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

Venkata K. V. V. Bathalapalli[1], Saraju P. Mohanty[2 [0000−0003−2959−6541]], Elias Kougianos[3 [0000−0002−1616−7628]], Babu K. Baniya[4], and Bibhudutta Rout[5]

[1] Department of Computer Science and Engineering, University of North Texas, USA.
VenkatakarthikvishnuvardBathalapalli@my.unt.edu
[2] Department of Computer Science and Engineering, University of North Texas, USA.
saraju.mohanty@unt.edu
[3] Department of Electrical Engineering, University of North Texas, USA.
elias.kougianos@unt.edu
[4] Dept. of Computer Science & Digital Technologies, Grambling State University, USA.
Baniyab@gram.edu
[5] Department of Physics, University of North Texas, USA.
bibhudutta.rout@unt.edu

Abstract. This paper presents a Hardware-assisted security primitive that integrates Physically Unclonable Functions (PUF) and IOTA Tangle for device authentication in the Internet-of-Medical-Things (IoMT). The increasing market and scope for the IoMT is due to its potential in enhancing and improving the efficiency of health services across the globe. As the applicability of IoMT is increasing, various security vulnerabilities are surfacing and hindering its adoption. Device and data security are pivotal for Healthcare Cyber-Physical Systems (H-CPS) since a vulnerable working ecosystem in healthcare to various security attacks could risk the patient's lives. To ensure the authenticity of IoMT, the proposed security scheme uses Masked Authentication Messaging (MAM), which is the second level communication protocol for secure data storage, retrieval and sharing in IOTA Tangle. MAM works in three modes: Public, Private and Restricted. The proposed security primitive has been developed in *Restricted mode* for ensuring the utmost security by storing the PUF key of the IoMT in Tangle using MAM. PUFs are one of the most widely adopted hardware security primitives which work based on nanotechnology to build a secure fingerprint that guarantees the integrity of consumer electronic devices. For validating PUFchain 3.0, a strong arbiter PUF module, which supports higher number of Challenge Response Pairs (CRP), has been configured on two FPGA boards on both the IoMT and the edge server sides for validation. The proposed security scheme has taken less than 1 minute to upload the transaction onto Tangle through MAM and less than 2 seconds to retrieve the data, which substantiates its robustness and potential for sustainable and secure Smart Healthcare.

Keywords: Internet-of-Medical-Things(IoMT) · Distributed Ledger Technology (DLT) · Physically Unclonable Function (PUF) · Hardware-Assisted Security (HAS) · Security-by-Design (SbD) · Masked Authentication Messaging (MAM) · Blockchain

1 Introduction

IoMT devices generate large amount of fragmented data for different applications in Smart Healthcare. These fragmented data are being used for various clinical experiments and research [21]. Wearable and implantable medical electronic devices are placed inside and on the body to monitor various physiological parameters and generate data for analysis which are processed in cloud and edge computing systems [11, 16]. In order to address the privacy issues in smart healthcare, many researchers have adopted Distributed Ledger Technology (DLT) based solutions which provide immutability and confidentiality. Blockchain has been one of the most widely explored DLT for financial transactions since its inception in 2008 [18]. However, resource constrained IoT devices cannot sustain the computational resource requirements of blockchain. The IoT devices are vulnerable to various types of physical attacks where the authorized nodes can be replaced by the fake ones [5, 19, 24]. Authenticity of IoT devices at the Physical layer of H-CPS is also important, along with data confidentiality and privacy which can be addressed using PUFs. PUF-based security solutions can be embedded onto a chip and generate keys from the PUF design using process variations inside an Integrated Circuit (IC) [5, 9, 22] which can be used as security keys.

Using asymmetric keys for encryption and decryption of data can sometimes restrict access to medical professionals or patients. At the same time, a universal access key for encryption and decryption defeats the whole purpose of using security protocols. Hence a simple scalable approach for the authenticity of IoMT devices is needed [5]. PUFs do not require a database for key storage. The PUF keys can be generated instantly by taking advantage of micro manufacturing process variations [9,14,17,20]. Tangle is a DLT based solution which is a Directed Acyclic Graph (DAG) and has similar fundamental working principles as the Blockchain such as immutability, and irreversibility while being simple [2, 27]. Tangle also addresses the fundamental challenges in Blockchain which have been hindering its application in resource constrained decentralized and distributed Fog and Edge computing systems. It does not require miner and transaction fees to validate a transaction and add it to the Tangle DAG.

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. Section 4 explains MAM and its working. The working flow of device authentication and transaction validation in the proposed PUFchain 3.0 is explained in Section 5. Section 6 outlines the implementation details and Section 7 presents the conclusion and directions for future research.

2 Novel Contributions

In motivation to propose a novel approach for sustainable cybersecurity in IoMT, we propose a device authentication method by including PUF key of IoMT inside IOTA Tangle using MAM which reduces the chance for its vulnerability to various kinds of security attacks. The broad overview of PUFchain 3.0 is illustrated in Fig. 1.

The novel contributions of this paper include the following:

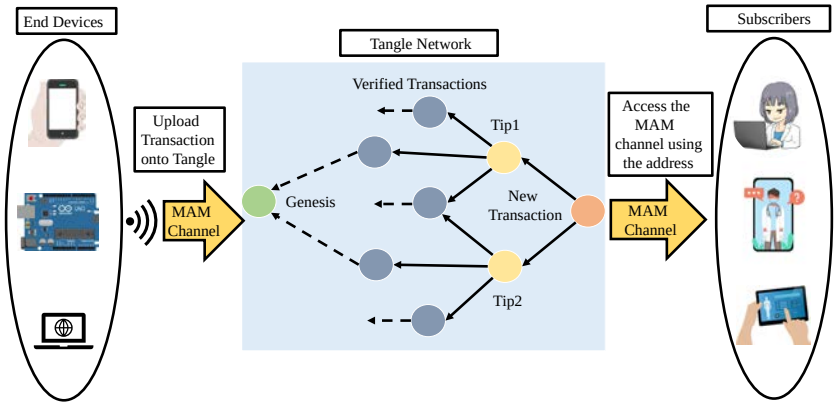


Fig. 1. Tangle DLT for a Secure H-CPS using MAM.

