Security-by-Design to Fortify Cyber-Physical Systems

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

Silicon University, Bhubaneswar, India – 10 Dec 2024

Homepage:
www.smohanty.org

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

Outline

- IoT/CPS – Big Picture
- Challenges in IoT/CPS Design
- Cybersecurity Solution for IoT/CPS
- Drawbacks of Existing Cybersecurity Solutions
- Security-by-Design (SbD) – The Principle
- Security-by-Design (SbD) - Specific Examples
- Is Physical Unclonable Function (PUF) a Solution for All Cybersecurity Problems?
- Is Blockchain a Solution for All Cybersecurity Problems?
- Conclusion

The Big Picture

Issues Challenging City Sustainability

Pollution

Water Crisis

Energy Crisis

Traffic

The Problem

- Uncontrolled growth of urban population
- Limited natural and man-made resources

Source: https://humanitycollege.org

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

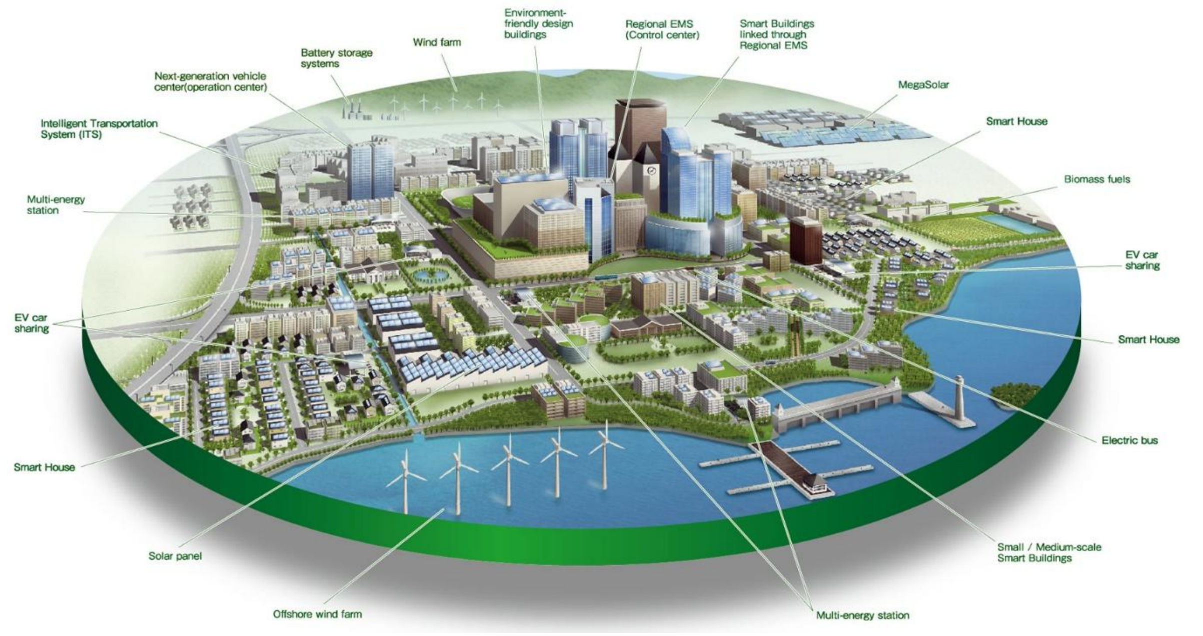
➢ Year 2050: 70% of world population will be urban

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

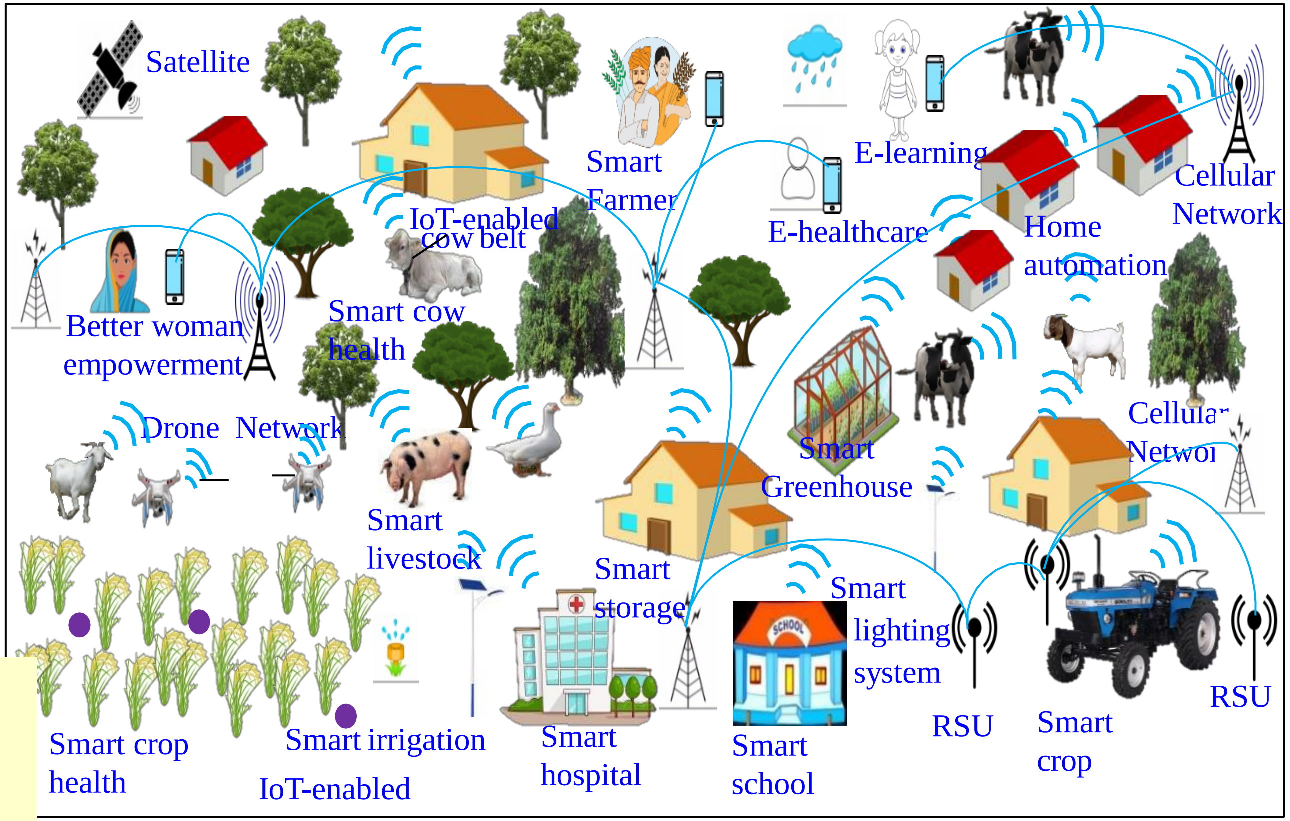
July 2016

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
Biomass fuels
Multi-energy station
EV car sharing
EV car sharing
Smart House
Smart House
Electric bus
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.

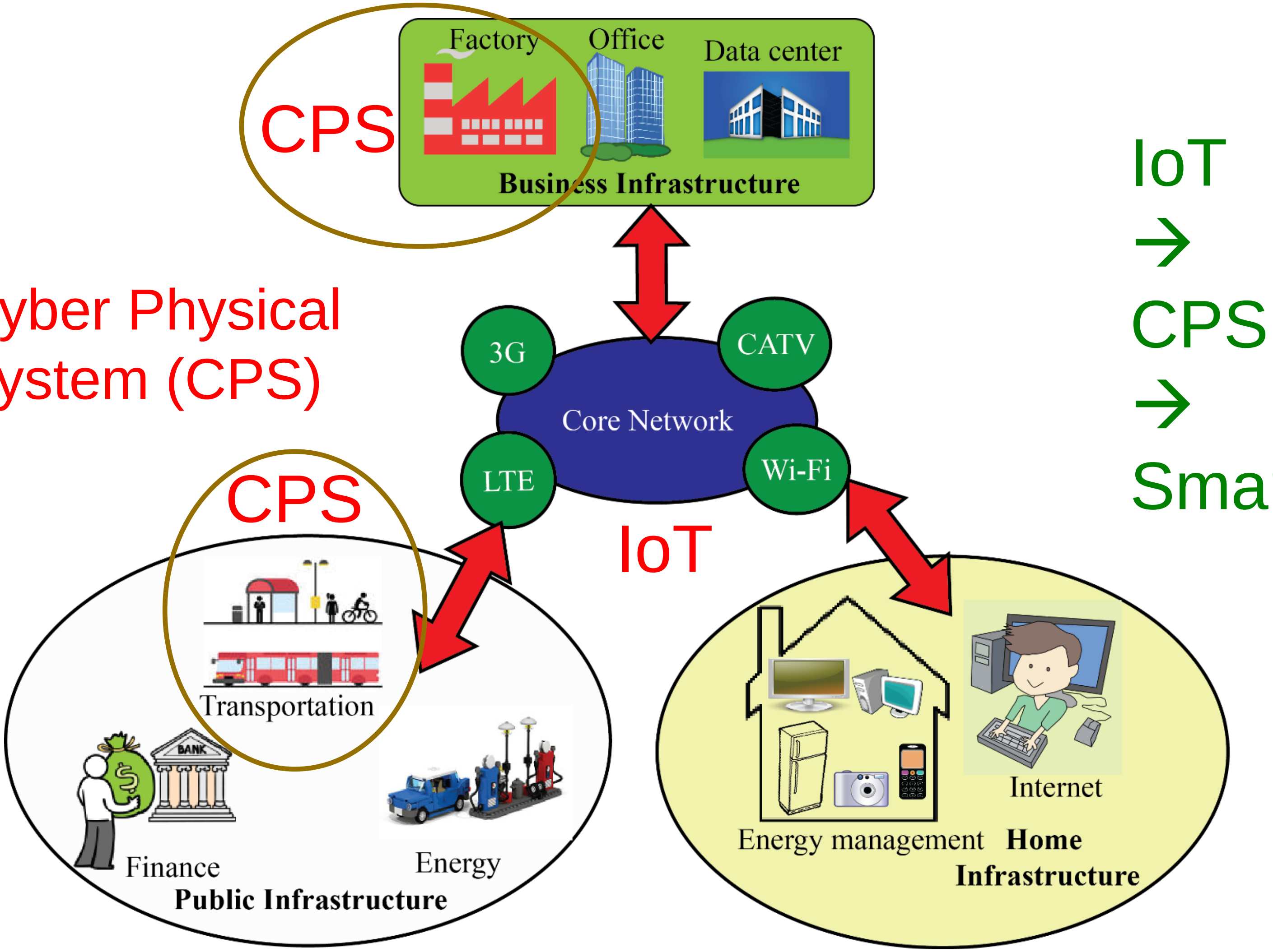
Smart Cities

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

IoT → CPS → Smart Cities or Smart Villages

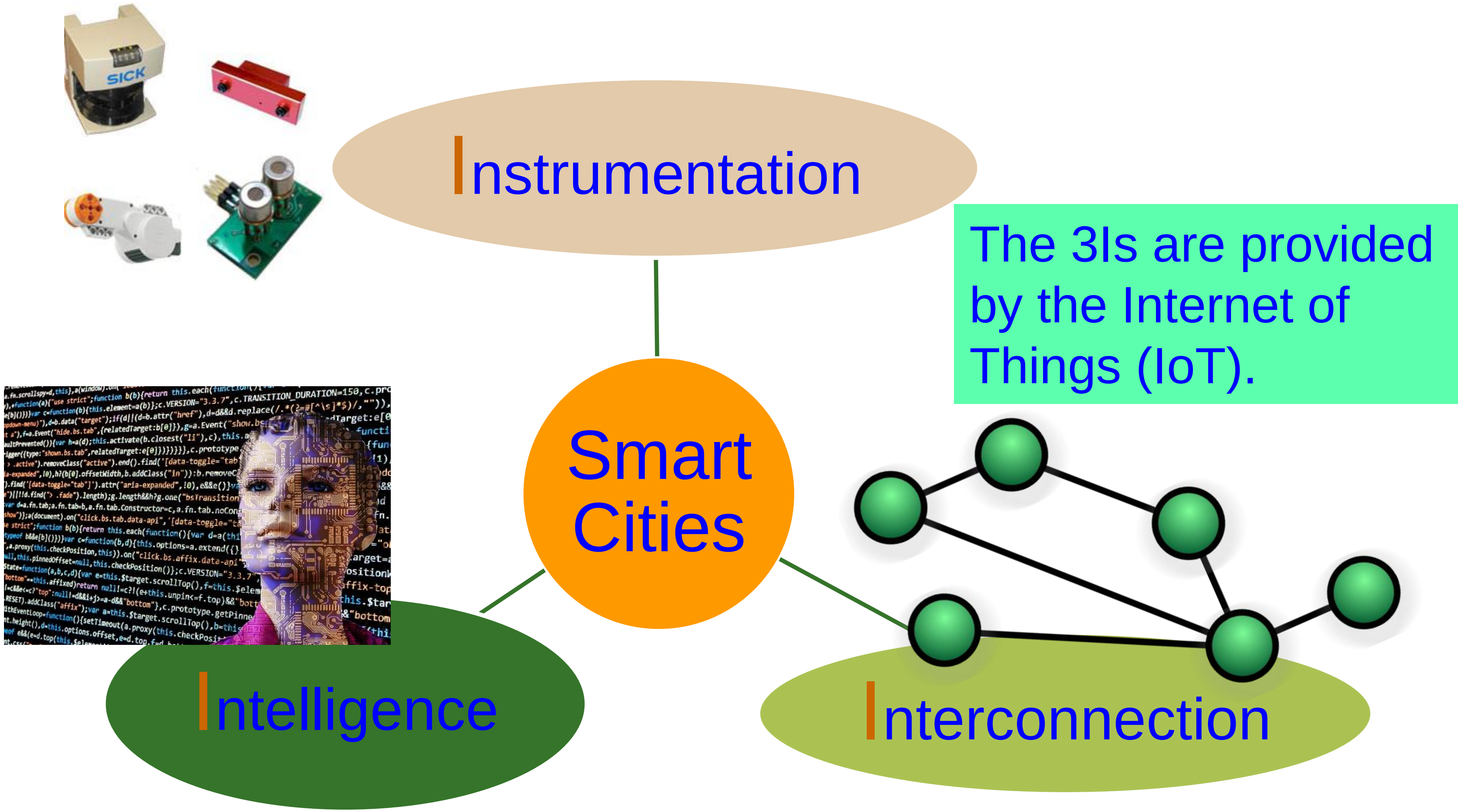


IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

IoT is the backbone

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

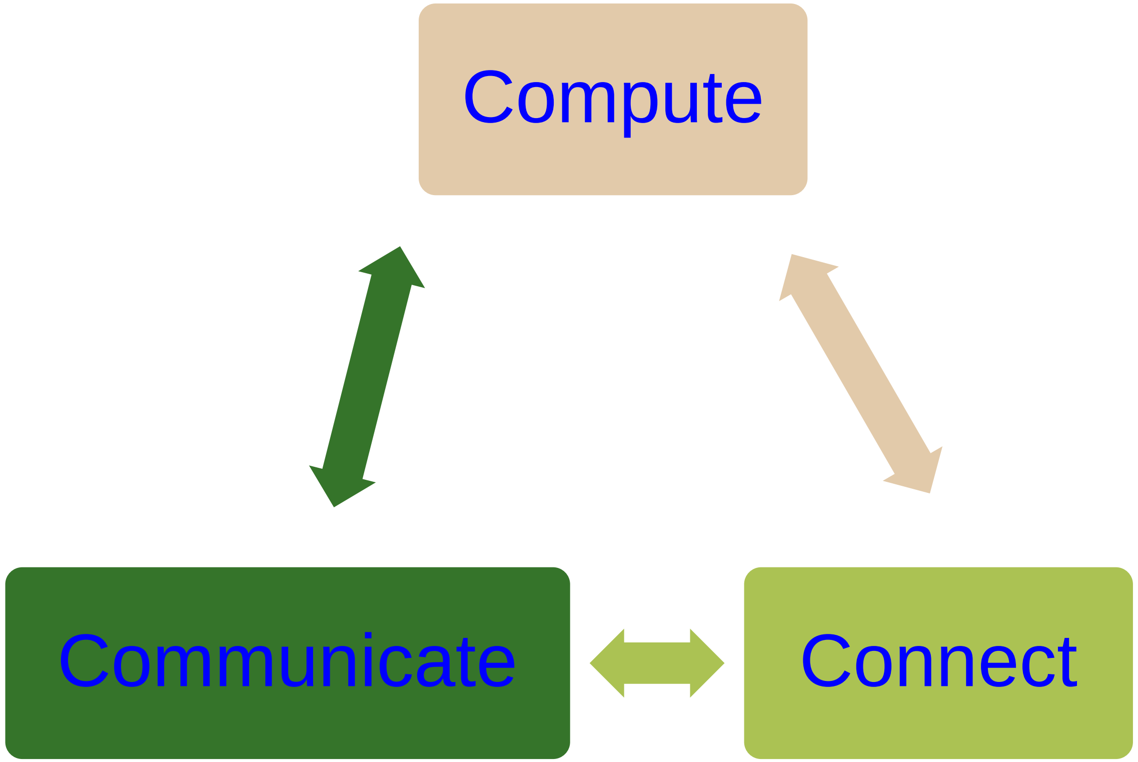
Smart Cities or Smart Villages - 3 Is



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

Source: Mohanty ISC2 2019 Keynote

Internet-of-Things (IoT) - 3 Cs

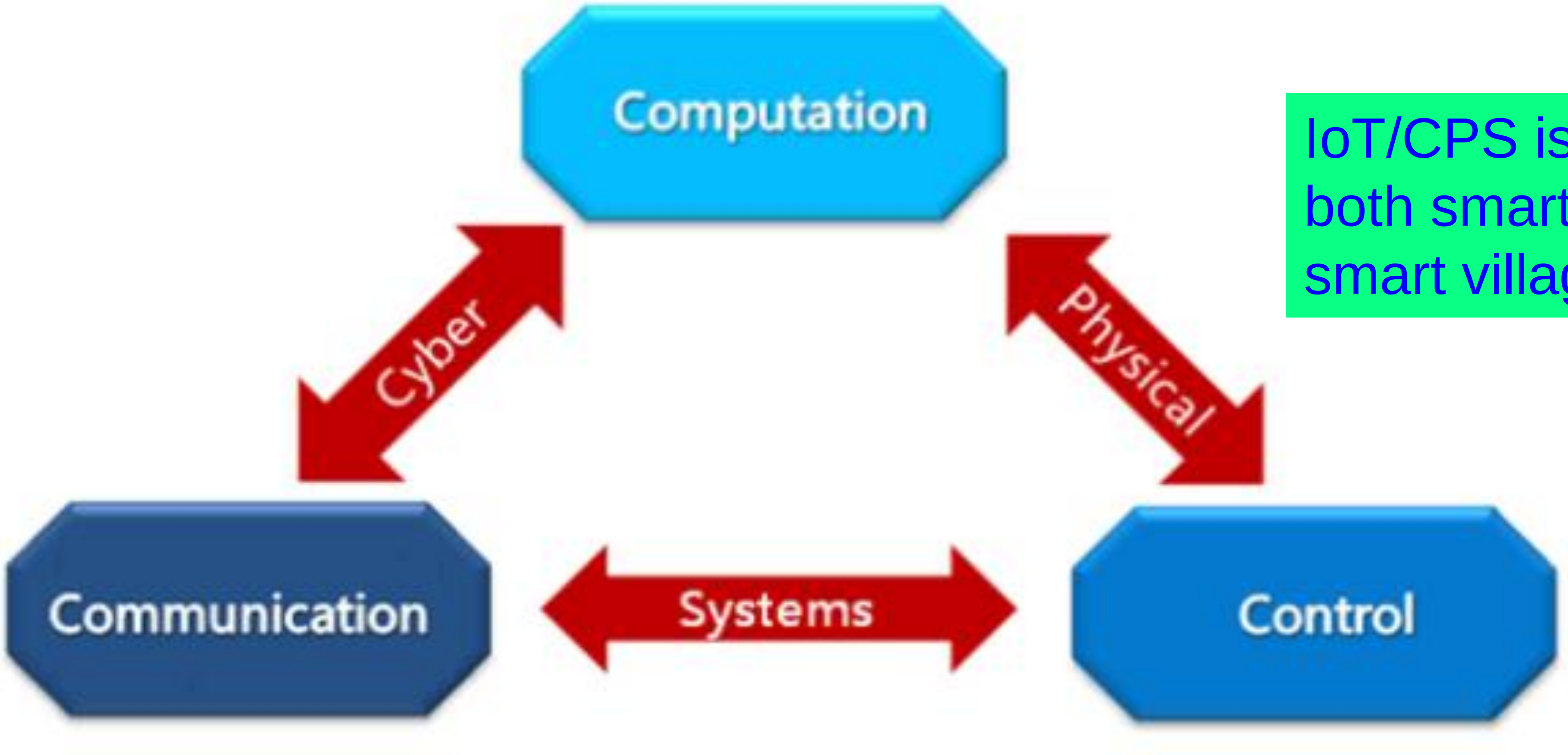


IoT/CPS is needed in both smart cities and smart villages.

3 Cs of CPS - Control, Compute, Communicate

Source: https://www.linkedin.com/pulse/3-cs-internet-things-iot-satish-rao-pullacheri

Cyber-Physical Systems (CPS) - 3 Cs

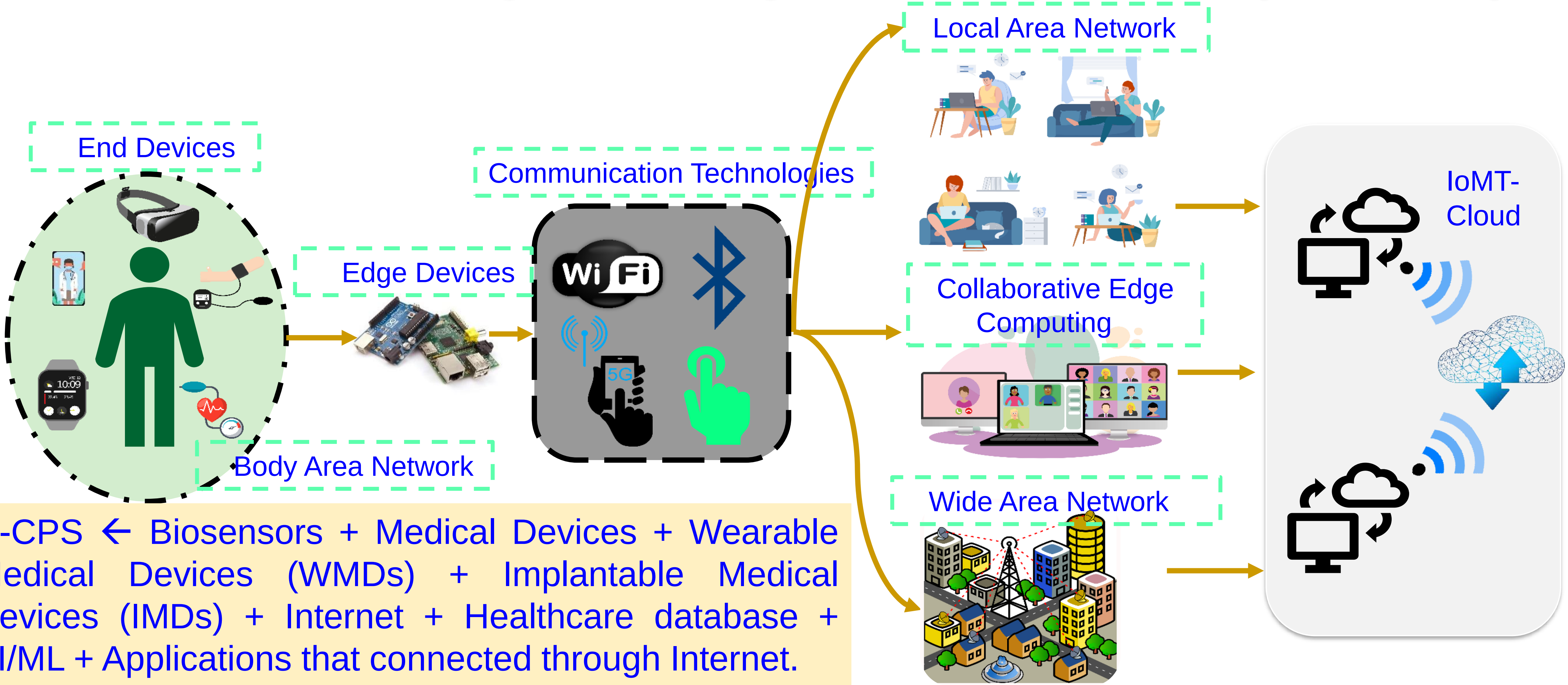


IoT/CPS is needed in both smart cities and smart villages.

3 Cs of IoT - Connect, Compute, Communicate

Source: G. Jinghong, H. Ziwei, Z. Yan, Z. Tao, L. Yajie and Z. Fuxing, "An overview on cyber-physical systems of energy interconnection," in *Proc. IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2017, pp. 15-21.

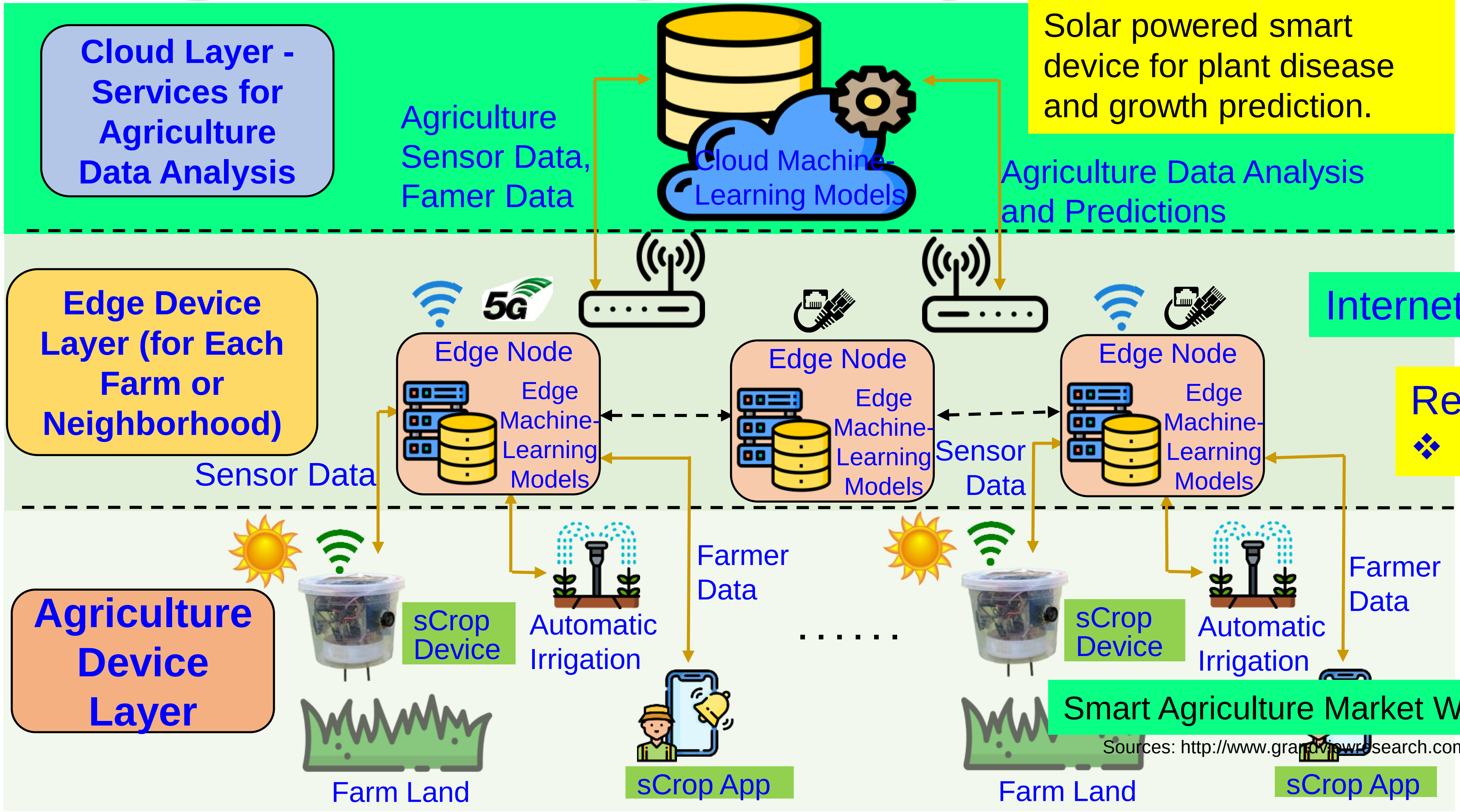
Healthcare Cyber-Physical System (H-CPS)



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

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

Agriculture Cyber-Physical System (A-CPS)



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

Solar powered smart device for plant disease and growth prediction.

Internet-of-Agro-Things (IoAT)

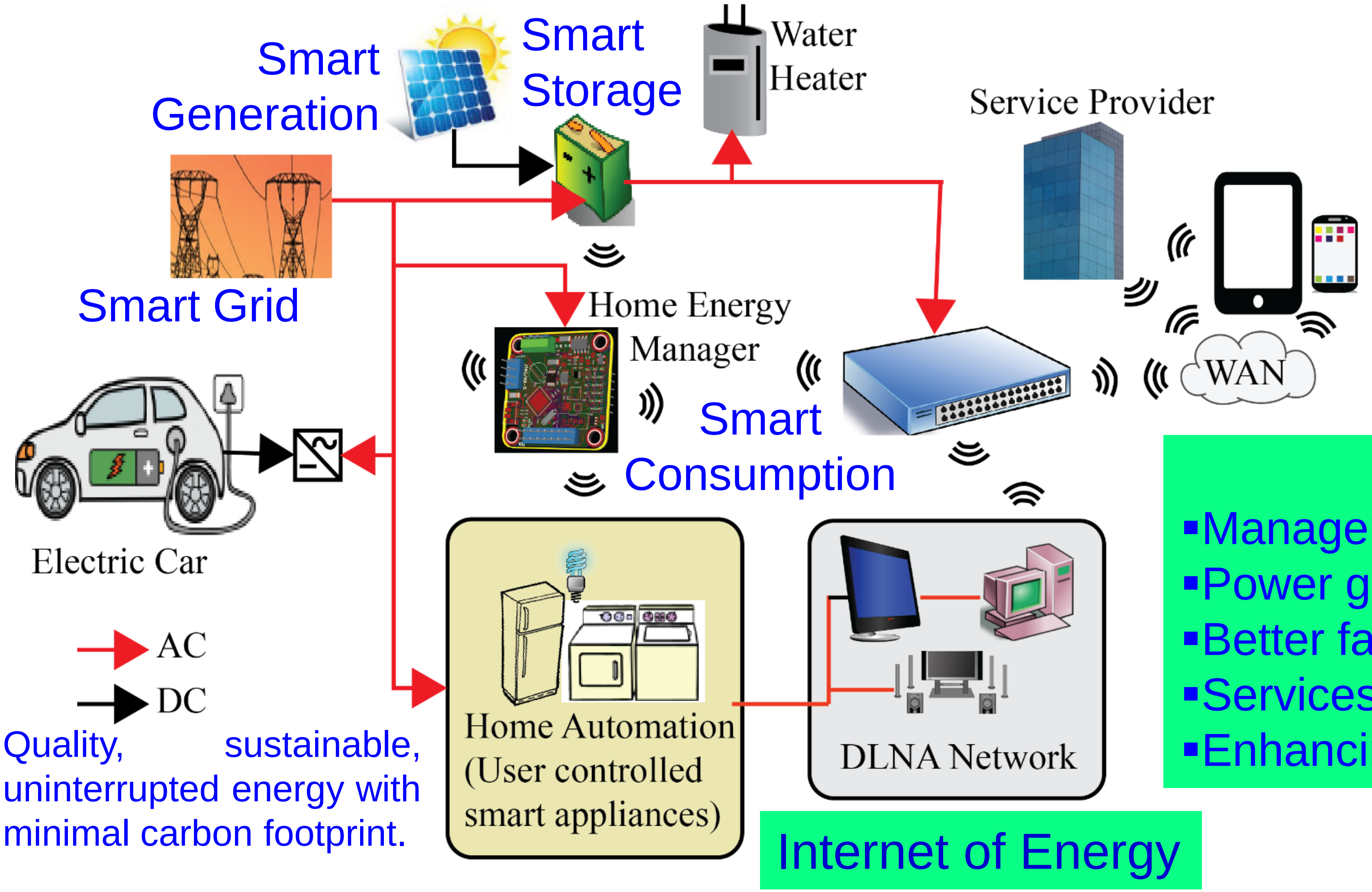
Requires:
- ❖ Data and System Security

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.

Energy Cyber-Physical System (E-CPS)



Quality, sustainable, uninterrupted energy with minimal carbon footprint.

Internet of Energy

Requires:

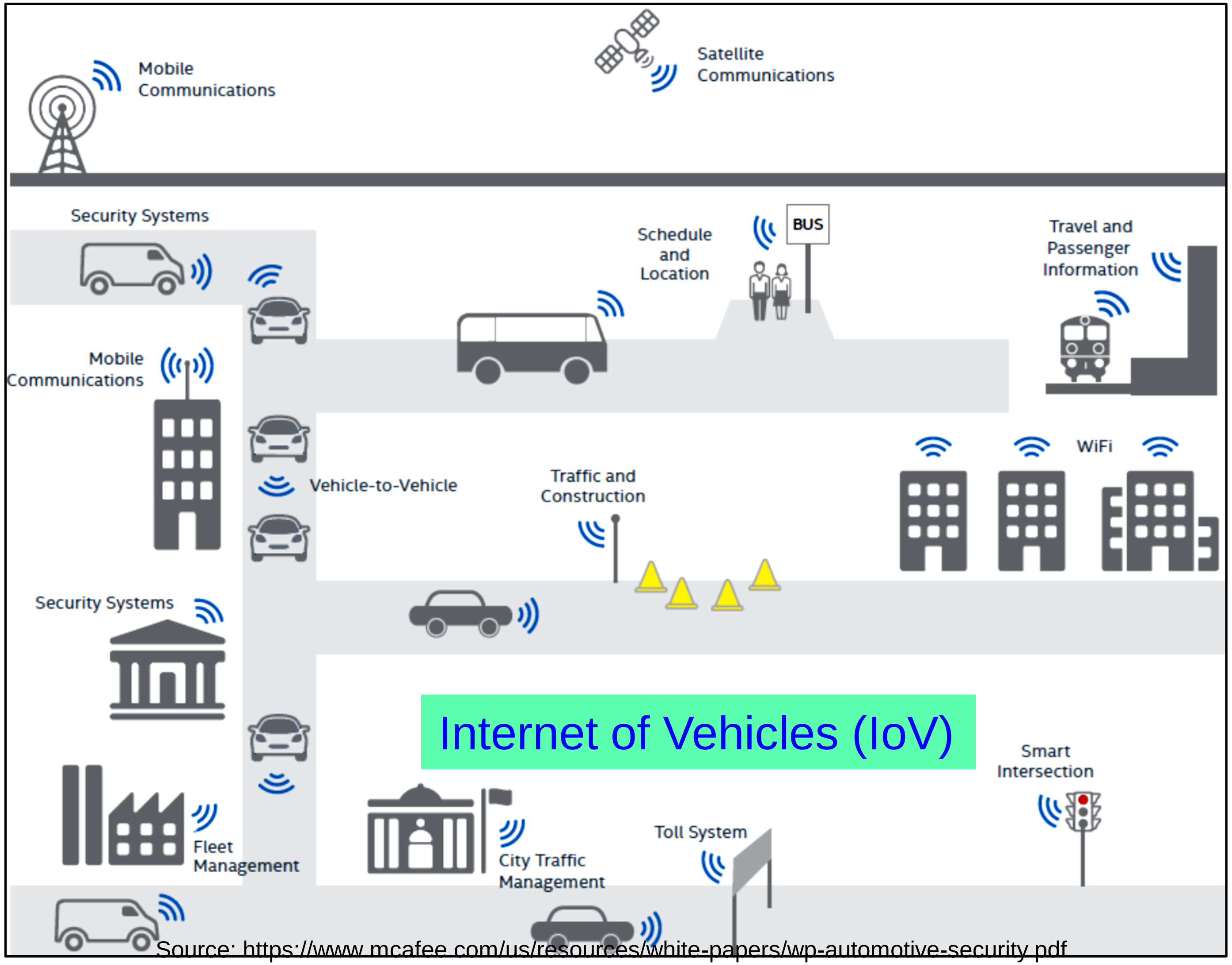
❖ Data, Device, and System Security

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.

