Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 1044282, 15 pages
https://doi.org/10.1155/2023/1044282

Research Article

A Lightweight Three-Party Mutual Authentication Protocol for Internet of Health Things Systems

Zhihui Wang,[1] Jianli Zhao,[2] Peng Sun,[1] Jingjing Yang,[1] Rui Wang,[1] and Xiao Zhang[1]

[1] *Hebei North University, Zhangjiakou 07500, Hebei, China*
[2] *State Grid Hebei Electric Power Research Institute, Shijiazhuang 050000, Hebei, China*

Correspondence should be addressed to Xiao Zhang; xzh1965@hebeinu.edu.cn

Received 10 February 2022; Revised 11 April 2022; Accepted 15 April 2022; Published 22 February 2023

Academic Editor: Muhammad Asghar Khan

In Internet of Health Things (IoHT) systems, there is a two-hop network structure between the authentication server TA, Internet of Things Connector (IotC), and wearable sensor (WS). Attackers can use the sensor layer network (the first hop) between the IotC and WS to steal patient's health-related information and undermine the security of the system and the privacy of sensitive information. To address this threat, this study proposes a lightweight identity authentication and key agreement protocol for third-party authentication servers TA, IotC, and WS. The results of the formal security proof, BAN logic analysis, and AVISPA tool simulation show that the scheme proposed in this study has an ideal security performance and can meet the security requirements of IoHT. In terms of performance, the proposed scheme could dynamically construct a sensor layer network (the first hop) and offline networking according to the diagnostic needs of doctors. Compared with other related protocols, the proposed scheme can significantly reduce the computing resource requirements of IotC and server TA and the resource requirements of database I/O operation of server TA in the application scenario of concurrent access of multiple WS nodes.

1. Introduction

The wearable technology market has reached US $116.2 billion in 2020 and is expected to increase to US $265.4 billion by 2026, with an annual compound growth rate of 18.0% [1]. The rapid growth of the market scale of wearable technology is also constantly promoting the integration of wearable or implantable device technology with IoT, cloud computing, and other information technologies into Internet of Health Things (IoHT) systems in the hospital environment [2]. These new technologies can help medical professionals obtain various types of health data information of target patients faster and better [3] and help medical institutions continuously improve the quality of medical services [4].

Figure 1 describes the general network structure of IoHT systems applied in the medical structure environment [5–8]. Its remarkable feature is the integration of the IoT, cloud computing, wearable, or implantable device technology. As shown in Figure 1, an IoHT system is composed of two interconnected network units: a data service unit and IoT unit. They are connected through a common set of cloud data storage servers.

The IoT unit is a two-hop network structure, similar to the IEEE 802.15.6 Wireless Body Area Network (WBAN) standard description [9] and the industrial Internet of Things [10]. Multiple wearable sensors (WSs) and Internet of Things Connectors (IotCs) constitute the first hop of an IoHT system, that is, the sensor layer network. The IotC and local real-time data monitoring terminal (LMT) or cloud data server form the second-hop transport layer network. In terms of function, it emphasizes the ability of real-time, fast, and accurate acquisition and two-way data transmission of Patient Health Information (PHI) [5, 8, 11], such as patient activity, blood pressure, heart rate, electrocardiogram (ECG), temperature, blood glucose, and blood oxygen level [12].

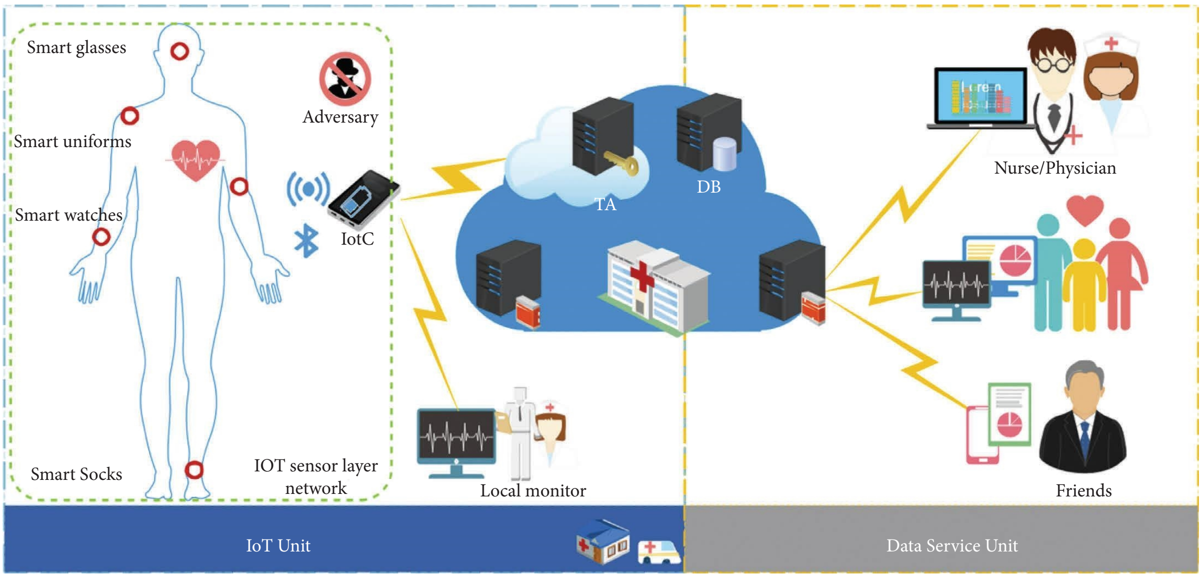


Figure 1: Network structure of the IoHT system.

1.1. Networking Requirements of Sensor Layer Networks. The main application environment of IoHT systems is the medical institutions that provide public medical and health services. Patients have a strong mobility and various other conditions. Therefore, the IoHT systems must collect the corresponding PHI data according to a patient's condition such as monitoring of blood glucose levels and blood pressure. Some data require a high real-time performance, such as heart rate data in intensive care or cardiac care environments. These have put forward the following special functional requirements or limitations for the network structure of the sensing layer of the IoHT systems:

(i) WS and IotC are small in size, easy to carry, and have limited computing resources; therefore, they are not suitable for jobs with a high amount of computing [13].

(ii) The correspondence between the patients and IotC was variable. The IotC ownership in IoHT systems is a medical institution that has a corresponding relationship with patients within a certain time range.

(iii) The types and number of WS nodes are large, and the server in the IoHT systems should have strong equipment access capability.

(iv) The WS nodes are rarely used in isolation. In most cases, these groups were included. IotC should be able to concurrently network multiple WSs.

(v) The combination of IotC and WS must be built according to the diagnostic needs of doctors [7].

(vi) To reduce the impact of remote network quality on IoHT system availability, the IotC and WS should have offline networking capabilities.

1.2. Requirements of IoHT Systems Lightweight Authentication Strategy. The correctness, timeliness, and credibility of PHIs can support doctors' decision making and help save or prolong patients' lives [14]. However, many theft events in PHI data [4] make the security of PHIs a hot issue for healthcare organizations. The Health Insurance, Portability, and Accounting Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) require all healthcare organizations to ensure the safety of health information.

Network attacks against IoT terminal devices, such as webcams [15], small routers [16], bluetooth door locks [17], intelligent thermostats [18], and theft of face recognition data [19], have made people gradually realize that IoT devices in IoHT systems may become a tool for attackers to launch network attacks and destroy the stability of IoHT systems or steal user-sensitive information.

The mutual Authentication and Key Agreement (AKA) mechanism between IoT access devices is an important link for building a secure health system (SHS) [20]. The VPN, SSL, TLS, and other security mechanisms are based on the Internet peer-to-peer communication mechanism, which can ensure data security on both sides, for example, the establishment of a secure data channel between the IotC and the data server [21]. However, because of the two-hop network structure of the IoT unit of IoHT systems and the networking requirements of the sensor layer network, it is very difficult to use VPN, SSL, TLS, and other protocols to build a mutual AKA in the first-hop network (sensor layer network). Therefore, the IoHT systems require a lightweight, anonymous, and secure mutual AKA protocol, that is, more suitable for network structures [22].

2. Related Work

The special structure and functional requirements of IoHT systems restrict their application in traditional security protocols. To deal with the threat of malicious attacks, improve the security level of IoHT systems, and meet the functional requirements of portable and ultralow power consumption of wearable sensors, various lightweight mutual AKAs have been proposed.

In 2015, He and Zeadally proposed a lightweight three-party authentication protocol to improve the identity authentication ability of controllers in ambient-assisted living systems [23]. Subsequently, in 2016, with the help of a third-party authentication server, He et al. realized lightweight identity authentication of users using a data aggregation device in the smart grid [24]. The two protocols are based on the elliptic curve (EC) theory and realize the support of third-party authentication servers; therefore, they have low overall resource consumption and high security, but the individual resource consumption of the controller is still high, and the support for sensing devices is insufficient.

In 2017, Li et al. [9] proposed an anonymous lightweight identity authentication and key agreement protocol for two-hop wireless body area networks (WBANs). The protocol is based on a hash function and XOR computing, which significantly reduces the demand for computing resources for wireless sensor devices. A hub node must undertake multiple functions, such as identity authentication, real-time data monitoring, data storage, and remote cloud data forwarding, which are not conducive to the implementation of a security protection strategy, is easier to capture, and has a single point of failure.

In 2018, Srinivas et al. [6] proposed a lightweight tripartite authentication scheme for WSs, users, and cloud servers based on cloud computing and big-data technology. The security of the scheme is verified using a formal real or random (ROR) model and the automatic verification tool AVISPA [25]. This scheme has significant advantages in terms of the communication and computing costs.

However, Srinivas' protocol must store the authentication information $\langle \mathrm{HID}_i, TC_{ji2} \rangle$ of all possible users in the memory of all the WSs in advance. This causes the wearable sensor of the protocol to have a large demand for storage resources and insufficient ability to resist WS theft attacks [16]. Simultaneously, we found that the construction of the sensor layer network of the protocol requires more manual processing, which is more suitable for networks with stable structures. Under the demand for on-demand construction of an IoHT system sensor layer network, labor and system maintenance costs will increase.

