PUFchain: Hardware-Assisted Scalable Blockchain

Presenter: Laavanya Rachakonda

P .Yanambaka[1], S. P. Mohanty[2], E. Kougianos[3] , and D. Puthal[4]

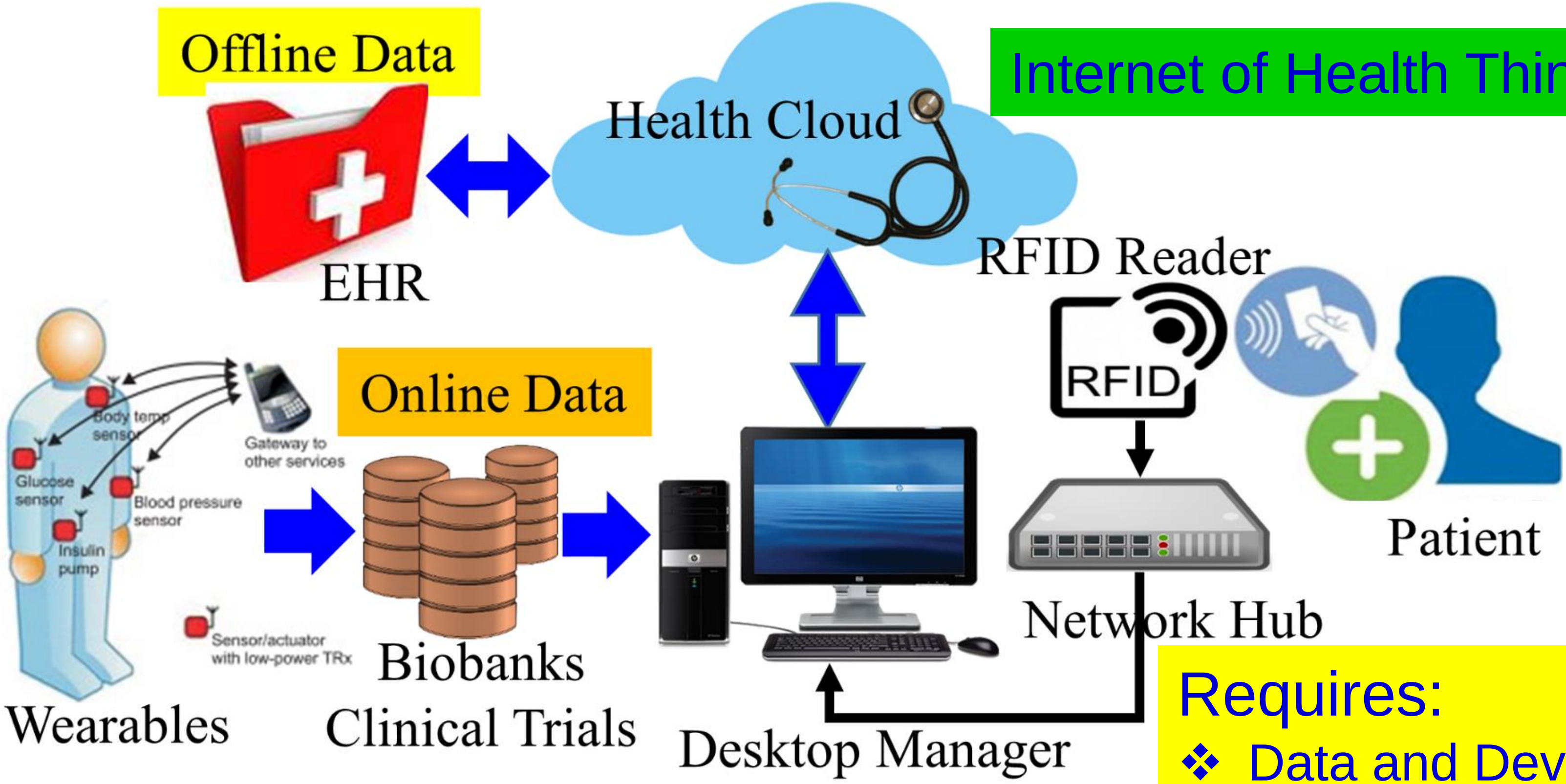
Central Michigan University, USA[1], University of North Texas, Denton, TX 76203, USA.[2,3] and Newcastle University, UK[4].

Email: yanam1v@cmich.edu[1], saraju.mohanty@unt.edu[2] , elias.kougianos@unt.edu[3] and Deepak.Puthal@newcastle.ac.uk[4]

Outline of Talk

- IoT, IoMT, IoE, Smart cities
- Cyber physical systems- Healthcare CPS
- Attacks on Embedded systems- Healthcare, IoT Security
- Fake Data and Fake Hardware
- Blockchain Technology –applications, challenges, need
- Hardware Assisted Security- PUF
- PUFchain- implementation and validation
- Conclusions and Future Research

Internet of Medical Things (IoMT)



Internet of Health Things (IoHT)

Requires:

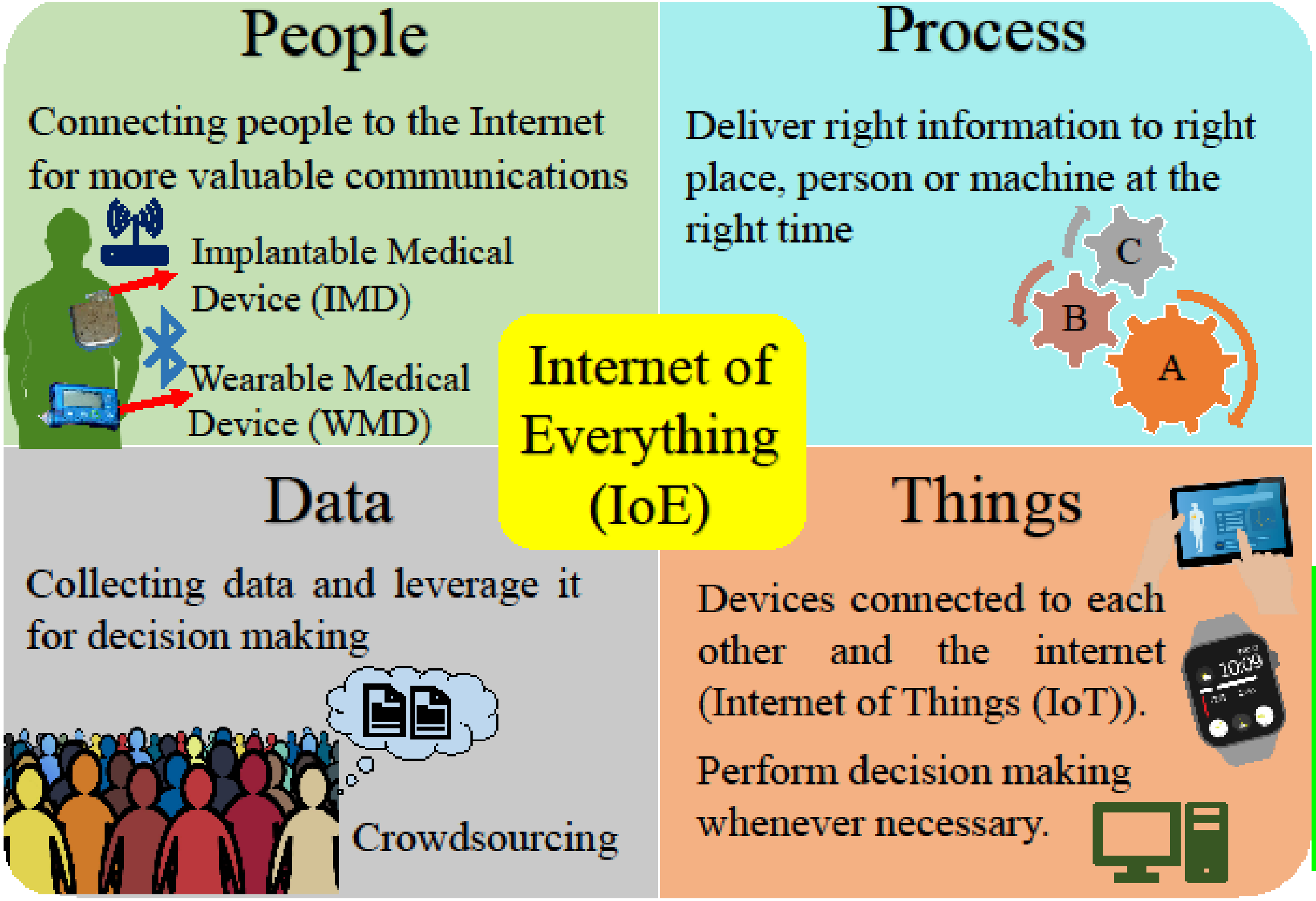
- ❖ Data and Device Security
- ❖ Data Privacy

IoMT is a collection of medical devices and applications that connect to healthcare IT systems through Internet.

