An Energy-Efficient and Modeling Attack-Resilient SNN-Driven PUF Security for Internet of Medical Things

Agila Harshini T, Harini Sriraman*
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

***Abstract*—The healthcare industry is rapidly evolving with the digitalisation of medical devices. Despite the advantages of IoMT devices, they remain vulnerable to cyberattacks that threaten patient data security. Authentication typically relies on a static key, making it susceptible mainly to modelling attacks. Existing techniques fail to balance security with lightweight operation for resource-constrained IoMT. A Physically Unclonable Function (PUF)-based technique provides genuine authentication with on-the-fly key generation but lacks resilience against modelling attacks. The proposed work presents a fusion of facial biometrics and a Spiking Neural Network(SNN) with a PUF. This fusion generates stronger entropy than conventional methods that rely on fixed stored keys. This work strengthens authentication by integrating user-specific facial biometrics, device-specific PUF responses, and SNN-induced nonlinearity. It enables joint authentication of both the device and the legitimate user. The experimental evaluation is conducted on the Digilent Basys3 Artix 7 FPGA board and achieves higher randomness in the generated responses, with a Shannon entropy of 0.693 nats and a normalized Hamming distance of 0.50. The security evaluation demonstrates that machine learning and deep learning attacks remain random-guess predictions, indicating that the proposed lightweight Face-SNN-PUF resists effective modelling of the challenge-response. Tailored for non-life-critical IoMT devices, the proposed resilient framework provides practical and energy-efficient authentication.**

Keywords*—PUF; SNN; biometric authentication; IoMT security; modeling attack

I. Introduction

The market for IoMT devices is growing, leading to easier monitoring of healthcare data through edge devices. To surveil and deliver healthcare to patients remotely, IoMT collects and transfers digital data to a server for processing. Despite the benefits, cybersecurity attacks are more prevalent among IoMT devices [2], [5], [13]. Healthcare data, when compromised by different attacks, can harm patients by disrupting personal data and causing financial loss or physical harm. The major security challenges are: Modeling attacks in which the attacker identifies and analyses the challenge-response pairs and creates a machine learning model to mimic the PUF behavior [4]; man-in-the-middle attacks that breach the device and enable reverse engineering or data extraction through physical access; authentication issues where the IoMT is vulnerable to cloning, spoofing, and replay attacks due to static or weak keys used in the device; and resource constraints, with the limited power and memory of small medical devices making them unsuitable to implement heavy cryptographic security [2], [11], [23]. Unlike other devices that cause only a data breach, IoMT leads to direct harm to patients. The existing PUF-based authentication models may remain vulnerable to modeling attacks when used without explicit binding between the user and the device. The proposed system combines three complementary entropy-contributing components: facial variability, randomness of spiking neurons, and PUF uniqueness to improve resistance against modeling attacks in IoMT authentication. Unlike conventional PUF-based authentication, the proposed work introduces a biologically inspired Neural Network to give temporal variability and non-linear challenge transformation. Fig. 1 shows the fusion model. The fusion of biometric features, spike dynamics, and hardware randomness increases the learning complexity of the challenge-response. The proposed work targets non-life-critical IoMT devices such as wearables and remote patient monitoring, where secure authentication with moderate latency is acceptable. Fig. 1 gives an illustration of the proposed fusion of the Face-SNN-PUF framework.

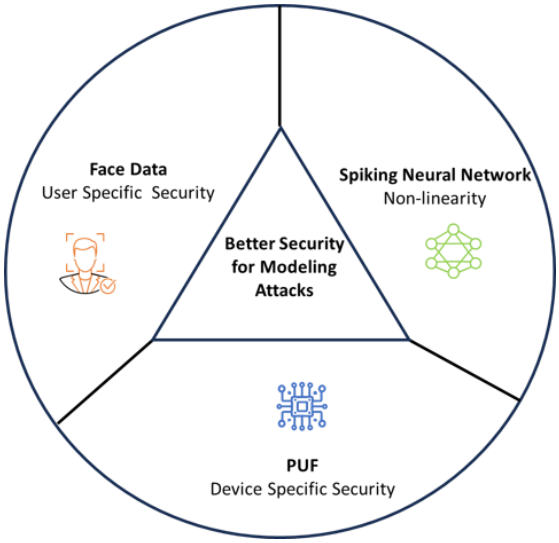

Fig. 1. Face-SNN-PUF fusion model.

The major contributions of this study are:

- A hybrid authentication framework integrating facial biometrics, Spiking Neural Networks, and Physically Unclonable Functions to ensure device and user authenticity.

*Corresponding author.

- The proposed Face-SNN-PUF enhances authentication security by combining biometric-derived entropy, non-linear transformation of SNN, and intrinsic PUF randomness, subsequently increasing resistance to modeling attacks.
- A detailed evaluation of security analysis against modeling attacks, using deep learning techniques, is provided.
- Lower computation and energy overhead compared to traditional cryptographic methods.

II. Related Work

To evaluate the proposed Face-SNN-PUF, the recent works in PUF-based authentication, biometric-assisted identity verification, and neuromorphic-based security are categorized and explored.