- Providing a minerless, low cost decentralized DLT for device authentication using PUFs and creating a secure channel for communicating IoMT data through MAM.
- A DLT that utilizes Proof of Work requiring minimal amount of computational resource requirements.
- A PUF based security approach where a PUF module can be integrated inside wearable and implantable IoMT devices and can generate a unique device fingerprint.
- A system that doesn't require transaction fees and allows secure communication through MAM.
- A robust multi level device authentication system for edge computing driven SC.
- A sustainable security solution which works in the Restricted mode of MAM where an authorization key is created to restrict unauthorized access to the MAM channel.

3 Related Research Overview

The success of Blockchain in financial transaction has increased its applicability in IoT based applications. However, the rate of transaction approval and time taken to append blocks in the Blockchain have driven researchers to explore the possibilities for other DLT based solutions that could address the aforementioned issues.

An approach for IoMT data sharing through Tangle was proposed [27] using MAM. Different sensors were interfaced with a Raspberry pi and the corresponding data was published in MAM restricted mode. This work however doesn't include a device authentication mechanism.

A scalable approach for integrating DLT with Blockchain was proposed [13] where IoT devices could be integrated with Tangle which could then connect to Blockchain in the backend through a connector node. In this approach, IoT devices have been classified as full and light nodes depending on their functionality. These devices can also function offline and upload transactions onto Tangle once they are approved by peers. Blockchain in this approach is proposed to be working in the cloud and IoT devices are integrated with Tangle through edge computing which reduces latency and facilitates

data processing capability at the source. This method however does not emphasize the security of IoT devices.

A mutual authentication protocol was proposed using PUF and Blockchain for multi server systems using Smart Contracts and Proof of Work. This approach uses one-way hash functions and a fuzzy extractor for biometric authentication. However this approach requires high computational resources.

Authors in [8] proposed a method in which PUF and Blockchain have been linked together for IC traceability in supply chain management using the Inter Planetary File System (IPFS). Various protocols were included to trace the ownership of a chip using PUF key and smart contracts thereby storing these PUF keys in the IPFS. To address the issues with consensus mechanisms like Proof of Stake (PoS) and with an objective of exploring Blockchain technology's use for hardware assisted security, a robust Proof of PUF-Enabled Authentication consensus mechanism for integrating PUF with Blockchain was implemented in [18]. The result, PUFchain, works by authenticating the PUF key of the device and its properties before uploading the data onto a database.

Most of the aforementioned approaches for HAS are utilizing Blockchain protocols like PoW, PoS and Ethereum Smart Contracts. PoW is a computationally intensive consensus algorithm which requires block validators or miners to achieve a nonce value to validate a block of transactions.

Proof of Stake (PoS) on other hand is a stake-based block validation process where the miner having higher amount of stake most probably is delegated with the responsibility of validating the transaction. To address the above issues, a Proof of Quality of Service based DAGs-to-Blockchain (PoQDB) consensus mechanism was proposed in [3]. In this approach, the IoT devices can upload the data onto Cobweb ledger where each transaction is authenticated using digital signature algorithm. After uploading data in Cobweb using the MQ Telemetry Transport (MQTT) protocol, the Edge server will upload the JSON data onto the Blockchain. However using private and public keys for authentication makes this protocol vulnerable to network and spoofing attacks.

4 Tangle DLT

4.1 IOTA Tangle

Tangle is a DLT which is based on a DAG, where a transaction validates two previous transactions to become part of the network. As the number of incoming transactions increases, the transaction validation rate also increases. It is a No Block, No Miner and No Fee DLT technology that has the inherent functionality of Blockchain while being lightweight and scalable. The unverified transactions in the DAG are called *'Tips'* [4]. The tips are selected based on a 'Markov Chain Monte Carlo (MCMC)' algorithm. The rate of approval of incoming transactions is defined by a Poisson point process where a predefined (λ) high controls the transaction approval simulation [4].

A coordinator node is responsible for selecting the unverified transactions and attaching them as tips to newly added transactions. The transactions are uploaded by clients onto Tangle through a coordinator node which performs Tip selection process for the incoming transaction to validate previous two transactions. Validating a Tip involves

verifying balances of the respective transaction from a Tip by performing minimal PoW which does not require much computational capability as it does in Blockchain [12].

Each transaction in Tangle is associated with a cumulative weight (CW) which is the number of transactions approved by the subsequent nodes either directly or indirectly [23]. If a node in Tangle has a predefined initial weight of 1 then its CW will be the sum of its initial weight and the CW of all subsequent nodes in the DAG which have either directly or indirectly approved it.

The MCMC method performs a random walk from the genesis node which is the initial node of Tangle and propagates throughout the network until it reaches the node whose transaction has not been referenced and validated by the subsequent nodes. A minimal amount of PoW is done to counter spamming attacks in Tangle. The flow of device registration and authentication mechanisms in PUFchain 3.0 are shown in Figs. 2, and 3.

