RESEARCH PAPER

Experimental Review of PUF-based Security for IoMT Devices against MitM Attacks

Agila Harshini T[1], Harini Sriraman[2*]

[1]Department of Computer Science and Engineering, Vellore Institute of Technology – Chennai, Tamil Nadu, India.

[2*]Department of Computer Science and Engineering, Vellore Institute of Technology – Chennai, Tamil Nadu, India.

Corresponding Author
Harini Sriraman
Email ID : harini.s@vit.ac.in

ABSTRACT

The Internet of Medical Things (IoMT) driven by numerous factors, is growing at a faster pace, including technological advancements, the burden of chronic diseases, and rising demand for remote healthcare. The outcome of this demand raises privacy and security issues in digital healthcare. In the healthcare industry, where critical tasks are performed using IoMT devices, security is a major concern due to the risk of various attacks associated with these devices. As IoMT devices are resource-constrained, a secure and energy-efficient security solution is an integral need. In recent times, the use of PUF (Physically Unclonable Functions) in IoT architecture and their potential to address security vulnerabilities are gaining popularity. In this work applicability of PUF for IoMT security scenarios is thoroughly studied. A demonstration to prove the resilience of PUF-based security mechanisms, in terms of confidentiality, integrity, and energy efficiency for healthcare scenarios employing IoMT devices, is provided. An Anderson PUF is implemented on an FPGA-based testbed. Its resilience against keylogger, password guessing, and ARP spoofing attacks is examined. The proposed PUF achieves 49.8 % uniqueness, 97.2 % reliability, and 49.5 % randomness, demonstrating strong resistance to machine learning attacks (maximum success probability ≈ 52 %).

Keywords: PUF security; Man-in-the-Middle attack; IoMT device

How to cite this article: Agila Harshini T, Harini Sriraman. Experimental Review of PUF-based Security for IoMT Devices against MitM Attacks. Int J Drug Deliv Technol. 2026;16(14s): 457-479. DOI: 10.25258/ijddt.16.14s.48

INTRODUCTION

IoMT devices:

Healthcare is revolutionized by incorporating advanced technologies in medical devices, providing personalized care. Wearable devices, such as smartwatches and fitness trackers, are among the most prevalent IoMT devices, enabling individuals to monitor their health metrics like heart rate, sleep patterns, and physical activity. Remote patient monitoring devices, including blood pressure monitors and glucose meters, facilitate real-time vital signs tracking, from longer distances without the physical presence of the patient by healthcare providers and give treatment promptly when needed. Implantable IoMT devices, such as pacemakers and insulin pumps, play a crucial role in managing chronic conditions by delivering personalized treatments and transmitting valuable data to healthcare professionals. Additionally, smart inhalers and medication adherence trackers enhance medication management, ensuring patients follow prescribed regimens. IoMT devices empower patients to monitor their health metrics and maintain a healthy lifestyle. It allows the doctors to track vitals and provide medication without the physical presence of the patient. Overall, IoMT devices contribute to a more connected and proactive approach to healthcare, promoting better patient outcomes and preventive care strategies.

Security Challenges in IoMT devices:

The vulnerabilities, such as weak encryption, poor access control in resource-constrained IoMT devices,

create exploitable gaps for attackers. Particularly, MitM attacks are dangerous, which makes the sensitive patient data insecure. Implementing a robust cryptographic security becomes difficult due to limited memory, processing power, and energy efficiency.

PUF security for IoMT devices:

A Physically Unclonable Function (PUF) is a security solution that uses the inherent randomness and unpredictability of physical manufacturing processes to generate unique "fingerprints" for each device that cannot be replicated. Traditional cryptographic methods store keys in memory, PUF produces uniqueness based on physical variations that is impossible to replicate, reducing the attack surface. PUFs leverage the unique attributes of IoMT systems that can establish a reliable and resilient security framework, mitigating risks and ensuring the integrity of sensitive medical data. PUF evades memory storage of keys. Various security solutions utilizing PUFs are employed to secure medical devices; however, they remain vulnerable to threats due to aging, temperature variations, and invasive attacks.

The major contributions of this work:

- A detailed analysis of vulnerabilities in IoMT devices, selectively focusing on the risk of Man-in-the-Middle attacks, is presented.
- Proposed the use of PUF as a lightweight security mechanism for IoMT devices, eliminating the need for cryptographic key storage in memory.
- An Anderson PUF implemented on an FPGA is experimentally validated against ARP spoofing, password guessing, and keylogger attacks, showing significant improvement in reducing MitM attack success rate.
- To enhance the security and machine learning attack resistance, the paper explores a hybrid PUF architecture.

Related Study:

The research contribution on security in IoMT devices is categorized into four major themes in Table 1. The work highlights how PUF-based primitives, lightweight cryptography, and system-level defences are developing the next generation of secure and energy-efficient IoMT frameworks.

