ITC 1/54
Information Technology and Control
Vol. 54 / No. 1/ 2025
pp. 329-344
DOI 10.5755/j01.itc.54.1.39944

A Lightweight Multi-Party Key Authentication Management Protocol Based on Cyber-Physical Systems

Received 2024/12/25 | Accepted after revision 2025/02/21

HOW TO CITE: Zhao, X., Peng, C., Tan, W., Ding, H. (2025). A Lightweight Multi-Party Key Authentication Management Protocol Based on Cyber-Physical Systems. *Information Technology and Control*, 54(1), 329-344. https://doi.org/10.5755/j01.itc.54.1.39944

A Lightweight Multi-Party Key Authentication Management Protocol Based on Cyber-Physical Systems

Xiaoran Zhao, Changgen Peng
The State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China

Weijie Tan
The Key Laboratory of Advanced Manufacturing Technology, Ministry of Education, Guizhou University, Guiyang, China

Hongfa Ding
The Information School, Guizhou University of Finance and Economics, Guiyang, China

Corresponding authors: cgpeng@gzu.edu.cn

In the era of digital healthcare, secure information interaction among users, gateways, and multiple devices in a cyber-physical system (CPS) is very important, but also very challenging. However, existing authentication schemes can only accomplish authentication between gateways and smart devices, and do not consider the authentication needs of gateways, users and multiple devices. In addition, users need to initiate multiple key authentication requests to complete multi-device authentication, which greatly increases the communication overhead and security risks. In response, this paper proposes a lightweight multi-party key authentication protocol based on cyber-physical system. On the basis of meeting the user, gateway and multi-device authentication requirements, the key authentication process is effectively simplified by the CPS architecture, and the user only needs to initiate a request to complete the three-party multi-device authentication, which greatly reduces the communication overhead, reduces the security risks, and improves the scheme's adaptability and generalization ability in large-scale device scenarios. Finally, the mathematical analysis confirms the reliability of the proposed scheme and points out that the scheme reduces the computational and communication requirements compared with similar methods, which is crucial for CPSs with limited resources.

KEYWORDS: Authentication Protocol; Digital healthcare; Key Agreement; Cyber-physical system.

1. Introduction

In the era of digital healthcare, the traditional Internet of Things (IoT) is struggling to cope with the many challenges posed by large-scale production and consumption and rapidly evolving smart healthcare services [1]. To this end, cyber-physical systems (CPS) have reformatively improved the efficiency of healthcare delivery by deploying sensors and other acquisition devices to provide a wide range of social healthcare services. However, while enjoying convenience, cyber-physical systems also have many security risks. Consumers can connect multiple smart devices simultaneously for health testing, and regional clusters of devices support user access to the CPS for data collection and analysis. In this process, the underlying devices store the collected data in a cloud server, which can only be accessed by legitimate managers and users. A little carelessness can lead to data and user privacy leakage, and if the data information is obtained by unscrupulous merchants or attackers, it will lead to irreversible and serious consequences. So to safeguard the legitimacy and privacy of the components in the cyber-physical system, authentication management between users, gateways and multiple devices becomes especially critical [3, 13].

Nowadays, more and more scholars have begun to study the authentication management techniques among multiple devices to ensure the security of communication under complex architectures. Ming et al. [14] proposed a one-to-many key authentication technique based on elliptic curve cryptography and Chinese remainder theorem, but its high computational complexity and communication overhead are not suitable for large-scale device communication in cyber-physical systems. Gaba et al. [10] proposed a sustainable healthcare tripartite authentication protocol based on zero-knowledge proof that utilizes physical unclonable features, biometrics, etc. to reduce communication and computational costs, but does not consider the case of multi-device authentication. It can be seen that as the consumer base continues to expand, the components in the cyber-physical system grow as well. The traditional authentication schemes are either unable to satisfy the need for three-way authentication between users, gateways and multiple devices, or the schemes are designed to be complex, with excessive communication cost and computational complexity, and cannot be adapted to resource-limited CPSs [22].

Therefore, in order to solve the above problems, simplify the authentication process, reduce the communication overhead, and satisfy the demand for three-party authentication among users, gateways, and multi-devices in cyber-physical systems, we propose a lightweight multi-party key authentication and management protocol with low power consumption, low cost, and process simplicity. The user only needs to initiate one request to complete the multi-device authentication including the gateway. The main contributions of this paper are as follows.

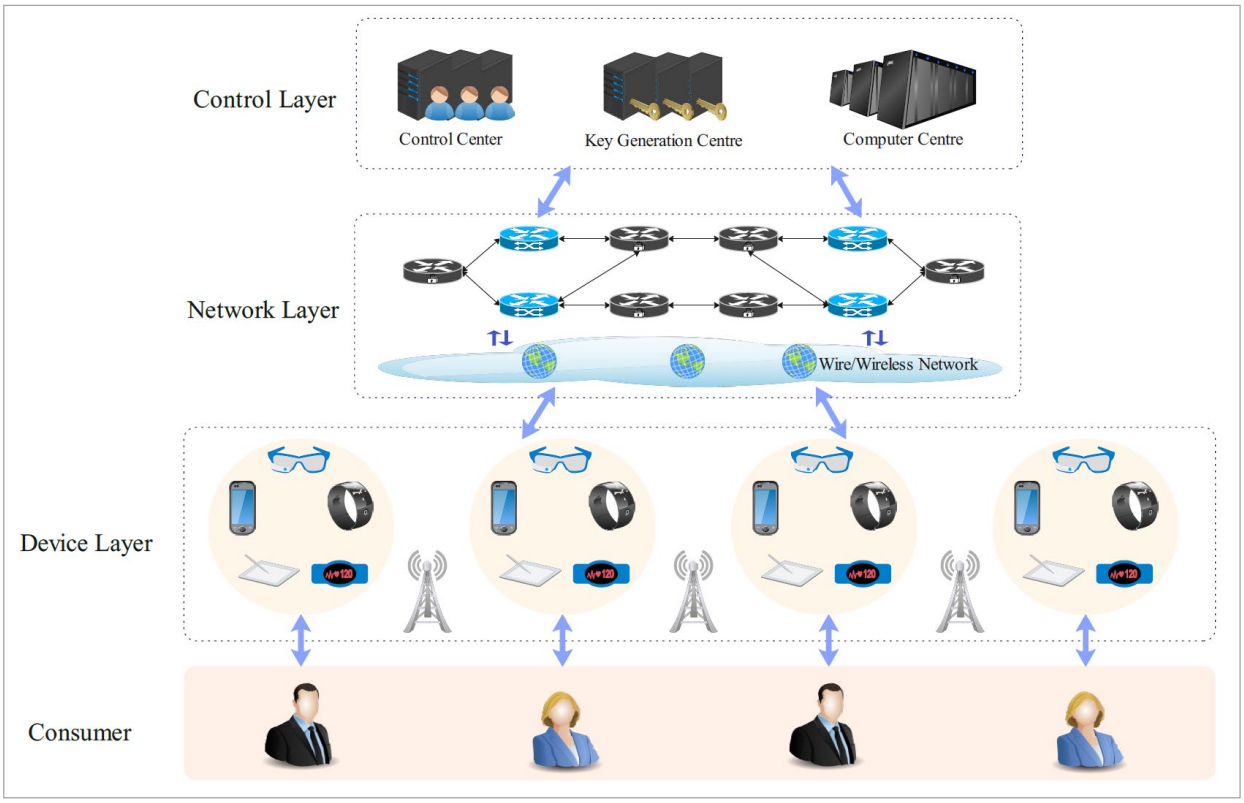
First, this paper proposes a lightweight multi-party key authentication management protocol based on cyber-physical system to solve the communication authentication problem of users, gateways and multiple devices in digital healthcare. Through three-factor authentication and bilinear mapping of users, it resists identity attacks and key exposure attacks to ensure the security of information interaction in the whole system.

Second, to meet the large-scale communication requirements of multi-device in cyber-physical systems, the scheme process is cleverly simplified, and the user only needs to initiate one authentication request to complete the multi-device authentication including the gateway, which greatly reduces the communication and computation overheads, and greatly improves the scheme's generalization capability.

