Cybersecurity – An Overview

Fulbright Lecture 2023 – KL Deemed University

Guntur, India, 1-31 July 2023

Homepage

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

Outline

- Internet of Things (IoT)
- Security and Privacy Challenges
- Introduction to Cryptography
- Introduction to Watermarking
- Hardware Assisted Security
- Physical Unclonable Functions (PUF)
- Blockchain
- Conclusion

Big Picture

The Internet of Things (IoT)

In the IoT era, the number of devices connected to the internet is exponentially increasing.

The Internet of Things - Applications

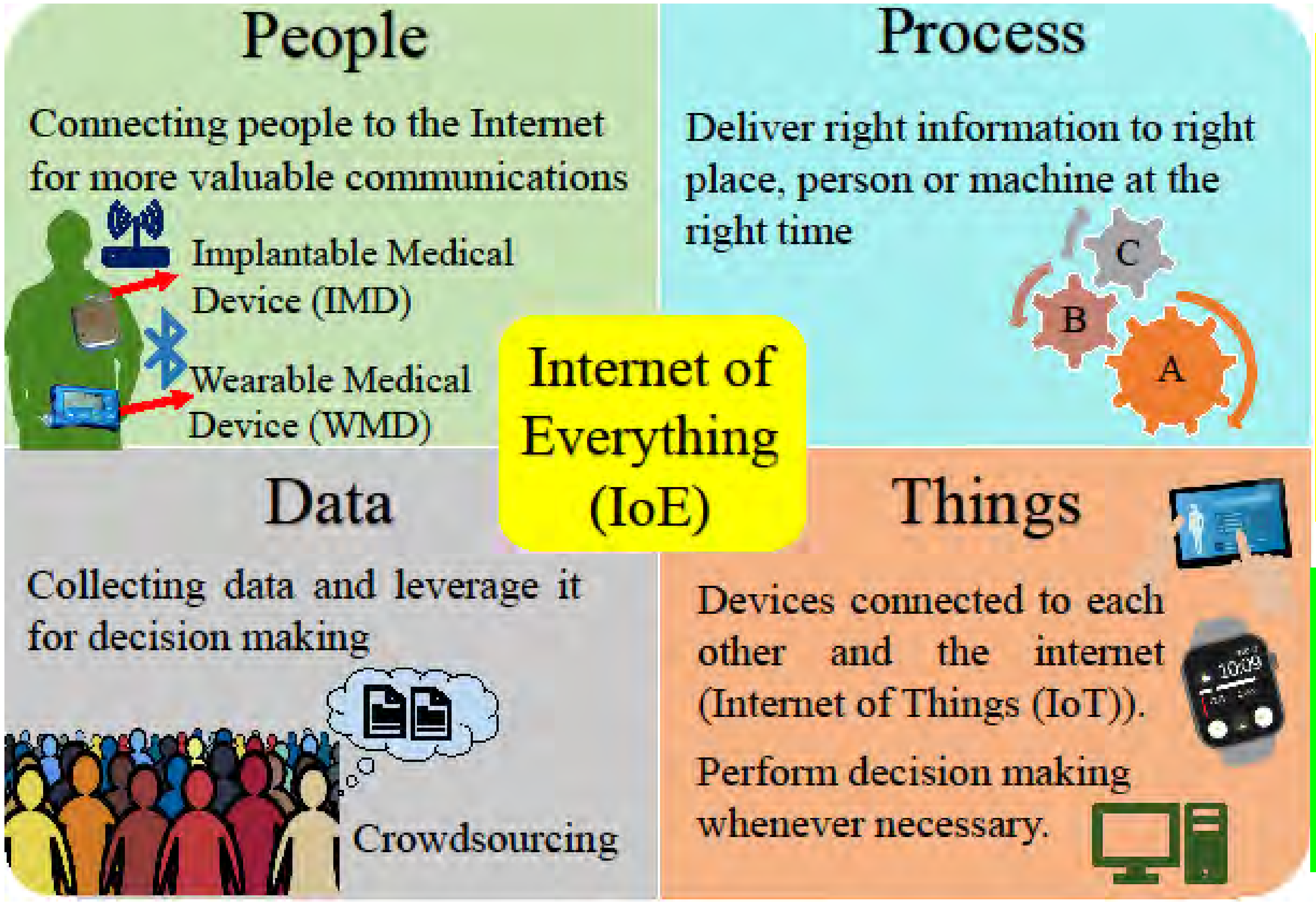
And many more...

Internet of Things (IoT) Statistics

- Estimated $475B market by 2020 and $6T spent on IoT solutions between 2015 and 2020.
- Improving human experience and better safety are provided with the help of IoT device generated data.
- Cisco predicts machine to machine connections will increase from 1.5B in 2018 to 3.3B in 2021.

Source: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#3e4e5afb1480

Internet of Every Things (IoE)

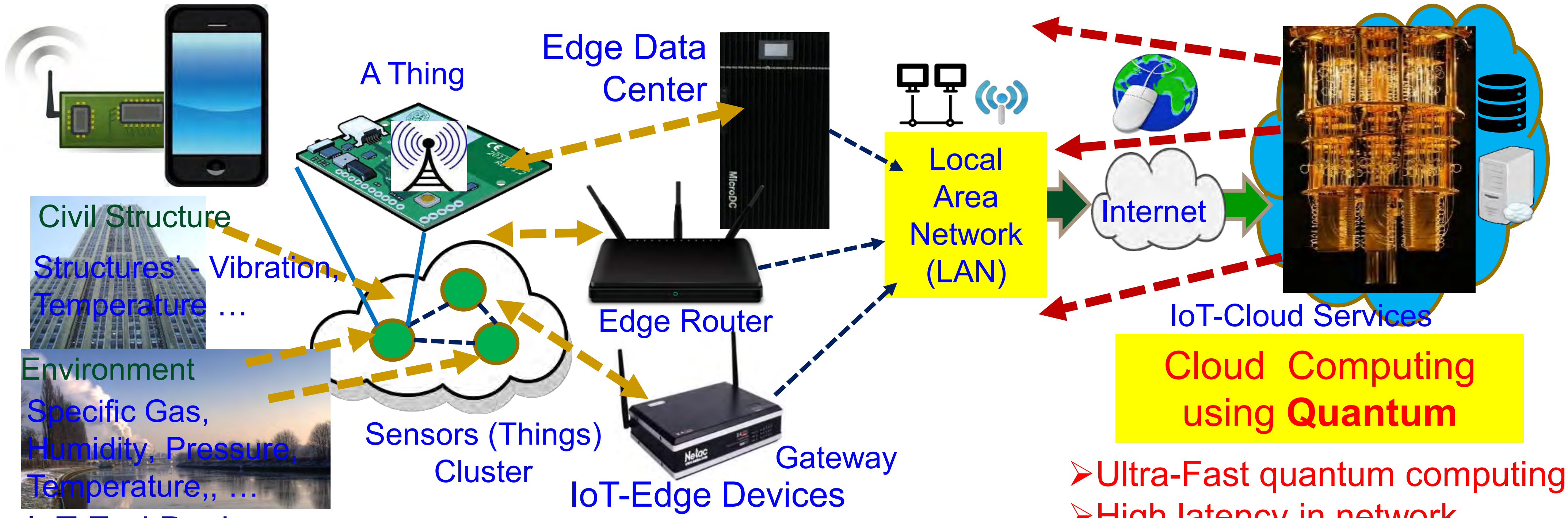


Requires:
- Data, Device, and System Security
- Data, Location, and System Privacy

Need of the Hour:
- Security/Secure by Design (SbD)
- Privacy by Design (PbD)

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

Cybersecurity Nightmare ← Quantum Computing



In-Sensor/End-Device Computing

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

Edge Computing

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

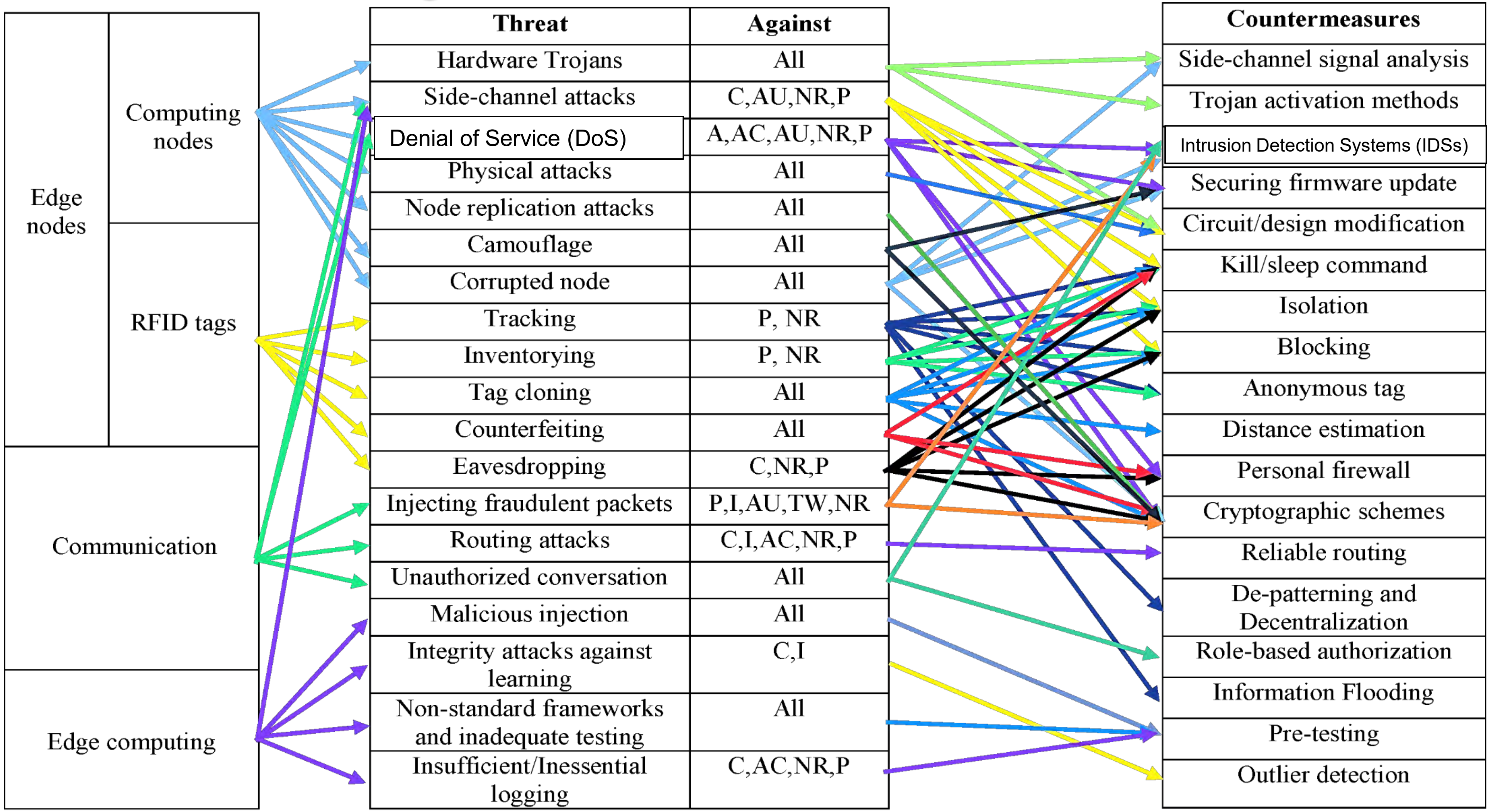
Cloud Computing using Quantum

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

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

Cybersecurity – Various Aspects

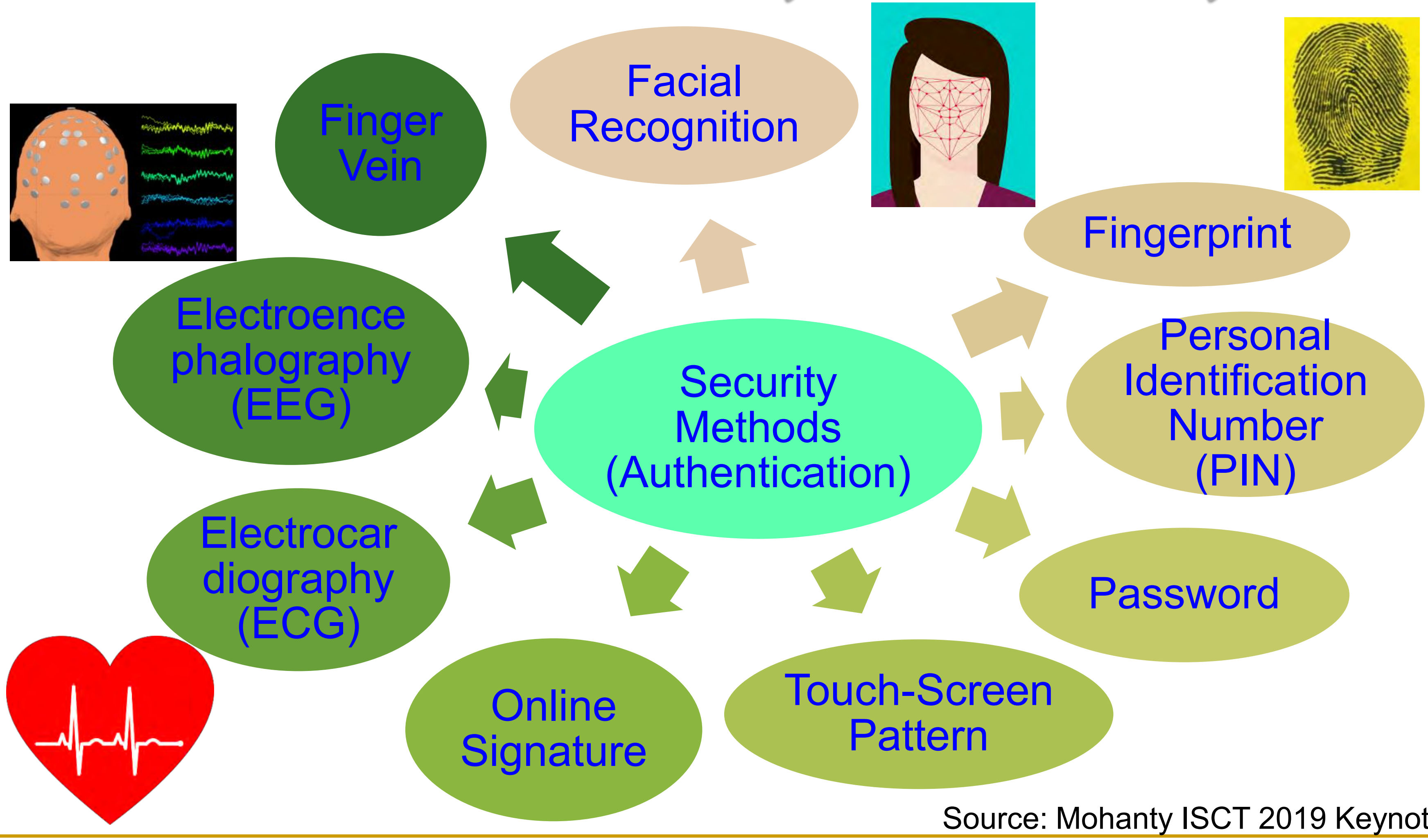
IoT Security - Attacks and Countermeasures



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

Source: Nia 2017,IEEE TETC 2017

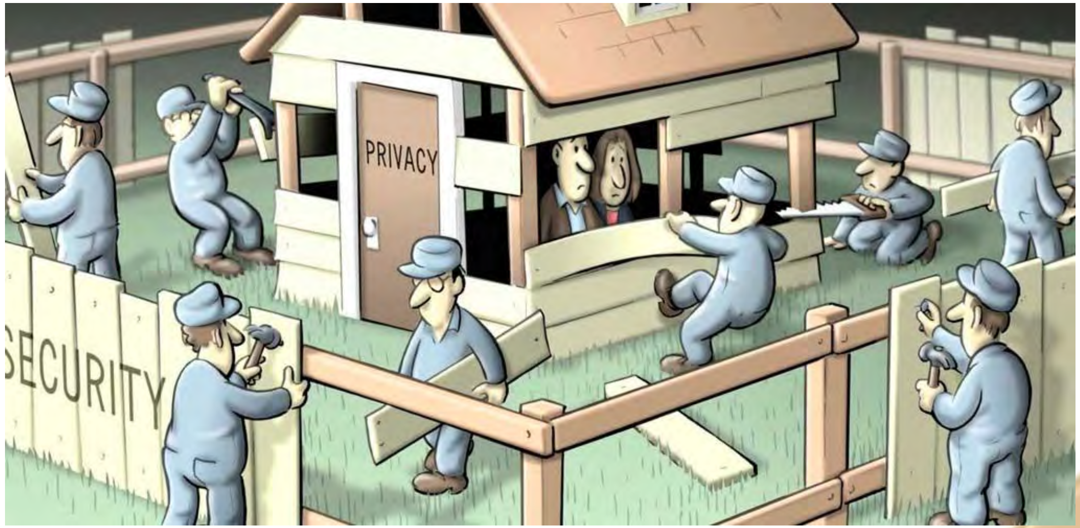
Security, Authentication, Access Control – Home, Facilities, ...

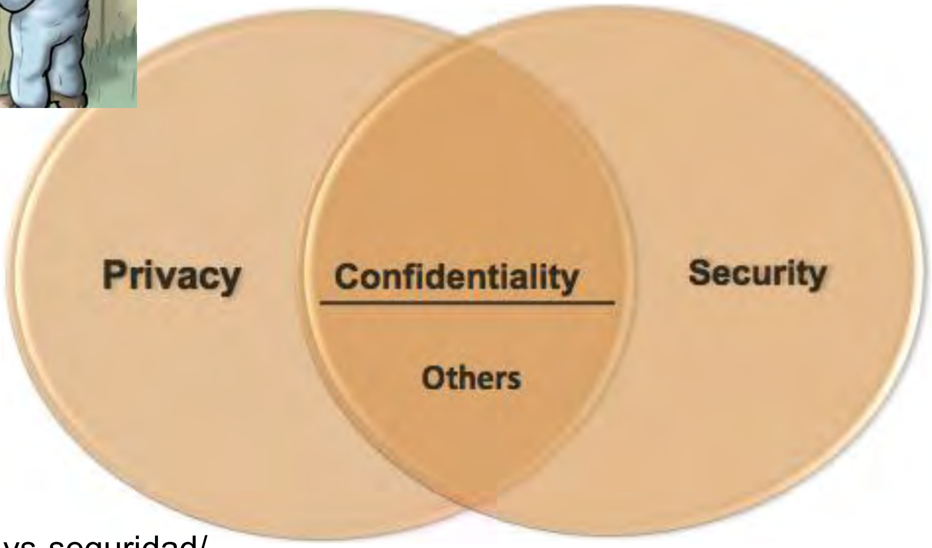


Source: Mohanty ISCT 2019 Keynote

Security, Privacy, and Copyright

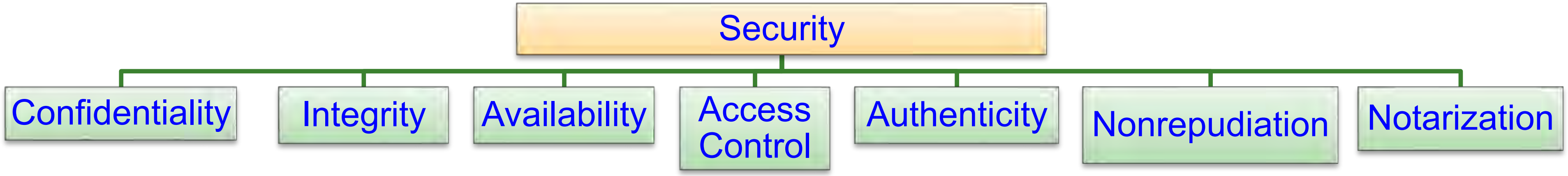
Security, Privacy, IP Rights





Source: https://blogs.deusto.es/master-informatica/privacidad-vs-seguridad/

Security – Different Aspects



Cyber Attacks

September 2017: Cybersecurity incident at Equifax affected 143 million U.S. consumers.

Hacked: US Department Of Justice

Who did it: Unknown

What was done: Information on 10,000 DHS and 20,000 FBI employees.

Details: The method of the attack is still a mystery and it's been said that it took a week for the DOJ to realize that the info had been stolen.

February 2016

Hacked: Yahoo #2

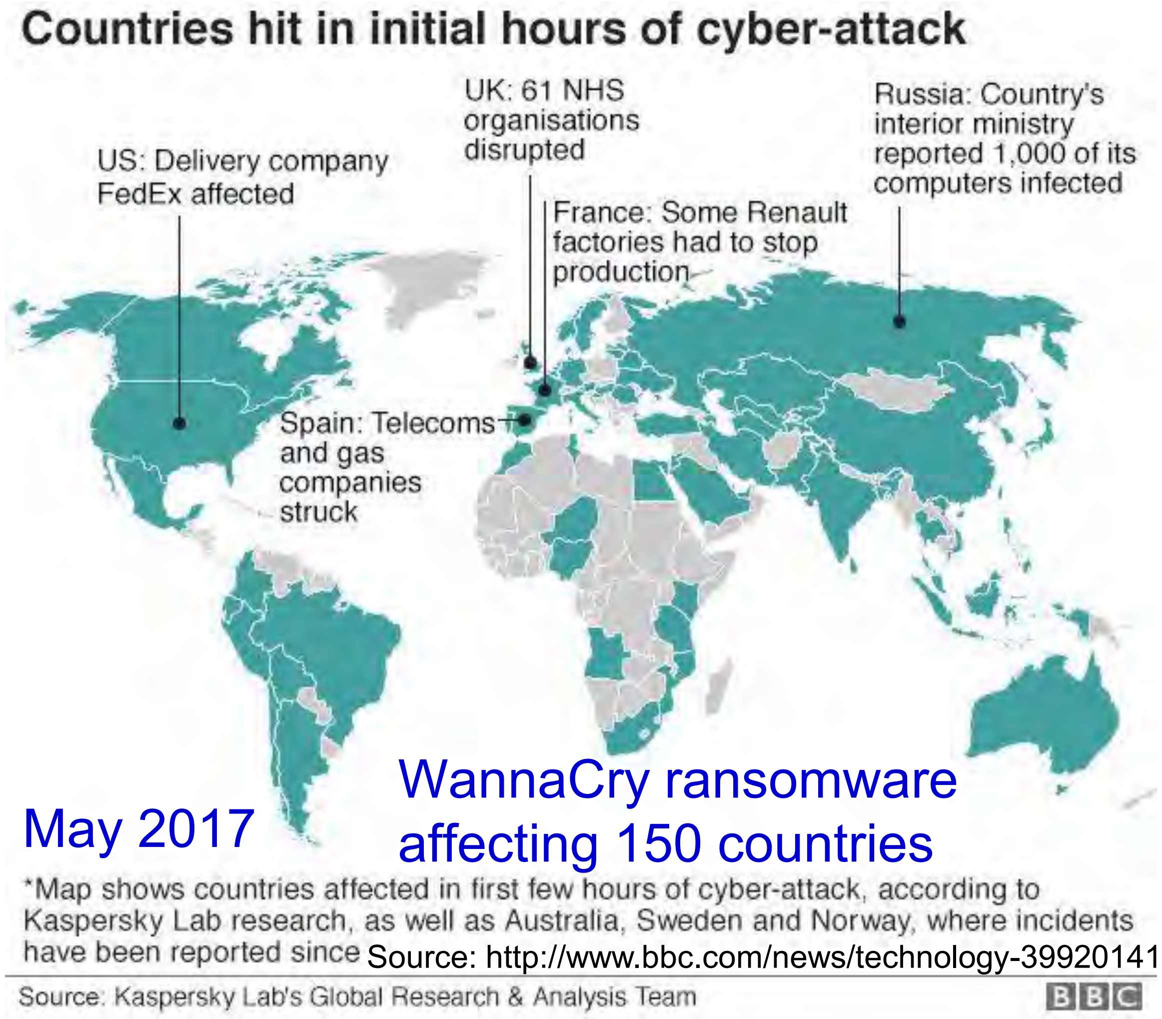
YAHOO!

Who did it: Unknown

What was done: 1 billion accounts were compromised.

Details: Users names, email addresses, date of birth, passwords, phone numbers, and security questions were all taken.

December 2016



May 2017

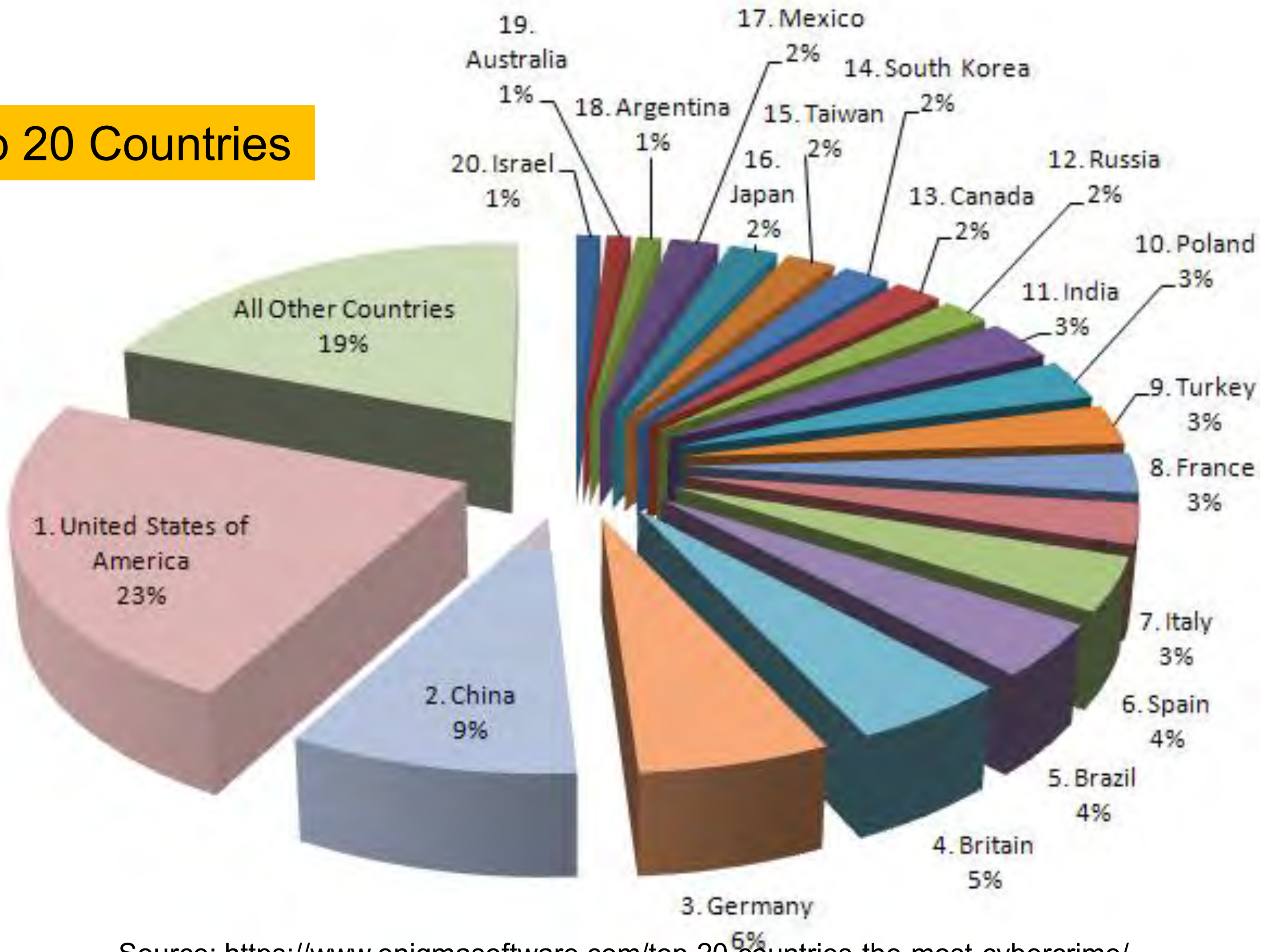
WannaCry ransomware affecting 150 countries

Source: http://www.bbc.com/news/technology-39920141

Source: https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/#73bb0bee48e3

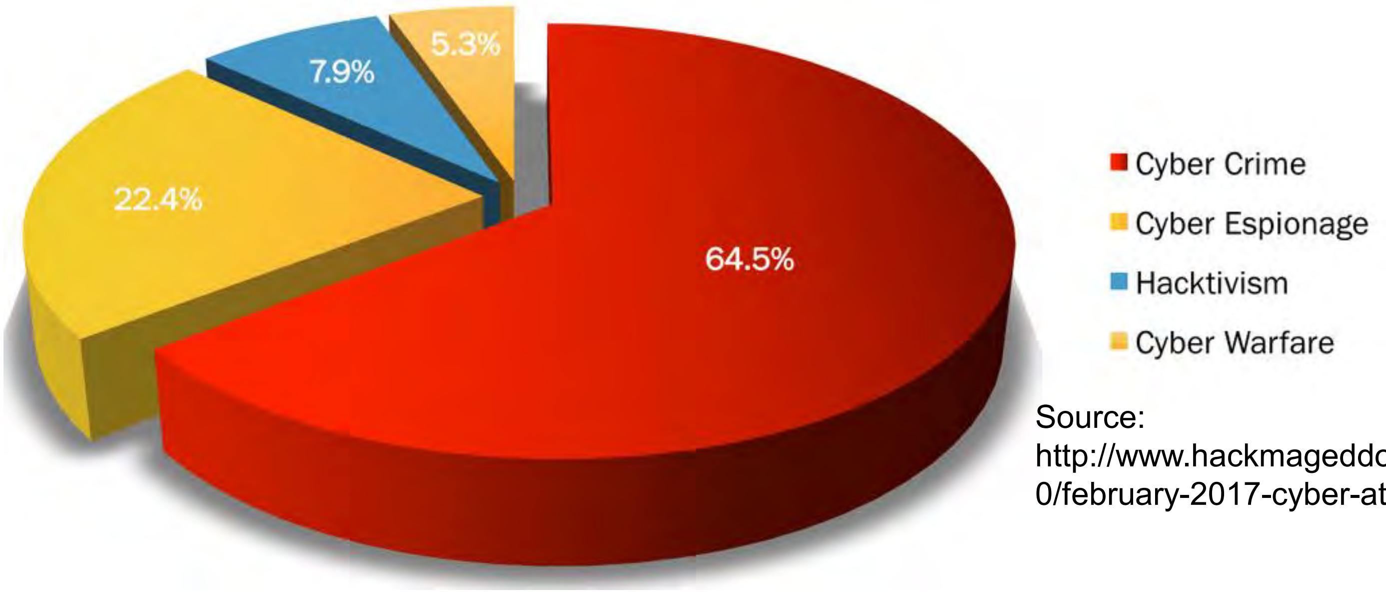
Security - Information, System …

Cybercrime – Top 20 Countries



Source: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Security - Information, System …



Source: http://www.hackmageddon.com/2017/03/20/february-2017-cyber-attacks-statistics/

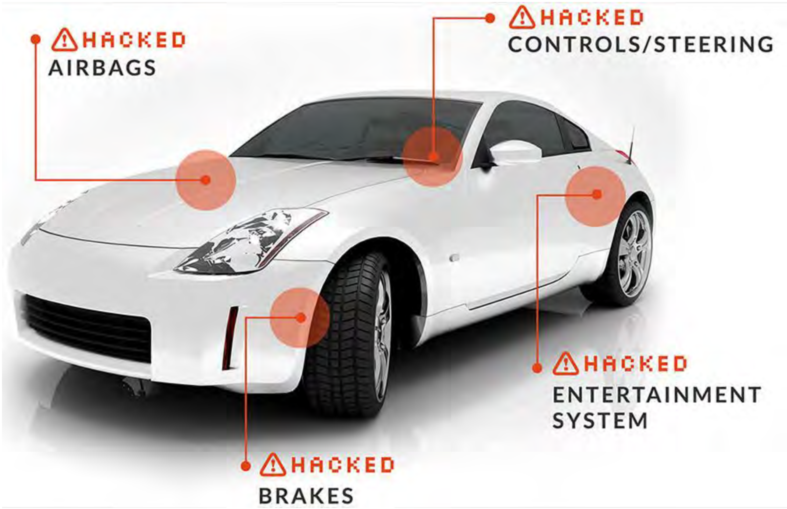
- Cybercrime damage costs to hit $6 trillion annually by 2021
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021

Source: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Security Challenge - 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/

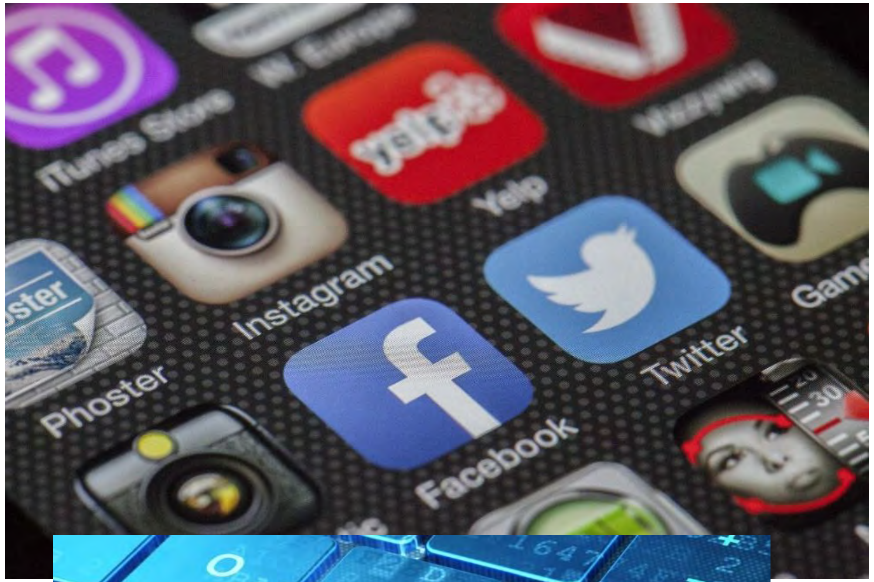
Source: http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/

Smart Grid Attacks can be Catastrophic

Threats	Vulnerabilities	Source of Threats	Attacks	Impacts
Security group knowledge	Management deficiencies of network access rules; Inaccurate critical assests documentation	Phishers	Stuxnet	Ukraine power attack, 2015
Information leakage	Unencrypted services in IT systems; Weak protection credentials	Nation	Night Dragon	Stuxnet attack in Iran, 2010
Access point	Improper access point; Remote access deficiency; Firewall filtering deficiency	Hacker	Virus	Browns Ferry plant, Alabama 2006
Unpatched System	Unpatched operating system; Unpatched third party application	Insider	Denial of service	Emergency shut down of Hatch Nuclear Power Plant, 2008
Weak cyber security	Buffer overflow in control system services; SQL injection vulnerability	Terrorist	Trojan horse	Slammer attack at Davis-Besse power plant, 2001
		Spammers	Worm	Attacks at South Korea NPP, 2015
		Spyware / Malware authors	Zero day exploit	
			Logical bomb	
			Phishing	
			Distributed DoS	
			False data Injection attack	

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, March 2019.

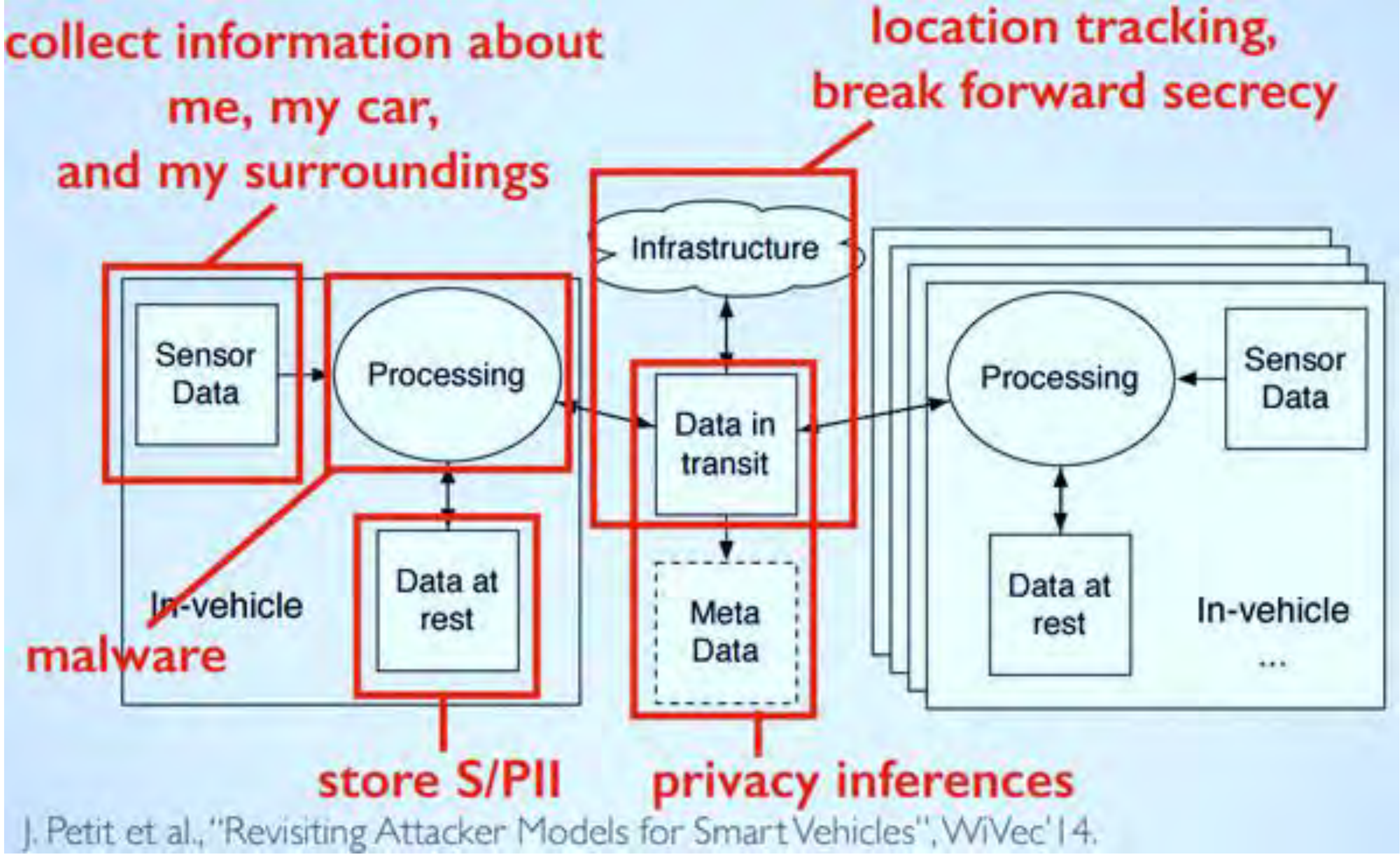
Privacy



Source: http://ciphercloud.com/three-ways-pursue-cloud-data-privacy-medical-records/

Source: http://blog.veriphyr.com/2012/06/electronic-medical-records-security-and.html

Privacy Challenge – System



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

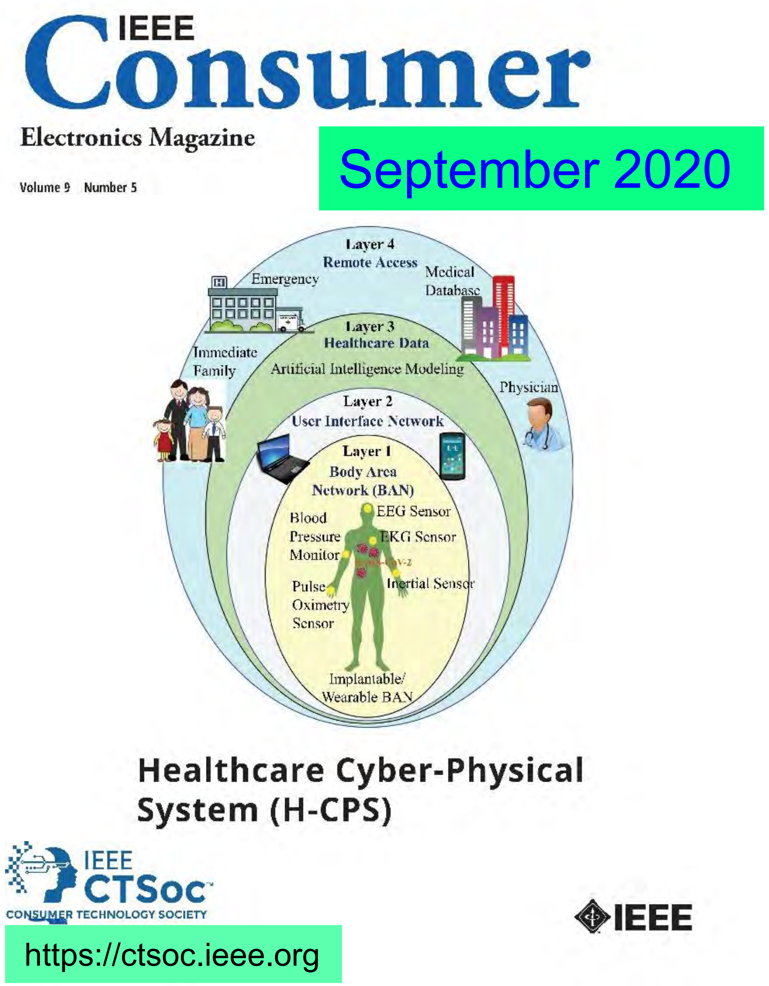
Privacy Challenge – Location

https://www.finjanmobile.com/mobile-location-services-privacy-and-security-issues/