To enhance the ability of wearable devices to protect sensitive data and resist WSs theft attacks, Das et al. [5] proposed a lightweight tripartite authentication and session key scheme between WSs and mobile terminals (MT) (i.e., smartphones) carried by the same user. The security of the protocol was verified using a real or random model and AVISPA tool. Compared with the previous scheme, this method has certain advantages in terms of resource consumption. However, Jiang et al. [26] pointed out that the Das scheme does not resist offline password-guessing attacks, and attackers can use desynchronization attacks to destroy the synchronizer of identity update between WS and MT [26] and provided an improved scheme. Jiang's scheme offers advantages in terms of security and resource consumption. However, we also found that there were still some problems with Jiang's scheme.

(i) This method is suitable for application in personal health monitoring. In Jiang's scheme, the user is an MT and the WS is the owner, who lacks the basic function of adjusting the combination relationship of the user, MT, and WSs according to the patient's condition and the doctor's diagnostic needs.

(ii) There is a security risk in the denial-of-service (DOS). In Jiang's protocol, MT lacks the necessary verification for message M1, so attackers can use this to send many wrong M1, thus exhausting the computing, communication, and server database I/O resources of MT and the cloud server (CS) to achieve the purpose of DOS.

(iii) The computing resource requirements for concurrent MT access to multiple WS nodes must be improved. When the MT needs to access multiple WS nodes, the MT and CS have more repeated calculations and higher demand for computing resources.

(iv) The capability of offline networking between MTs and WSs must be improved. In the process of accessing the WS, the server CS must be online and provide corresponding services.

(v) The CS has a high demand for I/O database resources. Each time the MT accesses the WS, at least three queries and one database update operation are required. In an IoHT system environment, this may lead to a shortage of CS database resources, affect the number of WS nodes accessed, and weaken the server's ability to resist DoS attacks.

To enhance the ability of identity authentication between the Internet of Things connector (IotC) and local real-time data terminal, Srinivas et al. proposed a novel temporal credential-based anonymous lightweight user authentication mechanism for the Internet of Drones (IoD) environment [27]. The security of the scheme is proved using a real or random (ROR) model and automated validation of Internet security protocols and applications (AVISPA). However, this scheme does not support the dynamic construction of a sensor layer network. In 2020, Wang et al. [7] proposed a lightweight WSs and WNC mutual authentication protocol based on the elliptic curve cryptography (ECC) algorithm. With the help of a cloud-assisted authentication service, the protocol can realize mutual authentication and key negotiation of a wearable network connector (WNC) access to WSs designated by doctors. However, this scheme has shortcomings in terms of protection against ID. The attacker uses this to track the specified WSs and obtain sensitive data by analyzing the communication frequency and data volume. However, compared to the schemes of Srinivas, DAS, and Jiang, the resource consumption of their sensing terminals remains high.

3. Preliminaries

3.1. Elliptic Curve (EC). Let E be an elliptic curve over a finite field F_p defined by the following equation: $y^2 = x^3 + ax + b (\mathrm{mod}\, p)$, where $x, y, a, b \in F_p$ and $(4a^3 + 27b^2) \mathrm{mod}\, p \neq 0$. $E(F_p)$ represents a cyclic group constructed from points on elliptic curve E and infinity ∞.

3.2. Scalar Multiplication. When $P \in E(F_p)$, there is a multiplication formula: $t \cdot P = P + P + \ldots + P(t\,\text{times})$ holds.

3.3. Elliptic Curve Discrete Logarithm Problem (ECDLP). When $P \in E(F_p)$ and integer t are known, it is easy to calculate $= t \cdot P$, where $Q \in E(F_p)$. When Q and P are known, it is very difficult to calculate the value of the integer t.

3.4. Elliptic Curve Cryptography (ECC). A public-key algorithm based on ECDLP security is called elliptic curve cryptography (ECC). Compared with RSA, ECC requires fewer computing and storage resources [28, 29].

3.5. Elliptic Curve Diffie–Hellman Discrete Logarithm Problem (ECDHDLP). Assuming $c, d \in F_p$ and $G, c \cdot G, d \cdot G \in E(F_p)$, when the values of c and $d \cdot G$ or d and $c \cdot G$ are known, it is easy to calculate $c \cdot d \cdot G \in E(F_p)$, but when $c \cdot G$ and $\mathrm{d} \cdot G$ are known, it is very difficult to calculate $c \cdot d \cdot G$.

3.6. Fuzzy Extractor (FE). This is a highly secure biometric recognition method. It contains $(\delta_i, \tau_i) = \mathrm{Gen}(\mathrm{Bio}_i)$ and $\delta'_i = \mathrm{Rep}(\mathrm{Bio}'_i, \tau_i)$ functions [5], where $\mathrm{Bio}_i, \delta_i, \tau_i \in 0, 1^l$. When the deviation between Bio'_i and Bio_i is less than t, $\delta_i = \delta'_i$ can be obtained.

3.7. Collision-Resistant Hash Function. The hash function can convert any long input string $\{0, 1^*$ into a fixed-length value $\{0, 1^L$. If the hash values of two different input strings are the same, the two strings form a set of hash collisions. $Adv_{HASH}(\mathscr{A})$ denotes the advantage of adversary $\mathscr{A}$ in identifying hash collisions: when $\mathrm{Adv}_{\mathrm{HASH}}(\mathscr{A}) \leq \varepsilon$, ε is a real number sufficiently small to be ignored. This hash function is called a collision-resistant hash function.

3.8. Parameters and Symbols. Table 1 lists the names and descriptions of parameters, methods, and symbols required by the proposed protocol. To prevent replay attacks, all participants in the IoHT system network have their own independent timing unit, T, and can maintain synchronization with the system clock of the IoHT systems.

4. The Proposed Scheme

Mutual authentication protocols between devices are typically based on mutually trusting secret information [30]. The combined relationship between patients and IotC and between IotC and WS in IoHT systems often needs to be changed, and the resources of IotC and WS are limited and very different. In this case, the three-party mutual authentication scheme, including the third-party server TA, has clear advantages in terms of communication and storage resources [30]. Therefore, based on the ECDLP and hash function, we propose a lightweight AKA scheme that uses anonymous third-party devices.

4.1. Devices Registration. Figure 2 describes the registration process of IotC. At this stage, TA records the IotC identity and generates a new authentication code TC_i. The numerical numbers of (1), (2), . . ., (7) in Figure 2 are in the order in which IotC and TA execute the protocol at this stage. To enhance the flexibility of the administrator's workplace, we have strengthened the security protection of the communication process. For example, the tracking of equipment is prevented by formulas $ID_i^* = ID_i \oplus h(B \| T_{i1})$ and $D_i = ?ID_i^* \oplus h(B_x \| T_{s1})$; TA calculates $V = ?h(ID_i \| PW_i \| B \| T_{i1})$, and the identity authentication of IotC and administrator users is realized. The registration process of WS is similar to that described in Figure 2.

4.2. IotC Binding to a Patient. The corresponding relationship between the patient and the IotC in the IoHT systems is variable. IotC has only a corresponding relationship with the patient within a certain time range. To meet this demand, this study proposed a strategy for binding IotC$_i$ to a patient. During the validity period, IotC$_i$ and the server TA (PID, PTC) were used to mark the correspondence between IotC$_i$ and the patient. Figure 3 shows the detailed process of binding IotC$_i$ receptor binding to a patient. Numerical numbers such as "(1), (2), . . ., (5)" in Figure 3 are the execution sequences of IotC$_i$ and TA in this stage.

(1) IotC$_i$ local authentication administrator.

(2) IotC$_i$ requests and determines the patient information. In this process, the formula $ID_i^* = ID_i \oplus h(B \| T_{i2})$ is used to encrypt the ID of IotC$_i$ to prevent device tracking.

(3) TA authenticates IotC$_i$. TA uses the formula $B' = S_{TA} \cdot A$ to calculate the ID decryption key of IotC$_i$. IotC identity is verified using $V_1 = ?h(ID'_i \| TC_i \| A \| T_{i2})$.

(4) TA binds a patient to IotC$_i$. The TA selects a user userID and calculates $\mathrm{PID} = h(ID'_i \| \mathrm{user}ID \| c \| T_{S2})$ and $\mathrm{PTC} = h(PID \| TC_i \| T_{S2} \| B')$.

(5) IotC$_i$ binds a patient. After receiving message M_4, IotC$_i$ uses the information to calculate PID and PTC. Subsequently, the key is calculated using the formulas $\mathrm{Gen}(\mathrm{Bio}_n) = (\delta_n, \tau_n)$ and $UK = h(ID_i \| \delta_n)$, and the PID and PTC are encrypted and saved using the formula $w_n = E_{UK}(\mathrm{PID}, \mathrm{PTC}')$.

4.3. TA Authorizes IotC. The ability of the sensor layer network to support the patient's condition and the doctor's diagnosis requires variable correspondence between a patient and multiple WS nodes. This relationship can be replaced by that between $IotC_i$ and multiple WS nodes after the patient is bound to IotC$_i$.

Therefore, this study proposes a strategy for TA to authorize IotC to access WS nodes and use (NID, AC [1, . . ., n]) to mark the corresponding relationship between an IotC and multiple WS nodes. Figure 4 describes the process of IotC$_i$ obtaining the access authorization of a WS node. When multiple WS nodes require access, the variable Ac_j is an array.

Table 1: Parameters, methods, and symbols.

