International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secure, Lightweight, and Anonymous Authentication Scheme for Healthcare IoT

Jaydeep Gheewala*[1], Pariza Kamboj[2]

Submitted:25/05/2024 **Accepted:**01/07/2024 **Published:**09/07/2024

Abstract: Continuously monitoring patients and offering remote healthcare services can be supported by the H-IoT, which comprises body sensor networks (BSNs), wearable devices, gateways, and healthcare servers. While H-IoT significantly improves the efficiency and availability of health services, it also brings critical security and privacy problems such as transmitting sensitive medical information through public networks and resource-constrained devices the deployment environment of medical sensors which can be physically compromised [10], [13], [17]. In particular, a difficult issue of research is the design techniques that can construct authentication and key agreement mechanisms, which at the same time need to be lightweight, keep patient anonymity information and withstand physical capture attacks.

Lightweight authentication schemes of the existing literature using symmetric key cryptography and hash functionin'gs yield low computational complexity but, in general do not ensure strong anonymity and protection against physical attacks [2],[6], [14]. On the other hand, PUFbased solutions enhance hardware-level security but are often restricted by additional communication overhead or donot have a complete formal security proof [3]–[5], [21], [22]. Furthermore, a number of recent works demonstrate that many healthcare-based authentication protocols are based on informal security arguments and do not inspire confidence that they are secure against a computationally-strong adversary [17], [25].

In order to meet these challenges, this paper presents a lightweight, secure and privacy-preserving authentication and key agreement scheme designed for Healthcare IoT settings. The introduced scheme combines the light-weight cryptographic primitives with hardware-backed secret identity for achieving mutual authentication, patient privacy as well as resistance against replay, impersonation, man-in-the-middle and lost token attacks. The security of the scheme is formally verified by BAN logic [15] and AVISPA tool [16], demonstrating the correctness of authentication and security of session keys. Furthermore, performance comparison indicates that the proposed protocol is more computationally and communication efficient than existing healthcare IoT authentication designs [1], [5], [19] and can be deployed on the resource-constrained medical equipment.

Keywords: *Healthcare Internet of Things; Lightweight authentication; Mutual authentication; Key agreement; Patient anonymity; Physical Unclonable Function (PUF); Body sensor networks; Formal security verification; BAN logic; AVISPA*

1. Introduction

As an enabler of the H-IoT, H et al internet of medical things (HIMoT) has been developed to enable body sensor networks based on wireless technologies and which integrate body sensor networks with wearable medical appliances, gateways (e.g., moving miniature servers), edge cloud server, and core cloud healthcare servers in order to monitor patients continuously for the home-based health-care service [10], [13]. Assuming the in-line acquisition and real-time transmission of physiological parameters, including heart rate, blood pressure, glucose level and electrocardiogram (ECG) signals, H-IoT systems will make great contributions to healthcare efficiency, accessibility and quality of nursing. However, the provisioning of H-IoT systems also poses severe security and privacy threats as it involves the exchange of extremely sensitive medical data over insecure wireless mediums and resource-limited medical sensor devices being physically exposed [17], [25].

Authentication is a basic security need for H-IoT systems since unauthorized access to medical devices or patient’s information could lead to privacy violations, wrong clinical decision-making and even loss of life [17], [25]. Traditional authentication and key management schemes, especially public-key cryptosystems-based ones, are not applicable to H-IoT systems, because medical sensor nodes and wearable devices are low computational power, memory and energy resources [2], [6]. As a result, lightweight authentication and key agreement protocols are identified as the main research bottleneck for healthcare-oriented IoT applications.

In order to overcome efficiency barriers, several lightweight authentication schemes using symmetric cryptosystem and hash function are proposed for IoT [2], [6] and healthcare [14]. While those techniques minimized computational and communication

1 Sarvajanik College of Eng. & Tech, Comp. Eng. Dept.

ORCID ID : 0000-0002-3508-983X

2 Sarvajanik College of Eng. & Tech, Comp. Eng. Dept.

ORCID ID : 0000-0001-5936-2047

** Corresponding Author Email: author@email.com*

cost for the servers, they were not able to provide important security properties such as patient anonymity, untracability and being secure against impersonation, replay and stolen device attacks [9], [10]. These limitations are particularly challenging in health-care settings, where devices are used in unshielded hostile environments and patient privacy needs to be carefully considered [25].

