PMsec 2.0: A Security-By-Design Solution for Doctor's Dilemma Problem in Smart Healthcare

Presenter Name: Venkata K. V. V. Bathalapalli

Affiliation: University of North Texas

Venkata K. V. V. Bathalapalli[1], S. P. Mohanty[2], E. Kougianos[3], Vasanth Iyer[4], and Bibhudutta Rout[5]

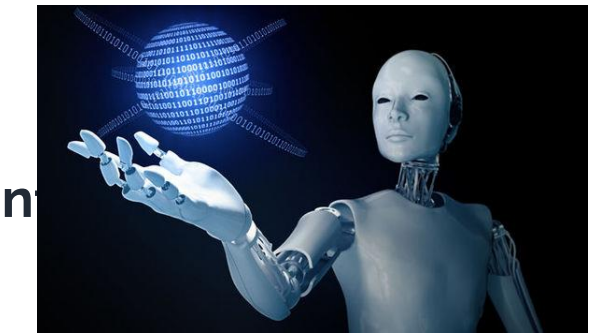
Email: **vb0194@unt.edu, saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3], iyerv@gram.edu[4], bibhudutta.rout@unt.edu[5]**

21st OITS International Conference on Information Technology (OCIT 2023)
December 13th - 15th, 2023

Outline

- Cybersecurity in Smart Healthcare
- Physical Unclonable Functions (PUF) as SbD Primitive
- Overview of TPM
- Overview of PMsec: A SbD Approach for security in IoMT
- Doctor's Dilemma Problem
- Architectural Overview of Proposed PMsec 2.0
- Experimental implementation Overview
- Conclusion & Future Research Directions

Security-by-Design (SbD) – The Principle



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

- Security by Design (SbD) ensures the security and privacy of a system right from the beginning of the design phase
- Privacy by Design (PbD) Treat privacy concerns as design requirements rather than trying to retrofit privacy controls after it is built.
- SbD works on identifying the system's security vulnerabilities at the design stage.
- Principle of Least Privilege with defined access permissions to users.
- Real Time risk assessment and Threat detection.

Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," in *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4-5, 1 March 2020, doi: 10.1109/MCE.2019.2954959.

Security by Design (SbD)-Principles

7 Fundamental Principles

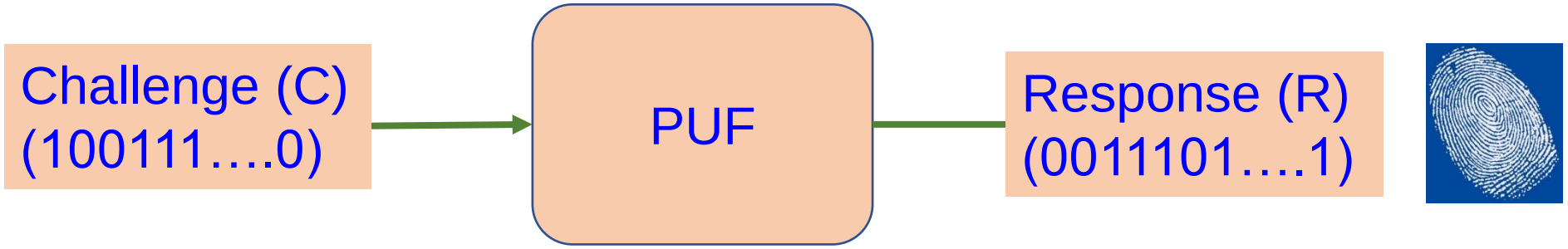
- Proactive not Reactive
- Security/Privacy as the Default
- Security/Privacy Embedded into Design
- Full Functionality - Positive-Sum, not Zero-Sum
- End-to-End Security/Privacy - Lifecycle Protection
- Visibility and Transparency
- Respect for Users

Physical Unclonable Functions (PUF)

21st OITS International Conference on Information Technology (OCIT 2023)
December 13th - 15th, 2023

Physical Unclonable Functions (PUFs) - Principle

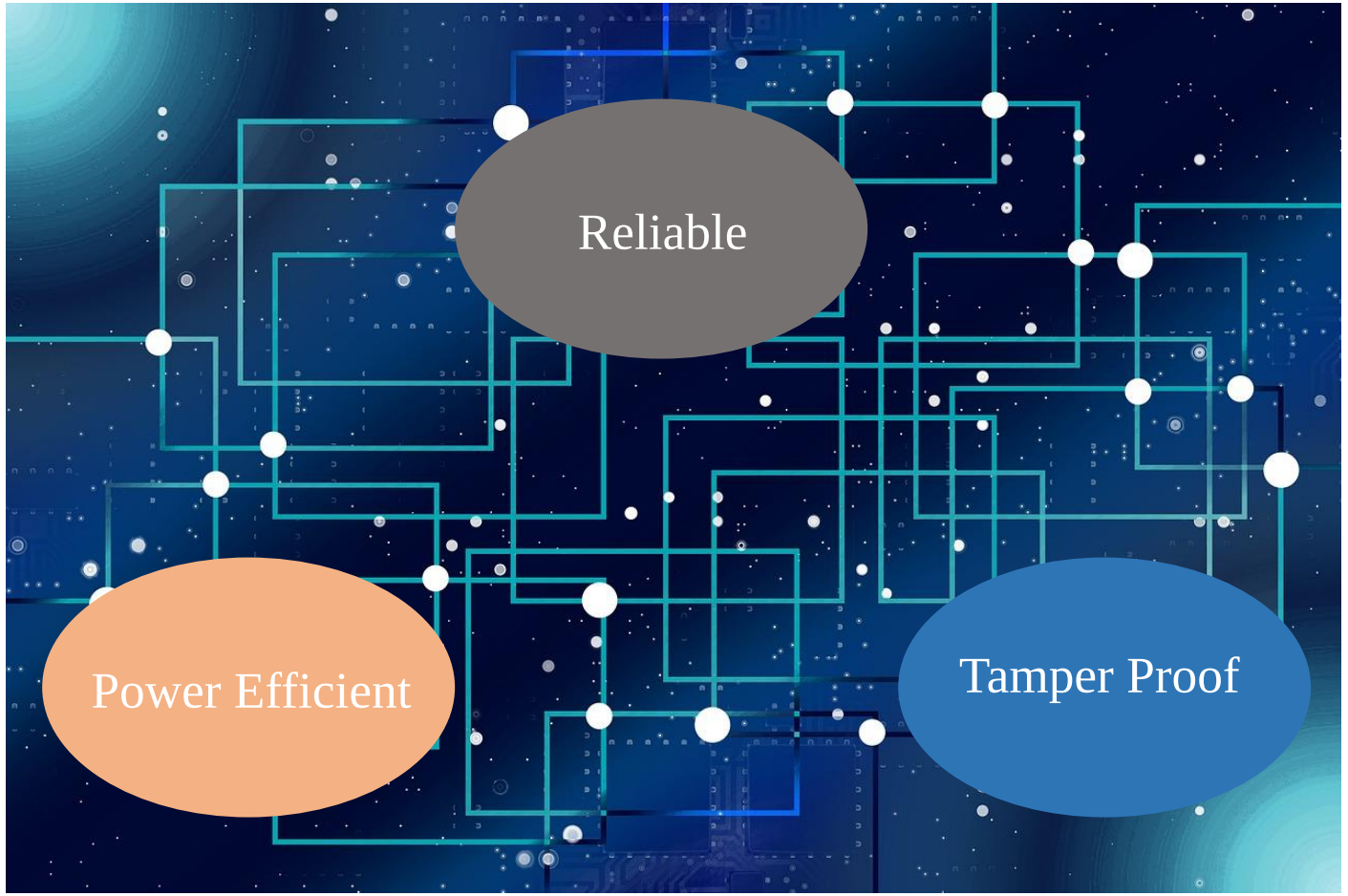
- Physical Unclonable Functions (PUFs) are primitives for security.
- PUFs are easy to build and impossible to duplicate.
- The input and output are called a Challenge Response Pair.