Notation	Description	Notation	Description
TA	Cloud authentication server	IotC	A wearable Internet of Things connector
s_{TA}, P_{TA}	Server key pair $P_{TA} = s_{TA} \cdot G$	$\Delta\text{t}, \Delta\text{T}$	Effective time
WS	A wearable device	T_i	Current time of device i
G	Selected elliptic curve base point	$= ?$	Determine whether they are equal
status	Status of equipment	$\oplus$	XOR operation
$\Vert$	Concatenation operation	SK	Session key
PID	Temporary ID of the patient after binding with IotC	PTC	Temporary identification code of the patient after binding with IotC
NID	Temporary network ID authorized by TA	Ac	Temporary authentication code authorized by the server
a, c, x, y	Random parameters	$h()$	Collision-resistant hash function
TC_i	Authentication code of device I	PW_i	Management key for device i
Bio	User's biometric information	$\text{Rep}(\cdot)$	Deterministic reproduction function
Gen (.)	Probabilistic generation function	τ	Reproduction parameter from $Gen(.)$
δ	Biometric key from Gen (.)	E ()/D ()	Encryption/decryption method

$IotC_i$	Server TA
1) $read: \{P_{TA}, PW_i\}$	3) received M_1
2) $select: a, A = a \cdot G, B = a \cdot P_{TA}$	$\lvert T_{i1} - T_{s1} \rvert < \triangle t$
$ID^*{}_i = ID_i \oplus h(B \Vert T_{i1})$	$B' = s_{TA} \cdot A$
$V = h(ID_i \Vert PW_i \Vert B \Vert T_{i1})$	$ID_i = ID^*{}_i \oplus h(B' \Vert T_{i1})$
send $M_1: \{ID^*{}_i, A, T_{i1}, V\}$.	$search: status, PW_i\ by\ ID'{}_i$
	$V =? h(ID_i \Vert PW_i \Vert B \Vert T_{i1})$
6) receive M_2	4) $select: c, C = c \cdot \mathrm{G}$
$ID_i =? ID^*{}_i \oplus h(B_x \Vert T_{s1})$	$Q = c \cdot A$
$Q' = a \cdot \mathrm{C}$	$ID^*{}_i = ID_i \oplus h(B'_x \Vert T_{s1})$
$\mathrm{TC_i} = \mathrm{h}(ID_i \Vert Q' \Vert T_{s1})$	$\mathrm{T}C_i = \mathrm{h}(ID_i \Vert Q \Vert T_{s1})$
$V_0 =? \mathrm{h}(ID_i \Vert TC'_i \Vert T_{s1} \Vert Q')$	5) $V_0 = \mathrm{h}(ID_i \Vert TC_i \Vert T_{s1} \Vert Q)$
7) $f_i = TC'_i \oplus h(ID_i \Vert PW_i)$	$store: \{ID_i, TC_i\}$
$e_i = h(PW_i \oplus ID_i)$	$send\ M_2: \{ID^*{}_i, C, V_0, T_{s1}\}$
$store: P_{TA}, f_i, e_i$	

Figure 2: IotC registration phase.

$IotC_i$	Server TA
1) $read\ \ PW_i$	
$e_i =? h(PW_i \oplus ID_i)$	3) $receive\ M_3$
2) $TC'_i = f_i \oplus h(ID_i \Vert PW_i)$	$get: T_{S2}, \lvert T_{i2} - T_{S2} \rvert < \triangle t$
$select: a, A = a \cdot G, B = a \cdot P_{TA}$	$B' = S_{TA} \cdot A$
$ID^*{}_i = ID_i \oplus h(B \Vert T_{i2})$	$ID'{}_i = ID^*{}_i \oplus h(B' \Vert T_{i2})$
$V_1 = h(ID'{}_i \Vert TC_i \Vert A \Vert T_{i2})$	$search: ID'{}_i\ get\ TC_i$
$send\ M_3: \{ID^*{}_i, A, V_1, T_{i2}\}$	$V_1 =? h(ID'{}_i \Vert TC_i \Vert A \Vert T_{i2})$
	4) $Find: userID$
5) $received\ \ M_4$	$Select: c$
$PID = PID^* \oplus h(B \Vert T_{i2})$	$PID = h(ID'{}_i \Vert userID \Vert c \Vert T_{S2})$
$V_2 =? h(PID \Vert TC'{}_i \Vert T_{S2})$	$PID^* = PID \oplus h(B' \Vert T_{i2})$
$User\ Input\ Bio_n$	$PTC = h(PID \Vert TC_i \Vert T_{S2} \Vert B')$
$Gen(Bio_n) = (\delta_n, \tau_n)$	$Store: \{PID, PTC\}$
$u_n = \mathrm{h}(\mathrm{ID}_i \Vert \delta_n \Vert \tau_n)$	$V_2 = h(PID \Vert TC_i \Vert T_{S2})$
$PTC' = h(PID \Vert TC'_i \Vert T_{S2} \Vert B)$	$send\ M_4: \{PID^*, V_2, T_{S2}\}$
$UK = h(ID_i \Vert \delta_n)$	
$w_n = E_{UK}(PID, PTC')$	
$Store: \{u_n, \tau_n, w_n\}$	

Figure 3: IotC binding patient process.

4.4. IotC Offline Access to WS Node.

IoHT systems must meet the needs of offline construction of the sensor layer network in real working scenarios. Therefore, this study proposes a strategy in which TA authorizes once, and IotC can access the specified WS node offline many times within the authorization time range. Figure 5 describes the implementation process of the AKA policy of IotC$_i$ offline access to WS_j.

(1) IotC$_i$ authenticates the users locally. IotC$_i$ verifies the user's identity by using the fuzzy extractor function and decrypts and calculates the NID, Ac_j, and T_{s3}, which are required to access WS_j.

$IotC_i/patient_i$	Server TA
1) $Input\ and\ \ \delta'{}_n = Rep(Bio_n, \tau_n)$	
$u_n =? h(ID_i \Vert \delta'{}_n \Vert \tau_n)$	2) ... $\Longrightarrow: M_5$
$UK = h(ID_i \Vert \delta'{}_n)$	$get: T_{s3}, /T_{i3} - T_{s3} \rvert\ <? \triangle t$
$\{PID, PTC'\} = D_{UK}(w_n)$	$B' = S_{TA} \cdot A$
$select: a, A = a \cdot G, B = a \cdot P_{TA}$	$PID = PID^* \oplus h(B' \Vert T_{i3})$
$PID^* = PID \oplus h(B \Vert T_{i3})$	$\lvert T_{s2} - T_{s3} \rvert\ <? \triangle T$
$V_3 = h(PID \Vert T_{i3} \Vert PTC' \Vert A)$	$search: PTC, WS_j\ by\ PID$
$M_5: \{PID^*, A, V_3, T_{i3}\} \quad \Longrightarrow TA$	$V_3 =? h(PID \Vert T_{i3} \Vert PTC \Vert A)$
	3) $select: c, C = c \cdot G, Q = c \cdot A$
4) $Q' = a \cdot C \qquad M_6: \Longleftarrow TA$	$NID = h(PID \Vert Q \Vert PTC \Vert T_{s3})$
$Ac_j = E_j \oplus h(Q' \Vert PTC' \Vert T_{s3})$	$Ac_j = h(NID \Vert ID_j \Vert TC_j \Vert T_{s3})$
$V_4 =? h(Q' \Vert Ac_j \Vert T_{s3} \Vert PTC)$	$E_j = Ac_j \oplus h(Q \Vert PTC \Vert T_{s3})$
$NID' = h(PID \Vert Q' \Vert PTC' \Vert T_{s3})$	$V_4 = h(Q \Vert Ac_j \Vert T_{s3} \Vert PTC)$
$w_n = E_{UK}(PID, PTC', NID, Ac_j, T_{s3})$	$\Longleftarrow M_6: \{C, V_4, E_j, T_{s3}\}$
$Store: w_n$	

Figure 4: TA authorizes IotC$_i$ access to WS node.

(2) Login WS_j. IotC$_i$ calculates the variable values of TID, Y, T_{s3}, and V_5 in turn. Message M_7 is combined and broadcast to the sensor layer network.

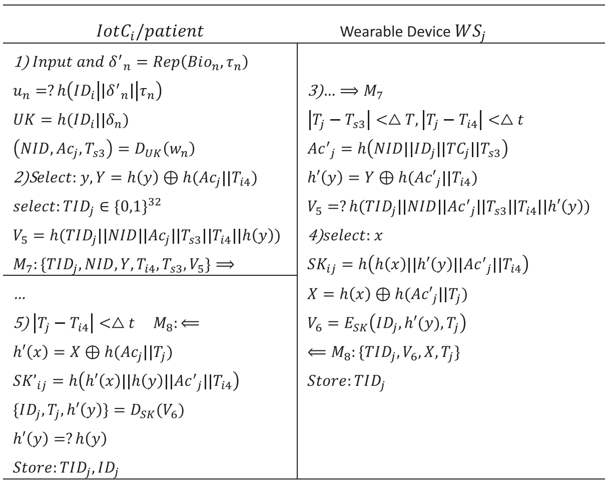
(3) WS_j verifies IotC$_i$. After receiving message M_7, WS_j uses the formula $|T_j - T_{s3}| < \triangle T$, $|T_j - T_{i4}| < \triangle t$ to verify the authorization validity $\triangle T$ and data transmission validity $\triangle t$, and $\triangle T$ is much greater than $\triangle t$. Then, WS_j uses the formula $h(TID_j \| UID \| Ac_j \| T_{s3} \| T_{i4} \| h(y))$ to verify the access authorization of IotC$_i$.

(4) Calculate the session key SK. After the identity authentication of IotC$_i$ is successful, WS_j uses the formula $SK_{ij} = h(h(x) \| h'(y) \| Ac'_j \| T_{i4})$ to calculate the session key SK_{ij} between WS_j and $IotC_i$. WS_j continues to calculate the values of variables X and V_6 and returns the message M_8 to IotC$_i$.

(5) IotC$_i$ authenticates WS_j. After receiving the message M_8, IotC$_i$ uses the formula $|T_j - T_{i4}| < \triangle t$ to verify the time validity of the message. If valid, IotC$_i$ using TID$_j$ in the current message, select Ac'_j corresponding to sending message M_7 and calculate $SK'_{ij} = h(h'(x) \| h(y) \| Ac'_j \| T_{i4})$ to obtain SK'_{ij}. Then, calculate $\{ID_j, T_j, h'(y)\} = D_{SK}(V_6)$. If equation $h'(y) = ?h(y)$ holds, IotC$_i$ successfully authenticates WS_j identity.

