bioengineering

MDPI

Article

Securing Group Patient Communication in 6G-Aided Dynamic Ubiquitous Healthcare with Real-Time Mobile DNA Sequencing

Tuan-Vinh Le [1,2]

[1] Bachelor's Program of Artificial Intelligence and Information Security, College of Science and Engineering, Fu Jen Catholic University, New Taipei 24206, Taiwan; 155315@mail.fju.edu.tw
[2] Bachelor's Program of Medical Informatics and Innovative Applications, College of Science and Engineering, Fu Jen Catholic University, New Taipei 24206, Taiwan

Abstract: (1) Background: With an advanced technique, third-generation sequencing (TGS) provides services with long deoxyribonucleic acid (DNA) reads and super short sequencing time. It enables onsite mobile DNA sequencing solutions for enabling ubiquitous healthcare (U-healthcare) services with modern mobile technology and smart entities in the internet of living things (IoLT). Due to some strict requirements, 6G technology can efficiently facilitate communications in a truly intelligent U-healthcare IoLT system. (2) Research problems: conventional single user–server architecture is not able to enable group conversations where "multiple patients–server" communication or "patient–patient" communication in the group is required. The communications are carried out via the open Internet, which is not a trusted channel. Since heath data and medical information are very sensitive, security and privacy concerns in the communication systems have become extremely important. (3) Purpose: the author aims to propose a dynamic group-based patient-authenticated key distribution protocol for 6G-aided U-healthcare services enabled by mobile DNA sequencing. In the protocol, an authenticated common session key is distributed by the server to the patients. Using the key, patients in a healthcare group are allowed to securely connect with the service provider or with each other for specific purposes of communication. (4) Results: the group key distribution process is protected by a secure three-factor authentication mechanism along with an efficient sequencing-device-based single sign-on (SD-SSO) solution. Based on traceable information stored in the server database, the proposed approach can provide patient-centered services which are available on multiple mobile devices. Security robustness of the proposed protocol is proven by well-known verification tools and a detailed semantic discussion. Performance evaluation shows that the protocol provides more functionality and incurs a reasonable overhead in comparison with the existing works.

Keywords: 6G technology; third-generation sequencing (TGS); DNA-reading biosensor; ubiquitous healthcare (U-healthcare); patient-centric care; internet of living things (IoLT); dynamic group patient communication; sequencing-device-based single sign-on (SD-SSO); biometric authentication; elliptic curve cryptography (ECC)

Citation: Le, T.-V. Securing Group Patient Communication in 6G-Aided Dynamic Ubiquitous Healthcare with Real-Time Mobile DNA Sequencing. *Bioengineering* **2023**, *10*, 839. https://doi.org/10.3390/bioengineering10070839

Academic Editors: Mihaela Hnatiuc, Larbi Boubchir and Victor Hugo C. De Albuquerque

Received: 24 May 2023
Revised: 18 June 2023
Accepted: 14 July 2023
Published: 15 July 2023

1. Introduction

Third-generation sequencing (TGS) provides services with long deoxyribonucleic acid (DNA) reads and super short sequencing time [1–3]. In this technique, since single DNA molecules are sequenced directly, the sequencing time is reduced to a few hours, and even real-time data analysis process is enabled. In addition, TGS-based sequencers can be miniaturized while its DNA-reading biosensors are placed on the body to monitor human health and vital signs via blood, sweat, saliva, tissue, etc. [3]. This enables an onsite mobile DNA sequencing solution for facilitating ubiquitous healthcare (U-healthcare) services with modern mobile technology and smart systems in the internet of living things (IoLT) [3,4].

For instance, as shown in Figure 1, the SmidgION sequencer is a tiny device designed by the Oxford Nanopore [5] to be run on mobile devices (e.g., smart phones) using small batteries and apps [3]. The biosensors load biological samples into the sequencer, and the genomic data (e.g., FAST5 file, FASTQ file, or TXT file [5]) along with its analytical results are produced, building a sort of "lab-on-a-chip (LOC)" system [3,5–7]. Therefore, medical providers can rapidly screen for new viruses, paving a way for further discovering the IoLT. The researchers can also obtain onsite DNA sequences for specific end-to-end analysis. The U-healthcare is directly concerned with patient-centric therapies. To this end, a real-time mobile DNA sequencing service is completely a good fit as it can provide personalized treatments and holds promise for precision medicine research.

Figure 1. New innovative sequencers of the Oxford Nanopore [8].

Due to its excellent mobility, high operating frequency, high data transfer rate, and super low end-to-end communication delay, 6G mobile technology is attracting much attention in various application fields [9–11]. Strict requirements of 6G, which cannot be achieved by 5G, were particularly introduced for the healthcare sector, including an operating frequency of $\geq$1 THz, data transfer rate of $\geq$1 Tbps, communication delay of $\leq$1 ms, mobility of $\geq$1000 km/h, reliability of 10^{-9}, and a wavelength of $\leq$300 µm [10]. Due to such advances, 6G can efficiently support artificial intelligence (AI) functionalities [12] with seamless communications. As a matter of fact, it has certain advantages in establishing a truly intelligent U-healthcare IoLT system enabled by real-time mobile NDA sequencing techniques and advanced medical analysis. Patients and healthcare providers are allowed to communicate with each other in a reliable and high-speed network environment, possibly sharing large files or a huge amount of data.

1.1. Research Problems

Apart from individual services, healthcare providers may provide some special treatments for groups of patients (e.g., family). These patients may have similar diseases, signs, or symptoms. They can also be persons those who need similar procedures in the healthcare processes or medical treatments. Traditional single user–server architecture is not able to provide such group conversations where "multiple patients–server" communications and "patient–patient" communications are required.

The communications are carried out via the open Internet, which is not a trusted channel. Because heath data and medical information are very sensitive, security and privacy concerns in the communication systems have become extremely important. Cyber criminals may perform various attacks that can steal personal information of patients, violate user privacy, or disrupt services (e.g., impersonation attacks). During communication, care providers (e.g., medical professionals, physicians, doctors, etc.) also need to verified as a legitimate entity to avoid possibly fraudulent services or fake behaviors.

The U-healthcare services may be provided by different institutions, including hospitals, clinics, etc.; the number of services (e.g., hematologist, cardiologist, gastroenterologist, etc. [13]) is increasing over time. Therefore, the traditional single-server system model would be unable to satisfy the demand of users once they wish to enjoy massive medical services. When using services from multiple providers, remembering massive amounts of credentials (especially user passwords) for the login will certainly induce inconvenience and directly affect the efficiency of communications. In these systems, how to alleviate computational overhead and communicational overhead is also an important concern that needs to be considered.

1.2. Goals and Contributions

This paper proposes a dynamic group-based patient-authenticated key distribution protocol for 6G-aided U-healthcare services enabled by real-time mobile DNA sequencing. In the protocol, an authenticated common session key is distributed by the server to the patients. Using the key, patients in a healthcare group are allowed to securely connect with the service provider or with each other for specific purposes of communication. The author aims to introduce a protocol that achieves multiple innovative functionalities, high security robustness, and reasonable communication overhead. The main contributions of the paper are presented as follows.

(1) This work is the first to introduce 6G-assisted group-based U-healthcare services enabled by a real-time DNA sequencing technique constructed in IoLT environments. A patient-grouping solution helps in accelerating service communications and achieving better medical-centered services. With the assistance of 6G technology, onsite sequencing data produced by a portable TGS-based sequencer (connected to a patient's mobile device) is transmitted to the server in a real-time manner for further healthcare processes. Thereafter, the server shares analytical results and related medical information with the patients. These procedures are secured by common group keys generated by the proposed protocol. The server is also allowed to trace the users based on their registered information for achieving a truly patient-centric service.

(2) In the proposed protocol, a sequencing-device-based single sign-on (SD-SSO) function is introduced for the first time. Patients are allowed to store a single set of credentials (registered with multiple servers) on their DNA sequencers directly. Due to the SSO property, the patients only need to login to the system once per session to communicate with multiple providers. In addition, the proposed SD-SSO function is designed without the participation of a third-party center, which can reduce communication overhead and address the risk of adversaries hacking into the registration center and compromising all servers.

(3) A three-factor authentication mechanism is enabled in the protocol through the integration of password (the first factor), sequencing device (the second factor), and biometrics (the third factor). Lacking only one of the three factors will result in failure of the authentication. In this way, better patient privacy and perfect forward secrecy of group keys are assured for securing U-healthcare communications. In the protocol, patient password and patient biometrics are changeable, which further enhances the security robustness.

(4) The author introduces dynamic U-healthcare services enabled by a time-bound function. In this design, different services of a provider or multiple healthcare processes in a single service can be allotted in respective time ranges in accordance with specific requests. This solution makes providers flexibly adjust service time in order to provide more efficient medical processes as well as more convenient treatments for different kinds of patients. Controlling such access to the services using the time bounds can also address possible bottleneck issues where the services are requested at the same time by massive patients. Furthermore, a fast synchronizable key-derivation procedure is provided, which can rapidly reset communication keys for addressing desynchronization problems that could possibly occur in such a dynamic environment.

1.3. Paper Organization

The remainder of this article is structured as follows. Section 2 presents related works of the proposed protocol. Some technical preliminaries used in the work are provided in Section 3. In Section 4, the problem formulation describes the architecture model and formal security model of the proposed work. Section 5 details the design of the proposed protocol. Security evaluation and performance analysis of the proposed protocol are provided in Sections 6 and 7, respectively. The author concludes the proposal and discusses some of his future research works in the last section of the article.

2. Related Works

2.1. 5G, 6G, and U-Healthcare

In many countries, 5G mobile technology has been successfully developed and deployed as an enabler for supporting various sorts of networks and diverse applications [14]. However, in the era of digital transformation and emerging smart internet of things (IoT) applications, 5G needs some more advances to improve service delivery and business [15]. Moreover, 5G has some drawbacks and limitations in terms of functionalities in healthcare sector; for instance, it cannot provide holographic communication for medical applications due to its lower data rate [9,16]. To this end, 6G was introduced to fully address escalating technical demands, e.g., remote robotic surgery or other truly intelligent healthcare services enabled by the Intelligent Radio (IR) technique [17]. It achieves an ultra-high bandwidth (three times higher than that of 5G [18,19]) and a highly dynamic environment with a terahertz (THz) signal [18]. Therefore, 6G offers an ultra-high data transfer rate for revolutionizing U-healthcare communications. It is also fully backed by satellite [20], which completely facilitates ubiquitous care activities in medical networks at every geographical location. This article introduces a construction of 6G wireless technology for a time-bound-enabled DNA-based group healthcare application via IoLT-based biosensor networks. In addition, to the best of the author's knowledge, this is the first work to address security and privacy issues in a dynamic U-healthcare communication environment.

2.2. User Authentication and Key Negotiation Solutions

User authentication and key agreement solutions were discussed in many previously published works. Deebak and Al-Turjman [21] introduced a patient authentication scheme used in healthcare systems with cloud services; it overcame several security challenges that had been not successfully addressed in the protocol of Chiou et al. [22], e.g., lost device attacks or server impersonation attacks. Wang et al. [23] also proposed an improved key agreement mechanism for wireless body area networks (WBANs) that resolved some similar issues of Farash et al. [24]'s work. Kumar et al. [25] discussed a single-factor password-based patient authentication solution for cloud-based healthcare systems in the internet of medical things (IoMT). A two-factor data authentication scheme with access control was proposed by Gupta et al. [26] for an industrial healthcare infrastructure. Alam and Kumar [27] designed a session key establishment protocol for ensuring confidentiality of IoMT-based communications in COVID-19 and future pandemic scenarios. In addition, Thakare and Kim [28] discussed another two-factor cryptographic approach for user authentication in IoT networks, and Yu et al. [29] introduced a biometrics-based multi-server user authentication and key agreement mechanism using extended chaotic maps. Wong et al. [30] introduced a three-factor identification model applied to 5G-enabled e-health environments with multi-server architecture. However, Le and Hsu [31] indicated that biometrics noise had not been discussed and resolved in Wong et al. [30]'s work, which always makes the authentication procedure incorrect. Le and Hsu [31] then discussed various solutions [32] (error-correcting codes, fuzzy extractor, biohash function, etc.) for remedying this issue and proposed an improved protocol for securing communications in group e-health services. The author found the protocol of Le and Hsu [31] is not robust against stolen smart-card attacks as adversaries can obtain patients' passwords in unmasked forms using the power analysis method [33]. Another design of lightweight

group key agreement presented by Harn et al. [34] exploited some basic cryptographic operations and explained its potentials in several application networks. Based on principles of elliptic-curve cryptography (ECC), Tselikis et al. [35] also introduced an group key distribution scheme that provided privacy protection for communications. Both Harn et al. [34] and Tselikis et al. [35] did not include either biometric authentication function or three-factor authentication solutions in their designs. Meshram et al. [36] proposed a remote user password-based key negotiation scheme for application in smart cities based on smart cards and extended chaotic maps. Nevertheless, the service provider in Meshram et al. [36]'s scheme has to update a dynamic parameter in the database before each authentication is completed. This would sometimes result in unexpected desynchronization problems in the system. Based on the author's observation, although Thakare and Kim [28] and Meshram et al. [36] achieved user anonymity in their works, both are not able to assure user untraceability. Communicated transcripts in their proposed schemes contain fixed parameters that give adversaries opportunities to trace users' identities. Le [37] recently introduced a cross-server-authenticated patient key exchange protocol for U-healthcare in IoLT networks. Apart from its security robustness, Le [37]'s protocol cannot provide truly patient-centric services, as the server does not store any information of patients after its registration procedure finishes. In the registration phase of Le [37]'s approach, some credentials of the patients are stored in a single mobile entity, which cannot make U-healthcare services available on multiple devices. Furthermore, none of the above works discussed dynamic healthcare communication in group-based services.

3. Preliminaries

This section discusses some important technical aspects and mathematical preliminaries employed in the proposed approach, including sequencing biosensor technology, the biohash function, the time-bound function, and security complexity assumptions.