A. PUF-Based Authentication for IoMT

A stream cipher designed by a nonlinear feedback shift register is presented for data and device integrity by combining MAC and PUF response [1]. It is evaluated using NIST 800-22 and compared with existing ciphers using a heart disease dataset, and it presents a device authentication scheme using a hybrid oscillator arbiter PUF. PMsec authenticates the device before the data is read. It is suitable for low-power medical devices [2]. Based on blockchain and PUF, a scalable device authentication framework that achieves a uniqueness of 48.46% and reliability of 2.38% is proposed [3]. For role-based access, smart contracts are used. Ethereum's permissioned blockchain is developed as a proof of concept. To prevent the attacker from seizing the challenge bits, a protocol using a 64-bit arbiter PUF is presented that splits the challenge bits, and bit scrambling is also exploited by protocol extension. Also, the implications of modeling attacks by challenge patterns are studied [4].

PUF-based WMSNs protocol, a fuzzy extractor, a one-way hash function, and XOR operations are used for security [5]. Compared to other schemes, it requires low communication and computation costs. The proposed integration of PUF with IOTA and blockchain uses the Masked authentication message protocol to store and share data. With minimal energy requirements, decentralized access control is provided [6]. To authenticate the IoT sensor nodes, a PUF-based lightweight mechanism is proposed. The security resists network attacks and has low computational requirements and higher throughput [7]. A lightweight GAKA that uses PUF to solve secure transmission and data storage is given. It has higher computational efficiency than other systems [8]. The random variations in the PUF are affected by external factors. The proposed design has increased performance, reliability, and uniformity [9]. For resource-constrained devices, a RoT architecture based on PUF is proposed. It is robust and cost-efficient and uses SRAM and a syndrome-based fuzzy extractor, reinforcing device-centric security [10].

Combining the fingerprint of the device with an authentication protocol, a PUF-based identity framework for IoT devices is proposed. It is an identity management system at the IoT gateway layer with low latency. It has resistance to impersonation and replay attacks [11]. To support dynamic response generation, a configurable C-PUF is introduced. Demonstrates higher entropy and stability under varying environmental conditions [12]. Focusing on COVID-19 patient monitoring, a PUF-assisted key protocol for medical IoT is developed. With reduced computational cost, it uses device-generated randomness and mutual authentication [13]. A reconfigurable PUF-based authentication for healthcare IoT is proposed that reconfigures challenge-response and resists modeling attacks. Enhances authentication reliability and secure communication [14]. Ensuring secure key agreement in sensor, gateway, and cloud, a three-layer authentication protocol using PUF is presented. The authentication is verified with formal and simulation-based methods [15].

A PUF-based anonymous user authentication for IoT devices is developed. Balances anonymity and traceability through cryptographic primitives with high scalability and resistance to replay attacks [16]. Introduces memory-based Mc-PUF, utilising SRAM and DRAM timing variation. With high uniqueness and stability, it resists machine learning and modeling attacks [17]. Proposes a feedback-based PUF for resisting ML attacks. Provides a nonlinear challenge-response by using response-feedback loops. Shows strong resistance to logistic regression and SVM modeling [18]. Introduces a bias-independent PUF that applies delay calibration and symmetric routing for uniform response distribution. It is resistant to layout-induced imbalance [19]. A priority arbiter PUF that enhances a standard arbiter PUF is proposed. To improve delay sensitivity and uniqueness, a priority encoder is used. Achieves strong resistance to ML and environmental noise [20].

B. Biometric Integrated Approaches

The proposed neighbor-assisted, PUF-based three-factor authentication. 100% reliability is demonstrated [21]. The IoHT are vulnerable to insider threats and physical attacks. Mutual authentication with biometrics and PUF is proposed. The system is tested with automated validation of Internet security protocols [22]. A robust identity verification in medical sensors, a two-factor authentication using PUF and password, is designed. It has enhanced resistance to side-channel and impersonation attacks [23]. A combination of PUF with biometrics for hybrid authentication is explored for stronger identity. Highlights improved entropy [24].

C. Neuromorphic and SNN-Based Security

A spiking neural network-based framework for privacy in IoMT in the metaverse is presented. Neuron behaviour for adaptive and energy-efficient secure health data exchange is given [25]. A single spiking neuron model using membrane potential dynamics for an entropy source is proposed. Demonstrates strong behaviour of PUF with minimal hardware cost [26]. Proving that biological neuron firing can give a unique PUF response, implements neuron-spiked circuits to generate challenge-dependent outputs [27].

The above related studies primarily address user or device authentication separately. Existing PUFs have improved security by increasing the complexity of the architecture, XOR structures, feed-forward paths, or protocol-level protection. These approaches have fixed challenge-response behavior that introduces hardware overhead and computational complexity.

Primarily, few methods restrict CRP exposure, while others improve resistance to specific machine-learning models. The reviewed methods do not simultaneously address user device binding and energy awareness for IoMT devices. The proposed Face-SNN-PUF addresses this gap with modelling-attack resilience and user device binding. Table I gives a comparison of other authentication approaches to highlight the design objectives of the proposed framework.

