PUFchain 4.0: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT

Presenter: Venkata K. V. V. Bathalapalli

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

University of North Texas, Denton, TX, USA.[1,2,3,5] and
Grambling State University[4].

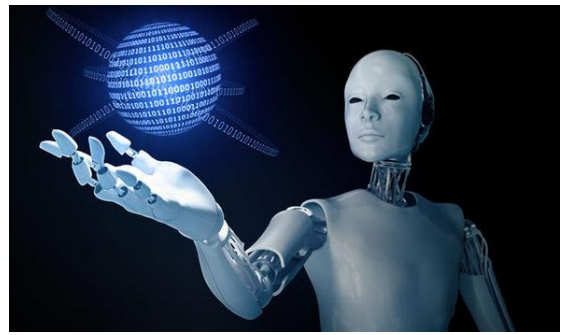
Email: **vb0194@unt.edu, saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3], iyerv@gram.edu[4], bibhudutta.rout@unt.edu[5]**

Outline

- Security-by-Design (SbD) Principle
- Novelty of Proposed PUF-based-TPM Solution
- PUFchain-Variants (PUFchain 1.0, PUFchain 2.0, PUFchain 3.0)
- Working Flow of Proposed PUFchain 4.0
- Experimental implementation Overview
- Conclusion & Future Research Directions

GLSVLSI 2023 - PUFchain 4.0

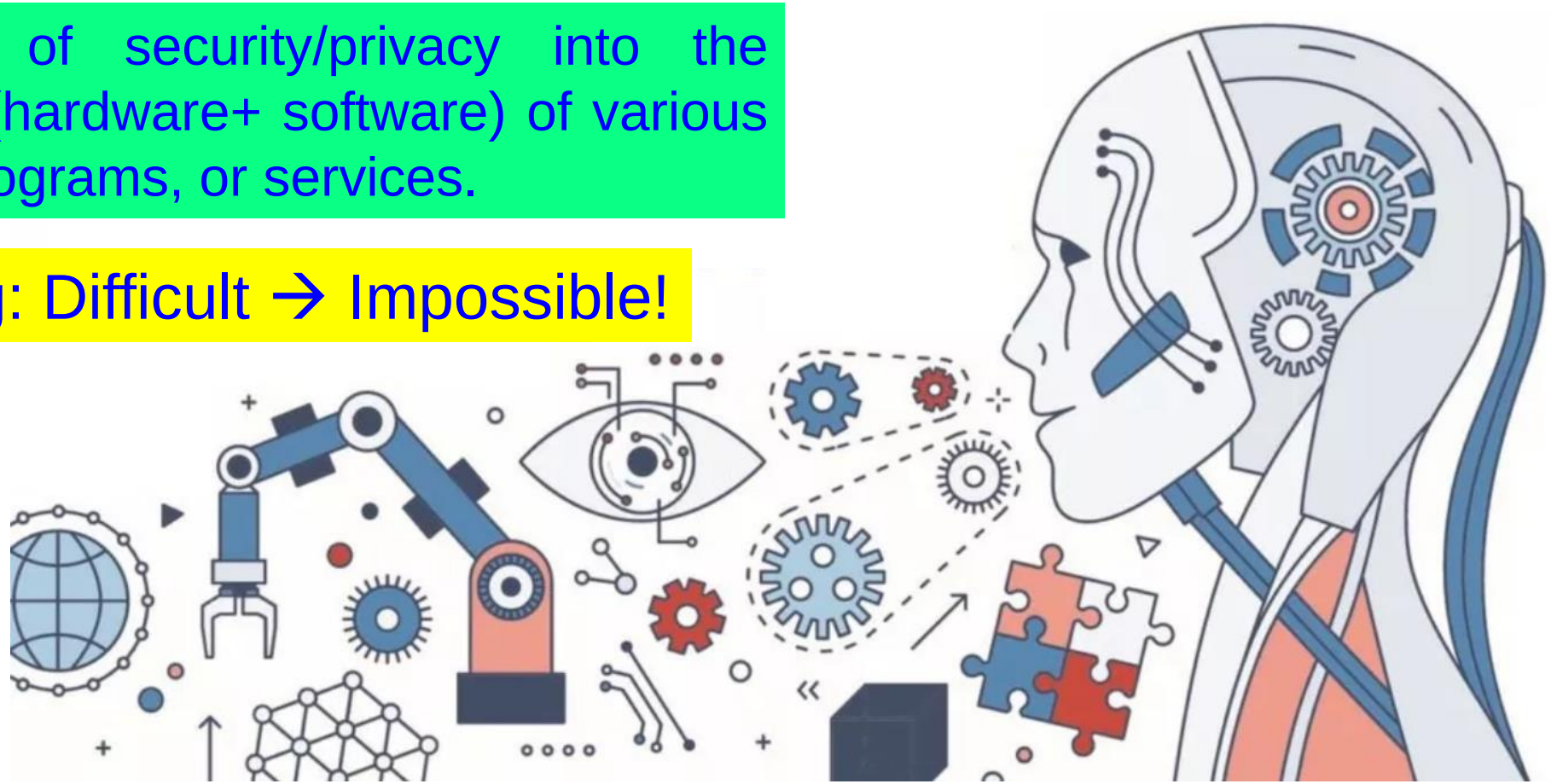
Security-by-Design (SbD) – The Principle



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

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

Retrofitting: Difficult → Impossible!



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

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

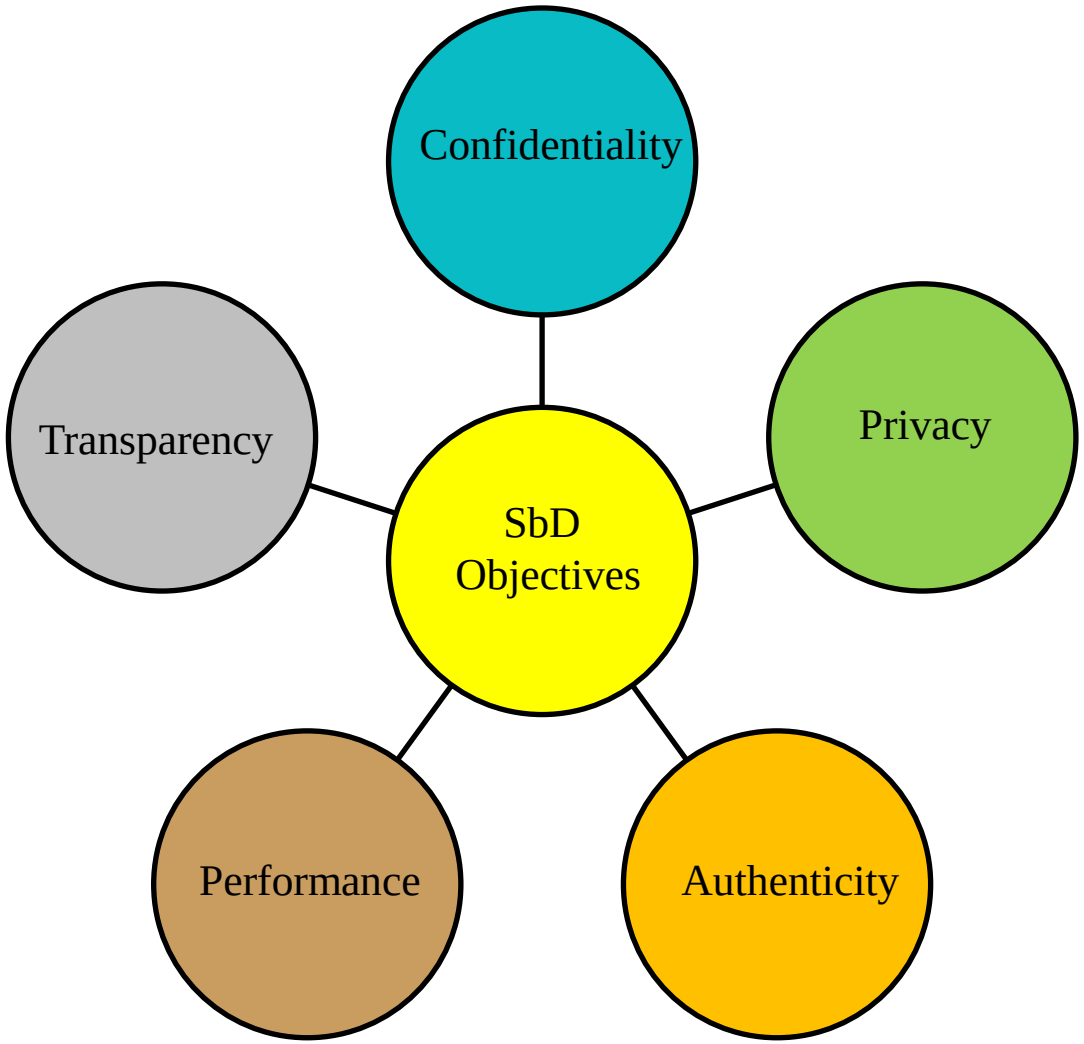
Security by Design (SbD)-Principles

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

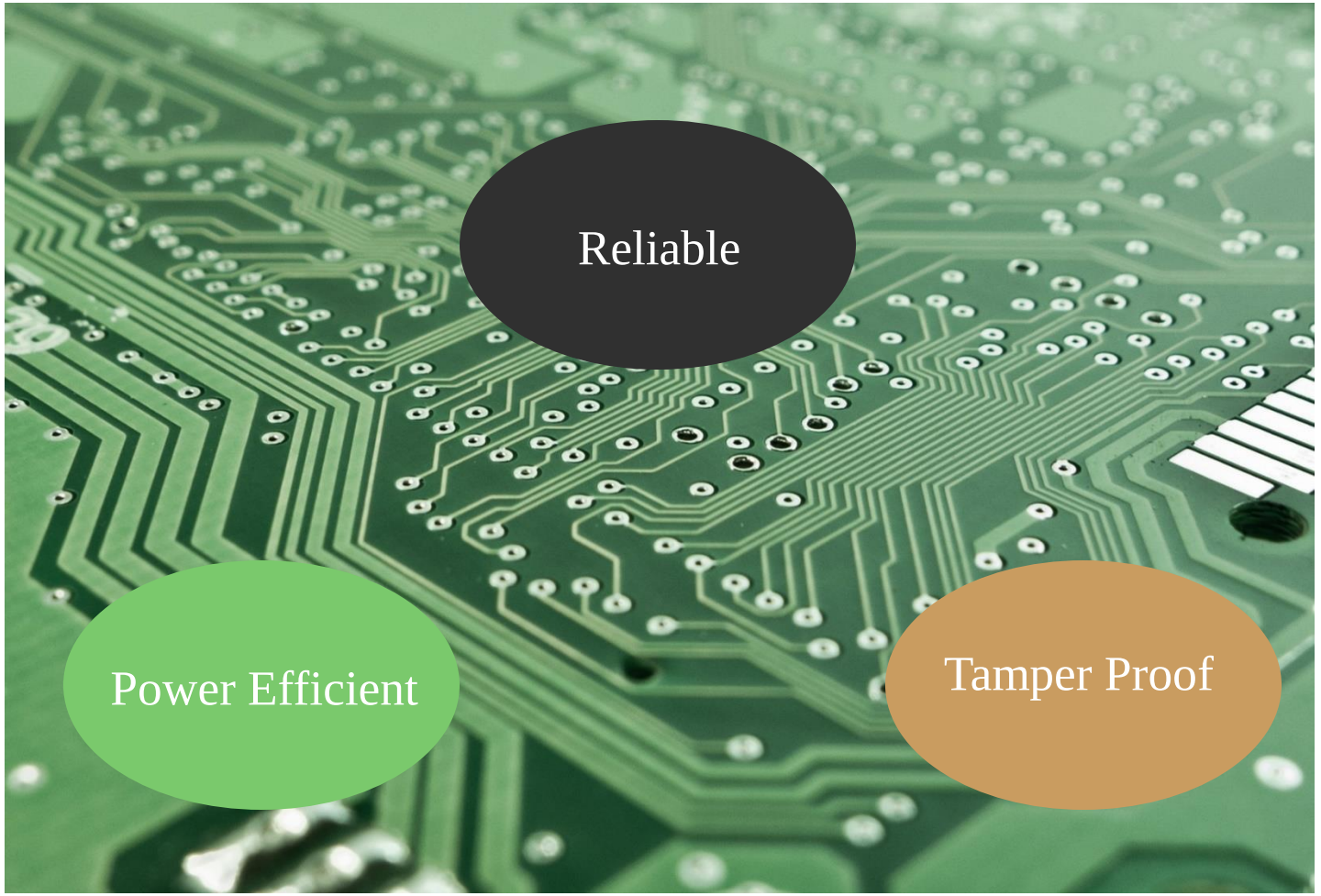
Source: S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4-5, 1 March 2020, doi: 10.1109/MCE.2019.2954959.