3.1. Sequencing Biosensor Technology

Second-generation sequencing (SGS) techniques, also known as next-generation sequencing (NGS) techniques, enable the process where millions of short deoxyribonucleic acid (DNA) fragments are sequenced in parallel [38]. Nevertheless, SGS comes with some drawbacks, including short read lengths and nonportability of the sequencers. In recent years, innovative healthcare services and medical research have required longer reads and shorter sequencing times, which led to the advent of TGS [3] and fourth-generation sequencing (FGS) [39]. From TGS, single DNA molecules are sequenced directly, reducing processing time from a few days to a few hours and enabling real-time analysis with sequence-based ultrarapid pathogen identification [3]. Sequencing devices can be miniaturized (for instance, SmidgION sequencer), and built-in DNA-reading biosensors on each tiny TGS-based sequencer can collect biological samples for monitoring human health and vital signs. In the proposed protocol, besides the sequencing function, the sequencer also serves as a token that stores user credentials used for authentication process, enabling service availability on multiple mobile devices including smart phones, smart tablets, etc. It is employed as the second authentication factor (something you have) in the proposed approach.

3.2. Biohash Function

As we know, biometric samples are enrolled via a noisy channel. The input biometrics samples in each authentication session are not identical; as a result, it causes false positive errors of the authentication. To this end, the biohash function can map the individuals' biometrics to specific binary strings and effectively tolerate noise [32]. Security of the biohash function is similar to conventional one-way hash functions [31]. The function also resolves the efficiency issue, which is a drawback of some related ideas, for instance, fuzzy extractor [32].

Definition 1. *Given a biohash function h_{bio}, the original biometrics B_i, and the newly input biometrics B_i' of an individual, it is inferred that B_i is different to B_i', but the difference between them is within a certain threshold. Due to the property of h_{bio}, we can achieve $h_{bio}(B_i) = h_{bio}(B_i')$.*

3.3. Time-Bound Function

Definition 2. *Given three time points $t, t_1, t_2 \in \{1, 2, \ldots, z\}$ and two values $p = h^{t_1-1}(\square)$ and $q = h^{z-t_2}(\triangle)$, where h is a one-way hash function and "$\square$, $\triangle$ " denotes some arbitrary parameters, a value $w = h(h^{t-t_1}(p)||h^{t_2-t}(q))$ is computable if and only if t satisfies $t_1 \leq t \leq t_2$. Note that z may be 24 (h), 1440 (min), or some value specifying the time of a single day. z may also be set for multiple days or more, based directly on time allocations of specific services and on security level of systems.*

3.4. Complexity Assumptions

The ECC is employed in the proposed approach. It is an asymmetric cryptosystem that offers better performance with smaller key space considering the same security level compared with the traditional ones [37]. Therefore, the ECC system is completely suitable for mobile communications in IoLT networks. In the proposed work, the author employs three security assumptions of the ECC including the elliptic curve discrete logarithm problem (ECDLP), the elliptic curve computational Diffie–Hellman problem (ECCDHP), and the elliptic curve factorization problem (ECFP). Suppose there is an elliptic curve $Ep(a, b) : y^2 = x^3 + ax + b(mod\ p)$ over a finite field Fp with a basic point $G_{(x,y)} \in E_p$; the assumptions are defined as follows.

Definition 3. *The ECDLP is to find the scalar $k \in Z_p$ such that $K_{(x,y)} = k \cdot G_{(x,y)}$, given $G_{(x,y)}, K_{(x,y)} \in E_p$.*

Definition 4. *The ECCDHP is to find the point $s \cdot t \cdot G_{(x,y)} \in E_p$, given $s, t \in Z_p$ and $G_{(x,y)}, s \cdot G_{(x,y)}$, $t \cdot G \in E_p$.*

Definition 5. *The ECFP is to find two points $s \cdot G_{(x,y)}, t \cdot G_{(x,y)} \in E_p$, given $s, t \in Z_p$ and $G_{(x,y)}, [s + t] \cdot G_{(x,y)} \in E_p$.*

4. Problem Formulation

This section discusses in details system model of the proposed approach along with some well-known adversarial capabilities. A well-known security model is also formulated based upon the rule of the protocol. Main cryptographic functions and notations used in the work are tabulated in Table 1.

Table 1. Notations used in the proposed approach.

Notation Used in the Protocol	Explanation
S_j	The j^{th} server
P_i	The i^{th} patient
prk_j, puk_j	Private key, public key of S_j
$P_{(x,y)}$	Basic point on the curve $Ep(a, b)$ with two coordinates x and y
ID_i	Identity of P_i
PW_i	Password of P_i
B_i	Biometrics of P_i
MD_i	Mobile device of P_i
SD_i	Sequencing device (sequencer) of P_i

Table 1. *Cont.*

Notation Used in the Protocol	Explanation
T	Timestamp
$\|\|$	Concatenating operation
$\oplus$	Exclusive-or (XOR) operation
$h(\cdot), h_{bio}(\cdot)$	One-way hash function, biohash function
$SE_k(\cdot), SD_k(\cdot)$	Symmetric encryption, symmetric decryption using a key k
$[\cdot]_{SD_i}$	Storing parameters in SD_i
$\mathcal{A}$	Adversary

4.1. System Model and Adversarial Capabilities

As shown in Figure 2, the main communicating entities in the system include patient P_i (in a group of multiple patients) and servers S_j (e.g., private doctors, genomic data scientists, etc.) who communicate with each other for conducting group services. DNA-based U-healthcare includes various services, namely, disease virus control, body fluid monitoring, blood-based prognostic tracking, and so on [3,40]. Taking family healthcare services as an example, multiple members P_i in a family may request a common DNA-based healthcare service provided by S_j. The service allows the family members to obtain medical data shared among them and to know of the health status of each other conveniently. As a spiritual element, family plays an important role in promoting our health as well as in improving quality of life [41]. In case of need, a family member may also render timely assistance to doctors in observing the other members' states of illness. Thus, it would significantly improve efficiency of long-term care or treatments and help in reducing the risk of medical incidents. To trigger the services, biological samples of P_i (e.g., saliva) are loaded into the sequencer SD_i that is inserted into P_i's mobile device MD_i in advance. Next, an onsite sequencing and data analysis process is run directly on SD_i; the DNA sequencing data generated is transmitted to S_j for point-of-care services. This procedure is secured by the group session key distributed by S_j to P_i in the proposed protocol. Since all patients receive an identical key from S_j, P_i is also able to share the data with other patients in the group. Thereafter, analytical results and related medical information based on the received DNA data are encrypted by the key before being sent back to a single patient or to multiple patients of the group. In the proposed architecture, these communications are carried out via the IR signal of the 6G technology. Due to its extremely high data transfer rate, 6G can offer a fully seamless experience for real-time U-healthcare services with large data sets produced by onsite mobile DNA sequencing. P_i can enjoy the services without constraints of time and physical location. As mentioned, a dynamic healthcare solution is also introduced in the system which allows the services to be flexibly allotted by separate time-bounds based on specific requests. Furthermore, the author recommends integrating some related advances, e.g., WBAN, into the system to enhance efficiency of the overall healthcare treatment process.

Prior to starting using the above services, P_i should register with multiple S_j using three factors, namely, password PW_i, sequencing device SD_i, and his/her biometrics B_i, establishing a multi-server communication environment. In order to receive the group keys, P_i uses a single set of registered credentials stored in SD_i to carry out the SD-SSO that sends a login and authentication request to S_j through a public IoLT network. In such an unreliable channel, there are possible security attacks that may induce serious consequences, e.g., violating patient privacy, destructing system architecture, or reducing reliability and quality of service, etc. Based on the author's observation, an adversary $\mathcal{A}$ may have the following capabilities to attack the proposed communication system.

- $\mathcal{A}$ has full control over the open IoLT, which enables $\mathcal{A}$ to intercept, insert, delete, or replay any transcripts conveyed between P_i and S_j.

- $\mathcal{A}$ may attempt to attack the past communications between P_i and S_j based on secret parameters or on a group session key $\mathcal{A}$ somehow retrieves from the current communicated messages.
- $\mathcal{A}$ may attempt to extract the secret values or registered credentials stored in a compromised SD_i and use them to attack the communication.
- $\mathcal{A}$ may be a privileged insider (e.g., member of a maintenance team) who can launch even more serious attacks upon a patient's registered information obtained from DB_j.
- $\mathcal{A}$ may also be a corrupted P_i or S_j that can trigger similar attacks on the communication.

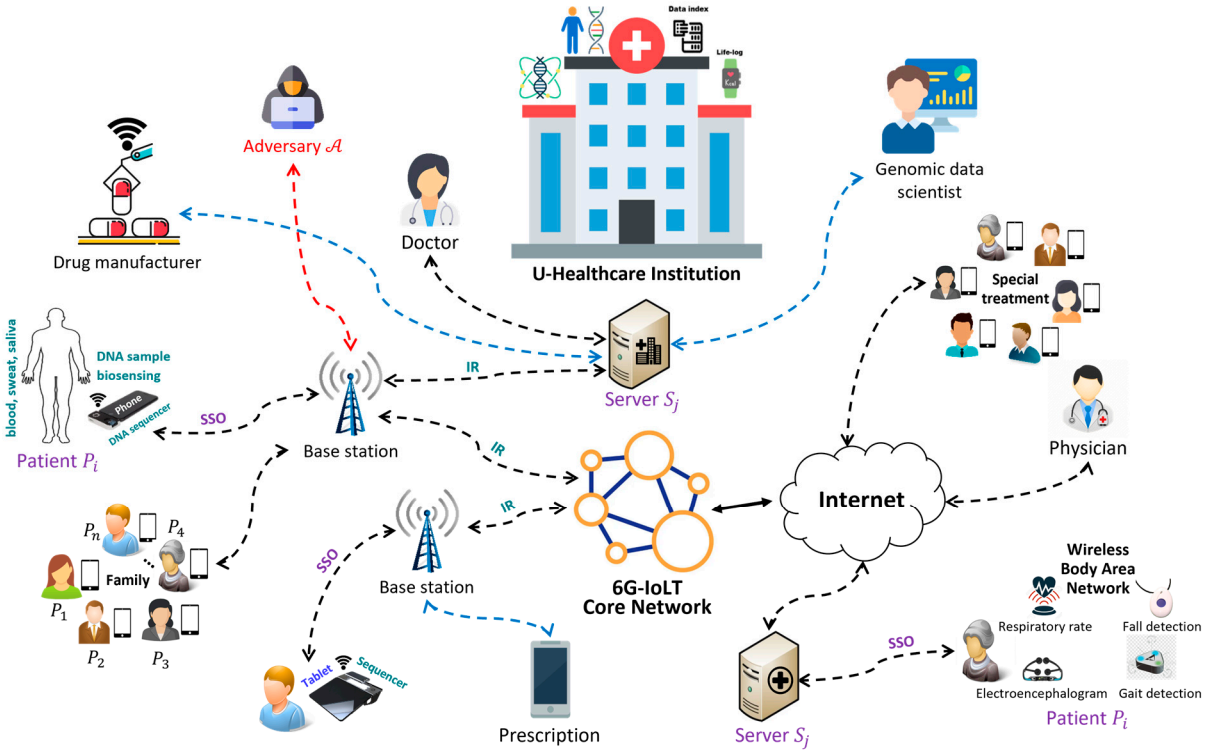

Figure 2. Architecture model of the proposed protocol.

4.2. Formal Security Model

Real-or-Random (RoR) is a well-known formal model used for analyzing success probability of an adversary in attacking cryptographic protocols [42]. In the model, suppose there are two main entities including a patient P and a server S who are communicating with each other via a public channel. Ç denotes a protocol challenger while the message communicated by P and S is denoted as m. The following queries should be executed by an adversary $\mathcal{A}$ to make various attacks.

(1) *Send*(Ç, m): This query allows $\mathcal{A}$ to request a message m to Ç; Ç replies to $\mathcal{A}$ based upon the procedure of the proposed protocol.
(2) *Execute*(P, S): In this query, $\mathcal{A}$ is allowed to eavesdrop the message m conveyed between P and S.
(3) *Reveal*(Ç): This query enables $\mathcal{A}$ to retrieve a session key computed by Ç in accordance with the procedure of the protocol.
(4) *Corrupt*(P, w): In a three-factor authentication protocol, this query returns to $\mathcal{A}$ password PW_i, parameters stored in sequencing device SD_i, and biometrics B_i if $w = 1$, $w = 2$, and $w = 3$, respectively.
(5) *Test*(Ç): This is a statistical test query. $\mathcal{A}$ is allowed to directly request Ç for the session key; Ç probabilistically replies to $\mathcal{A}$ upon the outcome of a tossed coin b.

Definition 6. *Let Adv^{IoLTHC} be the advantage of $\mathcal{A}$ running in polynomial time in a semantically breaking security system of the proposed protocol. We have $Adv^{IoLTHC} = |2Pr[b' = b] - 1|$, where IoLTHC stands for IoLT-based healthcare and b' is denoted as a guessed bit of the key.*

5. The Proposed Protocol

There are five procedures in the proposed protocol, including setup; user registration, login, and authentication; synchronizable key derivation; and password and biometrics change. For facilitating NDA-based U-healthcare processes, S_j is allowed to securely distribute a common key to a group of multiple P_i. The design details are as follows.

5.1. Setup Phase

At first, the system selects an elliptic curve over a finite field Fp $Ep(a,b) : y^2 = x^3 + ax + b(mod\ p)$ with a basic point $P_{(x,y)}$ of the order n of an additive cyclic group, where p is k-bit prime and n is a large number. For a neat design, the coordinates x and y of $P_{(x,y)}$ are always ignored during procedures of the protocol. S_m chooses a secret private key prk_j and computes its public key $puk_j = prk_j \cdot P$.

5.2. Registration Phase

This phase is carried out via a secure channel. P_i registers with S_j to become a legitimate patient for using U-healthcare services. As depicted in Figure 3, P_i and S_j perform the following steps for this procedure.

