







**Please cite the Published Version**

Ghaffar, Zahid , Kuo, Wen-Chung , Mahmood, Khalid , Alturki, Nazik , Saleem, Muhammad Assad  and Bashir, Ali Kashif  (2025) A Machine Learning Attack Resilient Authentication Protocol for AI-Driven Consumer Wearable Health Monitoring. IEEE Transactions on Consumer Electronics. ISSN 0098-3063

**DOI:** <https://doi.org/10.1109/tce.2025.3593648>

**Publisher:** Institute of Electrical and Electronics Engineers (IEEE)

**Version:** Accepted Version

**Downloaded from:** <https://e-space.mmu.ac.uk/641814/>

**Usage rights:**  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

**Additional Information:** This is an author accepted manuscript of an article published in IEEE Transactions on Consumer Electronics. This version is deposited with a Creative Commons Attribution 4.0 licence [<https://creativecommons.org/licenses/by/4.0/>]. The version of record can be found on the publisher's website.

**Enquiries:**

If you have questions about this document, contact [openresearch@mmu.ac.uk](mailto:openresearch@mmu.ac.uk). Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

# A Machine Learning Attack Resilient Authentication Protocol for AI-Driven Consumer Wearable Health Monitoring

Zahid Ghaffar, Wen-Chung Kuo, Khalid Mahmood *Senior Member, IEEE*, Nazik Alturki, Muhammad Asad Saleem, Ali Kashif Bashir *Senior Member, IEEE*

**Abstract**—The Internet of Medical Things (IoMT) is transforming healthcare by integrating interconnected consumer medical devices and sensors for remote patient health monitoring (RPHM). Integrating IoMT with Artificial Intelligence (AI) enables automated diagnostics and personalized healthcare while optimizing reliability and efficiency. It transforms healthcare by enabling RPHM through interconnected medical devices, wearable sensors, consumer health devices, and healthcare infrastructure. However, wireless communication among consumer wearable devices introduces significant security and privacy concerns, making them vulnerable to machine learning-based attacks, physical tampering, and impersonation threats. Although there are several authentication protocols, many do not provide robust resilience against these emerging threats. Therefore, we propose a machine learning attack resilient authentication protocol for AI-driven consumer wearable health monitoring to address these challenges. The protocol integrates an OPUF to mitigate machine learning-based attacks. We perform formal and informal security analyses, demonstrating that the proposed protocol provides mutual authentication, anonymity, and resistance to common security threats. Furthermore, the performance evaluation shows that the protocol significantly reduces communication and computation costs compared to existing protocols.

**Index Terms**—Authentication and Key Agreement, Authentication protocol, Remote Patient Health Monitoring

## I. INTRODUCTION

The Internet of Medical Things (IoMT) comprises a network of smart medical devices and sensors, enabling seamless data

This work is supported by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia through the Researchers Supporting Project PNURSP2025R333.

Zahid Ghaffar is with the Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Douliu 64002, Taiwan. (e-mail: chzahid337@gmail.com)

Wen-Chung Kuo is with the Department of Computer Science and Information Engineering, National Yunlin University of Science and Technology, Douliu 64002, Yunlin, Taiwan (e-mail: simonkuo@yuntech.edu.tw)

Khalid Mahmood is with the Graduate School of Intelligent Data Science, National Yunlin University of Science and Technology, Douliu 64002, Taiwan. (e-mail: khalidm.research@gmail.com)

Nazik Alturki is with Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh 11671, Saudi Arabia (email: Namalturki@pnu.edu.sa)

Muhammad Asad Saleem is with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, 611731 Chengdu, Sichuan, China, (e-mail: masadsaleem123@gmail.com)

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, M15 6BH, UK, and also with the Department of Computer Science & Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, UAE (e-mail: dr.alikashif.b@ieee.org)

(Corresponding Author: Khalid Mahmood)

exchange within modern healthcare systems. The increasing adoption of consumer-oriented wearable biosensors and internet-connected health devices has significantly enhanced remote patient health monitoring (RPHM). It drives major advancements in personalized healthcare technology [1]. These wearable healthcare devices provide cost-effective, real-time, and scalable remote healthcare services. RPHM leverages Artificial Intelligence (AI) techniques, including big data analytics, deep learning, and machine learning (ML), to improve traditional healthcare by ensuring timely medical interventions. AI-driven RPHM continuously tracks patient health through wearable biosensors such as electroencephalogram (EEG), electrocardiogram (ECG), smart bracelets, and gait sensors, enabling early detection of potential health risks. The continuous adaptation of AI-powered analysis refines diagnostic precision, enhancing the efficiency, reliability, and personalization of consumer wearable healthcare technologies [2].

Ensuring data privacy and security is a critical challenge in the public communication framework of RPHM. In such environments, interconnected consumer healthcare devices, wearable sensors, and medical infrastructure exchange real-time data over public channels, making the system vulnerable to security threats. Malicious users such as  $\mathbb{A}_d$  can exploit these vulnerabilities to gain unauthorized access to patient information, leading to serious personal and social consequences [3]. In addition to gaining unauthorized access,  $\mathbb{A}_d$  can compromise both long-term and short-term secrets, enabling the reconstruction of session keys and the disruption of system states. Furthermore,  $\mathbb{A}_d$  may exploit power analysis to extract stored keys and clone them, allowing impersonation of legitimate devices and bypassing authentication. Additionally, compromised healthcare data can be misused to track patient locations or expose medical records. Public communication networks are also susceptible to various cyberattacks, including impersonation, ephemeral secret leakage attacks, and ML or modeling [4]. ML or modeling attacks occur when attackers exploit AI-based security mechanisms to bypass authentication. They can analyze patterns in authentication requests to predict or forge valid credentials. Attackers may also train models on leaked authentication data to mimic legitimate users [5].

To address these concerns, researchers have proposed various protocols aimed at enhancing privacy and security, as summarized in Table I. It presents an analysis of recent authentication protocols, highlighting their development tech-

TABLE I: Summary of Related Work

Protocols	Year	Development Techniques	Benefits	Drawbacks/Flaws
Shihab and AlTawy [6]	2023	* Hash Function	* Resists desynchronization attacks * Resists replay attacks * Resists stolen device attacks	* Vulnerable to physical attacks * Prone to user impersonation attacks * Susceptible to machine learning attacks
Servati et al. [7]	2023	* ECC * Hash Function	* Resists server impersonation * Resists ephemeral secret leakage attacks * Resists stolen verifier attacks	* Prone to machine learning attacks * Prone to physical attacks * Susceptible to device impersonation attacks
Das et al. [8]	2023	* PUF	* Resists replay attacks * Offers Anonymity * Resists physical attacks	* Prone to stolen verifier attacks * Noisy PUF * Does not resist device impersonation attacks
Saini et al. [9]	2024	* Hash Function * Three factor	* Resists impersonation attacks * Offers Anonymity * Resists stolen verifier attacks	* Prone to ephemeral secret leakage attacks * Vulnerable to ML or modelling attacks * Does not offer perfect forward secrecy
Chen et al. [10]	2024	* Hash Function * ECC	* Resists impersonation attacks * Offers Anonymity * Resists stolen verifier attacks	* Susceptible to physical attacks * Vulnerable to ML or modelling attacks * Susceptible to ephemeral secret leakage attacks
Yu et al. [11]	2025	* Hash Function * Hybrid PUF	* Resists impersonation attacks * Resists ML or Modeling attacks	* Vulnerable to ephemeral secret leakage attacks

niques, security strengths, and vulnerabilities. Despite these advancements, many existing protocols remain susceptible to security threats, including physical tampering, impersonation, and ephemeral secret leakage attacks, underscoring the need for a more resilient authentication mechanism. Moreover, the main contributions of our work are as follows:

- 1) We propose a machine learning attack resilient authentication protocol for AI-driven RPHM by integrating OPUF with ECC. Our protocol combines the unpredictability of OPUF responses with ECC to ensure tamper-evident, device-specific authentication and secure key agreement.
- 2) We employ OPUFs to enhance the security of the authentication mechanism against ML or modeling attacks and physical tampering. Unlike conventional static PUFs, which produce repeatable responses and are vulnerable to pattern analysis, OPUFs generate a fresh, session-specific response, rendering modeling-based attacks ineffective. This novel design ensures tamper-evident, device-specific authentication that significantly advances prior static PUF-based protocols.
- 3) We incorporate lightweight cryptographic operations to enhance resource efficiency while significantly reducing communication and computation costs by an average of 23.62% and 40.54%, respectively.

## II. PRELIMINARIES

This section defines key concepts essential to our proposed approach. Additionally, the notations used throughout the paper are summarized in Table II.

TABLE II: Notations Table

Notations	Elucidations
$MGW_c$	Medical Gateway
$S_j$	$j_{th}$ Medical Sensor
$U_i$	$i_{th}$ User of system
$\lambda$	Master Secret Key of $MGW_c$
$SID_j$	Pseudonym of $S_j$
$IoMT$	Internet of Medical Things
$h(\cdot)$	One way hash function
$  $	Concatenation Operator
OPUF	One time Physically Unclonable Function
ECC	Elliptic Curve Cryptography
$C_i, \mathcal{R}_i$	Challenge Response Pair
$List_{CRP}$	List of Challenge-Response Pair for $S_j$
$P$	Generator of Elliptic Curve
$F.Gen()/F.Rec()$	Fuzzy Extractor and Re-generator Functions
$\mathbb{A}_d$	Adversary/Attacker

### A. Adversarial Capabilities

We adopt widely recognized threat models like the Dolev-Yao (DY) model [12] and Canetti and Krawczyk (CK) model [13] to rigorously define the capabilities of an adversary ( $\mathbb{A}_d$ ). Under the DY model,  $\mathbb{A}_d$  can intercept, manipulate, or forge messages within the communication channel. Moreover,  $\mathbb{A}_d$  replay any intercepted message. In contrast, the CK model grants  $\mathbb{A}_d$  with added capabilities, allowing them to compromise both long-term and short-term secrets in addition to capturing messages. With the help of these compromised secrets,  $\mathbb{A}_d$  can undermine the security of established session keys and system states. Apart from the assumptions mentioned earlier,  $\mathbb{A}_d$  can potentially leverage power analysis attacks to extract cryptographic keys stored in  $S_j$ 's memory.  $\mathbb{A}_d$  can further create a clone of stolen keys, using which he can impersonate the legitimate  $S_j$  by bypassing the authentication process.

### B. One Time Physically Unclonable Function

A One-Time Physically Unclonable Function (OPUF) leverages inherent device-specific physical characteristics  $\Psi$  to generate a unique, non-reusable response  $\mathcal{R}_i$  for each distinct challenge  $C_i$ . Formally,  $\mathcal{R}_i = f(C_i; \Psi)$ , where  $C_i$  has not been previously used. Each response is valid for one-time use, with the challenge history updated after each invocation to prevent reuse. The security strength of the OPUF is characterized by the entropy  $\sigma(\Psi) = \text{Entropy}(\mathcal{R}_i|\Psi)$ , ensuring unpredictability and resistance to replay and tampering attacks.

### C. Network Model

The remote patient health monitoring discussed in this paper is designed around three principal entities:  $S_j$ ,  $U_i$ , and  $MGW_c$ , all depicted in Fig. 1. The system operates primarily through these interconnected elements to ensure efficient and secure patient monitoring. Medical sensors are strategically placed on the patient's body within the operational environment. These sensors are tasked with continuously gathering health data, which they then transmit to the  $MGW_c$  for processing. Each sensor is registered with the  $MGW_c$ , which, in turn, provides a session key to encrypt the communications, thereby enhancing the security of the transmitted data.

In the proposed framework,  $U_i$  is authenticated by the trusted  $MGW_c$  through a smart card issued after registration. The  $MGW_c$  secures the identities of both users and

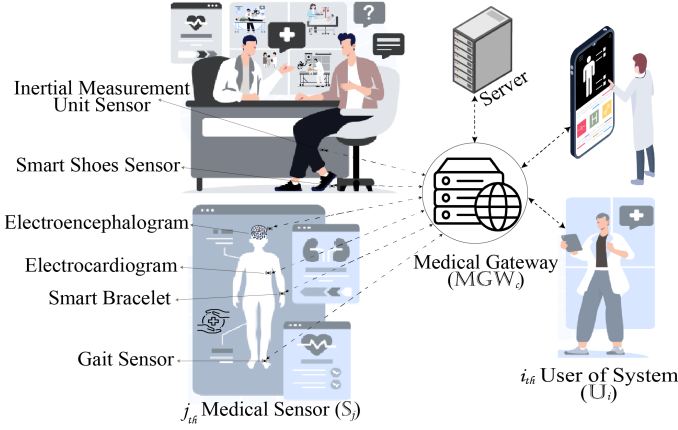


Fig. 1: Remote Patient Health Monitoring System

$S_j$ , and facilitates mutual authentication. Once authenticated, a session key is established via  $MGW_c$  to encrypt sensor data, ensuring that only authorized users can access the collected medical information. To support long-term access to patients' health data, the server securely stores and manages encrypted records received from  $MGW_c$ . This ensures that historical data remains available for diagnosis and analysis, even in the absence of real-time monitoring. Whether data is transmitted automatically or entered manually, the server provides a reliable and secure storage framework, reinforcing the integrity and availability of patient information in remote health monitoring systems.

### III. THE PROPOSED PROTOCOL

This section presents our machine learning attack resilient authentication protocol for AI-driven RPHM. This protocol is designed to provide robust security against evolving cyber threats. Unlike the traditional PUF, which relies on reusable challenge-response pairs and is susceptible to ML or modeling attacks, we integrate OPUF in our protocol with non-reproducible responses that make it more tamper-resistant. An illustration of our proposed authentication flow is also given in Fig. 2. The following subsections detail the step-by-step phases of the authentication process.

#### A. $U_i$ Registration Phase

In this phase, each user ( $U_i$ ) initiates registration by submitting their identity  $ID_i$ , password  $PW_i$ , and biometric data  $BIO_i$ . The user generates a random nonce  $r_i$  and computes  $HPW_i = h(ID_i || PW_i || r_i)$ , which is sent to the trusted gateway  $MGW_c$  along with  $ID_i$ . Upon receiving this,  $MGW_c$  computes  $D_i = h(ID_i || \lambda)$ , selects a  $k$ -bit string  $k_i$ , and derives  $B_i = h((h(ID_i || k_i || D_i) \oplus HPW_i) \bmod n_0)$ . It then sends  $\{B_i, D_i, k_i\}$  to  $U_i$ . The user, using their biometric input, generates  $(\alpha, \beta) \leftarrow F.Gen(BIO_i)$ , computes  $Key_i = h(ID_i || \alpha) \oplus k_i$  and  $DM_i = D_i \oplus k_i$ , and securely stores  $\{B_i, Key_i, DM_i, \beta, r_i\}$  for future authentication.