Source: http://www.icemiller.com/ice-on-fire-insights/publications/the-internet-of-health-things-privacy-and-security/

Source: http://internetofthingsagenda.techtarget.com/definition/IoMT-Internet-of-Medical-Things

Internet of Every Things (IoE)



People

Connecting people to the Internet for more valuable communications

Implantable Medical Device (IMD)

Wearable Medical Device (WMD)

Process

Deliver right information to right place, person or machine at the right time

Internet of Everything (IoE)

Data

Collecting data and leverage it for decision making

Crowdsourcing

Things

Devices connected to each other and the internet (Internet of Things (IoT)).

Perform decision making whenever necessary.

Requires:

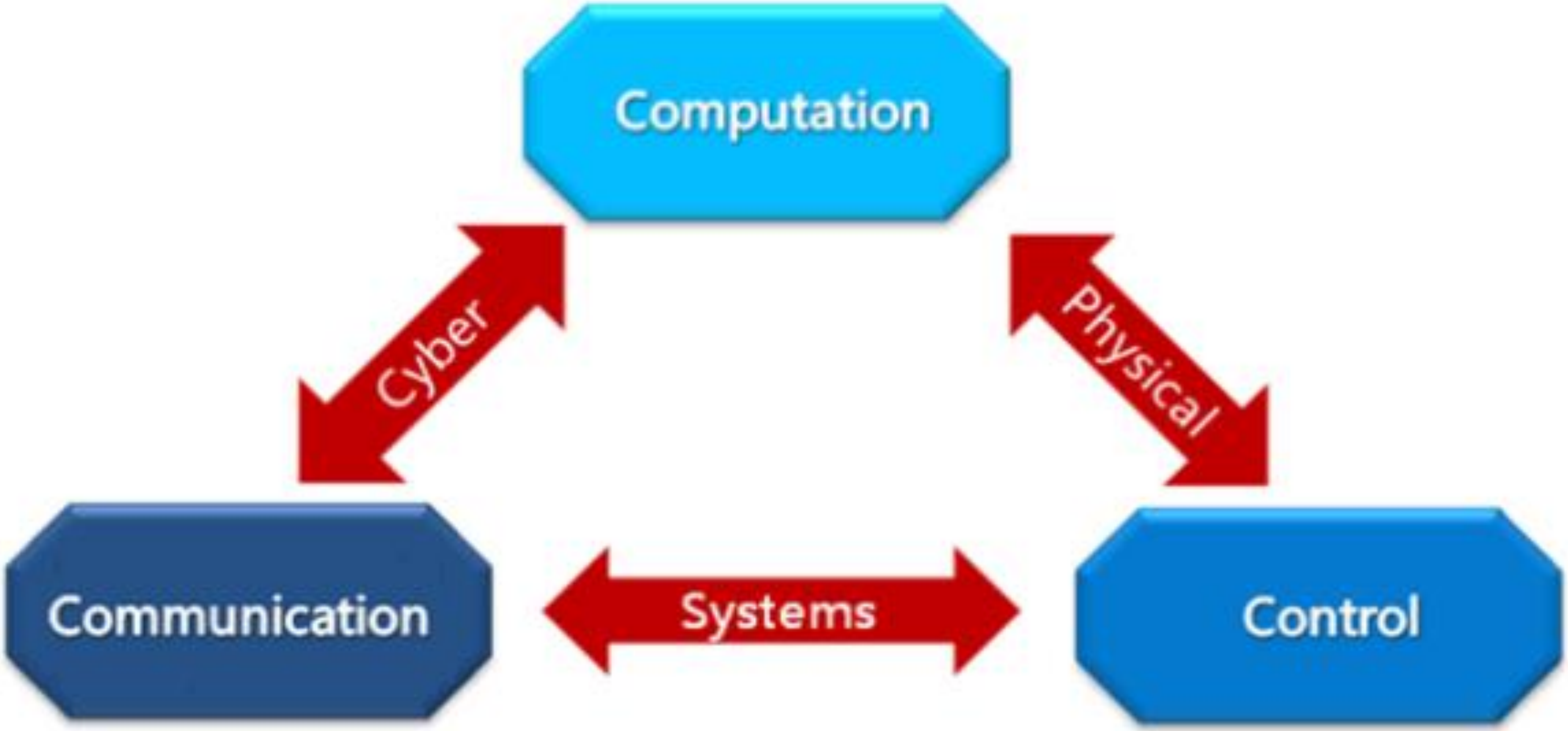
- Data, Device, and System Security
- Data, Location, and System Privacy

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.