Copyright - Media, Hardware, Software

Software Piracy

Smart Healthcare - Security 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

IoMT Security Issue is Real & Scary

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

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

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

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

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

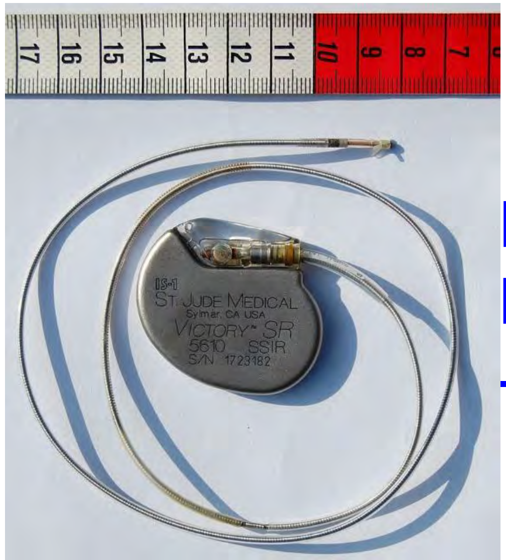
https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns

Implantable Medical Devices - Attacks

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

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

H-CPS Security Measures is Hard - Energy Constrained



Pacemaker Battery Life - 10 years

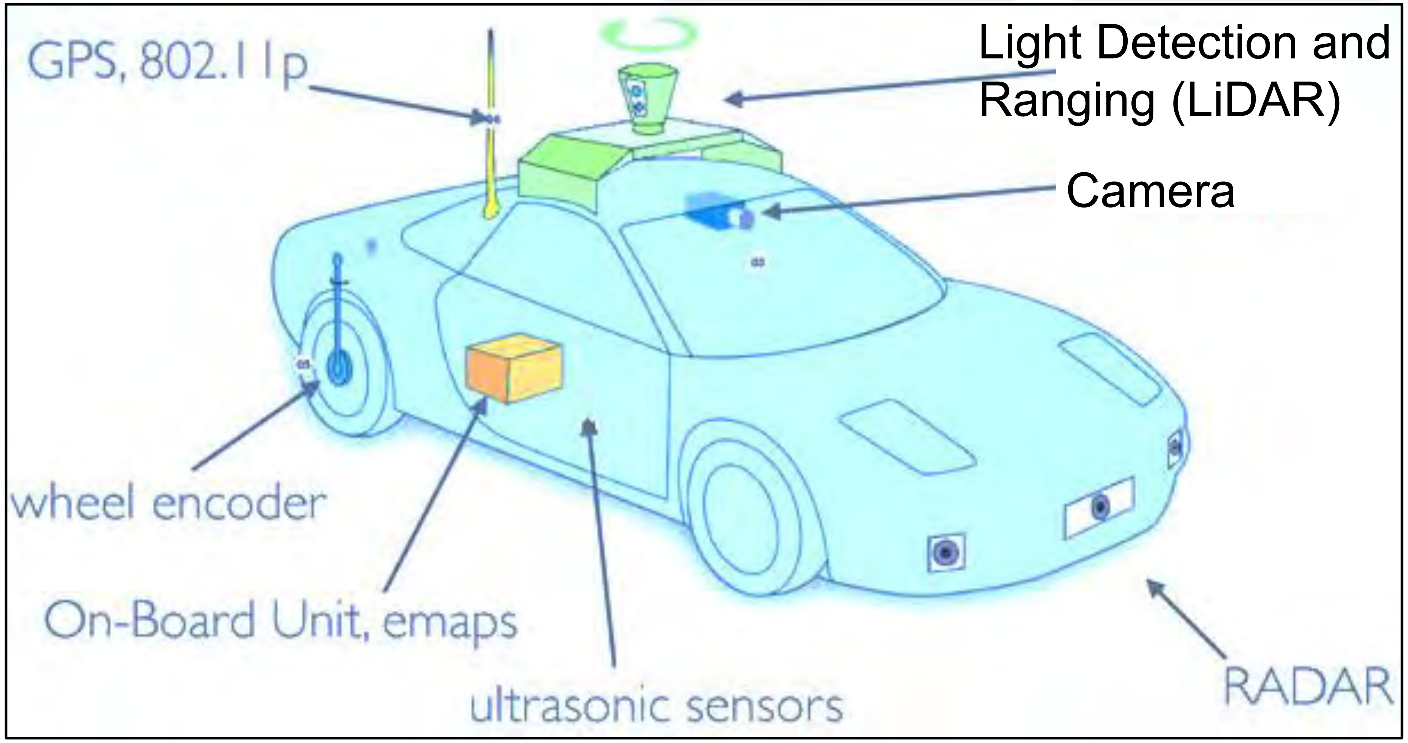
Neurostimulator Battery Life - 8 years

- 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

CE System Security – Smart Car

Selected Attacks on Autonomous Cars

- Replay
- Relay
- Jamming
- Spoofing
- Tracking



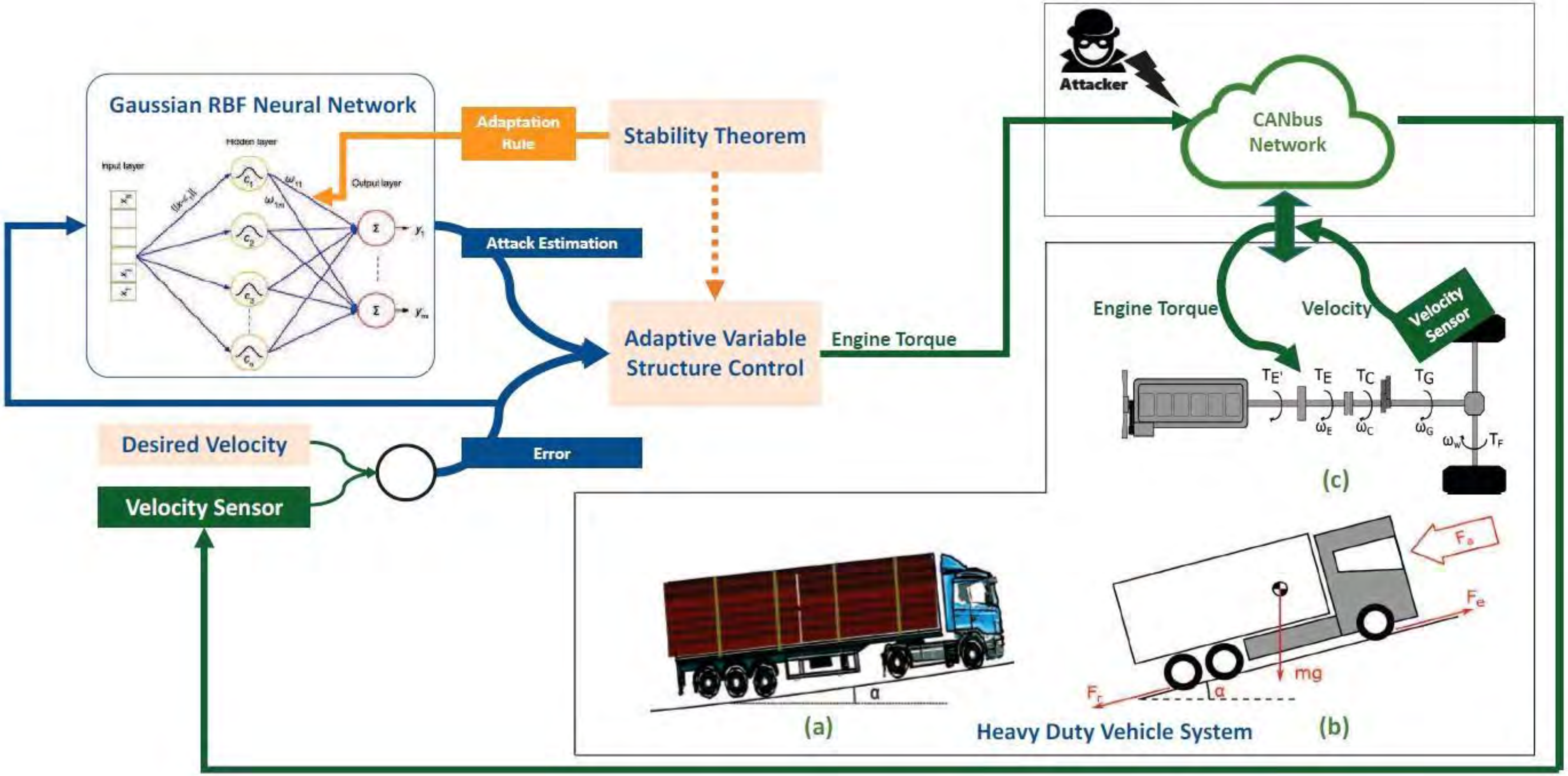
Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors
– Massive security issues.

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

Source: Petit 2015: IEEE-TITS Apr 2015

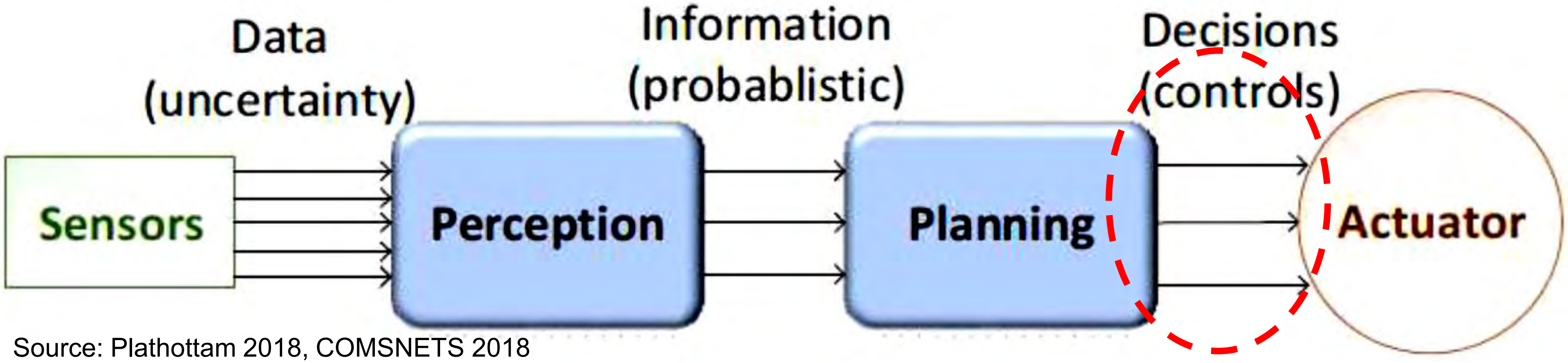
Source: https://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

Transportation CPS – Security Issue



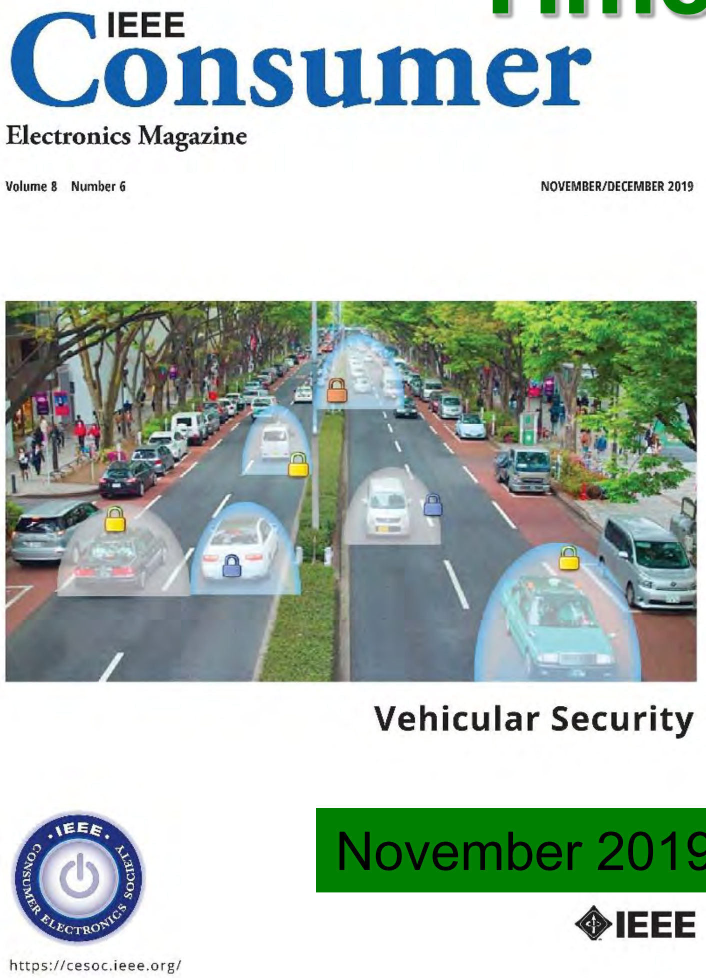
Smart Car – Modification of Input Signal of Control Can be Dangerous

- 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.

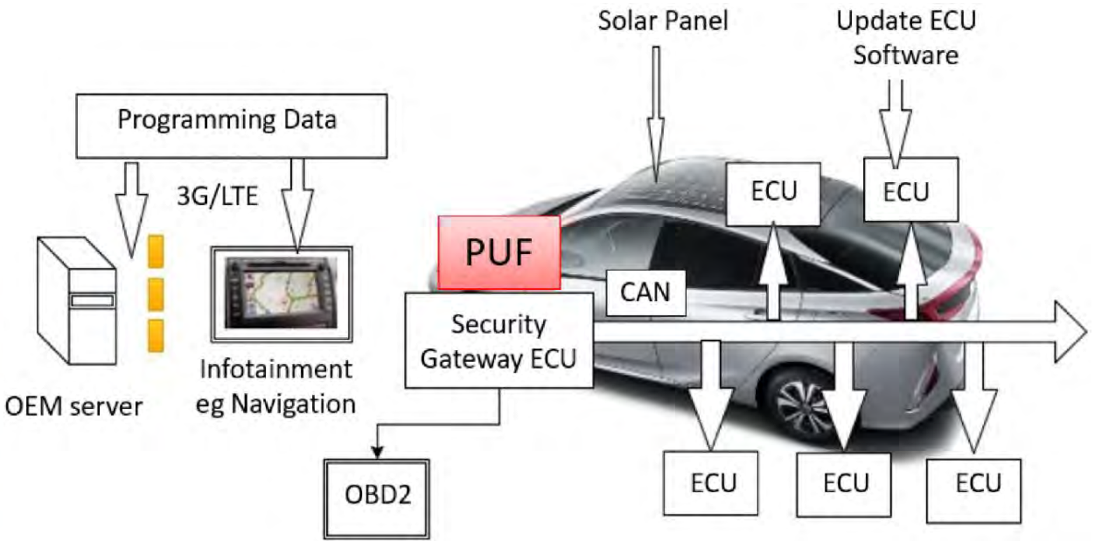


Source: Plathottam 2018, COMSNETS 2018

T-CPS Security is Hard – Time Constrained

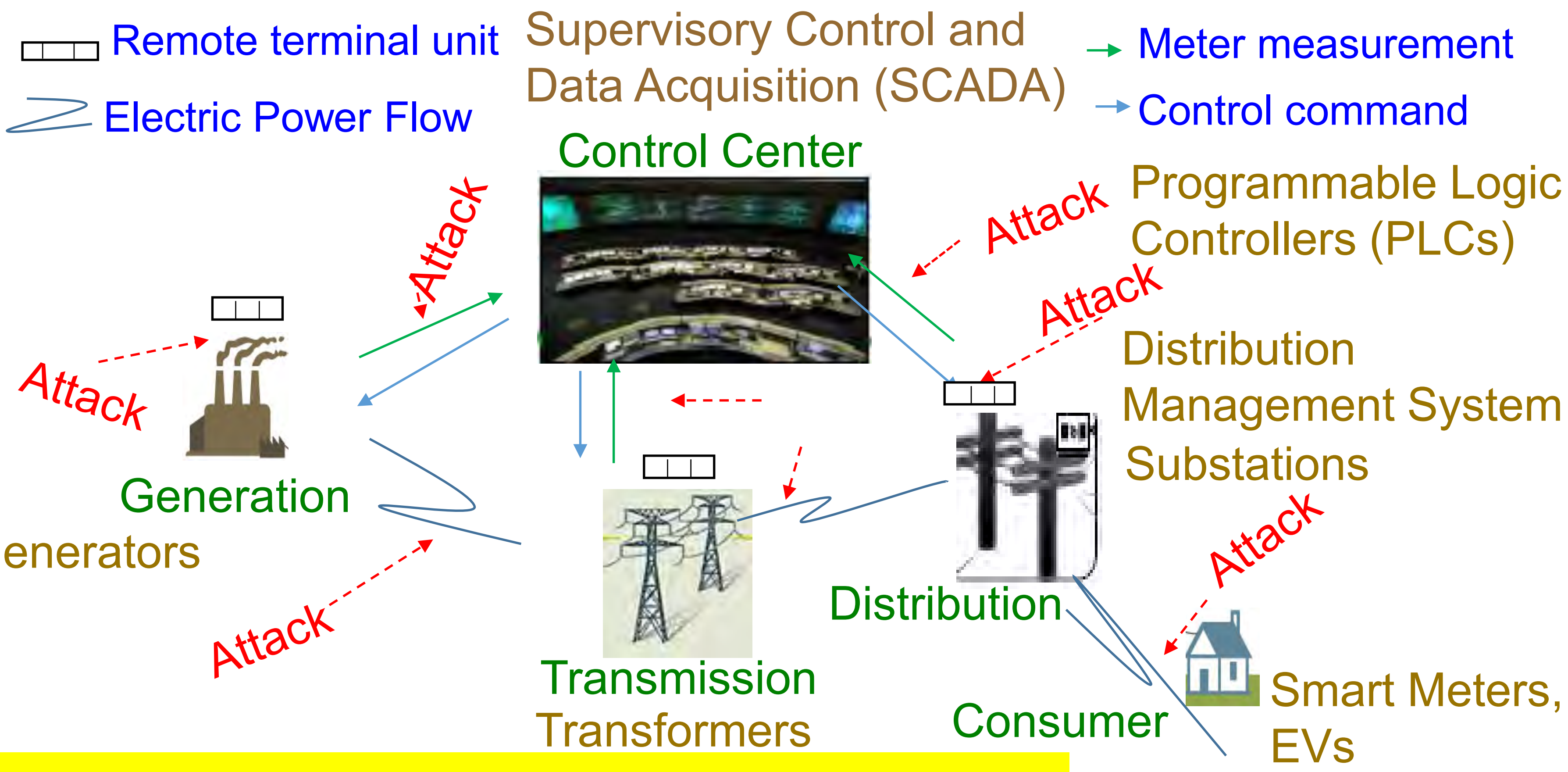


November 2019



Source: C. Labrado and H. Thapliyal, "Hardware Security Primitives for Vehicles," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 99-103, Nov. 2019.

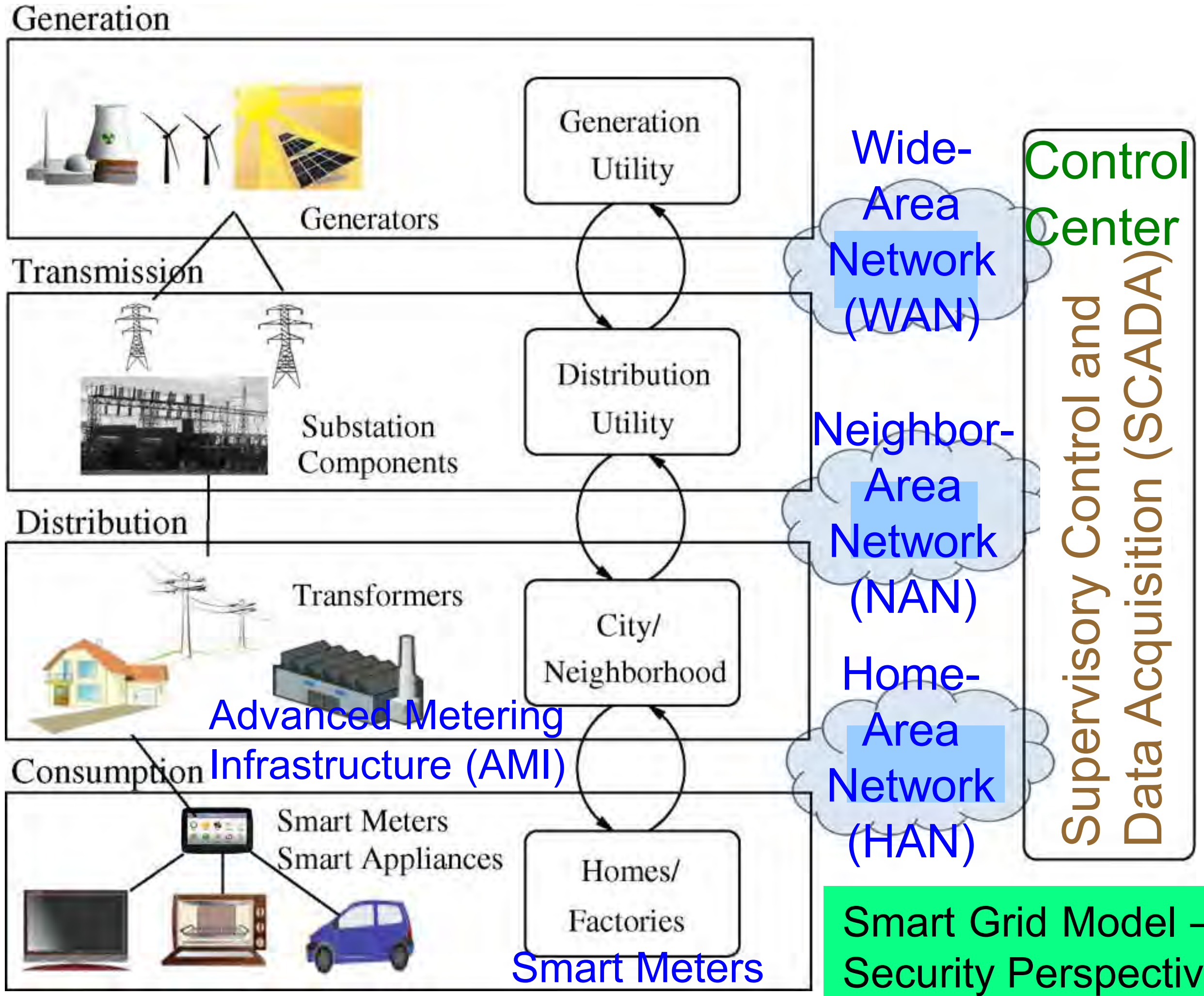
Smart Grid - Vulnerability



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 Grid - Vulnerability



Information and Communication Technology (ICT) components of smart grid is cyber vulnerable.

Data, Application/System Software, Firmware of Embedded System are the loop holes for security/privacy.

Network/Communication Components
Phasor Measurement Units (PMU)
Phasor Data Concentrators (PDC)
Energy Storage Systems (ESS)
Programmable Logic Controllers (PLCs)
Smart Meters

Smart Grid Model – CPS Security Perspective

Source: Y. Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure“, *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012.

Nonvolatile Memory Security and Protection

Source: http://datalocker.com

Nonvolatile / Harddrive Storage

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

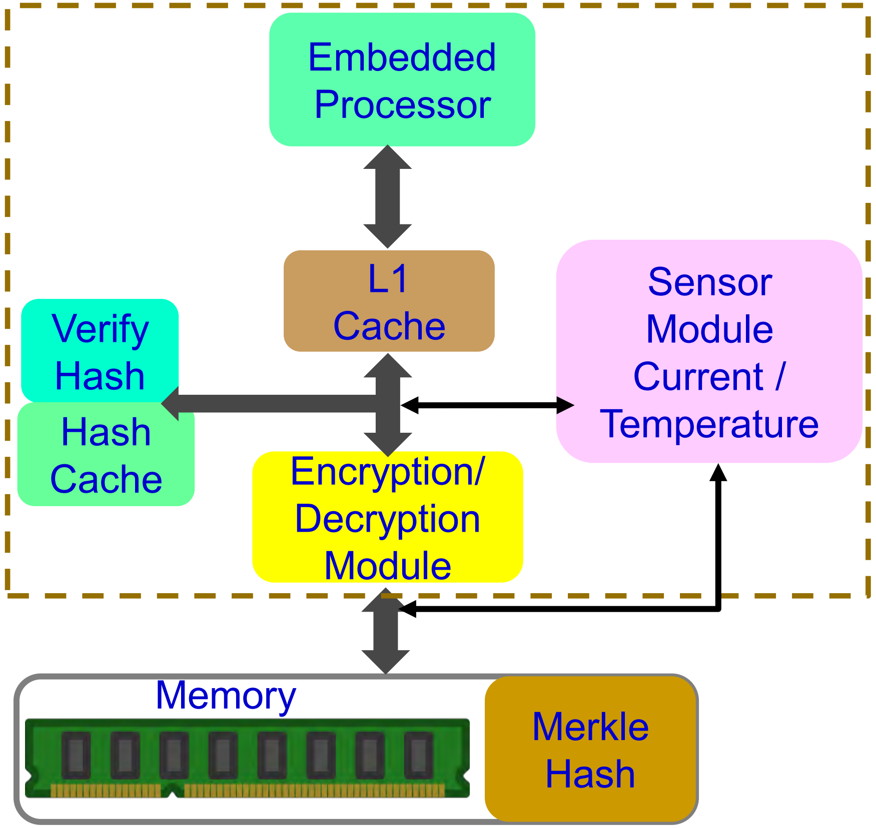
Software-based encryption to secure systems and partitions of hard drive.

Some performance penalty due to increase in latency!

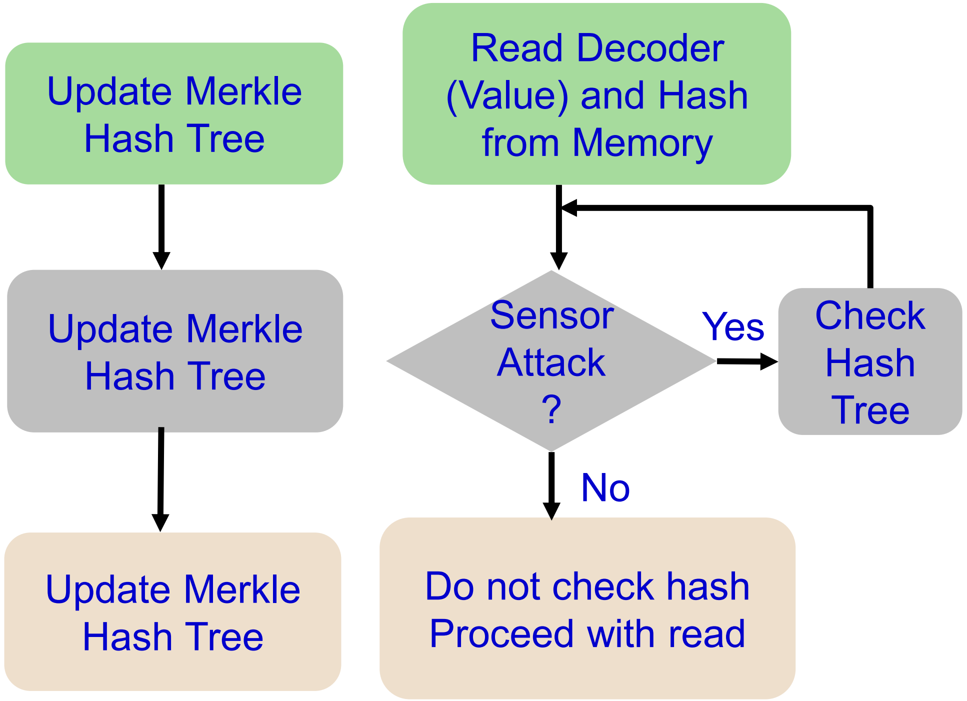
How Cloud storage changes this scenario?

Embedded Memory Security

Trusted On-Chip Boundary



On-Chip/On-Board Memory Protection



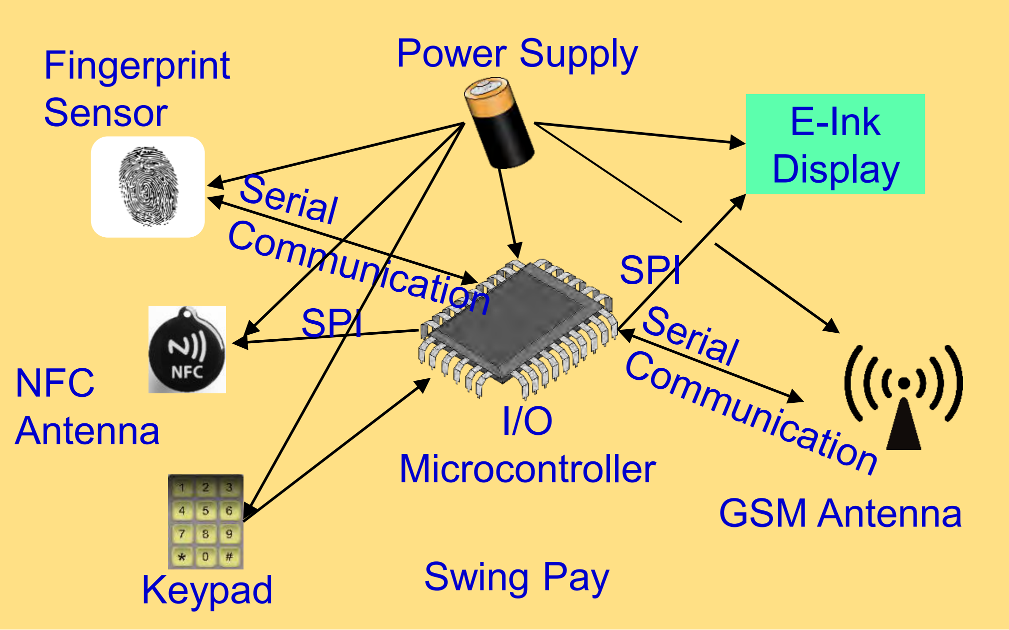
Write Operation

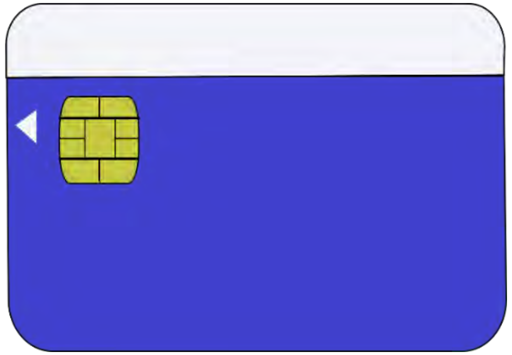
Read Operation

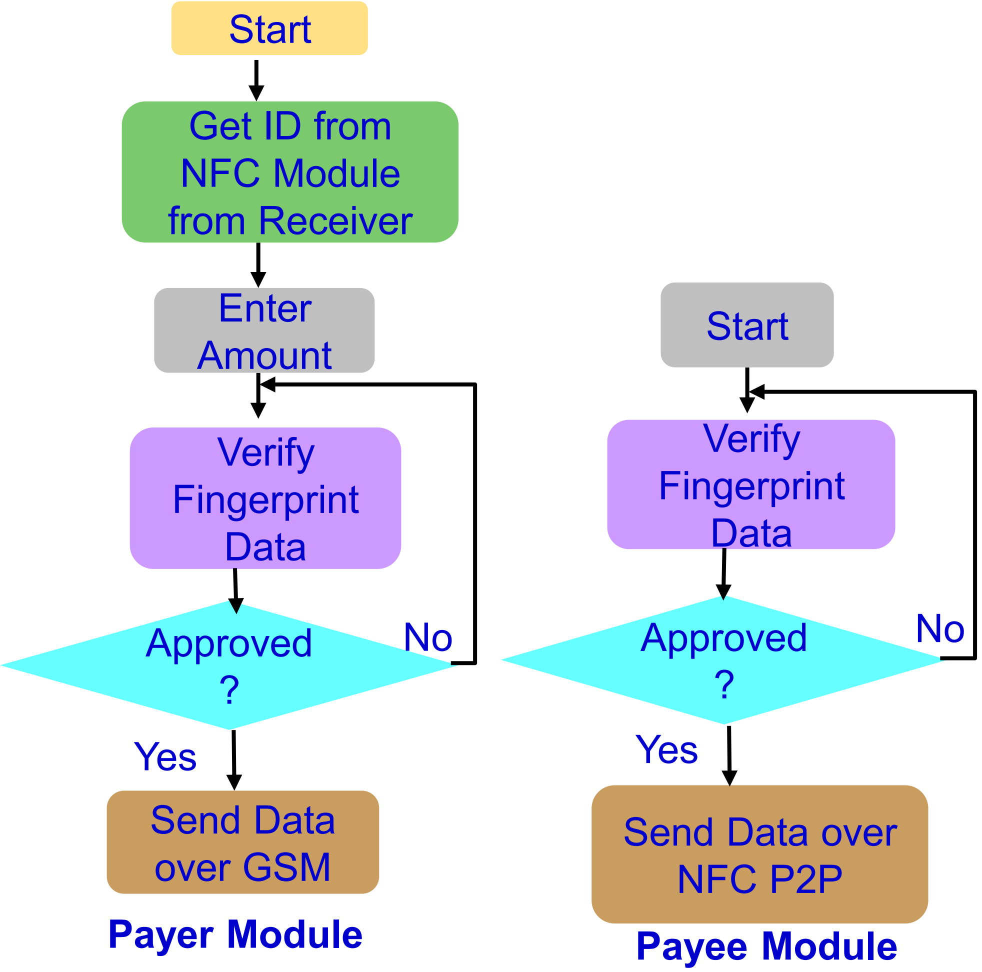
Memory integrity verification with 85% energy savings with minimal performance overhead.

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

Our Swing-Pay - NFC Cybersecurity Solution







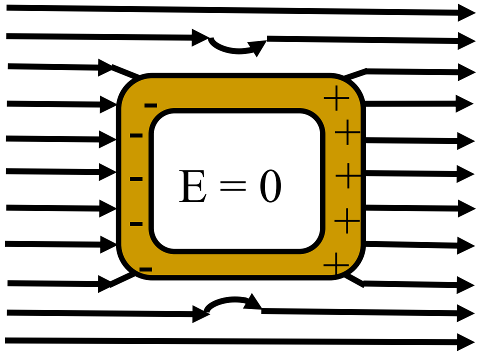
Source: S. Ghosh, J. Goswami, A. Majumder, A. Kumar, **S. P. Mohanty**, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs", *IEEE Consumer Electronics Magazine (MCE)*, Volume 6, Issue 1, January 2017, pp. 82--93.

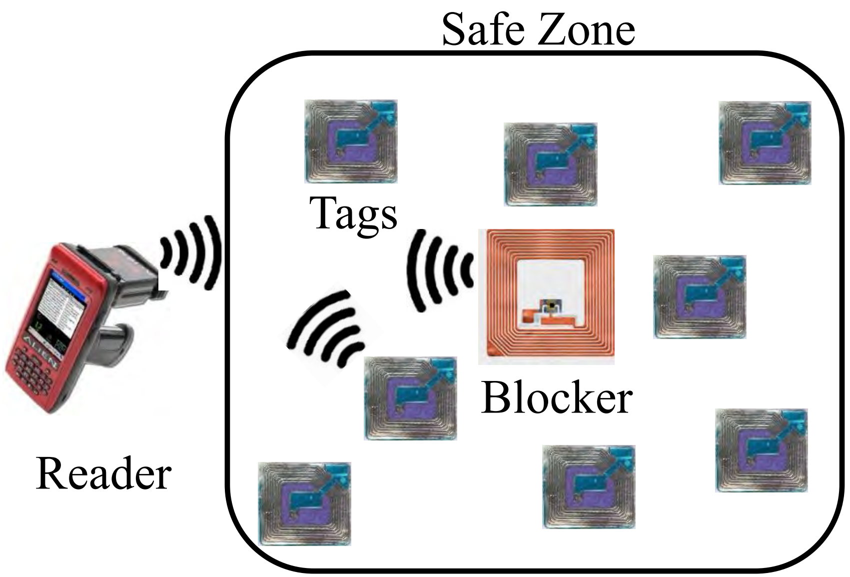
RFID Cybersecurity - Solutions

Selected RFID Security Methods

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

Faraday Cage

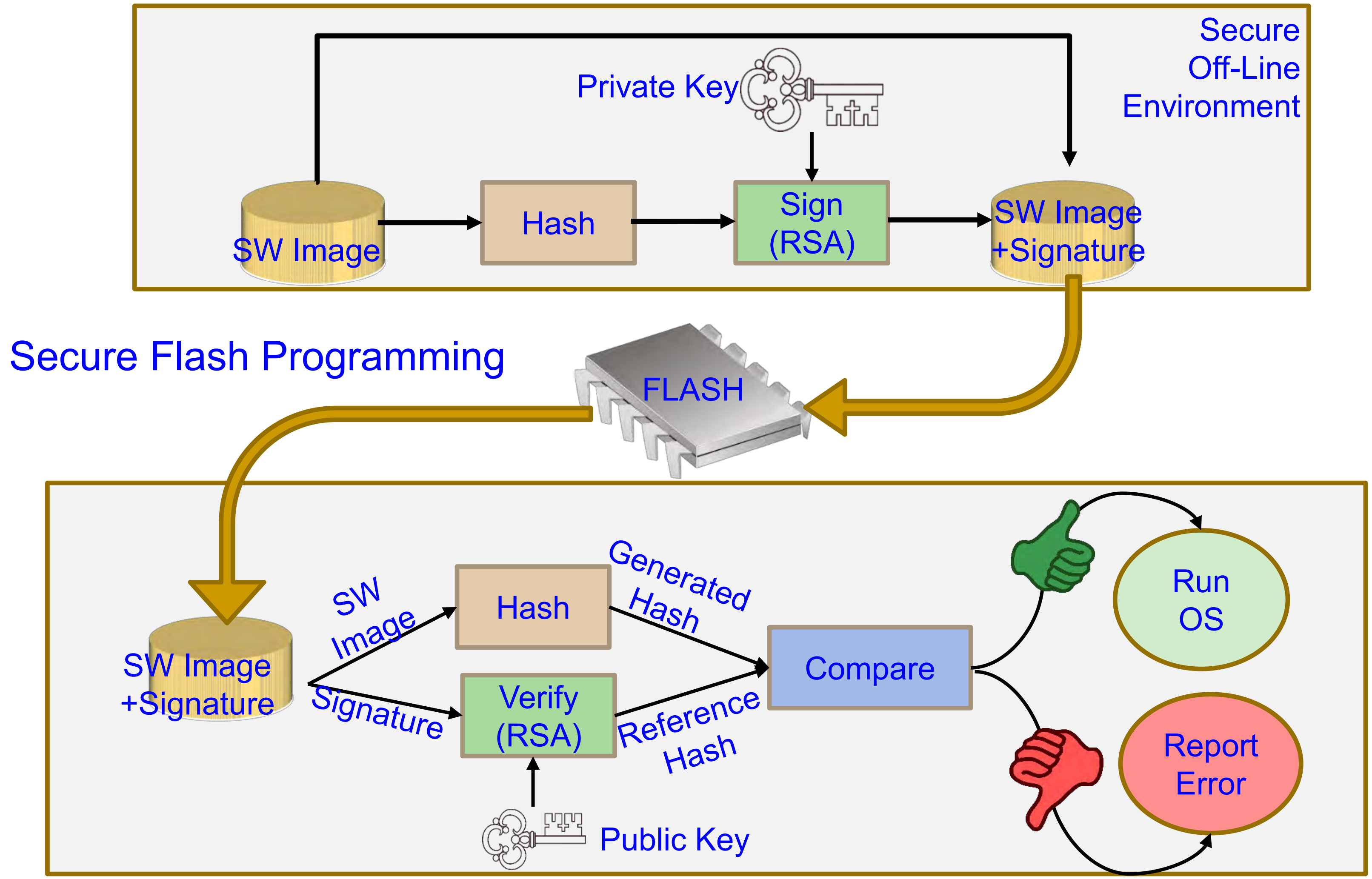




Blocker Tags

Source: Khattab 2017, Springer 2017 RFID Security

Firmware Cybersecurity - Solution



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

Smart Agriculture Cybersecurity

Smart Agriculture

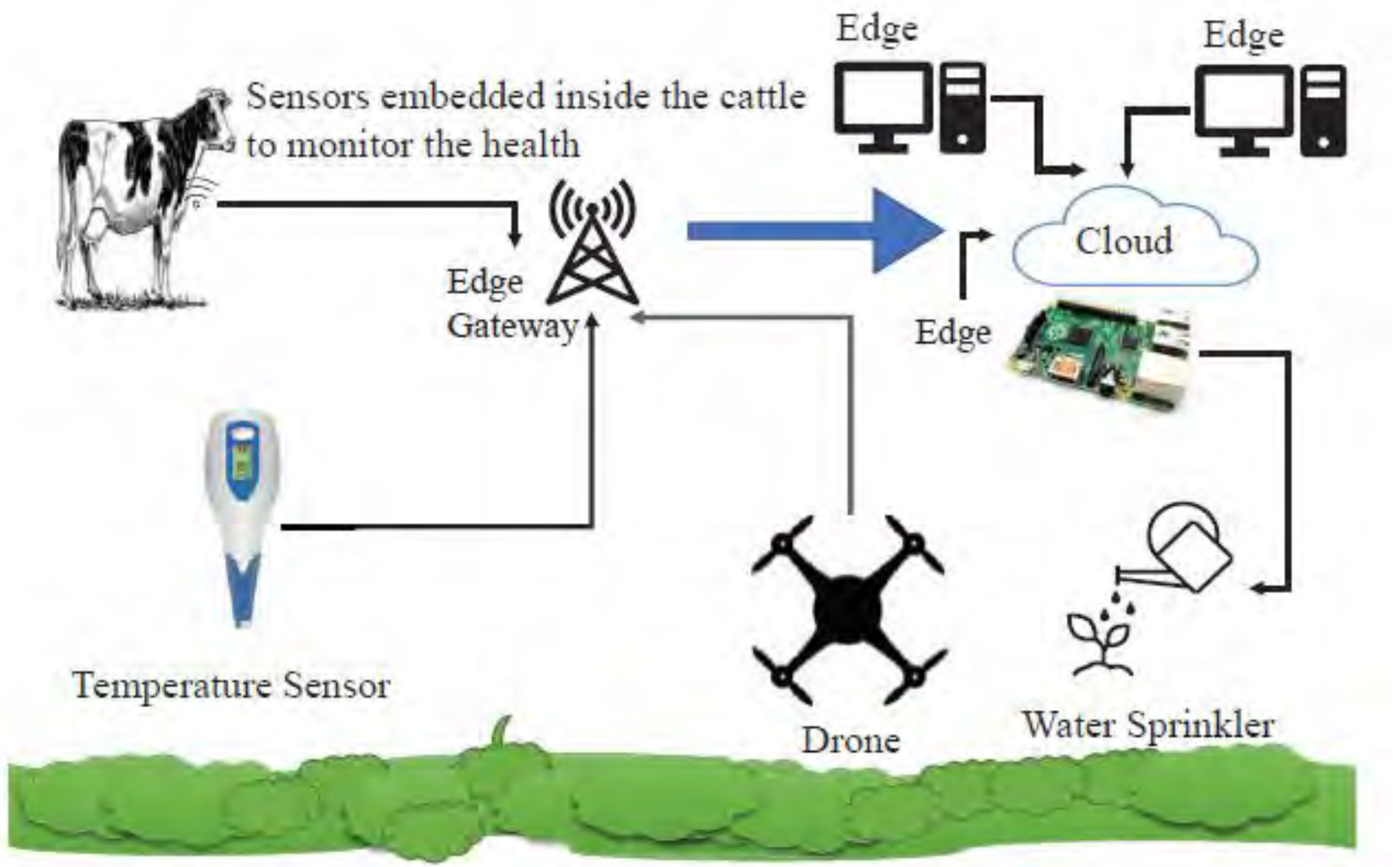
Smart Electronic Systems Laboratory (SESL)
UNT EST. 1890

