PUFchain4: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT

Venkata K. V. V. Bathalapalli
University of North Texas
Computer Science & Engineering
Denton, Texas, USA
vb0194@unt.edu

Saraju P. Mohanty
University of North Texas
Computer Science & Engineering
Denton, Texas, USA
saraju.mohanty@unt.edu

Elias Kougianos
University of North Texas
Electrical Engineering
Denton, Texas, USA
elias.kougianos@unt.edu

Vasanth Iyer
Grambling State University
Computer Science & Digital Technologies
Louisiana, USA
iyerv@gram.edu

Bibhudutta Rout
University of North Texas
Physics
Denton, Texas, USA
bibhudutta.rout@unt.edu

ABSTRACT

This paper presents a sustainable security solution using Physical Unclonable Function (PUF), Trusted Platform Module (TPM), and Tangle Distributed Ledger Technology (DLT) for sustainable Device and Data security in Internet-of-Things (IoT) driven Applications. DLT-driven Hardware-Assisted Security (HAS) solutions have gained much prominence due to the requirement of tamper-proof storage for hardware-assisted cryptography solutions. As the Internet of Things (IoT) application is more decentralized, designing complicated security mechanisms can impact its efficiency. In the proposed architecture, we presented a novel TPM Enabled PUF-based security mechanism with effective integration of PUF with TPM. The proposed mechanism is based on the process of sealing the PUF key in TPM, which cannot be accessed outside TPM and can only be unsealed by the TPM itself. A specified NV-index is assigned to each IoT node for sealing the PUF key to TPM using Media Access Control (MAC) address. Access to the TPM's Non-Volatile Random Access Memory (NVRAM) is defined by the TPM's Enhanced Authorization policies as specified by Trust Computing Group (TCG). The proposed architecture uses Tangle for sustainable data security and storage in decentralized IoT systems through Masked Authentication Messaging (MAM) scheme for efficient and secure access control to Tangle. We validated the proposed approach through experimental analysis and implementation, which substantiates the potential of presented PUFchain 4.0 for decentralized IoT-driven security solutions.

Conference acronym 'XX, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

KEYWORDS

Security-by-Design (SbD), Hardware-Assisted Security (HAS), Device Security, Data Security, Internet-of-Things, Trusted Platform Module (TPM), Physical Unclonable Function (PUF), Distributed Ledger

ACM Reference Format:
Venkata K. V. V. Bathalapalli, Saraju P. Mohanty, Elias Kougianos, Vasanth Iyer, and Bibhudutta Rout. 2018. PUFchain4: Integrating PUF-based TPM in Distributed Ledger for Security-by-Design of IoT. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 8 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

The evolution of IoT is revolutionizing and improving the efficiency of technological solutions in the areas of Healthcare, Agriculture, and transportation. Realizing the potential of intelligent electronic devices through edge cloud computing platforms for analysis and processing IoT sensor data has gained much traction and is becoming more viable [16]. However, the trustworthiness of IoT devices and Edge Cloud systems pose a question on the integrity of IoT devices and their data. Security approaches through symmetric and asymmetric keys have proven to be infeasible due to their vulnerability to multiple types of spoofing attacks through which a hacker can gain access to the system. A PUF-based solution for IoT security provides the hardware-level root of trust by creating a key pattern of random zeros and ones obtained from delays and frequency variation of logic elements inside a chip impacted by micro-level manufacturing variations during chip design and fabrication [6].

Trusted Platform Module is a hardware security primitive introduced by Trust Computing Group (TCG), which provides the root of trust for the computing platform as a simple System-On-Chip (Soc). It provides hardware-based security for cryptographic keys, random number generation, and hashing for cryptographic applications [14, 18, 19].

Each TPM has an Endorsement key (EK) which is generated, stored, and protected inside the TPM chip and can never be accessed outside the TPM. Cryptographic keys can be created by TPM, which, once encrypted by a TPM, can only be decrypted by the TPM itself, called Binding [3]. The system configuration parameters during the

boot process are stored in TPM's Platform Configuration registers (PCR). During the boot process, the firmware can check these parameters using the values stored in PCR to validate the system's integrity. The Storage Root Key (SrK) and EK are non-migratable keys protected by TPM. Storage Root Key can be regarded as a unique address of each owner of TPM. A new attestation key is created every time the owner of TPM changes [7]. TPM Non-Volatile memory (NVRAM) can seal and unseal the secret keys generated inside or outside TPM. A specified NV-index is defined for secure storage and retrieval of private keys. Access to TPM NVRAM can be user-defined and password-protected, following TCG's procedures.

