


Please cite the Published Version

Ghaffar, Zahid, Kuo, Wen-Chung, Mahmood, Khalid, Tariq, Tayyaba, Bashir, Ali Kashif  and Omar, Marwan (2024) A Machine Learning Attack Resilient and Low-Latency Authentication Scheme for AI-Driven Patient Health Monitoring System. IEEE Communications Standards Magazine, 8 (3). pp. 36-42. ISSN 2471-2825

DOI: <https://doi.org/10.1109/mcomstd.0001.2300055>

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/635869/>

Usage rights:  In Copyright

Additional Information: © 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Enquiries:

If you have questions about this document, contact 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 and Low-Latency Authentication Scheme for AI-driven Patient Health Monitoring System

Zahid Ghaffar, Wen-Chung Kuo, Khalid Mahmood*, *Senior Member, IEEE*, Tayyaba Tariq, Ali Kashif Bashir, *Senior Member, IEEE*, Marwan Omar

Abstract—The Internet of Medical Things (IoMT) and Artificial Intelligence (AI) models have transformed healthcare by enabling wireless communication for Remote Patient Health Monitoring (RPHM) services. Wireless technologies such as Wi-Fi and 6G support reliable and low-latency communication between AI models and IoMT devices. IoMT devices allow individuals to monitor their health remotely, reducing the need for hospital visits. Integrating IoMT with AI and 6G enables automated diagnostics and personalized care with reduced data transmission among involved entities. It also helps data-intensive applications achieve higher performance levels regarding throughput, reliability, low latency, and energy-efficient communication for AI-driven RPHM system. However, exchanging sensitive information over public channels makes IoMT vulnerable to potential security attacks. Designing effective and secure mutual authentication and key agreement scheme for RPHM has been challenging due to privacy and security concerns. Moreover, there is also a demand for reliable and low-latency communication for AI-driven RPHM systems. Many existing authentication schemes have limitations, including susceptibility to machine learning attacks and high latency rates. To overcome these issues, we present a machine-learning attack-resilient and low-latency authentication scheme for AI-driven RPHM. The proposed scheme utilizes a three-factor approach based on elliptic curve cryptography (ECC). It employs a one-time physical unclonable function (OPUF) to resist machine learning attacks on medical sensing devices. The scheme's security is evaluated through informal and formal analysis, demonstrating its security strength and persistence. Additionally, the scheme's performance is assessed using various metrics, confirming its superiority over related schemes and achieving a low latency rate.

Index Terms—Authentication Scheme, Mutual Authentication, Authentication and Key Agreement, One-Time Physical Unclonable Function (OPUF), Machine learning

I. INTRODUCTION

With the rapid progress in miniature wearable biosensors and connected devices to the Internet, Remote Patient Health Monitoring (RPHM) has gained substantial attention for offering lower-cost and more effective delivery of remote healthcare services [1], [2]. The RPHM encompasses a wide range of Artificial Intelligence (AI) algorithms, including big data analytics, deep learning, and machine learning, to bridge the gap between conventional healthcare and on-time delivery of medical services. The AI-driven RPHM proactively monitors the patient's health status through various wearable biosensors, such as electrocardiograms, gyroscopes, photoplethysmograms, etc., to estimate potential healthcare issues through AI-driven algorithms and generate actionable insights before the condition escalates [3]. Such algorithms are adaptive in nature and improve their accuracy over time, leading to enhanced effectiveness in remote patient health monitoring.

The aid of AI in RPHM has significantly offloaded the burden on healthcare resources, lowering hospital emergency and readmission department visits. It has extended healthcare services to geographically remote areas and underserved populations. It is projected to have a significant economic impact of 3-6 trillion dollars annually, with AI-driven RPHM services contributing 1–2.5 trillion by 2025 [4]. The AI-driven RPHM leverages ML algorithms that facilitate powerful processing and storage support for biosensors beyond their limits to offer real-time decision-making. It also leads to automated diagnostics and personalized care and accomplishes ultra-reliable and low-latency communications among involved entities. However, the intrinsic importance of transmitting healthcare data over public channels (i.e., the Internet) accentuated its vulnerability to numerous security susceptibilities and risks. To this end, it is essential to concentrate on safeguarding the integrity and confidentiality of such sensitive data while offering robust security against well-known attacks simultaneously [5], [6].