IoT Applications in Agriculture

- Internet of Things in
  - Field Agriculture
  - Aquaculture
  - Poultry and Livestock Breeding
  - Greenhouse
  - Plant Factory
  - Photovoltaic Agriculture
  - Solar Insecticidal Lamps

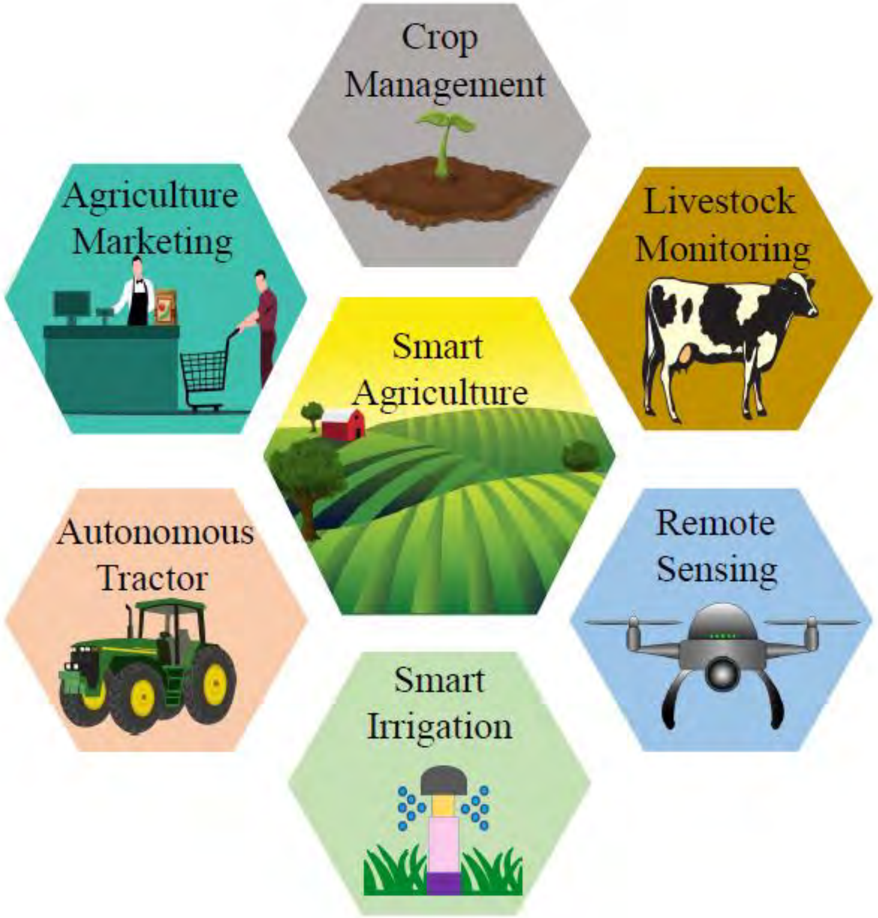
X. Yang *et al*., "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges," in *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273-302,

Internet-of-Agro-Things



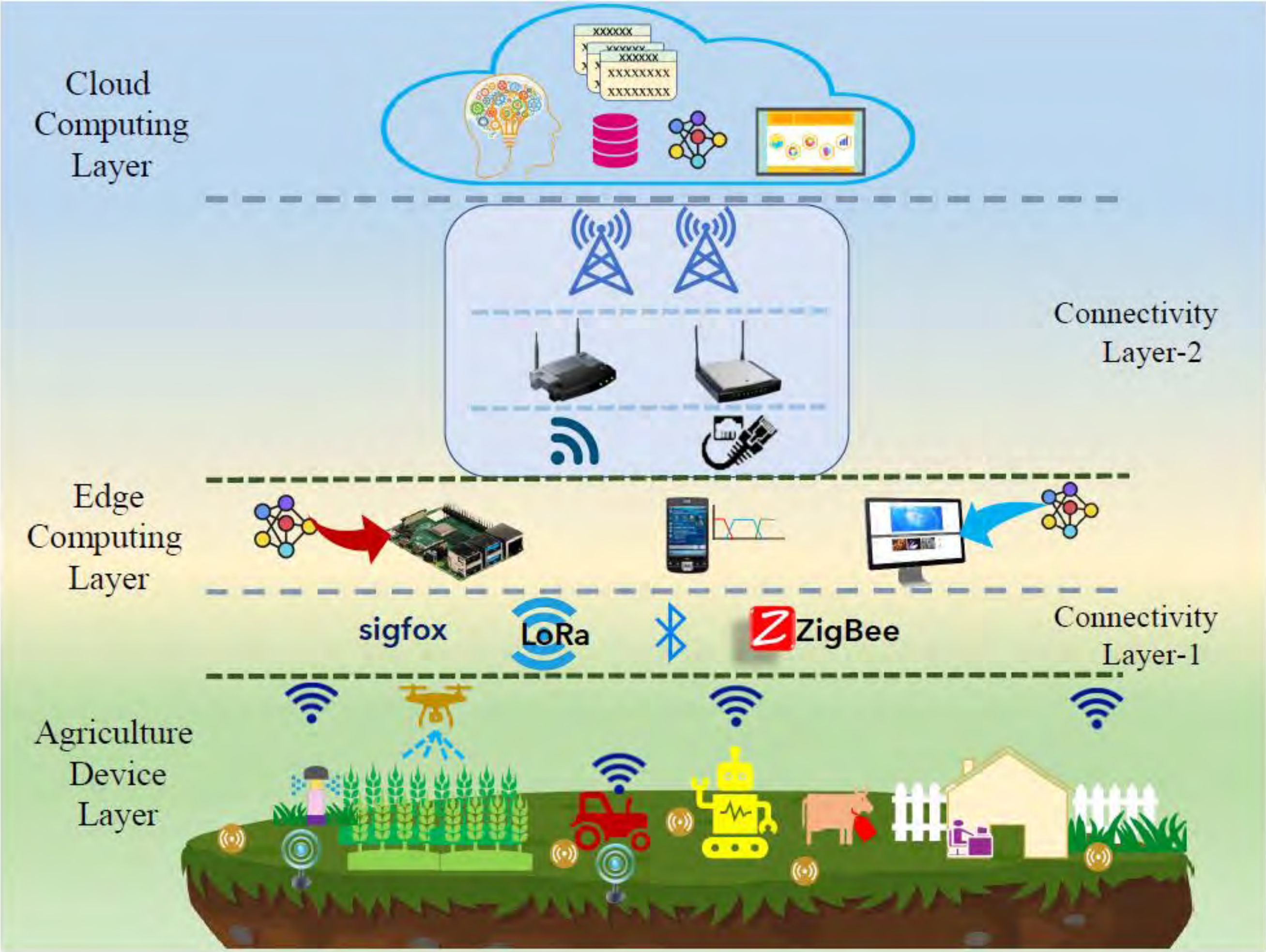
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, V. P. Yanambaka, B. K. Baniya, and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture", in *Proceedings of the OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375--380, DOI: https://doi.org/10.1109/OCIT53463.2021.00080.

IoT Applications in Agriculture



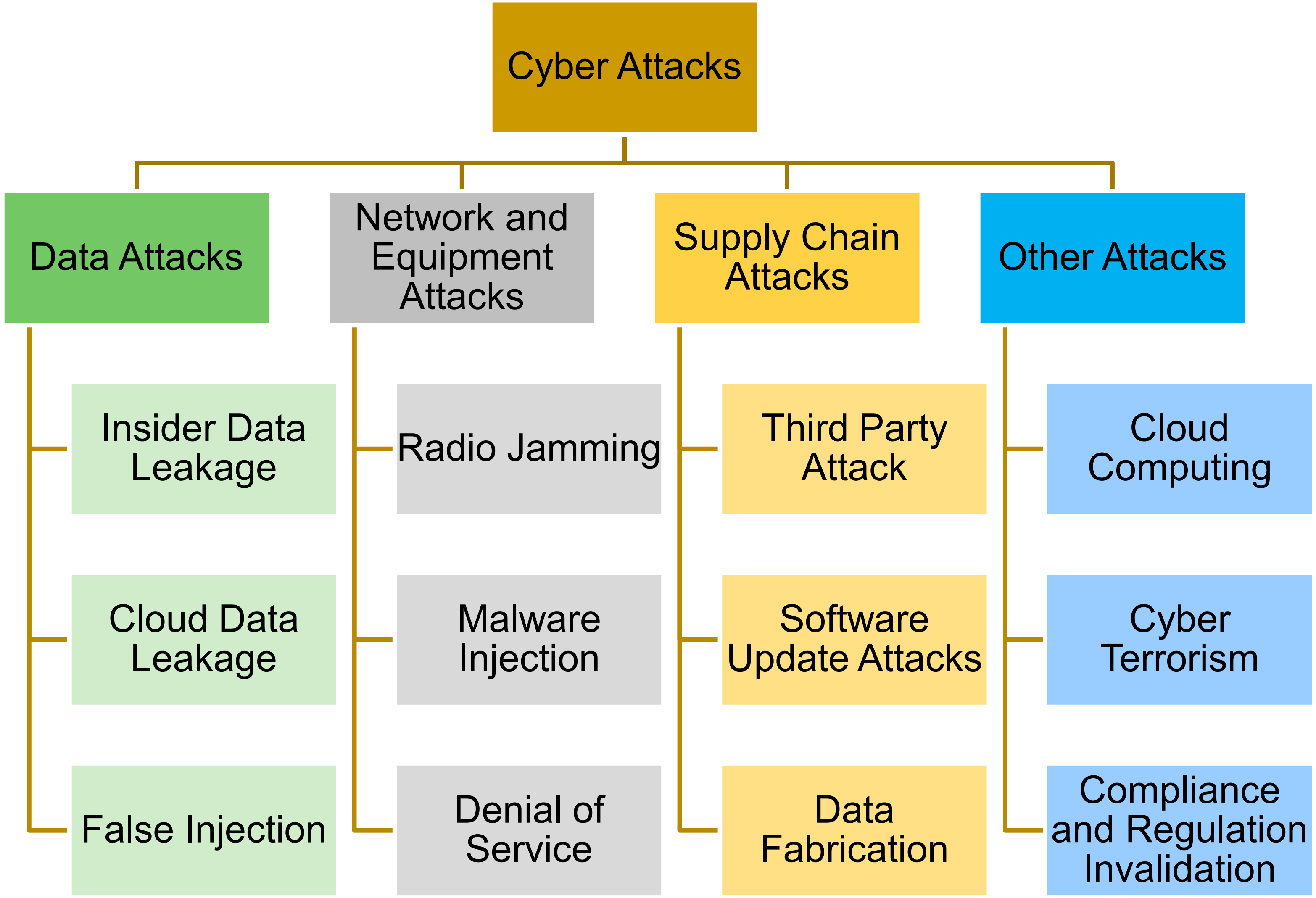
Source: A. Mitra, S. L. T. Vangipuram, A. K. Bapatla, V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, and C. Ray, "Everything You wanted to Know about Smart Agriculture", *arXiv Computer Science*, arXiv:2201.04754, Jan 2022, 45-pages.

Architecture of Smart Agriculture



Source: A. Mitra, S. L. T. Vangipuram, A. K. Bapatla, V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, and C. Ray, "Everything You wanted to Know about Smart Agriculture", *arXiv Computer Science*, arXiv:2201.04754, Jan 2022, 45-pages.

Security Challenges



Source: M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584

Challenges in Smart Agriculture

- Access Control
  - Develop farm specific access control mechanisms.
  - Develop data sharing and ownership policies.
- Trust
  - Prevent insider data leakage.
  - Zero day attack detection.
- Information Sharing
- Machine Learning and Artificial Intelligence Attacks
- Next Generation Network Security implementation
- Trustworthy Supply chain and Compliance

Source: M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584

Security Threats in Smart Agriculture

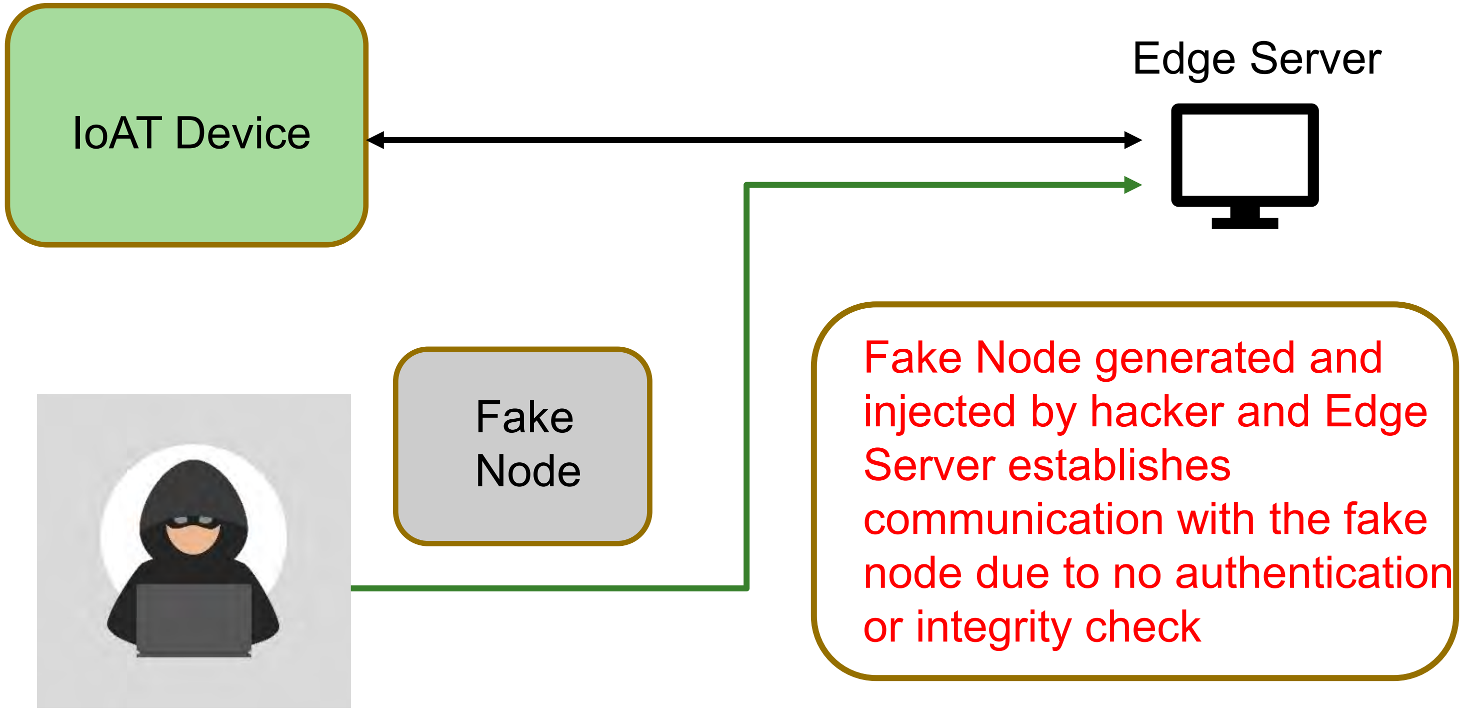
- Harsh Environment
- Threats from equipment
  - High voltage pulses
  - Interference
- Unauthorized access
- Interception of node communication
- Malicious data attacks
- Control system intrusion

X. Yang *et al*., "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273-302,

Security Threats – Some Solutions

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

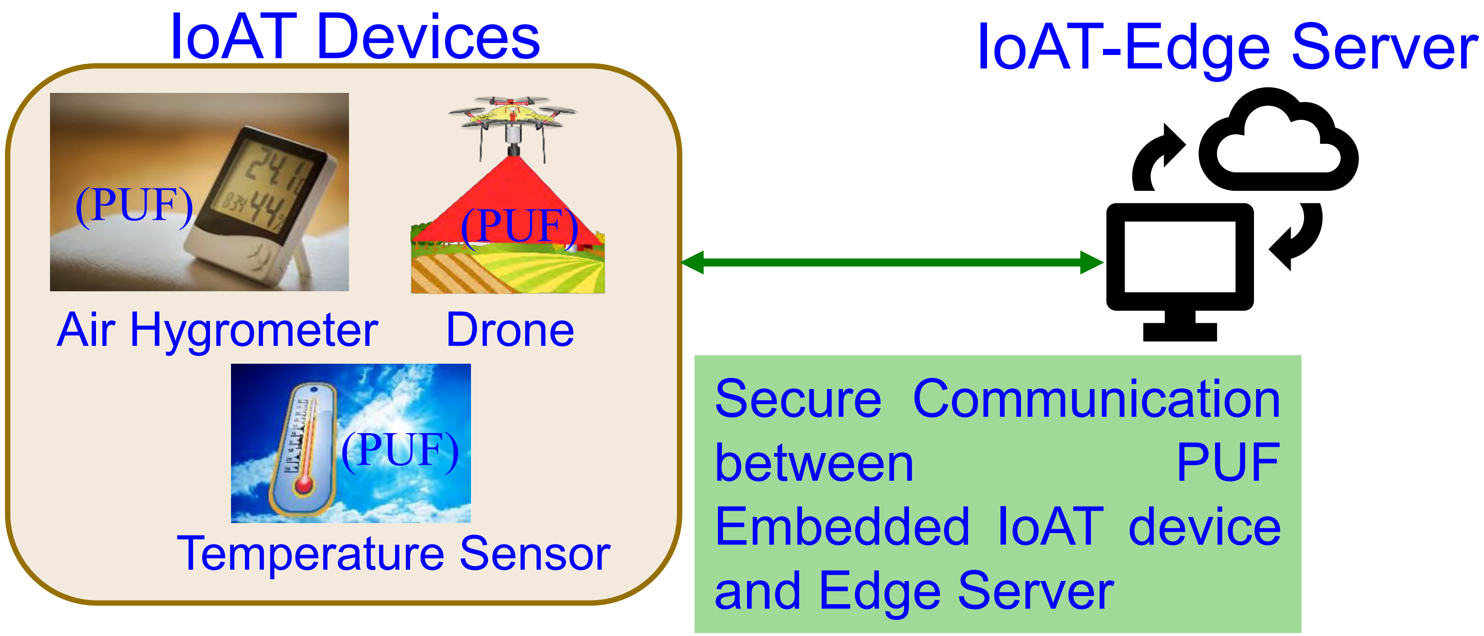
Our Secure Design Approach for Robust IoAT - Threat Model



Malicious Node Generation and replacement

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

Our Security-by-Design Approach for Robust IoAT



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

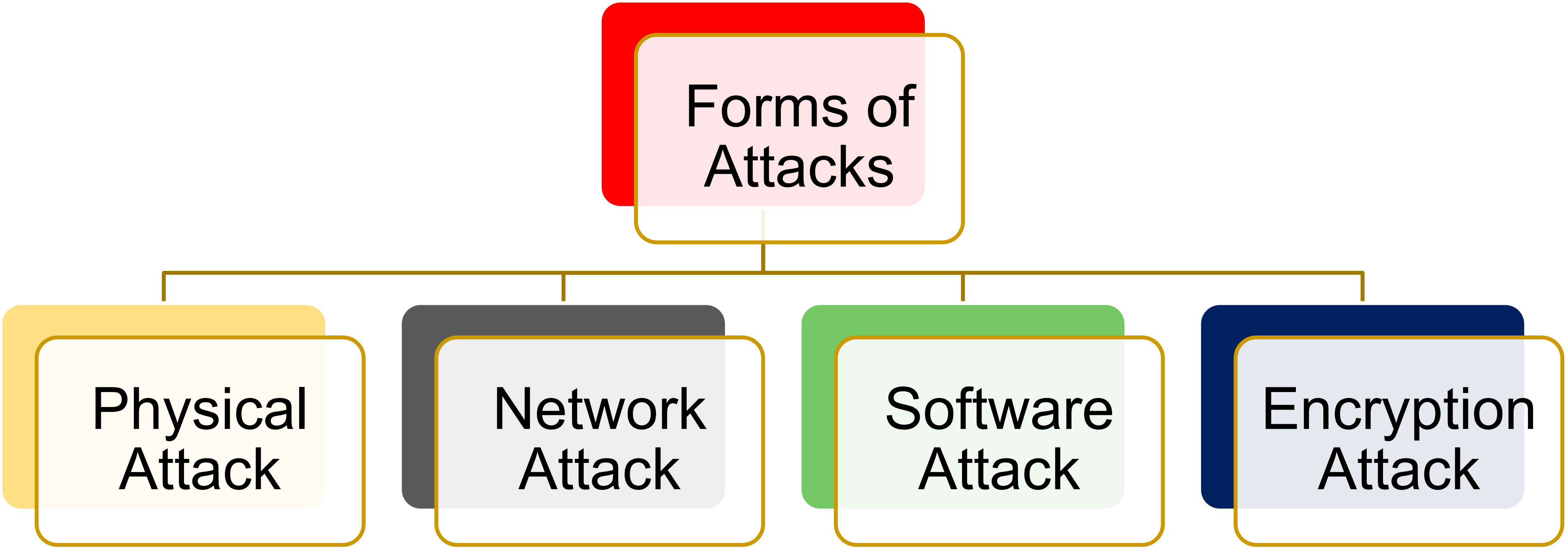
Source: V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. P. Yanambaka, B. K. Baniya and B. Rout, "A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture,“ in *Proc. 19th OITS International Conference on Information Technology (OCIT)*, 2021, pp. 375-380, doi: 10.1109/OCIT53463.2021.00080.

Smart Healthcare Cybersecurity

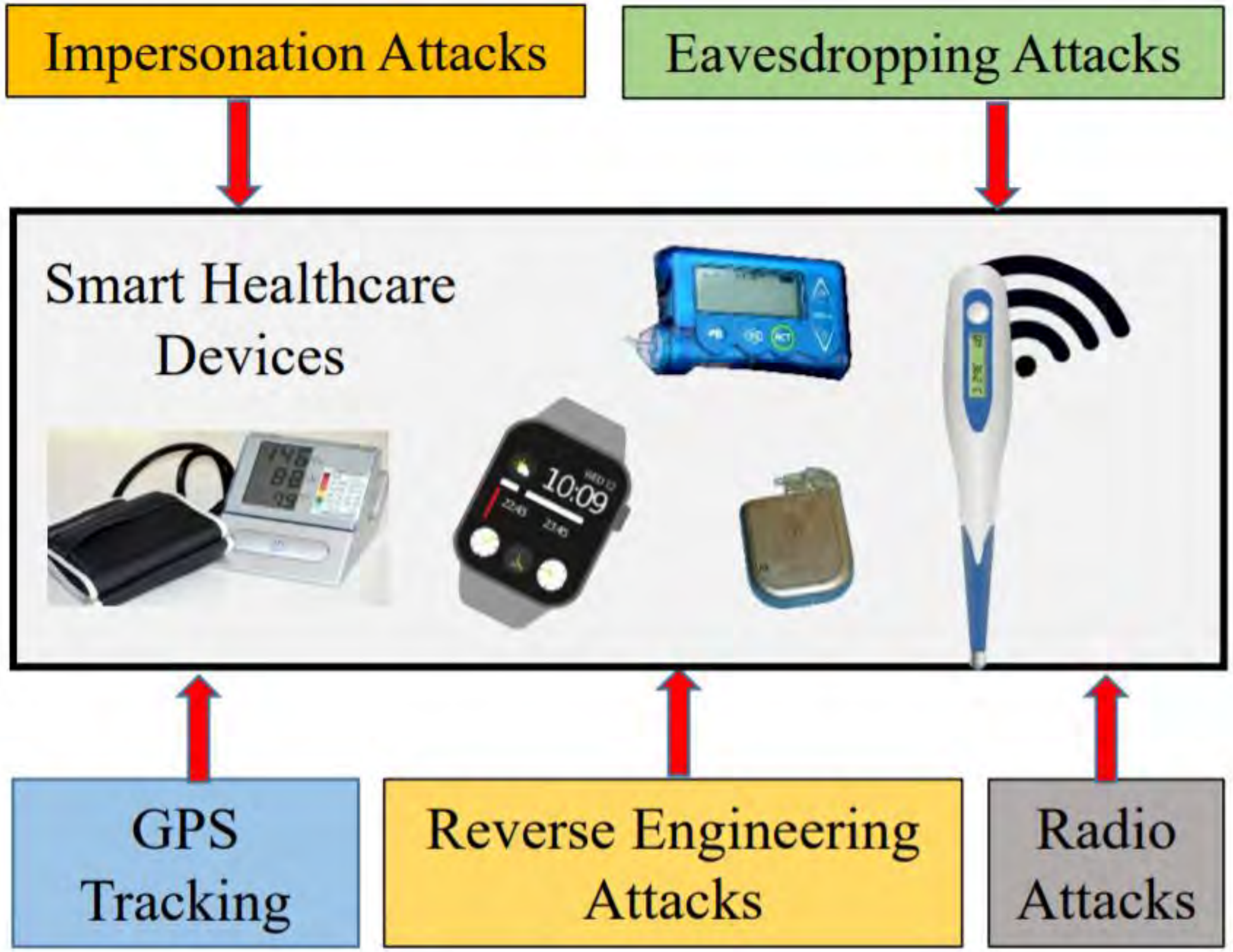
Smart Healthcare

- We have many devices such as wearables to track health.
- Examples
  - Wearable devices such as smart watch, smart glasses, etc.,
  - Implantable devices such as pacemaker, insulin pump, etc.,
- Constantly track data to stay healthy.
- Data is transmitted to the cloud for storage or tracking.
- Doctors can access the data for further diagnosis or prescription.

Various Forms of Attacks on Smart Healthcare

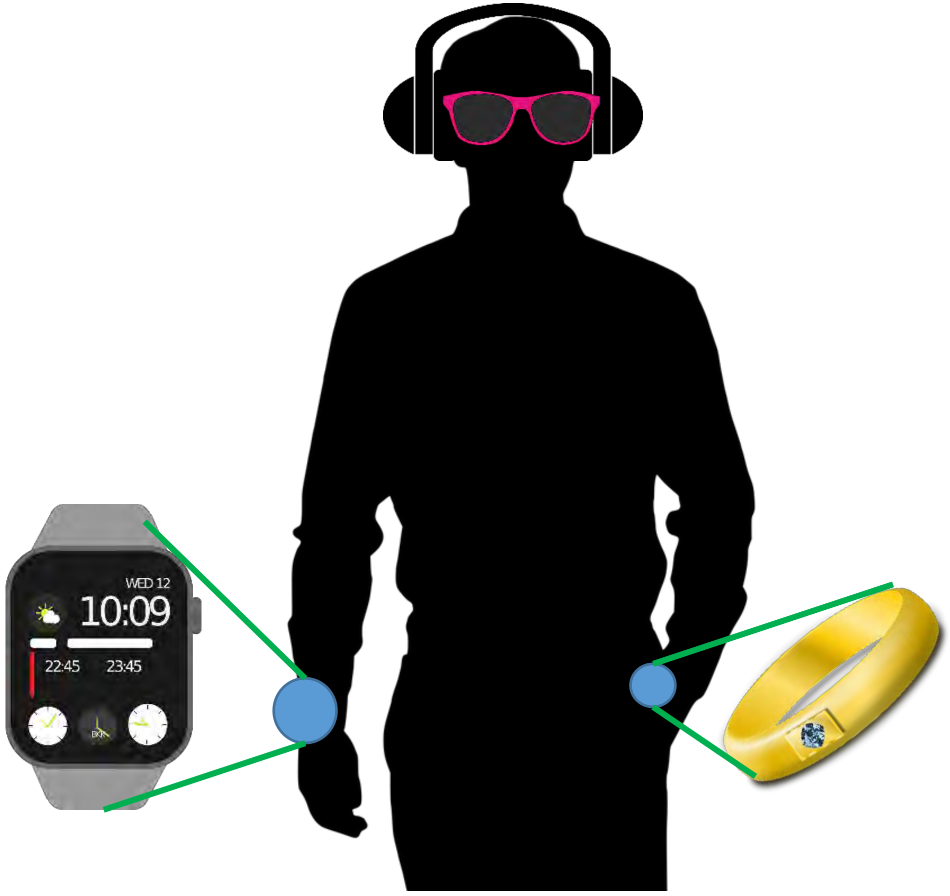


Smart Healthcare Security Threats



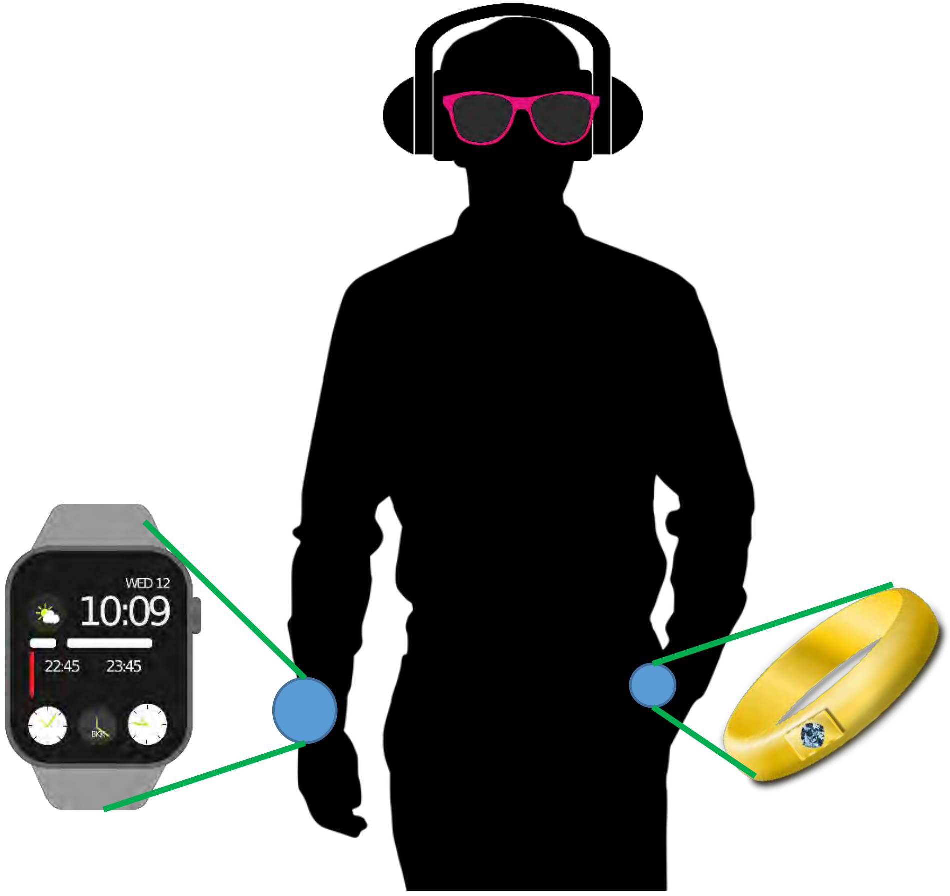
Various Attacks using or on Wearable Devices

- Compromise the privacy of bystanders.
- Compromise privacy and/or security of wearers.
- Unfettered access.
- Input interference.
- Side channel attacks.
- Hidden plagiarism.

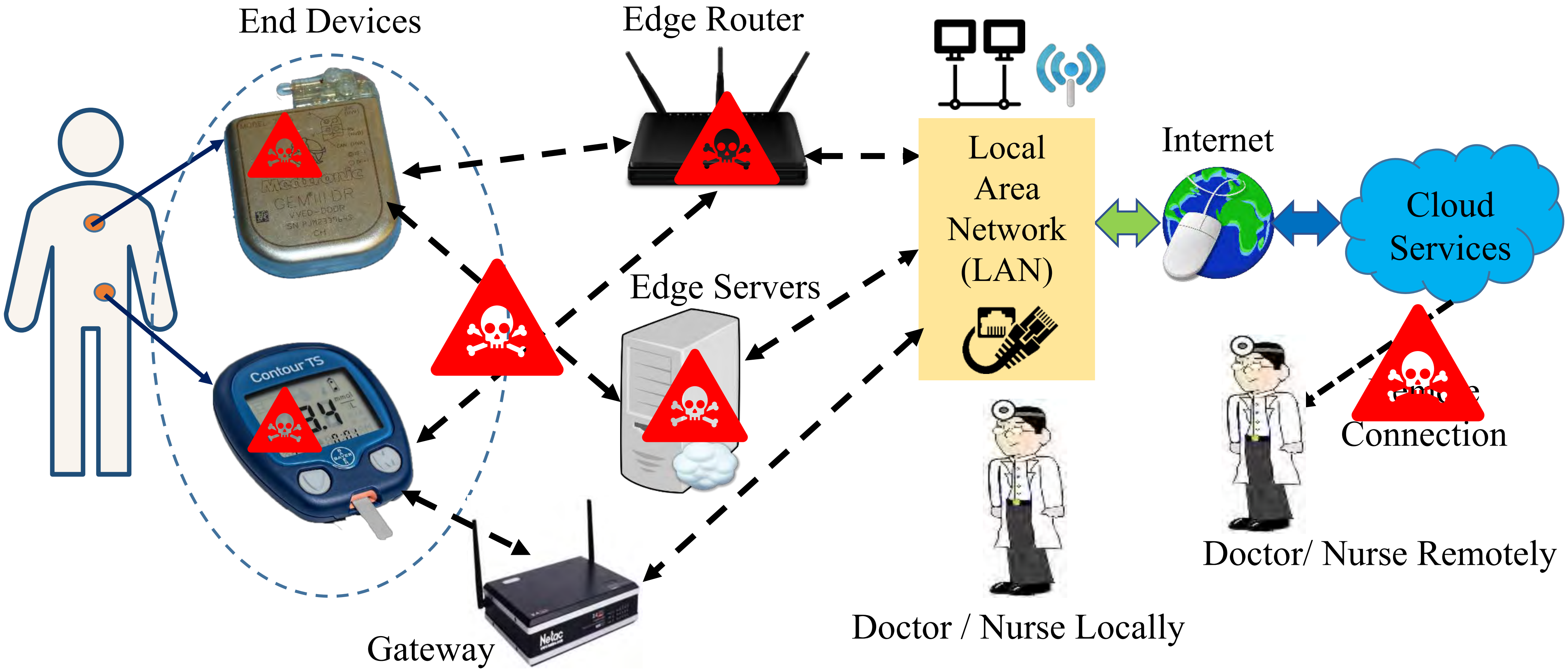


Various Attacks using Smart Watch

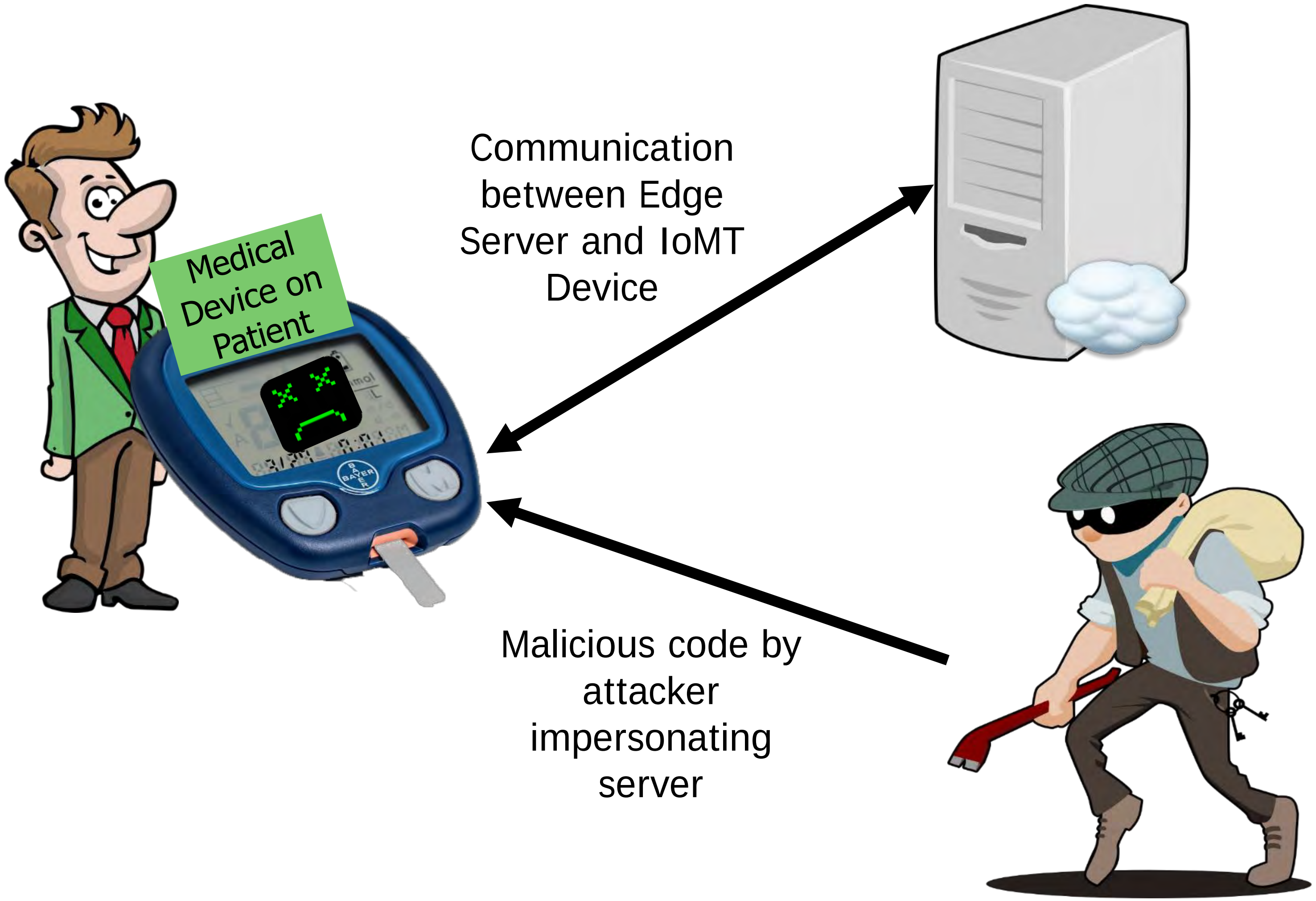
- Accelerometer, gyroscope can be used to analyze what a user is typing on the keyboard.
- Z-axis data from smart watch can be analyzed.
- Linear acceleration can be used to detect motion on a smart phone keyboard.