Third, we demonstrate the security of this approach in a well-recognized stochastic prediction model. In addition, the scheme is adaptable to a wide range of functions such as user revocation, smart device joining and exiting, and is resistant to a variety of common attacks. In this paper, we evaluate the computational and communication performance through quantitative analysis. Compared with related schemes, the scheme proposed in this paper has lower computational and communication costs when users access multiple smart devices simultaneously

The rest of the paper is organized as follows. Section related work briefly summarizes the related works on key authentication and management in CPS. Section preliminaries present the problem definition and preliminary knowledge. The proposed schemes section describes our specific program design and details. Safety analyses and proofs are described in section security

Figure 1
Cyber-physical systems framework



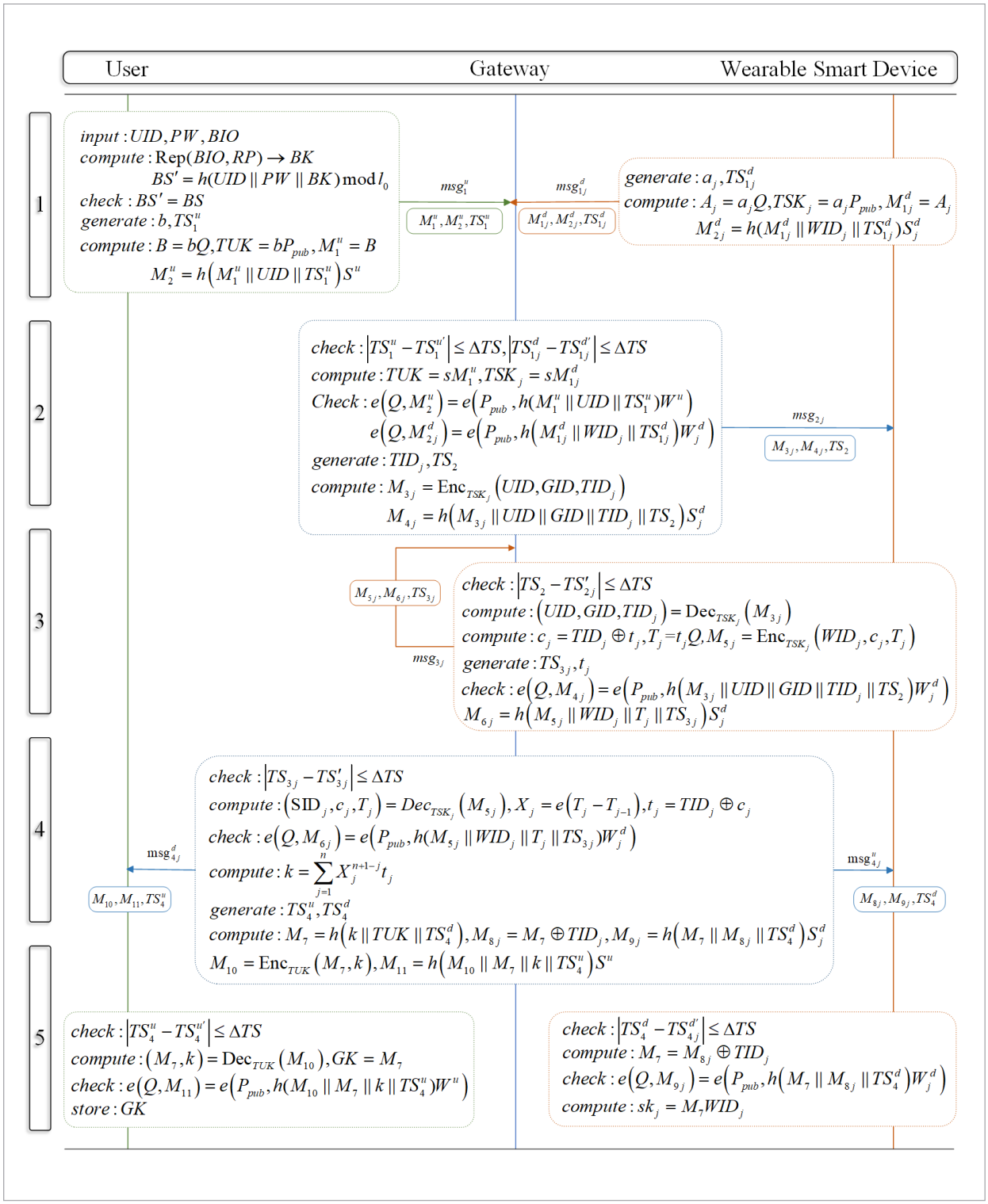
analysis. The experimental evaluations and comparison results are reported in Section performance evaluation. The last Section concludes the paper.

2. Related Work

As an important supporting technology for digital healthcare, cyber-physical systems bring great convenience to people's work and life. In his paper, Verma [18] stated that the current intractable epidemics require a robust intelligent healthcare system that integrates the physical world with the cyberworld by monitoring and controlling medical devices, patients, and external devices. In the same year, Chen et al. [7] proposed that healthcare cyber data is generated digitally and accessed remotely by healthcare professionals and patients during communication, device and information interactions in cyber-physical systems. In the following year, Al-Ghuraybi et al. [2] proposed that cyber-physical systems are designed for multi-party data sharing and transmission, and therefore have security issues in terms of authentication processes and prevention of unauthorized access.

To address secure transmission in digital healthcare, Bhattacharya et al. [4] proposed a blockchain-based deep learning-as-a-service framework for defending against conspiracy attacks based on lattice ciphers and digital signatures. Immediately after, Vinoth and colleagues [19] proposed a key agreement protocol integrating access control and multi-factor authentication keys in 2021. Subsequently, Gaba and colleagues [10] proposed a key agreement protocol for sustainable healthcare management based on zero-knowledge proofs to facilitate three-way authentication between users, devices, and gateways. Cao and colleagues [6] proposed a key authentication protocol aimed at securing communication between user groups. Although the above methods have better performance and security, they are not suitable for CPS multi-device data transmission authentication due

Figure 2
Authentication and Key Agreement Phase



to their excessive communication and computational costs and lack of generalization capability.

Xu et al. [20] in 2020 proposed a blockchain-based authentication and dynamic group key protocol, where each member of a group only needs to authenticate its neighboring members once to complete the authentication, which reduces the communication overhead but does not consider the authentication between users and devices. Salman et al. [16] proposed a lightweight protocol for key authentication and stated that it is the physically unavailable cloning function's first application in healthcare. Subsequently, Li et al. [12] proposed a revocable lightweight authentication scheme for resource-constrained devices in cyber-physical power systems based on certificate-less encryption. From the above literature, it can be seen that the existing lightweight key authentication schemes cannot satisfy the tripartite authentication requirements of users, gateways and multiple devices.

Preliminaries

3.1. CPS Key Authentication Process

The cyber-physical system provides a new and convenient production method for digital healthcare, and the medical institution can control the information interaction between the user and the wearable smart device to realize the whole life cycle monitoring of the patient's physical condition, and the system model is shown in Figure 1 The wearable device carried by the consumer transmits medical data information to the network layer for a round of integration and filtering, and then the network layer uploads the information to the control layer for data analysis and further testing. Among other things, doctors and staff at hospitals or healthcare institutions can use the cyber-physical system to detect and analyze consumers' physical conditions and patients' illnesses, facilitating the implementation of more accurate medical operations. However, there are still unscrupulous elements and third-party organizations that want to steal users' private information for profit. Therefore, key authentication and management protocols need to be used during transmission to ensure the security and legitimacy of both sides of the data interaction.

Table 1 shows the notation system that appears in this paper. In our system model, this process consists of four entities as detailed below.

Table 1
Notations and Descriptions

Symbol	Description
KMC	Key management center
GW	Gateway
U	User
WSD_j	jth wearable smart device
GID	Identity of GW
UID	Identity of U
TID_j	Temporary identity of WSD_j
s, P_{pub}	Private key and public key of GW
W_j^d, A_j, T_j	The WSD's public key
S_j^d, a_j, t_j	The WSD's private key
W^u, B	The User's public key
S^u, b	The User's private key
TSK_j	Temporary key between GW and smart device WSD_j
TUK	Temporary key between GW and U
GK	The session key
r	Variables
PW, BIO	Password, and biometrics of U
TS_m^n	Current timestamp
ΔTS	Maximun transmission delay

Key Management Centre (KMC): Located at the control layer, KMC is a trusted entity responsible for managing wearable smart devices, authorisation gateways and user registration.