Over the past few years, privacy-preserving authentication mechanisms have been considered as one of the concrete security solutions for any network scenario. Various researchers have presented valuable and innovative research in the domain of RPHM. However, most of the presented work

This work was supported in part by the National Science and Technology Council (NSTC), Taiwan, under Grant NSTC 111-2222-E-224-005-. The authors thank Dr. Khalid Mahmood at the National Yunlin University of Science and Technology for his valuable guidance and suggestions throughout this research work.

Zahid Ghaffar and Tayyaba Tariq are with the Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Douliu 64002, Taiwan. (e-mails: chzahid337@gmail.com, tayyaba.tariq.tt@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)

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, M15 6BH, UK. (e-mail: dr.alikashif.b@ieee.org)

Marwan Omar is with the Information Technology and Management, Illinois Institute of Technology, USA (e-mail: momar3@iit.edu)

Mohammed J.F. Alenazi is with the College of Computer and Information Sciences, Department of Computer Engineering, King Saud University, Riyadh, Saudi Arabia (email: mjalenazi@ksu.edu.sa)

(Corresponding Author*: Khalid Mahmood)

TABLE I: Comparative Analysis of Existing Work

Schemes	Year	Development Techniques	Benefits	Drawbacks/Flaws
Sharif et al. [7]	2019	* ECC * Hash Function	* Offers Mutual Authentication * Resists Desynchronization Attack	* Fails to resist Impersonation attack * Vulnerable to password guessing and secret key leakage attack
Li et al. [8]	2020	* ECC * Three Factor	* Provides Mutual authentication * Resists User Impersonation attack	* Violates user anonymity * Prone to sensor impersonation attack
Wang et al. [9]	2021	* PUF * Block-chain	* Resists Impersonation Attack * Ensures Perfect Forward Secrecy * Resists Stolen Mobile device attack	* Vulnerable to machine learning attack * Susceptible to a Man-in-the-Middle attack * Prone to Session key Disclosure attack
Li et al. [4]	2021	* Hash Function * XoR Operation	* Resists server impersonation * Resists offline password guessing attack * Resists stolen smart card attacks	* Vulnerable to sensor masquerading attack * Prone to Stolen verifier attack * Vulnerable to Desynchronization attack * Susceptible or machine learning or modeling attack
Masud et al. [10]	2021	* Hash Function	* Resists gateway impersonation * Resists Replay attack * Provides Mutual Authentication	* Susceptible to offline password guessing attack * Violates User Anonymity * Susceptible to User Masquerading and privileged insider attack
Yu et al. [11]	2022	* PUF * Blockchain	* Resists Man-in-the middle attack * Resists offline password guessing attack	* Vulnerable to sensor impersonation attack * Prone to Stolen verifier attack * Vulnerable to Machine Learning or modeling attack * Susceptible to ESL Attack
Shihab et al. [12]	2023	* Hash Function	* Resists Desynchronization attack * Resists Replay attack * Resists stolen device attacks	* Vulnerable to Physical capturing attack * Prone to User masquerading attack * Vulnerable to Stolen verifier attack * Susceptible or machine learning or modeling attack

either suffers from computational inadequacies or is exposed to known security threats [13]. In Table I, we summarize the struggles encountered by researchers in related studies, along with their cryptographic techniques, advantages, and disadvantages. These schemes aim to tackle security challenges related to communication among participating entities. They employ various techniques like hash functions, elliptic curve cryptography, chaotic maps, and physical uncloneable functions (PUF) to achieve authentication, conditional privacy, message security, and confidentiality. However, most of these schemes exhibit weaknesses, such as susceptibility to machine learning or modeling attacks and the requirement of a trusted authority for authentication, which may increase the risk of insider attacks and make them vulnerable to physical attacks. Furthermore, these weaknesses enable attackers to tamper with mobile sensing devices, thus compromising user safety and privacy.