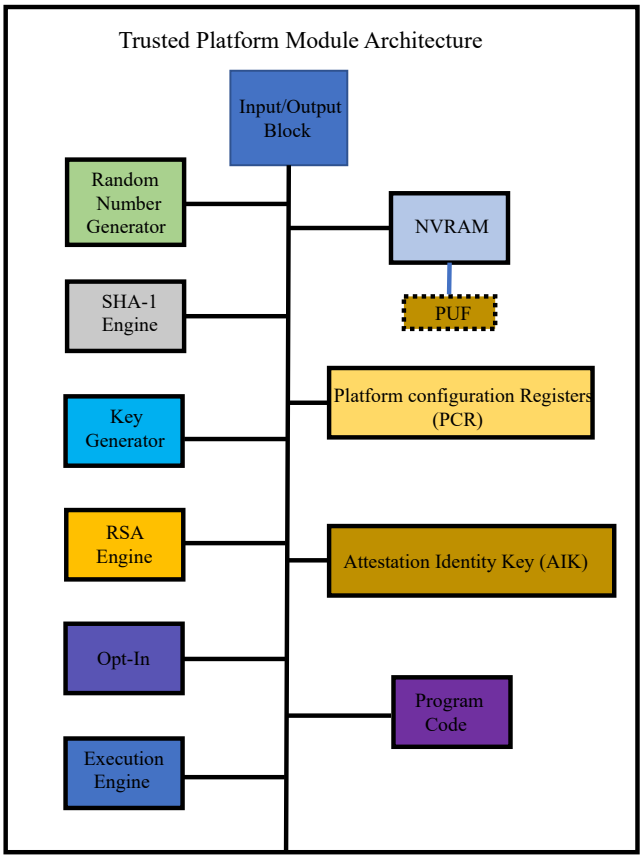


Figure 1: TPM Architecture with proposed PUF Integrated Approach [2].

The rest of the paper is organized in the following manner. Section 2 presents the novel contributions of this paper. Section 3 presents the security schemes and various DLT-based security solutions in SC. The working flow of device authentication and transaction validation mechanism of proposed PUFchain 4.0 is explained in Section 4. Section 5 outlines the implementation details and Section 6 presents the conclusion and directions for future research.

2 NOVEL CONTRIBUTIONS

Novel Contributions of this paper are:

- A sustainable Hardware-Assisted security approach using TPM and PUF for ensuring the root of trust for Security-by-Design of IoT.
- A security mechanism that utilizes 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 fee-less DLT for data security in IoT.

Internet of Everything (IoE) is an emerging terminology defined as an intelligent integration of *"Things," "Process," "People," and "Data"*. IoE can be considered an extension of IoT with effective networking and sustainable data processing capabilities to provide intelligent Information and communication technology infrastructure. Security is essential for the successful realization of IoT-based applications [17]. The architectural overview of PUFchain 4.0 is illustrated in Fig.2.

2.1 Problem Statement

For smart healthcare applications, the integrity and authenticity of devices connected to the Edge Computing platform is essential as the patient's health parameter analysis at an Edge or Cloud platform is based on the obtained physiological data from these devices [9].

The vulnerability of IoT devices to spoofing, brute force attacks on asymmetric and symmetric keys generated by various cryptographic algorithms, and the infeasibility of IoT to sustain the computational power capability of complex crypto-algorithms opened the doors for PUF-based approach for IoT security [5]. PUF-enabled security for SC has proven effective as IoT's authenticity is developed using Integrated Circuit (IC) chip fabrication properties.

However, PUF keys require reliable storage to store the keys securely. Unreliable hold of the PUF key can compromise its device security. Various ways of accessing to PUF key by adversaries through spoofing and sniffing attacks have posed a question on its feasibility. Providing secure storage for PUF-generated cryptographic keys is essential to realizing the potential of PUF-based cryptography. TPM is a hardware-secure crypto-processor and can provide robust storage to the PUF key by sealing it inside TPM NVRAM, which cannot be accessed by the adversary and can only be unsealed by the TPM itself.

2.2 Proposed Solution

From a data perspective, tangle a Distributed Ledger Technology (DLT) has become sustainable, providing immutability to data and assisting in Hardware-Assisted security by providing decentralized

