Article

PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in the Healthcare Cyber-Physical Systems

Venkata K. V. V. Bathalapalli [1,†], Saraju P. Mohanty [2,†], Elias Kougianos [3,‡], Vasanth Iyer[4,‡] and Bibhudutta Rout[5,†]

1 Dept. of Computer Sci. and Eng., University of North Texas; vb0194@unt.edu
2 Dept. of Computer Sci. and Eng., University of North Texas; saraju.mohanty@unt.edu
3 Dept. of Electrical Engineering, University of North Texas; elias.kougianos@unt.edu
4 Dept. of Computer Sci., and Digital Technologies, Grambling State University; iyerv@gram.edu
5 Dept. of Physics, University of North Texas; bibhudutta.rout@unt.edu

Abstract: This article presents a novel hardware-assisted distributed ledger-based solution for simultaneous device and data security in smart healthcare. This article presents a novel architecture that integrates PUF, Blockchain, and Tangle for Security-by-Design (SbD) of Healthcare Cyber-Physical-Systems (H-CPS). Healthcare systems around the world have undergone massive technological transformation and have seen growing adoption with the advancement of Internet-of-Medical-Things (IoMT). The technological transformation of healthcare systems to Telemedicine, e-health, connected health, and remote health is being made possible with the sophisticated integration of IoMT with Machine Learning, Big Data, Artificial Intelligence (AI), and other technologies. As healthcare systems are becoming more accessible and advanced, security and privacy have become pivotal for the smooth integration and functioning of various systems in H-CPS. In this work, we have presented a novel approach that integrates PUF with IOTA Tangle and Blockchain and works by storing PUF keys of a patient's Body Area Network (BAN) inside Blockchain to access, store, and share globally. Each patient has a network of smart wearables and a gateway to obtain the physiological sensor data securely. To facilitate communication among various stakeholders in healthcare systems, IOTA Tangle's Masked Authentication Messaging (MAM) communication protocol has been used that securely enables patients to communicate, share, and store data on Tangle. The MAM channel works in the restricted mode in the proposed architecture which can be accessed using the patient's gateway PUF key. Furthermore, the successful verification of PUF enables patients to securely send and share physiological sensor data from various wearable and implantable medical devices embedded with PUF. Finally, healthcare system entities like physicians, hospital admin networks, and remote monitoring systems can securely establish communication with patients using MAM and retrieve the patient's BAN PUF keys from the Blockchain securely. Our experimental analysis shows that the proposed approach successfully integrates three security primitives PUF, Blockchain, and Tangle providing decentralized access control and security in H-CPS with minimal energy requirements, data storage, and response time.

Keywords: Smart Healthcare; Healthcare Cyber-Physical-Systems (H-CPS); Physical Unclonable Function (PUF); Hardware-Assisted Security (HAS); Masked Authentication Messaging (MAM); Security-by-Design (SbD); Blockchain; Tangle.

Citation: Lastname, F.; Lastname, F.; Lastname, F. Title. *Sensors* **2023**, *1*, 0. https://doi.org/

Received:
Revised:
Accepted:
Published:

1. Introduction

The application of IoMT has made Healthcare systems more advanced by integrating various technologies like Machine Learning (ML), Big Data, and Blockchain [1,2]. Smart e-health service applications are becoming more adaptable through the integration of Medtronic devices for patient physiological metrics monitoring and sensing. Telemedicine, e-health, and connected health are emerging healthcare ecosystems with advanced network communication technologies like 5G, and 6G supporting data sensing, communication, and analysis through AI and ML technologies. Medtronic devices play an important role in realizing the potential of these applications. However, the potential security vulnerabilities

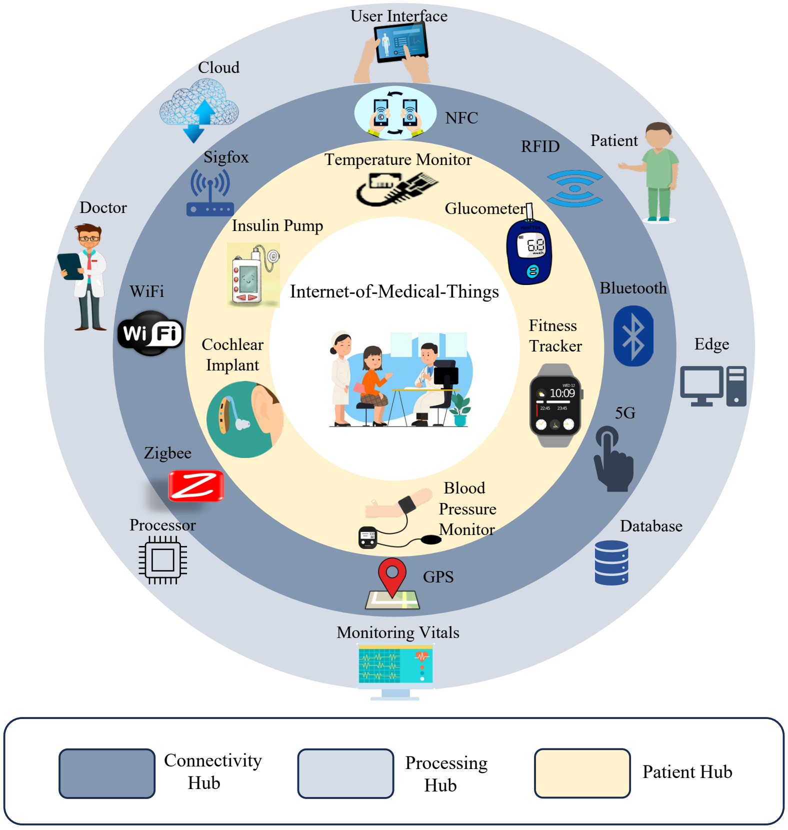


Figure 1. Healthcare-Cyber-Physical-System.

1.1. Cybersecurity in Smart Healthcare

IoMT is a collection of heterogeneous smart Medtronic devices with diverse functionalities and capabilities that can sense and process various parameters and is grouped as a hub on the patient to analyze the patient's physiological parametric data as shown in Fig.2. The data from these heterogeneous devices is analyzed and processed for effective analysis, decision making, and monitoring of patient health. [3,4]. These devices are not computationally capable of processing the data and require ML and AI-supported capabilities for processing and decision making which can be supported by Edge, Cloud, and Fog computing paradigms. Wearable and implantable medical electronic devices are placed inside and, on the body, to monitor various physiological parameters and generate data. These devices can be smart pumps to deliver insulin dosage, Pacemakers that can simulate neurological signals inside the brain, and an active fitness tracker monitoring heart rate and Blood pressure [5,6]. Various security attacks are possible through eavesdropping, spoofing, and sniffing to obtain sensitive patients' physiological information using security vulnerabilities associated with the system. An adversary can intercept the communication between an IoMT device and the health service entity with computing capabilities to obtain access to the system and control it. This can pose a question on data integrity and device authenticity in IoMT, which may jeopardize the Healthcare service applications [7,8].

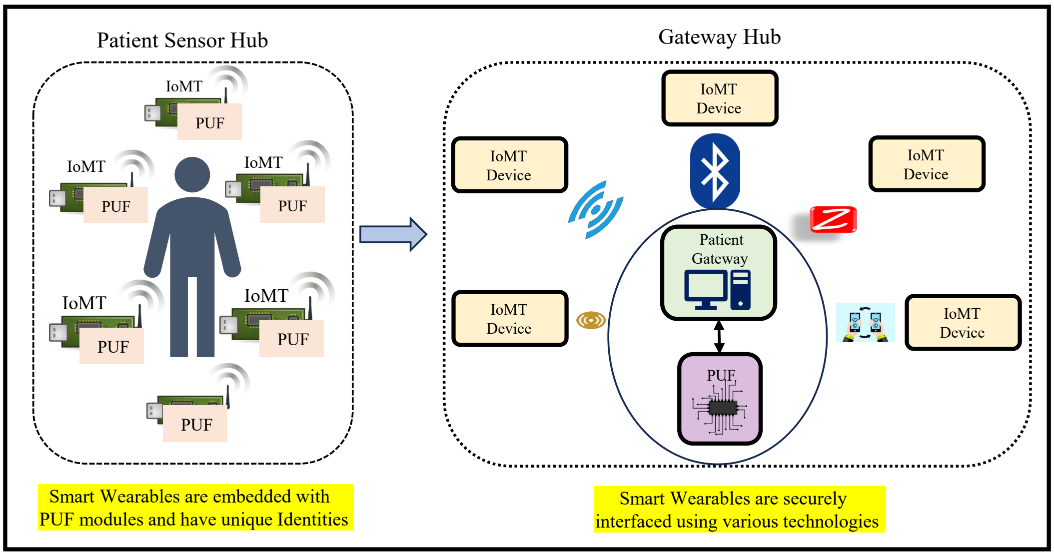


Figure 2. Patient's Body Area Network

To address the data privacy issues in smart healthcare, many researchers have adopted Distributed Ledger Technology (DLT) based solutions that provide immutability and confidentiality to data [9,10]. DLT can facilitate authorized access to data and can counter any adversarial measure to tamper with the data. These functionalities have made the DLT based approach for providing security and privacy to data more alluring specifically in the areas of Banking, Finance, e-Health, and Smart Cities which demand utmost secrecy and confidentiality of data in their applications.

The IoMT devices are vulnerable to various types of physical attacks [11,12]. Cybersecurity solutions are often based on software-based approaches that work based on symmetric and asymmetric key cryptography schemes. These approaches require non-volatile memory or drives for key storage and retrieval. Using asymmetric keys for encryption and data decryption can sometimes restrict access to medical professionals, or patients [13]. This sort of dependence on memory has made these security protocols more vulnerable to various ML attacks where an attacker can obtain access to the secret key and the system [14]. SbD is one of the new paradigms that has attracted much attention from the research community. This approach focuses on building a security model right from the design stage. PUF is a prominent SbD that is a unique hardware identity generation scheme.

Various Hardware-Assisted security (HAS) approaches for cybersecurity are being adopted using PUF and Trusted Platform Modules (TPM) to achieve the objective of SbD [11,15]. PUF-based security solutions include a PUF module that is embedded in a chip and can generate keys from the PUF design using process variations inside an Integrated Circuit (IC) [11,15,16]. The generated keys can be used as security keys or identities for that PUF module on the chip. PUFs do not require a database for key storage and PUF responses are generated instantly by taking advantage of micro-manufacturing process variations during chip fabrication [15,17,18]. Data confidentiality, integrity, privacy, and device authentication are requirements for sustainable SC. Blockchain has been one of the most widely explored DLTs for financial transactions since its inception in 2008 [19]. However, resource constrained IoT devices cannot sustain the computational resource requirements of blockchain's consensus mechanisms like Proof-of-Work (PoW). Data immutability, integrity, and privacy in SC are guaranteed by Blockchain through its scalable, decentralized physiological data management using energy efficient consensus mechanisms [11].

The motivation for this research is to ensure the security of IoMT devices and their data where Patient's BAN PUF keys are securely stored inside a global Blockchain to provide end-point security. Tangle is used for secure communication of patient's physiological sensor data and its access is controlled using a unique identity generated by PUF for the patient's gateway. The proposed architecture works on integrating PUF with a DLT for providing a sustainable security primitive for IoMT-driven Smart Healthcare as illustrated in Fig. 3.

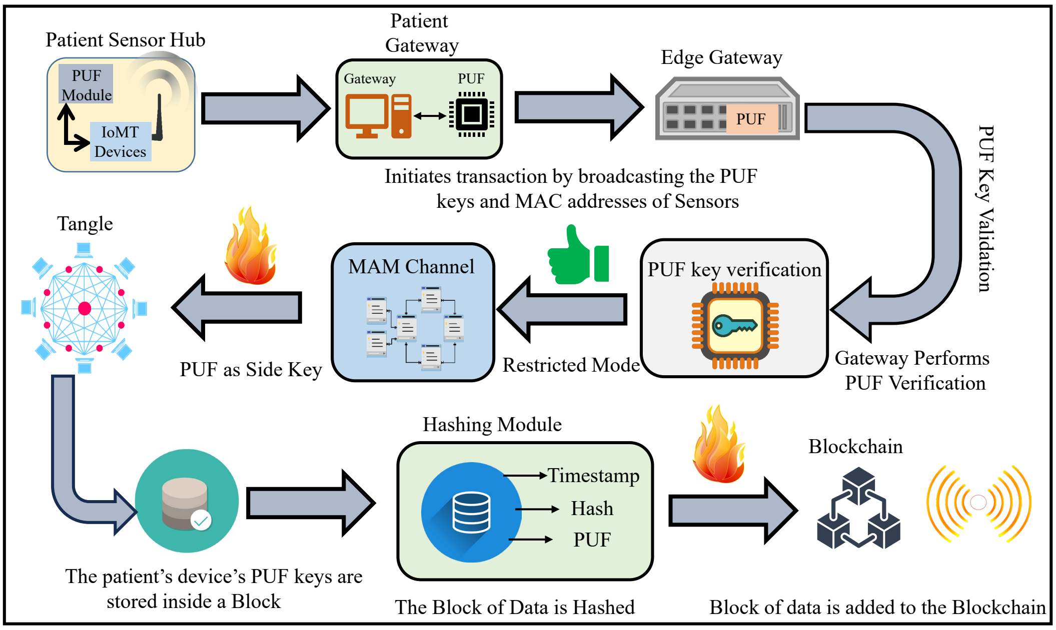


Figure 3. Architectural overview of Proposed SbD approach for H-CPS .

