FAIDM for Medical Privacy Protection in 5G Telemedicine Systems

Tzu-Wei Lin 1 and Chien-Lung Hsu 1,2,3,4,5,*

1 Graduate Institute of Business and Management, Chang Gung University, Taoyuan 333, Taiwan; d0640001@cgu.edu.tw
2 Department of Information Management, Chang Gung University, Taoyuan 333, Taiwan
3 Healthy Aging Research Center, Chang Gung University, Taoyuan 333, Taiwan
4 Department of Visual Communication Design, Ming-Chi University of Technology, Taoyuan 243, Taiwan
5 Administration, Chang Gung Memorial Hospital, Taoyuan 333, Taiwan
* Correspondence: clhsu@mail.cgu.edu.tw

Featured Application: This work can be applied in 5G telemedicine systems which can remote monitor health condition of patients and provide medical related data to medical professional. Devices on patients, which are IoT devices, should be managed properly, and proposed scheme can achieve the purpose while preserving privacy.

Abstract: 5G networks have an efficient effect in energy consumption and provide a quality experience to many communication devices. Device-to-device communication is one of the key technologies of 5G networks. Internet of Things (IoT) applying 5G infrastructure changes the application scenario in many fields especially real-time communication between machines, data, and people. The 5G network has expanded rapidly around the world including in healthcare. Telemedicine provides long-distance medical communication and services. Patient can get help with ambulatory care or other medical services in remote areas. 5G and IoT will become important parts of next generation smart medical healthcare. Telemedicine is a technology of electronic message and telecommunication related to healthcare, which is implemented in public networks. Privacy issue of transmitted information in telemedicine is important because the information is sensitive and private. In this paper, 5G-based federated anonymous identity management for medical privacy protection is proposed, and it can provide a secure way to protect medical privacy. There are some properties below. (i) The proposed scheme provides federated identity management which can manage identity of devices in a hierarchical structure efficiently. (ii) Identity authentication will be achieved by mutual authentication. (iii) The proposed scheme provides session key to secure transmitted data which is related to privacy of patients. (iv) The proposed scheme provides anonymous identities for devices in order to reduce the possibility of leaking transmitted medical data and real information of device and its owner. (v) If one of devices transmit abnormal data, proposed scheme provides traceability for servers of medical institute. (vi) Proposed scheme provides signature for non-repudiation.

Keywords: telemedicine; 5G; anonymity; identity management; medical privacy preservation

1. Introduction

5G (the fifth generation) networks, also known as next generation of 4G, is the newest standard of mobile telecommunication from 3GPP which is being deployed, providing high-speed network, big capacity, and scalability [1,2]. 5G networks have an efficient effect in energy consumption and provide a quality experience via a large number of communication devices [3]. End point devices transmit data and request for services through a small base station (SBS) and major base station (MBS) [1,4,5]. A device connects with SBS by using a high-band spectrum (5G mmWave) technology and device-to-device (D2D) communication, which is one of the key technologies of 5G networks [1,4,5]. Moreover, 5G combines and
connects virtual systems to cloud environments through artificial intelligence and helps derive different calculating models [6]. 5G will totally change connected services and devices through higher reliability, connectivity, and cloud storage [6]. Because 5G network is a multi-server environment, conventional schemes for single server structure are not suitable [3]. Many reasons lead to multi-server environment requirements including load balance, expanded coverage, and security [3].

IoT becomes a focus because of being predicted to be an important component of 5G networks [1]. IoT applying 5G infrastructure changes application scenario in many fields especially real-time communication between machines, data, and people [7]. Moreover, 5G network can work with amount of IoT devices [7]. We can see a form of 5G-based IoT networks which assembles smart phone, virtual reality, sensors, and other numerous wireless communication devices [3]. As the result, IoT with 5G technology influences social life largely [3].

