sensors

MDPI

Article

LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things

Chien-Ming Chen [1], Zhaoting Chen [1], Saru Kumari [2] and Meng-Chang Lin [3,*]

[1] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China; chienmingchen@ieee.org (C.-M.C.); SDKJDXchen@163.com (Z.C.)
[2] Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, Uttar Pradesh, India; saryusiirohi@gmail.com
[3] Graduate Institute of Nanomedicine and Medical Engineering, College of Biomedical Engineering, Taipei Medical University, Taipei 115, Taiwan
* Correspondence: mengchanglin@tmu.edu.tw

Abstract: The Internet of Health Things (IoHT), which is an extension of the Internet of Things (IoT) in healthcare, has provided a new type of telemedicine approach. In IoHT, wearable sensors are used to collect patient health data, and information is transmitted remotely to doctors who can develop accurate treatment plans and provide timely telemedicine services to patients. However, patient health data are transmitted over a public channel, which means that the privacy and medical data of patients are at significant risk of leakage and can be confronted by serious security problems. We proposed a lightweight authentication protocol known as LAP-IoHT for IoHT environments to overcome the various threats that are currently faced by IoHT. We verified the security of LAP-IoHT using a Real-or-Random model and demonstrated its significant performance advantage by conducting a comparative analysis with other similar protocols for a better adaptation to the IoHT environment.

Keywords: Internet of Health Things; authentication; network security

check for updates

Citation: Chen, C.-M.; Chen, Z.; Kumari, S.; Lin, M.-C. LAP-IoHT: A Lightweight Authentication Protocol for the Internet of Health Things. *Sensors* **2022**, *22*, 5401. https://doi.org/10.3390/s22145401

Academic Editor: Jemal Abawajy

Received: 26 May 2022
Accepted: 13 July 2022
Published: 20 July 2022

1. Introduction

The rapid development of communication technologies has resulted in the extensive application of the Internet of Things (IoT) [1–4]. By using wireless networks to connect devices and various servers, IoT [5] provides a new means of communication that further enables interaction between virtual environments and the real world. Sensors [6,7] are the most common and versatile IoT devices. Wireless sensor networks (WSNs) [8–10] consist of numerous sensors to monitor specific areas and collect data. Hence, sensors and WSNs play an essential role in IoT development. At present, IoT is widely deployed in various applications and environments, such as manufacturing [11], environmental protection [12], smart cities [13,14], and intelligent transportation [15,16]. The rapid increase in the number of IoT devices demonstrates the importance and development potential of IoT, which is gradually improving the quality of life and making intelligent living and digital life possible.

Furthermore, the Internet of Health Things (IoHT) [17,18], which is a subset of IoT, is used extensively in healthcare scenarios [19–21]. In IoHT, wearable sensors [22,23] are implanted into the human body or set on body surfaces depending on the disease condition, thereby continuously monitoring the physiological indicators of the patient. These wearable sensors collect real-time data from the human body and transmit them to servers. Doctors can remotely analyze these data in order to provide timely medical services to patients. As the development of the healthcare sector is closely linked to people's lives, IoHT can prevent several chronic diseases, save patient transportation costs, protect the health of healthcare professionals, reduce the possibility of conflicts between doctors and patients, and help family members to remain abreast of patients' current conditions. IoHT provides higher-quality healthcare services, improves the level and efficiency of services, and optimizes the use of healthcare resources.

Security and privacy [24–27] have become the primary challenges of IoHT. In an IoHT system, the medical information of patients collected by sensors is transmitted over open networks. Since this information is highly sensitive, it must be protected from unauthorized users or malicious attackers, who may steal, modify, and delete health data, corrupt medical records, and even threaten the lives of patients. Moreover, attackers may target medical devices by hijacking and forging such devices, resulting in the denial of service and, in severe cases, possible damage to medical devices. Therefore, exploring a security mechanism to address the current environment and eliminate threats in IoHT is necessary.

This study proposed a lightweight authentication protocol (LAP) known as LAP-IoHT for IoHT environments. In LAP-IoHT, all participants, including the users and wearable sensors, are authenticated by the gateway. Subsequently, a shared session key is established for each communication session. LAP-IoHT encrypts the biometric features of the users to ensure anonymity. To demonstrate the security and reliability of this approach, we applied the Real-or-Random (ROR) model to analyze LAP-IoHT. The experimental results indicated that LAP-IoHT exhibits improved communication and computationally efficient performance.

The main contributions of this study are as follows:

(1) To address the current security issues frequently encountered in healthcare IoT systems, we designed a three-factor IoHT-based protocol that incorporates authentication and key negotiation, thereby guaranteeing privacy and access control.
(2) The introduction of biometrics, which protects the anonymity of users with unique information, can provide better user experience and privacy protection. In addition to using common one-way hash functions and simple XOR operations, we adopted asymmetric encryption and decryption in the protocol to provide higher security.
(3) Based on a shared ROR model, we performed a formal security analysis to evaluate the security, soundness, and integrity of the session key and protocol. Moreover, the informal security analysis provided strong evidence that the protocol is resistant to currently known security attacks.
(4) We conducted a comparative study and analyzed the performance of several protocols of the same type, taking into account the computational cost, time efficiency, and security properties. The results demonstrated that our protocol exhibits a significant performance advantage.

The remainder of this paper is organized as follows: Section 2 describes related work. In Section 3, we outlined the proposed LAP-IoHT protocol. Sections 4 and 5 provide the security analysis and performance evaluation, respectively. Finally, Section 6 concludes the paper.

2. Related Work

IoT is widely adopted in healthcare monitoring systems. Onasanya et al. [28] proposed an IoT healthcare system for cancer care. Sun et al. [29] developed a medical record search protocol for IoT healthcare to ensure privacy preservation. Zhang et al. [30] proposed an isolation computing technology for cloud-based IoT healthcare. In 2020, Selvaraj et al. [31] reviewed the challenges and opportunities in IoT healthcare systems. Furthermore, several researchers have emphasized security and privacy issues. In 2019, Alassaf et al. [32] simulated the implementation of cryptographic functions for data in IoT healthcare. Kumari et al. [33] described a secure framework for medical systems in 2020. In 2021, Hossien et al. [34] introduced a privacy-preserving architecture for IoT healthcare based on blockchain. Wang et al. [35] proposed privacy preservation in IoT-enabled healthcare systems.

Moreover, several authentication protocols are available for IoHT. A summary of the applications of IoT in the medical industry is presented in Table 1. In 2015, Amin et al. [36] argued that elliptic curve cryptography could provide improved security for IoHT, but the protocol was not resistant against offline password-guessing attacks and privileged insider attacks. Challa et al. [37] proposed a three-factor authentication protocol for IoHT in 2018. However, once the sensor node was obtained by a malicious attacker, it broke the security of the protocol [37]. In 2019, Preeti et al. [38] designed a protocol that applied a WSN to IoHT and used a smart card. However, their protocol did not provide perfect forward security or resistance against sensor node capture attacks. Aghili et al. [39] proposed an access control and ownership transfer protocol for IoHT systems. Unfortunately, Amintoosi et al. [40] pointed out that the protocol of Aghili et al. [39] could not provide perfect forward security and was vulnerable to malicious sensor and server spoofing attacks. They also proposed a low-cost protocol for IoHT. In 2019, Gupta et al. [41] proposed a protocol that used wearable medical devices for IoHT to prevent attackers from modifying patient health information. However, Hajian et al. [42] pointed out that this protocol [41] did not protect information against privileged insider attacks, offline password-guessing attacks, and de-synchronization attacks. The proposed protocol of Hajian et al. [42] also could not provide perfect forward security and was vulnerable to session-key disclosure and impersonation attacks. To improve the security of the protocol, Kumar et al. [43] used digital signatures to encrypt the IoHT protocol communication process. Recently, Yu et al. [44] proposed a more realistic application-compliant authentication protocol designed around blockchain and physically unclonable functions while also enhancing mutual authentication between entities.

Table 1. A summary of the application of the Internet of Things in the medical industry.

