SN Computer Science manuscript No.
(will be inserted by the editor)

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

Venkata K. V. V. Bathalapalli · Saraju P. Mohanty* · Elias Kougianos · Babu K. Baniya*** · Bibhudutta Rout†**

the date of receipt and acceptance should be inserted later

Received:10 March 2022 / Accepted: date XXX

Abstract This article presents the first-ever hardware assisted blockchain for simultaneously handling device and data security in smart healthcare. This article presents the hardware security primitive Physical Unclonable Functions (PUF) and Blockchain Technology together as PUFchain 2.0 with a two level authentication mechanism. The proposed PUFchain 2.0 security primitive presents a scalable approach by allowing Internet of Medical Things (IoMT) devices to connect and obtain PUF keys from the edge server with an embedded PUF module instead of connecting a PUF module to each device. The PUF key, once assigned to a particular Media Access Control (MAC) address by the miner, will be unique for that MAC address and cannot be assigned to other devices. PUFs are developed based on internal micro manufacturing process variations during chip fabrication. This property of PUFs is integrated with blockchain by including the PUF key of the IoMT into blockchain for authentication. The robustness of the proposed Proof of PUF Enabled authentication consensus mechanism in PUFchain 2.0 has been substantiated through test bed evaluation. Arbiter PUFs have been used for the experimental validation of PUFchain 2.0. From the obtained 200 PUF keys, 75% are reliable and the Hamming distance of the PUF module is 48%. Obtained database outputs along with other metrics have been presented for validating the potential of PUFchain 2.0 in smart healthcare.

Keywords Internet-of-Medical-Things (IoMT) · Physical Unclonable Functions (PUF) · Blockchain · Proof of PUF Enabled Authentication(PoP) · Wearable Medical Devices (WMD) · Implantable Medical Devices (IMD) · Healthcare Cyber-Physical System (H-CPS)

Venkata K. V. V. Bathalapalli
Dept. of Computer Sci. and Eng., University of North Texas
E-mail: VenkatakarthikvishnuvardBathalapalli@my.unt.edu

Saraju P. Mohanty (Corresponding Author)
Dept. of Computer Sci. and Eng., University of North Texas
E-mail: saraju.mohanty@unt.edu

Elias Kougianos
Dept. of Electrical Eng., University of North Texas
E-mail: elias.kougianos@unt.edu

Babu K. Baniya
Dept. of Computer Science & Digital Technologies, Grambling State University
E-mail: Baniyab@gram.edu

Bibhudutta Rout
Department of Physics, University of North Texas
E-mail: bibhudutta.rout@unt.edu

1 Introduction

The demand for IoMT devices is increasing not just for advancing healthcare technologies and services, but also for facilitating ease of living by reducing human intervention in monitoring health parameters and effectively easing the use of these advanced technologies for the people. As it is becoming more simple, efficient and effective, the IoMT market is expanding along with its associated security vulnerabilities. Battery operated IoMT devices cannot sustain complex cryptographic key security protocols [8]. Blockchain Technology utilization in Smart Healthcare facilitates secure Electronic Health Record Management which is essential to ensure the confidentiality and integrity of patients' sensitive medical records [19,30]. In banking and financial transactions, the blockchain is introduced as a distributed, decentralized, immutable, and irreversible ledger technology where every node in the network maintains a complete record. Whenever a transaction occurs

between any two nodes in the network, all participants in the network are acknowledged about the transaction details. The data, once entered into a blockchain cannot be removed or changed and the respective data is hashed and a block is created and added to the blockchain. The block will be maintained at all nodes in that network [21]. PUFs generate cryptographic keys which are unique to the PUF module and for that particular challenge input. PUFs have been one of the most widely adopted hardware security primitives for IoT based applications due to their simplicity, robustness and energy efficiency [17].

The blockchain together with PUFs can bring more integrity, privacy, and confidentiality in the vibrant healthcare industry. PUF supported IoMT devices can be authenticated using the blockchain and the respective data can be stored in a distributed ledger thereby assuring the integrity of IoMT devices and their data.

The introduction of 5G is making Smart Healthcare applications more accessible to people through smart phones which support high bandwidth, low latency and high speed [13]. Fig. 1 illustrates the applications of PUFchain 2.0. in Smart Healthcare.

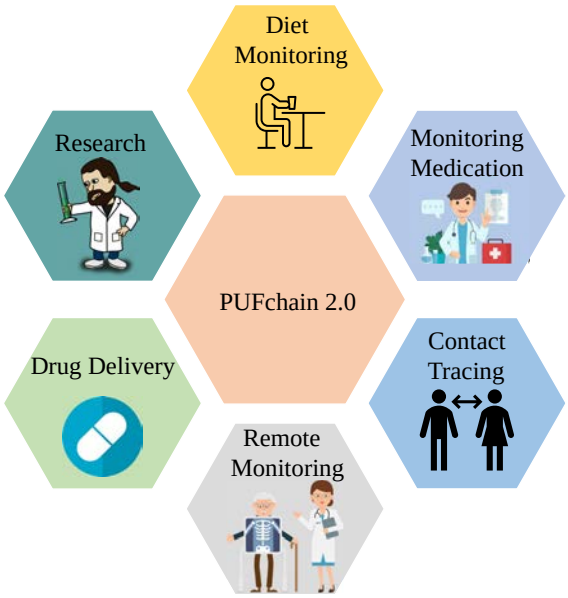


Fig. 1: PUFchain 2.0 in Smart Healthcare

1.1 Smart Healthcare: Healthcare-Cyber Physical Systems (H-CPS)

Improving the efficiency of health services by including advanced technologies like IoT, Artificial Intelligence, Machine Learning and Big data to facilitate ease of living is called Smart Healthcare [30].

In Smart Healthcare, the physiological parameters of patients can be monitored precisely using implantable and wearable medical devices which are placed on and inside the body. The remote monitoring using the IoT helps in tracking a patient's movement, eating habits, sleep schedule, heart rate and blood pressure using implantable and wearable sensors which are connected to the Internet and can communicate with each other. Therefore, a patient's fall detection or heart seizure can be accurately determined using IoMT [28].

Telemedicine can be defined as a communication interface between doctors and patients which utilizes telecommunications and the IoMT to provide clinical health remotely without requiring the physical presence of doctor and patients [7, 19].

1.2 IoMT

The market for the IoMT is increasing during the COVID-19 crisis and is expected to have a substantial growth in the coming years [22, 35]. The IoMT can be categorized as wearable and implantable devices. Wearable medical devices are used to monitor health parameters like heart beat, blood pressure and other fitness related metrics. These devices can be used just like a jacket. Implantable medical devices are placed inside the body through surgical processes like the cochlear implant, a consumer electronic device which consists of a microphone, speech processor, a transmitter, and receiver to provide assistance for the hearing impaired [30]. Fig. 2 details the classification of IoMT.

The IoMT devices embedded on a patient collect sensitive data related to physiological parameters and send the information to the edge server and the cloud for analysis, processing, and decision making. The cloud is a centralized computing architecture whereas the edge is a decentralized computing paradigm that performs swift processing, analysis, and decision making. The cloud can be used for data storage and processing of data that takes a long time. Edge computing works by performing computations near the sensors for processing the data. The edge can also perform actuation by sending commands to implantable medical device actuators.

When the sensed physiological data from the IoMT devices suggest a chance for brain seizure, for example, instead of waiting for the commands from a doctor who needs to access the data from the cloud to analyze and

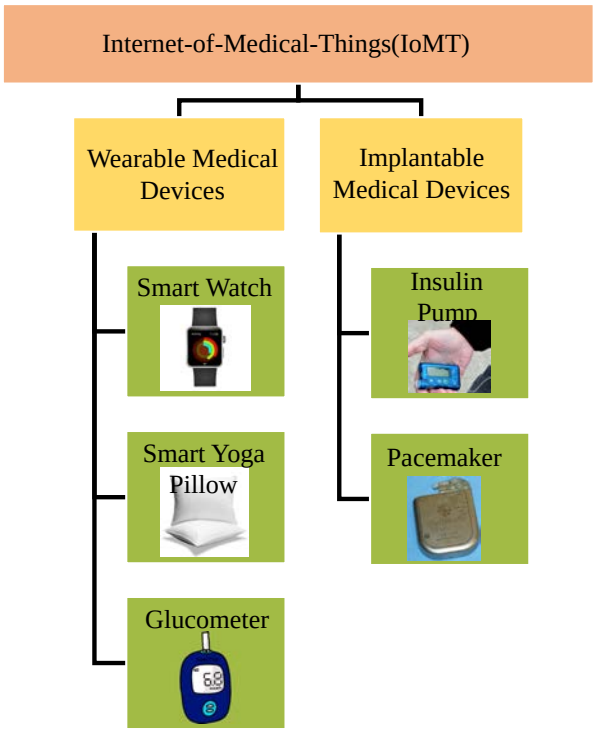


Fig. 2: A Selected Devices of IoMT

suggest medication, the edge can send commands directly to a pacemaker-like device inside the brain which can stimulate neurological signals through electrodes which are implanted surgically. In this way edge computing can be used for critical healthcare applications which require faster processing. Similarly, heart seizure can be identified by monitoring respiration. Nasal sensors can be used for analyzing the respiration rate by monitoring the temperature values while breathing [2].

1.3 Architecture of IoMT in Smart Healthcare

The sensors that perform data sensing and collection become the center components of the Smart Healthcare architecture. This layer can be called physical layer. This layer includes WMD and IMD [11, 31] placed on and inside a patient.

The second layer of IoMT is the communication layer where sensed data from these sensors are sent to an edge or cloud. Various technologies like Bluetooth, RFID, WiFi, LoRaWAN , Zigbee and 5G can be used for enabling communication between the IoMT devices and edge.

The third layer is the edge cloud layer which includes processing, analyzing, and data storage. The fourth layer is the application layer which deals with conveying the analyzed data on physiological parameters to the user securely.

The network layer and the edge cloud layer constitute an important part in the architecture where security, privacy, and quality of data from the IoMT play an important role in decision making. Along with data, hardware integrity also is an essential component as these devices are battery operated, and high level cryptographic schemes are not compatible. Hence low power, energy efficient device security primitives are essential for ensuring the authenticity of hardware. The security of the physical layer constitutes an important part in the IoMT system architecture. Fig. 3 illustrates the architecture of Smart Healthcare.