Nowadays, medical healthcare systems face many challenges, such as infrastructure, connections, professional requirements, data management, and real-time monitoring [8]. About 40% countries have less than one doctor for one thousand population and less than 18 sickbeds for ten thousand population according to global survey data from 2005 to 2015 [8,9]. 5G networks have expanded rapidly around the world including in healthcare [5]. Internet of things (IoT) with a 5G environment provides solutions for network layers, including enhancing quality of service, router and jamming control, and resource optimization, to solve some challenges of smart medical healthcare [1]. Lloret et al. utilized a smart phone to continuously monitor chronic patients in IoT with a 5G environment [10]. Chen et al. proposed a mobile medical system based on IoT with a 5G environment to continuously evaluate and monitor diabetes patients [11]. This augers a new and reliable business model of medical health with 5G technology. 5G and IoT will become important parts of the next generation smart medical healthcare [1].

Medical privacy is of the utmost importance. Once leaked, it not only brings huge economic losses and loss of credibility to hospitals and other related institutions, but also does potential harm to patients, and, more importantly, it can even endanger lives of patients, which will seriously damage the healthy development of medical industry [12]. Unfortunately, the healthcare industry has lagged to meet users’ expectations. The health data, which is stored in conventional system, are very difficult to share due to varying standards and data formats, i.e., current healthcare ecosystem is ill-suited for the instantaneous needs of modern user. Maintaining privacy of user data is very important and failure to this will result in implications related to financial as well as legal sectors [13]. If a person’s medical information is the key to finding clinical treatment, how to maintain the privacy of health records is a central issue that determines the success of medical practice. Increasingly, people interact with health-care providers, using digital media technologies [14–16]. Accompanying the acceleration of medical data collection are rapid advancements in algorithmic computing capacities to aggregate, analyze, and draw sensitive inferences about individuals from their health data [15,17–19].

Since the above description, federated anonymous identity management (FAIDM) for medical privacy protection in telemedicine systems is proposed in this paper, which can provide a secure way to protect medical privacy. There are some properties below. (i) The proposed scheme provides federated identity management which can manage identity of devices in a hierarchical structure efficiently. (ii) Identity authentication will be achieved by mutual authentication. (iii) The proposed scheme provides session key to secure transmitted data which is related to privacy of patients. (iv) The proposed scheme provides anonymous identities for devices in order to reduce the possibility of leaking transmitted medical data and real information of device and its owner. (v) If one of devices transmit abnormal data, the proposed scheme provides traceability for servers of medical institute. (vi) the proposed scheme provides signature for non-repudiation.

The rest of this paper is organized as follows. We introduce related works in Section 2, including telemedicine, healthcare certificate, ID-based cryptosystem, definitions of Cheby-
shev chaotic maps, and chaotic maps-based signature which we apply in our scheme. In Section 3, we describe the proposed scheme. We discuss the security and performance analysis of proposed scheme in Sections 4 and 5, respectively. Finally, some concluding remarks are presented.

2. Related Works

In this section, we introduce telemedicine, Chebyshev chaotic maps, healthcare certificate, chaotic maps-based signature, and some related works.

2.1. Telemedicine

Telemedicine is a technology of electronic message and telecommunication related to healthcare [20,21]. The patient will send healthcare related information, which is important, sensitive, and private, to healthcare services through public networks when using telemedicine technology [21]. Medical professionals can know users’ health condition if they are able to view the information immediately [21]. Data transmission security will be discussed, such as eavesdropping, man-in-the-middle attack, data tempering attack, message modification attack, and data interception attack [22]. Technical support is not enough though Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and Safe Harbor Laws have been made which provide personal information privacy [22–24].

A general telemedicine system can be divided to three levels [25]. Level 1 (primary healthcare unit) consist of users with webcam, smart phone, or wearable devices; Level 2 (city or district hospital) is clinic or local hospital which patient may visit before being transferred to large hospital or medical center; Level 3 (specialty center) will take part in telemedicine in case of rare disease or incurable disease [25]. Figure 1 illustrates a remote patient monitoring system in 5G IoT architecture which can assist medical professional to monitor remote patient’s biodata through specific devices [2,25,26]. Mobile health plays an important role on medical healthcare monitoring and alarm system and clinical data storage and maintenance system. In remote patient monitoring systems, wearable devices and mobile phones belong to a sensor layer which is responsible for gathering measured data. Measured data is transmitted to network layer, IoT gateway for example, through small base station (SBS) communication. After that, data will be transmitted out of the local area network to major base station (MBS), such as 5G link, through MBS communication. Both the network layer and communication layer are responsible for data processing. Finally, data will be transmitted to a medical services servers of clinic or local hospital called architecture layer, such as an electronic health records (EHR) system, cloud storage, and analytics. Authorized medical professionals in the main hospital can access medical services servers to monitor a patient. Authorized medical professionals in specialty center will involve and observe measured data in case of rare disease or incurable disease.