Objectives of SbD/PbD



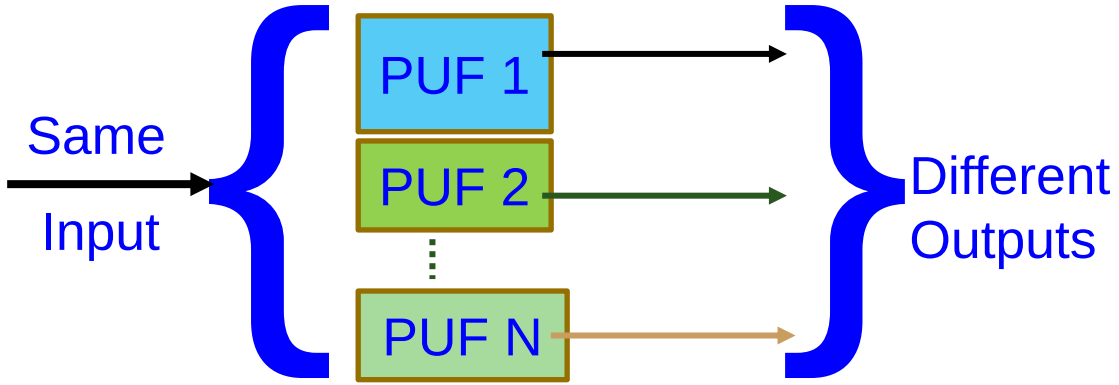
Physical Unclonable Function (PUF)-Introduction

PUF: A Hardware-Assisted Security Primitive



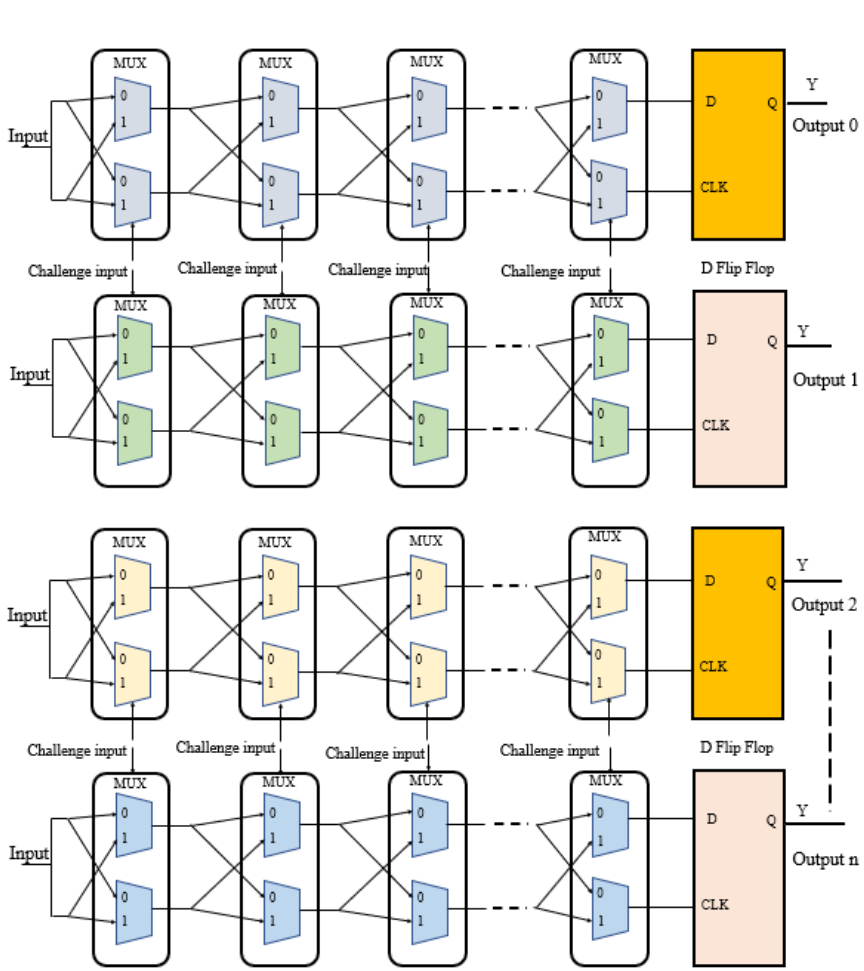
- A secure fingerprint generation scheme based on process variations in an Integrated Circuit
- PUFs don't store keys in digital memory, rather derive a key based on the physical characteristics of the hardware; thus secure.
- A simple design that generates cryptographically secure keys for the device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

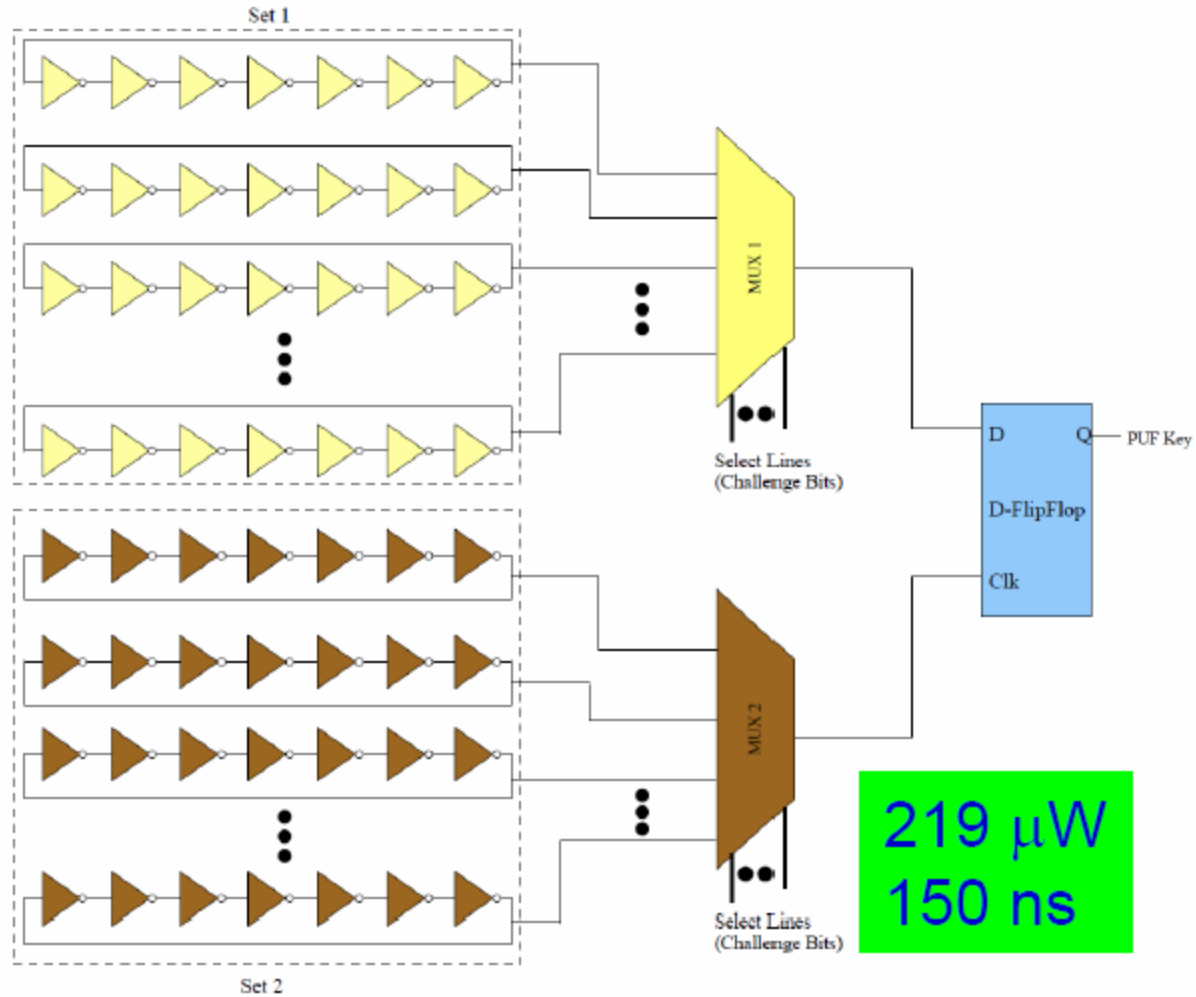
PUF Key Generation and Working



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

PUF Designs



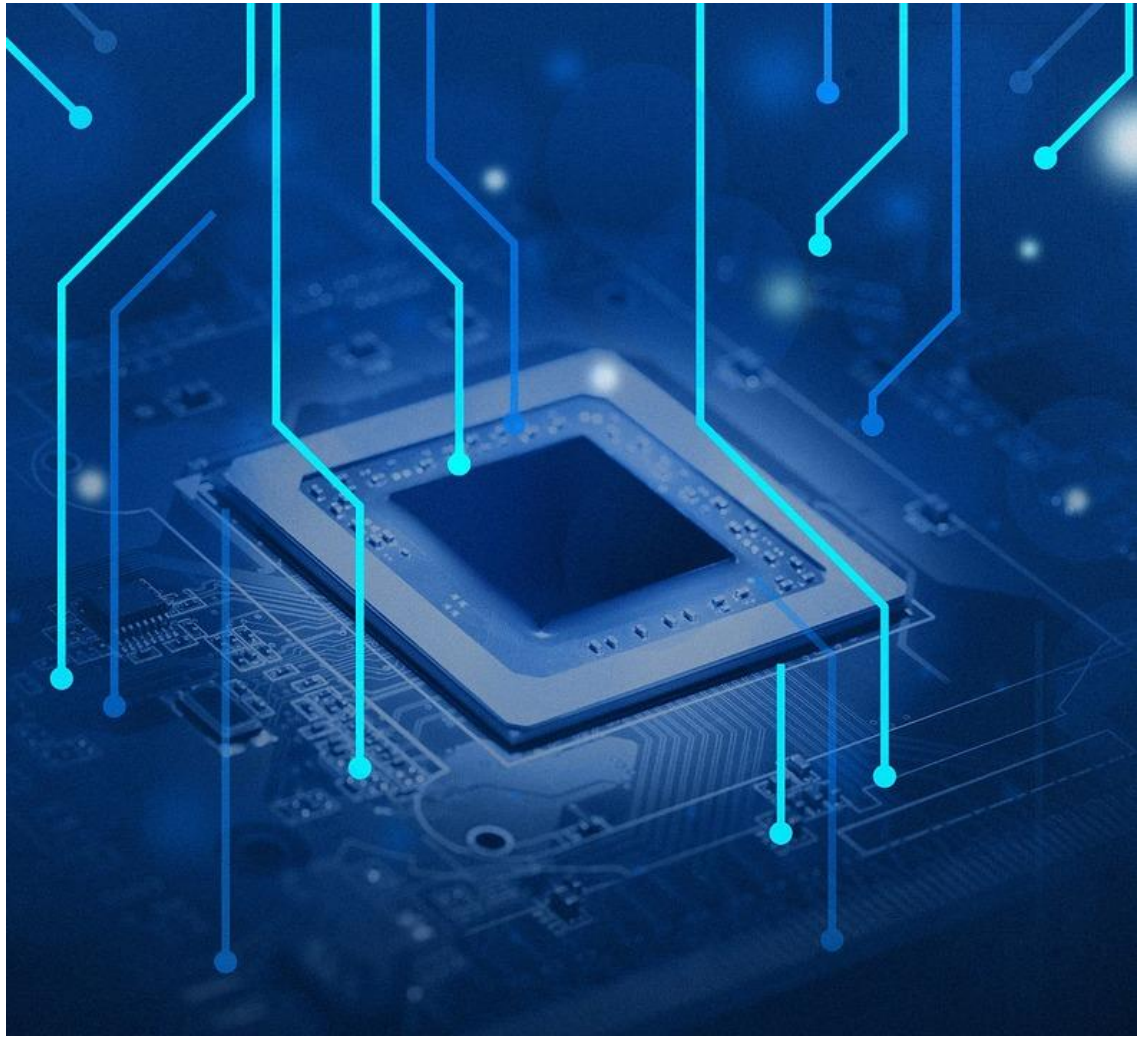


Source: iSES 2019 Demo (PMsec: PUF-Based Energy-Efficient Authentication of Devices in the Internet of Medical Things (IoMT))

Trusted Platform Module (TPM)-Overview

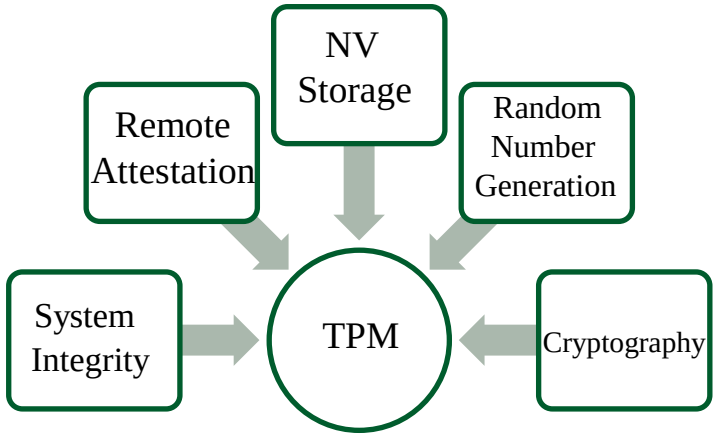
Trusted Platform Module-Introduction

- A TPM is a secure cryptoprocessor that offers a range of capabilities to enhance the security of a computing system.
- TPM's Non-Volatile Memory (NVRAM) enables the sealing and unsealing of secret keys and the storage of passwords generated inside or outside TPM.
- TPMs perform remote attestation of an entity for security and privacy
- Additionally, TPMs provide extensive support for cryptographic operations such as encryption, decryption, and digital signatures.



