Article

VXorPUF: A Vedic Principles - Based Hybrid XOR Arbiter PUF for Robust Security in IoMT

Md Ishtyaq Mahmud [1], Pintu Kumar Sadhu [1], Venkata P. Yanambaka [2] and Ahmed Abdelgawad [1]

[1] College of Science and Engineering, Central Michigan University, Mount Pleasant, MI 48858, USA; sadhu1pk@cmich.edu (P.K.S.); abdel1a@cmich.edu (A.A.)
[2] Department of Mathematics and Computer Science, Texas Woman's University, Denton, TX 76204, USA; vyanambaka@twu.edu (V.P.Y.)
* Correspondence: mahmu4m@cmich.edu

Abstract: The Internet of Medical Things (IoMT) is playing a pivotal role in the healthcare sector by allowing faster and more informed hospital care, personalized treatment, and medical solutions. Several authentication systems are used to safeguard the data and authenticate the devices, but some of them are inefficient and some of them have some limitations. A very effective and trustworthy solution for resource-constrained medical devices is provided by Physical Unclonable Functions (PUF) - based identity and authentication systems. This paper proposes VXorPUF, a Vedic Principles - Based Hybrid XOR Arbiter PUF. Modeling attacks were performed on the proposed architecture and an accuracy of 49.80 % was achieved. Uniqueness, Reliability and Randomness were the figures of merit used to evaluate PUF. A further study was evaluated the uniformity of (m,n,p)-OAN-XOR-PUF, and a result of 43.75% was found, which is close to the ideal value of arbitrary PUF response.

Keywords: Internet of Medical Things; Arbiter PUF; security and privacy; physical unclonable function; machine learning; authentication framework

1. Introduction

The IoMT has become an integral part of our daily life. Due to recent technological breakthroughs and the advent of low-power, high-performance IoT devices, establishing an IoT ecosystem has become simple and straightforward. Several fields are being utilized by the Internet of Things, including Smart Grid, Smart Self-driving Cars, IoT Farming, Smart Homes, Smart Healthcare, Military, Smart Cities, and Smart Industrial facilities. The demand for smart healthcare system using medical devices is high in the technology market besides of other applications of IoT. IoMTs are the potential of today's medical systems, in which every medical equipment will be hooked up to The internet and supervised by healthcare practitioners [1]. In IoMTs, highly sensitive personal health information is mainly collected, so maintaining patients' privacy and security is essential to helping reduce the risk of negative consequences on their health or causing their death in the worst case scenario [2].

With the global pandemic, majority of the population has become health-aware and started using fitness trackers, health monitors and smart devices to improve the quality of life. This has given rise to an increased cyber attacks on the IoMT ecosystem [3]. Fig. 1 shows the IoMT ecosystem where patient's medical data is collected through smart medical devices and sensors. Using the internet, applications for the IoMT are able to receive raw data collected by smart devices. The information is subsequently sent on to the medical practitioners and medical professionals, who respond to the people who require assistance. The data needs to be stored and cleaned through IoMT applications before sending to the laboratories. In addition, there is a need to use additional software, and apps to assist with both the display of and analysis of the medical data.

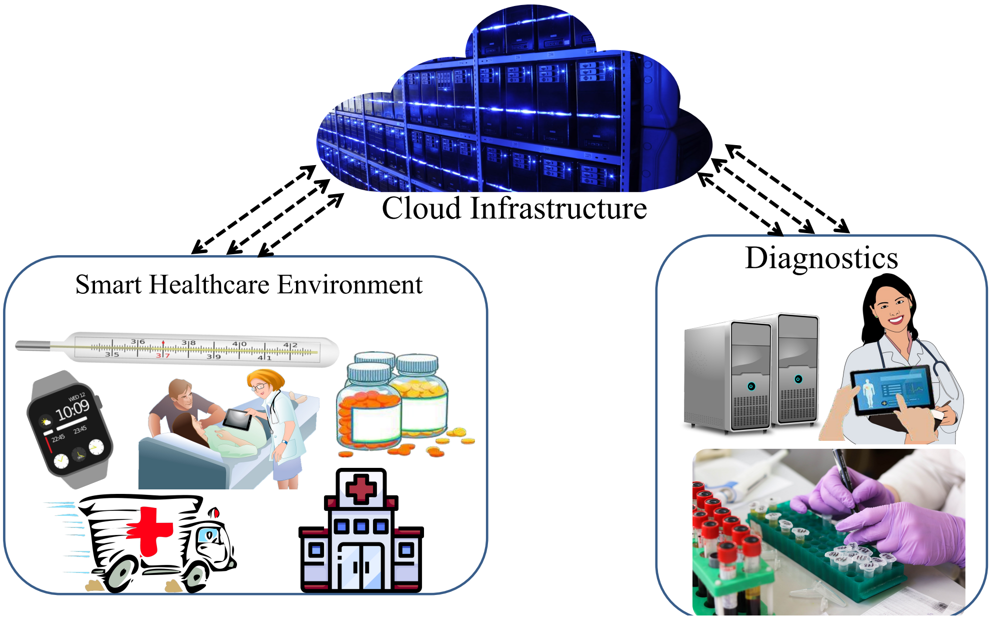

Figure 1. The Internet of Medical Things (IoMT)

Devices indicated that poor or restricted resources, such as CPU computing power, ROM, RAM, and battery life, are classified as constrained IoMT devices [4]. Although the devices are modest in size and lack the functionality to operate for intended job, constrained IoMT devices provide a wide range of functionalities. IoMT devices with resource-constraints are capable of collecting raw data from patients such as heart rate, glucose level, and other parameters and transmitting it to healthcare practitioners for promising treatment [5]. The IMD's ecosystem is more promising because of low-power wireless technology [6] (RFID, NFC, BLE, WIFI, SigFox, Bluetooth, Ingenu, Weightless Zigbee, LoRa and Z-Wave) that require less battery life. These IoT devices have fewer microcontroller units (MCUs), less computing capability, and less random access memory (ROM) than others. They also require fewer functionality for wireless network protocols. Typically, devices with limited resources include 8-32 bit microcontroller units, up to 32 kb RAM, and up to 256 kb read-only memory (ROM). In comparison to other wireless technologies, LoRa, SigFox, Ingenu, and Weightless have the highest computational power of MCU and ROM, which range from 16 to 32 bits and 32 to 512 kb, respectively. Furthermore, in TX mode, resource-constrained devices require 10 mW to 500 mW of power. Adapting resource-constrained devices to IoMT devices poses a significant challenge, as IoMT requires quick computing resources and increased storage capacity to retain raw data from patients on a continuous basis [7]. Also, Security issues of transmitting and collecting data have become a major worry of the IoMT system due to resource-constrains. 6G and beyond technology are now being used extensively in IoMT due to their tremendous bandwidth and fast response times [1].

IoMT is regulated to increase clinical safety through the use of wireless medical sensor networks (WMSNs) [8]. In WMSNs, edge medical devices first measure patient's medical condition and collect data such as pressure level, heart rate, glucose level and then sent it to the medical practitioners through gate-way nodes(GWNs) for analyzing. A GWN with a large amount of computing power and memory capacity can serve as a useful medium between Sensor Nodes (SNs) and MPs because SNs are limited in resources and cannot perform sophisticated operations. WMSN security and privacy must be addressed because of unanticipated threats in public communication [9].