Protocols	Advantages	Limitations
Amin et al. [36]	(1) Resist impersonation attack (2) Resist smart card stolen attack (3) Resist replay attack	(1) Cannot resist privileged insider attack (2) Cannot resist offline password guessing attack
Challa et al. [37]	(1) Provide user anonymity (2) Resist offline password guessing attack (3) Resist man-in-the middle attack	(1) Cannot resist sensor node capture attack
Preeti et al. [38]	(1) Provide mutual authentication (2) Resist DoS attack (3) Resist known-session-specific temporary information attack	(1) Cannot provide perfect forward security (2) Cannot resist sensor node capture attack
Aghili et al. [39]	(1) Provide user untraceability (2) Resist de-synchronization attack (3) Resist DoS attack	(1) Cannot provide perfect forward security (2) Cannot resist malicious sensor attack (3) Cannot resist server impersonation attack
Amintoosi et al. [40]	(1) Resist known-session-specific temporary information attack (2) Provide perfect forward security (3) Resist privileged insider attack	–
Gupta et al. [41]	(1) Provide perfect forward security (2) Resist impersonation attack (3) Provide anonymity and untraceability	(1) Cannot resist privileged insider attack (2) Cannot resist offline password guessing attack (3) Cannot resist de-synchronization attack
Hajian et al. [42]	(1) Resist replay attack (2) Resist privileged insider attack (3) Resist de-synchronization attack	(1) Cannot provide perfect forward security (2) Cannot resist session key disclosure attack (3) Cannot resist impersonation attack
Kumar et al. [43]	(1) Resist privileged insider attack (2) Resist man-in-the-middle attack (3) Resist replay attack	–
Yu et al. [44]	(1) Provide user untraceability and anonymity (2) Resist session key disclosure attack (3) Provide mutual authentication	–

3. Proposed LAP-IoHT

3.1. Network Model

Figure 1 depicts the overall network model of the proposed protocol. This model describes a typical IoHT environment. The architecture includes three entities: users, a gateway, and wearable sensors:

(1) Wearable sensors are set on the bodies of patients. They can observe various body indicators, such as the electrocardiogram (ECG), electromyography (EMG), electroencephalogram (EEG), respiratory rate, pulse, blood pressure, blood glucose, and oxygen saturation. These wearable sensors should be registered with a gateway before being deployed to human bodies for precise management.

(2) Users are organizations or groups of people who can view the health data of patients. For example, users may be hospital administrators, doctors, pharmacists, nurses, families of patients, data analysts, and drug trialists. If a person needs to enter the network and view patient medical data, the person must register with the gateway in advance and become a legitimate user with the appropriate authorities.

(3) The gateway in our IoHT architecture acts as a trusted server. Prior to entering this network, all wearable sensors and users should register with the gateway. Subsequently, the gateway manages the list of all sensors and legitimate users.

Assume that a user desires to obtain data from a specific wearable sensor. This user transmits a request to the gateway and the gateway forwards this request to the sensor. After receiving the request, the wearable sensor sends the data to the user with the help of the gateway. Since medical data are personal and private, all communications among the users, gateway, and sensors should be confidential. The most straightforward method for achieving this is to encrypt the transmitted data.

The gateway can authenticate users and sensors using the proposed protocol. Moreover, a shared session key is established for each session.

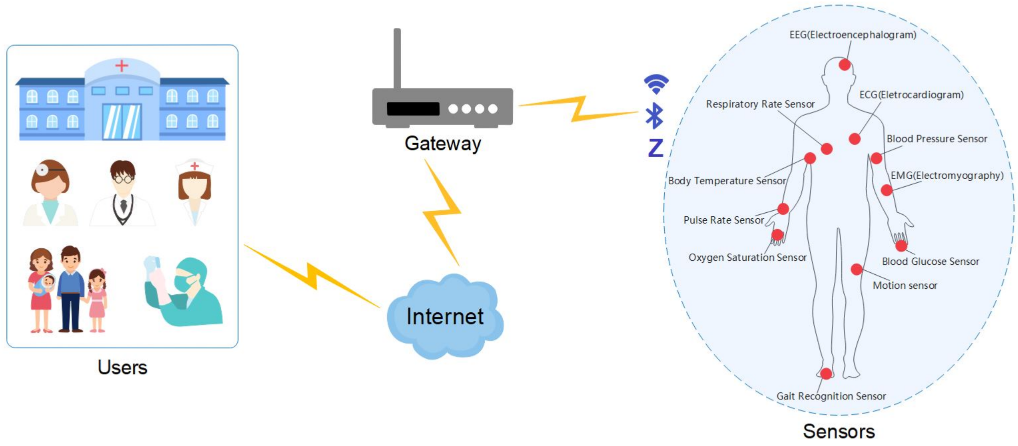

Figure 1. System model.

3.2. LAP-IoHT

This section presents the proposed LAP-IoHT protocol for IoHT, which consists of three phases: user registration, sensor registration, and login and authentication. The notations and symbols are defined in Table 2.

3.3. User Registration Phase

Assume that user U_i desires to become a legitimate user. This user must register with GWN. Figure 2 shows the steps that are involved in this phase. The messages are transmitted through a secure channel.

(1) U_i prepares his or her own ID_i and PW_i and unique biometric Bio and selects a random number r_1. Subsequently, U_i computes $HID_i = h(ID_i \parallel r_1)$, $Gen(Bio) = (\sigma_i, \tau_i)$,

$HPW_i = h(PW_i \parallel \sigma_i)$, and $N = PW_i \oplus h(ID_i \parallel \sigma_i)$. Thereafter, U_i transmits $\{HID_i$, HPW_i, $N\}$ to GWN.

(2) GWN first verifies whether HID_i has already been registered. Thereafter, GWN calculates $D_1 = h(HID_i \parallel N)$, $D_2 = h(D_1 \parallel G_j) \oplus HPW_i$, $D_3 = D_2 \oplus N$, and $D_4 = h(HID_i \parallel G_j) \oplus D_1$. Subsequently, GWN stores $\{HID_i, D_1\}$ in its database and transmits $\{D_1$, D_3, $D_4\}$ to U_i.

(3) U_i computes $\Omega_i = N \oplus r_1$ and $M = h(N \parallel r_1) \oplus HID_i$, and then stores $\{D_1$, D_3, D_4, Ω_i, $M\}$ in his or her smart card.

Table 2. Notation definitions.

Notations	Descriptions
U_i	ith user
ID_i	Identity of U_i
PW_i	Password of U_i
Bio	Biometrics of U_i
SN_j	jth sensor node
SID_j	Identity of SN_j
GWN	Gateway node
G_j	Private key of GWN
pbs	Public key of SN_j
pvs	Private key of SN_j
SK	Session key
T_s	Time stamp, where s = 1, 2, 3, 4
r_1, r_u, r_g, r_s	Temporary random number
$\oplus$	XOR operation
$\parallel$	Concatenate operation
$h(\cdot)$	Hash function
$Gen(\cdot)/Rep(\cdot)$	Fuzzy extractor/reproduction function
ENC/DEC	Asymmetric encryption/decryption
$\rightarrow$	The public channel
$\Rightarrow$	The secure channel
$\mathcal{A}$	Adversary

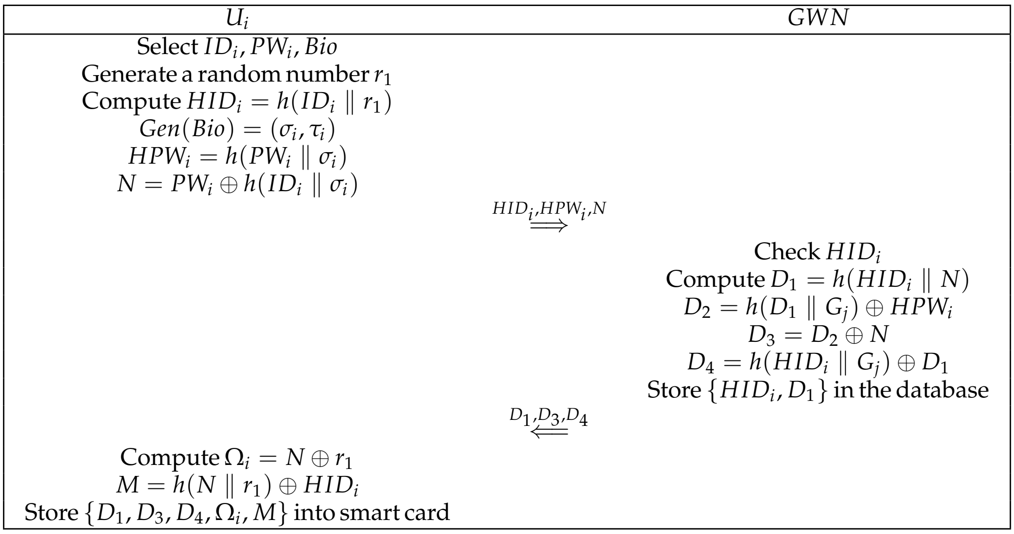

Figure 2. User registration phase.