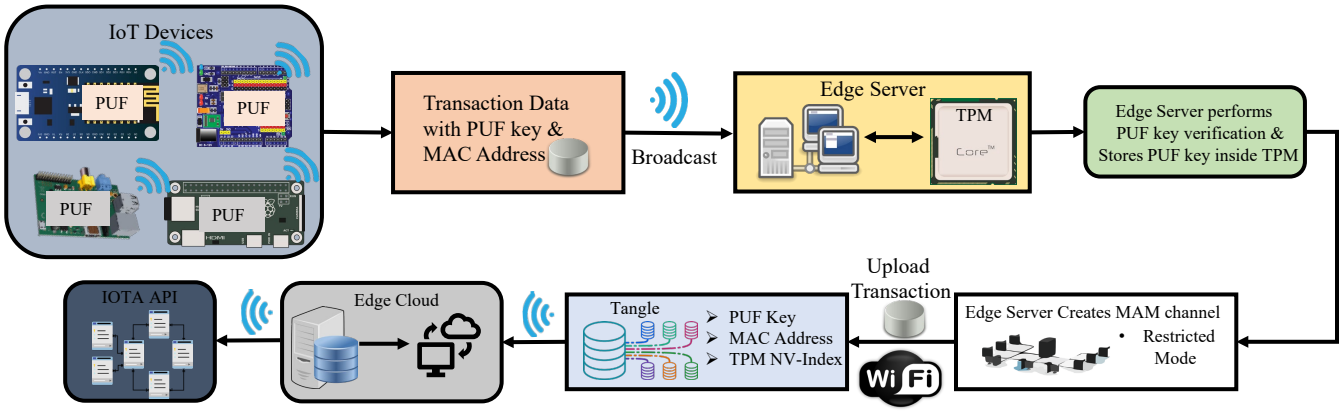


Figure 2: Architectural Overview of Proposed Security-by-Design approach (PUFchain 4.0) for Emerging Internet-of-Everything

storage to hardware-secure cryptographic keys. Being a miner-less DLT, it solves the problems of scalability, latency, and power consumption issues in Blockchain technology-based approaches like Smart Contract, which have proven to be computationally infeasible for resource-constrained devices [1].

Hardware TPM can support cryptographic applications, system integrity, and random number generations as these applications are supported through TPM, which works by creating an EK and SrK whose private portion can never be accessed outside TPM and are proven to be much more reliable [10, 13]. Sealing the PUF key inside TPM can restrict unauthorized access to the PUF key and can never be accessed outside TPM. The TPM can only unseal the locked PUF key. This approach provides a new security paradigm for PUF-Based TPM-supported security solutions.

3 RELATED RESEARCH

To address the device integrity issues in IoMT, A novel TPM-based remote attestation scheme is proposed in work [14] where the root of trust is extended from a Trusted system with embedded hardware TPM to all devices without TPM by developing a shadow TPM module in the kernel form at these devices. This approach proposes to build a trusted platform for IoMT by extending TPM functionality to all IoMT with or without embedded TPM. Cao et al.[8] proposed a software-based device attestation scheme to verify the authenticity of IoT, which offers to address proxy attacks and reduce the time required to perform remote attestation.

The idea of integrating Blockchain technology with PUF has been implemented by Mohanty et al.[15] for sustainable IoT devices and data security. This approach works by storing the PUF key of IoT in an immutable Blockchain using PUF and hashing modules.

A distributed TPM-based attestation framework was proposed using Blockchain's Hyperledger fabric [12] to decentralize the attestation mechanism. This work claims to be the first to integrate the device attestation with Blockchain technology for IoT security. In comparison, the proposed PUFchain 4.0 is developed using Hardware TPM and PUF and facilitates secure storage for the PUF key in TPM. This work also presents and validates a proof of concept that integrates scalable DLT with effective access control mechanisms using PUF-based TPM. Compared to the Blockchain-based attestation scheme, this work uses Tangle, a fee-less, and miner-less DLT, for secure data storage.

TPM-based remote attestation framework for verifying the integrity of processes running in the device is proposed by Sundar et al. [19]. This work is based on the software TPM and uses Hashed Message Authentication (HMAC) protocol. A robust fog node authentication scheme using TPM by Aslam et al. [4] uses TPM based certification scheme to validate the platform integrity of fog nodes in AVISPA under the Dolev-Yao intruder model. This approach is claimed to be resistant to impersonation and replay attacks. However, this method works by evaluating the integrity of the software state's fog node and automating the certification mechanism. In comparison, the architecture proposed in this paper works by assessing the integrity of an IoT node from the hardware level using PUF based security mechanism.

4 PROPOSED PUF-BASED TPM INTEGRATED NOVEL DLT (PUFCHAIN 4.0) ARCHITECTURE

4.1 Proposed PUFchain 4.0

The security framework is proposed to be implemented on an IoT network with decentralized heterogeneous intelligent electronic devices. In this architecture, the PUF module is responsible for generating. device's unique signature based on the PUF module embedded with it. Another device cannot use the PUF key of one IoT as its secure digital signature. The TPM in the proposed architecture is embedded with an Edge Server and is responsible for securely storing the PUF-based digital signature of the cluster of IoT devices connected to an Edge server. If a group of IoT nodes is connected to an ES, then each IoT gets a specified NV-index based on its MAC address using the command "*tpm2_nvdefine*". To unseal or read the sealed PUF key, a user can specify advanced security features to access specified NV-index using user passwords.