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

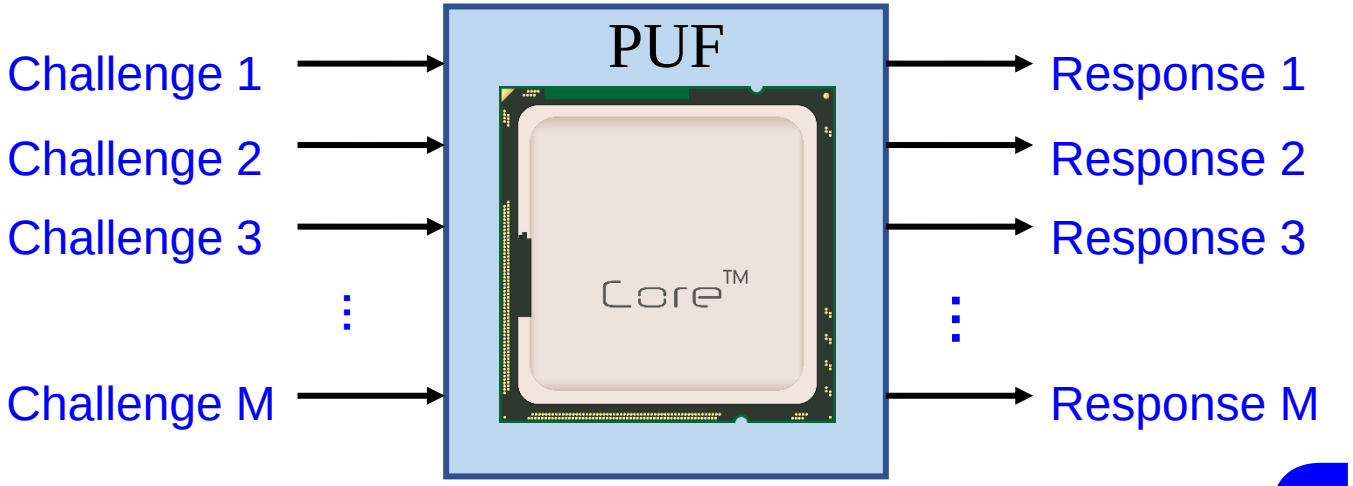
Source: S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

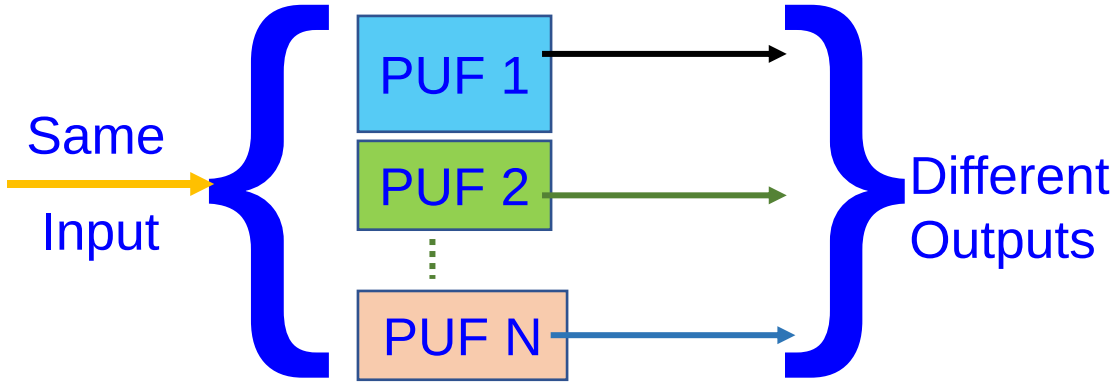
PUF as a SbD Primitive



- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device authentication

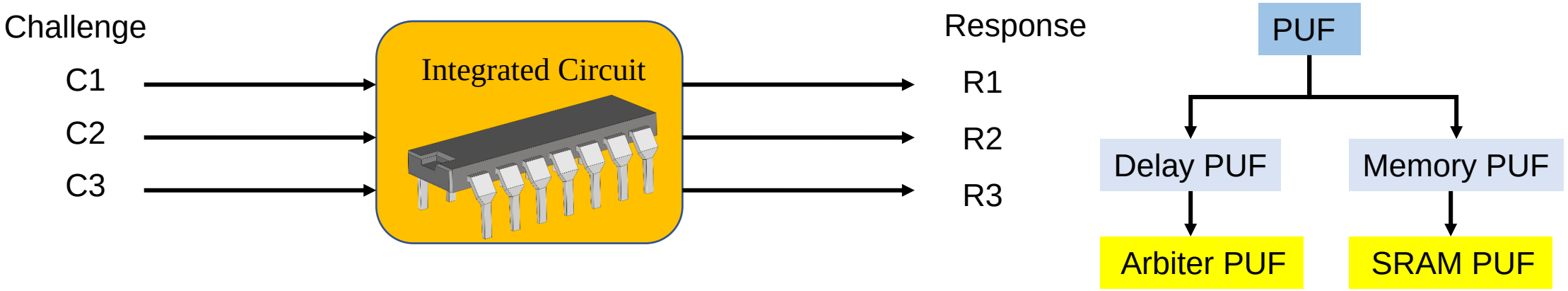
PUF Key Generation and Working





Source: International Symposium on Smart Electronics Systems (iSES) 2019 Demo (PUFchain: Hardware-Integrated Scalable Blockchain)

Classification of PUF …



- A PUF generating large number of CRP is a strong PUF and PUF supporting a small number of CRP is considered as Weak PUF.
- A PUF can be categorized as Delay and Memory based PUF. Delay PUF is based on the variations in wiring and variations at gates in silicon. Memory based PUF is based on the instability in the startup phase of SRAM cell.