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:

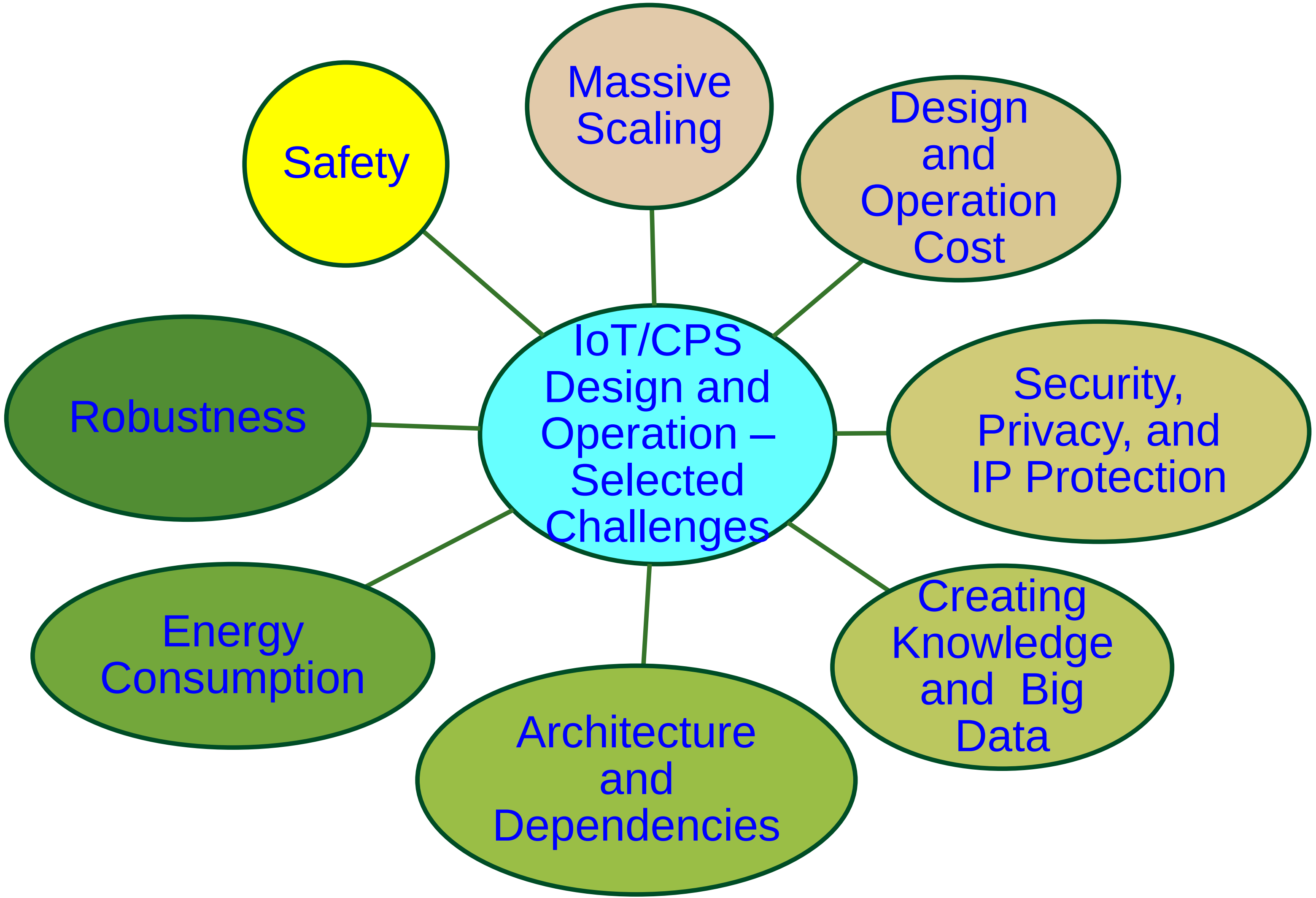
- ❖ Data, Device, and System Security
- ❖ Location Privacy

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

Source: Datta 2017, CE Magazine Oct 2017

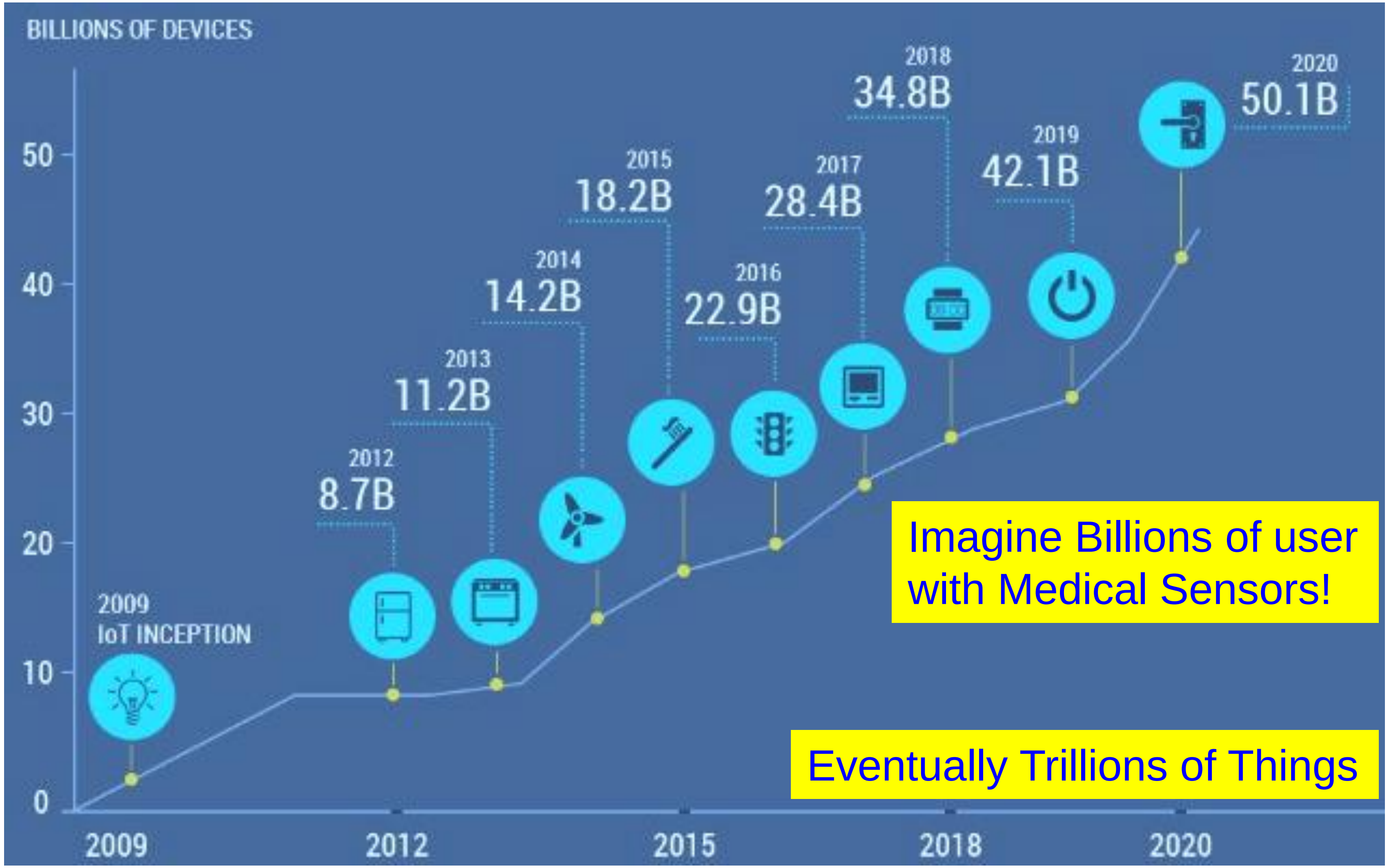
Challenges in IoT/CPS Design

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

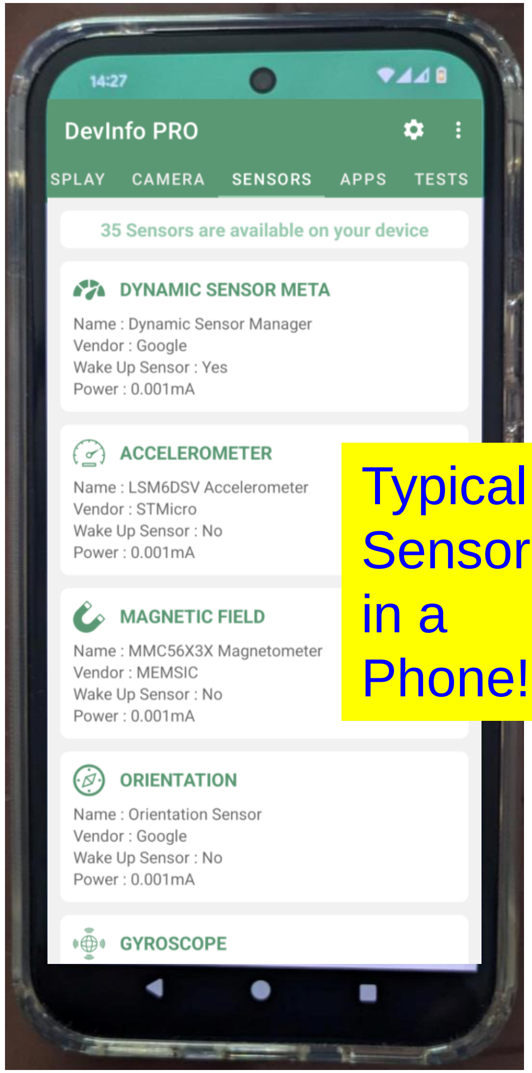
Massive Growth of Sensors/Things



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



35 Sensors are available on your device

DYNAMIC SENSOR META
Name : Dynamic Sensor Manager
Vendor : Google
Wake Up Sensor : Yes
Power : 0.001mA

ACCELEROMETER
Name : LSM6DSV Accelerometer
Vendor : STMicro
Wake Up Sensor : No
Power : 0.001mA

MAGNETIC FIELD
Name : MMC56X3X Magnetometer
Vendor : MEMSIC
Wake Up Sensor : No
Power : 0.001mA

ORIENTATION
Name : Orientation Sensor
Vendor : Google
Wake Up Sensor : No
Power : 0.001mA

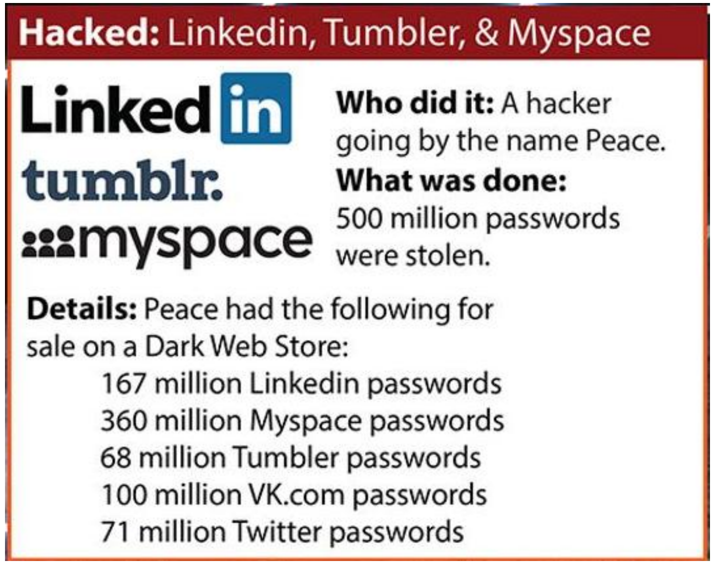
GYROSCOPE

Typical Sensors in a Phone!

Security Challenges – Information

Online Banking

Credit Card Theft



Hacked: Linkedin, Tumbler, & Myspace

LinkedIn
tumblr.
myspace

Who did it: A hacker going by the name Peace.

What was done: 500 million passwords were stolen.

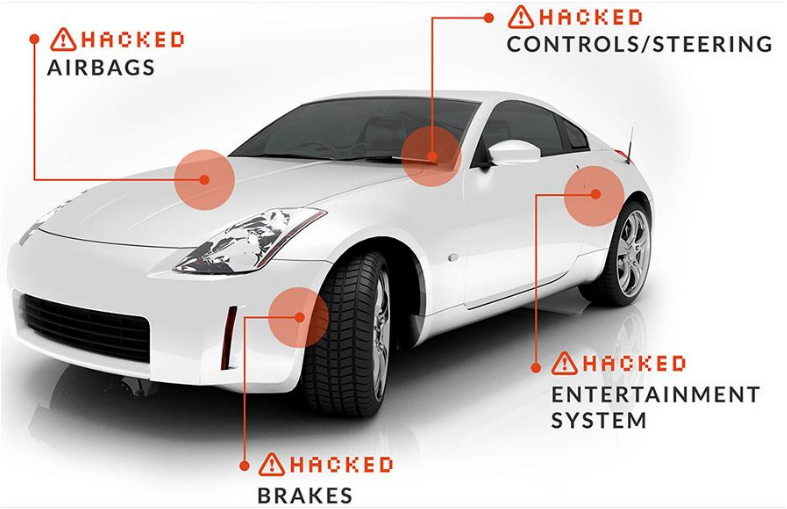
Details: Peace had the following for sale on a Dark Web Store:

167 million Linkedin passwords
360 million Myspace passwords
68 million Tumbler passwords
100 million VK.com passwords
71 million Twitter passwords

Personal Information

Credit Card/Unauthorized Shopping

Cybersecurity Challenges - System



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

Power Grid Attack

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

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

Attacks on IoT Devices

Impersonation Attack

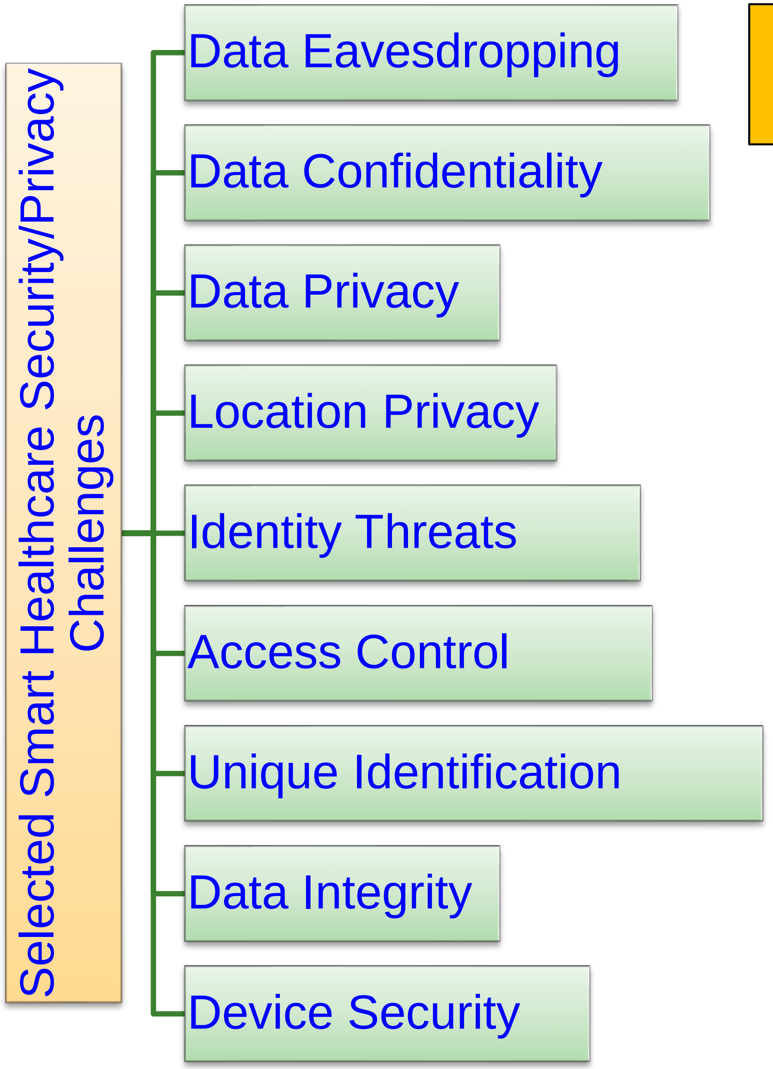
Reverse Engineering Attack

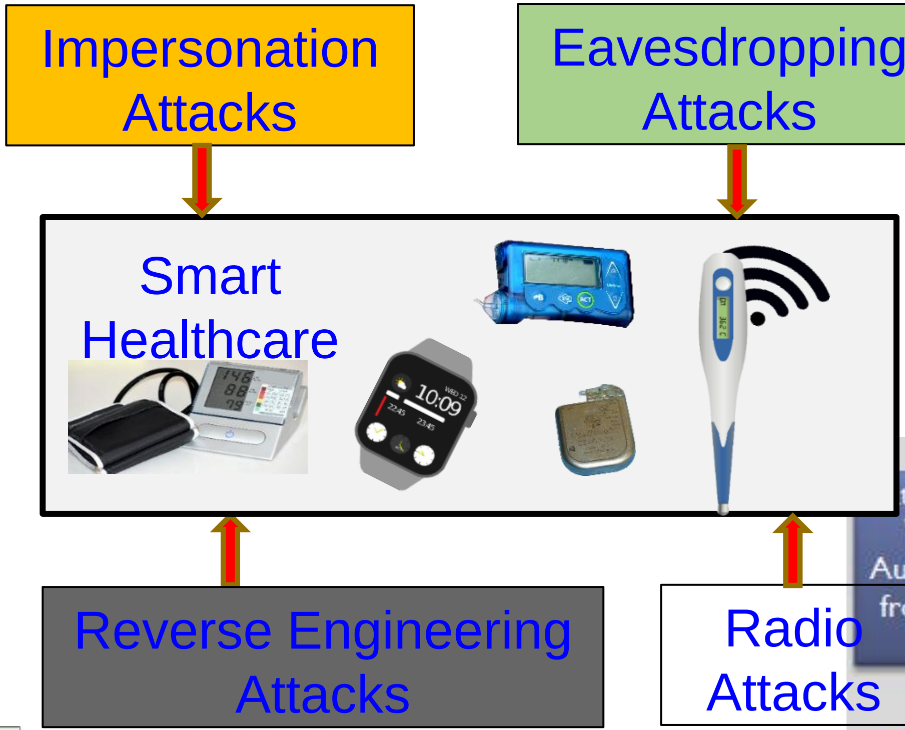
Denial of Service Attack

Dictionary and Brute Force Attack

Eavesdropping Attack

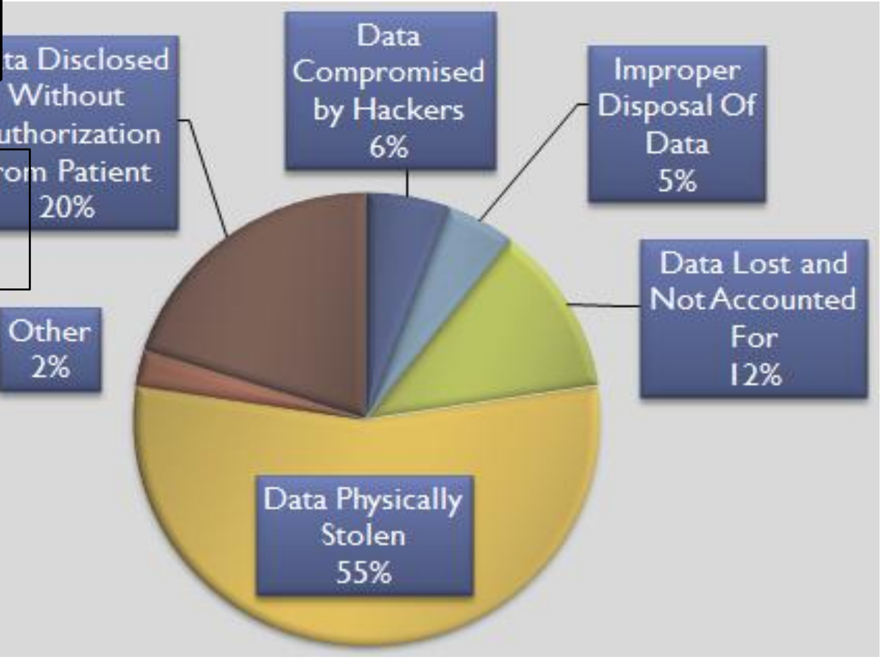
Smart Healthcare - Cybersecurity and Privacy Issue





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/

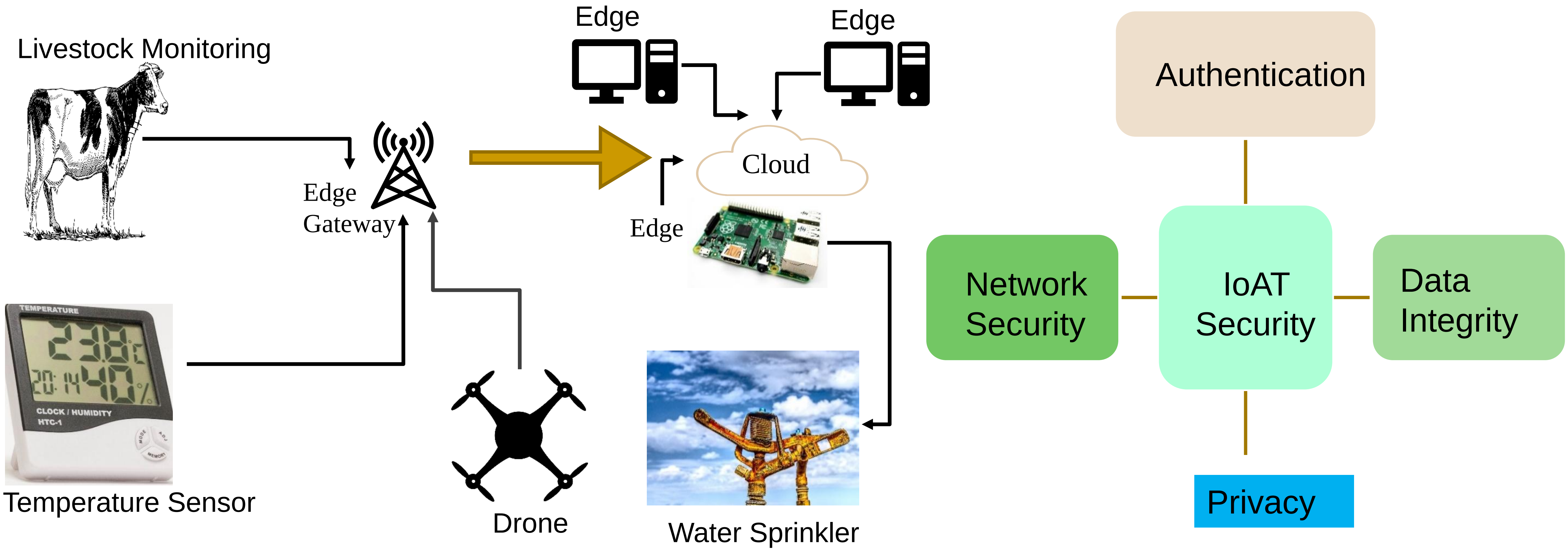
- Software vulnerabilities in some medical devices could leave them susceptible to hackers, FDA warns:

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:

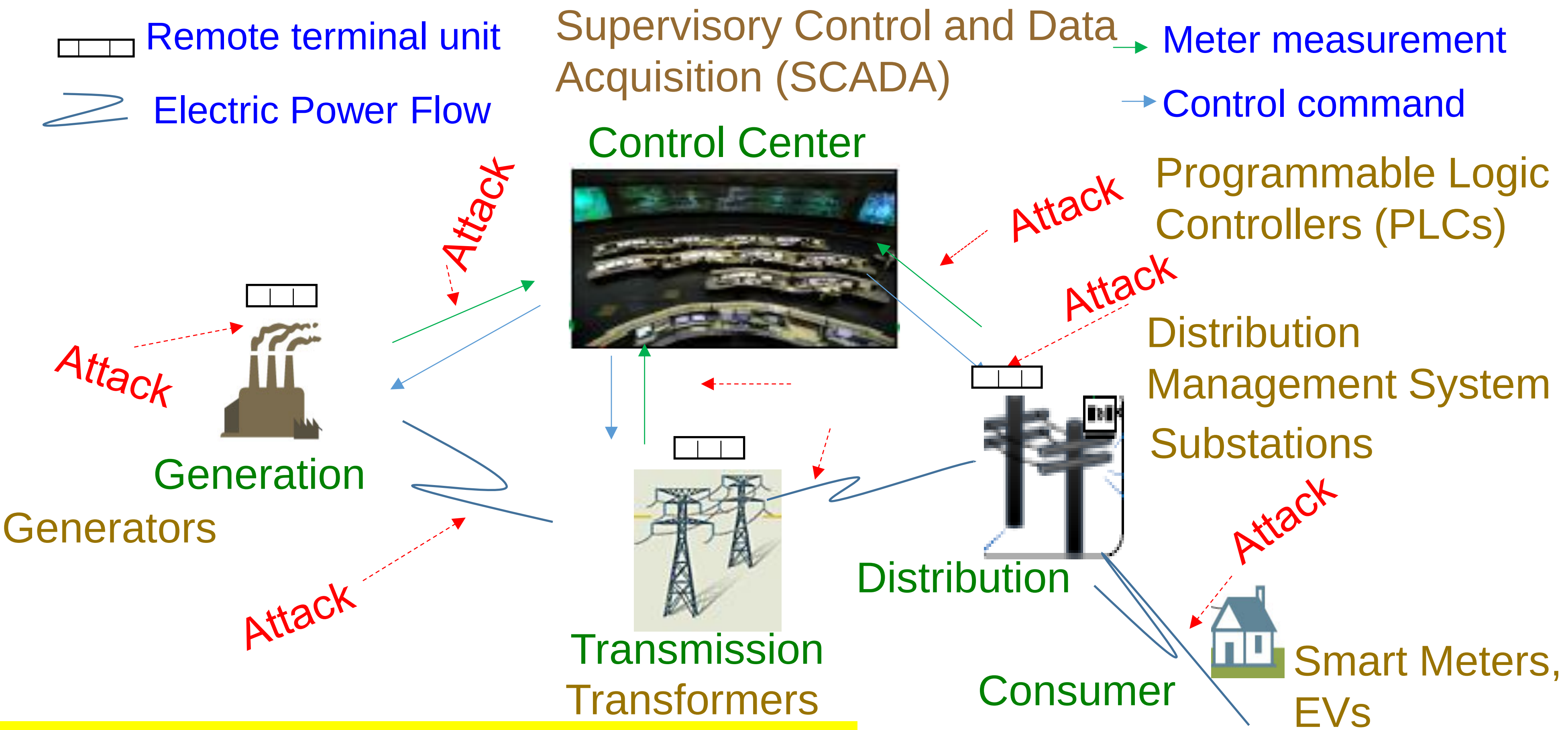
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

Internet of Agro-Things (IoAT) - Cybersecurity Issue



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

Smart Grid - Vulnerability



Remote terminal unit

Electric Power Flow

Supervisory Control and Data Acquisition (SCADA)

Meter measurement

Control command

Control Center

Programmable Logic Controllers (PLCs)

Distribution Management System

Substations

Generation

Generators

Transmission

Transformers

Distribution

Consumer

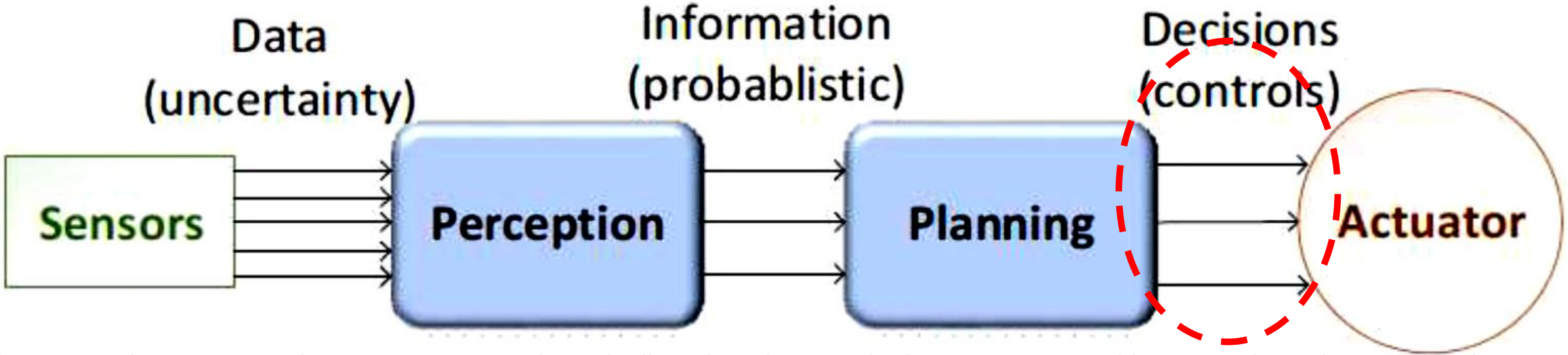
Smart Meters, EVs

ICT components of smart grid is cyber vulnerable.

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

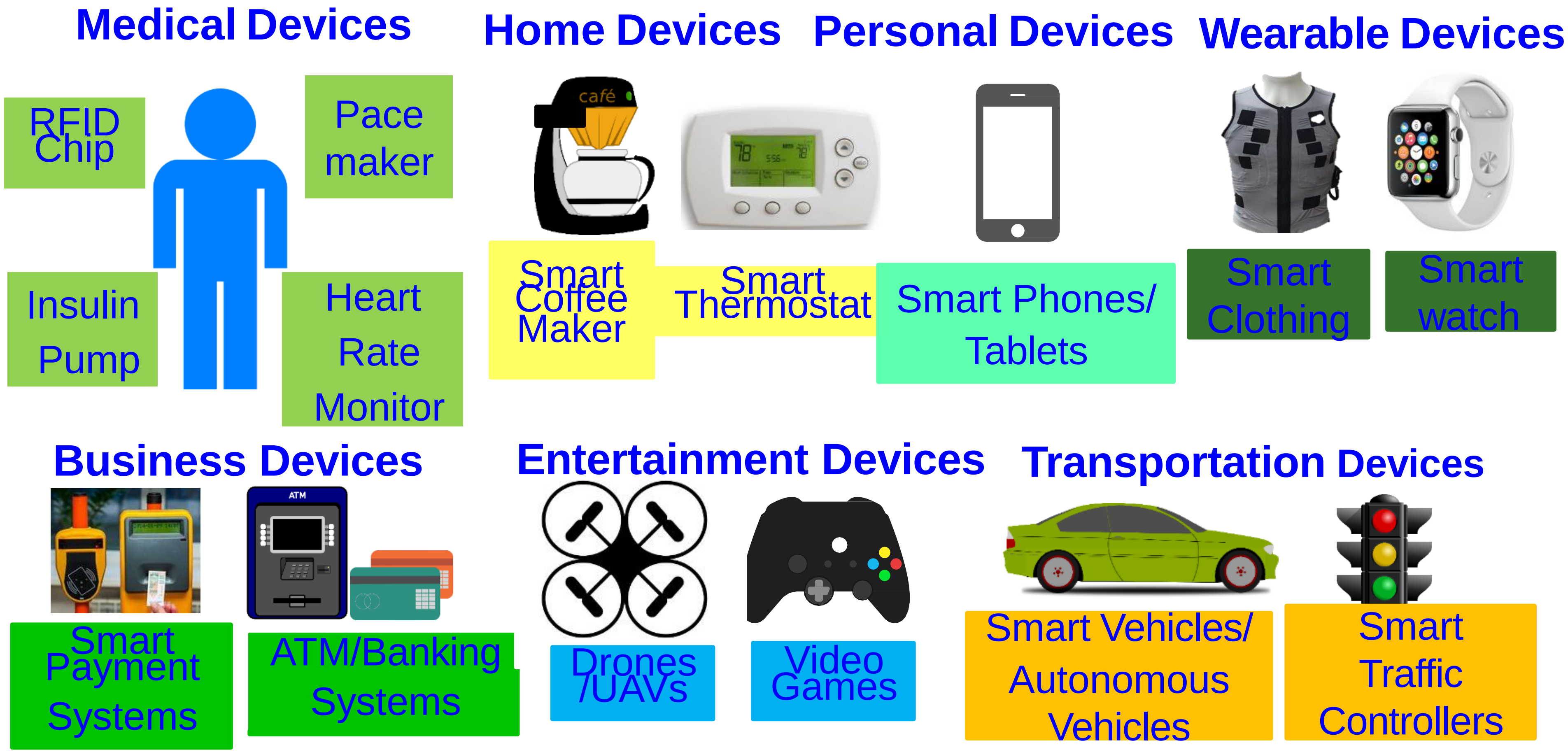
Smart Car – Modification of Input Signal of Control Can be Dangerous

- ➢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: S. J. Plathottam and P. Ranganathan, "Next Generation Distributed and Networked Autonomous Vehicles: Review," in *Proc. 10th International Conference on Communication Systems and Networks (COMSNETS)*, 2018, pp. 577-582, DOI: https://doi.org/10.1109/COMSNETS.2018.8328277.

CE Systems – Diverse Security/ Privacy/ Ownership Requirements



Medical Devices

RFID Chip

Pace maker

Insulin Pump

Heart Rate Monitor

Home Devices

Smart Coffee Maker

Smart Thermostat

Personal Devices

Smart Phones/ Tablets

Wearable Devices

Smart Clothing

Smart watch

Business Devices

Smart Payment Systems

ATM/Banking Systems

Entertainment Devices

Drones /UAVs

Video Games

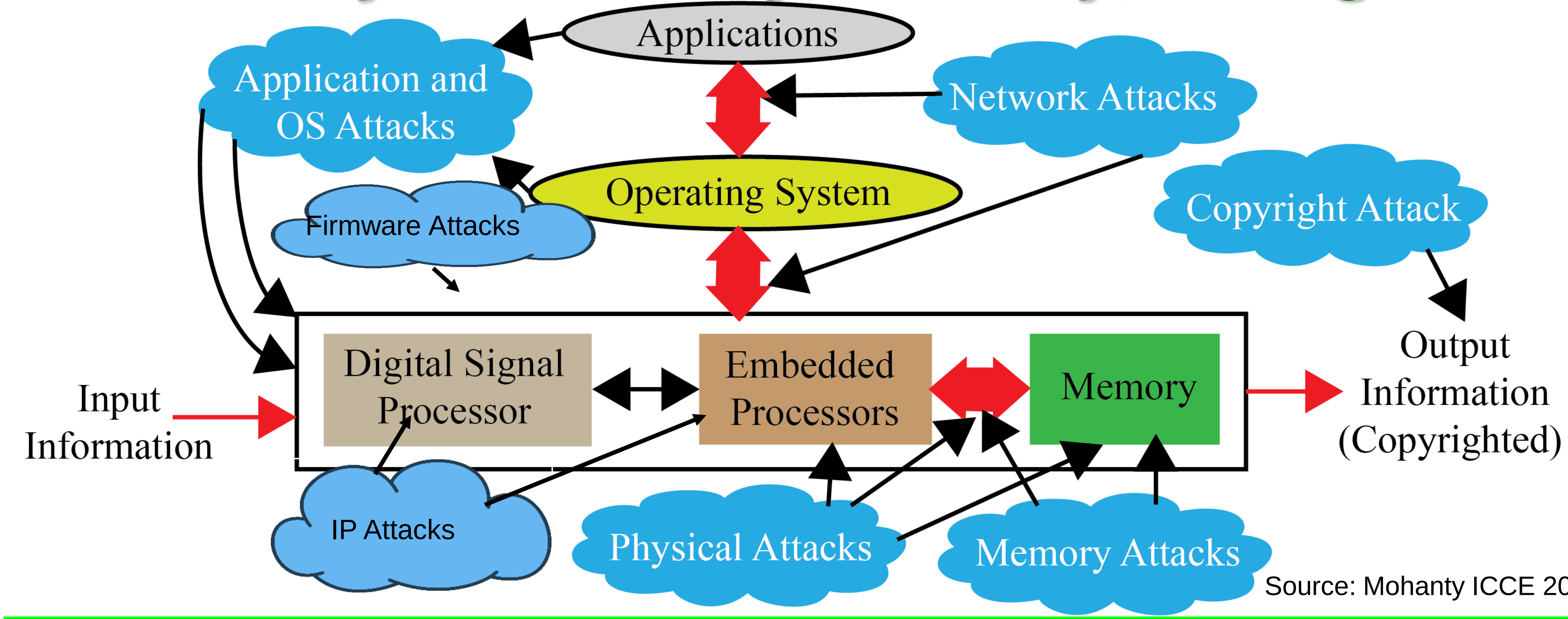
Transportation Devices

Smart Vehicles/ Autonomous Vehicles

Smart Traffic Controllers

Source: D. A. Hahn, A. Munir, and S. P. Mohanty, “Security and Privacy Issues in Contemporary Consumer Electronics”, IEEE Consumer Electronics Magazine (CEM), Volume 8, Issue 1, January 2019, pp. 95--99.

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



Source: Mohanty ICCE 2018 Keynote

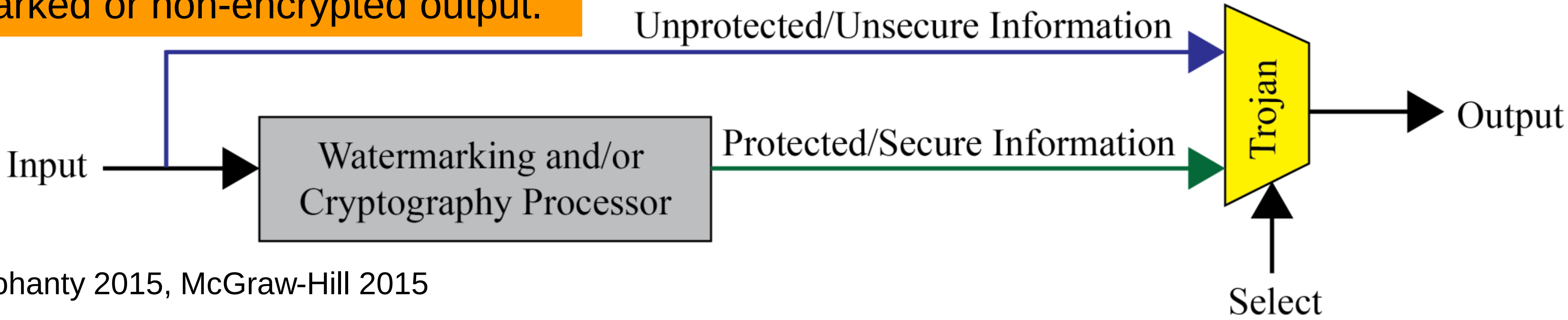
Diverse forms of Attacks, following are not the same: System Security, Device Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

Trojans can Provide Backdoor Entry to Adversary

Provide backdoor to adversary.
Chip fails during critical needs.

Information may bypass giving a non-watermarked or non-encrypted output.

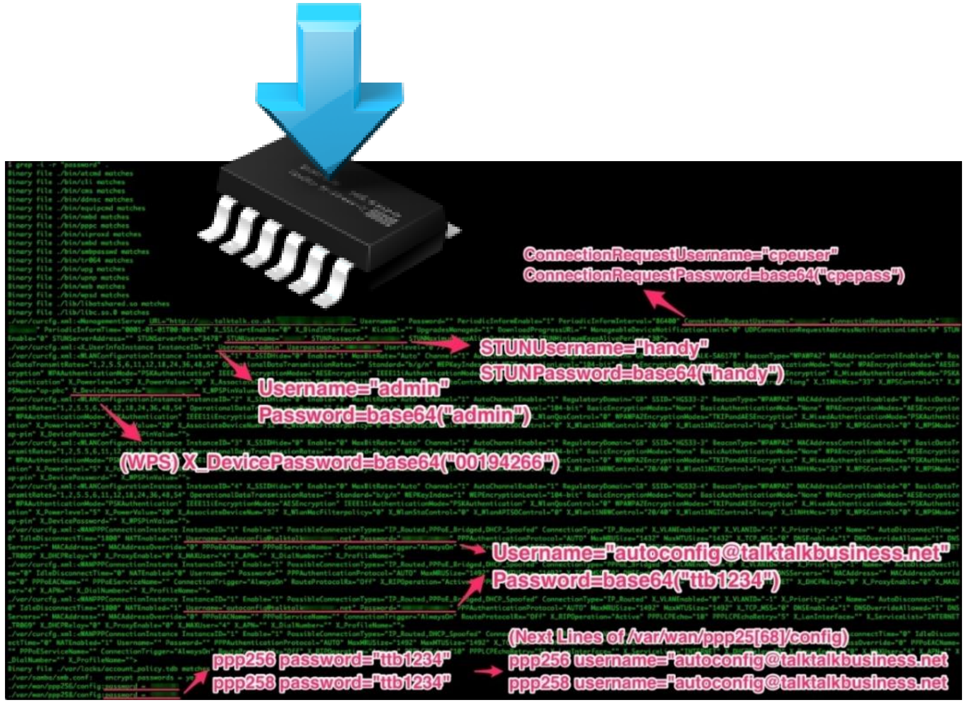
Hardware Trojans



Unprotected/Unsecure Information
Input
Watermarking and/or Cryptography Processor
Protected/Secure Information
Trojan
Output
Select

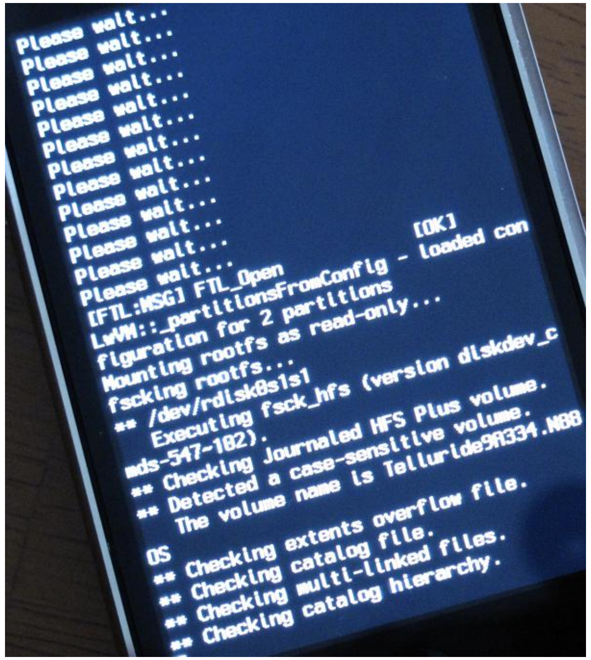
Source: Mohanty 2015, McGraw-Hill 2015

Firmware Reverse Engineering – Security Threat for Embedded System



```
ConnectionRequestUsername="cpeuser"
ConnectionRequestPassword=base64("cpepass")
STUNUsername="handy"
STUNPassword=base64("handy")
Username="admin"
Password=base64("admin")
(WPS) X_DevicePassword=base64("00194266")
Username="autoconfig@talktalkbusiness.net"
Password=base64("ttb1234")
(Next Lines of /var/wan/ppp25[68]/config)
ppp256 password="ttb1234"
ppp258 password="ttb1234"
ppp256 username="autoconfig@talktalkbusiness.net"
ppp258 username="autoconfig@talktalkbusiness.net"
```

Extract, modify, or reprogram code



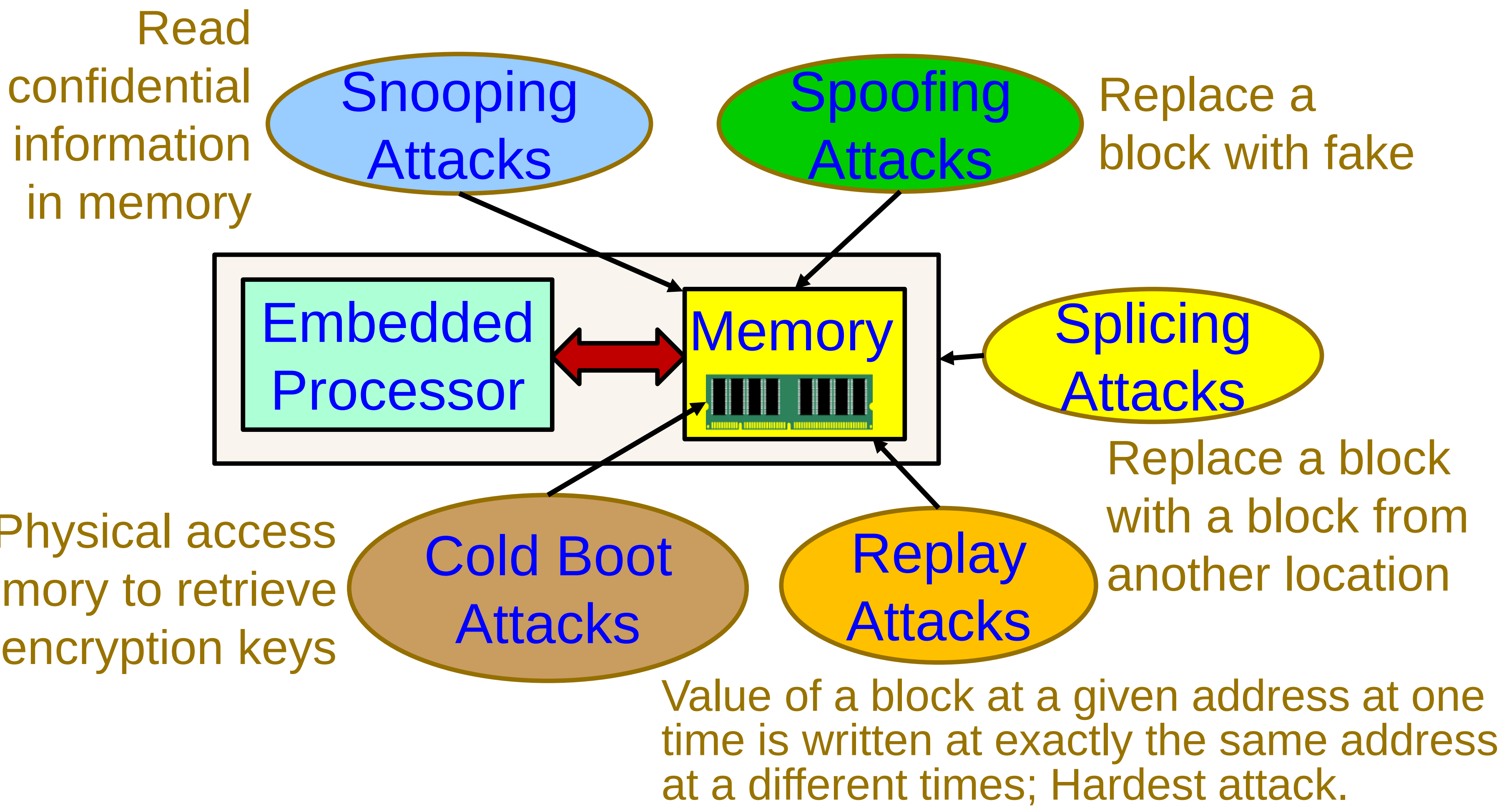
```
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...
Please wait...                     [OK]
[FTL:MSG] FTL_Open
LwVM::_partitionsFromConfig - loaded con
figuration for 2 partitions
Mounting rootfs as read-only...
fscking rootfs...
** /dev/rdisk0s1s1
   Executing fsck_hfs (version diskdev_c
mds-547-102).
** Checking Journaled HFS Plus volume.
** Detected a case-sensitive volume.
** The volume name is Telluride9A334.N88
   
OS
** Checking extents overflow file.
** Checking catalog file.
** Checking multi-linked files.
** Checking catalog hierarchy.
```

OS exploitation,
Device jailbreaking

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

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

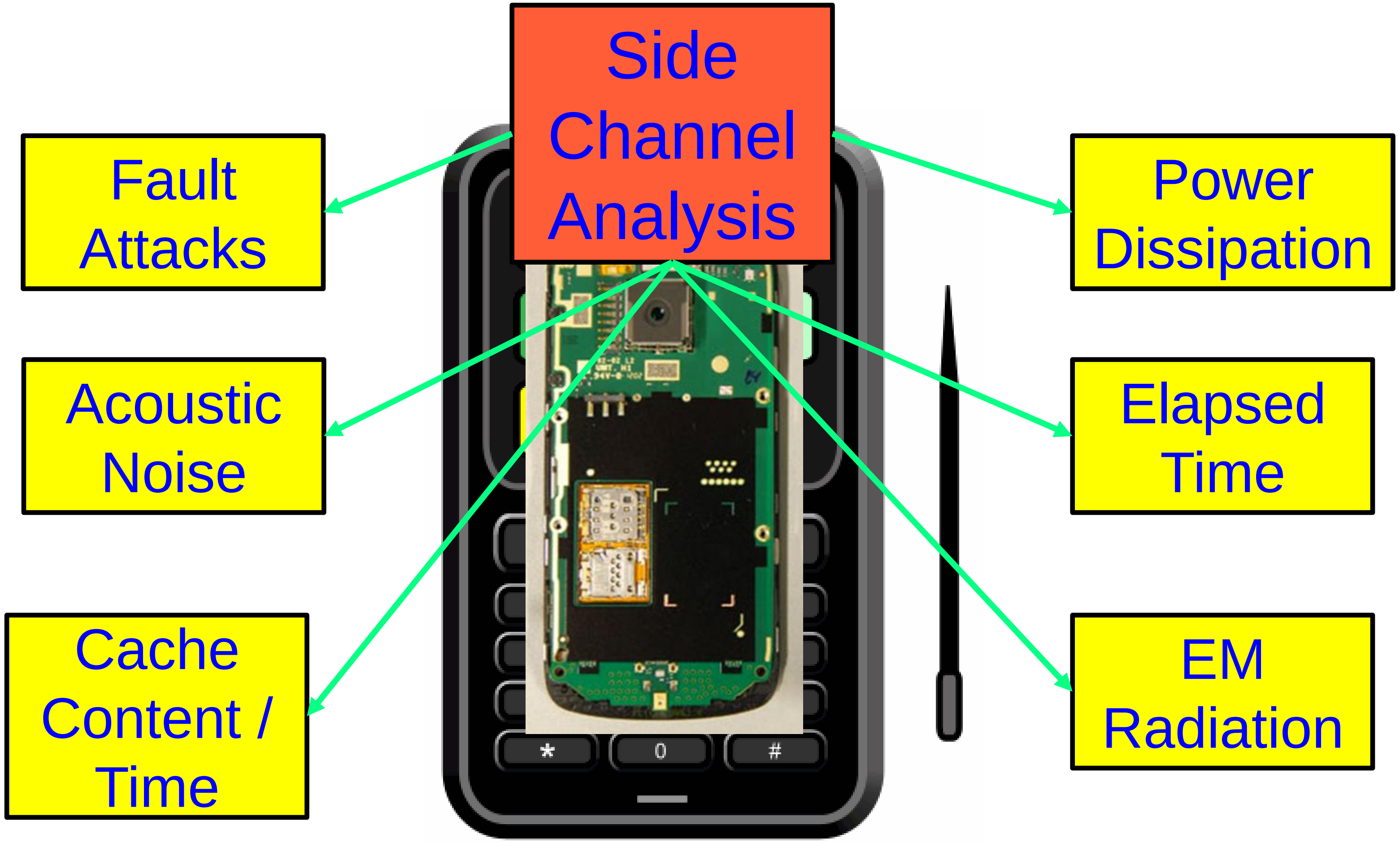
Attacks on Embedded Systems’ Memory



Read confidential information in memory
Snooping Attacks
Spoofing Attacks
Replace a block with fake
Embedded Processor
Memory
Splicing Attacks
Replace a block with a block from another location
Physical access memory to retrieve encryption keys
Cold Boot Attacks
Replay Attacks
Value of a block at a given address at one time is written at exactly the same address at a different times; Hardest attack.

Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, “TSV: A Novel Energy Efficient Memory Integrity Verification Scheme for Embedded Systems”, *Elsevier Journal of Systems Architecture*, Vol. 59, No. 7, Aug 2013, pp. 400-411.

Side Channel Analysis Attacks



Side Channel Analysis

Fault Attacks

Acoustic Noise

Cache Content / Time

Power Dissipation

Elapsed Time

EM Radiation

Breaking Encryption is not a matter of Years, but a matter of Hours.

Source: Parameswaran Keynote iNIS-2017

Security, Privacy, and IP Rights

Hardware
Trojan

System Security

Data Security

System Privacy

Data Privacy

Counterfeit Hardware
(IP Rights Violation)

Source: Mohanty ICIT 2017 Keynote

A GUIDE TO THE CE INNERVERSE

IEEE Consumer Electronics MAGAZINE

VOL. 6, NO. 3, July 2017

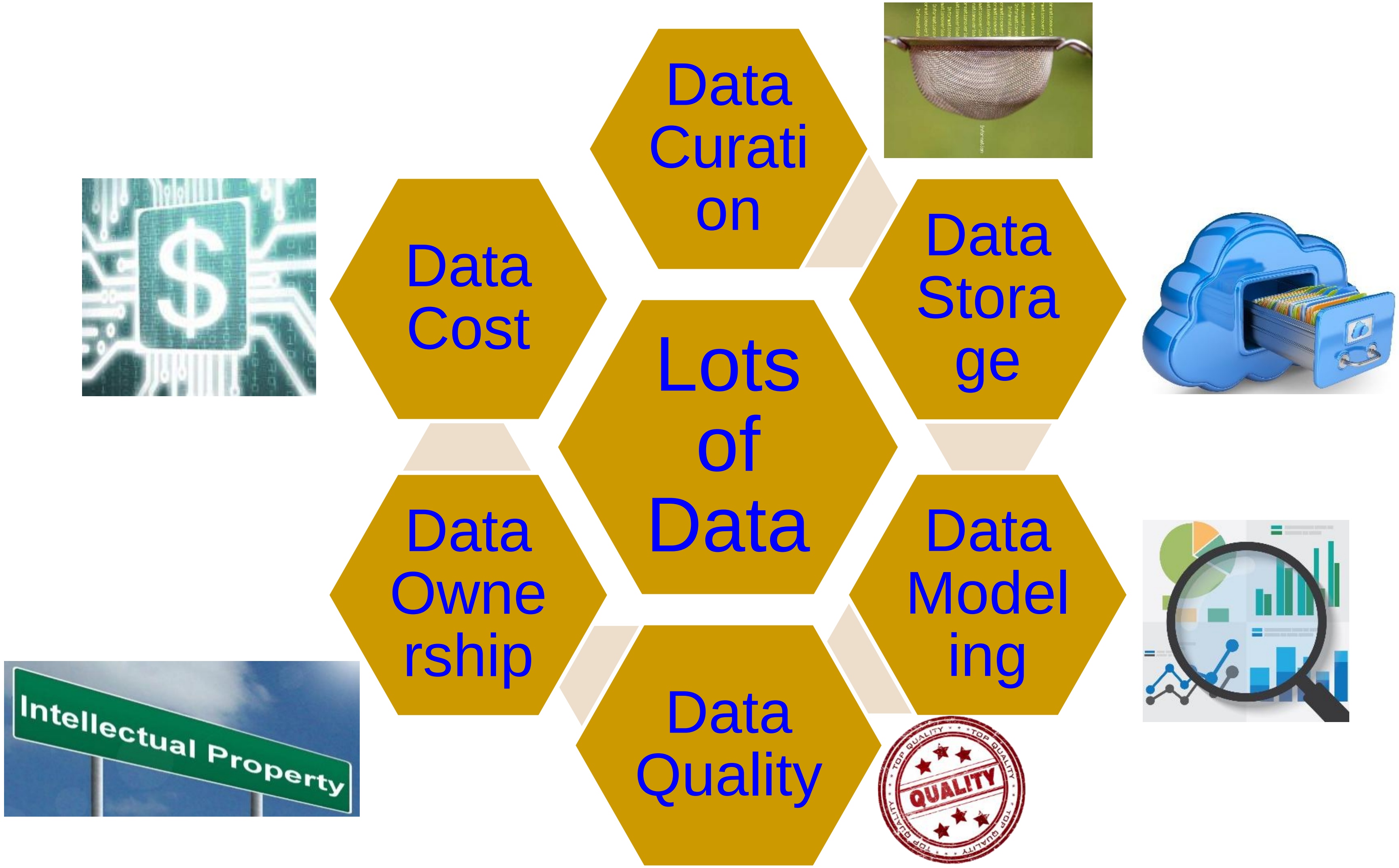
Feeling Secure?

Examining Hardware IP Protection and Trojans

IEEE

July 2017

Challenges of Data in IoT/CPS are Multifold



Lots of Data

Data Curation

Data Storage

Data Modeling

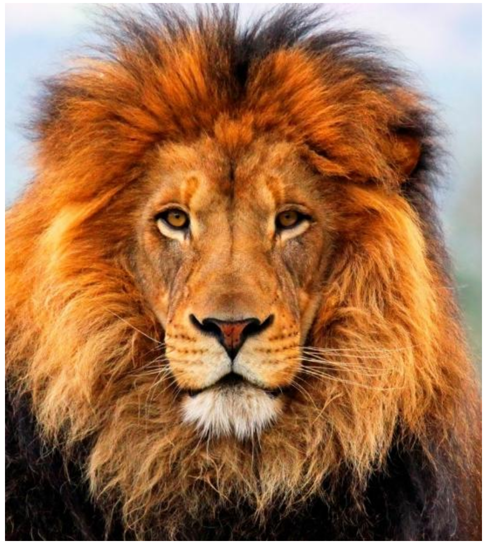
Data Quality

Data Ownership

Data Cost

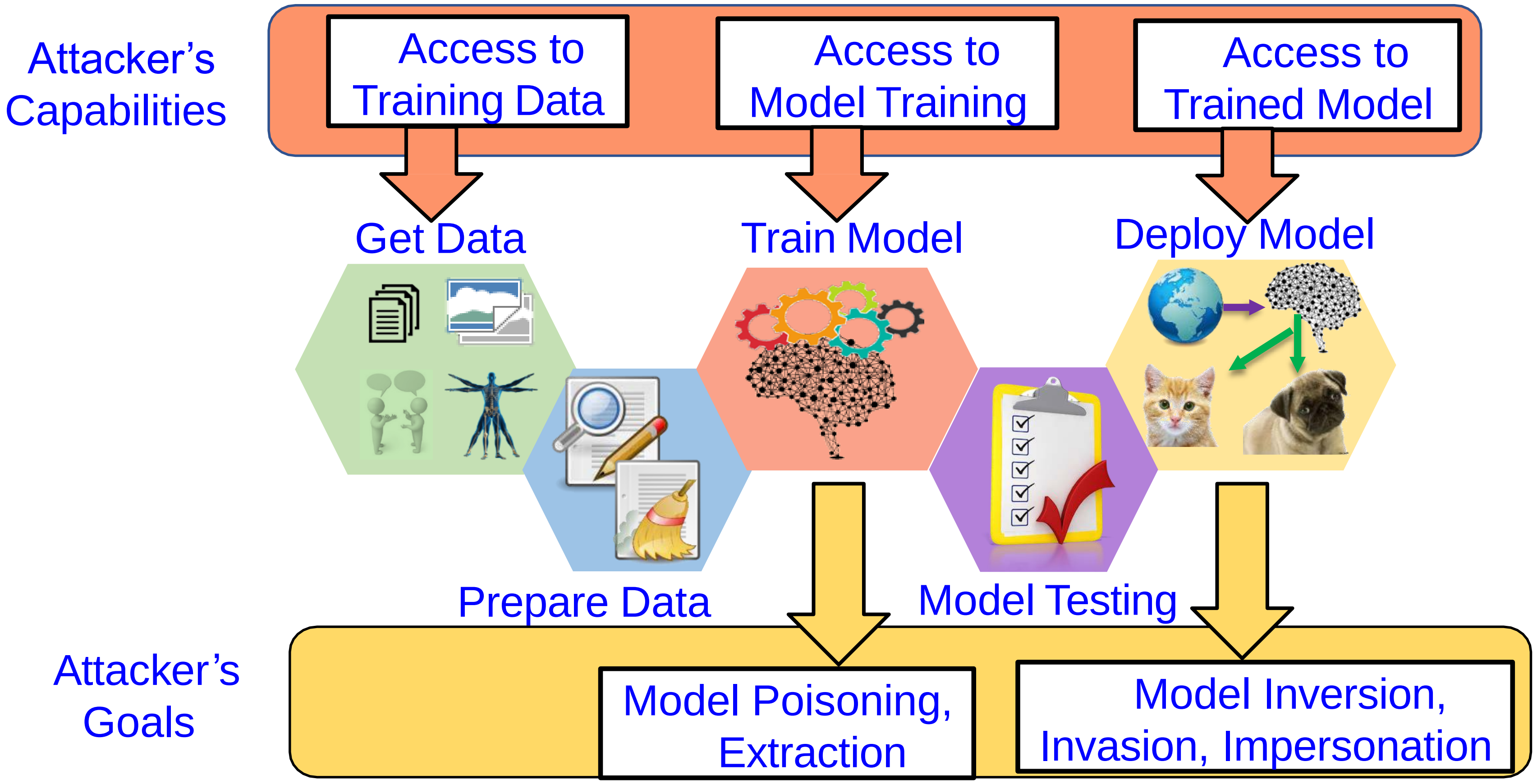
DNNs are not Always Smart

- Why not use Fake Data?
- "Fake Data" has some interesting advantages:
  - Avoids *privacy issues* and side-steps *new regulations* (e.g. General Data Protection Regulation or GDPR)
  - Significant cost reductions in data acquisition and annotation for big datasets



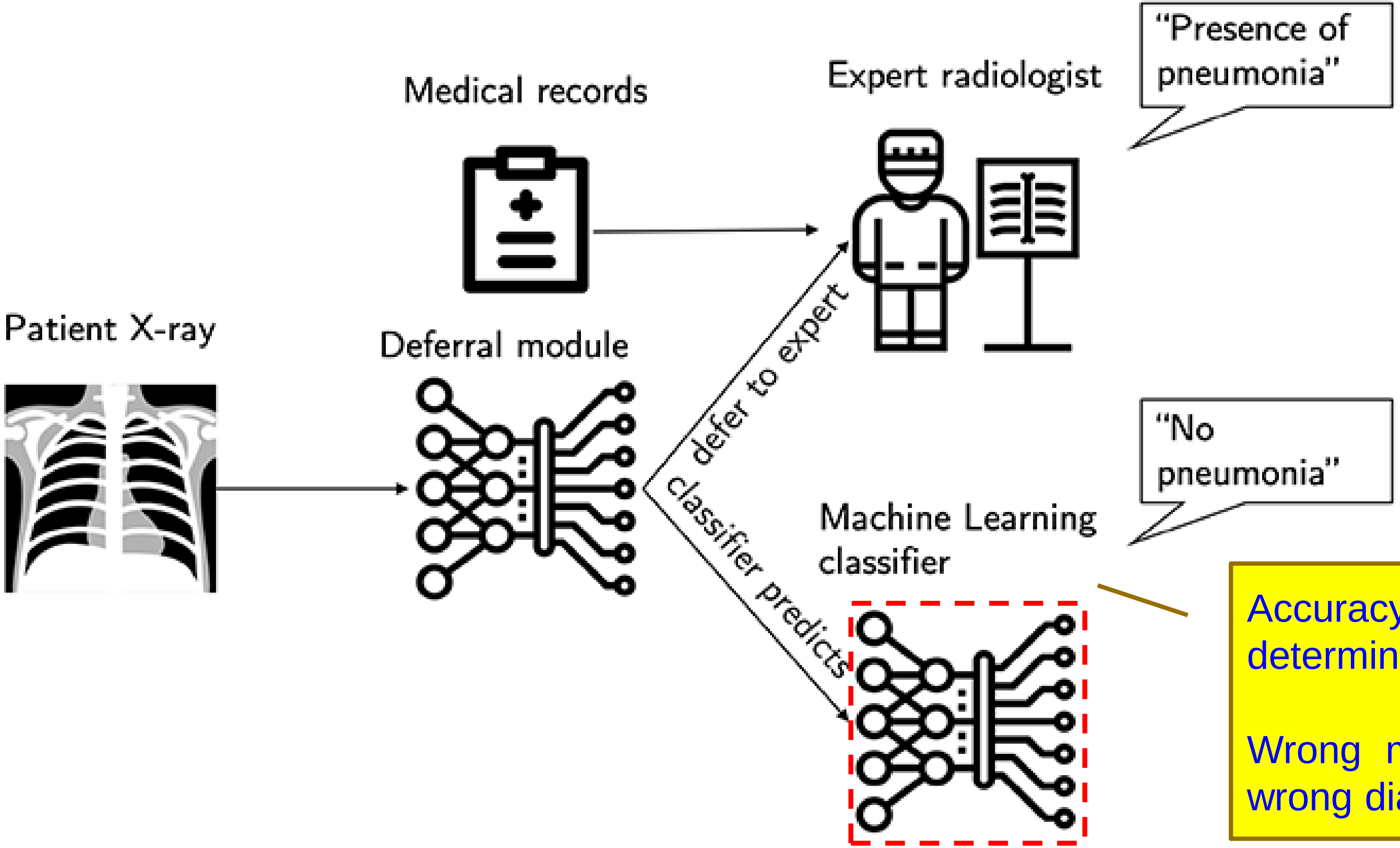
Source: Corcoran Keynote 2018

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

Wrong ML Model → Wrong Diagnosis

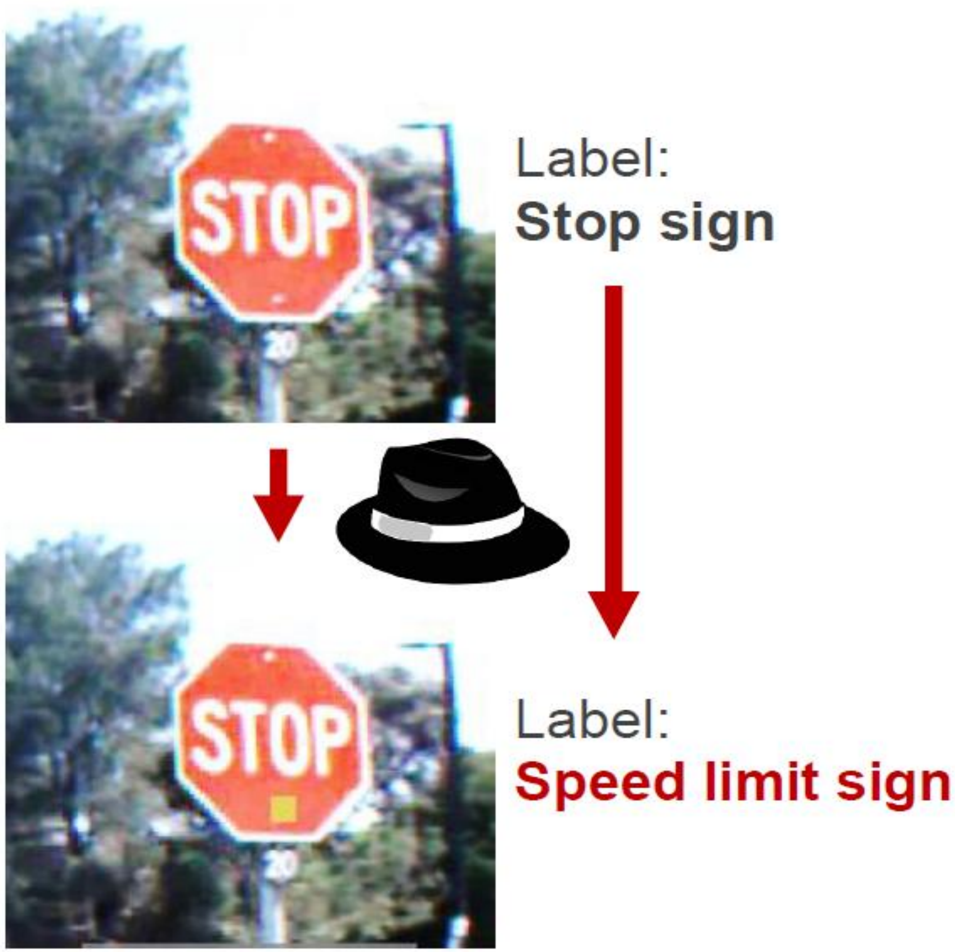


Accuracy is important determine pneumonia

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

AI Security - Trojans in Artificial Intelligence (TrojAI)



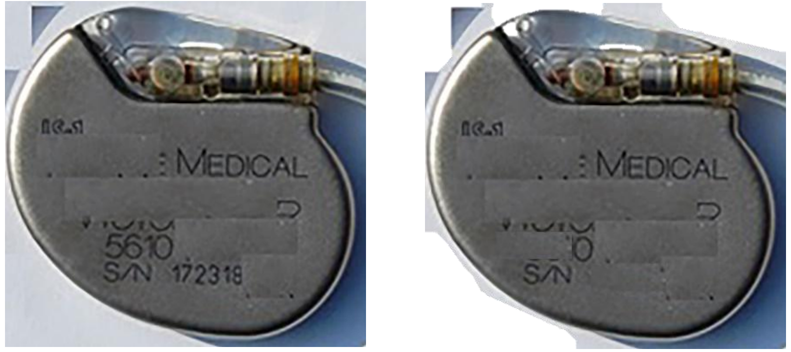
Source: https://www.iarpa.gov/index.php?option=com_content&view=article&id=1150&Itemid=448

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

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

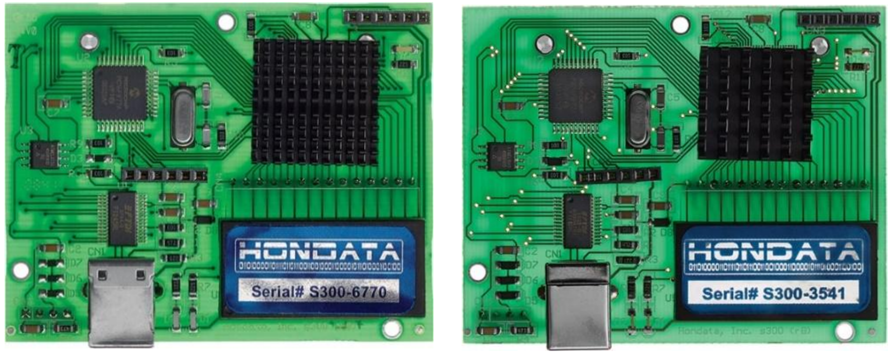
AI can be fooled by fake data

AI can create fake data (Deepfake)



Authentic Fake

An implantable medical device



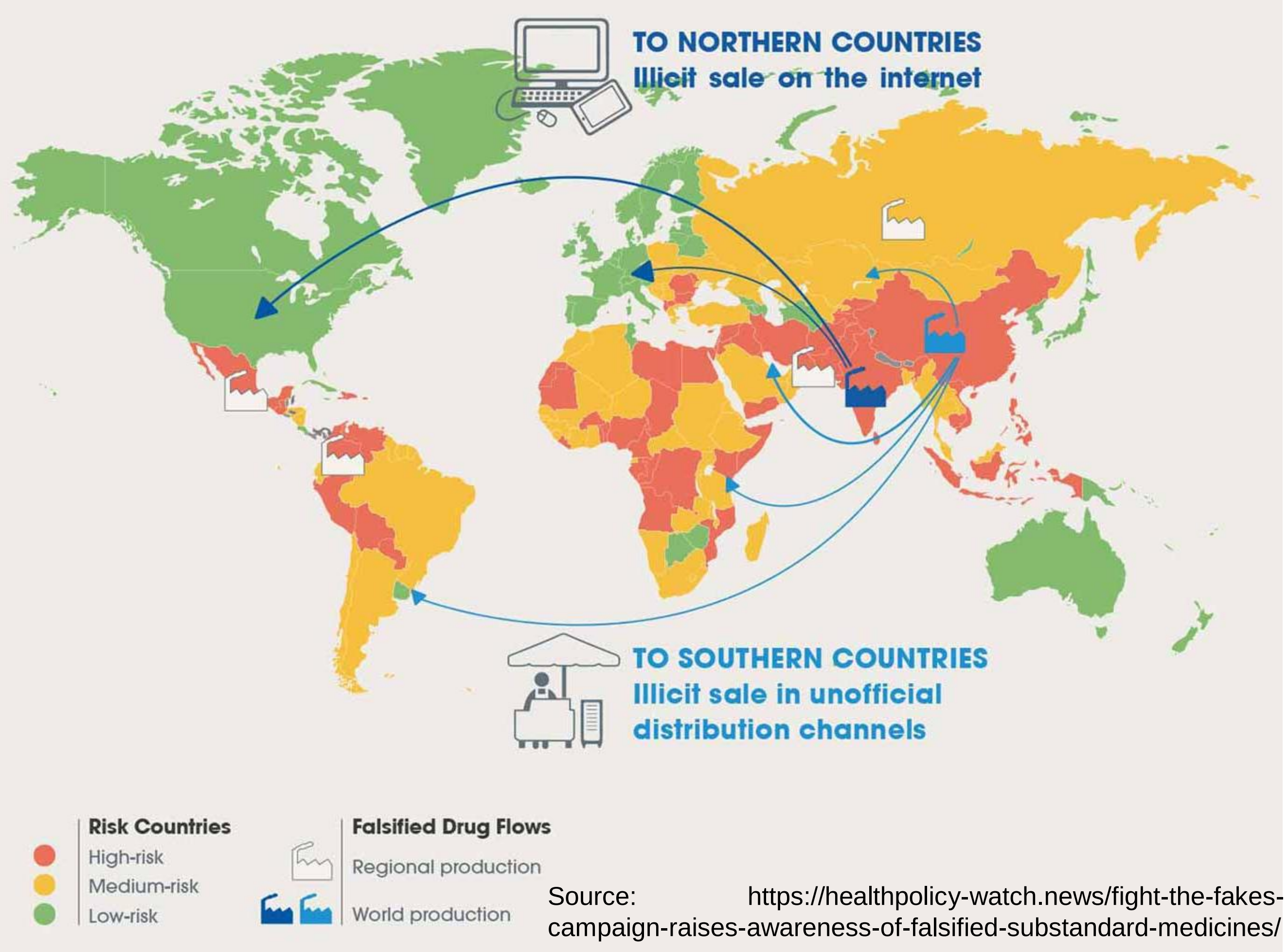
Authentic Fake

A plug-in for car-engine computers

Fake Medicine - Serious Global Issue

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

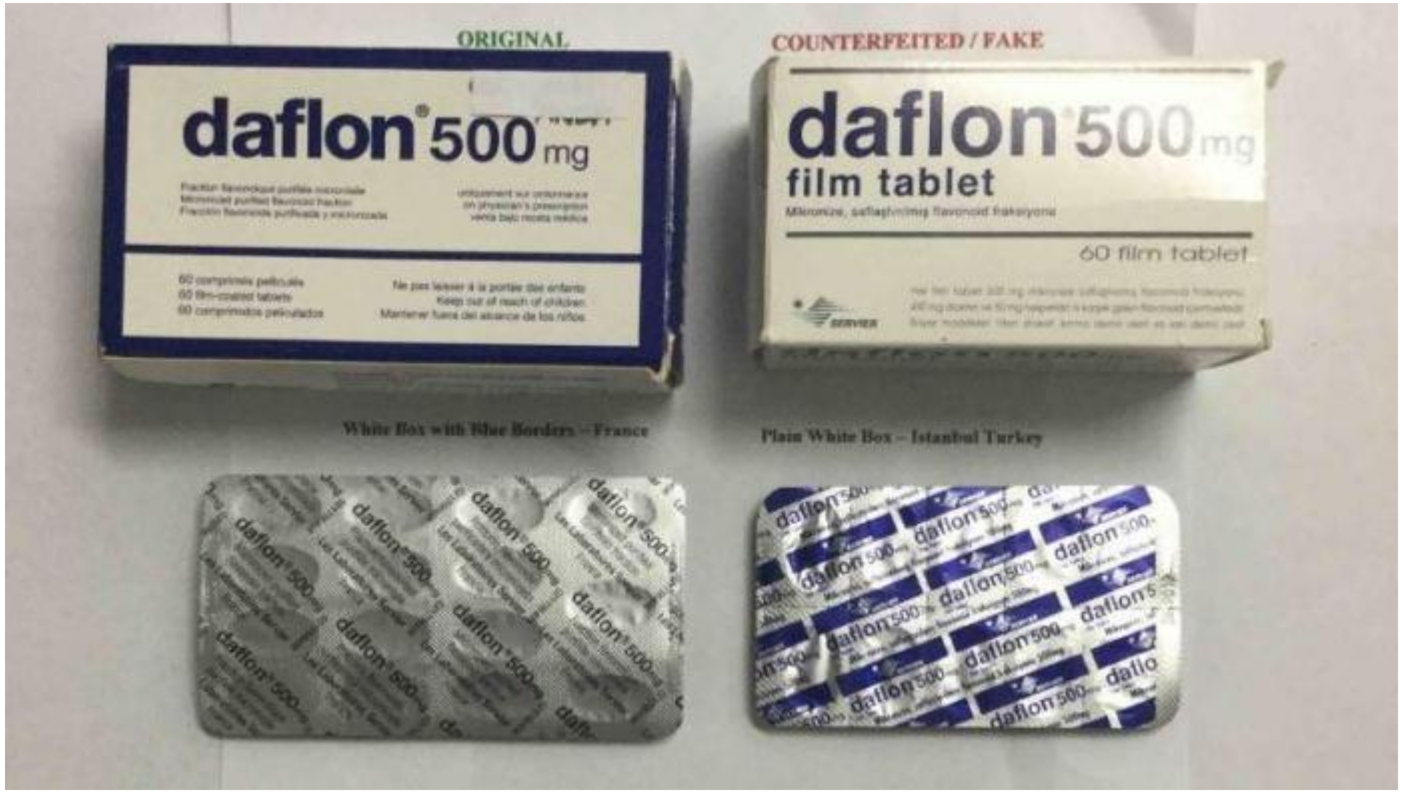
Source: https://fraud.org/fakerx/fake-drugs-and-their-risks/counterfeit-drugs-are-a-global-problem/



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

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

Counterfeits in Healthcare



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

The original product:

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

The fake product:

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

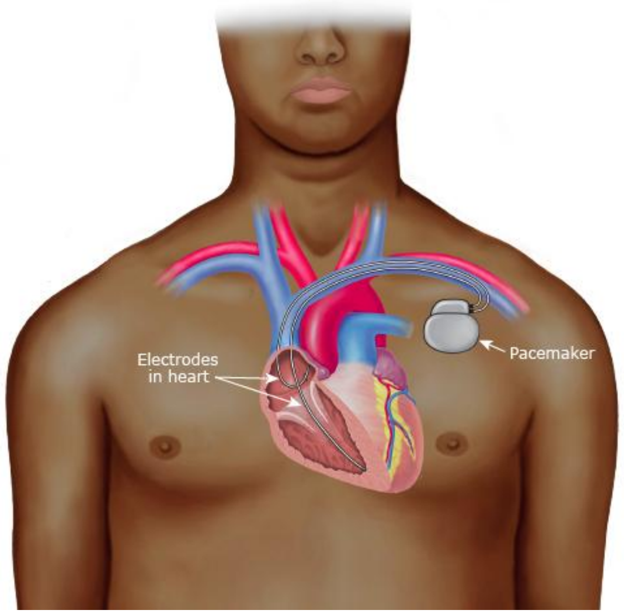
Daflon 500 is used to treat gravitational (stasis) dermatitis and dermatofibrosclerosis

Fake is Cheap – Why not Buy?

Fake ECU Inside

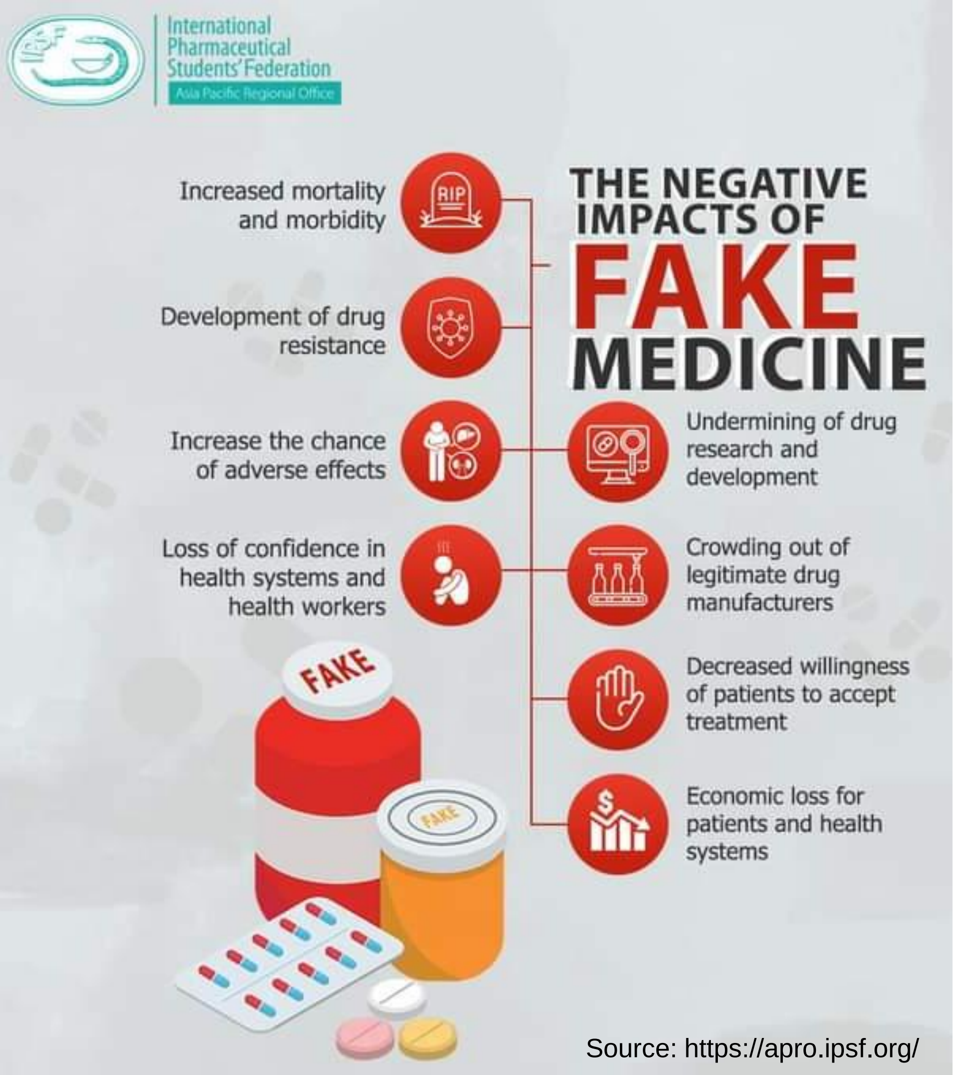
Source: https://www.quora.com

Is my Pacemaker Authentic or Fake?