A network of blocks known as a blockchain is used to store information with electronic signature. Blockchain utilizes a number of fundamental technologies, including decentralized consensus methods, cryptographic hashes, and digital signatures, to operate

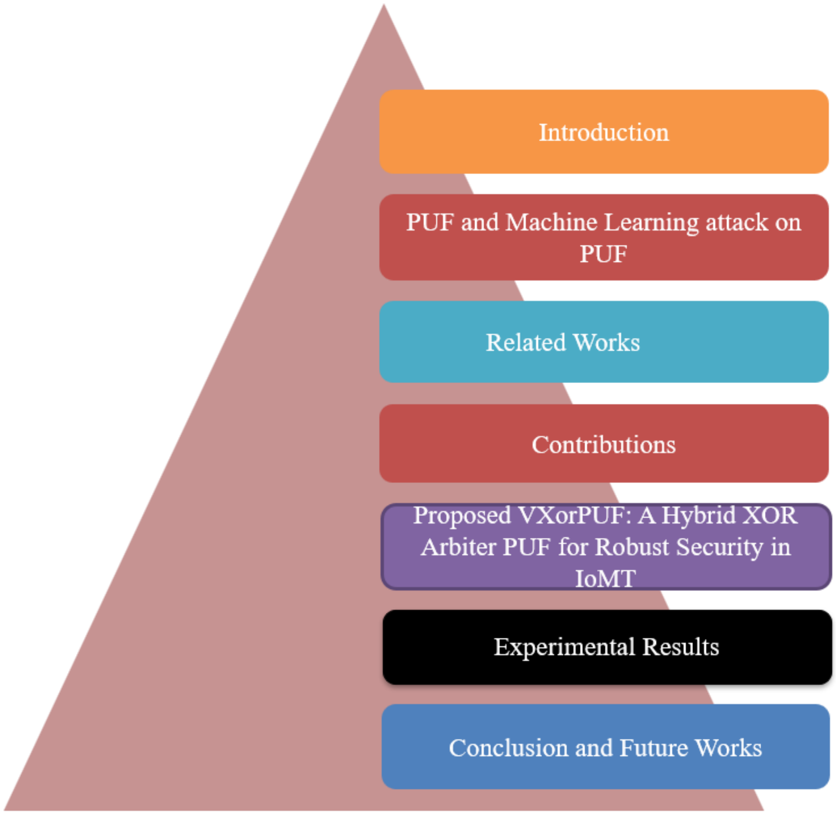
Introduction
PUF and Machine Learning attack on PUF
Related Works
Contributions
Proposed VXorPUF: A Hybrid XOR Arbiter PUF for Robust Security in IoMT
Experimental Results
Conclusion and Future Works

Figure 2. Outline of this paper.

in a distributed system [10]. There is no need for any intermediates to authenticate and validate the activities because they all take place in a decentralized system. Blockchain offers certain important features including decentralization, transparency, immutability, and auditability [11]. There are several applications for blockchain technology across a number of industries, including finance, healthcare, supply chains, digital media platforms, and remote service delivery [12]. Blockchain technology has additional uses, such as energy production and distribution, crowdfunding, electronic voting, identity authentication, and controlling public records [13].

For IoT ecosystems, security and privacy are absolutely essential. A strong authentication architecture helps protect an IoT system from many threats. To secure the data and authenticate the devices, several IoT authentication schemes are used, however some of them are ineffective and some of them have some limitations. PUF and blockchain may potentially be a viable option for IoT system authentication [14]. Blockchain is an emerging technology that combines hardware security primitives using PUFs to solve a variety of IoT system requirements, including bandwidth, connectivity, scalability, and energy. Combining Blockchain and PUF enables an effective architecture that ensures data authenticity and device reliability in IoT networks [15]. For the reliable and lightweight WMSN authentication, a combination of blockchain and PUF might well be beneficial [9]. The advantages of implementing Blockchain algorithms in IoT systems are numerous. It can be used for edge device authentication and verification in addition to maintaining data confidentiality and privacy.

The outline of the main ideas in this work is shown in Fig. 2. The IoMT, security, and privacy, the blockchain on PUF, and the resources that contained IoMT devices are discussed in the first section. The second section emphasizes PUFs and the attack on PUFs through machine learning. In the third section, we talked about some earlier research on PUF-based security for IoMT devices. In the fourth section, we proposed a hybrid XOR arbiter PUF that is reliable for IoMT devices. We talked about the uniqueness, reliability, randomness, and uniformity of our suggested XOR PUF in the experimental results section. In this section, we also used a machine learning attack on puf to verify the reliability of our proposed models. At the conclusion of this study, we reviewed our findings and offered some insightful recommendations for the works to come.

2. PUF and Machine Learning attack on PUF

PUF are the Hardware Assisted Security primitives for reliable and lightweight security in resource-constrained environments, such as the IoT and IoMT devices. A PUF creates secret keys from intricate physical characteristics of a material that are challenging to duplicate or clone, rather than preserving secrets [16]. PUF receives inputs in the form of "challenges" and outputs "responses" made up of genuine random numbers. PUF can be classified in three ways, silicon PUFs, non-silicon PUF and security based PUFs. Fig. 3 shows the PUF classification.

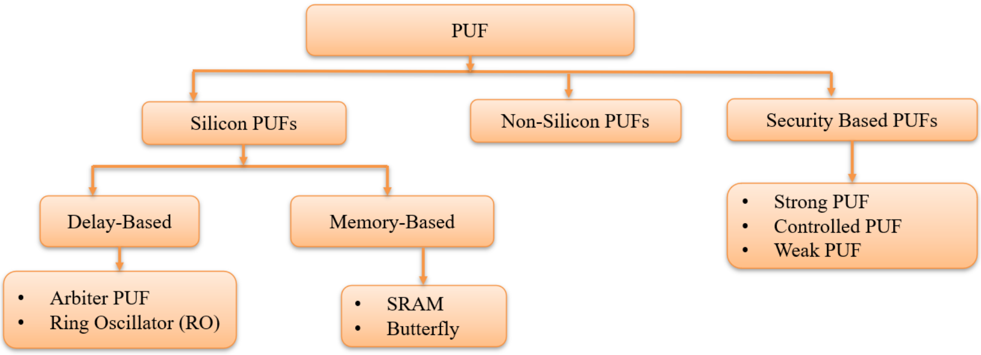

Figure 3. Classification of PUFs

In [17], the phrase "silicon PUFs" was used to describe physically unclonable devices created using traditional integrated circuits. Since silicon PUF does not require any modifications to the production process, it is undoubtedly the most simple PUF. The three main types of silicon PUFs are delay-based PUFs, memory-based PUFs, and analog electronic PUFs. These classes can be divided depending on the many sources of variation [18].

Arbiter PUF is delay basde PUF, which is one of the popular PUF. Each IC has its own distinct delay characteristics as a result of the manufacturing variations of transistors and wires; Lee et al. [19] made use of this characteristic to create arbiter-based PUF, which is secret information specific to each IC. The purpose of the arbiter PUF is to consciously induce a race condition among two digital routes on a silicon chip. Despite the fact that the two approaches are identical and therefore should cause the same delay, unexpected minor differences throughout the fabrication process guarantee that one option will ultimately be faster compared to the other. The routes are filled with multiplexers, also known to as "Switch Components". The multiplexers receive challenge bits as select inputs. The comparison pathways are either kept the same or are reversed by each switching component. As a result, there are many different potential paths. One of the major drawbacks of PUF for the metastablity of the delay flip-flop is that it has comparatively poorer reliability [20]. In order to prevent irreversible changes in the digital circuitry of a network, it is crucial to research the effects of aging on PUF. On the PUF modeling attack has a significant impact because to the aging effect [21]. Digital circuits eventually fail due to the aging effect, which reduces performance. [22] they mentioned that due to the aging effect PUF response could be unreliable though there is no effect on randomness of PUF. Fig. 4 depicts the structure of Arbiter PUF.