TABLE I. COMPARISON OF IOMT AUTHENTICATION AND SECURITY FRAMEWORKS

S.No	Security Metric	Biometric-only system	PUF-only System	Proposed Face Biometric–SNN–PUF
1	Resistance to Spoofing	High (with fake data)	Strong (Unique to device, no user binding)	Strong(User biometric + PUF must match)
2	Resistance to ML and DL Modeling	Vulnerable	Weak (PUF can be modeled)	Improved resistance by SNN-induced nonlinearity (ML/DL results are given in Section IV)
3	Cloning Resistance	Weak (Biometrics can be copied)	Strong(Unique per chip)	Strong (Requires Match in User device domain)
4	Lightweight Efficiency	Moderate (needs storage)	Lightweight	Lightweight (PUF+SNN power ~0.004 W)
5	Entropy	Limited (~6-8 bits)	Arbiter PUF (~10-12 bits)	Spike+ PUF (~13-14 bits)

III. PROPOSED FRAMEWORK OF FACE-SNN-PUF

The proposed work combines the biometric (face), Spiking Neural Network (SNN), and arbiter PUF, providing lightweight and secure authentication for IoMT devices. 10000 CRPs are collected as a dataset from the UART connected to the board for analysis. Fig. 2 shows the architecture of the proposed Face-SNN-PUF system.

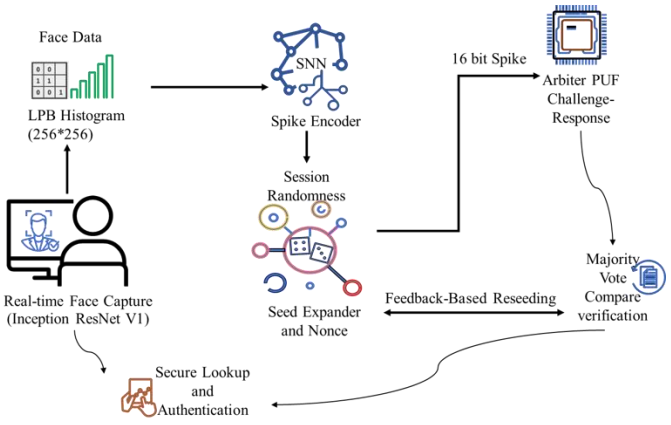

Fig. 2. Architecture of the Face-SNN-PUF system.

1) The biometric data is captured from the user in real-time. The facial images of ten users are captured and registered for authentication. Genuine authentication was evaluated using samples from the corresponding registered user. The samples from other users were used to evaluate imposter authentication attempts. Using a pre-trained InceptionResNetV1 via FaceNet, deep embeddings are extracted. Separately, the detected facial region is processed using lightweight Local Binary Pattern (LBP) extraction. The lightweight LBP(Local Binary Pattern) compares each pixel with 8 neighbours to form an 8-bit binary number(0-255). The LBP histogram counts the number of times each LBP code occurs. Each histogram bin value is multiplied by its corresponding index and summed to produce a compact biometric-derived value. For reproducibility, the LBP uses a radius of 1 pixel with 8 sampling points. The 16-bit final face signature is obtained by applying a modulo 2^{16} operation on the weighted sum. The bitmask keeps only the last 16 bits of the sum to ensure compactness for the FPGA; this 16-bit value is used as a compact biometric-derived input to the hardware authentication pipeline, whereas biometric recognition is performed using the InceptionResNetV1 embedding similarity. A 16-bit width can efficiently fit into the Basys 3 FPGA board. To examine the inter-person variation of the compact representation, the LBP-based face generation procedure was evaluated using ten different facial samples.

2) The SNN(biologically inspired spike-based) reads the person identifier (PID) derived from the face signature. Then selects one of the thresholds for that PID. To provide a source of variability for repeated identical person ID, a free-running jitter counter is added. The extracted features are encoded into spike trains by an SNN encoder module. The spiking variability and threshold selection are clock-edge jitter-influenced by the 100 MHz on-board oscillator and metastable delay variations. The SNN engages a leaky integrate-and-fire neuron model with discrete threshold levels from a predefined range [Tmin, Tmax]. The effective threshold is chosen dynamically based on the PID and jitter count value.

3) To provide non-linearity, the spike generator maps a person's identity and features into the spiking activity (spike 16). To introduce session-level variation, an 8-bit free-running nonce counter is implemented on the FPGA. The nonce is reset to zero and incremented at each rising edge of the 100 MHz system clock. The seed expander combines the biometric-derived input, selected SNN threshold, and the current 8-bit nonce to generate the 16-bit PUF seed. The nonce is generated internally by the FPGA and is not transmitted by the host application; therefore, no separate nonce-exchange or synchronization message is required between the Python application and the FPGA. The 16-bit arbiter PUF with LFSR-driven challenges is seeded with the input. The arbiter PUF consists of 16 delay stages, and challenges are generated using a 16-bit linear feedback shift register (LFSR) with a maximal-length primitive polynomial. The PUF gives a device-specific challenge-response pair. To improve the stability of the response, each challenge is evaluated multiple times and a majority voting scheme is applied across repeated measurements. The majority of responses are stored in a secure lookup table. During

enrollment, reference responses are recorded for a fixed set of challenges. During authentication, live responses are matched against the enrolled references. During authentication, the live facial embedding is compared with the enrolled user using the cosine similarity. A minimum threshold of 0.60 is used, with the per-user threshold determined from the mean enrollment similarity minus a margin of 0.05. Authentication requires consistent recognition for three consecutive frames for access to be granted. For validation of the attack analysis, 10,000 challenge-response pairs (CRPs) are collected over UART from the FPGA.