After performing PUF key verification, the ES seals it inside TPM using "*tpm2_nvwrite*" command. Tangle DLT is used in this work to harness the advantages of integrating a DLT that does not require a centralized authority or miner to validate and add a transaction as in Blockchain. Tangle is a Directed Acyclic Graph

(DAG) based ledger technology that requires minimal proof of work to avoid the validation of unverified transactions. This feature makes it as secure as Blockchain while being simple and lightweight. The effectiveness of the proposed transaction validation process in PUFchain 4.0 compared with the Block validation process in Blockchain is shown in Fig.3. While fetching the transaction, a new root address is obtained to upload the next upcoming transaction onto the channel. This root address will only be sent to the verified IoT node. This reduces the chance for an adversary to gain access to the MAM channel since the access is defined based on the PUF-based identity. Giving TPM-based secure storage to the PUF key can prevent spoofing attacks on the PUF key.

4.2 Working of Proposed PUFchain 4.0

This is a novel security mechanism we proposed in the current paper to integrate Tangle and TPM with PUF for lightweight and robust authentication of IoT devices. This algorithm utilizes Masked authentication messaging protocol and traditional network communication schemes for sustainable PUF key verification and TPM-based NVRAM storage for PUF key. The enrollment and Authentication phases of the proposed consensus mechanism are illustrated in the Algorithm 1, and 2.

Algorithm 1: Device Enrollment Algorithm

Input: Generating challenge response pairs (CRP) from PUF module of IoMT
Output: Broadcasting transaction to Edge Server (ES)

Edge device generates Challenge Response pairs (*CRP*) from the PUF module
Evaluate PUF keys and create device unique identity P_{ID}
// Calculate Uniqueness, Reliability, Inter-HD & Intra-HD
if *If obtained PUF key Rx is standard* **then**
    $P_{ID} \rightarrow Rx$
    // PUF Key is assigned as pseudo identity of the Client
Edge node creates a transaction (T_{Rx}) and forms a Block of Data
// Block consists of C_{Rx}, Media Access Control Address (MAC) and Block metrics
// $[P_{ID}, MAC, Data] \rightarrow T_{Rx}$
Edge node broadcasts transaction to Miner
// Edge Node$\rightarrow T_{Rx} \rightarrow$ Miner
ES receives the broadcasted transaction from Edge Node
// Edge Node$\rightarrow T_{Rx} \rightarrow$ES
ES stores the transaction T_{Rx} in secure database
// ES$\rightarrow T_{Rx} \rightarrow P_{ID}$

Initially, IoT devices with embedded PUF modules initiate a transaction consisting of a PUF key and MAC Address. The figure of merits of PUF keys are evaluated, and one of the PUF keys Rx is selected as P_{ID}: Pseudo identity of the IoT device. The P_{ID} along with MAC address (MAC) of the IoT and timestamp, is sent as a Block transaction to the Edge Server. Edge Server receives the transaction T_{Rx} from the IoT node and extracts P_{ID}, and MAC address from T_{Rx} and then stores them securely.

During verification, the Edge server receives an authentication request and transaction data $T_{Rx'}$. The new PUF key of IoT is extracted from $T_{Rx'}$ and compared with the enrolled PUF key P_{ID}. If PUF keys are matched, the MAC address (MAC) is retrieved and assigned a specified NV-Index by Edge Server by accessing TPM. A new NV-Index is assigned to seal the PUF key of IoT based on the MAC address. Once an NV-Index from TPM is assigned to a MAC, it cannot be given to any other device. The PUF key $P_{ID'}$ is then sealed inside TPMs NVRAM using NV-Index. The NV-index can be made as a *'Persistent handle'* in TPM. To unseal or read the PUF key from TPM, the NV-Index corresponding to MAC Address is retrieved and can be used to read the sealed PUF key inside hardware TPM. The edge server will become the client node for IOTA and uploads the TRx' onto Tangle. The device enrollment and authentication phases of the proposed PUFchain 4.0 are illustrated in Fig.4. Once P_{ID} is stored inside TPM, Edge server then creates a MAM channel in restricted mode and uploads the verified transaction onto Tangle along with NV-Index. The transaction is then uploaded onto Tangle.

