PMsec 2.0: A Security-By-Design Solution for Doctor's Dilemma Problem in Smart Healthcare

Venkata K. V. V. Bathalapalli
Dept. of Computer Science and Engineering
University of North Texas.
Email: vb0194@unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas.
Email: saraju.mohanty@unt.edu

Elias Kougianos
Electrical Engineering
University of North Texas.
Email: elias.kougianos@unt.edu

Vasanth Iyer
Computer Science and Digital Technologies
Grambling State University.
Email: iyerv@gram.edu

Bibhudutta Rout
Dept. of Physics
University of North Texas.
Email: bibhudutta.rout@unt.edu

***Abstract*—The rapid adoption of Internet-of-Medical-Things (IoMT) has revolutionized e-health systems, particularly in remote patient monitoring. With the growing adoption of Internet-of-Medical-Things (IoMT) in delivering technologically advanced health services, the security of Medtronic devices is pivotal as the security and privacy of data from these devices are directly related to patient safety. PUF has been the most widely adopted hardware security primitive which has been successfully integrated with various Internet-of-Things (IoT) based applications, particularly in smart healthcare for facilitating device security. To facilitate security and access control to IoMT devices, this work proposes a novel cybersecurity solution using PUF for facilitating global access to IoMT devices. The proposed framework presents an approach that enables the patient's body area network devices supported by PUF to be securely accessible and controllable globally. The proposed cybersecurity solution has been experimentally validated using state-of-the-art SRAM PUF, a delay based PUF, and a trusted platform module (TPM) primitive.**

***Index Terms*—Internet-of-Medical-Things (IoMT); Cybersecurity; Security-by-Design (SbD); Physical Unclonable Functions (PUF); Trusted Platform Module (TPM)**

I. Introduction

The evolution of Telemedicine, e-Health, and m-Health for delivering sophisticated medical services is being made possible through the application of IoMT devices. These smart Medtronic devices facilitate physiological data sensing and collection. However, openly accessible IoMT devices can be maliciously tampered with and controlled easily thereby enabling adversaries to control Medtronic devices on patients. Implementation of cryptographic security schemes has proven to be unreliable due to the requirement of non-volatile memory for storing the secret keys which again can be vulnerable to various kinds of advanced security attacks [1], [2]. Security-by-Design (SbD) is a novel phenomenon that emphasizes integrating security and privacy primitives at the design stage of a consumer electronics system. The objective of SbD is ensuring the security of smart electronics systems with security/privacy primitive as functionality enabled by default in its working [3]. It also specifies that security/privacy specifications should not be complicated and must be understandable for the ease of use of a consumer electronic system.

PUF has been a prominent hardware SbD primitive that uses device unique properties and generates a cryptographic identity and has most widely been used for IoMT security. Existing PUF-based device authentication protocols mostly work based on an approach where a server authenticates a PUF-embedded IoMT device by extracting the PUF key and performing a comparison to verify its identity [4]. This sort of approach often falls short when IoMT devices are part of a Global Smart Health system where different hospital networks around the globe must remotely access and authenticate the IoMT devices on the patient's body area network [5]. To address this issue, the proposed work presents a novel remote device authentication mechanism to facilitate access control to the PUF-embedded IoMT devices. A broad picture of the proposed cybersecurity solution in smart healthcare is given in Fig. 1.

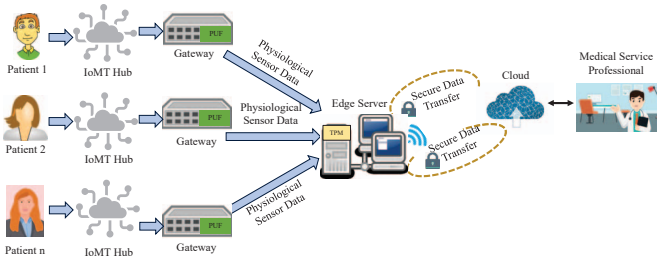


Fig. 1: Broad Picture of Proposed Cybersecurity Solution for IoMT.