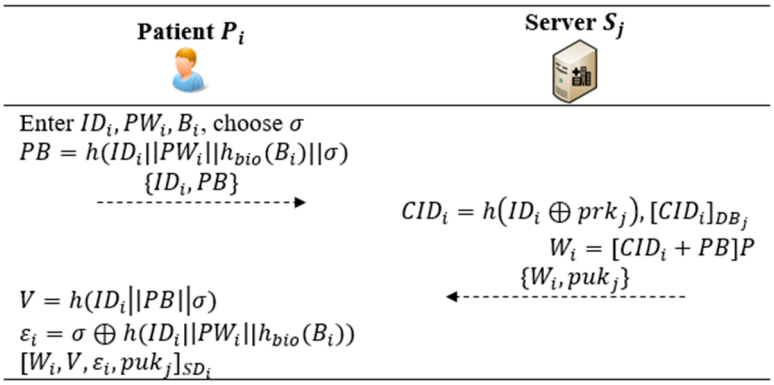

Figure 3. Registration procedure of the proposed protocol.

Step R1: P_i inserts SD_i into MD_i and selects an identity ID_i, a password PW_i, and a biometrics value B_i. P_i selects a random number σ, and computes $PB = h(ID_i||PW_i||h_{bio}(B_i)||\sigma)$. Next, P_i sends $\{ID_i, PB\}$ to S_j.

Step R2: Receiving the message $\{ID_i, PB\}$, S_j computes $CID_i = h\left(ID_i \oplus prk_j\right)$ and checks if CID_i exists in DB_j, which can trace registered users for achieving patient-centered services in the U-healthcare system. Next, S_j computes $W_i = [CID_i + PB]P$, stores CID_i in DB_j, and sends $\{W_i, puk\}$ to P_i.

Step R3: Upon the received $\left\{W_i, puk_j\right\}$, P_i computes $V = h(ID_i||PB||\sigma)$ and $\varepsilon_i = \sigma \oplus h(ID_i||PW_i||h_{bio}(B_i))$. Finally, P_i stores $\left\{W_i, V, \varepsilon_i, puk_j\right\}$ in SD_i and the registration is completed. In this way, the service availability is enabled on multiple mobile devices MD_i.

Remark 1: *Each P_i has a unique value of CID_i stored in DB_j. Based on CID_i, S_j can easily identify P_i, refer to the past records, and focus on the particular care needs of P_i, enabling patient-centered services.*

5.3. Login and Authentication Phase

This procedure is carried out via a public channel. P_i uses their registered credentials to login to S_j. P_i and S_j authenticate with each other and compute a secret shared session key

used for group healthcare communications. Suppose there are n patients participating in a group communication, Figure 4 presents the procedure where a session key is established.

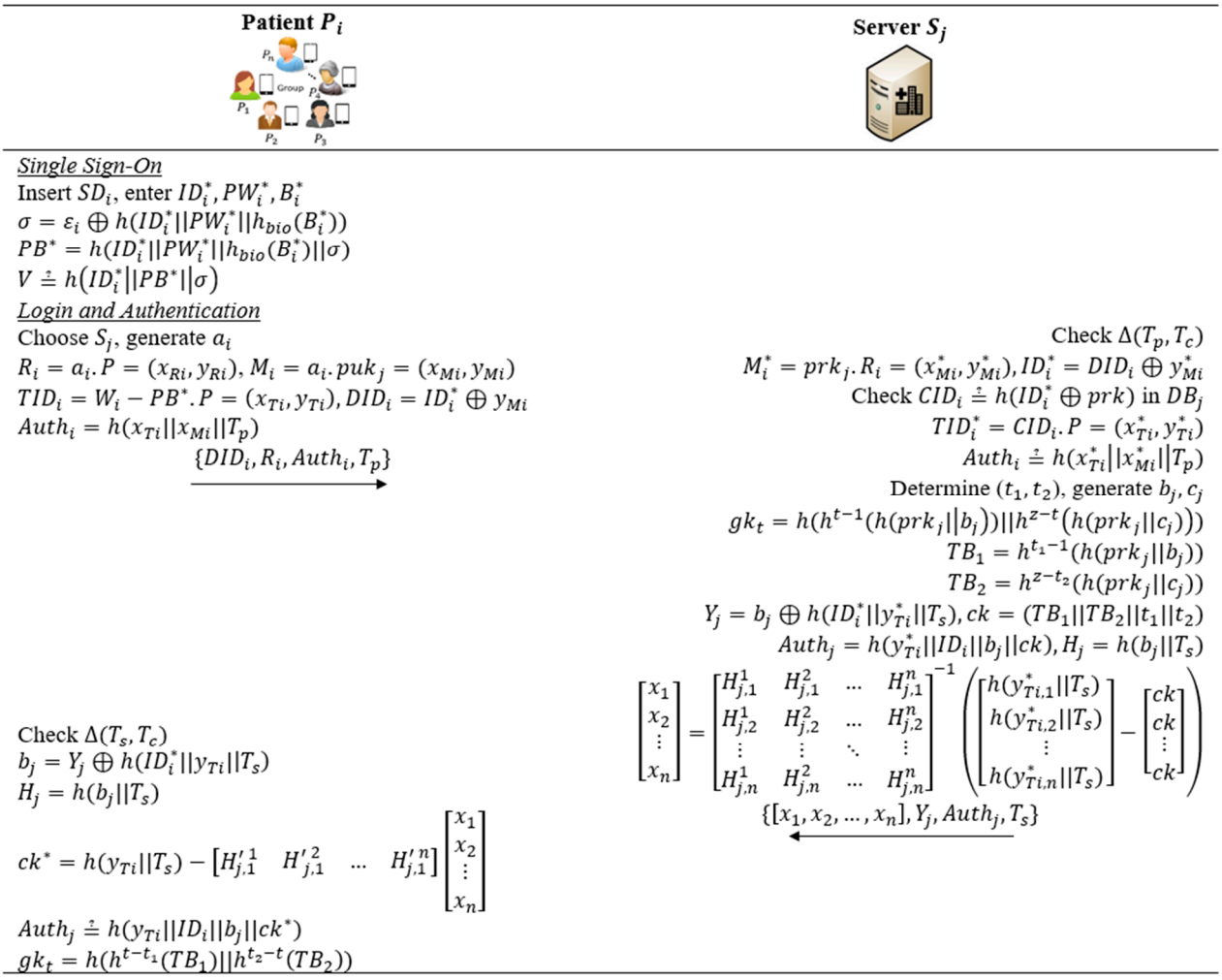

Figure 4. Login and authentication procedure of the proposed protocol.

Step A1: P_i inserts SD_i into MD_i and enters credentials ID_i^*, PW_i^*, B_i^*. P_i computes $\sigma_i = \varepsilon_i \oplus h(ID_i^* || PW_i^* || h_{bio}(B_i^*))$ and $PB^* = h(ID_i^* || PW_i^* || h_{bio}(B_i^*) || \sigma)$. The check $V \stackrel{?}{=} h(ID_i^* || PB^* || \sigma))$ is performed. If the check holds, the SD-SSO is completed and P_i is allowed to select a server S_j in the interface of an app installed in MD_i for enjoying a specific service. To this end, P_i chooses a random number a_s and a timestamp T_p, then computes $R_i = a_i \cdot P = (x_{Ri}, y_{Ri})$, $M_i = a_i \cdot puk_j = (x_{Mi}, y_{Mi})$, $TID_i = W_i - PB^* \cdot P = (x_{Ti}, y_{Ti})$, $DID_i = ID_i^* \oplus y_{Mi}$, and $Auth_i = h(x_{Ti} || x_{Mi} || T_p)$. P_i conveys message $\{DID_i, R_i, Auth_i, T_p\}$ to S_j for the purposed of login.

Step A2: Upon receiving the message $\{DID_i, R_i, Auth_i, T_p\}$, S_j checks the timestamp T_p and computes $M_i^* = prk_j \cdot R_i = (x_{Mi}^*, y_{Mi}^*)$ and $ID_i^* = DID_i \oplus y_{Mi}^*$. S_j checks $CID_i \stackrel{?}{=} h(ID_i^* \oplus prk_j)$ in its database and checks $Auth_i \stackrel{?}{=} h(x_{Ti}^* || x_{Mi}^* || T_p)$ for confirming the legitimacy of P_i. Next, S_j determines a time bound (t_1, t_2), chooses two random numbers b_j, c_j, and computes a group dynamic key at a time point t by $gk_t = h(h^{t-1}(h(prk_j || b_j)) || h^{z-t}(h(prk_j || c_j)))$. S_j computes $TB_1 = h^{t_1-1}(h(prk_j || b_j))$, $TB_2 = h^{z-t_2}(h(prk_j || c_j))$, $Y_j = b_j \oplus h(ID_i^* || y_{Ti}^* || T_s)$, $ck = (TB_1 || TB_2 || t_1 || t_2)$, and $H_j = h(b_j || T_s)$.

The value ck is masked by generating multiple $\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} H_{j,1}^1 & H_{j,1}^2 & \dots & H_{j,1}^n \\ H_{j,2}^1 & H_{j,2}^2 & \dots & H_{j,2}^n \\ \vdots & \vdots & \ddots & \vdots \\ H_{j,n}^1 & H_{j,n}^2 & \dots & H_{j,n}^n \end{bmatrix}^{-1}$ $\left(\begin{bmatrix} h(y_{Ti,1}^* || T_s) \\ h(y_{Ti,2}^* || T_s) \\ \vdots \\ h(y_{Ti,n}^* || T_s) \end{bmatrix} - \begin{bmatrix} ck \\ ck \\ \vdots \\ ck \end{bmatrix} \right)$. S_j conveys a message $\{[x_1, x_2, \dots, x_n], Y_j, Auth_j, T_s\}$ to P_i.

Step A3: Upon receiving the above message, P_i checks the timestamp T_s and computes $b_j = Y_j \oplus h(ID_i^* || y_{Ti} || T_s$, $H_j = h(b_j || T_s)$, and $ck^* = h(y_{Ti} || T_s) - \begin{bmatrix} H_{j,1}'^1 & H_{j,1}'^2 & \dots & H_{j,1}'^n \end{bmatrix}$ $\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$. Next, S_j checks $Auth_j \stackrel{?}{=} h(y_{Ti} || ID_i || b_j || ck^*)$. If the check holds, the value $ck^* = (TB_1 || TB_2 || t_1 || t_2)$ is successfully verified. S_j computes the dynamic group key at the time point t by $gk_t = h(h^{t-t_1}(TB_1) || h^{t_2-t}(TB_2))$. In this way, all members P_i in a group of n patients have received the same key gk_t for U-healthcare communications.

Remark 2: *The design allows the time bound (t_1, t_2) to be flexibly changed without having to renew the registration. P_i would be notified of the updated time bound through the app's notification during the communication session or through some channel (e.g., email) before the communication gets started.*

Remark 3: *Upon specific requests, P_i and S_j are allowed to compute multiple group keys at different time points t by $gk_t = h(h^{t-1}(h(prk_j || b_j)) || h^{z-t}\left(h(prk_j || c_j)\right))$ and by $gk_t = h(h^{t-t_1}(TB_1) || h^{t_2-t}(TB_2))$, respectively. The key gk_t is used as a symmetric encryption key to protect communications between S_j and multiple P_i, and between P_i and P_i.*

5.4. Synchronizable Key-Derivation Phase

In this procedure, P_i and S_j are allowed to quickly compute a new group key to enhance security and to address desynchronization problems in patient–patient communications or in patient–server communications. For example, S_j distributes a key gk_8 at 8:00 a.m. to the group; then, S_j uses this key for encrypting the data; if a patient P_i joins the communication at 9:00 a.m. and obtains the key gk_9, P_i is not able to decrypt the data encrypted using gk_8. It is likely that multiple patients would be in this situation or that some similar situations happen at the same time. This causes a serious communicational desynchronization in the system, since multiple keys would be generated at different time points for a single service. To this end, two values TB_1 and TB_2 should be renewed in order to reset the communication with a new common key computed without having to repeat the many steps of the previous procedure. Figure 5 describes specific steps performed in this phase.

Step D1: S_j generates a number d, which can be regarded as the number of key derivations. Upon a time point t^*, S_j computes a new group key $gk_{t^*}^d = h(h^{t^*-1}(h(prk_j || b_j || d)) || h^{z-t^*}\left(h(prk_j || c_j || d)\right))$ and two new values $TB_1^d = h^{t_1-1}(h(prk_j || b_j || d))$ and $TB_2^d = h^{z-t_2}(h(prk_j || c_j || d))$. S_j generates a symmetric ciphertext $C_d = SE_{gk_t}(TB_1^d || TB_2^d)$ using previous key gk_t, and conveys $\{C_d\}$ to P_i.

Step D2: Upon receiving the message, P_i decrypts C_d and obtains TB_1^d, TB_2^d. Finally, P_i computes the new group key by $gk_{t^*}^d = h(h^{t^*-t_1}(TB_1^d) || h^{t_2-t^*}\left(TB_2^d\right))$ at the time point t^*. In this way, the key gk_t computed in the previous phase (Section 5.3) is changed to the key $gk_{t^*}^d$ for resolving possible desynchronization issues of similar communications.

Remark 4: *The time point t and the time point t^* may or may not be identical based on the time allocation of specific services.*

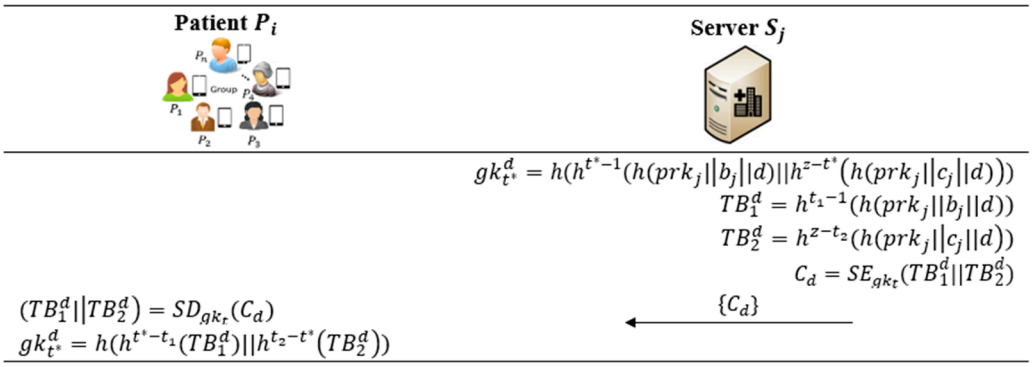

Figure 5. Synchronizable key-derivation procedure of the proposed protocol.