Gateway (GW): Located at the network layer, in the early stages of key agreement, GW is responsible for helping users using wearable technology authenticate each other.

User (U): That is, the consumer, who can choose to use a variety of smart devices to collect and send data and initiate a session key agreement query by accessing the smart card via GW.

Wearable Smart Device (WSD): WSD_j denotes the j th wearable smart device, which is responsible for collecting data in the cyber-physical system and transmitting it to U and GW. The KMC completes the basic setup of the WSD, and subsequently assists U in completing the registration and authorization of the GW. Using the GW, the user and the WSD reach a consensus on the session key to ensure that the communication is protected. In addition, WSDs typically have a certain amount of computing power and storage capacity and can be joined or disconnected at any time.

3.2. Threat Model

In the suggested scheme, both [9] and [5] threat models are employed. Based on this, it's clear that an adversary can modify, delete, falsify, and replicate messages.

U and WSD are not considered trustworthy because they can be easily stolen. KMC and GW, on the contrary, are considered trustworthy operators and will not be harmed. Additionally, an adversary may have access to transient information, such as session status, session key, and certain confidential information of the user.

3.3. Fuzzy Extractor

The fuzzy extractor is responsible for generating and reconstructing the biometric key, which includes the following two algorithms:

$\mathrm{Gen}(BIO) \to (BK, BP)$: The biometrics feature BIO is used as the entry point, probability algorithm generates the biometric key BK and the rebuilding parameters BP.

$\mathrm{Rep}(BIO', BP) \to BK$: The deterministic algorithm generates a biometric key BK with the biometrics feature BIO' like BIO and rebuilding parameter BP as an entry.

4. The Proposed Schemes

This part meticulously outlines a robust multi-party authentication and key agreement framework, encompassing the initialization, deployment of smart devices, user registration, gateway authorisation, authentication and key agreement processes, cancellation, updating passwords and biometrics, updating temporary universal keys, and stages of smart device joining and leaving. Figure 2 illustrates the specific process of key authentication and negotiation.

4.1. Initialization Phase

KMC executes the initial setup for the system by executing these steps.

Step 1: Generates a cyclic additive group G_1 of order q, a cyclic multiplicative group G_2 of order q, a generator Q of G_1, and $e: G_1 \times G_1 \to G_2$ is a bilinear map. For points (x, y) belonging to G_1 or G_2, we only focus on x. Subsequently, $msk \in \mathbb{Z}_q^*$ is chose as the master secret key.

Step 2: KMC selects identity GID for GW, computes $s = h(GID \| msk)$ as GW private key. Based on this, the corresponding public key is calculated by $P_{pub} = sQ$.

Step 3: KMC selects a cryptographic hash function, represented as $h: \{0,1\}^* \to \mathbb{Z}_q^*$.

Step 4: Key management centre releases $\{G_1, G_2, e, q, P_{pub}, GID, Q, h\}$ as an parameter of its system.

4.2. Wearable Smart Devices Registration Phase

Before deployment begins, KMC generates the identity of $WSD_j (j \in [1, n])$ and the corresponding key. The following is a formal representation of the exact process.

Step 1: The KMC generates a unique the smart devices identity WID_j, computes $W_j^d = h\left(WID_j\right), S_j^d = sW_j^d$ and sends parameters $\left\{WID_j, W_j^d, S_j^d\right\}$ to WSD_j.

Step 2: All wearable smart devices stores $\left\{WID_j, W_j^d, S_j^d\right\}$ in thememory of WSD_j.

4.3. User Registration Phase

U registers with KMC through a dependable channel. The thorough method is mathematically represented as follows.

Step 1: U selects a distinct identity UID by random and forwards it to KMC through a safety channel.

Step 2: After receiving UID, KMC stores the UID in its database and securely transmits a smart card containing $\{Q, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), h(\cdot)\}$ to U.

Step 3: Upon receiving the smart card, U inputs his identifier UID, code PW, and biometric data BIO. Subsequently, User's smart card SC retrieves the biometric key BK and the reconstruction parameter RP using the fuzzy extractor $\mathrm{Gen}(BIO) \to (BK, RP)$. Following this, SC calculates $BS = h(UID \| PW \| BK)$ mod l_0, with the integer l_0 selected by the smart card, determining the effectiveness of obstructing online guessing attack using fuzzy verifier.

Step 4: KMC computes $W^u = h(UID)$, $S^u = sW^u$ and sents $\{W^u, S^u\}$ to U.

Step 5: The smart card holds $\{BS, RP, l_0\}$ saved by U.

4.4. Gateway Registration Phase

KMC helps GW to make registration settings.The precise mathematical depiction of this process can be described as below.

Step 1: KMC securely transmits s to GW.

Step 2: Through a secure path, KMC sends $\{WID_j\}$, $j \in [1, n]$ and UID to GW.

4.5. Authentication and Key Agreement Phase

U and all wearable smart devices $\{WSD_1, WSD_2, ..., WSD_n\}$ make mutual authentication and agree to distinct session keys via GW, necessitating U and WSD_j to both generate temporary keys and transmit their settings to the GW. The detailed process is represented in mathematical terms as follows.

Step 1: $U \to GW : msg_1^u$,

$WSD_j \to GW : msg_{1j}^d$

- Initially, U adds his smart card into the reader, entering his unique identity UID, the password PW, and biometrics BIO. Subsequently, the smart card SC of U reconstructs the biometric key BK using a fuzzy extractor $\mathrm{Rep}(BIO, RP) \to BK$. Immediately after that, calculate $BS' = h(UID \| PW \| BK)$ mod l_0 and verifies if $BS' = BS$. If not, the login request will be stopped. Otherwise, the validation of U succeeded. Immediately after that, U selects a stochastic b along with the present timestamp TS_1^u, computes $B = bQ$, $TUK = bP_{pub}$, $M_1^u = B$, $M_2^u = h(M_1^u \| UID \ \ TS_1^u) S^u$. $msg_1^u = \{M_1^u, M_2^u, TS_1^u\}$ is transmitted to GW through U via an open channel.
- WSD_j generates a random a_j and the current timestamp TS_{1j}^d. WSD_j computes $A_j = a_j Q$, $TSK_j = a_j P_{pub}$. $M_{1j}^d = A_j$, $M_{2j}^d = h(M_{1j}^d \| \ WID_j \| \ TS_{1j}^d) S_j^d$. $msg_{1j}^d = \{M_{1j}^d, M_{2j}^d, TS_{1j}^d\}$ is sent to GW by WSD_j via an open channel.

Step 2: $GW \to WSD_j : msg_{2j}$

- When GW gets msg_1^u from U, it verifies if $|TS_1^u - TS_1^{u'}| \le \Delta TS$, where $TS_1^{u'}$ represents the moment GW obtained msg_1^u. Subsequently, GW calculates $TUK = sM_1^u = sB$. Verification of condition $e(Q, M_2^u) = e(P_{pub}, h(M_1^u \| \ UID \ \ TS_1^u) W^u)$, ceases upon the check's failure.
- Upon receiving msg_{1j}^d, GW checks whether $|TS_{1j}^d - TS_{1j}^{d'}| \le \Delta TS$, where $TS_{1j}^{d'}$ is the time that WSD_j received msg_{1j}^d. Subsequently, GW computes $TSK_j = sM_{1j}^d = sA_j$, GW check whether $e(Q, M_{2j}^d) = e(P_{pub}, h(M_{1j}^d \| \ WID_j \ \ TS_{1j}^d) W_j^d)$, aborts if the check fails.
- GW generates a unique TID_j as temporary identity of the WSD_j and chooses the current timestamp TS_2 and computes $M_{3j} = Enc_{TSK_j}(UID, GID, TID_j)$, $M_{4j} = h(M_{3j} \| \ UID \ \ GID \ \ TID_j \ \ TS_2) S_j^d$. Finally, GW sends the message $msg_{2j} = \{M_{3j}, M_{4j}, TS_2\}$ to wearable smart device $WSD_j (j \in [1, n])$.