UAV's can also be used in remote diagnosing and treatment where they can be used for medication using Deep Neural Network for COVID-19. They can also be used for contact tracing and carrying medical supplies from one place to another [23].

The rest of the paper is organized in the following manner: Section 2 presents the novel contributions of the current paper. Section 3 presents the applications of Smart Healthcare and related research on its security issues. PUFs and their characteristics are explained in the Section 4. Blockchain Technology and its importance in IoT based applications are explained in Section 5. Section 6 presents the proposed novel PUFchain 2.0 primitive for security in smart healthcare. Experimental results are given in Section 7. Section 8 presents the conclusion and direction for future research.

2 Novel Contributions of this Paper

2.1 Problem Formulation

In the IoMT, when a fake node is generated and the original node is impersonated by a malicious one, then it can send wrong data to the edge server. As there is no device authentication mechanism in place, the fake node is assumed to be the original one and health data is accepted from the fake node and by processing the data, the edge server sends commands to actuators. Then wrong dose of medication is administered to the patient which could risk the patient's life [35].

To counter this, many symmetric or asymmetric cryptography based key security mechanisms have been proposed, but all these key security primitives require a memory to store the secret key which could be vulnerable to various kinds of security attacks. The success of Blockchain Technology in Bitcoin transactions has made it one of the formidable solutions for security in healthcare due to it its transparency and irreversibility. The main challenges for realizing the potential of

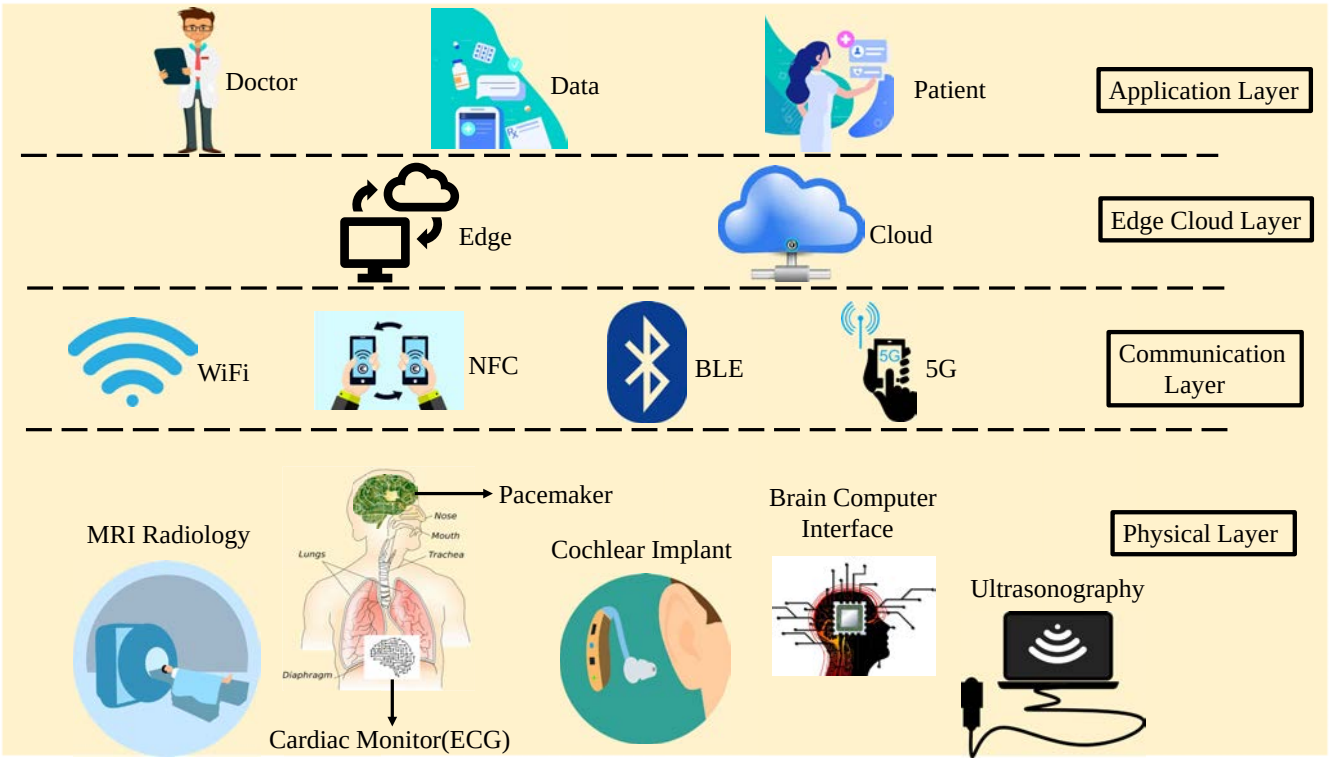


Fig. 3: Layered Architecture of Smart Healthcare.

Blockchain integration in Smart Healthcare are its energy consumption and computational resource requirements [21].

PUFs have shown the way for time and energy efficient key generation mechanism for security in IoT based applications. The novel feature of PUF to generate keys without requiring a non-volatile memory for key storage and its simplicity and robustness in design and application have made it one of most reliable security alternatives in Smart Healthcare [10, 37].

2.2 Hardware-Assisted Secure Blockchain - The PUFchain

In this paper a novel Blockchain assisted PUF based IoMT security mechanism is proposed for edge computing driven smart healthcare.

The PUF key is stored in an immutable Blockchain through robust PUF Enabled computationally efficient Blockchain consensus mechanism for IoMT device authentication. The PUF key is not just a plain cryptographic key generated algorithmically but is developed using the intrinsic delay variations in wiring the microelectronic components inside an electronic device. These variations make the response bit to be either zero or one randomly. More process variations in the design result in more random response bits. The PUF key is tested and evaluated to determine whether the obtained key is unclonable, reliable and unique before applying it for the security solution

PUFchain [21] presents a novel PUF based Blockchain using a Hybrid Arbiter Oscillator PUF module in Proof of Authentication consensus mechanism which has shown much more efficiency in performance as compared to Proof of Authentication (PoAh) consensus mechanism. Its results have shown enhanced performance efficiency in power consumption thereby substantiating the application of the Blockchain as more suitable for security in IoT based applications [26].

The proposed PUFchain 2.0 consists of a two level authentication mechanism for secure smart healthcare applications. As compared to PUFchain protocol which consists of a single level authentication mechanism, the proposed PUFchain 2.0 security primitive proposes a two level authentication approach which consists of MAC and PUF key verification for IoMT device authentication using a 64-bit Arbiter PUF module which is connected to a Server (Miner) and can generate PUF keys for IoMT devices.

A scalable approach for IoMT integration is proposed by assigning unique PUF keys for all the devices virtually from the server which is connected to a PUF module instead of connecting each device to an indi-

vidual PUF module. After verification of device unique properties, PUF key is assigned to the MAC address of each device and is sent back to the client. The PUF key assigned to a MAC address is tested before assignment. The Authentication server checks whether the obtained PUF key meets the standard requirements of PUF metrics and then assigns it to the devices accordingly. Performance evaluation of PUFchain 2.0 and its comparison with PUFchain is given in Section 7.

2.3 Proposed Solution

The proposed PUFchain 2.0 consists of enrollment and authentication phases. During the device enrollment phase, the IoMT device sends its MAC Address to the Authentication Miner in an encrypted form through secure User Datagram Protocol (UDP) socket encryption and decryption protocol. The server receives the message in encrypted form and decrypts the MAC address. The server then extracts a PUF key from the PUF module and assigns it to the device and sends it back to the client. The idea of integrating PUF with Blockchain is due to its simple design which is energy efficient, power optimized and can produce an output which cannot be extracted from the device even when the same PUF design is used [37].

The IoMT device performs data extraction and forms a block using the obtained PUF key, MAC Address, data and time stamp. The block of data is sent to the server for verification. Figure 4a illustrates the enrollment process in PUFchain 2.0.

In the authentication phase, the server receives the block of data and extracts the MAC address. The Authentication Server checks the integrity of the block by comparing the received MAC address from the block of data and the MAC Address received in the encrypted form. If the obtained MAC address in the encrypted form and the MAC Address in the received block are matching, the first level of authentication is considered as successful. Once MAC Verification is done, the PUF key is extracted from the PUF module corresponding to the assigned MAC Address and compared with the one in the block of data. If the PUF keys are matching, then the second level of authentication is successful and the device is considered as authenticated. The authentication process in PUFchain 2.0 is explained in Figure 4b.

The block of data is validated and hashed using the SHA-256 algorithm and broadcasted to all the client nodes in the Blockchain network.

2.4 Novelty of the Proposed Solution

Scalability is one of the challenges for PUF integration into the Blockchain Technology. By assigning the PUF keys to the MAC Address which is unique to each device and making sure that the PUF key assigned to one MAC address is unique to that MAC, various types of impersonation attacks can be avoided since the PUF key is a unique identifier built using the variations in internal micro manufacturing process of a chip. By authenticating the MAC along with the PUF key of the device, a two level verification is done as the PUF is being accessed by the client remotely through the server. The MAC address being an IoT device property cannot be duplicated and can be used as a secure identity for the device. If the initial MAC verification is unsuccessful, the server will discard the block of data from the device. Instead of connecting each and every IoMT device to the PUF module, the PUF module can be connected to the Miner and PUF keys can be extracted from the PUF module, checked and assigned to the client virtually. Once authentication is successful then the block of data with PUF key and MAC is hashed and entered into a decentralized ledger which is maintained at all the nodes thereby ensuring data and device security.