3.4. Sensor Registration Phase

A wearable sensor must also be registered before joining the network. Assume that sensor SN_j desires registration with GWN. Figure 3 depicts the detailed steps involved in this phase. The messages are submitted via a secure channel:

(1) SN_j sends its identity SID_j to GWN.

(2) GWN generates a random number b and calculates the pseudo-identity PID_j of SN_j, where $PID_j = h(SID_j \parallel b)$. Subsequently, GWN calculates $HSID_j = h(SID_j \parallel G_j)$ and $SG = h(HSID_j \parallel G_j) \oplus PID_j$ with its own private key G_j. GWN also uses an asymmetric encryption system to encrypt PID with the public key of SN_j. At this point, GWN calculates $L = ENC_{pbs}(PID_j)$, sends $\{SG, L\}$ to SN_j, and stores $\{SID_j, PID_j\}$ in the database.

(3) SN_j stores $\{SG, L\}$ in its own memory.

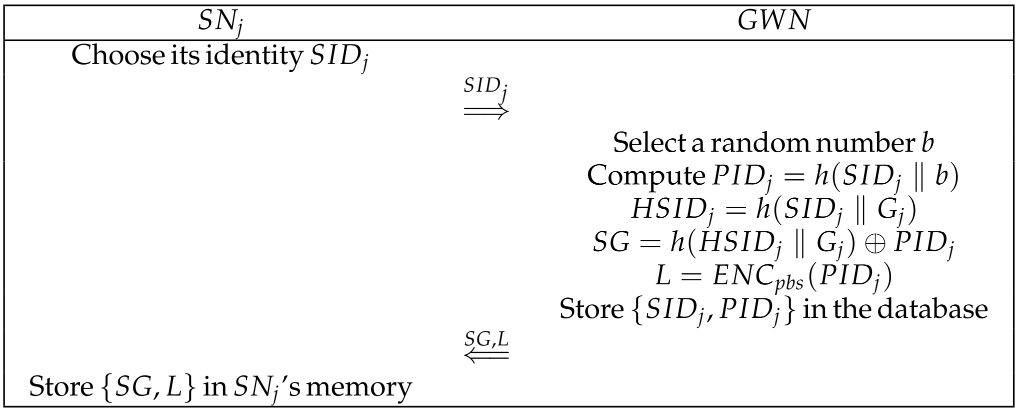

Figure 3. Sensor registration phase.

3.5. Login and Authentication Phase

If U_i requires connection to a specific wearable sensor SN_j, GWN needs to verify the legitimacy of the user. Subsequently, U_i, GWN, and SN_j build a session key to encrypt the messages among them. In this phase, several parameters (e.g., M', X'_{UG}, X'_{GS}, X'_{SG}, and X'_{Gu}) are calculated. Figure 4 illustrates this phase, the details of which are as follows:

(1) U_i inserts his or her smart card into a smart card reader/computer and provides his or her identity ID_i, password PW_i, and biometrics Bio. This computer calculates $\sigma_i = Rep(Bio, \tau_i)$, $N = PW_i \oplus h(ID_i \parallel \sigma_i)$, and $M' = h(N \parallel r_1) \oplus HID_i$, where $r_1 = \Omega_i \oplus N$ and $HID_i = h(ID_i \parallel r_1)$. Subsequently, it determines whether M' is equal to M stored in the smart card. If $M' = M$, the computer generates r_u and timestamp T_1 and calculates $HPW_i = h(PW_i \parallel \sigma_i)$, $B_1 = D_3 \oplus N \oplus HPW_i$, and $B_2 = B_1 \oplus r_u$. U_i calculates $X_{UG} = h(T_1 \parallel r_u \parallel HID_i \parallel B_2)$ and then sends $\{HID_i, B_2, X_{UG}, T_1\}$ to GWN.

(2) GWN first verifies the freshness of T_1 and retrieves the corresponding D_1 from its own database according to HID_i. Thereafter, GWN calculates $B_1 = h(D_1 \parallel G_j)$, $r_u = B_1 \oplus B_2$, and $X'_{UG} = h(T_1 \parallel r_u \parallel HID_i \parallel B_2)$. If X'_{UG} and the received X_{UG} are equal, GWN generates a random number r_g and current timestamp T_2. Subsequently, GWN calculates $HSID_j = h(SID_j \parallel G_j)$, $B_3 = r_u \oplus h(HSID_j \parallel G_j)$, $B_4 = D_1 \oplus h(B_3 \parallel SID_j \parallel r_u)$, $B_5 = r_g \oplus h(D_1 \parallel r_u)$, $B_6 = B_3 \oplus PID_j$, and $X_{GS} = h(T_2 \parallel r_u \parallel r_g \parallel SID_j \parallel B_5)$. Thereafter, GWN transmits $\{B_4, B_5, B_6, X_{GS}, T_2\}$ to SN_j.

(3) SN_j verifies the freshness of T_2 and then obtains PID_j by decrypting L with his or her private key pus. Thereafter, SN_j calculates $B_3 = B_6 \oplus PID_j$, $r_u = B_3 \oplus SG \oplus PID_j$, $D_1 = B_4 \oplus h(B_3 \parallel SID_j \parallel r_u)$, $r_g = B_5 \oplus h(D_1 \parallel r_u)$, and $X'_{GS} = h(T_2 \parallel r_u \parallel r_g \parallel SID_j \parallel B_5)$. SN_J determines whether X'_{GS} is the same as the received X_{GS}. If so, SN_j generates T_3, r_3, and computes $B_7 = r_s \oplus h(SG \parallel D_1 \parallel r_g)$, $B_8 = PID_j \oplus B_7$,

$X_{SG} = h(T_3 \parallel r_g \parallel r_s \parallel B_7 \parallel SG)$, and $X_{SU} = h(r_u \parallel r_s \parallel SID_j \parallel D_1)$. Finally, SN_j calculates the session key SK as $h(r_u \parallel r_g \parallel r_s)$. At this point, SN_j transmits $\{B_8, X_{SG}, X_{SU}, T_3\}$ to GWN.

(4) GWN first verifies the freshness of T_3, and calculates $B_7 = B_8 \oplus PID_j$, $SG = h(HSID_j \parallel G_j) \oplus PID_j$, and $r_s = B_7 \oplus h(SG \parallel D_1 \parallel r_g)$. Subsequently, GWN verifies the legitimacy of SN_j by determining whether $h(T_3 \parallel r_g \parallel r_s \parallel B_7 \parallel SG)$ is equal to X_{SG}. If they are equal, GWN generates a timestamp T_4, computes $B_9 = D_1 \oplus B_1$, $B_{10} = B_9 \oplus h(HID_i \parallel G_j) \oplus r_s$, and $B_{11} = SID_j \oplus h(B_1 \parallel r_s)$, and produces a session key $SK = h(r_u \parallel r_g \parallel r_s)$. GWN provides $X_{GU} = h(T_4 \parallel r_u \parallel r_g \parallel B_{10})$ for mutual authentications with the user and sends $\{B_5, B_{10}, B_{11}, X_{GU}, X_{SU}, T_4\}$ to U_i.