Machine Learning (ML) based modeling attack resistance is a significant need For PUF circuits. There have been reports of some Arbiter PUF compositions that have resisted modeling attacks and frequently need a lot of computer power for effective modeling [24].

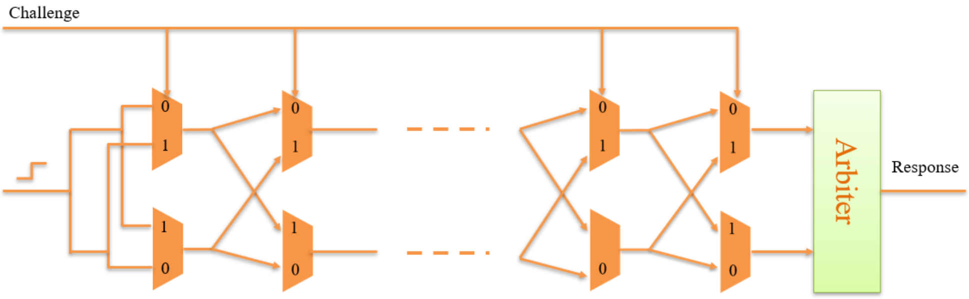

Figure 4. Architecture of Arbiter PUF [23]

ML, a highly parameterized strategy to produce predictions from observational data by employing specialized algorithms, is a key tool for conducting modeling threats [25]. In the recent past, ML has been utilized for PUF security research, where an attacker attempts to create a duplicate PUF model [26]. Attacker also makes an effort to accurately estimate the PUF response [27]. Modeling attack resistance is essential for PUFs because to ML's huge development and rising prominence in both science and industry.

3. Related Works

In today's digital revolution, Protecting patients' personal and medical information from unauthorized users, interpretation, and modification is a top priority. Security is becoming an increasing vital concern of makers and healthcare providers, because IMDs provides a significant services to the patients. Here is a review of some of the contributions the researchers made to the intelligent IoMT security framework.

Kwarteng et al. [28] mentioned some security threats of IMDs. DoS (Denial of Service) attack is one of them, this type of attack reduce the battery life expectancy. Reply Attack, try to change the status of IMDs by resend the identical request from a controller who already trusted. The researchers also discussed Software Injection, Man in the middle, and Side Channel attacks. Kautras et al. [29] addressed security protocols and constraints of IoT devices, when they adapt to the IoMT specialized network typologies. The researcher also identified alternative mitigation control that can be used to safeguard IoMT systems. Hatzivasilis et al. [30] mentioned BYOD (bring your own device) is another essential part of smart medical sectors that must be safeguarded in order to protect our patients' personal information.

Rahman et al. [31] demonstrated the significant vulnerability assessments for IoMT devices in WMSNs, as well as serious security flaws, in order to prevent hostile cyber-attacks. Furthermore, they discussed existing cryptographic authentication procedures to protect smart medical devices from cyber-attacks and discussed feasible solutions for addressing security weaknesses. Kumar et al. introduced cyber-attacks into IoMT networks, which are rapidly growing nowadays in hospital environment. They also introduced a solution for spotting cyber-attacks in fog-cloud infrastructure [32]. Nandy et al. presented a Swarm-Neural Network (Swarm-NN) technique for securing healthcare data while storing and sending information from the edge to the server with greater accuracy. This approach also detects threats and keeps track of the data's accuracy and parameters [33].

Almogren et al. [34] introduced sybil security risks, in which a single person creates several phony social media profiles in order to spread destructive misinformation. A fuzzy logic-based trust management (TM) technique has been presented by the researcher for mitigating the sybil security risk in medical environment and healthcare systems. Papaioannou et al. referred to a few hypothetical risks including potentially significant security mechanisms of IoMT devices [35]. Karmakar et al. [36] introduced a security design for forthcoming network virtualization platforms like OpenMANO. Furthermore, they explained how this security design used trusted healthcare network functionalities to authenticate IoMT devices. Wazid et al. explored some potential architecture and their implementations of IoMT ecosystems, as well as various malware attack and their symptoms. They also gave a comparison of the various malware detection systems that are currently in use, as well as some challenges and recommendations for future research [37].

Hardware Assisted Security (HAS) is a promising security solution for lightweight and robust security in IoMT. There are various security solutions proposed for the IoMT ecosystem [38,39]. PUF is a hardware assisted module to generate natural random numbers for cryptographic purposes [40]. PUF uses the manufacturing variations introduced during the fabrication of Integrated Circuits (IC) to generate the random numbers. The inputs and outputs of PUF are called "challenge - response pairs" (CRPs). PUF is used as a hardware security primitives for various applications, such as device authentication, communication, intellectual property protection, and so on [41,42].

Many designs of PUF were developed over the past few years for different applications. With the advancements in deep learning, PUF is vulnerable to modeling attacks [43,44]. Research has been going on to design a modeling attack resistant PUF [45]. Though many architectures were designed to resist the modeling attacks, the accuracy of such designs has always been over 70 % [44,45]. With the high performance computing and developments in deep learning techniques, modeling attacks on PUF are becoming more aggressive and successful. This paper presents VXorPUF modeling attack resistant PUF for IoMT devices.

The researchers [46] prototyped the lattice PUF to secure IoT device against machine learning attacks. In Lattice PUF, the PUF logic proper required 45 slices, and the fuzzy extractor required 233 slices. In all of their attacks, they used a variety of ML models, including logistic regression, support vector machines, and deep neural networks. After analyzing their model they got the accuracy of above 50.24%. Subthreshold current array PUF (SCA-PUF) was proposed to resistant the machine learning attack [47]. In addition, amplifier-chain-based XOR-PUF[48] was also proposed. By employing 1 million CRPs as training datasets and an artificial neural network, the researchers achieved an accuracy of 50.70%. Furthermore, [49] the researcher demonstrated MPUF, which notably prevents ML attack. Their MPUF also performs better when it comes to randomness, reliability and uniqueness. After analyzing the machine learning model they got the prediction accuracy of 53.80%.

The researchers [24] introduced deep neural network based attack on wide variety of PUFs. They considered 64-bit and 128-bit arbiter PUF for modeling attack on PUFs. The attack is reasonably resilient to input dataset noise and computationally viable for the majority of real PUF designs. Though they need to be theoretically justify their proposed modeling attack on PUFs. Canaday et al. [50] proposed a uniqhe model-free ML attack, which model is based on deep learning based algorithms. Their framework against strong PUFs, which makes use of both collected CRP data from a particular target PUF and data gathered from additional PUF instances of the same type. The researchers also noted that their framework performed better than a number of other robust PUFs that are currently ML-resistant. Wang et al. [51] proposed a new ML-resistant robust PUF design. Their approach offers a way to combine inverted responses with regular ones, and that way ML algorithms are unable to generate a reliable model of the internal PUF.

4. Contribution

For an IoT security system that is both lightweight and reliable, a large number of keys must be addressed. The number of devices utilized to design the PUF typically determines the length of the PUF key. The following are this paper's main contributions.