To achieve better performance of resistance against physical capture and device cloning attacks, PUF-based authentication schemes have attracted more attention [3]–[5], [21], [22]. PUFs leverage hardware device variability inherent in manufacturing to provide unique and unclonable responses which are not required to be stored as long-term secret keys within the device on-chip memory. PUF-based protocols enhance security and anonymity at hardware level, yet none of the current schemes take into consideration communication overhead, scalability, dynamic enrollment or formal security proofs [5], [22], [23].

It is essential to have a fine grained security analysis of authentication protocols tailored to the hostile environment. Systematic approaches such as BAN logic [15] and tools such as AVISPA [16] are usually employed in order to guarantee authentication correctness and privacy of session keys under the Dolev–Yao threat model. However, the majority of the authentication protocols in healthcare are either based on informal security arguments or have not been proved completely and this results on curtailing confidence in their capability to face well-articulated attacks [17], [25].

To counter these problems, in this paper, an efficient secure and privacy-preserving authentication and key agreement protocol for Healthcare IoT environments is presented. The proposed approach integrates light-weight cryptographic primitives with hardware-enabled identity protection to achieve mutual authentication, patient privacy and security against existing and emerging threats by a dual-layered defense mechanism suitable for real-world based resource-constrained medical devices. The formal security validation with BAN logic and AVISPA tool, the performance analysis confirm that our protocol achieves a trade-off between security and efficiency which is very suitable for practical H-IoT scenarios.

2. Related Work

In the context of IoT and healthcare environments, secure lightweight authentication has been an active research topic owing to scarce resource availability and sensitive nature of medical data [17], [25]. In the beginning, centralized or gateway-assisted authentication mechanisms were widely deployed on Healthcare IoT systems, where gateways act as mediators between sensor nodes and healthcare servers [10], [13]. While these approaches implement rudimentary mutual authentication, they commonly assume a trusted gateway and provide only simple measures to secure PHR identity, privacy as well as physical compromise for the patient and are rarely practicable in real-world healthcare situations.

For the sake of efficiency, many lightweight authentication protocols based on symmetric cryptography and hash functions have been proposed for IoT and smart environments [2], [6], [14]. These procedures reduce significantly computational and communication overheads, thereby, are suitable for low power devices. However, most of these are not designed for health services and provide limited protection against impersonation, replay, and stolen-device threats [9]. Furthermore, considerations of anonymity and untraceability are usually insufficiently discussed which is not satisfying in healthcare settings dealing with sensitive medical information [26].

Lightweight authentication protocols have also been proposed for smart grid and industrial IoT settings showing that they are scalable and efficient [1], [7], [11], [12]. Although these techniques are informative in terms of lightweight security design, their threat models and application scenarios are quite different from Healthcare IoT systems. In particular, the healthcare environment requires stronger privacy (our proposed solution does not compromise with user privacy; while majority of the aforementioned schemes do) followed by remaining two strict requirements related to mobility and security aspects making these schemes not directly applicable for H-IoT environments.

PUF-based authentication schemes are proposed for physical attack resistance and device cloning in [3]–[5], [21], [22]. PUF-based protocols leverage the intrinsic characteristics of hardware itself, thus an adversary is unable to capture long-term secret keys and mount a physical clone attack. Some systems even enhance privacy by adopting dynamic identities [5]. Nevertheless, the communication overhead is added for SENs based on PUFs: for use of some Geological formation data collection control or enrollment issues are introduced [22], [23] and dynamic device and user addition cannot be supported, which limits scalability in large-scale health care systems.

The formal treatment of security has become crucial for the verification of authentication protocols against adversaries. Logic BAN provides a logical setting for the analysis of authentication goals and belief consistency [15], while automated tools such as AVISPA can support the automation of systematic analysis under the Dolev–Yao model [16]. Even though, few healthcare based authentication protocols utilize complete formal proof. Most of the existing schemes are dependent on informal security argument and the potential vulnerabilities are not explored well enough [17], [25].

Recent survey works all demonstrate that existing Authentication mechanisms for Healthcare IoT solutions generally trade compactness or lightweight, with resilience or security assurance but rarely both [17], [25], [26]. Lightweight cryptographic solutions offer efficiency, but are vulnerable to physical attacks and privacy threats, and PUF-based designs improve the security at hardware stages with less cost but require higher complexity or without adequate formal verification proof. These results indicate that no single solution performs lightweight, anonymous, resistant to physical capture attacks and scalable authentication in Lua-Dir can be found under the formal security proof.