5.5. Password and Biometrics Change Phase

This procedure allows P_i to change their password and biometrics to enhance security. As shown in Figure 6, P_i and SD_i perform the following steps for updating these credentials.

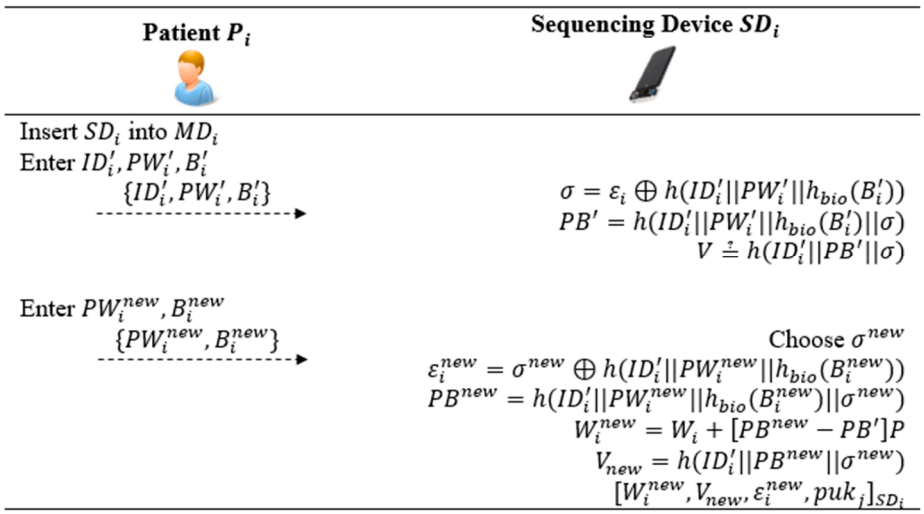

Figure 6. Password and biometrics change procedure of the proposed protocol.

Step C1: P_i inserts SD_i and enters ID_i', PW_i', B_i'. MD_i computes $\sigma = \varepsilon_i \oplus h(ID_i'||PW_i'||h_{bio}(B_i'))$ and $PB' = h(ID_i'||PW_i'||h_{bio}(B_i')||\sigma)$. It checks $V \stackrel{?}{=} h(ID_i'||PB'||\sigma)$. If the check holds, P_i is requested to enter new password PW_i^{new} and new biometrics B_i^{new}.

Step C2: Receiving PW_i^{new}, B_i^{new} from P_i, SD_i chooses a new σ^{new} and computes $\varepsilon_i^{new} = \sigma^{new} \oplus h(ID_i'||PW_i^{new}||h_{bio}(B_i^{new}))$, $PB^{new} = h(ID_i'||PW_i^{new}||h_{bio}(B_i^{new})||\sigma^{new})$, $W_i^{new} = W_i + [PB^{new} - PB]P$, and $V_{new} = h(ID_i'||PB^{new}||\sigma^{new})$. MD_i replaces W_i, V, ε_i with $W_i^{new}, V_{new}, \varepsilon_i^{new}$ in SD_i.

6. Security Certificate

In this section, the author provides the security certificate of the proposed protocol. An informal discussion, a logical analysis using BAN logic, and a formal mathematical proof using the RoR model are included for security evaluation as follows.

6.1. Sematic Security Discussion

In this subsection, the prevention of various well-known attacks in the protocol is presented in a detailed manner. The author also discusses multiple functionalities and security features achieved by the proposed work.

(1) *Replay attacks*: Suppose the message $\{DID_i, R_i, Auth_i, T_p\}$ is intercepted by $\mathcal{A}$ and it is resent to S_m to launch a replay attack in the next session. However, timestamp T_p in the protocol is employed to check if the message is resent. Moreover, when receiving the message $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$, $\mathcal{A}$ will also fail to compromise the key gk_t since $\mathcal{A}$ does not know of ID_i, y_{Ti} for retrieving the number b_j. Therefore, the replay attack is prevented in the proposed protocol.

(2) *MITM attacks*: On the received message $\{DID_i, R_i, Auth_i, T_p\}$, $\mathcal{A}$ may insert forged parameters and generate a candidate login message. $\mathcal{A}$ aims to act as a middle man to compromise the conveyed messages without being noticed by P_i and S_j. However, without the private key prk_j, $\mathcal{A}$ is not able to compute sufficient parameters for the verifications on CID_i and $Auth_i$. Similarly, without y_{Ti} and ID_i, $\mathcal{A}$ can also not compute a valid message $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ for the check on $Auth_j$ on the patient side. As a result, the protocol is free from MITM attacks.

(3) *Password and biometrics guessing attacks:* At first, $\mathcal{A}$ may attempt to directly enter a candidate password for logging to the system. However, the login request will be immediately rejected by SC_i upon the check $V \stackrel{?}{=} h(ID_i^*||PB^*||\sigma)$. Suppose the hash value PB is somehow known to $\mathcal{A}$, then $\mathcal{A}$ attempts to guess PW_i based on PB. Other than PW_i, the values $ID_i, PW_i, h_{bio}(B_i), \sigma$ are also included in the function generating PB. Therefore, it is extremely hard (with a negligible success probability) for $\mathcal{A}$ to guess the correct PW_i by computing candidate hashes and comparing them with the original PB. Using similar arguments, the biometrics B_i is also completely protected during the communication process. Moreover, my work provides password and biometrics update functions that further assure the security of PW_i and B_i. Therefore, a robust three-factor authentication mechanism is achieved in the proposed protocol.

(4) *Impersonation attacks:* Suppose the identity ID_i is somehow disclosed, then $\mathcal{A}$ obtains and uses it to generate a fake login message for impersonating P_i. However, it is not possible for $\mathcal{A}$ to launch this impersonation attack without PW_i, B_i since the protocol can resist password and biometrics guessing attacks, as stated above. Moreover, without the knowledge of y_{Ti}, $\mathcal{A}$ can also not retrieve b_j for further steps upon the known ID_i. Thus, impersonation attacks are resisted in the proposed protocol.

(5) *Lost/stolen sequencer attacks:* Suppose $\mathcal{A}$ has somehow stolen the sequencer SD_i; then, $\mathcal{A}$ retrieved all stored parameters. However, the important credentials ID_i, PW_i, B_i are not stored in SD_i directly. Obtaining the parameters $W_i, V, \varepsilon_i, puk_j$ inside SD_i is not sufficient for passing the verification $V \stackrel{?}{=} h(ID_i^*||PB^*||\sigma)$ and for generating a valid login request message $\{DID_i, R_i, Auth_i, T_p\}$. Thus, my protocol is robust against lost/stolen sequencer attacks.

(6) *Desynchronization attacks:* Two acknowledgement values $Auth_i$ and $Auth_j$ generated by P_i and S_j, respectively, are used for assuring a robust mutual authentication in the proposed protocol. $Auth_i$ and $Auth_j$ are deleted after the login and authentication procedure session is completed. In addition, after each synchronizable key-derivation procedure finishes, P_i and S_j do not update or store any redundant parameters used for the next communication sessions. Hence, desynchronization problems and related attacks are prevented in my work.

(7) *Privileged insider attacks:* Suppose there is a privileged insider $\mathcal{A}$ who can monitor data transmission during the registration and capture message $\{ID_i, PB\}$. Upon the reception of ID_i, it is not possible for $\mathcal{A}$ to compromise the communication due to the stated resistance to impersonation attacks. Using the value PB, $\mathcal{A}$ is also not able to compute a correct TID_i for the attack on $Auth_i$ without W_i stored in the smart card. In another scenario, even if $\mathcal{A}$ somehow obtains CID_i in the database, $\mathcal{A}$ still cannot pass the server verification without ID_i. Thus, the protocol can resist privileged insider attacks.

(8) *DoS attacks:* For analysis of DoS attacks, the author discusses some possible threats that may affect communication performance of the protocol. In the login phase, the system verifies P_i by $V \stackrel{?}{=} h(ID_i^*||PB^*||\sigma)$ upon the newly input credentials ID_i^*, PW_i^*, B_i^*. If

the check is not successful, the session will be immediately terminated. Hence, it is not possible for $\mathcal{A}$ is not able to flood the login and authentication procedure using multiple subsequent steps. On the other hand, upon the received message from P_i, S_j only operates two minor computations $M_i^* = prk_j \cdot R_i$ and $ID_i^* = DID_i \oplus y_{Mi}^*$ before the check $CID_i \stackrel{?}{=} h(ID_i^* \oplus prk_j)$ is made. Retransmitting massive messages $\{DID_i, R_i, Auth_i, T_p\}$ to S_j for disrupting its services would not be an efficient attack due to the redundant resources of S_j. Moreover, the communication will also be terminated once the check $\Delta(T_p, T_c)$ does not hold in the beginning. Therefore, DoS attacks are prevented in the protocol.

(9) *Robust mutual authentication*: In the proposed communication, P_i should be authenticated as a legitimate patient for preventing patients' identities and possibly costly services from being compromised. Upon receiving the login request $\{DID_i, R_i, Auth_i, T_p\}$ from P_i, using the private key, S_j computes M_i^* and retrieves ID_i^*, CID_i, DID_i. These parameters are used for the verification $Auth_i \stackrel{?}{=} h(x_{Ti}^* || x_{Mi}^* || T_p)$ that confirms the legitimacy of the patient P_i. On the other hand, based on the message $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$, P_i retrieves the number b_j to compute H_j, ck^*. These parameters are used for the check $Auth_j \stackrel{?}{=} h(y_{Ti} || ID_i || b_j || ck^*)$ of the acknowledgement that confirms legitimacy of the server S_j and assures true service provision. If one of the above checks fails, the session will be terminated and the session key will not be established successfully. Hence, a robust mutual authentication is achieved in the proposed protocol.

(10) *Patient anonymity and untraceability*: The identity ID_i is hidden in the parameter DID_i of the login message $\{DID_i, R_i, Auth_i, T_p\}$ requested by P_i. Also, the message $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ sent by S_j does not reveal ID_i to the public. Therefore, the anonymity of ID_i is guaranteed during the login and authentication process. The parameters contained in $\{DID_i, R_i, Auth_i, T_p\}$ and $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ in respective communication sessions are totally not identical since different random numbers and timestamps are used for the computations. Therefore, $\mathcal{A}$ is not able to identify any two login messages sent by the same patient P_i. Hence, the proposed protocol achieves patient anonymity and patient untraceability.

(11) *Message unlinkability*: When linking the parameters of all messages $\{DID_i, R_i, Auth_i, T_p, [x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ to each other, there are not any fixed values found. It means that it will not allow $\mathcal{A}$ to trace P_i for the purpose of guessing P_i's identity. Thus, a message unlinkability feature is achieved in the proposed protocol.

(12) *Perfect forward secrecy*: Suppose some sensitive data, secret parameters, or even a session key established in the current session are somehow revealed to $\mathcal{A}$. Upon receiving these vales, $\mathcal{A}$ attempts to attack the past communications. However, it is not possible for $\mathcal{A}$ to launch the attack since the values are completely not identical in different communication sessions due to the inclusion of random numbers and timestamp values in the computations. For instance, $\mathcal{A}$ cannot use the currency key $gk_t^{current} = h(h^{t-t_1}(TB_1) || h^{t_2-t}(TB_2))$ to compromise the message encrypted using a key gk_t^{past} established in the past session. If the long-term private key prk_j of S_j is compromised, the secrecy of gk_t^{past} is also not affected, because there are no associated parameters between them. Hence, a perfect forward secrecy is achieved in my protocol.

(13) *Perfect backward secrecy (known-key security)*: With similar arguments, the protocol is proven not to be vulnerable to a known-key attack, since compromise of the past key gk_t^{past} does not allow either a passive $\mathcal{A}$ to compromise the future key gk_t^{future} or impersonation by an active $\mathcal{A}$ in the future.

6.2. Logical Analysis Using BAN logic

In this subsection, the well-known BAN logic [43] is employed to further provide a logical analysis on the mutual authentication between P_i and S_j. Some rules and analytical logics in the tool are defined in advance. Next, the analysis demonstrates that P_i and S_j

believe the key gk_t is a secret value shared between them only. Some notations used for the analysis are provided in Table 2.

Table 2. Notations used in the analysis with BAN logic.

Notations Used in the BAN	Explanation
$X \mid\equiv M$	X believes a statement M
$X \lhd M$	X sees the statement M
$X \mid\sim M$	X once said the statement M
$X \Longrightarrow M$	X has jurisdiction over the statement M
(M, N)	M or N is one part of the formula (M, N)
$\langle M \rangle_N$	The statement M is combined with the formula N
$\#(M)$	The formula M is fresh, meaning it has not been sent in any previous messages
$X \overset{K}{\Leftrightarrow} Y$	Formula K is a secret known only by X and Y; only X and Y can use M to authenticate each other
$X \overset{G}{\leftrightarrow} Y$	Value G is known only to X and Y; it is used for their communication

In accordance with the principle of BAN logic and operation rules in my proposed protocol, the mutual authentication proof should satisfy the following four goals. In the protocol, the value ck is utilized by S_j to distribute TB_1 and TB_2 to P_i for computing the group key gk_t. Therefore, authenticity of both ck and gk_t should be proven, which can guarantee a completely authenticated key shared between the entities.