A. Motivation and Contributions

In a remote patient health monitoring environment, entities like Medical Gateway (MGW_c), Medical Sensor (S_j), and User (U_i) exchange real-time data over public channels, posing security risks including machine learning attacks. There are several schemes that have been developed to ensure secure communication among these entities. However, these schemes are prone to several attacks, as mentioned in Table I. This article aims to address these issues by proposing a privacy-preserving and anonymous authentication scheme. The devised scheme utilizes $\mathbb{O}PUF$ and ECC . The $\mathbb{O}PUF$ ensures resistance to unauthorized access by changing the scheme's behavior after each session. The proposed scheme safeguards the remote patient health monitoring environment, defending against physical attacks, man-in-the-middle attacks, masquerading, denial of service, and machine learning attacks. The following points highlight the notable contributions of the proposed scheme.

- 1) We introduce an ECC -based authentication scheme enhancing data privacy and anonymity between medical devices and servers. This approach bolsters communication trustworthiness and propels advancements in AI-driven RPHM privacy-preserving technologies.

- 2) The proposed scheme leverages $\mathbb{O}PUF$ to defend physical, modelling, and machine learning attacks by taking advantage of their random nature. Moreover, the dynamic design of our scheme ensures that its operational behavior is unique to each session, effectively introducing an additional layer of security.
- 3) We thoroughly examine the devised scheme's security through informal and formal analysis, showcasing its correctness, effectiveness, and resilience against potential threats.
- 4) We analyze the performance of the devised scheme, comparing it to existing approaches. The evaluation highlights the superior security features of the suggested scheme, including computation and communication overheads. The proposed scheme promises an average 34.75% reduction in computation overhead.

B. Road map of Article

The rest of this article is organized as follows: Section II presents preliminaries used to develop the scheme, Section III presents the proposed access control scheme, Section IV demonstrates its security, and Section V evaluates its performance. Finally, we conclude this article in Section VI.

II. PRELIMINARIES

This section describes the research methodology, architecture, and adversarial model. Assumptions in the adversarial model define adversary capabilities and limitations. This overview establishes the groundwork for a clear comprehension of the following sections.

A. Research Methodology

The research methodology in designing the authentication scheme for the AI-driven RPHM network model is structured with several significant presuppositions to shape a theoretical approach. This involves defining a network model to identify the communicants in the target environment while understanding their relationship in a broader sense, which is how the study unfolds. Then, we assessed the potential security

risks against well-known security attack modules, including scenarios like impersonation, privileged insider, and sensor node capture attacks. Considering these security risks, selecting countermeasures (i.e., the design of the authentication scheme), ranging from cryptographic methods to biometrics, adds a layer of security. We present a detailed discussion of our proposed solution outlining its key phases of the scheme, including setup and the registration process, contributing to a comprehensive and structured approach. We then provide an insight into the security strength of our solution by employing rigorous formal and informal analysis. Additionally, the scheme's performance is assessed using various metrics that enhance clarity and underscore the scheme's effectiveness and reliability within the IoT context.

B. Architecture for Remote Patient Health Monitoring System

The remote patient healthcare model proposed in this article consists of three key components: S_j , U_i , and the MGW_c . These components are illustrated in Fig. 1.

- 1) Medical Sensor: In a given deployed environment, various sensors are placed on patients' bodies. These sensors have a function to collect and sense data continuously and transmit the collected data to the MGW_c . To ensure secure communication among users, the S_j registers with MGW_c , which generates a session key (SK).
- 2) User: To collect the data sensed by the sensor node, they must be registered by MGW_c and receive a smart card to use for authentication with the sensor node. The medical terminal serves as a means of authentication by verifying the smart card and grants access to medical data.
- 3) Medical Gateway: MGW_c plays a critical role in the remote patient health monitoring network, as it is a trusted party that possesses the actual identities of both the S_j and the U_i . MGW_c is responsible for facilitating mutual authentication between S_j and U_i . The sensor node and U_i then register with MGW_c to obtain their secret information before negotiating a session key. This session key encrypts data collected by the sensor node, which is then transmitted to the MGW_c and made accessible to the U_i via the medical terminal. Fig. 1 depicts a remote patient health monitoring system.

C. Adversary model

This section explains the adversary's capabilities as defined in the DY [14] and CK [15] adversarial model. Within this model, an adversary (A_d) possesses significant control over communication carried out via the public channel. The adversary model encompasses two distinct types of adversaries: passive and active. We will now delve into a detailed discussion of each type.