Step 3: $WSD_j \to GW : msg_{3j}$

- When WSD_j gets msg_{2j} from GW, wearable smart device $WSD_j (j \in [1, n])$ verifies if $|TS_2 - TS_{2j}'| \le \Delta TS$, where TS_{2j}' represents the moment WSD_j obtained msg_{2j}. Subsequently, WSD_j calculates $(UID, GID, TID_j) = Dec_{TSK_j}(M_{3j})$. Verification of $e(Q, M_{4j}) = e(P_{pub}, h(M_{3j} \| \ UID \| \ GID \ \ TID_j \ \ TS_2) W_j^d)$, ceases upon the check's failure. Otherwise, WSD_j chooses the current timestamp TS_{3j}. Next, WSD_j chooses a random t_j and computes $c_j = TID_j \oplus t_j$, $T_j = t_j Q$, $M_{5j} = \mathrm{Enc}_{TSK_j}(\mathrm{WID}_j, c_j, T_j)$, and $M_{6j} = h(M_{5j} \| WID_j \| T_j \| \ TS_{3j}) S_j^d$. Finally, every wearable smart device $WSD_j (j \in [1, n])$ sends back the message $msg_{3j} = \{M_{5j}, M_{6j}, TS_{3j}\}$ to GW.

Step 4: $GW \to WSD_j : msg_{4j}^d$,

$GW \to U : msg_4^u$

- Upon receiving msg_{3j} from WSD_j, for every message msg_{3j}, GW verifies if $|TS_{3j} - TS_{3j}'| \le \Delta TS$, where TS_{3j}' represents the moment GW obtained msg_{3j}. Subsequently, GW calculates

$\left(\mathrm{WID}_j, c_j, T_j\right) = \mathrm{Dec}_{TSK_j}\left(M_{5j}\right)$, $X_j = e\left(T_j - T_{j-1}, Q\right)$, $X_1 = e(T_1 - T_n, Q)$, $t_j = TID_j \oplus c_j$, Check whether $e\left(Q, M_6^j\right) = e\left(P_{pub}, h(M_5^j \| WID_j \quad T_j \quad TS_{3j})W_j^d\right)$. If it holds, GW chooses the current timestamps TS_4^u, TS_4^d and computes $k = \sum_{j=1}^{n} X_j^{n+1-j} t_j$, $M_7 = h(k \| UID \quad TS_4^d)$, $M_{8j} = M_7 \oplus TID_j$, $M_{9j} = h(M_7 \| M_{8j} \quad TS_4^d)S_j^d$, $M_{10} = \mathrm{Enc}_{TUK}\left(M_7, k\right)$ and $M_{11} = h(M_{10} \| M_7 \| k \| TS_4^u)S^u$. Finally, GW sends the message $msg_{4j}^d = \left\{M_{8j}, M_{9j}, TS_4^d\right\}$ to WSD_j and sends $msg_4^u = \left\{M_{10}, M_{11}, TS_4^u\right\}$ to each U.

Step 5: The WSD_j performs the following operations.

- Upon receiving msg_{4j}^d from GW, each wearable smart device WSD_j checks whether $\left|TS_4^d - TS_{4j}^{d'}\right| \le \Delta TS$, where $TS_{4j}^{d'}$ is the time that WSD_j received msg_{4j}^d. Then, WSD_j computes $M_7 = M_{8j} \oplus TID_j$, check whether $e\left(Q, M_{9j}\right) = e\left(P_{pub}, h(M_7 \| M_{8j} \quad TS_4^d)W_j^d\right)$. Once the check fails, execution stops. In the end, WSD_j calculates the session key $sk_j = M_7 WID_j$.

Step 6: The U performs the following operations.

- Upon receiving msg_4^u from GW, U verifies if $|TS_4^u - TS_4^{u'}| \le \Delta TS$, where $TS_4^{u'}$ represents the moment U obtained msg_4^u. Then, U computes $\left(M_7, k\right) = \mathrm{Dec}_{TUK}\left(M_{10}\right)$, $GK = M_7$, check whether $e(Q, M_{11}) = e(P_{pub}, h(M_{10} \| M_7 \quad k \quad TS_4^u)W^u)$. aborts if the check fails.
- When U wants to communicate with WID_j, they can calculate a session key sk_j from the master session key GK as shown below: $sk_j = GKWID_j$.

5. Security Analysis

In this section, we first analyse the correctness of the above scheme with mathematics. The ProVerif tool is then used to validate security. At last, we perform informal security analysis on the proposed scheme.

5.1. Security Model

The security model is based on Real Random (ROR). It is easy to infer whether or not a scheme supports semantic security against an adversary $\mathcal{A}$ with $\mathcal{PPT}$. The model primitives are described as follows:

Participants: Our proposed scheme has multiple participants, which are U, GW and WSD_j. The instances α, β and γ of U, GW and WSD_j are denoted by $\prod_{U_i}^{\alpha}$, $\prod_{GW}^{\beta}$ and $\prod_{WSD_j}^{\gamma}$.

Partnership: Should $\prod_{U_i}^{\alpha}$ and $\prod_{WSD_j}^{\gamma}$ have the capability to directly exchange information, utilize identical session keys, and avoid creating session keys with other instances, they are acknowledged as partners.

Freshness: $\mathcal{A}$ session key, denoted as SK, is deemed to be fresh when it is newly established between parties represented by $\prod_{U_i}^{\alpha}$ and $\prod_{WSD_j}^{\gamma}$, and remains confidential, with no disclosure to an unauthorized third party, such as an adversary.

Adversary $\mathcal{A}$ can make the following queries:

Execute $\left(\prod_{U_i}^{\alpha}, \prod_{GW}^{\beta}, \prod_{WSD_j}^{\gamma}\right)$: With this query, $\mathcal{A}$ can eavesdrop on all information exchanged between honest communicators.

Send $\left(\prod_{U_i}^{\alpha}, \prod_{GW}^{\beta}, \prod_{WSD_j}^{\gamma}, m\right)$: Query is modelled as an active attack. When the inquiry of $\mathcal{A}$ for the message is received, a reply message is returned.

Reveal $\left(\prod_{U_i}^{\alpha}, \prod_{WSD_j}^{\gamma}\right)$: Through this query, $\mathcal{A}$ is capable of acquiring the group key SK related to the $\prod_{U_i}^{\alpha}$ and $\prod_{WSD_j}^{\gamma}$ conventions.

Corrupt $\left(\prod_{U_i}^{\alpha}, v\right)$: This query is designed to ensure the security of information that involves three distinct factors. When a request is received from entity $\mathcal{A}$, the corresponding data is provided in response.

- $v = 0$: Returns the password PW to $\mathcal{A}$.
- $v = 1$: Data from the smart card goes back to $\mathcal{A}$.
- $v = 2$: Returns the biometric BIO to $\mathcal{A}$.

Test $\left(\prod_{U_i}^{\alpha}, \prod_{WSD_j}^{\gamma}\right)$: The query emulates the semantic safety of the grouping key SK^* and operates a single time. When $\mathcal{A}$ receives a query, choose bit b at random. If $b = 1$, provide the session key SK^*, and if $b = 0$, opt for and return a string matching the length of SK^*.

Semantic security of session key: In the ROR model, the adversary's advantage in breaking the semantic security of the proposed scheme Σ is defined as

$Adv_{\mathrm{A}}^{\Sigma}(t)=\left|2\Pr\left[b'=b\right]-1\right|$. The advantage of Σ for success in an attack is negligible if the authentication and key management system Σ is safe from an adversary of $\mathcal{PPT}$.

5.2. Formal Security Proof

Theorem 1: Let's assume that $\mathcal{A}$ represents an adversary that is challenging the security of the proposed scheme $\sum$ within the given mathematical framework $\mathcal{PPT}$. Represent D and N to be uniformly distributed cryptography and biometry dictionaries. The advantage of $\mathcal{A}$ in disrupting the session key security in the suggested scheme is

$$\mathrm{Adv}_{\mathcal{A}}^{\Sigma}(t)\le\frac{q_h^2}{|\mathrm{Hash}|}+2\cdot\mathrm{Adv}_{\mathcal{A}}^{ECCDH}\left(t'\right)+2\cdot\max\left(\frac{q_s}{|N|},\frac{q_s}{|D|},\delta q_s\right),$$

where $|D|$, $|N|$, $|Hash|$, $Adv_{\mathcal{A}}^{ECCDH}\left(t'\right)$, δ, q_e, q_s and q_h represent the sizes of D and N, respectively, the range space of the hash function $h(\cdot)$, the dominance of $\mathcal{A}$ to crack the ECCDH problem within $\mathcal{PPT}$, the probability of the "false positive" case, and the number of *Execute* query, *Sent* query and *Hash* query.