Following the introduction, the rest of the paper is organized as follows: Section 2 presents the novel contributions of this paper. Section 3 discusses various hardware security schemes and DLT-based solutions in SC from the literature. The conceptual overview of SbD and the role of PUF as a formidable security primitive is given in section 4. Section 5 explains IOTA Tangle, transaction validation, and masked authentication messaging (MAM) concepts. A brief overview of Blockchain technology is given in section 6. The working flow of device authentication and transaction validation process in the proposed PUFchain 3.0 is explained in Section 7. Section 8 outlines the implementation details and section 9 presents the conclusion and directions for future research.

2. Novel contributions

In this section, we have explained the challenges and contributions of the present work in 2.1. We have presented the novelty and significance of our present work PUFchain 3.0 in 2.2. Finally, a brief overview of our PUFchain idea: "*First ever Hardware-Assisted Blockchain*" and its variants is given in 2.3.

2.1. Research Problems Addressed in the Current Paper

The proposed work has been envisioned to address the following questions:

- To the best of our knowledge, very few security primitives work on providing device and data-assisted security simultaneously for e-Health applications.
- Security gaps associated with Device's integrity, Data confidentiality, and authenticity in edge computing driven H-CPS.
- Lack of scalable and energy-efficient security approach for resource-constrained distributed systems in H-CPS.
- Sustainable approach for device integrity-based access control mechanism for Electronic health records (EHR) management.
- Energy efficient PUF architectures that are effective against machine learning and other attacks.

- Lack of sustainable, and energy-efficient hardware-assisted access control mechanism to the distributed ledger.
- A secure communication interface between various stakeholders in H-CPS with defined access and security.
- Presenting a security framework that could be integrated into real-world healthcare applications.
- Providing a cost-effective innovative approach to integrate various technologies for cybersecurity in smart healthcare.
- Enabling a patient to embed smart health devices that are secure and non-vulnerable to security attacks.

2.2. Novel Contributions of this Article

- Presenting a novel state-of-the-art integration of PUF, Blockchain, and Tangle for SbD of H-CPS. To the best of our knowledge, this is the first work on hardware-assisted security in H-CPS, that presents a PUF-based approach for access to DLT for device and data security in H-CPS.
- Presenting a novel PUF-based access control mechanism for Tangle.
- A novel Blockchain integrated framework for security in H-CPS using Smart contracts.
- Validating proposed framework in MAM's "Restricted mode" for secure access control to Tangle using PUF.
- An energy-efficient SbD approach that uses delay Arbiter and XOR PUF architectures.
- An Edge-Cloud driven approach for resource-constrained systems in H-CPS that has three layers: Physical layer, edge layer, and Blockchain layer as illustrated in Fig. 4.
- A novel energy-efficient approach that works on Blockchain using smart contracts for storing and retrieving PUF keys of IoMT devices inside a patient's Body area network (BAN).
- A security approach that facilitates secure access to patients' BAN and ensures the integrity of data from IoMT in resource-constrained distributed systems.

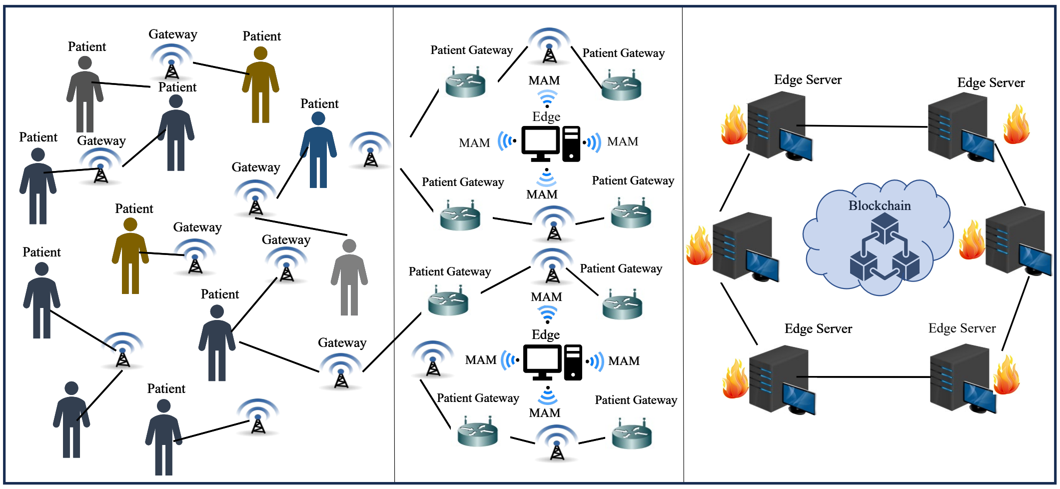


Figure 4. Layered view of PUFchain 3.0 Architecture

2.3. A Comprehensive Evaluation of PUFchain Primitives

The conceptual idea of PUFchain is presenting hardware-assisted secure distributed ledger for sustainable device and data security in the emerging Internet-of-Everything (IoE). Hardware-assisted security involves embedding advanced electronic systems with PUF for device integrity. PUF-embedded security facilitates each electronic system to obtain a unique device identity that can relate to Blockchain and other distributed ledgers. Table 1, and Fig. 5 present a comparative analysis of our PUFchain variants.

Table 1. Comparison of PUFchain Variants

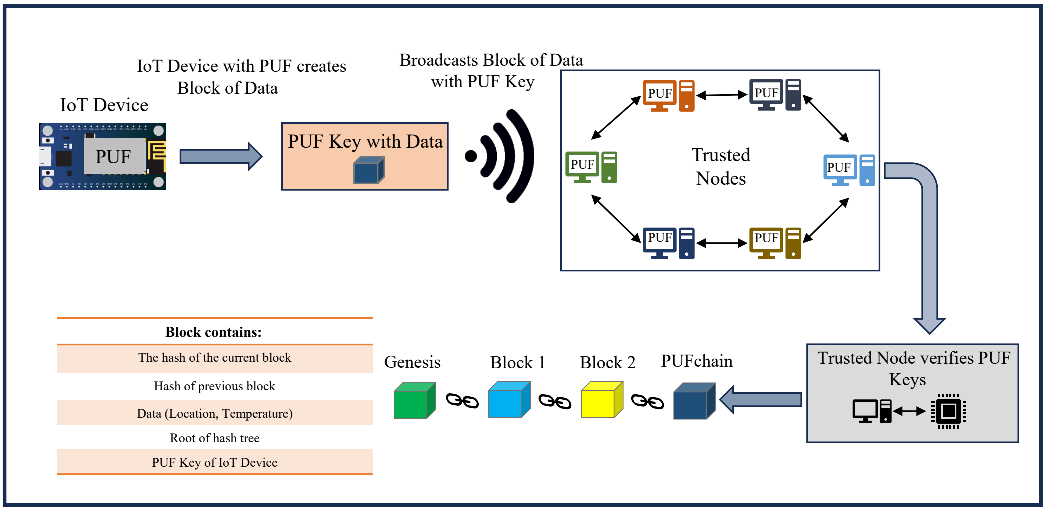
Research Work	Features	Security Approach
PUFchain [19]	The PUF-generated keys are securely stored inside the Blockchain for securely binding the identity of each device inside the Blockchain. PUF keys stored inside the Blockchain can be retrieved securely for advanced applications requiring security for IoT devices.	Proof-of-PUF-Enabled-Authentication (PoP)-PUF based Blockchain.
PUFchain 2.0 [11]	In PUFchain 2.0, for security and privacy in IoMT, a novel PUF-based Blockchain solution for IoMT device and data security that has a two-level authentication mechanism is proposed. This approach has a MAC address-based verification as an initial stage followed by the PUF key verification stage.	PUF Based Blockchain with MAC Address verification
PUFchain 3.0 [20]	For security and privacy in smart healthcare, all IoMT devices and their data are secured through PUF-assisted distributed ledger. This approach has PUF, Blockchain, and Tangle for simultaneous device and data security in H-CPS.	PUF-based distributed ledger using MAM and Smart Contracts

3. Related Works

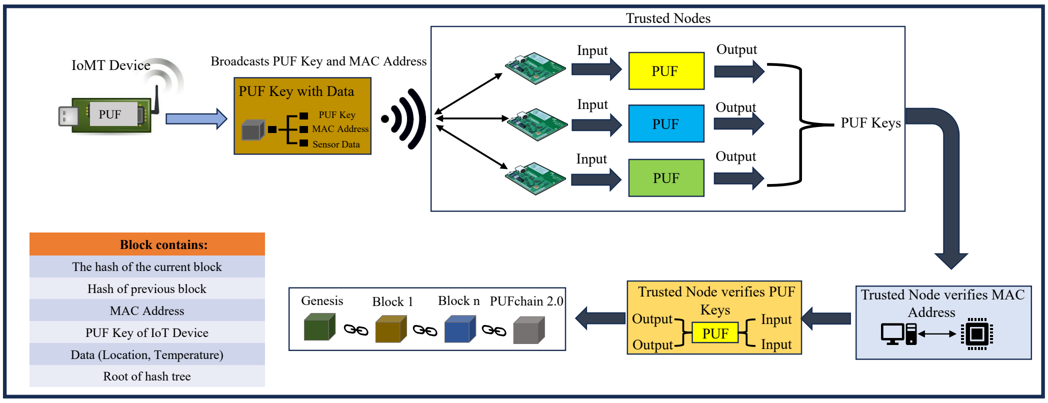
In this section, we have presented a brief review of related research on various distributed ledger technology-based cybersecurity solutions in smart healthcare. A comparative analysis of the proposed work PUFchain 3.0 with state-of-the-art research is given in Table 2.

Integration of hardware assisted distributed ledger for SbD of CPS has gained prominence for addressing security gaps in various CPS which include Healthcare CPS, Agriculture CPS, and Transportation CPS. Authors in [21] presented a scalable blockchain integrated distributed ledger solution for IoT applications. Their architecture has a Blockchain running in the backend and a Tangle at the front end. This approach claims to speed up the data processing from IoT devices by securely integrating with Tangle which then offloads the data storage to Blockchain in the cloud. In [22], authors propose an IC supply chain management system using PUF based Blockchain. Their work proposes a PUF based chip tracking system that uses Blockchain to securely record and trace the ownership of a chip. A consensus mechanism for IoT applications is proposed in [23]. Their work presented a consensus mechanism titled "PoQDB" which integrates Blockchain with CoBweb ledger to facilitate IoT data storage. The proposed work PUFchain 3.0 is an extension of the initially presented PUFchain [19], which is a novel integration of PUF and Blockchain using a Proof-of-PUF-Enabled-Authentication (PoP) consensus mechanism for IoT security.

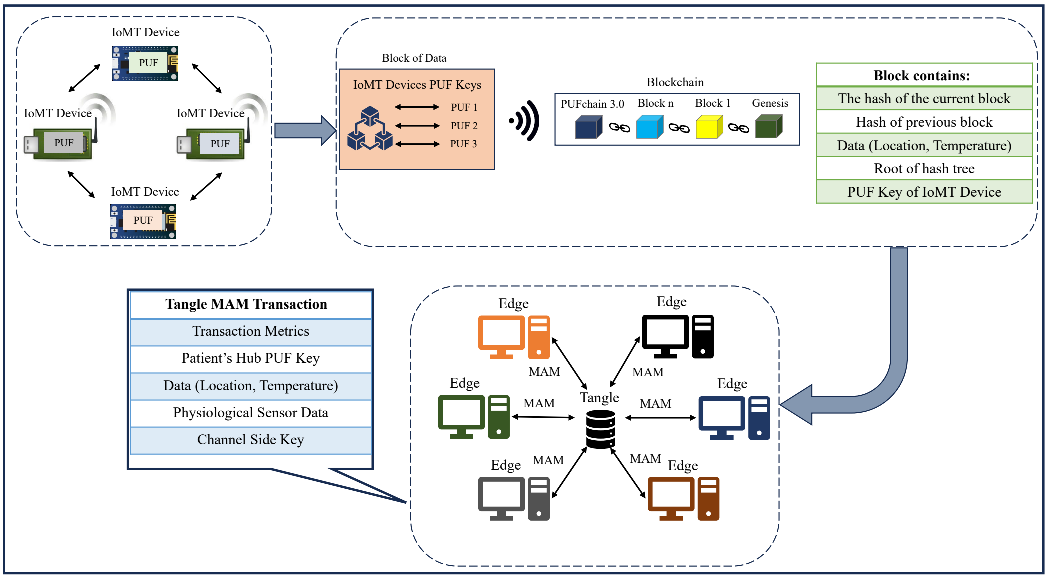
SbD of H-CPS is a focus area for many researchers since privacy and security issues have direct implications on the patient's life. A smart remote patient monitoring system using IOTA is presented in [24]. This research proposed and validated an IOTA MAM based approach for patient data access control and security. Using IPFS and MAM, their research validated an approach for patients' IoT device control and access using a secure web interface. A blockchain assisted solution for IoMT device security and access control is proposed in [25]. The motivation of their work is to provide security between different entities in healthcare systems. Blockchain-assisted IoMT key exchange mechanism is presented in [26]. Their work aims to address the single point failure problem in processing data securely from IoMT devices. They presented a private consortium Blockchain to



(a) PUFchain



(b) PUFchain 2.0



(c) Proposed PUFchain 3.0

Figure 5. PUFchain Variants

validate the work and proposed a scheme for securely establishing communication between authenticated IoMT devices. However, their work uses cryptography to secure the keys of IoMT devices which can be vulnerable to ML attacks. Authors in [9] propose a secure

IoMT data sharing scheme using IOTA MAM. Different modes of MAM were used to publish data onto Tangle which includes sensor and patient data. A PUF-based approach for the security of low-cost IoT devices in healthcare is proposed in [27] which presents a microcontroller based PUF that has 99% accuracy. Authors in [28] designed a blockchain enabled IoMT device authentication architecture that presents an approach for encrypted communication and certificate-based identity attestation in IoMT. Detection of IoMT device misfunctioning and behavior is another efficient approach for device security. Authors in [29] presented a privacy preserving IoMT device behavior detection using blockchain. In the paper, they validated this approach for insulin pumps to monitor patient's glucose levels.