Table 1 . Thematic classification of IoMT security with PUF integration

S.No	Theme & References	Techniques	Remarks
1	**Mutual Authentication & Key Management Protocols** 4, 5, 8, 10, 11, 12, 13, 14, 17, 18, 19, 21, 22, 23, 27, 37, 38, 40, 43, 54, 58, 61	- PUF-based secure communication protocols -Password-free authentication - Session key establishment - Blockchain-enabled authentication - Formal verification with BAN logic & AVISPA	These studies propose lightweight authentication frameworks where devices authenticate each other without heavy cryptography. PUF ensures device uniqueness, preventing cloning. Blockchain is used in some works for decentralized trust but adds computation overhead. Protocols are tested against replay, impersonation, and MITM attacks. Many achieve low latency and are suitable for constrained IoMT nodes.
2	**Hardware-Based Security & PUF Architectures** 7, 25, 26, 30, 34, 41, 47, 48, 49, 60	- Arbiter, XOR, Hybrid PUF designs - FPGA-intrinsic PUF implementations - Biometric-assisted PUFs (ECG/EEG fusion) - RAPUF and MRAM-based PUF	These works treat PUF as a hardware root-of-trust. Various architectures (Arbiter, XOR, Hybrid, RAPUF) are evaluated for uniqueness, randomness, and reliability. Biometric-PUF fusion enhances entropy and personalization. FPGA-based realizations prove practical deployability. Some papers focus on defending PUFs against ML modeling attacks, an important challenge for IoMT security.

		- Machine learning (ML) attack resilience	
3	**Lightweight Cryptography & Encryption for IoMT** 6, 24, 39, 43, 57	- Lightweight block ciphers (ASCON, obfuscated AES) - PUF-assisted encryption - NLFSR-based encryption - Homomorphic encryption for privacy-preserving medical data	These contributions design low-power encryption schemes tailored for IoMT's resource-limited nature. Ciphers like ASCON are NIST lightweight cryptography finalists, providing efficiency and security. Obfuscated AES and NLFSR + PUF encryption approaches combine hardware efficiency with unpredictability. Homomorphic encryption allows computation on encrypted medical data, but at a higher cost in performance.
4	**Surveys, Intrusion Detection & System-Level Security** 1, 2, 3, 9, 15, 16, 20, 28, 31, 32, 33, 35, 36, 42, 44, 45, 46, 50, 51, 52, 56, 59, 62	- Surveys on IoMT security - IDS (anomaly & ML-based) - Blockchain for medical data aggregation - Jamming & DoS attack classification - Ethical, privacy & regulatory challenges - PUF attack resilience	These works provide big-picture perspectives. Surveys outline IoMT vulnerabilities and countermeasures. IDS approaches detect real-time anomalies in medical networks, often using ML/AI. Blockchain is proposed for secure storage and data integrity, but may strain constrained devices. Some works focus on wireless jamming, DoS attacks, and energy-aware defenses. Ethical and regulatory challenges highlight the non-technical barriers in IoMT adoption.

The existing works explore PUF-based authentication protocols, hardware architectures, and lightweight encryption schemes, but they are limited to isolated hardware designs and protocol level solutions. These approaches come down with scalability changes, exposure to machine learning attacks, or high computational cost to be integrated with IoMT environment. The originality of this work lies in,

- ***Experimental validation on FPGA focused on MitM attacks:*** Implementing PUF design in hardware to show resilience against real-world attacks, where most of the work simulates or evaluates analytically.
- ***Hybrid PUF exploration with energy-efficient design:*** Instead of adopting a single PUF type, the paper highlights a combination of PUFs to enhance entropy, reliability, energy efficiency, and resistance.

MitM attacks on IoMT devices:

The inadequacy of legitimate security and data protection in healthcare data leaves individuals vulnerable to scams. Without satisfactory data protection, the digitization of healthcare is growing exponentially.

Attacks on IoMT devices on wearable devices for example in 2019, a fitness tracker company, though not publicly identified, suffered a data breach exposing millions of user records. The cause of the breach was attributed to a cloud storage misconfiguration. The details of personal information, health and fitness, and Data Location may be stolen. Another example of an attack on an implantable device happened in 2017, Unauthorized access to the devices was discovered in

pacemakers and defibrillators manufactured by Abbott (formerly St. Jude Medical), The vulnerability was found in the wireless communication protocol of the device which would have altered critical settings, deplete battery life, collect patient data. The attackers potentially exploited these weaknesses and gained unauthorized access to the devices remotely.

The protocols specifically used for IoMT devices are vulnerable to various attacks. Protocols lack strong encryption which leads to unauthorised access by attackers. The attacks are categorized by device-to-device, device-to-cloud, and device-to-edge gateway. In device-to-device, protocols like Bluetooth, WiFi, and Z-Wave are used. Attacks like sniffing, command injection, and impersonation are done to make the IoMT vulnerable because of the drawbacks in protocols like weak pairing, insecure inclusion, and easy device discovery. The device-to-cloud uses MQTT, LoRaWAN, and DDS protocols that are unencrypted, limited in the size of the network, or consume more bandwidth. These shortcomings grant illegal access to the attacker. Device-to-edge gateway connecting protocols, such as CoAP and UDP lack authentication and packet loss during transmission.