3 Related Research on Smart Healthcare and its Security

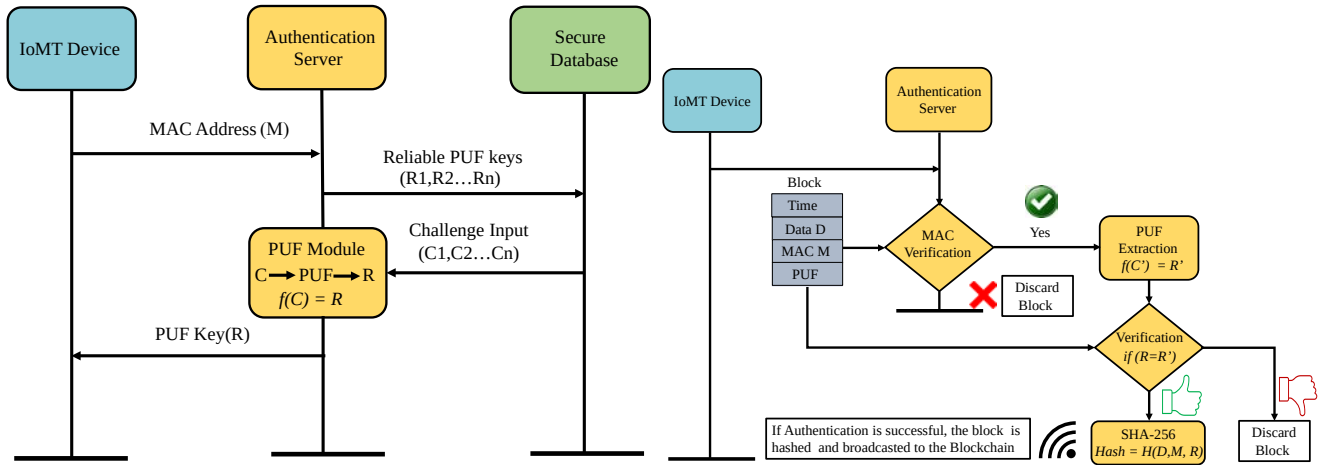
Smart Healthcare is one of the most attractive research areas, as evident from its role during the pandemic. Its applications and security have become focal points for researchers. Smart Healthcare and its applications are summarized in Table 1.

Device security has become a major issue where the vulnerabilities in medical electronic devices to impersonation attacks can have a negative impact on the overall security ecosystem [4]. For instance, if a cochlear implant's security is compromised, then it can be programmed by hacker to work in a way that could impact the patient [4]. Various security attacks on IoMT devices have shown the importance of authentication and confidentiality of IoMT devices and their data.

Impersonation attack: In an impersonation attack, a hacker can impersonate an authorized user's identity or secret key and obtains access to IoMT data [8].

Network Attacks: A network attack results in Denial of Service (DoS) from either server or device by disrupting the network interface between IoMT devices.

Brute Force Attack: In this type of attack, a hacker tries all possible secret keys until it matches with



(a) Device Enrollment Process

(b) Device Authentication Process

Fig. 4: Working of PUFchain 2.0

the original one. Security features like Blockchain technology and Bio metric identification can mitigate this type of attack [8].

In the area of hardware integrity in IoMT, various security protocols have been proposed to ensure sustainable and secure wearable and implantable medical devices for remote monitoring of patients' physiological health metrics. A mutual device authentication scheme is proposed by Yoon et al. [38] with an Authentication Server as a trusted intermediary in the IoMT. The security scheme is proposed to be effective against various machine learning and physical attacks.

A lightweight device authentication scheme for the IoT using PUFs is proposed in [14]. It works by updating each challenge-response pair for subsequent transactions after successfully verifying the PUF keys.

A PUF based lightweight security protocol using a simple one way hash and bit wise Exclusive OR operations is proposed to build a secure key management protocol for medical device integrity in [20].

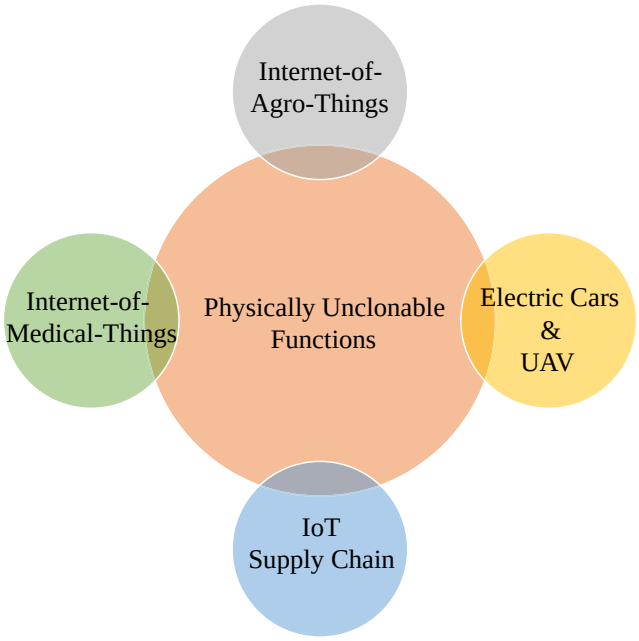


Fig. 5: Applications of PUF

4 Physical Unclonable Function (PUF)

A PUF is developed using micro manufacturing variations during the chip manufacturing process which includes fabrication, mask generation and testing. The PUF key of a particular Integrated Circuit (IC) is considered as the fingerprint for that IC. The PUF does not require memory for key storage. The keys are generated at run time using silicon manufacturing variations affected by various parameters like Ion implantation, Lithography, and environmental effects [17, 36]. Applications of PUFs are given in Fig. 5.

The input to a PUF and the output from a PUF are called as Challenge Response Pairs (CRP). A PUF can be categorized as a Strong or Weak PUF. A **Strong PUF** is the one that supports a large number of Challenges and Responses whereas a **Weak PUF** can hold a limited number of CRPs. PUFs can also be classified as Delay based PUFs and Memory based PUF. A delay based PUF is built based on the delay fluctuations associated with wiring of electronic components which leads to a race off condition between two signals in a symmetric circuit design. The memory PUF is based

Table 1: Smart Healthcare Devices and applications

Works	Application	Features	Type
Webster et al. 1995 [34]	Implantable Cardiac Monitoring pacemaker	Pacemaker embedded with a pressure monitor to stimulate neurological signals to monitor and properly maintain heart rate	Implantable Medical Device
Lindvqvist et al. 2006 [18]	Deep Brain Neurostimulators	Through implanted electrodes, Neurological signals with various amplitude are stimulated to cure brain related diseases	Implantable Medical Device
Bui et al. 2007 [3]	Biosensors	Set of sensors for monitoring various physiological parameters inside the body	Implantable Medical Device
Rachakonda et al. [27]	Smart Yoga Pillow	Blockchain assisted smart pillow for monitoring sleeping habits using IoMT	Wearable Medical Device
Mahender Kumar et al. [16].	SAI-BA-IoMT	AI integrated Blockchain assisted IoMT system for COVID-19 Diagnosing.	-
Sethuraman et al. [32]	My Wear	A smart garment to monitor the health parameters based on the muscle activity and stress levels.	Wearable Medical Device
Olokodana et al. [24]	EZcap	A Wearable to monitor seizure detection using kriging methods	Wearable Medical Device
Joshi et al. [9]	iGLU	A PUF embedded secure glucose monitoring with safe insulin dosage delivery system	Wearable medical device
Rachakonda et al. [29]	iMirror	A Smart mirror for stress analysis by automatic facial recognition and appropriate stress response system	Wearable medical device

on the instability in the transistors during the startup phase of a volatile memory cell. Arbiter PUF, Ring Oscillator and Butterfly PUF modules are most widely used delay PUFs. SRAM PUF and DRAM PUF are the prominent memory based PUFs.

The quality and robustness of a PUF can be determined using metrics which help in evaluating the strength of PUF keys. Hamming Distance, Uniqueness, Reliability, and Randomness are prominent PUF metrics.

Hamming Distance: Hamming distance between two PUF keys is the amount variability of bits in the two PUF keys. A PUF module with a Hamming Distance between 40 to 50 % is considered as a reliable one [10]:

$$IntraHammingDistance = ((HD(i,j)/64) * 100). \quad (1)$$

In the above expression, i, j are the two PUF keys with the length of 64 bits generated using the same PUF module.

Reliability of a PUF module is the ability to generate the same response output at varying operating and environmental conditions [21]:

$$Reliability = 100\% - IntraHammingDistance. \quad (2)$$

Uniqueness: The property of a PUF module to produce different outputs when two varying challenge inputs are given to the same PUF module is called uniqueness. When the same PUF module is built on another IC, uniqueness can be defined as a measure of amount of variability in the obtained PUF keys from the two PUF modules [10].

Randomness: Randomness of a PUF key is the measure of balance between number of zeros and ones in a PUF key. If the PUF key has equal number of random zeros and ones, then it is considered as secure PUF module which can sustain brute force and other key guessing attacks.

5 Blockchain Technology

Blockchain is an immutable decentralized transaction record maintained at each and every node in the network. Transactions between any two nodes in the network are validated and added to the chain using a standard protocol which is called a consensus mechanism. The nodes which have the privilege to validate the blocks are called Trusted nodes. Fig. 6 explains about applications of Blockchain Technology.

In financial transactions, a centralized approach for data storage, security and validation could bring more problems where entrusting the process of transaction validation to one entity at times could compromise the security of data. The distribution of responsibilities and power to validate transactions among a group of entities could bring more transparency, authenticity and reduces the chance for a single point failure [21].

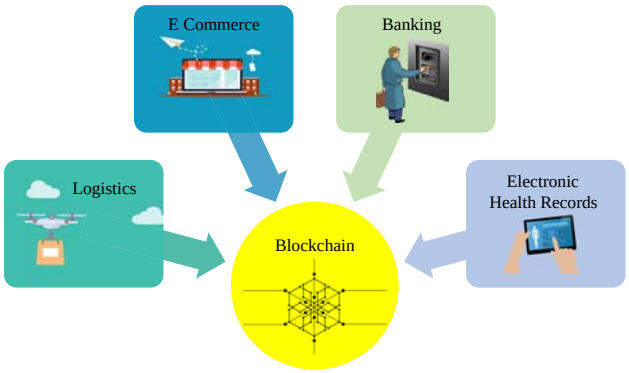


Fig. 6: Selected Applications of the Blockchain Technology.

In a banking transaction, if one person borrows some amount from another, then the transaction is stored inside a block and broadcasted through the network involving all concerned parties. The privileged nodes or miners examine the transaction based on the consensus mechanism and validate the block and add it into the Blockchain. Trusted nodes which perform successful validation are rewarded with trust points based on the consensus mechanism.

There are many categorizations of Blockchain Technology. Permissioned and Permissionless Blockchain are two important types where Permissioned Blockchain is the one that exists among small group of nodes and can be used for applications requiring more privacy and anonymity. A Public Blockchain is an open platform and can be used for more general applications [26]. For Healthcare, Private Blockchain is the most suited since confidentiality and privacy are required in healthcare which can be facilitated by a private Blockchain.