In fact, current authentication protocols in the case of Healthcare IoT systems exhibit clear trade-offs among efficiency, security, privacy and validation strength. This gap is what motivates the design of an authentication and key agreement protocol for healthcare, that meets a compromise between its lightweight

Table 1. Comparative Analysis of Existing Authentication Schemes**

Scheme	Domain	Lightweight	Anonymity	PUF-Based	Physical Attack Resistance	Formal Verification
Zhao *et al.* [1]	Smart Grid	✓	✗	✗	✗	✗
Reddy & Rao [2]	General IoT	✓	✗	✗	✗	✗
Zhuang & Li [3]	IoT	✓	✓	✓	✓	✗
Gupta & Varshney [4]	IoT	✓	✓	✓	✓	✗
Cui *et al.* [5]	Edge IoT	✓	✓	✓	✓	Partial
Oh *et al.* [6]	Smart Home	✓	✗	✗	✗	✗
Gope *et al.* [7]	Industrial WSN	✓	✓	✗	Partial	✗
Lara *et al.* [8]	Industrial IoT	✓	✗	✗	✗	✗
Trivedi & Patel [9]	IoT	✓	✗	✗	✗	✗
Yeh [10]	Healthcare IoT	Partial	✗	✗	✗	✗
Garg *et al.* [11]	Smart Grid	✓	Partial	✗	✗	✗
Kumar *et al.* [12]	Smart Energy	✓	Partial	✗	✗	✗
Moosavi *et al.* [13]	Healthcare IoT	Partial	✗	✗	✗	✗
Gaba *et al.* [14]	Smart Env.	✓	✗	✗	✗	✗
Jan *et al.* [21]	Healthcare IoT	✓	✓	Partial	Partial	✗
Jan *et al.* [22]	IoT	✓	✓	✓	✓	✗
Braeken *et al.* [23]	IoT	✓	✓	✓	✓	✗
Proposed Scheme	**Healthcare IoT**	✓	✓	✓	✓	**✓ (BAN + AVISPA)**

performance feature with the strength of privacy protection, and resistance against physical attacks to formal security verification as defined in this paper.

3. Comparative Analysis of Existing Authentication Schemes

This section provides a comparative study of important lightweight and PUF-based authentication protocols in the context of Healthcare IoT. The emphasis is placed on the aforementioned security aspects, efficiency, privacy support, resistance to physical attacks, and formal verification for proper H-IoT deployment [17], [25].

Lightweight authentication protocols based on symmetric key cryptography and hash functions are proposed to reduce the computational cost, which are suitable for resource-constrained devices [2], [6], [14]. Nevertheless, most of these solutions do not account for patient's anonymity and untraceability or provide defence against physical capture attacks (i.e. secret credentials are usually stored at the device memory [9], [10]). These limitations make them less suitable for medical context with personal medical data and physical access to the devices.

PUF-based authentication themed protocols strengthen clone and physical attack resistance with the elimination of stored long-term secrets and deployment of unique device identities at run time [3]–[5], [21], [22]. Some protocols [5] also enhance privacy by using dynamic identities and challenge–response mechanisms. However, many PUF-based methods either lead to higher communication overhead, do not scale well or cannot be extended dynamically by adding users or devices which marginalizes their application on wide-area healthcare systems [22], [23].

Formal security proofs are another point of contrast of our scheme with previous ones. Though BAN logic and AVISPA have been proven effective for verifying the correctness of authentication and secrecy of session key [15], [16], there are few formal verifications for healthcare authenticated protocols. Many existing schemes rely primarily on informal security arguments, leaving potential vulnerabilities insufficiently explored [17], [25].

Table I summarizes the comparative evaluation of representative schemes against key security and performance criteria relevant to Healthcare IoT systems. As observed, no single existing scheme simultaneously satisfies lightweight computation, strong privacy protection, physical attack resistance, formal verification, and healthcare-specific applicability. These limitations motivate the design of the proposed authentication and key agreement protocol, which aims to achieve a balanced trade-off among security, privacy, and efficiency.