Different attack scenarios and the vulnerabilities on IoMT devices are provided in the following (Fig 1)

Methodology of Key generation by PUF-implemented FPGA:

In a cryptographic processor, confidential keys are housed in a non-volatile memory that is backed by a battery, making it vulnerable to potential attacks by adversaries. Furthermore, in resource-constrained IoT applications, including a cryptoprocessor for security increases the size and cost of the device. Physical Unclonable Function (PUF) generates the secret key instantly by leveraging the intrinsic manufacturing variations of the Integrated Circuit (IC). The PUF's input and output form a Challenge-Response Pair (CRP). A weak PUF requires a one-bit challenge or an enable signal to activate the PUF circuit and produce a 1-bit response. The PUF cell is replicated linearly to generate n unique response bits. The CRPs obtained from the PUF are exploited directly as secret keys without storing them in non-volatile memory. The keys yielded by the PUF cell are unique and specific to the IC on which it is embedded. The Anderson PUF (REF) is a weak PUF that incorporates a carry chain, Flip-Flop, and shift register in its cell design as shown in Fig.2. The output from the SRA and SRB is given as input to one of the multiplexers in the carry chain primitive. The significance of complementary input to shift register is to generate a delay by SRA, SRB and carry chain primitive. The necessary delay is introduced by correctly placing SRA and SRB in the SLICE M. The two carry chain primitives also increase the delay by their nature and provide a glitch in the output of the carry chain connected to SRA.

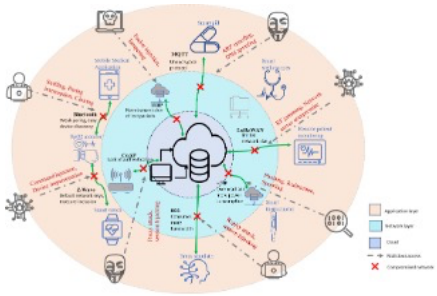

Fig. 1. MitM security threats on IoMT devices

This output is connected to the preset input of the Flip-Flop. The output of the Flip-Flop will be '1' if the preset input is high; otherwise, the output is '0'. The preset input's pulse width is highly significant in deciding the random response. Thus, the intrinsic Anderson PUF cells to produce a 32-bit response. The experimental results are validated by implementing the 32-bit Anderson PUF in 32 different areas of the SoC ZedBoard (28 nm). The Anderson PUF, being a weak PUF, is hard to model, and hence, it is robust against machine learning and mathematical modeling attacks. manufacturing variation of the IC results in different delays in the PUF cell in other SLICES. The FPGA fabric is partitioned into 32 parts to incorporate

Experimental procedure(Step-by-step*):*

Design and placement:

- Implement Anderson PUF cell (SRA, SRB)
- For SRA, SRB constrain each cell to SLICE M sites with complementary local routes
- Across the fabric, create 32 pblocks.

Activation timing:

- For every evaluation clear SRA,SRB and load complementary seeds, enable for one clock to launch transitions through carry chain.
- Sample FF output after a fixed time .

Data collection:

- Repeat Nrep evaluations at nominal PVT
- Store raw response bits per trail.

Stabilization and debiasing:

- Majority vote per bit over M rapid repeats to reduce transient flips.
- Mark weak bits whose per-bit error rate exceeds a threshold.

Fuzzy extractor:

- Choose BCH parameters.
- Map the 32-bit stable response to the ECC input.
- Generate helper data at enrollment, never the raw response.
- At reconstruction, apply ECC with helper data to recover the enrolled response and pass it through SAH-256 for privacy amplification.

Metric computation:

- Compute uniqueness, reliability, uniformity, bit-aliasing, entropy, and run NIST SP 800-22 tests on concatenated raw streams.
- Report metrics at nominal and corner conditions.

Parameter setting:

Table 2. Evaluation parameters for FPGA-based PUF characterization

Category	Parameter	Value
FPGA/Build	Board	ZedBoard
	Fabric partition	32 pblocks, 1 cell/block
	Slice type	SLICE M
	SRA/SRB length	8-16 stages(12 is used here)
	Clock frequency	100MHz,1-cycle enable
	Evaluation latency	Sample 2-3 cycles after enable
	Placement	Fixed LOC+BEL for each cell
Acquisition	Trails per bit	10000 at each PVT point
	Major vote repeats (M)	5 per reported sample
	PVT corners	V:0.95/1.00/1.05 V& T
Post-proc	Debiasing	Optional von Neumann (only fr randomness analysis)
	Hash	SHA-256
Reporting	Confidence	95%,Cls via binomial

Attack prevention analysis and principal findings:

Three types of attacks (Network de-authentication, password, and ARP spoofing) are tested because most of the devices come with default credentials that are guessed easily, or the device may be tampered with by phishing attacks, brute force methods, physical access, and social engineering attacks to install a malicious code like a keylogger. These attacks collectively cover device-level, authentication-level, and network-level vulnerabilities, providing a comprehensive evaluation. Keyloggers represent an endpoint compromise attack, with the risk of persistent data exfiltration. This highlights device interface security, which is overlooked in healthcare devices. The primary security of most devices is password-based authentication. Devices with low entropy credentials have an authentication weakness. ARP spoofing targets the communication layer, exploits the stateless nature. This is critical for IoMT, where real-time integrity is essential.