In this paper, we introduced a cryptographic protocol which can be applied in asynchronous telemedicine and synchronous telemedicine and provide communication security and user anonymity to protect patient’s privacy.

2.2. Healthcare Certificate

Medical and healthcare devices nowadays are required certifications under safety and functional requirements [27]. Meanwhile, healthcare service providers should go through a certification procedure based on ISO 27000 and 20000 series in order to process healthcare data [27]. However, different kinds of healthcare devices have different safety and privacy requirements [27]. Establishing a general certification for all healthcare sectors is difficult [27]. One of the solutions to the problem would be to design segregated schemes with links between them, such as a healthcare certificate issued by a trusted institution [27]. All medical and healthcare devices should be issued certificates to proof that they are qualified in safety and functional requirements [27]. In other words, using certified components can be a requirement in medical and healthcare field.
2.3. ID-Based Cryptosystem

In 1985, Shamir introduced the concept of identity-based (ID-based) cryptosystem [28]. The main difference from traditional public key cryptosystem is that it derives the user’s public key from public information that uniquely identifies the user. Since it is meaningful information, we do not need any certificate to prove the validity of the corresponding public key. In 2002, Gentry et al. proposed hierarchical ID-based cryptography, also called HIDC [29]. The major purpose of Gentry et al.’s scheme is reducing the loading of private key generation (called PKG) and the risk of key escrow [29]. In the structure of HIDC, there is a key generation center at each level, and the one at the top level is root PKG. The root PKG is the third trusted center, and there will be legal sub-level key generation centers where users under the same domain register to. In 2009, Yan et al. discovered that HIDC was suitable for cloud computing and improved the register phase in order to achieve federated identity management because as more and more cloud service providers provide various cloud services via different interfaces, federal identity management becomes a rising issue [30]. The cloud service providers in Yan et al.’s scheme can compose an alliance, and users can sign on with one account and use various cloud services [30]. However, Yan et al.’s scheme [30] only proposed mutual authentication for security except for rules of identity authentication code, and it did not mention the possible security problems of cloud computing. Nevertheless, Yan et al.’s scheme [30] does not provide user anonymity. Park et al. [31] proposed an HIDC scheme for VANETs which provided vehicle user anonymity, but it is not suitable for cloud computing. Shen et al. introduced an HIDC scheme with time-bound and key management for multicast systems [32]. Fremantle and Aziz [33] proposed a cloud-based federal identity management mechanism for IoT, and Maria et al. [34] proposed a lightweight federal identity management mechanism for IoT. However, federal identity management in 5G IoT environment is still lack of discussions, not to mention telemedicine in a 5G IoT environment.

2.4. Chebyshev Chaotic Maps

The chaotic system is characterized by a sensitive dependence on initial conditions, pseudo-randomness, and ergodicity [35–37]. These features have the excellent properties of diffusion and confusion, which are important in cryptography [35,36]. Researchers have proposed image encryption in chaotic maps [38,39]. Definitions of Chebyshev chaotic maps are introduced below.
Definition 1. The Chebyshev polynomial \( T_n(x) : [-1, 1] \rightarrow [-1, 1] \) is a polynomial in \( x \) of degree \( n \), defined as 
\[ T_n(x) = \cos(n \cos^{-1}(x)) \].

Definition 2. The recurrent relation of \( T_n(x) \) is defined as 
\[ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \] for any \( n \geq 2 \), \( T_0(x) = 1 \), and \( T_1(x) = x \).

Definition 3. One of the most important properties of Chebyshev polynomials is semi-group property which establishes \( T_s(T_r(x)) = T_{s+r}(x) \) for any \((s, r) \in \mathbb{Z} \) and \( s, r \in [-1, 1] \). The interval \([-1, 1]\) is invariant under the action of the map \( T_n(x) : [-1, 1] \rightarrow [-1, 1] \). Therefore, the Chebyshev polynomial restricted to the interval \([-1, 1]\) is a well-known chaotic map for all \( n > 1 \). It has a unique continuous invariant measure with positive Lyapunov exponent \( \ln n \). For \( n = 2 \), Chebyshev maps reduces to well-known logistic maps.