4. System Model and Threat Model

4.1 System Model

The authentication and key agreement protocol proposed is tailored for a standard Healthcare Internet of Things (H-IoT) setting, comprising the following components (Fig. 1):

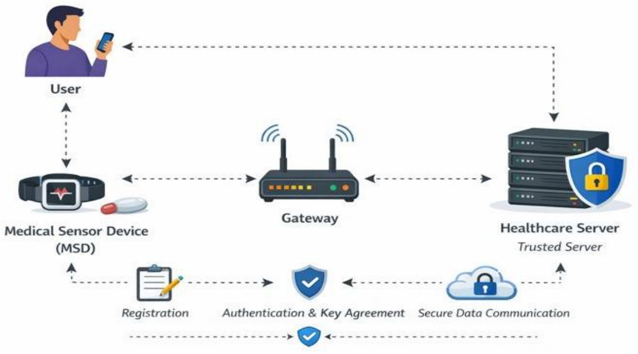
User
Medical Sensor Device (MSD)
Gateway
Healthcare Server
Trusted Server
Registration
Authentication & Key Agreement
Secure Data Communication

Fig 1. System Model

1. Medical Sensor Device (MSD):
The MSD represents resource-constrained wearable or implantable medical sensors that collect physiological data such as heart rate, blood pressure, glucose level, and ECG signals. Due to strict limitations in computation power, memory, and energy, MSDs are incapable of performing computationally expensive cryptographic operations. Each MSD is equipped with a Physical Unclonable Function (PUF) module to provide hardware-based identity and resistance to physical capture attacks [3]–[5], [22].

2. User (U):
The user refers to a patient or authorized medical personnel who accesses healthcare data through a smart device (e.g., smartphone, tablet). The user initiates authentication requests and communicates with the healthcare server through a gateway or public network. The user device is assumed to have moderate computational capabilities compared to MSDs.

3. Gateway Node (GW):
The gateway acts as an intermediary between MSDs and the healthcare server. It aggregates sensor data and forwards authentication and communication requests. The gateway is assumed to be honest-but-curious, meaning it correctly follows protocol operations but may attempt to infer sensitive information from intercepted messages [10], [13].

4. Healthcare Server (HS):
The HS is a trusted entity responsible for system initialization, user and device registration, authentication verification, and secure storage of medical records. The server has sufficient computational and storage resources and is assumed to be physically secure.

Communication Model
Communication among these components takes place over open and unsecured wireless channels, except during the initial secure system setup.

Communications between MSD–GW and U–HS are especially susceptible to interception and alteration due to their wireless nature [17], [25].

The proposed protocol consists of three main phases:
1. Registration Phase
2. Authentication and Key Agreement Phase
3. Secure Data Communication Phase

4.2 Threat Model

The security of this scheme is evaluated using the widely recognized Dolev–Yao (DY) threat model, which is frequently employed in IoT and healthcare security studies [15], [16], [17].

The adversary $\mathcal{A}$ is presumed to possess the following capabilities:

1. Eavesdropping and Message Manipulation:
$\mathcal{A}$ can intercept, modify, replay, and inject messages transmitted over public communication channels between U, MSD, GW, and HS.

2. Replay and Man-in-the-Middle (MITM) Attacks:
$\mathcal{A}$ can record previous authentication messages and attempt replay or MITM attacks to impersonate legitimate entities.

3. Impersonation Attacks:
$\mathcal{A}$ may attempt to impersonate a legitimate user, sensor device, or gateway by exploiting compromised credentials or intercepted messages.

4. Physical Capture Attacks:
MSDs are assumed to be deployed in unattended environments. Thus, $\mathcal{A}$ may physically capture an MSD and extract all stored information from its memory. However, extracting the intrinsic PUF response is assumed to be computationally infeasible [3], [22], [23].

5. Stolen Device Attacks:
$\mathcal{A}$ may obtain a user's smart device and attempt offline guessing or credential extraction attacks using stored data.

6. Known Session-Specific Temporary Information:
$\mathcal{A}$ may obtain temporary random numbers used in previous sessions but should not be able to derive long-term secrets or session keys.

Security Assumptions: Cryptographic hash functions are assumed to be one-way and collision-resistant, PUF responses are assumed to be unique, unclonable, and unpredictable, The healthcare server is trusted and uncompromised, Side-channel attacks (e.g., power analysis) are beyond the scope of this work.

4.3 Security Goals

Based on the above system and threat models, the proposed protocol aims to achieve the following security objectives:

- Mutual authentication among U, MSD, and HS
- Secure session key establishment
- Patient anonymity and untraceability
- Resistance to replay, impersonation, MITM, and stolen-device attacks
- Resistance to physical capture and cloning attacks
- Forward secrecy of session keys Model and Threat Model

5. Proposed Authentication Protocol

This section presents the proposed secure, lightweight, and privacy-preserving authentication and key agreement protocol designed for Healthcare IoT environments. The protocol aims to provide mutual authentication among the User (U), Medical Sensor Device (MSD), and Healthcare Server (HS) while ensuring patient anonymity, resistance to physical capture attacks, and low computational overhead suitable for resource-constrained medical devices.