The proposed framework works on facilitating access control to PUF embedded devices remotely for secure authentication. TPM is another SbD primitive like PUF which is a hardware secure cryptoprocessor that supports various applications in cryptographic key generation, storage, remote

979-8-3503-5823-0/23/$31.00 ©2023 IEEE

attestation, and in facilitating security for computing systems through secure boot process [6], [7]. It is a simple chip from the Trust Computing Group (TCG) and is a prominent security primitive that helps in IoT based applications. The proposed architecture aims to explore the scope of integrating PUF and TPM SbD primitives using TPM's remote attestation scheme and PUF key verification. This protocol can facilitate the PUF embedded IoMT device to be securely accessed for authentication by a remote entity. TPM's remote attestation mechanism can be used to verify the integrity of healthcare systems accessing patient's PUF embedded sensors [8], [9].

The rest of the paper is organized in the following manner: Section II presents the novel contributions of the current paper. Section III discusses the existing works on PUF based access control primitives in IoMT. Section IV presents a comprehensive overview of the proposed SbD for facilitating global access control to authenticate PUF embedded IoMT. Experimental validation of the proposed work has been presented in Section V outlines the implementation details. Section VI presents the conclusion and directions for future research.

II. Novel Cointributions of the Current Paper

A. Problem Statement

Verifying the integrity of IoMT devices through PUF key extraction and verification schemes is often done by the embedding of PUF based security solutions with low power IoMT devices. However, the low computational and resource constrained smart health electronic devices cannot harness the potential of PUF if the security solution is resource intensive. Also, the question of how the PUF can be embedded into Implantable electronic devices like pacemakers and how the key is extracted and verified remains unanswered. If the PUF is really integrated inside IoMT devices, the impact of adding a security layer to devices like pacemakers can impact its performance and reduce its battery efficiency where the average battery life is around 8-10 years. When a patient moves to a different location and would like to access healthcare from different hospital networks, how is the communication established between the new hospital network and the patient's body area network which consists of Medtronic devices inside or on the patient as illustrated in the Fig. 2 is the question which we would like to address in this work.

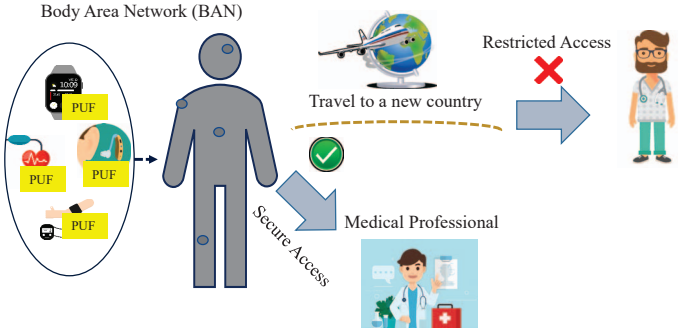


Fig. 2: Doctor's Dilemma Problem.

B. Proposed Solution

The motive of this work is to facilitate access to Medtronic devices embedded with PUF securely in such a way that the patient could access health care services even when traveling to a different part of the world. For instance, the pacemaker or insulin pump embedded inside the patient could be accessed securely by any hospital around the world with minimal performance tradeoffs. This work aims to present an approach where the devices need not be embedded with PUF but could obtain a unique PUF identity securely without having it embedded. This approach could simplify utilization and facilitate secure access to IoMT devices by enabling a TPM embedded solution that works on verifying the integrity of an entity remotely where each server or cloud communicating with these devices has a unique security feature supported by TPM.

C. Novelties of the proposed work PMsec 2.0

The novel contributions of the proposed work PMsec 2.0 include the following:

1) A novel cybersecurity approach in Smart Healthcare that facilitates the PUF embedded IoMT devices to be accessed globally.
2) An authentication mechanism that does not require devices in the patient's body area network to typically have PUF embedded but can obtain a unique PUF generated identity from the central PUF module remotely.
3) Evaluating the scope of the proposed security scheme through the integration of PUF and TPM.
4) A vibrant security scheme involving multiple levels of authentication for enabling access to core device PUF key.
5) Using TPM's remote attestation scheme for verifying the integrity of the Edge server in the proposed edge computing driven cybersecurity solution.