5 EXPERIMENTAL VALIDATION

A hardware TPM module has been connected to the Edge server (Single Board Computer) to validate the proposed security scheme. Edge nodes with embedded PUF (Arbiter PUF) Broadcast a Block

Algorithm 2: Device Authentication Algorithm

Input: Block of Data $T_{Rx'}$ from Edge Node
Output: Sealing PUF key inside TPM with a specified NV Index and uploads data to Tangle

ES receives transaction data from Edge during verification.
// $T_{Rx'} \rightarrow$ES
Edge server receives the PUF key ($P_{ID'}$) from $T_{Rx'}$
ES extracts newly extracted PUF key of Edge from received Block of data ($T_{Rx'}$)
ES compares enrolled PUF key and obtained PUF key
if *If* $P_{ID} = P_{ID'}$ **then**
    // PUF key is verified successfully
Edge server access Hardware TPM Module
// Edge Server (ES)$\rightarrow$ TPM
ES access TPM'S NVRAM to seal the PUF key $P_{ID'}$
// ES$\rightarrow$TPM$\rightarrow$NV-Index
A specified NV- Index is obtained T_{ID} for specified MAC Address M_{ID}
// TPM$\rightarrow$NVRAM$\rightarrow M_{ID} \rightarrow T_{ID}$
ES writes PUF key to NV-index T_{ID}
// ES$\rightarrow$ $P_{ID'} \rightarrow T_{ID}$
ES creates a MAM channel
// ES$\rightarrow$MAM$\rightarrow$Restricted
ES becomes new Tangle node, validates and uploads transaction data onto network
// ES$\rightarrow$ $TRx' \rightarrow$Tangle

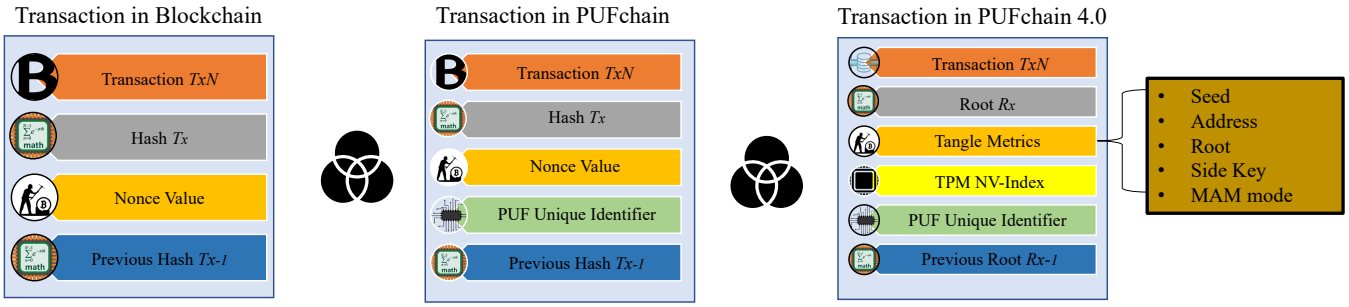
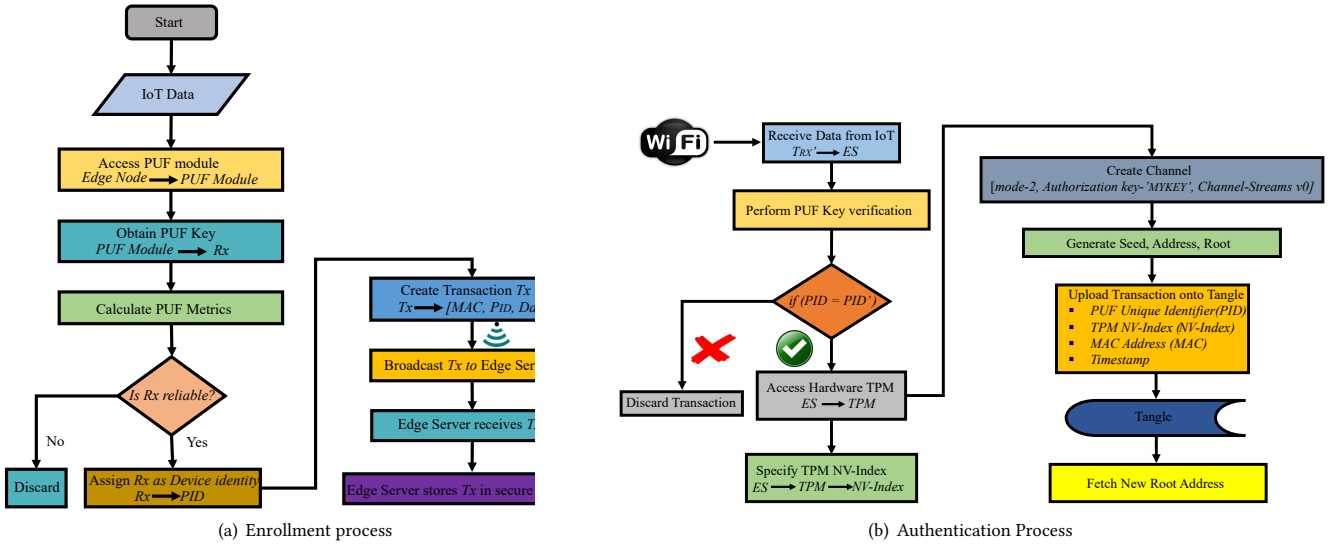