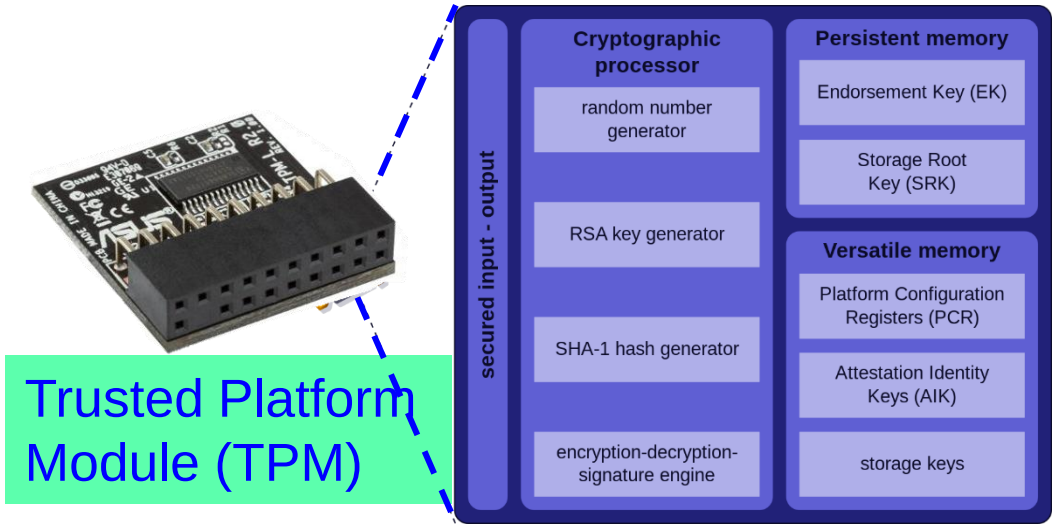
Functionality of TPM

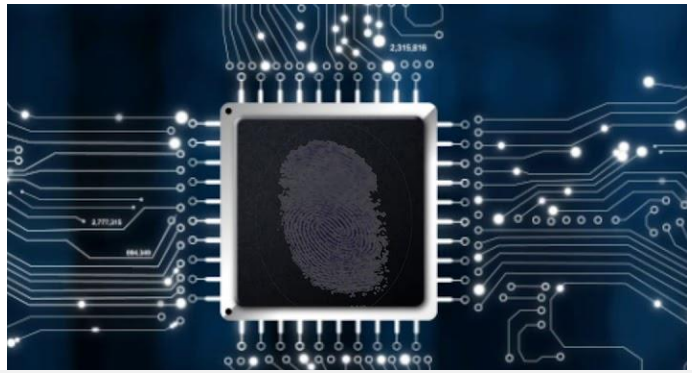
- A TPM consists of a cryptographic sub-system along with two memories, one non-volatile and one volatile. The Endorsement Key (EK) is an RSA key with a 2048-bit length, stored at the non-volatile memory, and is created by the TPM manufacturer to be able to identify this unique chip.
- A specified NV-index is defined for ensuring secure storage and retrieval of private keys. Access to TPM NVRAM can be user-defined and password-protected, following TCG's procedures.
- TPM's attestation identity key is a cryptography key used to generate a digital signature during remote attestation.
- The system configuration parameters during the boot process are stored inside the TPM's Platform Configuration registers (PCR).



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.

PUF versus TPM





Physical Unclonable Functions (PUF)

Source: Electric Power Research Institute (EPRI)

TPM:

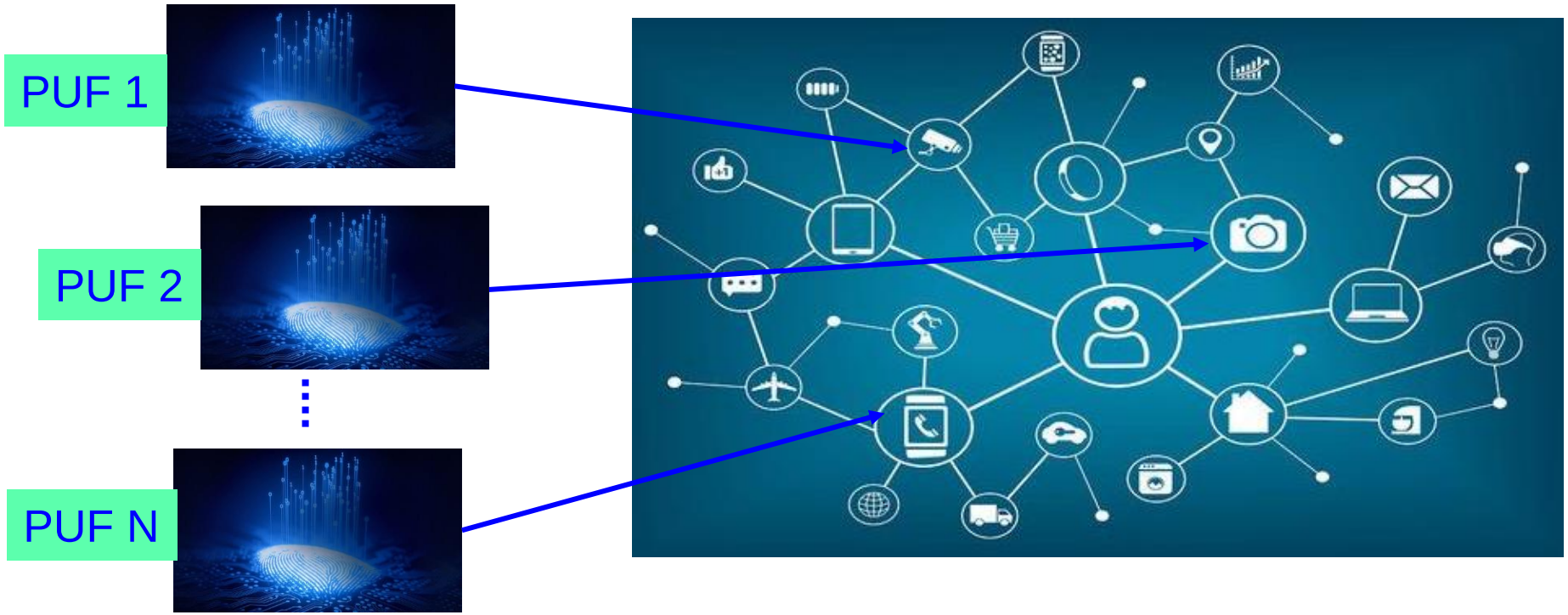
1) The set of specifications for a secure crypto-processor and
2) The implementation of these specifications on a chip

PUF:

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

Our PUFchain

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

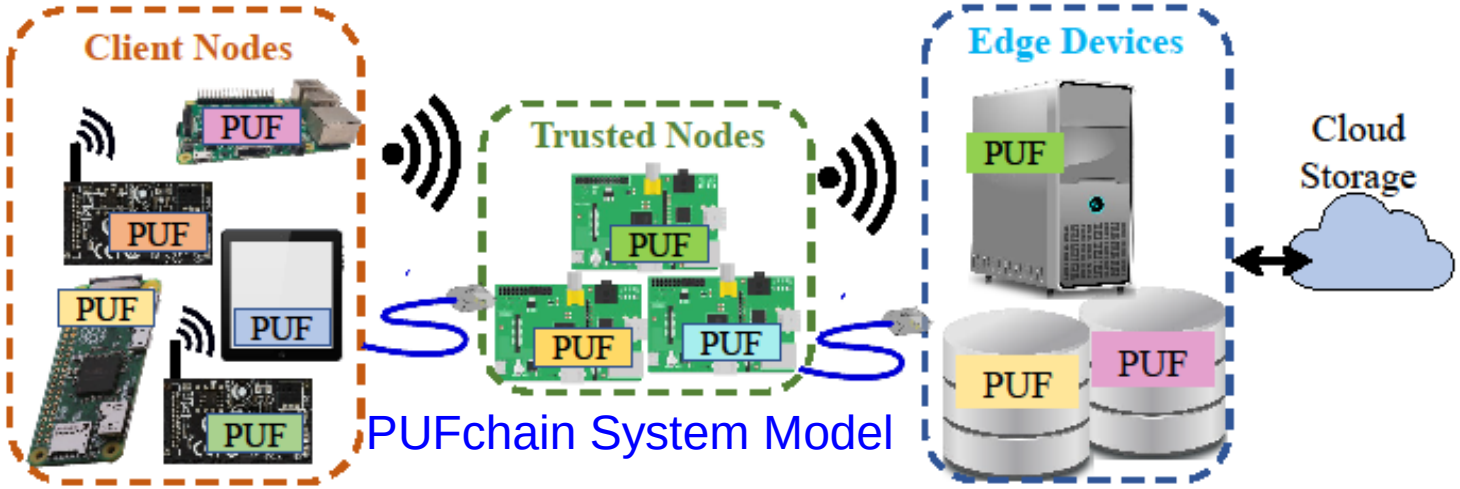


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

Our PUFchain – 4 Variants

Research Works	Distributed Ledger Technology	Focus Area	Security Approach	Security Primitive	Security Principle
PUFchain	Blockchain	IoT / CPS (Device and Data)	Proof of Physical Unclonable Function (PUF) Enabled Authentication	PUF + Blockchain	Hardware Assisted Security (HAS) or Security-by-Design (SbD)
PUFchain 2.0	Blockchain	IoMT/CPS (Device and Data)	Media Access Control (MAC) & PUF Based Authentication	PUF + Blockchain	Hardware Assisted Security (HAS) or Security-by-Design (SbD)
PUFchain 3.0	Tangle	IoT/CPS (Device and Data)	Masked Authentication Messaging (MAM)	PUF + Tangle	Hardware Assisted Security (HAS) or Security-by-Design (SbD)
PUFchain 4.0 (This Paper)	**Tangle**	**IoT/CPS (Device)**	**PUF Based TPM**	**PUF + TPM Tangle**	**Hardware Assisted Security (HAS) or Security-by-Design (SbD)**

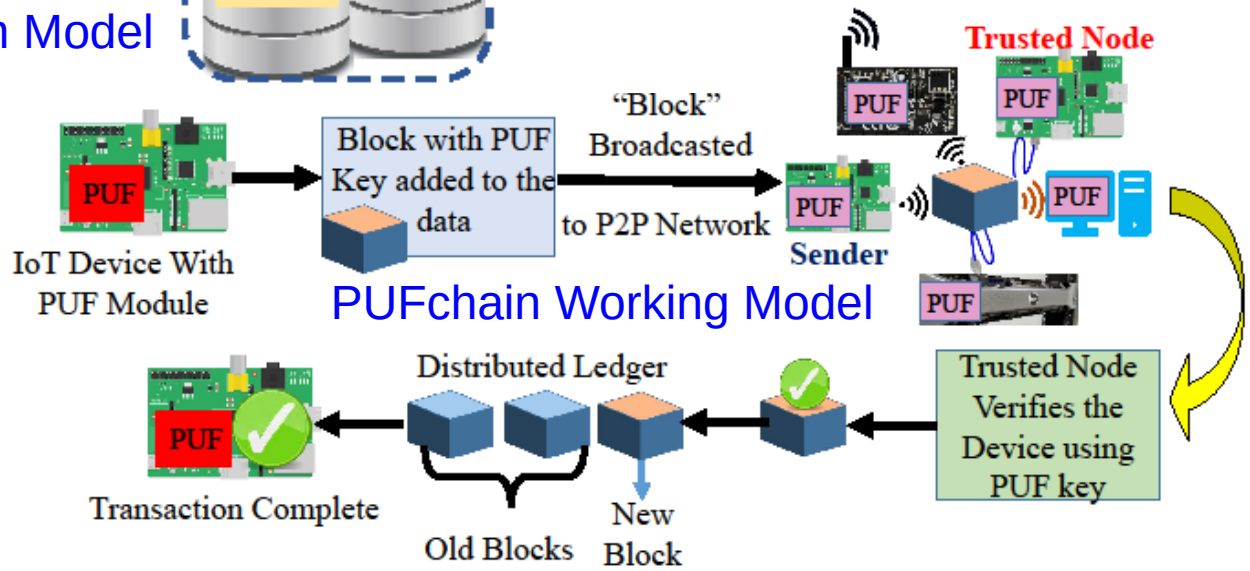
PUFchain: Our Hardware-Assisted Scalable Blockchain