For reproducibility, the key design and implementation parameters of the proposed Face-SNN-PUF are summarized in Table II.

TABLE II. KEY IMPLEMENTATION PARAMETERS OF THE PROPOSED FRAMEWORK

Module	Key parameter	Description
Hardware platform	FPGA board	Xilinx Basys 3 (Artix-7 XC7A35T-1CPG236C
Development environment	Tool	Xilinx Vivado
Biometric pursuit	Face embedding model	InceptionResNetV1 (FaceNet, pre-trained)
Feature reduction	Local Binary Pattern (LBP)	Radius 1, Neighbors 8
Face signature	Dimensionality reduction	LBP histogram weighted sum, reduced to 16 bits using modulo 216
Neuromorphic encoding	SNN neuron model	Leaky Integrate-and-Fire (LIF)
SNN variability source	Threshold selection	PID-dependent threshold with jitter-based variation
PUF architecture	Arbiter PUF	16-bit arbiter PUF
Challenge generation	LFSR configuration	16-bit LFSR
Seed construction	Entropy fusion	Concatenation of spike output, threshold index, and session nonce
Response stabilization	Noise mitigation	Majority voting over repeated evaluations
Scalability	Design extensibility	Extensible to higher PUF bit-widths with resource trade-offs

B. Attack Model

The attacker is assumed to have access to collected CRPs and may attempt modeling attacks. Potentially stronger capabilities, such as access to captured facial images, inferred PID information, or observed intermediate signals, are recognized as possible attack surfaces of the proposed framework. To examine the robustness of the modeling-attack evaluation, the experiments were repeated using five different random seeds. Logistic Regression, Random Forest, and MLP achieved mean prediction accuracies of 48.63%, 49.49%, and 49.67%, respectively, with standard deviations of 1.15%, 0.69%, and 1.25%. The corresponding mean ROC-AUC values were 0.481, 0.498, and 0.493, respectively. The target classes contained 5056 zero samples and 4944 one samples, indicating a nearly balanced distribution. In addition, the maximum absolute Pearson correlation between an individual challenge bit and the target was approximately 0.0131, while the maximum observed mutual information was 8.55×10^{-5}bits. These results demonstrate that the evaluated models remained close to the random-guessing baseline and did not identify a strong predictive relationship in the evaluated CRP data.

IV. RESULTS AND ANALYSIS

The biometric template and PUF keys are not stored. Reproducing this behaviour is hard, even with full access to the device. The proposed Face-SNN-PUF has favourable entropy, uniqueness, and strong resistance to DL-based modeling attacks. Fig. 3 represents the randomness of the proposed model PUF keys. The values are centred around 8, which shows a balanced distribution of 1s and 0s across the collected samples. Fig. 4 shows the uniqueness comparison of the PUF with existing works [3], [4], [22], [25].

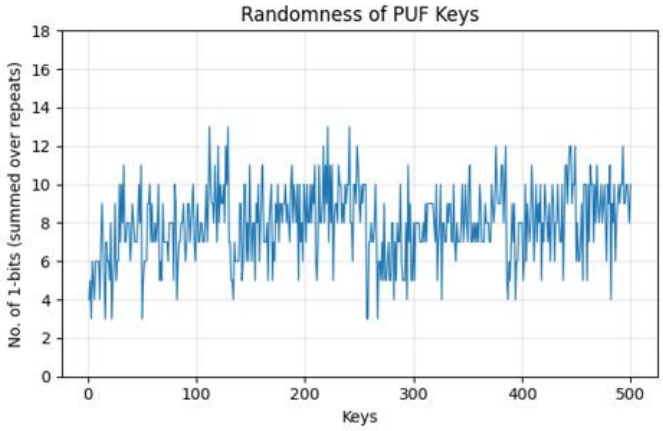

Fig. 3. Randomness analysis of the PUF keys.

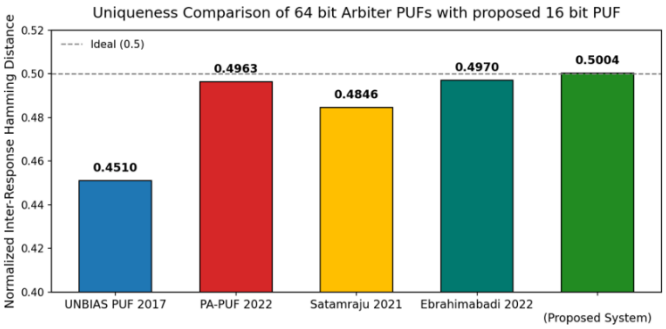

Fig. 4. Comparison of uniqueness of the PUF keys.