Fake battery inside

Source: https://nypost.com/



International Pharmaceutical Students' Federation
Asia Pacific Regional Office

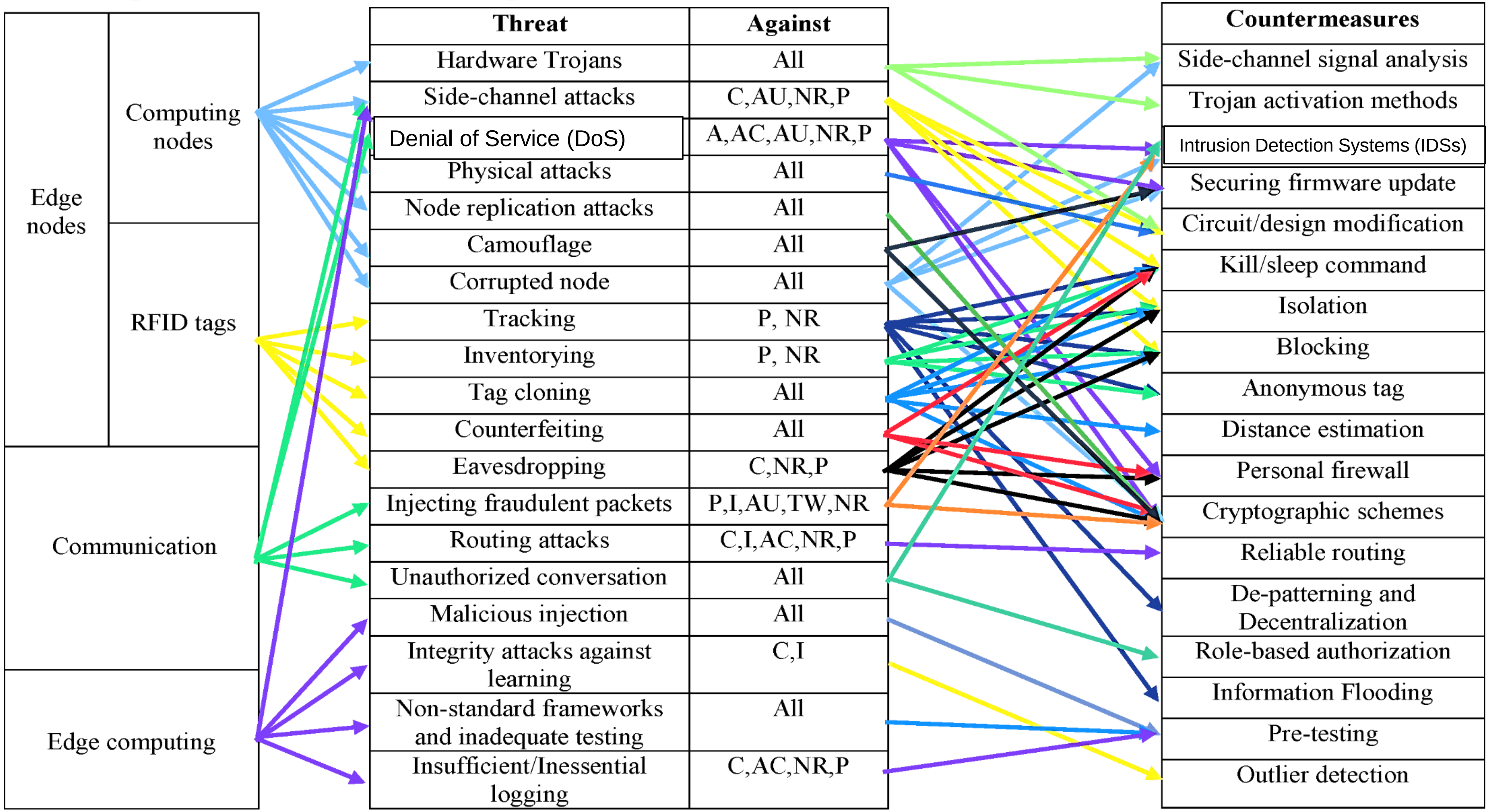
THE NEGATIVE IMPACTS OF FAKE MEDICINE

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

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

Cybersecurity Solution for IoT/CPS

IoT Cybersecurity - Attacks and Countermeasures



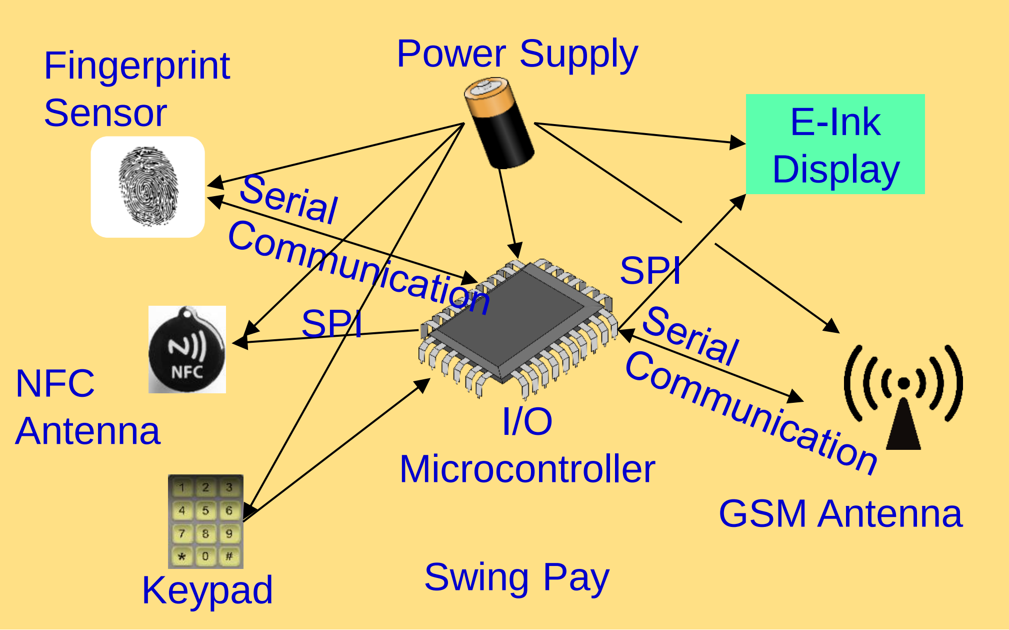
Threat	Against
Hardware Trojans	All
Side-channel attacks	C,AU,NR,P
Denial of Service (DoS)	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P, NR
Inventorying	P, NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	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

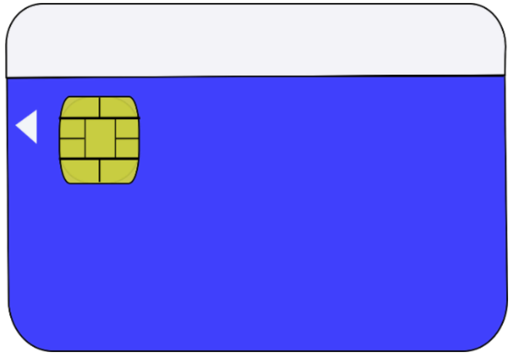
Countermeasures
Side-channel signal analysis
Trojan activation methods
Intrusion Detection Systems (IDSs)
Securing firmware update
Circuit/design modification
Kill/sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De-patterning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

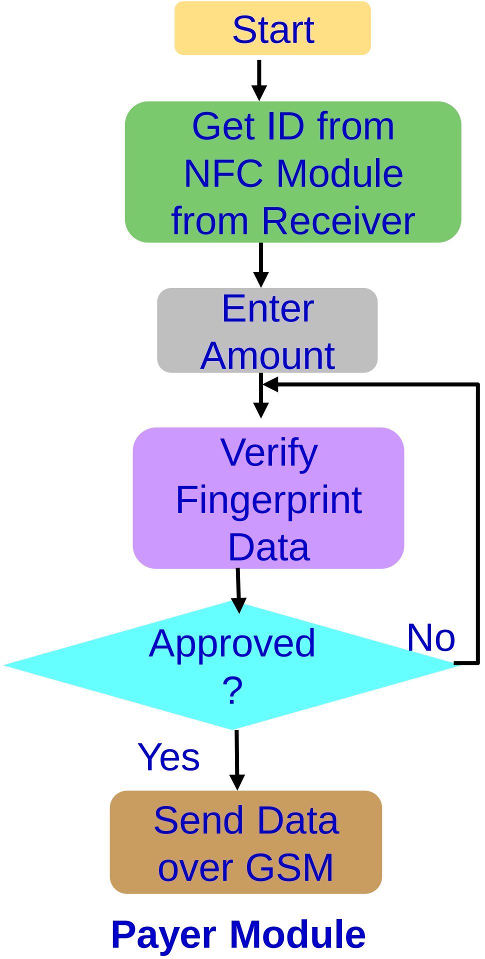
C- Confidentiality, I – Integrity, A - Availability, AC – Accountability, AU – Auditability, TW – Trustworthiness, NR - Non-repudiation, P - Privacy

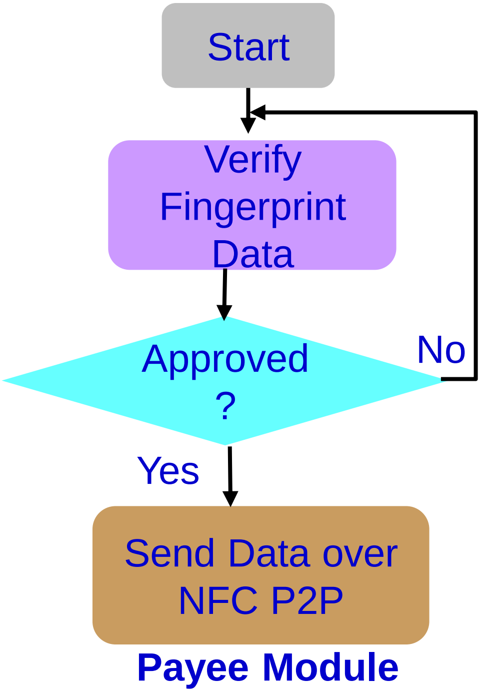
Source: A. Mosenia, and Niraj K. Jha. "A Comprehensive Study of Security of Internet-of-Things", *IEEE Transactions on Emerging Topics in Computing*, 5(4), 2016, pp. 586-602.

Our Swing-Pay: NFC Cybersecurity Solution



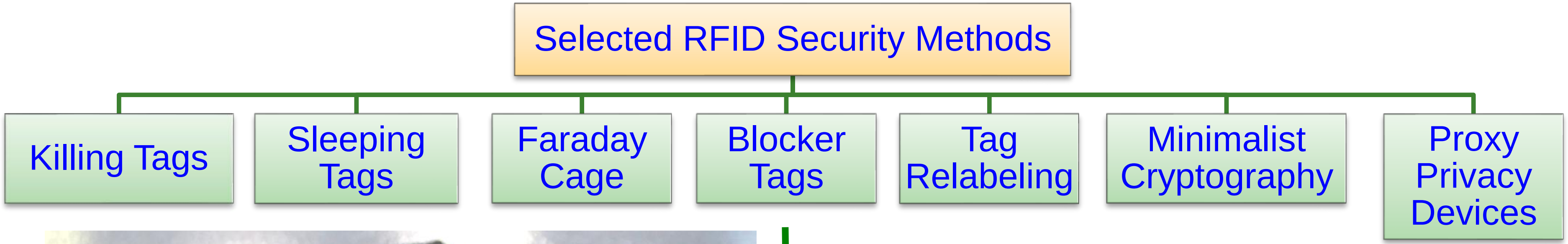






Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

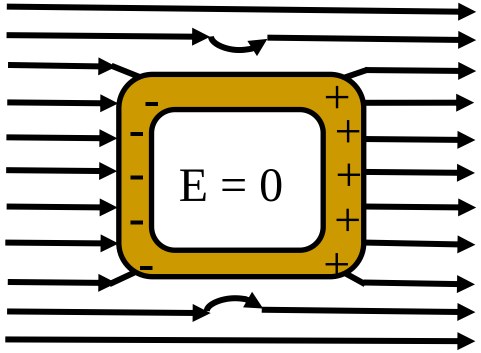
RFID Cybersecurity - Solutions

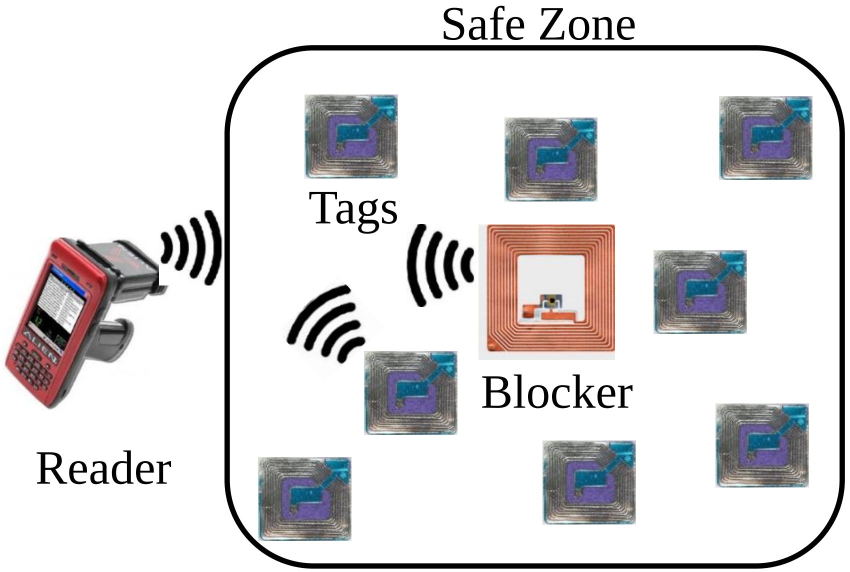


Selected RFID Security Methods

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

Faraday Cage

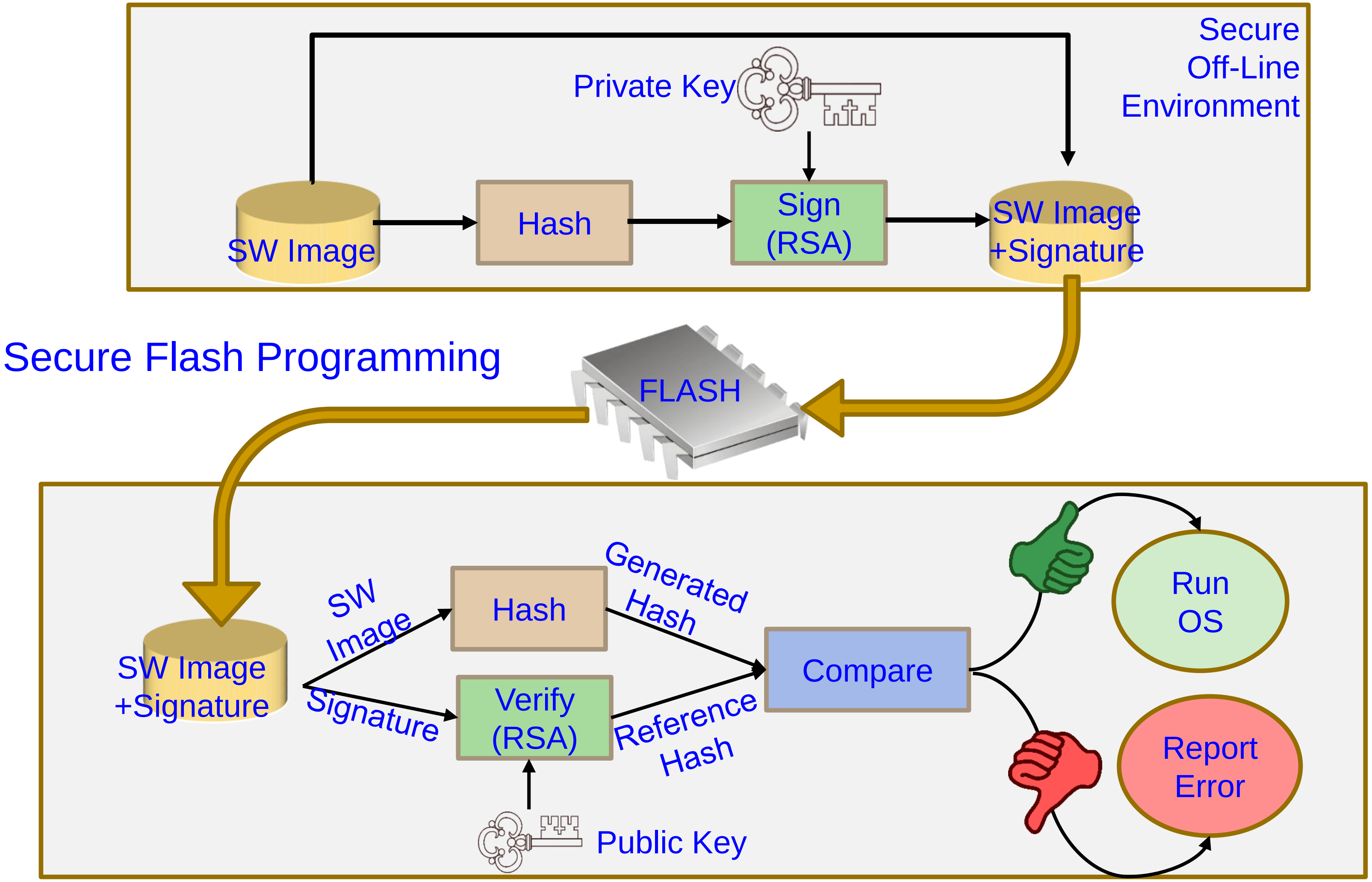




Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution



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

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

Nonvolatile / Harddrive Storage

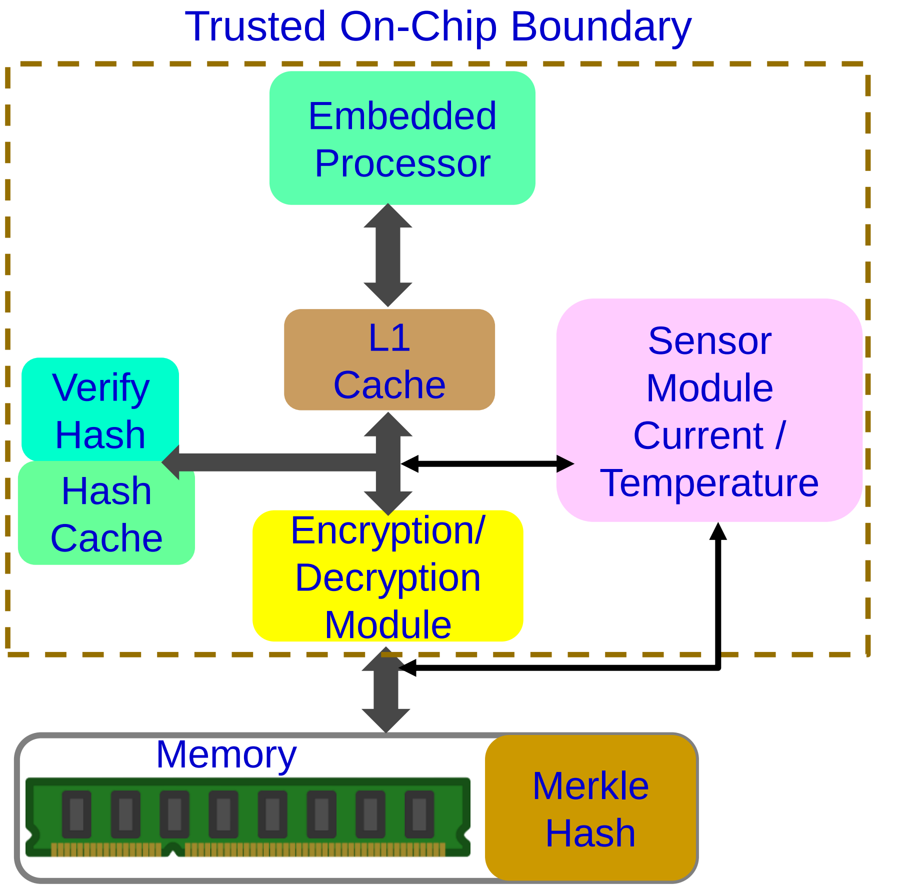
Hardware-based encryption of data secured/protected by strong password/PIN authentication.

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

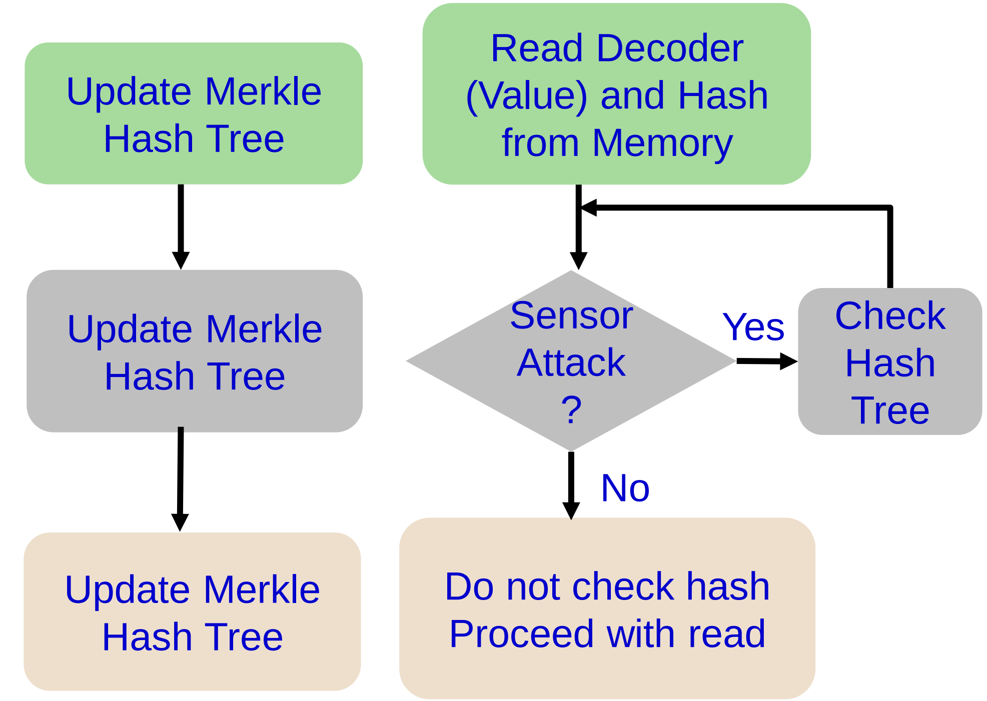
Some performance penalty due to increase in latency!

How Cloud storage changes this scenario?

Embedded Memory Security



On-Chip/On-Board Memory Protection



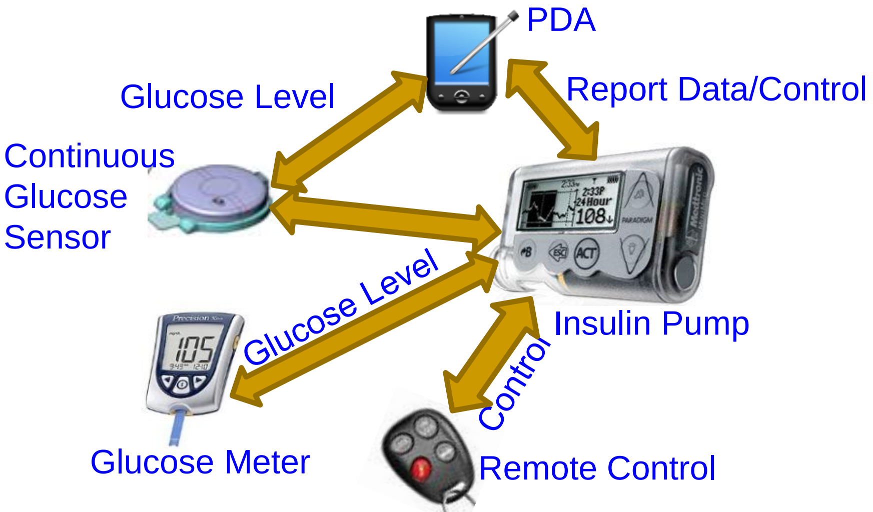
Write Operation

Read Operation

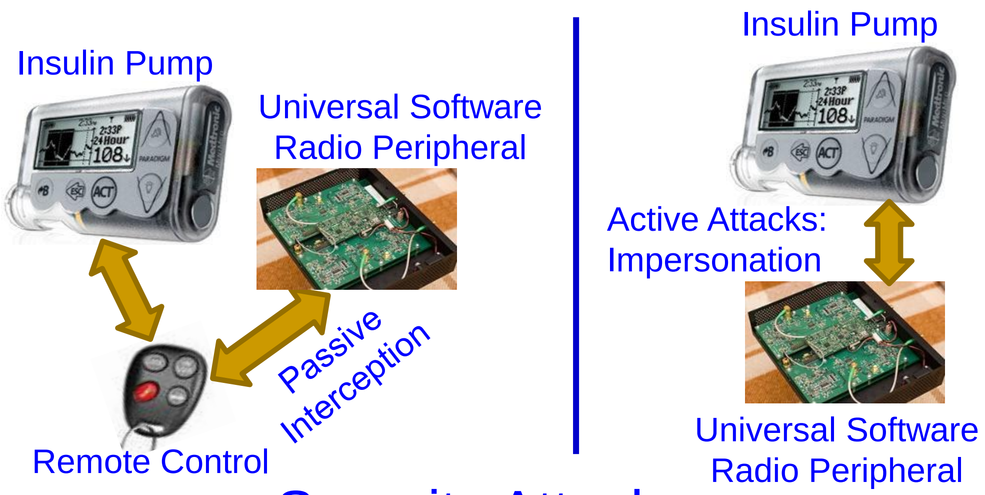
Memory integrity verification with 85% energy savings with minimal performance overhead.

Source: S. Nimgaonkar, M. Gomathisankaran, and S. P. Mohanty, "MEM-DnP: A Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems", *Springer Circuits, Systems, and Signal Processing Journal (CSSP)*, Volume 32, Issue 6, December 2013, pp. 2581--2604.

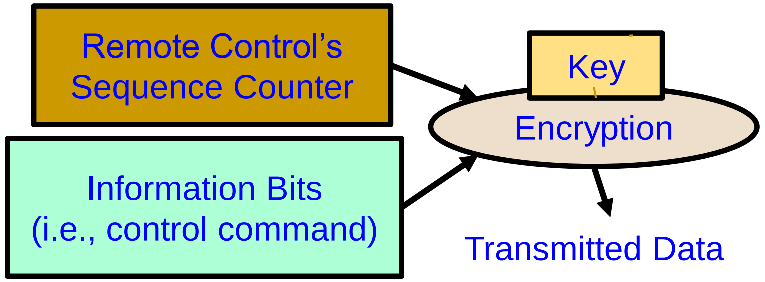
Smart Healthcare Cybersecurity



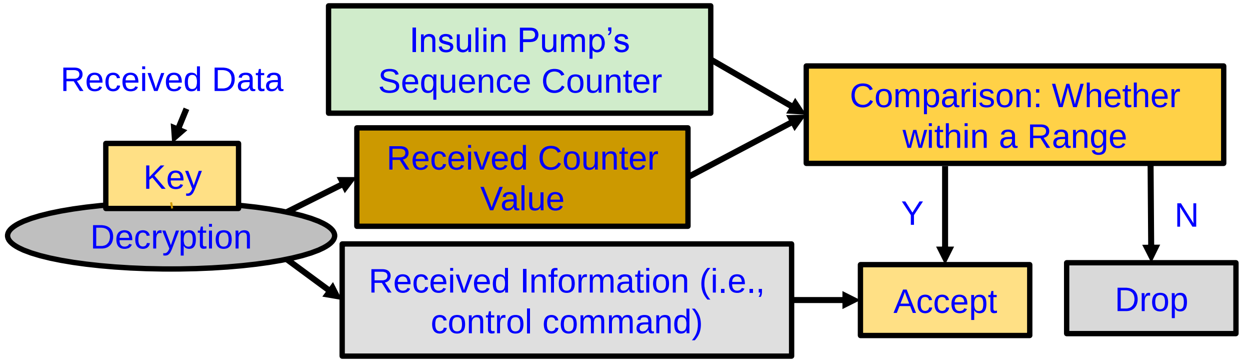
Insulin Delivery System


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

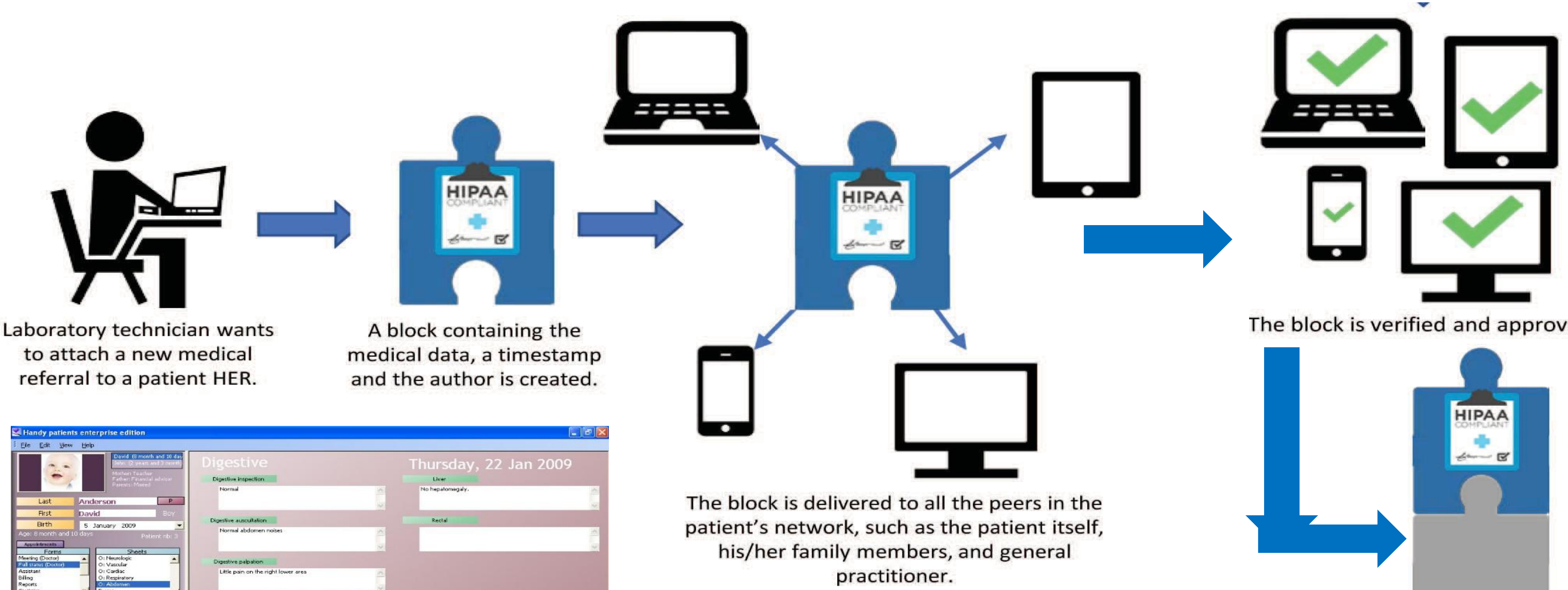
Rolling Code Encoder in Remote Control


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

Rolling Code Decoder in Insulin Pump

Source: Li and Jha 2011: HEALTH 2011

Blockchain in Smart Healthcare

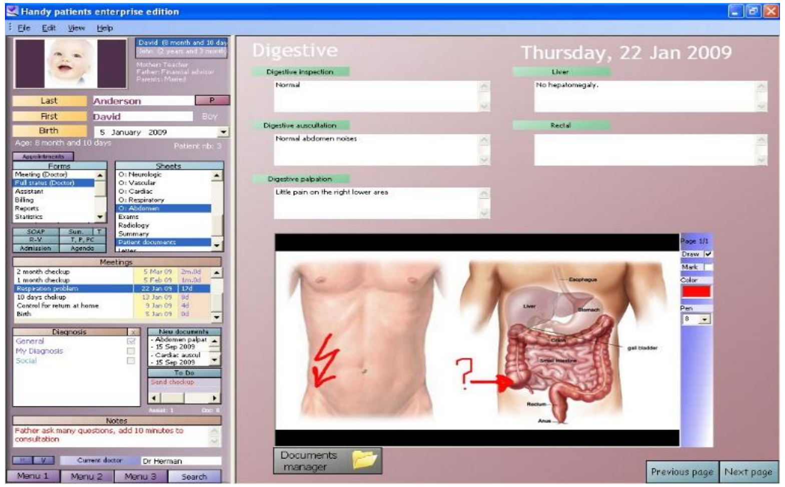


Laboratory technician wants to attach a new medical referral to a patient HER.

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

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

The block is verified and approved.



David (8 month and 10 days)
John (2 years and 3 months)
Mother: Teacher
Father: Financial advisor
Parents: Maried

Last: Anderson
First: David
Boy
Birth: 5 January 2009
Age: 6 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

Assist: 1 Doc: 8

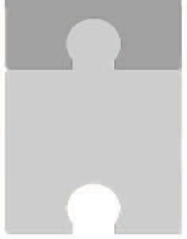
Notes
Father ask many questions, add 10 minutes to consultation

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

Can it preserve privacy?

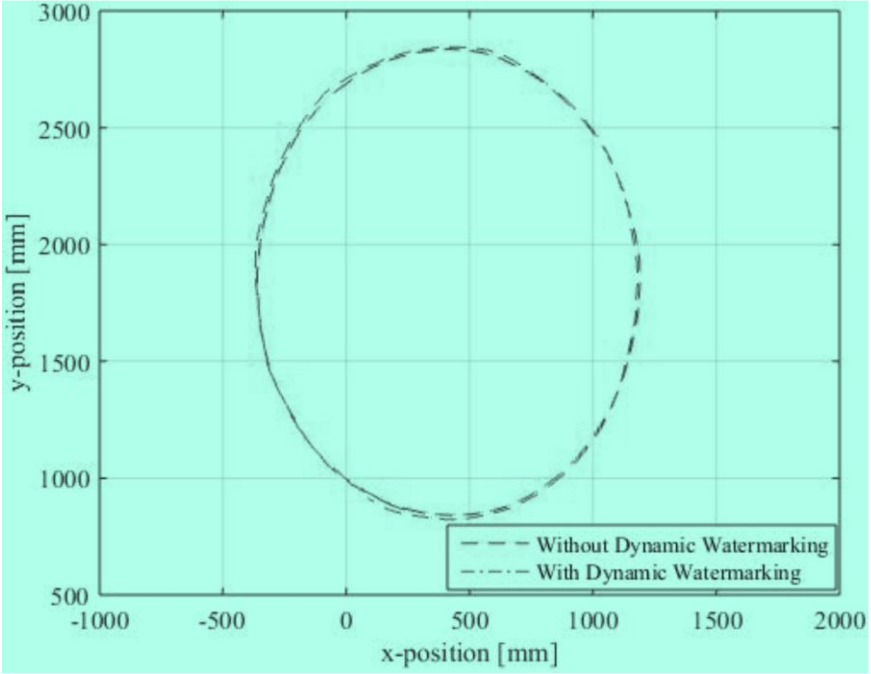


The block is inserted in the chain and linked with the previous blocks.

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

Autonomous Car Cybersecurity – Collision Avoidance

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



Source: Ko 2016, CPS-Sec 2016

Drawbacks of Existing Cybersecurity Solutions

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

IT Cybersecurity

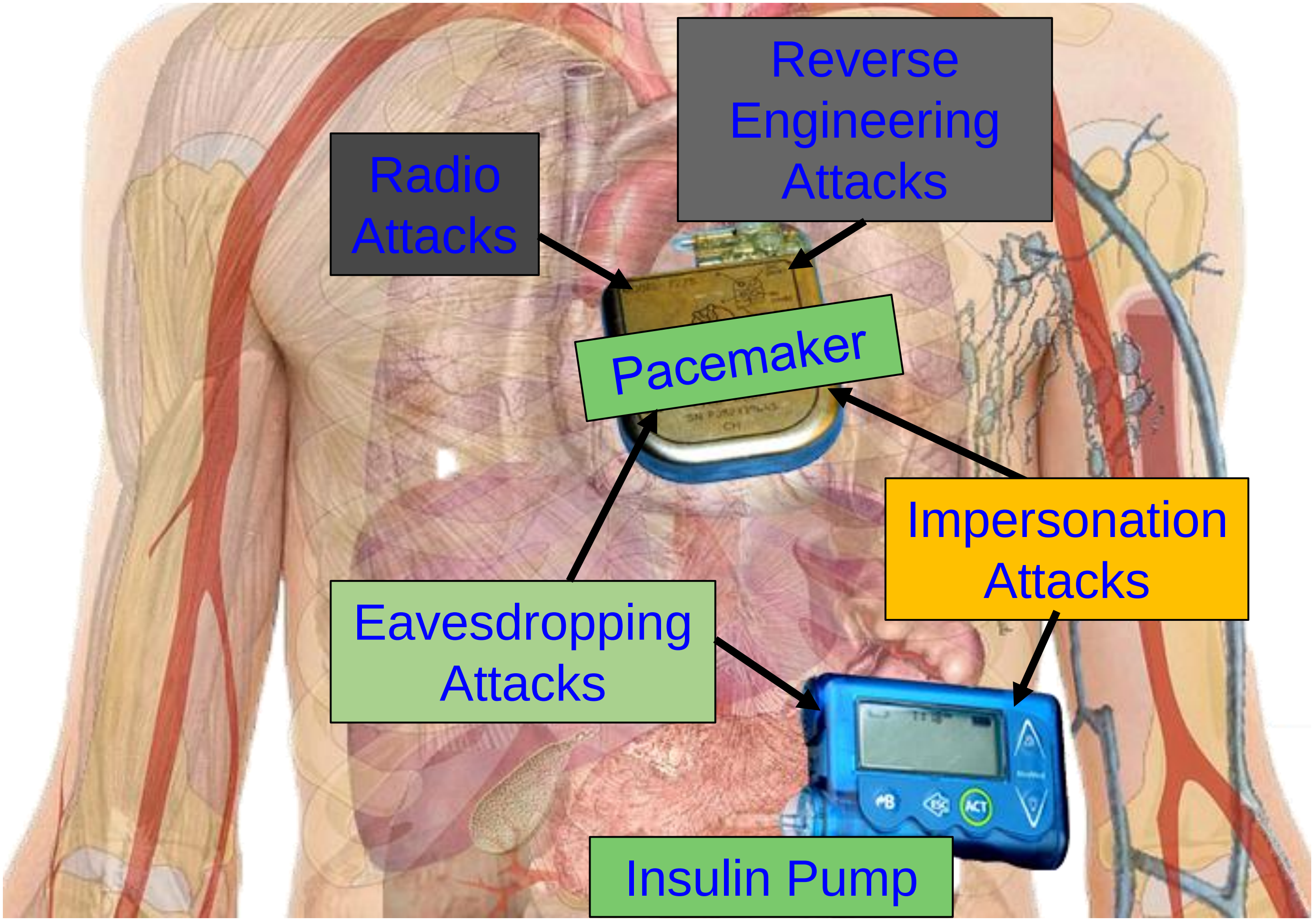
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

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

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

Cybersecurity Measures in Healthcare Cyber-Physical Systems is Hard

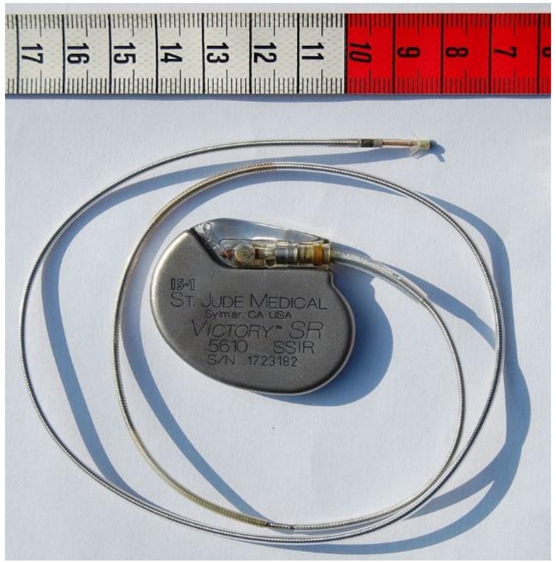


Collectively (WMD+IMD): Implantable and Wearable Medical Devices (IWMDs)

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



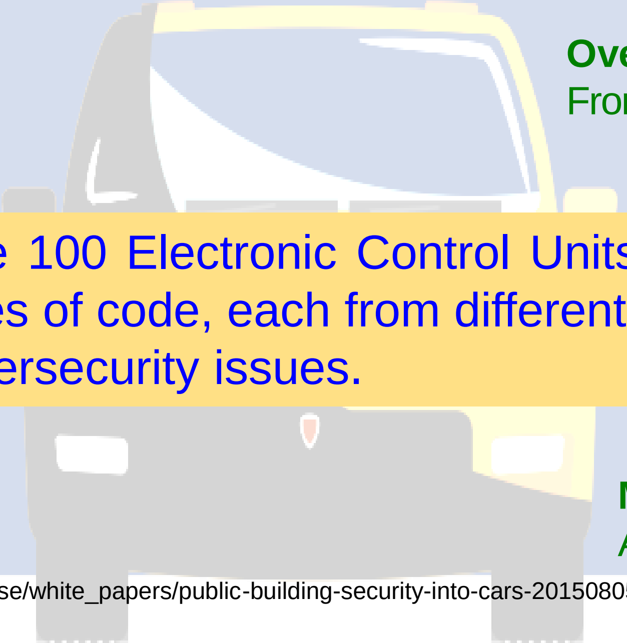
Pacemaker
Battery Life
- 10 years

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 On-board Diagnostics (OBD-II)

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

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

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

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

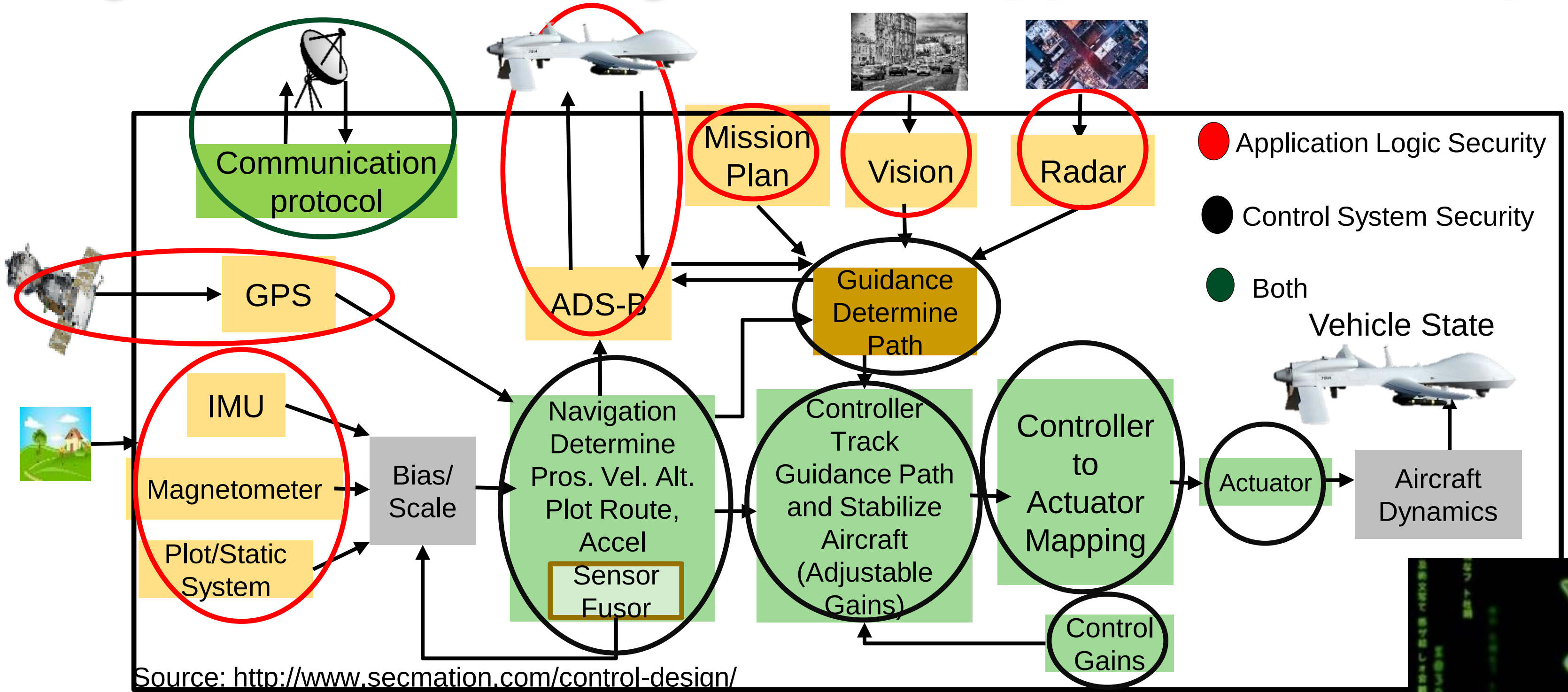
Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf

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

Security Mechanism Affects:
- Latency
- Mileage
- Battery Life

Car Cybersecurity – Latency Constrained

UAV Cybersecurity - Energy & Latency Constrained



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

Cybersecurity Mechanisms Affect:

Battery Life | Latency | Weight | Aerodynamics

UAV Security – Energy and Latency Constraints

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

Smart Grid Security Constraints

Smart Grid – Security Objectives

- Availability
- Integrity
- Confidentiality

Smart Grid – Security Requirements

- Identification
- Authentication
- Authorization
- Trust
- Access Control
- Privacy

Smart Grid – Security Solution Constraints

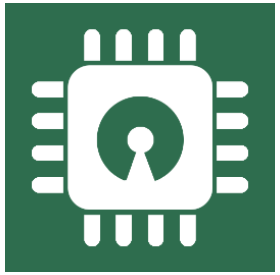
- Transactions Latency
- Communication Latency
- Transactions Computational Overhead
- Energy Overhead on Embedded Devices
- Security Budget

Source: R. K. Pandey and M. Misra, "Cyber security threats - Smart grid infrastructure," in *Proc. National Power Systems Conference (NPSC)*, 2016, pp. 1-6.

