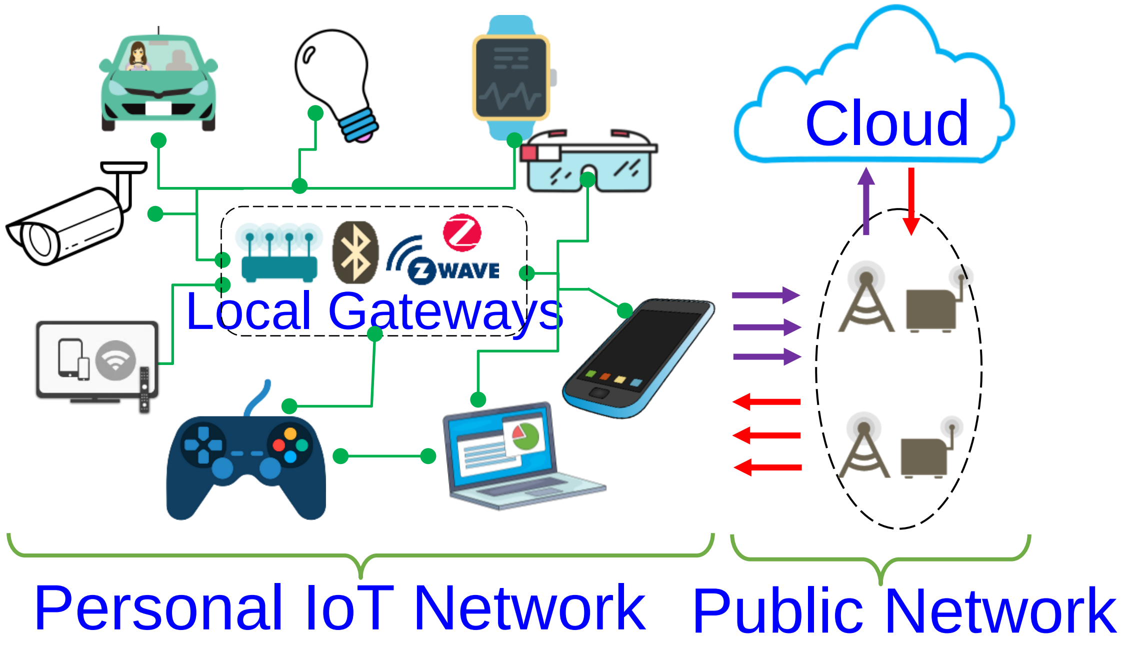
PIoT on Person

Bluetooth-Enabled PIoT Devices

PIoT at Home

Communication Medium in Close Proximity

Wireless LAN



Cloud

Local Gateways

ZWAVE

Personal IoT Network

Public Network

Source: B. P. S. Sahoo, S. P. Mohanty, D. Puthal and P. Pillai, "Personal Internet of Things (PIoT): What is it Exactly," *IEEE Consumer Electronics Magazine*, Vol. 10, No. 6, Nov 2021, pp. 58--60.

PIoT - A group of connected devices focused mainly in homes and the immediate proximity of an individual.

Conclusions

Conclusions

- Cybersecurity and Privacy are important problems in IoT-driven Cyber-Physical Systems (CPS).
- Various elements and components of IoT/CPS including Data, Devices, System Components, AI need security.
- Both software and hardware-based attacks and solutions are possible for cybersecurity in IoT/CPS.
- Cybersecurity in IoT-based H-CPS, A-CPS, E-CPS, and T-CPS, etc. can have serious consequences.
- Existing cybersecurity solutions have serious overheads and may not even run in the end-devices (e.g. a medical device) of CPS/IoT.
- Security-by-Design (SbD) advocate features at early design phases, no-retrofitting.
- Hardware-Assisted Security (HAS): Security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system.

Future Directions

- Privacy and/or Security by Design (PbD or SbD) needs research.
- Cybersecurity, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS) need more research.
- Cybersecurity of IoT-based systems (e.g. Smart Healthcare device/data, Smart Agriculture, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable Smart City and Smart Villages: need sustainable IoT/CPS

Acknowledgement(s)

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112 and HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.