(5) The computer of U_i inspects the timestamp from GWN, and computes $r_s = B_1 \oplus B_{10} \oplus D_4$ and $r_g = B_5 \oplus h(D_1 \parallel r_u)$. Thereafter, it calculates X'_{GU} and verifies whether $X'_{GU} = X_{GU}$. Subsequently, it calculates $X'_{SU} = h(r_u \parallel r_s \parallel SID_j \parallel D_1)$, where $SID_j = B_{11} \oplus h(B_1 \parallel r_s)$. At this time, U_i can successfully calculate the session key $SK = h(r_u \parallel r_g \parallel r_s)$. Obviously, U_i, GWN, and SN_j have the same session key at this point.

U_i	GWN	SN_j
U_i provide ID_i, PW_i, Bio Compute $\sigma_i = Rep(Bio, \tau_i)$ $N = PW_i \oplus h(ID_i \parallel \sigma_i)$ $r_1 = \Omega_i \oplus N, HID_i = h(ID_i \parallel r_1)$ $M' = h(N \parallel r_1) \oplus HID_i$ Check $M' \overset{?}{=} M$ Generate r_u, T_1 Compute $HPW_i = h(PW_i \parallel \sigma_i)$ $B_1 = D_3 \oplus N \oplus HPW_i, B_2 = B_1 \oplus r_u$ $X_{UG} = h(T_1 \parallel r_u \parallel HID_i \parallel B_2)$ $\xrightarrow{HID_i, B_2, X_{UG}, T_1}$		
	Check the validity of T_1 Retrieve D_1 from database Compute $B_1 = h(D_1 \parallel G_j)$ $r_u = B_1 \oplus B_2$ $X'_{UG} = h(T_1 \parallel r_u \parallel HID_i \parallel B_2)$ Check $X'_{UG} \overset{?}{=} X_{UG}$ Generate r_g, T_2 Compute $HSID_j = h(SID_j \parallel G_j)$ $B_3 = r_u \oplus h(HSID_j \parallel G_j)$ $B_4 = D_1 \oplus h(B_3 \parallel SID_j \parallel r_u)$ $B_5 = r_g \oplus h(D_1 \parallel r_u), B_6 = B_3 \oplus PID_j$ $X_{GS} = h(T_2 \parallel r_u \parallel r_g \parallel SID_j \parallel B_5)$ $\xrightarrow{B_4, B_5, B_6, X_{GS}, T_2}$	
		Check the validity of T_2 Compute $PID_j = DEC_{pvs}(L)$ $B_3 = B_6 \oplus PID_j, r_u = B_3 \oplus SG \oplus PID_j$ $D_1 = B_4 \oplus h(B_3 \parallel SID_j \parallel r_u)$ $r_g = B_5 \oplus h(D_1 \parallel r_u)$ $X'_{GS} = h(T_2 \parallel r_u \parallel r_g \parallel SID_j \parallel B_5)$ Check $X'_{GS} \overset{?}{=} X_{GS}$ Generate r_s, T_3 Compute $B_7 = r_s \oplus h(SG \parallel D_1 \parallel r_g)$ $B_8 = PID_j \oplus B_7, SK = h(r_u \parallel r_g \parallel r_s)$ $X_{SG} = h(T_3 \parallel r_g \parallel r_s \parallel B_7 \parallel SG)$ $X_{SU} = h(r_u \parallel r_s \parallel SID_j \parallel D_1)$ $\xleftarrow{B_8, X_{SG}, X_{SU}, T_3}$
	Check the validity of T_3 Compute $B_7 = B_8 \oplus PID_j$ $SG = h(HSID_j \parallel G_j) \oplus PID_j$ $r_s = B_7 \oplus h(SG \parallel D_1 \parallel r_g)$ $X'_{SG} = h(T_3 \parallel r_g \parallel r_s \parallel B_7 \parallel SG)$ Check $X'_{SG} \overset{?}{=} X_{SG}$ Generate T_4 Compute $SK = h(r_u \parallel r_g \parallel r_s)$ $B_9 = D_1 \oplus B_1$ $B_{10} = B_9 \oplus h(HID_i \parallel G_j) \oplus r_s$ $B_{11} = SID_j \oplus h(B_1 \parallel r_s)$ $X_{GU} = h(T_4 \parallel r_u \parallel r_g \parallel B_{10})$ $\xleftarrow{B_5, B_{10}, B_{11}, X_{GU}, X_{SU}, T_4}$	
Check the validity of T_4 Compute $r_s = B_1 \oplus B_{10} \oplus D_4$ $r_g = B_5 \oplus h(D_1 \parallel r_u), SK = h(r_u \parallel r_g \parallel r_s)$ $X'_{GU} = h(T_4 \parallel r_u \parallel r_g \parallel B_{10})$ Check $X'_{GU} \overset{?}{=} X_{GU}$ $SID_j = B_{11} \oplus h(B_1 \parallel r_s)$ $X'_{SU} = h(r_u \parallel r_s \parallel SID_j \parallel D_1)$ Check $X'_{SU} \overset{?}{=} X_{SU}$		

Figure 4. Login and authentication phase.

4. Security Analysis

This section first describes the capabilities that the attacker $\mathcal{A}$ may possess. Subsequently, we demonstrate that our method is secure against different types of attacks. Finally, we use the Real-or-Random (ROR) model to show that our LAP-IoHT protocol is provably secure.

4.1. Adversary Model

We consider the well-known Dolev–Yao (DY) adversary model [45] and assume that an attacker $\mathcal{A}$ has the following capabilities:

(1) $\mathcal{A}$ can eavesdrop, block, replay, alter, and delete messages that are sent over a public channel.
(2) $\mathcal{A}$ can steal the smart card or smart device of a user and obtain the information stored therein.
(3) $\mathcal{A}$ can capture a sensor node to extract the information stored therein.
(4) $\mathcal{A}$ can obtain the long-term key of the gateway and acquire the contents stored therein as an internal privileged person.

4.2. Protection against Well-Known Attacks

4.2.1. Replay Attack

In LAP-IoHT, messages that are transmitted via a public channel have timestamps, such as T_1, T_2, T_3, and T_4. These timestamps ensure the freshness of the messages and resist replay attacks. Moreover, X_{UG}, X_{GS}, X_{SG}, X_{SU}, and X_{GU} include random numbers. Timestamps and random numbers are two effective means of preventing replay attacks. Thus, LAP-IoHT is resistant against replay attacks.

4.2.2. User Impersonation Attack

Assume that $\mathcal{A}$ can obtain the private key G_j of GWN. Even if $\mathcal{A}$ intercepts the parameters T_1, HID_i, and B_2 via a public channel, $\mathcal{A}$ still cannot obtain r_u because $\mathcal{A}$ cannot obtain B_1 and D_1. Therefore, $\mathcal{A}$ fails to calculate X_{UG}, cannot pass the authentication of GWN, and cannot imitate U_i for communication. Thus, LAP-IoHT can effectively resist user impersonation attacks.

4.2.3. Server Impersonation Attack

Suppose that $\mathcal{A}$ can obtain a smart card for U_i. However, $\mathcal{A}$ does not know the value of SID_j and the private key G_j of the gateway; therefore, $\mathcal{A}$ cannot pass the authentication of SN_j by computing X_{GS} and cannot successfully imitate the gateway. Hence, our protocol can defend against server impersonation attacks.

4.2.4. Privileged Insider Attack

If $\mathcal{A}$ is an insider of GWN, $\mathcal{A}$ can obtain HID_i, D_1, SID_j, and PID_j, which are stored in the database of GWN. However, $\mathcal{A}$ cannot successfully obtain the session key because he or she does not know r_u, r_g, and r_s. Thus, the proposed protocol can defend against privileged insider attacks. Therefore, we can state that the proposed protocol is secure against insider attacks.

4.2.5. Known Session Specific Temporary Information Attack

We assume that the temporary random number r_u is obtained using $\mathcal{A}$. If $\mathcal{A}$ wishes to calculate the session key SK, three parameters r_u, r_g, and r_s are required. However, $\mathcal{A}$ cannot know r_g because he or she cannot obtain PID_j. Furthermore, $\mathcal{A}$ cannot obtain r_s. Thus, our protocol is not affected by temporary information leakage.