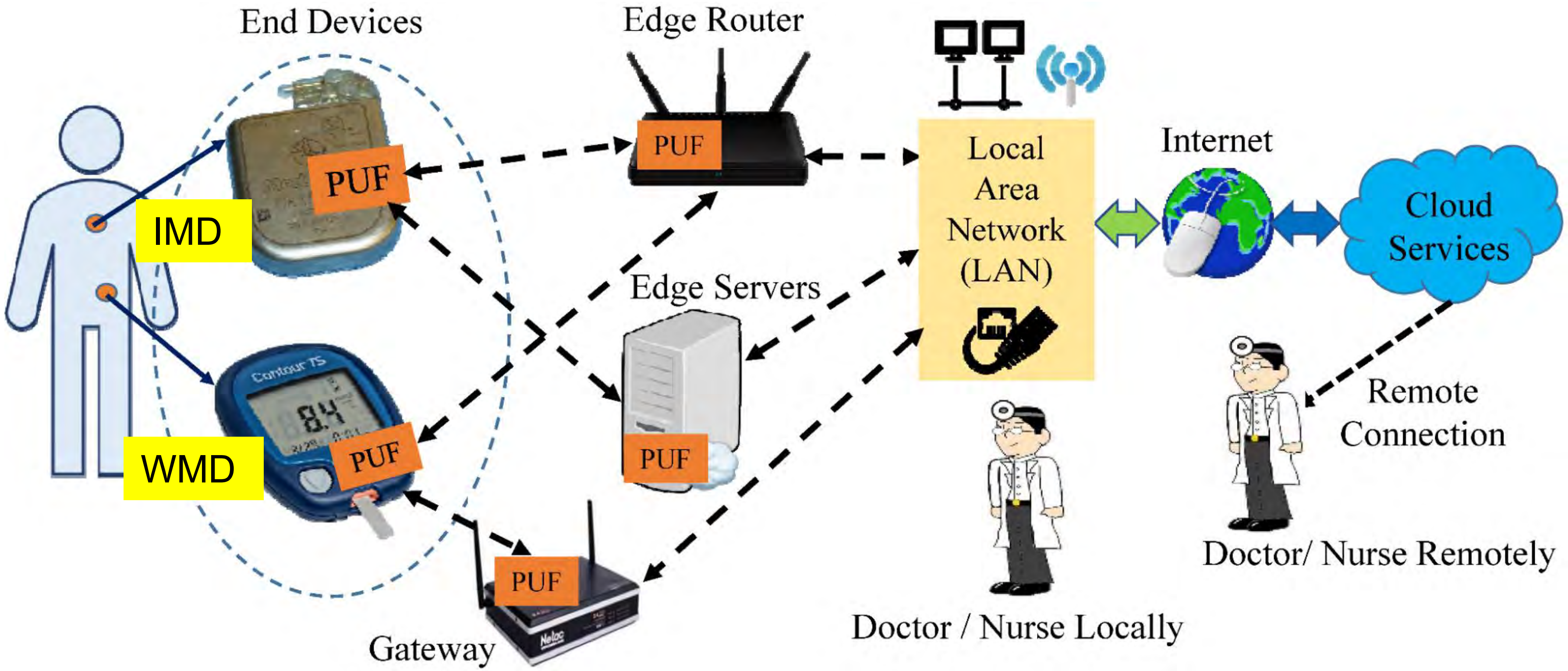
Possible Vulnerable Areas in a Typical Smart Healthcare System



Our PMsec: PUF Based Authentication

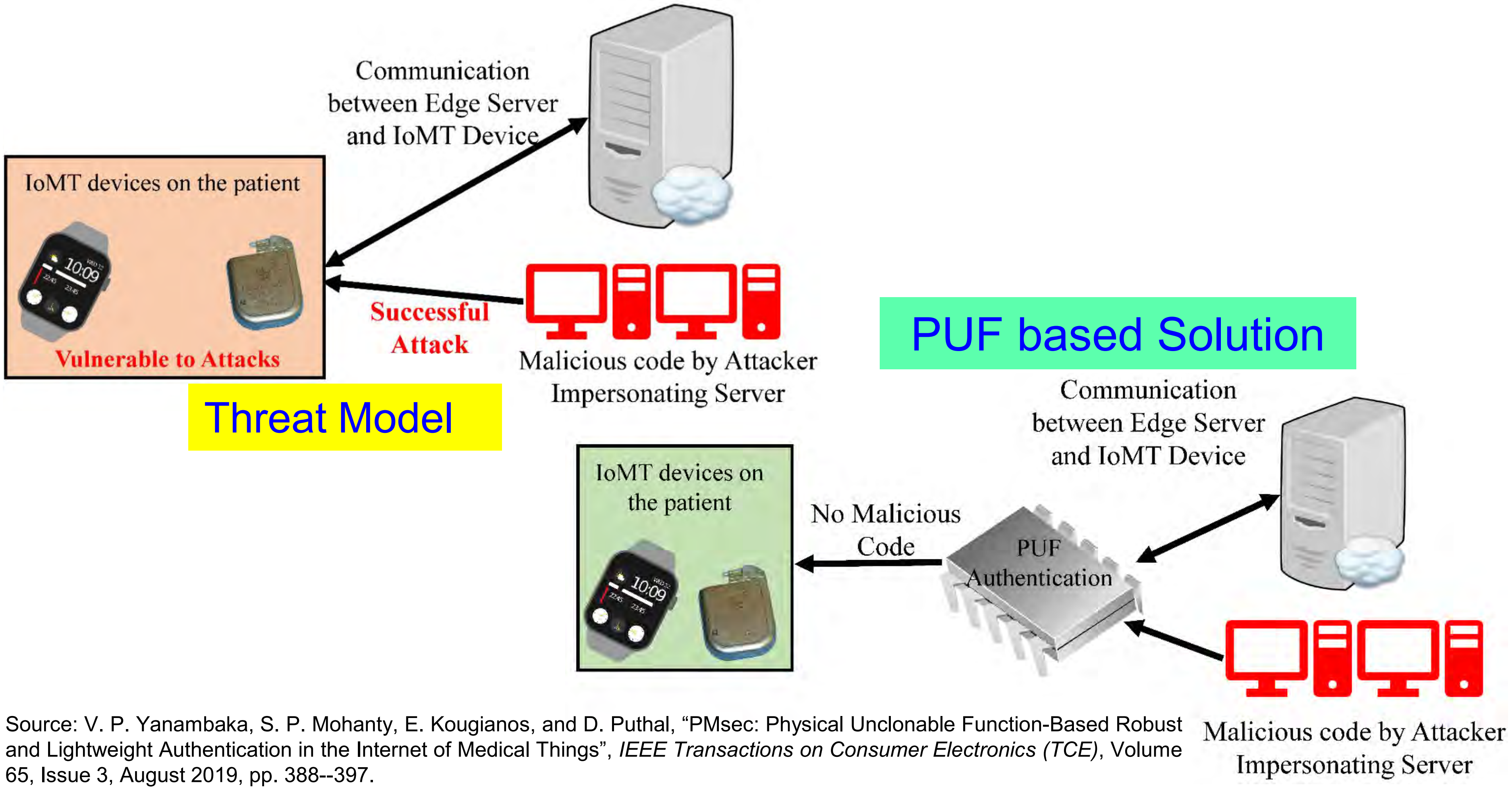


Secure Design Approach for Robust Security in Healthcare CPS



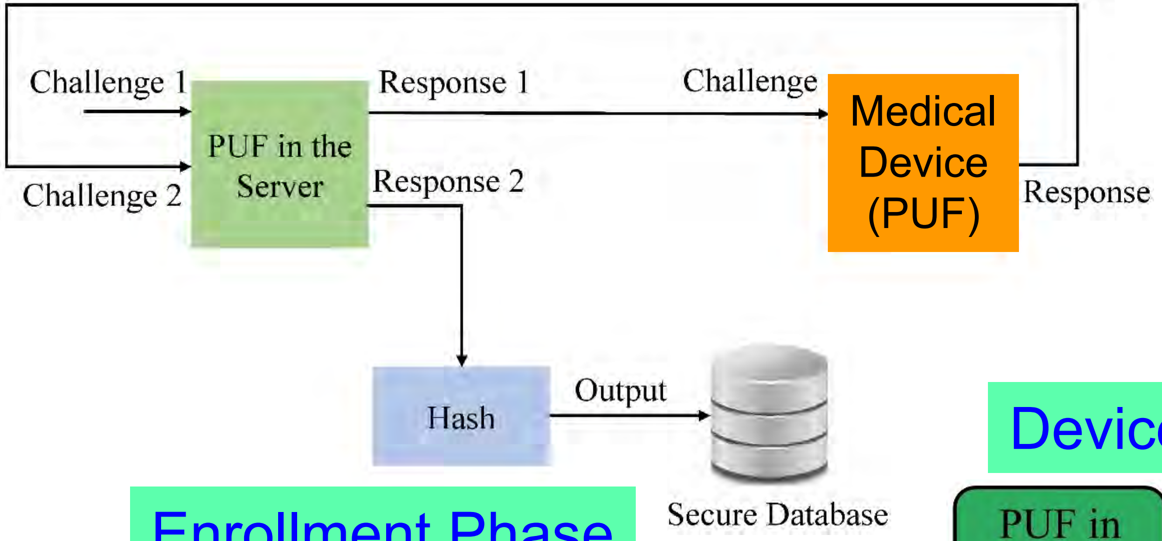
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things”, *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Secure Design Approach for Robust Security in Healthcare CPS



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

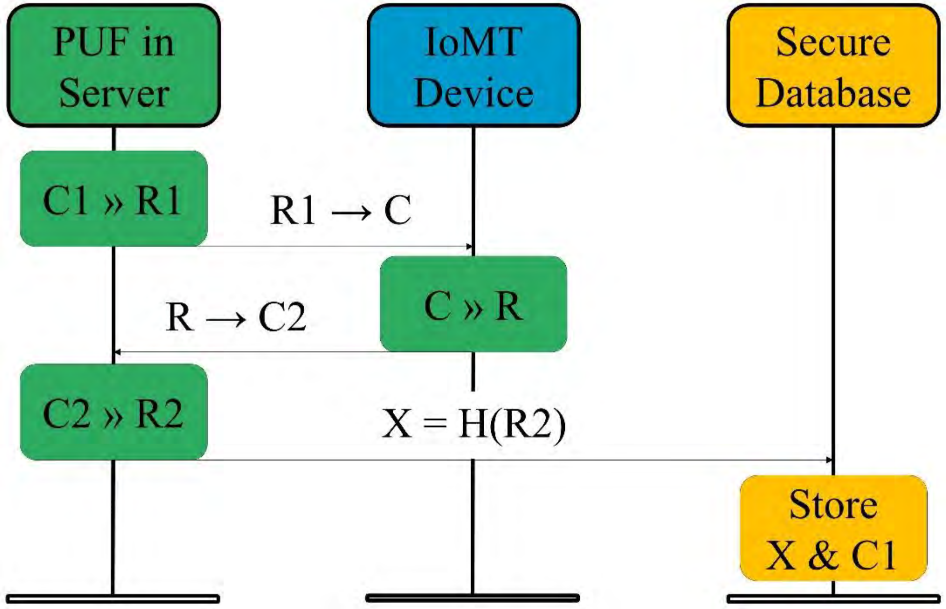
Proposed PMsec



Enrollment Phase

At the Doctor
- as a new Device comes for an User

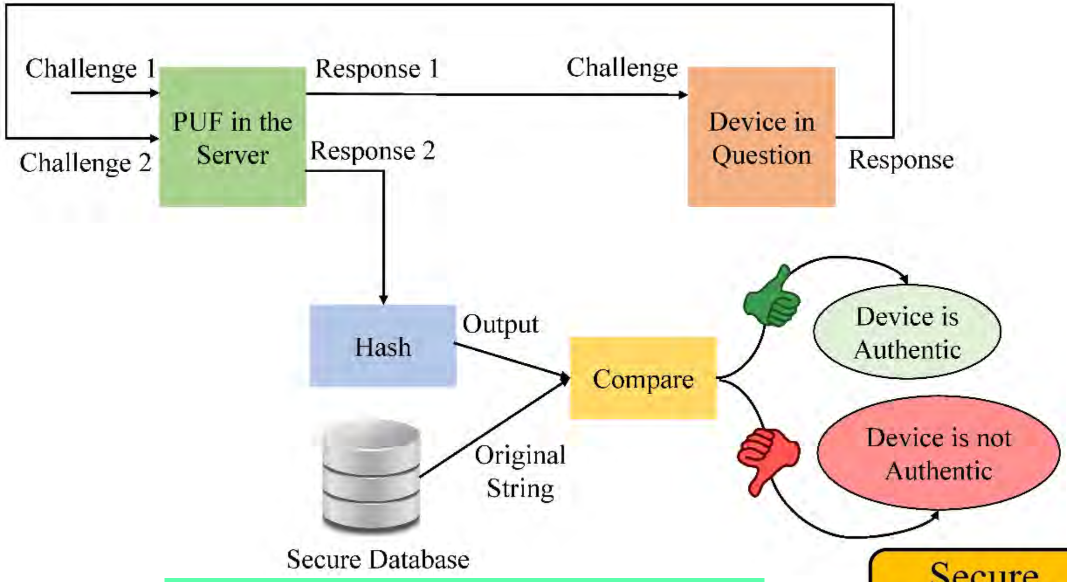
Device Registration Procedure



PUF Security Full Proof:
- Only server PUF Challenges are stored, not Responses
- Impossible to generate Responses without PUF

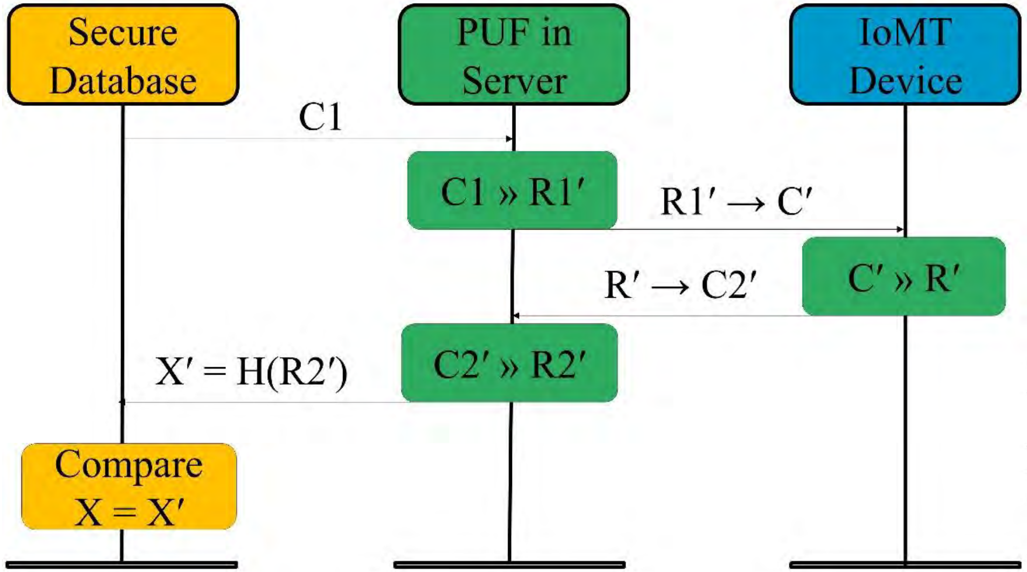
Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

Proposed PMsec



Authentication Phase

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.

PMsec in Action

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

Output from Server during Enrollment

COM4

Send

Output from IoMT Device

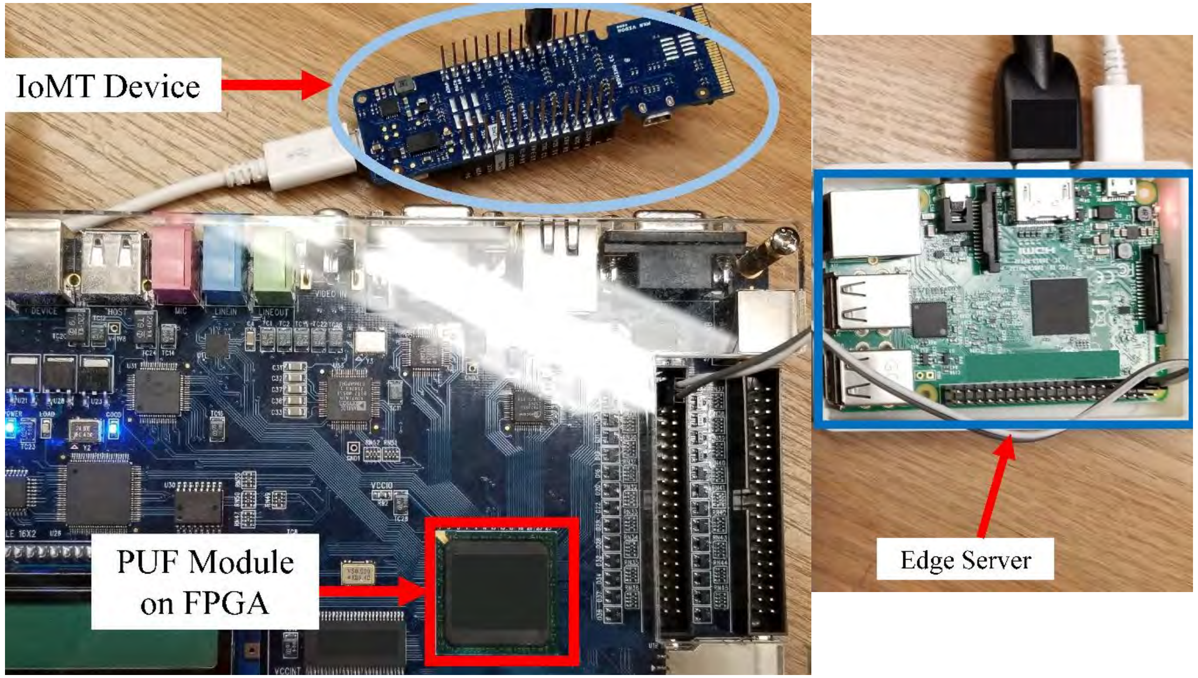
```
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 101110000101110010111100010111100010110100110111001010010100011
Sending key for authentication
```

Output from Server during Authentication

```
>>>
Hello
------------Authentication Phase------------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  101110000101110010111100010111100010110100110111001010010100011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>>
```

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

PMsec Module



Average Power Overhead – ~ 200 μW

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 (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

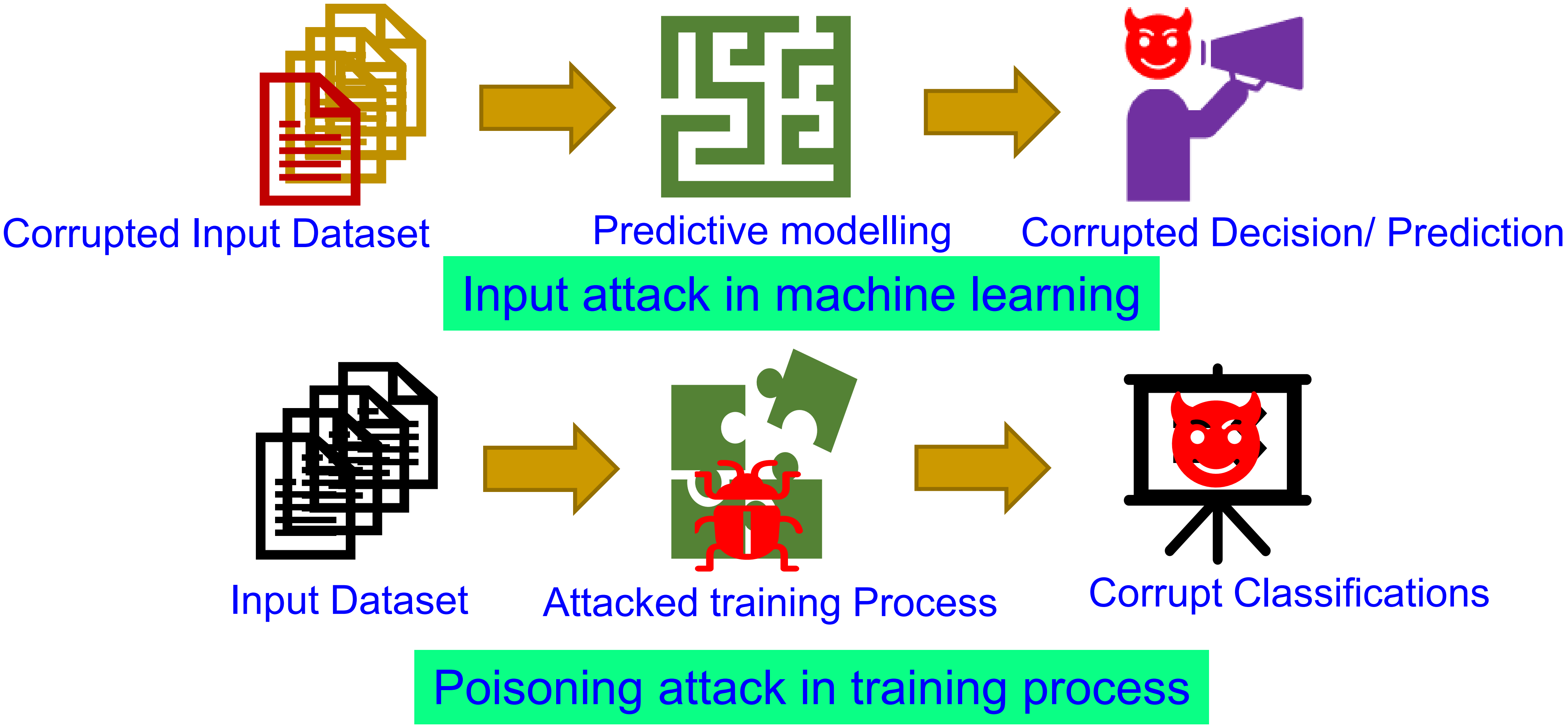
AI Cyberscurity

AI/ML - Vulnerability

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

Source: Sandip Kundu ISVLSI 2019 Keynote.

AI/ML – Cybersecurity Issue



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

AI/ML – Cybersecurity Issue

Classifications of Cyber Security Concerns in AI

- **Attacker's Capabilities**
  - Access to Training Data
  - Access to Model Training
  - Access to Trained Model
- **Attacker's Goal**
  - Model Poisoning, Extraction
  - Model Inversion, Impersonation
  - Model Invasion

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

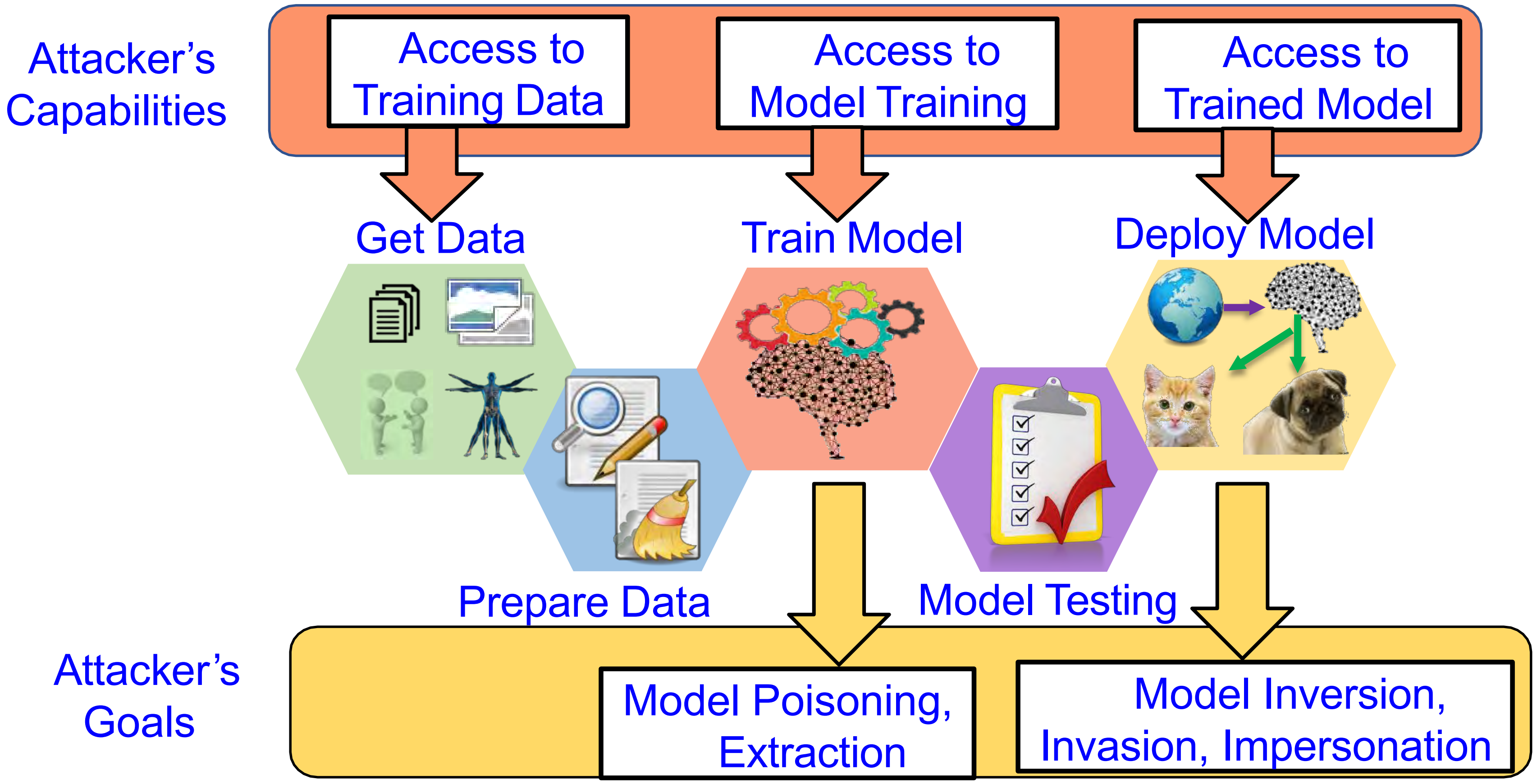
AI/ML Models - Classification of Security and Privacy Concerns

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

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

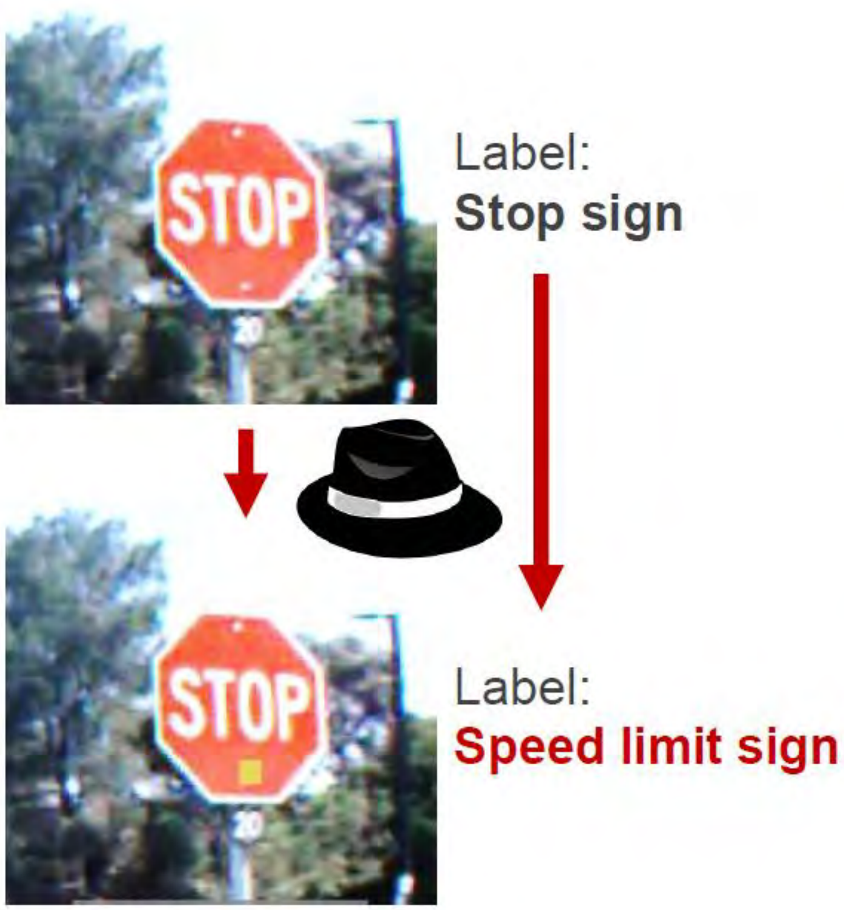
Source: Sandip Kundu ISVLSI 2019 Keynote.

AI Security - Attacks



Source: Sandip Kundu ISVLSI 2019 Keynote.

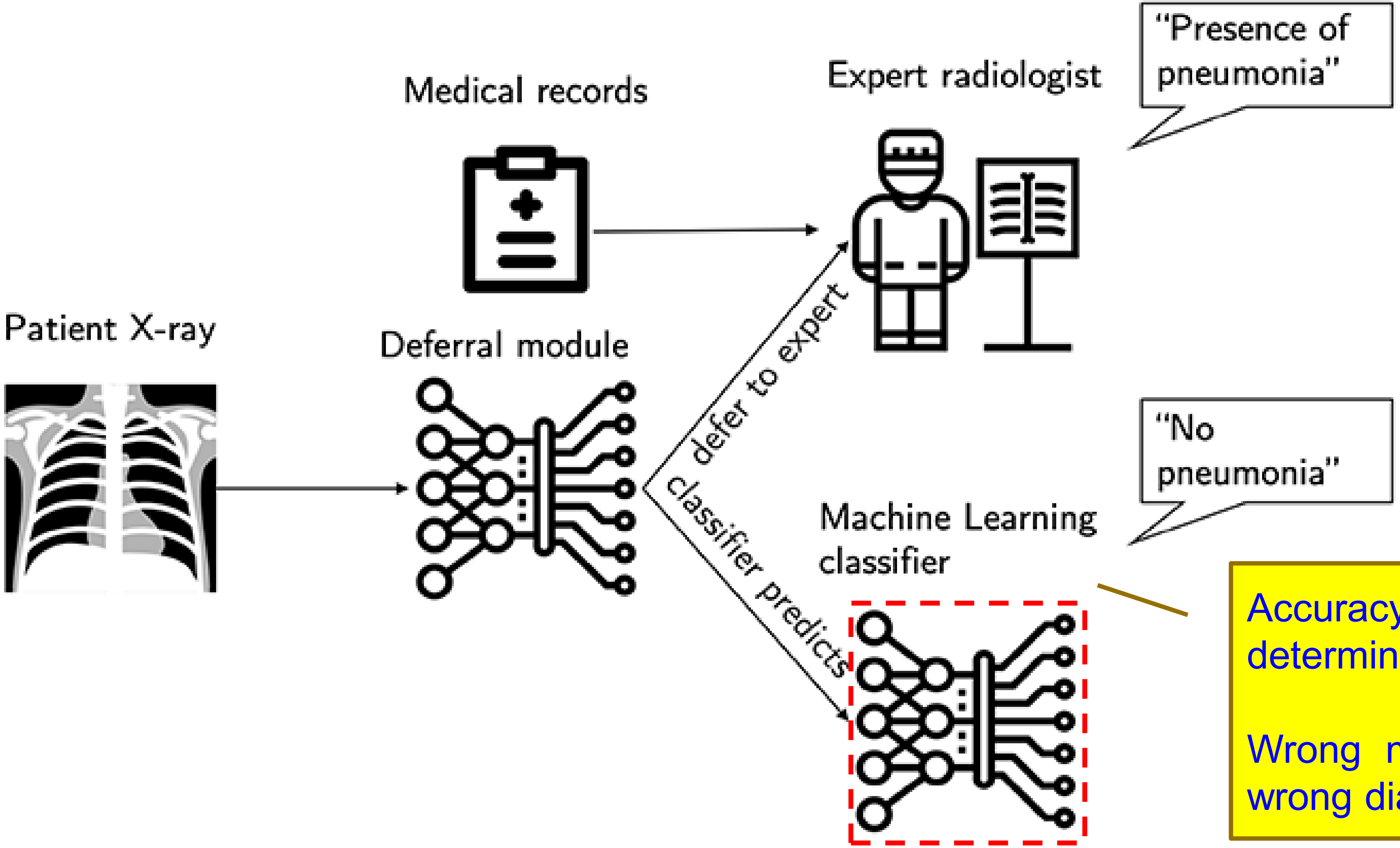
AI Security - Trojans in Artificial Intelligence (TrojAI)



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

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

Wrong ML Model → Wrong Diagnosis



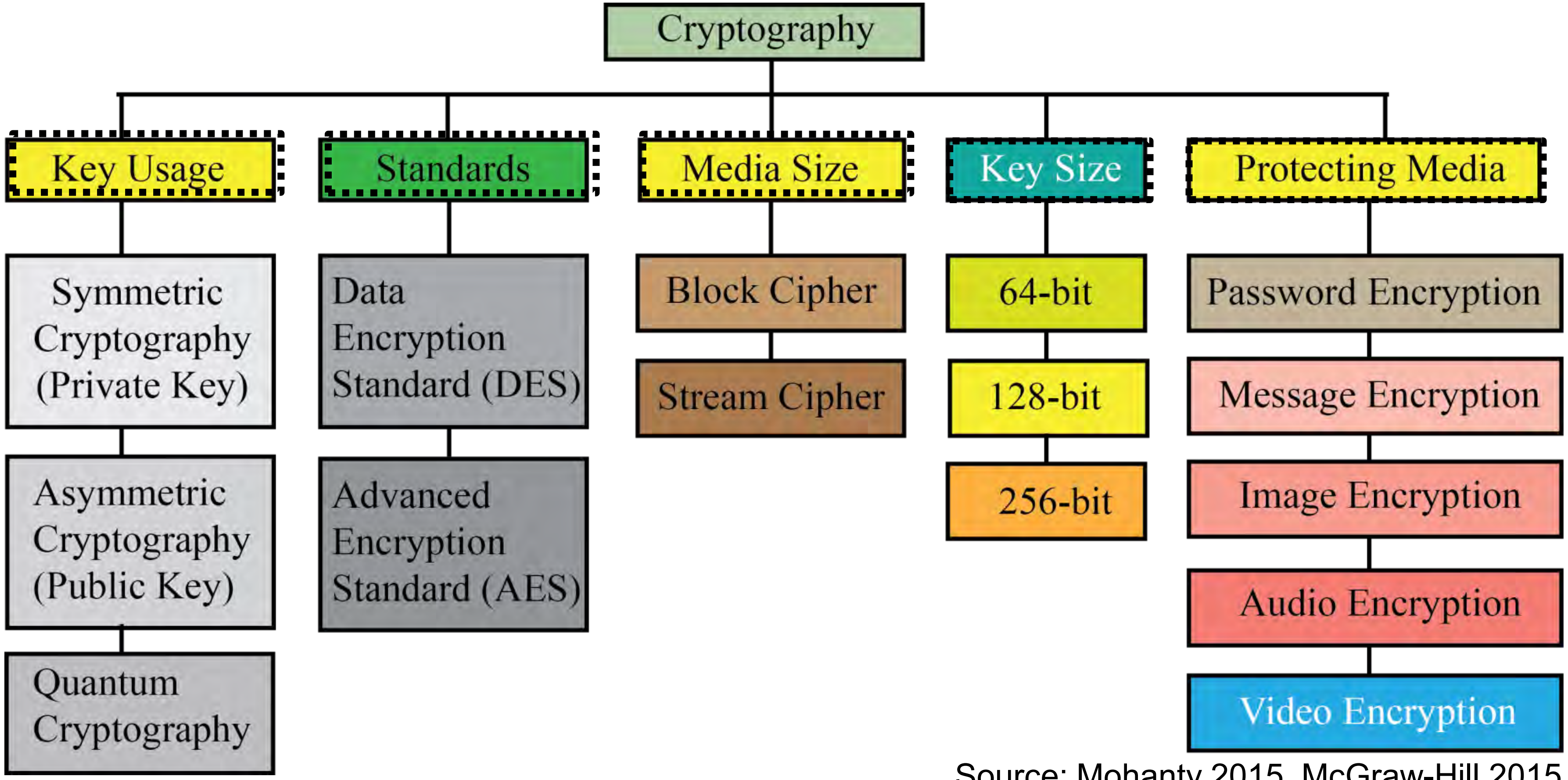
Accuracy is important determine pneumonia

Wrong model can lead to wrong diagnosis altogether

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

Cryptography

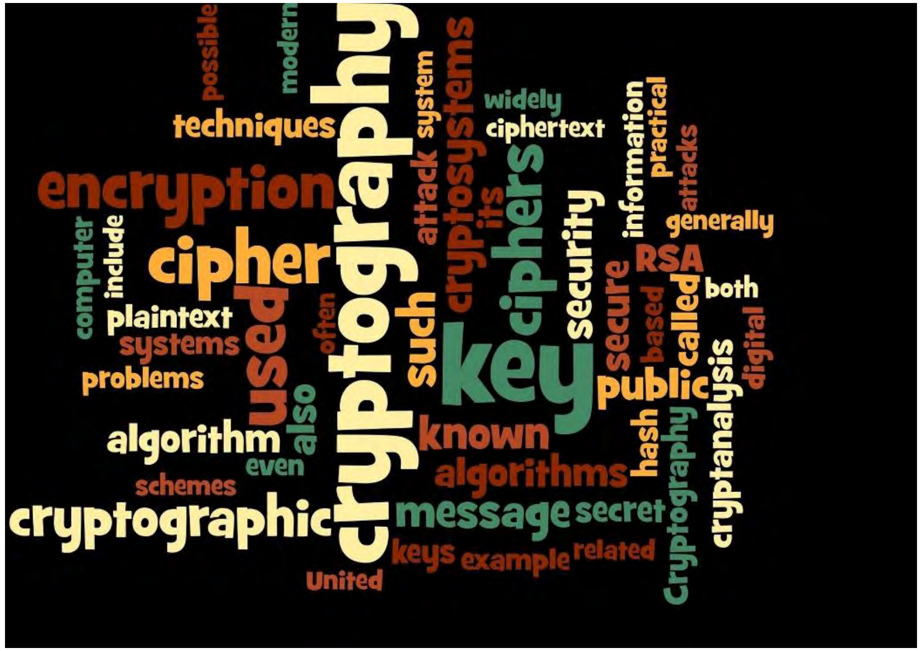
Information Protection - Cryptography



Source: Mohanty 2015, McGraw-Hill 2015

Cryptography

Cryptography is study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents.



Source: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

Cryptographic Concepts

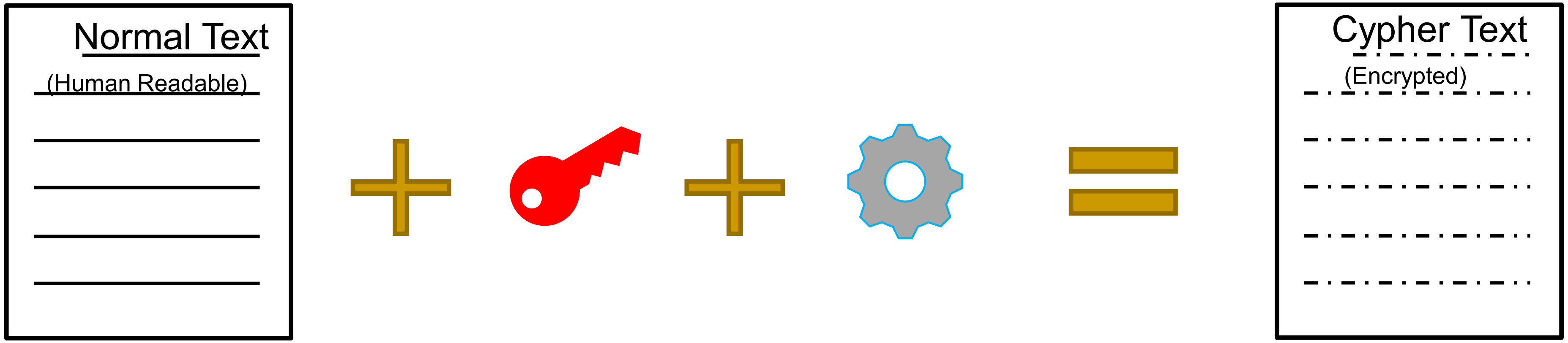
- Encryption and Decryption
  - Used for communication.
  - Not easy to read an encrypted text.
- Cryptographic Hashing Algorithms
  - Input of a hashing function can be of any size – bytes, megabytes, or gigabytes.
  - Output of hashing function will be a fixed size.

Many applications use Encryption and Decryption

- Encryption and decryption has many applications
- It helps share secrets and makes sure the text is not tracked.
- Increased confidentiality
- Encryption makes sure the data is not altered., prevents plagiarism
- Major communication applications use end-to-end encryption and decryption.
  - Helps protect privacy and security.

Encryption and Decryption

- Normal text is encrypted into a cyphertext.



- Once encrypted, cannot be readable until decrypted.
- Useful for sharing secrets.

https://www.guru99.com/difference-encryption-decryption.html#:~:text=data%20during%20communication.-,Encryption%20is%20a%20process%20which%20transforms%20the%20original%20information%20into,as%20passwords%20and%20login%20id.

Algorithms for Encryption and Decryption

- Symmetric Key Cryptography
  - Have the same key for encryption and decryption.
  - Pre-shared keys are used in this algorithm.
  - Have to share the key with both the parties.
  - Difficult to securely share the keys
- Asymmetric Key Cryptography
  - Use two sets of keys for encryption and decryption
  - Secure as a private key need not be shared with the other party.
  - Needs more memory for processing.