For sustainable device and data security in smart healthcare, we proposed PUF based Blockchain solution named PUFchain 2.0 [11]. In this work, we validated and presented a PUF based Blockchain consensus mechanism for simultaneous device and data security. We observed the potential of hardware-assisted distributed ledgers for security in smart healthcare. The proposed PUFchain 3.0 work extends the potential of PUF based distributed ledger in smart healthcare by facilitating decentralized security and access control to IoMT devices and their data in H-CPS. In comparison with the related research, our work presents an architecture to address both device and data security with minimal latency and better scalability thereby facilitating secure access control and security in smart healthcare.

Table 2. Comparative analysis with state-of-the-art Research.

Research Works	Application	Security Primitive	Platform	Mechanism
Hellani et al. 2021 [21]	IoT (Data)	Blockchain & Tangle	Edge-Cloud	Smart Contracts
Mohanty et al. 2019 [19]	IoT (Device & Data)	PUF, Blockchain	Edge	Proof-of-PUF-Enabled-Authentication
Al-Joboury et al. 2021 [23]	IoT (Data)	Blockchain & Cobweb	Cloud	IoT M2M Messaging (MQTT)
Wang et al. 2022 [30]	IoMT (Device)	Blockchain	Edge	Smart Contracts
Chaudhary et al. 2021 [22]	Hardware Supply Chain	PUF, Blockchain	Edge-Cloud	Smart Contracts
Venkata et al. 2022 [11]	IoMT (Device)	PUF, Blockchain	Edge	Media Access Control (MAC) & PUF based Authentication
Satra et al. 2023 [14]	IoMT (Device)	PUF	Edge	Machine Learning
Fotopoulos et al. 2020 [28]	IoMT (Device)	Blockchain	-	Self- Sovereign Identity (SSI)
Zheng et. al 2023 [9]	IoMT (Data)	IOTA Tangle & Blockchain	Edge	MAM
Proposed PUFchain 3.0 [20]	**IoMT(Device & Data)**	**PUF, Tangle, Blockchain**	**Edge-Cloud**	**Masked Authentication Messaging, smart contracts**

4. Role of Physical Unclonable Functions as SbD Primitive

4.1. Security-by-Design

SbD or Privacy-by-Design (PbD) is a system development paradigm for smart electronics that emphasizes the security of an electronic system at the development stage considering the intrinsic properties at the design, manufacturing, testing, and implementation. The principles and objectives of SbD as explained in Fig. 6 mainly envision to avoid performance tradeoffs in security primitives at the application stage of an electronic system [31,32]. The

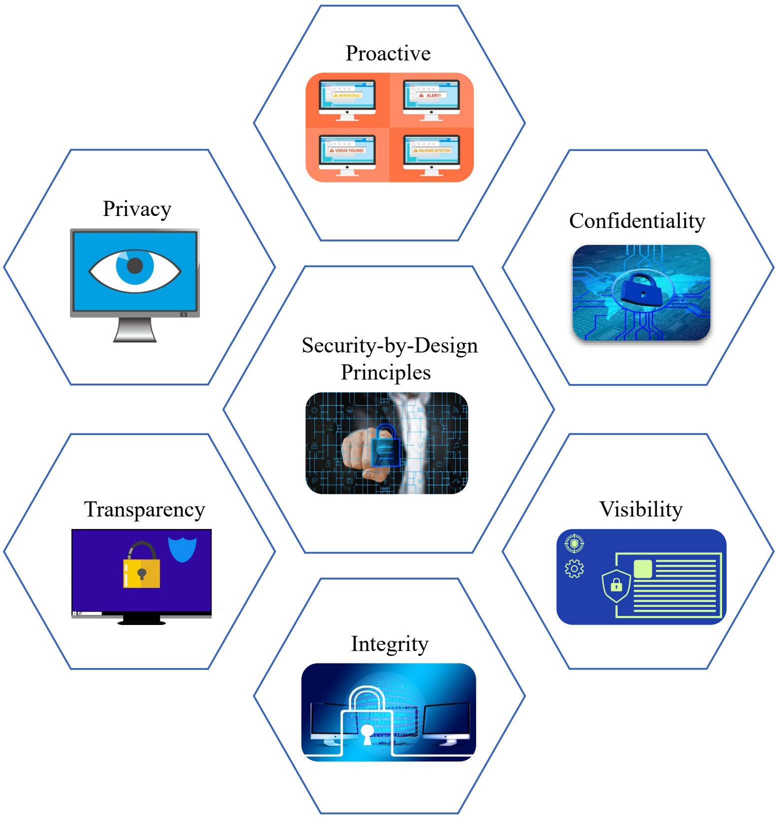


Figure 6. Security-by-Design Principles

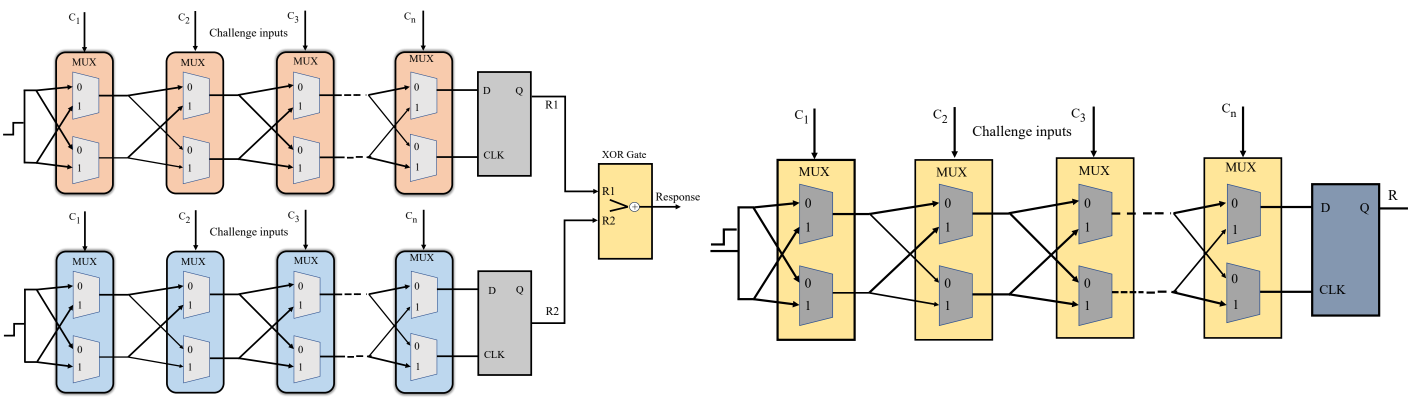
principles of SbD are:

1. *Proactive but not reactive:* Existing cybersecurity solutions for smart electronics mostly focus on the security at application level. SbD promotes security as a design stage metric that is enabled by default.
2. *End-to-End Security*: Security of the system should be considered right from the design stage to manufacturing, deployment, application, and maintenance.
3. *Security as Default*: Security primitive should be enabled by default in the system and cannot be an optional primitive for the users to choose from.
4. *Least Privilege*: Users of an electronic system should have the privileges to run the applications and should not have access to tamper with the system's security specifications.
5. *Transparency*: The security principles should be clearly transparent and easily understandable. The users of an SbD-enabled system should have access to change their security level based on their choice and should be able to clearly understand its functionality.
6. *User Centric*: Ease of security principles and deployment is an essential aspect of SbD. The security primitives should not be burdensome for the users.
7. *Full Functionality*: The security primitive should have efficient performance and should not have performance tradeoffs that might impact the system's functionality and applications.

4.2. PUF for SbD of H-CPS

PUF is a hardware security primitive that uses device inherent manufacturing imperfections and generates a unique cryptographic identity. Each electronic device has a unique topology due to the manufacturing variations during the fabrication of an Integrated Circuit (IC) which is the building block of a consumer electronic system [33]. As each device has a distinct topology, unique keys can be derived based on its device property variations such as frequency, delay, or startup phase of a volatile memory cell. Process variations can be observed during various stages of an IC fabrication process such as lithography, ion implantation, metallization, and packaging [20]. The variations introduced during these processes will slightly differentiate each device from the corresponding ones even if they have the same fab, processes, and design. PUF works by deriving a key of random zeros and ones using the device's intrinsic properties. PUFs can be classified based on the mapping of physical properties. PUF modules that work based on the propagation delays and frequency variations in an IC to build a unique bit stream are delay-based PUFs. Arbiter and Ring oscillator, XOR, and Butterfly PUF are widely used delay PUFs. These are also referred to as strong PUFs that can support the extraction of many random zeros and ones as a bit stream which is essential for security applications. Similarly, Static Random Access Memory (SRAM) and Dynamic Random Access Memory (DRAM) are prominent memory PUF modules that work by generating a unique response based on the variations in the memory structures such as Flip Flops, and an SRAM cell. The structure of Arbiter and XOR PUF used for experimental validation in this work are presented in Fig. 7. PUF module works on the physical randomness of devices by mapping a challenge input to a unique response output string. The uniqueness of this primitive is that it does not generate the same responses for varying challenge inputs. Also, two different PUF modules tested against the same challenge input will have varying bits of random zeros and ones as responses [19,34]. The responses from PUF are evaluated against various metrics to verify the strength of keys. Some of the Figure-of-merits (FoM) of PUF are illustrated as follows:

- ***Uniqueness***: Verifying the extent of variation of responses from a PUF circuit on two devices is referred to as uniqueness. This is measured by calculating the average inter-hamming distances of responses from the PUF module on two devices tested with the same set of challenges.
- ***Reliability***: The stability of a PUF is determined by determining the variation of responses at different environmental conditions. This is an essential metric in evaluating a PUF strength since the responses of PUF must be stable under noise as well as at varying operating conditions.
- ***Randomness***: of a PUF is its ability to produce a response key with an equal number of randomly distributed 1's and 0's. Ideally, a PUF response should have exactly an equal number of ones and zeros in the response bit stream.
- **Diffuseness:** Diffuseness of a PUF is obtained by calculating the average Intra-Hamming distance of PUF responses to verify the extent of variation of response for varying challenge inputs in the same PUF.



(a) XOR Arbiter PUF **(b)** Arbiter PUF Instance Generating 1-bit Output

Figure 7. Architectures of Delay PUFs Experimentally Validated in the Proposed Work

5. IOTA Tangle: A DAG Blockchain

IOTA Tangle is a DAG-based Blockchain that has a Tangle structure. It is a distributed ledger from IOTA and one of the most suitable DLT based solutions in IoT applications due to its miner and feeless functionality. All the transactions in Tangle are part of Directed acyclic graph (DAG) structure . The major advantage of this structure is that it increases the transaction validation rate exponentially when compared with the traditional Blockchain structure that has all the transactions aligned sequentially [24]. Every new transaction on Tangle from a node validates unconfirmed transactions called "Tips" to become part of the structure. Every incoming transaction validates tips using Proof-of-Work and therefore increasing the number of incoming transactions substantially increases the rate of validated transactions. Tips are selected using the 'Markov Chain Monte Carlo (MCMC)' random walk algorithm which traverses the DAG and obtains the transactions to be validated [35,36]. Proof-of-Work (PoW) validates a transaction by calculating the nonce and solving cryptographic puzzles. Once the tips are validated by an incoming transaction, then these transactions become confirmed in Tangle. PoW in Tangle is computationally resource efficient in comparison with Blockchain's PoW consensus mechanism [37].

Each transaction node in Tangle has a cumulative weight which is calculated by adding its initial weight and the cumulative weight of all the transactions directly or indirectly approve it[38,39]. In this DLT, a coordinator is responsible for overall transaction validation and approval. At present, the IOTA foundation is the coordinator that releases the milestones defining transaction validation rules. Simply, a coordinator is responsible for the overall functioning of the transaction validation approval process in Tangle [40]. A milestone is a stage where confirmed transactions become irreversible and final on Tangle [41].