III. Related Prior Research

In this Section, we have presented a comprehensive overview of state-of-the-art research on PUF based security primitives in IoMT and IoT.

A PUF based privacy preserving scheme for telecare medical information systems has been presented in [10]. This work performs secure edge device and gateway registration in IoMT using a biometric and password verification scheme and verifies the effectiveness of this scheme by testing it against various security attacks. To ensure effective data integrity, access control, and transparency, a robust Blockchain integrated PUF based approach is proposed in [11]. This work performs the integration of smart contracts with PUF and presents a hybrid security mechanism for IoMT security.

A client server model for PUF key verification in IoMT has been presented in [1], [2]. This work uses PUF key verification, hash generation, and a comparison approach to effectively counter security vulnerabilities. A mutual authentication scheme for wireless body area networks proposed in [12], presents an approach for PUF based security to IoMT devices and works on establishing a mutual authentication

session between edge devices on patients and communicating gateway nodes.

PUF and Elliptic curve cryptography based IoMT device authentication mechanism is proposed in [13]. A lightweight XOR, hash function, and PUF have been used for validating the proposed approach in the fog computing platform and work in consortium Blockchain. To obtain privacy and confidentiality of sensor data in IoMT, authors in [14] proposed a Blockchain based user privacy preserving and authentication scheme using biometrics and signature. The authors claim that this work can facilitate secure authentication of users in mobile edge computing environments for IoMT.

Authors in [15] proposed a lightweight PUF-based Wi-Fi authentication protocol that works on improving the effectiveness of Wi-Fi protocol with PUF for secure session establishment. A random number generator has also been used for generating a seed for establishing communication and presents an approach for secure communication between IoT devices and Wi-Fi routers.

We have proposed the state-of-the-art integration of PUF with TPM in [5] for IoT security where we integrated PUF with TPMs NVRAM and securely uploaded the data in Tangle DLT. In [16], a Blockchain based remote attestation framework was presented which works by sharing the TPM's platform integrity details through shared Blockchain. Authors in [17], presented a PUF based blockchain consensus mechanism for IoMT security where a two level authentication mechanism is proposed for remotely verifying IoMT device integrity.

In comparison to the above cited works, the proposed PMsec 2.0 work presented a device authentication mechanism that works on globally accessing PUF embedded IoMT devices and performing PUF key verification and platform integrity validation of edge and cloud using TPM. This work also presents a start-of-art integration of PUF and TPM which can be a potential solution for cybersecurity in smart healthcare.

IV. Proposed Authentication Protocol: PMsec 2.0

This Section illustrates the vision of the proposed security mechanism and explains how the proposed scheme could be integrated with the architecture of IoMT. It also outlines how the PUF is accessed remotely through a global access control mechanism.

A. Architecture of proposed security framework

The architecture of a smart healthcare framework includes smart health electronic devices (ED) embedded in the patient, edge gateway (EG) for obtaining the physiological sensor information which typically connects the hub of ED on a patient, cloud for analysis, and DLT for securely storing the information. The proposed framework works by providing a unique identity to each one of the devices on the patient through the PUF. EG securely establishes an authentication session for obtaining information from these devices using the PUF generated cryptographic identities. Simply, a patient with an embedded ED can travel to a different location, and a new medical service provider (MSP) can securely access the patient's ED and verify its PUF generated identity by establishing a secure session with the patient's EG.

PUF module is typically embedded with EG and all the ED on the patient can securely obtain a unique PUF generated identity. This can reduce the overhead on low power ED and can smoothen the process of device authentication. Each ED can be enrolled by obtaining a unique PUF identity tied to its device properties such as media access control address (MAC). A unique PUF generated key for EG can act as its identity for establishing communication with the Edge server or cloud for data storage and analysis. EG's PUF key can act as a session key for authentication sessions between the Edge server and EG thereby server can access individual ED on patients through the gateway and perform its PUF key validation.

B. PUF based IoMT device security

The proposed authentication protocol works by providing a hardware generated cryptographic identity for a hub of ED. A patient with ED can obtain a PUF identity for each ED where the EG of the patient has complete access and control which is embedded with a PUF. The Edge server, which is also a secure entity with a supported TPM can access a group of EG's and their PUFs to validate and verify their integrity. Once EG's integrity is verified, the ES can access the hub through EG's verified identity and can verify the IoMT device identity individually and access it.