Definition 4. In order to enhance property of Chebyshev chaotic maps, Zhang [40] proved that the semi-group property holds for Chebyshev polynomials defined on interval \([-\infty, +\infty]\). This paper utilizes the following enhanced Chebyshev polynomials.
\[ T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \mod N \]
where \( n \geq 2 \), \( x \in (-\infty, +\infty) \), and \( N \) is a large prime number. According to the equations, the semi-group property still holds, and the enhanced Chebyshev polynomials also commute.
\[ T_s(T_r(x)) \mod N = T_{s+r}(x) \mod N = T_s(T_r(x)) \mod N \]

Definition 5. Chaotic maps-based discrete logarithm problem (CMDLP). Given two elements \( x \) and \( y \), it is computationally infeasible to find the integer \( n \) such that \( T_n(x) \mod N = y \).

Definition 6. Chaotic maps-based Diffie-Hellman problem (CMDHP). Given three elements \( x \), \( T_r(x) \mod N \), and \( T_s(x) \mod N \), it is computationally infeasible to compute \( T_{s+r}(x) \mod N \).

2.5. Chaotic Maps-Based Signature

Chebyshev chaotic maps has been utilized not only in authentication, key agreement schemes but signature schemes. Chain and Kuo first proposed a digital signature scheme based on chaotic maps [41]. Several signature schemes based on chaotic maps have been proposed recently. For example, Tahat and Hijazi [42] proposed an enhanced signature scheme to improve Chain and Kuo’s [41]; Tahat et al. proposed an ID-based cryptographic model for Chebyshev chaotic maps to demonstrate the transformation model of ID-based schemes [43]; Tahat et al. proposed an ID-based blind signature based on chaotic maps [44]. Meshram et al. focused on online/offline short signature schemes and proposed schemes using chaotic maps [45], such as ID-based short signature scheme and subtree-based short signature scheme for wireless sensor network [46]. In this paper, we apply Meshram et al.’s ID-based online short signature scheme [45].

3. Proposed Scheme

In this paper, we proposed a FAIDM for medical privacy protection in 5G telemedicine systems. The notations of the scheme are shown as Table 1. The system structure of proposed scheme includes remote server node, gateway node (GWj), and constrained node (CNij). A constrained node is in a sensor layer of a proposed 5G IoT remote patient monitoring system structure and can be in devices which gather measured data, such as sensors or wearable devices that can be carried by a human. The role of these devices consists of monitoring or sensing the environment, so they collect and transmit data to gateway nodes. For example, in a healthcare application, sensors can be planted in or on a human’s body in order to collect health-related data. Gateway nodes, which are SBSs/MBSs, are in the network or communication layers of the proposed 5G IoT remote
patient monitoring system structure, and it can be assumed that the gateway nodes have enough energy resources, performance processors, and memory. Gateway nodes process received data collected by the different constrained nodes and forward the to the remote server node. Remote server node is in architecture layer of proposed 5G IoT remote patient monitoring system structure and can be assumed that remote server node has no limitations of computing resource. Medical professionals in the architecture layer can continuously follow a patient’s health status based on data received. Note that the interaction between communication and the architecture layer should be secure which may be guaranteed by functions in the core network, such as authentication server function (AUSF), authentication credential repository and processing function (ARPF), subscription identifier de-concealing function (SIDF), and security anchor function (SEAF) [47,48], but secure communication between these two layers is not discussed in our scheme. The remote server node takes part in the system initialization and generating system parameters. A constrained node has to register to any legitimate gateway node for becoming legitimate. A gateway node has to register to the remote server node for becoming legitimate. When a patient wears a wearable healthcare device and goes home from hospital, the device transmits measured data through an IoT gateway (GW_i) at home which is in different domain from hospital. The system structure is show as Figure 2.