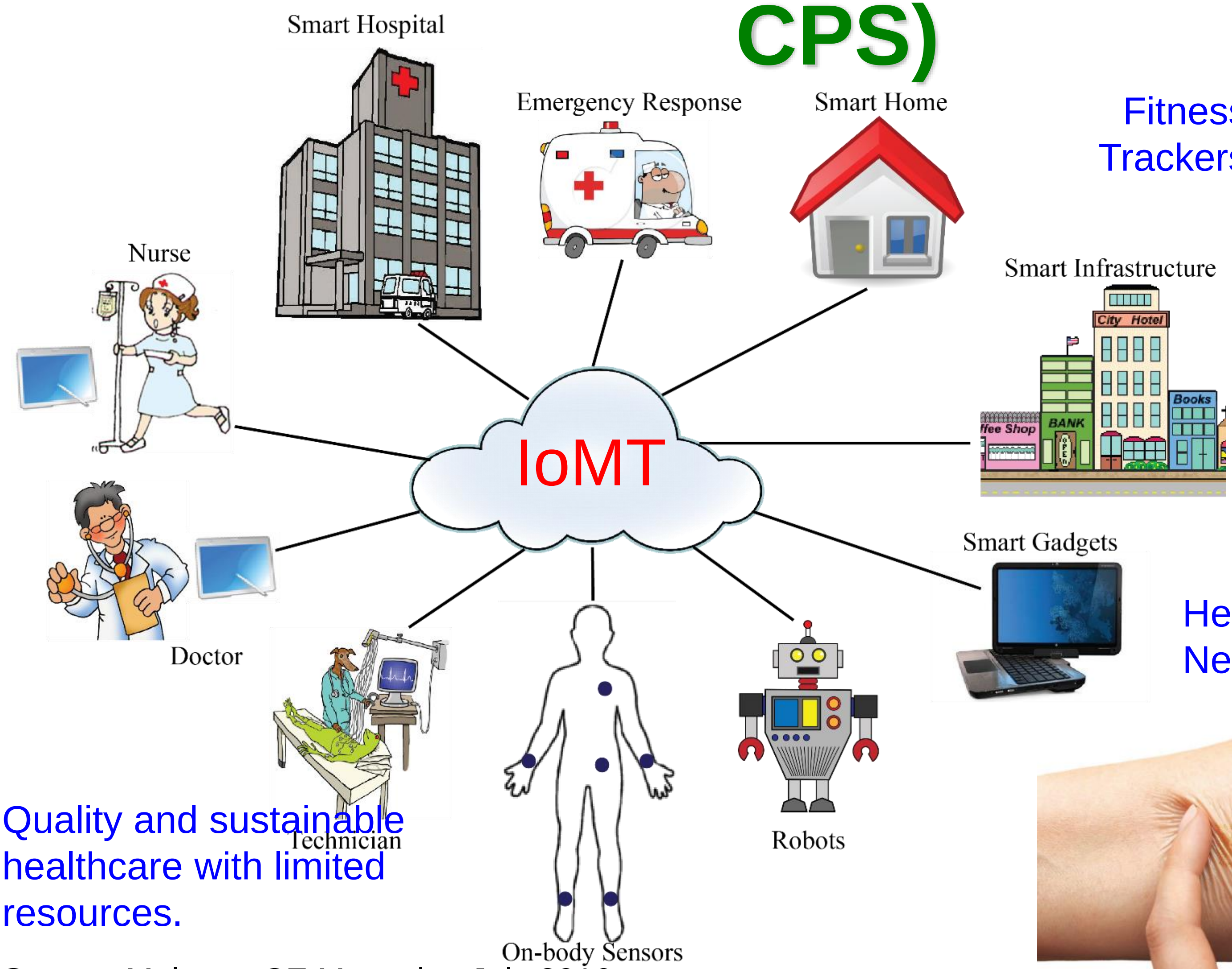
Cyber-Physical Systems (CPS) - 3 Cs



3 Cs of IoT - Connect, Compute, Communicate

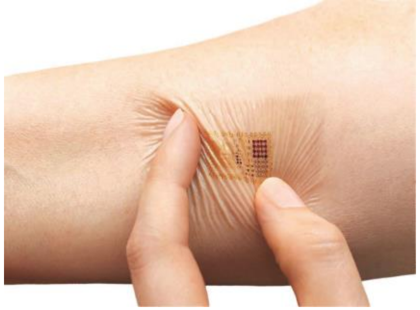
Source: G. Jinghong, H. Ziwei, Z. Yan, Z. Tao, L. Yajie and Z. Fuxing, "An overview on cyber-physical systems of energy interconnection," in *Proc. IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2017, pp. 15-21.

Healthcare Cyber-Physical System (H-CPS)



Fitness Trackers

Headband with Embedded Neurosensors



Embedded Skin Patches

Quality and sustainable healthcare with limited resources.

Source: Mohanty CE Magazine July 2016

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

AI can be fooled by fake data

AI can create fake data (Deepfake)

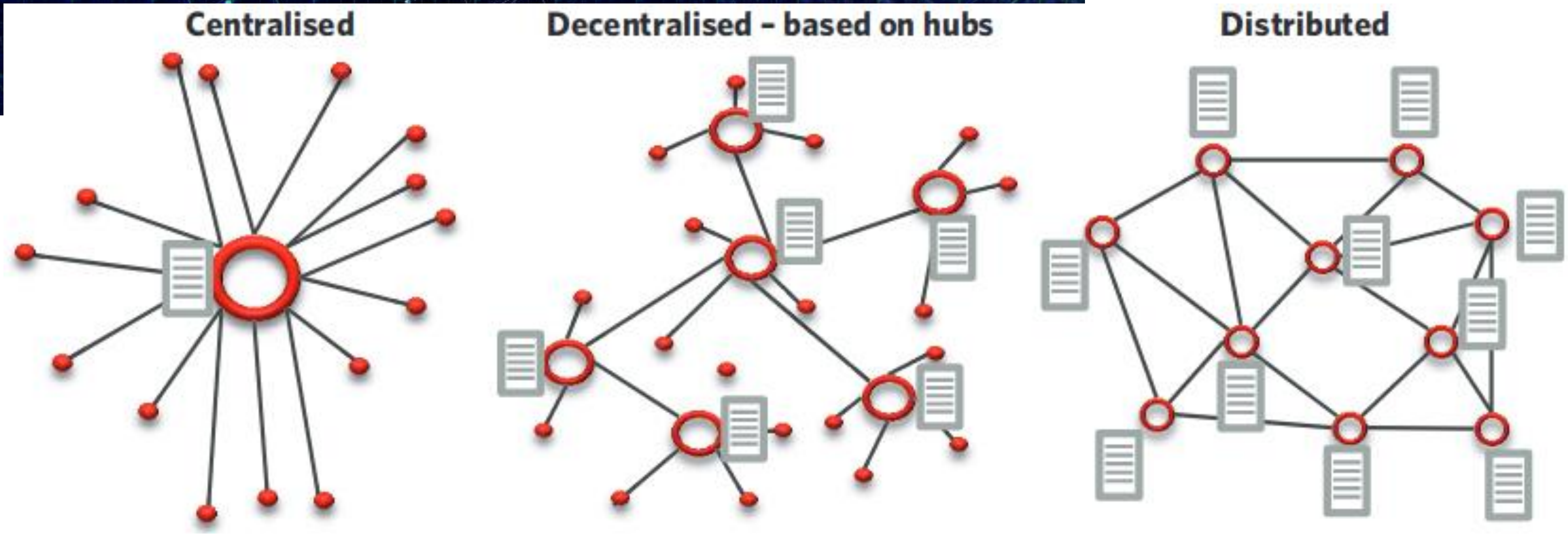
Authentic Fake

An implantable medical device

Authentic Fake

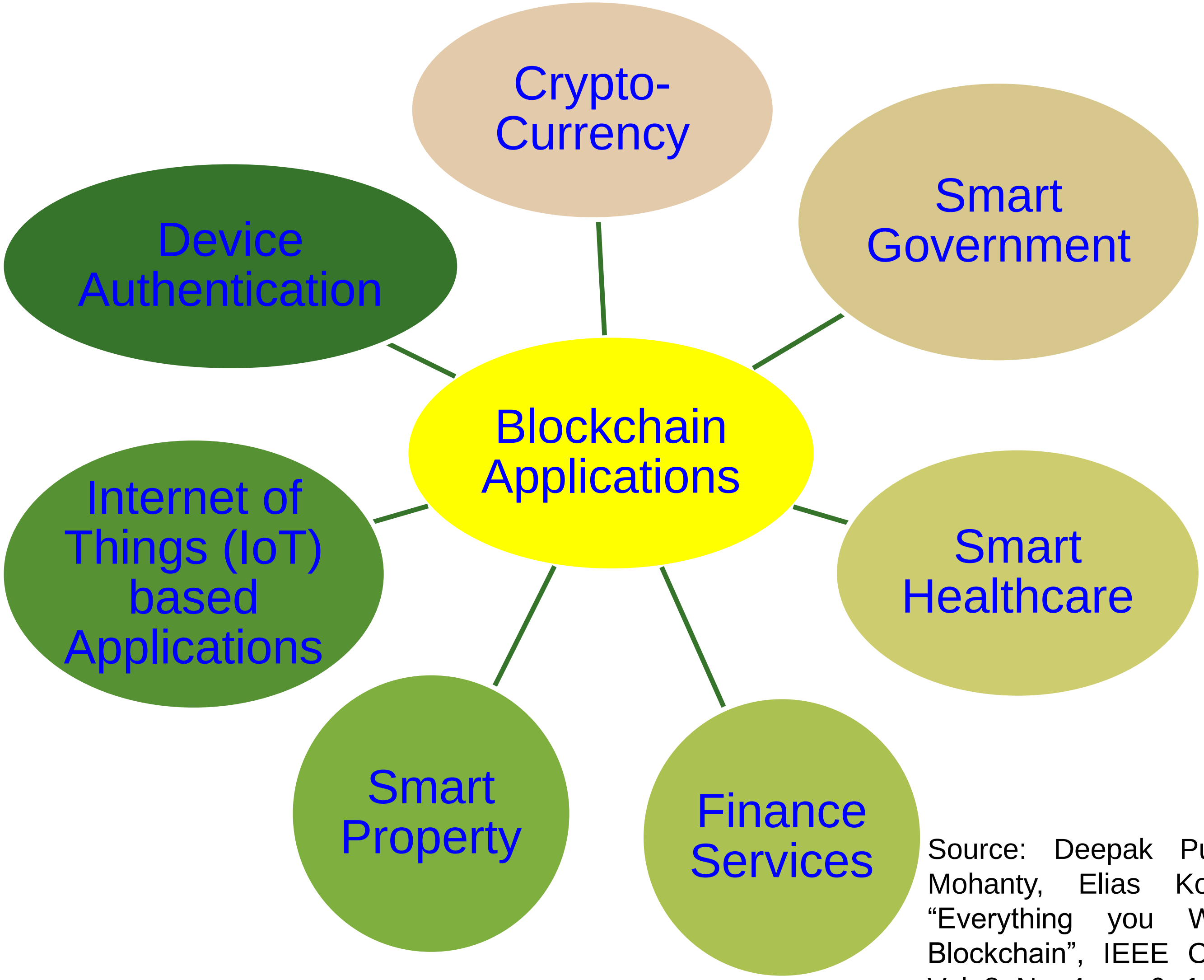
A plug-in for car-engine computers

Blockchain Technology



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

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 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.