1) ***Device and Gateway Enrollment Phase in PMsec 2.0*** For enrolling in the IoMT hub, the PUF module at EG is tested with various challenge-response pairs. Challenge Response pairs (CRP) are tested and evaluated for PUF metrics and CRPs satisfying requirements are selected and assigned to each individual ED and sealed to their MAC. EG with embedded PUF obtains a unique PUF key for securely establishing a session with ES for securely transmitting data. The unique key used in session establishment acts as the identity of EG. The process of enrollment is clearly illustrated stepwise in Algorithm 1.
2) ***PUF enabled Authentication Phase in PMsec 2.0*** Each Edge server or Cloud working to access a device in the hub of the patient's body area network initially establishes a session with the corresponding EG and verifies its authenticity. The ES, after successfully verifying the integrity of EG can obtain access to the patient's body network and verify the integrity of each device's PUF-generated identity. Once a particular ES obtains access to a patient's hub, the corresponding transaction is recorded and shared across the network of clients (MSP). The steps involved in the authentication phase are explained in Algorithm 2.
3) ***Remote Attestation Phase in PMsec 2.0***

   Each ES with a TPM can authenticate another ES mutually by sharing platform integrity credentials. This could be done by generating a quote that contains details

of integrity credentials and transmitting it to another ES for verification. This can facilitate the secure exchange of patient data with ES globally. The generated Quote contains TPM's platform configuration register (PCR) values which are hash values of platform integrity parameters that can be TPM's unique credentials pertaining to a system and are consolidated in a Quote which can be shared with other systems for verification. The quote is generated by TPM's unique Endorsement and Attestation identity keys (AIK) which are RSA keys and are unique identities for a TPM. A broad overview of the proposed PMsec 2.0 scheme is presented in Fig. 3.

Algorithm 1 Enrollment Phase in PMsec 2.0.

Input: PUF CRP's
Output: Unique PUF identity for each device.
1: **for** N number of devices **do**
2: Access PUF Module and extract PUF Keys at and EG
Challenge $C \rightarrow$ *PUF Module* $\rightarrow$ *Response* R
3: Test PUF CRPs
4: Receive enrollment MAC of device MAC_{ED}
5: Assign a unique PUF key for each MAC PUF_{ED}
6: Store MAC and corresponding challenge for each device in the hub inside a secure database
7: Extract unique PUF key for EG PUF_{REG}
8: Enroll
9: **end for**

Algorithm 2 Authentication and quote generation Phase in PMsec 2.0.

Input: Secure session between ES and EG
Output: access to ED hub
1: Access PUF Module and extract PUF Key for ES
$C_{ES} \rightarrow PUF_{ES} \rightarrow R_{ES}$
2: Receive EG's Identity
$R_{EG} \rightarrow$ ES
3: **if** R_{EG} == $R_{EG'}$ **then**
4: EG is authenticated
5: **end if**
6: Obtain patient's hub ID
1) Unique PUF key for each hub generated at EG
2) $EG \rightarrow PUF_{PID}$
7: Verify individual ED's PUF key from the hub
8: **if** PUF_{ED}==$PUF_{ED'}$ **then**
9: ED is verified
10: **end if**
11: ES records transactions in a secure database
12: ES accesses TPM
- $ES \rightarrow TPM$
- Obtain EK and AIK
- Access PCR values (SHA-1, and SHA-256)
- Generate Quote

13: Broadcasts it to global hospital networks or MSPs

V. Experimental Results

For experimental evaluation, Arbiter PUF has been tested on Basys 3 FPGA (xc7a35tcpg236-1) from Digilent. For validating TPM, a Geek Pi TPM 2.0 module with Infineon Optiga SLB 9670 System-on-Chip (SoC) is interfaced with a Raspberry Pi 4 board. SRAM PUF has been implemented on the OKdo E1 development board from nxp semiconductors and the board has been programmed on MCUXpresso IDEv11.6.0_8187. The experimental setup and prototype evaluation have been presented in Fig. 4, Table I, and II.