As outlined in the system model in Section 4, the protocol is divided into three main phases: Registration Phase, Authentication and Key Agreement Phase, and Secure Data Communication Phase.

5.1 Notations and Assumptions

Table II provides a summary of the notations used in the protocol.

Notation	Description
U	User (patient or medical staff)
MSD	Medical Sensor Device
HS	Healthcare Server
ID_U	Identity of user U
ID_MSD	Identity of medical sensor device
SID	Pseudonym identity
PUF(·)	Physical Unclonable Function

Notation	Description
R	PUF challenge
P	PUF response
h(·)	One-way hash function
⊕	Bitwise XOR operation
N_U, N_MSD	Random nonces
SK	Session key
T	Timestamp

Assumptions:

- HS is fully trusted and secure.
- Communication channels are insecure.
- MSD is equipped with a PUF module.
- Hash functions are collision-resistant and one-way.

5.2 Registration Phase

The registration process is carried out over a secure channel prior to deployment to set up system parameters and credentials.

5.2.1 User Registration

1. Initially, the user U chooses an identity ID_U and sends it to HS.
2. HS then creates a distinct pseudonym identity SID_U for U.
3. HS computes a secret parameter:

$$A\_U = h\ (ID\_U \parallel x)$$

where x represents the master secret of HS.

4. HS securely retains ⟨SID_U, A_U⟩ and supplies the necessary parameters to the user's device.

5.2.2 Medical Sensor Device Registration

1. MSD submits its identity ID_MSD to HS, which then
2. generates a challenge R and forwards it to MSD.
3. MSD computes the PUF response:

$$P = PUF(R)$$

4. HS computes and stores:

$$A\_MSD = h\ (ID\_MSD \parallel P \parallel x)$$

5. MSD only stores ⟨R⟩, ensuring no long-term secret is kept, thus providing protection against physical capture attacks.

5.3 Authentication and Key Agreement Phase

This phase facilitates mutual authentication and the establishment of a secure session key among U, MSD, and HS over an insecure channel.

Step 1: User → MSD

1. U generates a nonce N_U and timestamp T_U.
2. U computes:

$$M\_1 = h\ (SID\_U \parallel N\_U \parallel T\_U)$$

3. U sends ⟨SID_U, M_1, T_U⟩ to MSD.

Step 2: MSD → HS

1. MSD verifies T_U.
2. MSD generates nonce N_MSD and computes P = PUF(R).
3. MSD computes:

$$M\_2 = h\ (SID\_U \parallel P \parallel N\_MSD \parallel T\_MSD)$$

4. MSD sends ⟨SID_U, M_1, M_2, N_MSD, T_MSD⟩ to HS.

Step 3: HS Verification

1. HS retrieves A_U and A_MSD.
2. HS verifies M_1 and M_2.
3. If verification succeeds, HS computes the session key:

$$SK = h\ (A\_U \parallel A\_MSD \parallel N\_U \parallel N\_MSD)$$

4. HS generates authentication tokens M_3 and M_4 for U and MSD.

Step 4: HS → MSD → U

1. HS sends ⟨M_3, M_4⟩ to MSD.
2. MSD verifies M_4 and forwards M_3 to U.
3. U verifies M_3.
4. Upon successful verification, all entities share the same session key SK.

5.4 Secure Data Communication Phase

After the authentication is completed successfully, MSD encrypts sensing data with session key SK and sends them to HS through gateway in secure way. The session key has forward secrecy since it is updated frequently.

5.5 Security Properties Discussion

The proposed protocol has the following security service guarantees: Mutual authentication, Confidentiality of session key Privacy and Untraceability of patient nodes Protection against replay, impersonation, MITM and physical capture attack No long-term secret is stored at MSD.

In the following section, we present a formal verification with BAN logic and AVISPA in order to support the mentioned statements.

6. Security Analysis

This paper analyzes the security of the authentication and key agreement protocol according to the threat model described in Section 4 and protocol operations described in Section 5. It is shown that the model satisfies necessary security properties for Healthcare IoT by means of informal attack analysis and formal verification readiness.

6.1 Mutual Authentication

The User (U), Medical Sensor Device (MSD) and Healthcare Server are mutually authenticated through the protocol.