Proof 1: To demonstrate its safety, we define a set of 5 successive games, represented by $\prod_k, k\in[0,4]$. The symbols Suc_k and $\Pr\left[Suc_k\right]$ signify the event and probability, respectively, of $\mathcal{A}$ accurately predicting bit b in the $\prod_k$ game. It can be demonstrated that the probability of adversary $\mathcal{A}$ succeeding in the game is negligible.

Game G_0: To start, $\mathcal{A}$ needs to choose bit b. Under the ROR model, it can be established that the initial game $\prod_0$ is equivalent to the proposed solution. Therefore,

$$\mathrm{Adv}_{\mathcal{A}}^{\Sigma}(t)=\left|2\Pr\left[\mathrm{Suc}_0\right]-1\right|.$$

Game G_1: The game simulates an eavesdropping attack initiated by $\mathcal{A}$. During the phase of authentication and key agreement, the adversary $\mathcal{A}$ is capable of acquiring information that has been transmitted across the public channel by performing the Execute operation $\left(\prod_{U_i}^{\alpha},\prod_{GW}^{\beta},\prod_{WSD_j}^{\gamma}\right)$ $msg_{1j}^{d}=\left\{M_{1j}^{d},M_{2j}^{d},TS_{1j}^{d}\right\}$, $msg_{2j}=\{M_{3j},M_{4j},TS_2\}$, $msg_{3j}=\left\{M_{5j},M_{6j},TS_{3j}\right\}$, $msg_{4j}^{d}=\{M_{8j},M_{9j},TS_4^{d}\}$, $msg_4^{u}=\{M_{10},M_{11},TS_4^{u}\}$. Subsequently, $\mathcal{A}$ executes the Test $\left(\prod_{U_i}^{\alpha},\prod_{WSD_j}^{\gamma}\right)$ query to ascertain if the resultant Test $\left(\prod_{U_i}^{\alpha},\prod_{WSD_j}^{\gamma}\right)$ query is the actual session key SK^* or merely a random string. Nevertheless, as per the scheme that has been put forward, the session key $GK=h\left(k\|\ TUK\ \ TS_4^{d}\right)$ contains the secret information k, TUK and TS_4^{d} that $\mathcal{A}$ cannot obtain from the eavesdropping messages msg_1^{u}, msg_{1j}^{d}, msg_{2j}, msg_{3j}, and msg_{4j}^{d}, msg_4^{u}. By utilizing the Execute $\left(\prod_{U_i}^{\alpha},\prod_{GW}^{\beta},\prod_{WSD_j}^{\gamma}\right)$ query, the probability of $\mathcal{A}$ accurately predicting the bit 'b' remains unaffected. Therefore, it can be concluded that

$$\Pr\left[Suc_1\right]=\Pr\left[Suc_0\right].$$

Game G_2: In contrast to $\prod_1$, the game emulates an active attack scenario by incorporating additional send queries and hash queries. In Game $\prod_2$, $\mathcal{A}$ deceives the participants $\left(\prod_{U_i}^{\alpha},\prod_{GW}^{\beta},\prod_{WSD_j}^{\gamma}\right)$ into accepting counterfeit information. $\mathcal{A}$ is able to uncover potential vulnerabilities in the key through a series of repeated hash queries. Subsequently, $\mathcal{A}$ executes a Test $\left(\prod_{U_i}^{\alpha},\prod_{WSD_j}^{\gamma}\right)$ query and determines if the result of this Test $\left(\prod_{U_i}^{\alpha},\prod_{WSD_j}^{\gamma}\right)$ query corresponds to the actual session key sk_j or if it is an arbitrary string. However, it can be seen from the proposed scheme that all messages contain timestamps, random numbers and generic temporary keys to ensure randomness. Therefore, when $\mathcal{A}$ makes sends $\left(\prod_{U_i}^{\alpha},\prod_{GW}^{\beta},\prod_{WSD_j}^{\gamma},m\right)$ queries, the probability of message collision is negligible. Con-

sequently, by the principle of the birthday paradox, it can be deduced that

$$\left|\Pr\left[Suc_1\right]-\Pr\left[Suc_2\right]\right| \le \frac{q_h^2}{2|\,Hash\,|}.$$

Game G_3: The game can be modelled as an active attack. At the beginning of the G_3, the adversary $\mathcal{A}$ generates a fake pseudonym TID_j and then uses the same TID_j to drive the other secret parameters to compute the group key GK. Suppose that in a given session, $\mathcal{A}$ has the ability to capture all the information exchanged between U, GW, and WSD_j. To correctly guess the grouping key $GK = M_7 = h\left(k \| UID \quad TS_4^d\right)$, $\mathcal{A}$ needs to guess $k^* = \sum_{j=1}^{n} X_j^{n+1-j} t_j$, and TS_4^d correctly. However, $\mathcal{A}$ must know either WSD_j or U private key TSK_j, TUK to obtain WID_j, UID, k which is equivalent to solving the ECDLP in $\mathcal{PPT}$. Therefore, it can be derived that

$$\left|\Pr\left[Suc_2\right]-\Pr\left[Suc_3\right]\right| \le \mathrm{Adv}_{\mathcal{A}}^{ECCDH}\left(t'\right).$$

Game G_4: The procedure incorporates the Corrupt $(\prod_{U_i}^{\alpha}, y)$ query to encapsulate the security aspects of three-factor message authentication. Utilizing this query, $\mathcal{A}$ is capable of impersonating U, engaging with GW, and thereby acquiring the session key GK. In G_4, the premise is that $\mathcal{A}$ can acquire a maximum of two factors, given that the most adverse circumstances are taken into account. As a result, the situation can be divided into the following three distinct scenarios:

Case 1: $\mathcal{A}$ obtains PW and the data $\{Q, BS, RP, l_0, \mathrm{h}(\cdot), \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot)\}$ from the smart card by utilizing the Corrupt query for each, denoted as Corrupt $\left(\prod_{U_i}^{\alpha}, 0\right)$ and Corrupt $\left(\prod_{U_i}^{\alpha}, 1\right)$. Given that $\mathcal{A}$ has the capability to make quiries, the probability of $\mathcal{A}$ accurately replicating U_i stands at $\frac{q_s}{|N|}$.

Case 2: $\mathcal{A}$ gains access to the PW and BIO through the use of querying Corrupt $\left(\prod_{U_i}^{\alpha}, 0\right)$ and Corrupt $\left(\prod_{U_i}^{\alpha}, 2\right)$. Because $\mathcal{A}$ lacks access to the information contained within the smart card as well as information about BS, the probability that $\mathcal{A}$ succeeds in impersonating U is extremely low.

Case 3: Access to $\{Q, BS, RP, l_0, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot), \mathrm{h}(\cdot)\}$ and is gained by $\mathcal{A}$ through the use of querying Corrupt $\left(\prod_{U_i}^{\alpha}, 1\right)$ and Corrupt $\left(\prod_{U_i}^{\alpha}, 2\right)$. Since $\mathcal{A}$ can make q_s, the probability that $\mathcal{A}$ succeeds in imitating U is $\frac{q_s}{|N|}$.