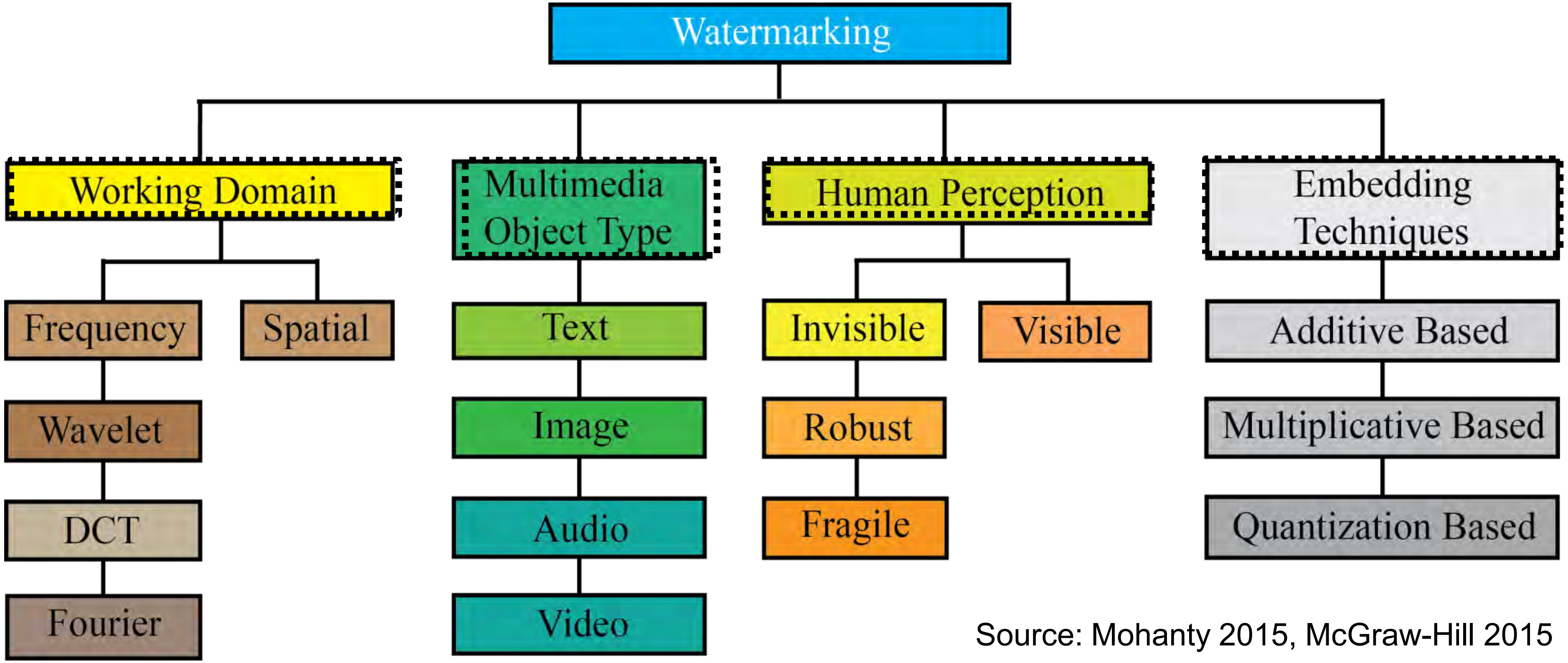
Cryptographic Hashing

- It is a mathematical function that can map any size of data to a fixed size output.
- It is deterministic – A same input always results in the same output.
- Hashing function is not reversible, i.e., hash cannot be used to get the input.
- It is highly unlikely two inputs have the same hash.
- Examples include SHA2, SHA256, etc.,

https://en.wikipedia.org/wiki/Cryptographic_hash_function

Watermarking

Copyright Protection - Watermarking



Source: Mohanty 2015, McGraw-Hill 2015

Multimedia Piracy – Movie/Video

High

Studio

Cinema

On-line

Video on Demand

Piracy Threat Level

DVD/Blu-ray

Pay-TV Broadcasting

Free-to-Air Broadcasting

Low

“Film piracy cost the US economy $20.5 billion annually.”

Source: http://www.ipi.org/ipi_issues/detail/illegal-streaming-is-dominating-online-piracy

Multimedia Piracy – Music/Audio

"The U.S. economy loses $12.5 billion in total output annually as a consequence of music theft."

Source: https://www.riaa.com/reports/the-true-cost-of-sound-recording-piracy-to-the-u-s-economy/

DRM - Definition

- Digital Rights Management (DRM) is a generic term that refers to any of several technologies used by publishers, creators, or owners to control access and usage of digital data.
- Typically a DRM system:
  - Protects intellectual property by encrypting the data so that it can only be accessed by authorized users.

    and/or

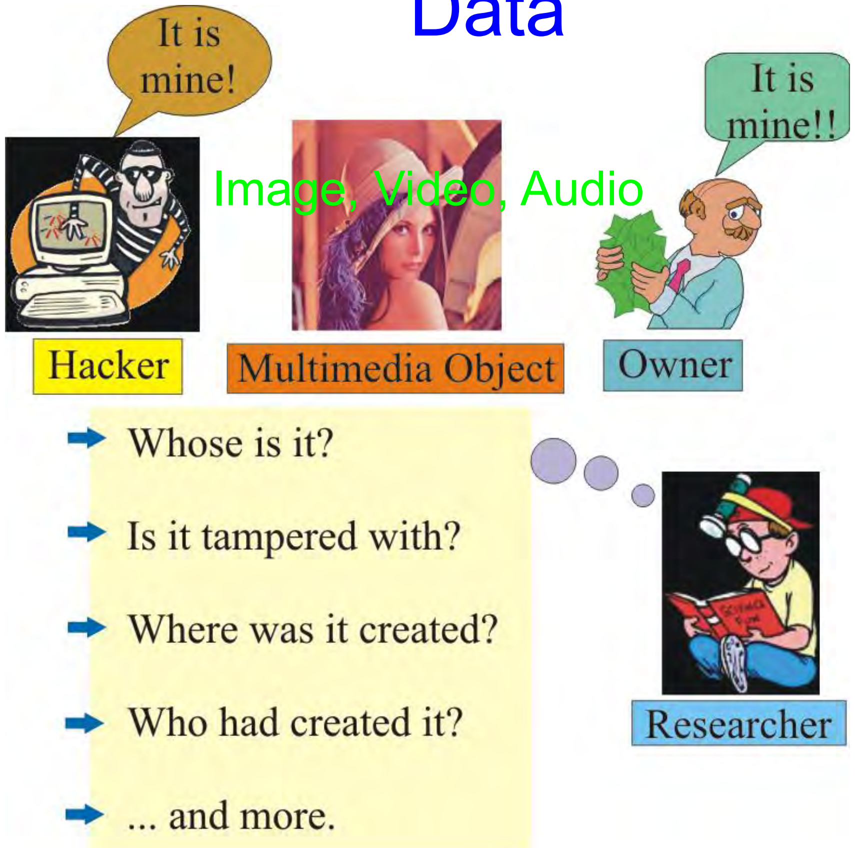
  - Marks the content with a digital watermark so that the content can not be freely distributed.

DRM - Techniques

- Encryption
- Watermarking
- Scrambling
- Digital certificates
- Secure communications protocols
- Fingerprinting
- Hashing
- …… and more

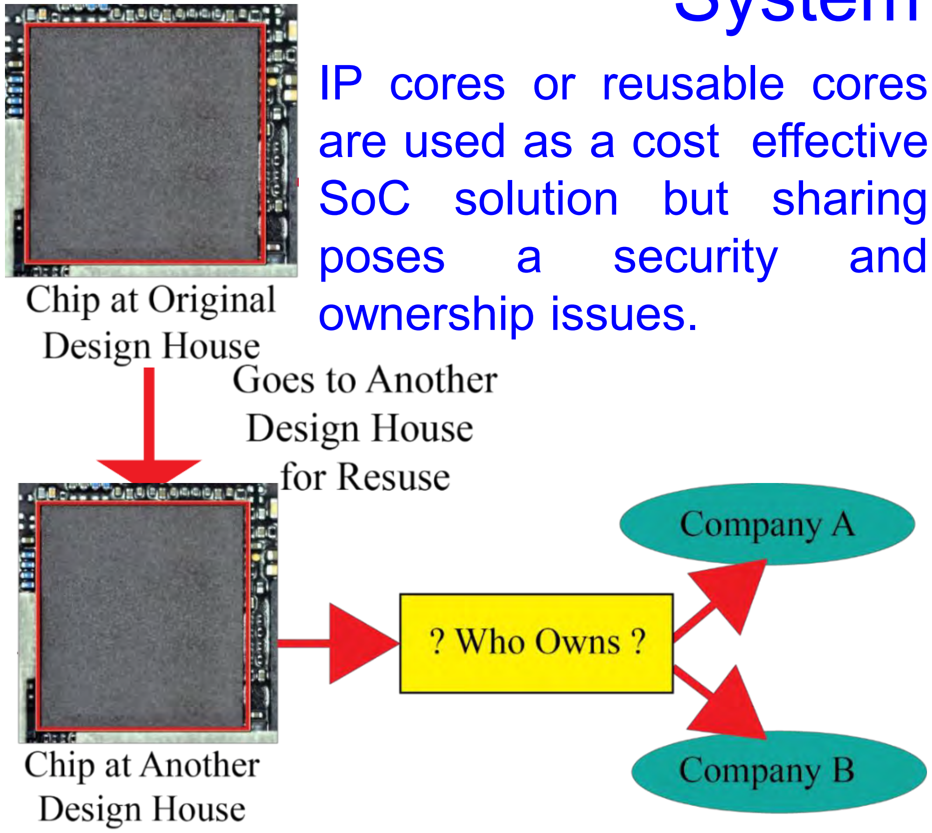
Data and System Authentication and Ownership Protection – My 20 Years of Experiences

Data



System

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



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.

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

AI can be fooled by fake data

AI can create fake data (Deepfake)

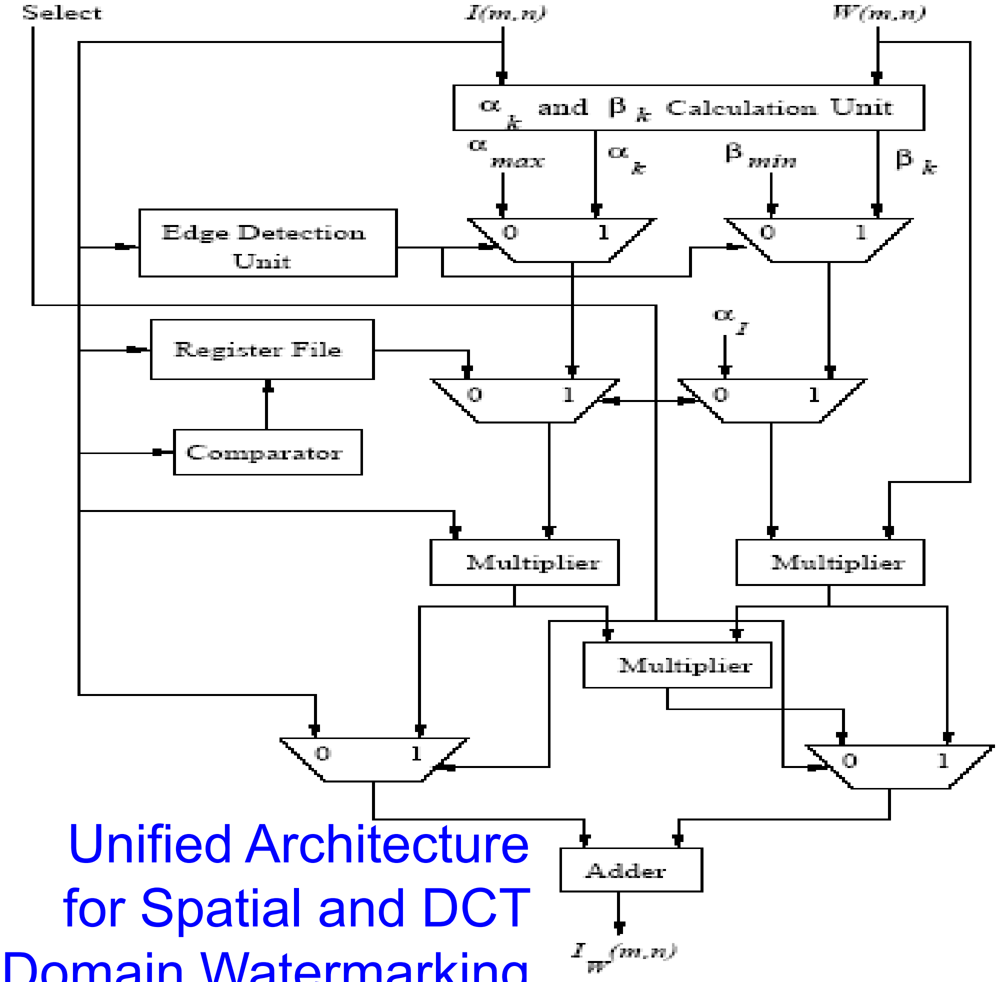
Authentic Fake

An implantable medical device

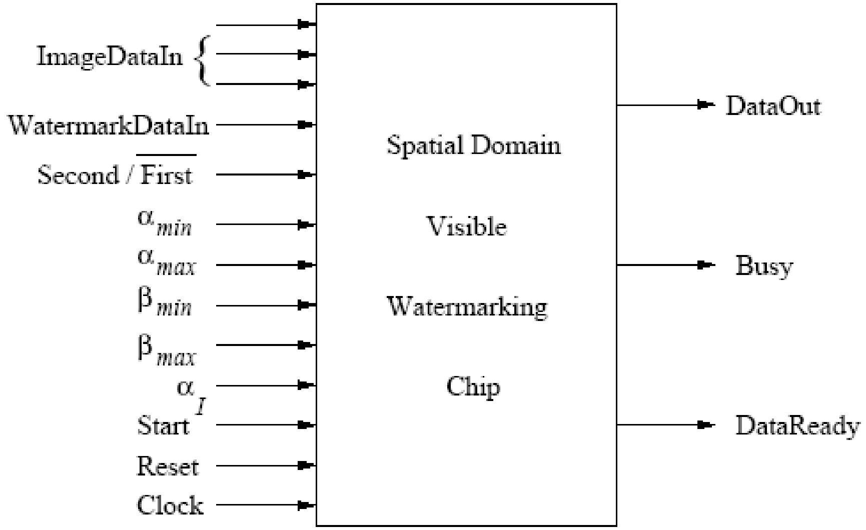
Authentic Fake

A plug-in for car-engine computers

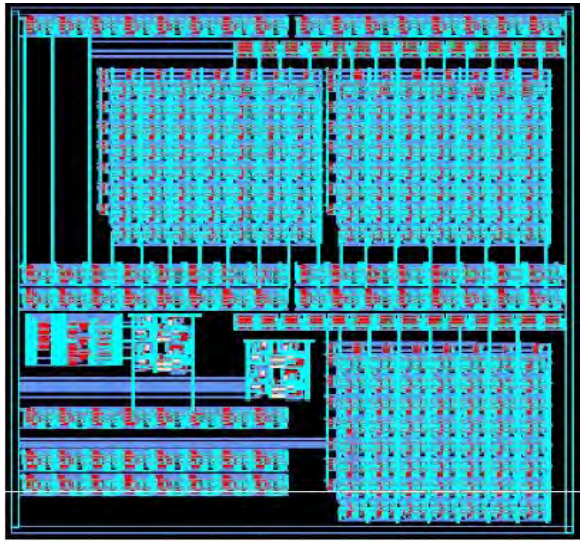
Our Design: First Ever Watermarking Chip for Source-End Visual Data Protection



Unified Architecture for Spatial and DCT Domain Watermarking



Pin Diagram



Chip Layout

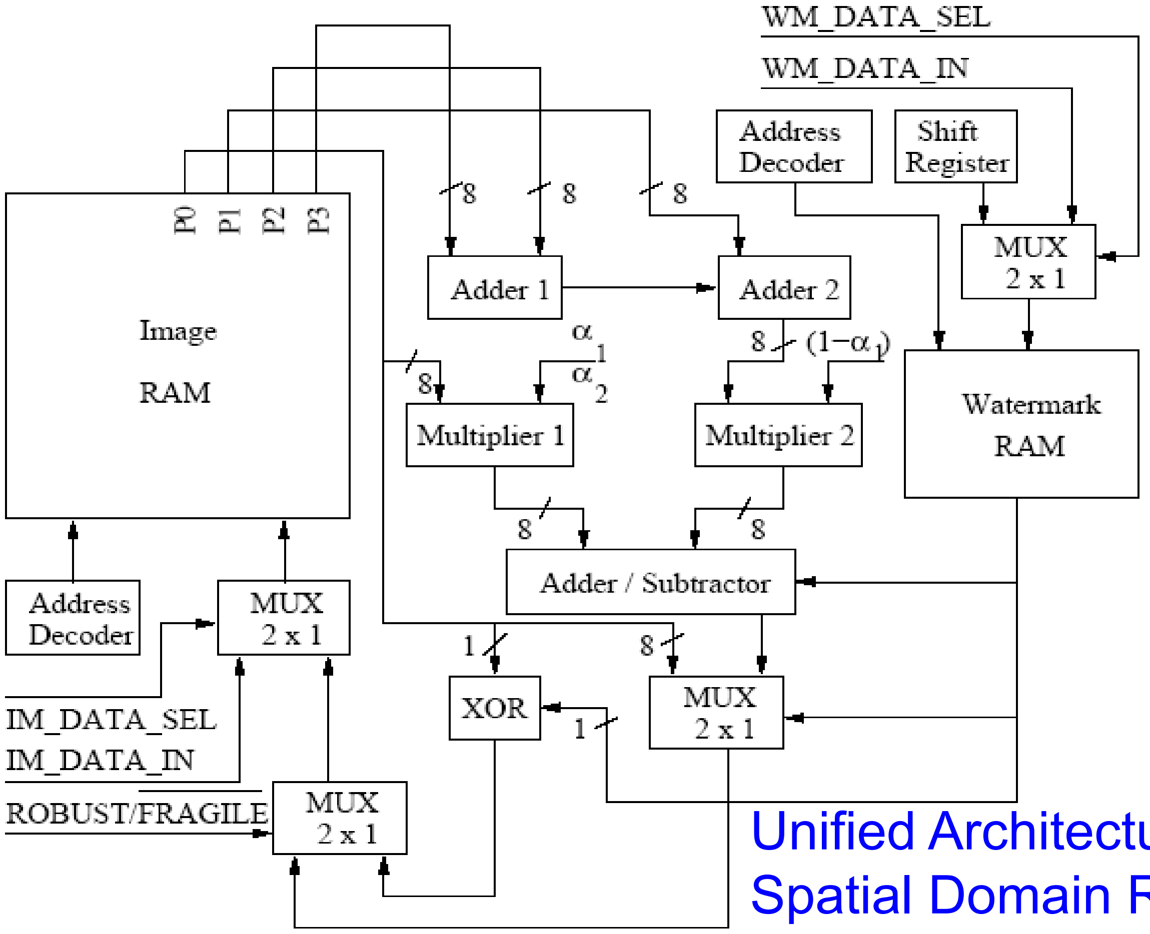
Chip Design Data

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

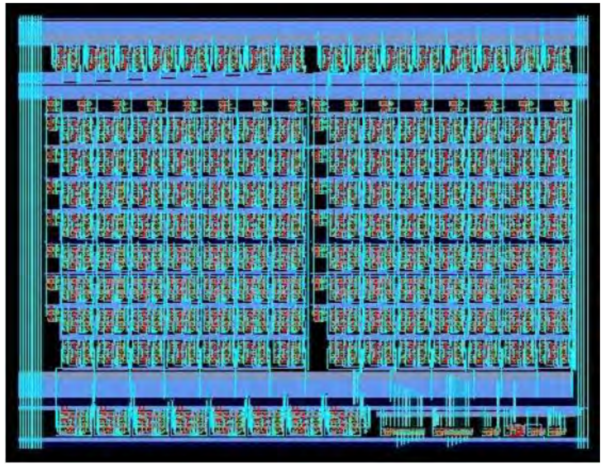
Power Consumption: 6.9 mW, Operating Frequency: 292 MHz

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

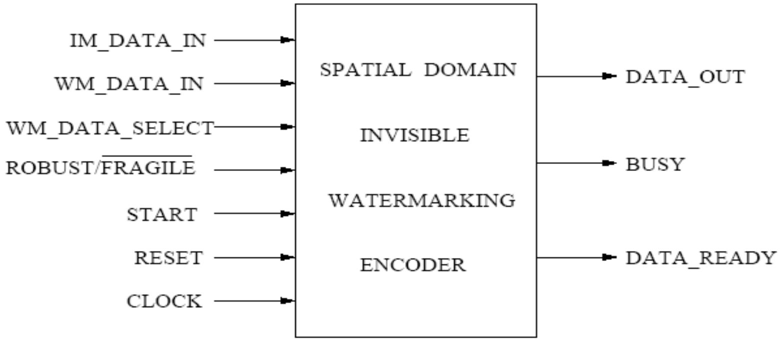
Our Design: First Ever Watermarking Chip for Source-End Visual Data Integrity



Unified Architecture for Spatial Domain Robust and Fragile Watermarking



Chip Layout

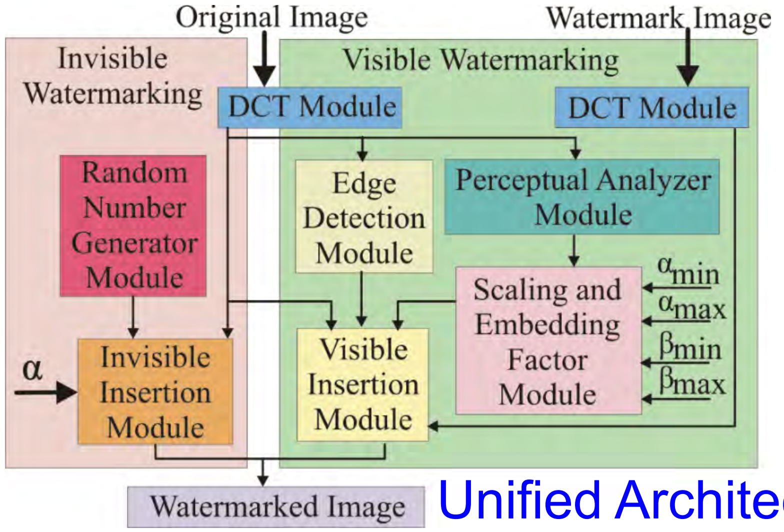


Pin Diagram

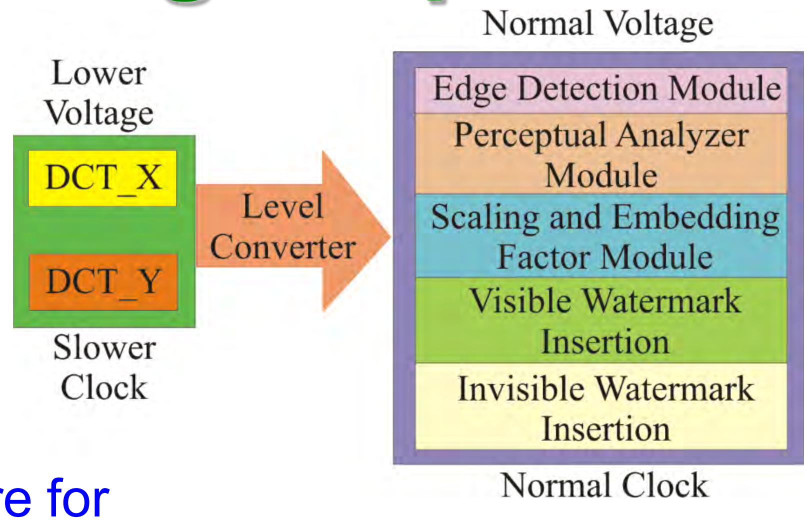
Chip Design Data
Total Area : 0.87 sq mm, No. of Gates: 4,820
Power Consumption: 2.0 mW, Frequency: 500 MHz

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)*, September 2007, Volume 1, Issue 5, pp. 600-611.

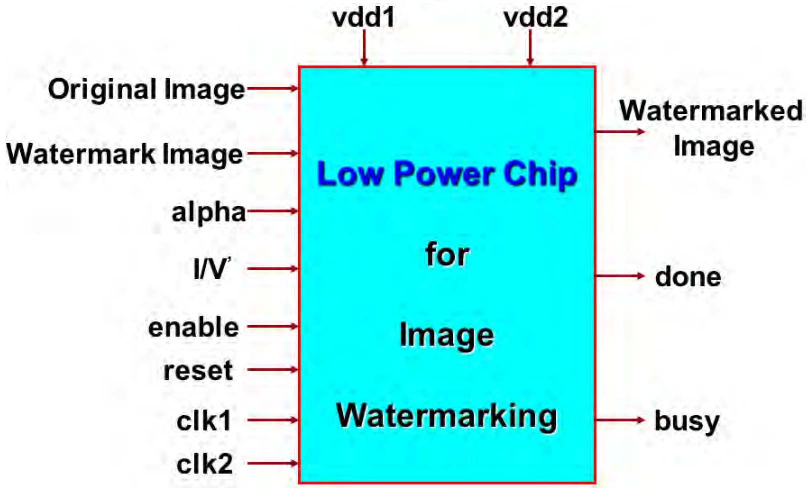
Our Design: First Ever Low-Power Watermarking Chip for Data Quality



Unified Architecture for DCT Domain Watermarking

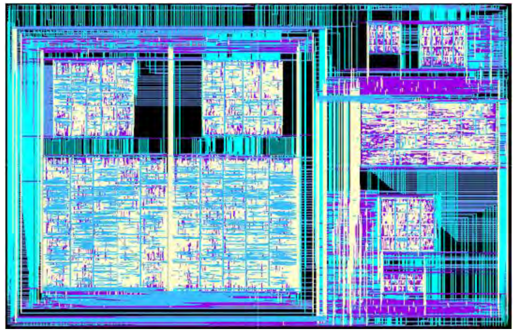


DVDF Low-Power Design



Pin Diagram

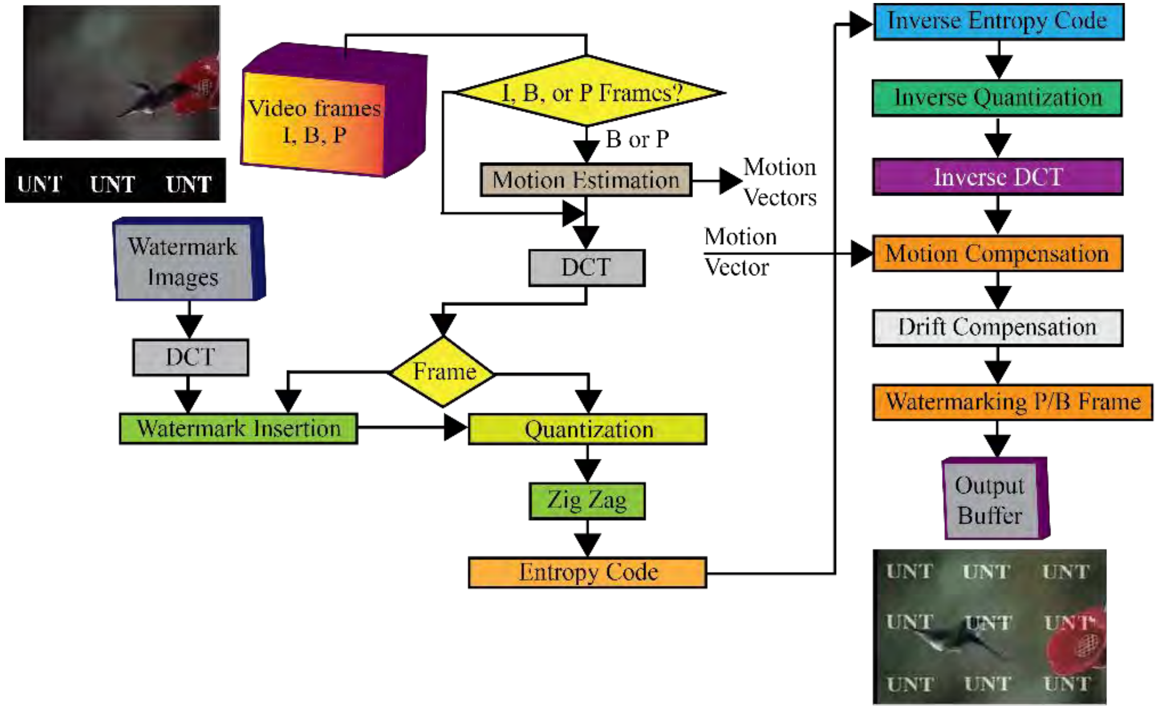
Chip Design Data
Total Area : 16.2 sq mm, No. of Transistors: 1.4 million
Power Consumption: 0.3 mW, Operating Frequency: 70 MHz and 250 MHz at 1.5 V and 2.5 V



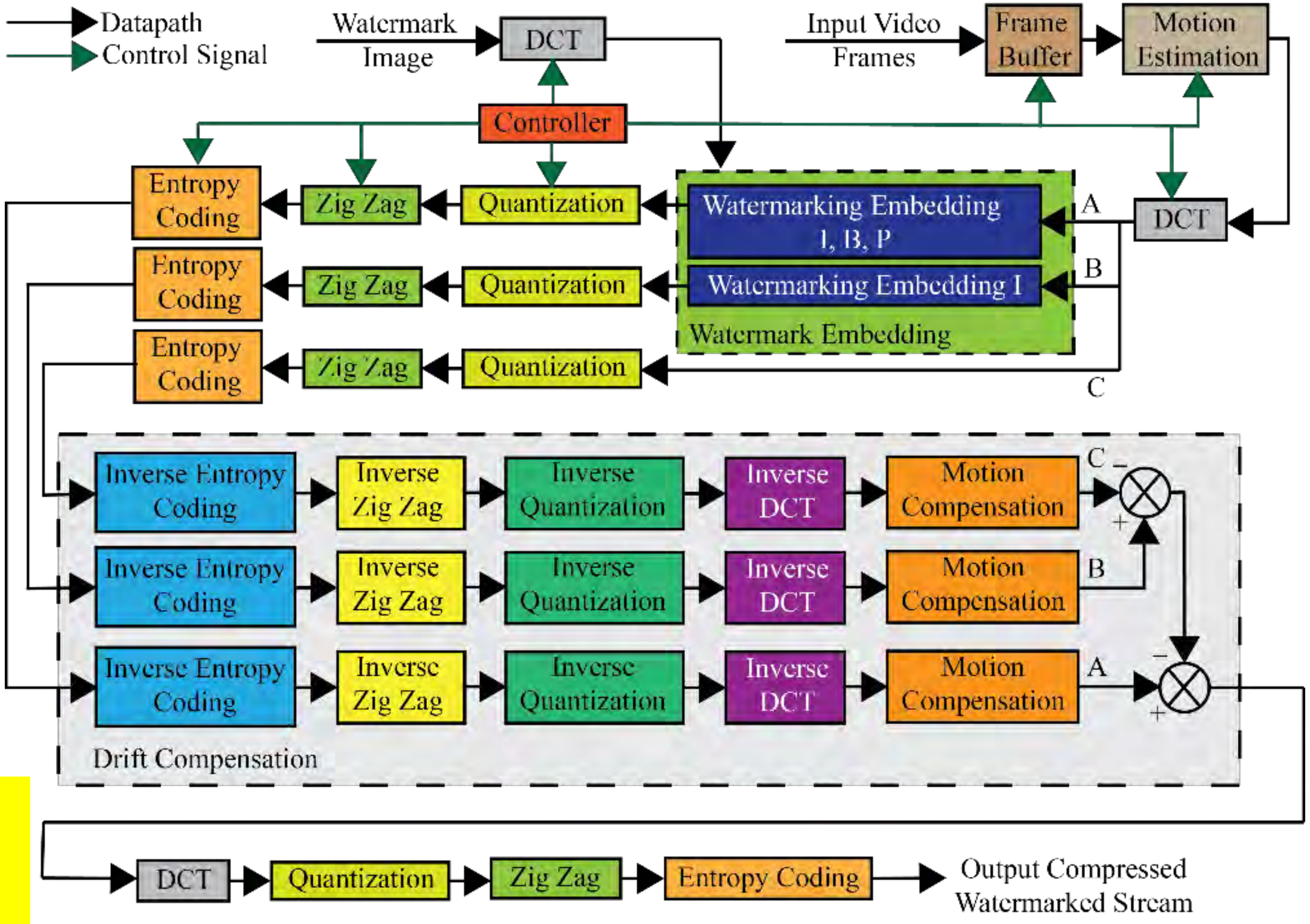
Chip Layout

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 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

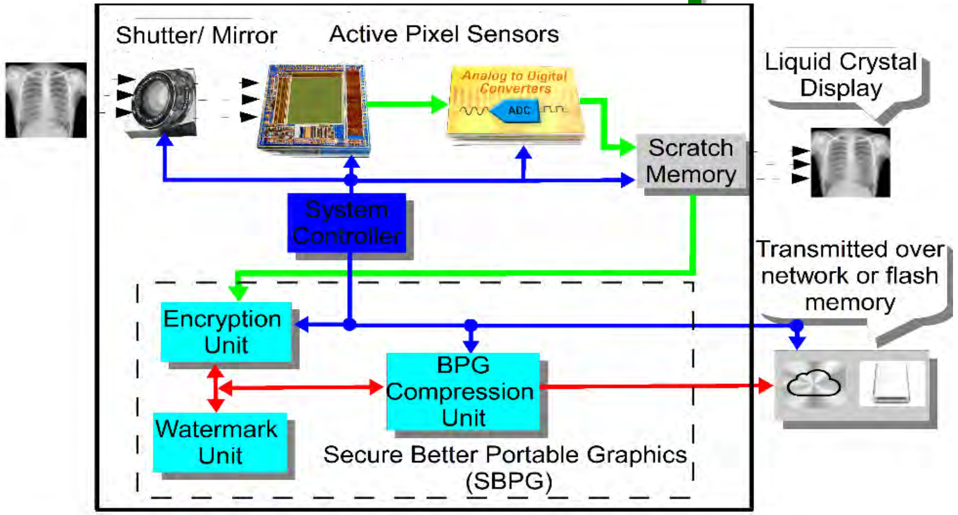
Resource: 28322 LE, 16532 Registers, 9 MUXes

Operating Frequency: 100 MHz

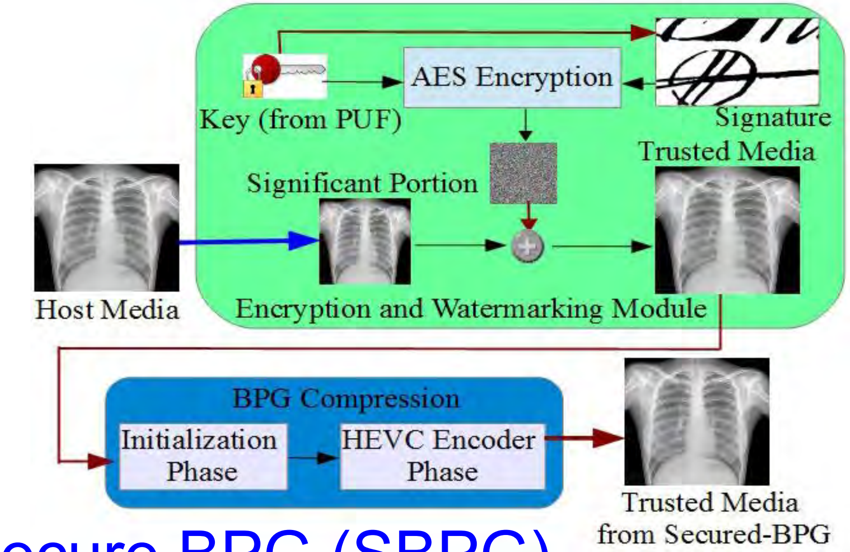
Throughput: 43 fps

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.

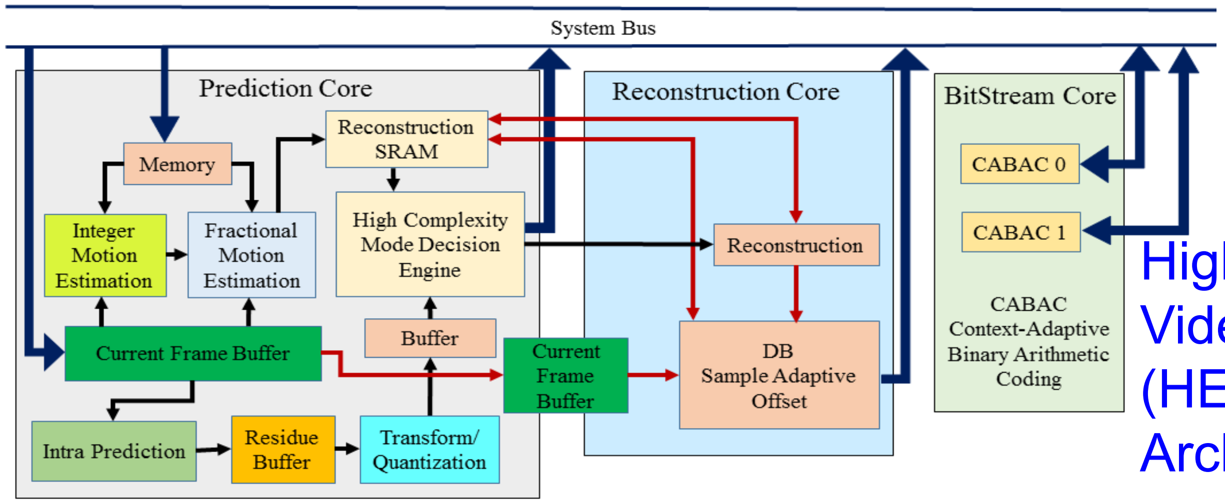
We Introduced First Ever Secure Better Portable Graphics (SBPG) Architecture



Secure Digital Camera (SDC) with SBPG



Secure BPG (SBPG)

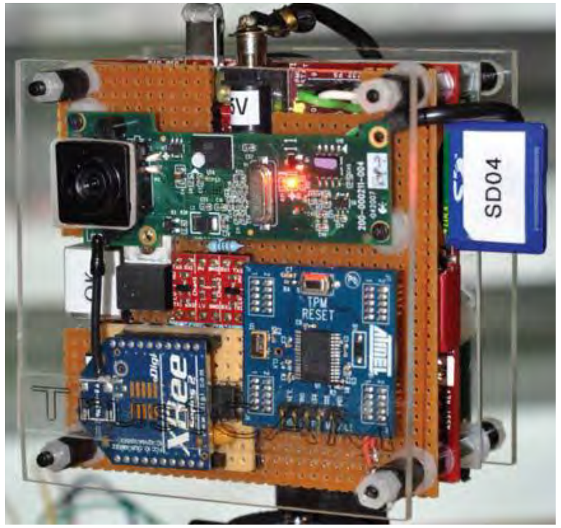


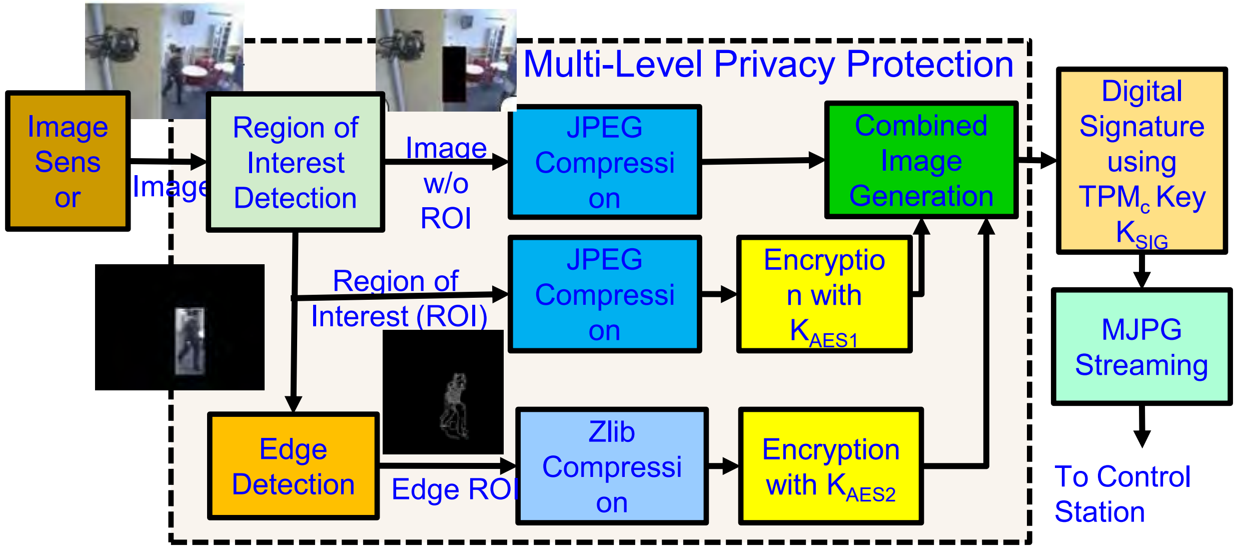
High-Efficiency Video Coding (HEVC) Architecture

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.