4.5. IotC Online Access WS.

In the proposed scheme, when IotC obtains access authorization for the WS, the process of accessing the specified WS for the first time can be regarded as an online access. That is, after IotC completes all the operations described in Figure 4 and obtains NID, Ac_j, and T_{s3}, it can directly transfer to the number "(2)" in Figure 5, mark the part, and begin to enter the WS node.



$IotC_i/patient$	Wearable Device WS_j
1) Input and $\delta'_n = Rep(Bio_n, \tau_n)$	
$u_n =?\, h\left(ID_i \Vert \delta'_n \Vert \tau_n\right)$	$3) \ldots \Longrightarrow M_7$
$UK = h(ID_i \Vert \delta_n)$	$\lvert T_j - T_{s3} \rvert < \triangle T, \lvert T_j - T_{i4} \rvert < \triangle t$
$\left(NID, Ac_j, T_{s3}\right) = D_{UK}(w_n)$	$Ac'_j = h\left(NID \Vert ID_j \Vert TC_j \Vert T_{s3}\right)$
$2) Select{:}\ y, Y = h(y) \oplus h(Ac_j \Vert T_{i4})$	$h'(y) = Y \oplus h(Ac'_j \Vert T_{i4})$
$select{:}\ TID_j \in \{0,1\}^{32}$	$V_5 =?\, h(TID_j \Vert NID \Vert Ac'_j \Vert T_{s3} \Vert T_{i4} \Vert h'(y))$
$V_5 = h(TID_j \Vert NID \Vert Ac_j \Vert T_{s3} \Vert T_{i4} \Vert h(y))$	$4) select{:}\ x$
$M_7{:}\ \{TID_j, NID, Y, T_{i4}, T_{s3}, V_5\} \Longrightarrow$	$SK_{ij} = h\left(h(x) \Vert h'(y) \Vert Ac'_j \Vert T_{i4}\right)$
…	$X = h(x) \oplus h(Ac'_j \Vert T_j)$
$5) \lvert T_j - T_{i4} \rvert < \triangle t \quad M_8{:} \Longleftarrow$	$V_6 = E_{SK}\left(ID_j, h'(y), T_j\right)$
$h'(x) = X \oplus h(Ac_j \Vert T_j)$	$\Longleftarrow M_8{:}\ \{TID_j, V_6, X, T_j\}$
$SK'_{ij} = h\left(h'(x) \Vert h(y) \Vert Ac'_j \Vert T_{i4}\right)$	$Store{:}\ TID_j$
$\{ID_j, T_j, h'(y)\} = D_{SK}(V_6)$	
$h'(y) =?\, h(y)$	
$Store{:}\ TID_j, ID_j$	

Figure 5: IotC_i offline access to WS_j node.

4.6. IotC Accesses Multiple WS Nodes Concurrently. In a multi-WS access scenario, Figure 5 shows that the variable Ac_j in the authorization process is an array AC [1, . . ., N]. AC [1, . . ., N] contains the access verification codes for multiple WS nodes. At this time, IotC generates a corresponding message TID and message M_7 for each element in AC [1, . . ., N], according to the operation described in Figure 5. The messages of multiple M_7 structures were then sent continuously.

After WS_j receives the first M_7 structure message, WS_j starts to execute all operations in the "(3)" mark section in Figure 5. Until $V_5 = ?h(\mathrm{TID}_j \| \mathrm{NID} \| Ac'_j \| T_{s3} \| T_{i4} \| h'(y))$ meets the equality, stop receiving and go to the part marked with "(4)."

In the case of multiple WS concurrent access, after IotC_i receives M_8, IotC_i uses the TID in M_8 to select the corresponding AC to improve the concurrent access capability of IotC_i.

4.7. Replacement and Change of WS Nodes. When the patient's condition development or other conditions need to adjust the IotC, this can be realized by sequentially executing the process described in Figures 4 and 5. When only the WS needs to be adjusted, this can be realized by sequentially executing the process described in Figures 4 and 5.

5. Security Analysis

This section proves the security performance and antiattack ability of the proposed protocol through formal methods.

5.1. Security Model. The scheme proposed in this study belongs to the identity authentication and key agreement (AKA) protocol. Therefore, we provide the corresponding security model and formal proof process based on [31–33]. In this model, $\mathbb{P}$ denotes the proposed scheme. I presents the participants in the scheme, which can be TA, $IotC_i$, or WS_j. Attacker $\mathscr{A}$ can be described by the following random oracles:

(i) Excute$(TA, \mathrm{Iot}C_i, WS_j)$: attacker $\mathscr{A}$ intercepts all messages exchanged between any two parties

(ii) Send(I, m): attacker $\mathscr{A}$ sends forged message M to I and receives feedback form

(iii) Reveal(I): attacker $\mathscr{A}$ obtains the composition information of the session key and launches a known key attack

(iv) Corrupt(I): attacker $\mathscr{A}$ can obtain the long-term key of I to verify the strong forward security performance of the session key SK

   (i) Corrupt(IotC): attacker $\mathscr{A}$ can obtain $\{ID_i, TC_i,\}$ of IotC

   (ii) Corrupt(WS): attacker $\mathscr{A}$ can obtain $\left\{ID_j, TC_j\right\}$ of WS

(v) Test(I): Attacker $\mathscr{A}$ uses a coin toss test to challenge session key {SK}. When $\rho = 1$, the correct session key SK is returned, and when $\rho = 0$, a random string is returned.

(vi) Hash$(m, h(m))$: Attacker $\mathscr{A}$ calculates the hash value of message M.

Definitions and assumptions need to be used in the definition and false proof process.

5.1.1. Partnering. If a group of participants in the protocol, the instances of IotC_i and WS_j, can pass the mutual identity authentication and negotiate a consistent session key SK, we call them partners.

5.1.2. Fresh. If a session is not disclosed, it is called a fresh session.

5.1.3. Security. When attacker $\mathscr{A}$ destroys the security advantage $\mathrm{Adv}_p(\mathscr{A}) \leq \varepsilon$ of protocol $\mathbb{P}$, it means that $\mathbb{P}$ is secure and satisfies $\mathrm{Adv}_p(\mathscr{A}) = |2\,\mathrm{Pr}\,[\mathrm{Succ}] - 1|$, where ε is a real number small enough to be ignored, and Pr [Succ] represents the probability that attacker $\mathscr{A}$ successfully destroys the security of $\mathbb{P}$.

Assumptions 1. The basic algorithms used in the proposed scheme, such as the elliptic curve discrete logarithm problem (ECDLP), elliptic curve Diffie–Hellman discrete logarithm problem (ECDHDLP), fuzzy extractor (FE), hash function, and symmetric-key encryption algorithm (Enc), are secure; that is,$\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}) \le \varepsilon$, $\mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A}) \le \varepsilon$, $\mathrm{Adv}_{FE}(\mathscr{A}) \le \varepsilon$, $\mathrm{Adv}_{\mathrm{HASH}}(\mathscr{A}) \le \varepsilon$, $\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A}) \le \varepsilon$.

5.2. Security Proof

Theorem 1. *The advantage of $\mathscr{A}$ in $\mathbb{P}$ is given by*

$$\mathrm{Adv}_p(\mathscr{A}) \le 2\frac{q_h^2}{2^l} + 22\frac{(q_h + q_s)}{2^l} + 4\frac{(q_s + 2T_m)}{2^q} + 2\frac{q_s}{|\mathfrak{H}|} + 2\frac{q_h^4}{2^{2l+2}} + 2\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A}) + \frac{q_h^2}{2^l} \max\{\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A})\}. \tag{1}$$

In the above formula, q is the order of elliptic curve finite cyclic group $E(F_p)$; $|\mathfrak{H}|$ represents the length of the dictionary; l is the length of the hash value, q_e, q_s,and q_h, respectively, represent the number of times $\mathscr{A}$ executes Excute(), Send(), and Hash() queries, respectively, and T_m represents the calculation times of elliptic curve scalar multiplication.

Proof. This process is similar to those in References [31–33] and takes place over five games G_0 to G_7. Succ_i represents that $\mathscr{A}$ wins in the game G_i and successfully destroys the security of protocol $\mathbb{P}$.

G_0: This game simulates that attacker $\mathscr{A}$ uses the random oracle model to launch a real attack on $\mathbb{P}$, so we can obtain $\mathrm{Adv}_p(\mathscr{A}) = |2\,\mathrm{Pr}\,[\mathrm{Succ}_0] - 1|$.

G_1: This game simulates attacker $\mathscr{A}$ launching a passive attack on protocol $\mathbb{P}$. Attacker $\mathscr{A}$ intercepts message $\mathrm{M}_3 - M_8$ through $\mathrm{Excute}(TA, \mathrm{Iot}C_i, WS_j)$ and stores it in the list L. Because the key SK is not transmitted in the above message, passive attacks will not increase the advantage of attacker $\mathscr{A}$. Thus, $\mathscr{A}$ can be obtained $\mathrm{Pr}[\mathrm{Succ}_1] = \mathrm{Pr}[\mathrm{Succ}_0]$.

G_2: To improve the advantage, attacker $\mathscr{A}$ applies the collision principle based on G_1 and uses an oracle $\mathrm{Hash}(m, h(m))$ and $\mathrm{Test}(I)$ to launch multiple attacks. In this case, attacker $\mathscr{A}$ guesses or collides with the key SK, and the success probability is $q_s/|\mathfrak{H}| + q_h^2/2^{l+1}$; destroying the security of the symmetric-key algorithm, and the success probability is $\mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A})$. At this point, the advantage of attacker $\mathscr{A}$ can be described as $\mathrm{Pr}[\mathrm{Succ}_2] - \mathrm{Pr}[\mathrm{Succ}_1] \le q_s/|\mathfrak{H}| + q_h^2/2^{l+1} + \mathrm{Adv}_{\mathrm{Enc}}(\mathscr{A})$.