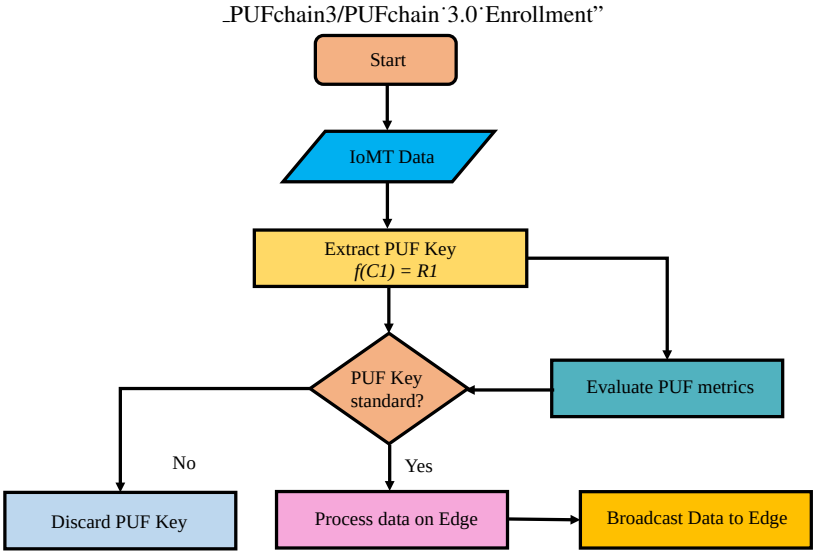


Fig. 2. Procedural flow of Enrollment Process in PUFchain 3.0

4.2 MAM Overview

MAM is one of the communication protocols for sending and receiving the encrypted information in Tangle through a channel by signing the message using the Merkle Hash Tree (MHT) signature algorithm. The message can be accessed by the receiver using the address of the channel. Whenever a new message of any length and size is uploaded on Tangle a channel is created and the receivers can immediately access the data using the root of the MHT [7, 10]. The transaction in MAM consists of the actual message and the MHT signature of the source [25]. MAM works mainly in three modes: Public,

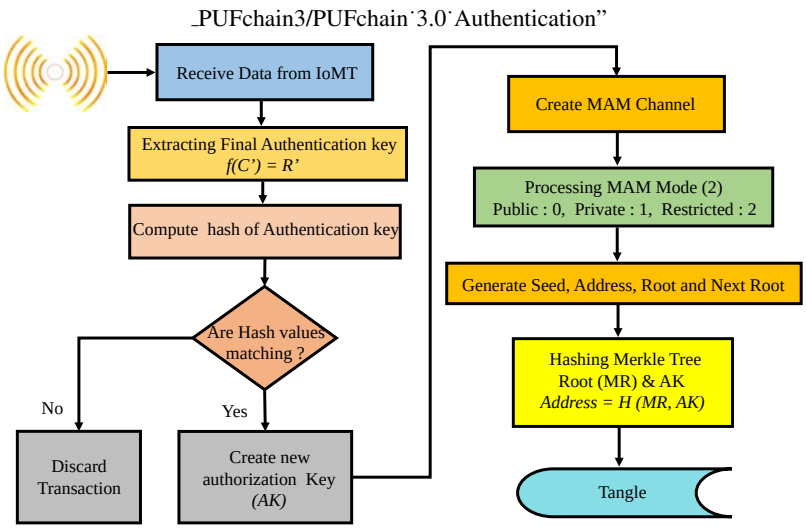


Fig. 3. Procedural Flow of Authentication process in PUFchain 3.0

Private and Restricted. The working flow of MAM in restricted mode is illustrated in Fig. 4.

Public Mode: In Public mode, the IoT device which is the source collects the data and uploads it onto Tangle. A MAM channel with an address is generated for secure exchange of information. The address of the channel will be the root of the Merkle Tree. The subsequent transaction has to be submitted to the MAM channel using this fetched root.

Private Mode: For applications requiring privacy and confidentiality, as in the case of health record management, the root of the Merkle tree is hashed and the obtained hash is used as the address of the channel to publish and access the data.

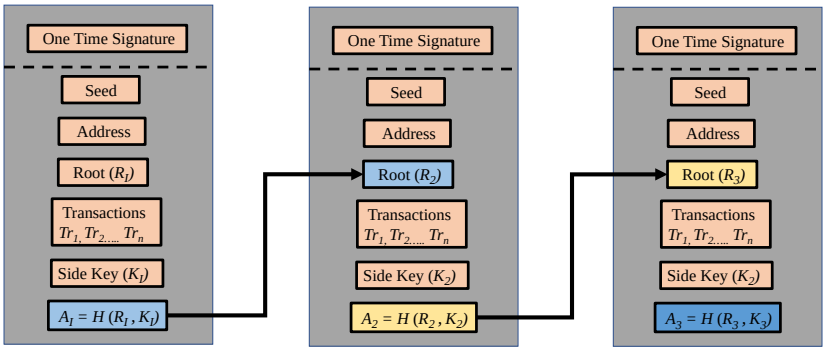


Fig. 4. Masked Authentication Messaging Modes in Restricted Mode

Restricted Mode: The restricted mode of MAM works by using a channel *Authorization key* or *Side key* along with the Merkle root. The address of the channel for the next transaction is generated by computing the hash of the Merkle root and side key. The message subscriber's access to MAM channel is based on this combined hash value which is confidential and acts as a security layer for machine to machine communications using Tangle.

5 PUFchain 3.0: A Hardware Assisted Robust Authentication mechanism using Tangle

The main object of PUFchain 3.0 is to explore the potential of Tangle for hardware assisted security in SC to address the issues with existing device authentication mechanisms which require a non volatile memory to store the secret keys used for authentication. This system also proposes an approach where the conventional network communication protocols which are vulnerable to various types of spoofing attacks could be removed and the IoMT device embedded with a PUF module could connect to an edge server and access the MAM channel only after successful authentication.

Once the IoMT broadcasts the data, the edge server receives the data which contain its fingerprint and performs the authentication by extracting the PUF key and comparing it with the obtained one. If the authentication is successful, the PUF key of the device can be used as the side key for the MAM channel. The edge server creates the MAM channel and uploads the data onto the MAM channel whose address is generated using the side key and the root of the Merkle tree.

Once the transaction is uploaded onto Tangle, a new root is created which will be specific for that channel and a particular client can upload the data in subsequent transactions using the new fetched root.

Each transaction in MAM has a reference address to the next one. The reference address will change based on the working MAM mode. The side key could be changed at any point of time if the secrecy of the side key is anticipated to be compromised [2,7]. The whole transaction in PUFchain 3.0 works in MAM restricted mode where the MAM channel could be accessed using an authentication key based on PUF along with the hash of the root of Merkle Tree [2,6].