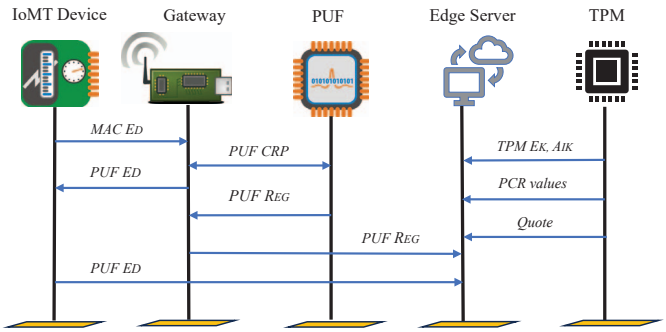


Fig. 3: PMsec 2.0 Security Primitive.

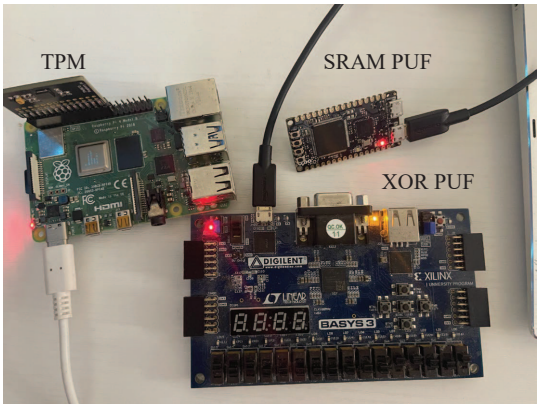
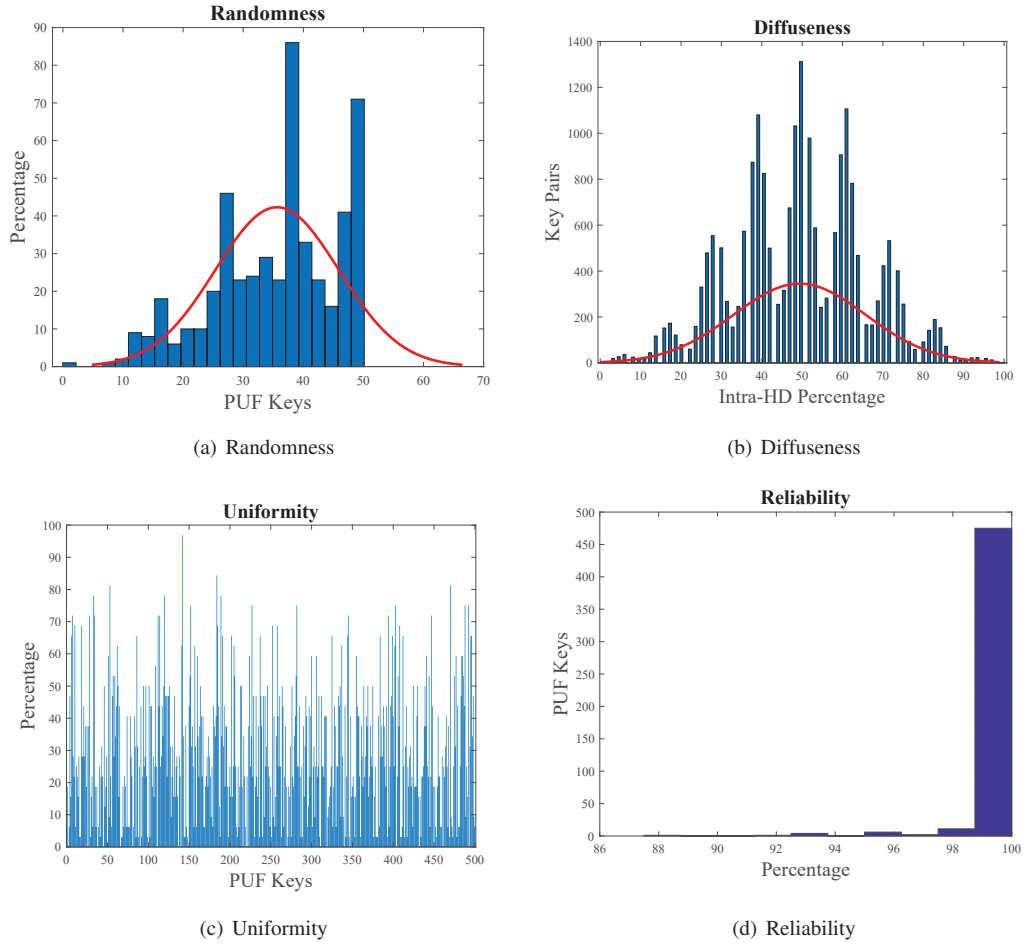