G_3: Attacker $\mathscr{A}$ indirectly attacks SK through Ac_j based on G_2: Attacker A can destroy the security of the symmetric-key algorithm. The methods and success probability of attacker $\mathscr{A}$ are as follows:

(i) Attacker $\mathscr{A}$ collides with the value of Ac_j, and the success probability is $q_h^2/2^{l+1}$.

(ii) Attacker $\mathscr{A}$ intercepts NID and T_{s3} in M_7, collides with ID_j and TC_j values, and uses the formula $Ac_j = h(NID\|ID_j\|TC_j\|T_{s3})$ to calculate Ac_j, with a success probability of $q_h^4/2^{2l+2}$.

(iii) Attacker $\mathscr{A}$ uses the formula $Ac_j = E_j \oplus h(\mathrm{Q}\|\mathrm{PTC}\|T_{s3})$ to calculate the value of Ac_j, where Q and PTC are unknown variables, and the success probability is $\max\{\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A})\}q_h^2/2^{l+1}$.

At this point, the advantage of attacker $\mathscr{A}$ can be described as $\mathrm{Pr}[\mathrm{Succ}_3] - \mathrm{Pr}[\mathrm{Succ}_2] \le q_h^2/2^{l+1} + q_h^4/2^{2l+2} + \max\{\mathrm{Adv}_{\mathrm{ECDLP}}(\mathscr{A}), \mathrm{Adv}_{\mathrm{ECDHDLP}}(\mathscr{A})\}q_h^2/2^{l+1}$.

G_4: This game simulates that attacker $\mathscr{A}$ uses $\mathrm{Send}(\mathrm{Iot}C_i, M_8)$ query to send a forged message M_8 to enhance his advantage. In this case, attacker $\mathscr{A}$ evaluates the success according to the message returned by $\mathrm{Iot}C_i$. The simulator must check whether M_8 is in the list L. To verify the formula $h'(y) = ?h(y)$, attacker $\mathscr{A}$ must test the values of $h(x)$, Ac_j', and SK'_{ij}. Therefore, attacker $\mathscr{A}$ can obtain $\mathrm{Pr}[\mathrm{Succ}_4] - \mathrm{Pr}\ [\mathrm{Succ}_5] \le 3(q_h + q_s)/2^l$.

G_5: This game simulates that attacker $\mathscr{A}$ uses $\mathit{Send}(WS_j, M_7)$ query to send a forged message M_7 to enhance its advantage. In this case, attacker $\mathscr{A}$ passes the formula $V_5 = ?h(TID_j\|NID\|Ac_j'\|T_{s3}\|T_{i4}\|h'(y))$ for verification, and the values of $h(y)$, Ac_j', TC_j, and ID_j need to be tested. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_5] - \mathrm{Pr}[\mathrm{Succ}_4] \le 4(q_h + q_s)/2^l$.

G_6: This game simulates that attacker $\mathscr{A}$ uses $\mathit{Send}(\mathit{Iot}C_i, M_6)$ query to send a forged message M_6 to enhance his advantage. In this case, attacker $\mathscr{A}$ must test the values of Q', PID, and PTC. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_5] - \mathrm{Pr}[\mathrm{Succ}_4] \le (\mathrm{q_s} + 2\mathrm{T_m})/2^{\mathrm{q}} + 2(q_h + q_s)/2^l$.

G_7: This game simulates that attacker $\mathscr{A}$ uses $\mathrm{Send}(TA, M_5)$ queries to send a forged message M_5 to enhance its advantage. In this case, attacker $\mathscr{A}$ must test the values of B, PID, and PTC. At this point, the advantage of attack $\mathscr{A}$ is $\mathrm{Pr}[\mathrm{Succ}_6] - \mathrm{Pr}[\mathrm{Succ}_5] \le (\mathrm{q_s} + 2\mathrm{T_m})/2^{\mathrm{q}} + 2(q_h + q_s)/2^l$.

Therefore, combining the advantages of G_0–G_7 attacker $\mathscr{A}$, we can get Theorem 1. □

5.3. BAN Logic Proof of the Proposed Protocol. In this chapter, we use the Burrows–Abadi–Needham (BAN) logic [30, 34, 35] to formally prove the security of the device AKA protocol proposed in this study. We assumed that the symbols P and Q represent participation in the communication session, X and Y are messages sent or received by the participants, and K is the session key. Table 2 lists the relevant symbols, descriptions, and logic rules often used in the BAN logic. To save space, only Figure 5 is listed as a formal proof describing the content.

Table 2: BAN logic notation and rules.

$P \mid \equiv X$	P believes the message X
$P \lhd X$	P sees the message X
$P \mid \sim X$	P once said the message X
$P \mid \Rightarrow X$	P has jurisdiction over the message X
$\#(X)$	The message X is fresh
$P \overset{Y}{\rightleftharpoons} YQ$	Only P and Q know X
$P \overset{K}{\leftrightarrow} Q$	P and Q share key K
(X, Y)	X or Y is a part of message (X, Y)
$\{X_K$	X is encrypted with K
$(X)_K$	X is hashed with K
R1	Message meaning rule: $(\mathrm{P} \mid \equiv \mathrm{P} \overset{\mathrm{K}}{\leftrightarrow} \mathrm{Q}, \mathrm{P} \lhd \mathrm{X_K}/\mathrm{P} \mid \equiv \mathrm{Q} \mid \sim \mathrm{X}),\ (\mathrm{P} \mid \equiv \mathrm{P} \overset{\mathrm{Y}}{\rightleftharpoons} \mathrm{YQ}, \mathrm{P} \lhd \{\mathrm{X_Y}/\mathrm{P} \mid \equiv \mathrm{Q} \mid \sim \mathrm{X})$
R2	Nonce verification rule: $(\mathrm{P} \mid \equiv \#(\mathrm{X}), \mathrm{P} \mid \equiv \mathrm{Q} \mid \sim \mathrm{X}/\mathrm{P} \mid \equiv \mathrm{Q} \mid \equiv \mathrm{X})$
R3	Jurisdiction rule: $(\mathrm{P} \mid \equiv \mathrm{Q} \mid \Rightarrow \mathrm{X}, \mathrm{P} \mid \equiv \mathrm{Q} \mid \equiv \mathrm{X}/\mathrm{P} \mid \equiv \mathrm{X})$
R4	Freshness rule: $(\mathrm{P} \mid \equiv \#(\mathrm{X})/\mathrm{P} \mid \equiv \#(\mathrm{X}, \mathrm{Y}))$,
R5	Belief rule: $(\mathrm{P} \mid \equiv \mathrm{X}, \mathrm{P} \mid \equiv \mathrm{Y}/\mathrm{P} \mid \equiv (\mathrm{X}, \mathrm{Y}))$, $(\mathrm{P} \mid \equiv (\mathrm{X}, \mathrm{Y})/\mathrm{P} \mid \equiv \mathrm{X})$, $(\mathrm{P} \mid \equiv \mathrm{Q} \mid \equiv (\mathrm{X}, \mathrm{Y})/\mathrm{P} \mid \equiv \mathrm{Q} \mid \equiv \mathrm{X})$

According to the functional characteristics of the protocol proposed in this study, the security of the AKA process of IotC_i accessing WS_j can be decomposed into five security verification objectives under the BAN logic. They are, respectively, G1: WS_j trust TA, G2: WS_j trust IotC_i, G3: WS_j trust SK_{ij}, G4: IotC_i trust SK_{ij}, and G5: IotC_i trust WS_j.

5.3.1. G1: WS_j Authenticates TA. In BAN logic, the message M_7: $\{\mathrm{TID}_j, \mathrm{NID}, Y, T_{i4}, T_{s3}, V_5\}$ in Figure 5 is converted to $(\mathrm{TID}_j, \mathrm{NID}, T_{i4}, T_{s3}, Y, T_{i4ACj}, (\mathrm{TI\ D}_j, \mathrm{NID}, T_{s3}, T_{i4}, Y)_{ACj})$. After receiving M_7, WS_j calculates $AC_j' = (\mathrm{NID}, ID, T_{s3})_{TCj}$, and the target G1 can be represented by the formula $WS_j \mid \equiv TA \mid \sim AC_j'$. When the equation $V_5 = ?h(\mathrm{TID}_j \| \mathrm{NID} \| AC_j' \| T_{s3} \| T_{i4} \| Y)$ holds, AC_j is not tampered with.

WS_j gets $WS_j \mid \equiv TA \overset{TC_j}{\longleftrightarrow} WS_j, W\ \ S_j \mid \equiv TA \mid \equiv TA \overset{TC_j}{\longleftrightarrow} C_j W\ S_j, WS_j \lhd (\mathrm{NID}, ID_j, T_{s3})_{TCj}$

Uses R1: $(WS_j \mid \equiv TA \overset{TC_j}{\rightleftharpoons} WS_j, W\ S_j \lhd (\mathrm{NID}\ , ID, T_{S3})_{TC_j} / WS_j \mid \equiv TA \mid \sim (NID, ID, T_{S3})_{TC_j})$

Gets G1: $WS_j \mid \equiv TA \mid \sim AC_j'$

5.3.2. G2: WS_j Trust IotC_i. In the protocol proposed in this study, IotC_i uses NID to mark the identity after binding with patient information and obtaining WS access authorization. Therefore, the target G2 can be represented by the formula $WS_j \mid \equiv \mathrm{NID}$.