Hardware-Assisted Security (HAS)

- Hardware-Assisted Security: Security provided by hardware for:

  (1) information being processed,

  (2) hardware itself,

  (3) overall system

Privacy by Design (PbD)

Security/Secure by Design (SbD)

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

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

IR Hardware Security

Memory Protection

Digital Core IP Protection

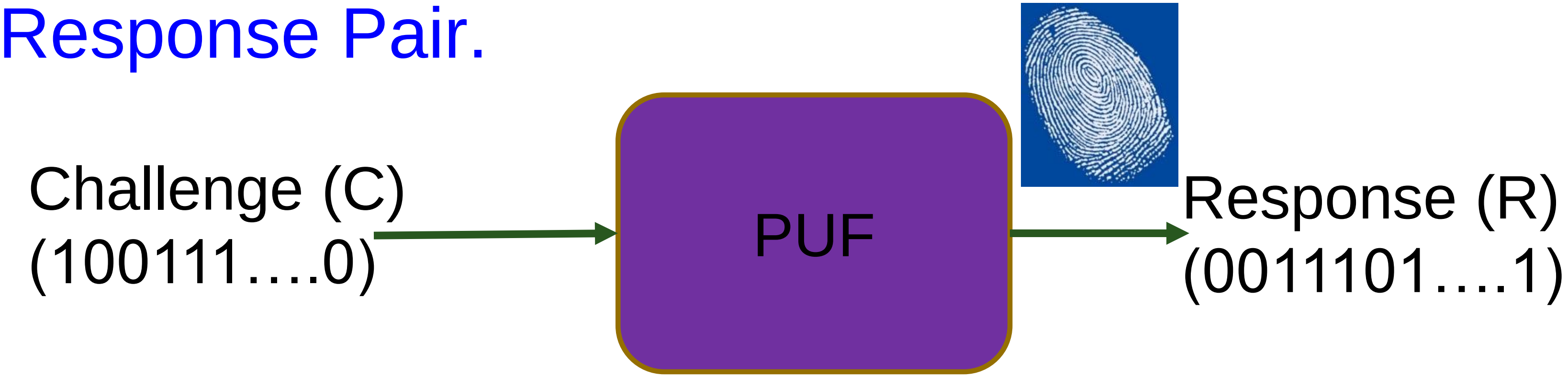
Source: Mohanty ICCE 2018 Panel

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 (PUFs)

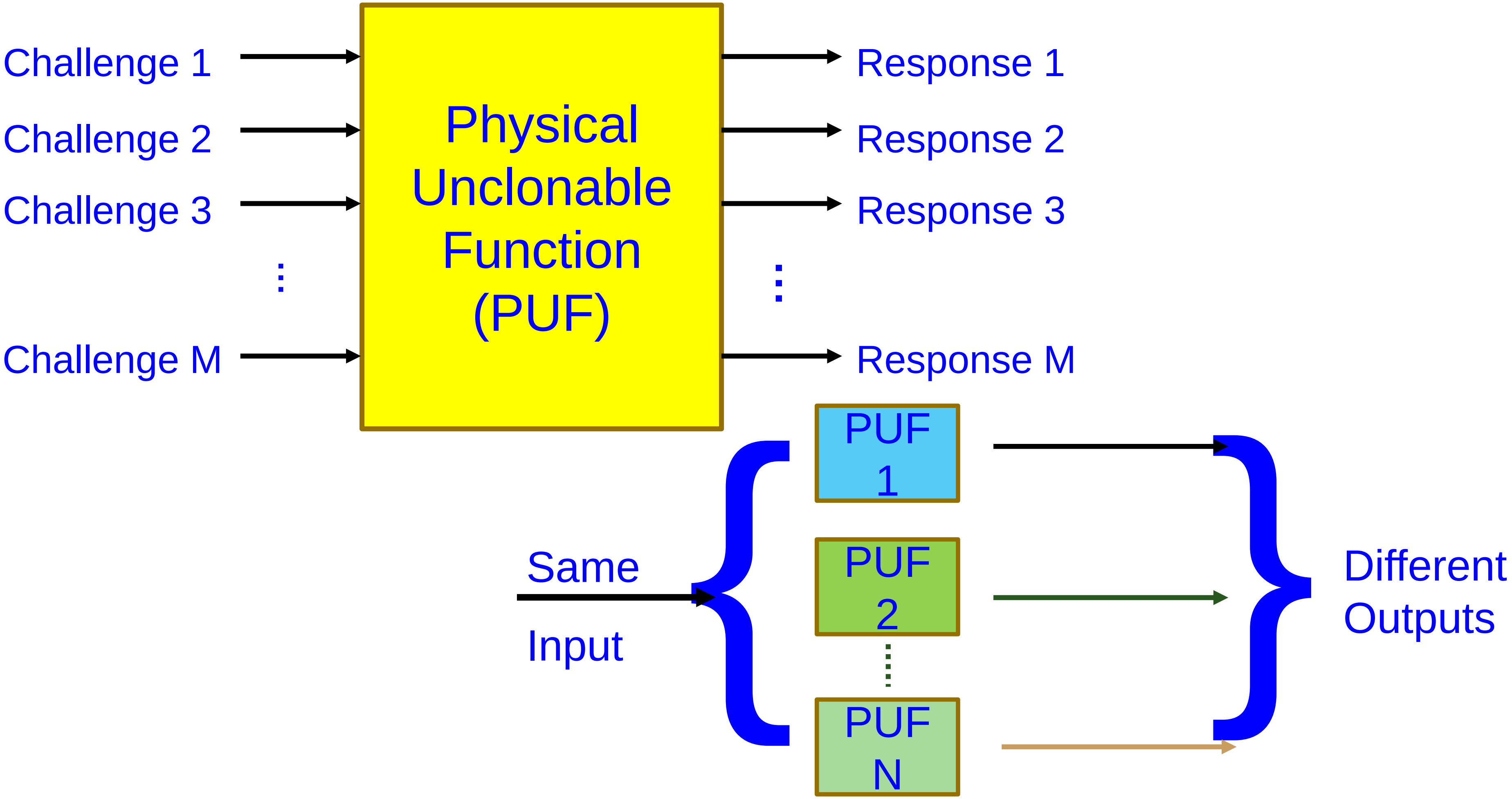
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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.