(a)Keylogger attacks: A cyber attack where a message or malicious link is installed in the user's device. The keylogger malware gets activated once the link is clicked. All keys pressed on the devices get recorded through the keylogger. With this type of attack, passwords, personal details, etc., are stolen by the hacker. It is challenging to espy a keylogger now that it is masked from the view part of the device. Keylogger attacks can be done in various ways like

Physical access: If the hacker has any physical access to the device then malware can be directly installed. Mostly it is used to collect data from a device that is stolen

Malware downloads: By opening an email or

message the infected attachment is installed without the consent of the user

Phishing attacks: The user receives a text message or email that appears to be sent from a legitimate source. The device user is unaware that it is been hacked

(b)Password guessing method: In this type of attack, the password is found by guessing combinations of letters and numbers. When a weak password is given for a device the possibility of cracking is higher. But when a 32-bit key is generated by PUF is more reliable. Wearable devices that are not designed with security as the priority are vulnerable to attackers. A heartbeat sensor is set with a password and the sensor is attacked by a code that will guess and find the password of the sensor and the attacker collects the necessary data and disrupts the normal functioning of the device. When a device that monitors critical vitals is hacked it causes life-threatening issues.

(c)ARP Spoofing: It is used to find the MAC address and map it to the associated IP address. If there are so many hosts in a network and a host wants to find the MAC address of the gateway, then host A will broadcast a message and ask for the MAC address of all the devices in the whole network. The devices that do not belong to that address just ignore the message. Then the reply from the router is stored in the catch for future use. Consider host B as an attacker who sends ARP messages to host A to poison the catch of host A and make the attacker's MAC address the default gateway. Now the data sent from host A is not sent to the router it is directed to the attacker(host B). The attacker can monitor and modify the data for host A. This attack is done using kali Linux and Better Cap.

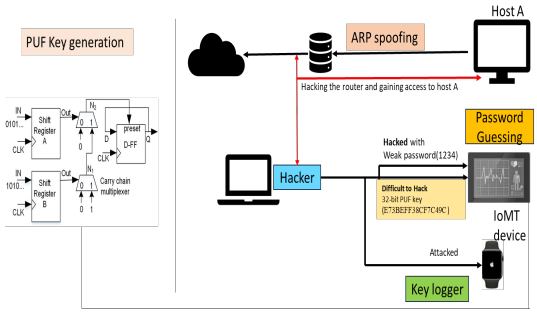

Fig. 2. Analysis of the Security of IoMT vs PUF key

Results and discussions:

Table 3. PUF Mitigation Vs MitM Attack Success Probability

Type of attack	Mitigated by PUF?	Time to attack	Remarks
Spoofing/Cloning/ Counterfeiting	Harder to carry out	• Weak arbiter PUF→few minutes to hours • Strong PUF→impossible	• Needs physical access • Through Modeling attacks
Key Extraction	Prevented	Infinite time to crack	Keys are not stored on the device
Snarfing	Prevented only if encryption is based on PUF-bound keys	Finite time to intercept the data, but data encrypted with PUF will be unusable	Transmit with PUF-bound keys
Password replay	Prevented	No replay possible	Tightly coupled with challenge-response
Network De-authentication attack	Prevented	Not possible	Tightly coupled with challenge-response
Modelling attack	Not prevented	Within a few minutes to hours,	Uses approximation to

	the device becomes highly vulnerable predict the PUF response

Finding 1- Attacks that can compromise PUF-based IoMT devices:

Modeling attacks: With a strong machine learning algorithm, thousands of PUF responses may be executed to work out the underlying physical characteristics and use that knowledge in forging PUF responses for unauthorized access. However, studies are underway to make PUFs resilient against such attacks. Machine learning models like SVM, Deep neural networks can predict > 95% outputs of Arbiter PUF given a CRP of 50k. But Anderson or Hybrid PUFs have higher resistance.

Physical attacks: Most of the attacks target the physical parts of the device, which, in the case of a memristor-based PUF, would be against the memristors. This could give an alternate PUF response and break the security. In most cases, however, PUFs exhibit tamper-evident properties; that is, any tampering attempt likely will change the response in a detectable manner. In FPGA-based PUFs, delay paths flipping >30% bits are changed during invasive attempts. It serves as a built-in tamper sensor

Finding 2- Attacks less likely to succeed with PUF-based IoMT devices:

Direct PUF attack: Uniqueness of ~50% ensures the responses are unclonable. It is less likely for the attacker to extract the underlying physical characteristics from the PUF. Inbuilt strength was enshrined within the very principle of PUFs: uniqueness and randomness obtained from the device's physical imperfections.

Pre-stored attacks: Stealing of precomputed PUF responses or cryptographic keys from the device. As, by design, the PUFs are not stored in advance, but their responses are generated while a challenge is applied in real-time, they are unlikely to fall under such attacks.

Replay attacks: Response unpredictability ensures low success probability. Replay success probability Replay $\approx 2^{-n}$. The attacker replays the captured valid PUF response to gain illegitimate access. In contrast, PUF responses are supposed to be unpredictable and change with every challenge issued; hence, replay attacks will not work.