- The HS verifies U using authentication with pseudonym identity which is different from the PSN and a fresh nonce created at the moment of its request.
- MSD is proven based on its corresponding PUF response, which is unforgeable and unclonable.
- User U and MSD authenticate HS by verifying confirmation messages which are computed as a function of fresh session attributes.

As all authentication messages are tied to a fresh nonce and evaluated by HS, any unauthentic party is detected and discarded. Thus the protocol provides strong mutual authentication among all of participating entities.

6.2 Session Key Security

The session key SK= h (N_U || N_MSD || PID_U) is generated using fresh nonces contributed by both U and MSD.

- The session key is never transmitted over the network.
- An adversary cannot derive SK without knowledge of both nonces and the authenticated pseudonym.
- Compromise of one session does not affect other sessions, ensuring session independence.

Hence, the protocol guarantees confidentiality and freshness of session keys.

6.3 Resistance to Replay Attacks

Replay attacks are prevented by the use of:

- Fresh random nonces N_U and N_MSD
- Timestamps for message freshness verification

Any replayed message containing outdated parameters is detected and discarded during verification. Therefore, the proposed scheme is resistant to replay attacks.

6.4 Resistance to Man-in-the-Middle Attacks

Under the Dolev–Yao threat model, an adversary may intercept and modify messages. However:

- Authentication messages are cryptographically bound to nonces and pseudonym identities.
- Any modification of transmitted messages results in verification failure at HS.

As a result, the adversary cannot impersonate any legitimate entity or establish a valid session key, ensuring resistance to man-in-the-middle attacks.

6.5 Resistance to Impersonation Attacks

Impersonation attacks are prevented as follows:

- User impersonation is infeasible without valid pseudonym credentials.
- MSD impersonation is infeasible due to the PUF-based identity, which cannot be duplicated or predicted.
- HS impersonation is prevented since U and MSD verify server-generated authentication confirmations.

Thus, the protocol effectively resists impersonation attacks.

6.6 Resistance to Physical Capture Attacks

Medical sensor devices are often deployed in unattended environments and may be physically captured. In the proposed protocol:

- MSD stores no long-term secret keys.
- Device identity relies on PUF responses, which are hardware-intrinsic and unclonable.

Even if an adversary extracts all stored data from a captured MSD, they cannot reproduce valid PUF responses. Hence, the protocol is secure against physical capture and cloning attacks.

6.7 User Anonymity and Untraceability

The real identity ID_U of the user is never transmitted over public channels.

- Only a pseudonym identity (PID_U) is used during authentication.
- Fresh nonces ensure that authentication messages differ across sessions.

Therefore, an adversary cannot link multiple protocol sessions to the same user, ensuring user anonymity and untraceability, which are critical for healthcare applications.

6.8 Forward Secrecy

Forward secrecy is ensured because session keys are derived exclusively from fresh nonces.

- Compromise of long-term credentials or pseudonym information does not reveal past session keys.
- Each session key is independent of previous sessions.

Thus, the protocol provides forward secrecy.

6.9 Formal Security Validation Readiness

The authentication goals and message exchanges defined in Section 5 are well-suited for formal verification.

- BAN logic is used to prove mutual authentication and session key agreement.
- AVISPA is employed to validate secrecy and authentication properties under the Dolev–Yao model.

The formal analysis results are presented in the following section.

7. Performance Evaluation

This section assesses the performance of the proposed authentication protocol concerning computational cost, communication overhead, and its appropriateness for resource-limited Healthcare IoT devices. The evaluation is performed analytically and compared with representative existing schemes discussed in Section 3.

7.1 Computational Cost Analysis

The proposed protocol is designed using lightweight cryptographic operations, namely:

- One-way hash functions
- XOR operations
- PUF response generation at the medical sensor device

No public-key cryptographic operations or complex modular exponentiations are used, which significantly reduces computational overhead. During the authentication and key agreement phase:

- The user performs a small number of hash and XOR operations.
- The medical sensor device performs hash operations and a single PUF evaluation.
- The healthcare server performs hash-based verification and session key generation.

Compared with conventional public-key–based authentication schemes, the proposed protocol requires substantially lower computation, making it suitable for low-power and resource-constrained medical sensor devices.

7.2 Communication Overhead Analysis

The communication overhead of the proposed protocol is determined by the number and size of messages exchanged during authentication.

- The protocol completes authentication in three message exchanges among U, MSD, and HS.
- All transmitted messages consist of hash outputs, pseudonym identities, nonces, and timestamps, resulting in fixed-length messages.
- No certificates or large cryptographic parameters are transmitted.

