A Lightweight Hardware Secure and Reliable Framework using Secure and Provable PUF for IoT Devices against the Machine Learning Attack

[1]Annapurna K Y, [2]Deepali Koppad
[1]annapurnaky@pes.edu, [2]deepali.koppad@msrit.edu
[1] PES University, Bangalore, India
[2] Ramaiah Institute of Technology, Bangalore, India

Received: June 20, 2021. Revised: December 13, 2021. Accepted: January 16, 2022. Published: January 17, 2022.

Abstract— IoT (Internet of Things) has been expanding into various business activities and people's lives; however, IoT devices face security challenges. Further, the establishment of reliable security for IoT constrained devices is considered to be ongoing research due to several factors such as device cost, implementation area, power consumption, and so on. In addition to these factors, hardware security also poses major challenges like above mentioned; further Physical Unclonable Functions (PUFs) offer a promising solution for the authentication of IoT devices as they provide unique fingerprints for the underlying devices through their challenge-response pairs. However, PUFs are vulnerable to modelling attacks; in this research work, a lightweight hardware security framework is designed that provides the security for light edge devices. The proposed hardware security framework introduces the three-step optimized approach to offer a secure and reliable solution for IoT device authentication. The first step deals with the designing of SP-PUF, the second step deals with introducing obfuscation technique into the same, and the third step deals with introducing the authentication mechanism. A machine learning attack is designed to evaluate the model and the proposed model is evaluated considering the different stages. This research work is evaluated in two parts; the first part of the evaluation is carried out for the security mechanism through machine learning algorithm attack i.e., logistic regression, Neural Network, and SVM; further evaluation is carried out considering the PUF evaluation parameter as uniqueness and reliability. At last, comparative analysis suggest that proposed hardware security framework is safe against the machine learning attacks and achieves high reliability and optimal uniqueness.

Keywords—Hardware security, IoT security, Machine Learning, Physically Unclonable Function

I. Introduction

IoT aka Internet of Things is considered as the vast networking paradigm that tends to connect the different objects or things through the sensor technology to the internet; this sensor technology includes computer networks, database technology, communication technology, RFID (Radio Frequency Identification). Moreover, it is estimated that nearly 31 billion devices in the present year could extend up to 75 billion in the year 2025; further IoT extends the data exchange and communication scope from personal computers and servers to the things that are used in normal life. An increase in IoT devices has put a lot more attention to security as increased interconnectivity raises concerns regarding cyber-attacks [1][2]. Thus, it is required to have a secure and robust and secure model which requires confidentiality, data integrity; moreover, considering the huge diversity of IoT frameworks, security assurance is way more challenging than the normal network. The security attacks in the IoT framework include sensitive information leakage, malicious malfunctions, etc. In general, there are two main technologies for IoT security i.e., device authentication and secret key storage. key generation is based on the cryptography technique that requires high complexity. However, in most IoT-based applications, resources are limited; these resources include the battery power, memory, and CPU. Thus, classic cryptographic approach becomes highly improbable to implement in IoT-based solutions; to get rid of that, a lightweight approach is used for IoT security [3] [4].

In recent years, PUF (Physically unclonable function) has emerged as the lightweight IoT based security primitive for authentication; PUF is a novel technology that exploits the manufacturing variability of IC (Integrated Circuit) and acts as IC's fingerprint where input is given as the "challenge" and output is received as "response" [5]. Hence PUF can model CRPs (Challenge-Response Pairs). Furthermore, PUF can be defined as the physical entity that is capable of producing the output depending on the physical structure which is quite

difficult to clone; thus, it provides the flexibility to design efficient security attacks against the various physical attacks including the side-channel attack. PUFs are embedded in the fabrication process and CRPs subset are registered after the fabrication process in the enrolment phase and these CRPs are used while authenticating the device [6]. Moreover, in terms of IoT-based applications, PUF benefits from the authentication protocol where physical characteristics of the transmitter in devices (like Wireless Sensor Network) can be known and secured in the server as a general mechanism [7]. This phenomenon of PUF for lightweight security is considered a promising technique. In general, PUF is classified into two distinctive categories i.e. weak PUF and strong PUF based on the CRPs space. Strong PUFs are used mainly for the authentication protocol and weak PUFS are used for the generation of cryptographic keys. Arbiter-PUF family-like XoR-PUF, Arbiter PUF, and feed-forward PUF are few successful strong PUF that have been identified. However, rise in concept of machine learning has raised a bar for the hardware security; machine learning attack involves training the model in efficient way to predict the response through iterative approach [8]. Thus, due to the characteristics of machine learning model and well organized algorithm most of the PUF structure fails and this causes failure of hardware security framework. Moreover, apart from the efficiency of machine learning algorithm there are other reasons such as relying on recent conjunctures that are made from the empirical findings. Thus, there are several research gaps which have been discussed further in second section and it suggests that there is an urgent requirement of hardware security framework that can offer secure and reliable solution to the light edge devices like IoT devices.

A. Motivation and contribution of research work

In recent years, advancements in various technologies like communication platforms, wearable technology, and sensor technology have caused the huge data deluge in the IoT domain and further advancement had caused security as a concern from the hardware perspective. Moreover, IoT security should be a lightweight mechanism. PUF is a recent promising mechanism that gives the hardware security for IC application; PUF tends to exploit the intrinsic process which maps the challenge set to response set. Furthermore, PUF is considered device-specific hence it can be used for the authentication and identification of the IC and key generation-based cryptographic method. In recent years, the development of Machine learning has caused and exposed the various vulnerabilities in the PUFs including non-invasive, semi-invasive, and invasive attacks. Thus, motivated by the application of PUF and challenges, this research work designs a hardware security framework using the PUF technique which helps to survive against the various machine learning attack.

1. This research work designs and develops a hardware security framework for secure and reliable solution to the light edge devices security. Further, considering the hardware security primitive, research analyses the different types of strong PUF and highlights the shortcoming against machine learning;
2. Proposed hardware security framework is carried out in three stages i.e., designing the SP-PUF architecture is introduced to secure the devices, second step includes designing an optimal obfuscation technique is designed to hide the mapping relations among challenge and response. Third and last step includes introducing an authentication protocol is introduced to avoid direct access to the response.
3. A machine learning attack is designed to evaluate the model and the proposed model is evaluated considering the different stages.
4. The proposed security framework is evaluated in two parts; the first part is evaluated for security under the ML attack like logistic regression, Neural Network, and SVM algorithm; the second part of the evaluation is PUF architecture evaluation in terms of reliability

This particular research is organized such that the first section starts with a background of IoT and related hardware security; further development of PUF is discussed along with its vulnerabilities against the machine learning attacks. Moreover, the first section ends with the motivation and contribution of the research work. The second section reviews the various PUF based security mechanism for hardware security; further, their shortcomings are highlighted along with their methodologies. A novel SP-PUF (Secure and provable PUF) along with the different optimized processes is mathematically presented in the third section of the research work. At last, performance evaluation for security mechanism and evaluation mechanism is carried out in the fourth section of research.