- We suggested using the Veda theorem to lengthen the key in order to avoid the the large number of device to collect PUF keys.
- Conventional XOR PUF requires 64 times response generation using 64 challenges. Whereas the presented paper only requires one 64-bit challenge which eliminates the requirement of challenge key size. Moreover, 13 times response generation is required instead of 64 times.

- After applying the Vedic theory, we obtained nearly optimal uniqueness, randomness, and reliability values of PUFs.
- We found that the ML accuracy for the VEDA sequence was 49.80%, indicating that the VEDA PUF is vulnerable to ML assault.

5. Proposed VXorPUF: A Hybrid XOR Arbiter PUF for Robust Security in IoMT

The proposed VXorPUF uses the ancient Vedic principles at the core of the architecture to generate the modeling attack resistant CRPs. Veda-PUF, a controlled PUF architecture for robust lightweight design was proposed in [52]. VXorPUF uses the principle behind Veda-PUF as a controller mechanism to design a Hybrid XOR Arbiter PUF resistant to modeling attacks.

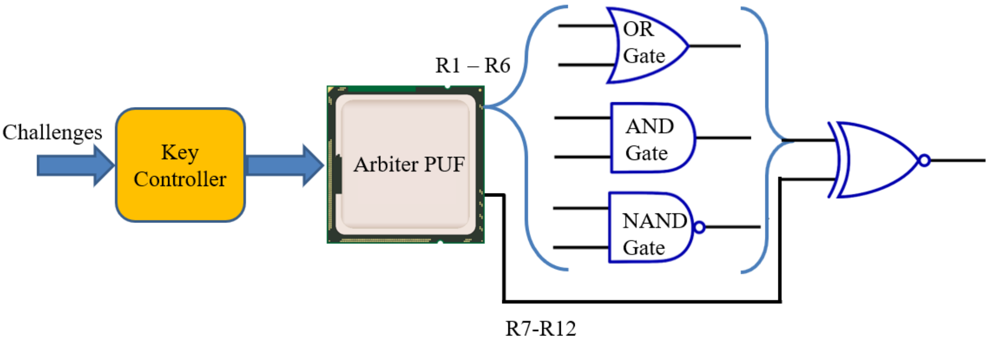

Figure 5. Proposed VXorPUF Architecture

As shown in Fig. 5, The challenges given to the PUF are processed through a key-controller. This uses the vedic-principles to increase the key length to create 12 keys out of the challenge. Using the vedic principle, ghana, and jata, 3 bits of the challenge are repeated 13 times. For instance, consider three bits b_1, b_2, and b_3. Following is the expansion for the three bits:

$$s_1 = [b_1, b_2][b_2, b_1][b_1, b_2, b_3][b_3, b_2, b_1][b_1, b_2, b_3] \tag{1}$$

Equation 1 is used to generate 12 keys out of the challenge and give to the Arbiter PUF. Out of the 12 keys, 6 keys are selected and sent through AND, OR and NAND logic gates. The outputs of the logic gate are sent to an XOR gate for consolidation. The rest of the keys, 7 - 12, are passed to the XOR gate at the final stage. The final response is collected from the XOR gate and used for cryptographic purposes.

The proposed VXorPUF methods divided into three steps that is presented in Algorithm 1.

1. **Challenge extension using key controller**: The original challenge C_c will pass through key controller where Verdic principle will be applied. The controller will produce extended challenge R_c. The produced key will be divided into 12 partial 64-bit challenges which is represented by C_p. If the requirement of processing controller is valid then it will process further otherwise drop the challenge.
2. **PUF response generation**: Partial challenges C_p will act as input challenge C_a of the PUF. Each challenge will generate unique response R_a for each challenge. In this stage 12 responses will be generated using 64-bit Arbiter PUF.
3. **VXorPUF response production**: After inserting the PUF responses into the OR-AND-NAND block, PUF output is received. This block will generate 64-bit output using 12 64-bit responses. For example, to generate first output bit, bit-1 of first 2 responses will go to AND gate, next two responses first bit will go to NAND gate, first bit of fifth and sixth response will be used as input of OR gate. Three output of logic gates and first bit of response seven to twelve will be the input an XOR gate. The XOR gate

Algorithm 1: Device Enrollment Phase

```
Input  : Challenges ($C_c$) to PUF in IoMT Device
Output : Responses from VXorPUF module $R_v$

Select the challenges for Key Controller $C_c$;
for each controller challenge $C_c$ do
    if Controller requirements met then
        $R_c \leftarrow C_c$;
        // $R_c$ = Controller response
        $R_c = C_p$;
        // Controller response($R_c$) devided into 12 challenges ($C_p$) for
           PUF
    else
        Drop the challenge;
for each challenge $C_p$ (12 times) do
    if PUF requirements met then
        $C_a \leftarrow C_p$;
        // $C_a$ = Arbitter PUF challenge
        $R_a = C_a$;
        // Arbiter PUF Response($R_a$) is considering as input challange
           ($C_a$) of Arbiter PUF
    else
        Drop the challenge;
for each VedaPUF input $R_i$ do
    $R_v \leftarrow$(OR$\oplus$AND$\oplus$NAND) $\leftarrow R_i$;
    // $R_i$ is the combined responses ($R_a$)
    Secure Database $\leftarrow R_v, C_a$;
    // $R_v$ = (OR$\oplus$AND$\oplus$NAND)-PUF output
    // Store the input challenge and VedaPUF output pair in secure
       database.
```

will produce the first bit of the output. Consequently, rest bits will be generated and finally the input challenge of the key controller and the VedaPUF output will be saved in a secure database.

6. Experimental Results

The PUF is designed using a Field Programmable Gate Array (FPGA). A 64-bit arbiter PUF was employed among other PUFs, and it can produce CRPs, satisfying the necessary PUF requirements. Xillinx Basys 3 FPGA was used to prototype the VXorPUF. One FPGA was attached to a Raspberry Pi in the experimental setup to create an MD. FPGAs' PUFs were used to implement the challenges, and linked Raspberry Pis were employed to compile the responses. The output bit for the arbitrator PUF is determined by comparing the amount of time needed to traverse a signal. The work was implemented with the help of Google Colab, BASYS3 FPGA, and Raspberry Pi 4 B+. The CRPs are collected from the PUF module. 500000 keys were selected as a challenge and 500000 responses were collected from the VXorPUF.

The core component used in the VXorPUF prototype was a 64-bit Arbiter PUF. The challenges and the responses were 64-bits in length. Besides modeling attack resistance, the PUF has to satisfy the figures of merit (FoM) for the keys to be used for cryptographic applications. This paper considers three FoMs, uniqueness, reliability and randomness.

6.1. Uniqueness

A uniqueness of PUF is the ability of the module to generate a unique key at the module. A key generated by a PUF for a respective challenge is unique to the module and cannot be generated by a different challenge. Hamming distance is used to calculate the uniqueness of the keys generated from the PUF.