#### B. $S_j$ Registration Phase

A trusted  $MGW_c$  being the trusted authority, performs the registration of each medical sensor ( $S_j$ ), where ( $j = 1, 2, 3, \dots$ ,

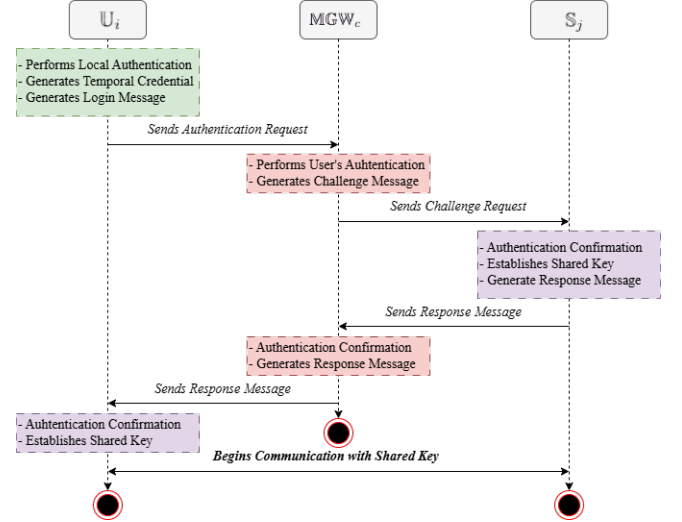


Fig. 2: Illustration of the Authentication Flow

$n_s$ ) in an IoMT environment. The communication between  $S_j$  and  $MGW_c$  in this stage occurs on a private channel. In order to register each  $S_j$ ,  $MGW_c$  selects a unique identity  $SID_j$  for each  $S_j$ . After that,  $MGW_c$  produces a list of challenge response pairs  $CRP$ , and calculates  $k_j = h(SID_j || \lambda)$ , where  $\lambda$  is a master secret key of  $MGW_c$ . After performing the above steps,  $MGW_c$  keeps the information  $\langle k_j, CRP_j \rangle$  against each  $SID_j$ .

#### C. Authentication and Key Agreement Phase

This phase represents the login and authentication phase among User ( $U_i$ ), Medical Sensor ( $S_j$ ), and Medical Gateway ( $MGW_c$ ). This communication occurs on an open or insecure channel. During this, we determine the session key among  $U_i$ ,  $S_j$  and  $MGW_c$ . We execute the following steps for a specific session to establish the session key as depicted in Fig. 3.

- 1: First of all,  $U_i$  inputs  $ID_i$ ,  $PW_i$  and imprints  $BIO_i$  and determines  $\alpha \leftarrow REP(BIO_i, \beta)$ ,  $k_i = h(ID_i || \alpha) \oplus Key_i$ ,  $D_i = DM_i \oplus k_i$ ,  $B_i \stackrel{?}{=} h((h(ID_i || k_i || D_i) \oplus HPW_i) \bmod n_0)$ . Further,  $U_i$  engenders an arbitrary nonce  $a$  and determines  $J_1 = aP$ ,  $J_2 = aX$ ,  $J_3 = (ID_i || k_i) \oplus J_2$ ,  $J_4 = SID_j \oplus h(J_1 || J_2)$ ,  $J_5 = h(ID_i || SID_j || k_i || D_i || J_2)$  and then transmits login request message  $W_1 \leftarrow \{J_1, J_3, J_4, J_5\}$  towards  $MGW_c$  via insecure channel.
- 2: After getting request message  $W_1 \leftarrow \{J_1, J_3, J_4, J_5\}$  from the particular  $U_i$ ,  $MGW_c$  computes  $J_2 = \lambda \cdot J_1$ ,  $(ID_i || k_i) = J_3 \oplus J_2$ ,  $SID_j = J_4 \oplus h(J_1 || J_2)$ ,  $D_i = h(ID_i || \lambda)$ ,  $J_5 \stackrel{?}{=} h(ID_i || SID_j || k_i || D_i || J_2)$ .  $MGW_c$  retrieves  $\{CRP_j, k_j\}$  against  $SID_j$  and computes  $(\alpha_j, \beta_j) \leftarrow F.Gen(R_j)$ ,  $J_6 = C_j \oplus SID_j$ ,  $J_7 = h(SID_j || k_j || J_1 || \alpha_j)$ . After that, it transmits  $W_2 \leftarrow \{J_1, J_6, J_7\}$  towards  $S_j$ .
- 3: After receiving the message  $W_2 \leftarrow \{J_1, J_6, J_7\}$  from  $MGW_c$ ,  $S_j$  determines  $C_j = J_6 \oplus SID_j$ ,  $R_j \leftarrow (C_j)$ ,  $(\alpha_j, \beta_j) \leftarrow F.Gen(R_j)$ ,  $J_7 = h(SID_j || k_j || J_1 || \alpha_j)$ . After that,  $S_j$  engenders an arbitrary nonce  $c$  and determines  $J_8 = cP$ ,  $J_9 = cJ_1$ ,  $J_{10} = \alpha_j \oplus J_8$ ,

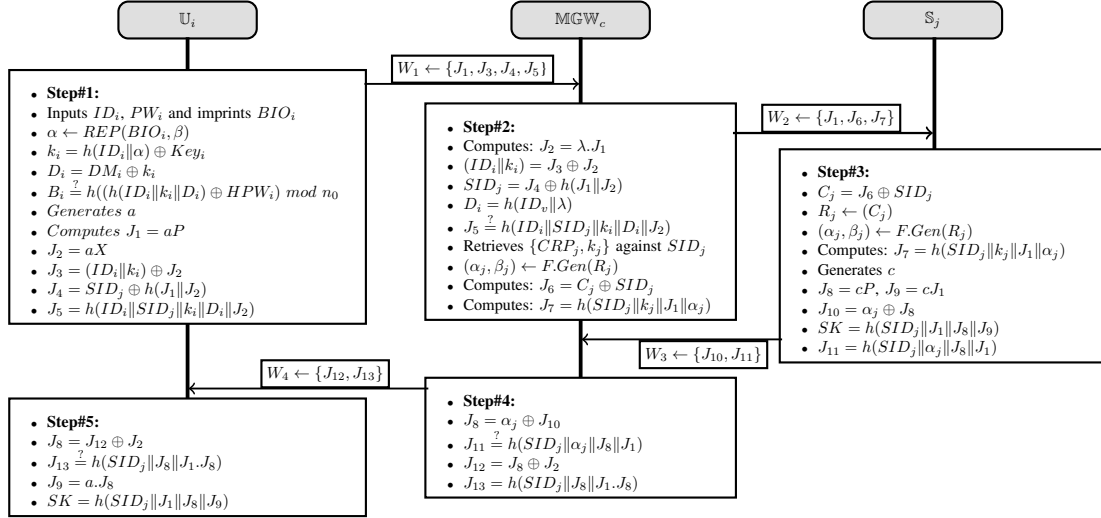


Fig. 3: Login and Authentication phase for Patient's e-healthcare Monitoring

$SK = h(SID_j || J_1 || J_8 || J_9)$ ,  $J_{11} = h(SID_j || \alpha_j || J_8 || J_1)$ . Further, it transmits the  $W_3 \leftarrow \{J_{10}, J_{11}\}$  towards  $MGW_c$ .