5.1 Blockchain Technology in Smart Healthcare

Due to its characteristics of anonymity, decentralization, and irreversibility, the Blockchain Technology application in healthcare has become one of the most reliable solutions. All the medical records related to patients are now mostly in traditional paper or cloud based methods. Blockchain can be used for secure storage of data where all the patients' records in a hospital can be stored in a decentralized ledger which guarantees the integrity of patient sensitive personal data by hashing the blocks and maintaining a record at all parties and can therefore restrict access to unauthorized users [5, 33].

In the pharmaceutical supply chain, if a ledger is maintained at each stage starting from the point where a product is manufactured to the stage where it finally reaches the end consumer, a step by step verification can be done at each point and it can be beneficial as more efficiency and accountability can be brought into the system. According to a report from the World Health Organization, improper management of supply chain in healthcare has resulted in deaths of millions of people [12, 15]. The products can therefore be tracked and checked at each stage during the supply chain process starting from clinical trials to distribution stage where it is being administered or prescribed to a patient [6, 19]. The applications of Blockchain Technology in Smart Healthcare are illustrated in Fig. 7.

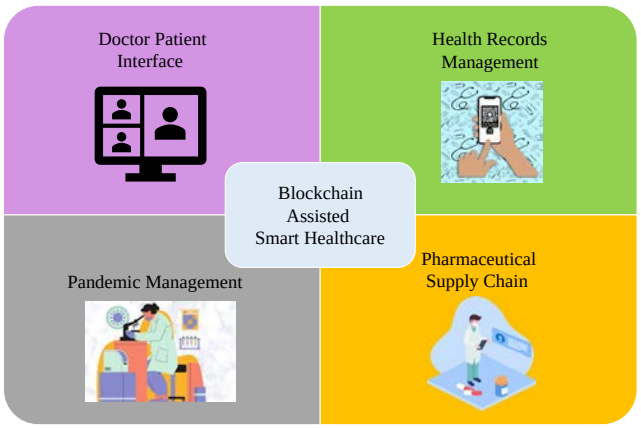


Fig. 7: Blockchain Assisted Smart Healthcare.

5.2 Consensus Mechanisms in the Blockchain

The transactions among the network of nodes are validated and added to the Blockchain based on an agreement which are the operating procedure guidelines for transaction validation [25]. Operating guidelines are called Consensus Mechanisms.

Proof of Work (PoW): PoW is a consensus mechanism developed for Bitcoin transactions where the privileged nodes or Miners use computational resources to obtain a Nonc,e which is a target value set as per the

consensus mechanism. If two or more miners successfully achieve the Nonce value which is the hash value of the block required to be added, then a condition called fork arises. Then all the blocks are accepted and added to the Blockchain [25].

Proof of Stake (PoS): PoS is a consensus mechanism where miners are selected based on the cryptocurrency stake. After successful validation of blocks, the miner is incentivized with a certain amount of stake. The objective of PoS consensus mechanism is to address the computational resource requirement in PoW. The disadvantage in PoS is lack of standardization in determining the Miners. This makes the nodes with high stake to continuously become miner which may make the other nodes with low stake to be inactive.

Proof of Activity (PoA): An activity based consensus protocol where nodes participating in the block validation and broadcasting process will be able to receive some stake as a reward while the nodes not involved in the process will not able to win. The objective of PoA is to encourage the nodes in network to be active so that all the nodes can be taken into confidence for block validation process which can address the problem in Proof of Stake where the entire process is concentrated among certain privileged nodes with higher amount of stake [25].

Proof of Authentication (PoAh): PoAh has been developed with the objective of integrating IoT with blockchain. In PoAh, once a block is received, it is added to the chain only after successful authentication. The authentication is done by verifying the properties of IoT devices and on successfully adding the block, the trust value of miners increases by one unit. The miners with higher trust value are more preferred for subsequent block validation processes than miners with lower trust value [26].

5.3 PoP Consensus Mechanism for IoT Security

PUF based authentication mechanism in an IoT based environment consists of group of IoT devices as network of nodes where each node collects the data and sends the data to trusted nodes in the network for block validation. Along with the data, the PUF key of the respective device is also included in the block of data.

The trusted node listens to the message and receives the block. It verifies the integrity of the device by extracting the PUF key from the block of data and performing key extraction. The obtained PUF key and the PUF key in the block are compared and verified. Once the PUF key verification is successful, the block of data is hashed and added to the immutable ledger [1, 21].

Consensus mechanisms in Blockchain and their properties are presented in Table 2.

6 Proposed Blockchain Integrated PUF Enabled Security Mechanism for IoMT: PUFchain 2.0

Blockchain Technology which is considered as a data security primitive is integrated with secure hardware fingerprints (PUF) for device authentication of wearable and implantable electronic medical devices in Healthcare. The idea of PUFchain 2.0 is presented in Figure 8.

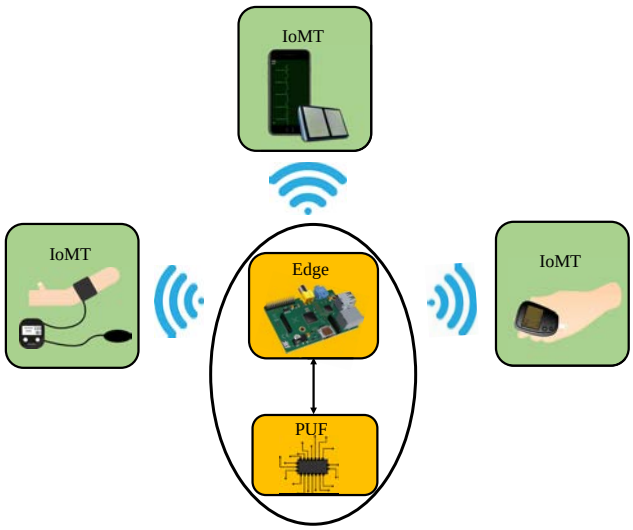


Fig. 8: PUFchain 2.0

Blockchain consists of blocks where each block contains a hash value which is the identity of that block. All blocks in the Blockchain are connected to one another using the previous hash value which is also included in the block of data. The hash is computed on the block of data containing information from the IoMT device and the hash value of the previous block.

The data, once entered inside a block, cannot be tampered and changed as the hash values of previous blocks will also change. PUF key of IoT device in proposed PUFchain 2.0 is included in the block of data so the device ID is registered in the Blockchain and cannot be changed. Hence during device authentication, when PUF keys are extracted, they can be verified from the Blockchain and authentication of IoMT devices can be successful by efficient integration of PUF and Blockchain technologies. The architecture and working of proposed PUFchain 2.0 in Smart Healthcare is illustrated in Fig.9.

Table 2: Characteristics of Blockchain Consensus Mechanisms [25, 26].

Consensus Algorithm	Features	Challenges
Proof of Work	Miners compete to find hash value of the Block	High computational resources
Proof of Stake	Miners entrusted for block validation are determined using their cryptocurrency stake which reduces computational burden	Does not take all the nodes with low stake into confidence
Proof of Authentication	Block of data from IoT is validated only after successful verification of its device properties	Does not include Hardware security aspect
Proposed Proof of PUF-Enabled Authentication	Validates the Block from IoT device by verifying its PUF key which is the fingerprint for the Electronic Devices thereby guaranteeing the authenticity of IoT devices with more time efficiency.	No Challenges

In the proposed PUFchain 2.0, to authenticate the IoMT devices, they initially enroll using their device properties and obtain the PUF key assigned by the miner, which is unique to that device. Once the data collection is done, the block of data is sent to the Miner for validation. Algorithms 1 and 2 illustrates the enrollment and authentication phases in PUFchain 2.0 for secure Smart Healthcare.

Algorithm 1: Device Enrollment Phase of PUFchain 2.0

Input: MAC address of the Client is Sent to Miner(Edge Server) using secure Socket Encryption and Decryption
Output: Unique PUF Key Rx assigned to Client using the MAC Address

Client Node sends its MAC address to the Miner in encrypted form using Secure Socket encryption and Decryption
`// Client→Encrypted MAC Address→ Miner`
Miner Decrypts the MAC a ddress
`// Miner→Decryted MAC Address`
Miner: Select Challenge Input(C) and obtain PUF key
PUF→f(C)=R `// C→PUF→ R`
if *PUF key(R) is standard* **then**
    PUF Key→**MAC Address M**
    `// PUF Key is assigned to the MAC Address of the Client`
Miner sends back unique PUF key assigned to client
`// Miner→`R`→ Client`

Trusted nodes receive the data and check the authenticity of these devices by extracting the IoMT device credentials (PUF key) and MAC address from the block and perform a key extraction process by giving a challenge input and obtain the response output from the PUF module.

7 Experimental Results

The experimental setup in PUFchain consists of two single board computers as edge devices and an edge server for authentication and data validation. The PUF module is connected serially to edge server through serial communication with 9600 Baud rate.

PUF and hashing module is developed on Digilent Basys 3 Artix-7 Xilinx FPGA. In the Enrollment phase, the MAC address is sent to the edge server in encrypted form through Universal data gram protocol secure socket encryption and decryption program. The received MAC address is decrypted by the edge server. The PUF key is extracted by the miner and is checked. The PUF key is sent back to the IoMT device where it forms a block of data with its MAC, PUF, timestamp and IoMT data.

Two Client edge nodes are assigned two different PUF keys based on their MAC address. The PUF Key assigned to a MAC Address will be its key forever and the same PUF key will not be assigned to different MAC Address. Two transactions have been initiated from two clients and after authenticating, validating and adding the transaction from one client node to the Blockchain, the Miner broadcasts the validated block to both the client nodes in the network. The transaction validation and outputs of the transaction from 1st client node are shown in Figure 10. Figure 10a, and Figure 10b show the transaction outputs of 1st client at Client1 and Client2. Block validation and authentication outputs at the Miner for the 1st Transaction are shown in Figure 10c.

The design and architecture of proposed PUF module in PUFchain 2.0 is shown in Fig.11. Since the PUF key assigned to one device is unique to that device, the transaction initiated by the second client will be assigned a different PUF key that is permanent for that client. Transaction validation outputs for the 2nd client transactions are shown in Figure.12a, 12b and 12c.