4.2.6. Stolen Smart Card Attack

$\mathcal{A}$ obtains $\{D_1, D_3, D_4, \Omega_i, M\}$ stored in the smart card that he or she has stolen. Even if $\mathcal{A}$ knows B_2 and D_1, $\mathcal{A}$ cannot obtain B_1 because he or she cannot obtain G_j. This implies that $\mathcal{A}$ cannot pass the server verification let alone establish a communication session key with GWN. Thus, LAP-IoHT is resistant against smart card theft attacks.

4.2.7. Perfect Forward Security

If $\mathcal{A}$ knows the G_j of the gateway when calculating the random number $r_u = B_1 \oplus B_2$, B_2 can intercept the transmitted information and the other parameter $B_1 = h(D_1 \parallel G_j)$. G_j is already known by $\mathcal{A}$, but as $D_1 = h(HID_i \parallel N)$, $\mathcal{A}$ cannot obtain N and HID_i and, hence, cannot know D_1. Since $\mathcal{A}$ cannot calculate r_u, he or she cannot obtain session key SK. Therefore, our protocol provides perfect forward security.

4.3. ROR Security Analysis

The ROR (Real-or-Random) model is a widely used security-proof method. The ROR model can obtain the probability of successfully breaking session key SK through several different game rounds. Therefore, we use the ROR model to perform a formal security analysis to demonstrate the security and accuracy of the protocol.

4.3.1. ROR Model

Our protocol comprises three entities: U_i, GWN, and S_j. We use $\Pi^x_{U_i}$, Π^y_{GWN}, and $\Pi^z_{S_j}$ to denote the x-th user, y-th gateway, and z-th sensor nodes, respectively, such that $R = \{\Pi^x_{U_i}, \Pi^y_{GWN}$, and $\Pi^z_{S_j}\}$. Suppose that attacker $\mathcal{A}$ can execute the following queries:

$Execute(R)$: When this query is executed, $\mathcal{A}$ can intercept the messages that are transmitted among entities U_i, GWN, and S_j over the public channel.

$Send(R, M)$: By executing this query, $\mathcal{A}$ can send message M to R and receive the response message from R.

$Hash(String)$: Through this operation, $\mathcal{A}$ can obtain the hash value of a fixed-length string after inputting it.

$Corrupt(R)$: By executing this query, $\mathcal{A}$ obtains the private value of an entity, such as long-term key, generated temporary information, or parameters that are stored in a smart card.

$Test(R)$: Assume that $\mathcal{A}$ executes this query and can determine the security of the session key by tossing coin C. If C = 1, $\mathcal{A}$ obtains the correct session key. Otherwise, $\mathcal{A}$ receives a random string.

Theorem 1: In the ROR model, we use $Adv^{\mathcal{P}}_{\mathcal{A}}$ as a function of the attacker's ability to compromise the protocol through query operations; that is, the probability that $\mathcal{A}$ can obtain the session key $Adv^{\mathcal{P}}_{\mathcal{A}} \leq q_h^2/|H| + q_s/2^{t-1}|D|$, where q_h and q_s represent the number of times to perform the $Hash$ and $Send$ queries, respectively, $|H|$ and $|D|$ represent the space range and dictionary size corresponding to the hash operation, respectively, and t represents the number of bits of biological information in the protocol.

4.3.2. Security Proof

To prove the accuracy of Theorem 1, we performed four rounds of game $GM_i(i = 0, 1, 2, 3)$, where $Succ^{GM_i}_{\mathcal{A}}$ denotes the probability of the attacker $\mathcal{A}$ winning in each round of the game. The details of the game are as follows.

GM_0: At the beginning of the game, $\mathcal{A}$ only needs to determine bit b and does not perform any query operation. Therefore, we can obtain

$$Adv^{\mathcal{P}}_{\mathcal{A}} = |2Pr[Succ^{GM_0}_{\mathcal{A}}] - 1|. \tag{1}$$

GM_1: GM_1 performs a wiretap operation on top of GM_0. In this round, $\mathcal{A}$ can only steal messages that are transmitted on the common channels $\{HID_i, B_2, X_{UG}, T_1\}$, $\{B_4, B_5, B_6, X_{GS}, T_2\}$, $\{B_8, X_{SG}, X_{SU}, T_3\}$, and $\{B_5, B_{10}, B_{11}, X_{GU}, X_{SU}, T_4\}$. $\mathcal{A}$ cannot execute the $Test$ queries to obtain the session key $SK = h(r_u \parallel r_g \parallel r_s)$ during communication because the values of the random numbers r_u, r_g, and r_s cannot be obtained based only on the information in the common channels. Therefore, the probability of $\mathcal{A}$ winning the game after performing an *Execute* query is equal to GM_0.

$$Pr[Succ_{\mathcal{A}}^{GM_1}] = Pr[Succ_{\mathcal{A}}^{GM_0}]. \tag{2}$$

GM_2: GM_2 is the third round of the game, in which the *Hash* query and *Send* operation have already occurred in GM_1. During the game, forgery is not possible because B_4, X_{UG}, B_4, B_5, X_{GS}, B_11, X_{SG}, X_{SU}, and X_{GU} are encrypted using hash functions. Moreover, the important parameters r_u, r_g, and r_s, which constitute the session key, are random in all sessions and do not cause hash conflicts. Thus, according to the birthday paradox, we obtain

$$|Pr[Succ_{\mathcal{A}}^{GM_2}] - Pr[Succ_{\mathcal{A}}^{GM_1}]| \leq q_h^2/2|H|. \tag{3}$$

GM_3: In this round, the *Corrupt* query is executed and the attacker $\mathcal{A}$ can obtain the private value of an entity, such as $\{SG, L\}$, $\{D_1, D_3, D_4, \Omega_i, M\}$, or $\{SID_j, PID_j, HID_i, D_1\}$. Moreover, $\mathcal{A}$ attempts to guess ID_i and PW_i; however, even if $\mathcal{A}$ can successfully guess ID_i and PW_i simultaneously, he or she still cannot obtain the random number r_u. Since $r_u = B_1 \oplus B_2$, $B_1 = D_3 \oplus N \oplus HPW_i$, $N = PW_i \oplus h(ID_i \parallel \sigma_i)$, $\sigma_i = Rep(Bio, \tau_i)$, and the probability of the biometric being estimated is $1/2^t$, $\mathcal{A}$ cannot obtain the biological eigenvalue Bio. If $\mathcal{A}$ can only enter the code a finite number of times, we know that

$$|Pr[Succ_{\mathcal{A}}^{GM_3}] - Pr[Succ_{\mathcal{A}}^{GM_2}]| \leq q_s/2^t|D|. \tag{4}$$

Since $\mathcal{A}$ can only win the game if the correct bit b is guessed, we obtain

$$|Pr[Succ_{\mathcal{A}}^{GM_3}]| = 1/2. \tag{5}$$

Using Equations (1)–(5) above, we obtain

$$\begin{aligned} &1/2Adv_{\mathcal{A}}^{\mathcal{P}} = |Pr[Succ_{\mathcal{A}}^{GM_0}] - 1/2| \\ &= |Pr[Succ_{\mathcal{A}}^{GM_1}] - Pr[Succ_{\mathcal{A}}^{GM_3}]| \\ &\leq |Pr[Succ_{\mathcal{A}}^{GM_2}] - Pr[Succ_{\mathcal{A}}^{GM_1}]| + |Pr[Succ_{\mathcal{A}}^{GM_3}] - Pr[Succ_{\mathcal{A}}^{GM_2}]| \\ &= q_h^2/2|H| + q_s/2^t|D|. \end{aligned} \tag{6}$$

Ultimately, we can obtain $Adv_{\mathcal{A}}^{\mathcal{P}} \leq q_h^2/|H| + q_s/2^{t-1}|D|$.