- 1) A passive A_d is capable of monitoring the communication channel among MGW_c , S_j , and U_i in an attempt to acquire the messages exchanged. This type of A_d can launch various attacks, such as offline password-guessing, man-in-the-middle, denial-of-service attacks, and temporary information attacks.

- 2) An active A_d can manipulate the exchanged messages, including forging, deleting, and modifying them, to obtain the secret information and identity of the parties involved. This type of adversary can launch various attacks, including reply, impersonation, stolen smart card, modification, MGW_c bypassing, sensor node capture, and insider attacks.

III. THE PROPOSED SCHEME

The present section aims to construct an access control scheme for AI-driven remote patient health monitoring, leveraging the security offered by ECC and OPUF to establish resilience against diverse forms of known attacks. Our proposed scheme's registration and authentication phases are expounded in subsequent subsections.

A. Registration Phase

The registration phase involves a prescribed set of procedures wherein each U_i validate their legitimacy and authorization. The U_i inserts his credentials, generating a random value and a corresponding hash. This U_i -provided information is then transmitted to the MGW_c . On getting the message, the MGW_c , acting as the trusted authority, executes computations, selects a unique string, and sends the computed values back to the U_i . Subsequently, the U_i performs additional computations and stores the resulting information in memory. Simultaneously, the MGW_c manages the registration of S_j within the AI-drive remote patient health monitoring system. Sensors, undergo secure registration under the medical gateway's supervision, utilizing private communication channels. Each sensor is assigned a unique identity; MGW_c generates challenge-response pairs and computes using a specific process involving the sensor's identity and a master secret key. The resulting information is retained by the MGW_c for each pseudo-identity, thereby completing the secure registration process. This integrated approach ensures both the secure validation of U_i and the registration of S_j in the AI-drive remote patient health monitoring system.

B. Authentication and Key Agreement Phase

The login and authentication phase involving U_i , S_j and MGW_c that communicates over an open or insecure channel. The goal is to establish a session key among three entities. Initially, U_i inputs his secret credentials, determines additional values, generates a login request message, and transmits it to MGW_c via the insecure channel. Upon receiving the login request message, MGW_c performs computations and retrieves information associated with the specific sensor, crafting a response message sent to S_j . Moreover, S_j processes the response message, determining the challenge-response pair and other values. S_j then generates a message and transmits back to MGW_c . Subsequently, MGW_c computes various parameters and sends a response message to the U_i . Finally, U_i processes information from the received message and verifies the authenticity, ultimately establishing the shared session key among all entities. This process ensures secure authentication within the AI-drive remote patient health monitoring system.