PUFchain System Model

Can provide:
Device, System, and Data Security

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

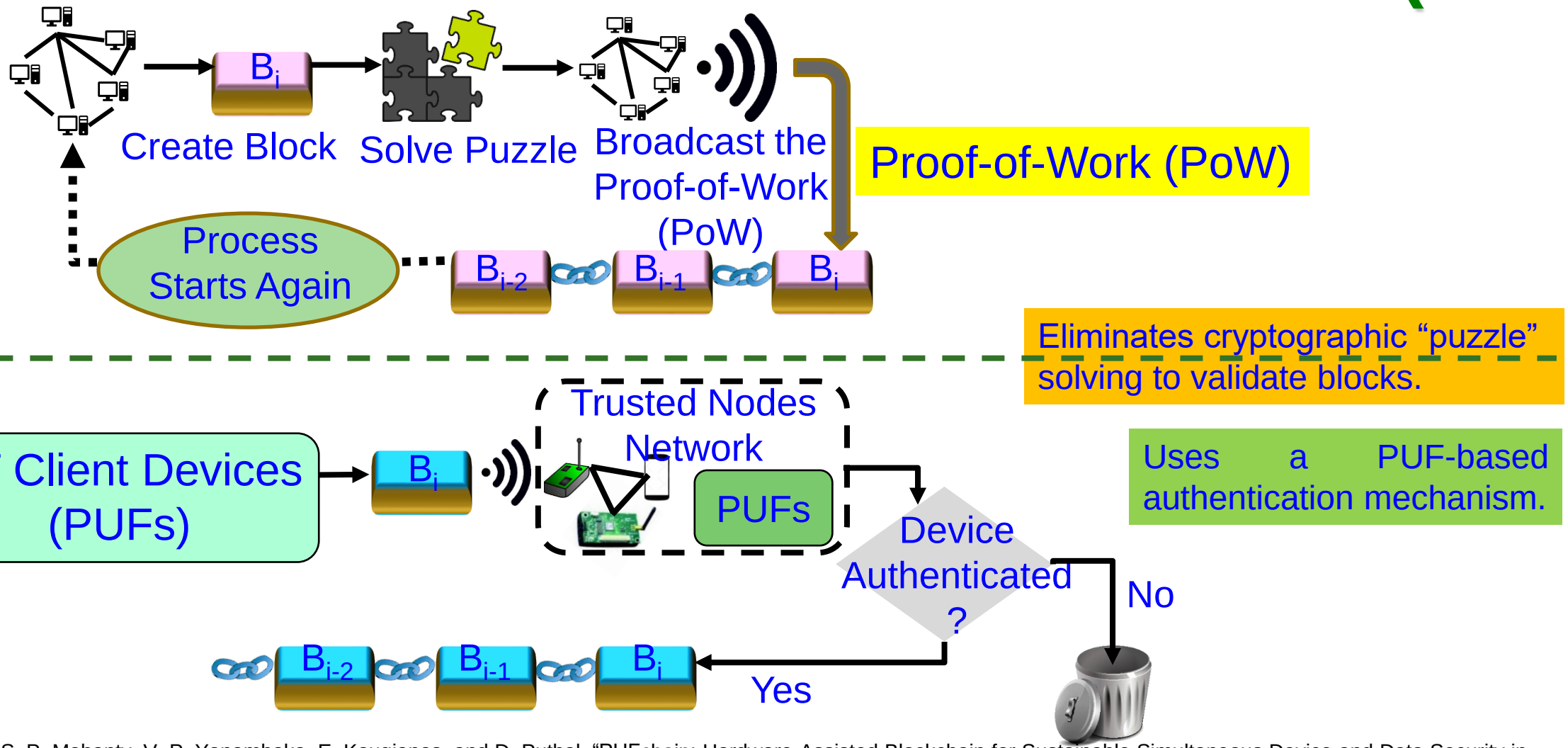


PUFchain Working Model

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

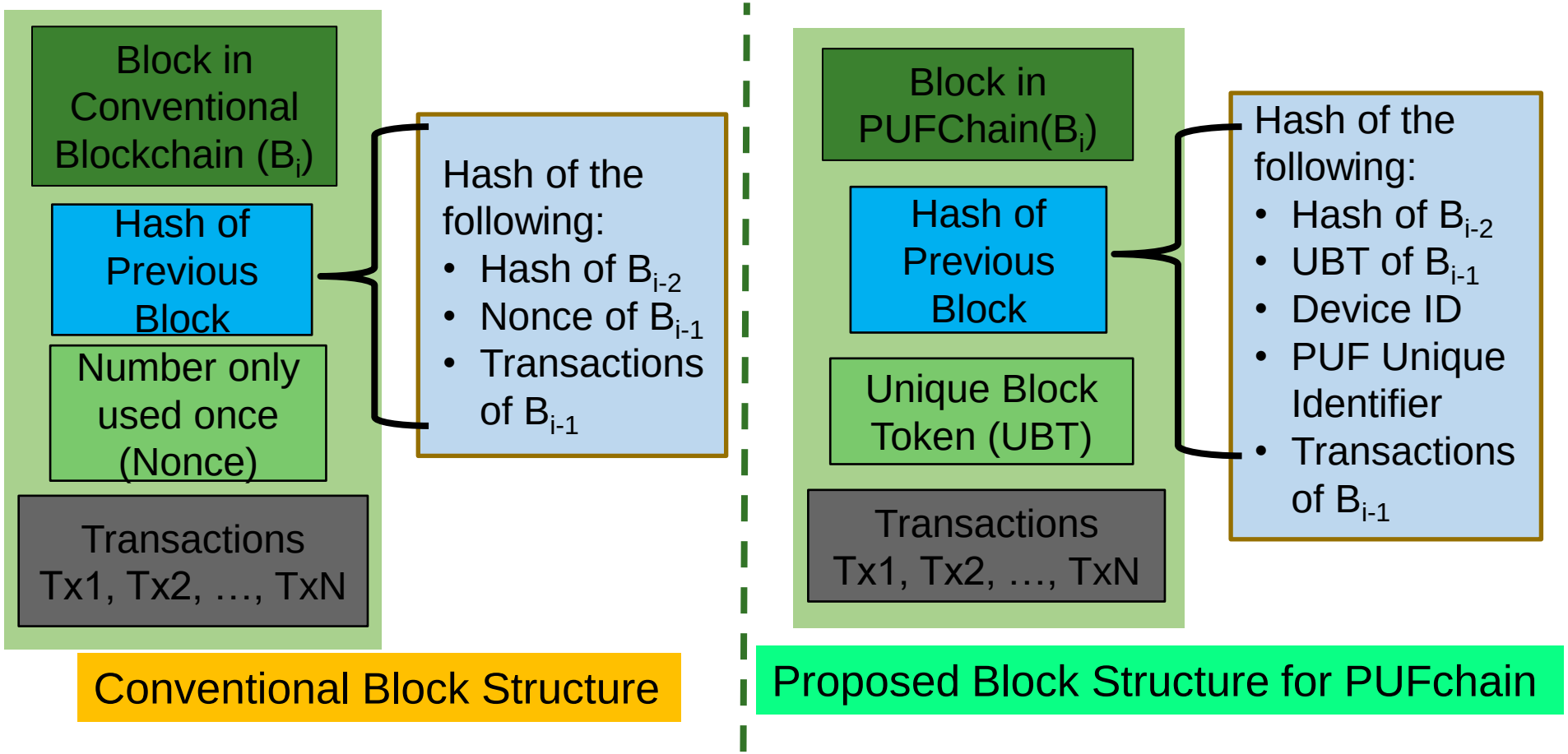
Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

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

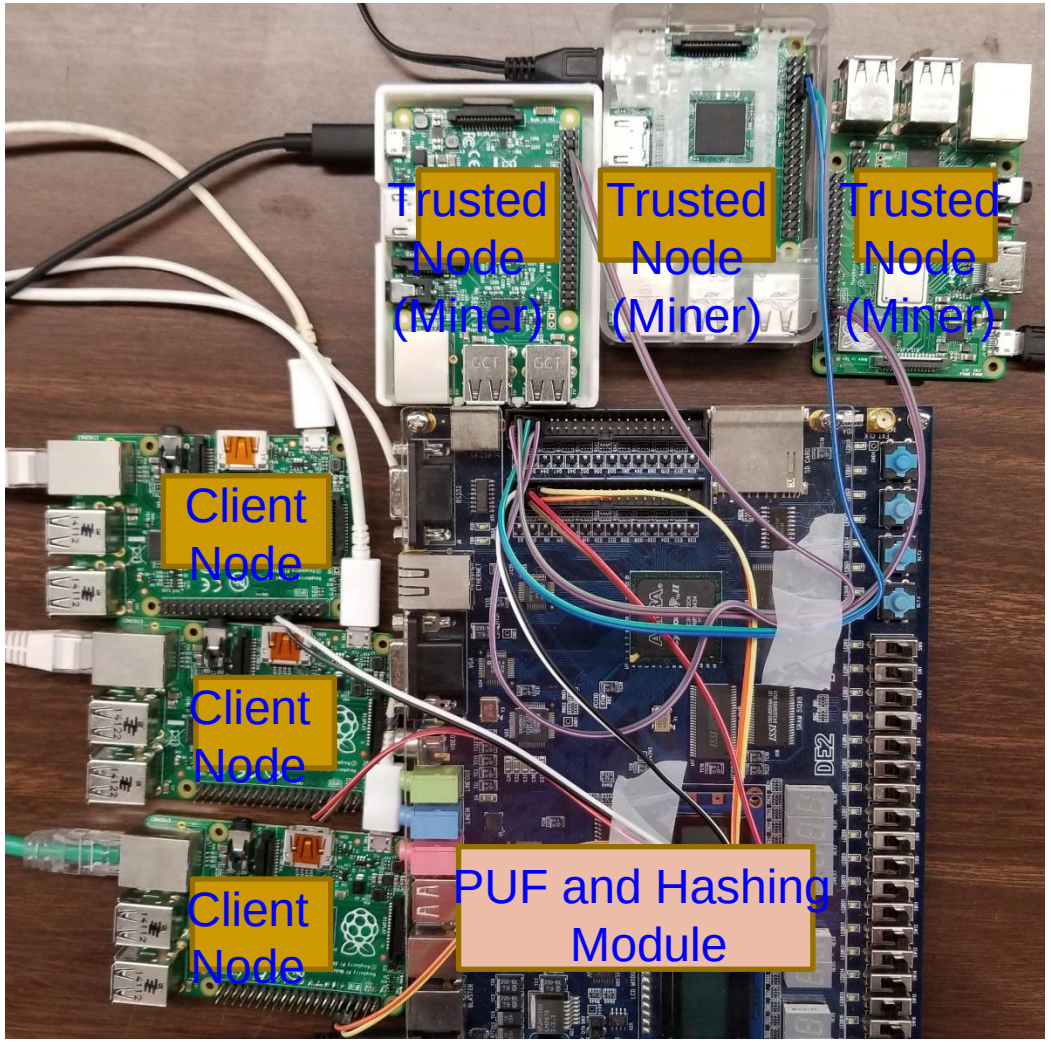


Source: S. P. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in Internet of Everything (IoE)", *IEEE Consumer Electronics Magazine (MCE)*, Vol. 9, No. 2, March 2020, pp. 8-16.

PUFchain: Proposed New Block Structure



Our PoP is 1000X Faster than PoW



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

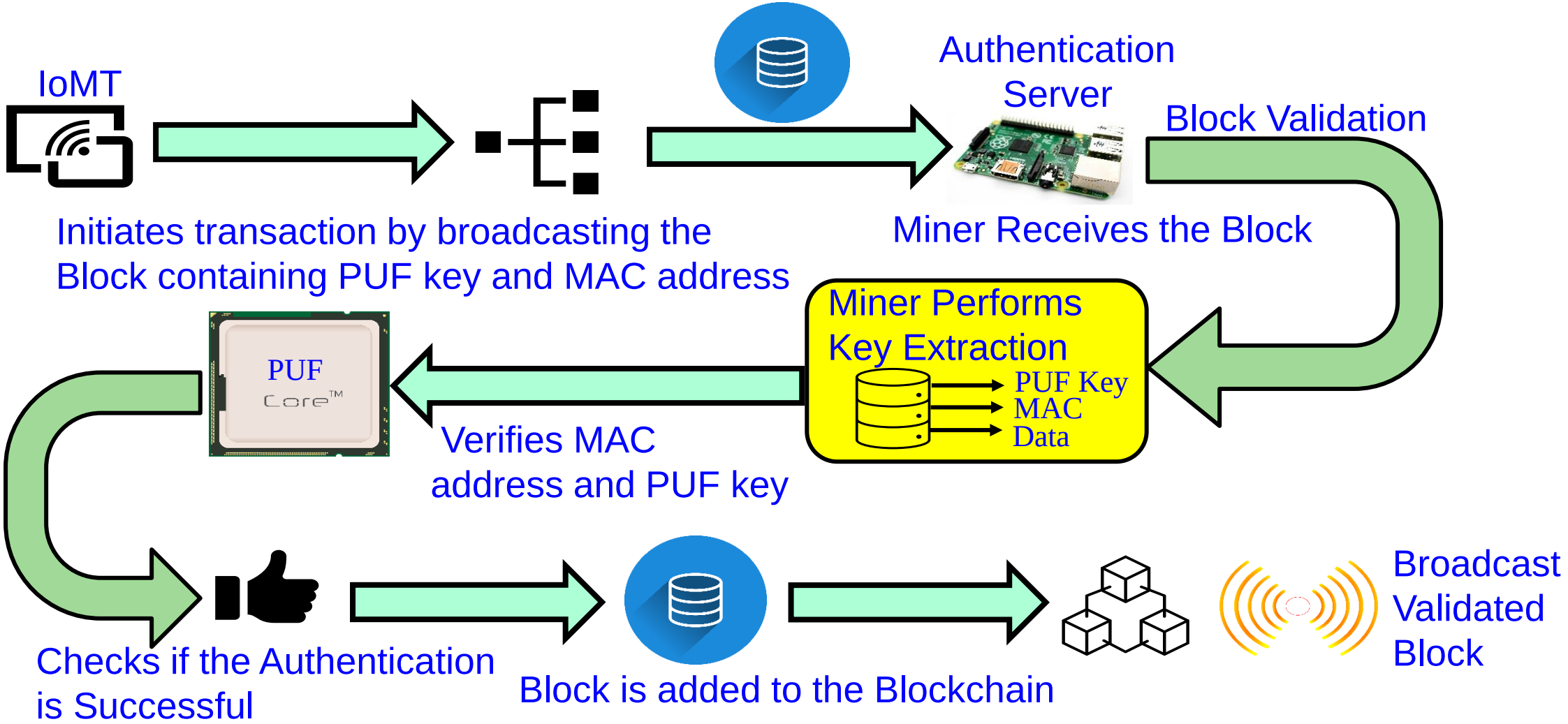
- ✓ PoP is 1,000X faster than PoW
- ✓ PoP is 5X faster than PoAh