II. Related Work

In this section of the research work, we discuss the various existing technique i.e., PUF based authentication that has focused on IoT security. We also focus on the various shortcoming of these research works. PUF based authentication is exploited for mitigating the concern regarding the key storage on vulnerable devices [11] [12]. In general, these discussed PUF based authentication mechanisms are lightweight, still, they suffer from different types of vulnerabilities such as impersonation attacks, replay attacks, and modeling attacks. Further, for device authentication and device security; [13] developed PUFs to create the private and public keys in the IoT networks, this particular technique is proven to be robust to replay attacks. However, it is computationally intensive; [14] presented an authentication approach where generated challenge bit is considered to the function of its previous one. Moreover, it is proven to be resilient against modeling attacks, however, leakage of a single challenge bit makes the process vulnerable for impersonation attacks. Further, obfuscation technique was proposed in [15] where challenge bit is mutated before PUF implementation, hence the response is generated for the mutated challenge and it does not respond directly to the challenge to avoid the interception. Thus, this technique tries to mislead the adversary through wrong CRPs injection to the designed

dataset to train the PUF model. However, all the above-discussed phenomena decrease the hardware overhead despite a decrease in the accuracy of PUF modeling. Further, [16] used strong PUF along with the obfuscation technique along with symmetric encryption approach created through the key generation using weak PUF approach; despite combining both types of PUF, it faces the area overhead. [17] proposed the obfuscated based PUF which was based on the noise bifurcation; however, it was compromised by the evolution strategy. Dual PUF strategies, one fake and one genuine PUF based PUF were designed where genuine PUF were utilized for the authentication whereas fake one is used for misleading the adversary, this adversary includes the eavesdrops of transmission line and provides the security [18] [19]. However, this technique suffers from power and area overhead; also there is an increase in traffic while exchanging the redundant Challenge-response pair. To overcome such issues, [20] designed an adversarial-based model for fooling the attacker that eavesdrops on the challenge-response; moreover, this approach tries to change the response considering the periodic manner. Furthermore, due to recent rise in Machine learning based algorithm PUF were exposed badly, thus few ML resistance mechanisms were developed and categorized into CRP obfuscation and structural non-linearization. structural non-linearization techniques [21] [22] were able to implement the CRPs mapping through developing the non-linear PUF structure. However, these techniques were not reliable and also, they can be modelled with high accuracy; further CRP obfuscation techniques were developed in [23] – [27] which tends to prevent the machine learning attackers to collect the CRP using the obfuscation technique. moreover, the current obfuscation technique has several disadvantages such as vulnerabilities against the advanced machine learning approach like Neural Network, expensive obfuscation technique, and reduction in reliability [28].

III. Proposed Methodology

Hardware security is a critical research area for IoT. PUF is one of the emerging hardware primitive to implement the security protocol. In this section, we design and develop a lightweight hardware security framework using the novel PUF architecture.

Fig 1. shows the workflow of the research work. At first, we analyze the different PUF architecture such as arbiter PUF, bistable PUF, and Ring oscillator PUF. Next, considering this PUF, we design a novel SP-PUF (Secure and provable PUF) to avoid cloning, later an obfuscation technique is implemented to obfuscate the relationship among the challenge and final response. Which means it tends to hide the mapping relationship among challenge and response.

A. Preliminaries for designing the novel PUF architecture

Physically unclonable function aka PUF is an optimized IC (Integrated Circuit) that takes input and generates a response that is not stored in memory.

General equation for PUF is given as $g: Y \rightarrow Z, Y\ belongs\ to\ [0,1]^{\Lambda}$ where g indicates one-way functions which map variable Y to Z. PUF generates various responses to the same challenge considering the ICs fabrication process that tends to provide uniqueness. Moreover, this characteristic makes PUF more unclonable as any physical attempt produces a whole other response as it highly impacts the generation process. Thus, considering the characteristics, it is used for privacy, access control, key generation, data integrity, and authentication. Also, PUF is energy-efficient and cost-effective.

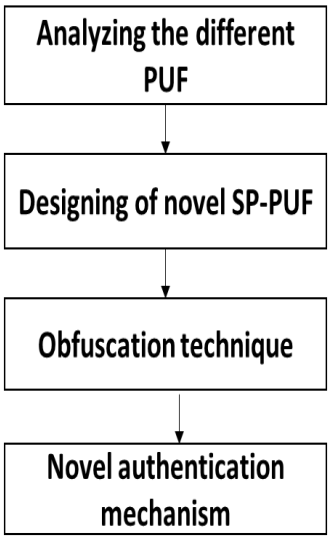

Fig. 1 Proposed PUF based secured framework for IoT device

Considering the security point of view, PUF structure can be described as at first, the server selects the challenge and responses are stored before it gets deployed; further these are used for security primitives. Once PUF is deployed, each communication seeks verification with CRP (Challenge-Response Pair). Once the server starts the communication, it sends the challenge to the node. Moreover, while designing the PUF architecture, PUF should hold the below characteristics.

1. Ideal PUF holds the randomness and distinct response for the different devices.
2. Reliability plays a major role in designing the PUF architecture, hence it should be consistent and reliable for given challenge considering the different environment.
3. Random response should be observed for the different challenge that makes difficult to model.

Furthermore, we discuss few successful PUF that has helped in designing the novel SP-PUF.

A 1. Arbiter PUF

Arbiter PUF as shown in Fig 2. is one of the strongest PUF which comprises two parallel multiplexer chains with $n-stage$; moreover, challenges are the inputs of multiplexers. In general, two distinctive multiplexers having the same stage share single input that determines signal transmission in either a cross way or parallel way.In

architecture, signal parameter $\boldsymbol{T}$ is input, propagation on two paths results arbiter of two signals.

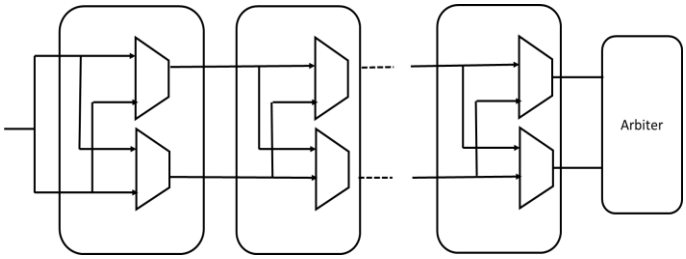

Fig. 2 Arbiter PUF

In general, Arbiter PUF is represented through delay model. Total delay model is formulated through propagation delay in every stage and given as:

$$\psi = \breve{\Theta}^{U}\ \breve{\Xi} \quad (1)$$

In (1), $\breve{\Theta}$ indicates the feature vector which further $\breve{\Xi}$ is function parameter of o bit challenge on $\mathbb{C}$ is given as:

$$\breve{\Xi}(\breve{\mathbb{C}}) = \left(\breve{\Xi}_1(\breve{\mathbb{C}})\ \breve{\Xi}_2(\breve{\mathbb{C}})\ \breve{\Xi}_3(\breve{\mathbb{C}}) \dots\dots\dots \breve{\Xi}_n(\breve{\mathbb{C}})\right)^T \quad (2)$$

In (2), $\breve{\Xi}_J(\breve{\mathbb{C}}) = \prod_{j=k}^{o}(1 - C_i), k = 1,2,3 \dots\dots, l$. Further, if ψ is greater than 0, the output of PUF i.e., $s = 1$, let's consider an output parameter $u = 2 * s - 1 (u\ belongs\ to\ [-1,1])$

$$t = sgm(\psi) = \text{sgm}(\breve{\Theta}^T\ \breve{\Xi}) \quad (3)$$

A 2. Bistable Ring and Ring Oscillator PUF

In general, a bistable ring shown in Fig 3. Comprises an even count of inverters to form the steady-state; this state among the nearest inverters gets the output as a single-bit response whereas ring oscillator PUF uses the delay difference of two ring oscillators with odd inverter numbers for generating the single unit response.