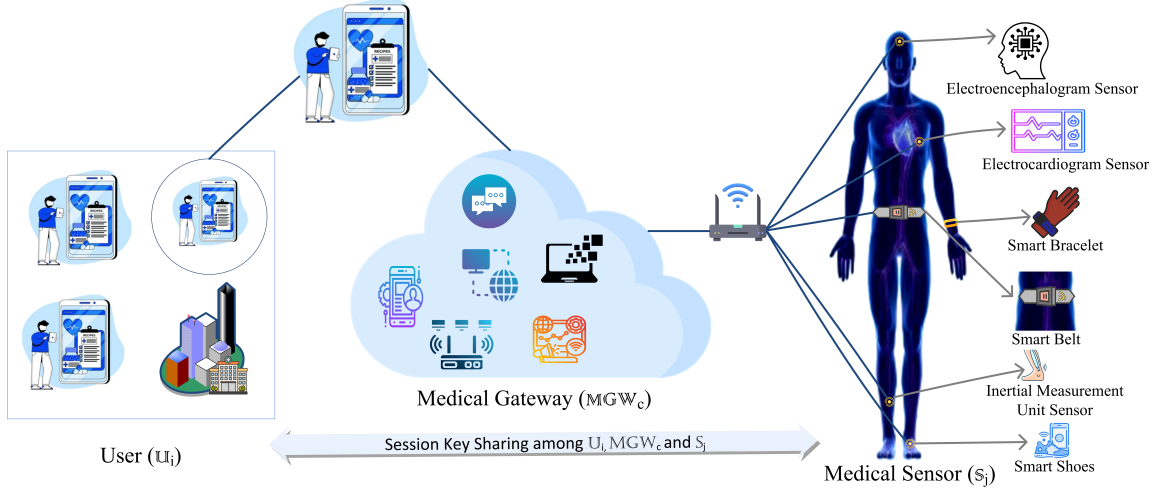


Fig. 1: AI-drive Remote Patient-health Monitoring System

IV. SECURITY EVALUATION

This section presents a comprehensive security analysis of the devised authentication scheme, utilizing the informal security evaluation is also employed to demonstrate that the suggested scheme is secure against all potential security attacks.

A. Informal Security Evaluation

The proposed authentication scheme has undergone a thorough informal analysis, and its significance lies in its ability to resist various attacks. This analysis revealed that the suggested scheme protects S_j , U_i , and MGW_c from unauthorized access to A_d . Additionally, the scheme incorporates various authentication measures to accomplish the intended goal of resisting diverse attacks.

1) *Mutual Authentication*: In the devised scheme, MGW_c legitimizes U_i by checking the legitimacy of values with the help of equality comparison. Similarly, U_i confirms MGW_c authenticity by comparing a set of values. Additionally, MGW_c authenticates the S_j using a similar method of comparing specific values against a combination of session key and unique identifiers. These verification processes ensure that each party is legitimate and authenticated. It is to be eminent that U_i , MGW_c and S_j will only negotiate and accept the session key if these authentication checks hold true. Consequently, the proposed scheme offers robust mutual authentication among involved entities.

2) *Device Tampering Attack Resistance*: Let us take the scenario where an A_d attempts to manipulate S_j using modeling or machine learning-based attacks to compromise its integrity. However, such repeated tampering attempts by A_d result in a sudden and noticeable alteration in the behavior of the embedded $OPUF$ within S_j . Consequently, the $OPUF$ ceases to provide its intended functionality, leading to a failure in generating the desired output during the execution attempt by A_d . Hence, any endeavors by A_d to tamper with or compromise S_j can be readily detected by the monitoring entity MGW_c . Furthermore, due to the inherent resistance

to cloning and replicating the $OPUF$, the proposed scheme effectively resists physical attacks based on machine learning techniques.

3) *Masquerading Attacks Resistance*: A masquerading attack refers to the deceptive actions undertaken by an A_d who assumes the identity of an authorized U_i within a registered system. The primary objective behind such fraudulent behavior is to illicitly acquire access to confidential data or engage in harmful actions. The proposed scheme exhibits robustness against various impersonation attacks, which are elucidated as follows.

- *U_i Masquerading Attack Resistance*: Let's assume that A_d attempts to develop publicly transmitted values to impersonate a legitimate U_i within our scheme. The calculation of these values necessitates knowledge of U_i 's confidential credentials. Consequently, A_d will be unable to produce valid messages as it requires the original identity and pseudo-identity of U_i . As a result, our scheme exhibits resilience against masquerading attacks from unauthorized U_i .
- *MGW_c Masquerading Attack Resistance*: Let us consider a scenario where an A_d intercepts the challenge message that is originally intended for the legitimate S_j and initiated by MGW_c . The objective of A_d is to impersonate the genuine MGW_c . To determine a valid challenge message, A_d needs to compute the valid values. However, the computation of those values requires pseudo-identity, which further includes the private key of MGW_c . As A_d does not possess the private key, they are unable to determine pseudo-identity. Consequently, A_d will not be able to develop a valid message on behalf of MGW_c . Therefore, the devised scheme ensures security against masquerading attacks targeting MGW_c .
- *S_j Masquerading Attack Resistance*: In our suggested scheme, if A_d tries to send a valid challenge message on behalf of legal S_j , A_d must calculate the legitimate value correctly. So, for the computation of that specific value, A_d must have the private key. A_d cannot get MGW_c 's private key. Therefore, our proposed scheme

ensures that it provides resilience against sensing device impersonation attacks.

4) *Session Key Leakage Attack*: Our scheme utilizes a session key SK that relies on confidential values. These values are not transmitted publicly, and the hash function applied after concatenation prevents the determination or guessing of the actual values. As a result, our scheme demonstrates robustness against session-key attacks.