Figure 3: Transaction in Blockchain, PUFchain, and PUFchain 4.0



(a) Enrollment process (b) Authentication Process

Figure 4: Working flow of Enrollment and Authentication process

of data with MAC Address and 64-bit PUF key to ES through Universal Data Communication protocol. PUF keys are obtained at a baud rate of 9600, and the TPM module is based on an Infenion SLB9670 chip. The TPM's NV RAM is accessed by specifying an NV Index(0X1500020) for Edge Node 1 to seal the PUF key. The MAC Address "dc: a6:32:c0:77:88" of Edge node 1 (Raspberry pi 4) is locked to the NV Index "0x1500020" by the Edge Server. Arbiter PUF module is used in this experiment with reliability of 99%. The PUF module is implemented using VIVADO 2020.2. The total On-Chip power for this design is 0.082W. The architecture of Arbiter PUF is

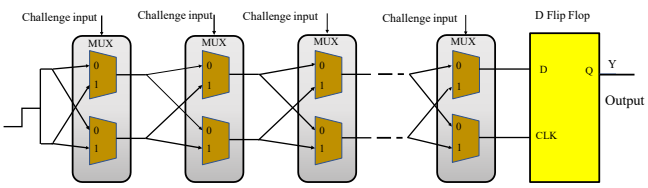


Figure 5: Arbiter PUF

Edge Node 2 with MAC address of "dc:a6:32:c8:d7:50" undergoes the enrollment and authentication processes. Once, the verification is done, an NV-Index of "0x1500021" with 128 Bytes of NV storage is assigned. The PUF key is stored inside the nv.dat file and sealed to the corresponding NV-Index. Both the transactions from Edge nodes 1 and 2 are validated, and a MAM channel with *"Restricted mode"* is created in IOTA Devnet. Two Edge Nodes are connected to the PUF module on Xilinx Artix-7 FPGA with the part number "xc7a35tcpg236-1" and an ES embedded with Hardware TPM module Fig.6.

The channel is Streams v0 channel, and the user-defined secret key for the channel is "MYKEY".Fig.7, Table.1, and 2 show the obtained outputs from our implementation. To upload a transaction and fetch a Tangle transaction from the MAM channel, the overall command execution time is 17380 ms, including the overall time to perform device authentication, seed, address, root, and channel creation. CPU execution time in user mode for the corresponding transaction is 6700 ms.

Table 1: Characterization of the Proposed PUFchain 4.0.

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
Data Security System	Tangle
Communication Protocol	Masked Authentication Messaging
TPM module	Geek Pi TPM 2.0
PUF Module	Arbiter PUF
PUF Key	64 Bit

Table 2: Performance Analysis of PUFchain 4.0.

Parameters	Results
NV Storage capacity	6k Byte
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

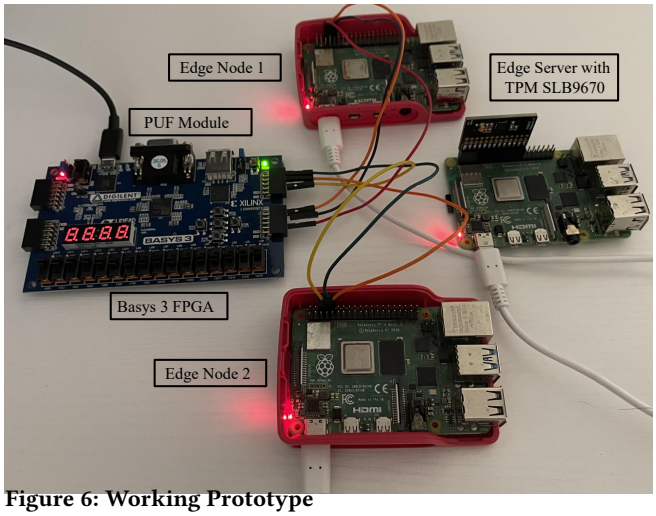


Figure 6: Working Prototype

6 CONCLUSION AND FUTURE RESEARCH

We 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.

In future work, we will explore leveraging the potential of other DLTs for HAS. Our focus will be on generating intelligent TPM-enabled PUF-based approaches for device authentication in IoT through DLT. Our future work will aim to provide a sustainable device and data security in IoT to leverage the true potential of IoT-based applications.