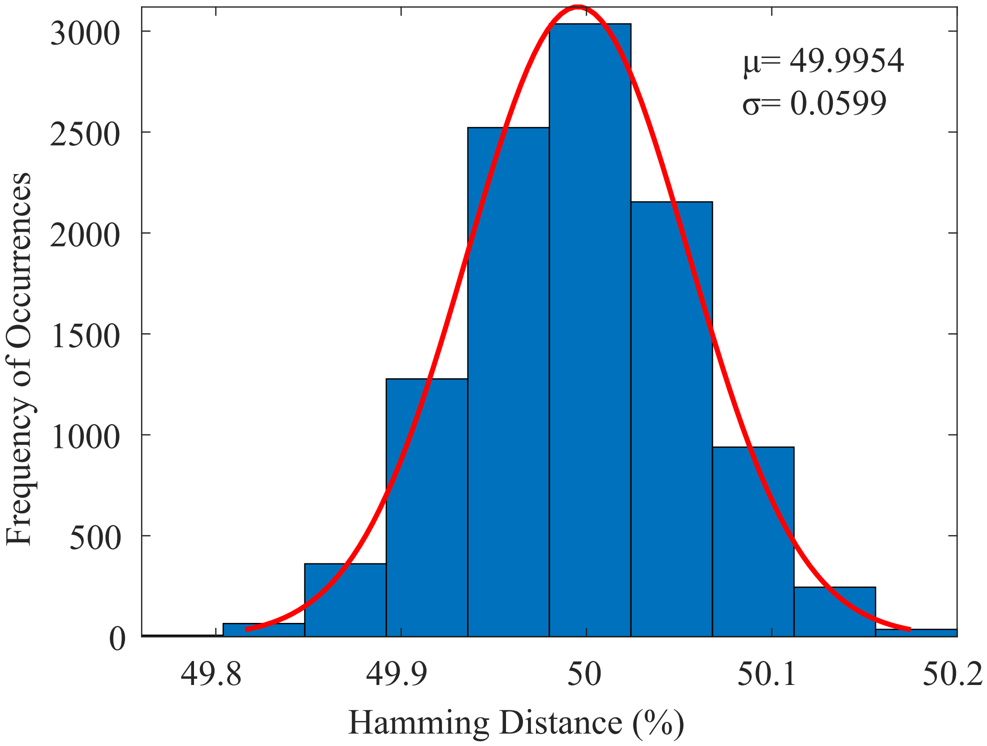

Figure 6. Uniqueness of PUF

Fig. 6 shows the uniqueness of VXorPUF. The ideal hamming distance of a PUF is 50 %. As shown in the figure, the proposed PUF design has a mean uniqueness of 49.9% and a standard deviation of 0.05%. These keys show a value close to the ideal values showing a strong key generation.

6.2. Randomness

Randomness of the keys are the number of 1 and 0 bits in the generated key. A uniform distribution of 1 and 0 in the final key shows a strong resistant to prediction and a better uniqueness. The ideal value of randomness of the PUF keys is 50 %. Fig. 7 shows the randomness of the keys generated by the VXorPUF. As shown in the figure the mean randomness is 49.9 % with a standard deviation of 6.2 %.

6.3. Reliability

Reliability of PUF is the ability to generate a consistent set of CRPs under various conditions. To test the reliability of the PUF, initially, the same challenge is repeated to test the response for multiple runs. The same test is repeated for multiple challenges considered during the testing phase. For given challenges, the VXorPUF showed a reliability of the 99.9 %. The PUF module is tested for reliability under temperature variations. Multiple temperature points were considered, from 50°F through 150°F at 15°F intervals. At each stage, the keys were collected to test for reliability. The VXorPUF showed a reliability of 99.9 % with a consistent generation of CRPs.

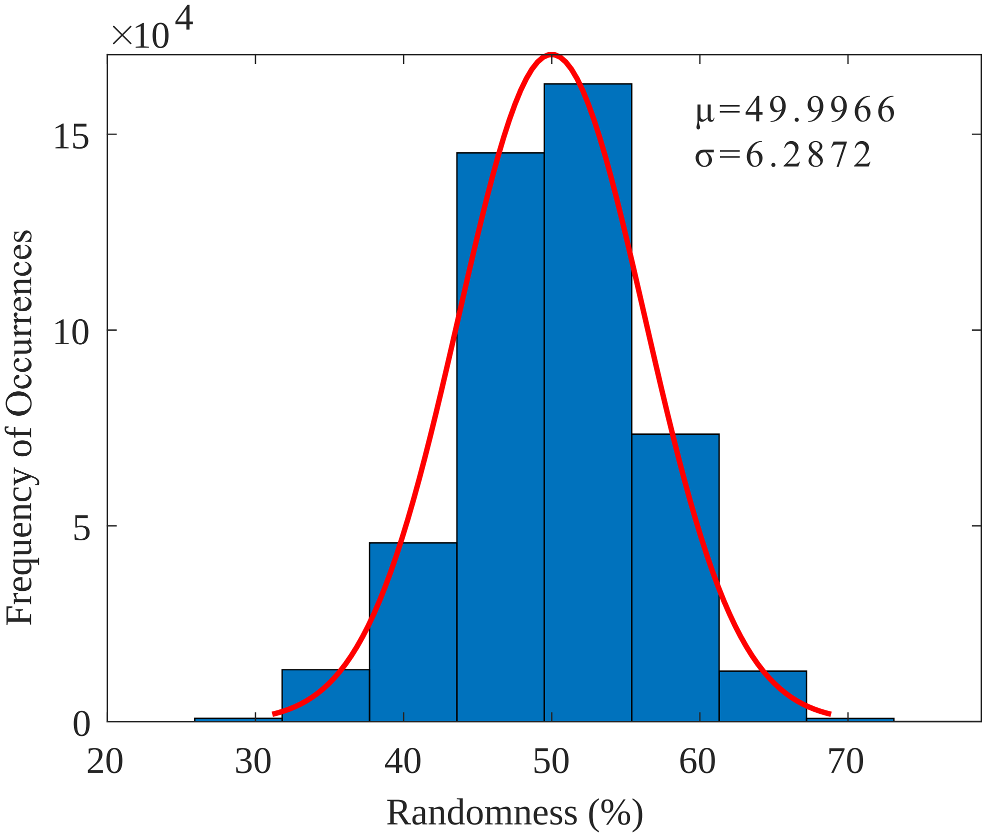

Figure 7. Randomness of PUF

6.4. Uniformity of OAN-XOR-PUF

Fig. 8 shows the overview of OAN-XOR(m-OR, n-AND, p-NAND)-XOR-PUF. The ratio of "0" or "1" response bits in a PUF is known as uniformity. This fraction needs to be 50% for really arbitrary PUF responses[53]. Calculating the uniformity is as follows: [54]

$$Uniformity = \frac{1}{n}\sum_{l=1}^{n} r_l \times 100\%$$

where n is the total number of responses, and this study's uniformity is set to 1%.

In order to indicate uniformity with the proportion of "1," we use the symbol U. Before reaching the uniformity of (m,n,p)-OAN-PUF, we analyzing the uniformity of m-OR-PUF, n-AND-PUF, and p-NAND-PUF.