5) *Ephemeral Secret Leakage (ESL) Attack*: Our framework combines long-term pseudo-identity and confidential ephemeral secrets to ensure the confidentiality of the session key. These secrets remain undisclosed and inviolable, preventing adversaries from deducing the session key. Even if the session key is compromised, the integrity of previously generated keys remains intact, maintaining perfect forward secrecy. Consequently, our scheme upholds the property of perfect forward secrecy.

6) *Resistance Against Machine Learning Attacks*: Conventionally, the PUF uses a static set of CRPs to verify the legitimacy of S_j . An A_d can easily predict the possible outcome (i.e., response) of PUF through ML or modeling attacks. However, in our scheme, we exploit OPUF , which uses a dynamic set of CRPS for each session of the authentication round. It is worth noticing that after the successful completion of each authentication round, OPUF updates its state and resets its configuration [16]. Therefore, the outcome of OPUF after reconfiguration is difficult to revert and uncontrollable through invasive methods. At the same time, the change in the configuration of PUF does not affect its security properties. To this end, OPUF preserves the backward and forward unpredictability of PUF outcomes. Hence, it becomes difficult for an A_d to predict the possible outcome of PUF performing any ML or modeling attacks.

7) *Provides Perfect Forward and Backward Secrecy*: In the devised scheme, the symmetric session key is derived with the combination of pseudo-identity and ephemeral secrets, which are selected by S_j and U_i . In this session key, ephemeral secrets are specific for each session. Even if the long-term secrets of U_i , MGW_c and S_j are exposed, it is infeasible for A_d to recover the previous and future SK since A_d resolves the intractable elliptic curve discrete logarithmic problem to obtain aP and cP. So, it is impossible to determine the previous and future SK . Therefore, the devised scheme offers perfect forward and backward secrecy.

V. COMPARATIVE EVALUATION

In this section, we present a detailed comparative analysis of our access control scheme along with other relevant schemes [4], [8], [11], [12]. Our analysis specifically focuses on evaluating these schemes' security functionalities, communication, and computation costs.

A. Implementation Setup

The proposed and related schemes comprise three entities, including MGW_c , S_j , and U_i . To get the experimental results, we implemented the key cryptographic operations of U_i , S_j and MGW_c , on mobile device, Arduino, and desktop system,

respectively. The specifications of these devices are as follows: The operating system used for desktop and mobile devices is Windows 11 Home and Android 12, respectively. The RAM utilized at Arduino, desktop, and mobile devices is SRAM:4KB, 8GB, and 12 GB, respectively. The processor utilized by Arduino, desktop, and mobile devices is Microcontroller: ATmega328, Intel(R) Core(TM) i7-1065G7, and Octacore, respectively. Moreover, we used Bouncy Castle [17] and PyCryptodome [18] libraries while implementing our code on mobile and desktop devices, respectively. Table II represents the execution times of cryptographic operations, including point multiplication (T_{ecpm}), one-way hash function (T_{owh}), and PUF (T_{PUF}) on their respective devices.

TABLE II: Execution Time of Cryptographic Operations

Operations	Execution Time (in milliseconds)		
	Arduino Device	Desktop System	Mobile Device
T_{ecpm}	0.013623	0.012535	0.008020
T_{owh}	0.015802	0.002746	0.004001
T_{PUF}	0.000280	N/A	N/A

B. Computational Cost Analysis

We have evaluated the computational overhead by utilizing the cryptographic functions such as T_{owh} (Execution time for one-way hash function), T_{pm} (Execution time for point multiplication), T_{OPUF} (Execution time for OPUF). We determined the computational overhead at U_i , MGW_c , and S_j . Excluding the registration process, which is a one-time event in our scheme, we focused solely on the computational overhead of the login and authentication phase.