4.4. Security Comparisons

We compare LAP-IoHT with other related protocols with similar architectures, such as those of Kumar et al. [43], Yu et al. [44], Amin et al. [36], Challa et al. [37], Aghili et al. [39], and Preeti et al. [38]. We set the following representations: A1: resist replay attack; A2: resist impersonation attack; A3: resist privileged insider attack; A4: perfect forward security; A5: resist known session specific temporary information attack; A6: resist stolen smart card attack; A7: resist offline password guessing attack; A8: resist sensor node capture attack; A9: resist de-synchronization attack; A10: resist session key disclosure attack. "Y" indicates that the protocol is invulnerable to this attack, and "N" indicates that the protocol is vulnerable to this attack. The results in Table 3 demonstrate that, with the continual development of technology and various attack methods, the other related protocols will be affected by the above attacks. Compared to these protocols, our method exhibits better security and sufficient advantages in resisting the above attacks to guarantee the security of communication sessions.

Table 3. Comparisons of security.

Protocols	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Ours	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Kumar et al. [43]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Yu et al. [44]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
Amin et al. [36]	*Y*	*Y*	*N*	*Y*	*Y*	*Y*	*N*	*Y*	*Y*	*Y*
Challa et al. [37]	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*N*	*Y*	*Y*
Preeti et al. [38]	*Y*	*Y*	*Y*	*N*	*Y*	*Y*	*Y*	*N*	*Y*	*Y*
Aghili et al. [39]	*Y*	*N*	*N*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*

5. Performance Comparison

In this section, we evaluate the performance of the proposed LAP-IoHT protocol by performing comparisons with other protocols, such as those proposed by Kumar et al. [43], Yu et al. [44], Amin et al. [36], Challa et al. [37], Aghili et al. [39], and Preeti et al. [38], in terms of the computation time and communication cost.

We used different devices to obtain the computation time and communication cost required for the certification stage in the performance comparison. We used a mobile phone, laptop computer, and desktop computer to simulate the user, gateway, and sensor nodes, respectively. The relevant parameters for the three devices are listed in Table 4. Table 5 presents the times required by different devices to perform certain operations. T_H denotes the time required to perform a single hash function operation, T_{SED} denotes the time required to perform a single symmetric encryption or decryption operation, T_{FE} denotes the time required to perform a single fuzzy extraction operation, T_{ASED} denotes the time required to perform a single asymmetric encryption or decryption operation, T_S denotes the time required to execute the digital signature operation, and T_{PM} denotes the time required to perform an elliptic curve point multiplication operation. As the communication times required by the connection and XOR operations are insignificant compared to the other operations, these can be ignored. Table 6 presents a comparison of the communication times of our proposed protocol and other similar protocols. Several communication costs arise in the communication process, and asymmetric encryption or decryption has an enormous overhead of 1024 bits. The length required for the elliptic curve point multiplication operation is 320 bits; the length of each block for symmetric encryption or decryption is 256 bits; the hash values and random numbers all have similar lengths of 160 bits; the identity, password, and biometrics are all 128 bits in length; the timestamps require a length of 32 bits. In Table 7, we compare the communication overheads of multiple protocols to determine the specific communication cost.

Table 4. Parameters of the devices.

Devices	Model	Operating System	Memory	Processor
mobile phone	MI 8	Android	6 GB	Qualcomm Snapdragon 845
laptop computer	DELL G15 5510	Windows 10	16 GB	Intel(R) Core(TM)i7-10870H
desktop computer	LENOVO 90M2A0A6CD	Windows 10	8 GB	Intel(R) Core(TM)i5-9500

Table 5. Execution time of operations.

Operations	MI 8	DELL G15 5510	LENOVO 90M2A0A6CD
T_{FE}	20.7028 ms	2.2823 ms	1.6197 ms
T_{ASED}	47.6405 ms	5.2520 ms	3.7272 ms
T_{PM}	0.00044 ms	16 ms	13 ms
T_{SED}	0.2009 ms	0.1551 ms	0.0879 ms
T_H	0.02812 ms	0.0031 ms	0.0022 ms
T_S	69 ms	270 ms	139 ms

Table 6. Comparison of time.

Protocols	*User*	*Gateway*	*Sensor Node*	Total Computation (ms)
Ours	$T_{FE} + 10T_H$	$14T_H$	$T_{ASED} + 7T_H$	24.77
Kumar et al. [43]	$2T_{PM} + 8T_H + 2T_S + 3T_{SED}$	$T_{SED} + 3T_H$	$T_{PM} + 10T_H + 2T_S + 2T_{SED}$	370.19074
Yu et al. [44]	$T_{FE} + 9T_H$	$9T_H$	$7T_H$	20.99918
Amin et al. [36]	$T_{SED} + 4T_{PM} + 7T_H$	$T_{SED} + 2T_{PM} + 6T_H$	$2T_{SED} + 3T_{PM} + 4T_H$	71.7578
Challa et al. [37]	$T_{FE} + 2T_{PM} + 9T_H$	$T_{PM} + 4T_H$	$6T_H$	36.9824
Preeti et al. [38]	$T_{FE} + 3T_{PM} + 15T_H$	$3T_{PM} + 11T_H$	$5T_H$	69.171
Aghili et al. [39]	$T_{FE} + 12T_H$	$16T_H$	$4T_H$	21.09864

Table 7. Comparison of cost.

Protocols	*User*	*Gateway*	*Sensor Node*	Total Communication Cost (bits)	Number of Messages
Ours	480	1504	512	2496	4
Kumar et al. [43]	1824	3424	1472	6720	4
Yu et al. [44]	672	1216	672	2560	5
Amin et al. [36]	960	1280	800	3040	4
Challa et al. [37]	832	224	352	1408	3
Preeti et al. [38]	832	1088	352	2272	4
Aghili et al. [39]	800	864	4352	2016	4

5.1. Computation Time

We use three devices to determine the computation time and communication cost. The times required to perform elliptic curve point multiplication, symmetric encryption/decryption, asymmetric encryption/decryption, single fuzzy extraction, and hash functions vary on different devices. Furthermore, the computation times required for the connection and XOR operations are insignificant compared to the other operations; thus, we ignore these in our evaluation.

The computation times of the proposed protocol and other similar protocols are listed in Table 6. Table 6 shows the computation costs of all protocols. The most time-consuming protocol is the protocol proposed by Kumar et al. [43], which includes elliptic curve point multiplication and digital signature operations. The protocol proposed by Yu et al. [44] is the least time consuming. Although our proposed protocol includes fuzzy extraction and asymmetric operations in the login and authentication processes, its computation time is relatively short.

5.2. Communication Cost

We assume that the output of asymmetric encryption/decryption is 1024 bits; the length required for the elliptic curve point multiplication operation is 320 bits; each block for symmetric encryption/decryption is 256 bits; the hashed value and random number are 160 bits; the identity, password, and biometrics are all 128 bits in length; the timestamps require a length of 32 bits.

According to Table 7, we can determine the communication costs of all the protocols. The communication costs of the protocols proposed by Kumar et al. [43], Yu et al. [44], Amin et al. [36], Challa et al. [37], Aghili et al. [39], and Preeti et al. [38] are 6720 bits (256 ∗ 7 + 32 + 256 ∗ 6 + 32 + 256 ∗ 7 + 32 + 32 + 256 ∗ 5 + 160 + 32), 2560 bits (160 + 160 + 160 + 160 + 32 + 160 + 160 + 32 + 160 + 160 + 160 + 32 + 160 + 160 + 32 + 160 + 160 + 160 + 160 + 32, 3040 bits (128 + 320 + 160 + 160 + 32 + 160 + 256 ∗ 3 + 320 + 32 + 256hl∗3 + 32 + 160), 1408 bits (160 + 160 + 320 + 160 + 32 + 160 + 32 + 32 + 160 + 160 + 32), 2272 bits (160 + 160 + 160 + 320 + 32 + 160 + 160 + 32 + 32 + 160 + 160 + 320 + 32 + 32 + 160 + 160 + 32), and 2016 bits (160 + 160 + 160 + 160 + 128 + 32 + 160 + 160 + 160 + 32 + 160 + 160 + 32 + 160 + 160 + 32), respectively. The communication cost of our proposed protocol is 2496 bits (128 + 160 + 160 + 32 + 160 + 160 + 160 + 160 + 32 + 160 + 160 + 160 + 32 + 160 + 160 + 160 + 160 + 160 + 32).