Compared to existing lightweight and PUF-based authentication schemes, the proposed protocol achieves lower or comparable communication overhead, which is particularly important for bandwidth-constrained wireless healthcare environments.

7.3 Storage Cost Analysis

The proposed protocol minimizes storage requirements:

- Medical sensor devices store only a PUF challenge and no long-term secret keys.
- Users store pseudonym-related parameters.
- Healthcare server stores registration information and verification parameters.

By avoiding the storage of sensitive secrets on MSDs, the protocol strengthens its protection against physical capture attacks and at the same time tolerates low memory usage.

7.4 Comparative Performance Discussion

See the comparison in Section 3.

- Symmetric key based algorithm is less computational demanding but not strong against the physical attacks.

- PUF-based protocols improve security in most cases, albeit at the expense of a slightly better commu-nication complexity or storage requirement.
- The proposed protocol is a good compromise with lightweight computation, small communication overhead, strong privacy protection and resistance against physical capture attacks.

This balance makes the proposed protocol suitable for realistic Healthcare IoT services.

Performance analysis results demonstrate that the proposed protocol is computationally efficient, lightweight in terms of communication and storage requirements, compatible with real-life Healthcare IoT environments, and provide stronger security guarantees at higher levels of computation as compared to existing protocols.

8. Conclusion

A lightweight privacy-preserving and secure authentication key agreement protocol for healthcare internet of things (H-IoT) environments was proposed in this paper. The proposed scheme was designed with the aim of addressing major security challenges that H-IoT systems encounter, i.e., resource constraints, patient privacy preservation and defense against physical capture attacks.

We set up a comprehensive system/threat model which reflects real-world healthcare deployment. It combines lightweight cryptographic primitives with PUF-based device authentication to provide mutual authentication, secure session key establishment and guarantee user's anonymity without the requirement of maintaining long-term secrets in medical sensor devices. The security tests, both formal and informal, reflected the facts that the protocol supports resistance to replay, impersonation, man-in-the-middle attacks, as well as physical capture.

Performance evaluations showed that the protocol requires low computation, communication, and storage resources, which is a suitable choice for medical devices with limited capabilities. Comparisons also indicated that the new scheme provides a better trade-off among security strength, and computation overhead than those of the existing authentication protocols.

Possible extensions to the protocol include dynamic device revocation, post-quantum lightweight cryptography, and real-world deployment/implementation testbed evaluation on a massive scale in large-scale Healthcare IoT settings. This scheme is a light-weight hash based operation with the addition of PUF-assisted identity protection, it was formal verified with BAN logic and AVISPA compared to other existing protocols that even though provide security and anonymity but involve high overhead or lack of complete fromal verfication this protocol provides balanced solution including light weight low overheads, strong security as in prexisting systems and is suitable for resource constrained HIoT environment.

We intend to extend our protocol in future work with mobility-aware authentication for smooth handoff of medical sensors across different gateways or healthcare domains. Moreover, next steps can include the experimentation and the performance evaluation of proposed scheme on real medical sensors hardware for energy consumption, latency and reliability under practical scenarios. Use of post-quantum lightweight cryptographic primitives can add to the overall robustness of the protocol against upcoming quantum risks. Last but note least the protocol could be further enhanced to enable a blockchain-assisted auditability or anomaly detection by machine learning as better trust and misuse prevention mechanisms in large-scale Healthcare IoT deployments.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] J. Zhao, S. Zeng, P. Luo, B. Zhao, and Z. Wang, “A lightweight multi-sensor concurrent identity authentication protocol for smart grids,” Measurement: Sensors, vol. 33, Jun. 2024, Art. no. 101131, doi: 10.1016/j.measen.2024.101131.

[2] A. Mahesh Reddy and M. Kameswara Rao, “A lightweight symmetric cryptography-based user authentication protocol for IoT-based applications,” Scalable Computing: Practice and Experience, vol. 25, no. 3, pp. 1647–1657, Apr. 2024, doi: 10.12694/scpe.v25i3.2692.

[3] Y. Zhuang and G. Li, “A lightweight PUF-based authentication protocol,” arXiv:2405.13146, May 2024.

[4] C. Gupta and G. Varshney, “A lightweight and secure PUF-based authentication and key-exchange protocol for IoT devices,” arXiv:2311.04078, Nov. 2023.