My Watermarking Research Inspired - TrustCAM



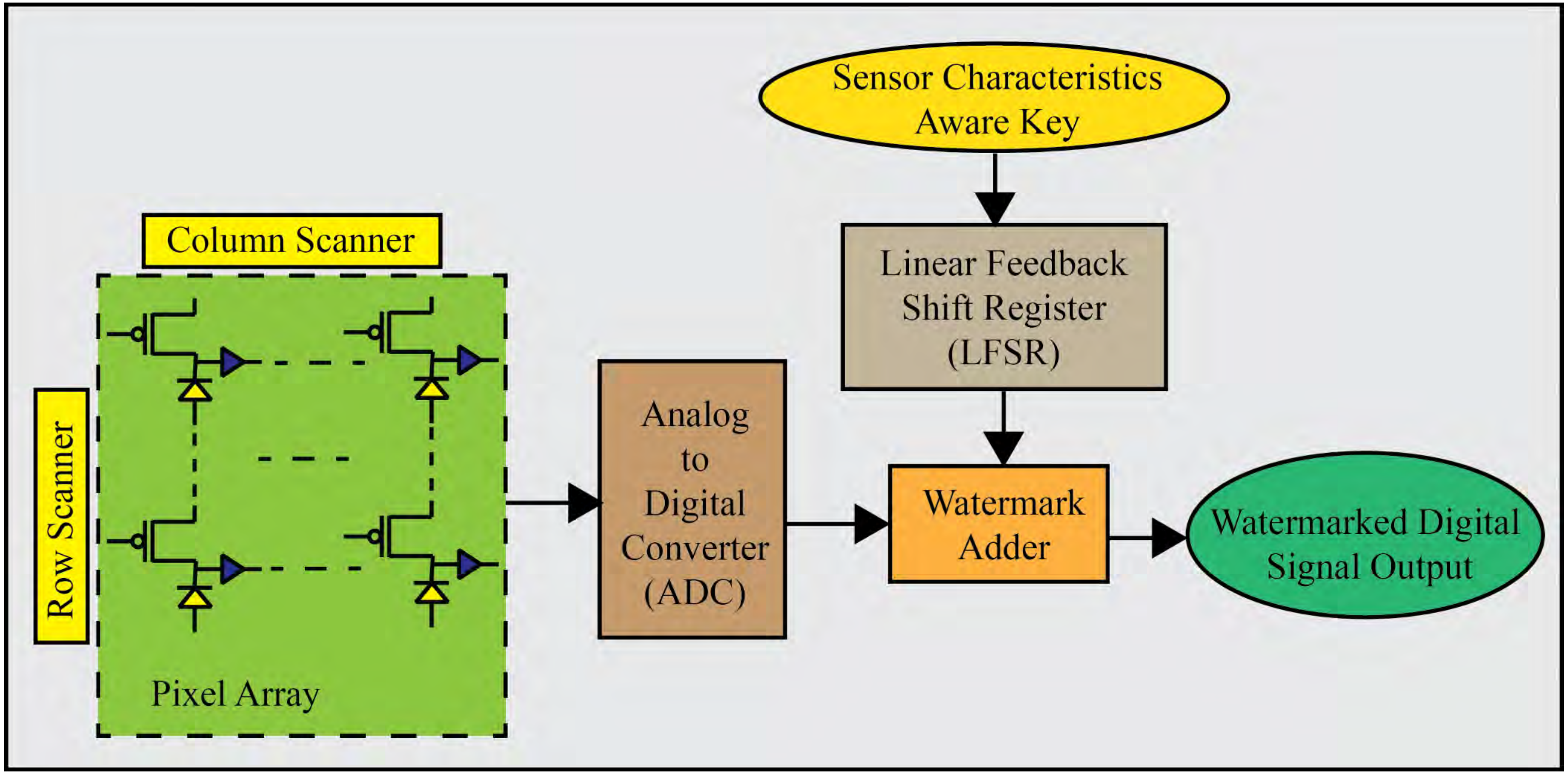


For integrity protection, authenticity and confidentiality of image data.

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

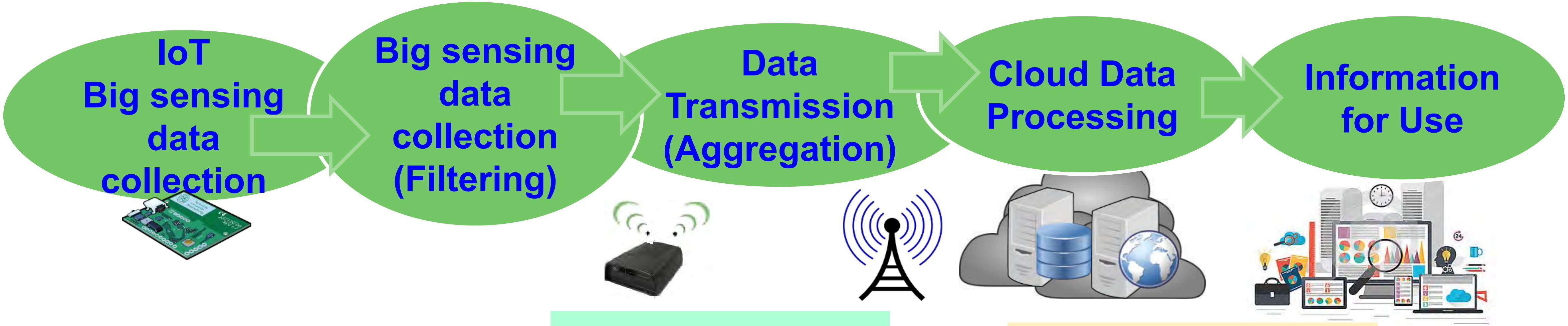
- Identifies sensitive image regions.
- Protects privacy sensitive image regions.
- A Trusted Platform Module (TPM) chip provides a set of security primitives.

My Watermarking Research Inspired – Secured Sensor



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.

Secure Data Curation a Solution for Fake Data?



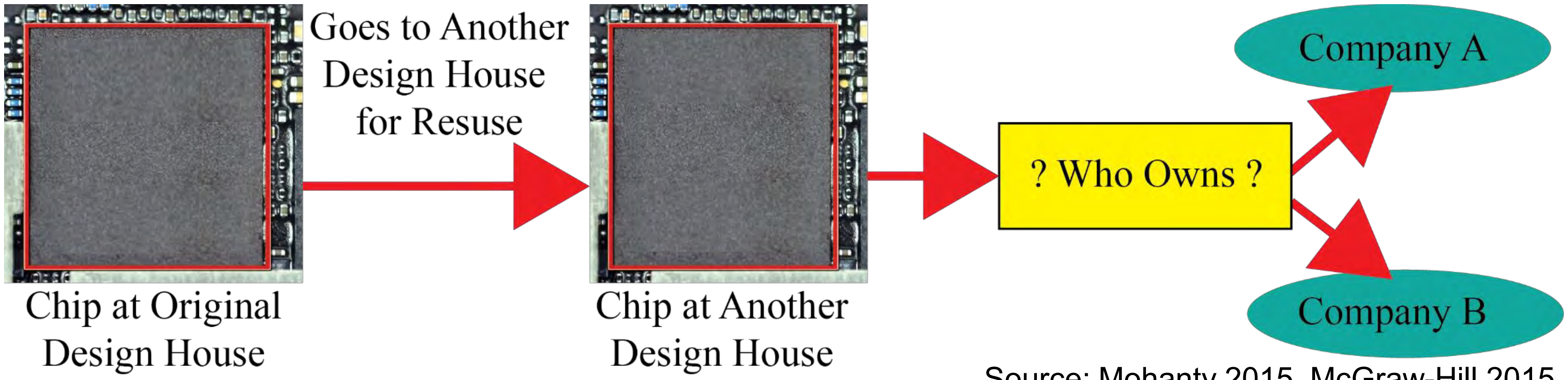
Edge Training:
- ➢ Data Signature
- ➢ Model Signature

Fake Data Defense:
- Stop (Shield)
- Detect

Cloud Training:
- ❖ Data Signature
- ❖ Model Signature

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.

Hardware IP Right Infringement



Source: Mohanty 2015, McGraw-Hill 2015

Hardware IPR Infringement

- False Ownership Claim
- Sub-licensing
- Piracy (Reverse Engineering)

Hardware Reverse Engineering

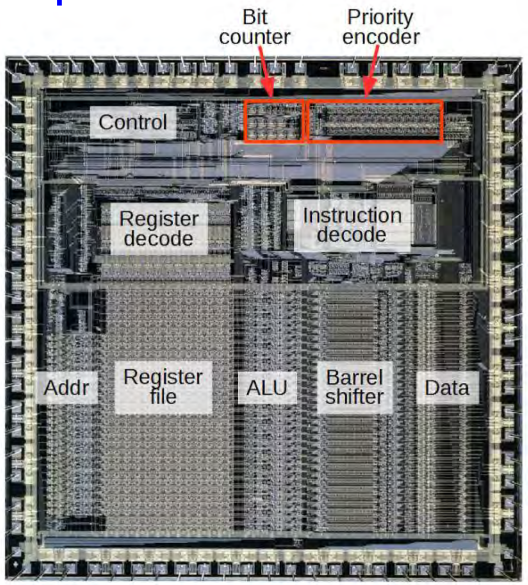
Source: http://legacy.lincolninteractive.org/html/CES%20Introduction%20to%20Engineering/Unit%203/u3l7.html

CE System disassembly
Subsystem identification, modification

Source: https://www.slideshare.net/SOURCEConference/slicing-into-apple-iphone-reverse-engineering

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

Chip-Level Modification



Source: http://pic-microcontroller.com/counting-bits-hardware-reverse-engineering-silicon-arm1-processor/

Cloned/Fake/Counterfeit Electronics

- Consumer Electronics is the 2nd most counterfeit product in USA.
- Between November 2007 and May 2010, U.S. Customs officials seized 5.6 million counterfeit microprocessors.
- The market value of the 2016 seized counterfeit goods, had they been genuine, amounted to $1.4 billion.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/
Source: http://247wallst.com/special-report/2017/04/29/10-most-counterfeited-products-in-america/

Counterfeit Hardware

2014 Analog Hardware Market (Total Shipment Revenue US $)

Wireless Market
$18.9 billion (34.8%)

Consumer Electronics
$9.0 billion (16.6%)

Industrial Electronics
$8.9 billion (16.5%)

Automotive
$8.5 billion (15.7%)

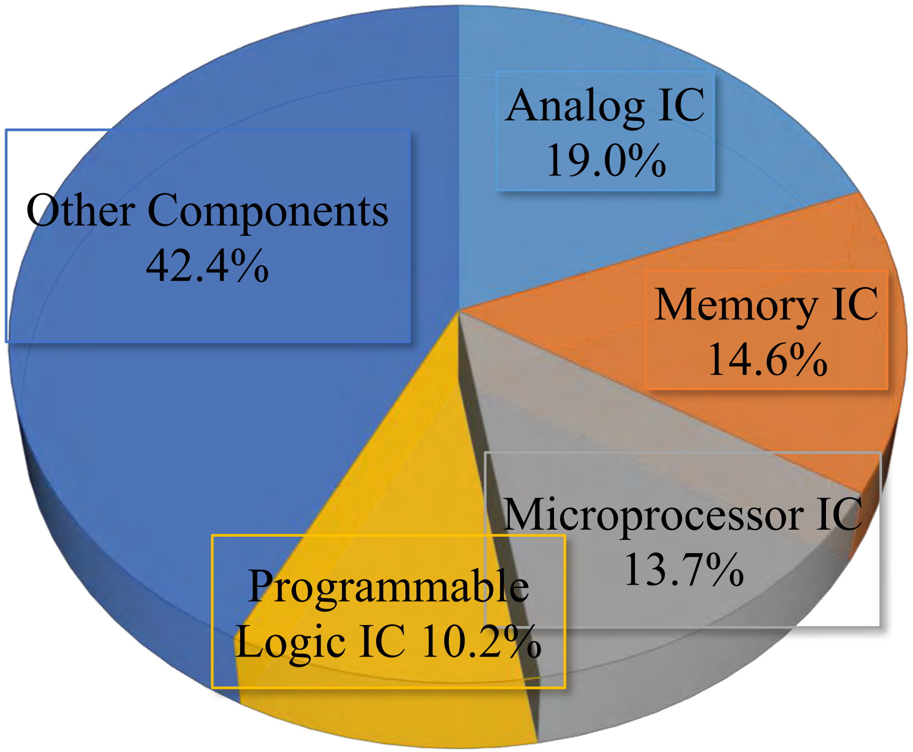
Data Processing
$6.0 billion (11%)

Wired Communications
$2.9 billion (5.4%)

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Top counterfeits could have impact of $300B on the semiconductor market.

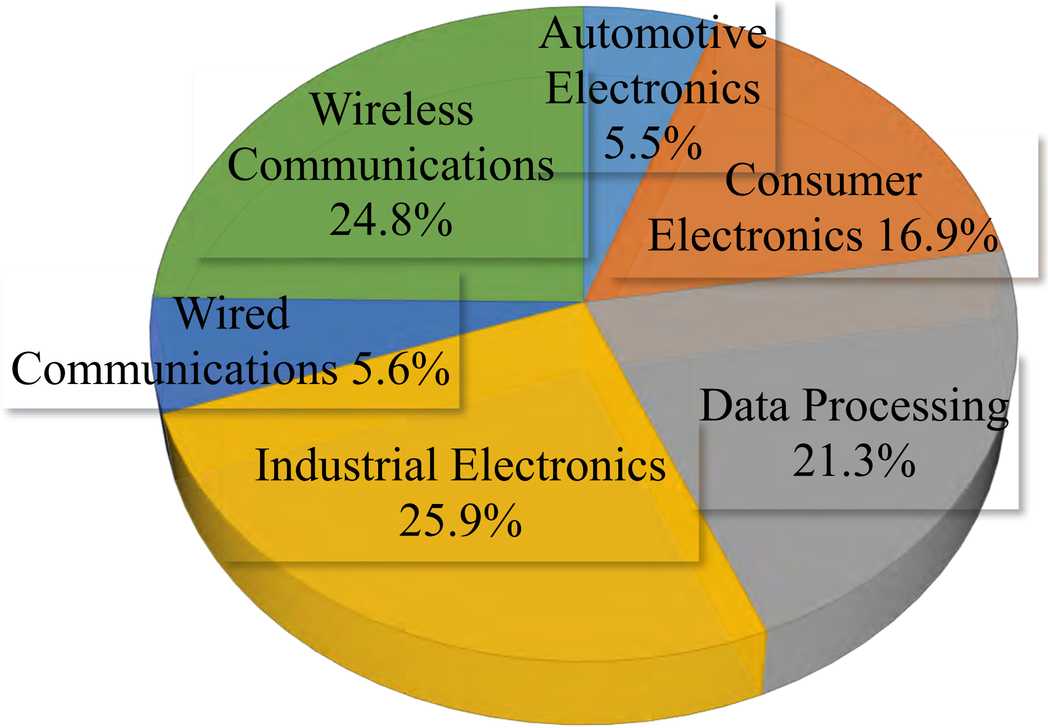
Counterfeit Hardware



Top counterfeits could have impact of $300B on the semiconductor market.

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Worldwide Electronics Revenue

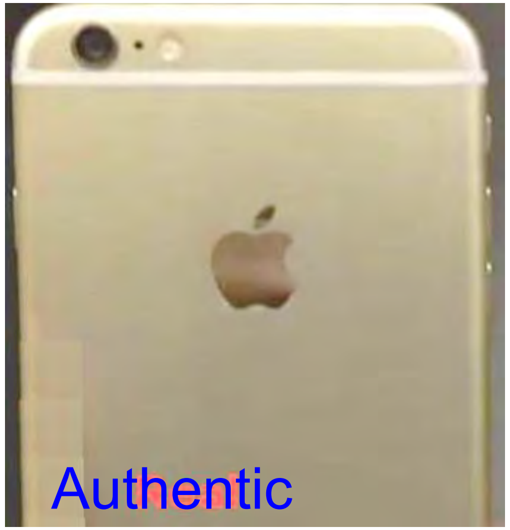


- Worldwide OEM factory revenue is more than 2 trillion dollars currently.

Source: https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october

Cloned/Fake Electronics Hardware – Example - 1

Source: https://petapixel.com/2015/08/14/i-bought-a-fake-nikon-dslr-my-experience-with-gray-market-imports/

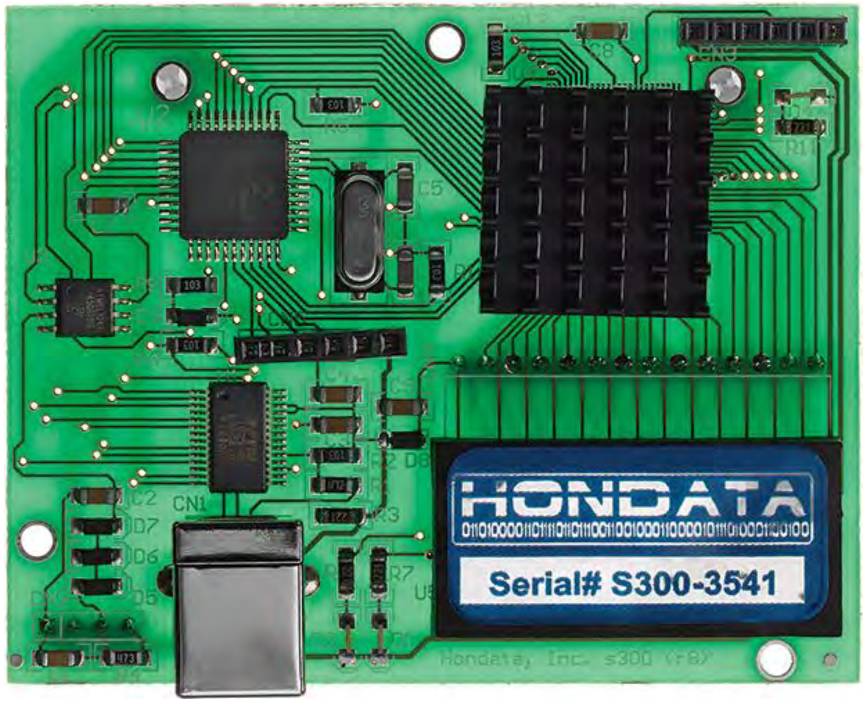


Source: http://www.manoramaonline.com/

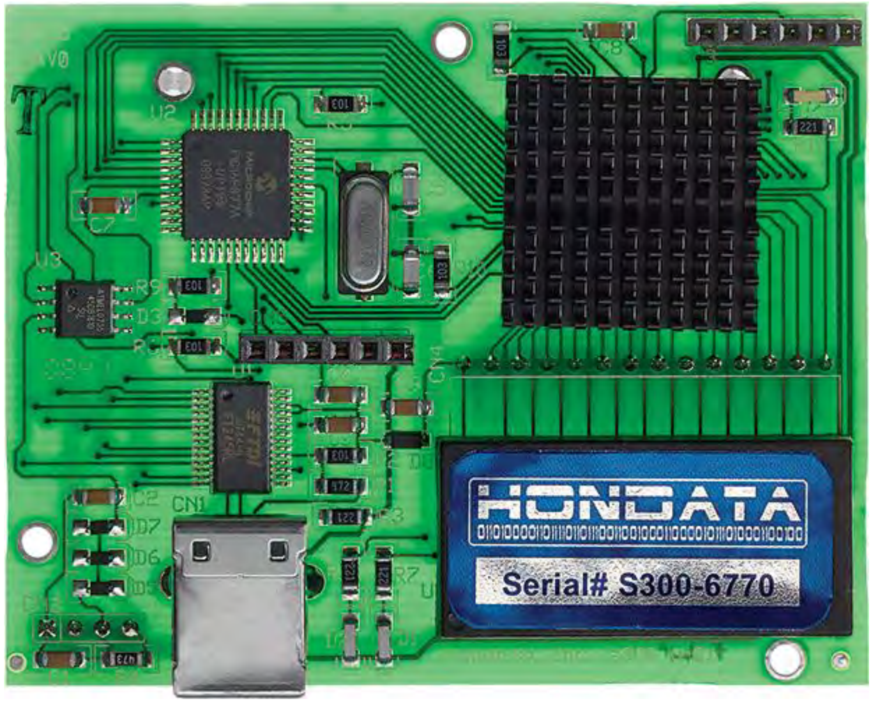
Source: http://www.cbs.cc/fake-capacity-usb-drives/

Typical Consumer Electronics

Cloned/Fake Electronics Hardware – Example - 2



Fake



Authentic

A plug-in for car-engine computers.

Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

Cloned/Fake Electronics Hardware – Example - 3

Fake　　　　Authentic

A typical rechargeable battery in a typical CE

Source: https://www.premiumbeat.com/blog/how-to-spot-counterfeit-camera-gear/

Cloned/Fake Electronics Hardware - What is the Problem? It is cheaper!

- Installing cloned hardware into networks can open door to hackers: man-in-the-middle attacks or secretly alter a secure communication path between two systems to bypass security mechanisms.
- Cloned hardware may lack the security modules intended to protect IoT devices, and so it opens up the user to cyberattack.
- If a hacker embeds a malicious hardware in a drone then he could shut it down or retarget it when it reached preset GPS coordinates.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

Cloned/Fake Electronics Hardware - What is the Problem? It is cheaper!

- Counterfeit battery can cause safety hazards.
- Counterfeit electronics embedded in missile guidance systems and aircrafts can have serious problems for the defense systems.
- According to the International AntiCounterfeiting Coalition, lost profits due to counterfeiting has resulted in the loss of more than 750,000 jobs in the United States.

Source: https://www.scientificamerican.com/article/electronic-chip-counterfeit-china/

Source: http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

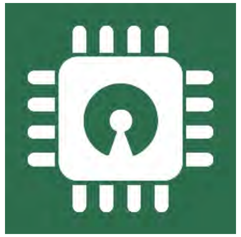
Hardware Assisted Security (HAS) or Security-by-Design (SbD)

Cybersecurity Attacks - Software and 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

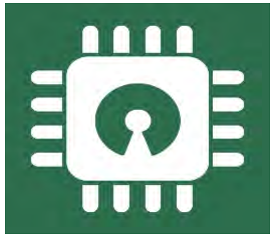
Source: Mohanty ICCE Panel 2018

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

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

IT Security

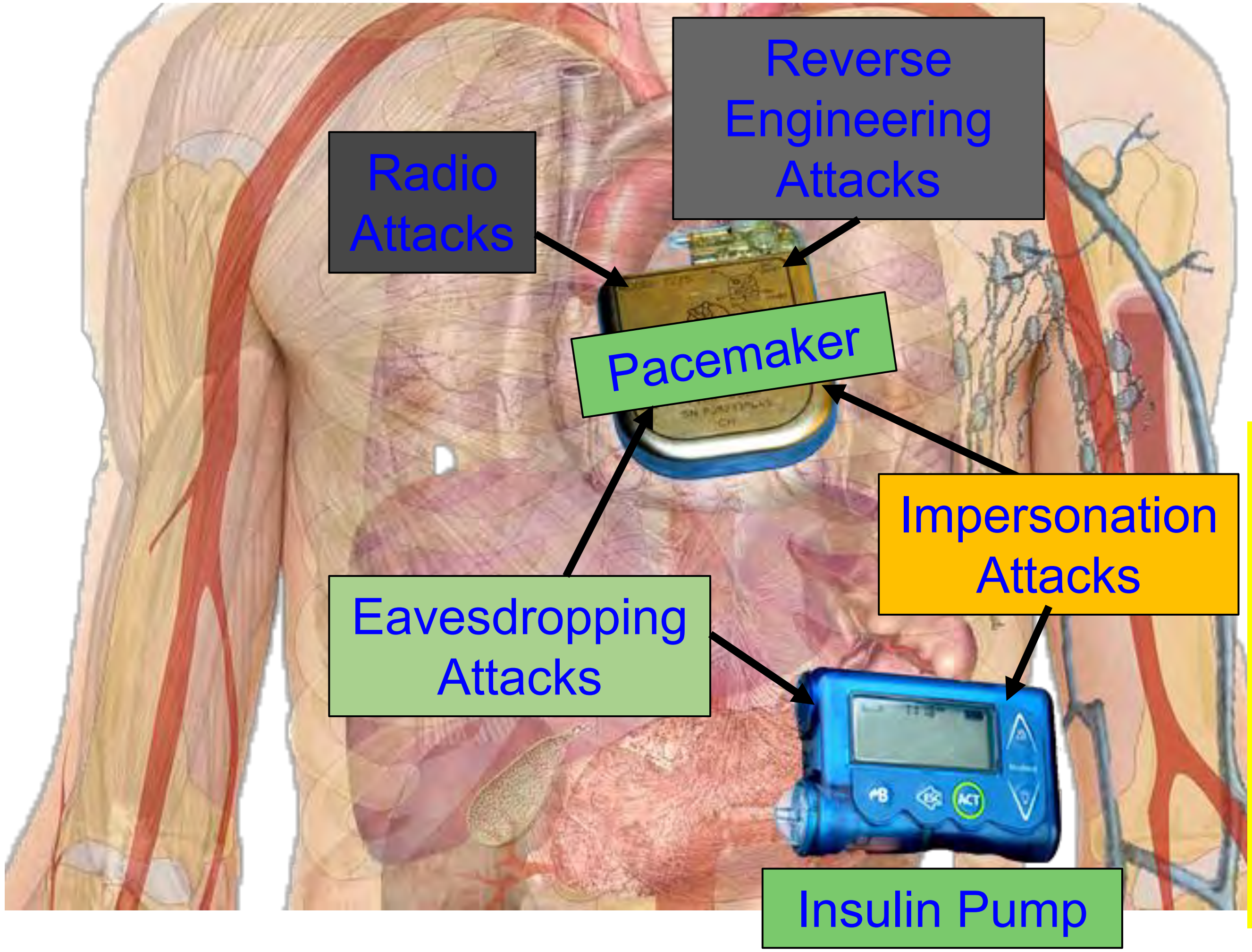
- IT infrastructure may be well protected rooms
- Limited variety of IT network devices
- Millions of IT devices
- Significant computational power to run heavy-duty security solutions
- IT security breach can be costly

IoT Security

- 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 Security of Consumer Electronics, Electronic Systems, IoT, CPS, etc. needs Energy and affects performance.

Security Measures in Healthcare Cyber-Physical Systems is Hard



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

Implantable and Wearable Medical Devices (IWMDs) -- Battery Characteristics:

→ Longer life
→ Safer
→ Smaller size
→ Smaller weight

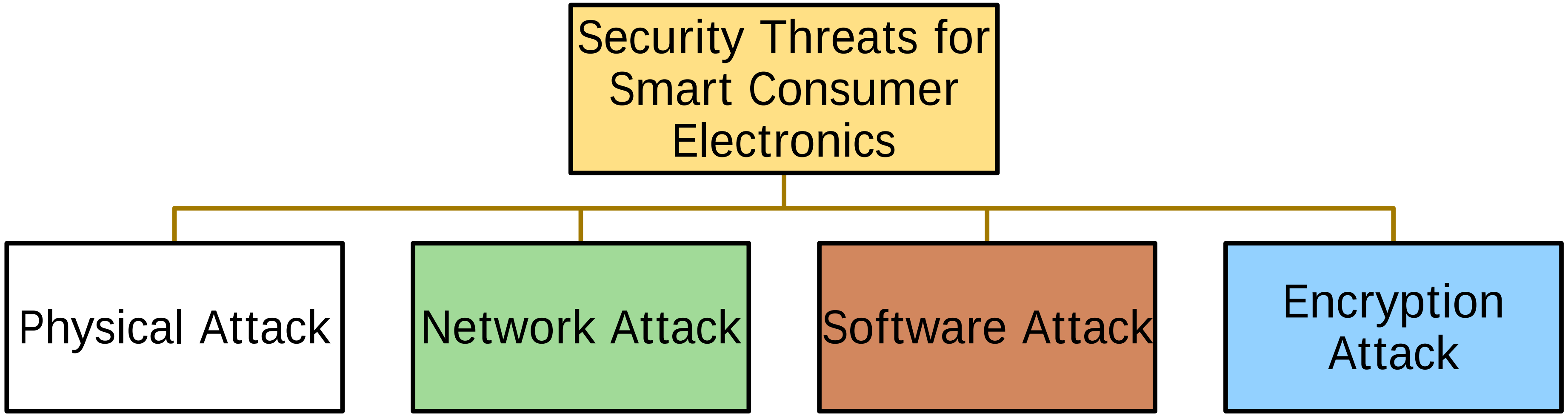
Security in the Internet of Things

"S" in IoT stands for Security... And yes, I'm aware there's no "S" in IoT.

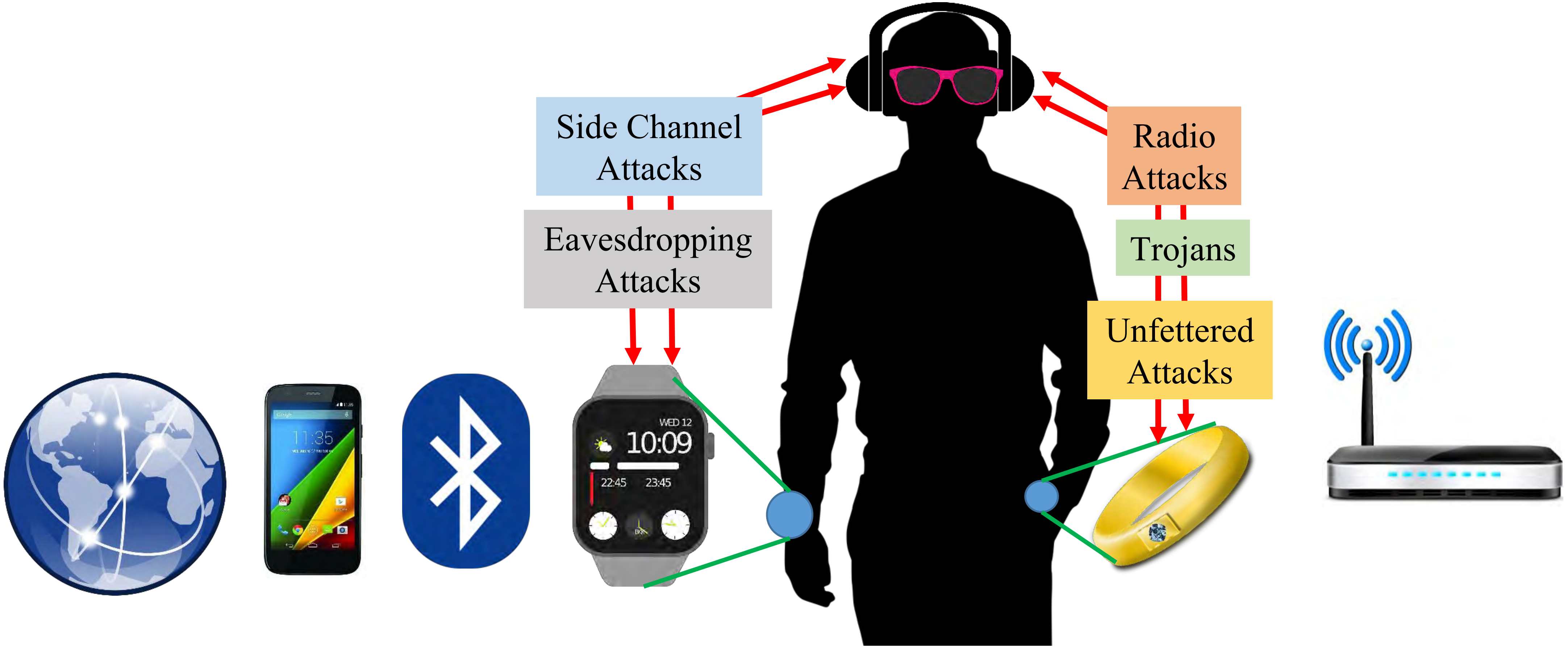
-Oleg Šelajev

Source: https://www.cnet.com/news/iot-attacks-hacker-kaspersky-are-getting-worse-and-no-one-is-listening/

Security Threats in the IoT



Attacks on IoT Devices



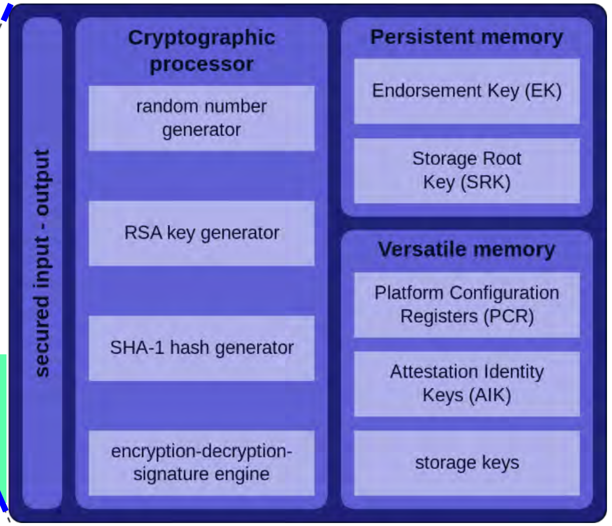
What is Hardware Assisted Security

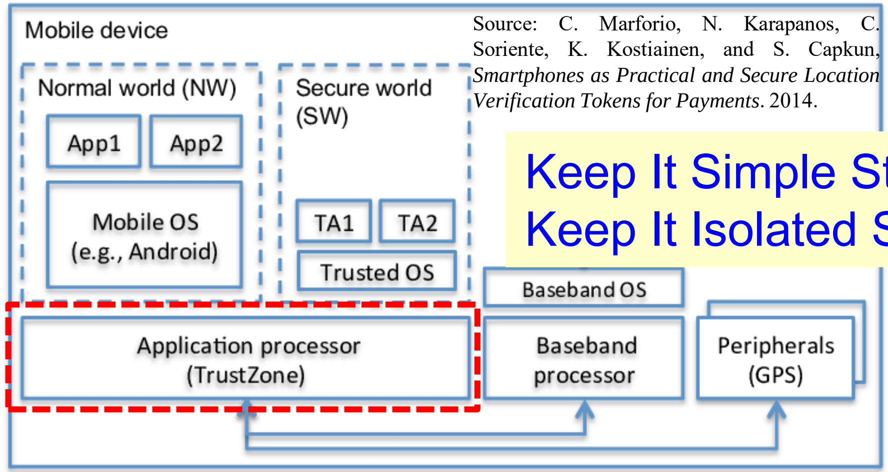
- Hardware components are used for performing cryptographic processes.
- Things in IoT does not have processing power – they are low power low performance devices.
- Cryptographic keys require enormous memory to store the keys which IoT architectures do not have.
- Additional Hardware Accelerators can help in improving the performance of operation.

Hardware Security 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)

Hardware-Assisted Security (HAS)

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

Privacy by Design (PbD)

Security/Secure by Design (SbD)

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

IR Hardware Security

Memory Protection

Digital Core IP Protection

Source: Mohanty ICCE 2018 Panel

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: Security/Protection provided by the hardware: for information being processed by a CE system, for hardware itself, and/or for the CE system.

Physical Unclonable Functions (PUF)

Lock and Key

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

Lock and Key

Problem???

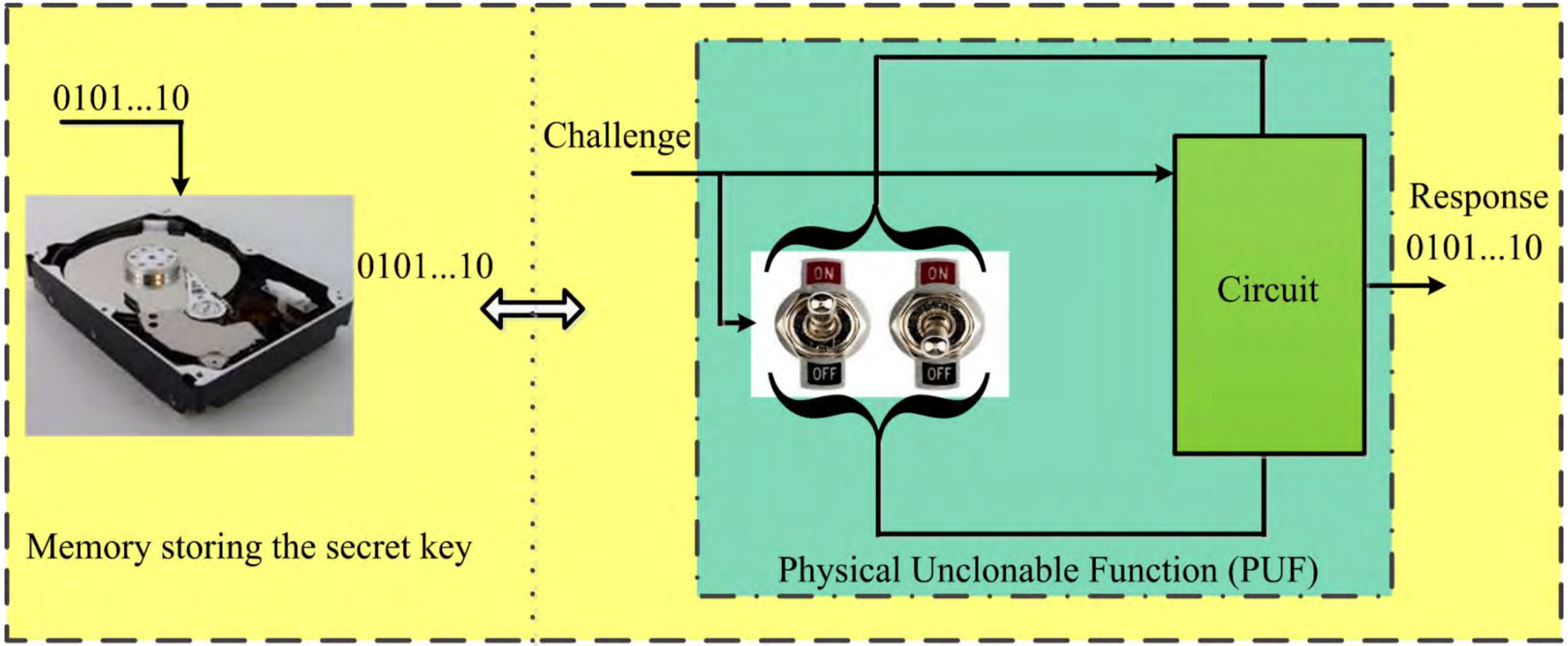
Novel Contributions

- Power-Optimized Hybrid Oscillator Arbiter Physical Unclonable Functions.
- Speed-Optimized Hybrid Oscillator Arbiter Physical Unclonable Functions.
- DL-FET-Based Hybrid Oscillator Arbiter Physical Unclonable Functions.
- Reconfigurable Robust Hybrid Oscillator Arbiter Physical Unclonable Functions.

Physical Unclonable Functions

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

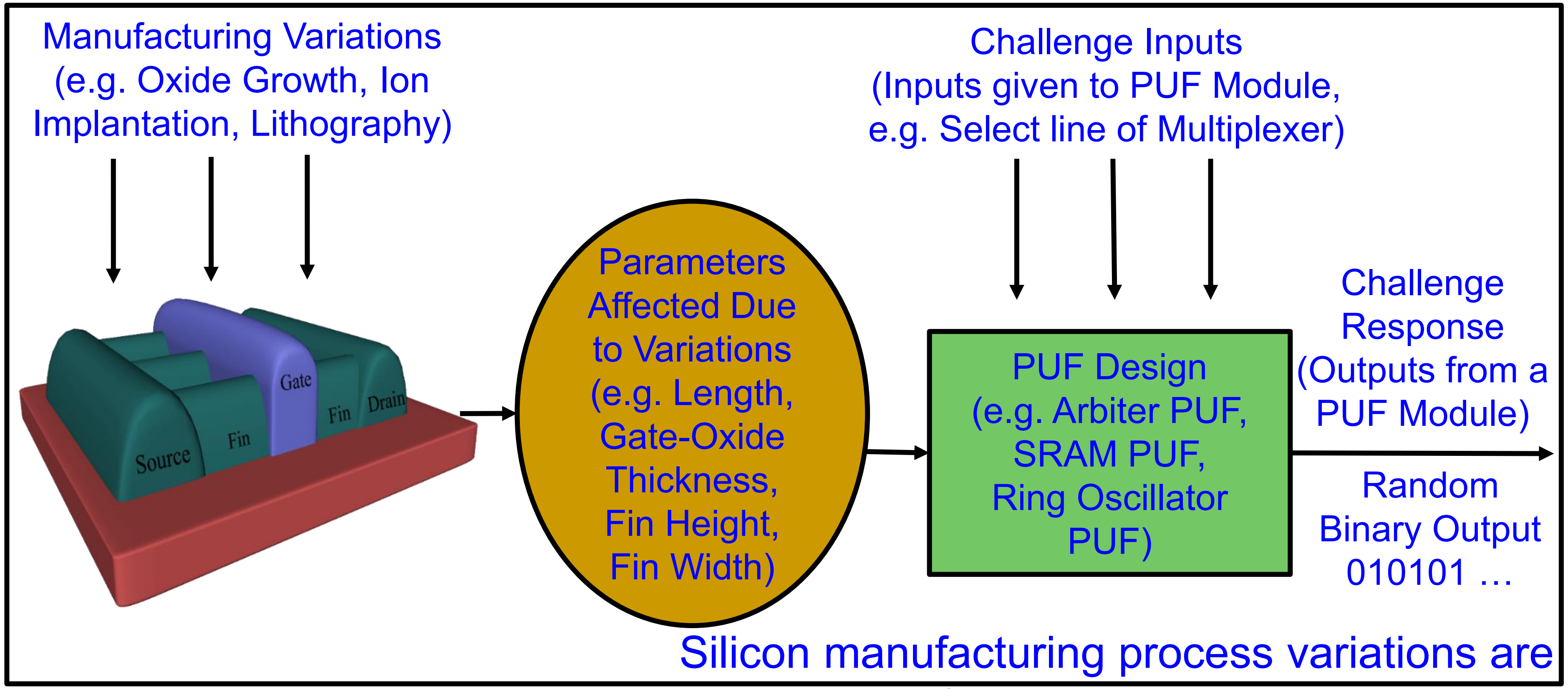
PUFs Don't Store Keys



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

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

PUF - Principle

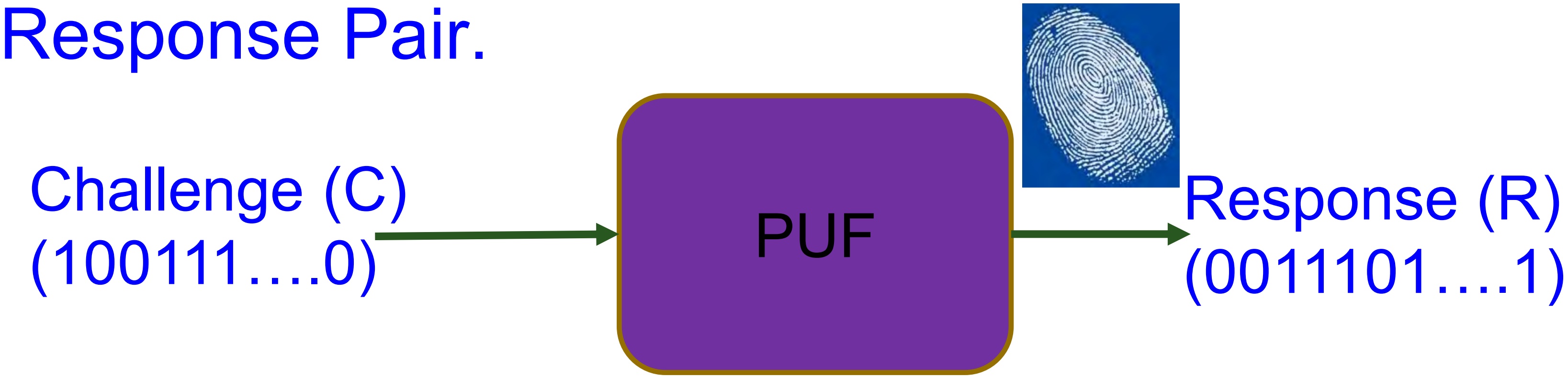


Silicon manufacturing process variations are turned into a feature rather than a problem.