Figures 5 and 6 compare the LAP-IoHT protocol with the other related protocols in terms of the computation times and communication costs. Although the communication costs of the LAP-IoHT protocol are higher than those of the protocols proposed by Challa et al. [37], Aghili et al. [39], and Preeti et al. [38], the run time of LAP-IoHT is much lower [37,38]. Moreover, the security of LAP-IoHT is higher than those of all three [37–39]. Furthermore, although the protocols proposed by Kumar et al. [43] and Yu et al. [44] are more secure, they do not offer any advantages in terms of communication costs. Therefore, it is easy to conclude that LAP-IoHT performs better than the related protocols. More importantly, it can be observed from Table 3 that LAP-IoHT has excellent security advantages. It can effectively resist various attacks, thereby providing security for communication sessions.

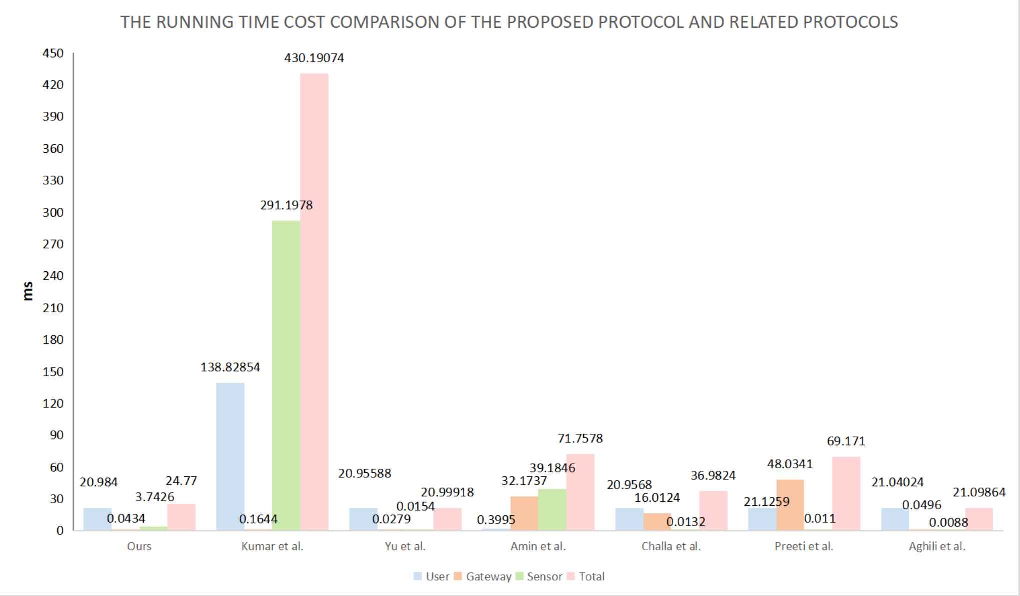

Figure 5. Running times.

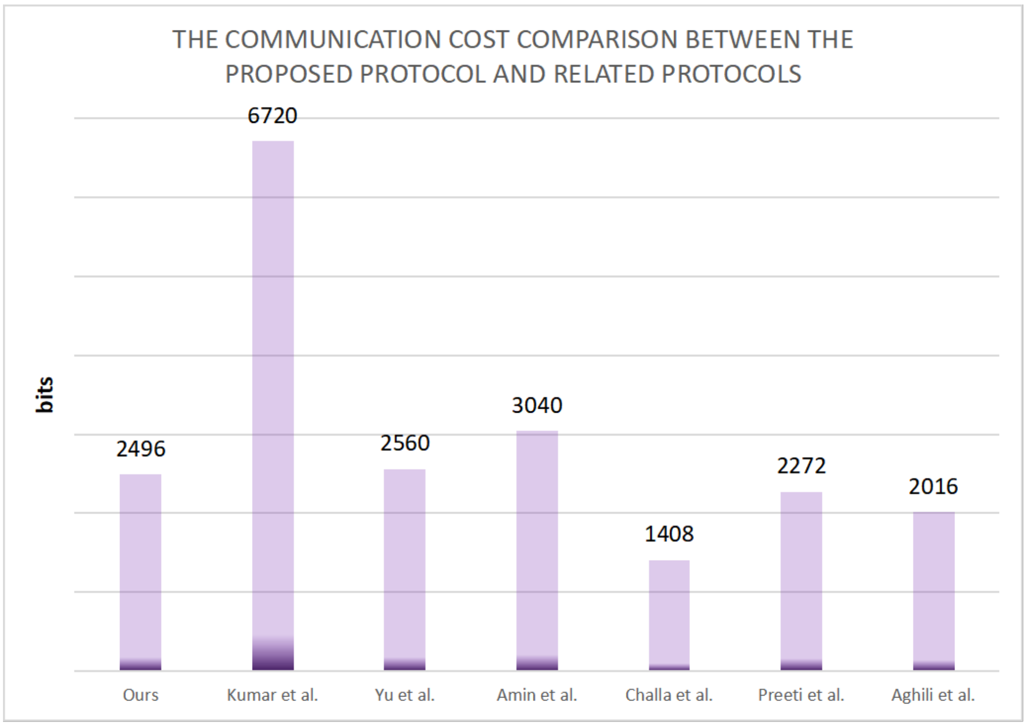

Figure 6. Communication costs.

6. Conclusions

Internet of Health Things (IoHT), which promotes intelligent healthcare, plays a pivotal role in the future e-healthcare environment. Due to its high sensitivity, the health data transmitted through a public channel should be protected from unauthorized access. This means that an authentication protocol is essential. This paper presented a more secure and reliable authentication protocol called LAP-IoHT for the Internet of Health Things. LAP-IoHT provides mutual authentication among users, sensors, and a gateway over a public channel. Moreover, a user and a sensor can establish a common session key after a protocol run. By using the ROR model and performing an informal analysis, it was proven that LAP-IoHT has adequate security and reliability as well as sufficient ability to resist various attacks. Furthermore, we compared LAP-IoHT with related protocols and found that our protocol is at the mid-to-upstream level in terms of time and communication costs, exhibiting a significant performance advantage. In summary, the proposed protocol offers specific practical value in the current environment and has more robust adaptability relative to the future development of IoHT.

Author Contributions: Conceptualization: C.-M.C. and Z.C.; methodology: C.-M.C. and Z.C.; formal analysis: S.K. and M.-C.L.; investigation: M.-C.L.; and writing—original draft preparation: C.-M.C., Z.C., S.K. and M.-C.L. All authors have read and agreed to the published version of the manuscript.

Funding: The authors received no specific funding for this study.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things;
WSN	Wireless sensor network;
IoHT	Internet of Health Things;
ECG	Electrocardiogram;
EMG	Electromyography;
EEG	Electroencephalogram;
DY	Dolev–Yao;
ROR	Real-or-Random;
XOR	Exclusive OR;
DoS	Denial of service.