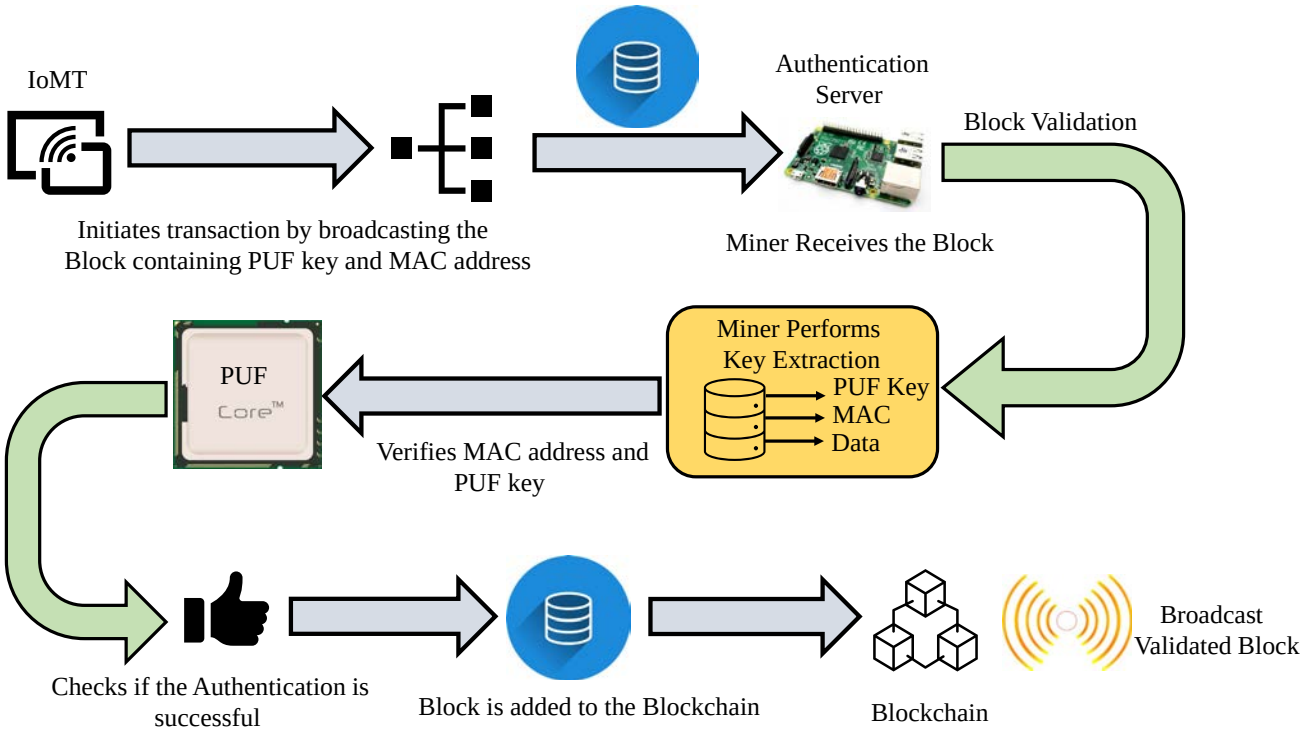


Fig. 9: PUFchain 2.0 for Secure Smart Healthcare.

The Miner receives the block of data through UDP and extracts the MAC from the block to check if the obtained MAC and received MAC address from the block are matching. Once the device authenticity is verified, PUF keys from the PUF module are compared with the one in the block. If the keys are matching, the block is hashed using SHA-256 and added to SQlite Blockchain database developed at all the nodes.

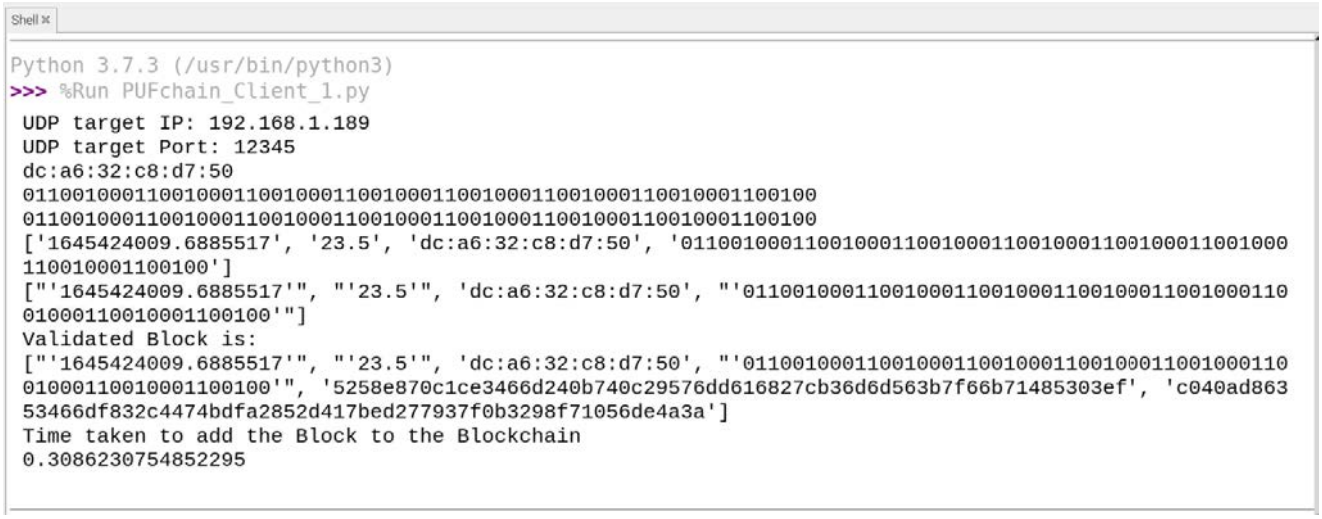
The obtained database outputs at 2 clients and Miner are shown in Figure.13a, Figure 13b and Figure 13c.

VIVADO is used to develop the PUF design and the code is transferred onto the FPGA board using UART serial communication. Baud rate of 9600 has been used to send and receive the challenges and responses. Python programming is used for developing Blockchain database and enabling serial communication with the FPGA board to extract the PUF keys. An SQLite database is used to develop the PUFchain 2.0 databases at both Client and Trusted nodes. Time is an important metric in evaluating the efficiency of an application in IoT. The proposed PUFchain 2.0 security primitive has shown very good results. Time taken to validate, authenticate and add the block to Blockchain at all the nodes are shown in Figure 14a, 14b, and 14c for both Clients and Edge server (Miner).

Time taken for miner from the point it received the block, perform key extraction, establishing connection with database, adding the block to the chain and finally sending it back to the Client node is approximately 3.6 seconds. On the Client side, time taken to broadcast the block, receive the data, and adding it to the chain is within 0.4 seconds. The power report from VIVADO has shown the total on-chip power for the PUF design after synthesis, implementation and bit stream generation is 81 mW. The standard deviation of Hamming distance percentage is 1.6% for the PUF module with a variance of about 2.5%. The Raspberry pi's power consumption while programming is between 3.1 to 3.5 Watts. Fig.15a shows the Hamming distance between the PUF keys of the Arbiter PUF module. Fig .15b gives the reliability of the PUF module and randomness of zeros and ones in the PUF keys from arbiter PUF module is shown in Fig. 15c.

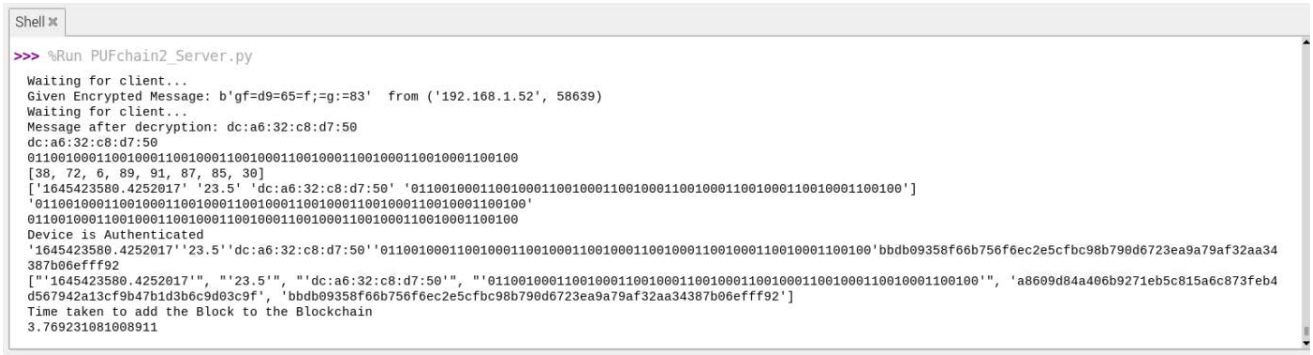
The arbiter PUF, which is a delay based strong and secure PUF module is used for implementing PUFchain 2.0. By supporting more challenge response pairs, the arbiter PUF established its position as one of the most widely used ones for cryptographic applications in the IoT. 64 instances of the PUF circuit design which consists of arbiter elements built using flip flops and multiplexers have been created to generate a 64-bit key. Fig.16 shows the prototype of PUFchain 2.0.

Metrics of the PUF substantiate its potential in a security application. 200 PUF keys were extracted and



(a) Output at the 1st Client

(b) 1st Client Transaction output at 2nd Client



(c) 1st Client Transaction output at Miner side

Fig. 10: 1st Client Transaction outputs

tested to evaluate the metrics of the PUF, using MATLAB. Randomness of 47% is achieved from the PUF keys and among 100 tested PUF keys, 75 responses have been regenerated successfully. The proposed Proof of PUF Enabled Authentication consensus mechanism is faster than proof of work which has a latency of 10 minutes [21]. The characteristics and experimental results of PUFchain 2.0 are given in Table 3, Table 4a, and Table 4b.

The comparison of PUFchain 2.0 with other security protocols is illustrated in Table 5. The PMsec protocol proposed in [35] for IoMT does not include the Blockchain for PUF key storage. In [21], the PUFchain (1.0) protocol utilizes single authentication which can be hacked or impersonated and all the devices need to be embedded with a PUF module for establishing communication with server.