5.1 PUF Overview

PUFs can be defined as fingerprint generating functions for electronic devices. PUFs are developed based on intrinsic manufacturing variations during chip fabrication. The stability of these parameters for ICs changes based on the location, temperature and the materials used. PUFs have been classified as *Strong* or *Weak* depending on the configuration. Arbiter PUF, Ring Oscillator PUF and Butterfly PUF are most widely used PUFs due to their power and speed optimized designs. The Arbiter PUF design is delay based, developed to create a PUF key using the micro manufacturing variations associated with wiring between the electronic components in an IC [15].

5.2 Working of proposed PUFchain 3.0

Device Registration Phase:

In the registration phase, the IoMT device embedded with the PUF module is tested with different challenge response pairs (CRP) and figures of merit of the PUF are evaluated. Table 1 presents the notation used in the proposed PUFchain 3.0. Strong and reliable PUF keys were selected and a random challenge input is tested on the PUF module embedded with the IoMT, and the corresponding PUF key is considered as its fingerprint. The micro controller connected to the client broadcasts the PUF data to Edge server (ES). The working flow of the Enrollment process in PUFchain 3.0 is illustrated in Algorithms 1, 2, and Fig. 5.

Step 1: Initially a PUF key for the challenge input C_{IN1} is extracted. The obtained PUF Key $R1$ from the PUF module of IoMT device PUF_{MID} is evaluated to compute PUF metrics. If 100% reliability is achieved, then P_{MID} is assigned as fingerprint of end IoMT device and broadcast to ES.

Step 2:As soon as it receives the broadcasted PUF key P_{MID} from the IoMT device, the ES extracts a PUF key by giving a challenge input C_{IN2} for the PUF module PUF_{MED} attached on its side and extracts P_{MED}.

Step 3:An exclusive OR (XOR) operation is performed on both the received and extracted PUF keys P_{MID}, P_{MED}. The XOR ed output P_{XOR} is broadcast back to the IoMT as a challenge input C_{IN3} on the client side. The IoMT device receives the input and performs key extraction. The obtained key R_{OUT2} is broadcast back as a challenge input C to the ES.

Step 4: The ES finally computes the SHA-256 Hash (H) of the obtained final PUF key R_{KOUT} for the corresponding input from IoMT. The obtained final hash value H_D is stored in a secure database.

Algorithm 1: 1st level Enrollment Process of PUFchain 3.0

Input: PUF key extraction from PUF module connected to IoMT client
Output: Reliable secure fingerprint for IoMT device to establish secure communication with Edge Server

1 Random C_{IN} generation for testing the PUF module.
2 Test the PUF module and perform PUF key extraction
`//` $PUF_{MID} \rightarrow f(C_{IN}) = R_{OUT}$
3 Perform PUF metric evaluation.
`// Calculate Uniqueness, Reliability, Inter-HD & Intra-HD`
4 **if** *PUF keys* R_{OUT} *are standard* **then**
5 $P_{MID} \rightarrow R_{OUT}$
`// PUF Key is assigned as pseudo identity of the Client`
6 Edge Gateway(EG) connected to IoMT stores the corresponding Key in secure database
`//` $P_{MID} \rightarrow$ EG

Device Authentication Phase: Once the IoMT is authenticated, the ES uploads the entire transaction process details in Tangle. The working flow of the authentication pro-

Table 1. Notations

Notation	Description
PUF_{MID}	PUF module on IoMT Side
PUF_{MED}	PUF module on Edge Server side
C_{IN}	Random Challenge Inputs
C_{IN1}	1st Challenge Input
C_{IN2}	2nd Challenge Input
R_{OUT}	Response Output from PUF module while testing
R_{KOUT}	Response Output from PUF module on ES side
$R_{KOUT'}$	Response Output from PUF module on ES side during authentication
R_{OUT2}	Response Output from PUF module on IoMT side during Enrollment
$R_{OUT2'}$	Response Output from PUF module on IoMT side during authentication
P_{XOR}	XOR ed output during enrollment
$P_{XOR'}$	XOR ed output during authentication
$P_{MID'}$	Pseudo identity of IoMT device (PUF Key) during authentication
$P_{MED'}$	Pseudo identity of Edge Server(PUF Key) during authentication
R_{KOUT}	Final Authentication key during enrollment
$R_{KOUT'}$	Final Authentication key during authentication
$\oplus$	XOR
A_K	Side Key
R_K	Merkle root
H	SHA-256 Hash Function
H_D	Hash output value during Registration
H_A	Hash output value during Authentication
A_M	New fetched root

cess and transaction update in the MAM channel are presented in Fig. 6 and Algorithm 3.

Step 1: Cryptographic identity of IoMT is verified by performing the PUF key extraction on both End device and ES side from their associated PUF modules.

Step 2: Challenge inputs (C_{IN1}, C_{IN2}) obtained during enrollment are retrieved from the database and given to two PUF modules.

Step 3: The obtained PUF keys ($P_{MID'}$, $P_{MED'}$) are evaluated and XOR ed. The output $C_{IN3'}$ is given as input to PUF on IoMT.

Step 4: The obtained $R_{OUT2'}$ is again tested on the PUF at ES and obtained final key $R_{KOUT'}$ is hashed. Attained hash value H_A is compared with the retrieved H_D.

Step 5: Once the device authentication is considered as successful by the ES, it creates a MAM channel to upload the transaction and fetch the address and broadcast it to the authenticated client to upload its data.

Step 6: The working mode of MAM is specified as '2' which is the restricted mode. An authorization key or side key A_K is created.