In moreover, due to the use of the fuzzy extractor, "false positives" may occur. Assuming that $\mathcal{A}$ inputs a counterfeit biometric feature, the likelihood of successfully spoofing the fuzzy extractor via its reproduction algorithm, represented by $\mathrm{Rep}(\cdot)$, is δ. Given that $\mathcal{A}$ is capable of making q_s queries, the probability of $\mathcal{A}$ successfully impersonating U is δq_s. As soon as the Corrupt $\left(\prod_{U_i}^{\alpha}, y\right)$ query is completed, $\mathcal{A}$ proceeds to issue a Test $\left(\prod_{U_i}^{\alpha}, \prod_{WSD_j}^{\gamma}\right)$ query and then ascertains if the outcome of this Test $\left(\prod_{U_i}^{\alpha}, \prod_{WSD_j}^{\gamma}\right)$ query corresponds to the actual session key GK or if it is instead a randomly generated string. However, the above cases cannot exist at the same time. Therefore

$$\left|\Pr\left[Suc_3\right]-\Pr\left[Suc_4\right]\right| \le \max\left(\frac{q_s}{|N|}, \frac{q_s}{|D|}, \delta q_s\right)$$

Finally, all oracles have been modelled in the previous game. If $\mathcal{A}$ succeeds in guessing bit b, then $\mathcal{A}$ wins the game. Since $\mathcal{A}$ does not know bit b, $\Pr\left[Suc_4\right] = \frac{1}{2}$. According to (3)-(7) the following result can be obtained

$$\begin{aligned}
\mathrm{Adv}_{\mathcal{A}}^{\Sigma}(t) &= 2 \cdot \left|\Pr\left[Suc_0\right] - \frac{1}{2}\right| \\
&= 2 \cdot \left|\Pr\left[Suc_1\right] - \Pr\left[Suc_4\right]\right| \\
&\le 2\left(\frac{q_h^2}{2\,|\,\mathrm{Hash}\,|} + \mathrm{Adv}_{\mathcal{A}}^{ECCDH}\left(t'\right)\right. \\
&\quad \left. + \max\left(\frac{q_s}{|N|}, \frac{q_s}{|D|}, \delta q_s\right)\right) \\
&= \frac{q_h^2}{|\,\mathrm{Hash}\,|} + 2 \cdot \mathrm{Adv}_{\mathcal{A}}^{ECCDH}\left(t'\right) \\
&\quad + 2 \cdot \max\left(\frac{q_s}{|N|}, \frac{q_s}{|D|}, \delta q_s\right)
\end{aligned}$$

5.3. Formal Security Analyses

1 Anonymity: UID of U is hidden in the ciphertext $M_2^u = \mathrm{Enc}_{TUK}(UID, eu)$, where $TUK = bP_{pub}$, $M_1^u = B = bQ$, b is a random number. For an adversary to acquire the UID, they must first possess either b or s and then calculate $TUK = sB = bP_{pub}$. Nevertheless, because of the inherent complexity of solving Diffie-Hellman problem, it is infeasible for an adversary to calculate TUK and thereby retrieve the UID within polynomial time. Likewise, the identity WID_j of WSD_j is embedded within the ciphertext $M_{6j} = \mathrm{Enc}_{TSK_j}\left(\mathrm{WID}_j, c_j, T_j\right)$ To acquire the identity WID_j, the adversary must possess the corresponding TSK_j. Nevertheless, TSK_j is exclusively held by GW and WSD_j that it is deployed for. It is clear that the adversary does not have access to TSK_j. Thus, the proposed scheme ensures the anonymity of both the U and WS2) Untraceability: The message $\left\{M_1^u, M_2^u, M_3^u, TS_1^u\right\}$ for each session is unique due to the incorporation of a random number b and a timestamp TS_1^u. Hence, the adversary is incapable of tracking the actions of U. Similarly, during each session, WSD_j selects distinct random numbers a_j, t_j, and timestamps TS_{1j}^d, TS_j^3 to calculate the messages $\mathrm{msg}_{1j}^d = \left\{M_{1j}^d, M_{2j}^d, TS_{1j}^d\right\}$, $\mathrm{msg}_{3j} = \left\{M_{6j}, M_{7j}, TS_{3j}\right\}$. Furthermore, the TID_j is refreshed following the completion of each authentication phase, making it impossible for an adversary to foresee the updated TID_j. Thus, it is out of the question for an adversary to trace the actions of WSD_j. Consequently, our proposed scheme ensures the untraceability of both U and WSD.

2 Forward and Backward Secrecy: The symmetric keys TSK_j and TUK are derived using the methodology of the Diffie-Hellman key exchange protocol. Regarding the grouping key GK, it can be determined by acquiring all the T_j values within the group. Within our proposed system, the event of a WSD_j joining or leaving the group necessitates an update of the T_j parameter on the part of all remaining devices. Consequently, our scheme ensures both forward and backward secrecy for the symmetric keys and GK.

3 Resist Smart Card Stolen Attack: Should adversary $\mathcal{A}$ acquire the smart card belonging to the registered user, they could potentially extract the data $\{Q, BS, RP, l_0, \mathrm{h}(\cdot), \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot)\}$ through the execution of a side-channel attack. Nevertheless, $\mathcal{A}$ remains uninformed about the confidential details pertaining to U, including the UID, PW, and BK, which constitute secret information. Consequently, $\mathcal{A}$ is unable to acquire the secret key TUK necessary to impersonate U. As a result, the proposed scheme is fortified against attacks that involve the theft of a smart card.

4 Replay Attack: Our scheme incorporates a series of timestamps from TS^u to TS^d in order to prevent replay attacks. Upon receiving a message, the receiver initially checks the authenticity of the timestamp to ensure its validity. Furthermore, each timestamp is embedded within the authentication parameters, signifying that the timestamp is immutable.

5 Resist Impersonation Attack:

– Resist the User Impersonation Attack: Should $\mathcal{A}$ aspire to impersonate U and commence a key agreement request, they must possess the secret key TUK. Nevertheless, the TUK is safeguarded by the UID, PW, and BK, all of which are exclusively known to U. Hence, the scheme is well-defended against user impersonation attacks.

– Resist the Gateway Impersonation Attack: GW computes $M_7 = h(k \| UID\ TS_4^d)$ and $M_{10} = \mathrm{Enc}_{TUK}(M_7, k)$, where $TUK = sM_1^u = sB$ and $TSK_j = sM_{1j}^d = sA_j$. If $\mathcal{A}$ endeavors to generate a valid message as the GW, it is imperative for them to acquire the private key s. Evidently, $\mathcal{A}$ lacks the capability to obtain s. As a result, the proposed scheme is fortified against attacks that involve gateway impersonation.

– Resist the Smart Device Impersonation Attack: For $\mathcal{A}$ to impersonate WSD_j, they must possess both the public temporary key TID_j and the private key TSK_j. It is clear that $\mathcal{A}$ does not possess access to such information. Consequently, the impersonation attack on the wearable smart device is safeguarded against.

6. Performance Evaluation

In this section, we examine our proposed scheme alongside related ones [19, 23, 8, 11, 15, 17, 21] focusing on a comparative analysis of security and functionality, computational requirements, communication ex-

penses, and suitability for industrial applications. For the configuration of the experiment, the experiment uses Python3.7 to build the system communication model under the deep learning framework Tensorflow1.15.0, perating system Ubuntu18.04, CUDA version CUDA10.0, GPU block NVIDIA Titan Xp, and 128G of RAM.

6.1. Functionality Features and Security

The comparative analysis of our proposed scheme with existing schemes, particularly regarding functionality and security aspects, is presented in Table 2. It is apparent that the schemes proposed by [23, 11, 15, 17] are all key management schemes for single wearable smart devices and do not support multi-party authentication. In addition, schemes such as [23, 8, 21] do not consider user revocation and device joining and leaving. This is important because the number of wearable smart devices increases or decreases as the demand of downstream tasks changes. Schemes such as [11, 15] do not consider anonymity, which makes the user's identity highly vulnerable to attack and the user's privacy and security is at risk. The scheme of [19] cannot guarantee forward and backward security, which puts the information of the authentication process at risk of leakage. The scheme of [21] is not resistant to user impersonation attacks, which makes the whole cryptographic authentication scheme unusable in the scenario of multi-device applications in cyber-physical systems. In contrast, our proposed solution fulfills all the functional characteristics and security requirements, which are particularly important in digital healthcare.

6.2. Computation Cost

Symbols t_{sym}, t_h, t_{pm}, and t_{bp} represent the computational time needed for implementing symmetric encryption or decryption, a generalised hash function operation, a dot-multiplication algorithm for elliptic curve cryptography algorithms, and a bilinear pairing operation, etc. Since the computational cost of the XOR operation and the dot-add operation is low, we do not bring in the computation here. Table 3 shows the specific energy consumption of the operations.