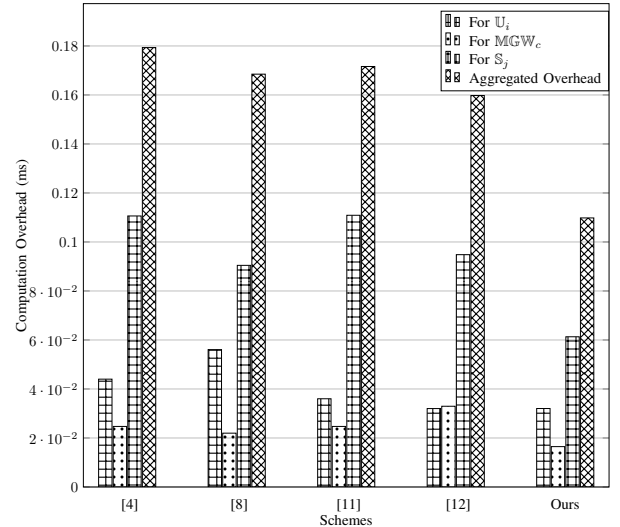


Fig. 2: Computation Overhead Comparison

In the devised scheme, S_j executes the following operations: $1T_{PUF} + 3T_{owh}$. So, the computation overhead at the S_j side is approximately 0.061309 ms. The cryptographic operation executed at the MGW_c side is $6T_{owh}$, and the computational overhead at MGW_c is approximately 0.016476 ms. Similarly, operations executed at U_i are $1T_{ecpm} + 6T_{owh}$, and the total computational overhead at U_i is approximately 0.032026 ms.

Therefore, the approximate computation overhead of the proposed scheme is 0.109811 ms. We utilize the same approach to determine the computation overhead of the other schemes in comparison. We show the detailed comparison of computation overhead among proposed and related schemes in Fig. 2.

C. Communication Overhead

In this section, we compare the communication cost of our scheme with those of existing schemes. As the registration phase is a one-time process, we solely focus on the communication overhead during the key agreement phase. To assess the communication overhead, we assume that the nonce, identity, password, and XOR operation each consist of 160 bits. Furthermore, the hash operation (SHA-256) produces a 256-bit output, and the size of the elliptic curve point is 320 bits.

In the devised scheme, the entities U_i , MGW_c and S_j transmits four messages. U_i sends first message (W_1) to MGW_c and exchanges 1088 bits. MGW_c sends W_2 to S_j , and exchanges 832 bits. After that, S_j sends W_3 to MGW_c and exchanges 576 bits. Similarly, MGW_c sends W_4 to U_i , requiring the exchange of 576 bits. As a result, the devised scheme has an overall communication overhead of $(1088+832+576+576)=3072$ bits. We calculated the communication overhead of other relevant schemes using a similar method, and the results are presented in Fig. 3.

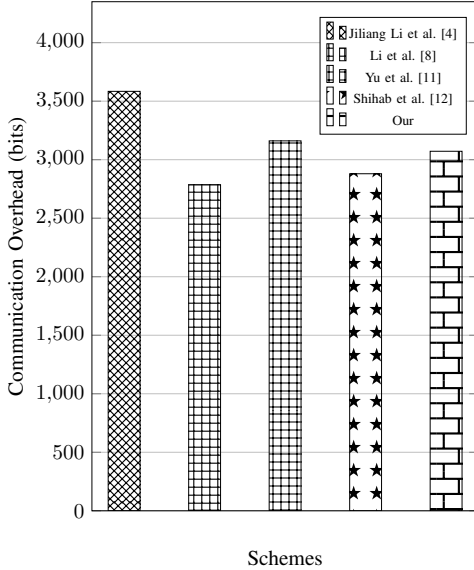


Fig. 3: Communication Overhead Comparison

D. Security Features Evaluation

Our proposed scheme outperforms similar schemes [4], [8], [11], [12] regarding security. The analysis in Table III shows that our scheme guarantees all security features while effectively resisting attacks like device impersonation, untraceability attacks, and machine learning attacks. Additionally, our scheme offers additional security features, such as resilience to machine learning and desynchronization attacks.