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

PUF-based Scalable Blockchain for
Smart Healthcare

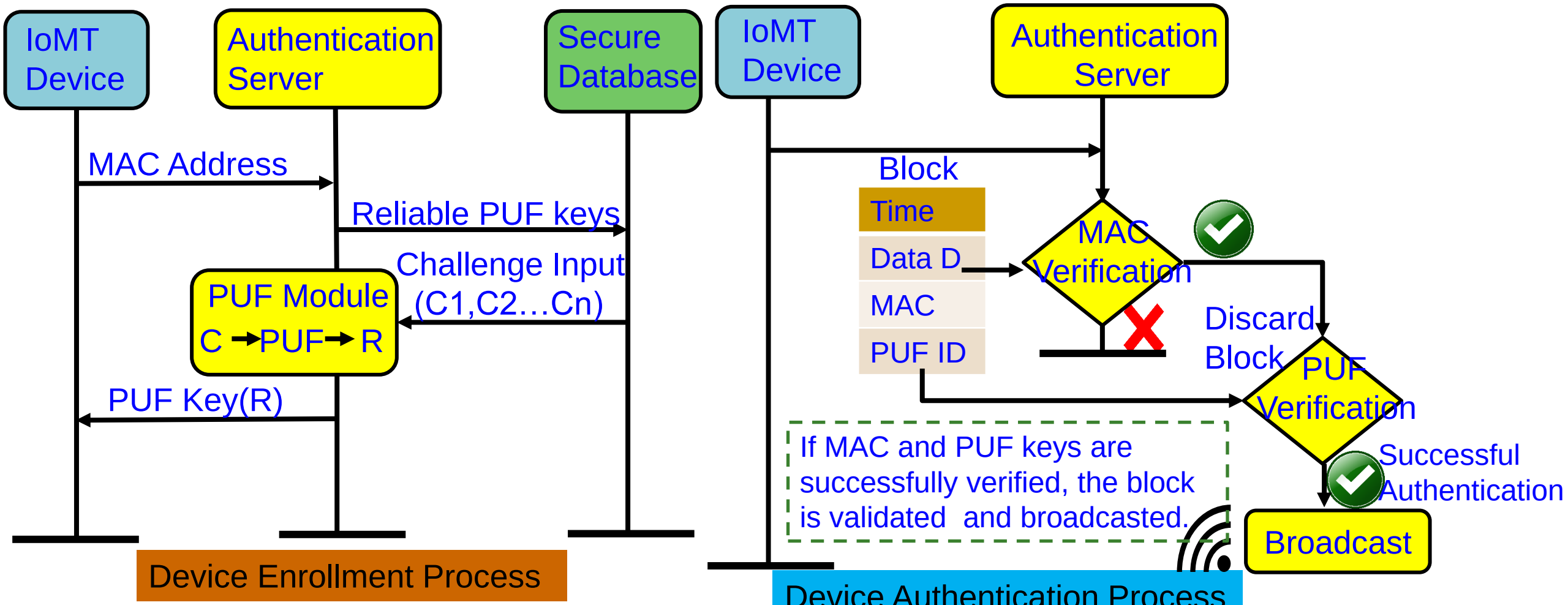
PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare

PUFchain 2.0: Our Hardware-Assisted Scalable Blockchain



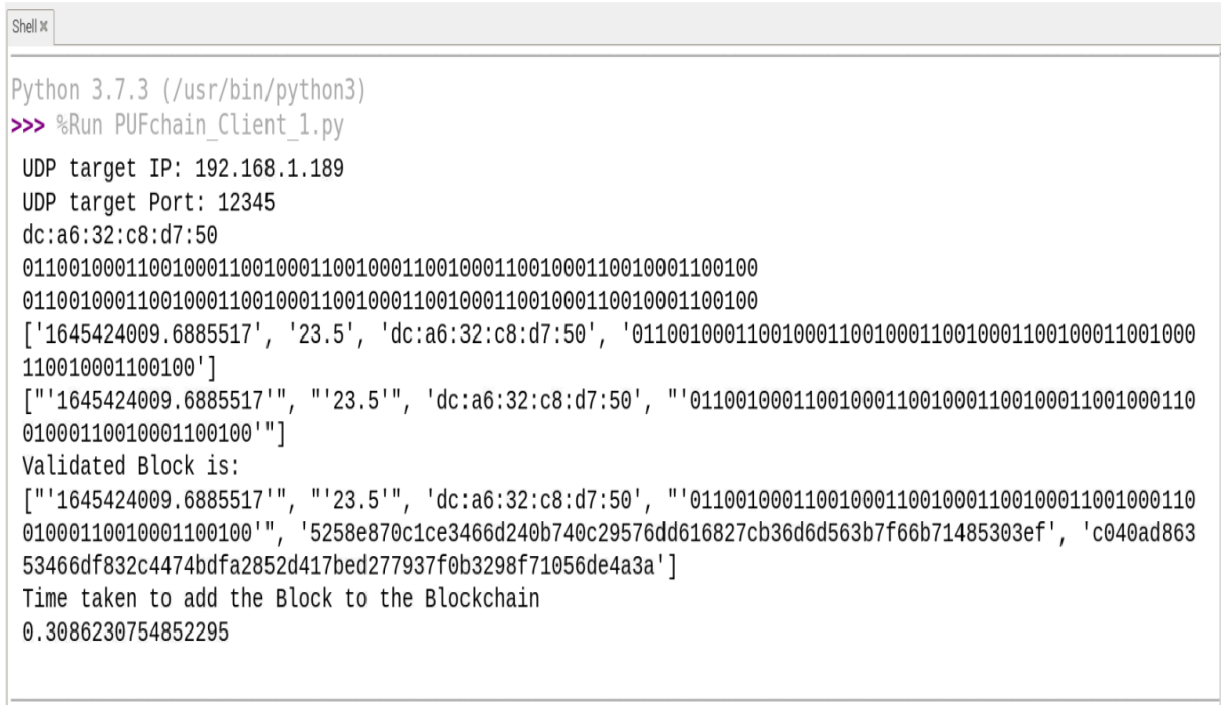
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

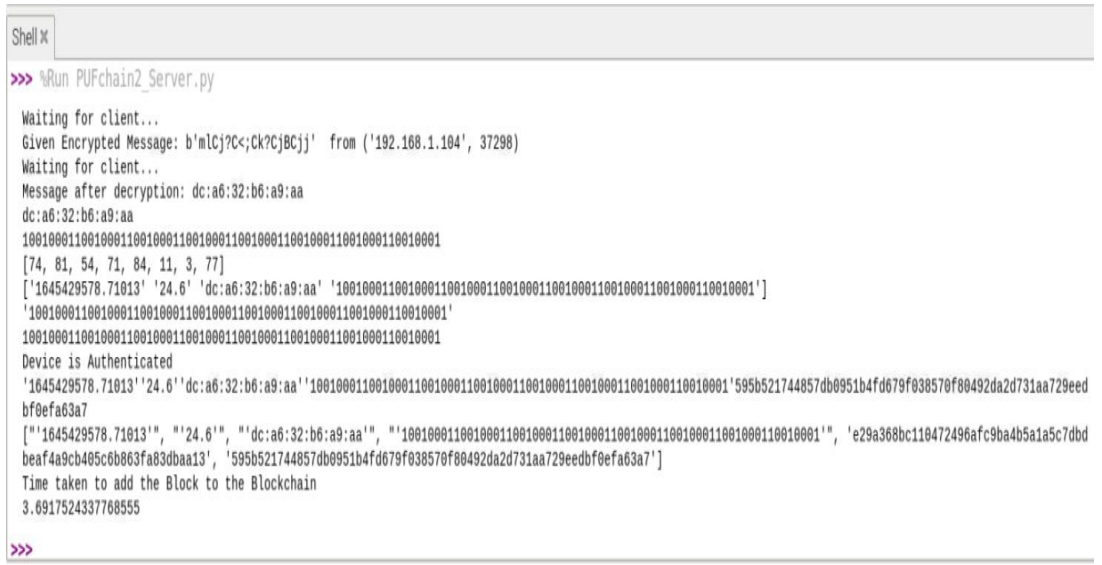
PUFchain 2.0: PUF Integrated Blockchain …



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

Implementation and Validation of PUFchain 2.0



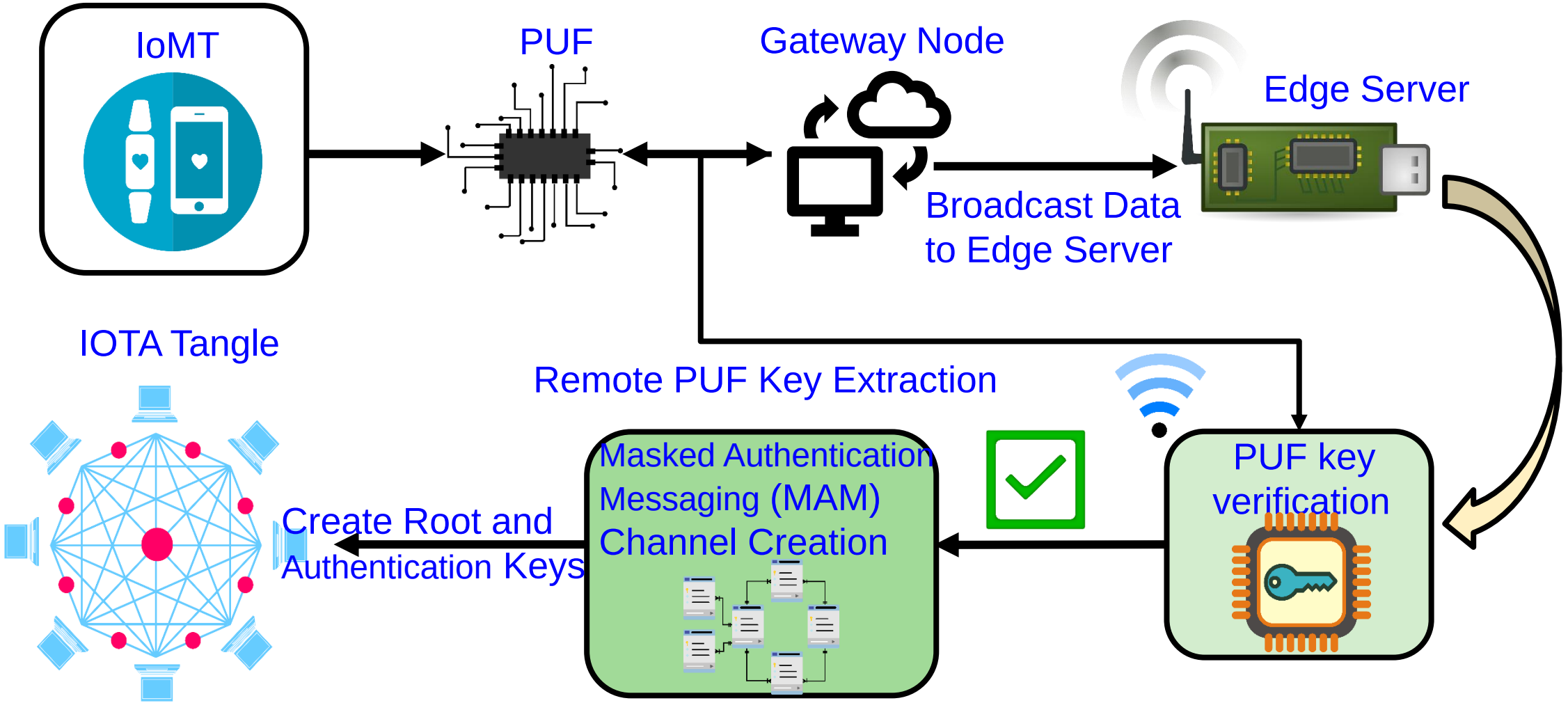


Source:V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare", *Springer Nature Computer Science (SN-CS)*, Vol. 3, No. 5, Sep 2022, Article: 344,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