Principle of Generating Multiple Random Response using PUF



Challenge 1

Challenge 2

Challenge 3

⋮

Challenge M

Physical Unclonable Function (PUF)

Response 1

Response 2

Response 3

⋮

Response M

Same Input

PUF 1

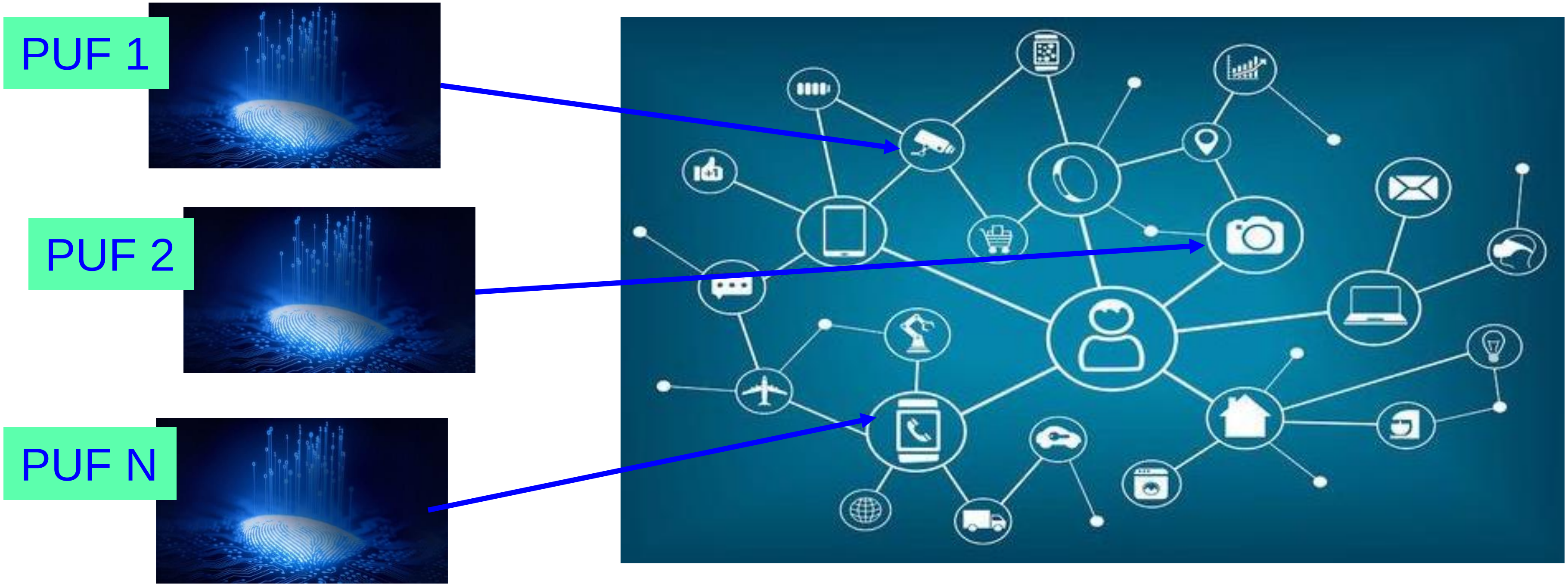
PUF 2

⋮

PUF N

Different Outputs

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

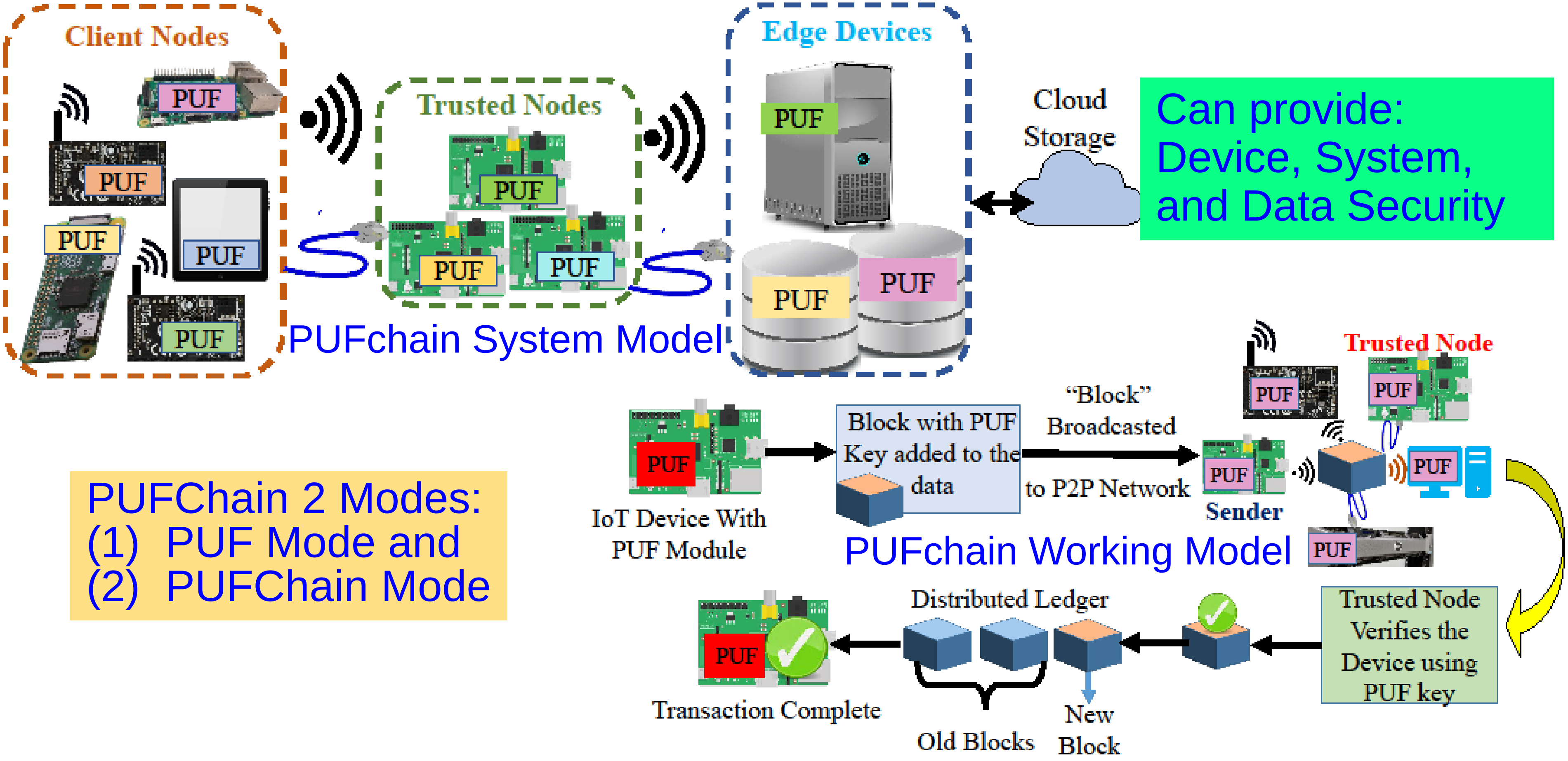


PUF 1

PUF 2

PUF N

PUFchain: The Hardware-Assisted Scalable Blockchain



PUFchain System Model

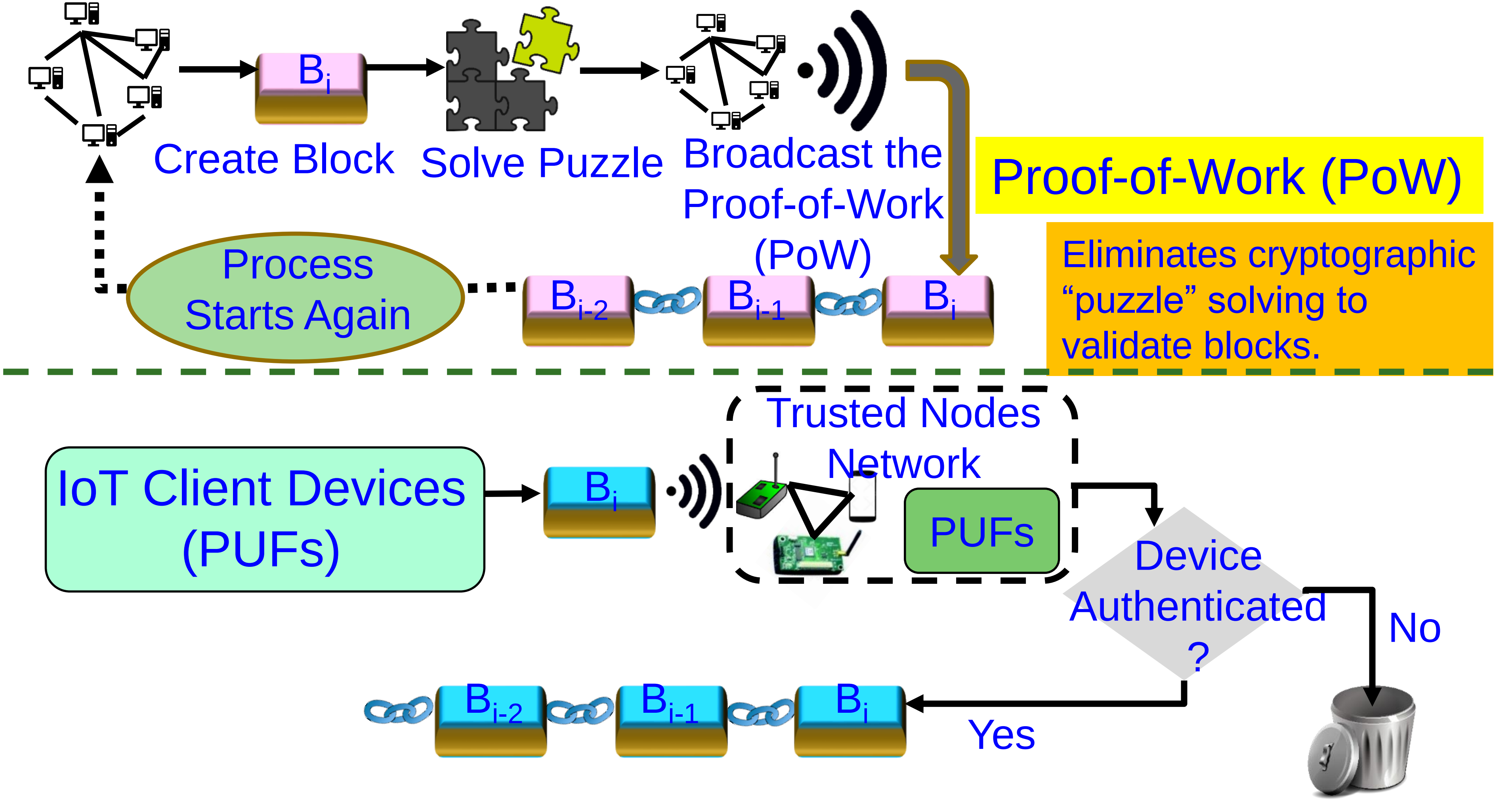
Can provide:
Device, System, and Data Security

PUFchain Working Model