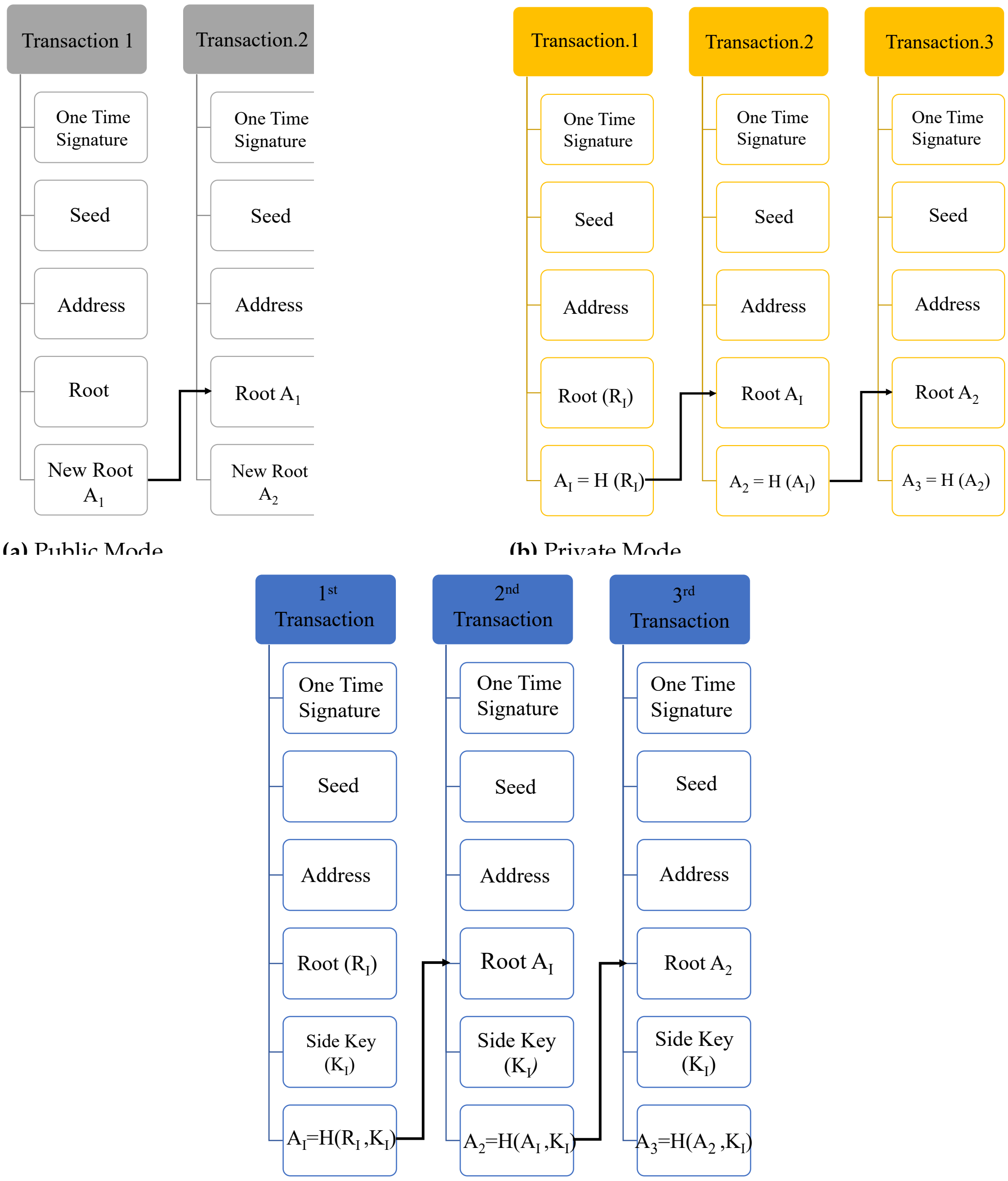
IOTA MAM is a secure messaging protocol that operates on the IOTA main network for sending and receiving the encrypted information in Tangle through a channel by signing the message using the Merkle Hash Tree (MHT) signature algorithm. The message can be accessed by the receiver using the channel's address and 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. MAM operates in three different communication modes: Public, Private, and Restricted [24].

Each channel mode has a distinct functionality and security level based on the application. Each transaction on the MAM channel has a reference to the next transaction address which links all the transactions on that channel. However, each MAM mode has a different way of working to access the new transaction address as illustrated below: [42–44]. MAM works mainly in three modes: Public, Private, and Restricted. The working flow of MAM in public, private, and restricted modes is illustrated in Fig. 8.

Public Mode: In Public channel mode, The Merkle tree root is used as the MAM transaction address. A MAM channel with an address is generated to secure information exchange. The address of the channel will be the root of the Merkle Tree. The subsequent transaction must be submitted to the MAM channel using this fetched root and anyone with the channel ID or address can access the channel and receive the messages.

Private Mode: In private mode, the address of a MAM transaction is obtained by hashing the root of Merkle root. For applications requiring privacy and confidentiality, as in the case of health record management, private mode is suitable and efficient since only the subscribers with root can decrypt the messages.

Restricted Mode: The restricted mode of MAM works by using a channel *Authorization key* or *Side key* along with the Merkle root. In this channel mode, along with the root, the side key is also hashed to obtain the transaction address on the channel. This mode provides the highest level of security for the transactions on MAM since only subscribers with an authorization key c



(a) Public Mode **(b)** Private Mode

(c) Restricted Mode

Figure 8. Masked Authentication Messaging

6. Overview of Blockchain Technology

The success of Blockchain in providing integrity and authenticity to data is not just limited to H-CPS but also in other areas of CPS like smart transportation, Industrial IoT, and Agriculture CPS. A simple decentralized data validation and verification system provided by Blockchain has made it the most alluring research area in the 21st century. Each transaction in blockchain is stored inside a block of data which is hashed and has reference to the previous block's hash. Miners are responsible for block validation in blockchain [11]. The validation of a block is done through a consensus mechanism that defines rules for choosing the miners and validating the transactions. Research on blockchain consensus mechanisms has become a focus area for the research community. In all the blockchain consensus mechanisms, a miner is required to validate the transaction, and various checks and balances are in place to negate the probability of fake block generation and validation. 51% percent attack is one of the challenges of Blockchain where fake nodes could control 51% of the block addition process [19]. Blockchain technology has been perceived to be a breakthrough in realizing the potential of Digital ledger technology (DiLT) for IoT-based applications. Blockchain's robustness and features have made integration with various technologies like AI and ML an important area to work on. As various security solutions using blockchain for data have already been proposed, more emphasis is being laid on exploring the possibilities for hardware-assisted blockchain for security [12,45]. Blockchain and tangle have varied data structures. In blockchain, the transactions are validated and added inside blocks which are aligned sequentially. Tangle is based on the Merkle tree, and it does not take much time to check whether a transaction is fake since it is a tree-based structure generation scheme [10,43]. Tangle transactions are signed using a one-time signature scheme (OTS). The Merkle tree consists of private keys as leaves which are hashed and consolidated to obtain the root address. Fig. 9 presents a comparative perspective of Blockchain and Tangle.

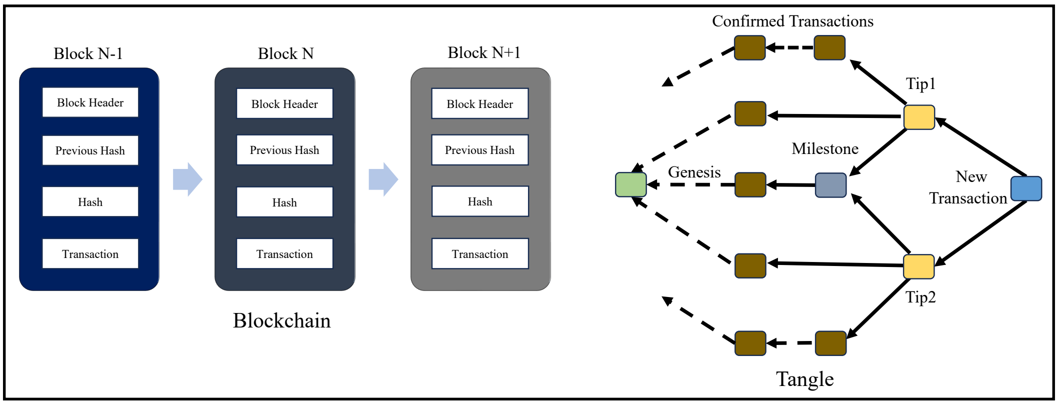


Figure 9. Blockchain vs Tangle

PoW, proof-of-stake (PoS), and proof-of-authentication (PoAh) are prominent consensus mechanisms. Each consensus mechanism has unique advantages and challenges that ensure a sustainable block validation process in the blockchain. Blockchain's prime working principles are confidentiality, integrity, and authenticity. All the advanced applications such as smart cities, healthcare, agriculture, and transportation have blockchain-assisted security solutions as they guarantee and provide integrity and immutability to data and facilitate decentralized access control. PoW consensus mechanism involves block validation which works based on solving a mathematical puzzle to obtain the hash value of a transaction. However, it has more computational and energy resource requirements. PoS includes a stake-based miner selection approach which works by selecting a miner with a large amount of stake. This approach can centralize the block validation to the nodes with a higher amount of stake. For hardware-assisted IoT-based applications, PoAh presents a device authentication mechanism that verifies the integrity of IoT devices to accept the data and validate transactions in IoT applications. Blockchain has been classified as public, private, and consortium based on the number of nodes in the network. Public blockchains have many nodes whereas private blockchains have a limited number of nodes. Public Blockchain has privacy issues since the copy of each transaction is shared globally among various stakeholders in the network. A consortium blockchain is a hybrid one that has features of both public and private blockchain.

EHR management is one of the most important applications of blockchain in healthcare. EHR stores the data, provides access only to authorized individuals, and can restrict unauthorized access. Private, public, and consortium Blockchain architectures achieve data confidentiality depending on the access control. Decentralized Ledger Technology (DeLT) is a database accessible to all trusted parties in the network to read and access the data. DLT, on the other hand, enables the trusted parties to upload and update the changes to data in the database.

7. PUFchain 3.0: Proposed Security-by-Design (SbD) approach for Smart Healthcare

In this section, we have briefly illustrated the architectural overview of the proposed SbD approach and its working in different phases in 7.1. The notations used for each of the components and their associated operations are given in Table 3.

7.1. Design and Analysis of Proposed Framework

The proposed work explores the scope of hardware-assisted distributed ledger and blockchain for robust security in H-CPS. The proposed framework uses blockchain's smart contracts, IOTA MAM, and PUF primitives for the security of devices and data in smart healthcare. In the proposed approach, the PUF-embedded smart sensors in the patient's health network or BAN could securely connect to the patient's gateway that is further connected to an edge for secure verification of PUF keys of IoMT devices. Once the verification is successful, the edge node initiates a MAM channel creation and uses the patient's gateway PUF key as the MAM channel side key for that hub. MAM is used to securely transfer data and upload data on Tangle. Therefore, each patient's physiological sensor data could be shared globally among various stakeholders in the H-CPS through a PUF-based integrity-checking scheme. Blockchain in the proposed framework works on storing each patient's PUF-generated device identities in a hub and can only be accessed by authorized stakeholders globally. This approach reduces the exposure of PUF keys of IoMT devices and reduces the need to store the PUF keys of all the devices inside a patient's hub. MAM can work on the patient's gateway key to securely access and upload data from these devices. Blockchain is operated by the stakeholders when a patient's sensor hub must be accessed, and the devices' integrity must be verified.

1. ***Patient's sensors and gateway's registration Phase:*** Initially, all the smart wearable and implantable medical devices are connected to a patient's gateway. These devices are connected to the gateway through various technologies like NFC, ZigBee, and BLE. All these devices have a PUF embedded key as their pseudo-identity. The gateway also has a unique PUF generated identity which acts as the address for this hub of devices. When the edge gateway receives an initiation request from the patient's gateway, it securely verifies the gateway's integrity by performing PUF key extraction and validation. Once the validation is successful, the Tangle transaction validation process starts. Initially, the edge gateway connects to a public IOTA node for securely interfacing with the IOTA tangle. IOTA node then creates a MAM channel to upload and share data. In the proposed approach, the MAM channel operates in the restricted mode which requires an authorization key for uploading and receiving data onto Tangle. The patient's gateway transaction is securely uploaded onto the channel. Uploaded transactions could be shared among various stakeholders who can only access in the restricted mode. The Procedural flow of transaction initiation, PUF key validation, and its metric evaluation process are illustrated in Fig. 10. Only after verifying the PUF's reliability, uniqueness, and randomness, the PUF module keys are assigned as pseudo identities to devices. The microcontroller connected to the client broadcasts the PUF Keys to the edge server (ES). Algorithms 1, 2 illustrate the working flow of the device registration phase in PUFchain 3.0.