Cybersecurity Attacks – Software Vs Hardware Based

Software Based

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



Hardware Based

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

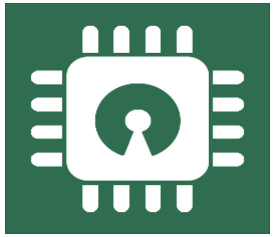
Source: Mohanty ICCE Panel 2018

Cybersecurity Solutions – Software Vs Hardware Based

Software Based

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

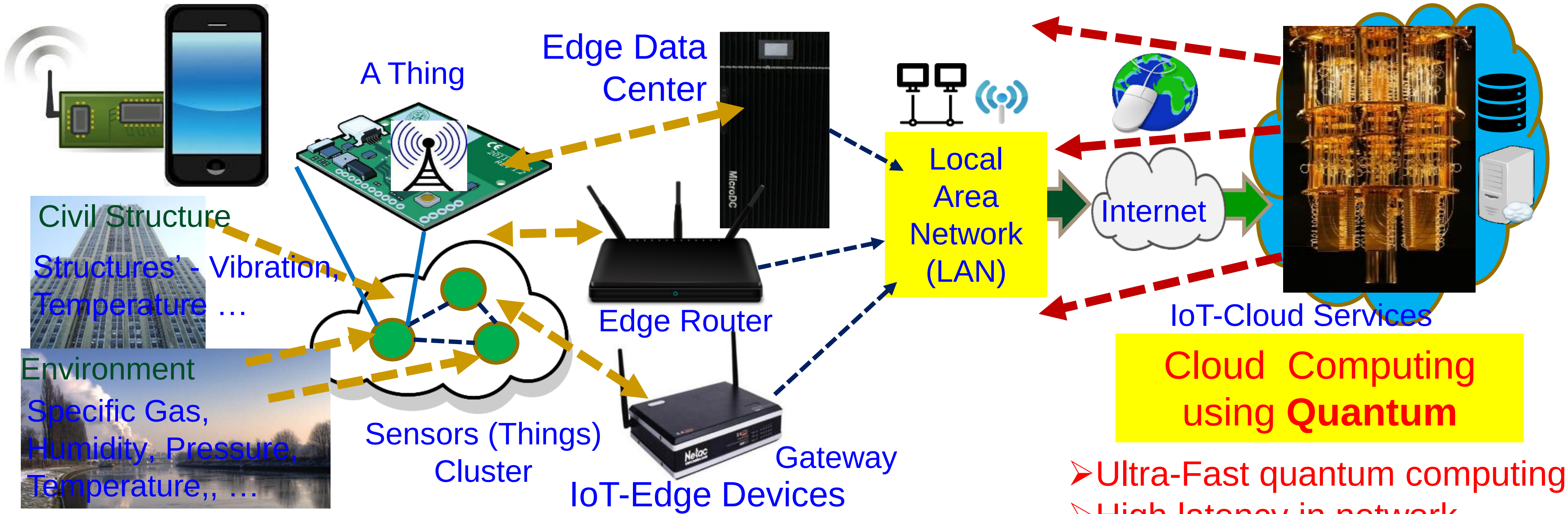
Hardware Based



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

Source: Mohanty ICCE Panel 2018

Cybersecurity Nightmare ← Quantum Computing



A Thing

Edge Data Center

Local Area Network (LAN)

Internet

IoT-Cloud Services

Civil Structure

Structures' - Vibration, Temperature …

Environment

Specific Gas, Humidity, Pressure, Temperature,, …

Sensors (Things) Cluster

Edge Router

Gateway

IoT-End Devices

IoT-Edge Devices

In-Sensor/End-Device Computing

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

Edge Computing

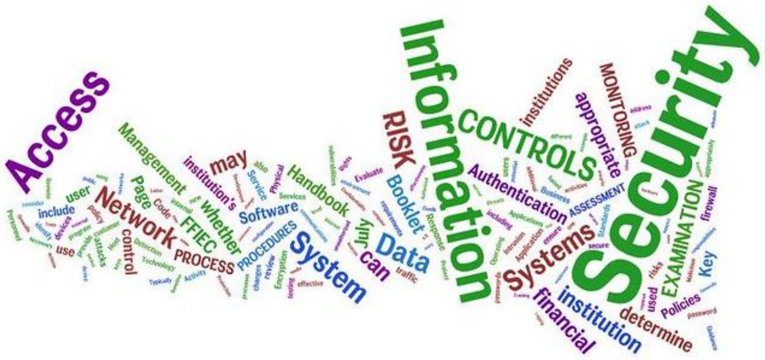
- Less computational resource
- Minimal latency in network
- Lightweight security

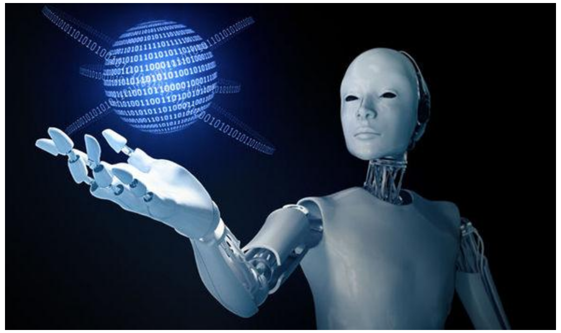
Cloud Computing using Quantum

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

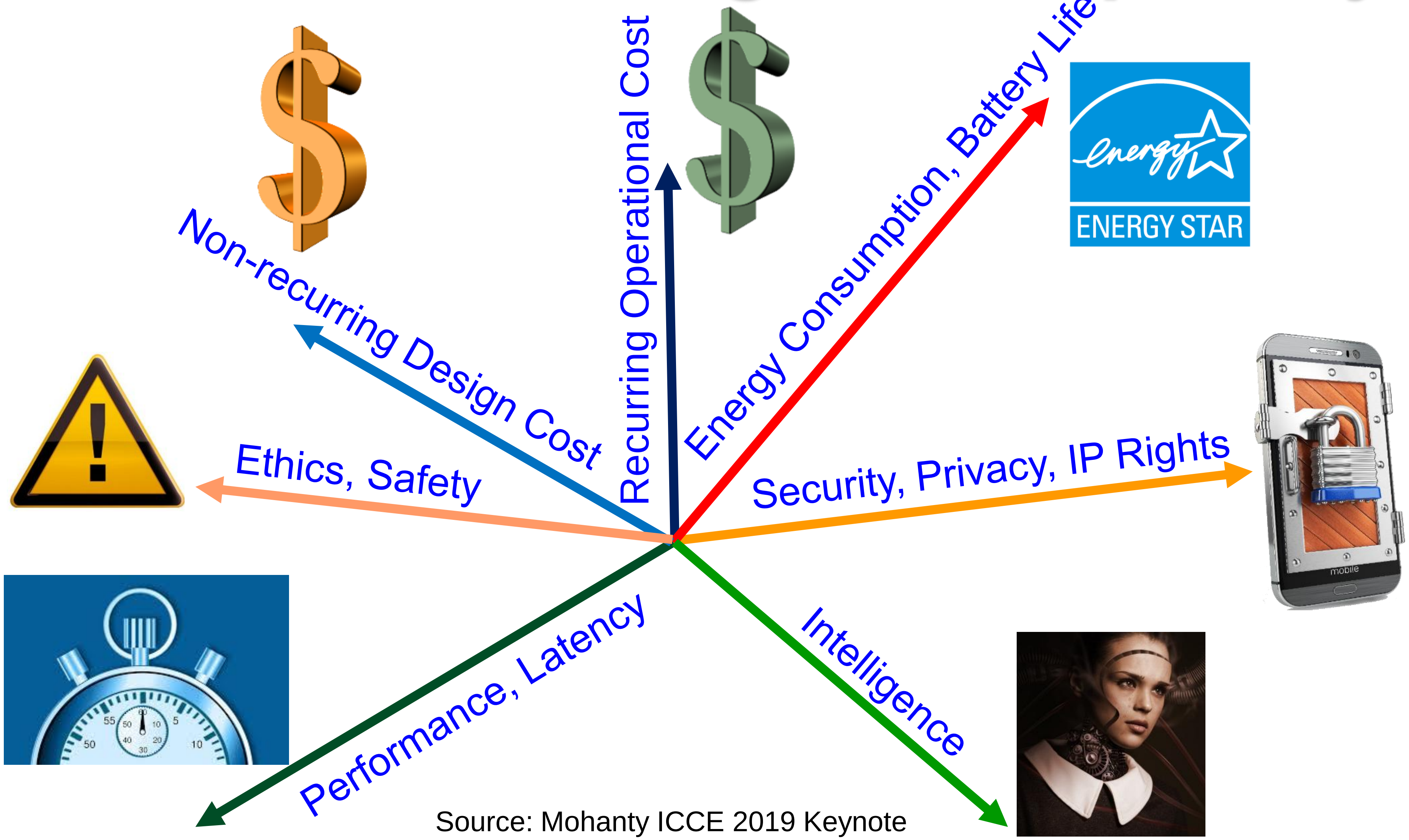
A quantum computer could break a 2048-bit RSA encryption in 8 hours.

Security-by-Design (SbD) – The Principle





IoT/CPS Design – Multiple Objectives



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

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)

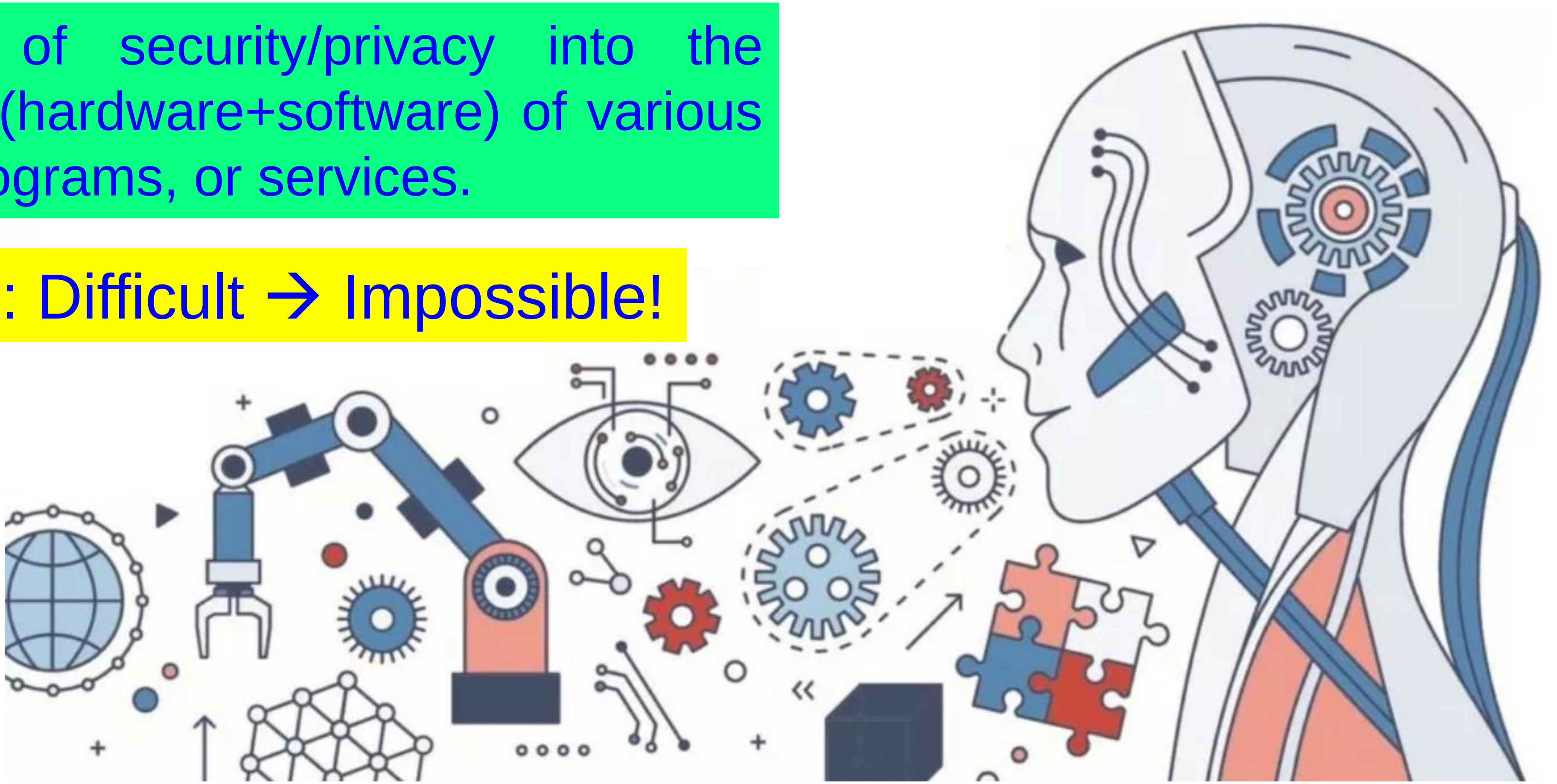
- ❖ GDPR makes Privacy by Design (PbD) a legal requirement

Security by Design
aka
Secure by Design (SbD)

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

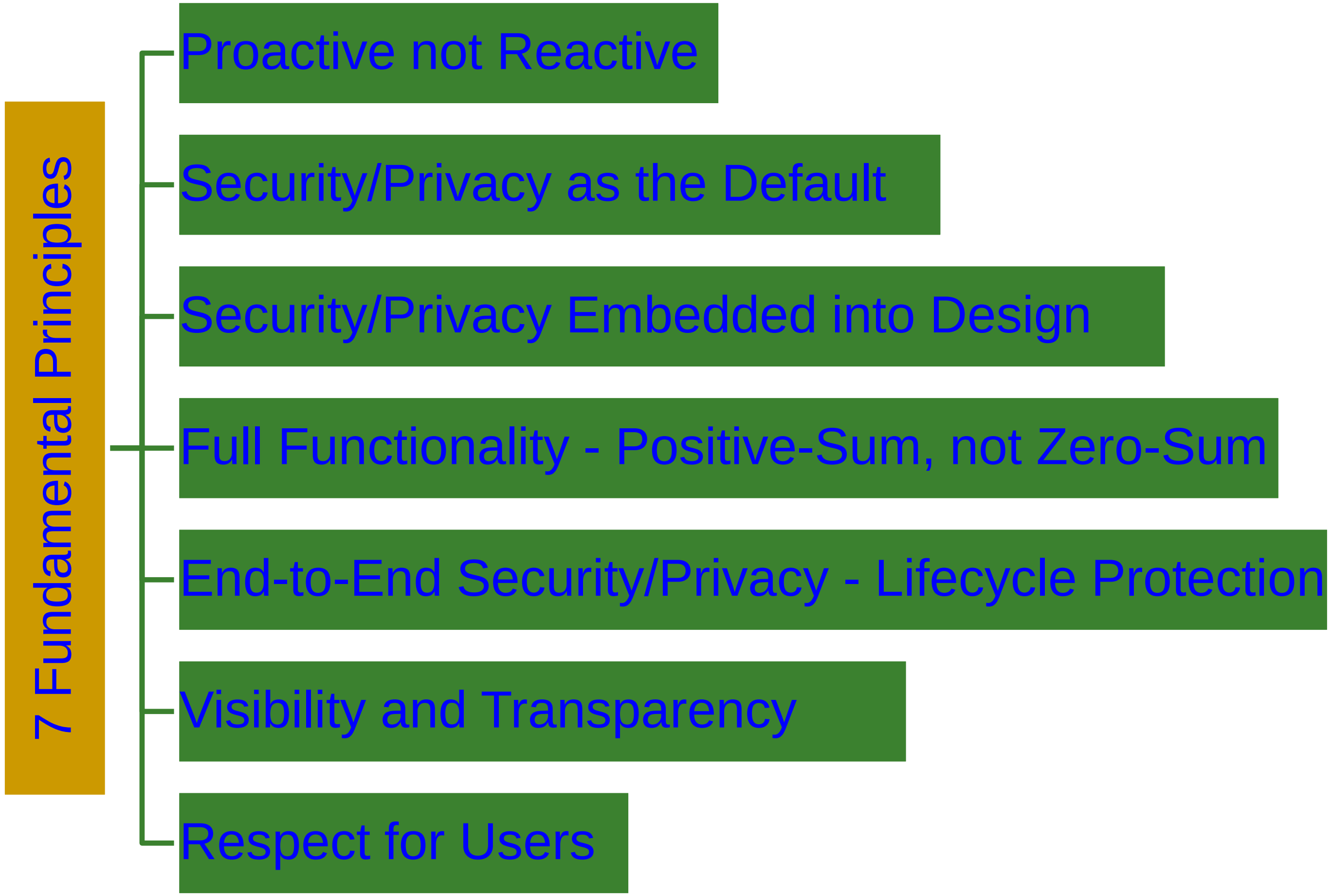
Embedding of security/privacy into the architecture (hardware+software) of various products, programs, or services.

Retrofitting: Difficult → Impossible!



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

Security by Design (SbD)



7 Fundamental Principles

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

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

Security-by-Design (SbD) – Principles …

- Security features should be Proactive not Reactive: Cybersecurity solutions for SbD approach should be done in a proactive fashion in anticipation that cyberscrurity issues will arise, instead of exploring solutions after cyberscrurity crisis takes place.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD) – Principles …

- Security should be Default: Cybersecurity features of the smart electronics should be default option in the context of hardware, software, and system specifications.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, “iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics”, in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD) – Principles …

- Security should be Embedded into Design: Cybsecurity solutions of a system should be integrated in the design and should be builtin as if the solutions cann't be separated from the system.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD) – Principles …

- Security should be incorporated as a Full Functionality - PositiveSum, not Zero-Sum without trade-offs: To facilitate effective integration with smart electronics, the SbD approach should have not tradeoffs and shouldn’t have energy, battery, and performance overheads.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, “iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics”, in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD)

- Security-Solutions should be End-to-End Security for Lifecycle Protection: The cybersecurity solutions should provide security in the entire life-cycle of the smart electronics, from design to deployment.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD)

- Security-Solutions should have Visibility and Transparency: The SbD approach in an Electronic system should be easily understandable and information should be visible and clear.

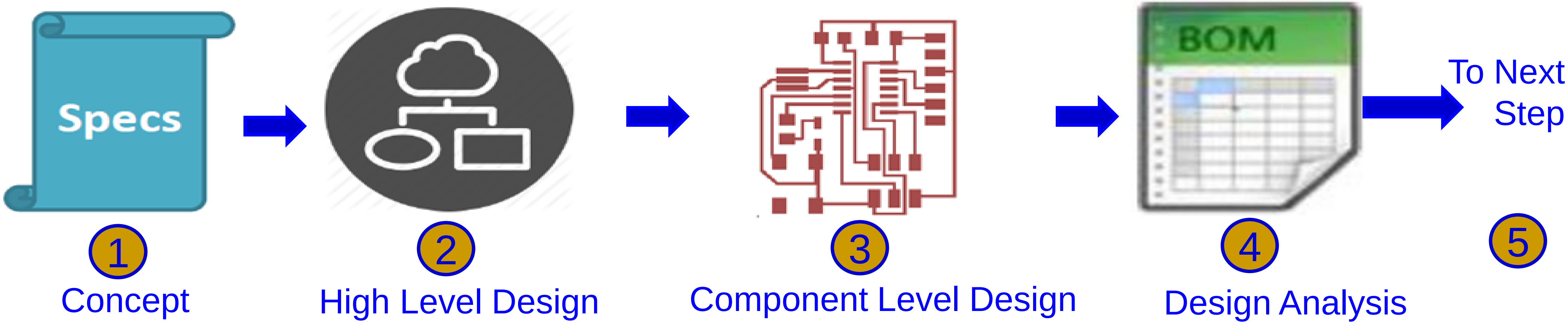
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

Security-by-Design (SbD)

- Security-Solutions should have Respect for Users: The cybsecurity solutions should respect the users in terms of their safety, privacy, and convenience.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, “iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics”, in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238586.

SbD Principle – IoT/CPS Design Flow …



1 Concept

2 High Level Design

3 Component Level Design

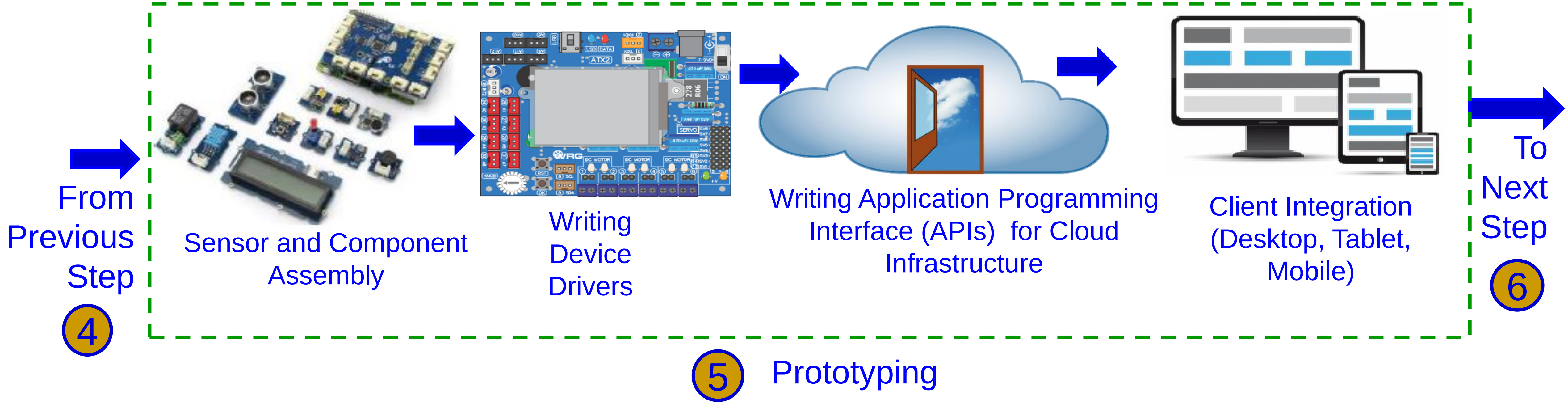
4 Design Analysis

5 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

SbD Principle – IoT/CPS Design Flow …



From Previous Step 4

Sensor and Component Assembly

Writing Device Drivers

Writing Application Programming Interface (APIs) for Cloud Infrastructure

Client Integration (Desktop, Tablet, Mobile)

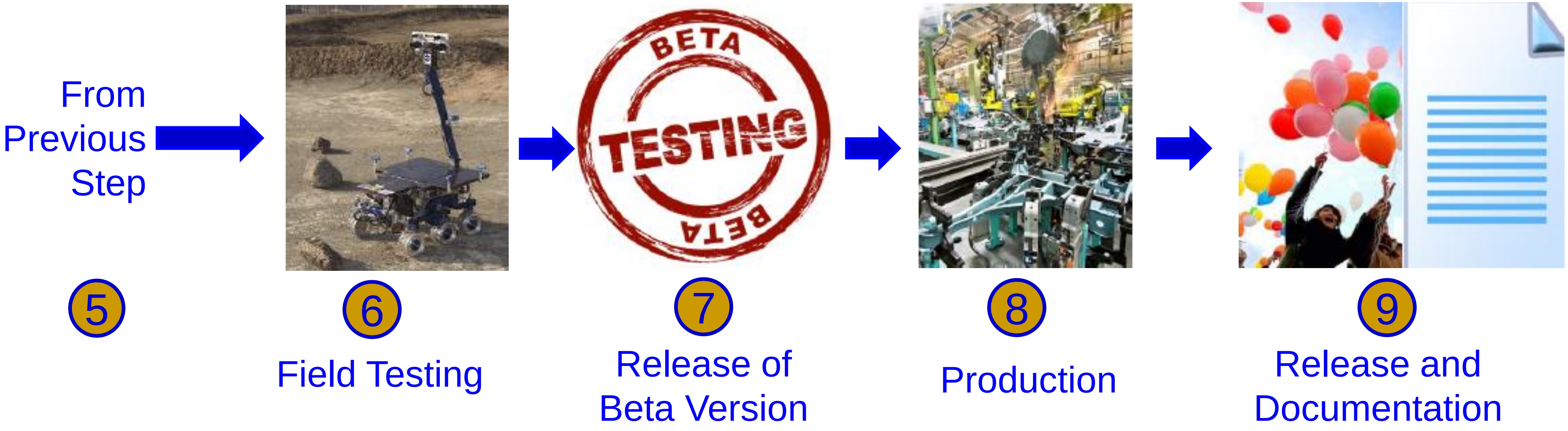
To Next Step 6

5 Prototyping

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

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

SbD Principle – IoT/CPS Design Flow

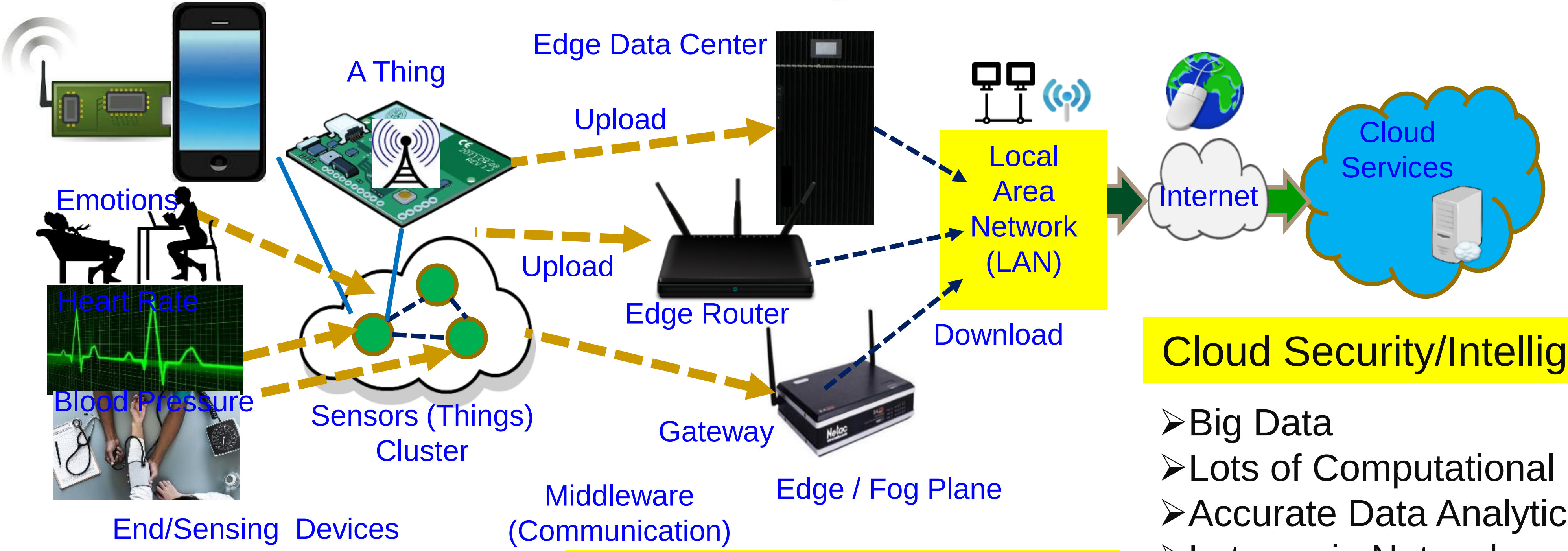


From Previous Step 5 → 6 Field Testing → 7 Release of Beta Version → 8 Production → 9 Release and Documentation

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

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

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

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

Heavy-Duty ML is more suitable for smart cities

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.

Trustworthy Electronic System

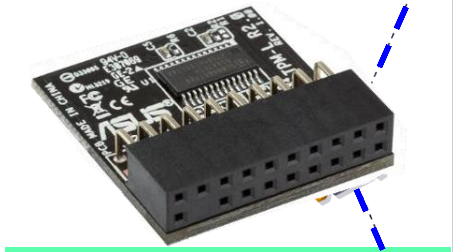
- A selective attributes of electronic system to be trustworthy:
  - It must maintain integrity of information it is processing.
  - It must conceal any information about the computation performed through any side channels such as power analysis or timing analysis.
  - It must perform only the functionality 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.

Hardware-Assisted Security (HAS)

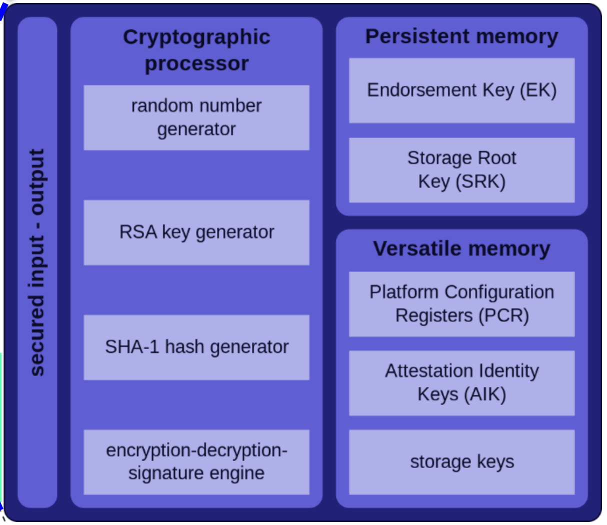
- Software based Security:
  - A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
  - Software based security approaches that rely on some form of encryption can’t be full proof as breaking them is just matter of time.
  - It is projected 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 Cybersecurity Primitives – TPM, HSM, TrustZone, and PUF

Hardware Security Module (HSM)



Trusted Platform Module (TPM)



secured input - output

Cryptographic processor

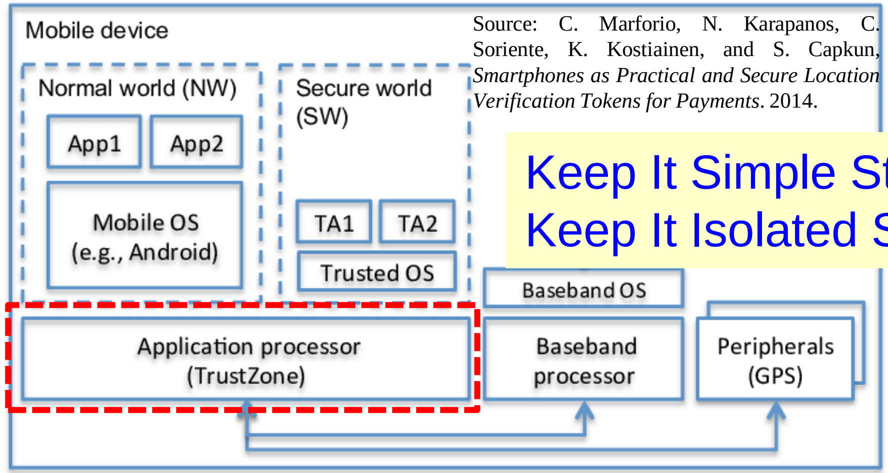
- random number generator
- RSA key generator
- SHA-1 hash generator
- encryption-decryption-signature engine

Persistent memory

- Endorsement Key (EK)
- Storage Root Key (SRK)

Versatile memory

- Platform Configuration Registers (PCR)
- Attestation Identity Keys (AIK)
- storage keys



Mobile device

Normal world (NW)

- App1
- App2
- Mobile OS (e.g., Android)

Secure world (SW)

- TA1
- TA2
- Trusted OS

Baseband OS

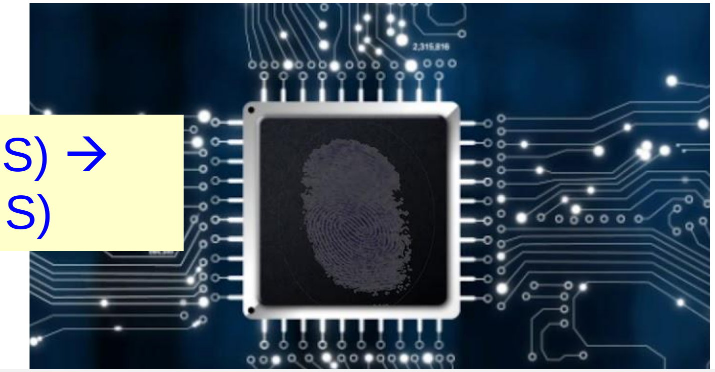
Application processor (TrustZone)

Baseband processor

Peripherals (GPS)

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

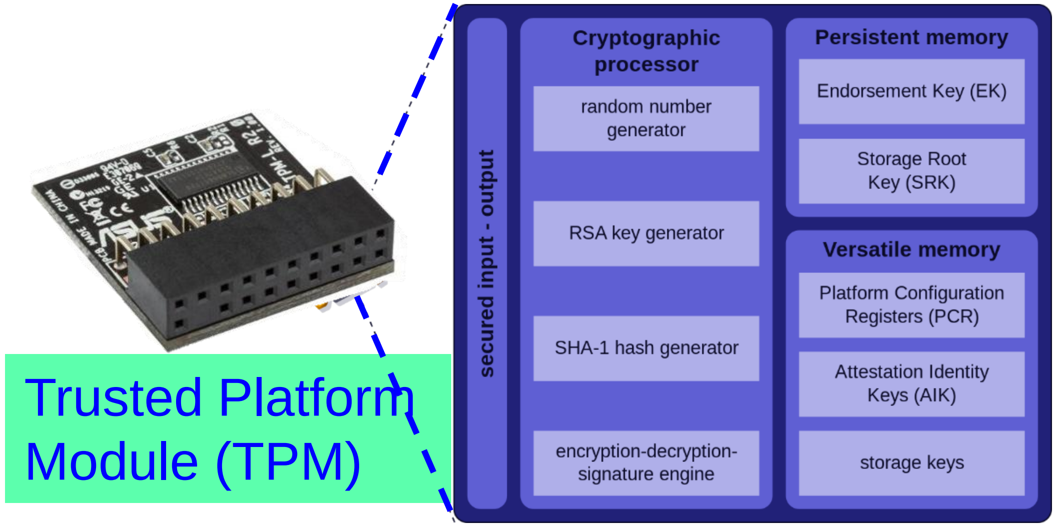
Keep It Simple Stupid (KISS) → Keep It Isolated Stupid (KIIS)



Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

PUF versus TPM



Trusted Platform Module (TPM)

secured input - output

Cryptographic processor

random number generator

RSA key generator

SHA-1 hash generator

encryption-decryption-signature engine

Persistent memory

Endorsement Key (EK)

Storage Root Key (SRK)

Versatile memory

Platform Configuration Registers (PCR)

Attestation Identity Keys (AIK)

storage keys

Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

TPM:

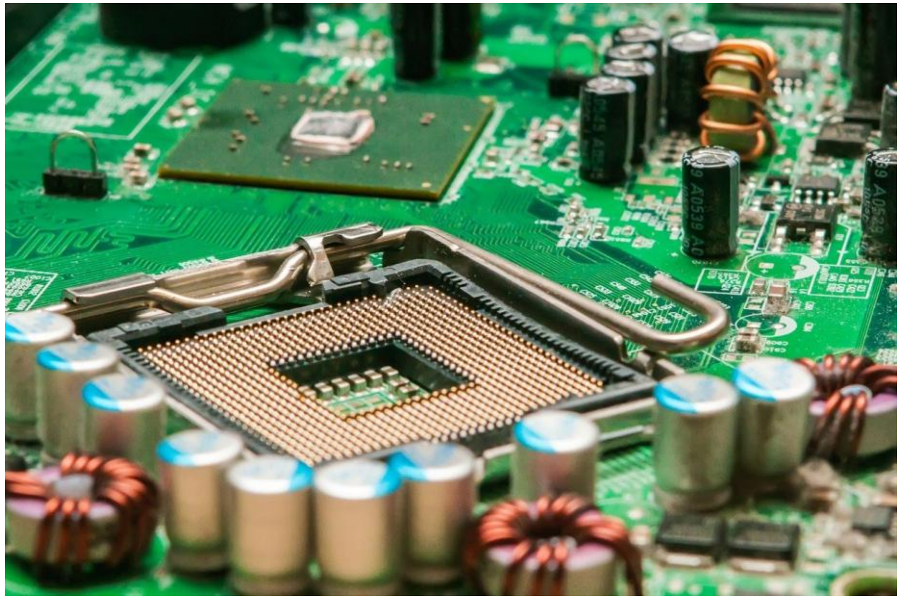
1) The set of specifications for a secure crypto- processor and
2) The implementation of these specifications on a chip

PUF:

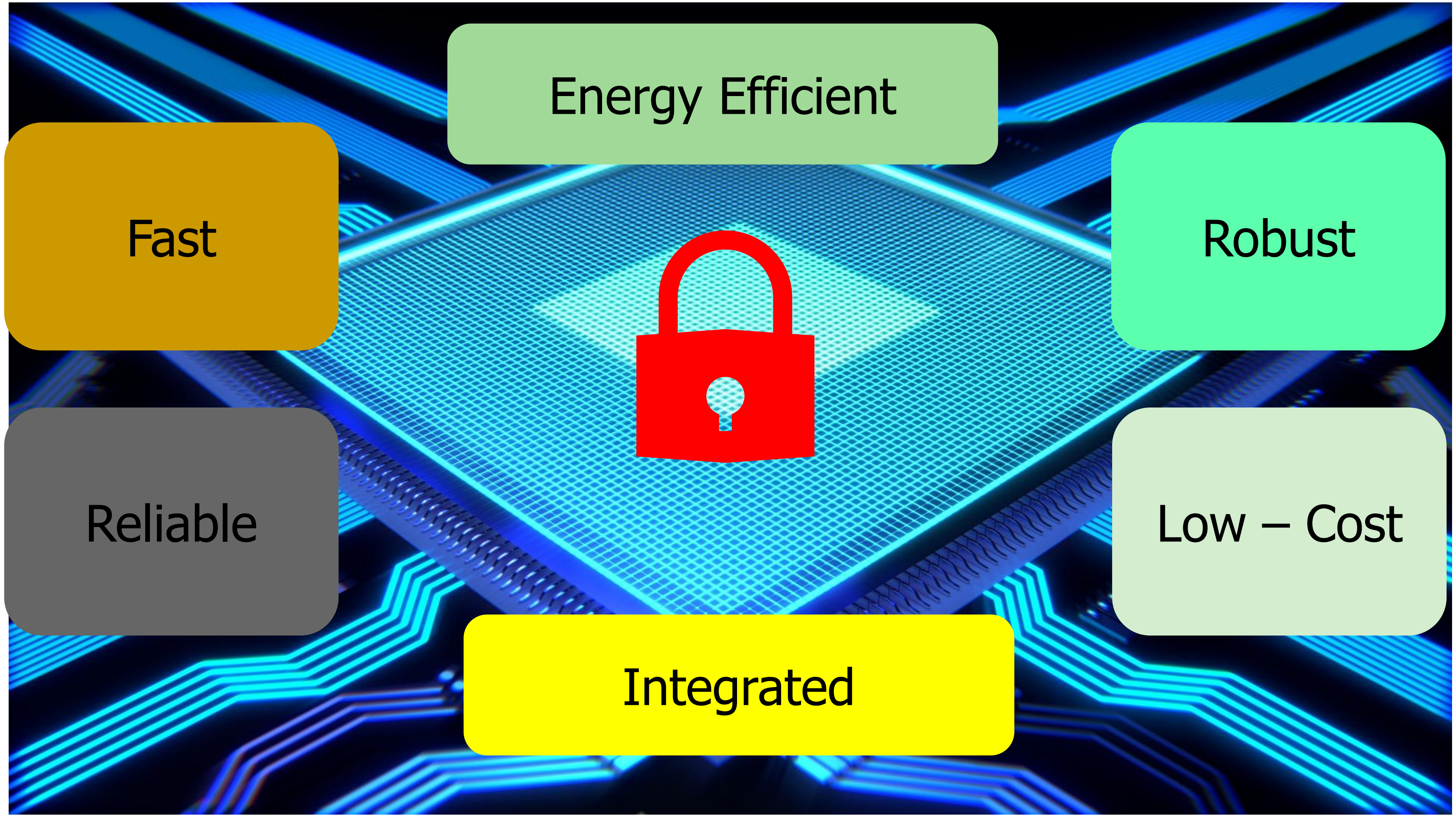
1) Based on a physical system
2) Generates random output values

PUF: A Hardware-Assisted Security Primitive

- PUF has a Challenge as an Input and Response as an Output
- Response output from the PUF design will be unique for the challenge input on that PUF design
- Arbiter PUF and Ring Oscillator PUF are the most widely used PUF designs for IoT applications
- Delay based PUF designs support higher number of Challenge Response pairs (CRP)