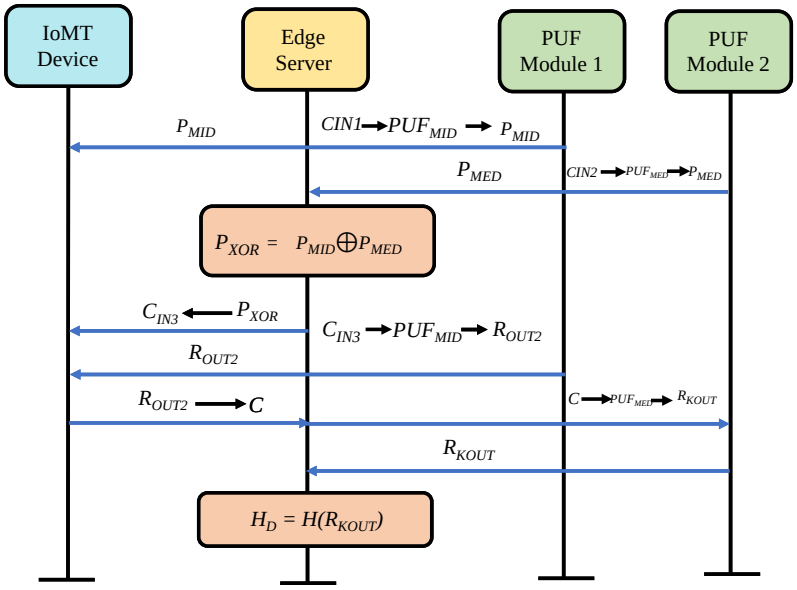


Fig. 5. Processing Flow of Device Enrollment in PUFchain 3.0

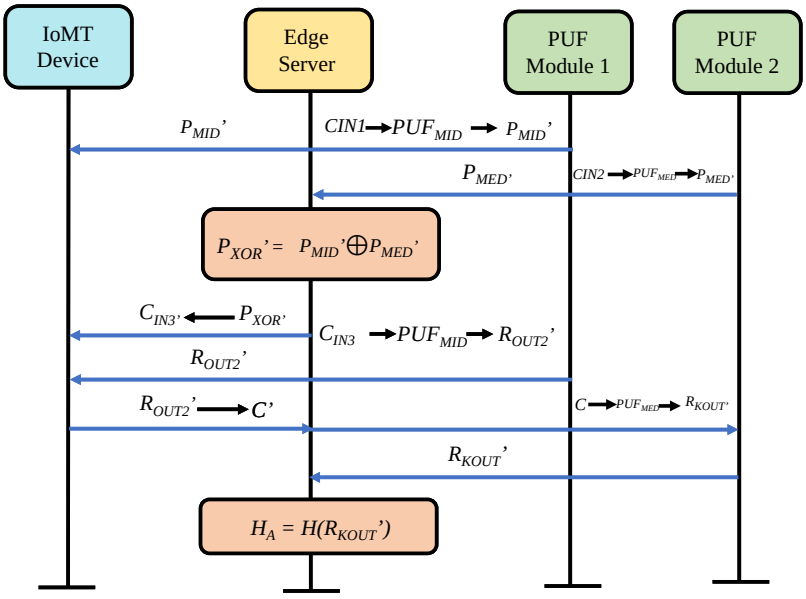


Fig. 6. Processing Flow of Device Authentication in PUFchain 3.0

Algorithm 2: 2nd Level Enrollment process of PUFchain 3.0

Edge Server (ES) receives PUF key from IoMT Client
// Selects a challenge input from C_{IN}
// $C_{IN} \rightarrow C_{IN2}$
// $P_{MID} \rightarrow$ ES
ES Performs PUF key extraction from PUF module
// $C_{IN2} \rightarrow R_{OUTED}$
ES performs PUF metric evaluation
if *Reliability of* R_{OUTED} ==*100%* then
    $R_{OUTED} \rightarrow PUF_{ED}$
    f(C_{IN2})$\rightarrow PUF_{ED}$
    $PUF_{ED} \rightarrow P_{MED}$
Perform XOR Operation
// $P_{XOR} \rightarrow P_{MID} \oplus P_{MED}$
ES sends XOR ed output as 2nd Challenge input to IoMT
// ES$\rightarrow P_{XOR} \rightarrow$ IoMT
IoMT gives corresponding XOR ed value as challenge input to its associated PUF module
// IoMT$\rightarrow P_{XOR} \rightarrow PUF_{MID}$
IoMT extracts response output for XOR ed Challenge Input
// $PUF_{MID} \rightarrow$ f$(C_{IN2}) \rightarrow R_{OUT2}$
IoMT sends PUF key as input to Edge Server
Edge performs PUF key extraction for the obtained input
// $PUF_{MED} \rightarrow$ f$(R_{OUT2}) \rightarrow R_{KOUT}$
SHA-256 hash function is used to compute hash on the obtained final authentication key
// Hash$\rightarrow$H$(R_{KOUT}) \rightarrow H_D$
Store the Hash value along with initial challenge inputs in a SDB
// $H_D, C_{IN1}, C_{IN2} \rightarrow$SDB

Step 7: The authorization key A_K for the MAM channel in the proposed security protocol is predefined as "MYKEY"

Step 8: Once the MAM channel is created, an API link is obtained and broadcast for the working nodes in H-CPS to view the MAM channel.

Step 9: Finally, hashing is performed on the root of the transaction R_K and A_K of the MAM channel to fetch the address (A_M) for the subsequent transaction. The new side key is defined as P_{MID} of IoMT.

Step 10: The subsequent transaction address (A_M) is broadcast back to the authenticated IoMT end device to upload.

The working mode of MAM is specified as "Restricted (2)". The secret key for the MAM is a predefined one which could be changed at any time depending on the security requirements.