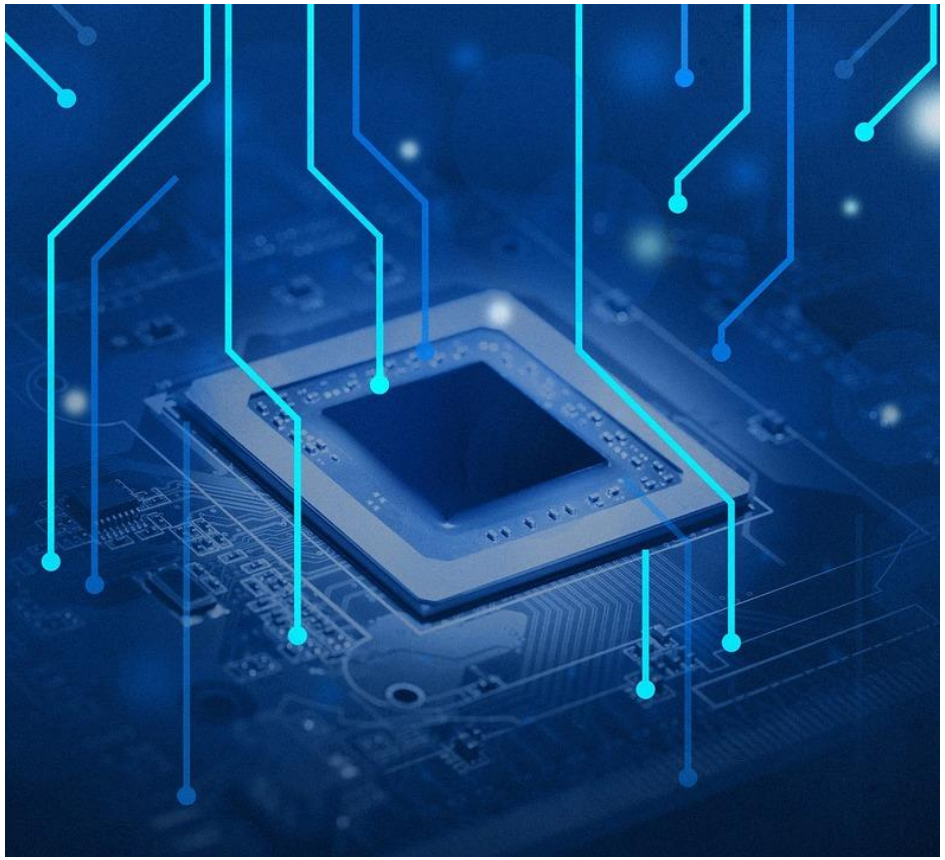
Source: S. Joshi, **S. P. Mohanty**, and E. Kougianos, "Everything You Wanted to Know about PUFs", *IEEE Potentials Magazine*, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Trusted Platform Module (TPM)

21st OITS International Conference on Information Technology (OCIT 2023)
December 13th - 15th, 2023

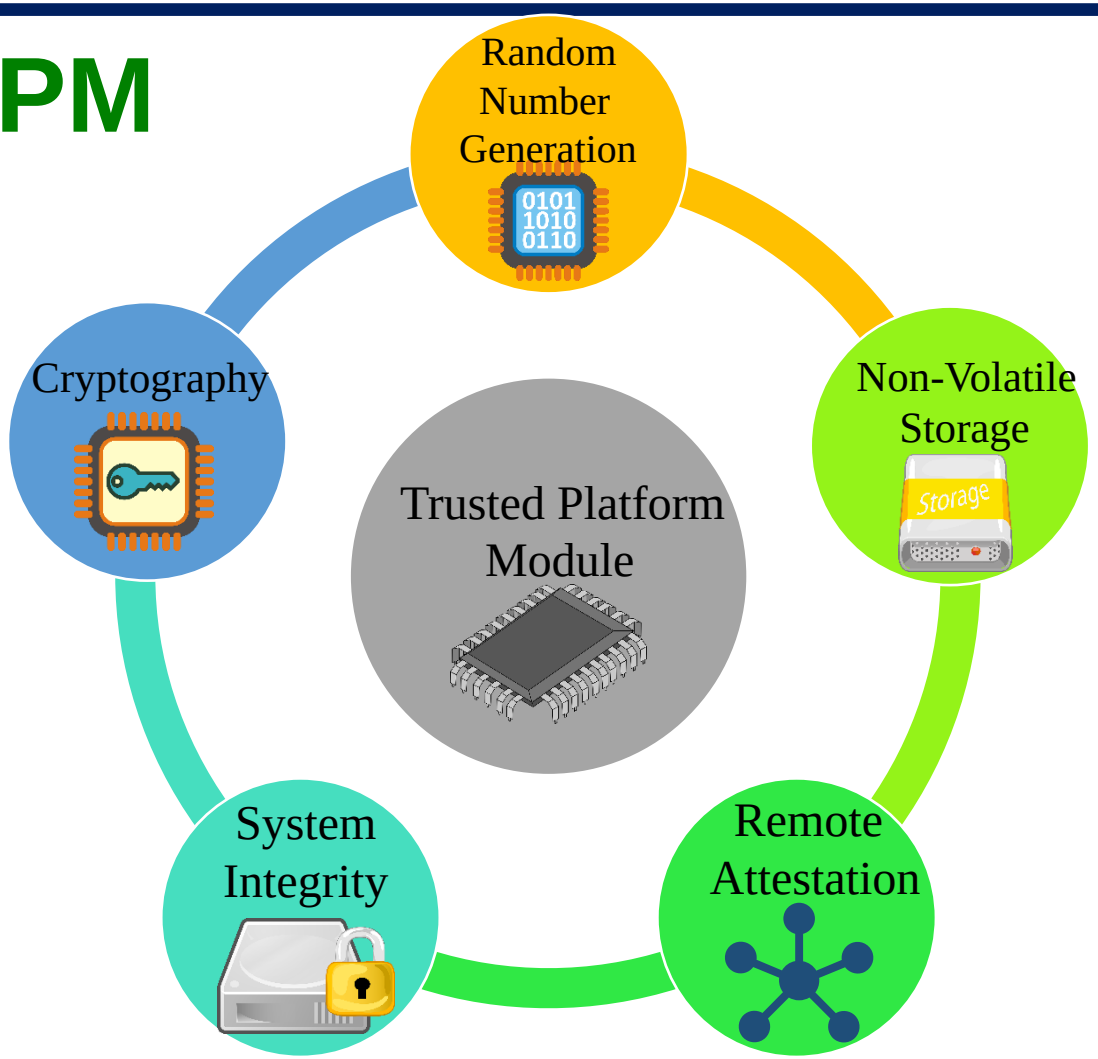
Trusted Platform Module - Overview

- A Trusted Platform Module (TPM) is a hardware security primitive that provides the root of trust for the computing platform as a simple System-On-Chip (Soc).
- A TPM provides a secure environment for cryptographic key storage, and system integrity measurement.
- TPM Non-Volatile Memory (NVRAM) can seal and unseal the secret keys generated inside or outside TPM.
- TPM's remote attestation scheme enables secure authentication of a computing system by a remote entity