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

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.

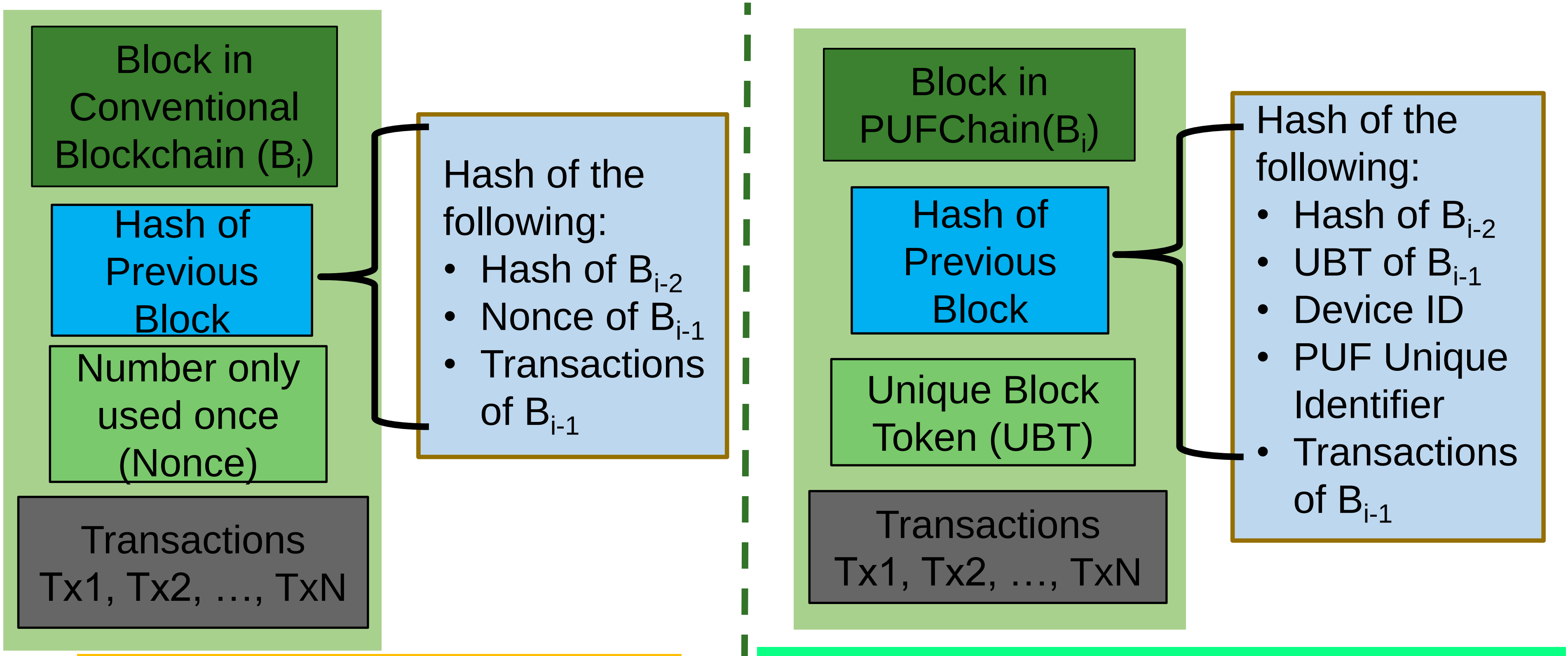
Our Proof-of-PUF-Enabled-Authentication (PoP)



Proof-of-Work (PoW)

Eliminates cryptographic “puzzle” solving to validate blocks.

PUFchain: Proposed New Block Structure



Block in Conventional Blockchain (B_i)

Hash of Previous Block

Number only used once (Nonce)

Transactions Tx1, Tx2, …, TxN

Hash of the following:

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

Conventional Block Structure

Block in PUFChain(B_i)

Hash of Previous Block

Unique Block Token (UBT)