Algorithm 3: Authentication process of PUFchain 3.0

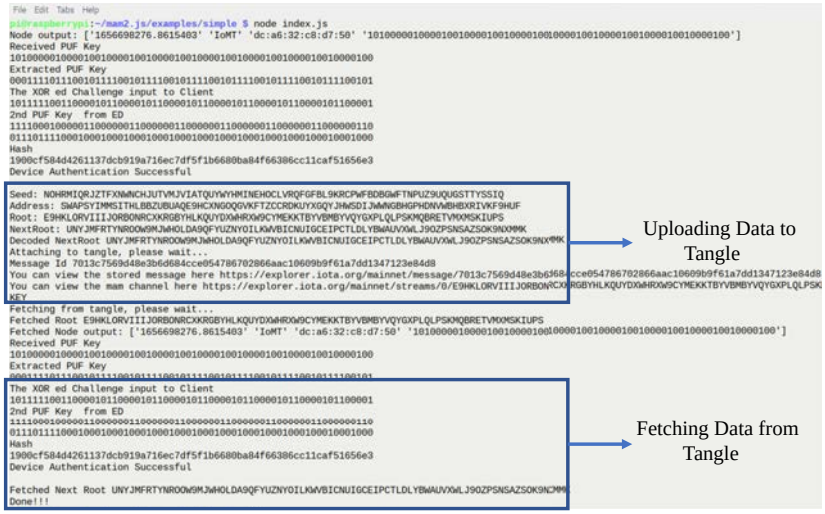
ES extracts challenge inputs from Secure Database
// SDB→C_{IN1}, C_{IN2}
IoMT and ES perform key extractions
// C_{IN1}→PUF_{MID}→$P_{MID'}$
// C_{IN2}→PUF_{MED}→$P_{MED'}$
Perform XOR operation and corresponding PUF key extractions
// $P_{XOR'}$→$PUF_{MID'}$ $\oplus$→$P_{MED'}$
Obtain final authentication key
// PUF_{MED}→$R_{KOUT'}$
Compute hash on obtained final authentication key
// Hash→H($R_{KOUT'}$)→ H_A
if H_A==H_D **then**
    Device Authentication is successful
    Create MAM channel
    Assign authorization key
    // MAM Channel→A_K
    // MAM Mode →Restricted (2)
    Upload Pseudo Identity of IoMT and ES
    // P_{MID} → Streams v0 (Channel)
    Fetch Next root
    // MAM Channel →New Root(N_R)
    Perform hash on side key and root
    // A_M →H(A_K, R_K)
    Broadcast New fetched root and new side key P_{MID}
else
    Discard the transaction
    Go to Step 1 for the new Transaction

6 Implementation and Validation

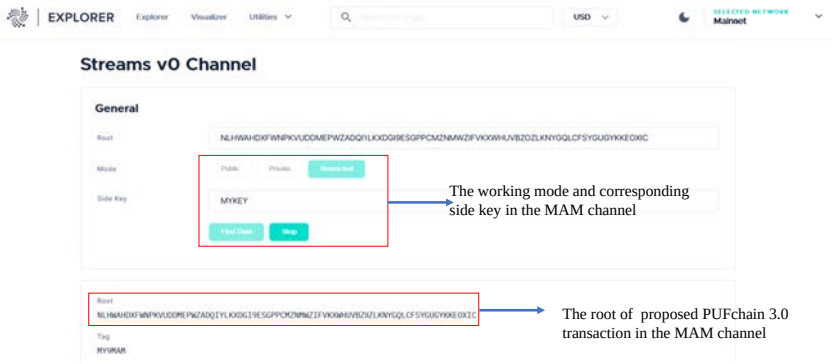
The proposed PUFchain 3.0 security is implemented using the Chrysalis version of IOTA Tangle. STREAMS is a new feature of Tangle which introduces new security features to improve the working ecosystem of Tangle by including cryptographic features [7]. The MAM channel used for this implementation has been STREAMS v0 channel. The working code MAM in Tangle is given in [1]. The time taken to upload a transaction into Tangle will be the total time taken for *Tip Selection, Transaction validation*. This is much shorter than the time taken to perform block addition in PoW which is 10 minutes [18]. The sample outputs of PUFchain 3.0 are given in Fig. 7.

The Single Board Computers (SBC) are connected to PUF modules built on two Xilinx FPGAs for PUF key extraction as, shown in Fig.8.

An Arbiter PUF is embedded on two Xilinx FPGA boards which are connected to Raspberry pi boards through pmod ports. Baud rate of 9600 is used to extract PUF keys from the Raspberry pis. Overall uniqueness of PUF keys from two PUF modules has



(a) Authentication and Transaction validation outputs



(b) STREAMS v0 Channel output

(c) Fetching Outputs from MAM channel

Fig. 7. Validation of PUFchain 3.0 in Tangle API

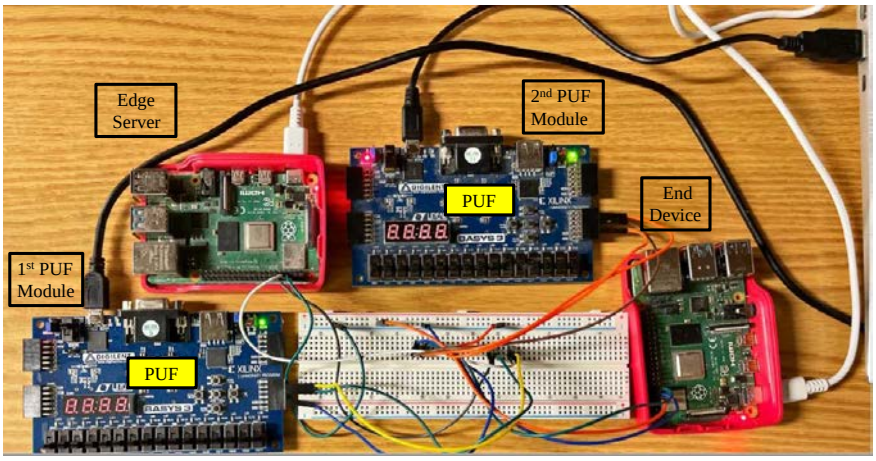


Fig. 8. Experimental Setup of PUFchain 3.0

been approximately 50%. The metrics of Arbiter PUF modules are given in Figs. 9 and 10.