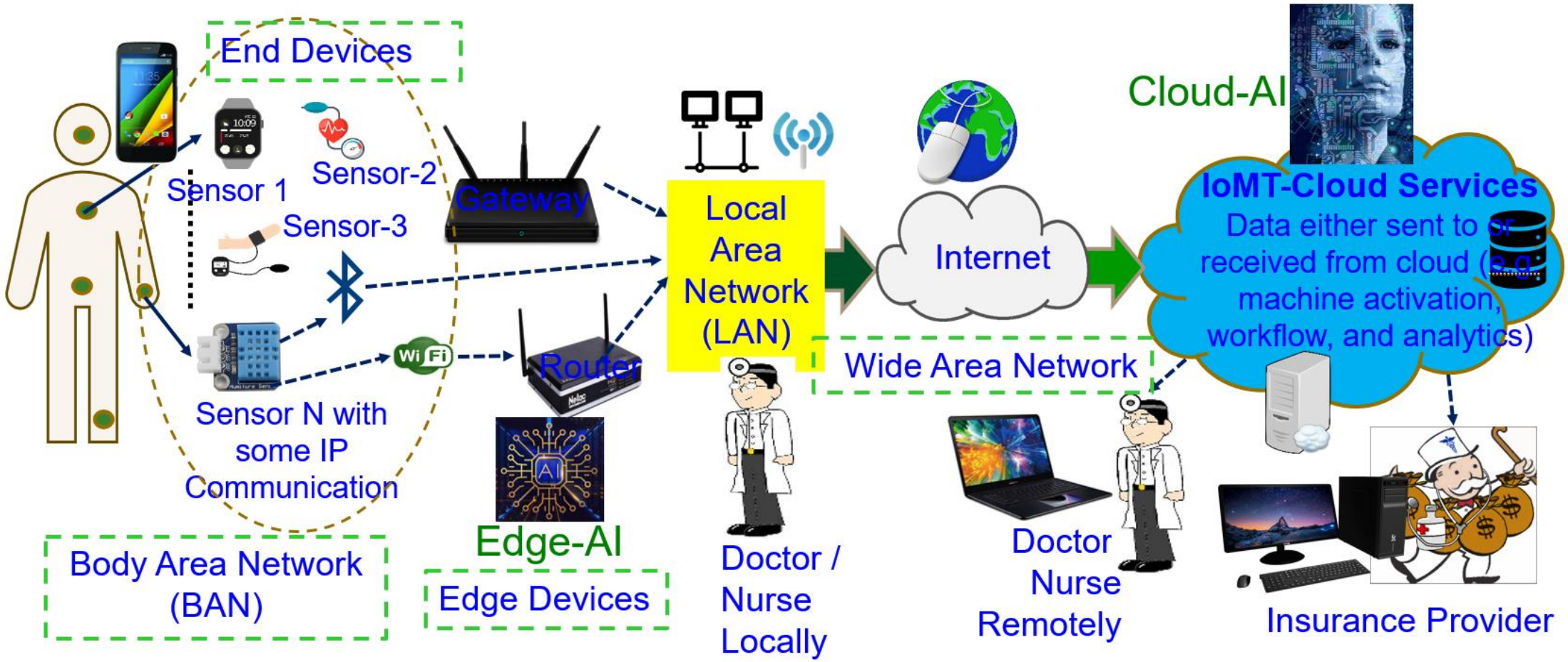
Functionality of TPM

- Secure Key Storage
- Hardware-Based Root of Trust
- Remote Attestation
- Secure Boot
- Sealed Storage and Sealing
- Random Number Generation



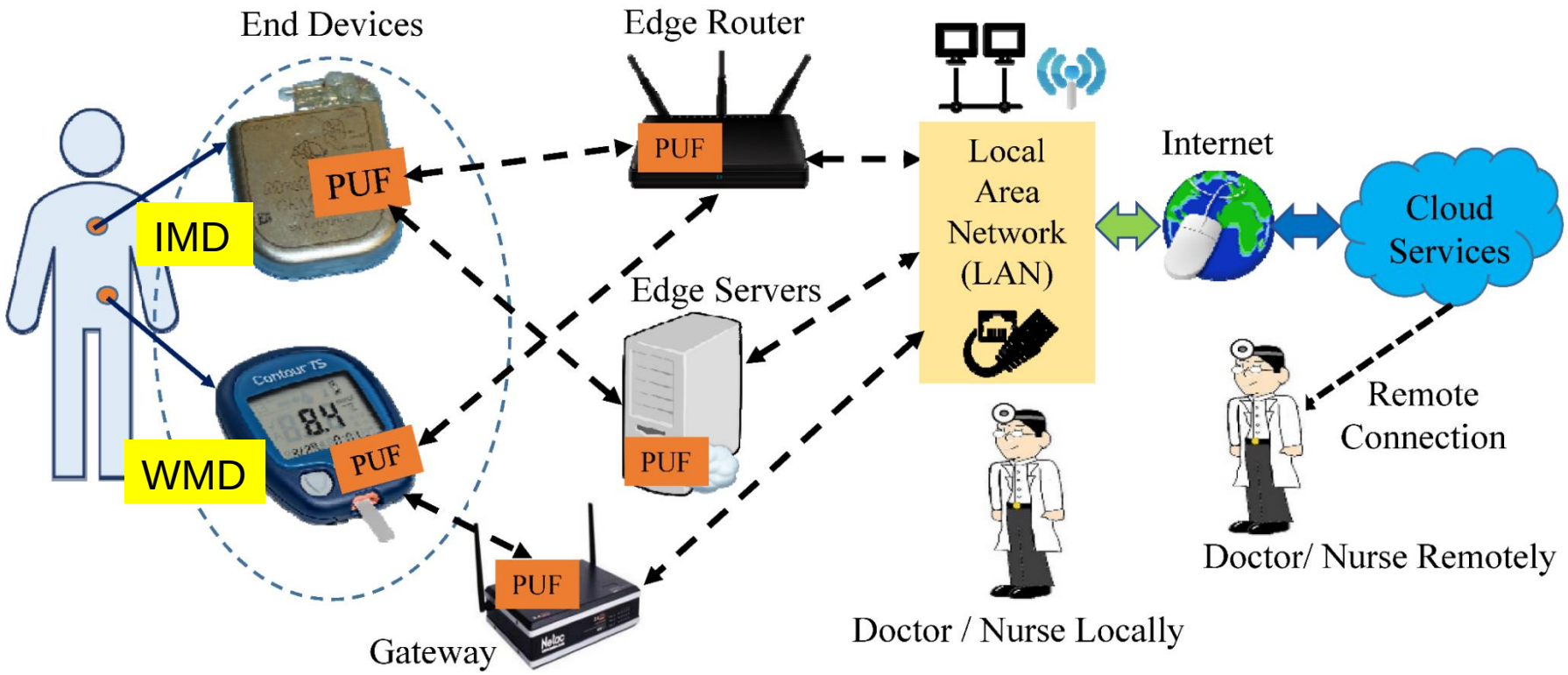
Source: M. Calvo and M. Beltrán, "Remote Attestation as a Service for Edge-Enabled IoT," *2021 IEEE International Conference on Services Computing (SCC)*, Chicago, IL, USA, 2021, pp. 329-339, doi: 10.1109/SCC53864.2021.00046.