A. Randomness and Uniqueness Analysis

The Shannon entropy and inter-response Hamming distance measures are analysed for the Bio-SNN-PUF to find the randomness and uniqueness. The measured Shannon entropy is 0.693, representing near-ideal randomness for a binary response distribution. This corresponds to the theoretical maximum entropy of a balanced binary distribution, indicating the generated responses exhibit near-ideal randomness. The average normalised inter-response Hamming distance is 0.5004, and the given challenges differ by approximately 50%. This shows that the PUF has strong uniqueness. Fig. 5 shows the quantitative analysis of the Bio-SNN-PUF's randomness and uniqueness. The samples produced ten different 16-bit values with no collision. The mean pairwise Hamming distance

between the generated values was 7.13 bits out of 16, with a minimum of 3 bits and a maximum of 11 bits. The overall proportion of 1-bits was 48.13%, indicating a reasonably balanced distribution of the generated compact values. These results provide an initial empirical assessment of inter-person variation.

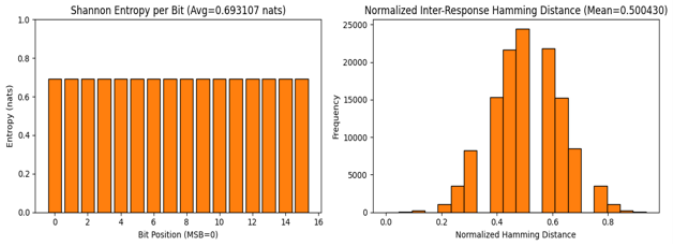

Fig. 5. Entropy and uniqueness of Face-SNN-PUF.

B. Entropy Analysis of SNN-Assisted

The randomness of spike 16 is evaluated by computing Shannon entropy (a measure of average randomness in 16-bit output), which gave 13.14 bits out of 16, and min-entropy (the worst-case predictability is captured) of 11.29 bits. This shows the response space is highly random. Even under worst-case conditions, the spike output retains entropy. The average per-bit entropy is 0.9999(good spread of 0s and 1s), which is nearly 16 independent effective bits. With the PUF having a unique response per device, the user-dependent biometric input and the spiking transformations increase the randomness. Fig. 6 shows the comparison to the existing works [20], [21]; the proposed model has higher entropy. The facial biometric, SNN, and PUF components are coupled. The face input determines the person identifier, which influences the SNN spike and threshold. These are combined with the session nonce to construct the PUF seed.

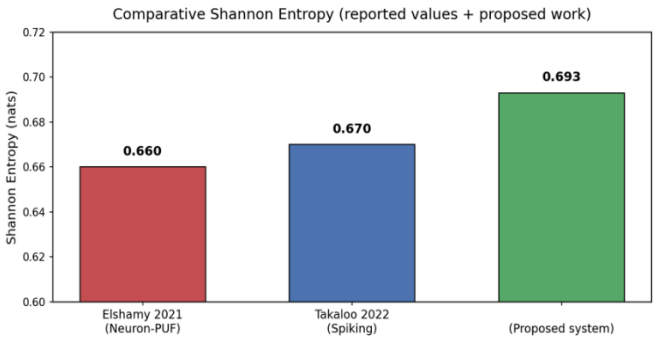

Fig. 6. Comparison of the entropy of the face-SNN-PUF.

C. Uniqueness and Reliability Analysis

The inter-challenge stability, the probability that two different challenges yield the same PUF response, is measured to characterize the uniqueness of generated responses. The average identical response is 52.6%, which is the inter-challenge collision rate. The intra-challenge Hamming distance is 1.52 bits out of 16. It is a measure of variation when the same challenges are repeated multiple times. It indicates the response consistency under repeated evaluations. This exhibits a moderate noise level but remains within the range of stochastic PUF designs.

D. Security Analysis

The security of the proposed work, Biometric + SNN + PUF, provides improved resistance to modeling compared to biometric-only or PUF-only approaches. It is more resistant to modeling and cloning. This balances strong security and lightweight efficiency that is practical for real-world security of IoMT devices.

A biometric-only or PUF-only system is weak and can be modelled. The proposed method introduces a nonlinear biometric input and the entropy of Spike patterns, which makes the approximation of the ML and DL model harder. The biometric data of each person gets a unique PUF instance through dynamic seed expansion. The spike latency, firing rate, and threshold randomness of the SNN introduce nonlinearity. The spike entropy ensures that the input-output correlation remains nonlinear and is highly device-specific, so the attacker cannot use an ML model to approximate it easily. The modeling is a supervised attack; the attacker collects the CRPs. 10000 CRPs are used, training=8000 and testing = 2000. The PUF seed is generated by the FPGA seed-expander logic using the biometric-derived input, selected SNN threshold, and the 8-bit free-running nonce counter. These features are used to train classifiers to predict responses for unseen challenges. The response prediction represents a binary classification problem, so an attacker without meaningful knowledge about PUF behaviour can only achieve 50% prediction accuracy, which is random guessing. The DL models are also ~50%, which states that the models cannot learn the pattern and an attacker fails to approximate the challenge-response relationship.

E. Resistance to Machine Learning-Based Modeling Attacks

The proposed system is evaluated for resilience against three ML-based classifiers. The accuracy achieved by Logistic Regression is 48.0%, Support Vector Machine 50.3%, and MLP 51.2%. Fig. 7 represents these accuracies. The results indicate that all machine learning models exhibit a random guess line prediction performance, which limits the attacker's ability to learn the challenge-response behavior.