SbD/HAS - Advantages



Energy Efficient

Fast

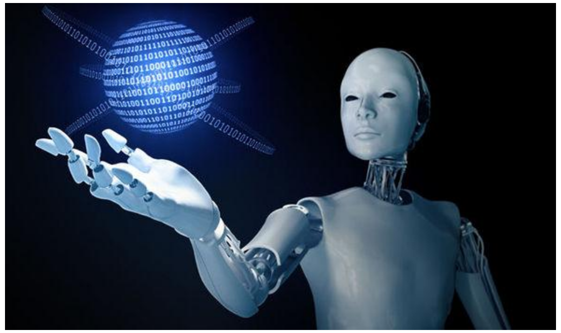
Robust

Reliable

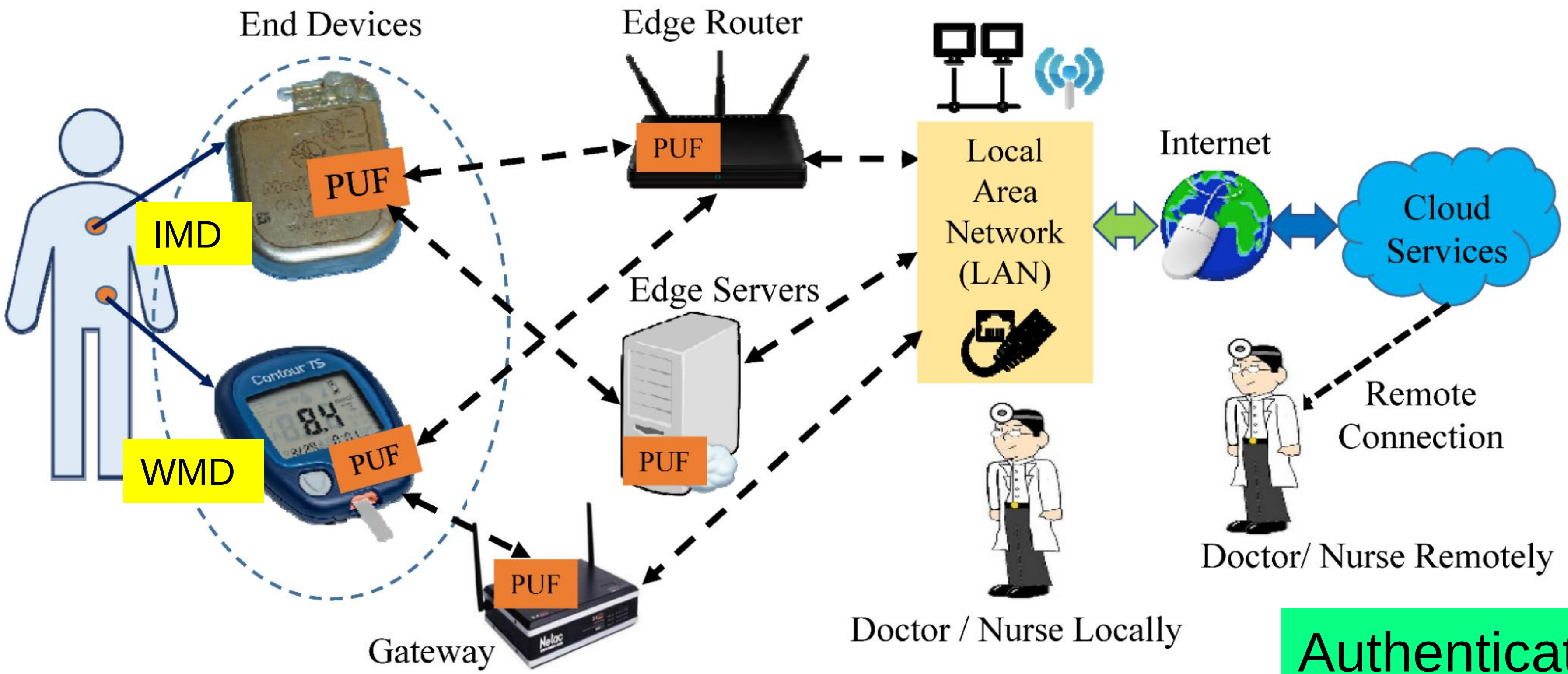
Low – Cost

Integrated

Security-by-Design (SbD) – Specific Examples



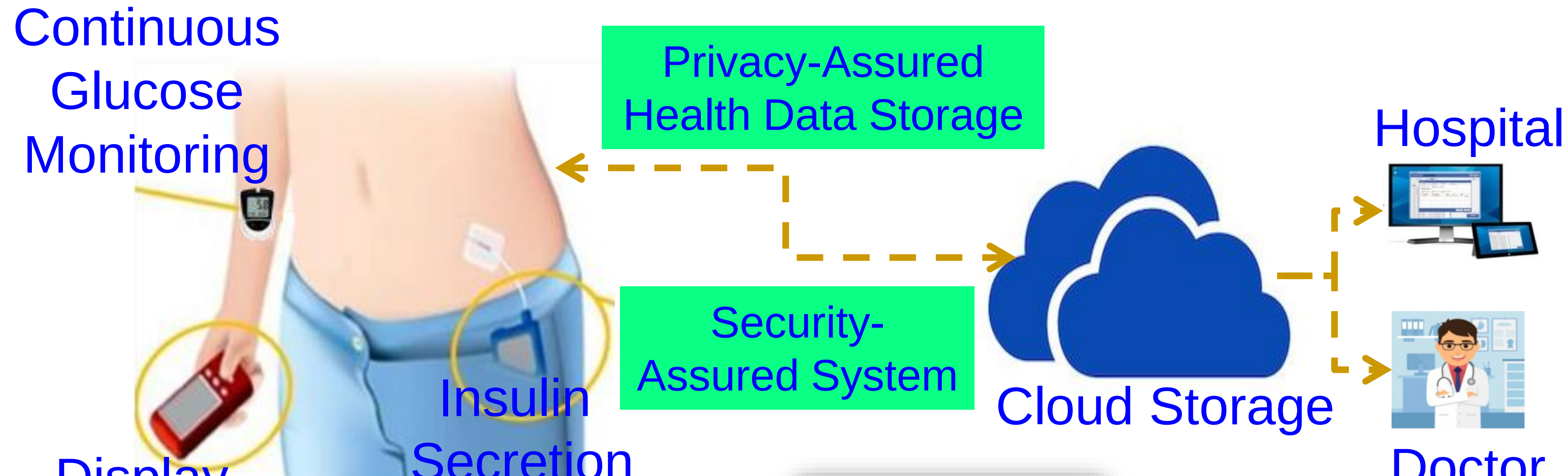
PMsec: Our Secure by Design Approach for Robust Security in Healthcare CPS

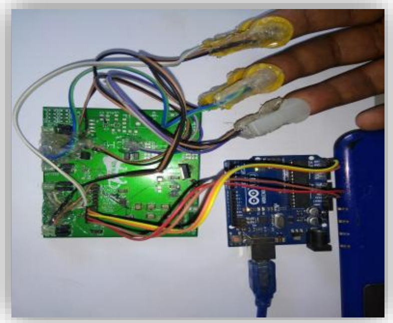


Authenticates Time - 1 sec
Power Consumption - 200 μW

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

iGLU: Accurate Glucose Level Monitoring and Secure Insulin Delivery

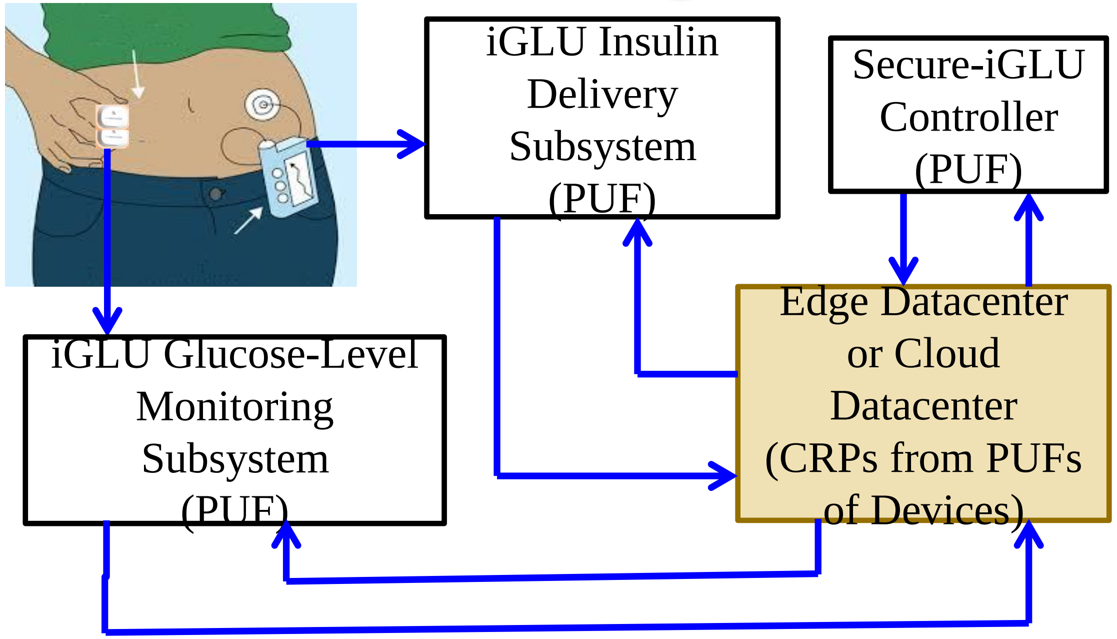

Continuous Glucose Monitoring
Privacy-Assured Health Data Storage
Hospital
Security-Assured System
Insulin Secretion
Cloud Storage
Doctor
Display of Parameters
Artificial Pancreases System (APS)



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

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

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



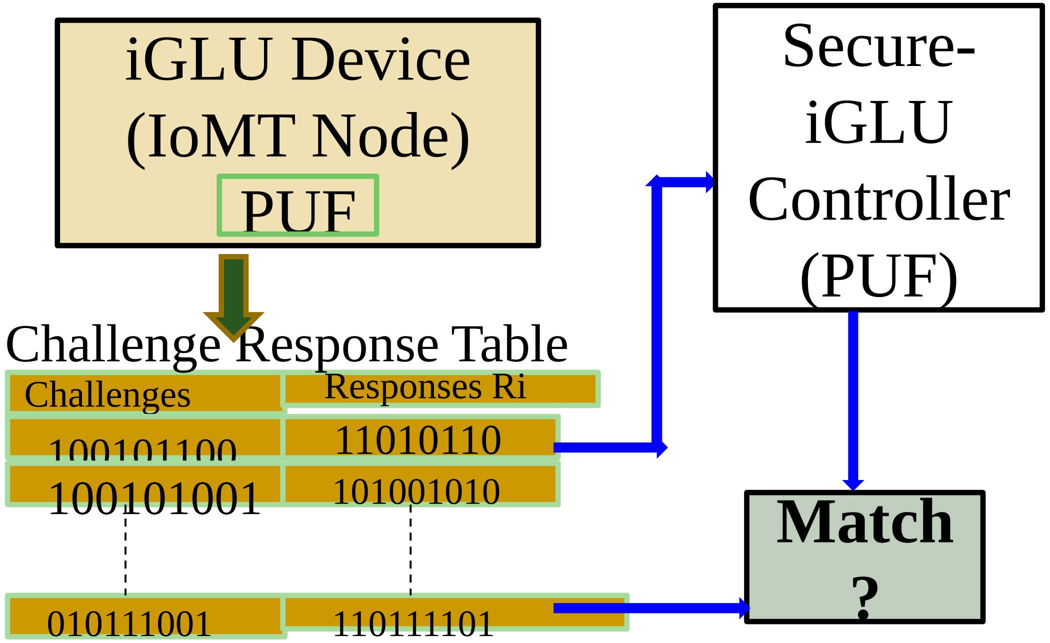
iGLU Insulin Delivery Subsystem (PUF)

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

Secure-iGLU Controller (PUF)

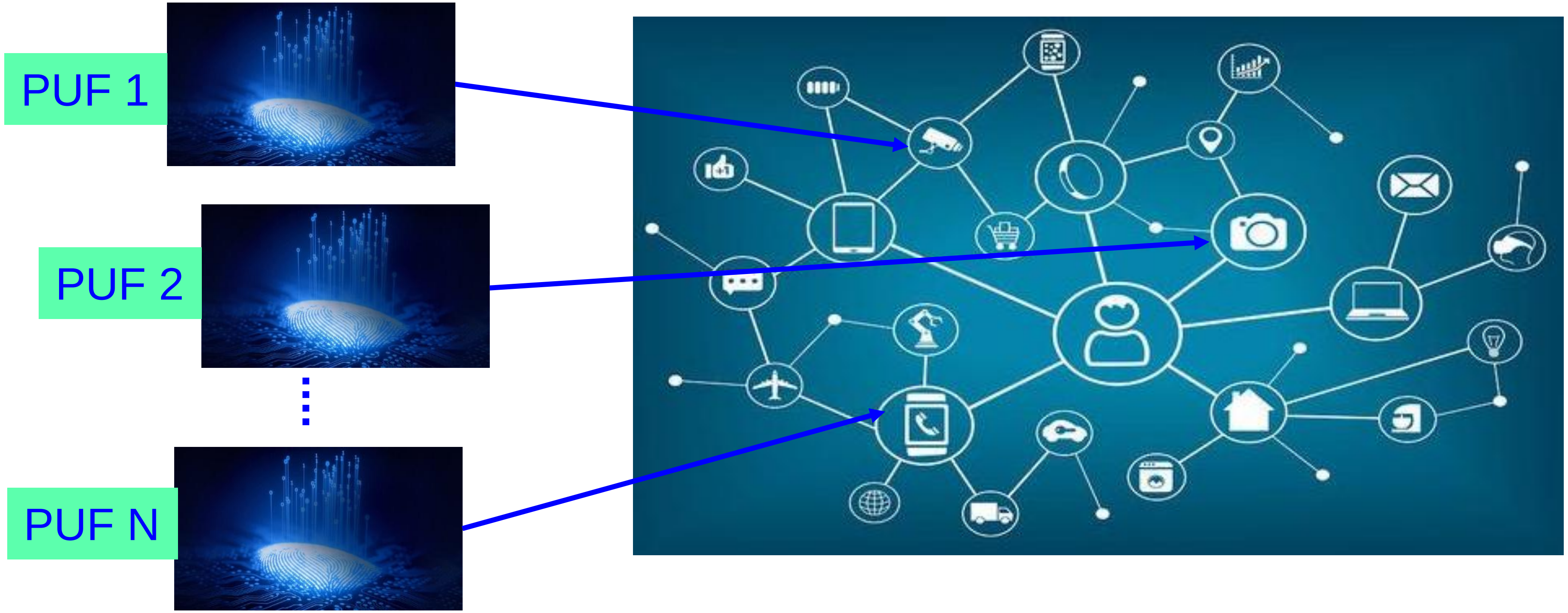
Match ?

Challenge Response Table

Challenges	Responses Ri
100101100	11010110
100101001	101001010
⋮	⋮
010111001	110111101

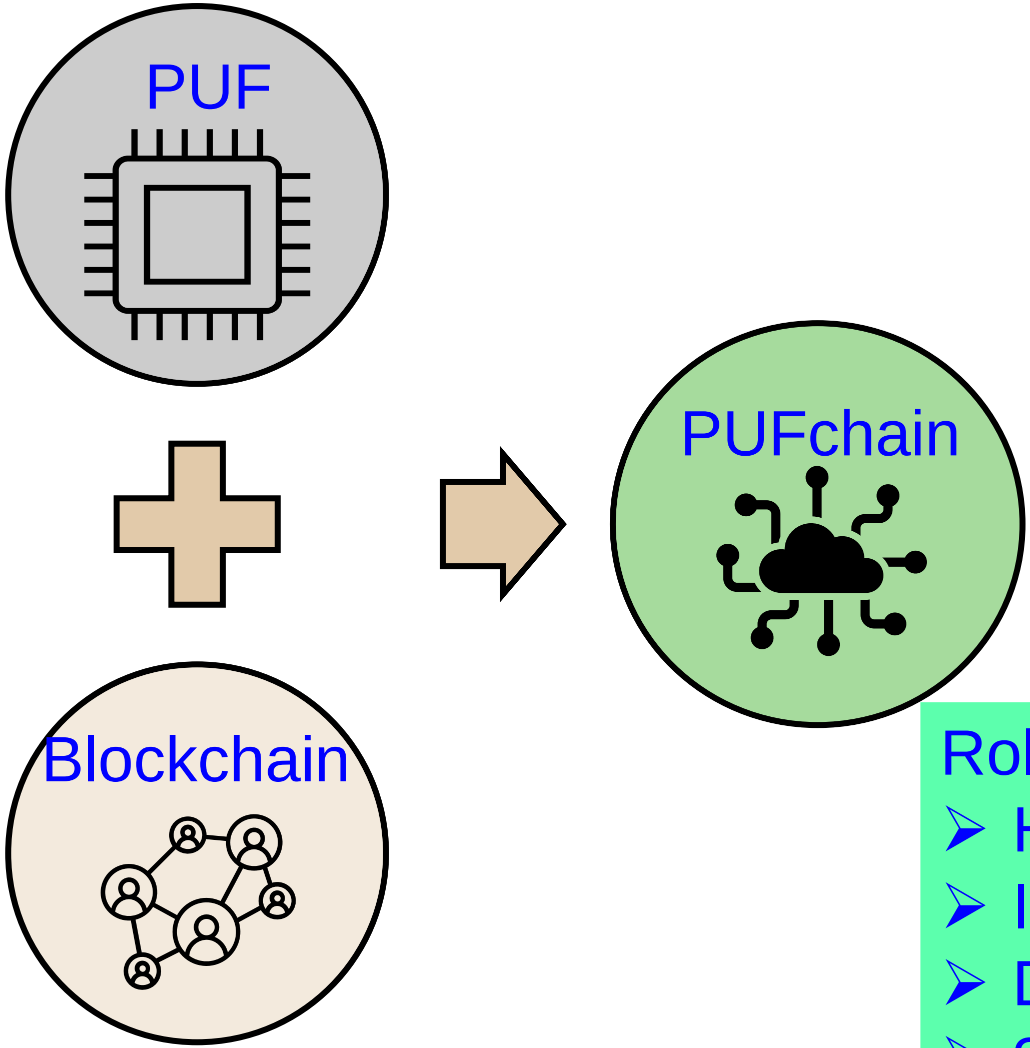
Source: A. M. Joshi, P. Jain, and S. P. Mohanty, “Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework”, *Proceedings of the 19th IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 440-445.

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



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

PUFchain – The Big Idea

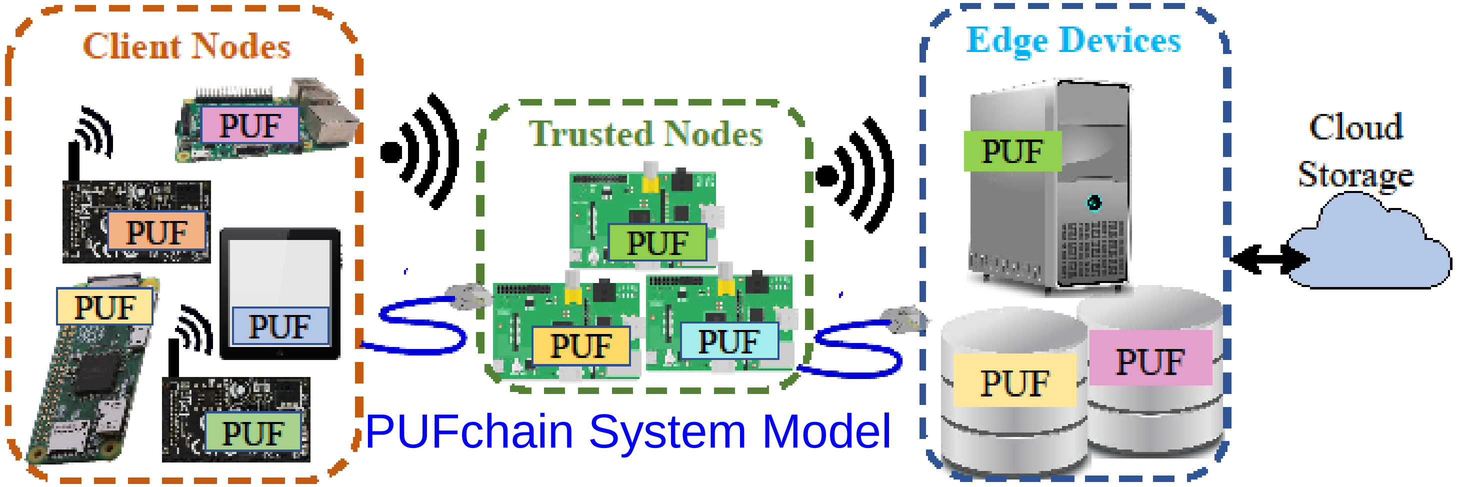


Blockchain Technology is integrated with Physically Unclonable Functions as PUFchain by storing the PUF Key into immutable Blockchain

Roles of PUF:

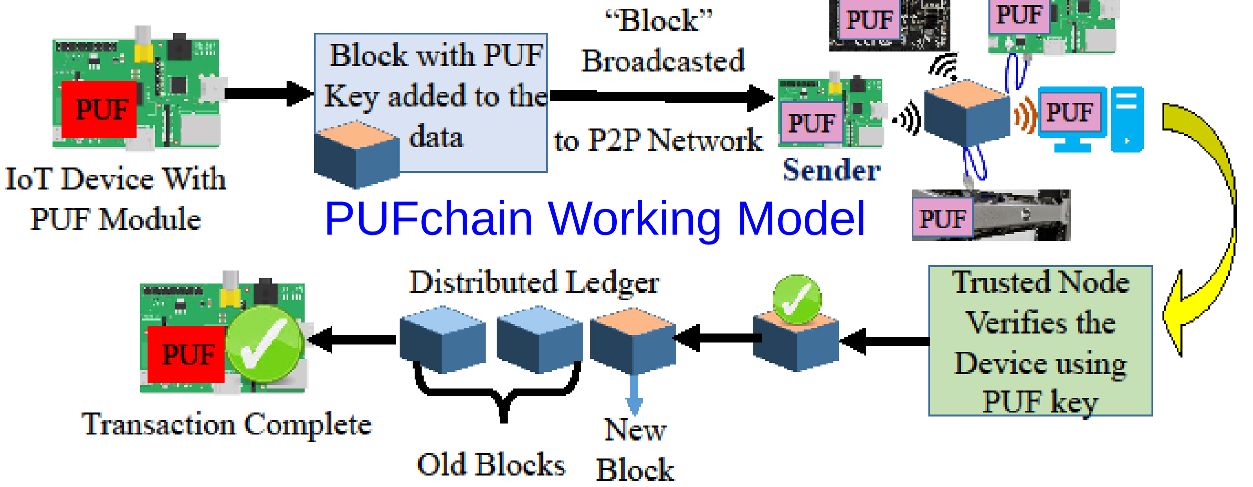
- Hardware Accelerator for Blockchain
- Independent Authentication
- Double-Layer Protection
- 3 modes: PUF, Blockchain, PUF+Blockchain

PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and
Data Security



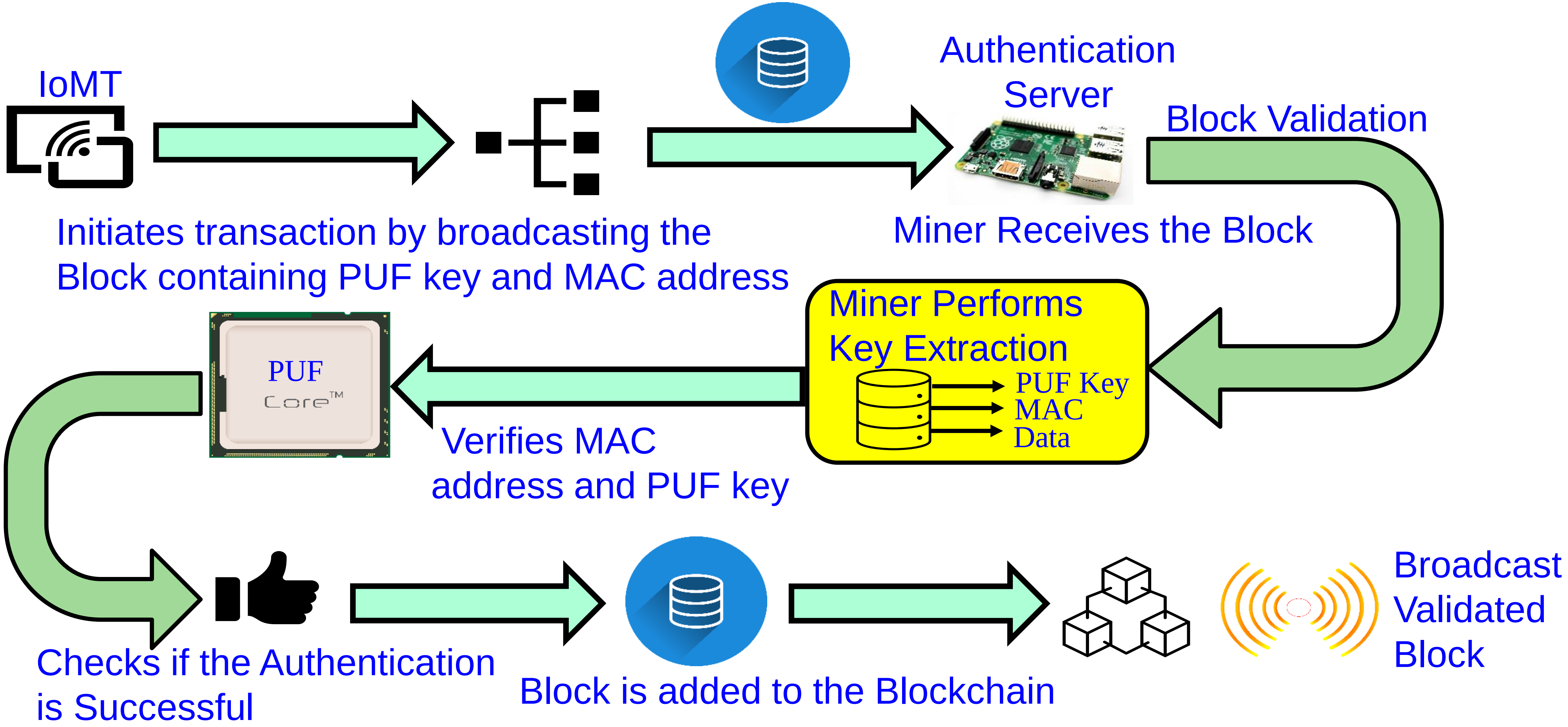
PUFchain Working Model

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.

PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



IoMT

Authentication Server

Block Validation

Initiates transaction by broadcasting the Block containing PUF key and MAC address

Miner Receives the Block

Miner Performs Key Extraction

Verifies MAC address and PUF key

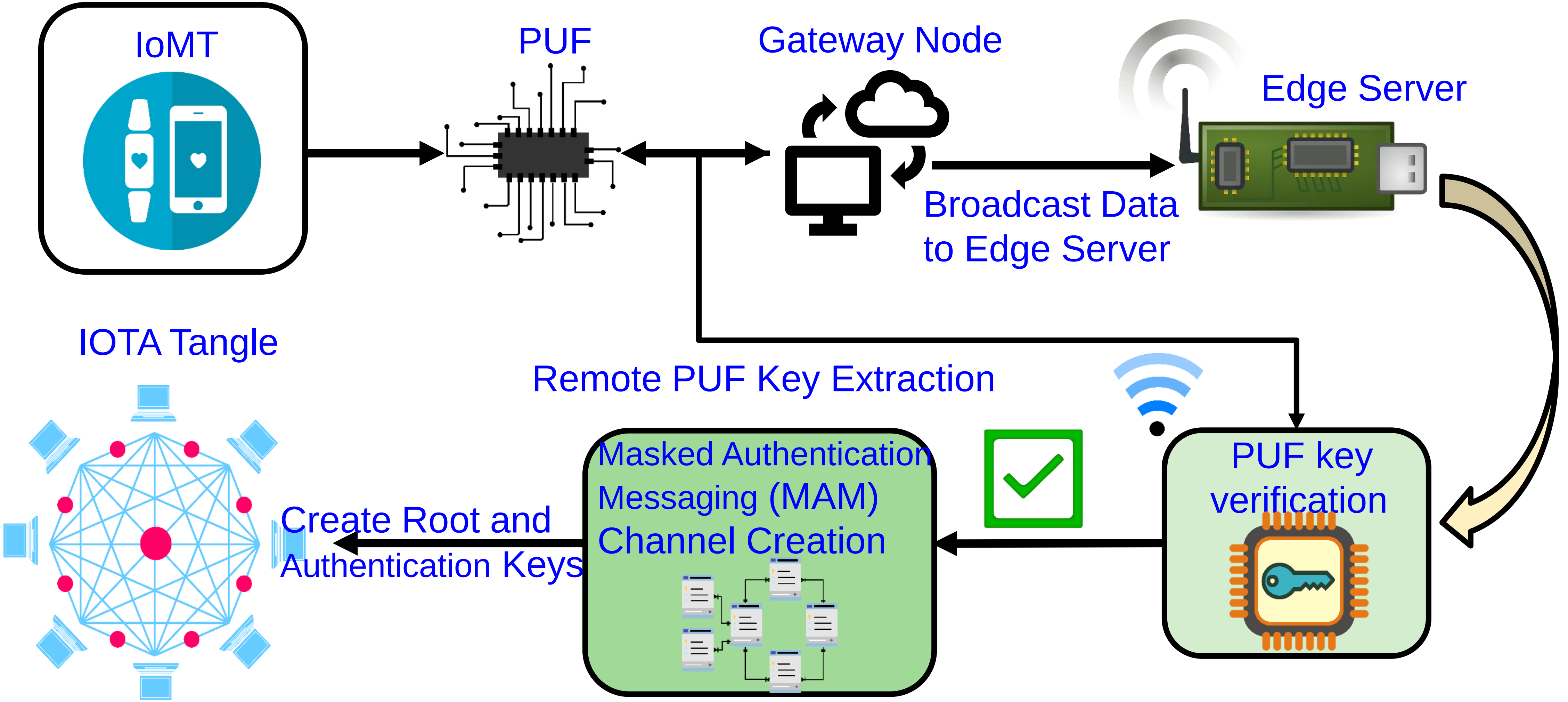
Checks if the Authentication is Successful

Block is added to the Blockchain

Broadcast Validated Block

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

PUFchain 3.0 - Architecture



IoMT

PUF

Gateway Node

Edge Server

Broadcast Data to Edge Server

IOTA Tangle

Remote PUF Key Extraction

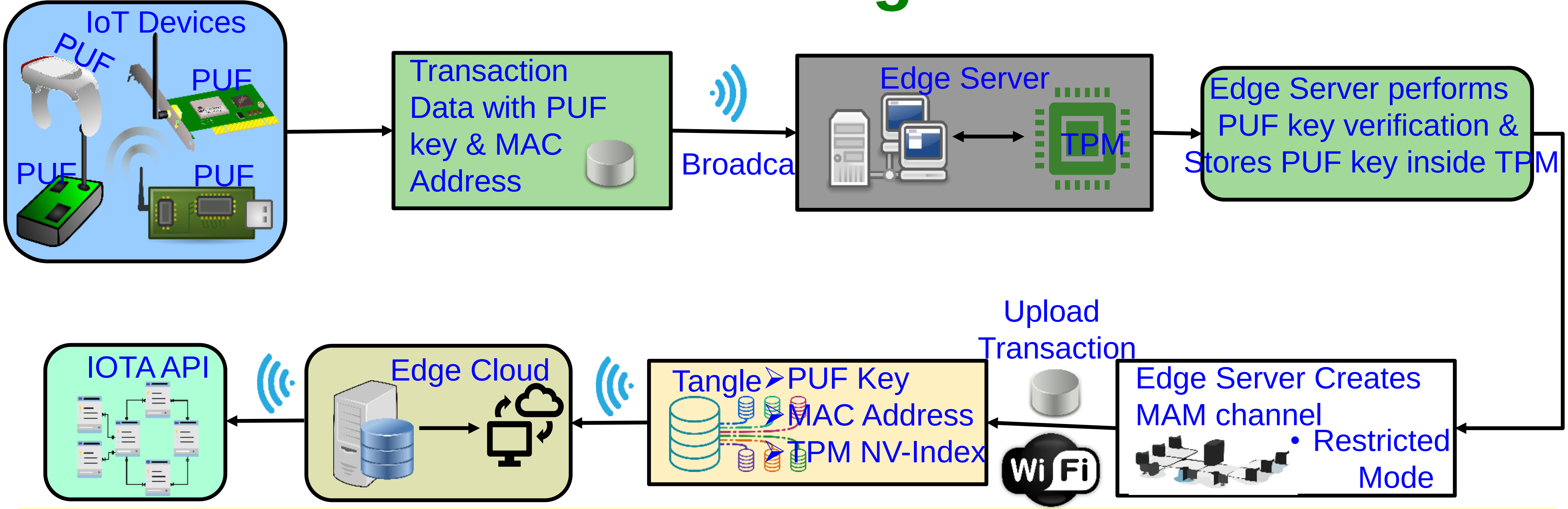
Masked Authentication Messaging (MAM) Channel Creation

PUF key verification

Create Root and Authentication Keys

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

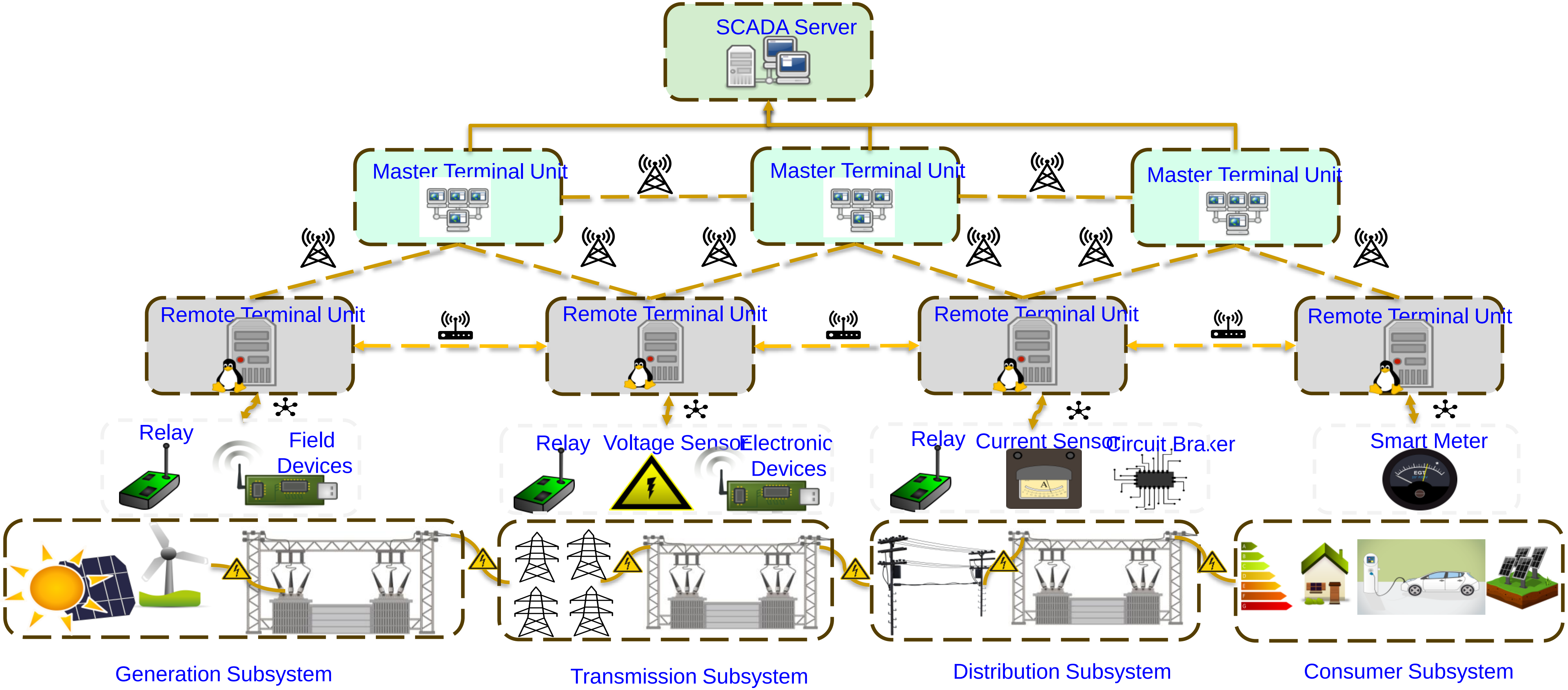
Our PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for SbD of IoT


IoT Devices
PUF
PUF
PUF
PUF
Transaction Data with PUF key & MAC Address
Broadca
Edge Server
TPM
Edge Server performs PUF key verification & Stores PUF key inside TPM
Edge Server Creates MAM channel
• Restricted Mode
Upload Transaction
Wi Fi
Tangle
➢PUF Key
➢MAC Address
➢TPM NV-Index
Edge Cloud
IOTA API

- Tangle is a simple fee-less, miner less Distributed Ledger Technology
- In Tangle, Incoming transactions must validate tips (Unverified Transactions) to become part of the Network.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 231--236, DOI: https://doi.org/10.1145/3583781.3590206.