SbD of H-CPS



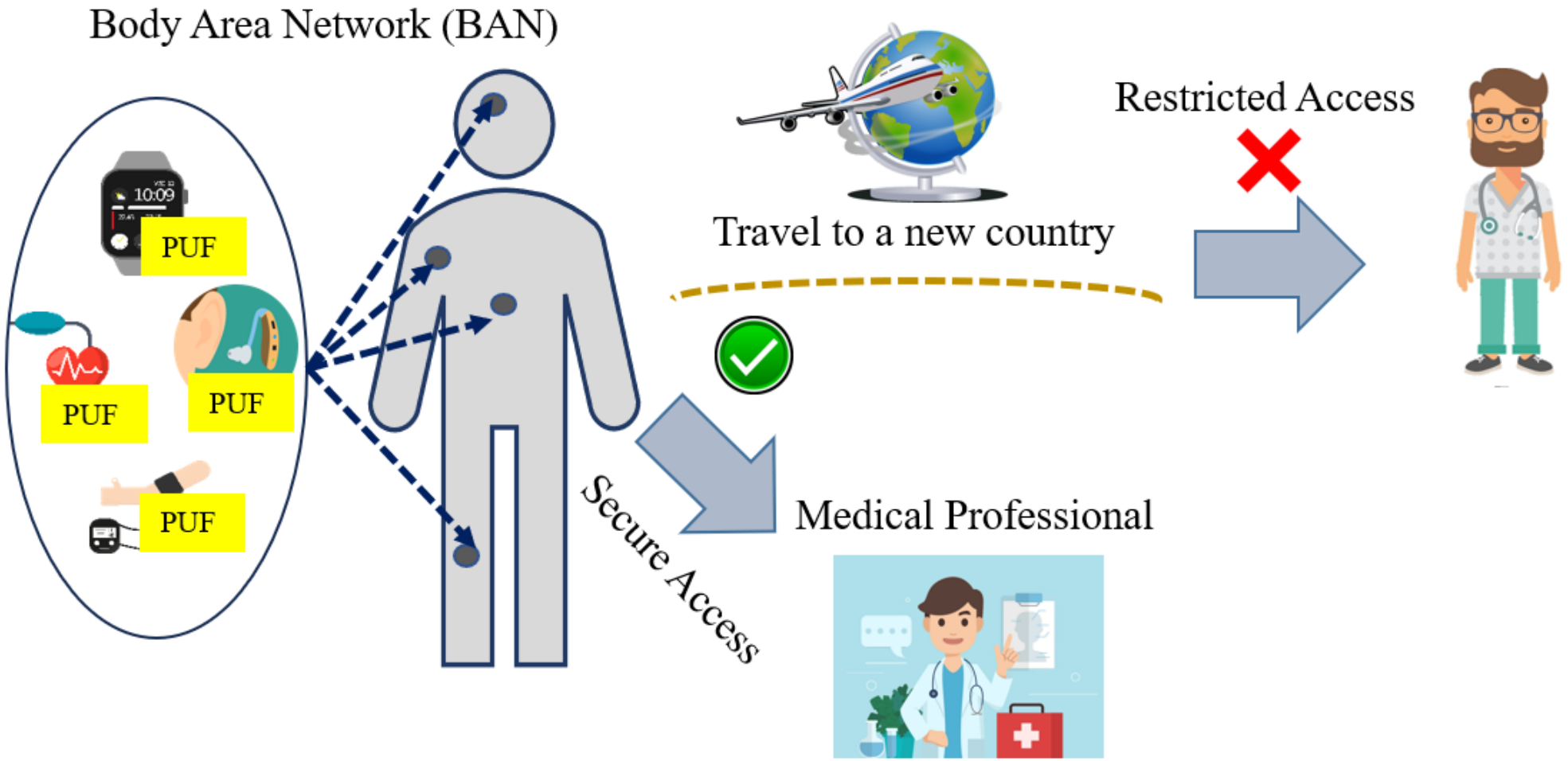
Source: S. P. Mohanty, Secure IoT by Design, Keynote, 4th IFIP International Internet of Things Conference (IFIP-IoT), 2021, Amsterdam, Netherlands, 5th November 2021.

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

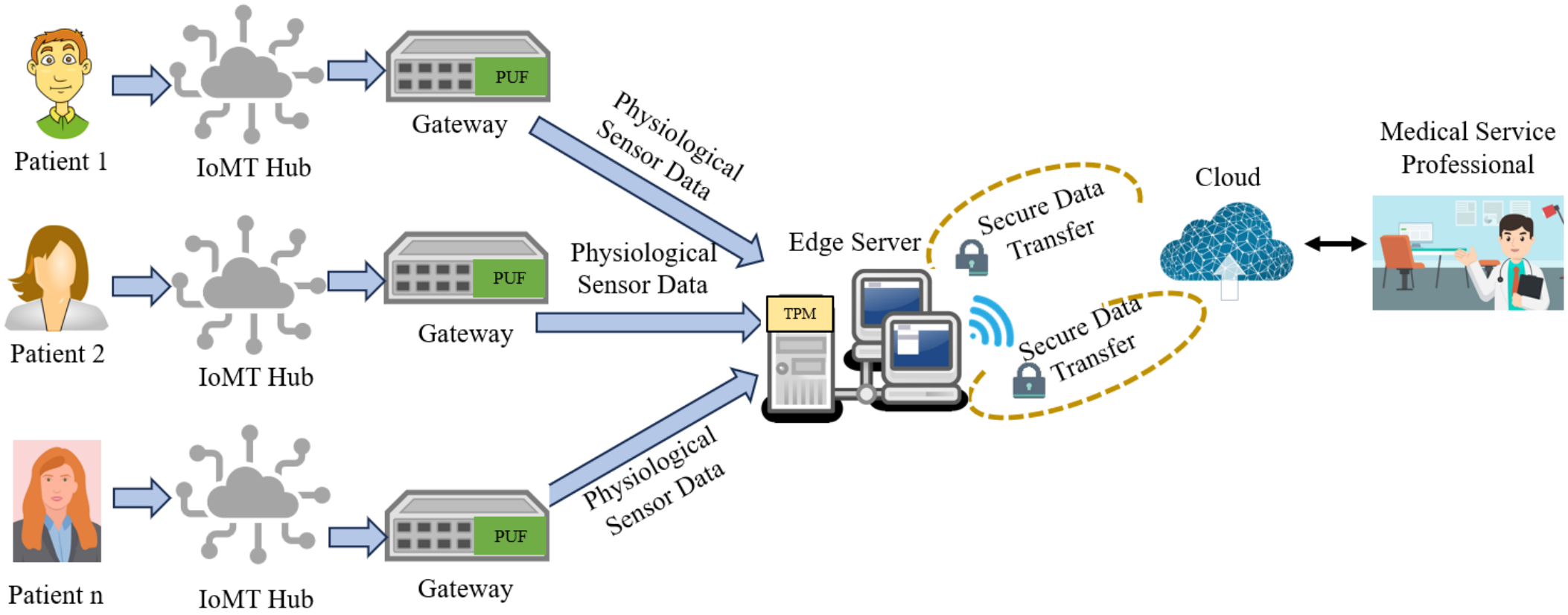


Source: V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things", *IEEE Transactions on Consumer Electronics (TCE)*, Volume 65, Issue 3, August 2019, pp. 388--397.