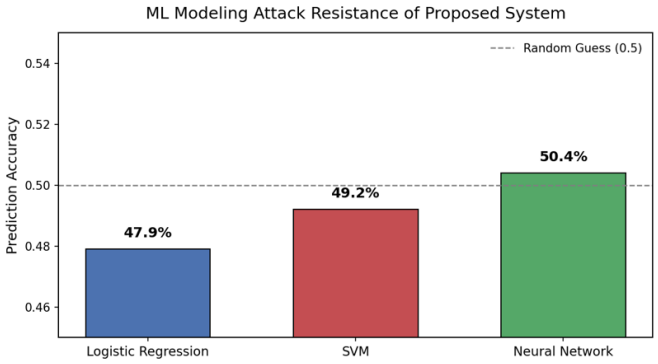

Fig. 7. Prediction performance of machine learning-based modeling attacks (Lower the deviation of random guessing, higher the security).

F. Resistance to Deep Learning-Based Modeling Attacks

Further evaluation of resilience against sophisticated modeling attacks: a DNN consisting of three layers(64-32-16 neurons and ReLU activation function) and an advanced deep learning model that uses a 1D-CNN front-end, residual blocks,

and batch normalisation are trained using the collected CRPs. The accuracies learned are 50.2% and 51.75%. The results in Fig. 8 show that the deep neural models prevent effective approximation of the challenge response of the Bio-SNN-PUF.

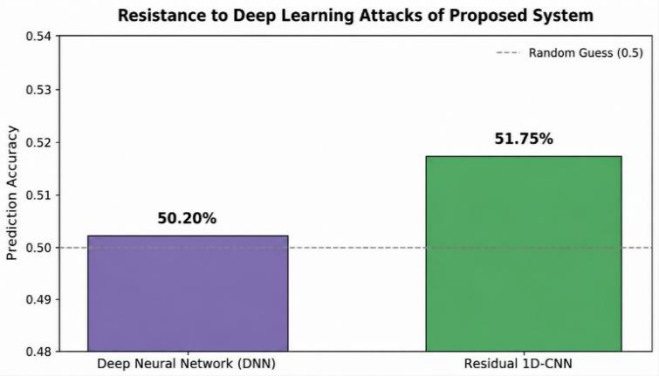

Fig. 8. Prediction performance of deep learning-based modeling attacks (Values close to random guessing indicate higher security).

G. Statistical Analysis of Modeling Attack Results

A systematic evaluation of modeling attacks is done using five models with five independent train-test splits. The Mean accuracy, Standard Deviation,95% Confidence level, and Mean ROC0AUC are calculated as shown in Table III. The results remain close to 50%, indicating the models did not obtain a consistent relationship. This means that none of the evaluated models was able to learn the response pattern. This consistency of results using ML and DL models supports modeling resistance.

TABLE III. STATISTICAL EVALUATION OF MODELING ATTACK

Model	Mean Accuracy	SD %	95%CI%	Mean ROC-AUC
Logistic Regression	49.51	0.63	48.73-50.29	0.491
SVM	49.80	1.36	48.11-51.49	0.502
MLP	49.95	2.02	47.45- 52.45	0.495
DNN	50.52	1.12	49.13-51.91	0.509
Residual 1D-CNN	49.66	1.40	47.92-51.40	0.490

H. Comparison of ML and DL Attack Resistance with Existing Works

The biometric and the SNN are encoded as a challenge, which will confuse the DL models. The attack resistance of the proposed system compared with the existing solutions [4], [9], [14], [18] demonstrates improved modeling resistance. Fig. 9 shows the prediction accuracy comparison with the existing work.

I. Cloning Resistance

The proposed work resists cloning because it requires the biometric details, the spike nonlinearity, and the FPGA data, which makes cloning practically infeasible. For a cloning attack to be successful, an adversary would need to reproduce the combined effects of the facial input, spike dynamics, and device-specific PUF, significantly increasing the difficulty of device cloning. The attacker requires multiple independent entropy sources for successful impersonation of user-specific biometrics, SNN spike patterns, and PUF variation for cloning.

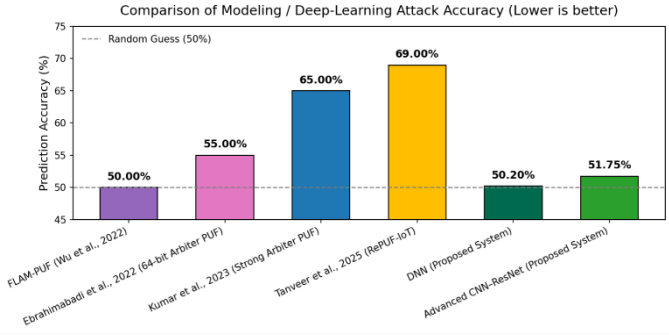

Fig. 9. Comparison of the DL attack resistance of the Face-SNN-PUF.