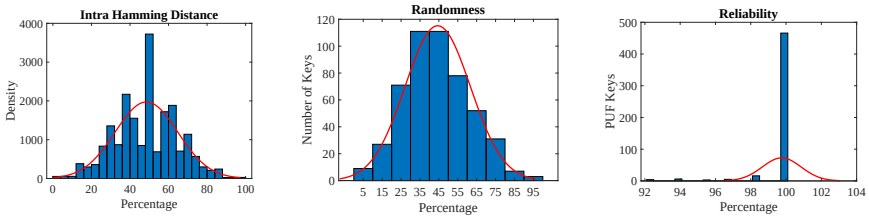


Fig. 9. Figure of Merits of 1st PUF module

Reliability has been approximately 100% when the two PUF modules have been tested with 500 PUF keys for four times at different instances of time and varying temperatures. The characterization of PUFchain 3.0 is given in Table 2.

The overall time to perform device authentication process in PUFchain 3.0 is between 2.7 to 3.6 seconds. Once the device authentication is done, the average time taken to upload the transaction onto Tangle Mainnet has been 28 seconds while the mean time to fetch the transaction has been approximately 1 second. The tabulated results of PUFchain 3.0 are given in Table 3 and comparative analysis of PUFchain 3.0 with the state of the art research is given in Table 4.

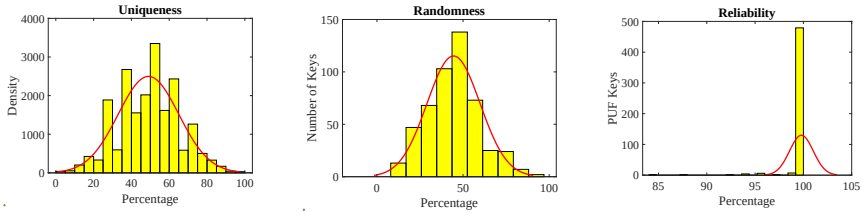


Fig. 10. Figure of Merits of 2nd PUF module

Table 2. Characterization of PUFchain 3.0

Parameters	Results
Application	Smart Healthcare
DLT	IOTA Tangle
Communication Protocol	MAM
PUF Module	Arbiter PUF
Programming	JavaScript, Verilog, Python
Working Mode	Restricted
IOTA Network	Mainnet
Number of PUFs	2
PUF	xc7a35tcpg236-1
Edge Server	Single Board Computer

Table 3. Metrics Evaluation of PUFchain 3.0

PUFchain 3.0 Serial No.	Time taken to fetch MAM transaction(sec)	Time to perform Device Authentication(sec)	Time to taken to upload transaction in Tangle network(sec)
1	1.073	3.66	17.31
2	1.266	3.66	19.91
3	1.288	3.66	13.60
4	0.914	3.28	6.18
5	1.288	3.18	58.40
6	1.057	3.72	55.61
7	1.213	3.32	28.54
8	1.12	3.04	32.0
9	1.235	2.96	19.9
10	1.099	2.72	31

7 Conclusions

Smart Healthcare is converging various technological solutions to enhance the quality of healthcare systems around the world. Various security solutions are being proposed to address the security vulnerabilities and realize the true potential of the IoMT, which constitutes an important part in H-CPS. This paper proposed and validated a sustain-

Table 4. Comparison with state of the art Research

Research Works	Security Protocol	DLT	Area	Approach	Security Primitive
Chaudhary et.al [8]	Auto-PUFchain	IPFS	IC Traceability	Smart Contracts	HAS
Al-Joboury and Al-Hemiary [3]	PoQDB	Blockchain and Cobweb	IoT	MQTT	Data Security
Wang et.al [26]	Blockchain and PUF-Based based Authentication Protocol	Blockchain	Smart Healthcare	Smart Contracts	HAS
Hellani et al. [13]	Tangle the Blockchain	Blockchain and Tangle	IoT	Smart Contracts	Data Security
Bathalapalli et al. [5]	PUFchain 2.0	Blockchain	Smart Healthcare	Proof-of-PUF Enabled Authentication	HAS
PUFchain 3.0 (Current Paper)	**PUFchain 3.0**	IOTA Tangle	Smart Healthcare	MAM	HAS

able security approach for device authentication and data confidentiality by utilizing PUF and IOTA Tangle. IOTA Tangle is becoming an alternative for Blockchain in IoT applications which are resource constrained decentralized systems due to its capability in offering a robust security for data as the Blockchain while being *'Miner and Transaction Free'*. By integrating PUF with Tangle, the device integrity can be ensured since each device fingerprint is stored in a DLT. A robust security protocol for device authentication has been implemented and stored in Tangle using MAM in restricted mode. The time taken to upload and retrieve the transaction in PUFchain 3.0 has been well within 1 minute which is almost $10\times$ times faster than the PoW consensus mechanism in Blockchain.

Exploring the possibility for a scalable Blockchain based consensus mechanism using PUF and IOTA Tangle to achieve the objective of SbD could be a direction for future research.