Table 3
Energy Consumption

Operations	Consumption
Symmetric Enc or Dec	0.00217mJ
Point multiplication	8.8mJ
Hash function	0.000108mJ
Bilinear pairing	47mJ

Table 2
Functional Comparison

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
Vinoth et al. [19]	✓	N/A	✓	✓	X	✓	✓	✓	✓	✓	✓
Zhang et al. [23]	✓	N/A	✓	✓	✓	✓	✓	✓	✓	N/A	X
Cui et al. [8]	✓	N/A	✓	✓	✓	✓	✓	✓	✓	N/A	✓
Zheng et al. [11]	✓	N/A	X	X	X	N/A	N/A	X	✓	X	X
Zhang et al. [15]	✓	N/A	X	X	✓	N/A	N/A	X	✓	X	X
Shin et al. [17]	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	X
Xu et al. [21]	✓	N/A	✓	✓	✓	X	N/A	✓	✓	✓	✓
Our Scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A_1: Mutual authentication. A_2: User revocation. A_3: Anonymity. A_4: Untraceability. A_5: Perfect forward secrecy. A_6: User impersonation attack. A_7: Gateway impersonation attack. A_8: Device impersonation attack. A_9: Replay attack. A_{10}: Device join/leave. A_{11}: One-to-many scheme

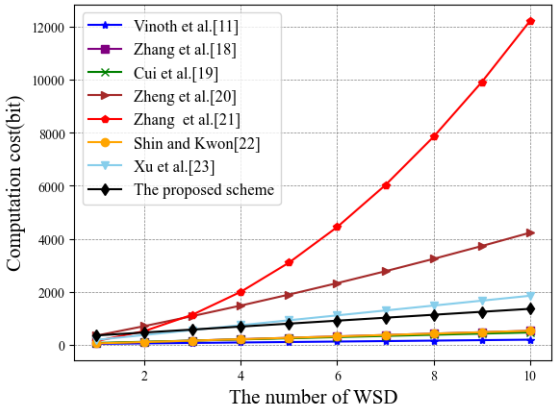
Table 4
Comparison of Computation Cost

Schemes	computation cost(ms)
Vinoth et al. [19]	$(4T_h + 2T_m + 3T_{sym})n$ $+15T_h + 2T_m + 3T_{sym}$
Zhang et al. [23]	$(22T_h + 6T_m + 6T_{sym})n$
Cui et al. [8]	$(19T_h + 5T_m)n + 6T_h + 3T_m$
Zheng et al. [11]	$((n+9)T_h + (n+6)T_m + 4T_{sym} + 6T_{bp})n$
Zhang et al. [15]	$((3n+2)T_m + 2nT_{bp})n$
Shin et al. [17]	$(31T_h + 6T_m)n$
Xu et al. [21]	$(4T_h + 5T_m + 2T_{sym} + 3T_{bp})n$
The proposed scheme	$(7T_h + 2T_m + 2T_{bp} + 3T_{sym})n$ $+7T_h + 6T_m + 4T_{bp} + 3T_{sym}$

Table 4 presents the comparative analysis of computational costs between our proposed scheme and the existing schemes as documented in [19, 23, 8, 11, 15, 17, 21]. The total computational costs of accessing a wearable smart device for the related schemes [19, 23, 8, 11, 15, 17, 21] and the proposed scheme are 35.2151, 52.8154, 70.4027, 343.6098, 138, 52.8033, 185.0047 and 352.4145 mJ, respectively. Our scheme is initially more computationally messy because of the use of bilinear pairs, but as the number of devices increases, our scheme is less computationally intensive than other schemes that use bilinear pairs. The total computational costs of the above scheme and the proposed scheme to access n wearable smart devices are $(4T_h + 2T_m + 3T_{sym})n + 15T_h + 2T_m + 3T_{sym}$, $(22T_h + 6T_m + 6T_{sym})n$, $(19T_h + 5T_m)n + 6T_h + 3T_m$, $((n+9)T_h + (n+6)T_m + 4T_{sym} + 6T_{bp})n$, $((3n+2)T_m + 2nT_{bp})n$, $(31T_h + 6T_m)n$, $(4T_h + 5T_m + 2T_{sym} + 3T_{bp})n$ and $(7T_h + 2T_m + 2T_{bp} + 3T_{sym})n + 7T_h + 6T_m + 4T_{bp} + 3T_{sym}$ mJ, respectively.

Figure 3 illustrates the correlation between the total computational cost and the number of wearable devices. From the Figure 3, it can be seen that the computational cost of the proposed scheme is slightly higher than the few researched schemes due to the use of bilinear pairs to resist the key exposure attack in the multi-smart device application scenario. Compared with multiple scenarios of [11, 15, 21] the proposed scheme in this paper reduces 0.88%, 0.26%, 0.67% respectively. The computational cost is the smallest among similar bilinear pair correlation schemes. It is worth emphasizing that this scheme provides a better choice for CPS with the same requirements.

Figure 3
Computation Cost Versus Number of Wearable Smart Device



6.3. Communication Cost

In this subsection, we conduct an analysis and comparison of the communication expenses associated with our proposed scheme versus those of related schemes, as referenced in [19, 23, 8, 11, 15, 17, 21]. As mentioned earlier, the length of the elements in $\mathbb{G}$, the length of the elements in $\mathbb{Z}_q^*$, the length of the symmetric encrypted ciphertext, the identity, the output of the hash function, and the timestamp are 160, 160, 128, 160, 160, 160, and 32 bits, respectively.

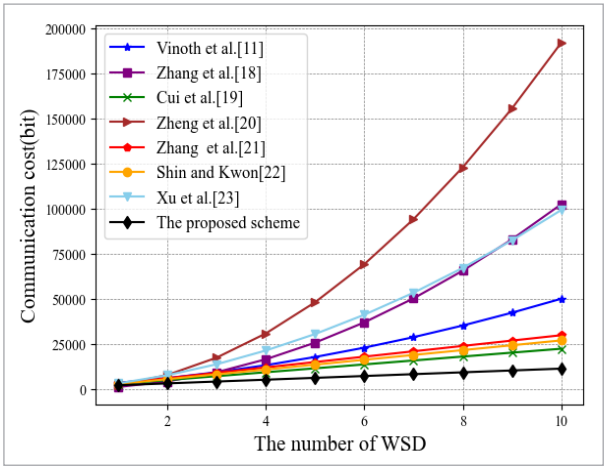
Table 5 illustrates the comparative outcomes regarding communication expenses between our proposed scheme and the pertinent schemes referenced in [19, 23, 8, 11, 15, 17, 21] in terms of communication costs, which are 3328, 1024, 2688, 1920, 2976, 2688, 3008 and 2016 bit. The total communication cost under n wearable smart devices are $320n^2 + 1664n + 1344$, $1024n^2$, $2176n + 512$, $1920n^2$, $2976n$, $2688n$, $768n^2 + 2240n$ and $1024n + 992$ bit.

Table 5
Comparison of Communication Cost

Schemes	Communication cost(bits)			Total communication cost(bits)	
	U_i	GW	WSD_j	a wearable smart device	n wearable smart devices
Vinoth et al. [19]	512	2144	672	3328	$320n^2$ +1664n + 1344
Zhang et al. [23]	N/A	N/A	1024	1024	$1024n^2$
Cui et al. [8]	672	832	1184	2688	$2176n + 512$
Zheng et al. [11]	N/A	N/A	1920	1920	$1920n^2$
Zhang et al. [15]	864	512	1600	2976	$2976n$
Shin et al. [17]	992	1184	512	2688	$2688n$
Xu et al. [21]	N/A	N/A	3008	3008	$768n^2 + 2240n$
Our Scheme	320	1024	672	2016	$1024n + 992$

Figure 4 illustrates how the total communication cost correlates with the quantity of wearable smart devices. It is observable that the communication cost of the proposed scheme is the smallest among all the schemes, and the gap between the rest of the schemes and the present scheme is getting wider and wider as the number of wearable smart devices increases. Under the premise of satisfying the above mentioned versatility and security, our solution achieves the minimisation of communication costs and greatly improves the ability to promote the application in cyber-physical system area equipment. Compared with the related scheme [19, 23, 8, 11, 15, 17, 21] the communication cost of our scheme is reduced by 0.77%, 0.89%, 0.49%, 0.94%, 0.62%, 0.58% and 0.88%, respectively (in case the number of equipment is 10). With the shortage of resources in the cyber-physical system, the scheme saves communication overheads to a great extent. In the digital healthcare multi-device communication scenario, the scheme has strong generalization capability and adaptability, which provides strong support for the further landing application of the scheme.