V. ENERGY EFFICIENCY

The energy efficiency of the proposed method exhibits low energy consumption, making it suitable for resource-constrained IoMT devices. Fig. 10 shows the power report of the implemented Face-SNN-PUF. The existing authentication methods [1], [2], [3] based on PUF, which primarily focus on security and consume high power, and the multifactor key authentication [4], [5], [26], although reliable, are less suitable for low-power devices. Neuron-inspired architectures [20], [21] focus on entropy generation but lack FPGA-level implementation. Compared to existing methods, the proposed work, implemented on an FPGA, offers reduced energy consumption, providing entropy and modeling attack resilience. Fig. 10 shows the measured power consumption of the proposed work implemented on the Basys 3 FPGA. The proposed Face-SNN-PUF operates at a clock frequency of 100 MHz, corresponding to a clock period of 10ns.

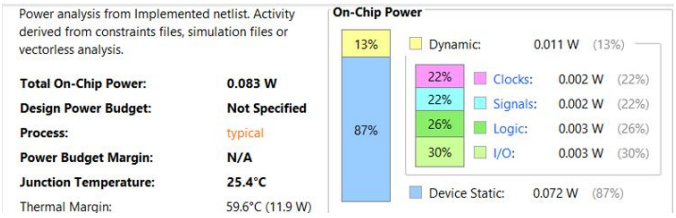

Fig. 10. Power report of the Face-SNN-PUF.

A. Energy Per Authentication

The energy consumption is calculated as,

$$E_{auth} = P_{dynamic} * T_{auth}$$

From the RTL cycle analysis, a complete authentication requires 294 clock cycles, including the 256 -cycle SNN processing window, PUF evaluations, and majority voting.

Therefore, the estimated latency is,

$$T_{auth} = 294 * 10ns = 2.94\ \mu s$$

The Vivado power analysis PUF+SNN estimates dynamic power consumption at 0.004W. SO the estimated energy per authentication is,

$$E_{auth} = 0.004 * 2.94 * 10\text{-}6 = 11.76nJ$$

The energy value is estimated from the Vivado power analysis and RTL-derived authentication latency.

VI. Conclusion and Future Work

The entropy is derived from three coupled components: the face biometrics, spiking neural nonlinearity, and the PUF. Their fusion is an effective security mechanism for improving ML and DL modeling resistance. It is suitable for resource-constrained IoMT devices due to its minimal FPGA usage. Compared to a conventional PUF-only or a biometric-only method, the proposed system transforms the biometric nonlinearly, making modeling attacks harder. There is no need for key storage, which offers resilience against spoofing and Man-in-the-Middle attacks. This facial biometric neuromorphic PUF security contributes towards the development of resilient and intelligent IoMT devices. Although the proposed work shows increased resistance against modeling attacks, the study has been evaluated on a single hardware platform and primarily for non-life-critical IoMT devices. Future investigations will consider multiple FPGA instances and environmental robustness. The future work will focus on extending the PUF to higher bit-widths for enhanced entropy, fusion of dynamic biometrics (ECG, iris) for different healthcare scenarios, and real-time deployment on wearable IoMT devices under practical operating conditions.

Availability of Data and Materials

The code and dataset used in the research are available at the GitHub link https://github.com/agilaharshini/Bio-SNN-PUF.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not- for-profit sectors.

Competing Interest

The authors (Dr. Harini S and Agilaharshini T) declare that there are no conflicts of interest related to this manuscript. No financial, professional, or personal relationships with organizations or individuals have influenced the research, analysis, or conclusions presented in this work.

Acknowledgment

The authors would like to take this opportunity to thank the management of Vellore Institute of Technology for providing the APC and encouragement to carry out this research.

References

[1] Punam Kumari, Bhaskar Mondal, “Lightweight encryption with data and device integrity using NLFSR and PUF for the Internet of Medical Things”,Internet of Things, Volume25,2024,101041,ISSN,25426605,https://doi.org/10.1016/j.iot.2023.101041.

[2] V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," in IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 388-397, Aug. 2019, doi: 10.1109/TCE.2019.2926192.

[3] Krishna Prasad Satamraju, B. Malarkodi,A decentralized framework for device authentication and data security in the next generation internet of medical things,Computer Communications,Volume 180,2021,Pages 146-160,ISSN0140-3664,https://doi.org/10.1016/j.comcom.2021.09.012.

[4] M. Ebrahimabadi, M. Younis and N. Karimi, "A PUF-Based Modeling-Attack Resilient Authentication Protocol for IoT Devices," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3684-3703, 1 March1, 2022, doi: 10.1109/JIOT.2021.3098496.

[5] Shao, X., Guo, Y. & Guo, Y. A PUF-based anonymous authentication protocol for wireless medical sensor networks. Wireless Networks 28, 3753–3770 (2022). https://doi.org/10.1007/s11276-022-03070-1

[6] Bathalapalli VKVV, Mohanty SP, Kougianos E, Iyer V, Rout B. PUFchain 3.0: Hardware-Assisted Distributed Ledger for Robust Authentication in Healthcare Cyber–Physical Systems. Sensors. 2024; 24(3):938. https://doi.org/10.3390/s24030938

[7] Kumar Chaudhary, R.R., Chatterjee, K. A Lightweight PUF based Multi-factor Authentication Technique for Intelligent Smart Healthcare System. Peer-to-Peer Netw. Appl. 16, 1975–1992 (2023). https://doi.org/10.1007/s12083-023-01509-6

[8] T. -F. Lee, X. Ye and S. -H. Lin, "Anonymous Dynamic Group Authenticated Key Agreements Using Physical Unclonable Functions for Internet of Medical Things," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 15336-15348, 15 Aug.15, 2022, doi: 10.1109/JIOT.2022.3149117.