References

1. IOTA Foundation. iotaledger. mam.js (2021), `https://github.com/iotaledger/mam.js`
2. Abdullah, S., Arshad, J., Khan, M.M., Alazab, M., Salah, K.: PRISED Tangle: A Privacy-Aware Framework for Smart Healthcare Data Sharing using IOTA Tangle. Complex & Intelligent Systems (January 2022). https://doi.org/10.1007/s40747-021-00610-8
3. Al-Joboury, I.M., Al-Hemiary, E.H.: A Permissioned Consensus Algorithm Based DAGs-to-Blockchain in Hierarchical Architecture for Decentralized Internet of Things. In: Proc. International Symposium on Networks, Computers and Communications (ISNCC). pp. 1–6 (2021). https://doi.org/10.1109/ISNCC52172.2021.9615865

4. Alshaikhli, M., Elfouly, T., Elharrouss, O., Mohamed, A., Ottakath, N.: Evolution of Internet of Things From Blockchain to IOTA: A Survey. IEEE Access **10**, 844–866 (2022). https://doi.org/10.1109/ACCESS.2021.3138353
5. Bathalapalli, V.K.V.V., Mohanty, S.P., Kougianos, E., Baniya, B.K., Rout, B.: PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare. SN Computer Science **3**(5) (June 2022). https://doi.org/10.1007/s42979-022-01238-2
6. Bhandary, M., Parmar, M., Ambawade, D.: A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In: Proc. 5th International Conference on Communication and Electronics Systems (ICCES). IEEE (June 2020). https://doi.org/10.1109/icces48766.2020.9137858
7. Carelli, A., Palmieri, A., Vilei, A., Castanier, F., Vesco, A.: Enabling Secure Data Exchange through the IOTA Tangle for IoT Constrained Devices. Sensors **22**(4), 1384 (February 2022). https://doi.org/10.3390/s22041384
8. Chaudhary, C.K., Chatterjee, U., Mukhopadhayay, D.: Auto-PUFChain: An Automated Interaction Tool for PUFs and Blockchain in Electronic Supply Chain. In: Proc. Asian Hardware Oriented Security and Trust Symposium (AsianHOST). pp. 1–4 (2021). https://doi.org/10.1109/AsianHOST53231.2021.9699720
9. Dey, K., Kule, M., Rahaman, H.: PUF Based Hardware Security: A Review. In: Proc. International Symposium on Devices, Circuits and Systems (ISDCS). pp. 1–6 (2021). https://doi.org/10.1109/ISDCS52006.2021.9397896
10. Gangwani, P., Perez-Pons, A., Bhardwaj, T., Upadhyay, H., Joshi, S., Lagos, L.: Securing Environmental IoT Data Using Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle. Future Internet **13**(12), 312 (December 2021). https://doi.org/10.3390/fi13120312
11. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., Jain, R.: Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE Internet of Things Journal **8**(11), 8707–8718 (June 2021). https://doi.org/10.1109/jiot.2020.3045653
12. Guo, F., Xiao, X., Hecker, A., Dustdar, S.: Characterizing IOTA Tangle with Empirical Data. In: Proc. IEEE Global Communications Conference GLOBECOM. IEEE (December 2020). https://doi.org/10.1109/globecom42002.2020.9322220
13. Hellani, H., Sliman, L., Samhat, A.E., Exposito, E.: Tangle the Blockchain:Towards Connecting Blockchain and DAG. In: Proc. IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). pp. 63–68 (2021). https://doi.org/10.1109/WETICE53228.2021.00023
14. Hori, Y., Yoshida, T., Katashita, T., Satoh, A.: Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs. In: Proc. International Conference on Reconfigurable Computing and FPGAs. p. 298–303. RECONFIG '10, IEEE Computer Society, USA (2010). https://doi.org/10.1109/ReConFig.2010.24, https://doi.org/10.1109/ReConFig.2010.24
15. Joshi, S., Mohanty, S.P., Kougianos, E.: Everything You Wanted to Know About PUFs. IEEE Potentials **36**(6), 38–46 (2017). https://doi.org/10.1109/MPOT.2015.2490261
16. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., Douligeris, C.: Security in IoMT Communications: A Survey. Sensors **20**(17) (2020). https://doi.org/10.3390/s20174828, https://www.mdpi.com/1424-8220/20/17/4828
17. Lee, Y.S., Lee, H.J., Alasaarela, E.: Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF). In: Proc. 9th International Wireless Communications and Mobile Computing Conference (IWCMC). pp. 1314–1318 (2013). https://doi.org/10.1109/IWCMC.2013.6583746

18. Mohanty, S.P., Yanambaka, V.P., Kougianos, E., Puthal, D.: PUFchain: Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE) (2019). https://doi.org/10.48550/ARXIV.1909.06496
19. Pelekoudas-Oikonomou, F., Zachos, G., Papaioannou, M., de Ree, M., Ribeiro, J.C., Mantas, G., Rodriguez, J.: Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. Sensors **22**(7), 2449 (March 2022). https://doi.org/10.3390/s22072449
20. Pescador, F., Mohanty, S.P.: Guest Editorial Security-by-Design for Electronic Systems. IEEE Transactions on Consumer Electronics **68**(1), 2–4 (2022). https://doi.org/10.1109/TCE.2022.3147005
21. R, M., K, G., Rao, V.V.: Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. In: Proc. IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). IEEE (April 2021). https://doi.org/10.1109/iemtronics52119.2021.9422615
22. Razdan, S., Sharma, S.: Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. IETE Technical Review (May 2021). https://doi.org/10.1080/02564602.2021.1927863
23. Shabandri, B., Maheshwari, P.: Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. In: Proc. 6th International Conference on Signal Processing and Integrated Networks (SPIN). pp. 1069–1075 (2019). https://doi.org/10.1109/SPIN.2019.8711591
24. Shi, S., Luo, M., Wen, Y., Wang, L., He, D.: A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems. Security and Communication Networks **2022**, 1–18 (03 2022). https://doi.org/10.1155/2022/6735003
25. Silvano, W.F., De Michele, D., Trauth, D., Marcelino, R.: IoT sensors integrated with the distributed protocol IOTA/Tangle: Bosch XDK110 use case. In: Proc. X Brazilian Symposium on Computing Systems Engineering (SBESC). pp. 1–8 (2020). https://doi.org/10.1109/SBESC51047.2020.9277865
26. Wang, W., Chen, Q., Yin, Z., Srivastava, G., Gadekallu, T.R., Alsolami, F., Su, C.: Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. IEEE Internet of Things Journal **9**(11), 8883–8891 (2022). https://doi.org/10.1109/JIOT.2021.3117762
27. Zheng, X., Sun, S., Mukkamala, R.R., Vatrapu, R., Meré, J.B.O.: Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. Journal of Medical Internet Research **21** (2019)