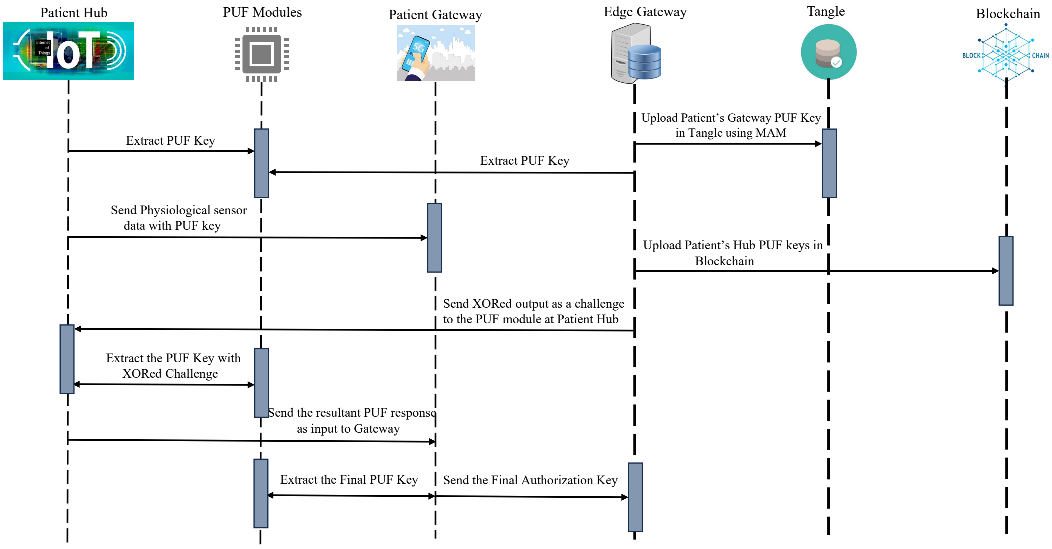


Figure 10. Procedural flow of PUFchain 3.0

Table 3. Notations.

Notation.	Description
P_{MID}	Pseudo Identity of IoMT Device
P_{ID}	PUF module at device
C_i	Challenge to IoMT device PUF
C_k	Challenge to gateway's PUF
R_i	Response to C_i
$IoMT_i$	Patient's hub
P_{MED}	Pseudo Identity of Patient Gateway
P_{ED}	PUF module at gateway
PUF_n	PUF Modules of all IoMT devices in Patient's hub
C_n	Random Challenges inputs
R_n	Response
C_i	Challenge input to IoMT Device $IoMT_i$ in hub
R_i	Extracted Response from PUF_I of $IoMT_i$ in the hub
R_p	Response output from Patient's gateway PUF module P_{ED}.
C_{XOR}	XORed output of R_i and R_p
r_{XOR}	Response output OF XORed Input
r_{OUT}	Final key from PUF module P_{ED}
$\oplus$	XOR
A_K	Side Key
R_K	Merkle root
H	SHA-256 Hash Function
H_D	hash value during Registration
H_A	Hash value during Authentication
A_M	fetched new transaction root

2. ***Patient's gateway access and control phase*** In MAM, while validating a transaction, a new root address is generated which is the subsequent transaction's hash. This is shared only with the intended recipient to successfully upload a new transaction. Using the side key, the new transaction's root is obtained by hashing the existing transaction's root with the side key [10,43,46]. Once the gateway's key is verified, its details are shared on the MAM channel by creating a transaction. The recipient can be either a server at a hospital, physician, or any other healthcare provider who

Algorithm 1: Enrolling Patient's Body Area Network Devices

Each IoMT device in the Patient's Body Area Network (BAN) has an embedded PUF module
// IoMT Device $\rightarrow$ PUF P_{ID}
Each PUF module is tested with random Challenge-Response Pairs (CRP's)
// $C_n \rightarrow PUF_{ID} \rightarrow R_n$
Perform PUF key extraction for an IoMT device P_{ID}
// $PUF_{ID} \rightarrow F(Ci) = Ri$
Evaluate Figure-of-Merits (FoM) of PUF module
Calculate Diffuseness, Uniqueness, Uniformity, and Reliability
if *FoM of* P_{ID} *are standard* **then**
    Assign R_i of P_{ID} as pseudo identity of IoMT device P_{ID}
    // $R_i \rightarrow P_{ID}$
    // Diffuseness is 50%, Reliability is 100%, Uniformity is 50%, and Uniqueness is 50%
The Patient's BAN consisting of several IoMT devices $IoMT_n$ connects to a gateway that securely stores the PUF keys of BAN in a secure database.
// $P_{MID} \rightarrow$ Patient Gateway (PG)
Patient's Gateway extracts a new PUF key from a PUF module
// $P_{ED} \rightarrow f(Ci) = P_{MED}$
Broadcast registration request to Edge gateway
// $P_{MED} \rightarrow$ EG

can access the channel to receive it only after their PUF pseudo-identity verification. Fig.11 and Algorithm 3 outline the validation and verification details. Now each administrative server at any hospital network around the world looking to access the patient's sensitive physiological data and access the IoMT devices on patients can securely connect to the patient's gateway hub from Tangle. A global blockchain in the cloud having all the patient's hub PUF keys can be accessed by the corresponding hospital network or healthcare provider to obtain the individual device's PUF key in a patient's BAN as explained in Fig. 12. The pseudo-PUF identities and challenges of all the devices are stored inside a blockchain and can be shared globally.

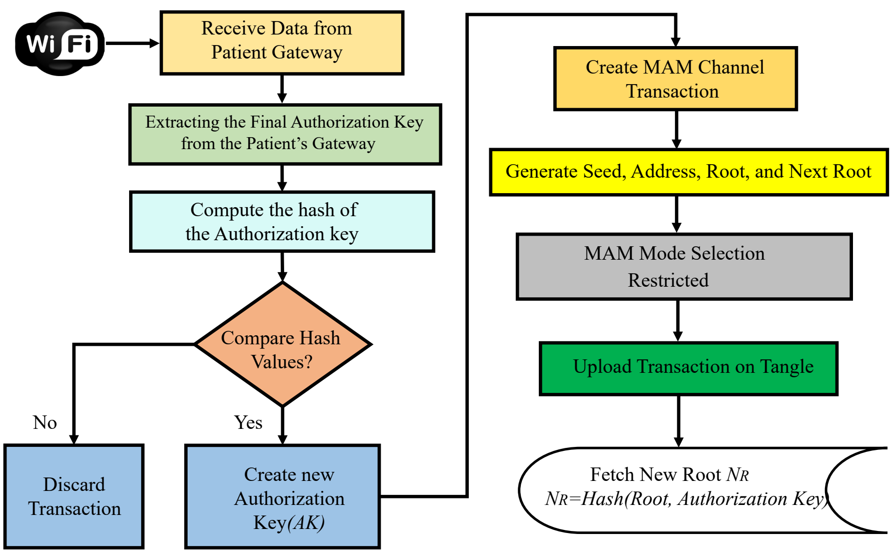


Figure 11. Procedural Flow of MAM channel creation and Transaction initiation

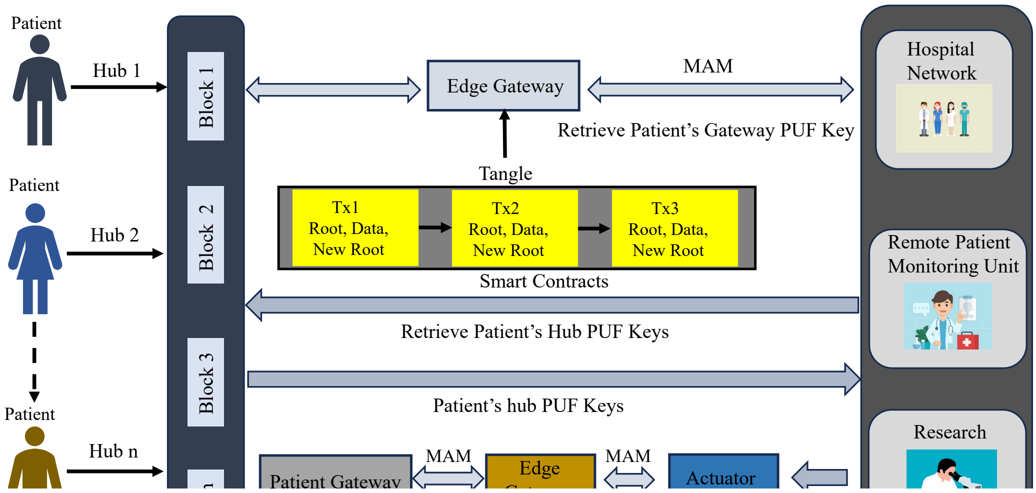
The Patient's gateway key is verified by the edge gateway which then initiates a new transaction on IOTA's MAM channel. After uploading the transaction, it is shared

Algorithm 2: Patient's gateway pseudo identity verification phase

Edge Gateway (EG) receives Pseudo Identity of PG
// Selects a challenge input from C_{IN} dataset
// $C_{IN} \rightarrow C_{IN2}$
// $P_{ED} \rightarrow$ EG
EG Performs XOR Operation of P_{MID} and P_{MED}
// $P_{XOR} \rightarrow P_{MID} \oplus P_{MED}$
ES sends XOR ed output as Challenge input to IoMT Device
// EG $\rightarrow C_{XOR} \rightarrow PUF_{ID}$
IoMT gives corresponding XOR ed value as challenge input to its associated PUF module
// $PUF_{ID} \rightarrow C_{XOR} \rightarrow r_{XOR}$
IoMT sends PUF key as input to EG.
// $r_{XOR} \rightarrow$ EG
Edge performs PUF key verification for the obtained inputs
// $r_{XOR} \rightarrow P_{ED} \rightarrow r_{OUT}$
if r_{OUT} *is reliable* **then**
  Assign r_{OUT} of P_{ED} as MAM channel Authorization keys
  Evaluate Metrics for all the devices in Patient's hub $IoMT_i$ // Diffuseness is 50%, Reliability is 100%, Uniformity is 50%, and Uniqueness is 50%

on the channel and the intended receiver can access the data in restricted mode. The working and procedural flow of the uploading transaction on MAM channel creation and its validation inside a node in proposed PUFchain 3.0 is presented in Fig. 13.

Step 1: IoMT device's integrity is verified by performing PUF key extraction from a set of challenges on the device's PUFs.
Step 2: Challenge inputs (C_i, C_k) are tested on the PUF modules at both gateway's and device's PUF modules in the hub.
Step 4: Obtained keys are evaluated by checking reliability, randomness, hamming distance, and other metrics.
Step 3: XOR operation is performed on the obtained PUF keys (P_{MID}, P_{MED}). The XOR output C_{XOR} is sent as challenge input to PUF at IoMT.
Step 4: The obtained r_{XOR} key is again tested as input to the PUF module at the gateway.
Step 5: Finally obtained key from the gateway is hashed and compared during the verification process by following all the above steps. The obtained final key r_{OUT} is hashed. Obtained hash value H_A is compared with the initially obtained hash H_D during registration.
Step 6: Once the device authentication is considered successful by the Edge gateway, it then creates a MAM channel to upload the transaction, fetch the address, and broadcast it to the authenticated client to upload its data.
Step 7: The working mode of MAM is chosen as restricted mode (2). An authorization or side key A_K is defined to access the channel in restricted mode.
Step 8: The authorization key A_K for the MAM channel in the proposed security protocol is the patient's gateway pseudo identity r_{OUT} which is required to store, share, and access data on IOTA tangle
Step 9: Once the new root is fetched, an access link is obtained and broadcasted to all the working nodes in H-CPS to access the transaction data from Tangle.
Step 10: Finally, the root of the transaction R_K and A_K of the MAM channel are hashed to fetch the address (A_M) of the new transaction. The new side key is r_{OUT} of the patient's BAN gateway.



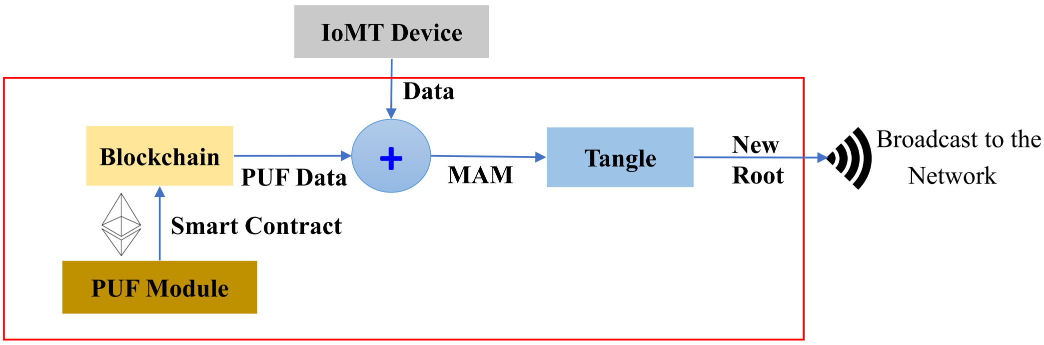


Figure 13. Working flow of PUFchain 3.0

7.2. Assumptions

The proposed experimental validation is based on the following assumption.

- All the IoMT devices have embedded PUF.
- A secure network communication exists between the IoMT node, patient's, and edge gateway during the enrollment and verification process.
- All the IoMT devices have a secure interface with the Patient's gateway using BLE, ZigBee, or other technologies.
- Edge gateway has a running blockchain instance locally.