[9] A. Kumar, K. Chatterjee and B. Mondal, "A Strong PUF-based Authentication for Medical IoT," 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA), Imphal, India, 2023, pp. 281-285, doi: 10.1109/ICIDeA59866.2023.10295174.

[10] C. Lee, M. Oh, D. Kwon, Y. Park and Y. Park, "PLAKA-MD: PUF-Based Lightweight Authentication and Key Agreement Scheme for Medical Devices in IoHT," in IEEE Internet of Things Journal, vol. 12, no. 12, pp. 19338-19353, 15 June15 2025, doi: 10.1109/JIOT.2025.3543488.

[11] Huang, Z., Wang, Q. A PUF-based unified identity verification framework for secure IoT hardware via device authentication. World Wide Web 23, 1057–1088 (2020). https://doi.org/10.1007/s11280-019-00677-x

[12] F. Amsaad et al., "Enhancing the Performance of Lightweight Configurable PUF for Robust IoT Hardware-Assisted Security," in IEEE Access, vol. 9, pp. 136792-136810, 2021, doi: 10.1109/ACCESS.2021.3117240.

[13] M. Masud et al., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15694-15703, 1 Nov.1, 2021, doi: 10.1109/JIOT.2020.3047662.

[14] M. Tanveer, A. G. Alharbi and S. A. Aldossari, "RePUF-IoT: Reconfigurable PUF-Based Authentication Protocol for IoT-Driven Healthcare Systems," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2025.3602311.

[15] A. M. Aminian Modarres, N. S. Anzabi-Nezhad and M. Zare, "A New PUF-Based Protocol for Mutual Authentication and Key Agreement Between Three Layers of Entities in Cloud-Based IoMT Networks," in IEEE Access, vol. 12, pp. 21807-21824, 2024, doi: 10.1109/ACCESS.2024.3361921.

[16] W. Wang and F. Wen, "A Robust Two-factor Medical Sensor Authentication Protocol Based on PUF," 2024 International Seminar on Artificial Intelligence, Computer Technology and Control Engineering (ACTCE), Wuhan, China, 2024, pp. 462-466, doi: 10.1109/ACTCE65085.2024.00100.

[17] Kavya Dayananda, Nima Karimian, When Physical Unclonable Function Meets Biometrics,arXiv, 14 Dec 2020

[18] L. Wu, Y. Hu, K. Zhang, W. Li, X. Xu and W. Chang, "FLAM-PUF: A Response–Feedback-Based Lightweight Anti-Machine-Learning-Attack PUF," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 11, pp. 4433-4444, Nov. 2022, doi: 10.1109/TCAD.2022.3197696.

[19] S. A. Khowaja, K. Dahri, M. A. Jarwar and I. H. Lee, "Spike learning based Privacy Preservation of Internet of Medical Things in Metaverse," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2023.3306704.

[20] M. Elshamy and H. -G. Stratigopoulos, "Neuron-PUF: Physical Unclonable Function Based on a Single Spiking Neuron," 2021 IEEE

27th International Symposium on On-Line Testing and Robust System Design (IOLTS), Torino, Italy, 2021, pp. 1-6, doi: 10.1109/IOLTS52814.2021.9486716.

[21] H. Takaloo, M. Ahmadi and A. Ahmadi, "Spiking Neurons: A New Entropy Source for Physically Unclonable Functions," 2022 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, TX, USA, 2022, pp. 170-174, doi: 10.1109/ISCAS48785.2022.9937747.

[22] Wang, W. C., Li, Z., Skudlarek, J., Larouche, M., Chen, M., & Gupta, P. (2017). UNBIAS PUF: A Physical Implementation Bias Agnostic Strong PUF. arXiv preprint arXiv:1703.10725.

[23] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," in IEEE Access, vol. 7, pp. 85627-85644, 2019, doi: 10.1109/ACCESS.2019.2926578.

[24] P. Williams, H. Idriss and M. Bayoumi, "Mc-PUF: Memory-based and Machine Learning Resilient Strong PUF for Device Authentication in Internet of Things," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 61-65, doi: 10.1109/CSR51186.2021.9527930.

[25] Singh, S., Bodapati, S., Patkar, S., Leupers, R., Chattopadhyay, A., & Merchant, F. (2022, October). Pa-puf: A novel priority arbiter puf. In 2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSI-SoC) (pp. 1-6). IEEE.

[26] P. K. Sadhu, V. P. Yanambaka, A. Abdelgawad and K. Yelamarthi, "NAHAP: PUF-Based Three Factor Authentication System for Internet of Medical Things," in IEEE Consumer Electronics Magazine, vol. 12, no. 3, pp. 107-115, 1 May 2023, doi: 10.1109/MCE.2022.3176420.

[27] E. -N. Sassalou et al., "A PUF-based Root-of-Trust for resource-constrained IoT devices," 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Crete, Greece, 2025, pp. 824-831, doi: 10.1109/CSR64739.2025.11130114.