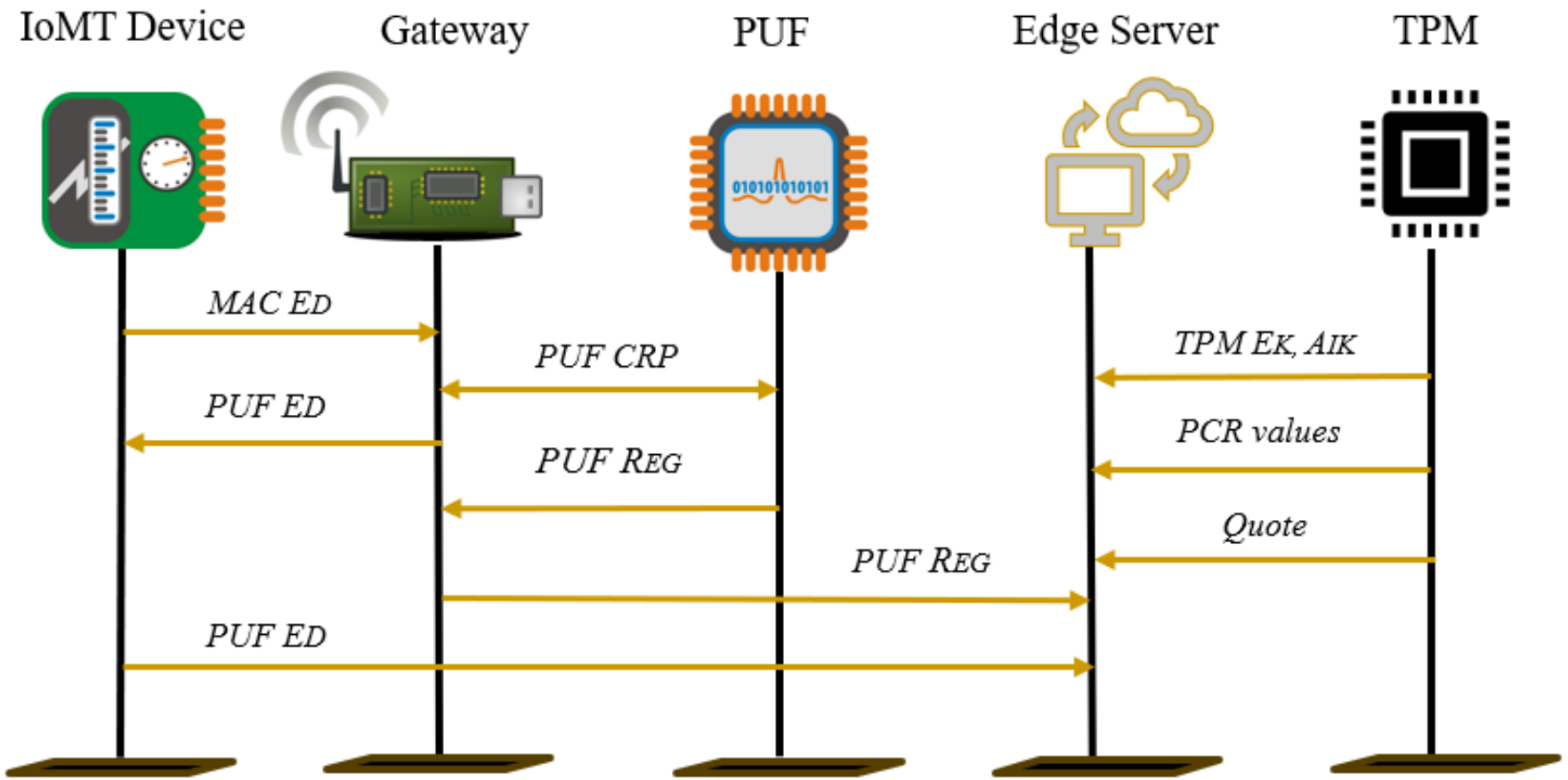
Doctors Dilemma Problem in Smart Healthcare



Architectural Overview of PMsec 2.0 Enabled H-CPS



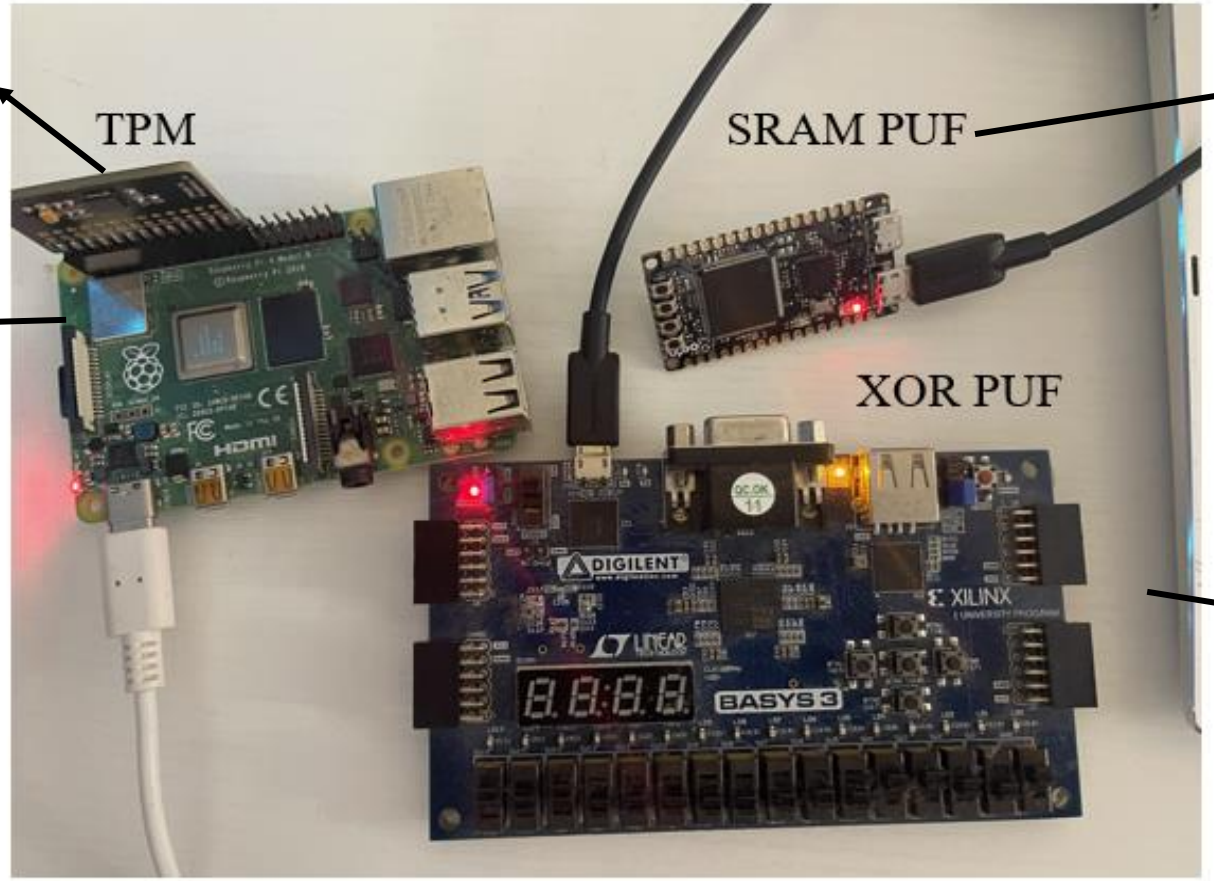
Working Flow of PMsec 2.0



Experimental Setup of PMsec 2.0

Geek Pi TPM 2.0 (Infineon SLB 9670 Chip)