8. Experimental Results

For experimental evaluation, All smart health devices inside the patient's BAN are interfaced with the patient's gateway and all the data processing can be done at the edge gateway. Two FPGA boards have been used for PUF module deployment on the patient and edge gateway side. The patient's gateway has an Arbiter PUF generated key and the edge has an XOR PUF Key as unique identities. Arbiter PUF can generate many keys for patients' BAN smart health devices. The proposed methodology has been written in

Algorithm 3: MAM channel and Blockchain validation phase

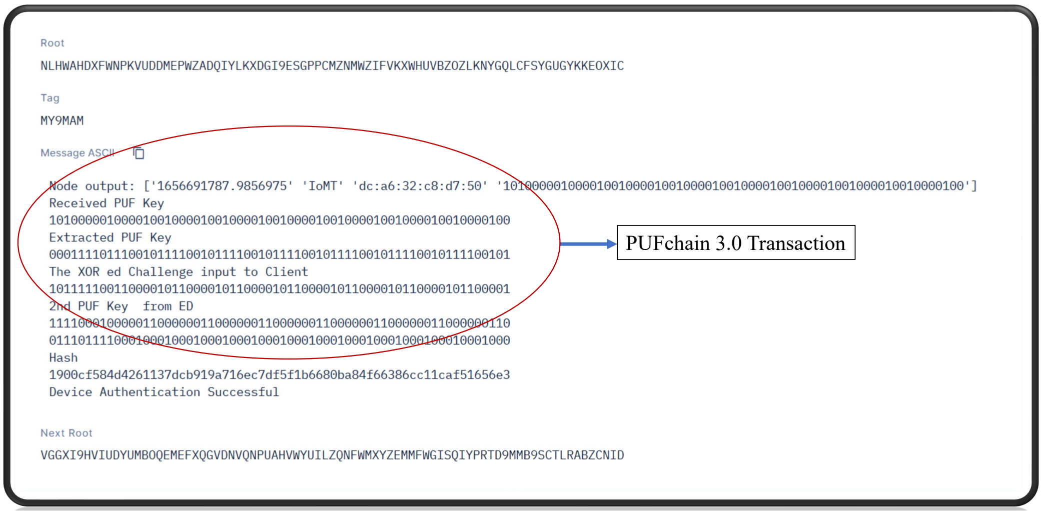
EG initiates MAM channel
Assign authorization key
// MAM Channel$\rightarrow A_K$
// MAM Mode $\rightarrow$Restricted(2), Public(0) ,private(1)
Choose Restricted Mode (2)
Upload Pseudo Identity of Patinet's hub and Patient's gateway. // P_{MID} $\rightarrow$ Streams v0 (Channel)
Choose Patient's gateway key as the channel side key
// $P_{MED} \rightarrow A_K$
Fetch Next root
// MAM Channel $\rightarrow$New Root(N_R)
Perform hash on side key and root
// A_M $\rightarrow$H(A_K,R_K)
Broadcast New fetched root and new side key A_M
// --------EG initiates Blockchain transaction-------
EG initiates a smart contract with different roles: Doctor, Patient
EG uplaods the patient's hub PUF data set
// -----$IoMT_n$-----
// $IoMT_{i1}$ $\rightarrow$H(C_{i1},R_{i1})
// $IoMT_{i2}$ $\rightarrow$H(C_{i2},R_{i2})
// $IoMT_{i3}$ $\rightarrow$H(C_{i3},R_{i3})
// |
// |
// $IoMT_{in}$ $\rightarrow$H(C_{in},R_{in})
Deploy Smart contract
Obtain Mined and Validated Block
Broadcast Validated Block globally to various stakeholders

JavaScript to publish and fetch transactions on Tangle. We have used the Chrysalis public IOTA node to access and upload transactions on the MAM channel. MAM channel in "restricted mode" has been considered for the proposed approach to ensure higher security. The whole methodology is evaluated on IOTA's Main net on Streams v0 Channel [47,48]. The hardware and software specifications of the experimental validation in this work are given in Table 4. The time taken to upload a transaction on Tangle will be the total time to generate *Tip* , validate the transaction using PoW, generate a MAM channel and corresponding transaction metrics - *seed, address, root*. Our experimental evaluation has shown that the overall time to perform transaction validation in the proposed work is comparatively faster than that of block addition in PoW, which is approximately 10 minutes [19]. The transaction evaluation and validation results are presented in Fig. 14.

A Ganache local test net blockchain is set up and connected to a MetaMask account for gas cost estimation and analysis. A smart contract has been deployed to securely store the generated PUF Challenge Response Pair (CRP) dataset inside the blockchain. Ganache Blockchain was configured on an Intel i7 2.8 GHz processor with 16 GB RAM. Xilinx FPGAs have been used for evaluating the Arbiter and XOR PUF modules for PUF key extraction as shown in Fig. 15. The FPGA boards used for evaluation are Xilinx Artix-7 Basys 3 (xc7a35tcpg236-1). Xilinx Vivado has been used to test the PUF design and the PUF logic has been programmed onto the FPGA board at a baud rate of 9600 bits using a Universal asynchronous receiver and transmitter (UART). 64-bit instances of Arbiter and XOR PUF elements have been generated to create 64-bit PUF keys for each one of the modules. Table 5 presents the Arbiter and XOR PUF evaluation results.

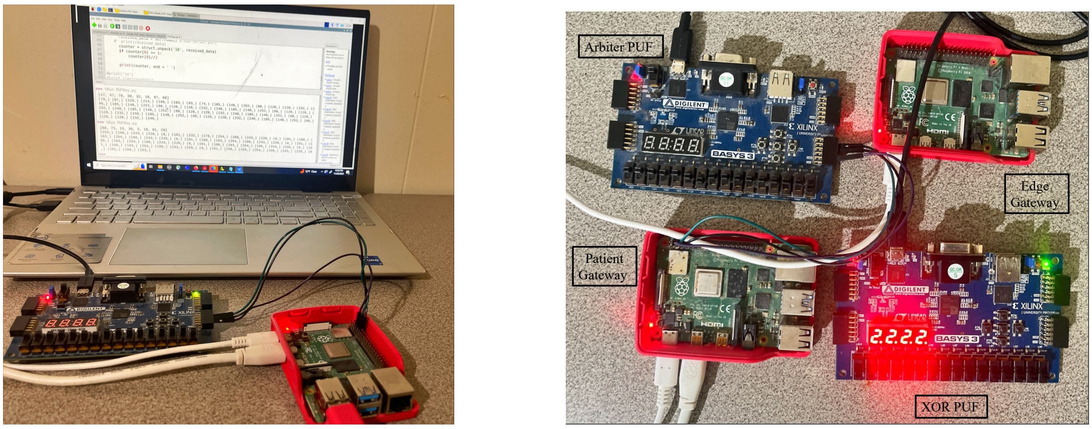
(a) Validating PUF key and creating MAM channel

(b) PUF Based MAM channel Access Authorization Policy



(c) Fetching Transaction from IOTA Explorer

Figure 14. IOTA Tangle Transaction Validation



(a) Extracting PUF Keys **(b)** Prototype

Figure 15. PUFchain 3.0 Experimental Setup

Single board computers have been used as edge nodes for distributed data processing from the IoMT devices. Raspberry Pi 4 2.0 GB boards have been used as edge and patient's gateway in the proposed system. These devices act as local nodes to perform device integrity verification and for creating MAM channel and uploading transactions on Tangle. Edge Gateway's power consumption has been evaluated using an energy meter which showed power consumption in the range of (2.7- 3.4) watts which is approximately the average consumption range of a pi. The PUF keys of each of the devices are initially verified before creating a new MAM channel and uploading the transaction onto Tangle.

Table 4. System Specifications

Parameters	**Results**
Application	Smart Healthcare
DLT	IOTA Tangle and Blockchain
PUF Module	Arbiter & XOR PUF
Programming	JavaScript, Verilog, Python, Solidity
IOTA Network	Main net
Tangle Communication Protocol	MAM
IOTA Node	Chrysalis
Working Mode	Restricted
MAM channel	streams v0
FPGA	Artix-7, Basys-3 (xc7a35tcpg236-1)
Block Validation	Solidity 0.8.18
Blockchain network	Ganache

Table 5. PUF Evaluation results

PUF Metrics	**Results**
PUF Key Extraction time	78 ms
XOR PUF Reliability	99.72%
Overall Hamming Distance of XOR PUF	48.66%
Overall Hamming Distance of Arbiter PUF	48.53%
Arbiter PUF Reliability	99.73%
Number of PUF keys	1000
Number of Instances	64
Total On-Chip Power	0.081 Watts
Device Authentication Time	3.66 s

The overall intra hamming distance of PUF keys from Arbiter and XOR PUF modules has been approximately 50%. The metrics of PUF modules are presented in Figs. 16 and

17. Reliability was approximately 100% when the two PUF modules were tested with 1000 PUF keys four times at different instances of time and at varying temperatures.

8.1. Why Restricted mode of MAM for PUFchain 3.0?

MAM as introduced in section 5, works in Public, Private, and restricted modes. However, the proposed approach works on MAM in the restricted mode. This is due to the requirement for device and data integrity from smart electronic devices. Restricted mode ensures the utmost level of security and works by generating a transaction address by hashing the hash of the root and an authorization side key. This work aims to leverage this property by using the PUF key of a device as its authorization key to access the channel and upload data to Tangle. In the proposed solution, doctors and medical professionals can access the channel securely and obtain access to the data from Tangle. This can ensure the integrity and authenticity of data as the data can only be uploaded onto Tangle after successfully validating the PUF keys of respective Medtronic devices.

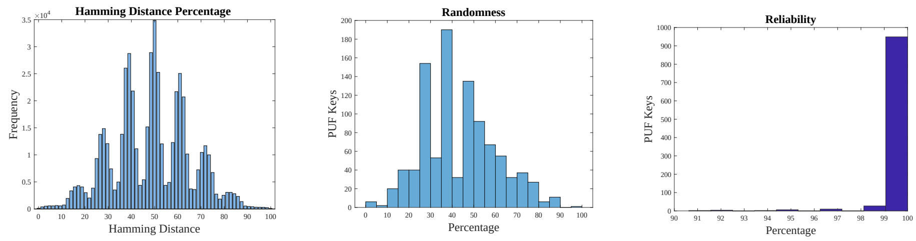


Figure 16. Arbiter PUF Metrics

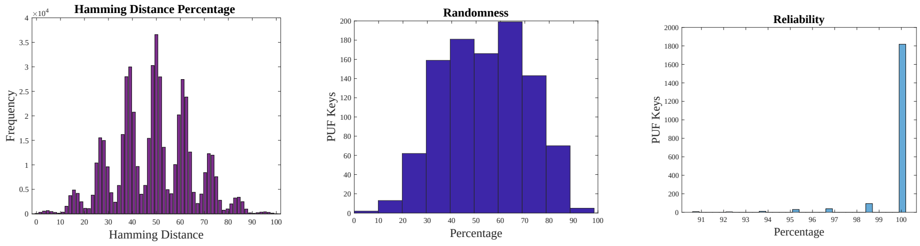


Figure 17. XOR PUF Metrics

The overall time to perform device authentication in PUFchain 3.0 is between 2.7 and 3.6 seconds. Once the device authentication is done, the average time to upload the transaction onto Tangle Main net has been 28 seconds, while the meantime to fetch the transaction has been approximately 1-2 seconds. The tabulated results of PUFchain 3.0 are given in Table 6. The transaction upload time includes the time taken to perform seed, address, root, and other Tangle transaction metrics. Also, it includes the waiting time for the IOTA public node to attach the transaction to Tangle and the time taken to perform PoW to validate unconfirmed transactions on Tangle.