TABLE III: Comparison on Security features

Schemes	IA_1	IA_2	IA_3	IA_4	IA_5	IA_6	IA_7	IA_8
Li et al. [4]	●	○	●	●	○	●	○	○
Li et al. [8]	●	○	●	●	●	●	●	N/A
Yu et al. [11]	●	○	●	●	○	○	●	○
Shihab et al. [12]	○	●	○	●	○	●	●	○
Proposed	●	●	●	●	○	●	●	●
IA_1 : Physical Capturing Attack; IA_2 : S_j impersonation Attack; IA_3 : U_i impersonation Attack;								
IA_4 : MGW_c Impersonation Attack; IA_5 : Stolen Verifier attack; IA_6 : ESL Attack;								
IA_7 : Desynchronization attack; IA_8 : Machine learning or modeling attack;								
●: Resists; ○: Does not Resists; N/A: Not Applicable								

The presented results demonstrate that our scheme is superior to comparative schemes regarding computation overhead and security features. It outperforms other schemes and offers additional security characteristics that distinguish it from previous works. Although our scheme has slightly higher communication costs compared to [8], [12], the extensive security justifies the trade-off features it provides. These enhancements make our scheme more comprehensive and secure, making the minor increase in communication costs an acceptable trade-off for improved security.

VI. CONCLUSION

The evolution in IoMT infrastructure, artificial intelligence, 6G, and wearable technology has led to remote patient health monitoring in the e-health environment. Developing these large-scale AI-enabled RPHM models necessitates robust support from computing, communication, and networks to ensure low latency, efficiency, stability, and reliability, especially in resource-contained environments. Physical unclonable functions are favoured for hardware-based security in mobile sensing devices with limited resources. However, PUF-based security faces challenges from machine learning attacks. Existing key agreement schemes are unsuitable for remote patient-health monitoring. This article presents a reliable authentication scheme using elliptic curve cryptography, leveraging one-time PUFs to ensure robust security against machine learning attacks. Extensive security analysis demonstrates resilience against various potential attacks. The proposed scheme has lower computation costs than related schemes, offering a promising remote patient health monitoring solution. Despite all of these advantages, it's crucial to acknowledge the limitations of our current proposed scheme, that it is not enough secure to resist all post-quantum attacks, which is a growing concern in this field. Therefore, we are committed to addressing this limitation and ensuring the long-term security of our system. In our future work, we plan to focus on the development of a robust lattice-based authentication scheme that can withstand post-quantum attacks, thereby fortifying the security of patient's critical information.

REFERENCES

- [1] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "Ai-driven data monetization: The other face of data in iot-based smart and connected health," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5581–5599, 2020.
- [2] M. Zia, M. S. Obaidat, K. Mahmood, S. Shamshad, M. A. Saleem, and S. A. Chaudhry, "A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1683–1690, 2022.

- [3] G. M. Dogheim and A. Hussain, "Patient care through ai-driven remote monitoring: Analyzing the role of predictive models and intelligent alerts in preventive medicine," *Journal of Contemporary Healthcare Analytics*, vol. 7, no. 1, pp. 94–110, 2023.
- [4] J. Li, Z. Su, D. Guo, K.-K. R. Choo, and Y. Ji, "Psi-maaka: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13 183–13 195, 2021.
- [5] K. Mahmood, M. 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*, 2022.
- [6] S. Shamshad, M. F. Ayub, K. Mahmood, S. Kumari, S. A. Chaudhry, and C.-M. Chen, "An enhanced scheme for mutual authentication for healthcare services," *Digital Communications and Networks*, vol. 8, no. 2, pp. 150–161, 2022.
- [7] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ecc-based mutual authentication and session key generation scheme for healthcare applications," *Journal of medical systems*, vol. 43, no. 1, p. 10, 2019.
- [8] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2019.
- [9] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, 2021.
- [10] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for iot-based healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2021.
- [11] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20 214–20 228, 2022.
- [12] S. Shihab and R. AlTawy, "Lightweight authentication scheme for healthcare with robustness to desynchronization attacks," *IEEE Internet of Things Journal*, 2023.
- [13] M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar, and K. Mahmood, "Security analysis on "a secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems"," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5557–5559, 2021.
- [14] 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.
- [15] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2001, pp. 453–474.
- [16] 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.
- [17] L. of the Bouncy Castle, "Bouncy castle crypto library," 2000. [Online]. Available: <https://www.bouncycastle.org/>
- [18] S. Legrandin, "Pycryptodome: A self-contained python package of low-level cryptographic primitives," 2013. [Online]. Available: <https://www.pycryptodome.org/>