1. Uniformity of m-OR-PUF:
   If all m inputs are 0's, the output of the OR logic operation will be "0". Uniformity of OR is expressed as,

   $$U_{OR} = 1 - \frac{1}{2^m}$$

   We can observe that, particularly when m is large, m-OR-PUF shows a bias toward response "1".
2. Uniformity of n-AND-PUF:

doi:10.20944/preprints202303.0499.v1

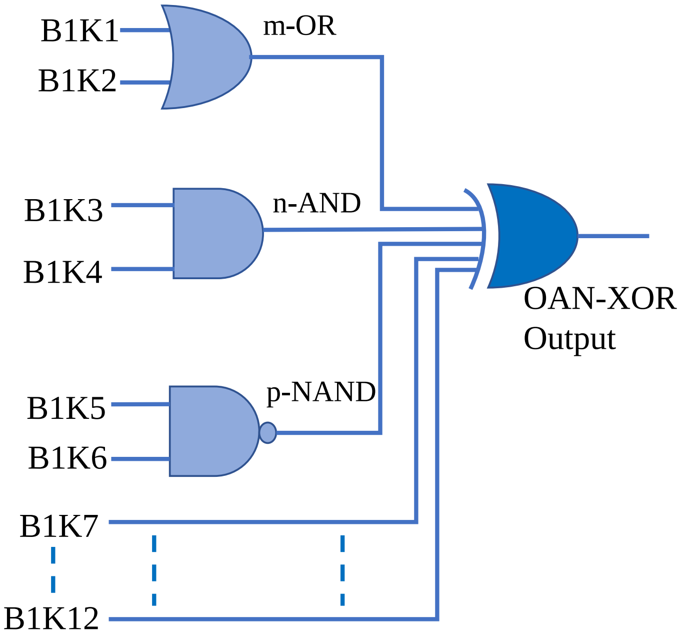

Figure 8. Overview of (m,n,p)-OAN-XOR-PUF

The output of the AND logic operation will be "1" if all n inputs are 1's. The expression for uniformity of AND is,

$$U_{AND} = \frac{1}{2^n}$$

We can observe that n-AND-PUF tends to favor the response "0," particularly when n is large.

3. Uniformity of p-NAND-PUF:
If all p inputs are 1's, the output of the NAND logic operation will be "0". Uniformity of NAND is expressed as,

$$U_{NAND} = 1 - \frac{1}{2^p}$$

4. Uniformity of OAN-PUF:
The response of OAN-PUF is '1', if one of the OR, AND, NAND PUF is '1' and all three equal '1'. The m-OR, n-AND, and p-NAND logic gates all have two inputs, hence m=n=p=2 in this situation.. The OAN-PUF uniformity is defined as follows:

$$
\begin{aligned}
U_{OAN} = {} & U_{OR}U_{AND}U_{NAND} + U_{OR}(1 - U_{AND}) \\
& (1 - U_{NAND}) + U_{AND}(1 - U_{OR})(1 - U_{NAND}) \\
& + U_{NAND}(1 - U_{OR})(1 - U_{AND}) \\
= {} & (1 - \frac{1}{2^m})\frac{1}{2^n}(1 - \frac{1}{2^p}) + (1 - \frac{1}{2^m})(1 - \frac{1}{2^n}) \\
& \frac{1}{2^p} + \frac{1}{2^n}\frac{1}{2^m}\frac{1}{2^p} + (1 - \frac{1}{2^p})\frac{1}{2^m}(1 - \frac{1}{2^n}) \\
= {} & \frac{(2^m - 1)(2^p - 1)}{2^{m+n+p}} \\
& \frac{(2^m - 1)(2^n - 1)}{2^{m+n+p}} \\
& + 1 + \frac{(2^p - 1)(2^m - 1)}{2^{m+n+p}} \\
= {} & \frac{3 * 3 + 3 * 3 + 1 + 3 * 3}{2^6} \\
= {} & \frac{28}{64} \\
= {} & 43.75\%
\end{aligned}
$$

After doing the OAN-PUF calculation, we have demonstrated that the (m,n,p)-OAN-PUF uniformity is 43.75%, which is near to the ideal values of 0.5 %. The m-OR-PUF and n-AND-biased PUF's uniformity does not spread and has no high impact on the (m,n,p)-OAN-PUF's final uniformity.

6.5. Machine Learning Method

Various architectures of PUF were generated through the PUF module and

In this work, 64 bit challenges were generated utilizing an arbiter PUF employing a BASYS 3 FPGA. The data was generated at the lab. For the purposes of making training, validation, and testing, the dataset was divided 80:20. The first 80% of training & validation will be used for training, with the rest for validation.

ML Stages	Amount of Data	Training	Testing
Pre-Processing	500000	400000	100000
Final Stage	455732	364585	91147

Table 1. Data for Machine Learning

The Machine Learning (ML) environment is created using Google Colab pro+ and runs totally in the cloud. The environment setup makes advantage of the NVIDIA Tesla K80, T4, and P100 GPU that is built into colab. Google colab Pro+ uses a 52 Gb high-RAM runtime to create an ML environment.

In this research multilevel binary classification were used. The widely used pattern recognition and classification algorithm logistic regression is most often applied to classification tasks. A logistic regression model was applied. Models based on this architecture consist of four layers, with rectified linear units (ReLU) acting as activation functions in each layer. 50 epochs were run to evaluate the performance of the models and locate the point at which the performance of the validation data leveled off. Different optimizer which were "Adam", "SGD", "RMSProp", "Adadelta", "Adagrad", "Adamax", "Nadam" tried to get the best performance of the machine learning model. Also, various activation function ("ReLU", "Sigmoid", "ELU") were used.

1. Pre-Processing Stage: Fig. 9 shows the training and validation accuracy of pre-processing stage. At this stage, the input and output data were both 64 bits.Accuracy is around 99.78% using activation function ReLU and optimizer Adam. ReLU and Adam outperformed other optimizer and activation functions when such factors were taken into account.
2. Final Stage: Fig. 10 depicts the last stage's training and validation accuracy.After submitting the 64 bit response to the AON-XOR operation, 64 bit data were obtained and used for machine learning at this stage. With the activation function ReLU and Adam optimizer, accuracy is around 49.80%. At this stage, different activation functions and optimizer were tested to compare them and forecast the most accurate model..

To compare the performance of the proposed VXorPUF, the machine learning modeling attack was performed on the Arbiter PUF before the post processing stage of the keys. An accuracy of 49.80% was achieved using the ReLU activation function and Adam optimizer. ReLU and Adam outperformed other optimizer and activation functions compared to the other optimizer. Fig. 10 and Fig. 9 has shown the performance of machine learning for the final stage and pre-processing stages, respectively.

Accuracy			Optimizer
ReLU	ELU	Sigmoid	
49.80%	49.85%	50.00%	Adam
49.85%	49.88%	50.00%	SGD
49.94%	49.85%	50.23%	RMSProp
50.19%	50.14%	49.90%	Adadelta
49.93%	49.82%	49.89%	Adagrad
50.18%	50.11%	50.22%	Adamax
50.17%	50.05%	49.95%	Nadam

Table 2. Analysis the Accuracy of Final Stage for Different Optimizer and Activation function

Table 2 displays the accuracy of final stage while focusing on different activation functions with optimizer. The best performance in this case is provided by the Adam optimizer with the activation function ReLU.

Table 3 demonestrate the comparison analysis of PUF model. Where we have considered the metrics of uniqueness, randomness and Machine learning model accuracy of PUF for comparing previous work with our work. They [49] used MRAM-PUF for their research work, where uniformity response id around 95% though the p-value is higher than