REFERENCES

[1] 2021. IOTA Foundation. iotaledger. mam.js. (2021). https://github.com/iotaledger/mam.js

[2] Mohammed Achemlal, Said Gharout, and Chrystel Gaber. 2011. Trusted Platform Module as an Enabler for Security in Cloud Computing. In *2011 Conference on Network and Information Systems Security*. IEEE. https://doi.org/10.1109/sar-ssi.2011.5931361

[3] Will Arthur and David Challener. 2015. *A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security* (1st ed.). Apress, USA.

[4] Mudassar Aslam, Bushra Mohsin, Abdul Nasir, and Shahid Raza. 2020. FoNAC - An automated Fog Node Audit and Certification scheme. *Computers & Security* 93 (2020), 101759. https://doi.org/10.1016/j.cose.2020.101759

[5] Venkata K. V. V. Bathalapalli, Saraju P. Mohanty, Elias Kougianos, Babu K. Baniya, and Bibhudutta Rout. 2022. PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Internet of Medical Things. In *Internet of Things. IoT through a Multi-disciplinary Perspective*. Springer International Publishing, 23–40. https://doi.org/10.1007/978-3-031-18872-5_2

[6] Venkata K. V. V. Bathalapalli, Saraju P. Mohanty, Elias Kougianos, Venkata P. Yanambaka, Babu K. Baniya, and Bibhudutta Rout. 2021. A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture. In *19th OITS International Conference on Information Technology (OCIT)*. IEEE. https://doi.org/10.1109/ocit53463.2021.00080

[7] Miguel Calvo and Marta Beltran. 2021. Remote Attestation as a Service for Edge-Enabled IoT. In *IEEE International Conference on Services Computing (SCC)*. IEEE. https://doi.org/10.1109/scc53864.2021.00046

[8] Jin Cao, Tong Zhu, Ruhui Ma, Zhenyang Guo, Yinghui Zhang, and Hui Li. 2022. A Software-based Remote Attestation Scheme for Internet of Things Devices. *IEEE Transactions on Dependable and Secure Computing* (2022), 1–1. https://doi.org/10.1109/tdsc.2022.3154887

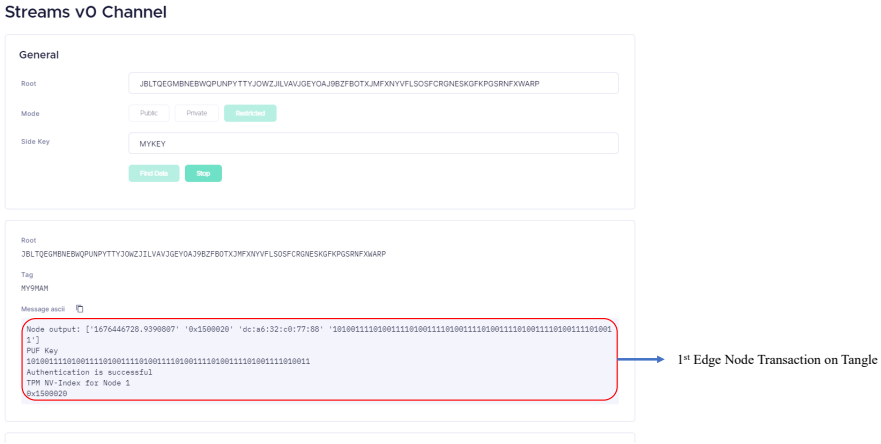
[9] Bhaskara S. Egala, Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. 2021. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet of Things Journal* 8, 14 (jul 2021), 11717–11731. https://doi.org/10.1109/jiot.2021.3058946

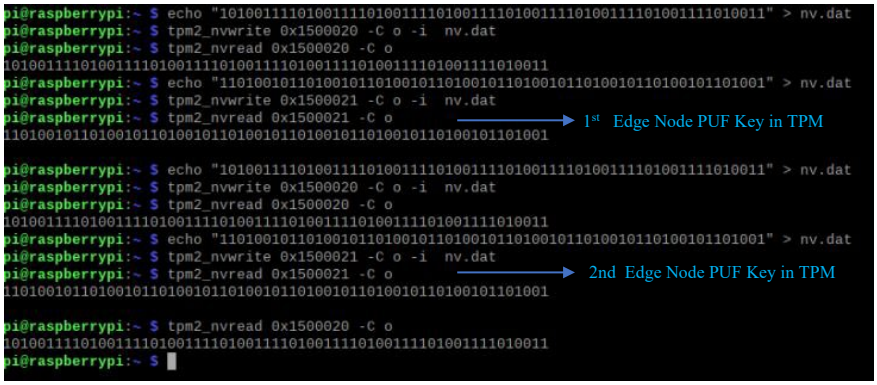
[10] Janusz Furtak. 2022. Data Exchange Protocol for Cryptographic Key Distribution System Using MQTT Service. In *Annals of Computer Science and Information Systems*. IEEE. https://doi.org/10.15439/2022f260