[5] J. Cui, J. Wang, H. Meng, J. Du, X. Cao, T. Xie, and Y. Yong, “Lightweight and anonymous mutual authentication protocol for edge IoT nodes with physical unclonable function,” Security and Communication Networks, vol. 2022, Art. no. 1203691, 2022, doi: 10.1155/2022/1203691.

[6] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, “A secure and lightweight authentication protocol for IoT-based smart homes,” Sensors, vol. 21, no. 4, Art. no. 1488, 2021, doi: 10.3390/s21041488.

[7] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, “Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks,” IEEE Trans. Ind. Informatics, vol. 15, no. 9, pp. 4957–4968, Sep. 2019, doi: 10.1109/TII.2019.2895030.

[8] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García, “Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things,” Sensors, vol. 20, no. 2, Art. no. 501, 2020, doi: 10.3390/s20020501.

[9] H. S. Trivedi and S. J. Patel, “Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things,” Computer Networks, vol. 178, Art. no. 107335, 2020, doi: 10.1016/j.comnet.2020.107335.

[10] K.-H. Yeh, “A secure IoT-based healthcare system with body sensor networks,” IEEE Access, vol. 4, pp. 10288–10299, 2016, doi: 10.1109/ACCESS.2016.2638038.

[11] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, “Secure and lightweight authentication scheme for smart metering infrastructure in smart grid,” IEEE Trans. Ind. Informatics, vol. 16, no. 5, pp. 3548–3557, May 2020, doi: 10.1109/TII.2019.2944880.

[12] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha,

"Lightweight authentication and key agreement for smart metering in smart energy networks," IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 4349–4359, Jul. 2019, doi: 10.1109/TSG.2018.2857558.

[13] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," Procedia Computer Science, vol. 52, pp. 452–459, 2015, doi: 10.1016/j.procs.2015.05.013.

[14] S. Gaba, G. Kumar, H. Monga, T.-H. Kim, and P. Kumar, "Robust and lightweight mutual authentication scheme in distributed smart environments," IEEE Access, vol. 8, pp. 69722–69733, 2020, doi: 10.1109/ACCESS.2020.2986480.

[15] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, Feb. 1990, doi: 10.1145/77648.77649.

[16] L. Viganò, "Automated security protocol analysis with the AVISPA tool," Electron. Notes Theor. Comput. Sci., vol. 155, pp. 61–86, 2006, doi: 10.1016/j.entcs.2005.11.052.

[17] M. A. Khan, I. U. Din, T. Majali, and B.-S. Kim, "A survey of authentication in Internet of Things-enabled healthcare systems," Sensors, vol. 22, no. 23, Art. no. 9089, 2022.

[18] Q. Xie, Z. Ding, and Q. Xie, "A lightweight and privacy-preserving authentication protocol for healthcare in an IoT environment," Mathematics, vol. 11, no. 18, Art. no. 3857, 2023. doi: 10.3390/math11183857.

[19] K. Kim, J. Ryu, Y. Lee, and D. Won, "An improved lightweight user authentication scheme for the Internet of Medical Things," Sensors, vol. 23, no. 3, Art. no. 1122, 2023. doi: 10.3390/s23031122.

[20] M. A. Jan, F. Khan, S. Mastorakis, and J. Li, "LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics," arXiv preprint, arXiv:2104.14906, 2021.

[21] M. A. Jan, F. Khan, S. Mastorakis, and J. Li, "PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment," Sensors, vol. 22, no. 18, Art. no. 7075, 2022. doi: 10.3390/s22187075.

[22] A. Braeken, P. Porambage, M. Stojmenovic, and A. Braeken, "PUF-based authentication protocol for IoT," Symmetry, vol. 10, no. 8, Art. no. 352, 2018. doi: 10.3390/sym10080352.

[23] J. Zhang, Y. Zhang, and W. Chen, "Secure PUF-based authentication systems: A survey," Sensors, vol. 24, no. 16, Art. no. 5295, 2024. doi: 10.3390/s24165295.

[24] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, and H. Tenhunen, "Authentication and authorization for IoT-based e-healthcare systems: A survey," IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1248–1289, 2020. doi: 10.1109/COMST.2019.2963177.

[25] A. P. Fotouhi, M. Bayat, A. K. Das, and K. K. R. Choo, "Authentication schemes in IoT-based healthcare systems: A survey," IEEE Internet Things J., vol. 8, no. 6, pp. 4184–4212, Mar. 2021. doi: 10.1109/JIOT.2020.3035418.