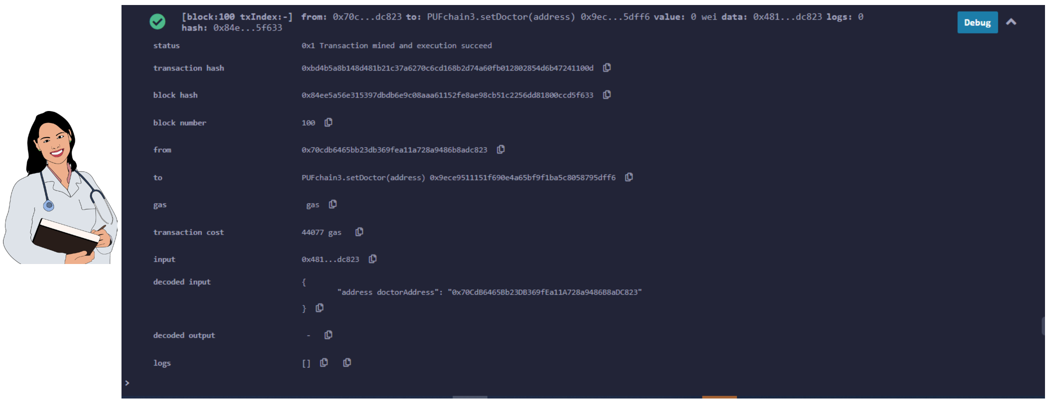
Table 6. Tangle Transaction Evaluation Results: Analysis of 10 Sample Transactions

Message ID	Attachment Time (s)	Fetch Time (s)	Root
9d9646d0d0536ee 9aede181660ab799 247b58548fe09 107e421643ae3c2581b3	13.8	1.38	KJAMAHXDTWOSOJAJ99UMX XRBBKHHUD NDHJVLTBNRQD UFSRQEQZDNYKTS BNGKUTUPYXYC STXLLZXSDP9KR
f2a2766970d6044 705af5d14fce0f5e0 e844b6a460bd 1960caf82148c0aa3600	26.6	1.66	HEXQBCPQSZYYJQXUMB UYKHRSNUOJNUU CPZFNAJLZDSZEUUAE RLLSPLKTBPVEHHECU TKDETPPXKXVYTXAG
2ac926abc3eeb3 11eaf8356945358b ced6e3836ef7e43d 84f517d756a551970d	23.0	1.33	ZCEOYFYQB MFXMAWMDHTUZ ZNJMJGA SEVBGBMOU LNHKSWZ OCAER9 KGXOEECLDWRJM CJJEVGRBAAYKINTSTM
daee1db6f01b59 4f07efaf1e04e 012e01fd ce53e714a83a 0414abb5256064ca5	22.5	1.67	E9ESRZ9B SXIXON9URUACLVJ BLHHNKUFGRI9D9 BQJUCAKWI9YQVTVT DAQCIWLQPSMXWUNCT QPTSBIUVUYF
152518578c56268af d2380bcedd64a 37379b7e200d20a dbbab9c71866567eee1	36.1	1.90	GNUJKSBQOGW JZTLXDHDSUFAFVTWH POQXXL9AVOAYZ VVU9YP LRSAKWNGTQ9W TGEURIP STYBOJLMCXGBTIW
b4c291bbc8b867d 7b912ab9a2cad 3e6d8bb8b 15fa022b3 db7cb14cf88f8c9775	20.5	1.52	OBSFYFONDRKIXRDWWB9T BQZYOMVOYK USLGAXYBS9VD MTMNZCXYYOVQX UU9OWUHWR DRHLHMRU KNHPTBMEH
3877bf6821b5df c36823ce a6eee1a e23b5b61 73c4e080 0dbd58 26516b8 5bbca8	2.16	1.61	GXNHDCAVIAUAIDPESPJ BBBYLH9PSIK9FJHMG ALYLAJAQUP ZOV9KIBNFXMBX HJAASZ ZATLE UQQGHEYO9IV
bee8195b378 2a51443 afb2087d91 eb5743 e31dcdb15f42 32d6ac8e932d 7d3513	7.80	1.51	SKGKMHKG9ZNIN JOXMDIONLULRFBZOQFDLQ TAIKUAOIQNMNQT DSYVS9SZKDTAB CYRVVOEARA9UWDFWVPBE
dde4579afe5 e10bb6a7 a5e0fb8b461 f62d752023e 38769f001f6 e7e5ea95e3a1	13.0	1.44	9GIY9J9UDCN CSYUKZKXBRSJQDZBIU9G HOBGNEBBHQ EPSZYKNCH9LSOBID9 BLPW9TSTNDLHWX JAXNVVASE
0dc5cfe486b1 ce772d8459b a5f95bd2836 2d8b69cfa 843fc4fc 47caa7d39c3a7	11.6	1.77	OMOTIFWLJ9DNRJ QBCGBIBMEMAMYKL FKCFMZOLSC C9WOWVWEO ICYFQDIY9UW HEIADXGMFATZU NJRLCTITK

8.2. Block Creation and Validation

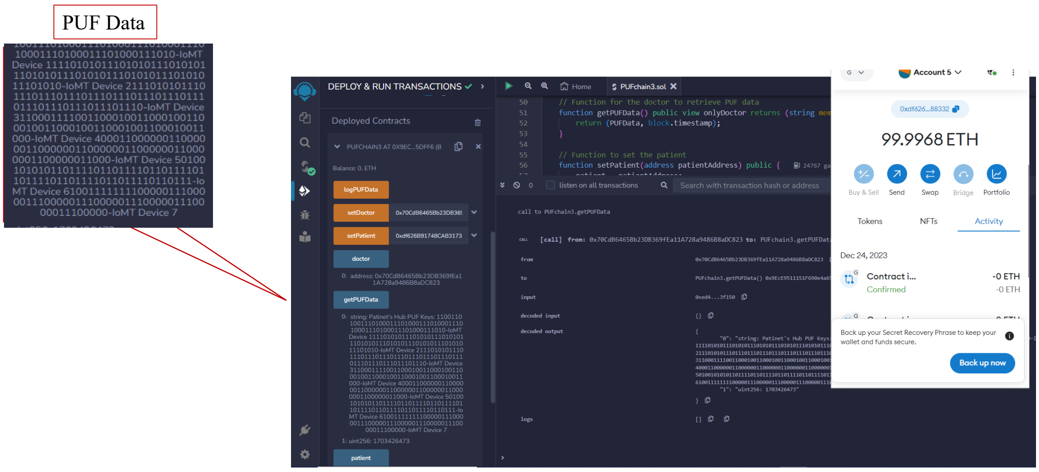
A smart contract has been deployed on Remix Ethereum IDE connected to a MetaMask wallet. Ganache blockchain running on a local host is connected to MetaMask and one of the ten accounts has been selected and connected to MetaMask wallet. A simple smart contract to store the Patient's PUF data set consisting of PUF keys has been executed and deployed onto the Ganache test network [49]. The Block creation, hashing, and transaction validation results have been presented in Fig. 18, and 19. Our prototype system worked on the local Ganache test net using network ID 5777 and smart contract address "0xe5f1c9A3cAD43bDa1E74 5d83799fB7AE59bE77b6". Two accounts have been assigned, one for healthcare professionals with contract address "0x70CdB6465Bb23D B369 fEa11A728a9486B8aDC823", and one for patient using the address "0xdf626B91748C AB3173 128a6F5cc 589C8Af18 8332". "logPUFData" function is initiated from the patient's side which securely logs the PUF keys of IoMT devices. The doctor or health professional initiates the "PUFData" function to securely retrieve the PUF keys of IoMT in the patient's BAN. Smart contract validation results of the proposed framework are given in Table. 7.

(a) Assigning Patient's Role and Logging PUF Data

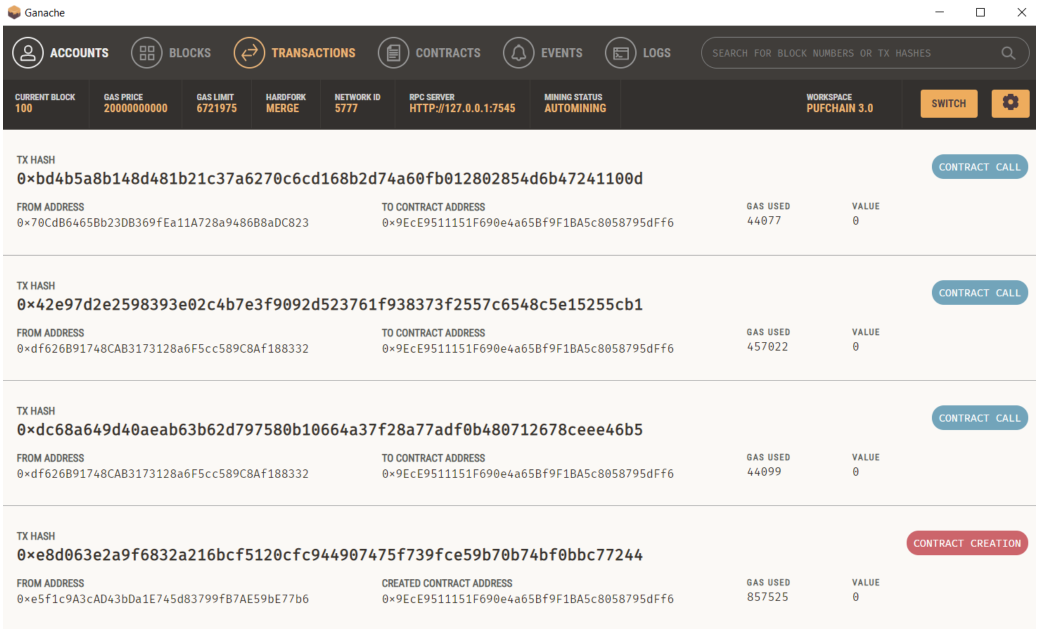


(b) Assigning Doctor's Role and Retrieving PUF Keys of Patient's BAN

Figure 18. Smart Contract Deployment and Role Assignment



(a) Transaction details of PUFchain 3.0 on Remix IDE



(b) Validated PUFchain 3.0 transactions on Ganache

Figure 19. Formal Verification of PUFchain 3.0

Table 7. Smart Contract Deployment Details

Smart contract lifecycle	Transaction Hash	Block hash	Gas Fees
Contract deployment	0xe8d063e2a9f6 832a 216bcf5120c fc944907475f739f ce 59b70b74bf0bbc77244	0x78d0ef9a76714407c3 1d777b40f8ce0da579ba9181 729cb753b9fe19d26ce73f	0.02600838 ETH
Patient's account initiation	0xdc68a649d40aeab63b6 2d797580b10664a37f2 8a77adf0b480712678ceee46b5	0x7488a604b74b7d9e7 404fac9705108c6ae25f530 d3f39aee97b93cdc2acec58f	0.00132949 ETH
PUF data storage	0x42e97d2e2598393e02c4b7 e3f9092d523761f938373 f2557c6548c5e15255cb1	0x0dc657518aaee3fc0fc 4f78691aee2b0c1229 48cd56ba 63b262937a529e49cd9	0.01637317 ETH
Doctor's account validation	0xbd4b5a8b148d481b21c 37a6270c6cd168b2d74a60 fb012802854d6b47241100d	0x84ee5a56e315397dbdb6e 9c08aaa61152fe8ae98 cb51c2256dd81800ccd5f633	0.00169751 ETH

9. Discussion and Conclusion

9.1. Principal Findings

This work explored the potential of hardware assisted distributed ledger technology-based security solutions in smart healthcare. We proposed a cybersecurity solution for H-CPS by integrating PUF, IOTA Tangle, and Blockchain. Tangle, being a distributed lightweight ledger offers great potential in smart healthcare as it is miner-less, fee less primitive while offering robust security as Blockchain. We experimentally demonstrated a security solution that uses Blockchain for securely storing the PUF keys of each of the IoMT devices in a patient's BAN. The patient's gateway having a unique pseudo identity from the PUF can communicate on MAM for sharing physiological sensor data globally.

This work demonstrated and evaluated two PUF modules: Arbiter and machine learning attack resistant XOR Arbiter PUF. 1000 PUF keys were extracted from these PUFs for 5 instances showing promising results with reliability of approximately 100%. Our analysis of related works shows that most of these works don't focus on PUF metrics and hardware assisted access control to the distributed ledger. Our work presents a hardware secure access control policy to DLT with effective evaluation of PUF metrics to facilitate attack resistant security framework. Table. 8 illustrates the comparative analysis of this work with related works.

Table 8. Security Analysis of PUFchain 3.0 in Comparison with Related Works

Research Works	System	Security Primitives	Hardware Assisted	Scalable	Hardware Efficient	Computationally Efficient
Wang et al. 2022 [30]	PUF and Fuzzy extractor enabled Blockchain	3	Yes	Yes	No	Yes
Chaudhary et al. 2021 [22]	PUF based Smart Contracts	2	Yes	Yes	No	Yes
Satra et al. 2023 [14]	ML assisted PUF	1	Yes	No	Yes	-
Al-Joboury et al. 2021 [23]	DAG-Blockchain	2	No	Yes	-	No
Fotopoulos et al. 2020 [28]	Blockchain assisted SSI	1	No	Yes	-	No
Zheng et. al 2023 [9]	IOTA MAM	1	No	Yes	-	Yes
PUFchain 3.0 [20]	Blockchain enabled PUF for Tangle's MAM	3	Yes	Yes	Yes	Yes

Our analysis further proves that even though Tangle MAM has been proposed in various works, it has not been integrated with hardware primitives as a comprehensive cybersecurity solution. To the best of our knowledge, this is the first novel integration of PUF, Blockchain, and Tangle for simultaneous device and data security in smart healthcare or other areas in IoT-based applications.

Our security analysis shows that eavesdroppers cannot intercept the communication and PUF keys of the patient's gateway shared on the MAM channel since the restricted mode channel ensures secure access using the patient's gateway PUF key. Also, consecutive transactions can be uploaded onto the channel only by sharing the obtained new root address and channel side key with the trusted authorized entities in the system. As a result, the proposed approach can withstand eavesdropping attacks. Additionally, our analysis shows that the message attachment times in restricted MAM mode are comparatively faster in this work as compared to [9] even though the public IOTA node's processing time may vary subject to network traffic. Also, in this work, PUF keys of IoMT inside BAN are not shared on the MAM channel but are securely stored in Blockchain which can be accessed by authorized entities through smart contracts thereby reducing the exposure of smart health devices' unique PUF-generated identities. Furthermore, the Arbiter and XOR PUF modules have shown better randomness and reliability in this work as compared to hybrid oscillator arbiter PUF in [19]. Achieving approximately 100% reliability substantiates the potential of PUF-based security for IoMT devices.