Raspberry pi 4



Okdo E1 Development Board

Basys 3 FPGA

PMsec 2.0 Results

Primitive	Metrics	Results
PUF Results	XOR PUF On-Chip-Power	0.081 Watts
	SRAM PUF Key Code	32-Byte
	Key Extraction Time	77ms
	Reliability	99.8%
	Validation Time	1.1 seconds
TPM Evaluation Results	Platform Configuration Registers	16-23
	NVRAM Storage	768 Bytes
	Pi-TPM Power Consumption Range	2.9-3.3 Watts

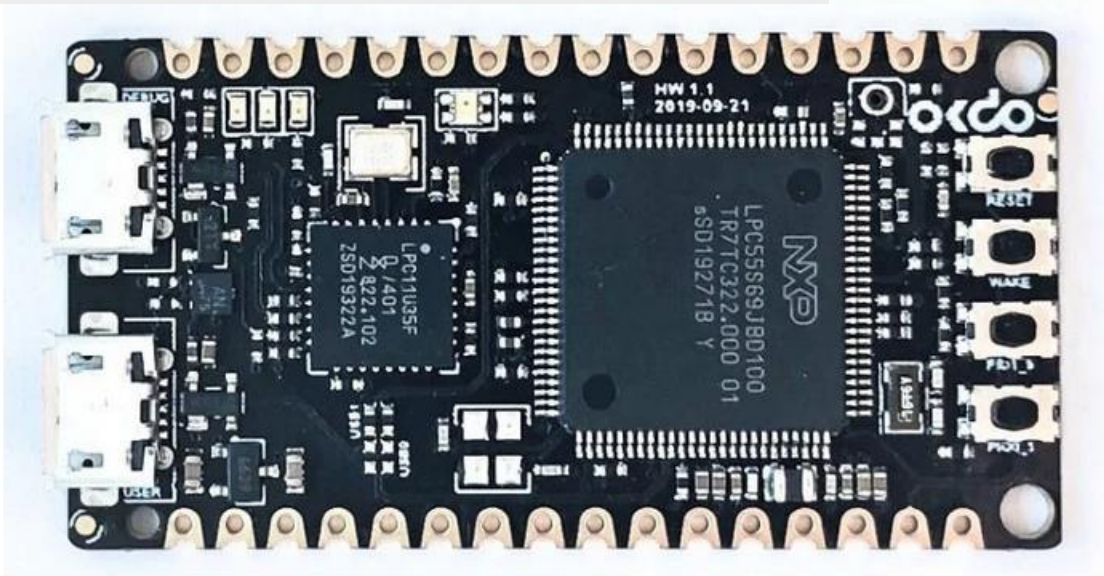
PUF Evaluation Results

Shell

```
>>> %Run PMsec2.py
 MAC Address
 dc:a6:32:c8:d7:50
 XOR Arbiter PUF Challenge Input
 [30, 10, 23, 39, 57, 37, 54, 64]
 Response
 ['1693234930.244491', 'dc:a6:32:c8:d7:50', '10101001001001110010011100100111001001110010011100100111001001110
 100111']
>>>
```

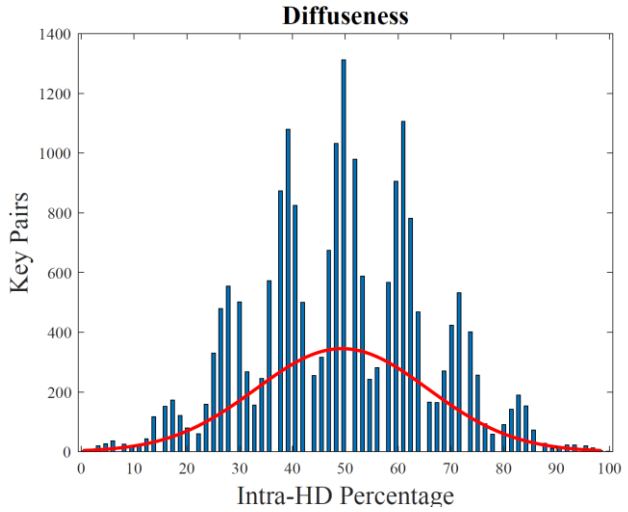
COM5 - PuTTY

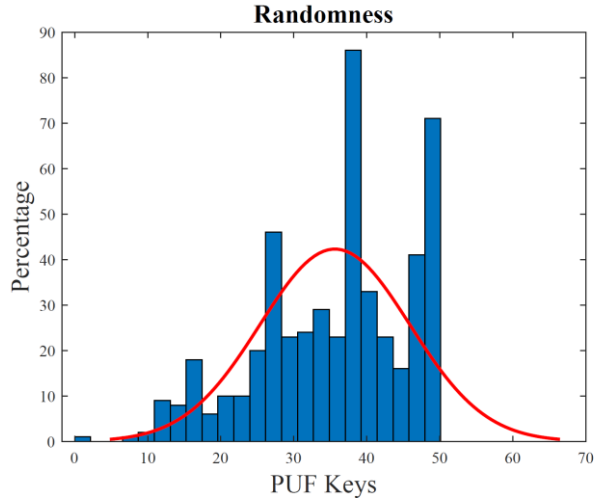
```
  48: b9 84 f3 50
Reconstruction of keycode:
size 16 bytes, index 1, type intrinsic

Key Code index > 0, Key will be printed
Key:

   0: a0 57 9c  0 fb 40 8a 89  3  b b4 17 a3 e5 71 99
****************** PUF state **********************
Allowed operations: Enroll  Start   SetKey  GetKey
                      no      no      yes     yes

PUF Status:         Busy   Success  Error
                      no      yes     no
**************************************************

1. Enroll PUF
2. Start and load AC to PUF
3. Misc. PUF commands
4. Generate Key Code
5. Get Key from Key Code
6. Encrypt / Decrypt AES block
7. Back
```