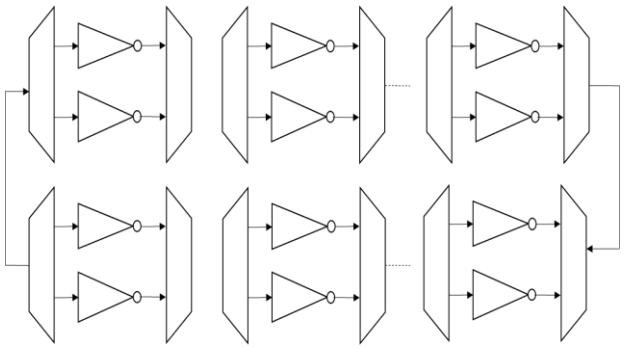

Fig. 3 Bistable ring structure

Further, configurable Ring Oscillator (RO) shown in Fig 4. selects the highest delay difference to improvise the PUF reliability using the multiplexers at every stage of the ring oscillator. In configurable RO different challenges give different responses. However, in every stage delay can be mapped, thus it is considered to be highly vulnerable to machine learning (ML) - based attacks like logistic regression, neural network, and SVM. Further, a more integrated approach combines the two distinctive PUF i.e., ring oscillator PUF and bistable ring PUF. To avoid the ML-based attack parity was utilized. Moreover, when the availability of '1' is even, then it works as the bistable Ring and if it is even then it acts as the ring oscillator; to avoid the ML attack, obfuscation technique is applied. Once the PUF is analyzed through the reverse engineering process, the obfuscation technique is exposed and this makes it useless. Furthermore, using the neural network approach, it is easy to attack and prove that they are efficient.

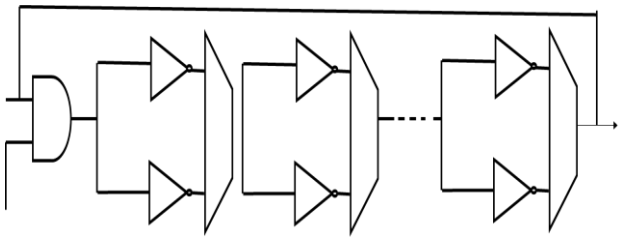

Fig. 4 Configurable Ring oscillator PUF

B. Secure and Provable (SP) – PUF

In this section the design and development of SP-PUF i.e., secure and provable PUF is discussed. Obfuscation mechanism is optimized along with authentication protocol. As shown in the Fig 5. front part of SP-PUF comprises multiplexers and inverters. Further, verification of the corresponding inverter is carried out through a challenge signal as the input to a multiplexer which further shows that if the challenge bit is zero then inverters are not selected. Signal transmission is determined by passing the challenge to a multiplexer. If the challenge bit is zero, then the path is not changed. SP-PUF possesses various working states. Hence, considering the various working states response is created through arbiter set and frequency counter (FC).

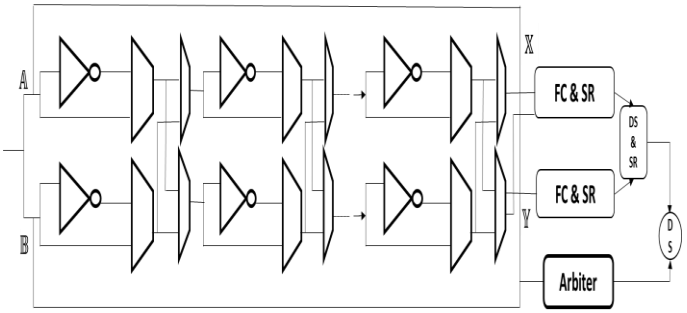

Fig. 5 SP-PUF architecture

Figure 5. represents one of the states of SP-PUF. The working state is explained using the following points.

- When the number of 'one' on even position challenge is 'zero' then the output would be from the signal $\mathbb{A}$ gets output from $\mathbb{X}$; also signal $\mathbb{B}$ gets output from $\mathbb{Y}$. In here if a number of 'one' on the challenge is odd then it works as the distinctive ring oscillator.
- FC indicates the frequency counter which is chosen for the rectangular module; further, the two links tend to generate the difference among the ring oscillator.

- When the number of 'one' on then even position challenge is even then it acts as the two distinctive bistable PUF.
- Moreover, to improvise the compatibility among the odd, XOR as exclusive direct sum i.e., DS is used to generate 'one' bit response.
- It does not matter whether a count of 'one' on the odd position is either even or odd, the complete signal forms a stable ring.
- At last, if the count of 'one' on even position challenge is odd, the signal $\mathbb{A}$ will be output form signal $\mathbb{Y}$ and $\mathbb{B}$ will be output from $\mathbb{X}$. Moreover, if the odd position is found to be none then it acts as the arbiter PUF.

SP-PUF holds the capability of selecting the working state flexibly and further with parity positions in the challenge makes SP-PUF more configurable. Further, o with the power of two is the challenge bits given to the multiplexer in o stage and indicated through $2o$; even position of the bits in the given challenge is denoted through $(\mathbb{C}_2, \ldots . \mathbb{C}_{2o})$ and odd position is given through $(\mathbb{C}_1, \mathbb{C}_3, \ldots . \mathbb{C}_{2o-1})$. Moreover, an odd position is used for choosing whether the inverter is connected to the particular link or not and even position depicts the transmission path occurrence between two links.

The figure 6 shows the different states of SP-PUF which can be explained through the parity perspective i.e., number of one in a given challenge.
If the "1" changes its bits to 0 on an even position, Q generates output in form of O and S generates the signal P as the output. If '1' on even position is odd then it behaves like the two distinctive ring oscillator PUF; also, comparator is chosen to work through a vertical rectangular module and oscillation frequency counter is chosen to work on the horizontal rectangular.