***Goal* 1:** $S_j \mid\equiv (P_i \overset{gk_t}{\leftrightarrow} S_j)$. S_j believes that the key gk_t computed is a secret value shared between P_i and S_j. (**G1**)

***Goal* 2:** $S_j \mid\equiv (P_i \overset{ck}{\leftrightarrow} S_j)$. S_j believes that the key ck computed is a secret value shared between P_i and S_j. (**G2**)

***Goal* 3:** $P_i \mid\equiv (P_i \overset{ck}{\leftrightarrow} S_j)$. P_i believes that the key ck computed is a secret value shared between P_i and S_j. (**G3**)

***Goal* 4:** $P_i \mid\equiv (P_i \overset{gk_t}{\leftrightarrow} S_j)$. P_i believes that the key gk_t computed is a secret value shared between P_i and S_j. (**G4**)

Two messages communicated in the login and authentication procedure of the protocol are included in the authentication proof.

Message 1: $P_i \rightarrow S_j : (ID_i^* \oplus y_{Mi}, x_{Ri}, y_{Ri}, h(x_{Ti}||x_{Mi}||T_p), T_p)$

Message 2: $S_j \rightarrow P_i : ([x_1, x_2, \ldots, x_n], b_j \oplus h(ID_i^*||y_{Ti}^*||T_s), h(y_{Ti}^*||ID_i||b_j||ck), T_s)$

Some logical rules of the tool used in the proof are provided as follows.

- Seeing rule (R1): $\frac{X|\equiv (X \overset{K}{\Leftrightarrow} Y), Y \lhd \langle A \rangle_K}{X|\equiv Y|\sim A}$;
- Interpretation rule (R2): $\frac{X|\equiv Y|\sim (A,B)}{X|\equiv Y|\sim A}$;
- Freshness rule (R3): $\frac{X|\equiv \#(A)}{X|\equiv \#(A,B)}$;
- Verification rule (R4): $\frac{X|\equiv \#(A), X|\equiv Y|\sim A}{X|\equiv Y|\equiv A}$;
- Jurisdiction rule (R5): $\frac{X|\equiv Y \Longrightarrow A, X|\equiv Y|\equiv A}{X|\equiv A}$;
- Belief rule (R6): $\frac{X|\equiv (A,B)}{X|\equiv A}$.

Along with the rules, the following assumptions are also used in the analysis.

- Assumption 1 (A1): $S_j \mid\equiv P_i \overset{K_{ij}}{\Leftrightarrow} S_j$;
- Assumption 2 (A2): $S_j \mid\equiv \#(T_p)$;
- Assumption 3 (A3): $S_j| \equiv P_i \Longrightarrow (x_{Ti}, x_{Mi}, T_p)$;
- Assumption 4 (A4): $S_j \Longrightarrow (t_1)$;
- Assumption 5 (A5): $S_j \Longrightarrow (t_2)$;

- Assumption 6 (A6): $S_j \Longrightarrow (b_j)$;
- Assumption 7 (A7): $S_j \Longrightarrow (c_j)$;
- Assumption 8 (A8): $S_j \Longrightarrow (prk_j)$;
- Assumption 9 (A9): $P_i \mid\equiv \#(T_s)$;
- Assumption 10 (A10): $P_i| \equiv S_j \Longrightarrow ([x_1, x_2, \ldots, x_n], b_j, y_{Ti}, T_s)$;
- Assumption 11 (A11): $P_i \Longrightarrow (ID_i)$.

In this way, an idealized form of the communicated messages is described as follows.
Message 1: $P_i \rightarrow S_j : (\langle ID_i, y_{Mi} \rangle_{K_{ij}}, x_{Ri}, y_{Ri}, \langle x_{Ti}, x_{Mi}, T_p \rangle_{K_{ij}}, T_p)$
Message 2: $S_j \rightarrow P_i : ([x_1, x_2, \ldots, x_n], \langle b_j, ID_i, y_{Ti}, T_s \rangle_{K_{ij}}, \langle y_{Ti}, ID_i, b_j, ck \rangle_{K_{ij}}, T_s)$

Based on the specified rules, assumptions, and procedure of the protocol, the logical analysis of mutual authentication between P_i and S_j in the proposed protocol is described by the following steps.

- $Step_1$: Based on the *Message* 1, we have $S_j \lhd (\langle ID_i, y_{Mi} \rangle_{K_{ij}}, x_{Ri}, y_{Ri}, \langle x_{Ti}, x_{Mi}, T_p \rangle_{K_{ij}}, T_p)$.
- $Step_2$: Using A1 and R1, we have $S_j \mid\equiv P_i \mid\sim (ID_i, y_{Mi}, x_{Ri}, y_{Ri}, x_{Ti}, x_{Mi}, T_p)$.
- $Step_3$: According to R2, we obtain $S_j \mid\equiv P_i \mid\sim (x_{Ti}, x_{Mi}, T_p)$.
- $Step_4$: Using R3 and A2, we have $S_j \mid\equiv \#(x_{Ti}, x_{Mi}, T_p)$.
- $Step_5$: Based on R4, $Step_3$, and $Step_4$, we obtain $S_j \mid\equiv P_i \mid\equiv (x_{Ti}, x_{Mi}, T_p)$.
- $Step_6$: According to R5, A3, and $Step_5$, we obtain $S_j \mid\equiv (x_{Ti}, x_{Mi}, T_p)$.
- $Step_7$: Based on R6 and $Step_6$, we obtain $S_j \mid\equiv x_{Ti}$, $S_j \mid\equiv x_{Mi}$, and $S_j \mid\equiv T_p$.
- $Step_8$: Due to $Step_7$, and $Auth_i = h(x_{Ti}||x_{Mi}||T_p)$, we obtain $S_m \mid\equiv Auth_i$.
- $Step_9$: Based on $Step_8$, A4, A5, A6, A7, A8, and $gk_t = h(h^{t-1}(h(prk_j||b_j))||h^{z-t}\left(h(prk_j||c_j)\right))$, we can obtain $S_j \mid\equiv (P_i \overset{gk_t}{\leftrightarrow} S_j)$ (**G1** achieved).
- $Step_{10}$: Based on $Step_8$, A4, A5, A6, A7, A8, and $ck = (h^{t_1-1}(h(prk_j||b_j))||h^{z-t_2}(h(prk_j||c_j))||t_1||t_2)$, we can obtain $S_j \mid\equiv (P_i \overset{ck}{\leftrightarrow} S_j)$ (**G2** achieved).
- $Step_{11}$: According to the *Message* 2, we have $P_i \lhd ([x_1, x_2, \ldots, x_n], \langle b_j, ID_i, y_{Ti}, T_s \rangle_{K_{ij}}, \langle y_{Ti}, ID_i, b_j, ck \rangle_{K_{ij}}, T_s)$
- $Step_{12}$: In accordance with R1 and A1, we obtain $P_i \mid\equiv S_m \mid\sim ([x_1, x_2, \ldots, x_n], b_j, ID_i, y_{Ti}, ck, T_s)$.
- $Step_{13}$: Based upon R2, we can obtain $P_i| \equiv S_m| \sim ([x_1, x_2, \ldots, x_n], b_j, y_{Ti}, T_s)$.
- $Step_{14}$: Using R3 and A9, we have $P_i| \equiv \#([x_1, x_2, \ldots, x_n], b_j, y_{Ti}, T_s)$.
- $Step_{15}$: Based on R4, $Step_{13}$ and $Step_{14}$, we obtain $P_i \mid\equiv S_j \mid\equiv ([x_1, x_2, \ldots, x_n], b_j, y_{Ti}, T_s)$.
- $Step_{16}$: According to R5, A10, and $Step_{15}$, we obtain $P_i \mid\equiv ([x_1, x_2, \ldots, x_n], b_j, y_{Ti}, T_s)$.
- $Step_{17}$: Based on R6 and $Step_{16}$, we obtain $P_i \mid\equiv [x_1, x_2, \ldots, x_n]$, $P_i \mid\equiv b_j$, $P_i \mid\equiv y_{Ti}$, and $P_i \mid\equiv T_s$.
- $Step_{18}$: In accordance with $Step_{17}$, while $H_j = h(b_j||T_s)$ and $ck = h(y_{Ti}||T_s) - \begin{bmatrix} H'^1_{j,1} & H'^2_{j,1} & \ldots & H'^n_{j,1} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$, we can obtain $P_i \mid\equiv (P_i \overset{ck}{\leftrightarrow} S_j)$ (**G3** achieved).
- $Step_{19}$: Due to $Step_{17}$, $Step_{18}$, A11, and $Auth_j = h(y_{Ti}||ID_i||b_j||ck)$, we obtain $P_i \mid\equiv Auth_j$.
- $Step_{20}$: Based on $Step_{18}$, $Step_{19}$, $ck = (TB_1||TB_2||t_1||t_2)$, and $gk_t = h(h^{t-t_1}(TB_1)||h^{t_2-t}(TB_2))$, we obtain $P_i \mid\equiv (P_i \overset{gk_t}{\leftrightarrow} S_j)$ (**G4** achieved).

In this way, the proposed protocol achieves all goals—**G1**, **G2**, **G3**, and **G4**. Therefore, it proves that P_i and S_j can mutually authenticate each other and gk_t is an authenticated key shared between them.

6.3. Formal Security Proof with RoR Model

Formal security proof of the proposed protocol is provided using the widely-accepted ROR model. Based on mathematical principles, its idea is to analyze the success probability of $\mathcal{A}$ in attacking the protocol. The goal is to demonstrate that this probability is a negligible advantage, assuring the sematic security of the approach. Various games are included in the analysis where $\mathcal{A}$ makes multiple attack queries discussed in Section 4.2 with an increased success probability. Notations used in the proof are described in Table 3.

Table 3. Notations used in the security proof with RoR Model.

Notations	Explanation
l_h	Size of a hash value
l_r	Size of a random number
l_{bio}	Size of a biometric value
q_h	Total hash oracle queries
q_s	Total *Send* queries
q_e	Total *Execute* queries
L_h	List of hash oracle outputs
L_r	List of random oracle results
L_t	List of transcripts conveyed between P_i and S_j
ε_{bio}	Biometric false-positive probability
C', s'	*Zipf* parameters

Definition 7. *When Ç receives the last communicated message in the protocol, Ç goes to an Accept state. All messages* $m_1 = \{DID_i, R_i, Auth_i, T_p\}$ *and* $m_2 = \{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ *are orderly concatenated, forming a session with an identification "s_id".*

Definition 8. $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *are defined to be partnered if* $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *simultaneously meet the following conditions: (1)* $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *are in an Accept state; (2)* $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *mutually authenticate each other in the same session s_id; and (3)* $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *are mutually a partner of each other.* $P_i^{T_c}$ *and* ${S_j}^{T_c^*}$ *are called "partners".*

Definition 9. *Ç is defined to be fresh if Ç simultaneously meets the following conditions: (1) Ç is in an accepted state; (2) Reveal(Ç) queries have never been submitted; and (3) less than three Corrupt* (P_i, n) *queries have been submitted. This is called the "freshness" rule.*

Definition 10. $Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}})$ *is denoted as the advantage of* $\mathcal{A}$ *in breaking the ECDLP assumption within an execution time* $t_{\mathcal{A}}$*. Because the assumption holds,* $Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}})$ *is a negligible probability.*

Definition 11. $Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}})$ *is denoted as the advantage of* $\mathcal{A}$ *in breaking the ECCDHP assumption within an execution time* $t_{\mathcal{A}}$*. Also,* $Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}})$ *is a negligible probability since the assumption holds.*

Definition 12. $Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}})$ *is denoted as the advantage of* $\mathcal{A}$ *in breaking the ECFP assumption within an execution time* $t_{\mathcal{A}}$*. Similarly,* $Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}})$ *is a negligible probability as the assumption holds.*

Theorem 1. Adv^{IoLTHC} *can be calculated in the following equation.*

$$\begin{aligned} Adv_{\text{Ç}}^{IoLTHC} \leq \tfrac{(q_s+q_e)^3+6q_s}{2^{Lr}} + \tfrac{{q_h}^2+20q_h}{2^{L_h}} + 2max\left\{\left(C'\cdot q_s^{s'}\right), q_s\left(\tfrac{1}{2^{l_{bio}}}, \varepsilon_{bio}\right)\right\} \\ +4q_h(q_s+q_e+1)Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}}) + 2q_h(q_s+q_e+1)Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}}) \\ +2q_h(q_s+q_e+1)Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}}) \end{aligned} \quad (1)$$

Since Equation (1) is obviously a negligible probability, the proposed protocol is semantically secure.

Proof. The author considers six games simulated for the proof including $G_0, G_1, G_2, G_3, G_4, G_5$ with increasing success probabilities of $\mathcal{A}$ in attacking the protocol. The ultimate goal of $\mathcal{A}$ is to retrieve the bit b using the *Test* query after each of the games finishes. $Pr[S_i]$ is denoted as success probabilities, in which E_f $(f = 0, 1, 2, 3, 4, 5)$ are events in respective games. I set a simulator Ş to play the role of the challenge Ç in the games. □

Game G_0: This is the starting game, which is identical to the real protocol in the RoR model. Ş tosses the coin b and the game is started. We obtain

$$Adv_{Ç}^{IoLTHC} = |2Pr[E_0] - 1| \tag{2}$$

Game G_1: This game executes all queries that are specified in the model. The queries are simulated in Table 4 in accordance with rules of my proposed protocol. In this way, G_1 creates three lists, namely, L_h, L_r, and L_t. Since G_0 and G_1 are indistinguishable, we have

$$Pr[E_1] = Pr[E_0] \tag{3}$$

Game G_2: In this game, the author considers collision probabilities of hash oracle queries and random oracle queries for all transcripts conveyed between P_i and S_j. Based on a property of the birthday paradox, the probability of the hash queries is at most $\frac{{q_h}^2}{2^{L_h+1}}$. During login and authentication procedures of the protocol, P_i and S_j generate three random numbers $\{a_i, b_j, c_j\}$ for constructing two messages $\{DID_i, R_i, Auth_i, T_p\}$ and $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$. Its total collision probability is $\frac{(q_s+q_e)^3}{2^{Lr+1}}$. Due to the indistinguishability between G_1 and G_2, the following equation is obtained:

$$|Pr[E_2] - Pr[E_1]| \leq \frac{(q_s + q_e)^3}{2^{L_r+1}} + \frac{{q_h}^2}{2^{L_h+1}} \tag{4}$$

Game G_3: G_3 is similar to G_2, but *Send*(Ç, m) queries are made for each communicated message. This game consists of two cases consistent with two messages sent by P_i and S_j.