Fig. 4: Experimental Setup.

The Okdo E1 board is connected serially to the system with an Intel Core i7 2.8 GHz processor using Putty. A baud rate of 115200 has been used for enrolling and activating the SRAM PUF key from the board after successfully debugging the code obtained from the repository [18] onto the board. XOR PUF is used as EG PUF for securely extracting PUF keys. A group of 500 PUF keys from Basys-3 FPGA board has been extracted and PUF metrics have been evaluated, Intra-HD of approximately 49% has been achieved, and reliability of 500 keys was evaluated for 4 times and 100% approximately is achieved which is essential as the reliable PUF key is essential for successful authentication. Diffuseness, uniformity, and randomness have also been evaluated and the Fig. 5 presents the figure-of-merits of XOR PUF.

Raspberry Pi 4 boards are used as an edge device and gateway. MAC address based PUF-based identity generation was done on pi as a gateway with an average power consumption of 3-3.3 watts. Experimental validation results of the proposed authentication scheme have been presented in Fig. 6.



(a) Randomness

(b) Diffuseness

(c) Uniformity

(d) Reliability

Fig. 5: PUF Metrics.

TABLE I: Evaluation of PMsec 2.0

Parameters	Details
Application	Smart Healthcare
Security Mechanism	PUF-based global access control
Computing	Edge-Cloud
PUF Modules	SRAM PUF, XOR PUF
TPM	Pi-based TPM (Geek Pi TPM 2.0)
Scheme	Remote Attestation

TABLE II: Experimental Analysis of PMsec 2.0

Primitive	Metrics	Results
PUF	XOR PUF On-Chip power	0.081W
	SRAM PUF Key Code	32-byte
	Key Extraction Time	77ms
	XOR PUF Reliability(25^0C)	99.80%
	Validation Time	1.1s
TPM	PCR	16-23
	Non-Volatile memory storage	768 Bytes
	Pi-TPM Power Consumption Range	2.9-3.3W

VI. Conclusion and Future Research

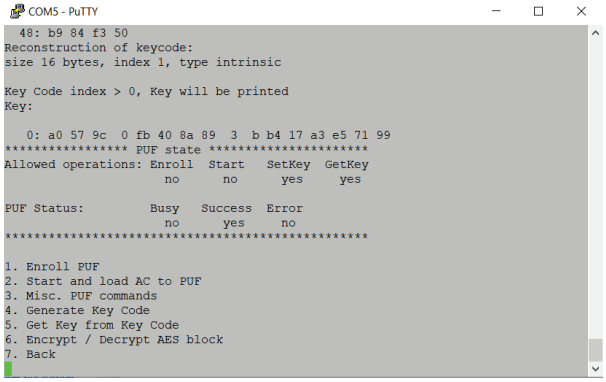
This work has successfully presented and validated a global access control framework to access and control PUF embedded IoMT devices. A novel PUF and TPM supported authentication scheme that verifies the integrity of devices in the proposed PUF driven cybersecurity scheme for IoMT truly substantiates the potential of the proposed cybersecurity solution in e-health, and telehealth ecosystems. As a direction for future research, a distributed ledger technology integration can be proposed for securely accessing data among different healthcare systems around the world.