WS_j gets $WS_j \mid \equiv TA \overset{TC_j}{\longleftrightarrow} WS_j$, $WS_j \mid \equiv \#T_{s3}$, $WS_j \mid \equiv TA \mid \Rightarrow (\mathrm{NID}, \mathrm{IDj}, T_{S3})_{TC_j}$

Uses R4: $(WS_j \mid \equiv \#T_{s3}/WS_j \mid \equiv \#(\mathrm{NID}, ID, T_{S3})_{TC_j})$

Uses R2: $(WS_j \mid \equiv \#(\mathrm{NID}, ID, T_{S3})_{TC_j}, WS_j \mid \equiv TA \mid \sim \mathrm{NID}, ID, T_{S3})_{TC_j} / WS_j \mid \equiv TA \mid \equiv (\mathrm{NID}, ID, T_{S3})_{TC_j})$

Uses R3: $(WS_j \mid \equiv TA \mid \Rightarrow (\mathrm{NID}, ID, T_{S3}\ )_{TC_j}, WS_j \mid \equiv TA \mid \equiv \mathrm{NID}, ID, T_{S3})_{TC_j}/WS_j \mid \equiv (\mathrm{NID}, ID, T_{S3})_{TC_j})$

Uses R5: $(WS_j \mid \equiv (\mathrm{NID}, ID, T_{S3})_{TC_j} / WS_j \mid \equiv \mathrm{NID}, WS_j \mid \equiv ID_j, WS_j \mid \equiv T_{S3})$

Gets G2: $WS_j \mid \equiv \mathrm{NID}$

5.3.3. G3: WS_j Trusts SK_{ij}. SK_{ij} is calculated using the formula $SK_{ij} = h(h(x) \| h(y))$, and its calculation security is based on a collision-resistant hash function. $h(x)$ is randomly generated by WS_j. G3 can be expressed using the formula $WS_j \mid \equiv h(y)$.

WS_j gets $WS_j \mid \equiv \#T_{i4}$, $WS_j \lhd h(y), T_{i4ACj}$, $WS_j \mid \equiv TA \mid \Rightarrow h(y), T_{i4ACj}$

Uses R1: $(WS_j \mid \equiv WS_j \overset{AC_j}{\rightleftharpoons} TA, WS_j \lhd h(y), T_{i4AC_j} / WS_j \mid \equiv TA \mid \sim (h(y), T_{i4}))$

Uses R2: $(WS_j \mid \equiv \#T_{i4}, WS_j \mid \equiv TA \mid \sim (h(y), T_{i4}) / WS_j \mid \equiv TA \mid \equiv (h(y), T_{i4}))$

Uses R3: $(WS_j \mid \equiv TA \mid \Rightarrow h(y), T_{i4AC_j}, WS_j \mid \equiv TA \mid \equiv (h(y), T_{i4})/WS_j \mid \equiv (h(y), T_{i4}))$

Uses R5: $(WS_j \mid \equiv (h(y), T_{i4})/WS_j \mid \equiv h(y), WS_j \mid \equiv T_{i4})$

Gets G3: $WS_j \mid \equiv h(y)$

5.3.4. G4: IotC_i *Trusts SK_{ij}.* In BAN logic, message M_8 is converted to $(\mathrm{TID}_j, ID_j, Y', T_{jSK_{ij}}, X, T_{jAC_j}, T_j)$. G4 can be represented using the formula Iot$C_i \mid \equiv SK_{ij}$.

IotC_i gets Iot$C_i \mid \equiv Ac_j$, Iot$C_i \mid \equiv$ Iot $C_i \overset{AC_j}{\rightleftharpoons} TA$, Iot$C_i \lhd h(x), T_j\}_{Ac_j}$, Iot$C_i \mid \equiv h(y)$

Uses R1: (Iot$C_i \mid \equiv$ Iot$C_i \overset{AC_j}{\rightleftharpoons} TID$, Iot$C_i \lhd h(x), T_j\}_{Ac_j}$/ Iot$C_i \mid \equiv TID \mid \sim (h(x), T_j)$)

Uses R4: (Iot$C_i \mid \equiv \#(T_j)$/Iot$C_i \mid \equiv \#(h(x), T_j)$)

Uses R2: (Iot$C_i \mid \equiv \#(h(x), T_j)$, Iot$C_i \mid \equiv TID \mid \sim (h(x), T_j)/WS_j \mid \equiv \mathrm{NID} \mid \equiv (h(x), T_j)$)

Uses R3: (Iot$C_i \mid \equiv TA \mid \Rightarrow$ Iot$C_i \overset{AC_j}{\rightleftharpoons} TA$, Iot$C_i \mid \equiv \mathrm{NID} \mid \equiv (h(x), T_j)$/Iot$C_i \mid \equiv (h(x), T_j)$)

Uses R5: $(\text{Iot}C_i \mid \equiv (h(x), T_j)/\text{Iot}C_i \mid \equiv h(x))$, $(\text{Iot}C_i \mid \equiv h(x), \text{Iot}C_i \mid \equiv h(y)/\text{Iot}C_i \mid \equiv (h(x), h(y)))$

Gets G4: Uses $\text{Iot}C_i \mid \equiv SK'_{ij}$

5.3.5. G5: $\text{Iot}C_i$ *Trusts* WS_j. G4 can be represented by the following formula $\text{Iot}C_i \mid \equiv ID_j$:

Uses R1: $(\text{Iot}C_i \mid \equiv \text{Iot}C_i \overset{SK_{ij}}{\rightleftharpoons} \text{TID}, \text{Iot}C_i \lhd \text{I}D_j, \text{h}'(\text{y}), T_j\}_{SK_{ij}}/\text{IoT}C_i \mid \equiv T\text{ID} \mid \sim (\text{I}D_j, \text{h}'(\text{y}), T_j))$

Uses R4: $(\text{Iot}C_i \mid \equiv \#(T_j)/\text{Iot}C_i \mid \equiv \#(\text{I}D_j, \text{h}'(\text{y}), T_j))$

Uses R2: $(\text{Iot}C_i \mid \equiv \#(\text{I}D_j, \text{h}'(\text{y}), T_j)$, $\text{Iot}C_i \mid \equiv \text{TID} \mid \sim (\text{I}D_j, \text{h}'(\text{y}), T_j)$ $/\text{Iot}C_i \mid \equiv \text{TID} \mid \equiv (\text{I}D_j,\ \text{h}'(\text{y}), T_j))$

Uses R3: $(\text{Iot}C_i \mid \equiv \text{TID} \mid \Rightarrow \text{Iot}C_i \overset{SK_{ij}}{\rightleftharpoons} \text{TID}, \text{Iot}\ \ C_i \mid \equiv \text{TID} \mid \equiv (\text{I}D_j, \text{h}'(\text{y}), T_j)/\text{Iot}C_i \mid \equiv (\text{I}D_j,\ \text{h}'(\text{y}), T_j))$

Uses R5: $(\text{Iot}C_i \mid \equiv (\text{I}D_j, \text{h}'(\text{y}), T_j)/\text{Iot}C_i \mid \equiv \text{I}\ D_j, \text{Iot}\ C_i \mid \equiv \text{h}'(\text{y}), \text{Iot}C_i \mid \equiv T_j)$

Gets G5: $\text{Iot}C_i \mid \equiv \text{I}D_j$

At this time, this study successfully uses the BAN logic to formally prove the security of the three-party AKA protocol proposed in this study and achieves all the security indicators.

6. Simulation of the Proposed Protocol

AVISPA [25, 36, 37] is an automated network protocol security verification tool. It includes a constraint-logic attacker search (Cl-AtSe) and an on-the-fly model checker (OFMC), which are two types of network attack simulation checkers. The results of AVISPA evaluation showed a certain degree of recognition. In this part, this study uses the AVISPA tool set for Figure 4 authorized access and equipment AKA process described in Figure 5 and conduct simulation security verification.

Figure 6 shows the HLPSL simulation model of the proposed protocol and the simulation attack process in the AVISPA software. Attacker A was added to the simulation process to verify the ability of the protocol to resist intermediate authentication attacks. Figure 7 evaluates the results of the HLPSL model in AVISPA software using two checkers: OFMC and Cl-AtSe. The results show that the proposed scheme is secure under the two inspector models and meets all specified security objectives.

7. Efficiency Evaluation and Comparisons

In this section, the requirements of computing resources and server I/O resources that have a significant impact on system stability are selected, and the lightweight three-party AKA scheme proposed in this study is evaluated. For convenience of description, we select the typical [5–7, 9, 23, 26] lightweight authentication and key agreement protocols in some recent studies for comparison.

7.1. Comparison of the Computation Cost. When the encryption algorithm is fixed, the higher the security level, the longer the key length, and more computing resources are required to be consumed [28]. An objective analysis of the resource consumption of the AKA scheme must be conducted at the same security level. Therefore, Table 3 is established by referring to the relevant experimental data and the results in references [6, 9, 23, 38, 39].

Table 3 lists the approximate time multiple relationships between the main mathematical calculation in some common security encryption algorithms and the SHA-1 hash calculation, and the unit is T_h. For the special T_{fe}, we have not yet found convincing public data; T_{xor} takes very little time and can be ignored.

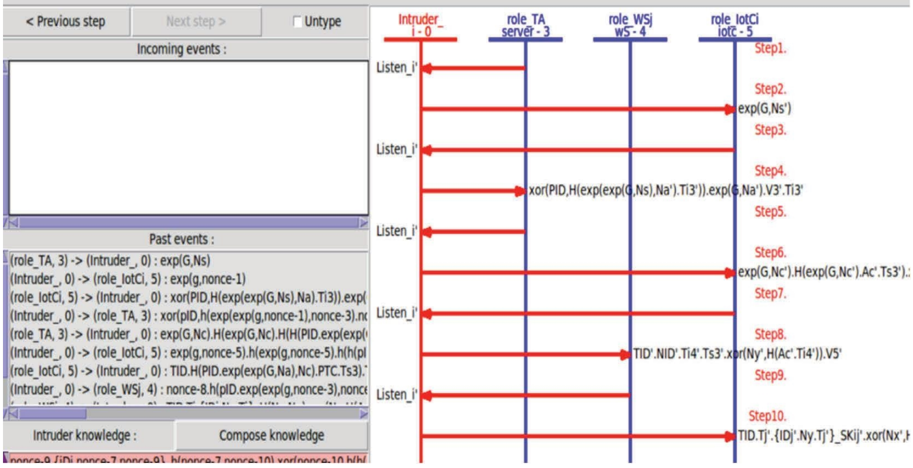
Table 4 compares the selected literature and the proposed AKA scheme in terms of the theoretical consumption of resources. Considering that IotC in the proposed scheme can support offline and concurrent access to multiple WS nodes within the authorization time range, the corresponding computing resource consumption is listed in Table 4.