+ *Case 1*: Query *Send*(S_j, m_1) is simulated in this case. Messages m_1 is computed from three values $ID_i^* \oplus y_{Mi}, a_i \cdot P, h(x_{Ti}||x_{Mi}||T_p) \in L_h$. To lauch the attack, the hash value PB should also be revealed to $\mathcal{A}$. It results in a total probability of $4\frac{q_h}{2^{L_h}}$ in total. Meanwhile, the random number a_i included in m_1 has a probability at most of $\frac{q_s}{2^{L_r}}$.

+ *Case 2*: Query *Send*(P_i, m_2) is executed in this case. To launch the attack, the values $b_j \oplus h(ID_i^*||y_{Ti}^*||T_s)$, $h(y_{Ti}^*||ID_i||b_j||ck)$, $H_j = h(b_j||T_s)$, $h(y_{Ti}||T_s)$, $h^{t_1-1}(h(prk||b_j))$, and $h^{z-t_2}(h(prk||c_j))$ containing messages m_2 should be known to $\mathcal{A}$. Therefore, its maximum probability is up to $6\frac{q_h}{2^{L_h}}$. Random numbers b_j, c_j have a probability of, at most, $2\frac{q_s}{2^{Lr}}$.

Since G_2 and G_3 are identical when these attacks are absent, we obtain

$$|Pr[E_3] - Pr[E_2]| \leq 10\frac{q_h}{2^{L_h}} + 3\frac{q_s}{2^{L_r}} \tag{5}$$

Game G_4: Guessing attacks executed by $\mathcal{A}$ are simulated in this game. The author includes five attack cases, which are described as follows.

+ *Case 1*: $\mathcal{A}$ runs query *Corrupt*$(P_i, w = 1)$ to guess PW_i of P_i. Next, $\mathcal{A}$ makes query *Send*(S_j, m_1) for the attacks. The probability in this case is at most $(C' \cdot q_s^{s'})$.

+ *Case 2*: $\mathcal{A}$ runs the query *Corrupt*$(P_i, w = 3)$ to retrieve B_i of P_i. $\mathcal{A}$ also executes query *Send*(S_j, m_1) to launch the attack; therefore, the collision probability is up to $max\left\{q_s(\frac{1}{2^{l_{bio}}}, \varepsilon_{bio})\right\}$.

+ *Case 3*: Suppose $\mathcal{A}$ employs power analysis to successfully retrieve parameters stored in SC_i. Upon *Hash* oracle queries, $\mathcal{A}$ aims to break the ECDLP to compromise the values CID_i, PB, a_i (based on the points W_i, R_i, respectively) in order to impersonate P_i. The probability in this case is at most $2q_h Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}})$.

+ *Case 4*: To trigger MITM attacks or impersonation attacks, $\mathcal{A}$ runs *Hash* oracle queries that break the ECCDHP assumption to compromise the point $M_i = a_i \cdot prk \cdot P$ given the points $R_i = a_i \cdot P$ and $puk = prk \cdot P$. Its maximum collision probability is up to $q_h Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}})$.

+ *Case 5*: To trigger similar attacks, $\mathcal{A}$ runs *Hash* oracle queries to break the ECFP to compromise two points $TID_i = CID_i \cdot P$ and $PB \cdot P$ given the point $W_i = [CID_i + PB]P$ (retrieved from SC_i using power analysis). In this case, the collision probability is at most $q_h Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}})$.

Table 4. All queries executed in the RoR model.

Hash query is executed as follows, where $\boldsymbol{m_i}$ are messages. If the record $(\boldsymbol{m_i}, \boldsymbol{h}(\boldsymbol{m_i}))$ is found in the list $\boldsymbol{L_h}$, return $\boldsymbol{h}(\boldsymbol{m_i})$; if not, choose $\boldsymbol{h}^{'}(\boldsymbol{m_i}) \in \boldsymbol{Z_p^*}$ and write $(\boldsymbol{m_i}, \boldsymbol{h}^{'}(\boldsymbol{m_i}))$ to $\boldsymbol{L_h}$; the list $\boldsymbol{L_r}$ is created by a similar procedure.
Reveal(Ç) query is executed by a simple procedure as follows. Once Ç is in an Accept state, a session key formed by Ç is returned.
Test(Ç) query is executed as follows. Ç tosses the coin $\boldsymbol{b}$. If $\boldsymbol{b} = 1$, the query returns an available key $\boldsymbol{gk_t}$; otherwise, it returns a random number.
Corrupt$(\boldsymbol{P_i}, \boldsymbol{w})$ query is executed as follows. If $\boldsymbol{w} = 1$, the query outputs password $\boldsymbol{PW_i}$. If $\boldsymbol{w} = 2$, the query outputs parameters stored in $\boldsymbol{SD_i}$. If $\boldsymbol{w} = 3$, the query outputs biometrics $\boldsymbol{B_i}$.
Execute$(\boldsymbol{P_i}, \boldsymbol{S_j})$ query is executed in succession with execution of *Send*(Ç, $\boldsymbol{m_i}$) query. It is presented as follows. $\boldsymbol{P_i}$ sends $\boldsymbol{m_1}$ to $\boldsymbol{S_j}$ and $\boldsymbol{S_j}$ sends $\boldsymbol{m_2}$ to $\boldsymbol{P_i}$. we have $< \boldsymbol{ID_i^*} \oplus \boldsymbol{y_{Mi}}, \boldsymbol{a_i \cdot P}, \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p}), \boldsymbol{T_p} > \leftarrow$ *Send*$(\boldsymbol{P_i}, start)$, $< [x_1, x_2, \ldots, x_n], \boldsymbol{b_j} \oplus \boldsymbol{h}(\boldsymbol{ID_i^*}||\boldsymbol{y_{Ti}^*}||\boldsymbol{T_s}), \boldsymbol{h}(\boldsymbol{y_{Ti}^*}||\boldsymbol{ID_i}||\boldsymbol{b_j}||\boldsymbol{ck}), \boldsymbol{T_s} > \leftarrow$ *Send*$(\boldsymbol{S_j}, < \boldsymbol{ID_i^*} \oplus \boldsymbol{y_{Mi}}, \boldsymbol{a_i \cdot P}, \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p}), \boldsymbol{T_p} >)$ At last, $\boldsymbol{m_1} =< \boldsymbol{ID_i^*} \oplus \boldsymbol{y_{Mi}}, \boldsymbol{a_i \cdot P}, \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p}), \boldsymbol{T_p} >$ and $\boldsymbol{m_2} =< [x_1, x_2, \ldots, x_n], \boldsymbol{b_j} \oplus \boldsymbol{h}(\boldsymbol{ID_i^*}||\boldsymbol{y_{Ti}^*}||\boldsymbol{T_s}), \boldsymbol{h}(\boldsymbol{y_{Ti}^*}||\boldsymbol{ID_i}||\boldsymbol{b_j}||\boldsymbol{ck}), \boldsymbol{T_s} >$ are returned.
Based on the logical procedure of the protocol, the *Send* query is simulated as follows. • $\mathcal{A}$ runs *Send*$(\boldsymbol{P_i}, start)$ query and Ç replies to $\mathcal{A}$ as follows. Ç computes $\boldsymbol{M_i} = \boldsymbol{a_i \cdot puk} = (\boldsymbol{x_{Mi}}, \boldsymbol{y_{Mi}})$, $\boldsymbol{R_i} = \boldsymbol{a_i \cdot P}$, $\boldsymbol{c_{i,m22}} = \boldsymbol{y_{i,m2}}^* \boldsymbol{r_{i,m1}} \boldsymbol{mod\ p}$, $\boldsymbol{TID_i} = \boldsymbol{W_i} - \boldsymbol{PB}^* \cdot \boldsymbol{P} = (\boldsymbol{x_{Ti}}, \boldsymbol{y_{Ti}})$, and $\boldsymbol{Auth_i} = \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p})$ and outputs $\boldsymbol{m_1} =< \boldsymbol{ID_i^*} \oplus \boldsymbol{y_{Mi}}, \boldsymbol{R_i}, \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p}), \boldsymbol{T_p} >$. • $\mathcal{A}$ runs *Send*$(\boldsymbol{S_j}, < \boldsymbol{ID_i^*} \oplus \boldsymbol{y_{Mi}}, \boldsymbol{R_i}, \boldsymbol{h}(\boldsymbol{x_{Ti}}||\boldsymbol{x_{Mi}}||\boldsymbol{T_p}), \boldsymbol{T_p} >)$ query and Ç replies to $\mathcal{A}$ as follows. Ç checks $\boldsymbol{T_p}$; computes $\boldsymbol{M_i^*} = \boldsymbol{prk \cdot R_i} = (\boldsymbol{x_{Mi}^*}, \boldsymbol{y_{Mi}^*})$ and $\boldsymbol{ID_i^*} = \boldsymbol{DID_i} \oplus \boldsymbol{y_{Mi}^*}$; checks $\boldsymbol{CID_i}$; computes $\boldsymbol{TID_i^*}$ and $\boldsymbol{Auth_i}$; computes $\boldsymbol{TB_1} = \boldsymbol{h}^{t_1 - 1}(\boldsymbol{h}(\boldsymbol{prk}||\boldsymbol{b_j}))$, $\boldsymbol{TB_2} = \boldsymbol{h}^{z - t_2}(\boldsymbol{h}(\boldsymbol{prk}||\boldsymbol{c_j}))$, $\boldsymbol{Y_j} = \boldsymbol{b_j} \oplus \boldsymbol{h}(\boldsymbol{ID_i^*}||\boldsymbol{y_{Ti}^*}||\boldsymbol{T_s})$, $\boldsymbol{ck} = (\boldsymbol{TB_1}||\boldsymbol{TB_2}||\boldsymbol{t_1}||\boldsymbol{t_2})$, $\boldsymbol{Auth_j} = \boldsymbol{h}(\boldsymbol{y_{Ti}^*}||\boldsymbol{ID_i}||\boldsymbol{b_j}||\boldsymbol{ck})$, and $\boldsymbol{H_j} = \boldsymbol{h}(\boldsymbol{b_j}||\boldsymbol{T_s})$; and generates $[x_1, x_2, \ldots, x_n]$ from $\boldsymbol{H_j}, \boldsymbol{y_{Ti}}, \boldsymbol{ck}$. Ç terminates the session if one of the above checks does not hold. Otherwise, Ç outputs $\boldsymbol{m_2} =< [x_1, x_2, \ldots, x_n], \boldsymbol{b_j} \oplus \boldsymbol{h}(\boldsymbol{ID_i^*}||\boldsymbol{y_{Ti}^*}||\boldsymbol{T_s}), \boldsymbol{h}(\boldsymbol{y_{Ti}^*}||\boldsymbol{ID_i}||\boldsymbol{b_j}||\boldsymbol{ck}), \boldsymbol{T_s} >$. The session key $\boldsymbol{S_j}$ obtains is $\boldsymbol{gk_t} = \boldsymbol{h}(\boldsymbol{h}^{t-1}(\boldsymbol{h}(\boldsymbol{prk}|\boldsymbol{b_j}))||\boldsymbol{h}^{z-t}(\boldsymbol{h}(\boldsymbol{prk}||\boldsymbol{c_j})))$. • $\mathcal{A}$ runs *Send*$(\boldsymbol{P_i}, < [x_1, x_2, \ldots, x_n], \boldsymbol{b_j} \oplus \boldsymbol{h}(\boldsymbol{ID_i^*}||\boldsymbol{y_{Ti}^*}||\boldsymbol{T_s}), \boldsymbol{h}(\boldsymbol{y_{Ti}^*}||\boldsymbol{ID_i}||\boldsymbol{b_j}||\boldsymbol{ck}), \boldsymbol{T_s} >)$ query and Ç replies to $\mathcal{A}$ as follows. Ç checks $\boldsymbol{T_s}$; computes $\boldsymbol{b_j}, \boldsymbol{H_j}, \boldsymbol{ck}^*$ based on some related parameters; and checks $\boldsymbol{Auth_j}$. If one of the checks does not hold, Ç terminates the session; otherwise, a session key $\boldsymbol{gk_t} = \boldsymbol{h}(\boldsymbol{h}^{t-t_1}(\boldsymbol{TB_1})||\boldsymbol{h}^{t_2-t}(\boldsymbol{TB_2}))$ is established, and the session is completed.