[11] Hala Hamadeh and Akhilesh Tyagi. 2019. Physical Unclonable Functions (PUFs) Entangled Trusted Computing Base. In *IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*. 177–180. https://doi.org/10.1109/iSES47678.2019.00047

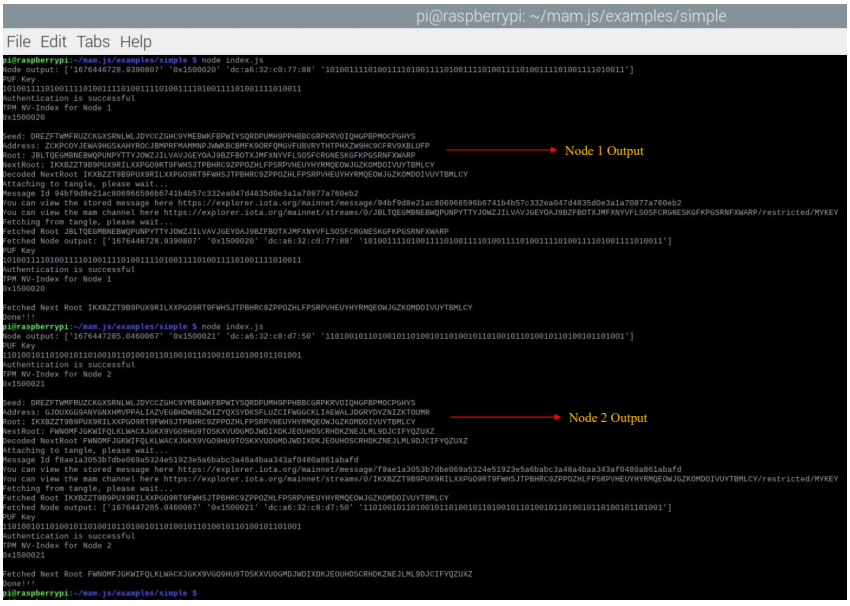
[12] Ira Ray Jenkins and Sean W. Smith. 2020. Distributed IoT Attestation via Blockchain. In *2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*. IEEE. https://doi.org/10.1109/ccgrid49817.2020.000-7

[13] Dawei Li, Yingpeng Zhang, Jian Cui, Di Liu, Yu Sun, Zhenyu Guan, and Xu Wang. 2022. Remote Audit Scheme of Embedded Device Software Based on TPM. In *IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*. IEEE. https://doi.org/10.1109/bigdatasecurityhpscids54978.2022.00021





(b) Sealing and unsealing PUF Key inside TPM by accessing NVRAM



(c) PUF Key Verification at Edge Server

Figure 7: Experimental Validation of PUFchain 4.0

[14] Di Lu, Ruidong Han, Yulong Shen, Xuewen Dong, Jianfeng Ma, Xiaojiang Du, and Mohsen Guizani. 2021. xTSeH: A Trusted Platform Module Sharing Scheme Towards Smart IoT-eHealth Devices. *IEEE Journal on Selected Areas in Communications* 39, 2 (February 2021), 370–383. https://doi.org/10.1109/jsac.2020.3020658

[15] Saraju P. Mohanty, Venkata P. Yanambaka, Elias Kougianos, and Deepak Puthal. 2020. PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE). *IEEE Consumer Electronics Magazine* 9, 2 (2020), 8–16. https://doi.org/10.1109/mce.2019.2953758

[16] Han Qiu, Meikang Qiu, Meiqin Liu, and Gerard Memmi. 2020. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. *IEEE Journal of Biomedical and Health Informatics* 24, 9 (September 2020), 2499–2505. https://doi.org/10.1109/jbhi.2020.2973467

[17] Anu Raj and Shiva Prakash. 2018. Internet of Everything: A survey based on Architecture, Issues and Challenges. In *5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*. 1–6. https://doi.org/10.1109/UPCON.2018.8596923

[18] Vinay Kumar Calastry Ramesh, Yoohwan Kim, and Ju-Yeon Jo. 2020. Secure IoT Data Management in a Private Ethereum Blockchain. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE. https://doi.org/10.1109/compsac48688.2020.0-219

[19] Shyam Sundar, Prabhakara Yellai, Siva Sankara Sai Sanagapati, Prayas Chandra Pradhan, and Sai Kiran Kumar Reddy Y. 2019. Remote Attestation based Software Integrity of IoT devices. In *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE. https://doi.org/10.1109/ants47819.2019.9117946