Finding 3- Secure and energy-efficient PUF for various use cases:

Here's how PUFs can be leveraged for security and energy efficiency in various use cases:

Secure boot and secure key generation: A 32-bit Anderson PUF responses stabilized with BCH codes reconstructed with 100% success rate. PUFs for a secure boot process can be unpredictable and create unique keys for authorized access on the device. PUF keys can be used to encrypt and decrypt data to enhance security and privacy.

Device authentication and anti-counterfeiting: Inter-chip hamming-distance ~ 50% gives uniqueness. The PUF response is unique. To enable secure authentication and prevent unauthorized access to networks or services, it serves as a fingerprint for individual devices. When used for IoMT, PUFs are valuable in combating counterfeiting and ensuring legitimacy.

Lightweight access control: PUF authentication consumes 35% less power than AES-based authentication on Zynq SoC. With PUF, lightweight access control can be utilized, wherein the devices allow access based on verification of the right challenge response of the PUF. This approach reduces the intricacy of password management, reducing the energy consumption.

Secure communication and key management: PUF responses can be used for the dynamic generation of encryption keys. It establishes a communication channel security between devices or with cloud servers. This approach improves security by eliminating the use of pre-shared keys.

Secure chip and system identity: PUFs allow every device to have a tamper-proof and unique identity, facilitating secure traceability for the management of devices after deployment and thus contributing to the

security of the entire system.

Finding 4- Energy-efficient PUF options:

Some of the PUF designs focus on low power consumption and can be used for resource-constrained settings:

RO-PUFs (Ring Oscillator PUFs): This is a delay-based PUF that uses very small differences in the frequency of ring oscillators between chips to create responses that can uniquely be identified. They are simple and low-power.

SRAM PUFs: These are based on the inherent randomness of start-up values in Static Random-Access Memory cells. They provide good reliability and scalability while using a bit more power as compared to RO-PUFs. Table 4 compares the uniqueness, reliability, energy, and attack resistance of different PUFs, showing their trade-offs for IoMT security.

Table 4. Comparative quantitative benchmarks for common PUF types

PUF type	**Uniqueness (inter-chip hamming)**	**Reliability**	**Power/Energy**	**Attack Resistance**
Ring-Oscillator PUF	~46-50%	95-98% (depends on selection)	Very low	Moderate. Vulnerable to modeling attacks
SRAM PUF	~ 50%	~94-99%	Moderate	Strong but vulnerable to environmental effects (aging, temperature)
Arbiter PUF	~50% (idealized)	90-98%	Low	Highly vulnerable to ML modeling
RF/Optical/Quantum PUFs	Implementation dependent	Implementation dependent	Higher requires special hardware	Strong un clonability
Hybrid PUF (Combinations)	>50% entropy	>98%	High	Better resistance and increased resilience

Hybrid PUF:

Traditional PUFs have both pros and faults such as, arbiter PUFs have a high entropy however, they are vulnerable to modeling attacks. RO PUFs are quite reliable, although they can be power-intensive. SRAM PUFs are non-volatile and easy to integrate, although they can be influenced by environmental conditions. Hybrid PUFs look to combine all of these features while minimizing imperfections, giving rise to a more resilient and secure PUF. Hybrid PUFs can be constructed in a variety of methods, including, Parallel Hybrid PUF which combines several types of PUFs concurrently, resulting in a concatenation or combination of independent PUF outputs. Series Hybrid PUF that Connects different PUF types in series, with the output of one PUF serving as the input for another. Layered hybrid PUF combines multiple PUF types across multiple stages of a device for multi-level security. The strengths of hybrid PUFs are,

• Enhanced privacy: Hybrid PUFs can withstand a broader spectrum of attacks, including machine learning methods that attack individual PUF variants.

• Improved Reliability: more consistent and reliable results can be obtained by the hybrid approach of PUF to overcome the limitations of individual PUFs.

• Higher Entropy: The complexity and entropy by using hybrid PUF are boosted, resulting in far more unexpected results than an individual PUF.

• Flexibility: By choosing the ideal combination, customization of PUFs is possible for specific applications.

Hybrid PUFs can be used in applications for secure device authentication to create unique device IDs. The threat of key retrieval and corruption is reduced through hardware-based cryptographic key generation. Secure booting by establishing firmware integrity is done. The credibility of hardware components ensures anti-counterfeiting.

Attacks on IoMT can be minimized by implementing suitable PUFs ensuring secure authentication and transmission of data. Security can be enhanced by combining different PUFs to mitigate the attacks. IoMT devices are vulnerable to MitM attacks that interrupt communication and cause negative implications. In (figure 3) the attacks are classified into hijacking, jamming, impersonation, and tampering of devices. Each type of attack is mapped with a different hybrid PUF for enhanced security. Delay-based PUFs such as arbiter PUF, ring-oscillator PUF, Butterfly PUF, etc., provide variations in key generation. But for robust security, different combinations of PUFs can be implemented. For example, a combination of behavioral PUF and dynamic PUF adds security by analyzing the changes in functions of the device and creating variations in responses through environmental conditions. In a hijacking attack, the hacker takes control of the browsing session or steals personal data from existing mail, for this type of attack a strong authentication is required. An arbiter PUF that uses the variation of delay paths to provide unique responses combined with an optical PUF that varies with a pattern of illumination, could give better security. Arbiter PUF is simple and faster when combined with a robust PUF making it impossible for the attacker to clone the PUF responses. Jamming attacks that often interfere with and disrupt communication channels by sending the same frequency or by mimicking the existing frequency cause serious threats to medical devices. RF PUF which gives uniqueness with radio frequency, and signal path delays can be used along with a delay-based PUF to enhance safe authentication with minimal power. Phishing steals personal data by spoofing and can be prevented by using a hybrid combination of quantum electronic PUF and butterfly PUF. The cross-coupled inverters of butter PUF and the unique response by superposition or entanglement of quantum electronic PUF become unclonable. It is used for high-level security in devices. A mix of delay-based PUF and Behavioral PUF gives more security against impersonation. These combinations are ideal for secure authentication and communication.