Because G_3 and G_4 are indistinguishable, we have

$$|Pr[E_4] - Pr[E_3]| \leq max\left\{\left(C' \cdot q_s^{s'}\right), q_s\left(\frac{1}{2^{l_{bio}}}, \varepsilon_{bio}\right)\right\} + 2q_h Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}}) + q_h Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}}) + q_h Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}}) \quad (6)$$

Game G_5: The author simulates attack scenarios on the forward secrecy property in this last game. Based on the current transcripts, *Execute*, *Send*, and *Hash* oracle queries are executed to retrieve group session keys generated by the old transcripts. The ECDLP assumption, ECCDHP assumption, and ECFP assumption are included in the simulation. To this end, the *Test* query is made to return the session key to $\mathcal{A}$. To launch the attacks, $\mathcal{A}$

has to at least break the ECDLP two times in a row, to break the ECCDHP one time, or to break the ECFP one time; therefore, the following equation is obtained:

$$\begin{array}{c} |Pr[E_5] - Pr[E_4]| \leq 2q_h(q_s + q_e)Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}}) \\ +q_h(q_s + q_e)Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}}) \\ +q_h(q_s + q_e)Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}}) \end{array} \tag{7}$$

After all games are made, the bit b' is guessed upon the probability of the *Test* query below:

$$Pr[E_5] = \frac{1}{2} \tag{8}$$

Applying property of the triangular inequality and results of Equations (3)–(8), we have

$$\begin{array}{c} |Pr[E_0] - \frac{1}{2}| = |Pr[E_1] - Pr[E_5]| \\ \leq |Pr[E_1] - Pr[E_2]| \\ +|Pr[E_2] - Pr[E_3]| \\ +|Pr[E_3] - Pr[E_4]| \\ +|Pr[E_4] - Pr[E_5]| \end{array} \tag{9}$$

Applying Equations (2)–(9), the following result is achieved:

$$\begin{array}{c} \frac{1}{2}Adv_{\text{Ç}}^{IoLTHC} = |Pr[E_0] - \frac{1}{2}| \\ \leq \frac{(q_s+q_e)^3}{2^{L_r+1}} + \frac{{q_h}^2}{2^{L_h+1}} + 10\frac{q_h}{2^{L_h}} + 3\frac{q_s}{2^{L_r}} + max\left\{\left(C' \cdot q_s^{s'}\right), q_s\left(\frac{1}{2^{l_{bio}}}, \varepsilon_{bio}\right)\right\} \\ +2q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}}) + q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}}) \\ +q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}}) \end{array} \tag{10}$$

Multiplying two sides of Equation (10) with a factor of 2, we can easily obtain the following final result:

$$\begin{array}{c} Adv_{\text{Ç}}^{IoLTHC} \leq \frac{(q_s+q_e)^3+6q_s}{2^{L_r}} + \frac{{q_h}^2+20q_h}{2^{L_h}} + 2max\left\{\left(C' \cdot q_s^{s'}\right), q_s\left(\frac{1}{2^{l_{bio}}}, \varepsilon_{bio}\right)\right\} \\ +4q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECDLP}(t_{\mathcal{A}}) + 2q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECCDHP}(t_{\mathcal{A}}) \\ +2q_h(q_s + q_e + 1)Adv_{\mathcal{A}}^{ECFP}(t_{\mathcal{A}}) \end{array} \tag{11}$$

As can be seen, Equation (1) and Equation (11) are consistent. Hence, Theorem 1 is claimed and the proposed protocol is proven to be secure, as $Adv_{\text{Ç}}^{IoLTHC}$ is a completely negligible advantage.

7. Performance Evaluation and Comparison

This section provides a detailed performance evaluation and presents a comparative study on multiple aspects of the protocols, including security properties and functionalities, computation overhead, and communication overhead.

7.1. Security Properties and Functionalities

The author provides the results of a comparison of security properties and functionalities of different works discussed in Section 2.2, which are tabulated in Table 5. As can be seen, the proposed protocol provides more functionality and achieves more security properties compared to the others. Especially notable is that only the proposed work introduces a 6G-aided group-based dynamic U-healthcare application. In addition, this work is the first to employ a sequencer to directly store user's registered credentials as well as use it as a separate factor for the authentication in a key agreement protocol.

Table 5. Security properties and functionalities of different protocols.

Attributes	[21]	[23]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[36]	[37]	Mine
Resists replay attacks	O	O	O	O	O	O	O	O	O	O	O	O
Resists MITM attacks	O	O	O	O	O	O	O	O	O	O	O	O
Resists online password guessing attacks	–	O	O	O	O	O	O	O	O	O	O	O
Resists offline password guessing attacks	–	O	O	O	O	O	O	O	O	O	O	O
Resists impersonation attacks	O	O	O	O	O	O	O	O	O	O	O	O
Resists lost sequencer or smart card attacks	O	O	–	O	–	–	O	X	X	O	O	O
Resists desynchronization attacks	O	O	O	O	O	O	O	X	O	X	O	O
Resists privileged insider attacks	O	O	O	O	O	O	O	O	O	O	O	O
Resists DoS attacks	O	O	O	O	O	O	O	O	O	O	O	O
Provides mutual authentication	O	O	O	O	O	O	O	O	O	O	O	O
Provides user anonymity	O	O	O	O	O	O	O	X	X	O	O	O
Provides user untraceability	O	O	O	O	O	X	O	O	O	X	O	O
Provides message unlinkability	O	O	O	O	O	X	O	O	O	X	O	O
Provides perfect forward secrecy	O	O	O	O	O	O	O	O	O	O	O	O
Provides perfect backward secrecy	O	O	O	O	O	O	O	O	O	O	O	O
Provides password update	–	O	O	X	O	O	O	X	X	O	O	O
Provides biometrics update	–	–	–	–	–	–	O	X	X	–	O	O
Provides three-factor authentication	X	X	X	X	X	X	O	O	O	X	O	O
Provides SD-SSO	X	X	X	X	X	X	X	X	X	X	X	O
Provides mathematics-based security proof	X	X	O	O	O	X	O	X	O	X	O	O
Provides group-based dynamic services	X	X	X	X	X	X	X	X	X	X	X	O
Provides LOC-based U-healthcare application	X	X	X	X	X	X	X	X	X	X	O	O
Supports patient-centric service	O	X	O	X	O	O	X	O	O	O	X	O

"O": the protocol achieves a specific attribute; "X": the protocol does not achieve a specific attribute; "–": A specific attribute is not available in the protocol.

7.2. Computation Overhead

Six of the eleven existing works above, which are the most relevant to the proposed approach, are included for evaluating the computation overhead and communication overhead. To estimate the overhead, the author calculates the running time of all cryptographic operations in the login and authentication phase of each protocol. Since XOR operations are so fast, its running time is assumed to be negligible. For simplicity, the computing times of a traditional one-way hash function and a biohash function are also considered to be similar, as the difference between them is too small [29,32]. The running time of each cryptographic operation used in the evaluation is tabulated in Table 6. The comparative results of the computation overhead evaluation are described in Table 7 and Figure 7. Giving the support of far fewer functional properties (specified in Table 5), the protocols of Yu et al. [29], Wong et al. [30], Le and Hsu [31], and Meshram et al. [36] incur less computing cost compared to that in the initial authentication procedure of the proposed work. However, overhead consumed in the fast key derivation of the proposed work is less than that of all other protocols, which makes it become the most efficient procedure.

Table 6. Time estimation of each cryptographic operation [44,45].

Notation	Operation	Computation Time (ms)
T_H	Hash function	≈0.00069
T_{PA}	EC point addition	≈0.0069
T_{PM}	EC point multiplication	≈0.508
T_{SED}	Symmetric encryption or decryption	≈0.00054
T_M	Modular squaring	≈0.00069
T_{QR}	Square root module N	≈1.169
T_{CM}	Chebyshev chaotic polynomial mapping	≈0.02881

Table 7. Comparison of computation overhead.

Protocols		P_i		S_j		Total Computation Time (ms)
		Computation Complexities	Computation Time (ms)	Computation Complexities	Computation Time (ms)	
Thakare and Kim [28]		$2T_H+T_{PA}+4T_{PM}$	≈2.04028	$6T_H+2T_{PA}+5T_{PM}$	≈2.55794	≈4.59822
Yu et al. [29]		$10T_H+2T_{CM}$	≈0.06452	$8T_H+2T_{CM}$	≈0.06314	≈0.12766
Wong et al. [30]		$7T_H+T_{SED}+T_M$	≈0.04953	$7T_H+2T_{SED}+T_{QR}$	≈1.17491	≈1.22444
Le and Hsu [31]		$9T_H+T_{SED}+T_M$	≈0.00744	$5T_H+2T_{SED}+T_{QR}$	≈1.17353	≈1.18097
Meshram et al. [36]		$11T_H+2T_{CM}$	≈0.06521	$9T_H+2T_{CM}$	≈0.06383	≈0.12904
Le [37]		$4T_H+T_{SED}+4T_{PM}$	≈2.03530	$2T_H+T_{SED}+3T_{PM}$	≈1.52592	≈3.56122
Mine	Initial authentication	$13T_H+T_{PA}+3T_{PM}$	≈1.53987	$16T_H+2T_{PM}$	≈1.02704	≈2.56691
	Fast key derivation	$3T_H+T_{SED}$	≈0.00261	$9T_H+T_{SED}$	≈0.00675	≈0.00936

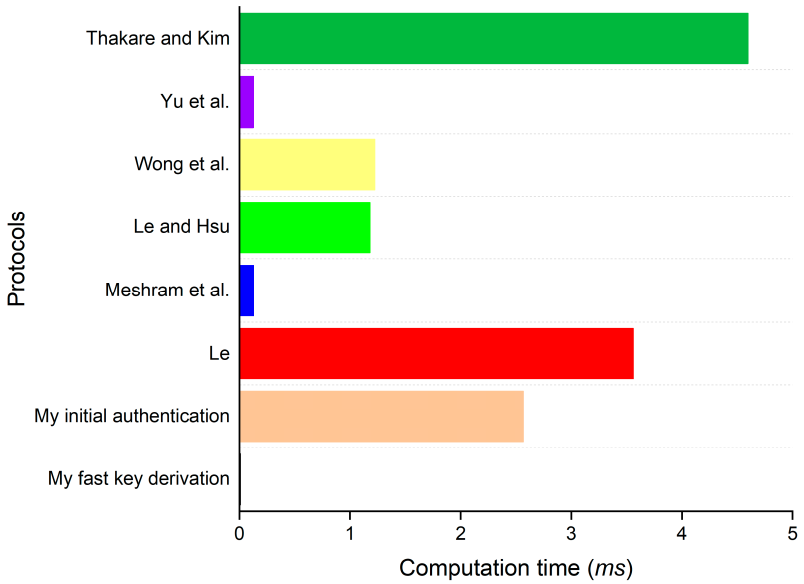

Figure 7. Graphical description of the comparison of computation overhead [28–31,36,37].

Apart from that, the author considers a scenario in which multiple S_j provide services to a single P_i. Here, the SD-SSO function is helpful since it allows P_i to enjoy multiple services using a single set of credentials for the login. The SD-SSO also save a little bit of computing cost as its operations, including $\sigma = \varepsilon_i \oplus h(ID_i^*||PW_i^*||h_{bio}(B_i^*))$, $PB^* = h(ID_i^*||PW_i^*||h_{bio}(B_i^*)||\sigma)$ and $V \stackrel{?}{=} h(ID_i^*||PB^*||\sigma)$, only need to be executed once before the communications with multiple S_j. According to the result depicted in Figure 8, when the number of servers S_j increases, both procedures of the proposed protocol (especially the fast key derivation) incur less and less overhead compared with that of the others. Furthermore, due to the group key, S_j in the proposed architecture only needs to encrypt health data once before sending it to all P_i while S_j in the other works (except Le and Hsu [31]) must encrypt the same data multiple times, which results in redundant computation costs. Moreover, the patients in those works are not able to directly communicate with each other without a common key. As a matter of fact, the proposed group communication solution in this work is the best fit for group-based U-healthcare services.

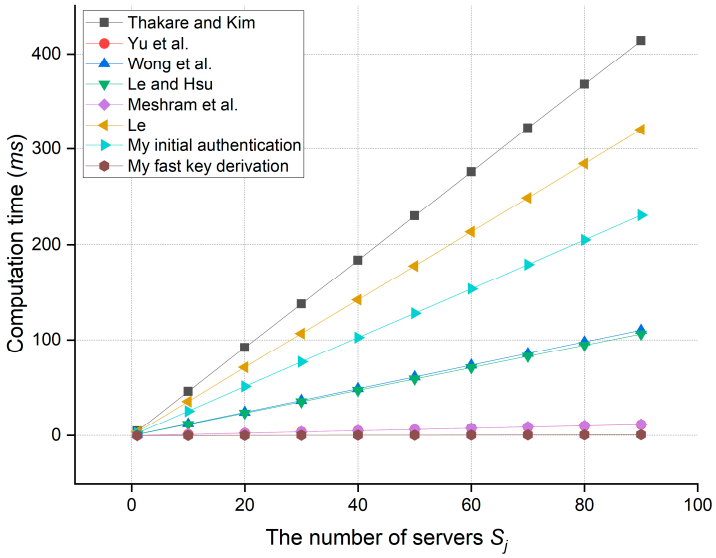

Figure 8. Computational comparison when the number of servers gradually increases [28–31,36,37].

7.3. Communication Overhead

In this evaluation, communication overhead includes the number of communication rounds and total length of all transmitted transcripts. Some parameters used for evaluating the overhead are provided in Table 8. In the initial authentication procedure of the proposed protocol, the transcripts of two communication rounds include $\{DID_i, R_i, Auth_i, T_p\}$ and $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$. For a fair comparison, $\{[x_1, x_2, \ldots, x_n], Y_j, Auth_j, T_s\}$ should contain parameters of a single patient, which only results in a single value x in the transcript. $\{DID_i, R_i, Auth_i, T_p\}$ and $\{x, Y_j, Auth_j, T_s\}$ consume a length of (160 bits + 320 bits + 160 bits + 32 bits) and (384 bits + 160 bits + 160 bits + 32 bits), respectively; the total length is (672 bits + 736 bits) = 1408 bits. Similarly, overhead values of all protocols are calculated and provided in Table 9. Figure 9 further provides a graphical description of the comparison. We can observe that the proposed protocol incurs less overhead than the works of Thakare and Kim [28], Le and Hsu [31], and Meshram et al. [36]. Due to providing the support of more functionality, the author's work consumes more costs compared to that of Yu et al. [29], Wong et al. [30], and Le [37]. Furthermore, when the proposed work executes the fast key-derivation process, its communication only incurs 256 bits (the length of C_d) and only one communication round. As a result, it is the most efficient out of all the protocols.

Table 8. Single length of multiple parameters [44,45].

Parameters	Length (Bits)
Asymmetric encryption or decryption (e.g., Rabin system)	1024
Chebyshev polynomial	1024
Symmetric encryption or decryption	256
Identity	128
Password	128
Biometrics	128
Random number	160
Hash value	160
EC point multiplication	320
Timestamp	32

Table 9. Comparison of communication overhead.