9.2. Limitations and Challenges

Using public IOTA nodes for validation, publishing, and fetching data on Tangle could delay and increase transaction validation and publishing times. Using smart contract-based validation can increase energy consumption and require computational resources. Other challenges also exist with the integration of PUF, Tangle, and Blockchain such as latency in transaction validation, network security issues, and blockchain smart contract validation cost or gas fees. Even though our approach works on the Ganache test net Blockchain, the actual deployment on the main net could incur gas costs. For the deployment of transactions on Tangle, MAM has been updated to a new protocol called IOTA streams [50] which is still under the development stage. Furthermore, integrating PUF for hardware security is a challenging process as the reliability of PUF can be impacted due to the aging of the device and its response to environmental factors. Also, various tradeoffs involved in the performance of PUF-embedded devices must be considered such as energy consumption, area, and speed while deploying PUF on smart health devices.

9.3. Conclusion & Future Research Directions

Hardware-assisted security solutions using blockchain, and distributed ledger have great potential for cybersecurity in smart healthcare. Privacy and integrity of patients' sensitive medical data are pivotal in the rapidly evolving remote healthcare monitoring systems facilitated through IoMT devices. Integrating a decentralized hardware-software SbD approach which emphasizes integrating security based on the design of an electronic system in H-CPS is the motivation for this work. The proposed work successfully integrates PUF, Blockchain, and IOTA Tangle as a scalable decentralized security primitive that provides sustainable and simultaneous security in H-CPS. The proposed architecture aims to leverage the scope of Blockchain technology to store the patient's BAN PUF keys to avoid the possibility of exposure and adversarial access to these keys. Using Tangle in this work securely facilitates identity-driven access control and data sharing among various stakeholders in H-CPS for processing patients' critical health data in real time. Furthermore, PUF enhances and focuses on security at the end device in the BAN hub. The possible integration of these three could further facilitate a secure interface between doctor and patient in advanced remote healthcare monitoring systems like telemedicine and e-health.

This work could be extended for sustainable security in autonomous vehicles by embedding PUF inside electronic control units and has a blockchain supported functionality for data security as well. The proposed work PUFchain 3.0 could be extended further to other areas of IoT-based applications, particularly in the areas of supply chain management and product tracking in electronics. This includes attaching a PUF-generated cryptographic identity to each product in the supply chain and tracking its movement securely using blockchain. Integration of these primitives for IC supply chain management and Industry 4.0 can also be a direction for future research.

Author Contributions: Conceptualization, Saraju P. Mohanty; Investigation, Venkata K. V. V. Bathalapalli; Writing – original draft, Venkata K. V. V. Bathalapalli; Writing – review

& editing, Saraju P. Mohanty and Elias Kougianos; Supervision, Elias Kougianos; Funding acquisition, Vasanth Iyer and Bibhudutta Rout.

Acknowledgements: A preliminary version of this work has been presented at the following conference paper [20].

This material is based upon work supported by the National Science Foundation under Grant number HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

1. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. *IEEE Consumer Electronics Magazine* **2018**, *7*, 18–28. https://doi.org/10.1109/mce.2017.2755378.
2. Sun, J.; Khan, F.; Li, J.; Alshehri, M.D.; Alturki, R.; Wedyan, M. Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things. *IEEE Internet of Things Journal* **2021**, *8*, 15663–15671. https://doi.org/10.1109/jiot.2021.3078702.
3. R, M.; K, G.; Rao, V.V. Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. In Proceedings of the Proc. IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), April 2021. https://doi.org/10.1109/iemtronics52119.2021.9422615.
4. Jia, X.; Luo, M.; Wang, H.; Shen, J.; He, D. A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things. *IEEE Internet of Things Journal* **2022**, *9*, 21838–21850. https://doi.org/10.1109/JIOT.2022.3181609.
5. 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* **2021**, *8*, 8707–8718. https://doi.org/10.1109/jiot.2020.3045653.
6. Mohd Aman, A.H.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *Journal of Network and Computer Applications* **2021**, *174*, 102886. https://doi.org/10.1016/j.jnca.2020.102886.
7. Jayaraman, I.; Shankar, A.; Ghalib, D.M.; Jayaraman, G.; Hua, Q.; Wen, Z.; Qi, X. Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U 6 HCS). *IEEE Access* **2020**, *8*, 216856–216872. https://doi.org/10.1109/ACCESS.2020.3040240.
8. Wazid, M.; Singh, J.; Das, A.K.; Shetty, S.; Khan, M.K.; Rodrigues, J.J.P.C. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. *IEEE Access* **2022**, *10*, 57990–58004. https://doi.org/10.1109/ACCESS.2022.3179418.
9. 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* **2019**, *21*, e13583. https://doi.org/10.2196/13583.
10. 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* **2022**. https://doi.org/10.1007/s40747-021-00610-8.
11. 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* **2022**, *3*. https://doi.org/10.1007/s42979-022-01238-2.
12. 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**, *2022*, 1–18. https://doi.org/10.1155/2022/6735003.
13. Amintoosi, H.; Nikooghadam, M.; Shojafar, M.; Kumari, S.; Alazab, M. Slight: A lightweight authentication scheme for smart healthcare services. *Computers and Electrical Engineering* **2022**, *99*, 107803. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107803.
14. Satra, S.; Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Octopus: A Novel Approach for Health Data Masking and Retrieving Using Physical Unclonable Functions and Machine Learning. *Sensors* **2023**, *23*, 4082. https://doi.org/10.3390/s23084082.
15. Dey, K.; Kule, M.; Rahaman, H. PUF Based Hardware Security: A Review. In Proceedings of the Proc. International Symposium on Devices, Circuits and Systems (ISDCS), 2021, pp. 1–6. https://doi.org/10.1109/ISDCS52006.2021.9397896.
16. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review* **2021**, *39*. https://doi.org/10.1080/02564602.2021.1927863.
17. Hori, Y.; Yoshida, T.; Katashita, T.; Satoh, A. Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs. In Proceedings of the Proc. International Conference on Reconfigurable Computing and FPGAs, USA, 2010; RECONFIG '10, p. 298–303. https://doi.org/10.1109/ReConFig.2010.24.
18. Lee, Y.S.; Lee, H.J.; Alasaarela, E. Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF). In Proceedings of the Proc. 9th International Wireless Communications and Mobile Computing Conference (IWCMC), 2013, pp. 1314–1318. https://doi.org/10.1109/IWCMC.2013.6583746.

19. 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.
20. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Kougianos, E.; Baniya, B.K.; Rout, B. 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, 2022; pp. 23–40. https://doi.org/10.1007/978-3-031-18872-5_2.
21. Hellani, H.; Sliman, L.; Samhat, A.E.; Exposito, E. Tangle the Blockchain:Towards Connecting Blockchain and DAG. In Proceedings of the Proc. 30th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2021, pp. 63–68. https://doi.org/10.1109/WETICE53228.2021.00023.
22. Chaudhary, C.K.; Chatterjee, U.; Mukhopadhayay, D. Auto-PUFChain: An Automated Interaction Tool for PUFs and Blockchain in Electronic Supply Chain. In Proceedings of the Proc. Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 2021, pp. 1–4. https://doi.org/10.1109/AsianHOST53231.2021.9699720.
23. 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 Proceedings of the Proc. International Symposium on Networks, Computers and Communications (ISNCC), 2021, pp. 1–6. https://doi.org/10.1109/ISNCC52172.2021.9615865.
24. Akbulut, S.; Semantha, F.H.; Azam, S.; Pilares, I.C.A.; Jonkman, M.; Yeo, K.C.; Shanmugam, B. Designing a Private and Secure Personal Health Records Access Management System: A Solution Based on IOTA Distributed Ledger Technology. *Sensors* **2023**, *23*, 5174. https://doi.org/10.3390/s23115174.
25. Wazid, M.; Gope, P. BACKM-EHA: A Novel Blockchain-enabled Security Solution for IoMT-based E-healthcare Applications. *ACM Transactions on Internet Technology* **2023**, *23*, 1–28. https://doi.org/10.1145/3511898.
26. Tomar, A.; Gupta, N.; Rani, D.; Tripathi, S. Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet of Things* **2023**, *23*, 100849. https://doi.org/10.1016/j.iot.2023.100849.
27. Vinko, D.; Miličević, K.; Lukić, I.; Köhler, M. Microcontroller-Based PUF for Identity Authentication and Tamper Resistance of Blockchain-Compliant IoT Devices. *Sensors* **2023**, *23*, 6769. https://doi.org/10.3390/s23156769.
28. Fotopoulos, F.; Malamas, V.; Dasaklis, T.K.; Kotzanikolaou, P.; Douligeris, C. A Blockchain-enabled Architecture for IoMT Device Authentication. In Proceedings of the Proc. IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE). IEEE, October 2020. https://doi.org/10.1109/ecice50847.2020.9301913.
29. Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE Journal of Biomedical and Health Informatics* **2023**, *27*, 710–721. https://doi.org/10.1109/jbhi.2022.3187037.
30. 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* **2022**, *9*, 8883–8891. https://doi.org/10.1109/JIOT.2021.3117762.
31. Pescador, F.; Mohanty, S.P. Guest Editorial Security-by-Design for Electronic Systems. *IEEE Transactions on Consumer Electronics* **2022**, *68*, 2–4. https://doi.org/10.1109/TCE.2022.3147005.
32. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Kougianos, E.; Iyer, V.; Rout, B. iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics. In Proceedings of the 2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, June 2023, pp. 1–6. https://doi.org/10.1109/isvlsi59464.2023.10238586.
33. Anandakumar, N.N.; Hashmi, M.S.; Chaudhary, M.A. Implementation of Efficient XOR Arbiter PUF on FPGA With Enhanced Uniqueness and Security. *IEEE Access* **2022**, *10*, 129832–129842. https://doi.org/10.1109/access.2022.3228635.
34. Liu, J.; Zhao, Y.; Zhu, Y.; Chan, C.H.; Martins, R.P. A Weak PUF-Assisted Strong PUF With Inherent Immunity to Modeling Attacks and Ultra-Low BER. *IEEE Transactions on Circuits and Systems I: Regular Papers* **2022**, *69*, 4898–4907. https://doi.org/10.1109/tcsi.2022.3206214.
35. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things From Blockchain to IOTA: A Survey. *IEEE Access* **2022**, *10*, 844–866. https://doi.org/10.1109/ACCESS.2021.3138353.
36. Rydningen, E.S.; Åsberg, E.; Jaccheri, L.; Li, J. Advantages and opportunities of the IOTA tangle for health data management. In Proceedings of the Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for Blockchain. ACM, May 2022. https://doi.org/10.1145/3528226.3528376.
37. Chen, Y.; Wang, Y.; Sun, B.; Liu, J. Addressing the Transaction Validation Issue in IOTA Tangle: A Tip Selection Algorithm Based on Time Division. *Mathematics* **2023**, *11*, 4116. https://doi.org/10.3390/math11194116.
38. Shabandri, B.; Maheshwari, P. Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. In Proceedings of the Proc. 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 1069–1075. https://doi.org/10.1109/SPIN.2019.8711591.
39. Pinjala, S.K.; Sivalingam, K.M. DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things. In Proceedings of the Proc. IEEE 5th World Forum on Internet of Things (WF-IoT), April 2019. https://doi.org/10.1109/wf-iot.2019.8767356.
40. Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. Characterizing IOTA Tangle with Empirical Data. In Proceedings of the Proc. IEEE Global Communications Conference GLOBECOM, December 2020, pp. 1–6. https://doi.org/10.1109/globecom42002.2020.9322220.
41. Rawat, A.; Daza, V.; Signorini, M. Offline Scaling of IoT Devices in IOTA Blockchain. *Sensors* **2022**, *22*, 1411. https://doi.org/10.3390/s22041411.

42. 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* **2021**, *13*, 312. https://doi.org/10.3390/fi13120312.
43. Carelli, A.; Palmieri, A.; Vilei, A.; Castanier, F.; Vesco, A. Enabling Secure Data Exchange through the IOTA Tangle for IoT Constrained Devices. *Sensors* **2022**, *22*, 1384. https://doi.org/10.3390/s22041384.
44. Lamtzidis, O.; Gialelis, J. An IOTA Based Distributed Sensor Node System. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1–6. https://doi.org/10.1109/glocomw.2018.8644153.
45. Mallick, S.R.; Goswami, V.; Lenka, R.K.; Sahoo, T.R.; Kumar, V.; Barik, R.K. Blockchain-based IoMT for an intelligent healthcare system using a drop-offs queue. In Proceedings of the First International Conference on Microwave, Antenna and Communication (MAC). IEEE, 2023, pp. 1–6. https://doi.org/10.1109/mac58191.2023.10176337.
46. Bhandary, M.; Parmar, M.; Ambawade, D. A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. In Proceedings of the Proc. 5th International Conference on Communication and Electronics Systems (ICCES), June 2020, pp. 827–832. https://doi.org/10.1109/icces48766.2020.9137858.
47. IOTA Foundation. iotaledger/mam.js. https://github.com/iotaledger/mam.js, 2021. Accessed in July 2022.
48. IOTA Foundation. iotaledger/mam.client.js. https://github.com/iotaledger/mam.client.js/, 2021. Accessed in July 2022.
49. Truffle Suite. Ganache UI. https://github.com/trufflesuite/ganache-ui, 2023. Accessed: November 2023.
50. IOTA Foundation. iotaledger/streams. https://github.com/iotaledger/streams, 2023. Accessed in November 2023.