PUF-based DLT for
Internet-of-Medical-Things Security

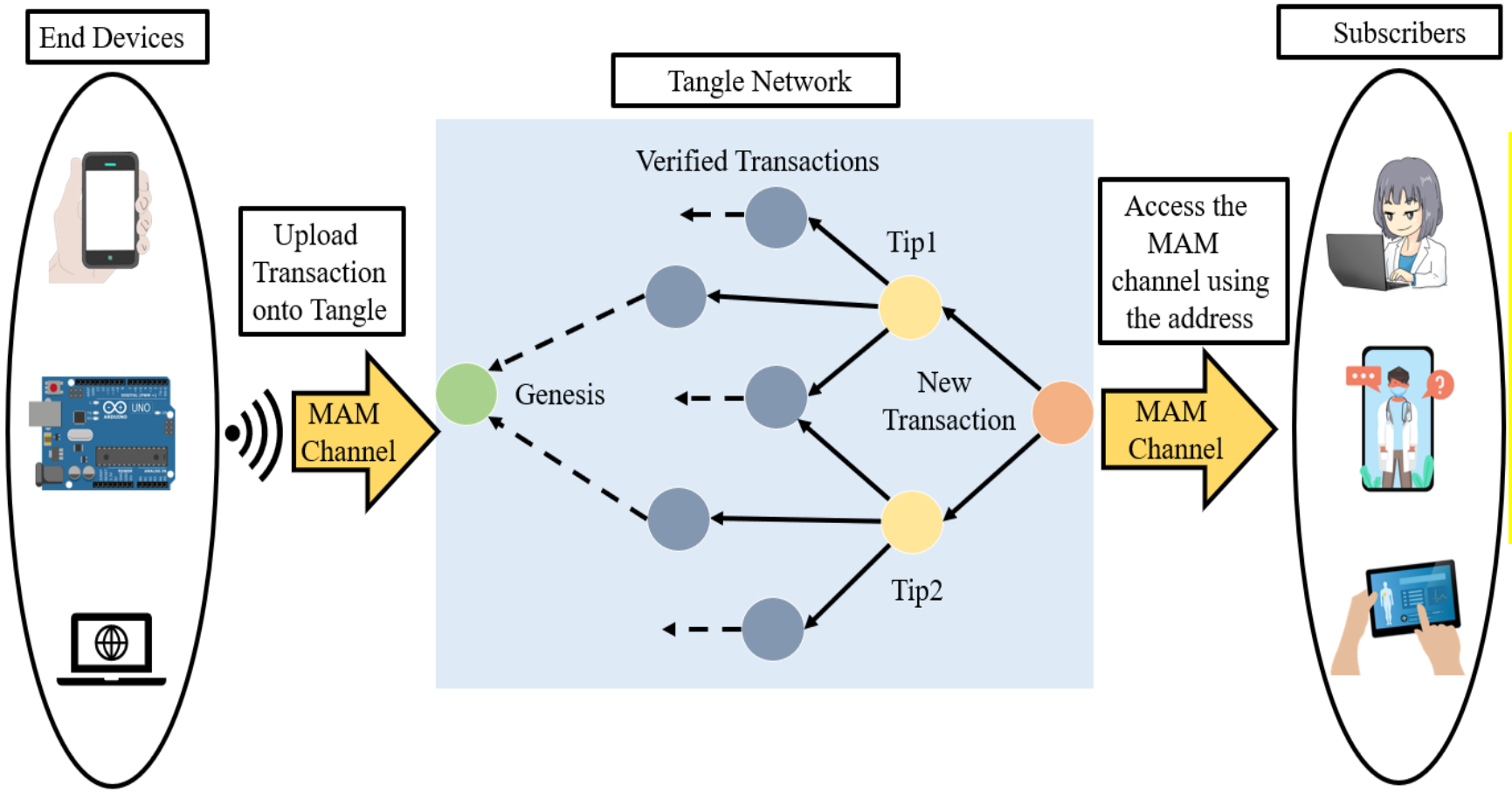
PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things

Architectural Overview of PUFchain 3.0



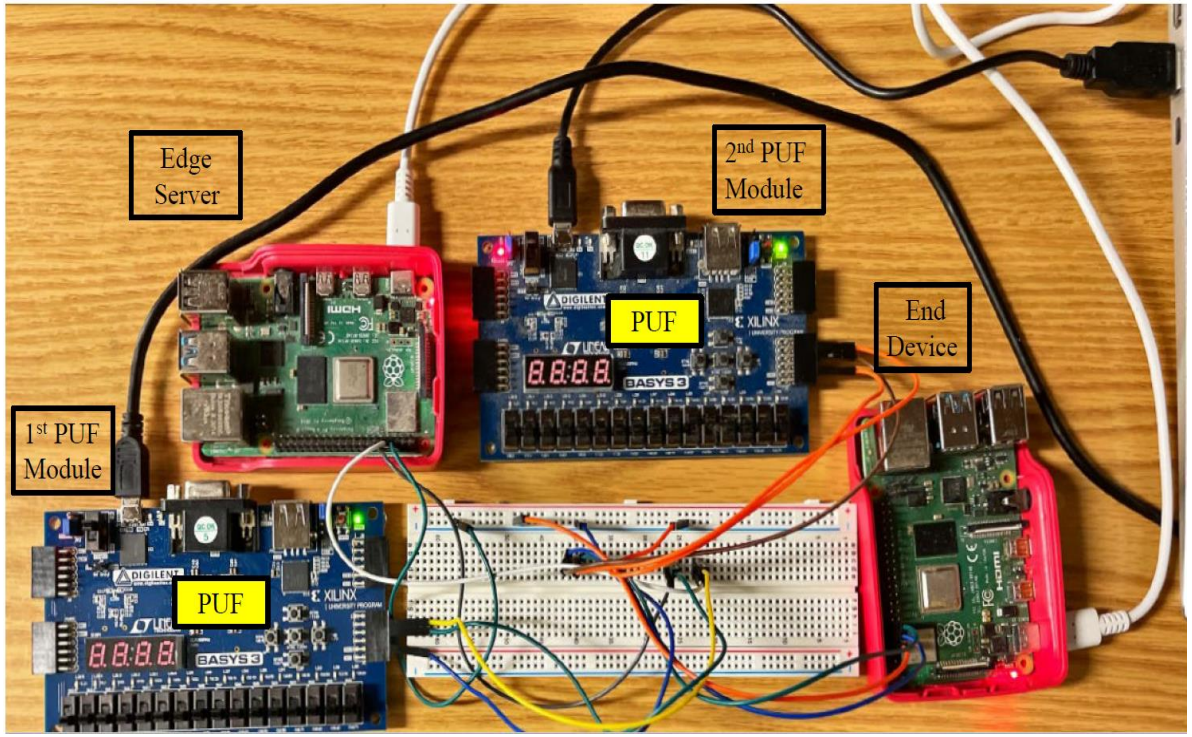
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40,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

Masked Authentication Messaging (MAM) in IOTA Tangle



- Provides Device and Data security in IoT
- Works in Three modes: Public, Private and Restricted

PUFchain 3.0: Prototype



PUFchain 3.0 Parameters	Specifications
Application	Internet-of-Medical Things
Database	Tangle
Programming Languages	JavaScript, Verilog, and Python
PUF Keys Extracted	500
PUF Design	Arbiter PUF
PUF Module	Xilinx xc7a35tcpg236-1
IOTA Network	Mainnet
Communication Protocol	Masked Authentication Messaging
Edge Server	Single Board Computer

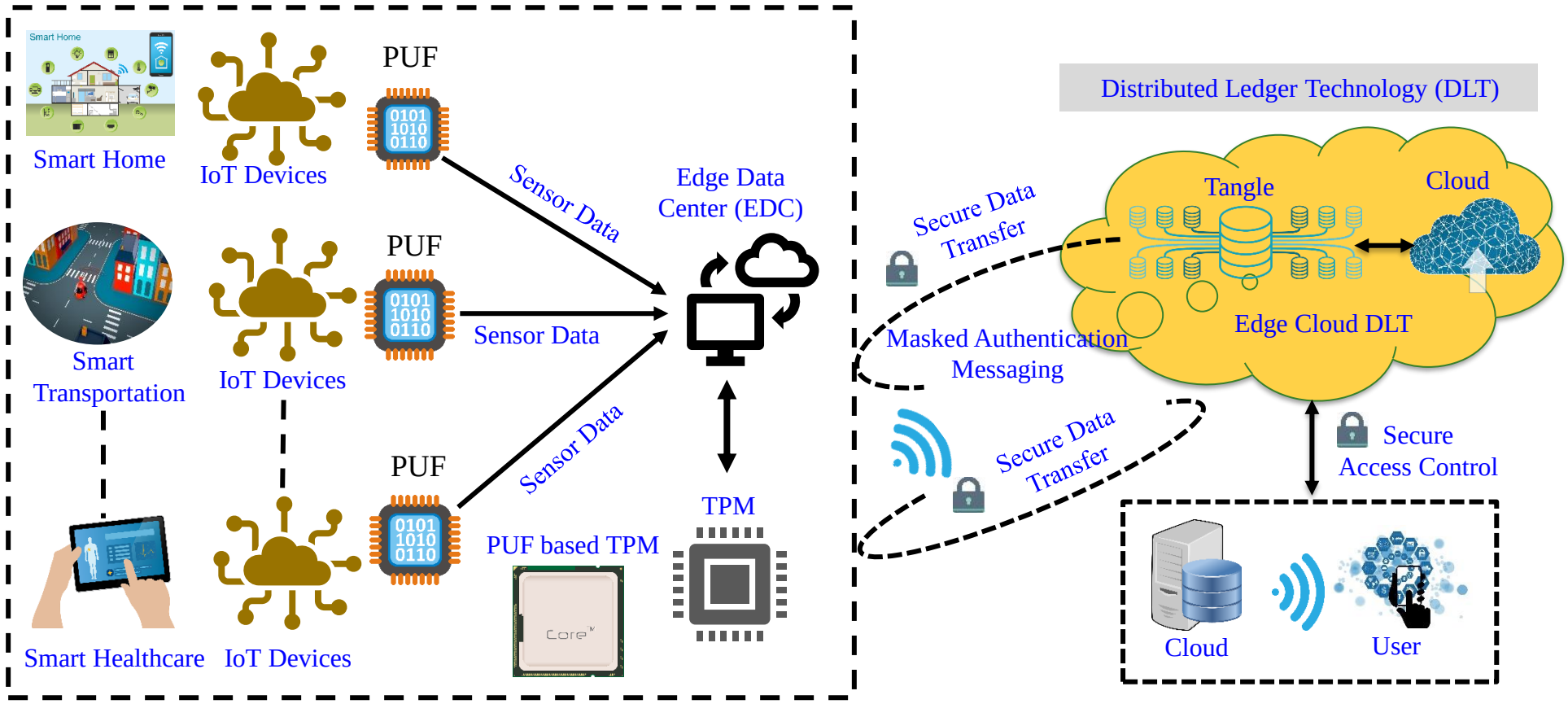
Source: V. K. V. V. Bathalapalli, **S. P. Mohanty**, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things", in *Proceedings of IFIP International Internet of Things Conference (IFIP-IoT)*, 2022, pp. 23--40,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

Our PUFchain 4.0

Novel Contributions

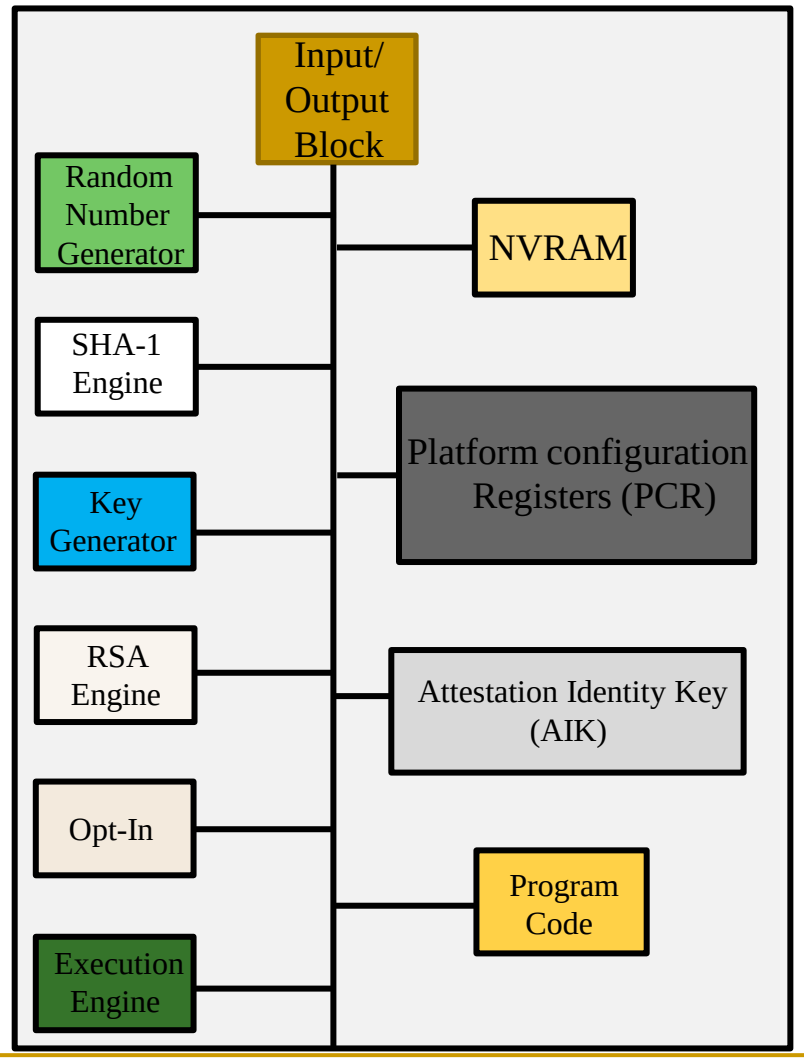
- A sustainable Hardware-Assisted security approach using TPM and PUF for ensuring the root of trust for the Security-by-Design of IoT.
- A security mechanism that utilizes Masked Authentication Messaging (MAM) for secure storage, retrieval, and authentication of IoT device properties and sensor data in Tangle.
- A robust approach for device integrity validation through the secure interface between TPM and PUF hardware security primitives.
- An approach that facilitates hardware-level secure storage for PUF key by accessing TPM Non-Volatile memory.
- A robust and lightweight security mechanism that can facilitate Hardware signature-based access control to DLT through a PUF-based TPM approach.
- A sustainable approach for PUF key verification and PUF-enabled TPM-based access control mechanism for miner-free and feeless DLT for data security in IoT.