- Upon getting message  $W_3 \leftarrow \{J_{10}, J_{11}\}$  from  $S_j$ ,  $MGW_c$  computes  $J_8 = \alpha_j \oplus J_{10}$ ,  $J_{11} \stackrel{?}{=} h(SID_j || \alpha_j || J_8 || J_1)$ ,  $J_{12} = J_8 \oplus J_2$ ,  $J_{13} = h(SID_j || J_8 || J_1 || J_8)$  and transmits  $W_4 \leftarrow \{J_{12}, J_{13}\}$  towards  $U_i$ .
- When  $U_i$  gets the information  $W_4 \leftarrow \{J_{12}, J_{13}\}$  from  $MGW_c$ , it computes  $J_8 = J_{12} \oplus J_2$ ,  $J_{13} \stackrel{?}{=} h(SID_j || J_8 || J_1 || J_8)$ ,  $J_9 = a \cdot J_8$  and lastly determines the  $SK = h(SID_j || J_1 || J_8 || J_9)$  which is mutually shared among the participating entities.

#### IV. SECURITY ANALYSIS

This section conducts a comprehensive security analysis of the proposed authentication protocol, utilizing both informal and formal methods as suggested in [14].

##### A. Informal Security Analysis

We conduct an informal analysis of the proposed protocol, focusing on its resilience to various security attacks.

1) *Ensures Anonymity*: In the proposed protocol, user ( $U_i$ ) keeps  $ID_i$  private. The transmitted public message  $W_1 \leftarrow \{J_1, J_3, J_4, J_5\}$  does not reveal any guess of  $ID_i$  to adversary ( $A_d$ ).  $J_3$  involves  $ID_i$  as  $J_3 = (ID_i || k_i) \oplus J_2$ . Each session employs a distinct  $J_3$  because  $J_2$  in  $J_3$  is session-specific as it is determined as  $J_2 = aX$ . This distinct  $J_3$  makes it impossible for  $A_d$  to track  $U_i$  through monitoring different messages from the same  $U_i$ . Moreover, to determine  $J_3$ ,  $A_d$  needs to calculate  $k_i$ , which requires the knowledge of actual  $ID_i$  and  $\alpha$ . However,  $A_d$  don't have access to these values. Therefore, this inability of  $A_d$  to trace actions or discern the real  $ID_i$  of  $U_i$  confirms the protocol's effectiveness in ensuring  $U_i$  anonymity.

2) *Resists Physical Attacks*: If  $A_d$  attempts to tamper  $S_j$  physically, the embedded PUF within  $S_j$  exhibits a sudden and noticeable behavioral alteration. This disruption prevents PUF from performing its intended functionality. It causes it to fail to generate the expected response  $(\alpha_j, \beta_j) \leftarrow F.Gen(R_j)$  during the physical attack attempt. Moreover,  $MGW_c$  verifies the response by validating  $J_{11} \stackrel{?}{=} h(SID_j || \alpha_j || J_8 || J_1)$ . As a result, any physical tampering on  $S_j$  by  $A_d$  is immediately detectable and resistable by  $MGW_c$ . Thus, the proposed protocol demonstrates robust resistance to physical attacks.

3) *Machine Learning and Modelling Attacks*: To formally argue the resilience of OPUF against modeling attacks (e.g., logistic regression, linear SVM), we define the OPUF as a probabilistic function  $f : C_i \times \Psi \rightarrow R_i$ , where  $C_i$  is the challenge space,  $\Psi$  is an internal hidden state (e.g., time, nonce), and  $R_i$  is the response space. The state  $s \in \Psi$  evolves after each invocation, ensuring that no two inputs  $(c_i, s_i)$  and  $(c_j, s_j)$  are the same across queries. This renders  $f$  a *non-repeatable oracle*, meaning the adversary observes at most one response per unique challenge-state pair. The adversary's goal is to learn a hypothesis function  $h : C_i \rightarrow R_i$  that minimizes prediction error:  $\Pr_{(c,s) \sim \mathcal{D}}[h(c) = f(c, s)]$ . However, due to the non-reusability of challenges and the evolving state, the learning setting lacks the identically distributed structure and repeated samples required for effective generalization. Therefore, for any machine learning algorithm  $A$ , we have:  $\Pr[A(c) = f(c, s)] \leq \frac{1}{|\mathcal{R}_i|} + \varepsilon$ , where  $\varepsilon$  is negligible. This bound implies that the adversary's success is no better than random guessing, establishing formal resistance against modeling attacks.

4)  *$U_i$ ,  $MGW_c$ , and  $S_j$  Impersonation Attacks*: The proposed protocol is resistant to impersonation attacks targeting  $U_i$ ,  $MGW_c$ , and  $S_j$ . To impersonate  $U_i$ , an adversary  $A_d$  must access secret values like  $ID_i$ ,  $k_i$ , and  $D_i$ , which are not exposed. Impersonating  $MGW_c$  requires computing values based on  $SID_j$  and  $k_j$ , both derived using the master secret  $\lambda$ , which is kept confidential. Similarly, impersonating  $S_j$  requires reproducing the non-clonable PUF response  $\alpha_j$  and

$SID_j$ , which are inaccessible without  $\lambda$ . Hence, the protocol ensures robust protection against all impersonation threats.

5) *Ephemeral Secret Leakage Attacks*: According to the assumptions outlined in Section II-A,  $\mathbb{A}_d$  could potentially reconstruct the session key if they gain access to the ephemeral secrets of a session. The session key is determined as  $SK = h(SID_j \| J_1 \| J_8 \| J_9)$ , where  $J_1 = aP$ ,  $J_8 = cP$  and  $J_9 = cJ_1$ . So, in the session key computation, the ephemeral secrets  $a$  and  $c$  are used. Since  $a$  and  $c$  remain private and are never publicly transmitted,  $\mathbb{A}_d$  cannot directly retrieve them. Even in the worst-case scenario, where  $\mathbb{A}_d$  manages to deduce  $SK$  for a specific session, previously established session keys remain uncompromised. Thus, our protocol ensures resilience against ephemeral secret leakage attacks.

6) *Ensures Perfect Forward Secrecy*: The  $SK$  is computed as  $SK = h(SID_j \| J_1 \| J_8 \| J_9)$ , incorporating the session-specific values  $J_1$ ,  $J_8$ , and  $J_9$ . These values are unique for each session. This approach ensures that even if the current session key is compromised, deriving previous session keys remains infeasible. Consequently,  $\mathbb{A}_d$  cannot exploit compromised values to reconstruct past session keys. Thus, the proposed protocol guarantees perfect forward secrecy.

## B. Formal Security Analysis

In this section, the proposed protocol undergoes a formal analysis within the random oracle model [13], [15] to demonstrate its provable security in meeting the specified security requirements. Additionally, the proof of the protocol is detailed in Theorem 1 to underscore the importance of session key agreement.