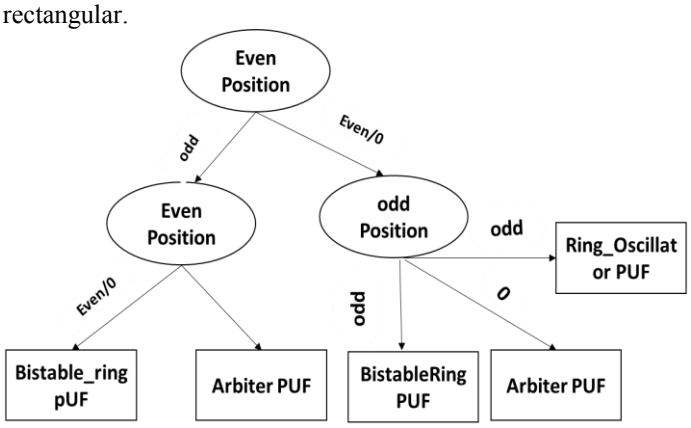

Fig. 6 Different states of SP-PUF

Two distinctive links are made to generate the unit bit response between their ring oscillator by frequency. It is observed that if 1 challenge bit is even on the even position then it acts as a two distinctive bistable ring PUF; working of SP-PUF is given as:

$$\begin{aligned} \mathbb{C}_{\beth} &= \mathbb{C} + S_{\lambda} \\ S_{\beth} &= g_{SP}(\mathbb{C}_{\beth}) \\ S_{\lambda} &= g_{SP}(\mathbb{C}_{\beth}) \\ S &= S_{\beth} + S_{\lambda} \end{aligned} \tag{4}$$

In (4), g_{SP} is indicated as the SP-PUF function; considering the Fig 6. there are four distinct cases of f_{CT}. In the cases shown below g_{sp} is the functionality of arbiter PUF, g_{BR} indicates the functionality of bistable ring oscillator PUF, g_{RO} indicates the ring oscillator PUF.

Case1: $g_{sp}(\mathbb{C}_{\beth}) = g_{sp}(\mathbb{C}_{even})$ where $\sum_{j_{odd}}^{2o} \mathbb{C}_{\beth}$ is zero

Case2: $g_{SP}(\mathbb{C}_{\beth}) = g_{BR}(C_{OSPOo})$ where $\sum_{j_{even}}^{2o} \mathbb{C}_{\beth}\ mod2$ is unit or $\sum_{i_{even}}^{2o} C_{xor}\ mod2$ is non-zero

Case3: $\sum_{j_{even}}^{2o} \mathbb{C}_{\beth}\ mod2$ is zero, $\sum_{j_{odd}}^{2o} \mathbb{C}_{\beth}\ mod2$ is zero and $\sum_{j_{odd}}^{2o} \mathbb{C}_{\beth}$ is non-zero $g_{SP}(\mathbb{C}_{\beth}) = g_{BR}(\mathbb{C}_{OOO}) + g_{BR}(\mathbb{C}_{PSP})$

Case4: $\sum_{j_{odd}}^{2o} \mathbb{C}_{\beth}\ mod2$ is unit, $\sum_{j_{even}}^{2o} \mathbb{C}_{\beth}\ mod2$ is zero where $g_{sp}(\mathbb{C}_{\beth}) = g_{RO}(\mathbb{C}_{\mathbb{AXA}} + \mathbb{C}_{\mathbb{BYB}})$

To summarize, the proposed obfuscation technique generates $2o \times 9$ cases.

C. *Security framework with machine learning attacks*

The Fig 5. suggests that the frequency of inverter be f_i with inverter i; to clone the ring oscillator PUF, the frequency difference among two columns creates the response. Let's consider any parameter $E = e_1, e_2, \ldots . , e_O$ represents the frequency difference among the inverters. $e_j = g_j - g_{o+j}$ is computed and the frequency difference for given unit time ð between lower and upper path is computed through the below equations.

$$g' = ð. \sum_{j=1}^{o} (g_j \times \mathbb{C}_j) \tag{5}$$

In (6), $\mathbb{C}$ indicates the challenge, then further assumptions can be made. If the frequency difference among the lower and upper paths is less than or equal to zero, then ring oscillator PUF is zero. Further, a response is one, if the frequency difference is greater than zero. Thus, using the above assumption, accuracy can be detected up to 99%. Let's consider c_j as the strength of NOR gate(bottom) of given jth stage; also consider u_j as the difference among the up and down strength of the NOR gate(top). Odd stages contribute to the positive response having strength $-u_j$ and even stage contributes positive response with having a strength u_j. Further, to differ the even and odd response, if the challenge bit is 0 then a positive response is written as $(-1)^j u_j$ and if the challenge bit is one then positive responses s given as $(-1)^j u_j$. For further convenience, we adopt the ξ_j and ς_j parameter and considering the jth stage, a positive response is formulated as: $\xi_j + \mathbb{C}\varsigma_j$ with $\mathbb{C}_j\ belong\ to\ (-1,1)$.

$$t' = \sum_{i=1}^{o} (\xi_j + \mathbb{C}\varsigma_j) \quad (6)$$

Refer to (6), $\mathbb{C}_j$ is jth challenge; further below assumption can be made. If t' is less than or equal to zero, then the response is zero, and if $t'$is greater than zero then the response of bistable ring PUF is one.

D. Modelling based on machine learning approach

Machine learning based model requires the training and testing data to evaluate the model. Also, the neural network based approach is considered as the highly preferable for attacking. Thus, a neural network based algorithm is developed to make the PUF provable against attacks. Here, CRPs are collected from different states of PUF, then using the algorithm given below in the table I, the proposed model is proved with improved accuracy and efficiency.

Table I. Neural Network Algorithm

Input: Challenge and Response Pairs Output: modeling accuracy to prove the security	
Step1:	Parameter initialization of neural network, set size $\mathbb{C}$
Step2:	For j= 0 to O) do If (number of one in $\mathbb{C}_j$==odd) then
	Substep1: initialize e_1 and e_2 with random process
	Substep2: Add $\mathbb{C}_j$ to the training set of e_1 and e_2

	If ($e_1 == better\ accuracy$)
	Add $\mathbb{C}_j$ to e_1
	Else if ($e_2 == better\ accuracy$) then
	Add $\mathbb{C}_j$ to e_2
	endif

Step3:	IF ($e_1\ and\ e_2 == threshold$) then
	Break
	Endif

Step4:	Else if If(number of one in $\mathbb{C}_j$==odd) then Substep1: initialize e_3 and e_4 with random process
	Substep2: Add $\mathbb{C}_j$ to the training set of e_3 and e_4 If ($e_1 == better\ accuracy$)
	Add $\mathbb{C}_j$ to e_1 Else if ($e_2 == better\ accuracy$) then Add $\mathbb{C}_j$ to e_2 end if

Step5:	If ($e_3\ and\ e_4 == threshold$) then
	Break
	End if
	End if

Step6:	End for

Here, the four distinctive working models are considered, which predict the better idea of being a strong PUF; moreover, prediction accuracy is computed through adding the new CRP and we use the model for training purpose. Considering the algorithm given in table I, e_1 and e_2 indicates the odd and odd-even challenge; also, even odd and even challenge modes are presented through e_3 and e_4. If the model accuracy increases by adding the new CRP, then CRPs are added to the dataset of a given model. This particular process is repeated until it reaches the threshold. This indicates the particular PUF mode has been breached through the designed algorithm and further training process is stopped.