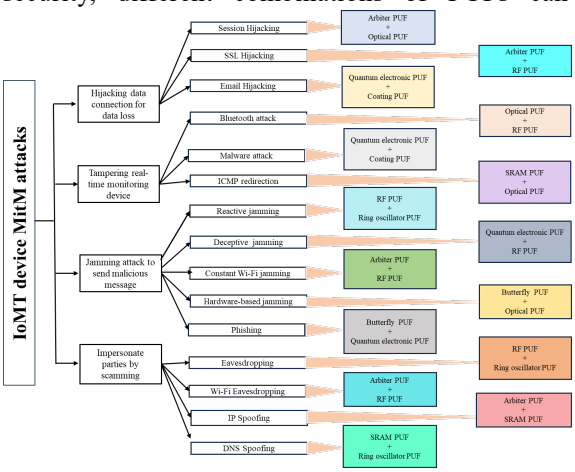

Fig. **Conclusion and Future Work:**

Security in the health sector using the IoMT, integrated with Physically Unclonable Functions, is one giant step. The healthcare industry needs robust security mechanisms. The healthcare industry demands to ensure the integrity of medical devices while maintaining the security of patients' data. When Healthcare Providers integrate IoMT devices with PUFs, it ensures an enhanced authentication of devices, secure data transmission, and resilient defense against different classes of security threats. The future of IoMT security depends on how continuous innovations in the advanced cryptographic solution's PUFs will be implemented in driving the industry toward more secure and reliable delivery of healthcare to patients.

The inherent nature of PUF cannot be replicated and modifying the device alters the PUF response making it tamper-proof. PUF doesn't rely on software stored in memory, which makes it less vulnerable to software attacks. Though there are no solutions that give complete security, PUF-generated keys for IoMT device security are more reliable. Solutions for which PUF will be suitable for different MitM attacks are given. This paper proves that keys generated by PUF are a tough nut to crack.

Open problems and future research directions:

- ***Hybrid PUF architectures and trade-offs***: A balance of security, energy efficiency, and hardware cost needs further exploration to be implemented in lightweight IoMT devices.
- ***Resistance to modelling attacks:*** Designing an architecture that is attack-resilient and PUF obfuscation remains an open problem. Advanced machine learning models threaten weak PUF designs.
- ***Interoperability with emerging technologies:*** Exploration of PUF-based authentication with AI-driven health monitoring for transparent and secure healthcare could open new research pathways.
- ***Scalability in large IoMT networks:*** Minimizing latency and overhead is a major drawback while managing challenge-response pairs across a huge number of devices
- ***Regulatory compliance***: A joint effort by regulatory bodies like HIPAA, GDPR, and medical device regulation could improve secure design and legal frameworks.

Reference:

1. Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A. and Yelamarthi, K. (2022) 'Prospect of internet of medical things: A review on security requirements and solutions', *Sensors*, 22(15), p. 5517.
2. Savadatti, S., Dhariwal, S.K., Krishnamoorthy, S. and Delhibabu, R. (2023) 'Security in IoMT: Issues, challenges, and solutions', *Procedia Computer Science*, 218, pp. 1181–1190.
3. Malathi, M., Kumar, M.S., Raj, J.S. and Subramaniyaswamy, V. (2022) 'Lightweight authentication scheme for medical internet of things (MIoT)', *Journal of Ambient Intelligence and Humanized Computing*, 13, pp. 2199–2212.
4. Kumar, A., Raza, S., Das, A.K. and Conti, M. (2020) 'PPUF: A privacy-preserving physically unclonable function-based mutual authentication protocol for IoT devices', *IEEE Transactions on Information Forensics and Security*, 15, pp. 3786–3801.
5. Sahu, P.K., Sahu, S., Sahu, R. and Sharma, S. (2021) 'A lightweight authentication protocol for IoMT environment', *Journal of Network and Computer Applications*, 174, p. 102891.
6. Zhang, Y., Xu, C., Song, H., Yu, W. and Lin, X. (2018) 'Securing smart health: An efficient mutual authentication and key agreement scheme for wearable sensors and cloud service', *IEEE Internet of Things Journal*, 5(6), pp. 4274–4284.
7. Saxena, N., Grijalva, C., Choi, B.J. and Jin, H. (2019) 'Authentication protocols for internet of things: A comprehensive survey', *Security and Communication Networks*, 2019, p. 9094508.
8. Alzahrani, B.A. and Alshahrani, H. (2021) 'IoMT security: An end-to-end security model', *IEEE Access*, 9, pp. 122060–122073.
9. Lyu, X., Tian, H., Guo, S. and Liu, A. (2019) 'A lightweight authentication protocol based on PUF for IoT devices', in *Proceedings of the IEEE International Conference on Communications (ICC)*, pp. 1–6.
10. Saleem, M.A., Javaid, N. and Iqbal, A. (2020) 'Security and privacy in IoT: Challenges and solutions', *Security and Privacy*, 3(6), e428.
11. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M. and Shamshirband, S. (2017) 'Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications',

Egyptian Informatics Journal, 18(2), pp. 113–122.