Protocols		No. of Communication Rounds	Length of Total Transcripts (Bits)
Thakare and Kim [28]		3	1440
Yu et al. [29]		3	1120
Wong et al. [30]		2	1344
Le and Hsu [31]		2	1440
Meshram et al. [36]		2	3072
Le [37]		2	1088
Mine	Initial authentication	2	1408
	Fast key derivation	1	256

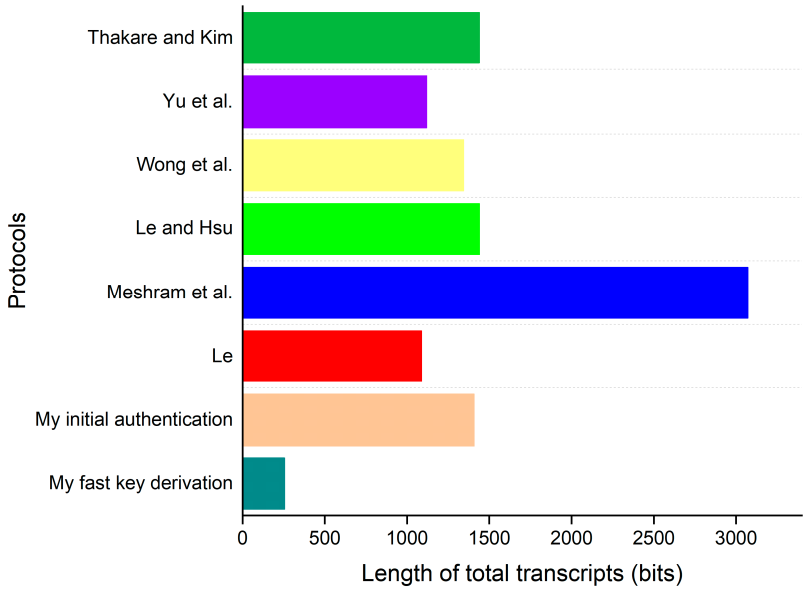

Figure 9. Graphical description of the comparison of communication overhead [28–31,36,37].

8. Conclusions

In this article, the author has proposed a group-based patient-authenticated key distribution protocol for 6G-aided dynamic U-healthcare services enabled by real-time mobile DNA sequencing. Seamless communications are provided by 6G technology regardless of patients' geographical locations. Sharing mobile DNA data for rapid analysis is a good solution for facilitating drug and vaccine development, which is one of the important concerns in the public health sector. Group service helps in improving medical treatments efficiently and promoting the use of smart health with more people participating. Patients in a healthcare group are allowed to securely connect with the service provider or with each other using a common group key generated from the protocol for the specific purposes of dynamic services. The group key generation process is protected by a three-factor authentication mechanism along with an efficient SD-SSO solution. Since all registered credentials are stored on a separate sequencer, the proposed work can enable service availability on multiple mobile devices. It is also able to facilitate a truly patient-centered service upon storing traceable information in the server database. Security analysis of the proposed protocol is presented using well-known verification tools, namely, the RoR model and BAN logic. A semantic discussion is also provided to further indicate its resistance to multiple security attacks. A detailed performance analysis of computation and communication overhead shows that the proposed approach consumes a rational cost compared to predecessor works.

In future works, performance of the initial authentication procedure can be further improved by including more lightweight cryptographic operations in the protocol. Another

patient authentication scheme with a new architecture model where multiple external doctors serving as data users join the healthcare processes will be considered. The author will also consider a new design of attribute-based access control for securing cloud-based U-healthcare services in IoLT networks.

Funding: This research was funded by National Science and Technology Council (Taiwan), grant number NSTC-112-2222-E-030-001; and by Fu Jen Catholic University (Taiwan), grant number A0211018-1.

Data Availability Statement: Not available.

Acknowledgments: The author would like to thank National Science and Technology Council (Taiwan) and Fu Jen Catholic University (Taiwan), for sponsoring this research. The author would also like to thank anonymous referees for their constructive comments, and thank editors for kindly coordinating the review process.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Milicchio, F.; Oliva, M.; Boucher, C.; Prosperi, M. Third-generation sequencing data analytics on mobile devices: Cache oblivious and out-of-core approaches as a proof-of-concept. *Procedia Comput. Sci.* **2018**, *134*, 219–226. [CrossRef]
2. Hassan, S.; Bahar, R.; Johan, M.F.; Mohamed Hashim, E.K.; Abdullah, W.Z.; Esa, E.; Abdul Hamid, F.S.; Zulkafli, Z. Next-Generation Sequencing (NGS) and Third-Generation Sequencing (TGS) for the Diagnosis of Thalassemia. *Diagnostics* **2023**, *13*, 373. [CrossRef]
3. Raza, K.; Qazi, S. Chapter 5—Nanopore sequencing technology and Internet of living things: A big hope for U-healthcare. In *Sensors for Health Monitoring*; Dey, N., Chaki, J., Kumar, R., Eds.; Academic Press: Cambridge, MA, USA, 2019; Volume 5, pp. 95–116.
4. Pizzolante, R.; Castiglione, A.; Carpentieri, B.; De Santis, A.; Palmieri, F.; Castiglione, A. On the protection of consumer genomic data in the Internet of Living Things. *Comput. Secur.* **2018**, *74*, 384–400. [CrossRef]
5. Bolognini, D.; Bartalucci, N.; Mingrino, A.; Vannucchi, A.M.; Magi, A. NanoR: A user-friendly R package to analyze and compare nanopore sequencing data. *PLoS ONE* **2019**, *14*, e0216471. [CrossRef] [PubMed]
6. Lacerda, J.M.T.; Valentim, R.A.M.; Araújo, B.G.d.; Morais, P.S.G.; Dantas, M.C.M. Service-oriented biomedical devices. In Proceedings of the 2014 IEEE Healthcare Innovation Conference (HIC), Seattle, WA, USA, 8–10 October 2014; pp. 203–206.
7. García-Hernández, L.A.; Martínez-Martínez, E.; Pazos-Solís, D.; Aguado-Preciado, J.; Dutt, A.; Chávez-Ramírez, A.U.; Korgel, B.; Sharma, A.; Oza, G. Optical Detection of Cancer Cells Using Lab-on-a-Chip. *Biosensors* **2023**, *13*, 439. [CrossRef] [PubMed]
8. Nanopore, O. Oxford Nanopore Announces £100 Million ($140M) Fundraising from Global Investors. Available online: https://nanoporetech.com/about-us/news/oxford-nanopore-announces-ps100-million-140m-fundraising-global-investors (accessed on 12 May 2023).
9. Nayak, S.; Patgiri, R. 6G Communication Technology: A Vision on Intelligent Healthcare. In *Health Informatics: A Computational Perspective in Healthcare*; Patgiri, R., Biswas, A., Roy, P., Eds.; Springer: Singapore, 2021; pp. 1–18. [CrossRef]
10. Chen, S.; Liang, Y.C.; Sun, S.; Kang, S.; Cheng, W.; Peng, M. Vision, Requirements, and Technology Trend of 6G: How to Tackle the Challenges of System Coverage, Capacity, User Data-Rate and Movement Speed. *IEEE Wirel. Commun.* **2020**, *27*, 218–228. [CrossRef]
11. Khattak, S.B.A.; Nasralla, M.M.; Rehman, I.U. The Role of 6G Networks in Enabling Future Smart Health Services and Applications. In Proceedings of the 2022 IEEE International Smart Cities Conference (ISC2), Pafos, Cyprus, 26–29 September 2022; pp. 1–7.
12. Nayak, S.; Patgiri, R. 6G Communication: Envisioning the Key Issues and Challenges. *EAI Endorsed Trans. Internet Things* **2020**, *6*, 166959. [CrossRef]
13. Barman, S.; Shum, H.P.H.; Chattopadhyay, S.; Samanta, D. A Secure Authentication Protocol for Multi-Server-Based E-Healthcare Using a Fuzzy Commitment Scheme. *IEEE Access* **2019**, *7*, 12557–12574. [CrossRef]
14. Noohani, M.Z.; Magsi, K.U. A Review Of 5G Technology: Architecture, Security and wide Applications. *IRJET J.* **2020**, *7*, 3440–3471. [CrossRef]
15. Yaacoub, E.; Alouini, M. A Key 6G Challenge and Opportunity—Connecting the Base of the Pyramid: A Survey on Rural Connectivity. *Proc. IEEE* **2020**, *108*, 533–582. [CrossRef]
16. Minglan, S.; Chaoying, Z.; Qiaoqiao, L.; Baolin, L.; Jianxiu, W. Holographic communication technology. In Proceedings of the 2021 International Conference on Neural Networks, Information and Communication Engineering, Qingdao, China, 27–28 August 2021.
17. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.A. The Roadmap to 6G: AI Empowered Wireless Networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
18. Chen, Z.; Ma, X.; Zhang, B.; Zhang, Y.; Niu, Z.; Kuang, N.; Chen, W.; Li, L.; Li, S. A survey on terahertz communications. *China Commun.* **2019**, *16*, 1–35. [CrossRef]

19. Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence. *IEEE Wirel. Commun.* **2020**, *27*, 126–132. [CrossRef]
20. Alraih, S.; Shayea, I.; Behjati, M.; Nordin, R.; Abdullah, N.F.; Abu-Samah, A.; Nandi, D. Revolution or Evolution? Technical Requirements and Considerations towards 6G Mobile Communications. *Sensors* **2022**, *22*, 762. [CrossRef]
21. Deebak, B.D.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 346–360. [CrossRef]
22. Chiou, S.-Y.; Ying, Z.; Liu, J. Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment. *J. Med. Syst.* **2016**, *40*, 101. [CrossRef]
23. Yuanbing, W.; Wanrong, L.; Bin, L. An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network. *IEEE Access* **2021**, *9*, 105101–105117. [CrossRef]
24. Farash, M.S.; Turkanović, M.; Kumari, S.; Hölbl, M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Netw.* **2016**, *36*, 152–176. [CrossRef]
25. Kumar, V.; Mahmoud, M.S.; Alkhayyat, A.; Srinivas, J.; Ahmad, M.; Kumari, A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. *J. Supercomput.* **2022**, *78*, 16167–16196. [CrossRef]
26. Gupta, D.S.; Mazumdar, N.; Nag, A.; Singh, J.P. Secure data authentication and access control protocol for industrial healthcare system. *J. Ambient Intell. Humaniz. Comput.* **2023**, *14*, 4853–4864. [CrossRef]
27. Alam, I.; Kumar, M. A novel authentication protocol to ensure confidentiality among the Internet of Medical Things in covid-19 and future pandemic scenario. *Internet Things* **2023**, *22*, 100797. [CrossRef] [PubMed]
28. Thakare, A.; Kim, Y.-G. Secure and Efficient Authentication Scheme in IoT Environments. *Appl. Sci.* **2021**, *11*, 1260. [CrossRef]
29. Yu, Y.; Taylor, O.; Li, R.; Sunagawa, B. An Extended Chaotic Map-Based Authentication and Key Agreement Scheme for Multi-Server Environment. *Mathematics* **2021**, *9*, 798. [CrossRef]
30. Wong, A.-K.; Hsu, C.-L.; Le, T.-V.; Hsieh, M.-C.; Lin, T.-W. Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks. *Sensors* **2020**, *20*, 2511. [CrossRef]
31. Le, T.V.; Hsu, C.L. An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments. *IEEE Access* **2021**, *9*, 53408–53422. [CrossRef]
32. Zhang, L.; Zhang, Y.; Tang, S.; Luo, H. Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement. *IEEE Trans. Ind. Electron.* **2018**, *65*, 2795–2805. [CrossRef]
33. Mangard, S.; Oswald, E.; Popp, T. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2007. [CrossRef]
34. Harn, L.; Hsu, C.; Xia, Z. Lightweight and flexible key distribution schemes for secure group communications. *Wirel. Netw.* **2021**, *27*, 129–136. [CrossRef]
35. Tselikis, C.; Douligeris, C.; Maglaras, L.; Mitropoulos, S. On the conference key distribution system with user anonymity. *J. Inf. Secur. Appl.* **2020**, *54*, 102556. [CrossRef]
36. Meshram, C.; Ibrahim, R.W.; Deng, L.; Shende, S.W.; Meshram, S.G.; Barve, S.K. A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment. *Soft Comput.* **2021**, *25*, 10037–10051. [CrossRef]
37. Le, T.-V. Cross-Server End-to-End Patient Key Agreement Protocol for DNA-Based U-Healthcare in the Internet of Living Things. *Mathematics* **2023**, *11*, 1638. [CrossRef]
38. Normand, R.; Yanai, I. An introduction to high-throughput sequencing experiments: Design and bioinformatics analysis. *Methods Mol. Biol.* **2013**, *1038*, 1–26. [CrossRef] [PubMed]
39. Mignardi, M.; Nilsson, M. Fourth-generation sequencing in the cell and the clinic. *Genome Med.* **2014**, *6*, 31. [CrossRef]
40. Jujjavarapu, C.; Anandasakaran, J.; Amendola, L.M.; Haas, C.; Zampino, E.; Henrikson, N.B.; Jarvik, G.P.; Mooney, S.D. ShareDNA: A smartphone app to facilitate family communication of genetic results. *BMC Med. Genom.* **2021**, *14*, 10. [CrossRef] [PubMed]
41. Borré Ortiz, Y.; Suarez, M.; Expósito, M. Importance and Recognition of the Family in Health Care: A Reflection for Nursing. *Nurs. Care Open Access J.* **2017**, *3*, 00084. [CrossRef]
42. Liu, W.; Wang, X.; Peng, W.; Xing, Q. Center-Less Single Sign-On With Privacy-Preserving Remote Biometric-Based ID-MAKA Scheme for Mobile Cloud Computing Services. *IEEE Access* **2019**, *7*, 137770–137783. [CrossRef]
43. Shohaimay, F.; Ismail, E.S. Improved and Provably Secure ECC-Based Two-Factor Remote Authentication Scheme with Session Key Agreement. *Mathematics* **2023**, *11*, 5. [CrossRef]
44. Le, T.V.; Lu, C.F.; Hsu, C.L.; Do, T.K.; Chou, Y.F.; Wei, W.C. A Novel Three-Factor Authentication Protocol for Multiple Service Providers in 6G-Aided Intelligent Healthcare Systems. *IEEE Access* **2022**, *10*, 28975–28990. [CrossRef]
45. Shuai, M.; Xiong, L.; Wang, C.; Yu, N. A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem. *Comput. Commun.* **2020**, *160*, 215–227. [CrossRef]