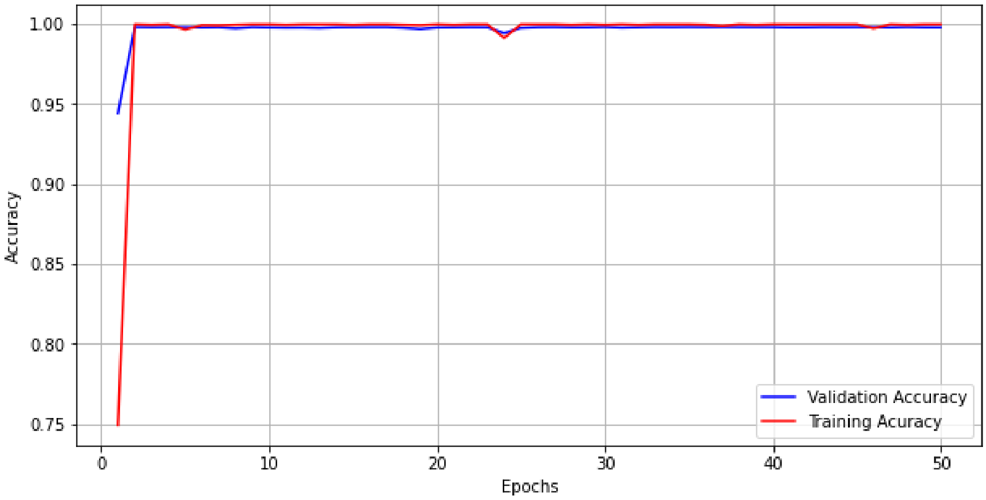

Figure 9. Accuracy of Pre-Processing Stage

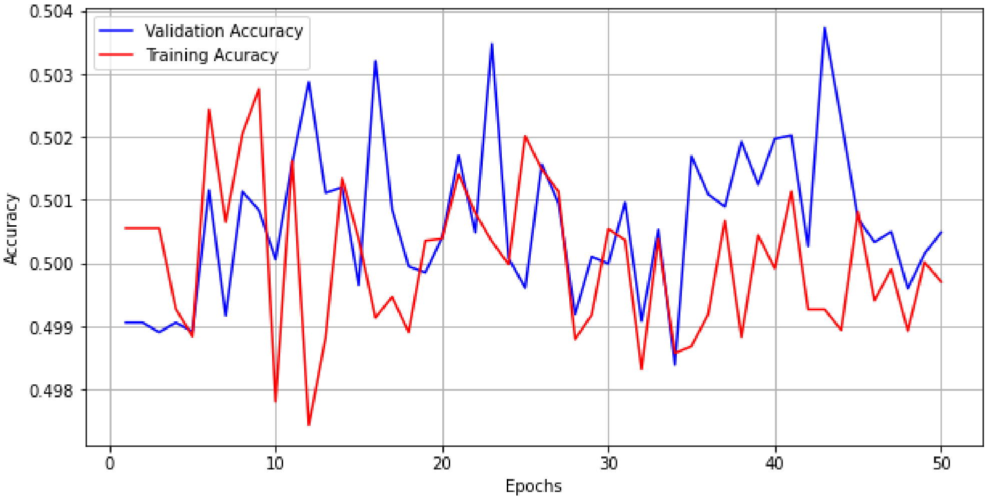

Figure 10. Accuracy of Final Stage

References	Randomness	Uniqueness	ML Models Accuracy
[46], 2020	49.98%	50%	50.24%
[47], 2019	52.8%	49.9%	60%
[48], 2021	—	49.92%	50.72%
[49], 2022	95%	49.76%	53.8%
Our Work	49.995%	49.9966%	49.80%

Table 3. Comparison Analysis of PUF

0.01. Which indicate that their MPUF is highly random. Our ML models accuracy is more encouraging when compared to other researchers' work; we obtained a 49.80% accuracy rate, indicating that our proposed PUF is more trustworthy. Additionally, we came close to optimal values for randomness and uniqueness while considering our proposed PUF.

7. Conclusion and Future Works

As patient personal information is transferred and emergency medical care is required, the healthcare environment's security and privacy are of utmost importance. Using Vedic methodology, we have demonstrated that PUF provides greater dependability and security in resource-constrained smart medical devices in healthcare system as compared to generic PUF-based authentication procedure. We have analyzed three Figures of Merit (FoMs), Uniqueness, Randomness, and Reliability of arbiter PUF and Veda-PUFs, and got the promising outcomes of Veda-PUF for resource-constrained devices. In addition, our proposed model preformed better and achieved the accuracy of 49.80%. In future study, we might consider bulk amount of PUF keys to evaluate how resistant the PUF against machine learning attack.

References

1. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review* **2021**, pp. 1–14.
2. Vaiyapuri, T.; Binbusayyis, A.; Varadarajan, V. Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications* **2021**, *12*, 731–737.
3. Hodgkiss, J.; Djahel, S. Securing Fuzzy Vault Enabled Authentication in Body Area Networks-Based Smart Healthcare. *IEEE Consumer Electronics Magazine* **2022**, *11*, 6–16. https://doi.org/10.1109/MCE.2020.2991387.
4. King, J.; Awad, A.I. A distributed security mechanism for resource-constrained IoT devices. *Informatica* **2016**, *40*.

5. Shoaran, M.; Haghi, B.A.; Taghavi, M.; Farivar, M.; Emami-Neyestanak, A. Energy-efficient classification for resource-constrained biomedical applications. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* **2018**, *8*, 693–707.
6. Mahmud, M.I.; Abdelgawad, A.; Yanambaka, V.P.; Yelamarthi, K. Packet Drop and RSSI Evaluation for LoRa: An Indoor Application Perspective. In Proceedings of the Proceedings of IEEE 7th World Forum on Internet of Things (WF-IoT), 2021, pp. 913–914. https://doi.org/10.1109/WF-IoT51360.2021.9595288.
7. Khor, J.H.; Sidorov, M.; Woon, P.Y. Public Blockchains for Resource-Constrained IoT Devices—A State-of-the-Art Survey. *IEEE Internet of Things Journal* **2021**, *8*, 11960–11982.
8. Siddiqi, M.A.; Tsintzira, A.A.; Digkas, G.; Siavvas, M.G.; Strydis, C. Adding Security to Implantable Medical Devices: Can We Afford It? In Proceedings of the Proceedings of EWSN, 2021, pp. 67–78.
9. Wang, W.; Qiu, C.; Yin, Z.; Srivastava, G.; Gadekallu, T.R.; Alsolami, F.; Su, C. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet of Things Journal* **2021**.
10. Monrat, A.A.; Schelén, O.; Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* **2019**, *7*, 117134–117151.
11. Kouhizadeh, M.; Sarkis, J. Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability* **2018**, *10*, 3652.
12. Al-Jaroodi, J.; Mohamed, N. Blockchain in Industries: A Survey. *IEEE Access* **2019**, *7*, 36500–36515. https://doi.org/10.1109/ACCESS.2019.2903554.
13. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics* **2019**, *36*, 55–81.
14. Diedhiou, O.N.; Diallo, C. An IoT mutual authentication scheme based on PUF and blockchain. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2020, pp. 1034–1040.
15. Asif, R.; Ghanem, K.; Irvine, J. Proof-of-PUF enabled blockchain: Concurrent data and device security for internet-of-energy. *Sensors* **2020**, *21*, 28.
16. Suragani, R.; Nazarenko, E.; Anagnostopoulos, N.A.; Mexis, N.; Kavun, E.B. Identification and Classification of Corrupted PUF Responses via Machine Learning. In Proceedings of the 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2022, pp. 137–140.
17. Lim, D.; Lee, J.; Gassend, B.; Suh, G.; van Dijk, M.; Devadas, S. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* **2005**, *13*, 1200–1205. https://doi.org/10.1109/TVLSI.2005.859470.
18. Zerrouki, F.; Ouchani, S.; Bouarfa, H. A survey on silicon PUFs. *Journal of Systems Architecture* **2022**, *127*, 102514.
19. Lee, J.; Lim, D.; Gassend, B.; Suh, G.; van Dijk, M.; Devadas, S. A technique to build a secret key in integrated circuits for identification and authentication applications. In Proceedings of the 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), 2004, pp. 176–179. https://doi.org/10.1109/VLSIC.2004.1346548.
20. Zalivaka, S.S.; Ivaniuk, A.A.; Chang, C.H. Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response. *IEEE Transactions on Information Forensics and Security* **2018**, *14*, 1109–1123.
21. Kroeger, T.; Cheng, W.; Guilley, S.; Danger, J.L.; Karimi, N. Effect of aging on PUF modeling attacks based on power side-channel observations. In Proceedings of the 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2020, pp. 454–459.
22. Maiti, A.; McDougall, L.; Schaumont, P. The impact of aging on an FPGA-based physical unclonable function. In Proceedings of the 2011 21st International Conference on Field Programmable Logic and Applications. IEEE, 2011, pp. 151–156.
23. Gao, Y.; Al-Sarawi, S.F.; Abbott, D.; Sadeghi, A.R.; Ranasinghe, D.C. Modeling attack resilient reconfigurable latent obfuscation technique for PUF based lightweight authentication. *arXiv preprint arXiv:1706.06232* **2017**.
24. Santikellur, P.; Bhattacharyay, A.; Chakraborty, R.S. Deep learning based model building attacks on arbiter PUF compositions. *Cryptology ePrint Archive* **2019**.
25. Wisiol, N.; Thapaliya, B.; Mursi, K.T.; Seifert, J.P.; Zhuang, Y. Neural Network Modeling Attacks on Arbiter-PUF-Based Designs. *IEEE Transactions on Information Forensics and Security* **2022**, *17*, 2719–2731.