Proposed PUF based TPM for SbD in IoT

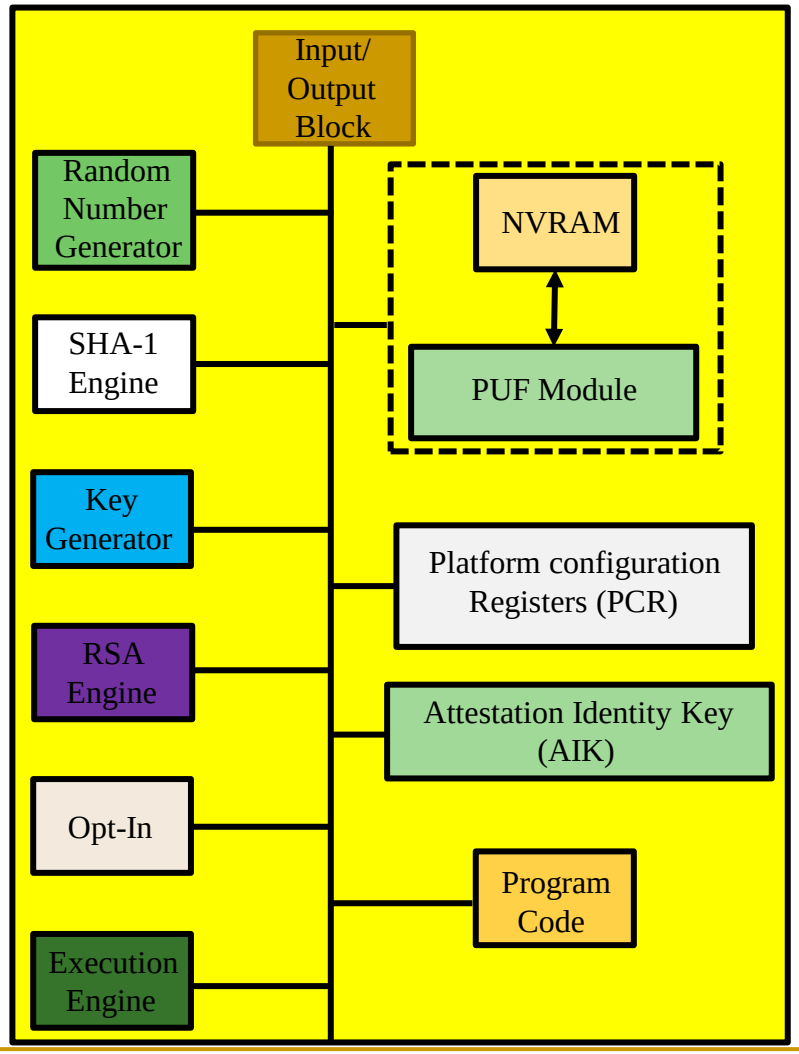


Architecture of Proposed PUF-based TPM

Conventional TPM Architecture



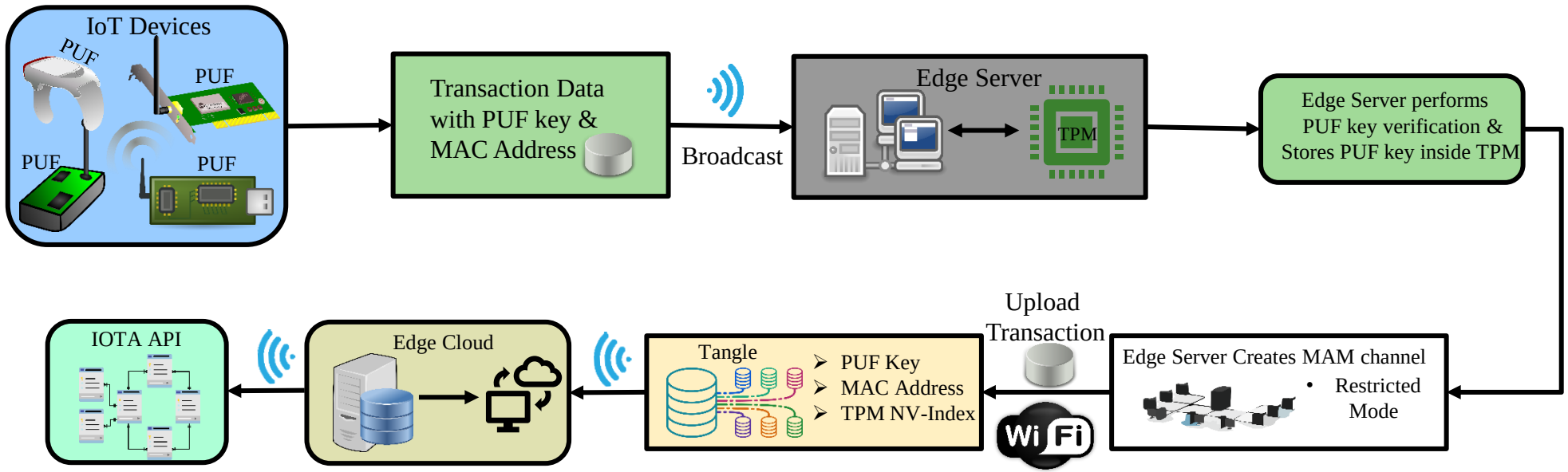
PUF-based TPM Architecture



Related Research Overview

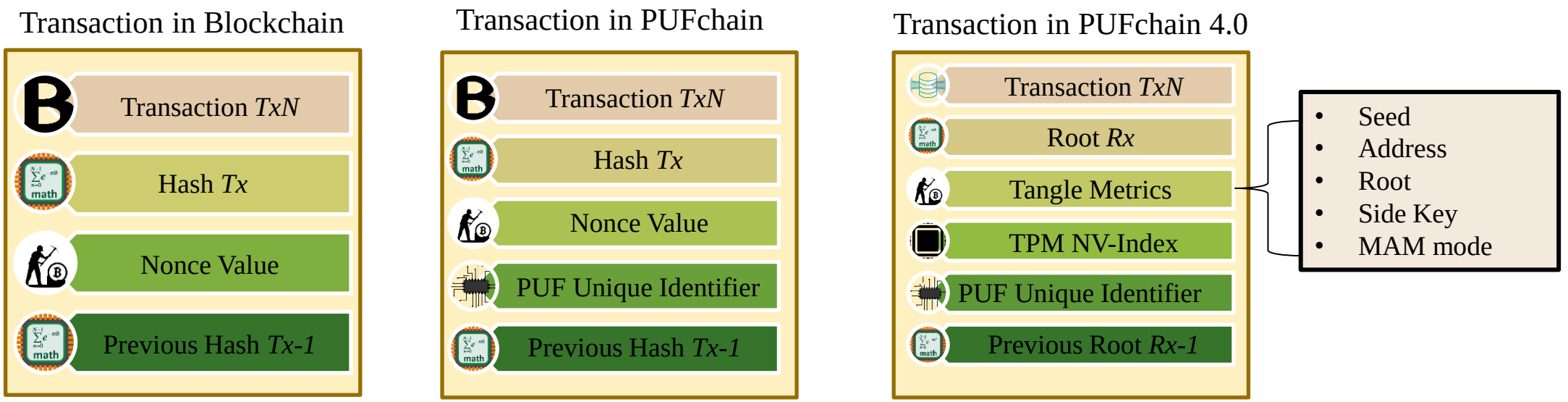
Work	Application	Security Primitive	Mechanism	TPM	Data Security Primitive
PUFchain[16]	IoT (Device & Data)	Physical Unclonable Functions (PUF)	Proof-of-PUF-Enabled Authentication	N/A	Blockchain (SQLite)
xTSeH [14]	Smart e-Health Device Security	Trusted Platform Module (TPM)	TPM-based Remote Attestation	Hardware TPM	N/A
A Software-based remote attestation [8]	IoT Device Security	N/A	Software-based Remote Attestation	Software TPM	N/A
Blockchain-based IoT Attestation [12]	IoT	TPM	Blockchain-Based Remote Attestation	Hardware TPM	Blockchain (Hyperledger Fabric)
This Paper PUFchain 4.0	**IoT (Device & Data)**	**TPM & PUF**	**PUF based TPM**	**Hardware TPM**	**Tangle**

Working Flow of Proposed PUFchain 4.0

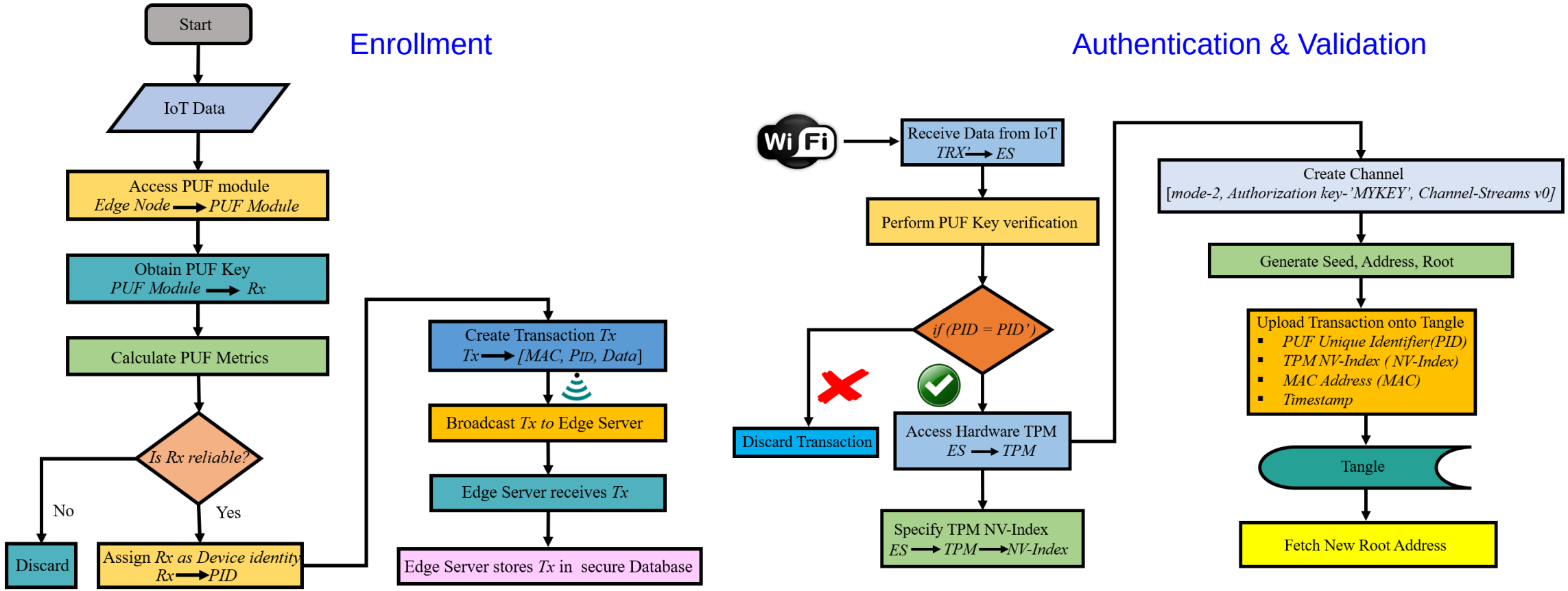


- Tangle is a simple fee-less, miner less Distributed Ledger Technology
- In Tangle, Incoming transactions must validate tips (Unverified Transactions) to become part of the Network.

Comparative Perspectives of Blockchain, PUFchain, and PUFchain 4.0



PUFchain 4.0:Enrollment and Authentication



Implementation and Validation

Sealing and unsealing PUF Key inside TPM by accessing NVRAM

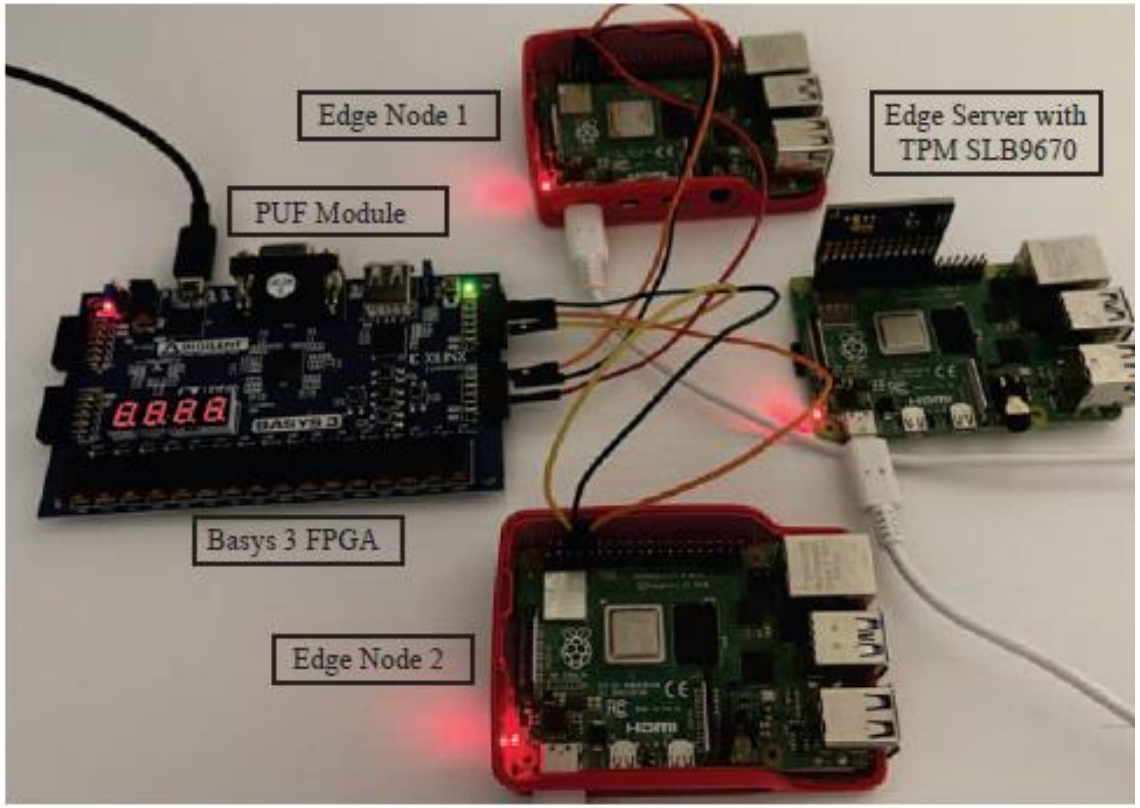
```
pi@raspberrypi:~ $ echo "10100111101001111010011110100111101001111010011110100111101001111010011" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500020 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $ echo "11010010110100101101001011010010110100101101001011010010110100101101001" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500021 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500021 -C o          ──────► 1st Edge Node PUF Key in TPM
11010010110100101101001011010010110100101101001011010010110100101101001

pi@raspberrypi:~ $ echo "10100111101001111010011110100111101001111010011110100111101001111010011" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500020 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $ echo "11010010110100101101001011010010110100101101001011010010110100101101001" > nv.dat
pi@raspberrypi:~ $ tpm2_nvwrite 0x1500021 -C o -i  nv.dat
pi@raspberrypi:~ $ tpm2_nvread 0x1500021 -C o          ──────► 2nd Edge Node PUF Key in TPM
11010010110100101101001011010010110100101101001011010010110100101101001

pi@raspberrypi:~ $ tpm2_nvread 0x1500020 -C o
10100111101001111010011110100111101001111010011110100111101001111010011
pi@raspberrypi:~ $
```