In the case of online access, the proposed protocols IotC and TA must perform the authorization process described in Figure 4. Therefore, when accessing the first WS node, the TA must perform three EC scalar multiplications and six hash calculations, that is, $2T_{sm} + 6T_h \approx 151T_h$ calculation time, IotC requires $1T_{fe}$+ 3 $T_{sm} + 13T_h + 3T_{\text{sym}} \approx 233.5T_h + 1T_{fe}$ calculation time, and WS requires $5T_h + 1T_{\text{sym}} \approx 6\text{T}_\text{h}$ calculation time. When the IotC offline line accesses the second WS node, the proposed scheme no longer needs to perform the authorization process described in Figure 4. Currently, IotC requires only a calculation time of $5T_h + 1T_{\text{sym}} \approx 6T_h$, whereas WS requires a calculation time of $5T_h + 1T_{\text{sym}} \approx 6T_h$.

Figure 8 shows a comparison of the schemes in Table 4 when only one WS node needs to be accessed. The x-axis represents the theoretically calculated resource demand quantity, and the unit is T_h. The computational performance of Li et al. [9] scheme is the best, and the proposed scheme has certain advantages.

Figure 9 shows the proposed scheme and compares the demand for computing resources with the protocol proposed by Jiang et al. [26] for multi-WS node access. The x-axis represents the number of access WS nodes, and the y-axis represents the theoretically calculated resource demand in units of T_h. Figure 9(a) describes the changes in the computing resource requirements of IotC. Figure 9(b) represents the change in computing resource demand of server TA. Figure 9(c) describes the change in overall computing resources. The increase in the number of nodes has little impact on IotC and the overall computing resource requirements in the scheme proposed in this study, which is better than Jiang's scheme.

7.2. Server Database I/O Resources. The number of WS, IotCs, and users in an IoHT system is huge, and the necessary information needs to be stored in the database. When



```
(role_TA, 3) -> (Intruder_, 0) : exp(G,Ns)
(Intruder_, 0) -> (role_IotCi, 5) : exp(g,nonce-1)
(role_IotCi, 5) -> (Intruder_, 0) : xor(PID,H(exp(exp(G,Ns),Na).Ti3)).exp(
(Intruder_, 0) -> (role_TA, 3) : xor(pID,h(exp(exp(g,nonce-1),nonce-3).nc
(role_TA, 3) -> (Intruder_, 0) : exp(G,Nc).H(exp(G,Nc).H(H(PID.exp(exp(
(Intruder_, 0) -> (role_IotCi, 5) : exp(g,nonce-5).h(exp(g,nonce-5).h(h(pI
(role_IotCi, 5) -> (Intruder_, 0) : TID.H(PID.exp(exp(G,Na),Nc).PTC.Ts3).
(Intruder_, 0) -> (role_WSj, 4) : nonce-8.h(pID.exp(exp(g,nonce-3),nonce
```

```
nonce-9.{iDj.nonce-7.nonce-9}_h(nonce-7.nonce-10).xor(nonce-10.h(h(
```

Figure 6: Simulation attack process of the proposed protocol.

```
% OFMC
% Version of 2006/02/13
   SAFE
DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
   /home/span/span/testsuite/results/3AKA2-12.1.if
GOAL
   as_specified
BACKEND
   OFMC
COMMENTS
STATISTICS
   parseTime: 0.00s
   searchTime: 0.01s
   visitedNodes: 5 nodes
   depth: 4 plies
```

(a)

```
SUMMARY
   SAFE
DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
   TYPED_MODEL
   BOUNDED_SEARCH_DEPTH
PROTOCOL
   /home/span/span/testsuite/results/3AKA2-12.1.if
GOAL
   As Specified
BACKEND
   CL-AtSe
STATISTICS
   Analysed : 5 states
   Reachable : 2 states
   Translation: 0.01 seconds
   Computation: 0.00 seconds
```

(b)

Figure 7: (a) OFMC report. (b) Cl-AtSe report.

Table 3: Time requirement of the calculation method.

Signs	Description	Times (T_h)
T_h	Hash function	= 1
T_{sym}	Symmetric encryption/decryption	≈1
T_{MAC}	Message authentication code	≈1
T_{pa}	EC point addition	≈12.5
T_{crt}	Chinese remainder theorem (CRT)	≈20
T_{me}	Modular exponentiation	≈60
T_{sm}	EC scalar multiplication	≈72.5
T_{sig}	Signature generation using ECDSA	≈92.5
T_{Ver}	Signature verification using ECDSA	≈147.5
T_{map}	Map-to-point on ECC	≈450
T_{pair}	ECC bilinear pairing	≈1500
T_{fe}	Fuzzy extractor function	—
T_{xor}	Time required for XOR operation	Negligible

Table 4: Comparison of calculated resource consumption.

Protocol	Server	SGW/IoetC/HN	STD/node	Total
Das et al. [5]	—	$10\ T_h + 1T_{fe}$	$7\ T_h$	$17\ T_h + 1\ T_{fe}$
Srinivas et al. [6]	$11T_h + 1T_{\mathrm{ctr}}$	$16T_h + 1T_{\mathrm{me}}$	$12T_h$	$118T_h$
Wang et al. [7]	$377\ T_h$	$75.5\ T_h$	$163.5\ T_h$	$661\ T_h$
Li et al. [9]	—	$5T_h$	$3T_h$	$8\ T_h$
He and Zeadally [23]	$77.5\ T_h$	$221.5\ T_h$	$149.5\ T_h$	$448.5\ T_h$
Jiang et al. [26]	$9T_h + 1sm$	$8T_h + 2T_{sm} + 1T_{fe}$	$4\ T_h$	$239.5\ T_h + 1T_{fe}$
Ours online, 1st node	$2\ T_{sm} + 6\ T_h \approx\ 151\ T_h$	$3\ T_{sm} + 13\ T_h + 3\ T_{\mathrm{sym}} \approx\ 233.5\ T_h + 1T_{fe}$	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$390.5\ T_h + 1\ T_{fe}$
Ours online, 2nd node	$1T_h$	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$13T_h$
Ours offline, 1st node	0	$8\ T_h + 2\ T_{\mathrm{sym}} + 1T_{fe} \approx\ 10\ T_h + 1T_{fe}$	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$16\ T_h + 1T_{fe}$
Ours offline, 1st node	0	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$5\ T_h + 1\ T_{\mathrm{sym}} \approx\ 6\ T_h$	$12T_h$

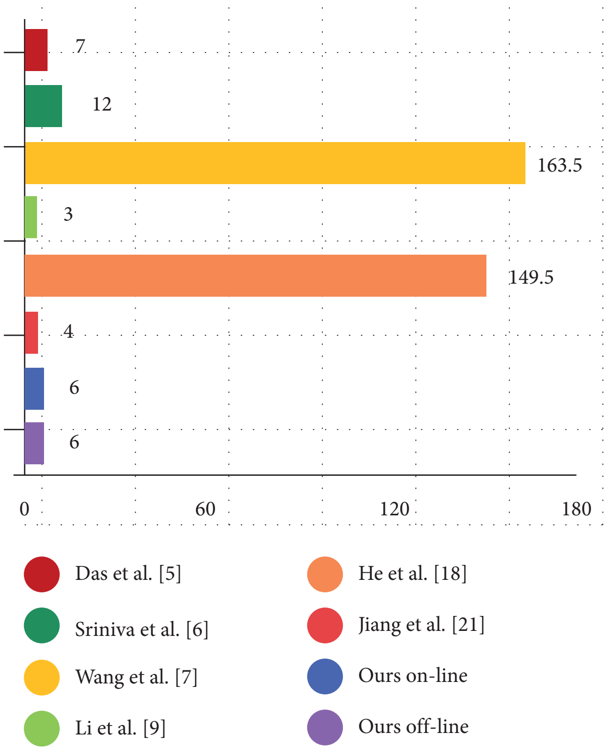
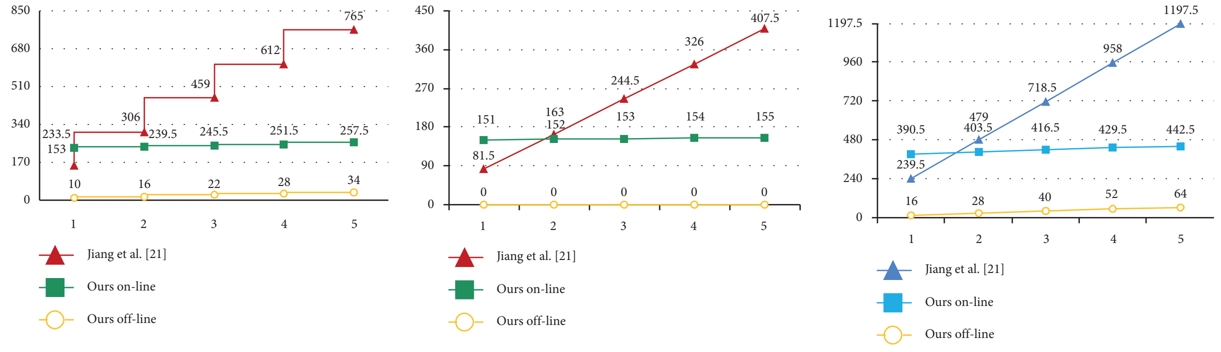


Figure 8: WS calculation time.



(a)

(b)

(c)

Figure 9: Computing resource requirements when multiple WS nodes are connected.

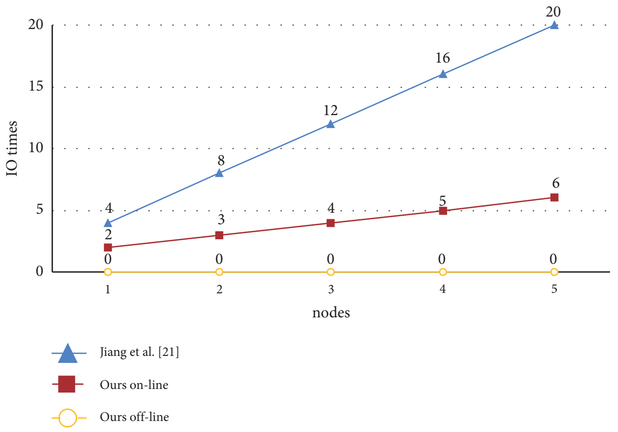


FIGURE 10: Comparison of server database I/O operations.