26. Gassend, B.; Lim, D.; Clarke, D.; Van Dijk, M.; Devadas, S. Identification and authentication of integrated circuits. *Concurrency and Computation: Practice and Experience* **2004**, *16*, 1077–1098.
27. Rührmair, U.; Sehnke, F.; Sölter, J.; Dror, G.; Devadas, S.; Schmidhuber, J. Modeling attacks on physical unclonable functions. In Proceedings of the Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 237–249.
28. Kwarteng, E.; Cebe, M. A survey on security issues in modern Implantable Devices: Solutions and future issues. *Smart Health* **2022**, p. 100295.
29. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT communications: A survey. *Sensors* **2020**, *20*, 4828.
30. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the Proceedings of 2019 15th international conference on distributed computing in sensor systems (DCOSS). IEEE, 2019, pp. 457–464.
31. Rahman, M.; Jahankhani, H. Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-attacks. In *Proceedings of Information Security Technologies for Controlling Pandemics*; Springer, 2021; pp. 307–334.
32. Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. *Computer Communications* **2021**, *166*, 110–124.
33. Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. *IEEE Journal of Biomedical and Health Informatics* **2021**, *26*, 1969–1976.
34. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *Proceedings of IEEE Internet of Things Journal* **2020**, *8*, 4485–4497.
35. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies* **2022**, *33*, e4049.
36. Karmakar, K.K.; Varadharajan, V.; Tupakula, U.; Nepal, S.; Thapa, C. Towards a security enhanced virtualised network infrastructure for Internet of Medical Things (IoMT). In Proceedings of the Proceedings of 2020 6th IEEE conference on network softwarization (NetSoft). IEEE, 2020, pp. 257–261.
37. Wazid, M.; Das, A.K.; Rodrigues, J.J.; Shetty, S.; Park, Y. IoMT malware detection approaches: analysis and research challenges. *IEEE Access* **2019**, *7*, 182459–182476.
38. Sadhu, P.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. NAHAP: PUF-Based Three Factor Authentication System for Internet of Medical Things. *IEEE Consumer Electronics Magazine* **2022**, pp. 1–1. https://doi.org/10.1109/MCE.2022.3176420.
39. Yoon, S.; Kim, B.; Kang, Y. Multiple PUF-based lightweight authentication method in the IoT. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), 2021, pp. 1198–1200. https://doi.org/10.1109/ICTC52510.2021.9620972.
40. Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E.; Puthal, D. PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. *Proceedings of IEEE Transactions on Consumer Electronics* **2019**, *65*, 388–397. https://doi.org/10.1109/TCE.2019.2926192.
41. Satamraju, K.P.; Balakrishnan, M. A Secured Healthcare Model for Sensor Data Sharing With Integrated Emotional Intelligence. *IEEE Sensors Journal* **2022**, *22*, 16306–16313. https://doi.org/10.1109/JSEN.2022.3189268.
42. Hu, Y.; Jiang, Y.; Wang, W. Compact PUF Design With Systematic Biases Mitigation on Xilinx FPGAs. *IEEE Access* **2022**, *10*, 22288–22300. https://doi.org/10.1109/ACCESS.2022.3151966.
43. Khalafalla, M.; Gebotys, C. PUFs Deep Attacks: Enhanced Modeling Attacks Using Deep Learning Techniques to Break The Security of Double Arbiter PUFs. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), 2019, pp. 204–209. https://doi.org/10.23919/DATE.2019.8714862.
44. Wisiol, N.; Thapaliya, B.; Mursi, K.T.; Seifert, J.P.; Zhuang, Y. Neural Network Modeling Attacks on Arbiter-PUF-Based Designs. *IEEE Transactions on Information Forensics and Security* **2022**, *17*, 2719–2731. https://doi.org/10.1109/TIFS.2022.3189533.
45. Wang, S.J.; Chen, Y.S.; Li, K.S.M. Modeling Attack Resistant PUFs Based on Adversarial Attack Against Machine Learning. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* **2021**, *11*, 306–318. https://doi.org/10.1109/JETCAS.2021.3062413.

46. Wang, Y.; Xi, X.; Orshansky, M. Lattice PUF: A strong physical unclonable function provably secure against machine learning attacks. In Proceedings of the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2020, pp. 273–283.
47. Zhuang, H.; Xi, X.; Sun, N.; Orshansky, M. A strong subthreshold current array PUF resilient to machine learning attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers* **2019**, *67*, 135–144.
48. Zhang, J.; Xu, C.; Law, M.K.; Jiang, Y.; Zhao, X.; Mak, P.I.; Martins, R.P. A 4T/Cell Amplifier-Chain-Based XOR PUF With Strong Machine Learning Attack Resilience. *IEEE Transactions on Circuits and Systems I: Regular Papers* **2021**, *69*, 366–377.
49. Ali, R.; Zhang, D.; Cai, H.; Zhao, W.; Wang, Y. A Machine Learning Attack-Resilient Strong PUF Leveraging the Process Variation of MRAM. *IEEE Transactions on Circuits and Systems II: Express Briefs* **2022**.
50. Canaday, D.; Barbosa, W.A.; Pomerance, A. A Novel Attack on Machine-Learning Resistant Physical Unclonable Functions. In Proceedings of the 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2022, pp. 25–28.
51. Wang, S.J.; Chen, Y.S.; Li, K.S.M. Modeling attack resistant PUFs based on adversarial attack against machine learning. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* **2021**, *11*, 306–318.
52. Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E.; Baniya, B.K.; Rout, B. Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT. In Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES), 2021, pp. 400–405. https://doi.org/10.1109/iSES52644.2021.00097.
53. Yao, J.; Pang, L.; Su, Y.; Zhang, Z.; Yang, W.; Fu, A.; Gao, Y. Design and Evaluate Recomposited OR-AND-XOR-PUF. *IEEE Transactions on Emerging Topics in Computing* **2022**.
54. Maiti, A.; Gunreddy, V.; Schaumont, P. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. Cryptology ePrint Archive, Paper 2011/657, 2011. https://eprint.iacr.org/2011/657.