E. Optimization of obfuscation mechanism

The active state of SP-PUF is determined through parity number in a given position of '1' in even positions. In case if attacker directly gathers CRP and classify it into three distinct categories based on the unit number is even and odd positions; this causes the successful cloning. Hence, here we designed an optimal and novel obfuscation technique that stops the revealing of any original response and challenge.

The Fig 7. shows the working of obfuscation technique, it suggests that the it is possible to access the circuit through the machine learning attack. Which can be described as six different states starting with the input challenge followed through PUF stages with R generation to obtain output.

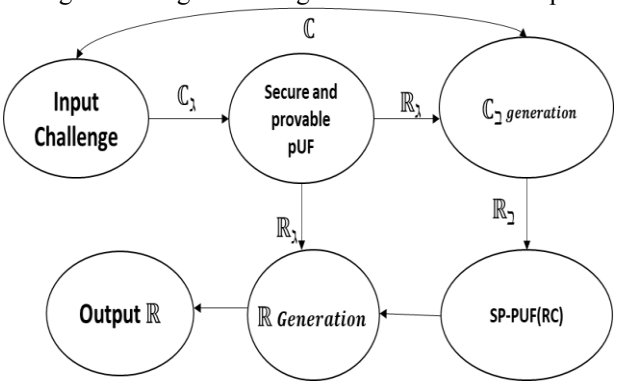

Fig. 7 Optimized obfuscation technique

To attack the circuit, the attacker divides the original data of CRP into two categories i.e., even or odd. Let's Consider that first phase of response is XORed along with the challenge C to create the real challenge C'. Although the attacker does not know the value of C', there is a chance of knowing the parity of "1" count in C' with 50% probability. Further, the probability of classification is computed through the equation (8).

$$class\_prob = \mathbb{C}_o^l 0.5^l 0.5^{o-l} \quad (8)$$

Referring to (8), 'l' indicates the classified pair and o indicates the CRP number. The obfuscation technique comprises the dual step mechanism i.e., initialization and obfuscation. In the initialization step, once SP-PUF is designed, we tend to verify CRPs stability through $\aleph_\lambda = [\mathbb{R}_\lambda, \mathbb{C}_\lambda]$ and it is stored in the server. In the obfuscation step, the server creates a challenge as C and through the random process $\aleph_\lambda$ pair is chosen which

further sends the $\mathbb{C}_\lambda$ and $\mathbb{C}$ to verify. When the device gets $\mathbb{C}$ and $\mathbb{C}_\lambda$, SP-PUF creates $\mathbb{R}_\lambda$ in PUF after giving input as $\mathbb{C}_\lambda$; a further real challenge $\mathbb{C}_\beth$ is created through XORing $\mathbb{C}$ and $\mathbb{R}_\lambda$, also $\mathbb{C}_\beth$ is given of SP-PUF to get $\mathbb{R}_\beth$ as working states. At last $\mathbb{R}$ is created through $XORing$ $\mathbb{R}_\lambda$ and $\mathbb{R}_\beth$, these are further parted into $\mathbb{R}_1$ and $\mathbb{R}_2$.

To improvise the security, SP-PUF use the obfuscation technique to provide the secrecy of relationship mapping between challenge-response pairs. An attacker is required to get the final response $\mathbb{R}$, challenge $\mathbb{C}$, and state's challenge as$\mathbb{C}_\lambda$; hence this obfuscation technique makes the attacker face a major challenge when trying to attack SP-PUF. To get $\mathbb{C}_\beth$, an attacker needs to get $\mathbb{R}_\lambda$ whereas the proposed obfuscation technique does not provide access to the $\mathbb{R}_\lambda$ this makes the proposed technique much more secure against Machine Learning attacks. Hence, to improvise the security solution, SP-PUF use the optimized obfuscation technique that hides mapping relationship among response and challenge pairs; to hack, an attacker requires the $\mathbb{C}_\lambda$, response $\mathbb{R}$, original challenge $\mathbb{C}$ to clone the SP-PUF. Considering the designed obfuscation technique, as our PUF model is the high precision SP-PUF; to clone the model, an attacker requires $\mathbb{C}_\beth$, before that they require $\mathbb{R}_\lambda$.

F. Authentication

In this section, we design dual authentication step i.e. initialization and authentication; In the initialization phase a $\mathfrak{E}_i$, $\aleph_\lambda$ is stored on the server; this server is enrolled through a given device by gathering $\mathbb{R}_\beth$ and soft model parameter i.e. n_j is trained for SP-PUF, further direct access $\mathbb{R}_\lambda$ is locked. In the authentication step, the server sends random prepared challenge and $\aleph_\lambda$ to a device that further generates the end response $\mathbb{R}$. The server adopts the soft model m to create an obfuscated response R', a further server receives $\mathbb{R}$ and authenticates; also server compares the hamming distance among $\mathbb{R}'$and $\mathbb{R}$ is bitwise. Hence, if the hamming distance $(\mathbb{R}, \mathbb{R}')$ is greater than τ then the authentication fails else it forwards. Authentication protocol includes three; first step includes generation of random challenge $\mathbb{C}_j$ and save$\aleph_\lambda$, second step includes training the soft model n_j third step includes Generation of random challenge $\mathbb{C}$.

IV. Performance Evaluation

This section of the research evaluates the proposed SP-PUF based secure architecture. Evaluation is carried out in two different security aspects, the first aspect is machine learning attack and the second aspect is evaluation of PUF considering its parameters like uniformity, uniqueness, and reliability. To perform the analysis, we have used python as the programming language along with a machine learning library like tensor flow, NumPy and panda.

A. Security evaluation

In this section, we use machine learning attacks namely neural network, logistic regression, and SVM (Support Vector Machine). These algorithms are based on machine learning.

A1. Logistic Regression

In the case of device authentication, the occurrence of response is either zero or 1, this is considering as the binary classification problem in machine learning. Logistic regression is considered as one of the fast and efficient algorithms, it has several inputs in the form of vector i.e. $C = (x_1, x_2, \ldots x_n)$ and output is obtained as Y through giving input to the classifier. The formula for same can be given as $Y = g(w_0 + w_1x_1 + w_2x_2 + \cdots . + w_nx_n)$. This approach uses the sigmoid function to achieve the Y closer to 1. Hence, we evaluate the three distinctive PUF i.e., integrated PUF, Configurable-Ring Oscillator PUF, and the proposed SP-PUF considering the logistic regression attack as shown in Fig 8, Fig 9 and Fig 10.