This paper presented a novel multi level device authentication approach which is capable of supporting more IoMT devices and can assign PUF keys virtually. This approach can enable more devices to integrate into

Algorithm 2: Authentication phase of PUFchain 2.0

Input: Block of Data from Client containing PUF key, IoMT data and MAC Address
Output: Block Validation and Authentication

1 IoMT collects data and forms a Block Bn including its Data, MAC Address and obtained PUF key(R) to the server
2 Bn→**M,R**;
`// IoMT→Data`
`// Block=IoMT Data(D)+PUF Key(R) +MAC Addres M`
3 Client Node broadcasts the Block B
4 Miner receives the Block B of Data from Client
5 Miner Extracts the MAC Address and performs authentication process
`// Block B->Miner`
6 **if** *MAC Address is matched* **then**
`// MAC verification is successful`
`// Miner performs PUF key Verification`
7 PUF→f(C')=R';
`// Miner→PUF→Key R'`
8 **if** *(R==R')* **then**
`// PUF key verification is successful`
9 Compute hash of the Block B
10 Hash=H(D, M, R) `// SHA-256 Hashing Algorithm is used to compute hash`
11 Add Block to the Blockchain
12 Broadcast the Validate Block B
13 **else**
14 Discard the Block
15 **else**
16 Discard the Block

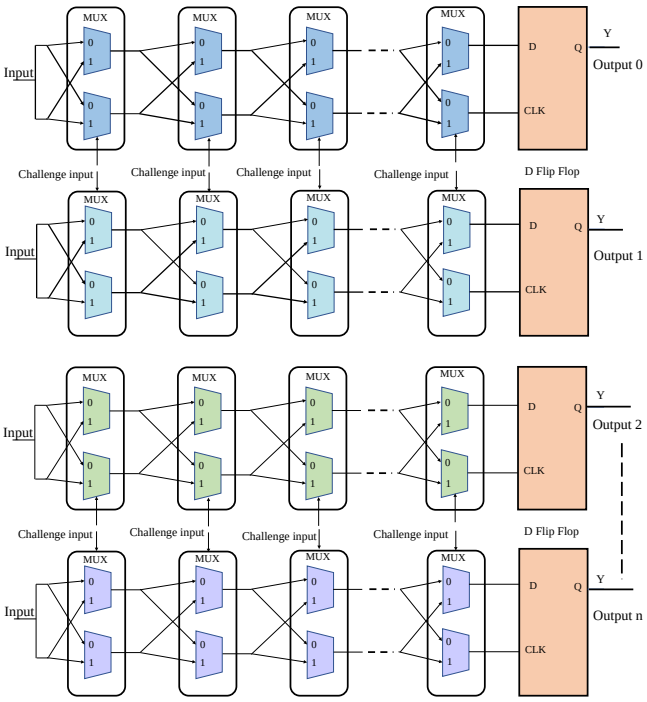


Fig. 11: Arbiter PUF Module

Table 3: Characterization of PUFchain 2.0

Parameters	Results
Client Node	IoMT
Trusted Node	Edge Server
PUFchain Database	SQLite
PUF Module	64 bit Arbiter PUF
IoMT	Single Board Computer
PUF and Hashing module	Xilinx Artix-7 FPGA
Edge Server	Raspberry pi 4
Communication	Serial(UART), UDP
Baud Rate	9600
Programming	Verilog, Python
Consensus Mechanism	Proof of PUF Enabled Authentication

the authentication scheme as these devices are assigned PUF keys virtually by miner.

8 Conclusion and Future Research

The success of smart healthcare lies in successful convergence of security and application. The applications of smart healthcare can facilitate ease of living. At the same time its security lapse can equally have catastrophic impact on its application. This paper presents PUFchain 2.0 with the objective of realizing the fullest potential of Blockchain Technology and PUF for secure Smart Healthcare security through time and energy efficient Proof of PUF Enabled Authentication Consensus mechanism. The implementation of proposed PUFchain 2.0 has shown better results in time and other performance metrics while being lightweight, scalable and robust.

The Blockchain and PUF integration together can contribute for secure smart healthcare which has been substantiated by the implementation and results. All the existing security protocols proposed for smart healthcare focus on either hardware assisted security or Blockchain based data security [35]. This paper proposed and implemented the PUFchain 2.0 primitive with both Blockchain and PUF together providing security where IoMT device authentication and integrity of data from these devices can be guaranteed through two level authentication protocol.

Table 4: Experimental Results of PUFchain 2.0 for Secure Healthcare.

PUFchain 2.0 Parameters	Values
Hamming Distance	48.2%
Number of PUF Keys	200
Variance	2.6%
Standard Deviation	1.6%
Blockchain Type	Private
Total On-Chip Power	0.081W
Security Mechanism	Two level Authentication
Reliable PUF Keys	75%
Intra Hamming Distance	24.8%
Randomness	41.8%

(a) Metric Evaluation for PUFchain 2.0

Parameters	2nd Client	1st Client	Miner
Time taken for Blockchain Transaction(ms)	309	314	3600
Number of Transactions	30	30	30
Mean(ms)	307	275	2740
Standard Deviation(ms)	70	84	1300

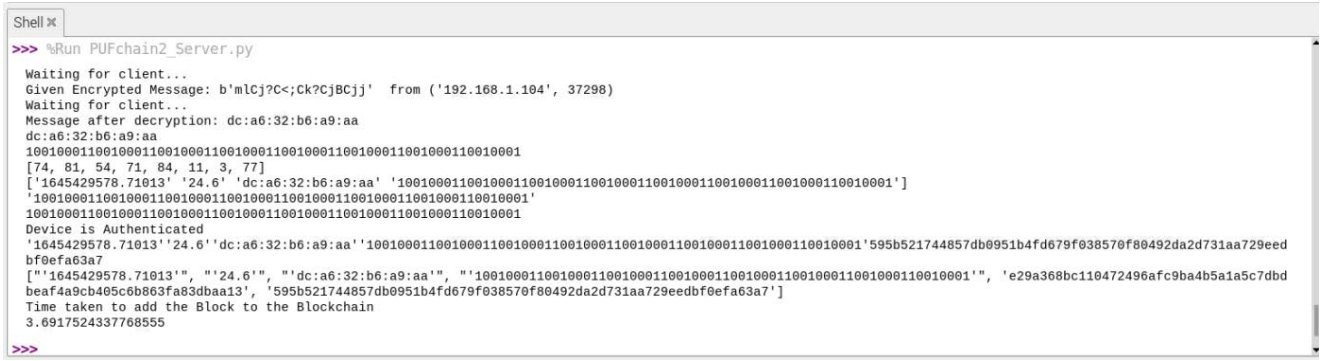
(b) Validation of Time Efficiency in PUFchain 2.0

Table 5: Comparison of PUFchain 2.0 with Other Security Protocols

Parameters	**PMsec** [35]	**PUFchain** [21]	**PUF based IoT Authentication** [14]	**PUFchain 2.0 [This Paper]**
Application	IoMT	IoT	IoT	Smart Healthcare
Prototyped Hardware	FPGA, 32-bit Microcontroller based board	Altera DE-2, Single Board Computer	Coretex-M4 based STM32F4 MCU	Xilinx Artix -7 Basys3 FPGA and Single Board Computers
Blockchain Type	-	Private	-	Private
Security Mechanism	PUF Key Verification	PUF key verification	PUF Key verification	MAC Address and PUF key verification
PUF Keys at Client	Serial PUF keys	Serial PUF keys	Serial PUF	Edge assigned PUF keys
PUF Circuit Design	Hybrid Oscillator Arbiter PUF	Ring oscillators	RC PUF, PHY PUF, Flash and PDRO PUF	Arbiter elements with Multiplexers and D-Flip Flop
Randomness	44%	47%	-	41.8%
Reliability	0.85%(FinFET)	1.25%	-	75% of the keys are reliable
Consensus Mechanism	-	Proof of PUF Enabled Authentication	-	Proof of PUF Enabled Authentication
Security Levels	Single level Authentication	Single Level Authentication	Single level Authentication	Two level Authentication
Blockchain Transaction Time(Client)	-	46.5 ms(Raspberry pi 3)	-	309 ms(Client 1), 314 ms(Client 2)
Blockchain Transaction Time(Miner)	-	120.03 ms(Raspberry pi 3)	-	3600 ms

(a) 2nd Client Transaction output at 1st Client.

(b) Output at the 2nd Client.



(c) 2nd Client Transaction output at Miner side.

Fig. 12: Outputs of the 2nd Client Transaction in PUFchain 2.0.

In future we envisage to work on extending PUFchain 2.0 security primitive to other areas of IoT based applications like Smart Agriculture and Autonomous vehicles security. One future research direction could be on linking PUFchain 2.0 with machine learning and AI technologies which could further enhance robustness and efficiency of AI and ML based applications in futuristic Healthcare Industry.

Compliance with Ethical Standards

The authors declare that they have no conflict of interest and there was no human or animal testing or participation involved in this research. All data were obtained from public domain sources.

Acknowledgment

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.