**Security Model:** Our formal security analysis incorporates three key entities:  $\mathbb{U}_i$ ,  $\text{MGW}_c$  and  $\mathbb{S}_j$ , which are represented as  $\Pi_{\mathbb{U}_i}^a$ ,  $\Pi_{\text{MGW}_c}^b$  and  $\Pi_{\mathbb{S}_j}^c$  respectively. To rigorously evaluate the protocol's security, we analyze the query capabilities of adversary  $\mathbb{A}_d$ , defined by  $K = \{\Pi_{\mathbb{U}_i}^a, \Pi_{\text{MGW}_c}^b, \Pi_{\mathbb{S}_j}^c\}$ . We outline the specific query operations that  $\mathbb{A}_d$  can execute to potentially undermine the security of the protocol as follows:

- *Execute*( $K$ ) :  $\mathbb{A}_d$  can intercept the exchanged messages between  $\mathbb{U}_i$ ,  $\text{MGW}_c$  and  $\mathbb{S}_j$  over the public channel. This query operation illustrates a passive attack scenario where an  $\mathbb{A}_d$  merely observes the exchanged information without altering it.
- *Hash*( $S_t$ ) : This query permits  $\mathbb{A}_d$  to submit a string  $S_t$  and receive the resultant hash value calculated by the hash function.
- *Send*( $K, M_{sg}$ ) :  $\mathbb{A}_d$  has the capability to transmit  $M_{sg}$  to ( $K$ ) and retrieve the response message from ( $K$ ).
- *Corrupt*( $K$ ) :  $\mathbb{A}_d$  can access confidential parameters of a specific entity, including the long-term key, temporarily produced information, and data maintained in the smart device.
- *Test*: The *Test* query facilitates evaluating the semantic security of the session key ( $SK$ ) formed during the entities' communication.  $\mathbb{A}_d$  conducts this query by tossing a coin  $Co_n$ , which can result in either 0 or 1. Should  $Co_n = 1$ ,  $\mathbb{A}_d$  gains access to the actual  $SK$ ; if  $Co_n = 0$ ,  $\mathbb{A}_d$  receives a random string identical in length to  $SK$ .

**Theorem 1:** Consider  $\mathbb{A}_d$  as an adversary with the capability to execute the aforementioned queries and launch attacks on our protocol  $PR$  within probabilistic polynomial time, to compromise the protocol's semantic security. The measure of  $\mathbb{A}_d$ 's success in compromising  $PR$  is presented as:

$$\text{Advgt}_{\mathbb{A}_d}^{PR}(\varphi) \leq \frac{q_{hs}^2}{|\text{Hash}|} + \frac{H_{Puf}^2}{|\text{OPUF}|} + 2 \left\{ \max \{C \cdot q_{s'}^s, \frac{q_{sd}}{2^{ln}}\} + \text{Advgt}^{ECDLP}(p_t) \right\}$$

Here,  $q_{hs}$  represents the total number of Hash queries executed,  $q_{sd}$  denotes the total number of Send queries executed,  $|\text{Hash}|$  corresponds to the range of the hash function  $h(\cdot)$ ,  $H_{Puf}$  indicates Puf queries and  $|\text{OPUF}|$  output range space queries are made, respectively.  $ln$  indicates the bit length of the arbitrary biometric key, and  $C$  and  $s'$  are constant parameters defined in Zipf's law [16].  $\text{Advgt}_{\mathbb{A}_d}^{ECDLP}(p_t)$  represents the advantage of an  $\mathbb{A}_d$  using algorithm to solve the discrete logarithm problem in polynomial time ( $p_t$ ).

We develop a series of games ranging from  $GM_0$  to  $GM_5$ , which include participants  $K$  and  $\mathbb{A}_d$ . To establish the security of the protocol, we rigorously analyze these games. Throughout the proof, the notation  $\text{Sucs}_{\mathbb{A}_d}^{GM_i}$  signifies the likelihood of participant A correctly predicting the outcome of a coin toss  $Co_n$  in game  $GM_i$ . The term  $\text{Advgt}_{\mathbb{A}_d}^{PR}(\varphi)$  represents the advantage that A has in successfully compromising the security of the protocol.

$GM_{(0)}$  : In the initial round,  $\mathbb{A}_d$  refrains from initiating any query operation and begins the game by tossing a coin  $Co_n$ . From this, we can derive:

$$\text{Advgt}_{\mathbb{A}_d}^{PR}(\varphi) = |2\text{Pr}[\text{Sucs}_{\mathbb{A}_d}^{GM_{(0)}}] - 1| \quad (1)$$

$GM_{(1)}$  : In this game,  $\mathbb{A}_d$  conducts the *Execute* query to simulate an eavesdropping attack. This allows  $\mathbb{A}_d$  to intercept the messages  $\{W_1, W_2, W_3, W_4\}$  transmitted over the public channel. After  $GM_{(1)}$ ,  $\mathbb{A}_d$  employs the *Test* query, utilizing the gathered parameters to calculate  $SK$ . However, because  $\mathbb{A}_d$  fails to intercept  $\{\alpha, k_i, D_i, J_5, C_i\}$ , the probability of  $\mathbb{A}_d$ 's success in this round does not exceed that of the previous round. Consequently, the probability for  $GM_{(1)}$  remains equivalent to  $GM_{(0)}$ , expressed as:

$$\text{Pr}[\text{Sucs}^{GM_{(1)}}] = \text{Pr}[\text{Sucs}^{GM_{(0)}}] \quad (2)$$

$GM_{(2)}$  : In this game, an active attack model is introduced by enabling  $\mathbb{A}_d$  to issue *Send* and *Hash* queries, unlike  $GM_{(1)}$ . The adversary attempts to deceive participants with forged messages and checks for hash collisions. However, since the exchanged messages  $W_1, W_2, W_3, W_4$  include dynamic and unpredictable elements (e.g., random numbers, identities, and long-term secrets), no collisions occur. Based on the birthday paradox, the probability of a successful collision remains negligible.

$$\text{Pr}[\text{Sucs}^{GM_{(2)}}] - \text{Pr}[\text{Sucs}^{GM_{(1)}}] \leq \frac{q_{hs}^2}{2|\text{Hash}|} \quad (3)$$

$GM_{(3)}$  : After obtaining the user's smart card and executing *Corrupt*( $K$ ),  $\mathbb{A}_d$  can extract sensitive information, such as  $\{B_i, \text{Key}_i, DM_i, \beta, r_i\}$ , which is encrypted and stored within the smart card's memory.  $\mathbb{A}_d$  must perform PUF queries to access this confidential information. Since the PUF generates a unique response for each distinct challenge,  $\mathbb{A}_d$  cannot find any collisions while conducting these queries. Consequently, we derive:

$$\text{Pr}[\text{Sucs}^{GM_{(3)}}] - \text{Pr}[\text{Sucs}^{GM_{(2)}}] \leq \frac{H_{Puf}^2}{2|\text{OPUF}|} \quad (4)$$

$GM_{(4)}$  : In this game,  $\mathbb{A}_d$  uses the *Corrupt* query to extract sensitive values from  $\mathbb{U}_i$ 's smart card via power analysis. Since the protocol relies on both a password  $PW_i$  and biometric key  $\alpha$  derived from  $BIO_i$ ,  $\mathbb{A}_d$  may attempt an offline password-guessing attack. However, success depends on knowing the  $ln$ -bit biometric key  $\alpha$ , with a guessing probability of approximately  $1/2^{ln}$ . Additionally, the system limits password attempts, and Zipf's law further reduces the attack's feasibility.