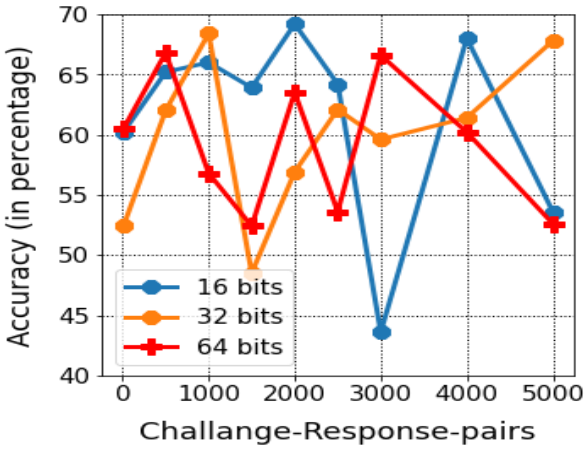

Fig. 8 Integrated PUF

Fig 8 shows the accuracy of Integrated PUF considering the different bits i.e., 16, 32, and 64 bits. Up to 5000 challenge-response pairs are considered for evaluation. In the Fig 8. it is observed that the accuracy level stays between 50-70% which is considered as a good estimation. Evaluation was carried out on a maximum of 5000 CRP.

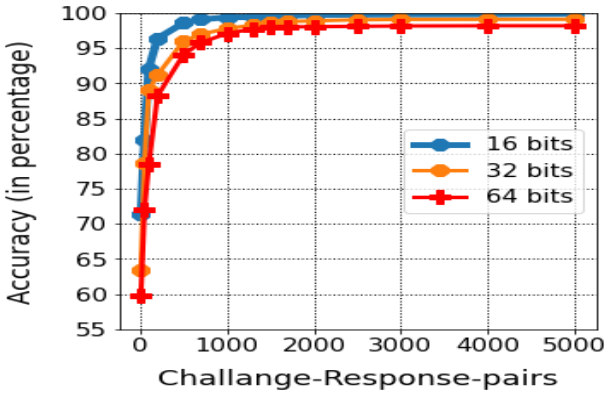

Fig. 9 Configurable Ring Oscilator PUF

Fig 9 shows the ring oscillator PUF considering the different states i.e., 16, 32, and 64 bits. It is observed that accuracy remains high which indicates that ring oscillator PUF is highly vulnerable against the logistic regression attack. Considering the logistic regression attack, high accuracy of up to 99% is observed which shows that this PUF is highly vulnerable.

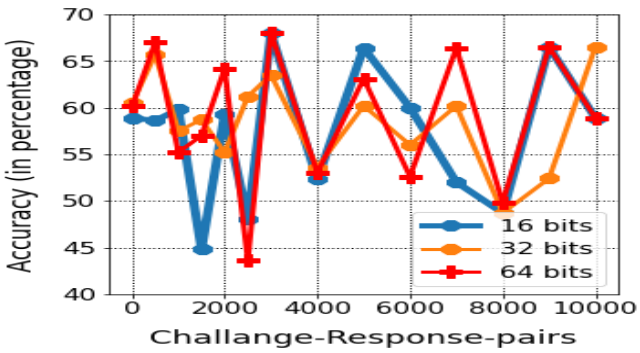

Fig. 10 SP-PUF

Fig 10. shows the accuracy performance of SP-PUF considering the different states i.e., 16 bits, 32bits and 64 bits; it is observed that the proposed SP-PUF performs marginally better with 50-65% of accuracy varying the challenge-response up to 10k pairs.

A2. Neural Network

In general, a neural network is a computing model which is inspired by a biological neural network; moreover, neural networks are nothing but a collection of connected units known as artificial neurons.

Neural Networks can optimize the weight parameter through training to fit for the suitable function. In this approach, each neuron comprises a minimum of one layer and, an output layer and activation function such as sigmoid. The characteristics of Neural Networks make the model learn so efficient that it can attack any convention PUF. A typical artificial neural network is as shown in Fig 11.

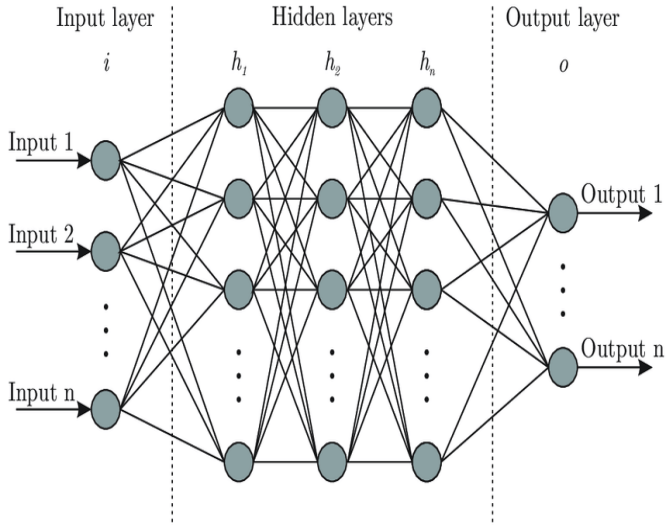

Fig. 11 Typical artificial neural network

Fig 12. shows the vulnerabilities of integrated PUF, through the figure it is observed that as the CRP increases there is marginal growth in accuracy which shows the high probability of getting attacked. Throughout the performance the accuracy of integrated PUF stays between 60-99%.

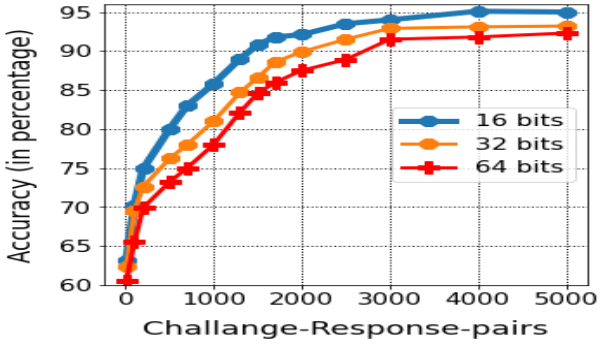

Fig. 12 Integrated PUF

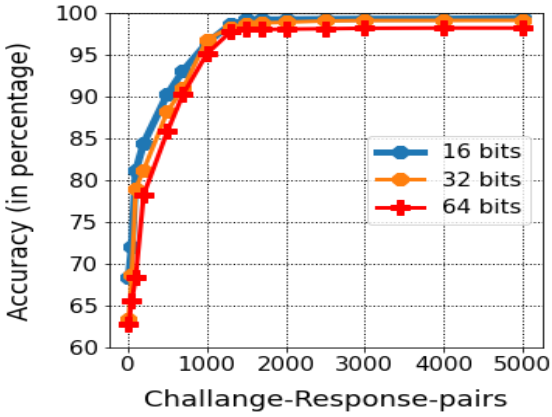

Fig. 13 Ring oscillator PUF

Similarly, Fig 13. shows the accuracy evaluation of Configurable Ring Oscillator and it is observed that neural network observes accuracy of 60-99% which is highly vulnerable. Fig 14. shows the Neural Network attack on the SP-PUF and it is observed that the accuracy stays between 52% to 58% for 10000 CRPs.