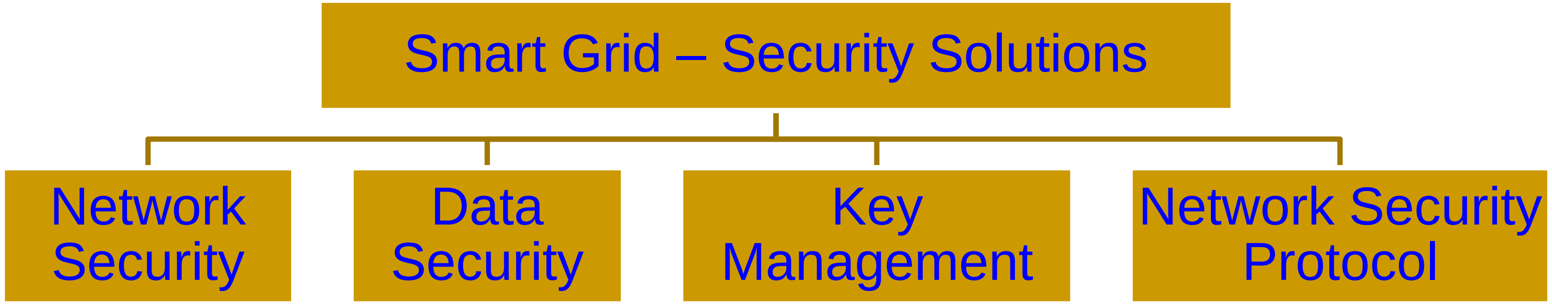
Smart Grid Cybersecurity



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

Serial/Wireless Wide Area Network Wireless Connection/LAN

Smart Grid Cybersecurity - Solutions



Smart Grid – Security Solutions

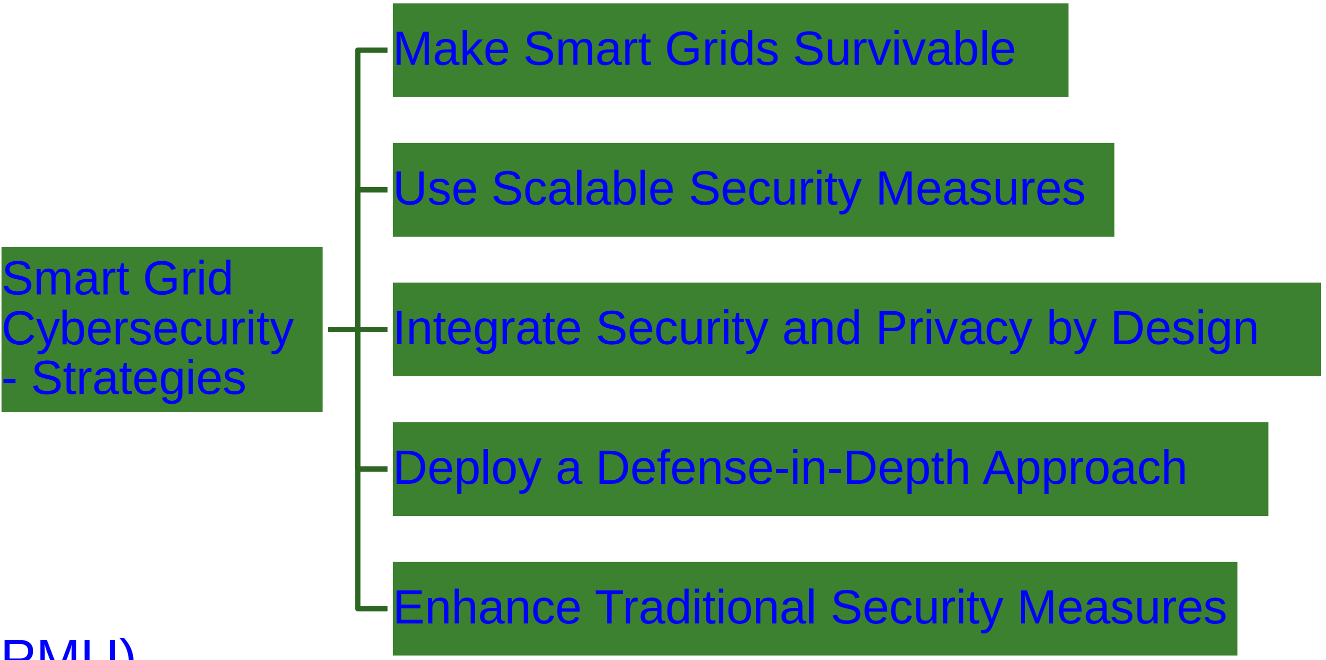
Network Security

Data Security

Key Management

Network Security Protocol

Smart Meter



Smart Grid Cybersecurity - Strategies

Make Smart Grids Survivable

Use Scalable Security Measures

Integrate Security and Privacy by Design

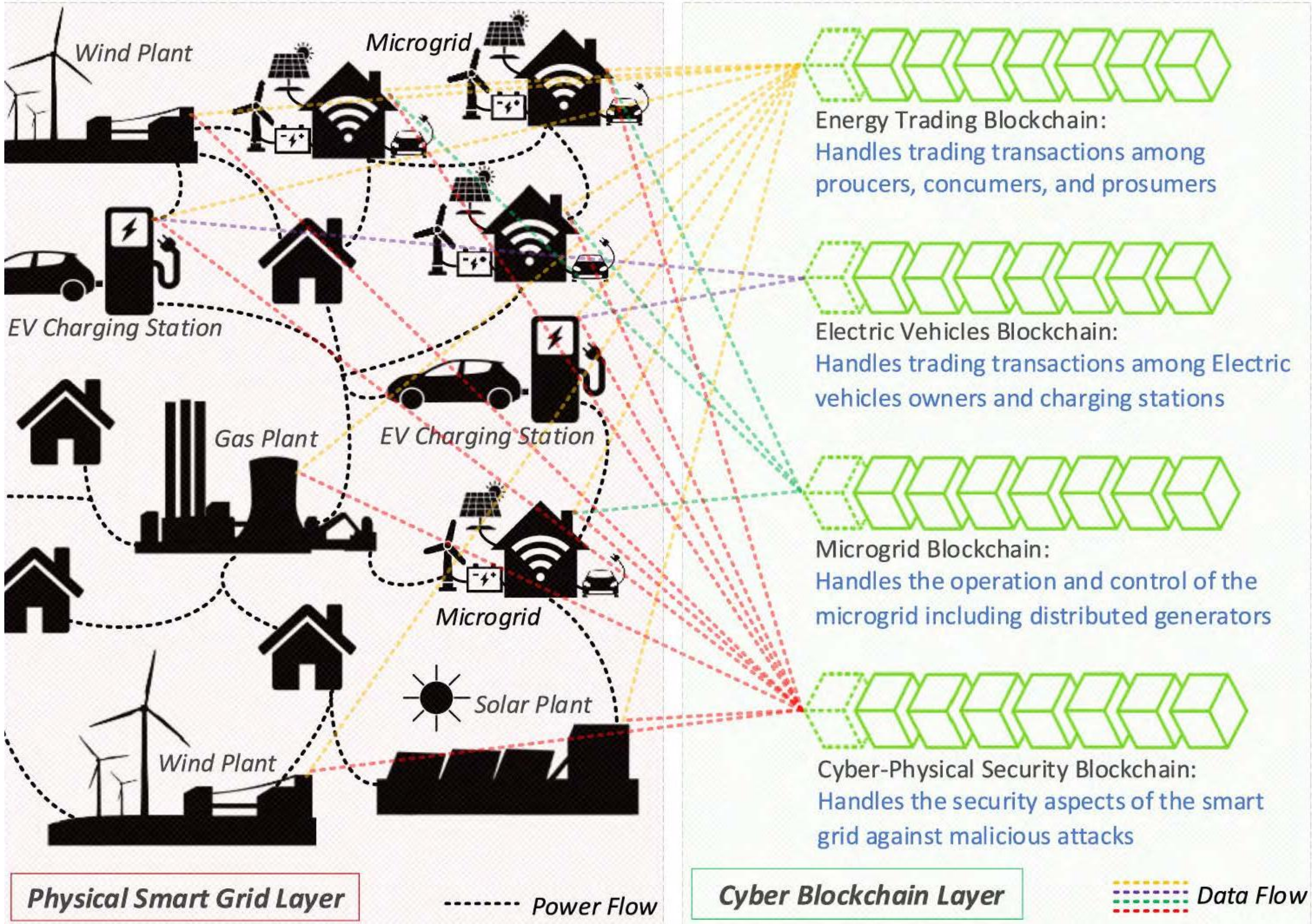
Deploy a Defense-in-Depth Approach

Enhance Traditional Security Measures

Phasor Measurement Unit (PMU)

Source: S. Conovalu and J. S. Park. "Cybersecurity strategies for smart grids", *Journal of Computers*, Vol. 11, no. 4, (2016): 300-310.

Smart Grid Security - Solutions



Energy Trading Blockchain:
Handles trading transactions among proucers, concumers, and prosumers

Electric Vehicles Blockchain:
Handles trading transactions among Electric vehicles owners and charging stations

Microgrid Blockchain:
Handles the operation and control of the microgrid including distributed generators

Cyber-Physical Security Blockchain:
Handles the security aspects of the smart grid against malicious attacks

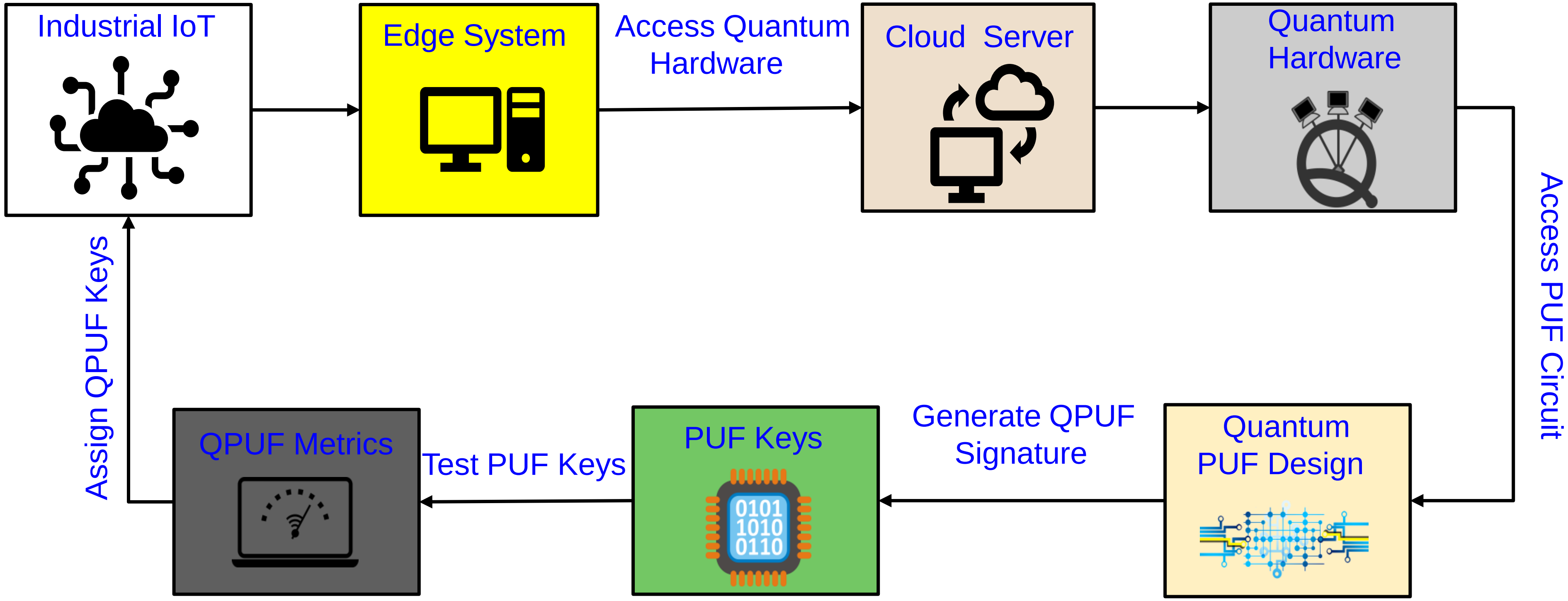
Source: A. S. Musleh, G. Yao and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," *IEEE Access*, vol. 7, pp. 86746-86757, 2019.

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.

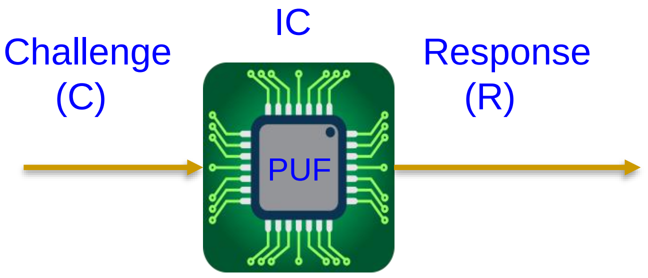
Source: https://embeddedcomputing.com/technology/processing/semiconductor-ip/demystifying-the-physically-unclonable-function-puf

Our QPUF: Quantum PUF for SbD of Industrial IoT

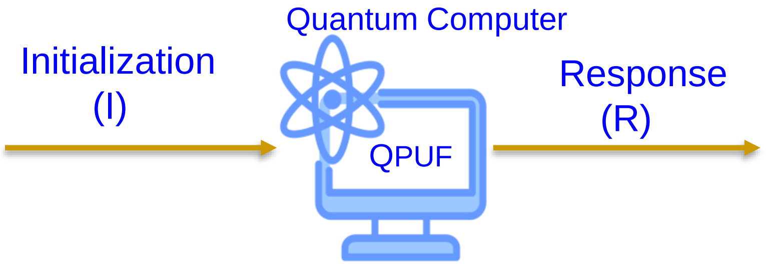


Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, C. Pan, and E. Kougianos, "QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things", in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2023, pp. 296--301, DOI: https://doi.org/10.1109/iSES58672.2023.00067.

Our QPUF 2.0 …



C	R
101101011	101001010
111001010	001101011
101001000	110110100
000101110	101110010



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

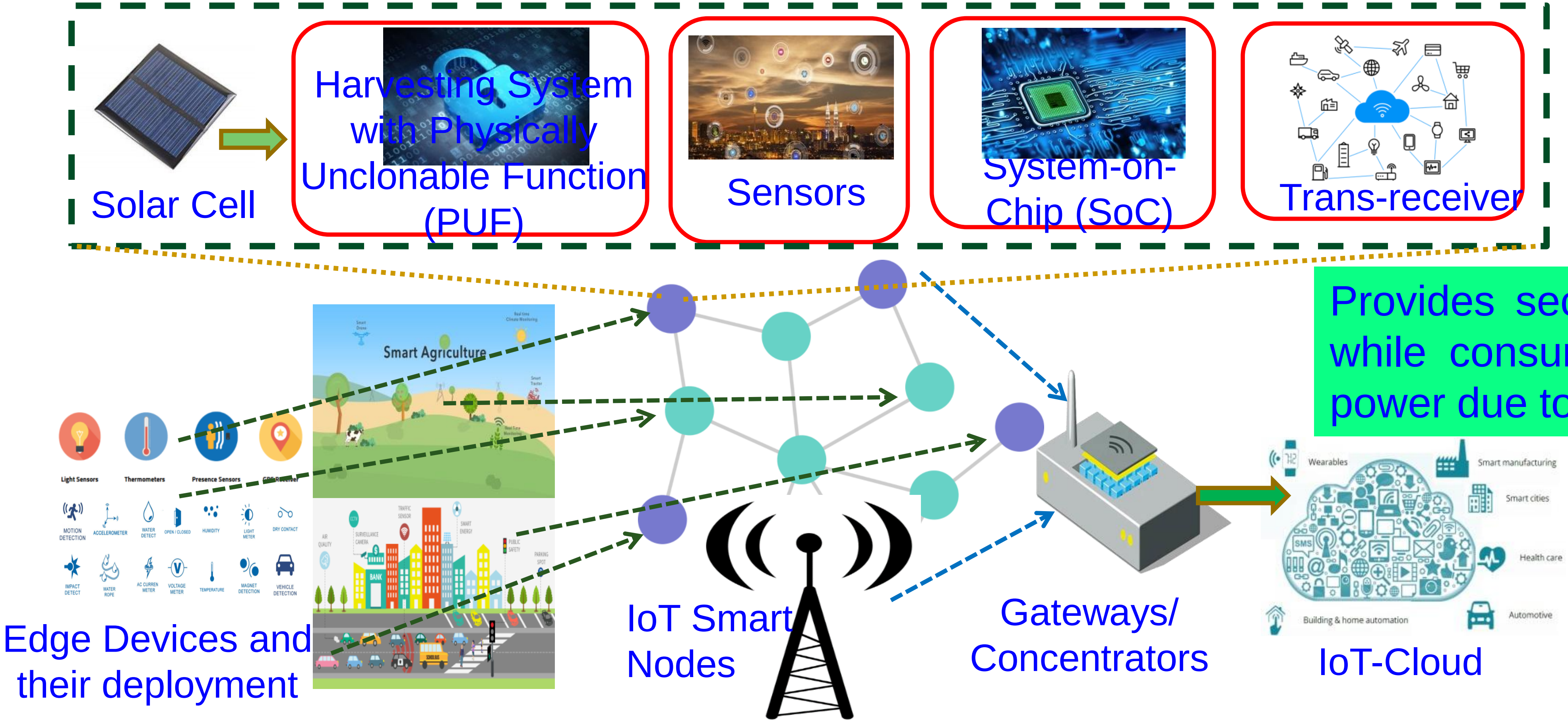
I1 → $(\frac{\pi}{2}, 0)$
$(\frac{\pi}{2}, 1)$
$(\frac{\pi}{2}, 0)$
$(\frac{\pi}{2}, 1)$
→R1

I2 → $(\frac{\pi}{5}, 1)$
$(\frac{\pi}{5}, 1)$
$(\frac{\pi}{5}, 0)$
$(\frac{\pi}{5}, 0)$
→R2 --------

In → $(\frac{\pi}{4}, 1)$
$(\frac{\pi}{4}, 0)$
$(\frac{\pi}{4}, 1)$
$(\frac{\pi}{4}, 0)$
→Rn

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

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



Solar Cell

Harvesting System with Physically Unclonable Function (PUF)

Sensors

System-on-Chip (SoC)

Trans-receiver

Edge Devices and their deployment

IoT Smart Nodes

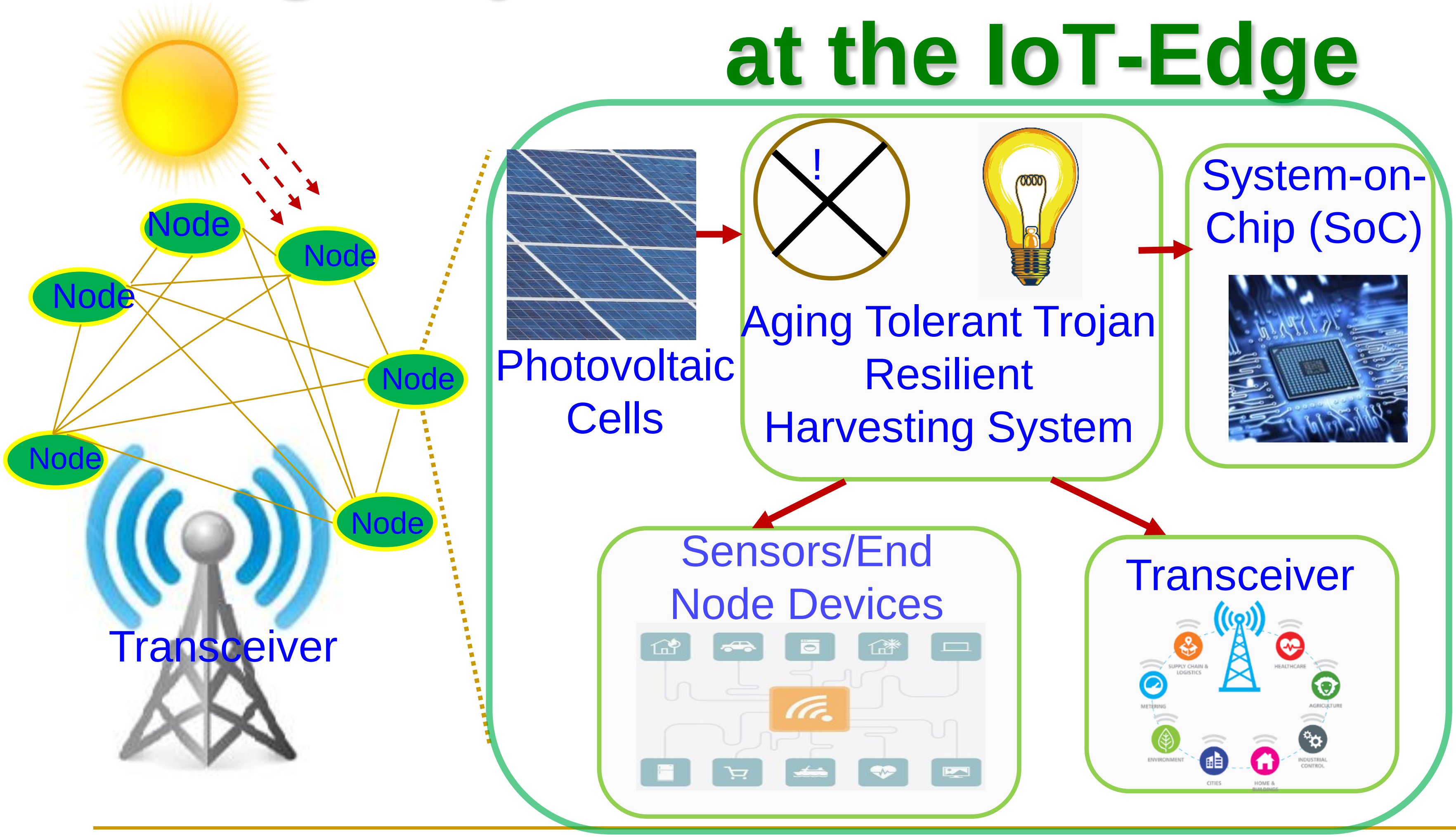
Gateways/ Concentrators

IoT-Cloud

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

Source: S. K. Ram, S. R. Sahoo, Banee, B.Das, K. K. Mahapatra, and S. P. Mohanty, “Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT”, *IEEE Transactions on Sustainable Computing*, Vol. 6, No. 2, April 2021, pp. 320—333, DOI: https://doi.org/10.1109/TSUSC.2020.2987616.

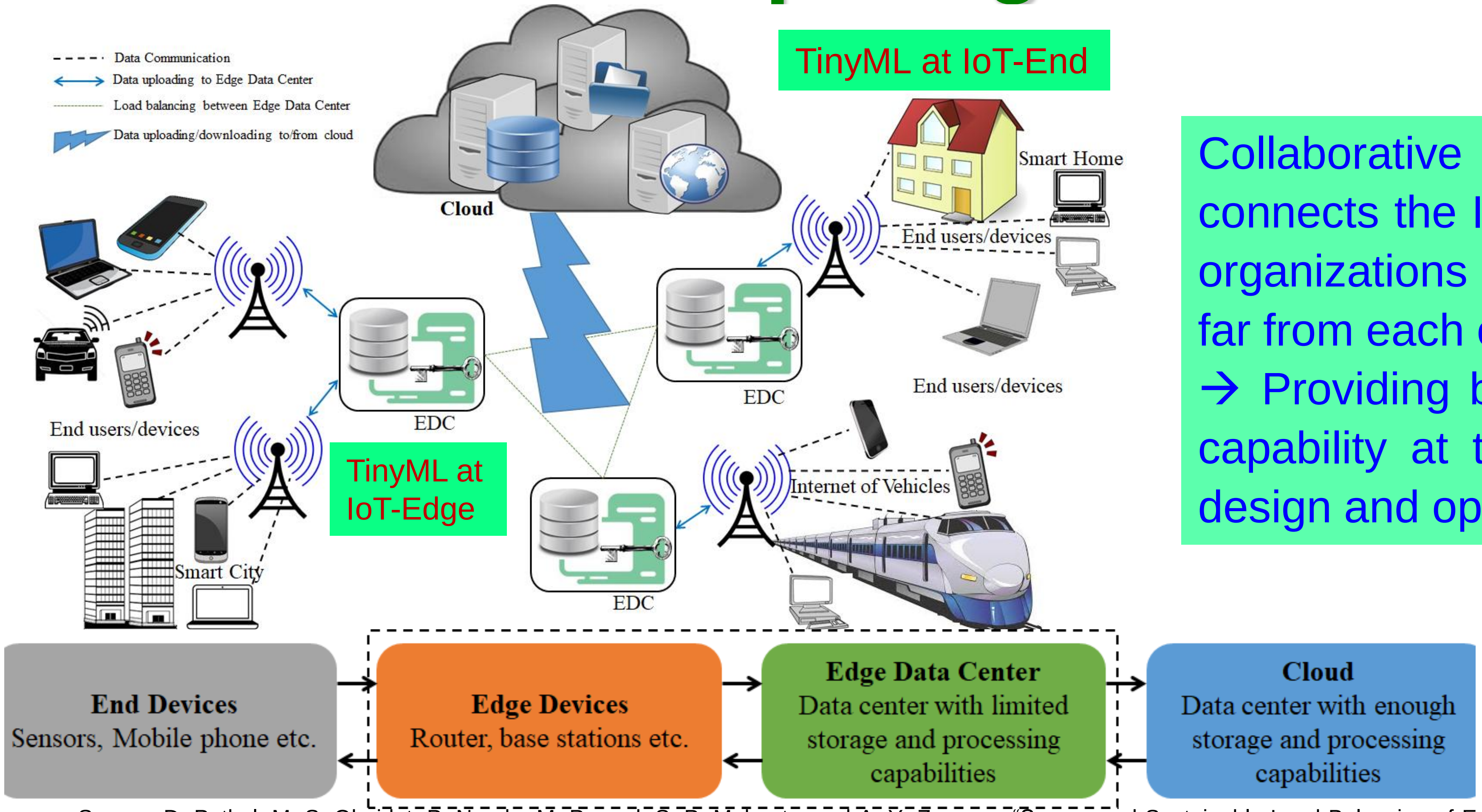
Our SbD based Eternal-Thing 2.0: Combines Analog-Trojan Resilience and Energy Harvesting at the IoT-Edge



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

Source: S. K. Ram, S. R. Sahoo, B. B. Das, K. K. Mahapatra, and **S. P. Mohanty**, "Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT", *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, Vol. 19, No. 2, March 2023, pp. 12:1--12:25, DOI: https://doi.org/10.1145/3575800.

Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



TinyML at IoT-End

TinyML at IoT-Edge

End Devices
Sensors, Mobile phone etc.

Edge Devices
Router, base stations etc.

Edge Data Center
Data center with limited storage and processing capabilities

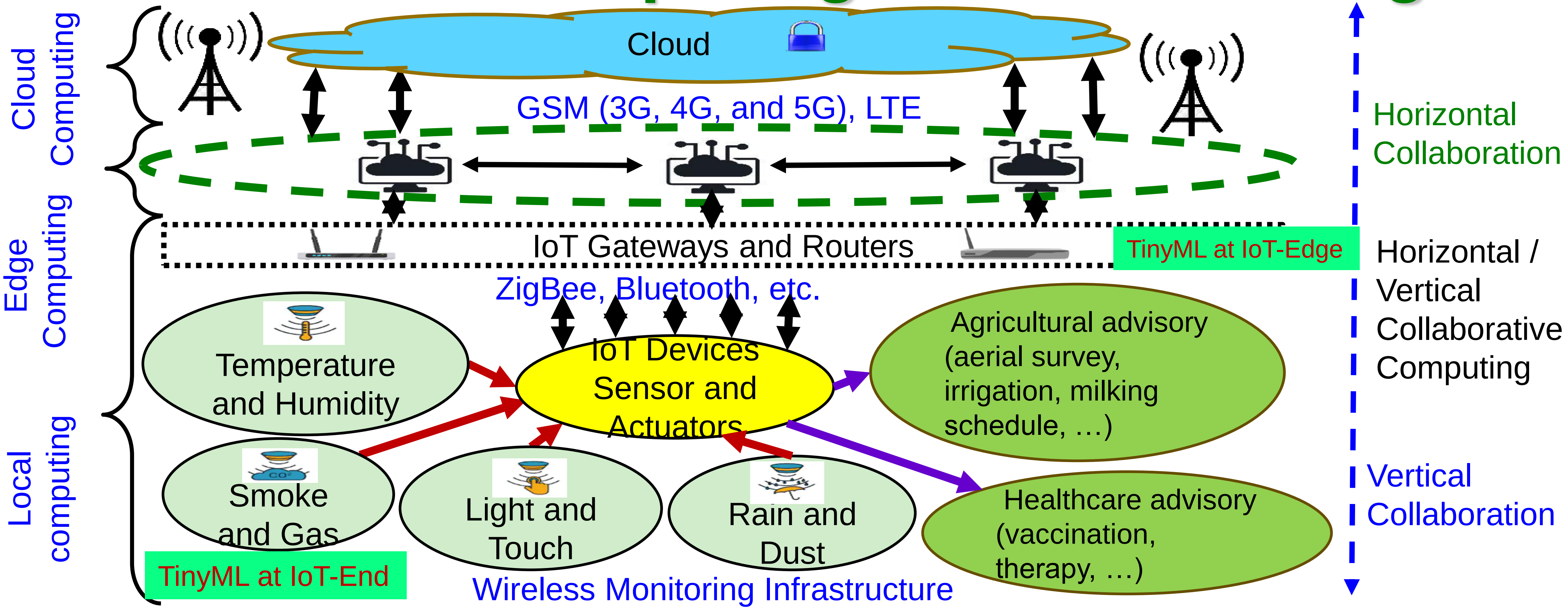
Cloud
Data center with enough storage and processing capabilities

Collaborative edge computing connects the IoT-edges of multiple organizations that can be near or far from each other

→ Providing bigger computational capability at the edge with lower design and operation cost.

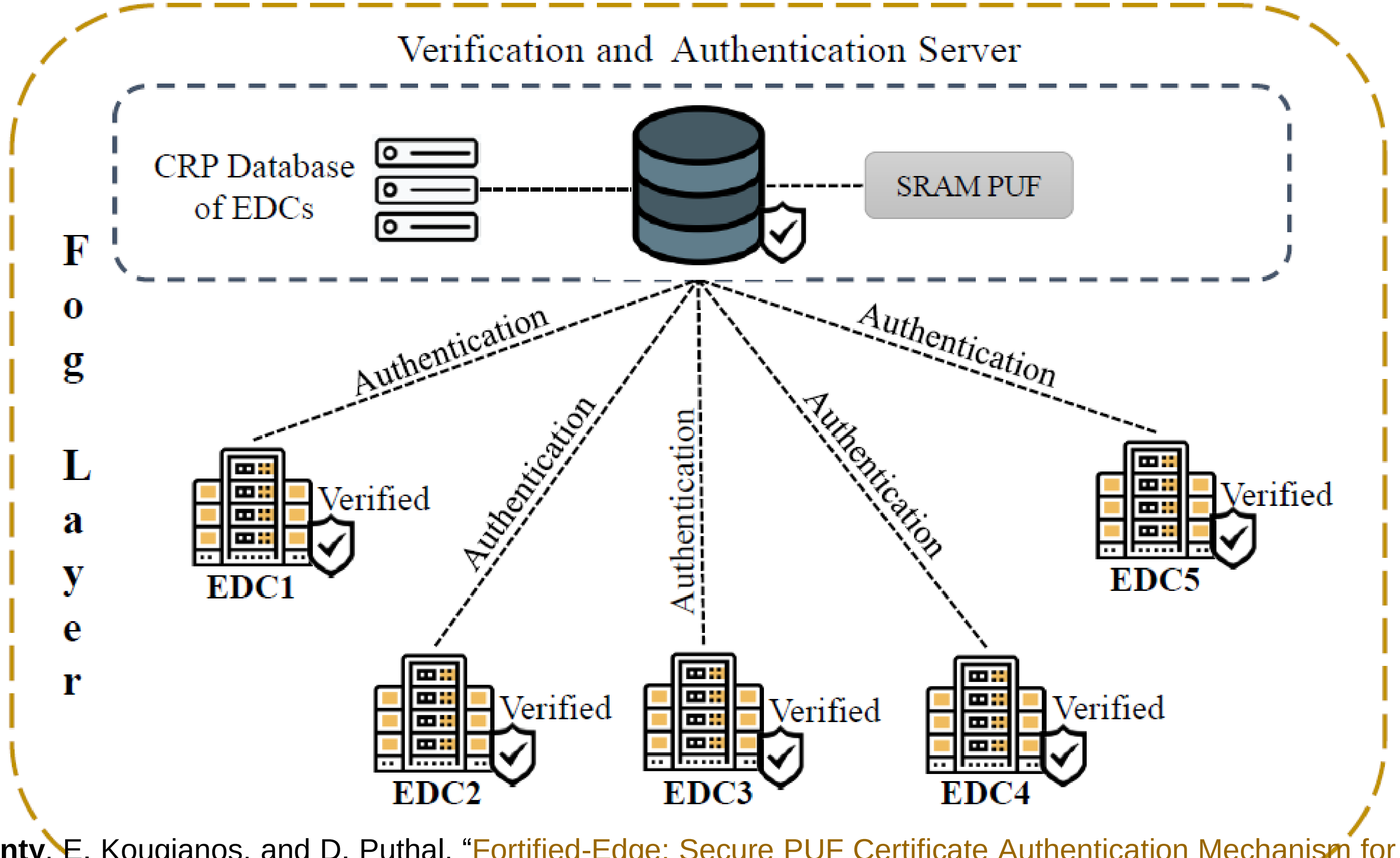
Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing", *IEEE Communications Mag*, Vol. 56, No 5, May 2018, pp. 60—65, DOI: https://doi.org/10.1109/MCOM.2018.1700795.

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, …)
CO2
Smoke and Gas
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

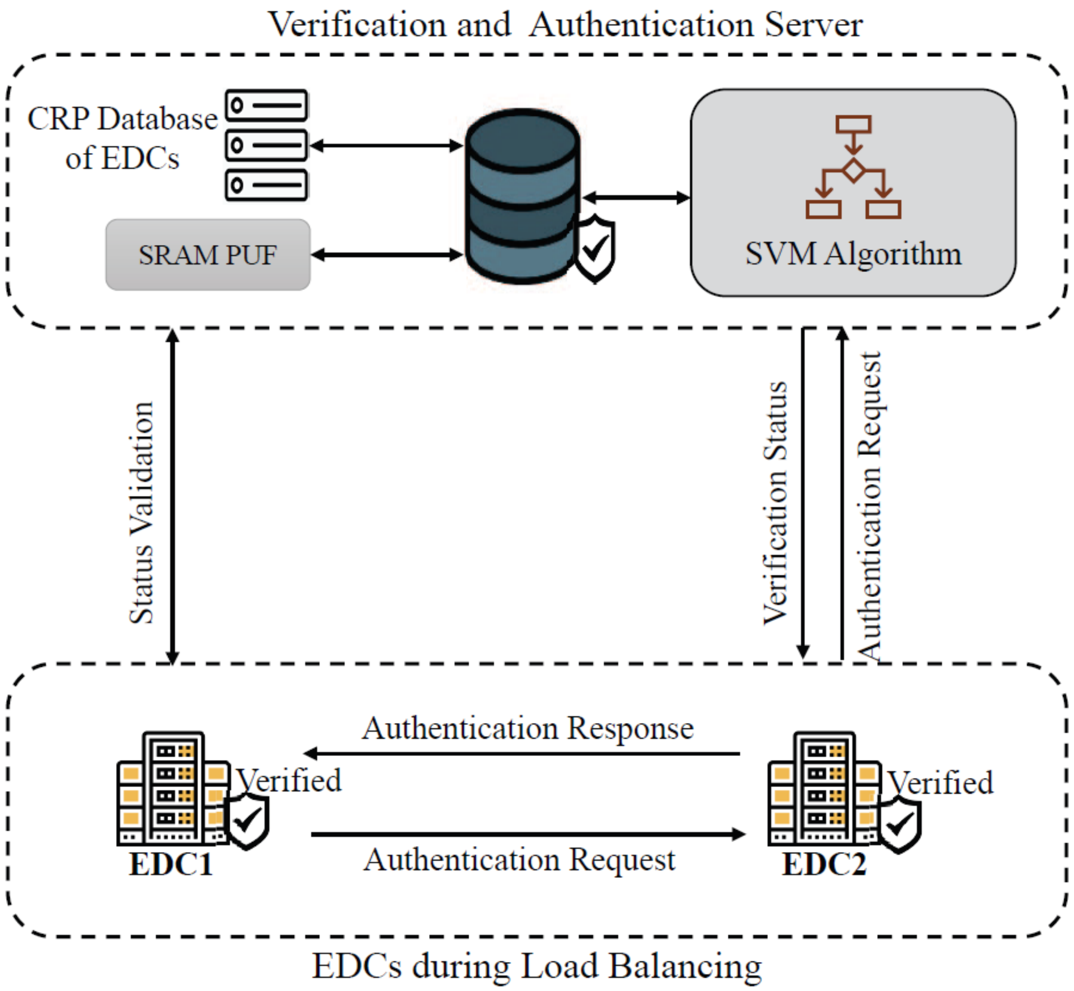
Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, “Collaborative Edge Computing for Smart Villages”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71, DOE: https://doi.org/10.1109/MCE.2021.3051813.

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



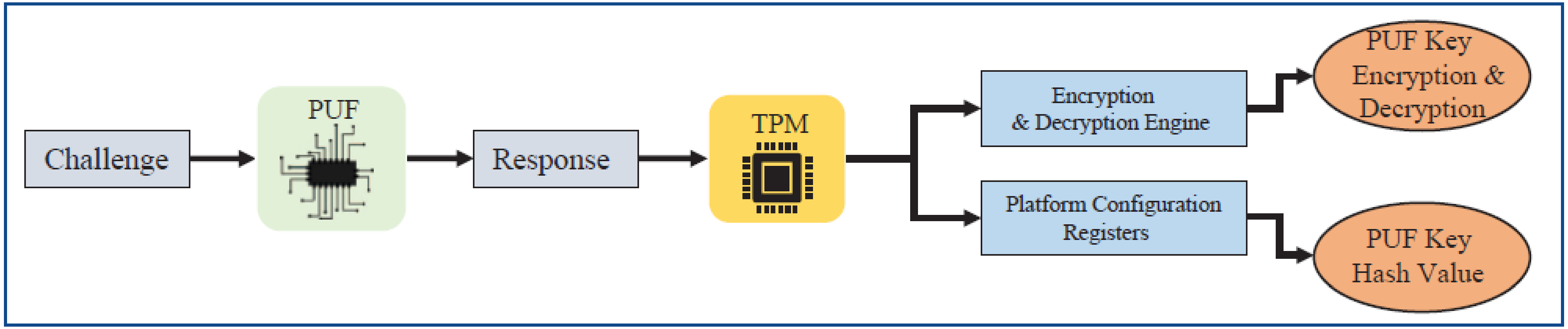
Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, “Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing”, in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 249--254, DOI: https://doi.org/10.1145/3583781.3590249.

Our Fortified-Edge 2.0: ML based Monitoring and Authentication of PUF-Integrated Secure EDC



Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, “Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center”, in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. 1-6, DOI: https://doi.org/10.1109/ISVLSI59464.2023.10238517.

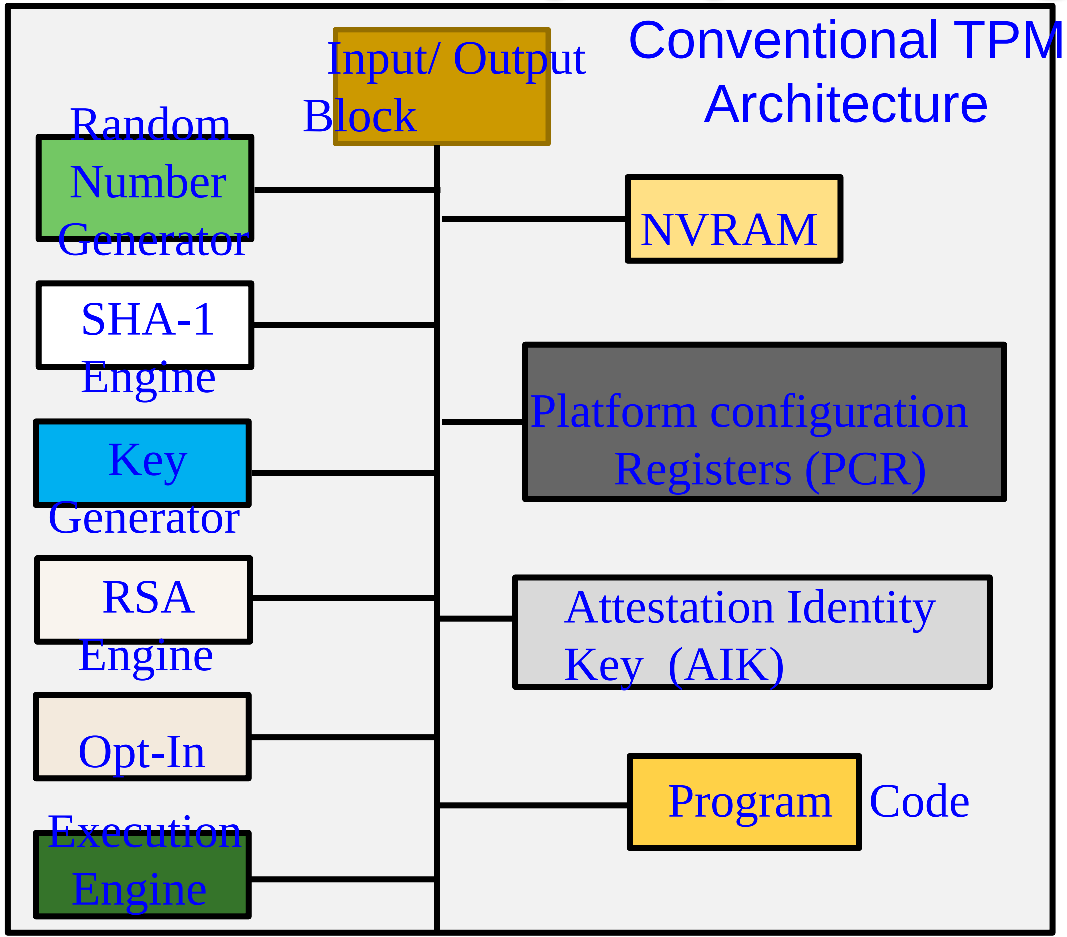
Our iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics

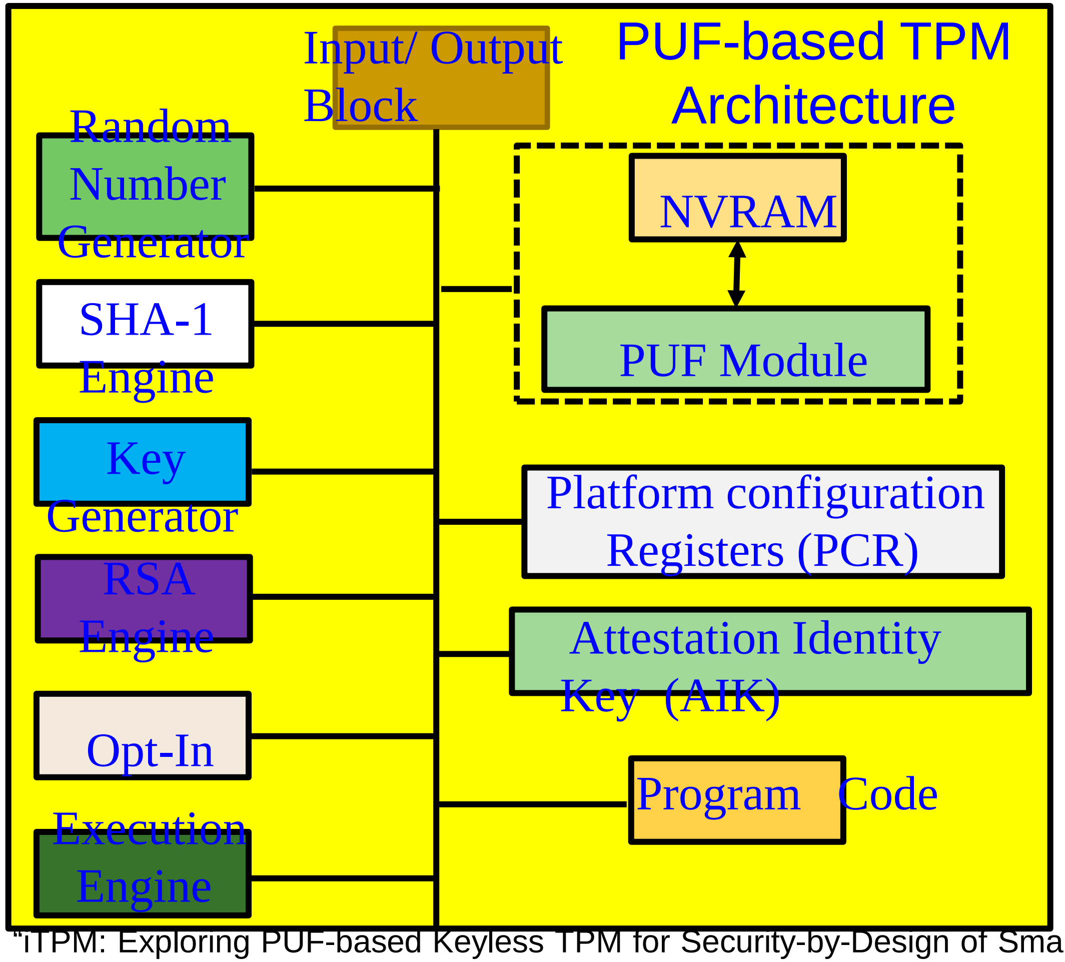

Challenge
PUF
Response
TPM
Encryption & Decryption Engine
Platform Configuration Registers
PUF Key Encryption & Decryption
PUF Key Hash Value

- The proposed SbD primitive works by performing secure verification of the PUF key using TPM's Encryption and Decryption engine. The securely verified PUF Key is then bound to TPM using Platform Configuration Registers (PCR).
- By binding PUF with PCR in TPM, a novel PUF-based access control. The policy can be defined, as bringing in a new security ecosystem for the emerging Internet-of-Everything era.

Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

Our iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics

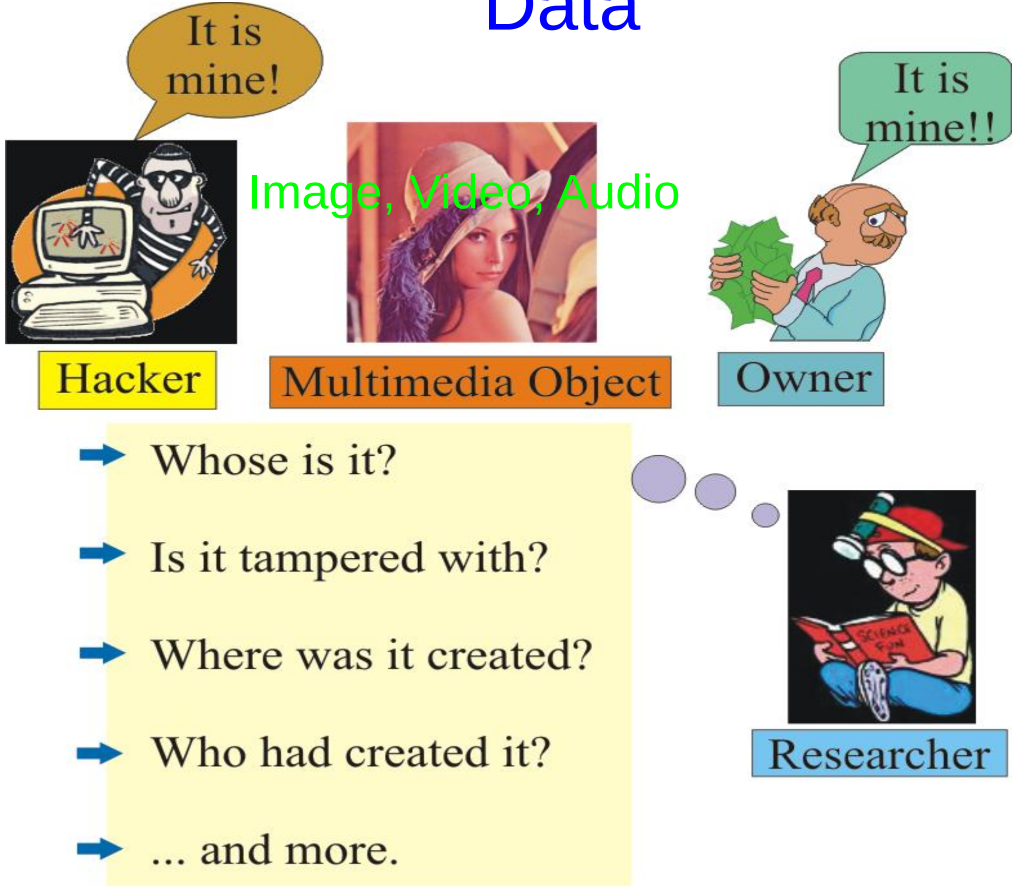




Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. Iyer, and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics", in *Proceedings of the IEEE-CS Symposium on VLSI (ISVLSI)*, 2023, pp. XXX, DOI: XXX.

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

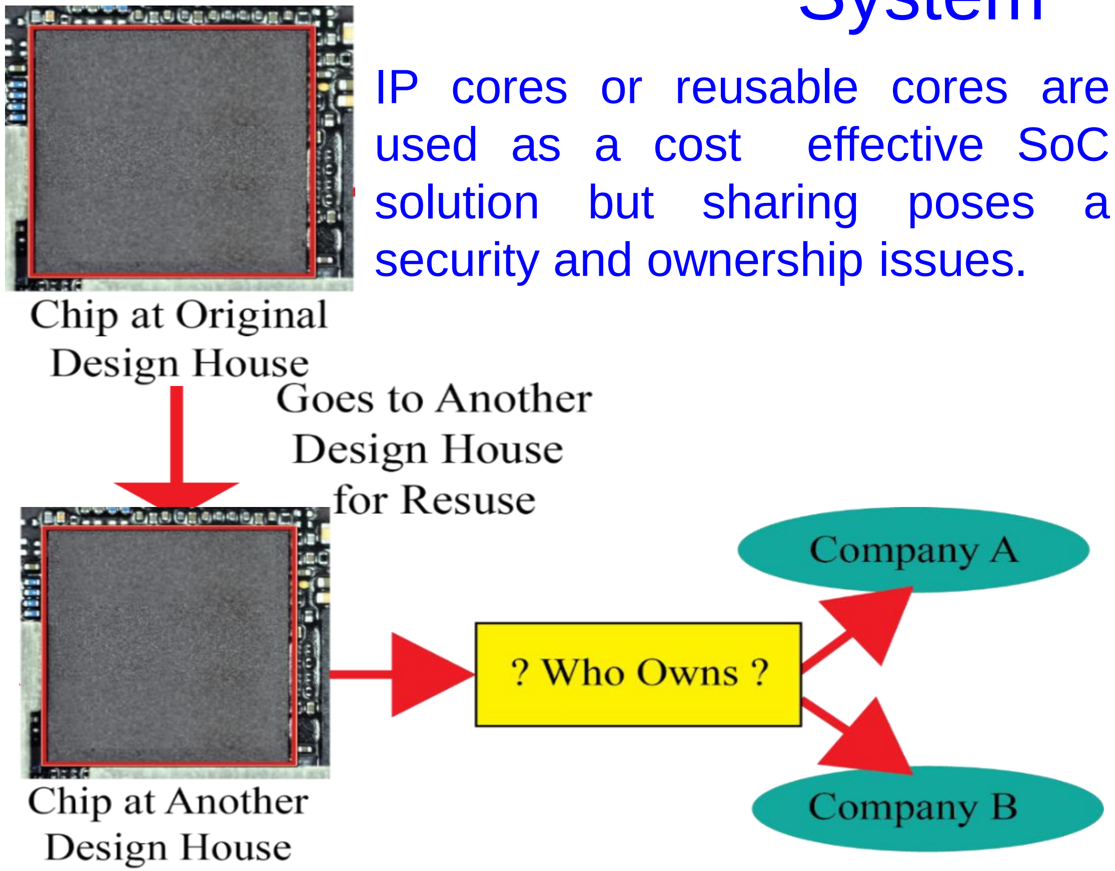
Data



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

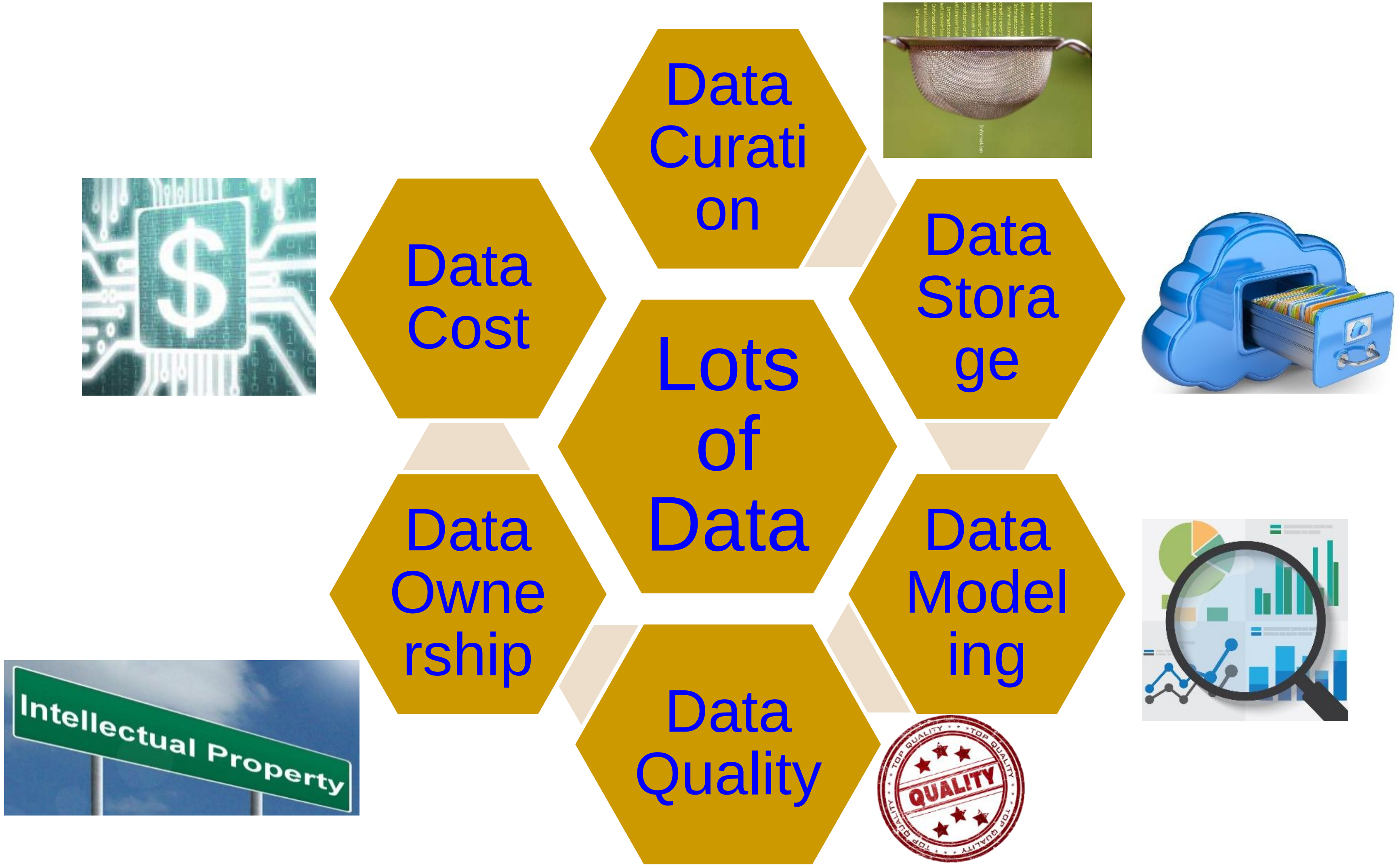
System

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.

Challenges of Data in IoT/CPS are Multifold



Lots of Data

Data Curation

Data Storage

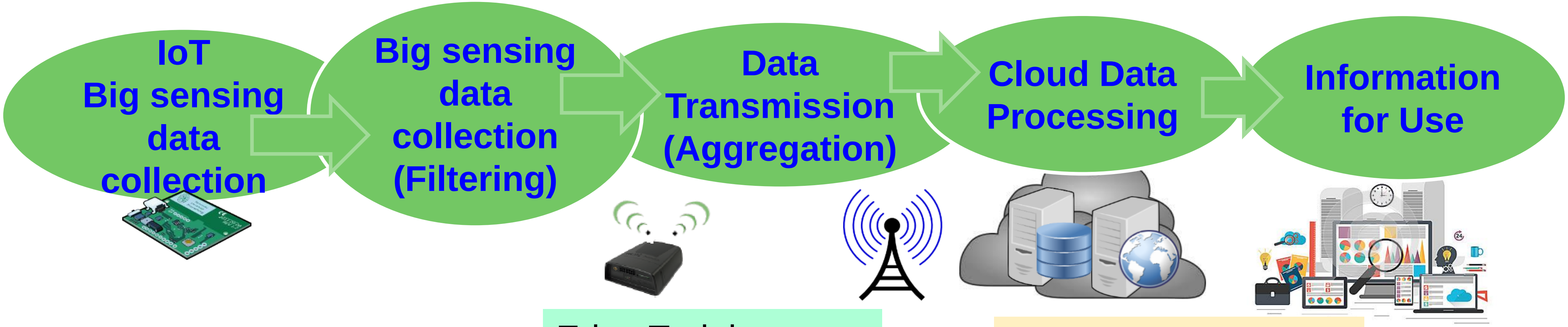
Data Modeling

Data Quality

Data Ownership

Data Cost

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

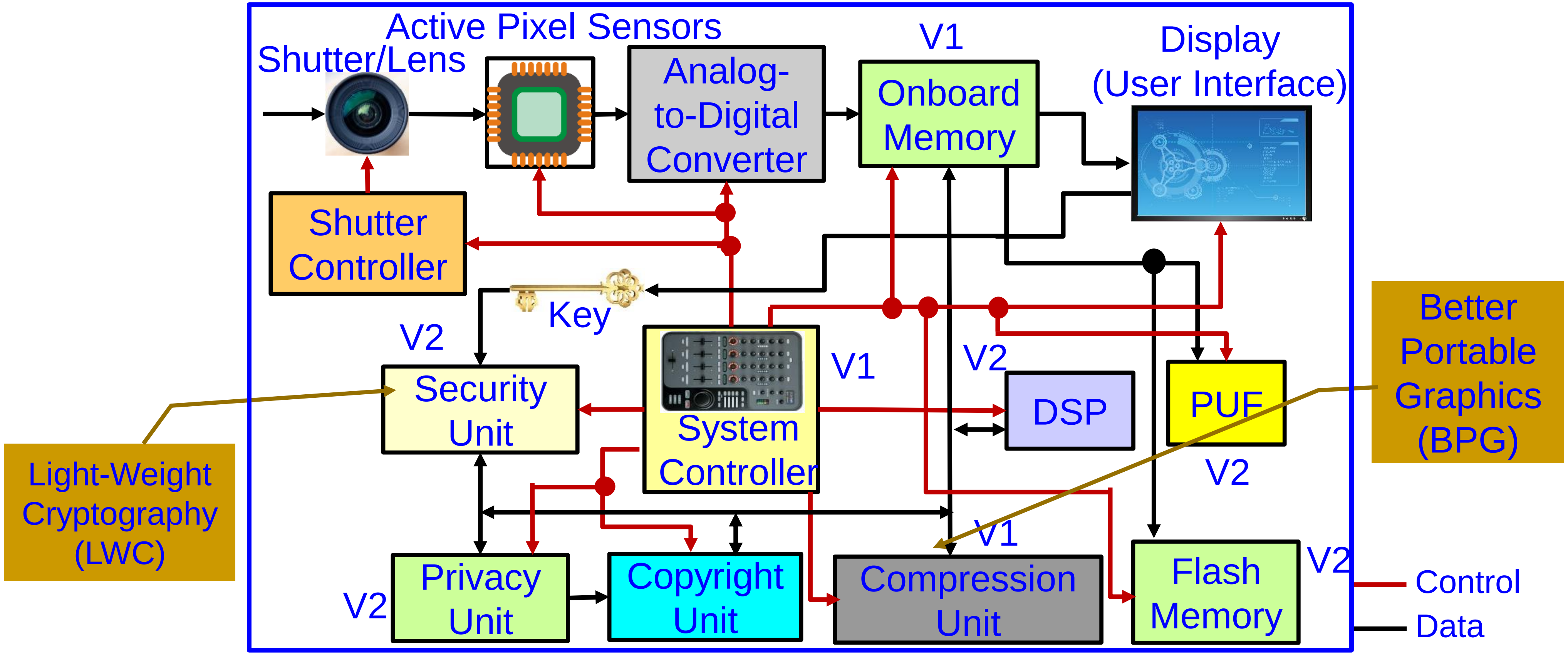
Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

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.

Secure Digital Camera (SDC) – My Invention

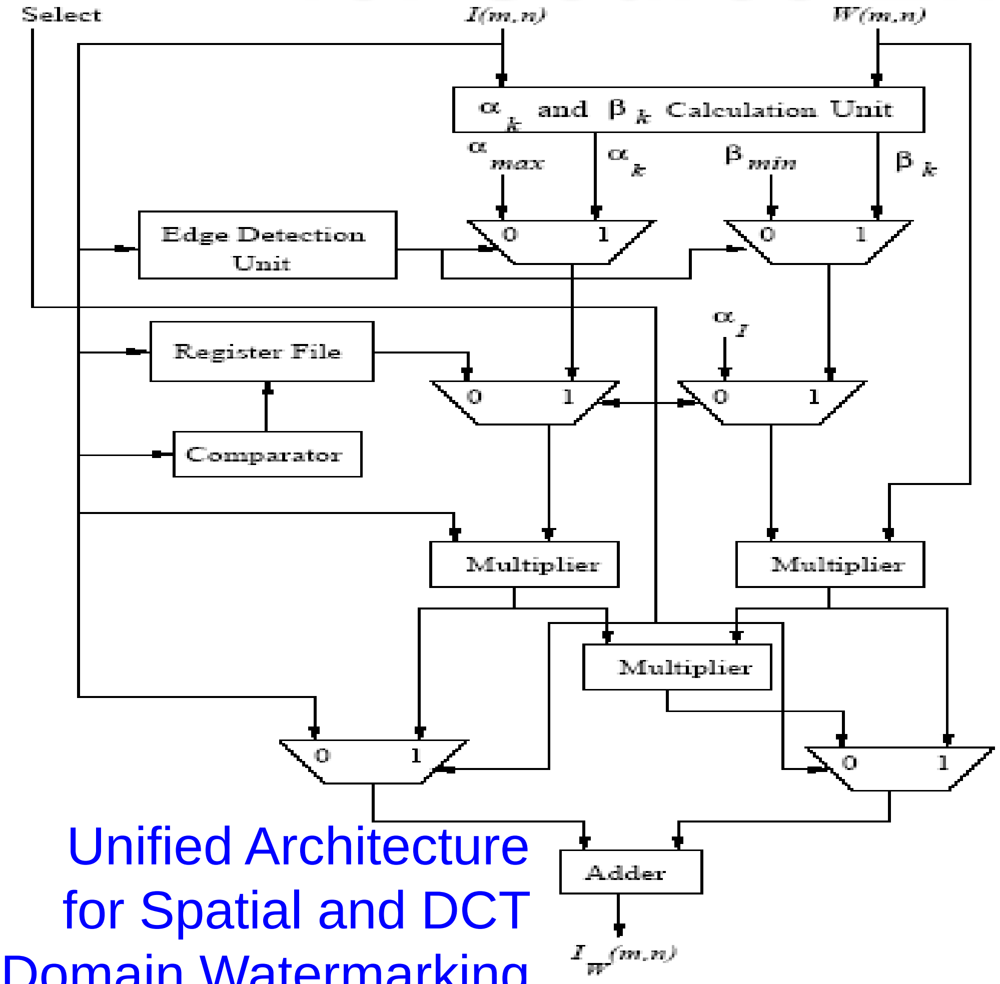


Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

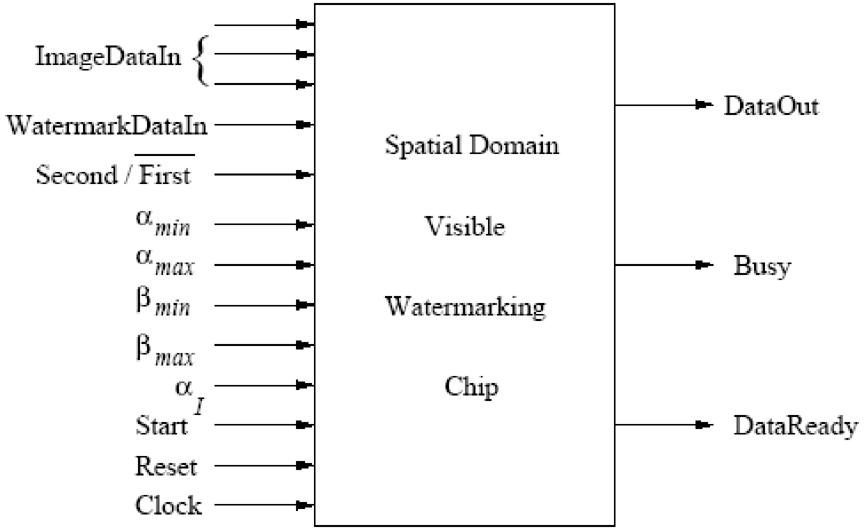
Security and/or Privacy by Design (SbD and/or PbD)

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

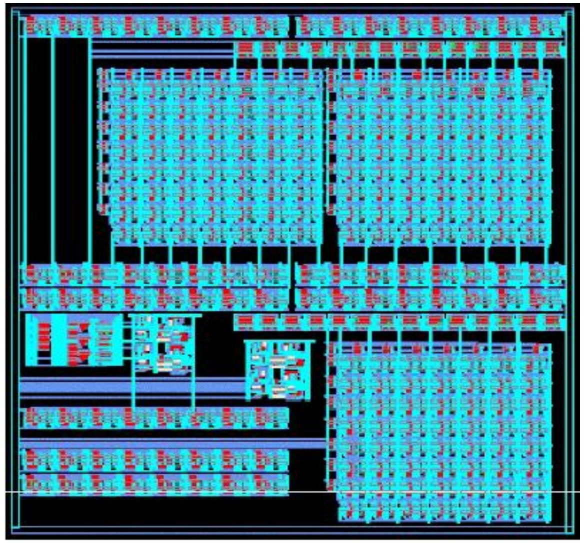
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

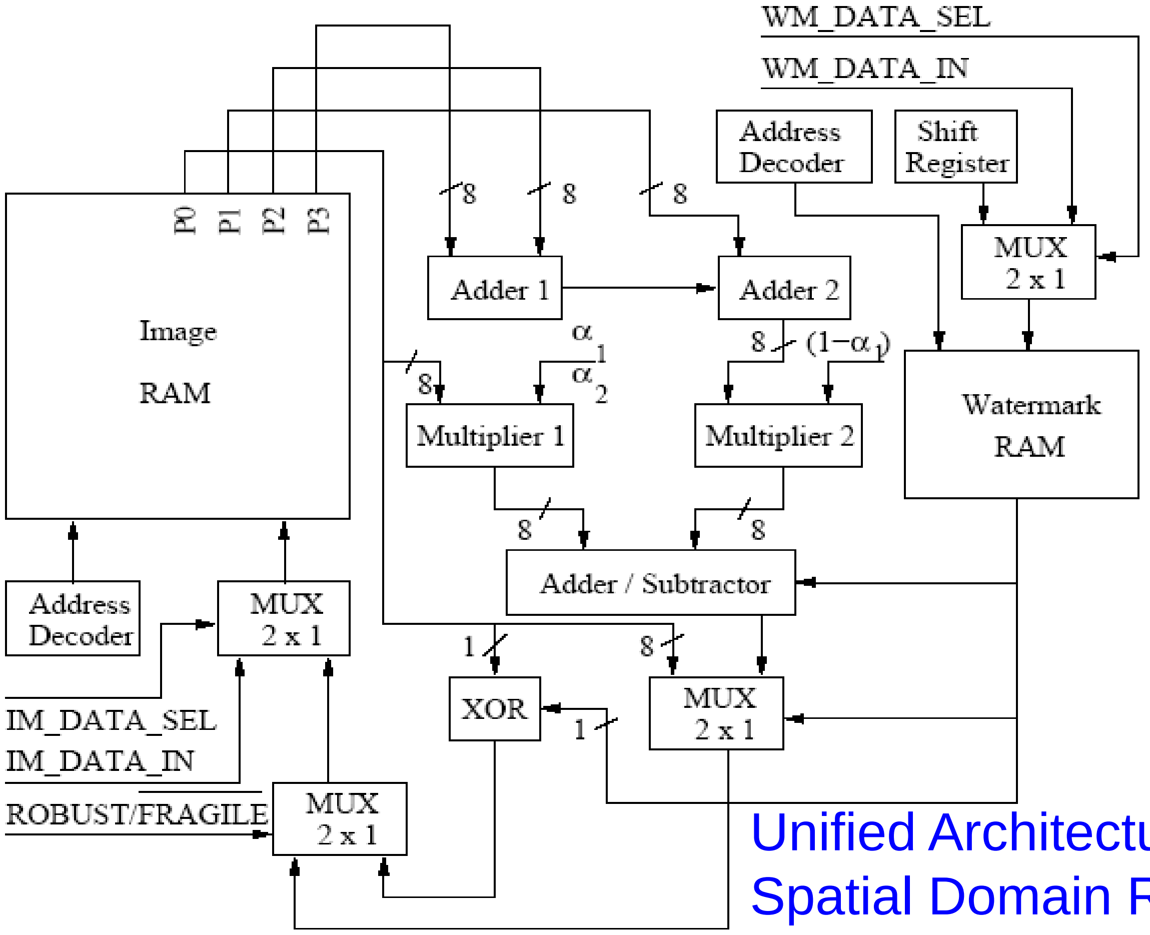
Chip Design Data

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

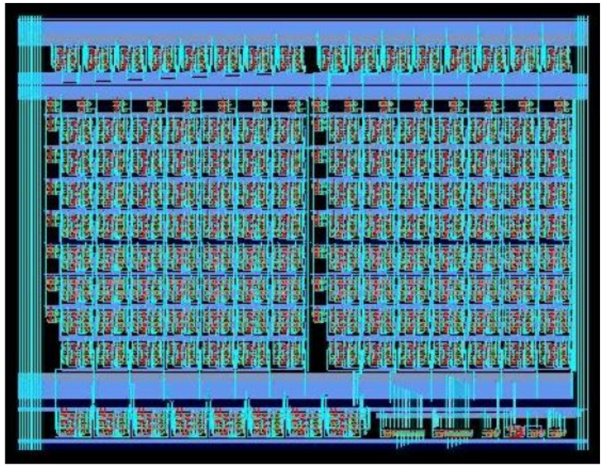
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

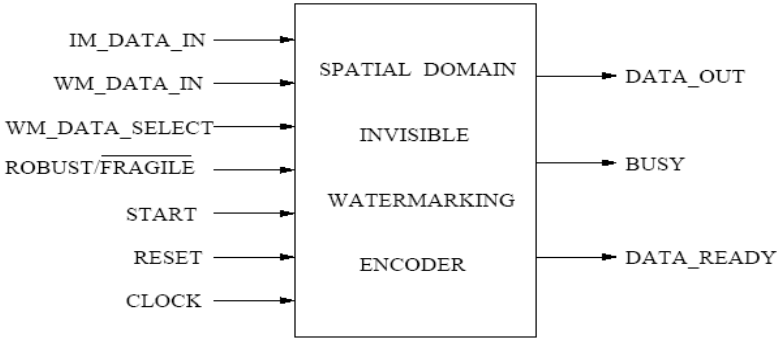
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout



Pin Diagram

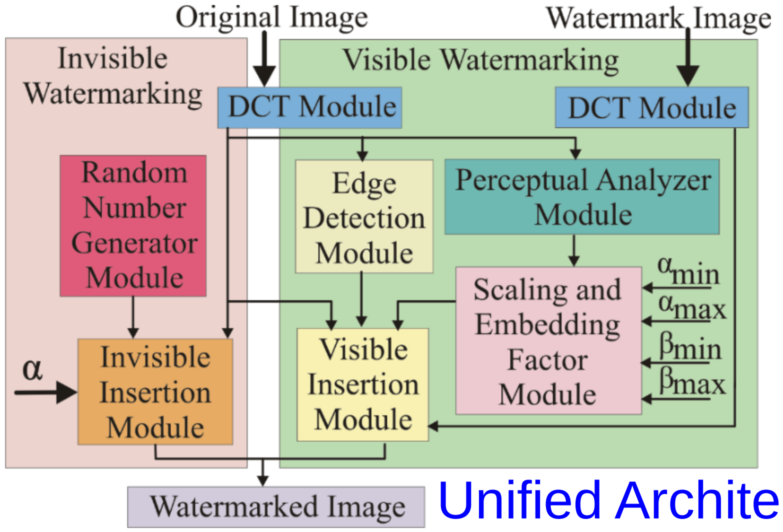
Chip Design Data

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

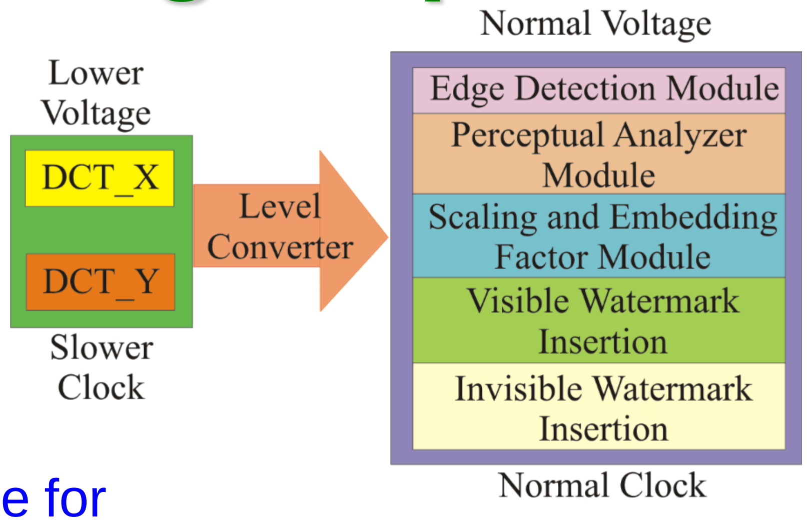
Power Consumption: 2.0 mW, Frequency: 500 MHz

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

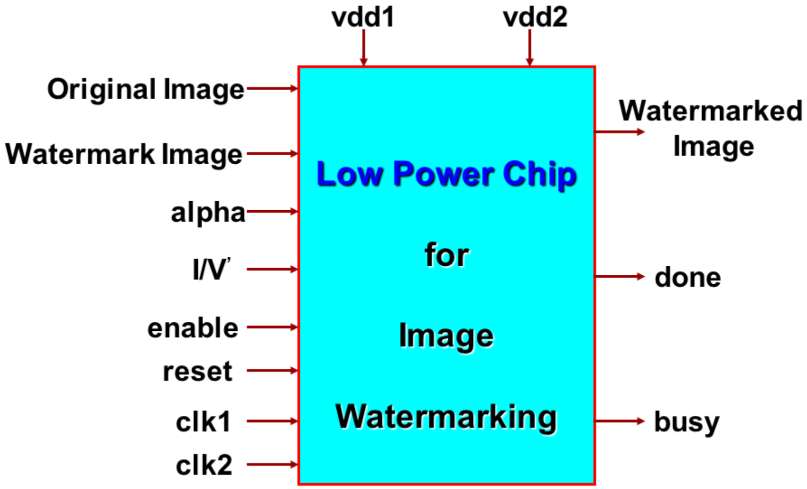


Unified Architecture for DCT Domain Watermarking

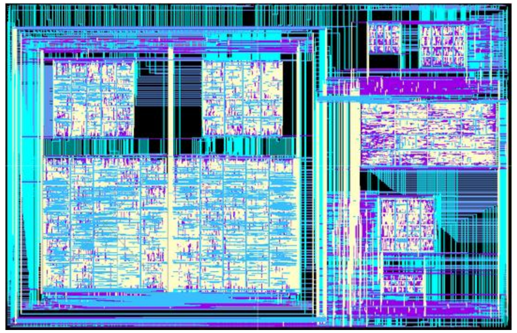


Lower Voltage
DCT_X
DCT_Y
Slower Clock
Level Converter
Normal Voltage
Edge Detection Module
Perceptual Analyzer Module
Scaling and Embedding Factor Module
Visible Watermark Insertion
Invisible Watermark Insertion
Normal Clock

DVDF Low-Power Design



Pin Diagram



Chip Layout

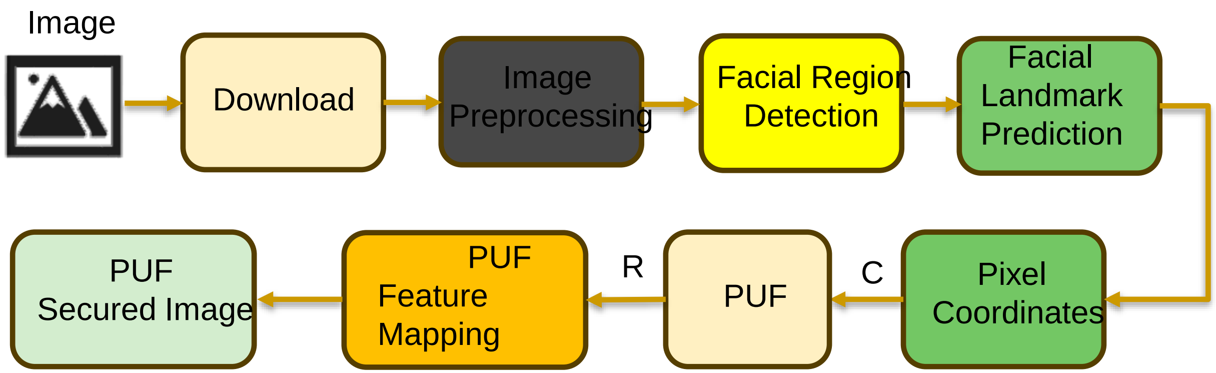
Chip Design Data

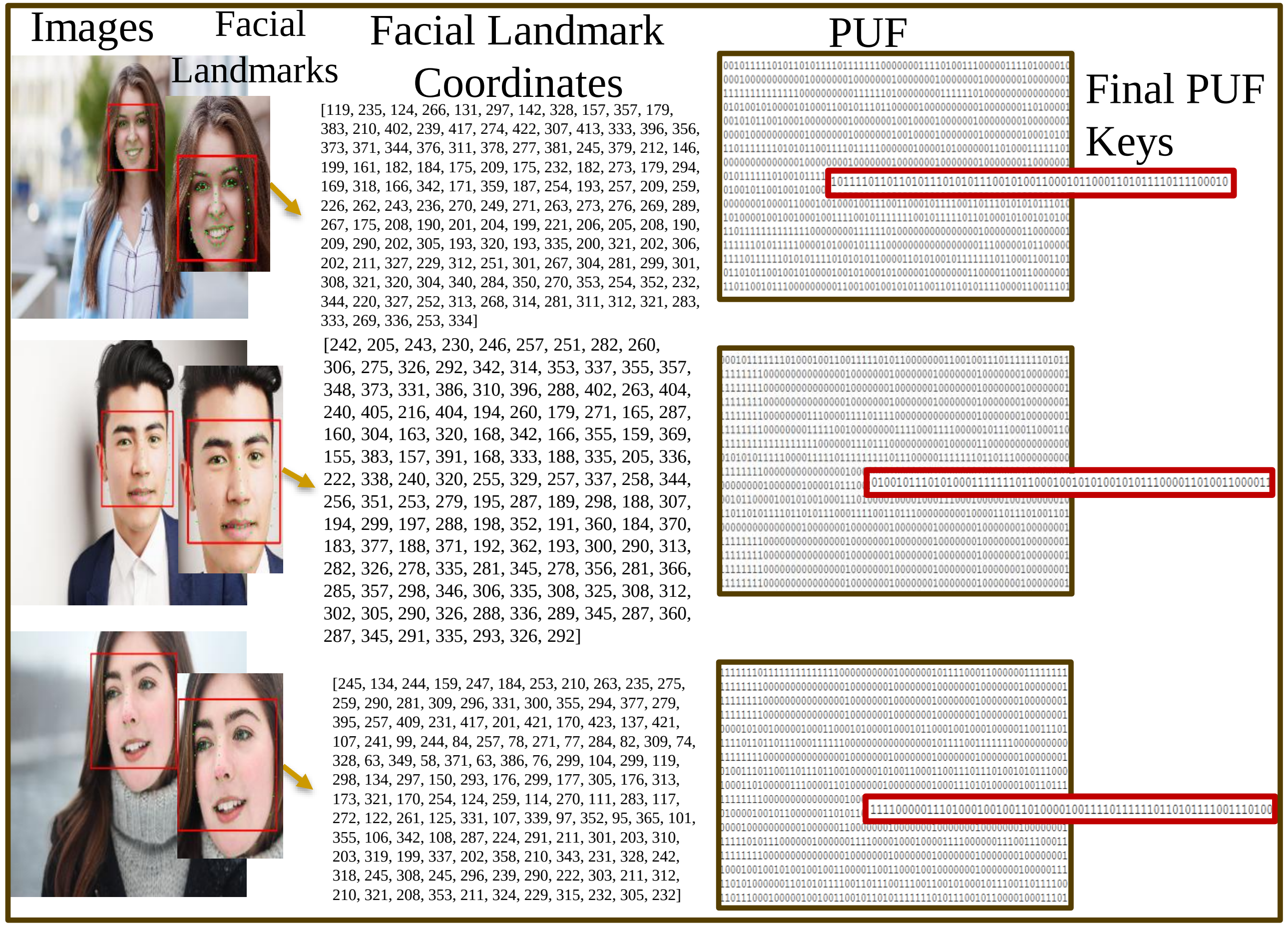
Total Area : 16.2 sq mm, No. of Transistors: 1.4 million

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.

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





[119, 235, 124, 266, 131, 297, 142, 328, 157, 357, 179, 383, 210, 402, 239, 417, 274, 422, 307, 413, 333, 396, 356, 373, 371, 344, 376, 311, 378, 277, 381, 245, 379, 212, 146, 199, 161, 182, 184, 175, 209, 175, 232, 182, 273, 179, 294, 169, 318, 166, 342, 171, 359, 187, 254, 193, 257, 209, 259, 226, 262, 243, 236, 270, 249, 271, 263, 273, 276, 269, 289, 267, 175, 208, 190, 201, 204, 199, 221, 206, 205, 208, 190, 209, 290, 202, 305, 193, 320, 193, 335, 200, 321, 202, 306, 202, 211, 327, 229, 312, 251, 301, 267, 304, 281, 299, 301, 308, 321, 320, 304, 340, 284, 350, 270, 353, 254, 352, 232, 344, 220, 327, 252, 313, 268, 314, 281, 311, 312, 321, 283, 333, 269, 336, 253, 334]

1011110110110101110101011100101001100010110001101011110111100010

[242, 205, 243, 230, 246, 257, 251, 282, 260, 306, 275, 326, 292, 342, 314, 353, 337, 355, 357, 348, 373, 331, 386, 310, 396, 288, 402, 263, 404, 240, 405, 216, 404, 194, 260, 179, 271, 165, 287, 160, 304, 163, 320, 168, 342, 166, 355, 159, 369, 155, 383, 157, 391, 168, 333, 188, 335, 205, 336, 222, 338, 240, 320, 255, 329, 257, 337, 258, 344, 256, 351, 253, 279, 195, 287, 189, 298, 188, 307, 194, 299, 197, 288, 198, 352, 191, 360, 184, 370, 183, 377, 188, 371, 192, 362, 193, 300, 290, 313, 282, 326, 278, 335, 281, 345, 278, 356, 281, 366, 285, 357, 298, 346, 306, 335, 308, 325, 308, 312, 302, 305, 290, 326, 288, 336, 289, 345, 287, 360, 287, 345, 291, 335, 293, 326, 292]

01001011101010001111111011000100101010010101110000110100110000011

[245, 134, 244, 159, 247, 184, 253, 210, 263, 235, 275, 259, 290, 281, 309, 296, 331, 300, 355, 294, 377, 279, 395, 257, 409, 231, 417, 201, 421, 170, 423, 137, 421, 107, 241, 99, 244, 84, 257, 78, 271, 77, 284, 82, 309, 74, 328, 63, 349, 58, 371, 63, 386, 76, 299, 104, 299, 119, 298, 134, 297, 150, 293, 176, 299, 177, 305, 176, 313, 173, 321, 170, 254, 124, 259, 114, 270, 111, 283, 117, 272, 122, 261, 125, 331, 107, 339, 97, 352, 95, 365, 101, 355, 106, 342, 108, 287, 224, 291, 211, 301, 203, 310, 203, 319, 199, 337, 202, 358, 210, 343, 231, 328, 242, 318, 245, 308, 245, 296, 239, 290, 222, 303, 211, 312, 210, 321, 208, 353, 211, 324, 229, 315, 232, 305, 232]

1111000001110100010010011010000100111101111110110101111001110100

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

Conclusion

Conclusion

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

Future Directions

- Security by Design (PbD) needs significant research.
- Cybersecurity, Privacy, IP Protection of Information, Device, and System in Cyber-Physical Systems or CPS need more research.
- Cybersecurity of IoT-based systems (e.g. Smart Healthcare device/data, Smart Agriculture, Smart Grid, UAV, Smart Cars) needs research.
- Sustainable IoT and CPS with integrated cybersecurity features can provide robust solutions.
- More research is needed for robust, low-overhead PUF design and protocols that can be integrated in any CPS.
- Cybersecurity solutions for the quantum computing era for system needs attention.