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

Physical Unclonable Functions (PUFs)

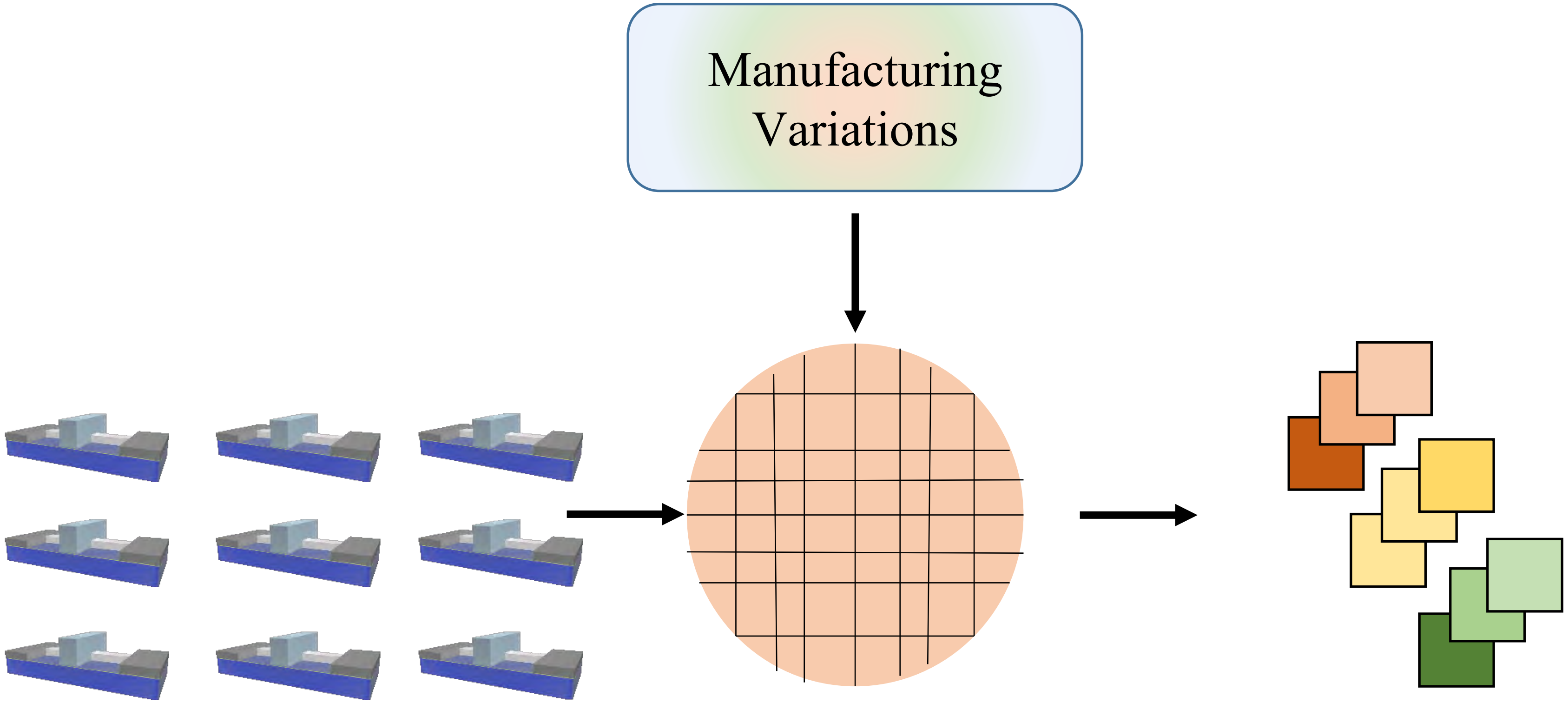
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

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

How PUFs Work?

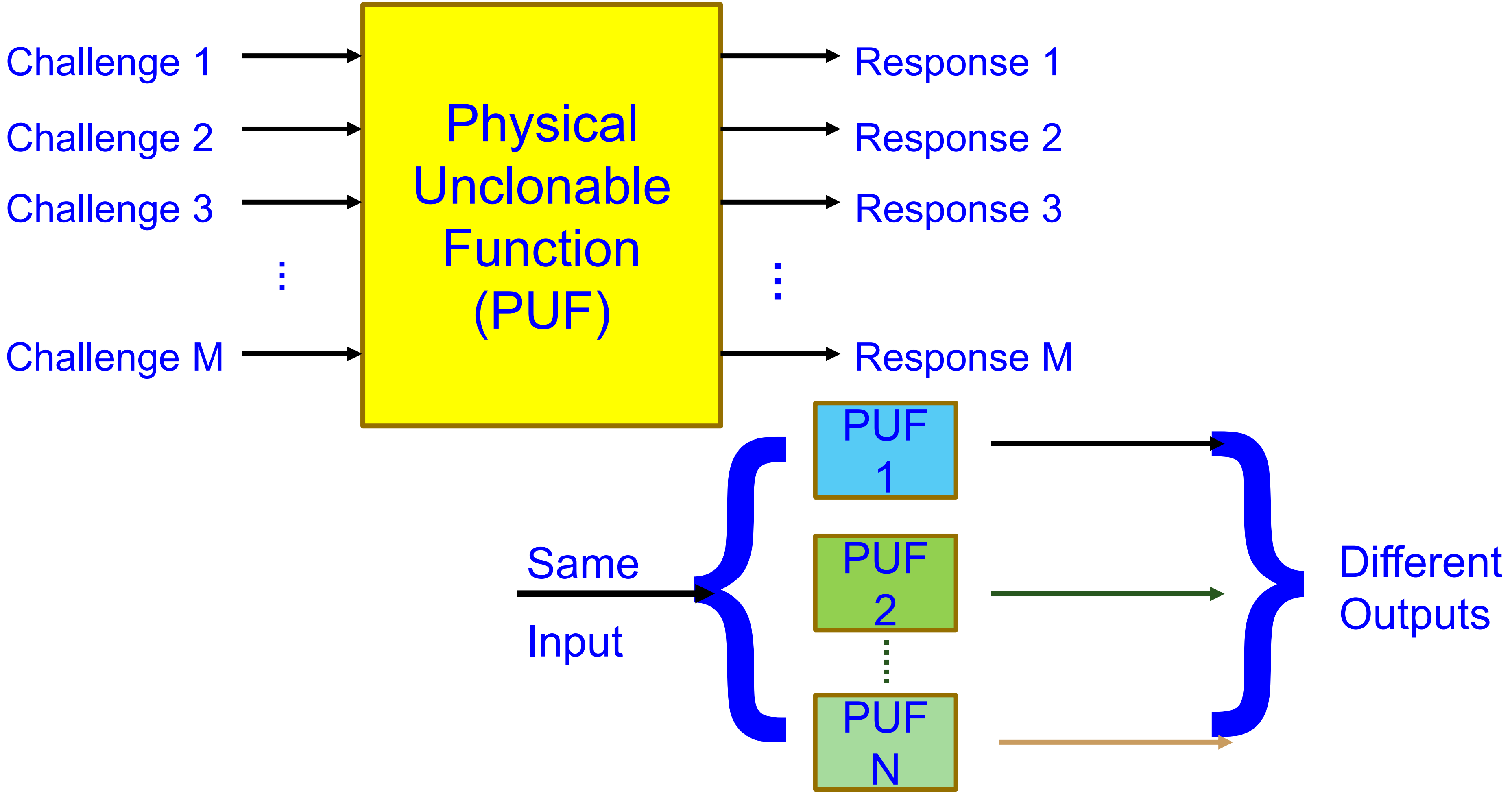


Transistors

Silicon wafer with manufacturing variations

Different PUF ICs with manufacturing variations

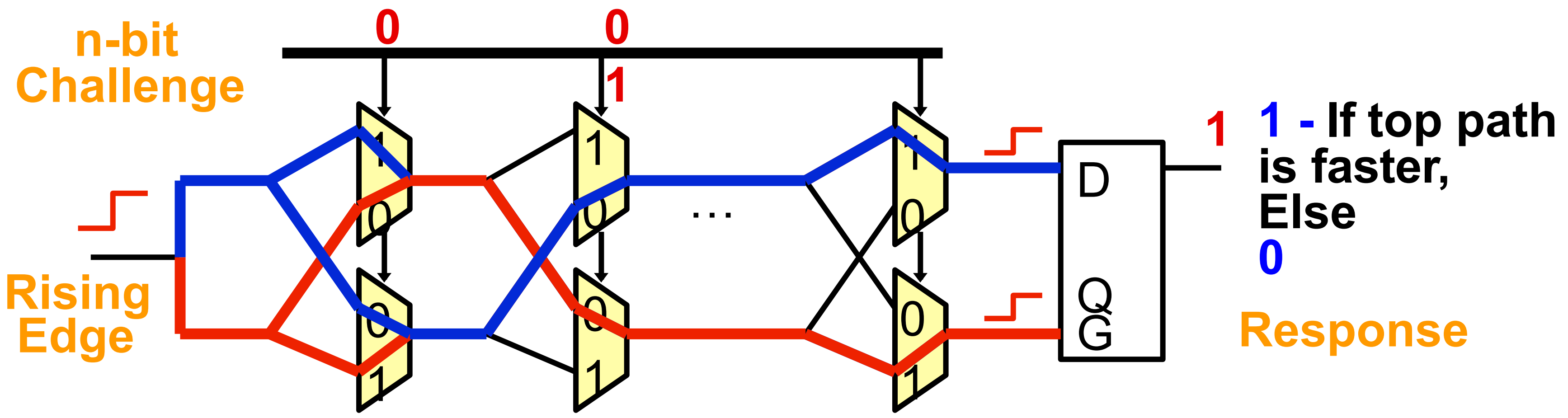
Principle of Generating Multiple Random Response using PUF



Why PUFs?

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

Principle of Generating Random Response using PUF

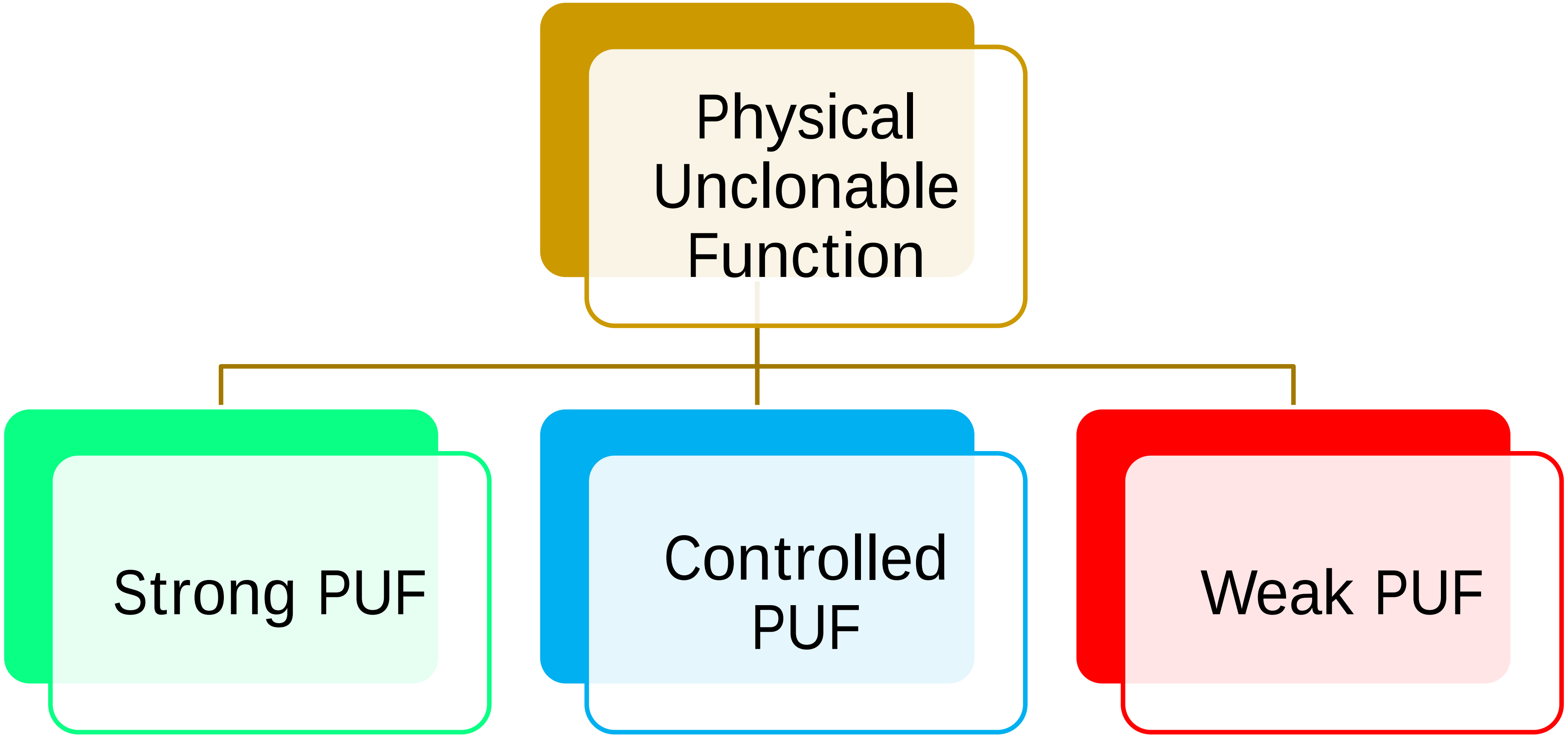


Compare two paths with an identical delay in design

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

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

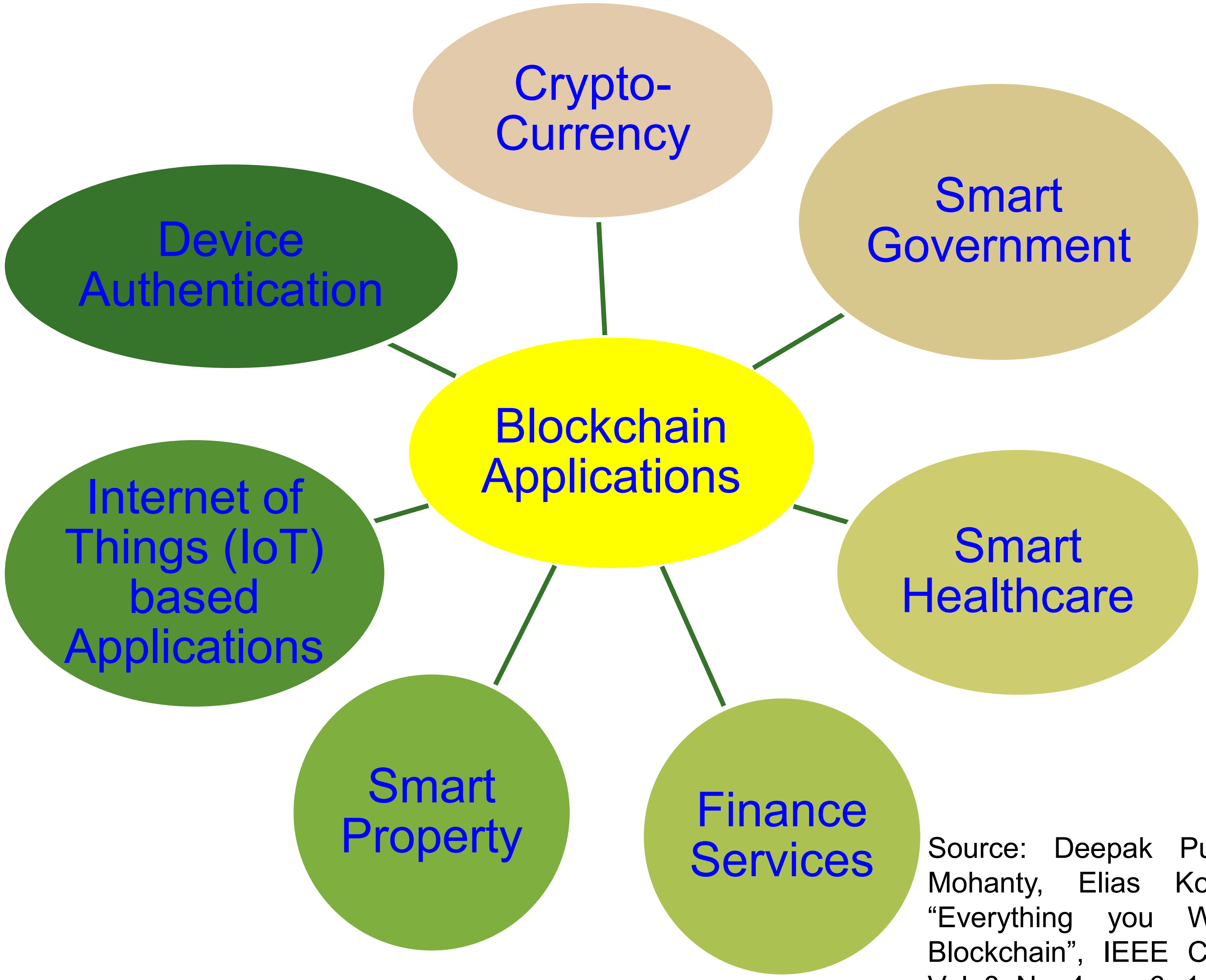
Types of PUF



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

Blockchain

Blockchain Applications



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

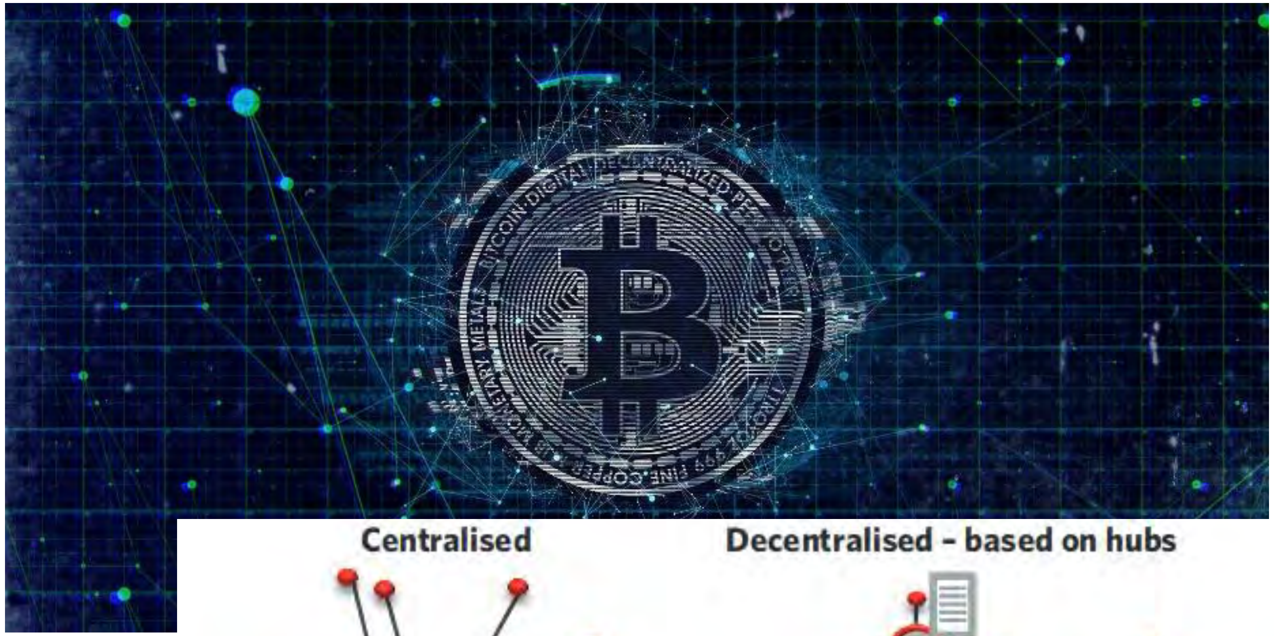
Blockchain Technology

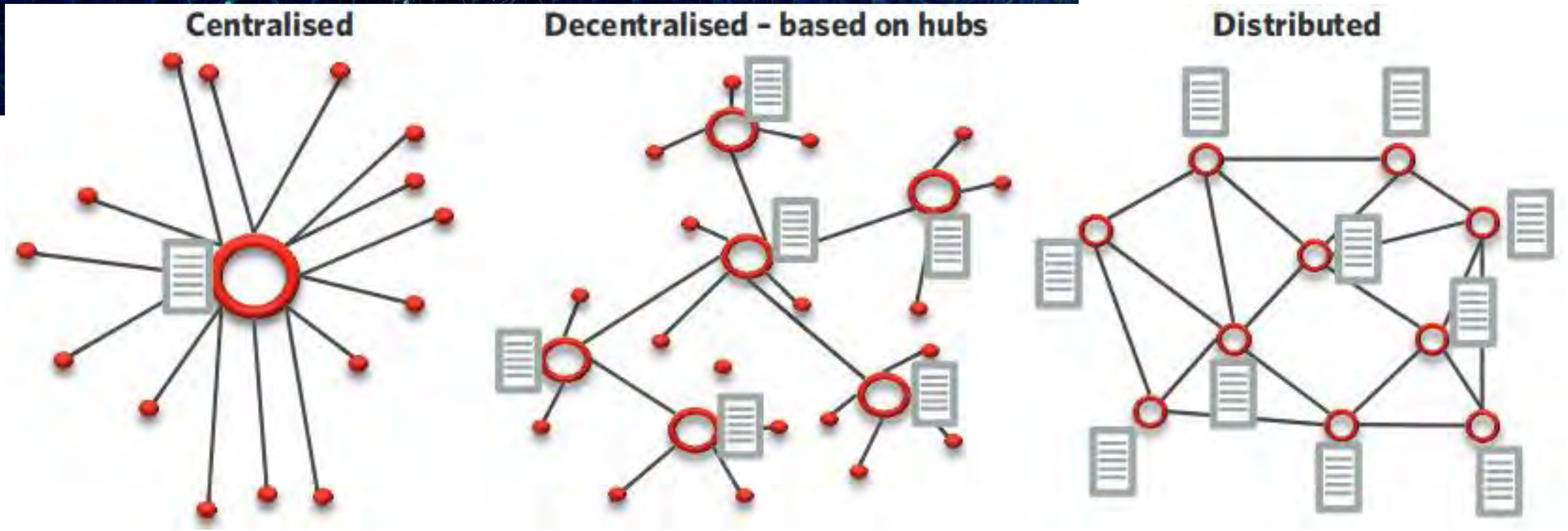
- Introduced by Satoshi Nakamoto in 2008 for cryptocurrency.
- Bitcoin first used Blockchain Technology.
- Used for data integrity and user anonymity.
- Once data is added to blockchain, it cannot be altered.

Blockchain Technology

- Uses a distributed ledger.
  - Every person that is in the network have access to all the transactions happened till date.
  - We can see all the transactions happened in Bitcoin since day 1.
  - Every node in the network will have a complete or partial copy of the ledger at their local storage.
- Advantages:
  - No central authority to complete transactions
  - Transparency.
  - Once a transaction is added to the ledger, it cannot be altered as it uses cryptographic hash.

Blockchain Technology





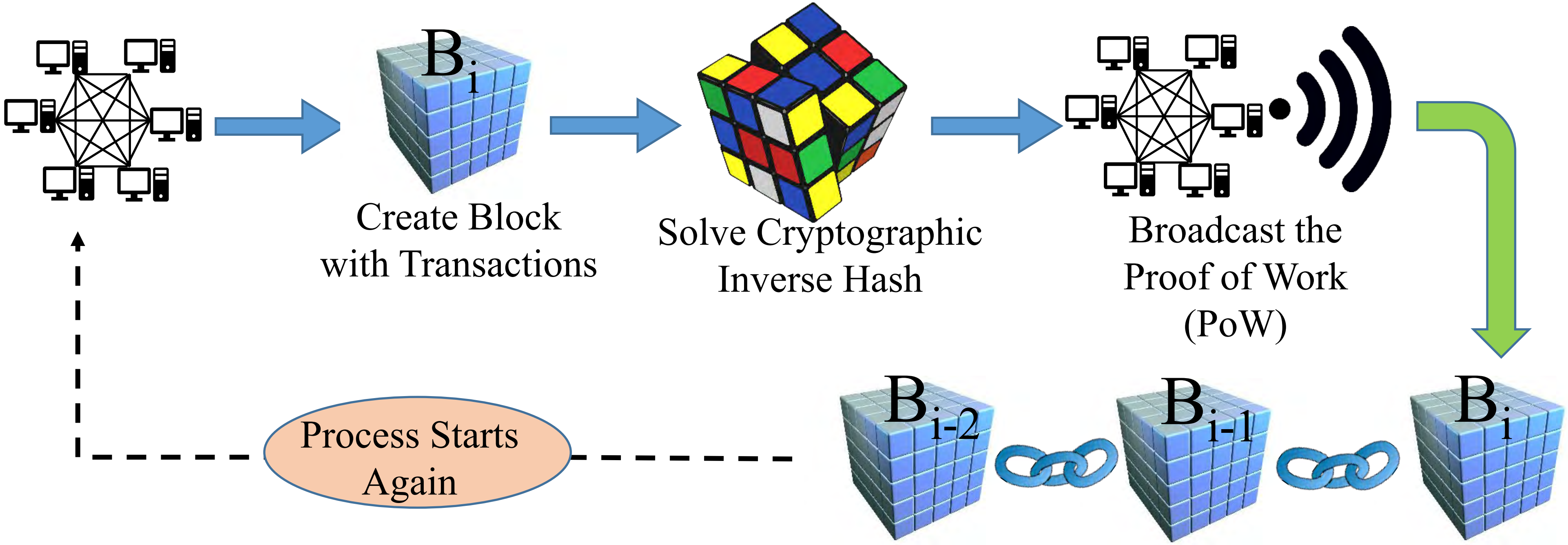
Source: https://icomalta.com/distributed-ledger-technology/

Blockchain – Consensus Algorithm

- No central authority is present in the blockchain.
- So a consensus algorithm is required to complete a transaction.
- Examples of the consensus algorithm
  - Proof of Work (PoW) – used by Bitcoin
  - Proof of Stake (PoS) – used by Etherium
- Multiple transactions are combined to form blocks.
- These blocks of transactions are validated using the consensus algorithm.

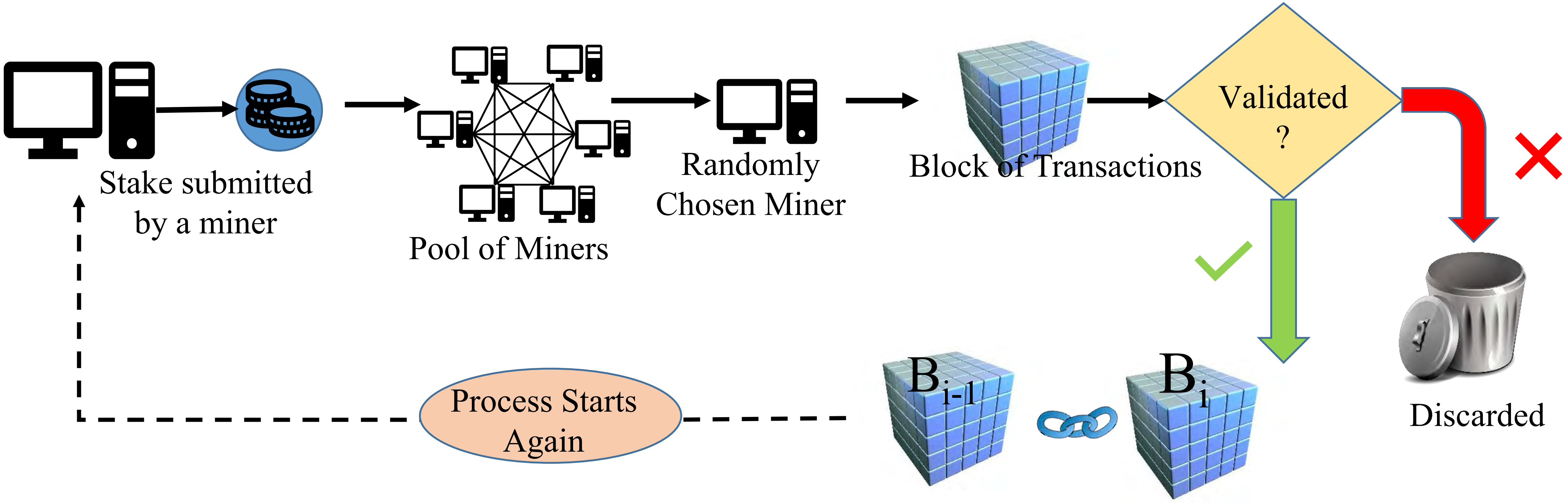
Blockchain – Consensus Algorithm

- Proof of Work



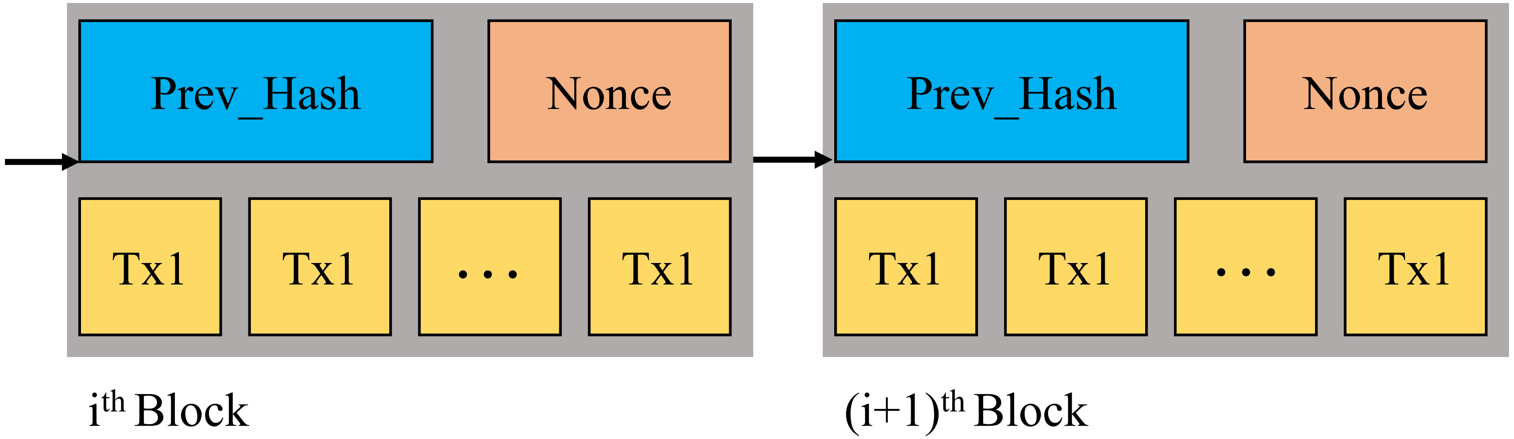
Blockchain – Consensus Algorithm

- Proof of Stake

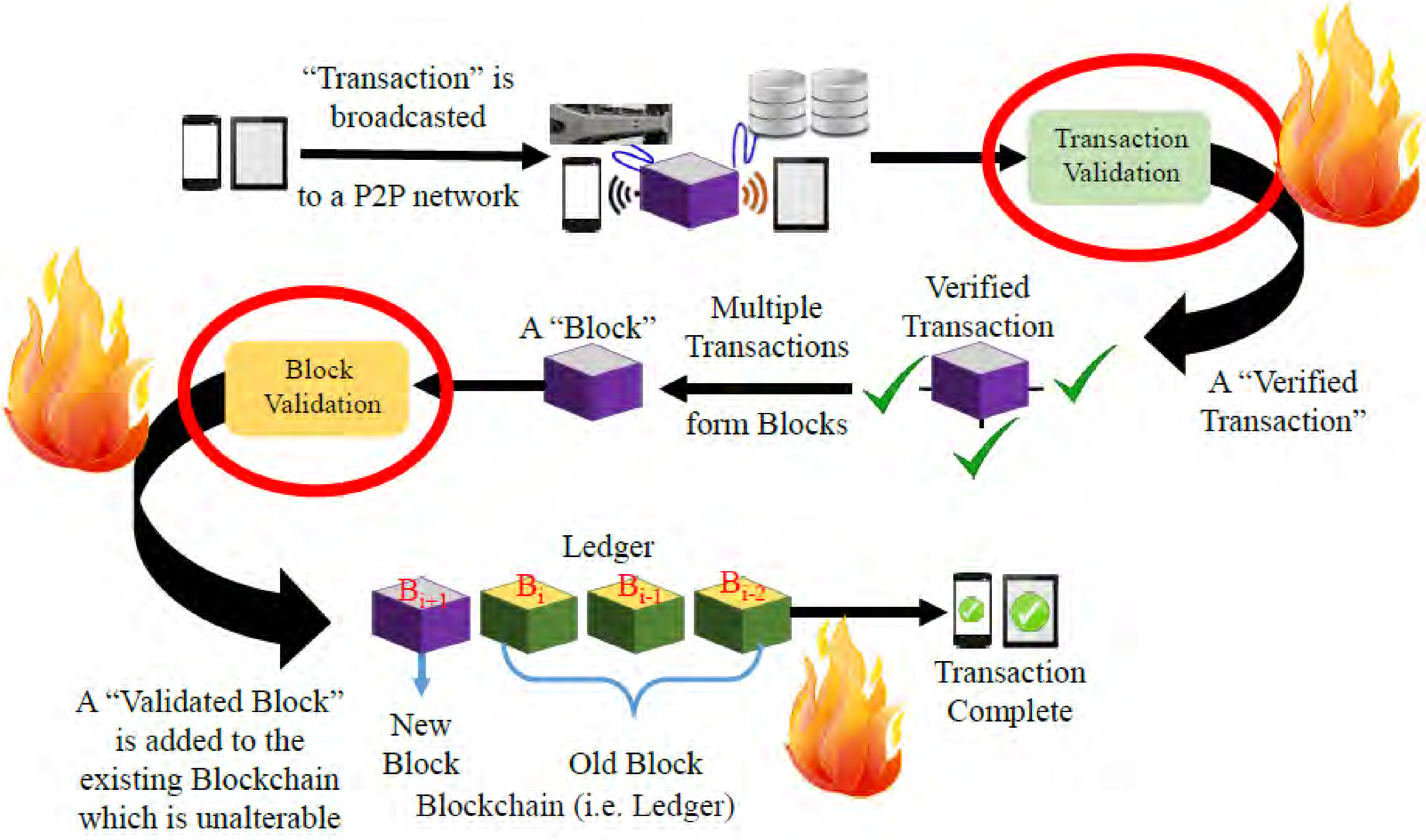


Blockchain – Block Structure

- Proof of Work
- Nonce – reverse hash calculation

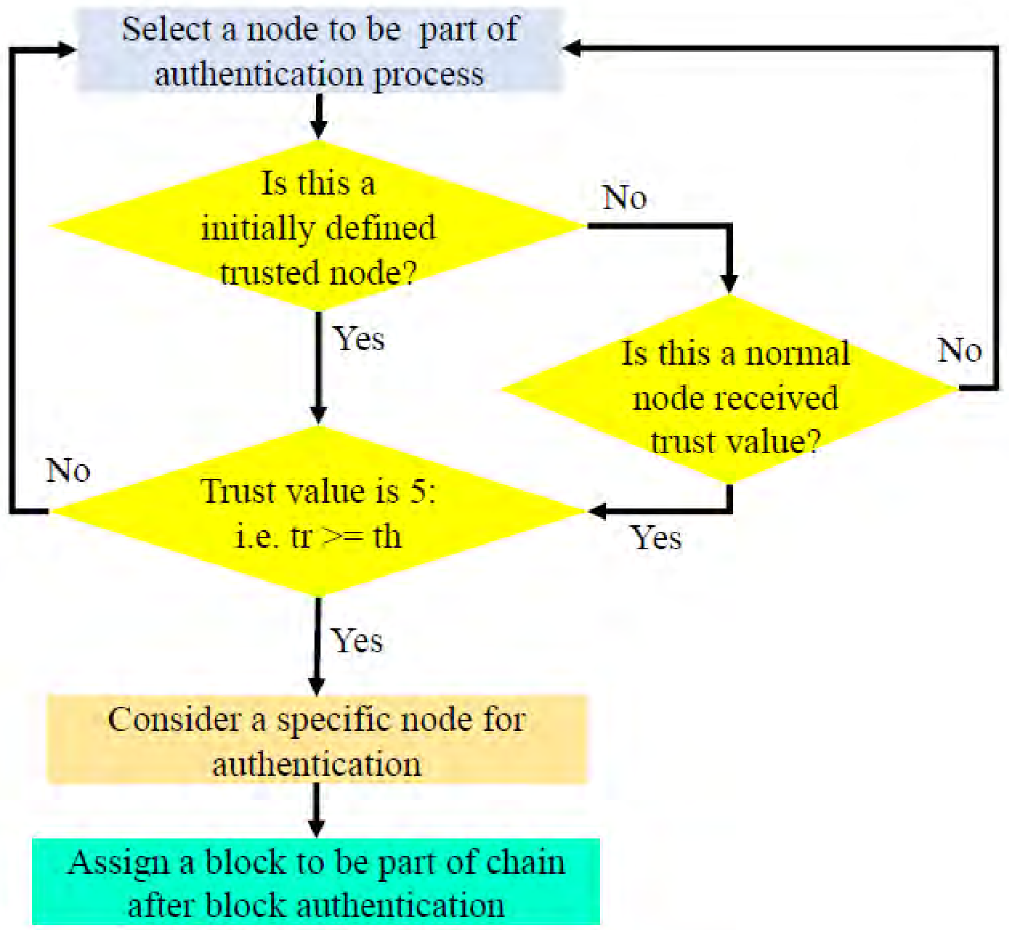


Block Validation Process



Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8662009.