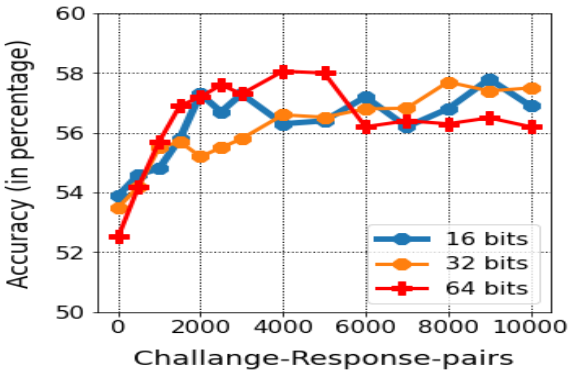

Fig. 14 SP-PUF

A3. SVM-ML algorithm

SVM is also known as the support vector machine that is capable of performing the binary classification through the mapping. This mapping is carried out to the known instances in the higher dimensional space. In well-trained SVM, kernel as a function is used for solving the selection of support vectors and the classification problem. In general, three distinctive kernels are used i.e., linear, multi-layer and radial

basis. A good classifier requires balancing of regularization coefficient.

Fig 15. shows the attack on integrated PUF using the SVM algorithm; through the figure, it is observed that the accuracy of integration PUF against the SVM algorithm remains between 55 to 85 % which is considered quite vulnerable.

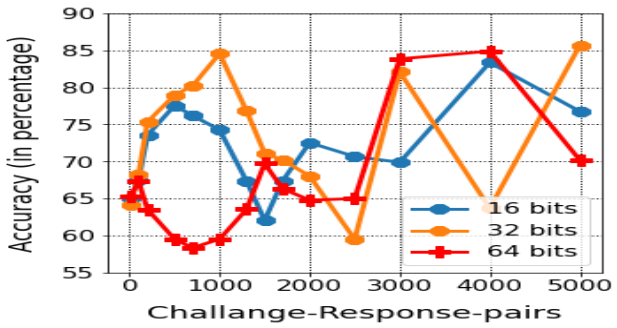

Fig. 15 Integrated PUF

Similarly, SVM was applied on the Ring oscillator-based PUF and high accuracy of up to 99% is observed and in general 65% to 95% of accuracy is observed.

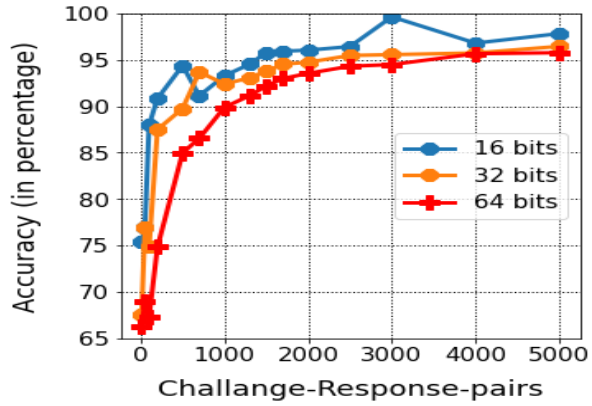

Fig. 16Ring-oscillator PUF

Fig 16. shows the accuracy evaluation on Ring oscillator PUF, and it is observed that for 16 bits the accuracy lies between 75% to 100%, for 32 bits it is in between 65% to 95%. In case of 64 bits, the accuracy lies between 65% to 95%. This shows that Ring-Oscillator PUF is also highly vulnerable.

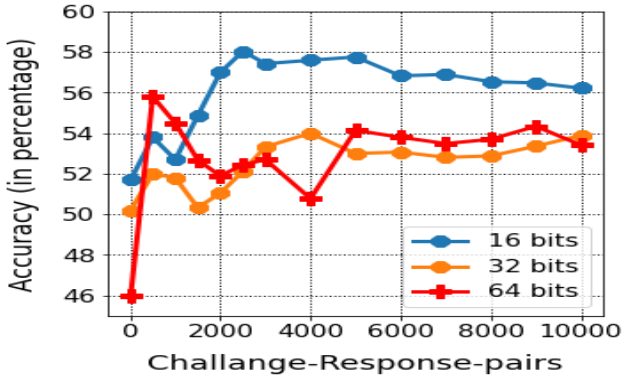

Fig. 17 SP-PUF

Fig 17. shows the accuracy evaluation on proposed SP-PUF architecture. In case of 16 bits, accuracy of SP-PUF remains between 52% to 58%. In case of 32 bits, accuracy remains 50% to 54%, whereas in case of 64 bits it remains between 46% to 54%. Evaluation of SP-PUF on accuracy shows the efficiency as it remains nearer to 50%.

B. PUF evaluation

PUF holds the ideal characteristics of uniqueness and reliability, this section evaluates the model in terms of these parameters.

B1. Uniqueness

Uniqueness is defined as the parameter that has the ability for differentiating among the devices considering the response of PUF. It can be computed as:

$$V_r = 1/4o^2 \sum_{v=1}^{2o} \sum_{w=1}^{2o} \mathbb{R}_w \quad (9)$$

Referring to (9), o indicates the PUF instances and $\mathbb{R}_w$ indicates the wth position in $\mathbb{R}$ and it has $2o$bit. In general, the ideal value of uniqueness should be 50%.

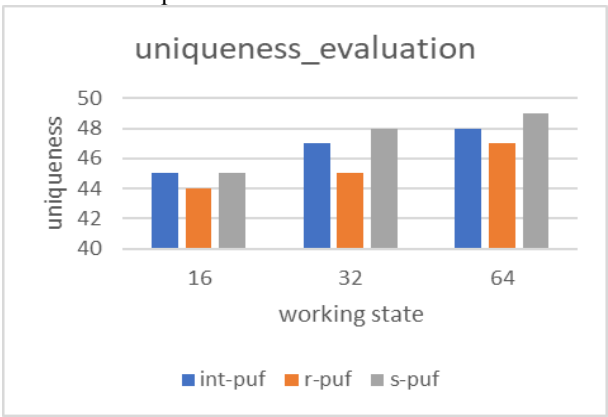

Fig. 18 Uniqueness comparison

Fig 18. shows the uniqueness evaluation considering the different stages i.e., 16-bit, 32-bit and 64-bit. In comparison with the Integrated PUF and Configurable ring oscillator, SP-PUF observes the better uniqueness than other PUFs.

B2. Reliability

A particular PUF is said to be reliable if the response of PUF is repeatable under certain circumstances; it can be mathematically formulated as:

$$\tau = 100\% - \left((n)^{-1} \left(\sum_{u=1}^{n} \frac{\mathbb{Z}(\mathbb{R}, \mathbb{R}'_u)}{2o} \, 100\% \right) \right) \quad (10)$$

Refer to (10), $\mathbb{R}$ indicates the $2o$ bit response, this response is extracted considering the normal circumstances. To evaluate the reliability, we take room temperature as the reference temperature and temperature is varied from -50^{0}C to 100^{0}C. Through the graph, it is observed that SP-PUF is better than the other PUF.

The detailed requirement of the reliability along with temperature is represented in detail in Fig 19. With the

comparison with different PUF considering three stages i.e., 16-bit, 32-bit and 64-bit by varying the temperature. The graph suggests that the proposed SP-PUF is equivalent to the reliability of Configurable Ring Oscillator PUF as Configurable-Ring oscillator is highly reliable.