$$Pr[Sucs^{GM_{(4)}}] - Pr[Sucs^{GM_{(3)}}] \leq \max \left\{ C \cdot q_s^s, \frac{q_{sd}}{2ln} \right\} \quad (5)$$

$GM_{(5)}$  : This is the final game, where  $\mathbb{A}_d$  attempts to pass authentication checks and derive key  $SK$  by intercepting the communication sequences:  $W_1 \leftarrow \{J_1, J_3, J_4, J_5\}$ ,  $W_2 \leftarrow \{J_1, J_6, J_7\}$ ,  $W_3 \leftarrow \{J_{10}, J_{11}\}$  and  $W_4 \leftarrow \{J_{12}, J_{13}\}$ . For reaching  $SK$ ,  $\mathbb{A}_d$  has to pass the mutual authentication checks (i.e.,  $J_5 \stackrel{?}{=} h(ID_i || SID_j || k_i || D_i || J_2)$ ,  $J_7 \stackrel{?}{=} h(SID_j || k_j || J_1 || \alpha_j)$ ,  $J_{11} \stackrel{?}{=} h(SID_j || \alpha_j || J_8 || J_1)$  and  $J_{13} \stackrel{?}{=} h(SID_j || J_8 || J_1 || J_8)$ ). For each authentication check,  $\mathbb{A}_d$  must produce a valid hash value without knowing all the correct secrets  $\{k = J_1, J_2, J_7, J_8\}$ . Here  $h$  is modeled as a random oracle and  $\mathbb{A}_d$  must query  $h(x)$  on the exact input  $k$ . Despite these efforts,  $\mathbb{A}_d$  fails to compute  $J_1 = aP$   $J_2 = \lambda \cdot J_1$ ,  $J_9 = a \cdot J_8$  and  $J_7 = h(SID_j || k_j || J_1 || \alpha_j)$  within a feasible time due to the complexities associated with the Elliptic Curve Discrete Logarithm Problem (ECDLP). Consequently,  $\mathbb{A}_d$ 's likelihood of success in  $GM_{(5)}$  can be quantified as follows.

$$Pr[Sucs^{GM_{(5)}}] - Pr[Sucs^{GM_{(4)}}] \leq \text{Advgt}_{\text{ECDLP}}(p_t) \quad (6)$$

Once all the games have been completed,  $\mathbb{A}_d$  makes a random guess for bit  $c$  using the Test query. Therefore, we obtain:

$$Pr[Sucs^{GM_{(5)}}] = \frac{1}{2} \quad (7)$$

As a result, it is evident that  $\mathbb{A}_d$  has only a negligible chance of compromising the semantics of  $SK$  in our protocol. The following result can be derived from equation (1,2) and (7).

$$\begin{aligned} \frac{1}{2} \cdot \text{Advgt}_{\mathbb{A}_d}^{PR} &= |Pr[Sucs^{GM_{(0)}}] - \frac{1}{2}| \\ &= |Pr[Sucs^{GM_{(1)}}] - Pr[Sucs^{GM_{(5)}}]| \end{aligned} \quad (8)$$

By applying the triangle inequality, we can obtain the following result from equations (3-6) and (8):

$$\begin{aligned} \frac{1}{2} \text{Advgt}_{\mathbb{A}_d}^{PR}(\varphi) &= |Pr[Sucs^{GM_{(1)}}] - Pr[Sucs^{GM_{(5)}}]| \\ &\leq |Pr[Sucs^{GM_{(1)}}] - Pr[Sucs^{GM_{(2)}}]| \\ &\quad + |Pr[Sucs^{GM_{(2)}}] - Pr[Sucs^{GM_{(3)}}]| \\ &\quad + |Pr[Sucs^{GM_{(3)}}] - Pr[Sucs^{GM_{(4)}}]| \\ &\quad + |Pr[Sucs^{GM_{(4)}}] - Pr[Sucs^{GM_{(5)}}]| \\ &\leq \frac{q_{hs}^2}{2|\text{Hash}|} + \frac{H_{Puf}^2}{2|\text{OPUF}|} + \max \left\{ C \cdot q_s^s, \frac{q_{sd}}{2ln} \right\} \\ &\quad + \text{Advgt}^{ECDLP}(p_t) \end{aligned} \quad (9)$$

At last, by multiplying both sides of the equation (9) by two, the required result can be obtained:

$$\text{Advgt}_{\mathbb{A}_d}^{PR}(\varphi) \leq \frac{q_{hs}^2}{|\text{Hash}|} + \frac{H_{Puf}^2}{|\text{OPUF}|} + 2 \left\{ \max \left\{ C \cdot q_s^s, \frac{q_{sd}}{2ln} \right\} + \text{Advgt}^{ECDLP}(p_t) \right\}$$

## V. PERFORMANCE EVALUATION

This section evaluates the performance of the proposed patient e-healthcare monitoring protocol, focusing on the computation cost, scalability analysis, communication cost, and

security features provision. The evaluation primarily considers the authentication phase only, as the registration phase for users and sensor nodes is relatively infrequent. The performance of the proposed protocol is further compared with competing protocols [6], [9], [10], [17]–[19] to determine its effectiveness. For comparative analysis, we only selected recent benchmark protocols designed specifically for our network model, emphasizing authentication, key management, and contemporary advancements in e-healthcare security to highlight our protocol's robustness and efficiency. The performance evaluation details are further elaborated in the following subsections.

### A. Experimental Setup

We have developed an experimental setup to determine the execution time of cryptographic operations utilized in the proposed and competing protocols. For the OPUF implementation, we utilized an SRAM-based OPUF deployed on an Xilinx Spartan-7 FPGA board. Moving forward, a Raspberry Pi model 3 (RPi3) has been employed to simulate the cryptographic operations performed on sensor nodes, considering the resource-constrained nature of IoT. Since the sensors do not have built-in processing capabilities, RPi3 handles the computation of cryptographic operations, ensuring efficient data processing and analysis. However, the operations executed on the medical gateway and user sides are implemented on a dedicated system and a mobile device, respectively. The specifications of the Raspberry Pi, dedicated system, and mobile device are listed in Table III. To ensure unbiased results, the cryptographic operations of the proposed and competing protocols were executed multiple times under identical conditions. The execution times for various cryptographic operations, corresponding to their respective implementation devices, are presented in Table IV.