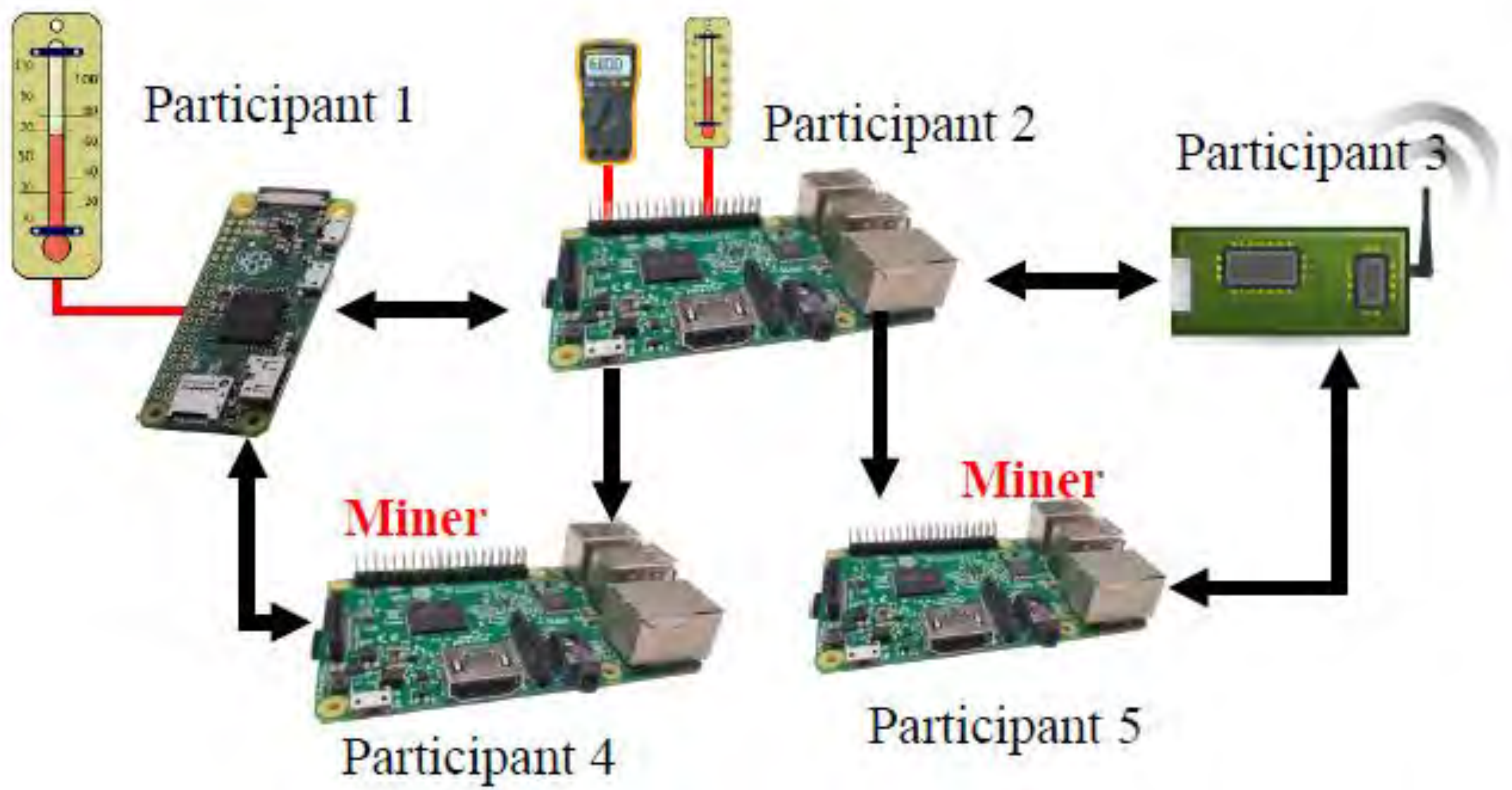
Miner Selection Process



- Successful Validation and authentication of a Block increases the trust value of Miner by 1
- Miners with a low trust value will be removed from the Block Validation process
- Identifying fake Block increases the trust value of miners substantially

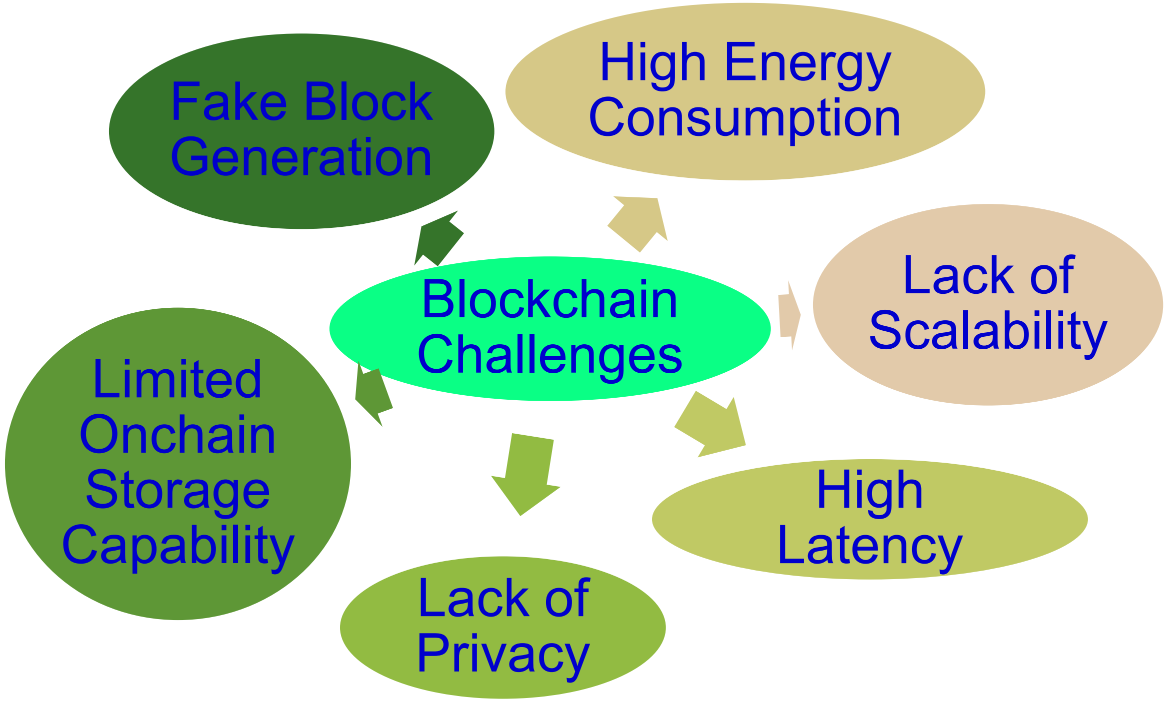
Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8662009.

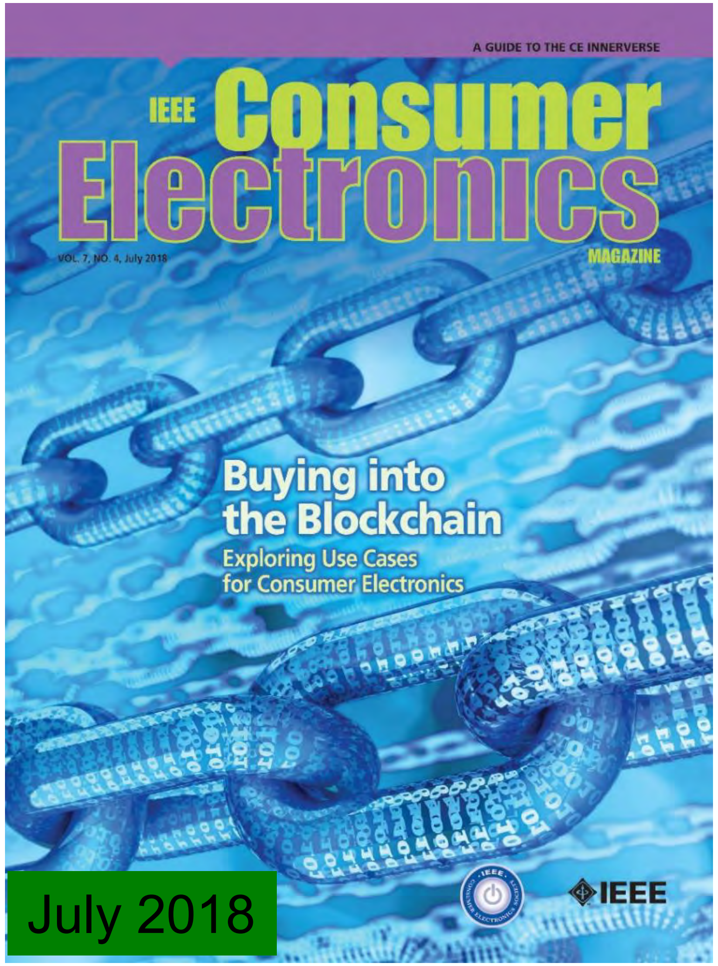
Blockchain for IoT Security



Source: D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp. 1-5, doi: 10.1109/ICCE.2019.8662009.

Blockchain has Many Challenges





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 (CEM)*, 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

=

80,000X

Energy consumption of a credit card processing

Blockchain has Security 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

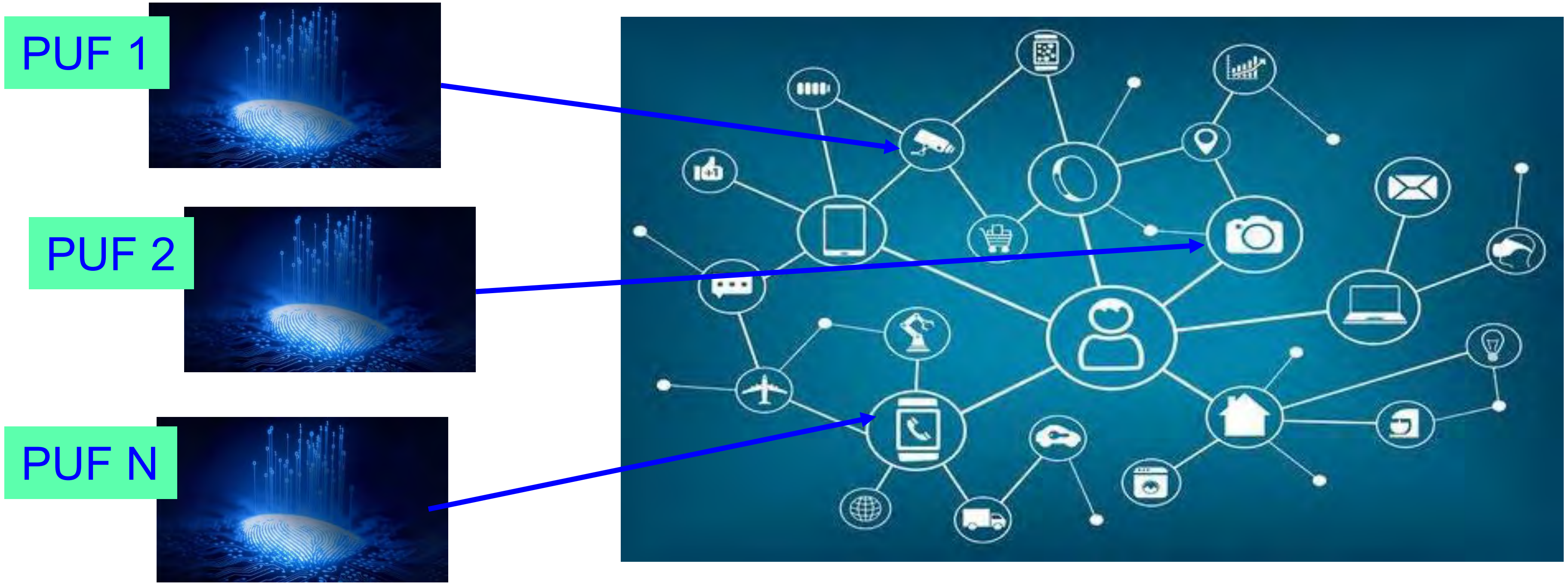
Source: N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 28–34, May 2019.

Blockchain has Serious Privacy Issue

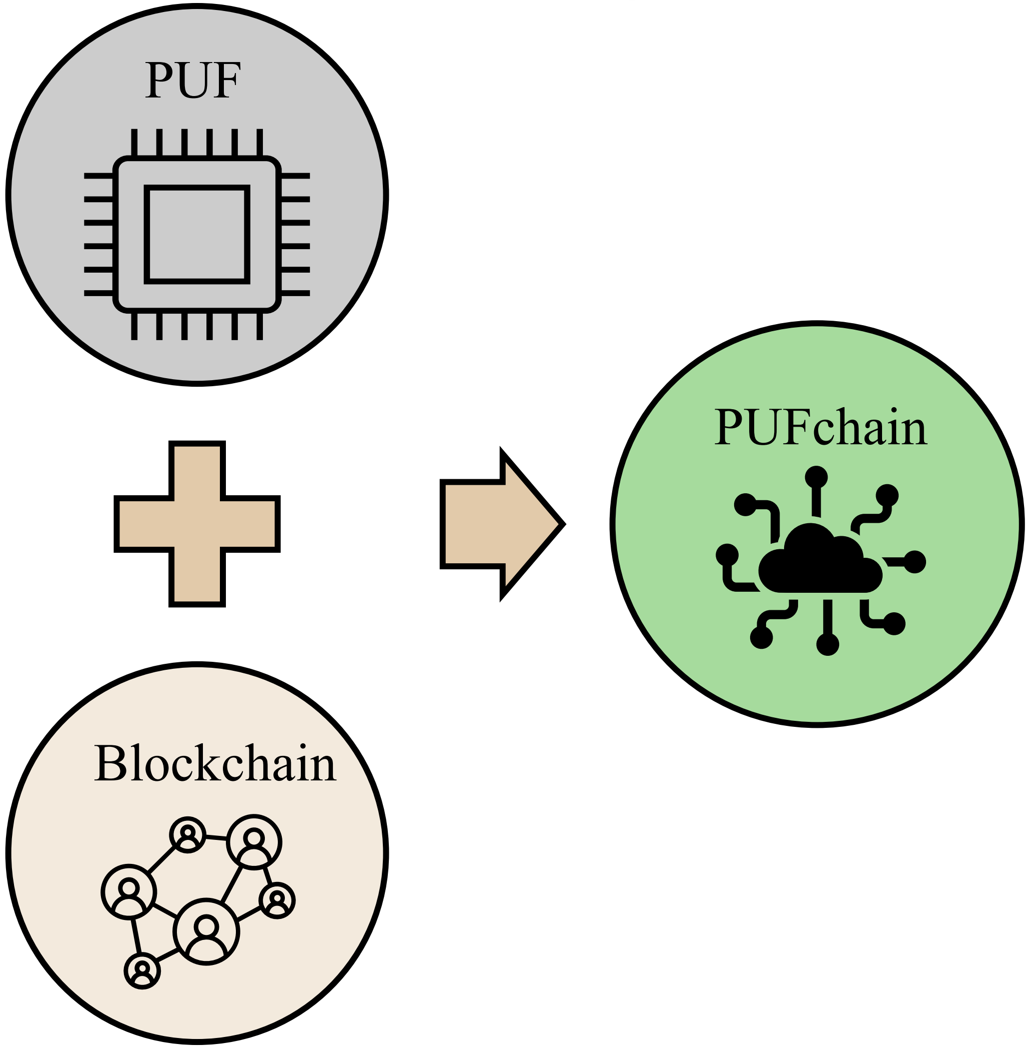
	Bitcoin	Dash	Monero	Verge	PIVX	Zcash
Origin	-	Bitcoin	Bytecoin	Bitcoin	Dash	Bitcoin
Release	January 2009	January 2014	April 2014	October 2014	February 2016	October 2016
Consensus Algorithm	PoW	PoW	PoW	PoW	PoS	PoW
Hardware Mineable	Yes	Yes	Yes	Yes	No	Yes
Block Time	600 sec.	150 sec.	120 sec.	30 sec.	60 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, 1 Sept. 2019.

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

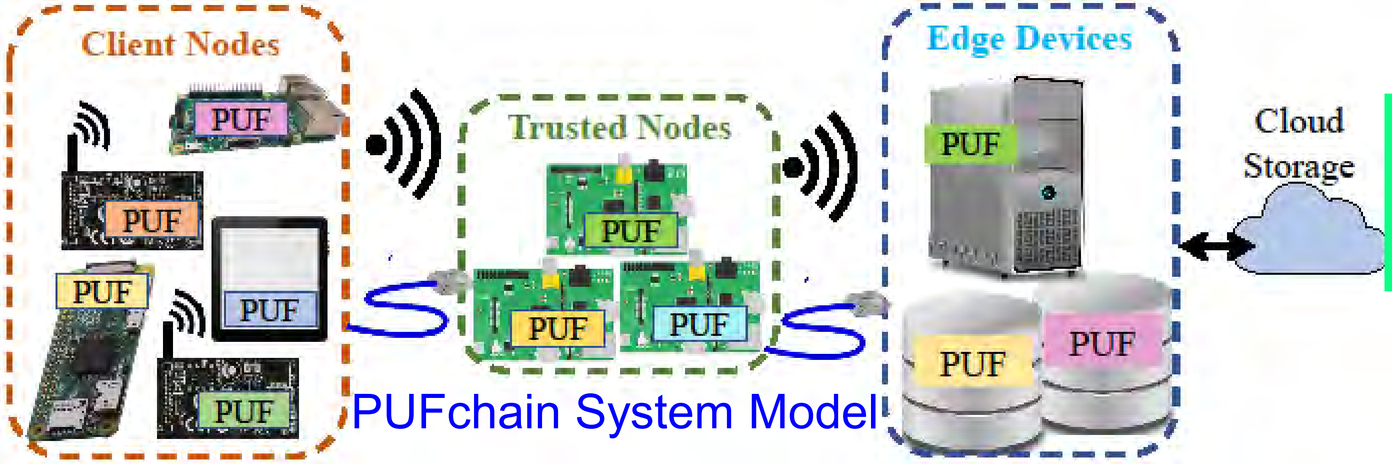


PUFchain



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

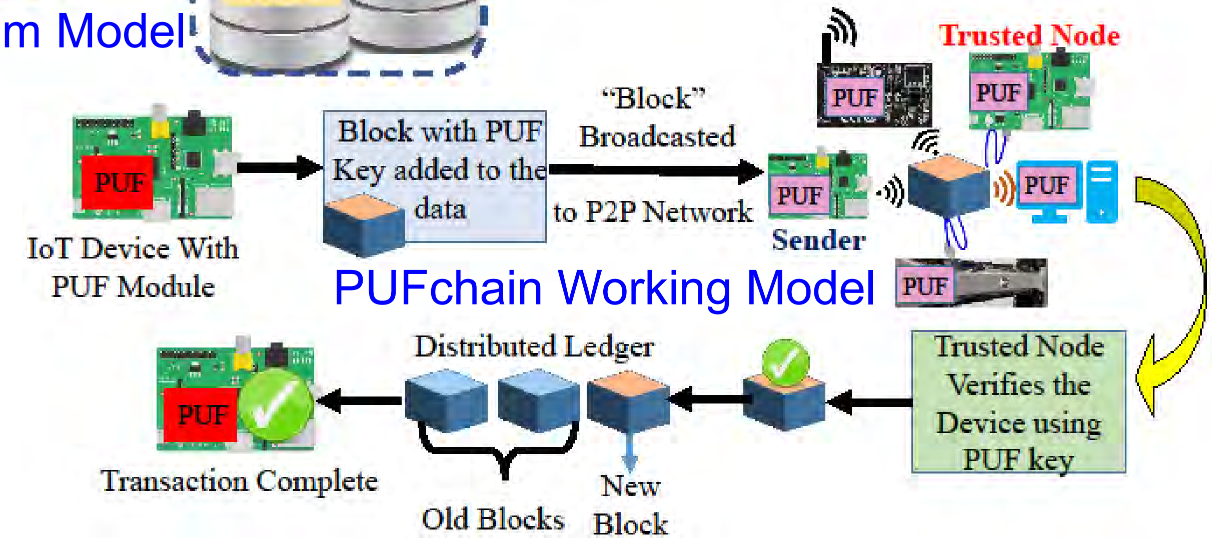
PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

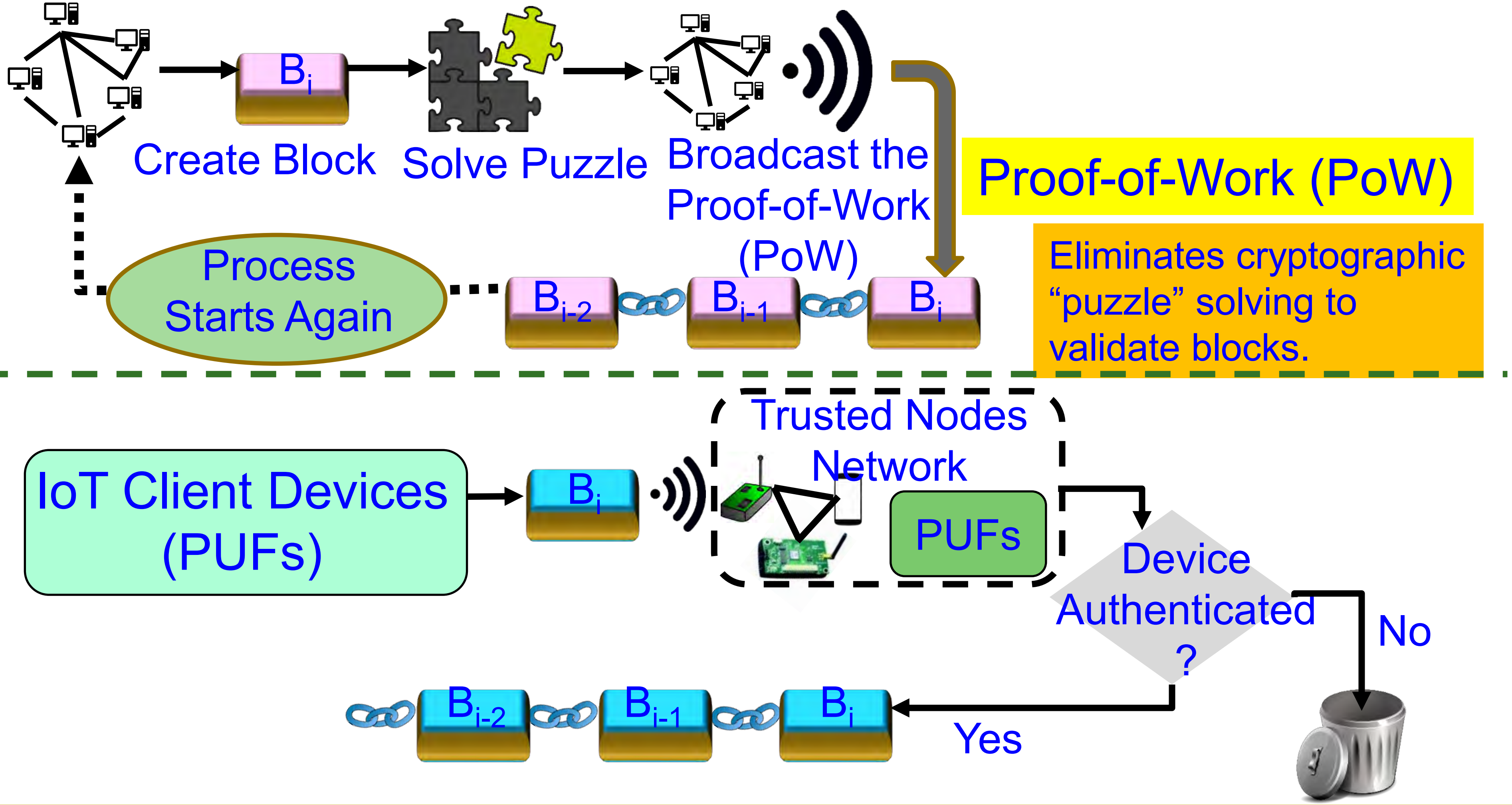
PUFChain 2 Modes:
(1) PUF Mode and
(2) PUFChain Mode



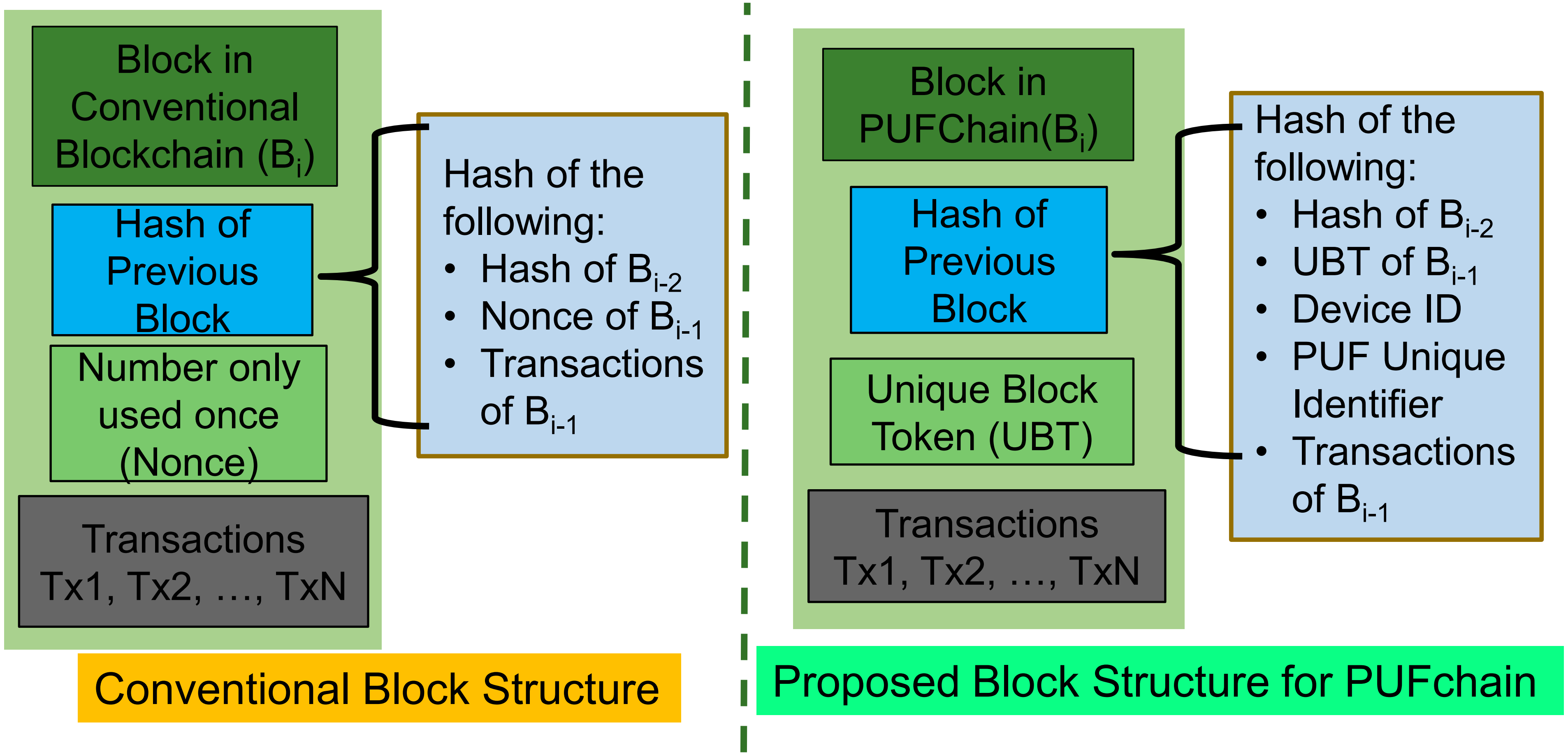
PUFchain Working Model

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. XX, No. YY, ZZ 2020, pp. Accepted.

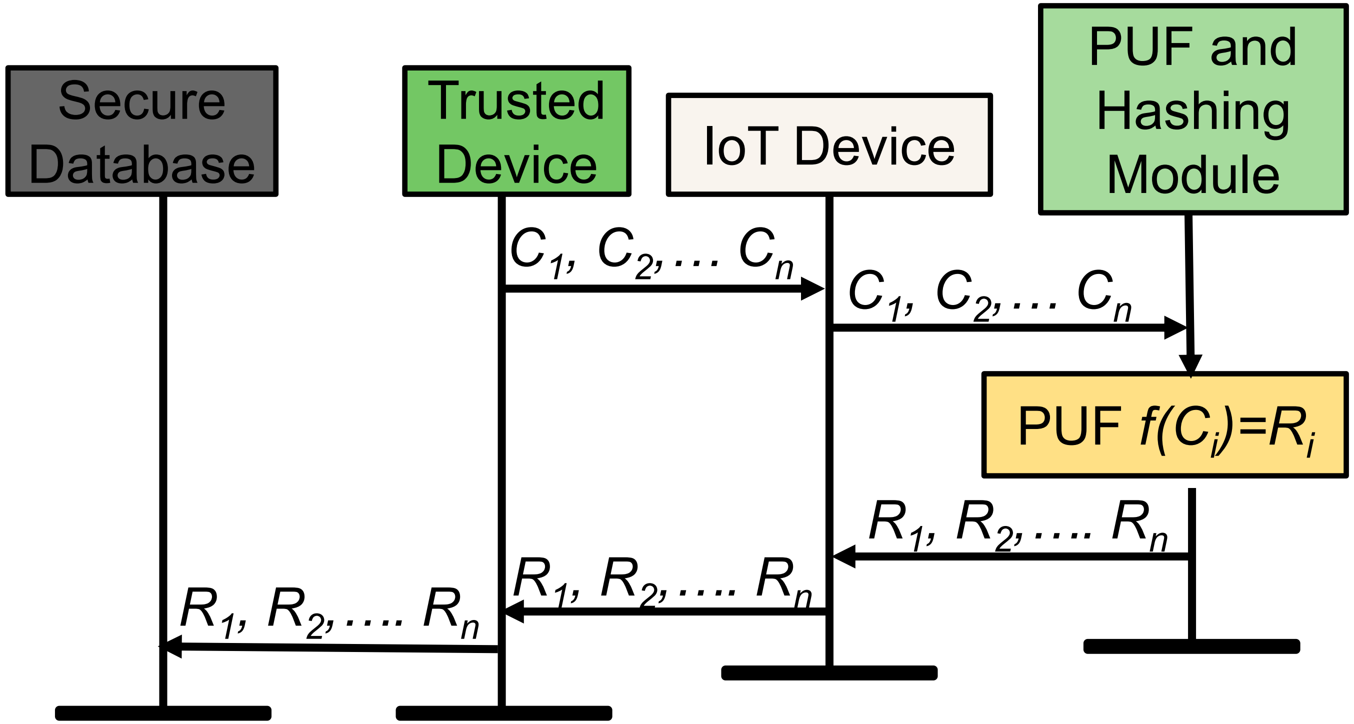
Our Proof-of-PUF-Enabled-Authentication (PoP)



PUFchain: Proposed New Block Structure

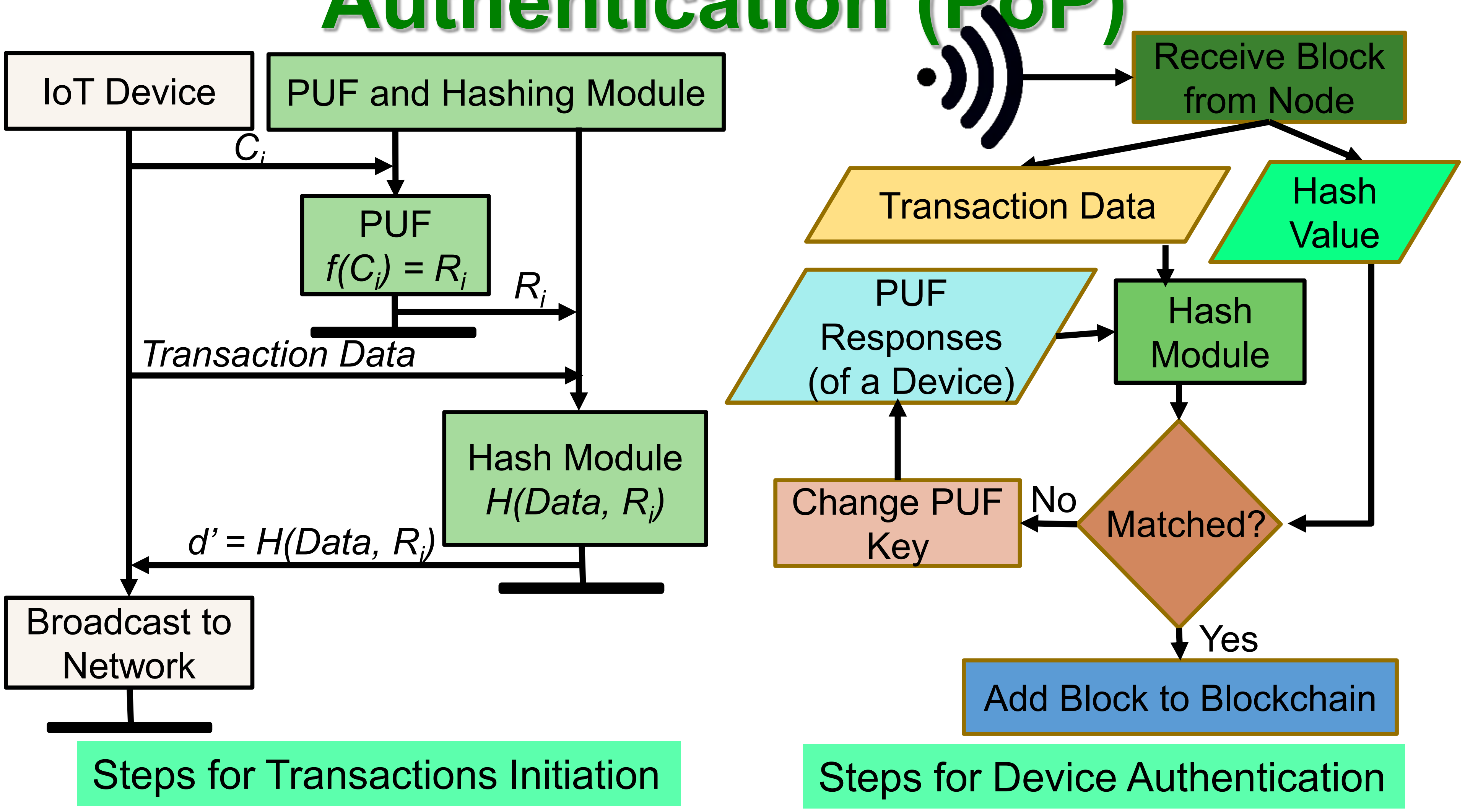


PUFchain: Device Enrollment Steps

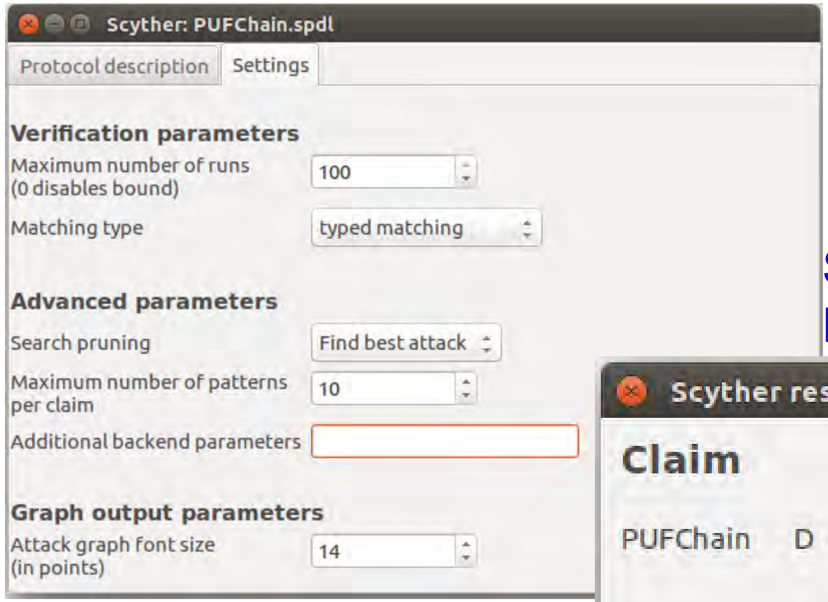


Device Enrollment Steps

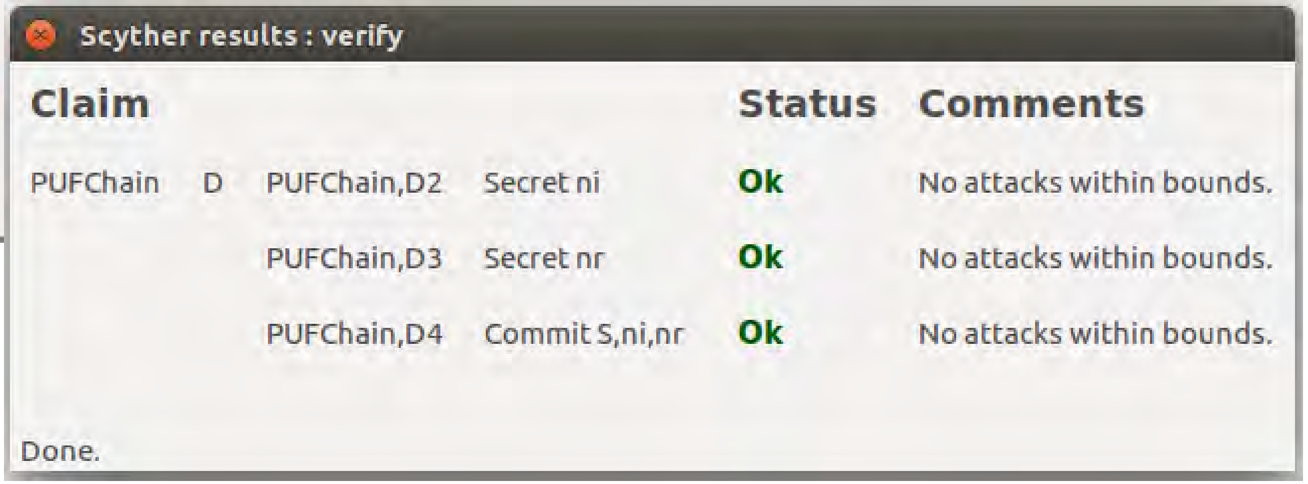
Steps of Proof-of-PUF-Enabled-Authentication (PoP)



PUFchain Security Validation

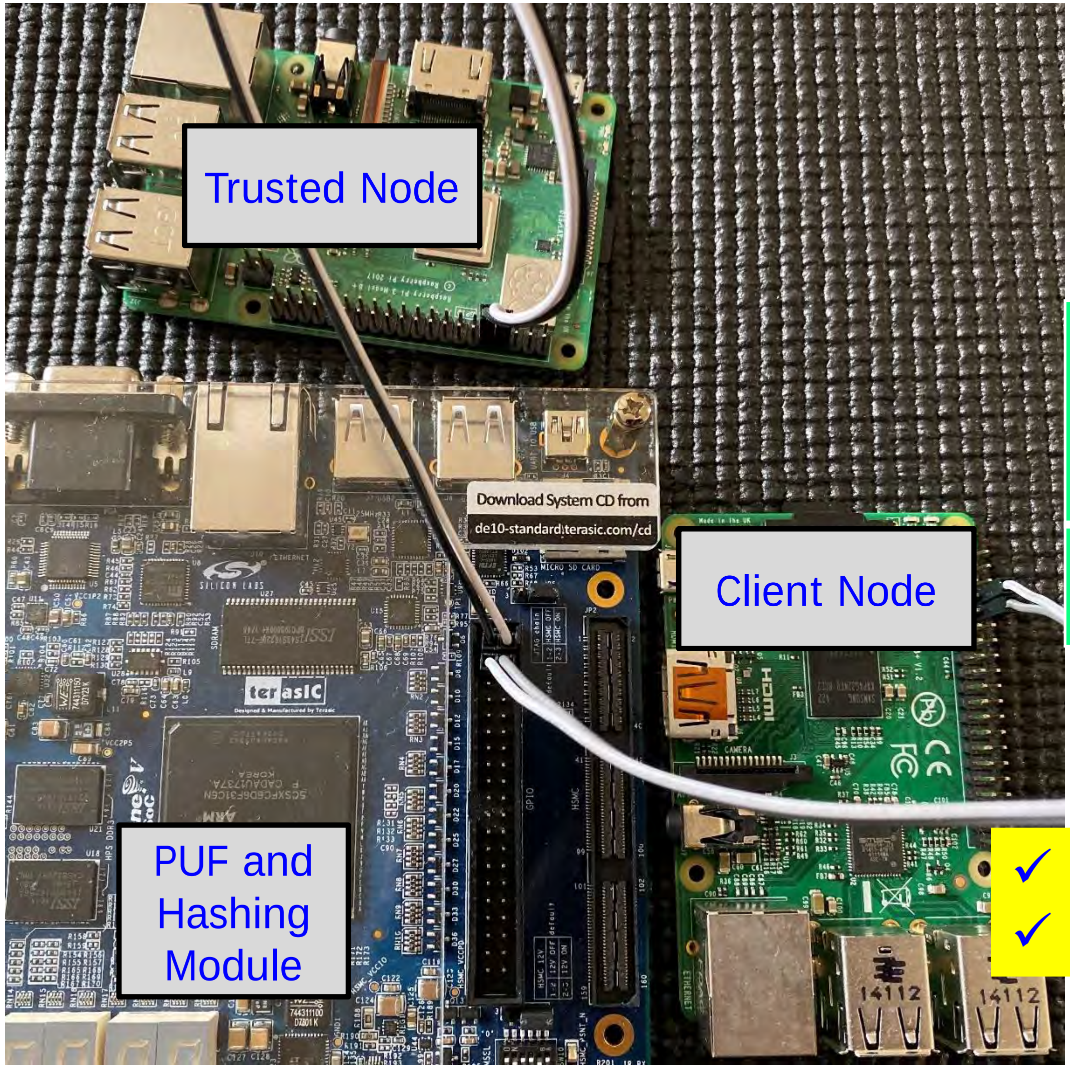


S - the source of the block
D - the miner or authenticator node in the networks



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

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

Conclusion

Conclusion

- Security risks are many in the world.
- Cryptography is one of the major components of our day-to-day life.
- Cryptography can help protect security and privacy of devices.
- Hardware Assisted Cryptography are used for low power low performance devices such as IoT architectures.

Conclusion

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

Key References

- S. P. Mohanty, V. P. Yanambaka, E. Kougianos and D. Puthal, "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 8-16, 1 March 2020, doi: 10.1109/MCE.2019.2953758.
- S. Joshi, S. P. Mohanty and E. Kougianos, "Everything You Wanted to Know About PUFs," in *IEEE Potentials*, vol. 36, no. 6, pp. 38-46, Nov.-Dec. 2017, doi: 10.1109/MPOT.2015.2490261.
- 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," in *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388-397, Aug. 2019, doi: 10.1109/TCE.2019.2926192.
- D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything you Wanted to Know about the Blockchain”, IEEE Consumer Electronics Magazine, Vol. 8, No. 4, pp. 6--14, 2018.
- V. P. Yanambaka, A. Abdelgawad and K. Yelamarthi, "PIM: A PUF-Based Host Tracking Protocol for Privacy Aware Contact Tracing in Crowded Areas," in *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 90-98, 1 July 2021, doi: 10.1109/MCE.2021.3065215.
- P. Sundaravadivel, E. Kougianos, S. P. Mohanty and M. K. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health," in *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18-28, Jan. 2018, doi: 10.1109/MCE.2017.2755378.