References

[1] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," *IEEE Trans. Consumer Electron.*, vol. 65, no. 3, pp. 388–397, 2019. [Online]. Available: https://doi.org/10.1109/TCE.2019.2926192

[2] V. Yanambaka, S. Mohanty, E. Kougianos, D. Puthal, and L. Rachakonda, "PMsec: PUF-based energy-efficient authentication of devices in the internet of medical things (IoMT)," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, December 2019, pp. 320–321. [Online]. Available: http://dx.doi.org/10.1109/iSES47678.2019.00079

(a) Sample TPM Remote attestation quote



(b) SRAM PUF generated Key

(c) MAC Address based PUF generated identity

Fig. 6: Experimental validation.

[3] S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, March 2020. [Online]. Available: https://doi.org/10.1109/MCE.2019.2954959

[4] A. M. Joshi, P. Jain, and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework," in *Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2020, pp. 440–445. [Online]. Available: https://doi.org/10.1109/ISVLSI49217.2020.00-17

[5] V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer, and B. Rout, "PUFchain 4.0: Integrating PUF-Based TPM in Distributed Ledger for Security-by-Design of IoT," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, 2023, p. 231–236. [Online]. Available: https://doi.org/10.1145/3583781.3590206

[6] D. Fu and X. Peng, "TPM-based remote attestation for Wireless Sensor Networks," *Tsinghua Science and Technology*, vol. 21, no. 3, pp. 312–321, June 2016. [Online]. Available: https://doi.org/10.1109/TST.2016.7488742

[7] Z. Xiaojian, W. Qi, L. Xin, Y. Qigui, and X. Min, "A Bidirectional Remote Attestation Method for Electricity 5G Edge Computing Nodes," in *Proc.7th International Conference on Signal and Image Processing (ICSIP)*, July 2022, pp. 713–718. [Online]. Available: https://doi.org/10.1109/ICSIP55141.2022.9886749

[8] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, June 2022. [Online]. Available: https://doi.org/10.1109/JIOT.2021.3117762

[9] F. Zerrouki, S. Ouchani, and H. Bouarfa, "PUF-based mutual authentication and session key establishment protocol for IoT devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 9, pp. 12 575–12 593, August 2022. [Online]. Available: https://doi.org/10.1007/s12652-022-04321-x

[10] S. Yu and K. Park, "PUF-PSS: A Physically Secure Privacy-Preserving Scheme Using PUF for IoMT-Enabled TMIS," *Electronics*, vol. 11, no. 19, p. 3081, Sepember 2022. [Online]. Available: http://dx.doi.org/10.3390/electronics11193081

[11] S. Yu and Y. Park, "A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20 214–20 228, October 2022. [Online]. Available: http://dx.doi.org/10.1109/JIOT.2022.3171791

[12] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF)," in *Proc. 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2013, pp. 1314–1318. [Online]. Available: https://doi.org/10.1109/IWCMC.2013.6583746

[13] X. Jia, M. Luo, H. Wang, J. Shen, and D. He, "A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21 838–21 850, November 2022. [Online]. Available: https://doi.org/10.1109/JIOT.2022.3181609

[14] Y. Zhang, B. Li, G. Liu, and Y. Li, "Privacy-Preserving Blockchain-based User Authentication with Device Group Authorization for Mobile Edge Computing," in *Proc. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, November 2022, pp. 990–996. [Online]. Available: http://dx.doi.org/10.1109/ICCCIS56430.2022.10037738

[15] M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, "A PUF based Light Weight Protocol for Secure WiFi Authentication of IoT devices," in *Proc. 8th International Symposium on Embedded Computing and System Design (ISED)*, December 2018, pp. 183–187. [Online]. Available: https://doi.org/10.1109/ISED.2018.8703993

[16] I. R. Jenkins and S. W. Smith, "Distributed IoT Attestation via Blockchain," in *Proc. 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)*, May 2020, pp. 798–801. [Online]. Available: https://doi.org/10.1109/CCGrid49817.2020.000-7

[17] V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, B. K. Baniya, and B. Rout, "PUFchain 2.0: Hardware-Assisted Robust Blockchain for Sustainable Simultaneous Device and Data Security in Smart Healthcare," *SN Computer Science*, vol. 3, no. 5, June 2022. [Online]. Available: https://doi.org/10.1007/s42979-022-01238-2

[18] Last Accessed on 15 Oct 2023. [Online]. Available: https://github.com/asvin-io/asvin-tutorials/tree/main/PUFdemo