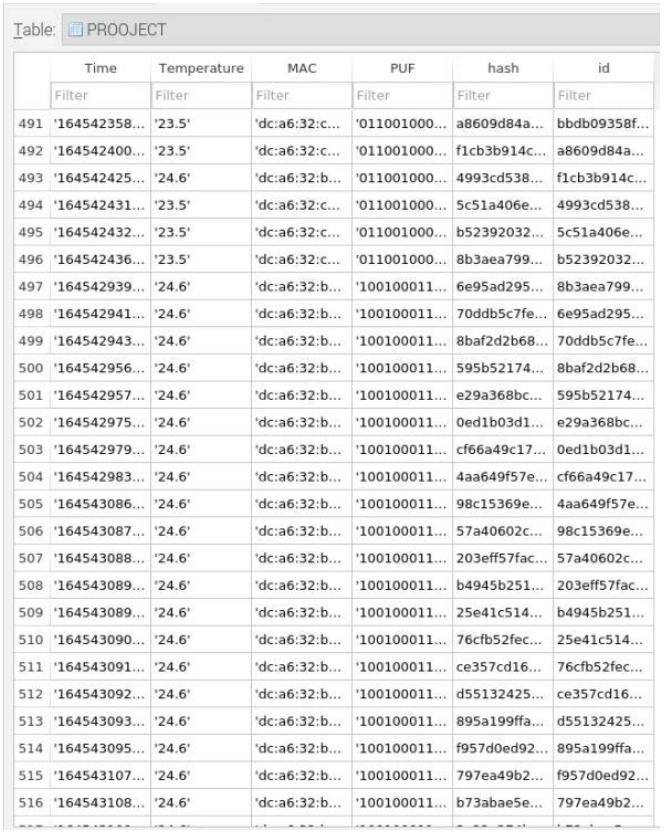


Table: PROOJECT

	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
491	'164542358...	'23.5'	'dc:a6:32:c...	'011001000...	a8609d84a...	bbdb09358f...
492	'164542400...	'23.5'	'dc:a6:32:c...	'011001000...	f1cb3b914c...	a8609d84a...
493	'164542425...	'24.6'	'dc:a6:32:b...	'011001000...	4993cd538...	f1cb3b914c...
494	'164542431...	'23.5'	'dc:a6:32:c...	'011001000...	5c51a406e...	4993cd538...
495	'164542432...	'23.5'	'dc:a6:32:c...	'011001000...	b52392032...	5c51a406e...
496	'164542436...	'23.5'	'dc:a6:32:c...	'011001000...	8b3aea799...	b52392032...
497	'164542939...	'24.6'	'dc:a6:32:b...	'100100011...	6e95ad295...	8b3aea799...
498	'164542941...	'24.6'	'dc:a6:32:b...	'100100011...	70ddb5c7fe...	6e95ad295...
499	'164542943...	'24.6'	'dc:a6:32:b...	'100100011...	8baf2d2b68...	70ddb5c7fe...
500	'164542956...	'24.6'	'dc:a6:32:b...	'100100011...	595b52174...	8baf2d2b68...
501	'164542957...	'24.6'	'dc:a6:32:b...	'100100011...	e29a368bc...	595b52174...
502	'164542975...	'24.6'	'dc:a6:32:b...	'100100011...	0ed1b03d1...	e29a368bc...
503	'164542979...	'24.6'	'dc:a6:32:b...	'100100011...	cf66a49c17...	0ed1b03d1...
504	'164542983...	'24.6'	'dc:a6:32:b...	'100100011...	4aa649f57e...	cf66a49c17...
505	'164543086...	'24.6'	'dc:a6:32:b...	'100100011...	98c15369e...	4aa649f57e...
506	'164543087...	'24.6'	'dc:a6:32:b...	'100100011...	57a40602c...	98c15369e...
507	'164543088...	'24.6'	'dc:a6:32:b...	'100100011...	203eff57fac...	57a40602c...
508	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	b4945b251...	203eff57fac...
509	'164543089...	'24.6'	'dc:a6:32:b...	'100100011...	25e41c514...	b4945b251...
510	'164543090...	'24.6'	'dc:a6:32:b...	'100100011...	76cfb52fec...	25e41c514...
511	'164543091...	'24.6'	'dc:a6:32:b...	'100100011...	ce357cd16...	76cfb52fec...
512	'164543092...	'24.6'	'dc:a6:32:b...	'100100011...	d55132425...	ce357cd16...
513	'164543093...	'24.6'	'dc:a6:32:b...	'100100011...	895a199ffa...	d55132425...
514	'164543095...	'24.6'	'dc:a6:32:b...	'100100011...	f957d0ed92...	895a199ffa...
515	'164543107...	'24.6'	'dc:a6:32:b...	'100100011...	797ea49b2...	f957d0ed92...
516	'164543108...	'24.6'	'dc:a6:32:b...	'100100011...	b73abae5e...	797ea49b2...

(a) Blockchain at Edge Server.

Table: PROJECT

	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
480	'164468824...	'23.5'	dc:a6:32:c8...	'100000111...	51bc310f3e...	c040ad863...
481	'164468825...	'23.5'	dc:a6:32:c8...	'100000111...	b7485913a...	c040ad863...
482	'164468826...	'23.5'	dc:a6:32:c8...	'100000111...	ac53cd459...	c040ad863...
483	'164468859...	'23.5'	dc:a6:32:c8...	'100000111...	91b8837b7...	c040ad863...
484	'164468860...	'23.5'	dc:a6:32:c8...	'100000111...	35fec3ce0b...	c040ad863...
485	'164468874...	'23.5'	dc:a6:32:c8...	'100000111...	a25323634...	c040ad863...
486	'164468880...	'23.5'	dc:a6:32:c8...	'100000111...	348c48472...	c040ad863...
487	'164468886...	'23.5'	dc:a6:32:b6...	'100000111...	64b1d0acb...	c040ad863...
488	'164468890...	'23.5'	dc:a6:32:b6...	'100000111...	4b73c73f67...	c040ad863...
489	'164468894...	'23.5'	dc:a6:32:c8...	'100000111...	8301bb336...	c040ad863...
490	'164468898...	'23.5'	dc:a6:32:c8...	'100000111...	7780c506f8...	c040ad863...
491	'164468901...	'23.5'	dc:a6:32:b6...	'100000111...	d2a5a37e8...	c040ad863...
492	'164468906...	'23.5'	dc:a6:32:c8...	'100000111...	b8c9d022c...	c040ad863...
493	'164468917...	'23.5'	dc:a6:32:b6...	'100000111...	d503eaa15...	c040ad863...
494	'164468919...	'23.5'	dc:a6:32:c8...	'100000111...	169f1b6c78...	c040ad863...
495	'164468922...	'23.5'	dc:a6:32:c8...	'100000111...	0cc29ad51...	c040ad863...
496	'164468946...	'23.5'	dc:a6:32:c8...	'100000111...	f16d68a7e2...	c040ad863...

(b) Blockchain at 1st Client.

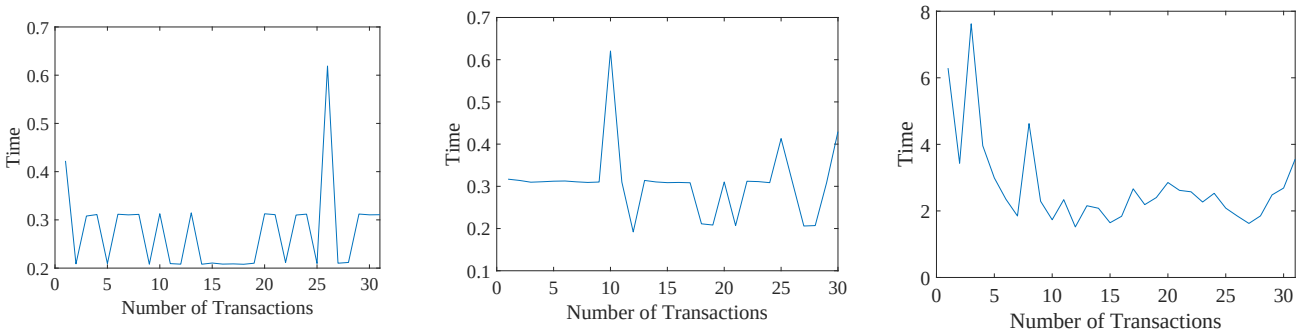
	Time	Temperature	MAC	PUF	hash	id
	Filter	Filter	Filter	Filter	Filter	Filter
28	'1644686449.9660056'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	b38f4e2c81e0351546d2acd389644b2e87...	ab884ea51eac38cd7d5603c08630cbf0545...
29	'1644686593.6336515'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	d3f44a110cd592d483c41ac1ecddebdce0e...	b38f4e2c81e0351546d2acd389644b2e87...
30	'1644686603.9765272'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	0882092393b4ae5eb9ce15dd01e6773bea...	d3f44a110cd592d483c41ac1ecddebdce0e...
31	'1644686614.4211583'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	6e28f0f930495f2510ad2e5fade3be8207f1...	0882092393b4ae5eb9ce15dd01e6773bea...
32	'1644686624.865872'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	de6b884ba48915127ef8ec59d0eb903e2cf...	6e28f0f930495f2510ad2e5fade3be8207f1...
33	'1644686645.9601705'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	62d4069859edfa3713be78b94507fbf2b6b...	de6b884ba48915127ef8ec59d0eb903e2cf...
34	'1644686656.4047632'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...	62d4069859edfa3713be78b94507fbf2b6b...
35	'1644686666.849594'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	ae28a86fca44f7898ee0a64c25d84fffcc6b...	80eb16b5f1f5f59097dffeb6c2c9800058c0f...
36	'1644686677.294728'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...	ae28a86fca44f7898ee0a64c25d84fffcc6b...
37	'1644686687.739273'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...	28a4d2ea2e6d05bb5550b29e86f1d2eca9...
38	'1644686708.6280165'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	f14b596a9741684cd42137569afb9cc9ffa9...	5e64d348f57353e92d2aa9ef09e2d3cd9b3...
39	'1644686719.0736935'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	70b906e51c0d0eb9174c0438e320365440...	f14b596a9741684cd42137569afb9cc9ffa9...
40	'1644686841.1356113'	'23.5'	dc:a6:32:c8:d7:50	'1000001110000011100000111000001111...	b318c9a9c5d6ae591ac48d37e57d40fcbc1...	70b906e51c0d0eb9174c0438e320365440...

(c) Blockchain at 2nd Client.

Fig. 13: Output of the proposed Blockchain PUFchain 2.0.