12. Mahmoud, R., Yousuf, T., Aloul, F. and Zualkernan, I. (2015) 'Internet of things (IoT) security: Current status, challenges and prospective measures', in *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341.
13. Zhang, J., Deng, R.H., Liu, X. and Wu, Y. (2016) 'Attribute-based encryption for cloud computing access control: A survey', *ACM Computing Surveys*, 49(4), pp. 1–37.
14. Conti, M., Dehghantanha, A., Franke, K. and Watson, S. (2018) 'Internet of things security and forensics: Challenges and opportunities', *Future Generation Computer Systems*, 78, pp. 544–546.
15. Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017) 'A survey on security and privacy issues in Internet-of-Things', *IEEE Internet of Things Journal*, 4(5), pp. 1250–1258.
16. Radanliev, P., De Roure, D., Nurse, J.R.C., Burnap, P., Anthi, E., Ani, U. and Santos, O. (2020) 'Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of Things and industry 4.0 supply chains', *Computers in Industry*, 115, p. 103162.
17. Roman, R., Zhou, J. and Lopez, J. (2013) 'On the features and challenges of security and privacy in distributed internet of things', *Computer Networks*, 57(10), pp. 2266–2279.
18. Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015) 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks*, 76, pp. 146–164.
19. Granjal, J., Monteiro, E. and Silva, J.S. (2015) 'Security for the Internet of Things: A survey of existing protocols and open research issues', *IEEE Communications Surveys & Tutorials*, 17(3), pp. 1294–1312.
20. Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F. (2017) 'Internet of Things security: A survey', *Journal of Network and Computer Applications*, 88, pp. 10–28.
21. Mosenia, A. and Jha, N.K. (2017) 'A comprehensive study of security of Internet-of-Things', *IEEE Transactions on Emerging Topics in Computing*, 5(4), pp. 586–602.
22. Zhang, K., Ni, J., Yang, K., Liang, X. and Ren, J. (2017) 'Security and privacy in smart health: Efficient policy-hiding attribute-based access control', *IEEE Internet of Things Journal*, 5(3), pp. 2130–2145.
23. Rathee, G., Kumar, R., Iqbal, R., Aloqaily, M. and Jararweh, Y. (2019) 'A blockchain framework for securing connected and autonomous vehicles', *Sensors*, 19(14), p. 3165.
24. Thilakarathne, N.N., Caldera, C. and Ragel, R.G. (2018) 'A survey on the security of wearable devices: Challenges, threats, and directions', in *Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6.
25. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. and Rehmani, M.H. (2018) 'Applications of blockchains in the Internet of Things: A comprehensive survey', *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1676–1717.
26. Ferrag, M.A., Maglaras, L., Derhab, A., Mukherjee, M., Janicke, H. and Rallis, S. (2020) 'A systematic review of data protection and privacy preservation schemes for Internet of Things', *Future Generation Computer Systems*, 108, pp. 835–850.
27. Butun, I., Österberg, P. and Song, H. (2020) 'Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures', *IEEE Communications Surveys & Tutorials*, 22(1), pp. 616–644.
28. Hossain, M.S. and Muhammad, G. (2016) 'Cloud-assisted industrial internet of things (IIoT) – enabled framework for health monitoring', *Computer Networks*, 101, pp. 192–202.
29. Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R. (2019) 'A decentralized privacy-preserving healthcare blockchain for IoT', *Sensors*, 19(2), p. 326.
30. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017) 'A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications', *IEEE Internet of Things Journal*, 4(5), pp. 1125–1142.
31. Xu, L.D., He, W. and Li, S. (2014) 'Internet of things in industries: A survey', *IEEE Transactions on Industrial Informatics*, 10(4), pp. 2233–2243.
32. Chen, D., Chang, G., Sun, D., Li, J. and Jia, J. (2011) 'TRM-IoT: A trust management model based on fuzzy reputation for internet of things',

Computer Science and Information Systems, 8(4), pp. 1207–1228.