Uploading Transaction Details onto Tangle

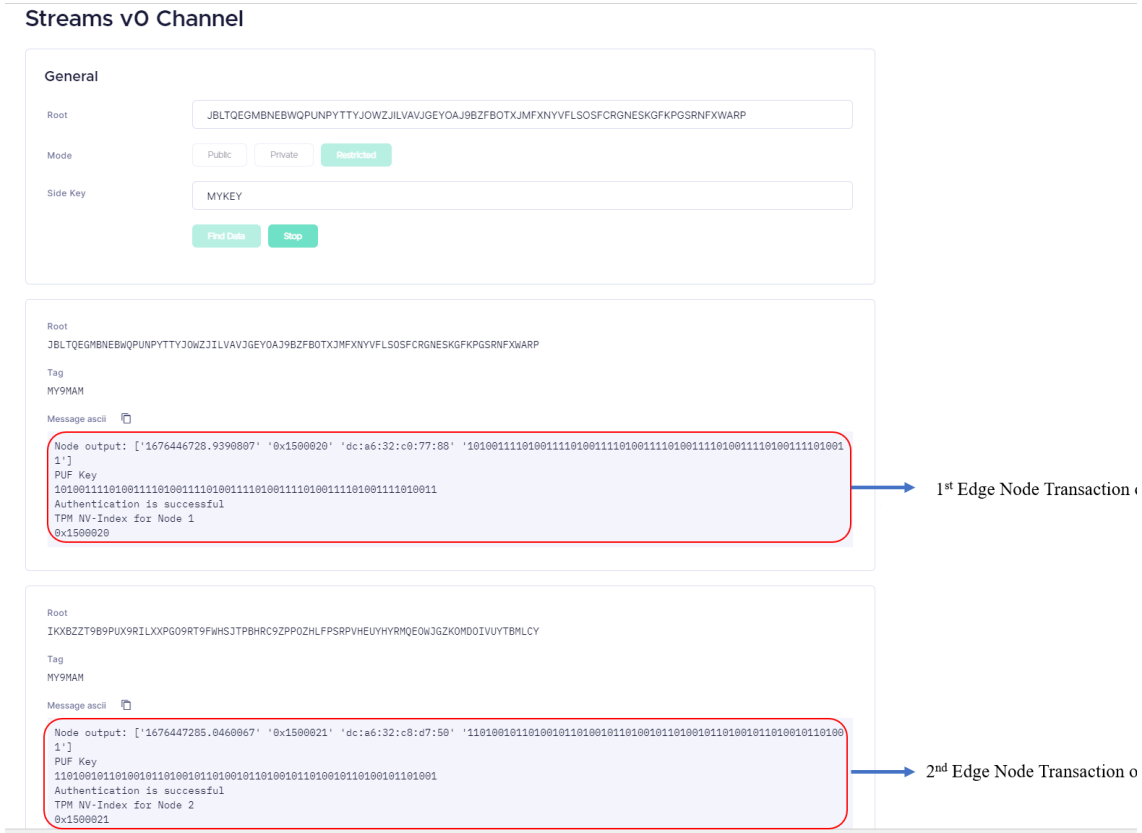
```
pi@raspberrypi: ~/mam.js/examples/simple
File  Edit  Tabs  Help
pi@raspberrypi:~/mam.js/examples/simple $ node index.js
Node output: ['1676446728.9390807' '0x1500020' 'dc:a6:32:c0:77:88' '10100111101001111010011110100111101001111010011110100111101001111010011']
PUF Key
10100111101001111010011110100111101001111010011110100111101001111010011
Authentication is successful
TPM NV-Index for Node 1
0x1500020

Seed: DREZFTWMFRUZCKGXSRNLWLJDYCCZGHC9YMEBWKFBPWIYSQRDPUMH9PPHBBCGRPKRVOIQHGPBPMOCPGHYS
Address: ZCKPCOYJEWA9HGSXAHYROCJBMPRFMAMMNPJWWKBCBMFK9ORFQMGVFUBVRYTHTPHXZW9HC9CFRV9XBLUFP   ──► Node 1 Output
Root: JBLTQEGMBNEBWQPUNPYTTYJOWZJILVAVJGEYOAJ9BZFBOTXJMFXNYVFLSOSFCRGNESKGFKPGSRNFXWARP
NextRoot: IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY
Decoded NextRoot IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY
Attaching to tangle, please wait...
Message Id 94bf9d8e21ac806966596b6741b4b57c332ea047d4835d0e3a1a70877a760eb2
You can view the stored message here https://explorer.iota.org/mainnet/message/94bf9d8e21ac806966596b6741b4b57c332ea047d4835d0e3a1a70877a760eb2
You can view the mam channel here https://explorer.iota.org/mainnet/streams/0/JBLTQEGMBNEBWQPUNPYTTYJOWZJILVAVJGEYOAJ9BZFBOTXJMFXNYVFLSOSFCRGNESKGFKPGSRNFXWARP/restricted/MYKEY
Fetching from tangle, please wait...
Fetched Root JBLTQEGMBNEBWQPUNPYTTYJOWZJILVAVJGEYOAJ9BZFBOTXJMFXNYVFLSOSFCRGNESKGFKPGSRNFXWARP
Fetched Node output: ['1676446728.9390807' '0x1500020' 'dc:a6:32:c0:77:88' '10100111101001111010011110100111101001111010011110100111101001111010011']
PUF Key
10100111101001111010011110100111101001111010011110100111101001111010011
Authentication is successful
TPM NV-Index for Node 1
0x1500020

Fetched Next Root IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY
Done!!!
pi@raspberrypi:~/mam.js/examples/simple $ node index.js
Node output: ['1676447285.0460067' '0x1500021' 'dc:a6:32:c8:d7:50' '11010010110100101101001011010010110100101101001011010010110100101101001']
PUF Key
11010010110100101101001011010010110100101101001011010010110100101101001
Authentication is successful
TPM NV-Index for Node 2
0x1500021

Seed: DREZFTWMFRUZCKGXSRNLWLJDYCCZGHC9YMEBWKFBPWIYSQRDPUMH9PPHBBCGRPKRVOIQHGPBPMOCPGHYS
Address: GJOUXGG9ANYGNXHMVPPALIAZVEGBHDW9BZWIZYQXSYDKSFLUZCIFWGGCKLIAEWALJDGRYDYZNIZKTOUMR   ──► Node 2 Output
Root: IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY
NextRoot: FWNOMFJGKWIFQLKLWACXJGKX9VGO9HU9TOSKXVUOGMDJWDIXDKJEOUHOSCRHDKZNEJLML9DJCIFYQZUXZ
Decoded NextRoot FWNOMFJGKWIFQLKLWACXJGKX9VGO9HU9TOSKXVUOGMDJWDIXDKJEOUHOSCRHDKZNEJLML9DJCIFYQZUXZ
Attaching to tangle, please wait...
Message Id f8ae1a3053b7dbe069a5324e51923e5a6babc3a48a4baa343af0480a861abafd
You can view the stored message here https://explorer.iota.org/mainnet/message/f8ae1a3053b7dbe069a5324e51923e5a6babc3a48a4baa343af0480a861abafd
You can view the mam channel here https://explorer.iota.org/mainnet/streams/0/IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY/restricted/MYKEY
Fetching from tangle, please wait...
Fetched Root IKXBZZT9B9PUX9RILXXPGO9RT9FWHSJTPBHRC9ZPPOZHLFPSRPVHEUYHYRMQEOWJGZKOMDOIVUYTBMLCY
Fetched Node output: ['1676447285.0460067' '0x1500021' 'dc:a6:32:c8:d7:50' '11010010110100101101001011010010110100101101001011010010110100101101001']
PUF Key
11010010110100101101001011010010110100101101001011010010110100101101001
Authentication is successful
TPM NV-Index for Node 2
0x1500021

Fetched Next Root FWNOMFJGKWIFQLKLWACXJGKX9VGO9HU9TOSKXVUOGMDJWDIXDKJEOUHOSCRHDKZNEJLML9DJCIFYQZUXZ
Done!!!
pi@raspberrypi:~/mam.js/examples/simple $
```

Continued…

Working Prototype



Transaction Outputs on IOTA Explorer



Performance Analysis of PUFchain 4.0

- Characterization

Parameters	Results
Application	IoT
Hardware Security Module	TPM, PUF
Hardware Security Mechanism	PUF-based Hardware TPM
TPM Board Specification	Infineon Optiga™ SLB 9670 TPM 2.0
TPM Storage	NVRAM
Free NV Memory	6962 Bytes
Data Security System	Tangle
Communication Protocol	Masked Authentication Messaging
TPM Module	Geek Pi TPM 2.0
PUF Module	Arbiter PUF
PUF Key	64 Bit

- Performance Analysis

Parameters	Results
NV Storage Capacity (Read/Write)	768 Bytes
Time to Generate PUF Key	87 ms
Power Consumption of Pi with TPM	2.7-3.3 Watt
Time to Perform Device Authentication	2000 ms
PUF Metrics	Reliability-99%
Time to Write PUF Key to TPM	real-299 ms, user-12 ms, and sys-19 ms
Time to Read PUF Key from TPM	real-411 ms, user-22 ms, and sys-10 ms

PUFchain 4.0: Performance Evaluation

Research Works	Application	DLT or Blockchain	Authentication Mechanism	Performance Metrics
Mohanty et al. 2020 - PUFchain	IoT (Device and Data)	Blockchain	Proof-of-PUF-Enabled Authentication	PUF Design Uniqueness - 47.02%, Reliability-1.25%
Chaudhary et al. 2021 - Auto-PUFchain	Hardware Supply Chain	Blockchain	Smart Contracts	Gas Cost for Ethereum transaction 21.56 USD (5-Stage)
Al-Joboury et al. 2021 - PoQDB	IoT (Data)	Blockchain & Cobweb	IoT M2M Messaging (MQTT)	Transaction Time - 15 ms
Wang et al. 2022 - PUF-Based Authentication	IoMT (Device)	Blockchain	Smart Contracts	NA
Hellani et al. 2021- Tangle the Blockchain	IoT (Data)	Blockchain & Tangle	Smart Contracts	NA
Bathalapalli et al. 2022-PUFchain 2.0	IoMT (Device)	Blockchain	Media Access Control (MAC) & PUF based Authentication	Total On-Chip Power - 0.081 W, PUF Hamming Distance - 48.02 %
PUFchain 3.0 in 2022	IoMT (Device)	Tangle	Masked Authentication Messaging	Authentication 2.72 sec, Reliability - 100% (Approx), MAM Mode-Restricted
PUFchain 4.0 (This Paper)	**IoT(Device & Data)**	**Tangle**	**PUF Based TPM (SbD)**	**PUF Key Generation Time-87 ms, PUF Reliability-99% Power Consumption-2.7-3.3 Watt**

Summary

- This paper proposed and validated a simple, lightweight, energy and time-efficient approach for IoT device authentication using PUF, TPM, and Tangle in this work. Sealing the PUF key to TPM hardware ensures hardware level root of trust.

- The proposed architecture exhibited an approach for DLT based access control mechanism through PUF-enabled TPM where the TPM's Endorsement and attestation key can be used to access and control the MAM communication channel to upload data onto Tangle.

- Simultaneously, the proposed approach used PUF based device authentication scheme for IoT, which generates a digital signature for each IoT based on process variations inside an IC.

- By Integrating the PUF with TPM in this work, we validated the potential of PUF-based TPM security solutions for IoT.

Future Research

- Idea of implementing PUF-based TPM scheme in Public and Private modes of MAM for the Security-by-Design (SbD) of Smart Electronics.
- 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.
- Extending the utilization of Masked Authentication Messaging in Public and Private Modes in PUF-based TPM approach for the security of Smart Electronics

Thank You !!