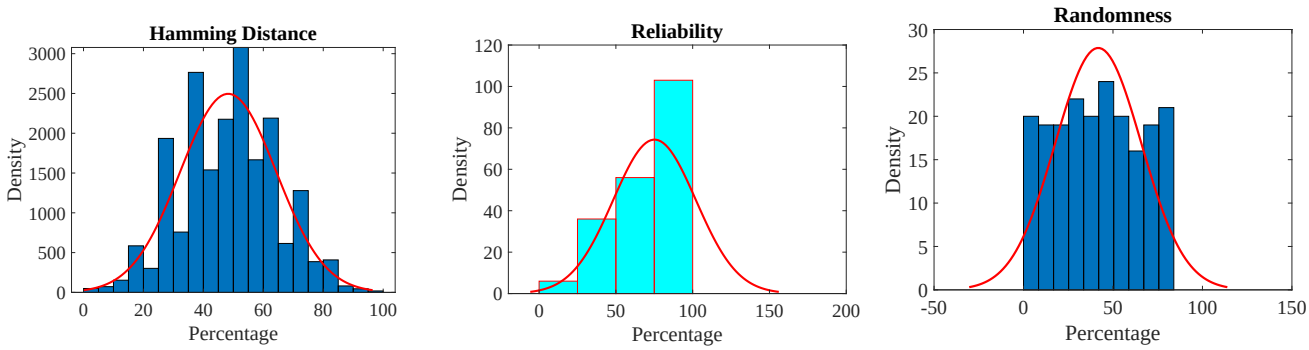
References

1. Asif, R., Ghanem, K., Irvine, J.: Proof-of-puf enabled blockchain: Concurrent data and device security for internet-of-energy. Sensors **21**(1) (2021). DOI 10.3390/s21010028. URL https://www.mdpi.com/1424-8220/21/1/28
2. Baker, S.B., Xiang, W., Atkinson, I.: Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access **5**, 26521–26544 (2017). DOI 10.1109/ACCESS.2017.2775180
3. Bui, F.M., Hatzinakos, D.: Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling. EURASIP Journal on Advances in Signal Processing **2008**(1) (2007). DOI 10.1155/2008/529879
4. Camara, C., Peris-Lopez, P., Tapiador, J.E.: Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics **55**, 272–289 (2015). DOI https://doi.org/10.1016/j.jbi.2015.04.007
5. Du, X., Chen, B., Ma, M., Zhang, Y.: Research on the application of blockchain in smart healthcare: Constructing a hierarchical framework. Journal of Healthcare Engineering



(a) 1st Client (b) 2nd Client (c) Miner

Fig. 14: Timing Analysis Results for PUFChain 2.0.



(a) Hamming_Distance (b) Reliability (c) Randomness

Fig. 15: A Selected metrics for PUFchain 2.0 Characterization.

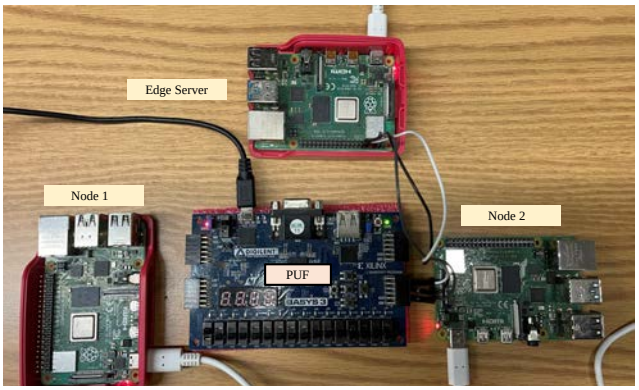


Fig. 16: Experimental Setup for PUFchain 2.0 prototyping and validation.

2021, 1–13 (2021). DOI 10.1155/2021/6698122

6. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for iot. Sensors **19**(2) (2019). DOI 10.3390/s19020326. URL https://www.mdpi.com/1424-8220/19/2/326
7. Fitzmaurice, J.: Telehealth research and evaluation: implications for decision makers. In: Proceedings Pacific Medical Technology Symposium-PACMEDTek. Transcending Time, Distance and Structural Barriers (Cat. No.98EX211), pp. 344–352 (1998). DOI 10.1109/PACMED.1998.769954
8. 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 (2021). DOI 10.1109/JIOT.2020.3045653
9. Joshi, A.M., Jain, P., Mohanty, S.P.: Secure-iglu: A secure device for noninvasive glucose measurement and automatic insulin delivery in iomt framework. In: 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 440–445 (2020). DOI 10.1109/ISVLSI49217.2020.00-17
10. Joshi, S., Mohanty, S., Kougianos, E.: Everything you wanted to know about pufs. IEEE Potentials **36**, 38–46 (2017). DOI 10.1109/MPOT.2015.2490261
11. Kelly, J.T., Campbell, K.L., Gong, E., Scuffham, P.: The internet of things: Impact and implications for health care delivery. J Med Internet Res **22**(11), e20135 (2020). DOI 10.2196/20135. URL http://www.jmir.org/2020/11/e20135/
12. Khezr, S., Moniruzzaman, M., Yassine, A., Benlamri, R.: Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences **9**, 1736 (2019). DOI 10.3390/app9091736
13. Khujamatov, K., Reypnazarov, E., Akhmedov, N., Khasanov, D.: Blockchain for 5g healthcare architecture. In: 2020 International Conference on Information Science and Communications Technologies (ICISCT), pp. 1–5 (2020). DOI 10.1109/ICISCT50599.2020.9351398
14. Kim, B., Yoon, S., Kang, Y., Choi, D.: Puf based iot device authentication scheme. In: 2019 International

Conference on Information and Communication Technology Convergence (ICTC), pp. 1460–1462 (2019). DOI 10.1109/ICTC46691.2019.8939751
15. Kim, C., Kim, H.J.: A study on healthcare supply chain management efficiency: using bootstrap data envelopment analysis. Health Care Management Science **22**(3), 534–548 (2019). DOI 10.1007/s10729-019-09471-7
16. Kumar, M., Rani, R.: Sai-ba-iomt: Secure ai-based blockchain-assisted internet of medical things tool to moderate the outbreak of covid-19 crisis. arXiv preprint arXiv:2108.09539 (2021)
17. Labrado, C., Thapliyal, H., Mohanty, S.P.: Fortifying vehicular security through low overhead physically unclonable functions. ArXiv **abs/2106.02976** (2022)
18. Lindqvist, J., Liimatainen, S., Katajamaki, T.: Secure pairing architecture for wireless mobile devices. In: 2006 IEEE 63rd Vehicular Technology Conference, vol. 2, pp. 823–827 (2006). DOI 10.1109/VETECS.2006.1682939
19. Lupton, D., Maslen, S.: Telemedicine and the senses: a review. Sociology of Health & Illness **39**(8), 1557–1571 (2017). DOI 10.1111/1467-9566.12617
20. Masud, M., Gaba, G.S., Alqahtani, S., Muhammad, G., Gupta, B.B., Kumar, P., Ghoneim, A.: A lightweight and robust secure key establishment protocol for internet of medical things in covid-19 patients care. IEEE Internet of Things Journal **8**(21), 15694–15703 (2021). DOI 10.1109/JIOT.2020.3047662
21. Mohanty, S.P., Yanambaka, V.P., Kougianos, E., Puthal, D.: Pufchain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (ioe). IEEE Consumer Electronics Magazine **9**(2), 8–16 (2020). DOI 10.1109/MCE.2019.2953758
22. Mushtaq, M., Shah, M.A., Ghafoor, A.: The internet of medical things (iomt): Security threats and issues affecting digital economy. In: Competitive Advantage in the Digital Economy (CADE 2021), vol. 2021, pp. 137–142 (2021). DOI 10.1049/icp.2021.2420
23. Naren, N., Chamola, V., Baitragunta, S., Chintanpalli, A., Mishra, P., Yenuganti, S., Guizani, M.: Iomt and dnn-enabled drone-assisted covid-19 screening and detection framework for rural areas. IEEE Internet of Things Magazine **4**(2), 4–9 (2021). DOI 10.1109/IOTM.0011.2100053
24. Olokodana, I.L., Mohanty, S.P., Kougianos, E., Sherratt, R.S.: Ezcap: A novel wearable for real-time automated seizure detection from eeg signals. IEEE Transactions on Consumer Electronics **67**(2), 166–175 (2021). DOI 10.1109/TCE.2021.3079399
25. Puthal, D., Malik, N., Mohanty, S., Kougianos, E., Das, G.: Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine **7**, 6–14 (2018). DOI 10.1109/MCE.2018.2816299
26. Puthal, D., Mohanty, S.: Proof of authentication: Iot-friendly blockchains. IEEE Potentials **38**, 26–29 (2019). DOI 10.1109/MPOT.2018.2850541
27. Rachakonda, L., Bapatla, A.K., Mohanty, S.P., Kougianos, E.: Sayopillow: A blockchain-enabled, privacy-assured framework for stress detection, prediction and control considering sleeping habits in the iomt. ArXiv **abs/2007.07377** (2020)
28. Rachakonda, L., Kothari, A., Mohanty, S.P., Kougianos, E., Ganapathiraju, M.K.: Stress-log: An iot-based smart system to monitor stress-eating. 2019 IEEE International Conference on Consumer Electronics (ICCE) pp. 1–6 (2019)
29. Rachakonda, L., Rajkumar, P., Mohanty, S.P., Kougianos, E.: imirror: A smart mirror for stress detection in the iomt framework for advancements in smart cities. In: 2020 IEEE International Smart Cities Conference (ISC2), pp. 1–7 (2020). DOI 10.1109/ISC251055.2020.9239081
30. Santhosh, E., Pradhan, A., Badarla, V., Mohanty, S.: Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet of Things Journal **PP**, 1–1 (2021). DOI 10.1109/JIOT.2021.3058946
31. Sethi, P., Sarangi, S.: Internet of things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering **2017**, 1–25 (2017). DOI 10.1155/2017/9324035
32. Sethuraman, S.C., Kompally, P., Mohanty, S.P., Choppali, U.: Mywear: A novel smart garment for automatic continuous vital monitoring. IEEE Transactions on Consumer Electronics **67**(3), 214–222 (2021). DOI 10.1109/TCE.2021.3085888
33. Tariq, N., Qamar, A., Khan, F.: Blockchain and smart healthcare security: A survey. Procedia Computer Science **175**, 615–620 (2020). DOI 10.1016/j.procs.2020.07.089
34. Webster, J.G., et al.: Design of cardiac pacemakers. IEEE New York, NY (1995)
35. Yanambaka, V., Mohanty, S., Kougianos, E., Puthal, D., Rachakonda, L.: Pmsec: Puf-based energy-efficient authentication of devices in the internet of medical things (iomt). In: 2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 320–321 (2019). DOI 10.1109/iSES47678.2019.00079
36. Yanambaka, V.P., Abdelgawad, A., Yelamarthi, K.: Pim: A puf-based host tracking protocol for privacy aware contact tracing in crowded areas. IEEE Consumer Electronics Magazine **10**(4), 90–98 (2021). DOI 10.1109/MCE.2021.3065215
37. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Making use of semiconductor manufacturing process variations: FinFET-based physical unclonable functions for efficient security integration in the IoT. Analog Integrated Circuits and Signal Processing **93**(3), 429–441 (2017). DOI 10.1007/s10470-017-1053-9
38. Yoon, S., Kim, B., Kang, Y., Choi, D.: Puf-based authentication scheme for iot devices. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1792–1794 (2020). DOI 10.1109/ICTC49870.2020.9289260