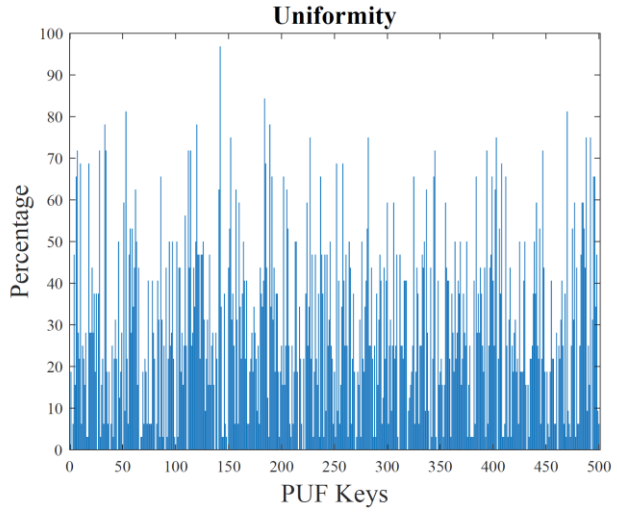


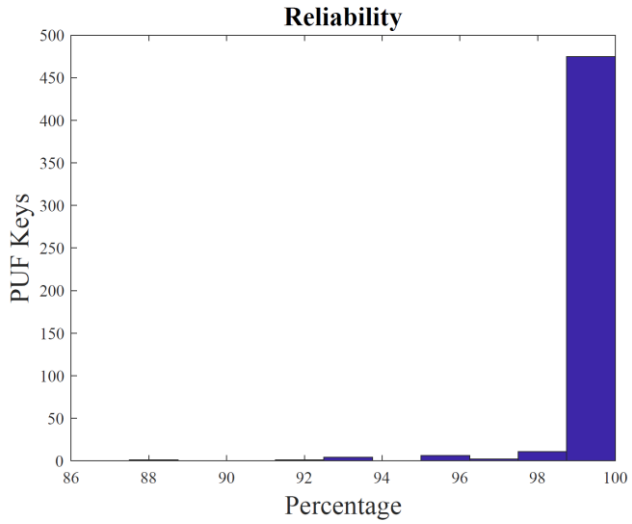
Source: https://asvin.io/physically-unclonable-function-setup/

XOR PUF Evaluation Results









TPM Remote Attestation Quote

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
pi@raspberrypi:~ $ sudo tpm2_quote -c 0x81010006 -l sha1:0,1+sha256:4,5 -q "12345678" -m q.quot
quoted: ff5443478018002200 0b2bae020c4d31bdc75c278712d539b957344309202716c487533354f984d9b4c400041234567800000000005f57dc0000000200000000010007005500 11cb0000000002000403030000000b033000000020
39f37f8d1931b3bdf767e7510dd69509fbf23af1f7654933d0a4d291cbdd4418
signature:
  alg: rsassa
  sig: 8de6a28f52d390c4df5dfc16f2a9cee788fdee6cc95d0265ecdf9f1965c24ad9efa78c75611165d001b1dd111734d872a9a0f16e1c70a9177e204fe872715b8dfeeb6f59d58ebc8ef4226d512ef44955f7d0c578c700fbc9bb7f772
2ef9cc55e2d005a3fffe27d24d83c965f9f1587107ccdce98222bcdbe3dad9f80d02ef9e4b87bf1348a137caccb6a5f31703b4376343c6bc20c328549ae1313a3697c5bb31f3729b1aaa440161ac2e45e6dec424086ea7dc55bfb78bdc54ae
2442eca689705127953a2cab34d63a8f24a3f889592834d53362f6be94fa673966c5561324939c2607839c00b1399023ea6981fdf6304eede333a66d2ad4fc3b7582e1a6863
pi@raspberrypi:~ $ sudo cat q.quot
TCG"
      +
       M1  \'  9 W4C    'S3T 4 Vx_W U
        :  eI3 r  D
pi@raspberrypi:~ $ sudo tpm2_print -t TPMS_ATTEST q.quot
magic: ff544347
type: 8018
qualifiedSigner: 000b2bae020c4d31bdc75c278712d539b957344309202716c487533354f984d9b4c4
extraData: 12345678
clockInfo:
  clock: 6248412
  resetCount: 2
  restartCount: 0
  safe: 1
firmwareVersion: 00cb110055000700
attested:
  quote:
    pcrSelect:
      count: 2
      pcrSelections:
        0:
          hash: 4 (sha1)
          sizeofSelect: 3
          pcrSelect: 030000
        1:
          hash: 11 (sha256)
          sizeofSelect: 3
          pcrSelect: 300000
    pcrDigest: 39f37f8d1931b3bdf767e7510dd69509fbf23af1f7654933d0a4d291cbdd4418
pi@raspberrypi:~ $ sudo tpm2_quote -c 0x81010006 -l sha1:0,1+sha256:4,5 -q "12345678" -m q.quot
quoted: ff5443478018002200 0b2bae020c4d31bdc75c278712d539b957344309202716c487533354f984d9b4c400041234567800000000006c46bf0000000200000000010007005500 11cb0000000002000403030000000b033000000020
39f37f8d1931b3bdf767e7510dd69509fbf23af1f7654933d0a4d291cbdd4418
signature:
  alg: rsassa
  sig: 81cc57a2747fa4063c948d25dff2144282fd29a7ccce4c7ab4a24c2b6b046a697d389faea1c7932470777cf3dec56676e029347609b484930105f9c52048b58348c09503fc2b91d05f8c8b29e44dde325a3606c385a3a92a32b4ef5
feb90ff168b914bc3f3ef785706b8d0eb7c314c7e3376d21143c9b7f98264e02e4a41f48e767e69ac9893eb81f904ffe865117229910ba649f9c64b9529c113da9df0ebbbd539b5dcefd307ef07dad2fded9b28bd41c383461f986203a0df1
1cc9f5e648e5f1b842af2b1f23aee1a2f1bda05680bf903b501b94dab17056cb700fea5007e9116ae91bbfdc1e0e952b7a19fe9b8b0c20d1f8ddbbd4c00c89bf7031d426e8a
pi@raspberrypi:~ $ sudo tpm2_print -t TPMS_ATTEST q.quot
magic: ff544347
type: 8018
qualifiedSigner: 000b2bae020c4d31bdc75c278712d539b957344309202716c487533354f984d9b4c4
extraData: 12345678
clockInfo:
  clock: 7095999
```

Summary

- This work has successfully presented and validated a global access control framework to access and control PUF-embedded IoMT devices.
- Security-by-Design (SbD) advocate features at early design phases, no-retrofitting.
- A novel PUF and TPM-supported authentication scheme that verifies the integrity of devices in the proposed PUF-driven cybersecurity scheme for IoMT.
- Successful integration of PUF with TPM truly substantiates the potential of the proposed cybersecurity solution in e-health, and telehealth ecosystems.
- A sustainable TPM-based novel approach for integrity verification in H-CPS using TPM's Remote Attestation scheme.

Future Research

- Idea of implementing PUF-based TPM scheme for the Security-by-Design (SbD) for secure Doctor Patient Interface.
- Exploring the feasibility of a Trusted Platform Module (TPM) integrated scalable Blockchain-based cryptographic scheme to attain the Security by Design (SbD) objective in IoMT.
- Working on an integrated access control mechanism for resource-constrained electronic devices using TPM
- Developing scalable and sustainable TPM-enabled IoT device authentication scheme for Fog, Edge, and Cloud Computing Paradigms.
- Extending iTPM scheme for the resource-constrained IoMT and Internet of Agro-Things security.
- As a direction for future research, a distributed ledger technology integration can be proposed for securely accessing data among different healthcare systems around the world.

Thank you