IotC is connected to WS, TA must perform the necessary data reading or writing operations to verify the privileges of users after IotC binding and authorize IotC to access the specified WS. The operation of the database requires server I/O resources. This operation is too frequent, which causes insufficient input-output resources and seriously affects the stability of the system.

In Jiang et al.'s scheme [26], privacy protection is realized and device tracking is prevented by synchronizing a set of one-time identity IDs between the WS and server CS. Thus, Ta must perform three queries and one updated data operation during the AKA process. Specifically, an IotC identity query, a temporary ID query of WS, avoids the repeated query of the one-time ID of the newly generated WS at one time and an operation to update the database with a new ID. The proposed scheme requires only one PID query and WS information query. Moreover, when the number of WS nodes increases, the number of queries must be increased to be equal to the number of authorized WS nodes. Figure 10 shows the changes in the I/O operation resource requirements of the server TA database in the case of multi-WS access in the proposed scheme and Jiang et al.'s scheme [26].

8. Conclusions

The rapid development of the Internet of Things and wearable sensing technology has continuously promoted Internet of Health Things (IoHT) systems in medical institutions. However, the IoHT systems not only provide a more convenient and faster channel for health detection data but also make sensitive Personal Health Information (PHI) face many new security risks. Physical channel security between Internet of Things Connectors (IotC) and wearable sensors (WS) is an important link for building IoHT systems into a secure health system (SHS).

Therefore, this study proposes a lightweight three-party authentication and key agreement (AKA) protocol that meets the characteristics of the two-hop structure and the requirements of multi-WS network monitoring. The results of the formal security proof, BAN logic analysis, and simulation experiment of the AVISPA tools show that the scheme proposed in this study can meet the expected security requirements. The results of the comparison with relevant protocols show that the protocol has certain advantages in WS individual computing resource consumption: in the scenario of multiple WS node applications, the increasing trend of computing resource demand of IotC and the server is not obvious, as the I/O operation resources of the server are not affected by the number of WS nodes.

Acronyms

AVISPA:	Automated validation of internet security protocols and applications
AKA:	Authentication and key agreement
BAN logic:	Burrows–Abadi–Needham logic
CS:	Cloud server
Cl-AtSe:	Constraint-logic attacker search
DOS:	Denial-of-service
EC:	Elliptic curve
ECC:	Elliptic curve cryptography
ECDLP:	Elliptic curve discrete logarithm problem
ECDHDLP:	Elliptic curve Diffie–Hellman discrete logarithm problem
FE:	Fuzzy extractor
IoT:	Internet of Things
IoHT:	Internet of Health Things
IotC:	Internet of things Connector
IoD:	Internet of Drones
I/O:	Input/Output
MT:	Mobile terminal
OFMC:	On-the-fly model checker
PHI:	Patient health information
SHS:	Secure health system
TA:	Third-party authentication server
WS:	Wearable sensor
WNC:	Wearable network connector.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Science and Technology Research Project of Hebei Province Colleges and Universities (Grant Z2020134) and the Natural Science Foundation of Hebei Province (Grant F2021405001) and the General Project of Hebei North University under Grant no. XJ2021005.

References

[1] researchandmarkets, "Wearable technology market by product (wristwear, headwear, footwear, fashion & jewelry, bodywear), type (smart textile, non-textile), application (consumer electronics, healthcare, enterprise & industrial), and geography - global forecast to 2026," 2021, https://www.

researchandmarkets.com/reports/5314641/wearable-technology-market-by-product-wristwear.

[2] S. B. Baker, W. Xiang, and I. Atkinson, “Internet of things for smart healthcare: technologies, challenges, and opportunities,” *IEEE Access*, vol. 5, pp. 26521–26544, 2017.

[3] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, “A survey on internet of things and cloud computing for healthcare,” *Electronics*, vol. 8, no. 7, p. 768, 2019.

[4] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in Healthcare 4.0,” *Computer Communications*, vol. 153, pp. 311–335, 2020.

[5] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, and Y. Park, “Design of secure and lightweight authentication protocol for wearable devices environment,” *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1310–1322, J, 2018.

[6] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 942–956, 2020.

[7] Z. Wang, L. Gong, J. Yang, and X. Zhang, “Cloud-assisted elliptic curve password authenticated key exchange protocol for wearable healthcare monitoring system,” *Concurrency and Computation: Practice and Experience*, vol. 34, no. 9, 2020.

[8] C.-T. Li, C.-C. Lee, and C.-Y. Weng, “A secure cloud-assisted wireless body area network in mobile emergency medical care system,” *Journal of Medical Systems*, vol. 40, no. 5, p. 117, 2016.

[9] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks,” *Computer Networks*, vol. 129, pp. 429–443, 2017.

[10] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, “Certificateless public key authenticated encryption with keyword search for industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3618–3627, 2018.

[11] A. K. Yetisen, J. L. Martinez-Hurtado, B. Ünal, A. Khademhosseini, and H. Butt, “Wearables in medicine,” *Advances in Materials*, vol. 30, no. 33, Article ID 1706910, 2018.

[12] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, “Authenticated key agreement scheme for fog-driven IoT healthcare system,” *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[13] P. A. H. Williams and V. McCauley, *Always Connected: The Security Challenges of the Healthcare Internet of Things*, IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 2016.

[14] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, “HaBiTs: blockchain-based telesurgery framework for healthcare 4.0,” in *Proceedings of the 2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Beijing, China, August 2019.

[15] P. A. Abdalla and C. Varol, “Testing IoT security,” *The Case Study of an IP Camera*, vol. 8, 2020.

[16] X. Zhang, J. Zhao, F. Yang, Q. Zhang, and X. Zhang, “An automated composite scanning tool with multiple vulnerabilities,” in *Proceedings of the 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China, October 2019.

[17] Z. Mu, W. Li, C. Lou, and M. Liu, “Investigation and application of smart door locks based on bluetooth control technology,” in *Proceedings of the 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, Dalian, China, April 2020.

[18] C. Doctorow, “Proof-of-concept ransomware for smart thermostats demoed at defcon,” Boing Boing, 2016, https://boingboing.net/2016/08/08/proof-of-concept-ransomware-fo.html.

[19] J. Yang, W. Zhang, J. Liu, J. Wu, and J. Yang, “Generating De-identification facial images based on the attention models and adversarial examples,” *Alexandria Engineering Journal*, vol. 61, no. 11, pp. 8417–8429, 2022.

[20] A. Dua, N. Kumar, A. K. Das, and W. Susilo, “Secure message communication protocol among vehicles in smart city,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359–4373, 2018.

[21] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, “LSCSH: lattice-based secure cryptosystem for smart healthcare in smart cities environment,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 24–32, 2018.

[22] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, “Fog computing for Healthcare 4.0 environment: opportunities and challenges,” *Computers & Electrical Engineering*, vol. 72, pp. 1–13, 2018.

[23] D. He and S. Zeadally, “Authentication protocol for an ambient assisted living system,” *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[24] D. He, N. Kumar, and J.-H. Lee, “Privacy-preserving data aggregation scheme against internal attackers in smart grids,” *Wireless Networks*, vol. 22, no. 2, pp. 491–502, 2016.

[25] A. Armando and L. Vigneron, “The AVISPA tool for the automated validation of internet security protocols and applications,” in *Computer Aided Verification*, K. Etessami and S. K. Rajamani, Eds., vol. 3576pp. 281–285, 2005.

[26] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, “User centric three-factor authentication protocol for cloud-assisted wearable devices,” *International Journal of Communication Systems*, vol. 32, no. 6, p. e3900, Apr, 2019.

[27] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, “TCALAS: temporal credential-based anonymous lightweight authentication scheme for internet of Drones environment,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[28] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, *Guide to Elliptic Curve Cryptography*, Springer, Berlin, Germany, 2003.

[29] A. H. Koblitz, N. Koblitz, and A. Menezes, “Elliptic curve cryptography: the serpentine course of a paradigm shift,” *Journal of Number Theory*, vol. 131, no. 5, pp. 781–814, 2011.

[30] M. Burrows and M. Abadi, “A logic of authentication,” *Proceedings of the Royal Society A: Mathematical, Physical Science*, vol. 426, pp. 233–271, 1989.

[31] E. Bresson, O. Chevassut, and D. Pointcheval, “Security proofs for an efficient password-based key exchange,” in *Proceedings of the 10th ACM conference on Computer and communications security*, Washington D.C. USA, October 2003.

[32] M. Abdalla, P. A. Fouque, and D. Pointcheval, “Password-based authenticated key exchange in the three-party setting,” in *Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography*, Les Diablerets, Switzerland, January 2005.

[33] F. Wu, L. Xu, S. Kumari, and X. Li, “A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101–116, 2017.

[34] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, “A three-factor anonymous authentication scheme for wireless sensor networks in internet of things

environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[35] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[36] H. Nicanfar and V. C. M. Leung, "Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 253–264, 2013.

[37] X. Li, J. Niu, S. Kumari, J. Liao, and W. Liang, "An enhancement of a smart card authentication scheme for multi-server architecture," *Wireless Personal Communications*, vol. 80, no. 1, pp. 175–192, 2015.

[38] B. Zhao, S. Zeng, H. Feng et al., "Lightweight mutual authentication strategy for internet of electric things," *Sustainable Energy Technologies and Assessments*, vol. 45, Article ID 101130, 2021.

[39] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: testing the limits of elliptic curve cryptography in sensor networks," in *Wireless Sensor Networks*, R. Verdone, Ed., vol. 4913pp. 305–320, 2008, http://link.springer.com/10.1007/978-3-540-77690-1_19.