Figure 4
Communication Cost Versus Number of Wearable Smart Device



7. Conclusions and Future Work

In this paper, we study the problem of communication authentication for users, gateways and multiple devices in digital healthcare cyber-physical systems. We propose a secure lightweight multi-party key authentication protocol to meet the authentication requirements of users, gateways and multi-devices, which uses bilinear pairs to solve the key anti-exposure problem. Only one key session needs to be established between the user and the wearable smart device to achieve multi-device key authentication, which greatly simplifies the authentication process, reduces the communication overhead and computational complexity, and increases the generalization capability of the scheme. We have conducted rigorous security proofs and analyses of the proposed scheme, and the results show that the proposed key agreement can cope with attacks in most scenarios, and due to its low communication and computation overhead, it

greatly improves its generalizability, and has a good generalization and application capability in the cyber-physical domain.

In the subsequent research work, we will continue to dig deeper into more efficient, convenient and robust key authentication and management protocols on the basis of ensuring the security of user communication and ensure that the protocol can be applied to multi-device transmission scenarios. In addition, we will also consider breaking through the difficulties of key authority control as well as user access control, and expand the concepts proposed in this paper to more application areas.

Acknowledgment

This work was supported in part by the Science and Technology Program of Guizhou Province (Grant-Number: [2023]434), and by the National Natural Science Foundation of China under Grants 62272124 and 2266010, the National Key Research and Development Program of China under Grant 2022YFB2701400 and the Natural Science Researching Program of D.o.E. of Guizhou (No. Qian Edu. Tech. [2023] 065, Qian Edu. Tech. [2023]014). We express our gratitude to the anonymous reviewers who have selflessly dedicated their time and expertise. Their insightful suggestions have significantly improved the manuscript's quality.

References

1. Adel, A. Future of Industry 5.0 in Society: Human-Centric Solutions, Challenges, and Prospective Research Areas. Journal of Cloud Computing, 2022, 11(1), 40. https://doi.org/10.1186/s13677-022-00314-5
2. Al-Ghuraybi, H. A., AlZain, M. A., Soh, B. Ensuring Authentication in Medical Cyber-Physical Systems: A Comprehensive Literature Review of Blockchain Technology Integration with Machine Learning. Multimedia Tools and Applications, 2024, 83(12), 35673-35707. https://doi.org/10.1007/s11042-023-17065-3
3. Alladi, T., Chamola, V., Sikdar, B., Choo, K. R. Consumer IoT: Security Vulnerability Case Studies and Solutions. IEEE Consumer Electronics Magazine, 2020, 9(2), 17-25. https://doi.org/10.1109/MCE.2019.2953740
4. Bhattacharya, P., Tanwar, S., BodkheKumar, U., Tyagi, S., Kumar, N. BinDaaS: Blockchain-Based Deep-Learning-as-a-Service in Healthcare 4.0 Applications. IEEE Transactions on Network Science and Engineering, 2021, 8(2), 1242-1255. https://doi.org/10.1109/TNSE.2019.2961932
5. Canetti, R., Krawczyk, H. Universally Composable Notions of Key Exchange and Secure Channels. Advances in Cryptology (EUROCRYPT 2002), Berlin, Heidelberg, 2002, 337-351. https://doi.org/10.1007/3-540-46035-7_22
6. Cao, X., Dang, L., Fan, K., Zhao, X., Fu, Y., Luan, Y. A Dynamic and Efficient Self-Certified Authenticated Group Key Agreement Protocol for VANET. IEEE Internet of Things Journal, 2024, 11(17), 29146-29156. https://doi.org/10.1109/JIOT.2024.3406757
7. Chen, F., Tang, Y., Wang, C., Huang, J., Huang, C., Xie, D., Wang, T., Zhao, C. Medical Cyber-Physical Systems: A Solution to Smart Health and the State of the Art. IEEE Transactions on Computational Social Systems, 2022, 9(5), 1359-1386. https://doi.org/10.1109/TCSS.2021.3122807
8. Cui, J., Zhang, X., Zhong, H., Zhang, J., Liu, L. Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment. IEEE Transactions on Information Forensics and Security, 2020, 15, 1654-1667. https://doi.org/10.1109/TIFS.2019.2946933
9. Dolev, D., Yao, A. On the Security of Public Key Protocols. IEEE Transactions on Information Theory, 1983, 29(2), 198-208. https://doi.org/10.1109/TIT.1983.1056650
10. Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., Alazab, M. Zero-Knowledge Proofs-Based Authenticated Key Agreement Protocol for Sustainable Healthcare. Sustainable Cities and Society, 2022, 80, 103766. https://doi.org/10.1016/j.scs.2022.103766
11. Jun, Z., Cheng, Y., Jinrong, X., Can, Z. A Dynamic ID-Based Authenticated Group Key Agreement Protocol. Proceedings of the 2015 4th National Conference on Electrical, Electronics and Computer Engineering, Atlantis Press, 2015, 1079-1084. https://doi.org/10.2991/nceece-15.2016.192
12. Li, X., Jiang, C., Du, D., Fei, M., Wu, L. A Novel Revocable Lightweight Authentication Scheme for Resource-Constrained Devices in Cyber-Physical Power Systems. IEEE Internet of Things Journal, 2023, 10(6), 5280-5292. https://doi.org/10.1109/JIOT.2022.3221943
13. Mathkor, D. M., Mathkor, N., Bassfar, Z., Bantun, F., Slama, P., Ahmad, F., Haque, S. Multirole of the Internet of Medical Things (IoMT) in Biomedical Systems for Managing Smart Healthcare Systems: An Overview of Current and Future Innovative Trends. Journal of In-

fection and Public Health, 2024, 17(4), 559-572. https://doi.org/10.1016/j.jiph.2024.01.013

14. Ming, Y., Yang, P., Mahdikhani, H., Lu, R. A Secure One-to-Many Authentication and Key Agreement Scheme for Industrial IoT. IEEE Systems Journal, 2023, 17(2), 2225-2236. https://doi.org/10.1109/JSYST.2022.3209868
15. Qikun, Z., Yong, G., Quanxin, Z., Ruifang, W., Yu-An, T. A Dynamic and Cross-Domain Authentication Asymmetric Group Key Agreement in Telemedicine Application. IEEE Access, 2018, 6, 24064-24074. https://doi.org/10.1109/ACCESS.2018.2799007
16. Shamshad, S., Mahmood, K., Hussain, S., Garg, S., Das, A. K., Kumar, N., Rodrigues, J. J. P. C. An Efficient Privacy-Preserving Authenticated Key Establishment Protocol for Health Monitoring in Industrial Cyber-Physical Systems. IEEE Internet of Things Journal, 2022, 9(7), 5142-5149. https://doi.org/10.1109/JIOT.2021.3108668
17. Shin, S., Kwon, T. A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things. IEEE Access, 2020, 8, 1. https://doi.org/10.1109/ACCESS.2020.2985719
18. Verma, R. Smart City Healthcare Cyber-Physical System: Characteristics, Technologies, and Challenges. Wireless Personal Communications, 2022, 122(2), 1413-1433. https://doi.org/10.1007/s11277-021-08955-6
19. Vinoth, R., Deborah, L. J., Vijayakumar, P., Kumar, N. Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT. IEEE Internet of Things Journal, 2021, 8(5), 3801-3811. https://doi.org/10.1109/JIOT.2020.3024703
20. Xu, Z., Li, F., Deng, H., Tan, M., Zhang, J., Xu, J. A Blockchain-Based Authentication and Dynamic Group Key Agreement Protocol. Sensors (Basel), 2020, 20(17). https://doi.org/10.3390/s20174835
21. Xu, Z., Liang, W., Li, K., Xu, J., Zomaya, A. Y., Zhang, J. A Time-Sensitive Token-Based Anonymous Authentication and Dynamic Group Key Agreement Scheme for Industry 5.0. IEEE Transactions on Industrial Informatics, 2022, 18(10), 7118-7127. https://doi.org/10.1109/TII.2021.3129631
22. Zhang, D., Wang, Q., Feng, G., Shi, Y., Vasilakos, A. V. A Survey on Attack Detection, Estimation, and Control of Industrial Cyber-Physical Systems. ISA Transactions, 2021, 116, 1-16. https://doi.org/10.1016/j.isatra.2021.01.036
23. Zhang, J., Cui, J., Zhong, H., Bolodurina, I., Liu, L. Intelligent Drone-Assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-Hoc Networks. IEEE Transactions on Network Science and Engineering, 2021, 8(4), 2982-2994. https://doi.org/10.1109/TNSE.2020.3029784