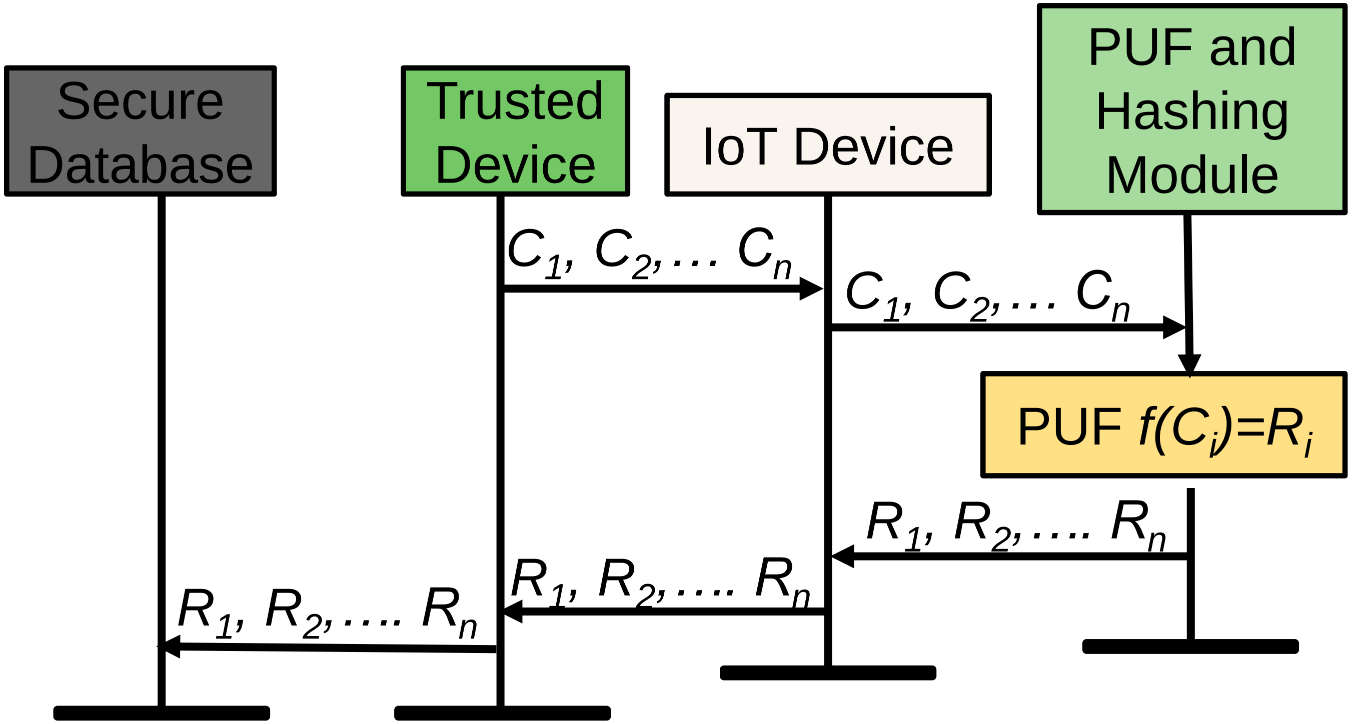
Transactions Tx1, Tx2, …, TxN

Hash of the following:

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

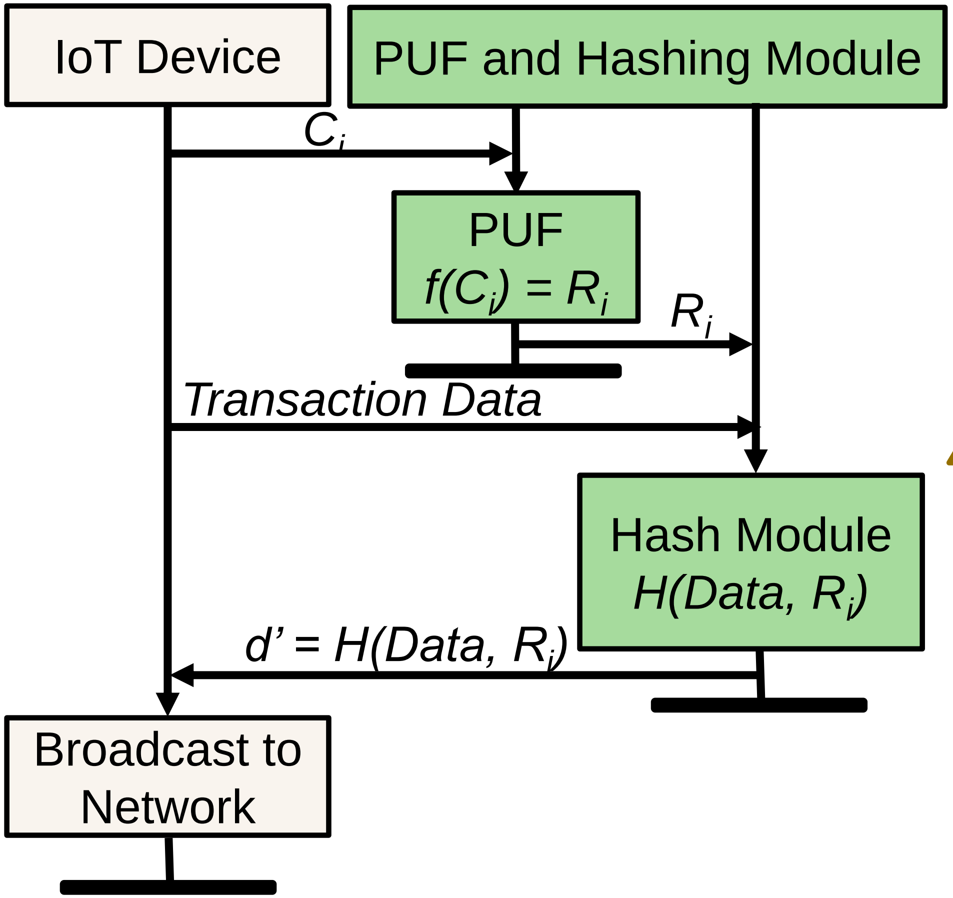
Proposed Block Structure for PUFchain

PUFchain: Device Enrollment Steps

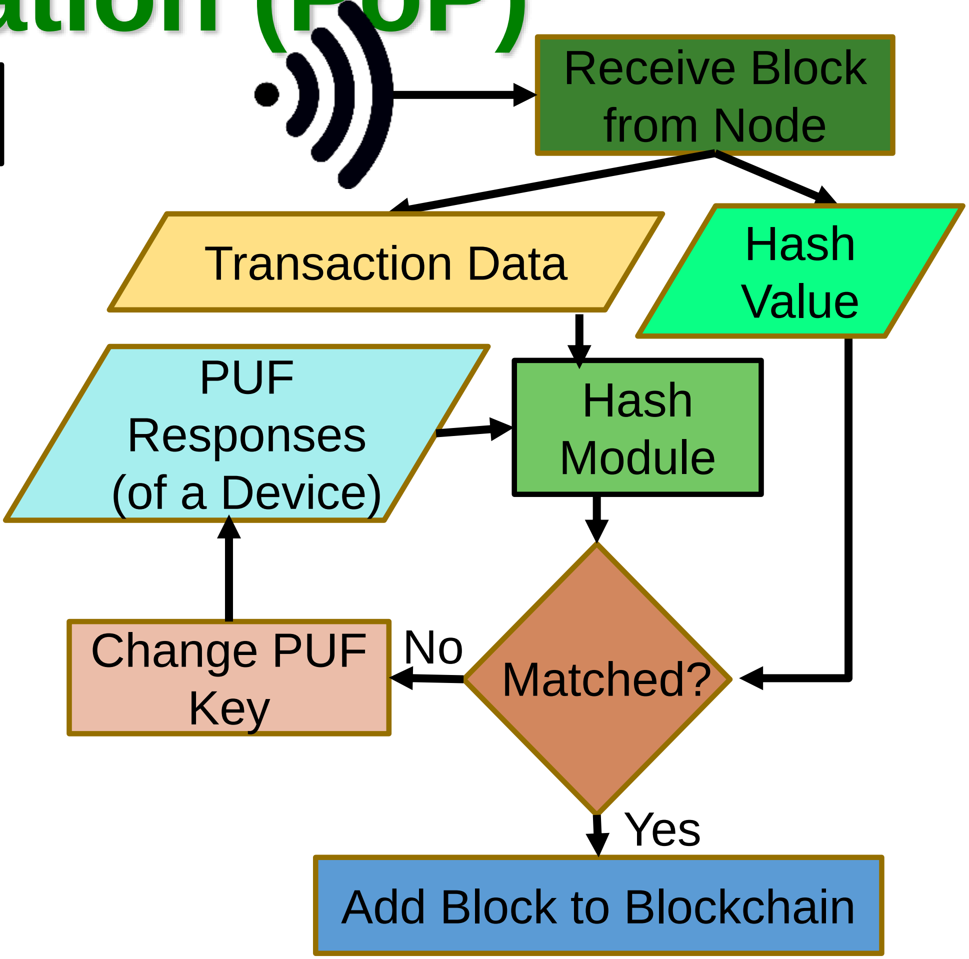


Device Enrollment Steps

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



Steps for Transactions Initiation

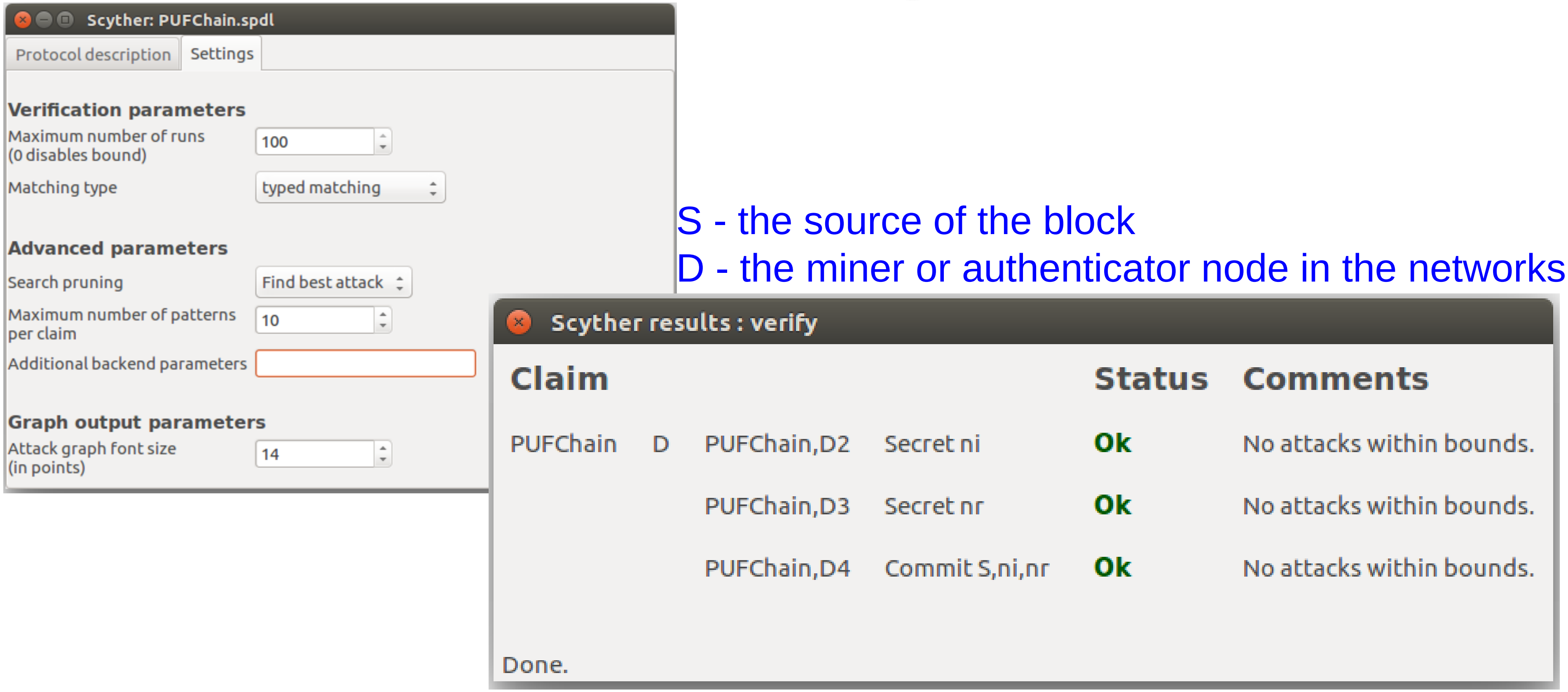


Steps for Device Authentication

PUFchain Security Validation

S - the source of the block

D - the miner or authenticator node in the networks



Verification parameters

Maximum number of runs (0 disables bound): 100

Matching type: typed matching

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

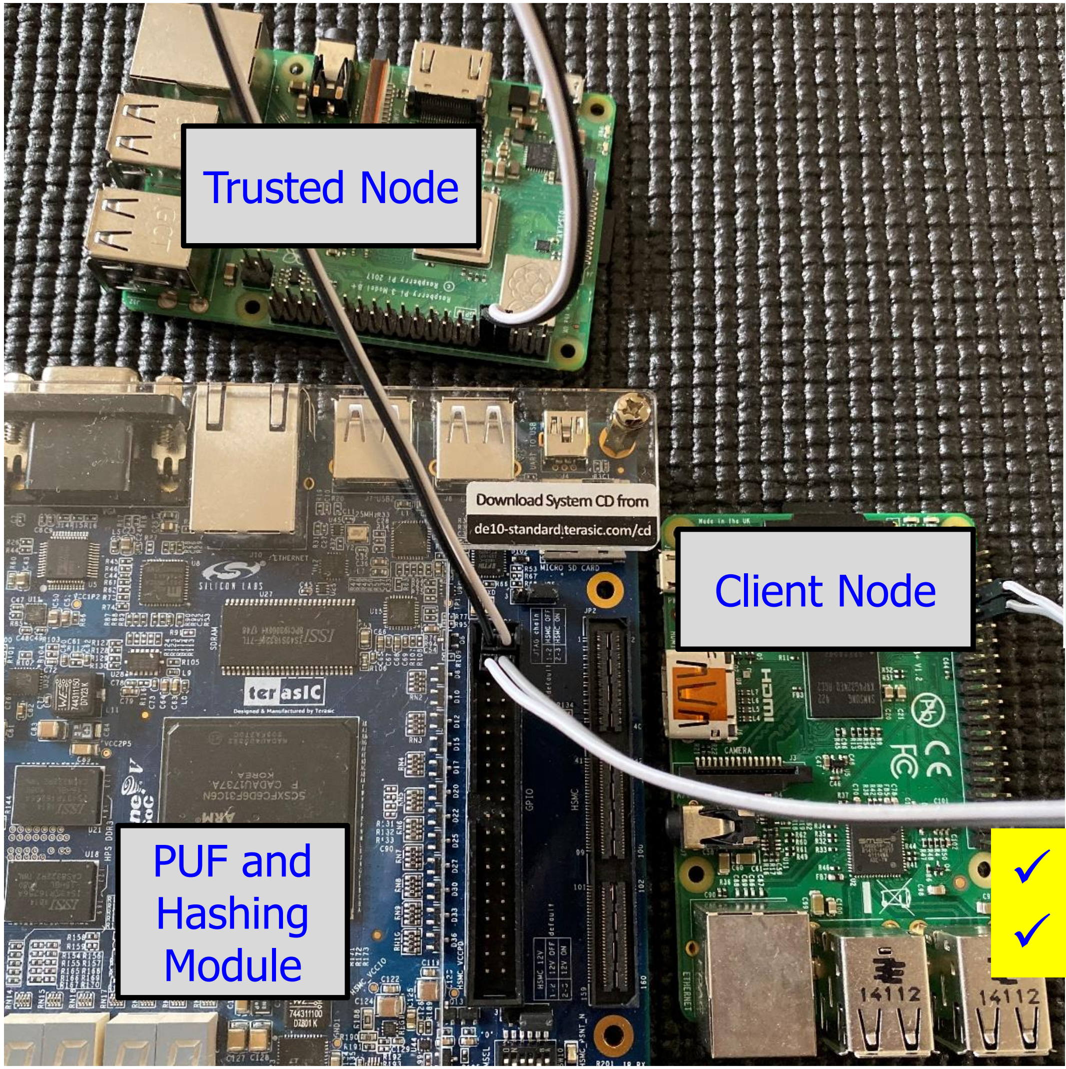
Attack graph font size (in points): 14

Claim				Status	Comments
PUFChain	D	PUFChain,D2	Secret ni	Ok	No attacks within bounds.
		PUFChain,D3	Secret nr	Ok	No attacks within bounds.
		PUFChain,D4	Commit S,ni,nr	Ok	No attacks within bounds.

Done.

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

Our PoP is 1000X Faster than PoW



Trusted Node

Client Node

PUF and Hashing Module

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

Conclusions

- 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.

Future Directions

Our Research interests include:

- Privacy and/or Security by Design (PbD or SbD).
- Security, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS).
- Security of systems (e.g. Smart Healthcare device/data, Smart Grid, UAV, Smart Cars).
- Sustainable Smart City: needs sustainable IoT/CPS
- Internet-of-Everything (IoE)- in which humans are active parts.

Acknowledgment

This material is based upon work supported by the National Science Foundation (NSF) under Grant No. OAC-1924112.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.