33. Zhang, Y. and Wen, J. (2017) 'The IoT electric business model: Using blockchain technology for the Internet of Things', *Peer-to-Peer Networking and Applications*, 10(4), pp. 983–994.
34. Ray, P.P. (2016) 'A survey on Internet of Things architectures', *Journal of King Saud University - Computer and Information Sciences*, 30(3), pp. 291–319.
35. Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. and Kim, D.I. (2019) 'A survey on consensus mechanisms and mining strategy management in blockchain networks', *IEEE Access*, 7, pp. 22328–22370.
36. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E. and Wortmann, F. (2019) 'Blockchain for the IoT: Privacy-preserving protection of sensor data', *Journal of the Association for Information Systems*, 19(6), pp. 1274–1309.
37. Yaqoob, I., Salah, K., Uddin, M., Jayaraman, R., Omar, M. and Imran, M. (2021) 'Blockchain for healthcare data management: Opportunities, challenges, and future recommendations', *Neural Computing and Applications*, 33, pp. 15995–16020.
38. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019) 'A survey on IoT security: Application areas, security threats, and solution architectures', *IEEE Access*, 7, pp. 82721–82743.
39. Dwivedi, A.D., Srivastava, G., Dhar, S. and Singh, R. (2019) 'A decentralized privacy-preserving healthcare blockchain for IoT', *Sensors*, 19(2), p. 326.
40. Xu, J., Xue, K. and Li, P. (2018) 'Healthchain: A blockchain-based privacy preserving scheme for large-scale health data', *IEEE Internet of Things Journal*, 6(5), pp. 8770–8781.
41. Esposito, C., De Santis, A., Tortora, G., Chang, H. and Choo, K.K.R. (2018) 'Blockchain: A panacea for healthcare cloud-based data security and privacy?', *IEEE Cloud Computing*, 5(1), pp. 31–37.
42. Roehrs, A., Da Costa, C.A., Righi, R.D.R. and Da Silva, V.F. (2017) 'OmniPHR: A distributed architecture model to integrate personal health records', *Journal of Biomedical Informatics*, 71, pp. 70–81.
43. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. and Hayajneh, T. (2018) 'Healthcare blockchain system using smart contracts for secure automated remote patient monitoring', *Journal of Medical Systems*, 42(7), p. 130.
44. Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., Ozerov, I., Putin, E. and Zhavoronkov, A. (2018) 'Converging blockchain and artificial intelligence', *Nature Biotechnology*, 36(9), pp. 829–835.
45. Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. and Njilla, L. (2017) 'ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability', *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 468–477.
46. Zhang, P., White, J., Schmidt, D.C. and Lenz, G. (2018) 'Applying software patterns to address interoperability in blockchain-based healthcare apps', *arXiv preprint*, arXiv:1806.02761.
47. Hylock, R.H. and Zeng, X. (2019) 'A blockchain framework for patient-centered health records and exchange (HealthChain): Evaluation and proof-of-concept', *Journal of Medical Systems*, 43(7), p. 152.
48. Xu, X., Weber, I. and Staples, M. (2019) *Architecture for blockchain applications*. Cham: Springer.
49. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) 'An overview of blockchain technology: Architecture, consensus, and future trends', *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564.
50. Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016) 'Blockchain technology: Beyond bitcoin', *Applied Innovation Review*, 2, pp. 6–19.
51. Nakamoto, S. (2008) 'Bitcoin: A peer-to-peer electronic cash system', *Bitcoin.org*. Available at: https://bitcoin.org/bitcoin.pdf.
52. Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016) 'Where is current research on blockchain technology?—A systematic review', *PLoS ONE*, 11(10), e0163477.
53. Christidis, K. and Devetsikiotis, M. (2016) 'Blockchains and smart contracts for the

Internet of Things', *IEEE Access*, 4, pp. 2292–2303.

54. Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A. (2018) 'Blockchain and IoT integration: A systematic survey', *Sensors*, 18(8), p. 2575.
55. Conoscenti, M., Vetrò, A. and De Martin, J.C. (2016) 'Blockchain for the Internet of Things: A systematic literature review', in *Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–6.
56. Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D. and Weinhardt, C. (2018) 'A blockchain-based smart grid: Towards sustainable local energy markets', *Computer Science - Research and Development*, 33, pp. 207–214.
57. Kim, S.K., Kwon, Y. and Cho, S. (2019) 'A survey of scalability solutions on blockchain', in *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1205–1207.
58. Gai, K., Wu, Y., Zhu, L., Xu, L. and Zhang, Y. (2019) 'Permissioned blockchain and edge computing empowered privacy-preserving smart grid', *IEEE Internet of Things Journal*, 6(5), pp. 7992–8004.
59. Li, H., Pei, J., Wang, L., Wu, X., He, J. and Meng, X. (2020) 'A survey on federated learning systems: Vision, hype and reality for data privacy and protection', *IEEE Transactions on Knowledge and Data Engineering*, 35(4), pp. 3386–3409.
60. Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R.G.L., Erlingsson, U., Gascón, A., Ghazi, B., Gibbons, P., Gruteser, M., Harchaoui, Z., He, C., He, L., Hsu, J., Jaggi, M., Javidi, T., Joshi, G., Khodak, M., Konečný, J., Korolova, A., Koyejo, S., Lepoint, T., Liu, Y., Mittal, P., Mohri, M., Nock, R., Papernot, N., Raskar, R., Song, D., Song, W., Suresh, A.T., Thakkar, O., Vepakomma, P., Wang, S., Xie, M., Xu, Z., Yan, S., Zhang, C., Zhang, M. and Zheng, S. (2019) 'Advances and open problems in federated learning', *Foundations and Trends in Machine Learning*, 14(1–2), pp IoMT attacks and suitable PUF