TABLE III: Specifications of Implementation Devices

Feature(s)	Implementation Devices		
	Raspberry Pi	Dedicated System	Mobile Device
Model	Raspberry Pi 3 Model B+	Lenovo V15 G4	Redmi Note 13
Operating System	Raspberry Pi OS	Windows 11	MIUI 14
Processing Speed	1.2 GHz	3.7 GHz	2.8 Ghz
RAM	1GB	16GB	8GB
Language	Python 3.12	Python 3.12	Python 3.12
Library	cryptography	cryptography	cryptography

TABLE IV: Execution Time of Cryptographic Operations

Operation(s)	Execution Time (ms)		
	Raspberry Pi	System	Mobile
Hash Function ( $E_h$ )	2.315	0.331	0.749
Point Multiplication ( $E_{pm}$ )	3.105	0.636	1.139
Symmetric Encryption/Decryption ( $E_{se/sd}$ )	2.602	0.310	0.911
One Time Physically Unclonable Function ( $E_{opuf}$ )	1.106	0.105	0.209
Fuzzy Extractor ( $E_{fe}$ )	0.905	0.110	0.195

### B. Analysis of Computation Cost

The computation cost of the proposed and competing protocols is evaluated based on the execution time of cryptographic operations listed in Table IV. In the authentication phase of the proposed patient e-healthcare monitoring protocol,  $\mathbb{U}_i$  performs seven hash functions, one point multiplication, and one fuzzy extractor operation, resulting in a total cost of  $7E_h +$



TABLE V: Computation Cost &amp; Communication Cost: A Comparative Analysis

Protocol	Computation Cost (ms)				Communication Cost (bits)			
	$U_i$	$MGW_c$	$S_j$	Accumulative Cost	$U_i$	$MGW_c$	$S_j$	Accumulative Cost
Proposed	$7E_h + 1E_{pm} + 1E_{fe} \approx 6.577$	$6E_h + 1E_{pm} + 1E_{opuf} \approx 2.837$	$3E_h + 1E_{fe} \approx 7.85$	17.26	992	1152	416	2560
[17]	$27E_h + 1E_{fe} \approx 20.418$	$12E_h \approx 3.972$	$13E_h \approx 30.095$	54.49	832	2176	672	3680
[6]	$8E_h \approx 5.992$	$10E_h \approx 3.31$	$5E_h \approx 11.575$	20.88	832	1920	672	3424
[9]	$15E_h + 2E_{pm} + 1E_{fe} \approx 13.708$	$10E_h + 4E_{pm} \approx 5.854$	$5E_h \approx 11.575$	31.14	1056	1088	672	3648
[10]	$9E_h + 1E_{se/sd} + 1E_{fe} \approx 7.847$	$8E_h \approx 2.648$	$15E_h + 1E_{se/sd} \approx 37.327$	47.82	1088	1504	672	3264
[18]	$11E_h + 2E_{se/sd} \approx 10.061$	$16E_h + 3E_{se/sd} \approx 6.226$	$6E_h + 1E_{se/sd} \approx 16.482$	32.78	960	1952	992	3904
[19]	$8E_h \approx 5.992$	$8E_h \approx 2.648$	$4E_h \approx 9.260$	17.90	832	1268	512	2612

$h$ : Hash Function,  $pm$ : Point Multiplication,  $se/sd$ : Symmetric Encryption/Decryption,  $opuf$ : One Time Physically Unclonable Function,  $fe$ : Fuzzy Extractor

$1E_{pm} + 1E_{fe} \approx 6.577$  ms. Similarly,  $MGW_c$  executes six hash functions, one point multiplication, and one OPUF operation, leading to a computation cost of  $(6E_h + 1E_{pm} + 1E_{opuf}) \approx 2.837$  ms. Additionally,  $S_j$  utilizes three hash functions and one fuzzy extractor, incurring a cost of  $(3E_h + 1E_{fe}) \approx 7.850$  ms. The cumulative computation cost of the proposed protocol sums to  $(6.577 + 2.837 + 7.850) \approx 17.26$  ms. In contrast, the computation costs of the competing protocols [6], [9], [10], [17]–[19] are 54.49, 20.88, 31.14, 47.82, 32.78, and 17.90 ms, respectively. A detailed comparison of the computation costs for the proposed and competing protocols is presented in Table V. The results demonstrate that the proposed protocol achieves a 40.54% reduction in computation cost compared to competing protocols, highlighting its lightweight nature.

### C. Scalability and Practical Limits

We determined the scalability of our protocol by increasing the number of iterations up to 100, simulating a large-scale e-healthcare deployment with simultaneous authentication requests. The results presented in Figure 4 show a linear increase in computation overhead, highlighting the protocol's ability to maintain efficient performance as the system scales. Notably, at 100 iterations, the computation overhead remains consistent, demonstrating that our protocol can effectively manage a rising volume of authentication requests. It achieves this while keeping computation overheads low and providing robust security assurances in real-world healthcare settings. This analysis underscores the protocol's scalability and its potential to handle large-scale deployments in practical healthcare environments.

### D. Analysis of Communication Cost

The communication cost of the proposed and competing protocols is evaluated based on the assumptions outlined in [20]. In the proposed patient e-healthcare monitoring protocol, the participating entities  $U_i$ ,  $MGW_c$ , and  $S_j$  exchange a total of four messages to complete the authentication process. The entity  $U_i$  initiates one message,  $W_1 \leftarrow \{J_1, J_3, J_4, J_5\}$ , with a total size of  $(320 + 160 + 256 + 256) = 992$  bits. Similarly,  $MGW_c$  transmits two messages:  $W_2 \leftarrow \{J_1, J_6, J_7\}$  and  $W_4 \leftarrow \{J_{12}, J_{13}\}$ , which require  $(320 + 160 + 256) = 736$  bits and  $(160 + 256) = 416$  bits, respectively, resulting in a total cost of  $(736 + 416) = 1152$  bits. Additionally,  $S_j$  sends one message,  $W_3 \leftarrow \{J_{10}, J_{11}\}$ , to  $MGW_c$ , with a total size of  $(160 + 256) = 416$  bits. The proposed protocol's total communication cost is  $(992 + 1152 + 416) = 2560$  bits. In comparison, the communication costs of the competing protocols [6], [9], [10], [17]–[19] are 3680, 3424, 3648, 3264,

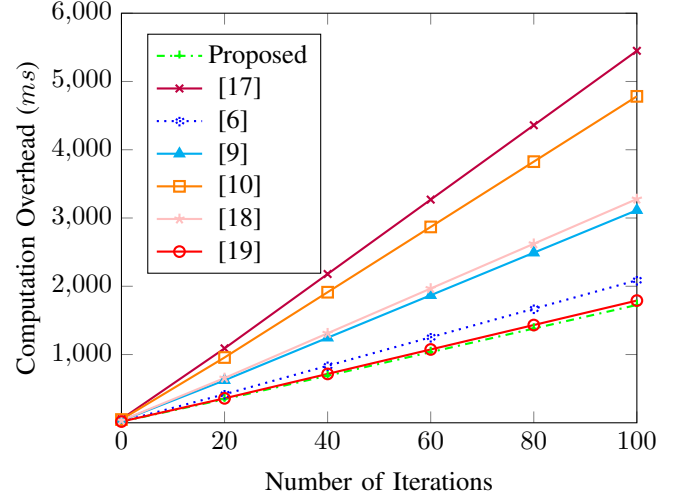


Fig. 4: Scalability Analysis

3904, and 2612 bits, respectively. A comparative analysis of the communication costs for the proposed and competing protocols is provided in Table V. The results demonstrate that the proposed protocol achieves a 23.62% reduction in communication cost compared to competing protocols.