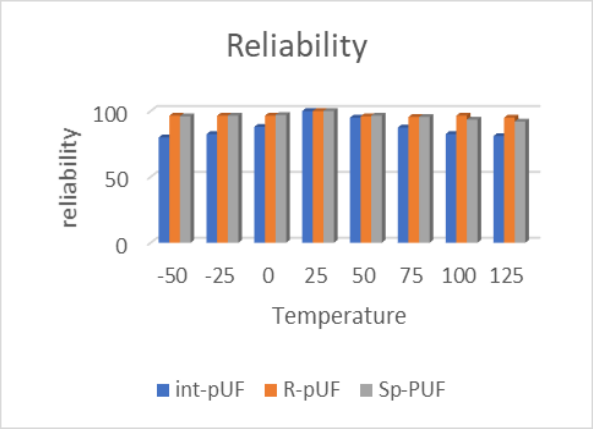

Fig. 19 Reliability comparison

V. CONCLUSION

Rapid development in semiconductor industry and further globalization has raised the bar for hardware security framework for light edge devices. The physical unclonable function provides the promising solution to authenticate IoT devices as it provides the novel fingerprints for various devices through CRP (Challenge-Response Pairs). Although, existing research claimed to be unclonable, machine learning exposes the vulnerabilities of PUF through modeling the PUF attacks. In this paper, we design and develop a novel PUF architecture named SP PUF; SP-PUF is a strong PUF based architecture that also acts as a different type of PUF. A machine-learning attack is designed to prove the model efficiency against the security. The proposed security framework consists of three parts i.e., at first designing of novel PUF architecture, the second part of the framework includes the introducing optimizes obfuscation technique to avoid the mapping of response; a third part of the framework includes the designing of authentication protocol to avoid the direct access to response. The proposed security framework is evaluated by attacking through the machine learning algorithm and it is observed that Sp-PUF architecture observes between 50-60% of accuracy which is equivalent to random guessing; also, uniqueness and reliability is considered for PUF architecture evaluation through uniqueness with nearly 50% of it and fair reliability. As a part of future work, it can be listed that the machine learning approaches can be compared on an single iteration and selection of the best technique. Thus, this research work proves that our proposed security framework is not only secure but efficient as well, as the proposed method is efficient with machine learning approach and it is sufficient to achieve the results hence its not tested with artificial intelligence conditions but can be considered as one of the future scope consideration..

References

[1]. M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.

[2]. M. Masud, G. S. Gaba, S. Alqahtani, G. Muhammad, B. B. Gupta, P. Kumar, and A. Ghoneim, “A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care,” IEEE Internet of Things Journal, 2020

[3]. W. Hu, C. H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, “An overview of hardware security and trust: Threats, countermeasures and design tools,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 40, no. 6, pp. 1010–1038, June 2021.

[4]. S. Bhunia and M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, 1st ed. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2018

[5]. T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, “A PUF taxonomy,” Applied Physics Reviews, vol. 6, no. 1, p. 011303, 2019.

[6]. B. Halak, M. Zwolinski, and M. S. Mispan, “Overview of PUF-based hardware security solutions for the Internet of Things,” in Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS), Oct. 2016, pp. 1–4, doi: 10.1109/MWSCAS.2016.7870046.

[7]. Y. Xu, Y. Lao, W. Liu, Z. Zhang, X. You, and C. Zhang, “Mathematical modeling analysis of strong physical unclonable functions,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 39, no. 12, pp. 4426–4438, Dec. 2020.

[8]. J. Delvaux, “Machine-learning attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 8, pp. 2043–2058, Aug. 2019.

[9]. S. V. S. Avvaru and K. K. Parhi, “Effect of loop positions on reliability and attack resistance of feed-forward PUFs,” in Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI), Jul. 2019, pp. 366–371.

[10]. H. Yıldız, M. Cenk, and E. Onur, “PLGAKD: A PUF-based Lightweight Group Authentication and Key Distribution Protocol” IEEE Internet of Things Journal, vol. 14, no. 8, pp. 1-14, 2020.

[11]. M. Majzoobi et al., “Slender PUF Protocol: a Lightweight, Robust and Secure Authentication by Substring Matching,” in S&P, 2012, pp. 33– 44.

[12]. Y. Lao et al., “Reliable PUF-Based Local Authentication with SelfCorrection,” TCAD, vol. 36, no. 2, pp. 201–213, 2016.

[13]. U. Chatterjee et al., “Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database,” IEEE TDSC, vol. 16, no. 3, pp. 424–437, 2019.

[14]. Hasan Tariq et al., "IoT/Edge Structural Health Monitoring System as a Life-Cycle Management tool for SDG-11 using Utility Computing Platform," WSEAS TRANSACTIONS on COMPUTERS, vol 18, 2019, pp. 175–184.

[15]. S. S. Zalivaka et al., "Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response," IEEE TIFS, vol. 14, no. 4, pp. 1109–1123, 2018.

[16]. E. I. Vatajelu et al., "On the encryption of the challenge in physically unclonable functions," in IOLTS, 2019, pp. 115–120.

[17]. M.-D. Yu et al, "A noise bifurcation architecture for linear additive physical functions," in HOST, 2014, pp. 124–129.

[18]. G. T. Becker, "On the pitfalls of using Arbiter-PUFs as building blocks," TCAD, vol. 34, no. 8, pp. 1295–1307, 2015.

[19]. C. Gu et al., "A modeling attack resistant deception technique for securing PUF based authentication," in Asian HOST, 2019, pp. 1–6.

[20]. S.-J. Wang et al., "Adversarial attack against modeling attack on PUF," in DAC, 2019, pp. 1–6.

[21]. R. Kumar and W. Burleson, "On design of a highly secure PUF based on non-linear current mirrors," in Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust (HOST) , May 2014, pp. 38–43.

[22]. K. THAMIZHMARAN, "IOT supported security considerations for network ", WSEAS TRANSACTIONS on COMMUNICATIONS, Volume 19, 2020, pp 113-123.

[23]. Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, "PUFFSM: A controlled strong PUF," IEEE Trans. Computer Aided Design Integrated Circuit Systems, vol. 37, no. 5, pp. 1104–1108, May 2018.

[24]. M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching," in Proc. IEEE Symp. Secur. Privacy Workshops, May 2012, pp. 33–44.

[25]. J. Ye, Y. Hu, and X. Li, "RPUF: Physical unclonable function with randomized challenge to resist modeling attack," in in Proc. IEEE Asian HOST, Dec. 2016, pp. 1–6.

[26]. Y. Wang, X. Xi, and M. Orshansky, "Lattice PUF: A strong physical unclonable function provably secure against machine learning attacks," in Proceedings of IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Dec. 2020, pp. 273–283.

[27]. S. V. S. Avvaru, Z. Zeng, and K. K. Parhi, "Homogeneous and heterogeneous feed-forward XOR physical unclonable functions," IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2485–2498, 2020.

[28]. J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," IEEE Trans. Computer Aided Design Integrated Circuit Systems, vol. 39, no. 10, pp. 2138–2151, Oct. 2020.