References

1. Huang, X.; Xiong, H.; Chen, J.; Yang, M. Efficient Revocable Storage Attribute-based Encryption with Arithmetic Span Programs in Cloud-assisted Internet of Things. *IEEE Trans. Cloud Comput.* **2021**. [CrossRef]
2. Liu, G.; Zhu, Y.; Xu, S.; Chen, Y.C.; Tang, H. PSO-based power-driven X-routing algorithm in semiconductor design for predictive intelligence of IoT applications. *Appl. Soft Comput.* **2022**, *114*, 108114. [CrossRef]
3. Chen, X.; Zhang, J.; Lin, B.; Chen, Z.; Wolter, K.; Min, G. Energy-efficient offloading for DNN-based smart IoT systems in cloud-edge environments. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *33*, 683–697. [CrossRef]
4. Shen, S.; Yang, Y.; Liu, X. Toward data privacy preservation with ciphertext update and key rotation for IoT. *Concurr. Comput. Pract. Exp.* **2021**, e6729. [CrossRef]
5. Cheng, H.; Shi, Y.; Wu, L.; Guo, Y.; Xiong, N. An intelligent scheme for big data recovery in Internet of Things based on multi-attribute assistance and extremely randomized trees. *Inf. Sci.* **2021**, *557*, 66–83. [CrossRef]
6. Cheng, H.; Wu, L.; Li, R.; Huang, F.; Tu, C.; Yu, Z. Data recovery in wireless sensor networks based on attribute correlation and extremely randomized trees. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 245–259. [CrossRef]
7. Zou, W.; Guo, L.; Huang, P.; Lin, G.; Mei, H. Linear time algorithm for computing min-max movement of sink-based mobile sensors for line barrier coverage. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6175. [CrossRef]
8. Chu, S.C.; Dao, T.K.; Pan, J.S. Identifying correctness data scheme for aggregating data in cluster heads of wireless sensor network based on naive Bayes classification. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 52. [CrossRef]
9. Xue, X.; Jiang, C. Matching Sensor Ontologies with Multi-Context Similarity Measure and Parallel Compact Differential Evolution Algorithm. *IEEE Sens. J.* **2021**, *21*, 24570–24578. [CrossRef]
10. Fan, F.; Chu, S.C.; Pan, J.S.; Lin, C.; Zhao, H. An optimized machine learning technology scheme and its application in fault detection in wireless sensor networks. *J. Appl. Stat.* **2021**, 1–18. [CrossRef]
11. Wei, D.; Xi, N.; Ma, X.; Shojafar, M.; Kumari, S.; Ma, J. Personalized Privacy-aware Task Offloading for Edge-Cloud-Assisted Industrial Internet of Things in Automated Manufacturing. *IEEE Trans. Ind. Inform.* **2022**. [CrossRef]
12. Xiaojun, C.; Xianpeng, L.; Peng, X. IOT-based air pollution monitoring and forecasting system. In Proceedings of the 2015 International Conference on Computer and Computational Sciences (ICCCS), Greater Noida, India, 27–29 January 2015; pp. 257–260.
13. Nikooghadam, M.; Amintoosi, H.; Islam, S.H.; Moghadam, M.F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *J. Syst. Archit.* **2021**, *115*, 101955. [CrossRef]
14. Yu, Z.; Zheng, X.; Huang, F.; Guo, W.; Sun, L.; Yu, Z. A framework based on sparse representation model for time series prediction in smart city. *Front. Comput. Sci.* **2021**, *15*, 151305. [CrossRef]
15. Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Zikria, Y.B. A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System. *IEEE Trans. Intell. Transp. Syst.* **2021**. [CrossRef]
16. Xiong, H.; Chen, J.; Mei, Q.; Zhao, Y. Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs. *IEEE Trans. Dependable Secur. Comput.* **2020**, 1. [CrossRef]
17. Dourado, C.M.; da Silva, S.P.P.; da Nobrega, R.V.M.; Reboucas Filho, P.P.; Muhammad, K.; de Albuquerque, V.H.C. An open IoHT-based deep learning framework for online medical image recognition. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 541–548. [CrossRef]
18. Rahman, M.A.; Hossain, M.S.; Showail, A.J.; Alrajeh, N.A.; Alhamid, M.F. A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. *Sustain. Cities Soc.* **2021**, *72*, 103083. [CrossRef]
19. Chaudhry, S.A.; Irshad, A.; Nebhen, J.; Bashir, A.K.; Moustafa, N.; Al-Otaibi, Y.D.; Zikria, Y.B. An anonymous device to device access control based on secure certificate for internet of medical things systems. *Sustain. Cities Soc.* **2021**, *75*, 103322. [CrossRef]
20. Wu, T.Y.; Wang, T.; Lee, Y.Q.; Zheng, W.; Kumari, S.; Kumar, S. Improved authenticated key agreement scheme for fog-driven IoT healthcare system. *Secur. Commun. Netw.* **2021**, *2021*, 6658041. [CrossRef]
21. Xiong, H.; Hou, Y.; Huang, X.; Zhao, Y.; Chen, C.M. Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs. *IEEE Syst. J.* **2021**, *16*, 2391–2400. [CrossRef]

22. Wu, T.Y.; Yang, L.; Meng, Q.; Guo, X.; Chen, C.M. Fog-driven secure authentication and key exchange scheme for wearable health monitoring system. *Secur. Commun. Netw.* **2021**, *2021*, 8368646. [CrossRef]
23. Chen, C.M.; Li, Z.; Chaudhry, S.A.; Li, L. Attacks and solutions for a two-factor authentication protocol for wireless body area networks. *Secur. Commun. Netw.* **2021**, *2021*, 3116593. [CrossRef]
24. Reddy, G.T.; Kaluri, R.; Reddy, P.K.; Lakshmanna, K.; Koppu, S.; Rajput, D.S. A novel approach for home surveillance system using IoT adaptive security. In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur, India, 26–28 February 2019.
25. Jian, M.S.; Wu, J.M.T. Hybrid Internet of Things (IoT) data transmission security corresponding to device verification. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–10. [CrossRef]
26. Yang, Y.; Zheng, X.; Guo, W.; Liu, X.; Chang, V. Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Inf. Sci.* **2019**, *479*, 567–592. [CrossRef]
27. Pereira, F.; Crocker, P.; Leithardt, V.R. PADRES: Tool for PrivAcy, Data REgulation and Security. *SoftwareX* **2022**, *17*, 100895. [CrossRef]
28. Onasanya, A.; Elshakankiri, M. Smart integrated IoT healthcare system for cancer care. *Wirel. Netw.* **2021**, *27*, 4297–4312. [CrossRef]
29. Sun, Y.; Liu, J.; Yu, K.; Alazab, M.; Lin, K. PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1981–1990. [CrossRef]
30. Zhang, Y.; Sun, Y.; Jin, R.; Lin, K.; Liu, W. High-performance isolation computing technology for smart IoT healthcare in cloud environments. *IEEE Internet Things J.* **2021**, *8*, 16872–16879. [CrossRef]
31. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Appl. Sci.* **2020**, *2*, 139. [CrossRef]
32. Alassaf, N.; Gutub, A. Simulating light-weight-cryptography implementation for IoT healthcare data security applications. *Int. J. Health Med Commun. (IJEHMC)* **2019**, *10*, 1–15. [CrossRef]
33. Kumari, A.; Kumar, V.; Abbasi, M.Y.; Kumari, S.; Chaudhary, P.; Chen, C.M. Csef: Cloud-based secure and efficient framework for smart medical system using ecc. *IEEE Access* **2020**, *8*, 107838–107852. [CrossRef]
34. Hossein, K.M.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. *Comput. Commun.* **2021**, *180*, 31–47. [CrossRef]
35. Wang, K.; Chen, C.M.; Tie, Z.; Shojafar, M.; Kumar, S.; Kumari, S. Forward Privacy Preservation in IoT-Enabled Healthcare Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1991–1999. [CrossRef]
36. Amin, R.; Islam, S.; Biswas, G.; Khan, M.K.; Kumar, N. An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography. *J. Med. Syst.* **2015**, *39*, 180. [CrossRef] [PubMed]
37. Challa, S.; Das, A.K.; Odelu, V.; Kumar, N.; Kumari, S.; Khan, M.K.; Vasilakos, A.V. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Comput. Electr. Eng.* **2018**, *69*, 534–554. [CrossRef]
38. Preeti, S.; Arup, K.P.; SK, H.I. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. *Comput. Methods Programs Biomed.* **2019**, *182*, 105504.
39. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [CrossRef]
40. Amintoosi, H.; Nikooghadam, M.; Shojafar, M.; Kumari, S.; Alazab, M. Slight: A lightweight authentication scheme for smart healthcare services. *Comput. Electr. Eng.* **2022**, *99*, 107803. [CrossRef]
41. Gupta, A.; Tripathi, M.; Shaikh, T.J.; Sharma, A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Comput. Netw.* **2019**, *149*, 29–42. [CrossRef]
42. Hajian, R.; ZakeriKia, S.; Erfani, S.H.; Mirabi, M. SHAPARAK: Scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement. *Comput. Netw.* **2020**, *183*, 107567. [CrossRef]
43. Kumar, V.; Mahmoud, M.S.; Alkhayyat, A.; Srinivas, J.; Ahmad, M.; Kumari, A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. *J. Supercomput.* **2022**, 1–30. [CrossRef] [PubMed]
44. Yu, S.; Park, Y. A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions. *IEEE Internet Things J.* **2022**. [CrossRef]
45. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]