### E. Security Comparison

This subsection presents a comparative analysis of the security features among the proposed and competing protocols [6], [9], [10], [17]–[19]. The comparison is conducted based on the cryptanalysis of the competing protocols. The detailed results of this analysis are provided in Table VI. As evident from the table, all competing protocols fail to offer resistance against physical and machine learning attacks. Additionally, protocols [17], [6], [9], and [18] do not ensure perfect forward secrecy. Moreover, protocols [6], [10], [18], and [19] are vulnerable to ESL attacks. In comparison, the proposed protocol effectively withstands various attacks and ensures a high level of security, demonstrating its superiority over competing protocols.

TABLE VI: Security Features: A Comparative Analysis

Features ↓ / Protocols →	Proposed	[17]	[9]	[10]	[6]	[18]	[19]
$E$ -Anonymity	✓	✓	✓	✓	✓	✓	✓
$W$ -Physical Attack	✓	✗	✗	✗	✗	✗	✗
$W$ -Machine Learning Attack	✓	✗	✗	✗	✗	✗	✗
$W$ - $U_i$ Impersonation	✓	✓	✓	✓	✓	✓	✓
$W$ - $MGW_c$ Impersonation	✓	✓	✓	✓	✓	✓	✓
$W$ - $S_j$ Impersonation	✓	✓	✓	✓	✓	✓	✓
$W$ -Stolen Verifier Attack	✓	✓	✓	✓	✗	✓	✓
$W$ -ESL Attack	✓	✓	✗	✗	✗	✗	✗
$E$ -Perfect Forward Secrecy	✓	✗	✗	✓	✗	✗	✓

✓: Yes; ✗: No;  $E$ : Ensures,  $W$ : Withstand



## F. Significance of Results

The results presented in Section V demonstrate the effectiveness of the proposed protocol in reducing both computation and communication costs, which are important for resource-constrained IoT devices in a healthcare environment. The computation overhead of the proposed protocol is reduced by 40.54% compared to competing protocols. This is particularly important for healthcare devices that rely on limited battery power. Additionally, the reduction in communication cost by 23.62% makes the protocol well-suited for environments with limited bandwidth, such as remote healthcare monitoring. These improvements in both computation and communication costs not only enhance the efficiency of the protocol but also ensure its scalability, as demonstrated by the consistent performance even with increasing authentication requests. Furthermore, the security comparison highlights the robustness of our protocol against various attacks, ensuring better overall security. These results emphasize the practical applicability of the protocol in real-world healthcare environments, where both security and resource efficiency are essential. By improving performance in terms of both security and efficiency, the proposed protocol is a viable solution for large-scale, secure healthcare monitoring systems.

## VI. CONCLUSION

This article proposes a machine-learning attack-resilient authentication protocol for AI-driven consumer wearable health monitoring in IoMT environments. The proposed protocol employs a three-factor authentication mechanism and elliptic curve cryptography to ensure robust security and efficiency. Additionally, integrating an OPUF strengthens resistance against machine learning or modelling attacks. Moreover, it resists physical tampering, impersonation, and ephemeral secret leakage attacks. We demonstrate the security of our protocol through informal and formal analysis, where the informal analysis highlights its ability to withstand potential security attacks, and the formal analysis validates its security. Furthermore, a comparative performance evaluation shows that the proposed protocol outperforms existing authentication protocols by significantly reducing communication and computation overheads. This makes it well-suited for resource-constrained consumer wearable healthcare devices. In future work, we will move beyond the current testbed and Raspberry Pi simulations towards real-time implementation on medical-grade hardware, addressing practical constraints such as reliability, certification, and clinical real-time processing requirements. This advancement will facilitate broader clinical validation and applicability in healthcare scenarios.

## REFERENCES

- [1] M. Nawaz Khan, H. Ur Rahman, T. Hussain, B. Yang, and S. Mian Qaisar, "Enabling trust in automotive iot: Lightweight mutual authentication scheme for electronic connected devices in internet of things," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5065–5078, 2024.
- [2] Z. Ghaffar, W.-C. Kuo, K. Mahmood, T. Tariq, S. Shamshad, A. K. Das, and M. J. Alenazi, "A lightweight and robust access control protocol for iot-based e-healthcare network," *IEEE Transactions on Mobile Computing*, pp. 1–12, 2025.
- [3] A. Sharma, S. Rani, A. K. Bashir, M. Krichen, and A. Alshammari, "A low-rank learning-based multi-label security solution for industry 5.0 consumers using machine learning classifiers," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 833–841, 2023.
- [4] S. M. Nagarajan, G. G. Devarajan, M. S. Thangakrishnan, T. V. Ramana, A. K. Bashir, and A. A. AlZubi, "Artificial intelligence-based zero trust security approach for consumer industry," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5411–5418, 2024.
- [5] P. Gope, O. Millwood, and B. Sikdar, "A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1971–1980, 2021.
- [6] S. Shihab and R. AlTawy, "Lightweight authentication scheme for healthcare with robustness to desynchronization attacks," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18 140–18 153, 2023.
- [7] M. R. Servati and M. Safkhani, "Eccbas: An ecc based authentication scheme for healthcare iot systems," *Pervasive and Mobile Computing*, vol. 90, p. 101753, 2023.
- [8] S. Das, S. Namasudra, S. Deb, P. M. Ger, and R. G. Crespo, "Securing iot-based smart healthcare systems by using advanced lightweight privacy-preserving authentication scheme," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18 486–18 494, 2023.
- [9] K. K. Saini, D. Kaur, D. Kumar, and B. Kumar, "An efficient three-factor authentication protocol for wireless healthcare sensor networks," *Multimedia Tools and Applications*, vol. 83, no. 23, pp. 63 699–63 721, 2024.
- [10] C.-M. Chen, Z. Chen, S. Kumari, M. S. Obaidat, J. J. P. C. Rodrigues, and M. K. Khan, "Blockchain-based mutual authentication protocol for iot-enabled decentralized healthcare environment," *IEEE Internet of Things Journal*, vol. 11, no. 14, pp. 25 394–25 412, 2024.
- [11] S. Yu, K. Park, and Y. Park, "A machine learning attack-resistant puf-based robust and efficient mutual authentication scheme in fog-enabled iot environments," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 20 652–20 669, 2025.
- [12] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [13] R. Canetti, A. Jain, and A. Scafuro, "Practical uc security with a global random oracle," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 597–608.
- [14] K. Mahmood, M. S. Obaidat, Z. Ghaffar, B. A. Alzahrani, S. Shamshad, M. A. Saleem, and S. Hussain, "Cloud-assisted secure and cost-effective authenticated solution for remote wearable health monitoring system," *IEEE transactions on network science and engineering*, vol. 10, no. 5, pp. 2710–2718, 2022.
- [15] M. F. Ayub, X. Li, K. Mahmood, M. J. F. Alenazi, A. K. Das, and G. Wang, "Provably secure efficient key-exchange protocol for intelligent supply line surveillance in smart grids," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 21 784–21 792, 2025.
- [16] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2776–2791, 2017.
- [17] M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty, "Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2697–2709, 2022.
- [18] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, 2024.
- [19] I. A. Kamil and S. O. Ogundoyin, "A lightweight mutual authentication and key agreement protocol for remote surgery application in tactile internet environment," *Computer Communications*, vol. 170, pp. 1–18, 2021.
- [20] M. A. Saleem, X. Li, K. Mahmood, Z. Ghaffar, Y. Xie, and G. Wang, "Provably secure authenticated key-management mechanism for e-healthcare environment," *IEEE Internet of Things Journal*, 2025.