Table 1. Notations of the proposed scheme.

| Notations                  | Definitions                                                                 |
|----------------------------|-----------------------------------------------------------------------------|
| $s_0$                      | The secrete value of remote server node $S$                                  |
| $s_i$                      | The secrete value of $i$th gateway node ($GW_i$)                            |
| $s_{ij}$                   | The secrete value of $ij$th constrained node ($CN_{ij}$)                    |
| $S_i$                      | Private key of $GW_i$ after registering to remote server node               |
| $S_{ij}$                   | Private key of $CN_{ij}$ after registering to $GW_i$                        |
| $aS_{ij}$                  | $CN_{ij}$’s anonymous private key issued by $GW_i$                         |
| $ID_i, ID_{ij}, aID_{ij}$  | Identity of $GW_i, CN_{ij}$ and $CN_{ij}$’s anonymous identity             |
| $Q_{0}, Q_{i}, Q_{ij}, Q_{aID}$ | Public parameters of generated by secrete values                           |
| $sk_{GW_i→CN_{ij}}$        | The session key of $CN_{ij}$ and $GW_i$                                    |
| $H_1(\cdot), H_2(\cdot), H_3(\cdot)$ | Collision-resistance one-way hash functions                               |
| $E_k(\cdot), D_k(\cdot)$  | The symmetric encryption and decryption using $k$ as the key                |
| $MAC_{GW_i}, MAC_{CN_{ij}}$ | The message authentication code algorithm of $GW_i$ and $CN_{ij}$          |
| $Cert_{HCA→S}$             | The certification issued by healthcare certification authority to remote server node $S$. |
| $Cert_{S→GW_i}$            | The certification issued by remote server node $S$ to $GW_i$ which is generate from $Cert_{HCA→S}$. |
| $Cert_{GW_i→CN_{ij}}$      | The certification issued by $GW_i$ to $CN_{ij}$ which is generate from $Cert_{S→GW_i}$. |

The proposed scheme consists of seven phases: System initialization phase, gateway node registration phase, constrained node registration phase, mutual authentication and key agreement phase, anonymous identity distribution phase, and anonymous signature and verification phase. The notations of proposed scheme are shown in Table 1.

Before system initialization phase, the healthcare services provider needs to apply for certificates $Cert_{HCA→S}$ from healthcare certification authority before providing healthcare services. The healthcare certification authority should be a credible and dependent institute, such as National Health Service Business Services Authority (NHSBSA) of United Kingdom [49], European Federation Gateway Service (EFGS) of European Commission [50], American Hospital Association Certification Center (AHA-CC) of USA [51], Pharmaceuticals and Medical Devices Agency (PMDA) of Ministry of Health, Labor and Welfare, Japan [52], or Healthcare Certification Authority (HCA) of Ministry of Health and Welfare, Taiwan [53]. The certificate $Cert_{HCA→S}$ is regarded as the root certificate in the system, and only certified healthcare services provider can obtain $Cert_{HCA→S}$.
3.1. System Initialization Phase

In the remote server node initial phase, the remote server node $S$, which provides telemedicine services and is certified by healthcare certification authority, sets up parameters by performing following steps.

Step 1: The healthcare certification authority issues a certificate $\text{Cert}_{\text{HCA}} \rightarrow S$ to remote server node $S$ which provides telemedicine services and is certified by healthcare certification authority.

Step 2: The remote server node $S$ generates a secret value $s_0$, a big prime $p$, and random number $x \in (-\infty, +\infty)$ and computes $Q_0 = T_{s_0}(x) \mod p$.

Step 3: The remote server node $S$ chooses a symmetric encryption algorithm $E_k(\cdot)$, a symmetric decryption algorithm $D_k(\cdot)$, collision-resistance one-way hash functions $(H_1(\cdot), H_2(\cdot), H_3(\cdot))$, and a collision-resistance secure one-way chaotic hash function $h_k(\cdot)$.

Step 4: The remote server node $S$ outputs public parameters $\{Q_0, p, x, H_1(\cdot), H_2(\cdot), H_3(\cdot), h_k(\cdot), E_k(\cdot), D_k(\cdot)\}$ and private parameters $s_0$.

Step 5: The gateway node $GW_i$ generates two large random primes $(p_i, q_i)$, $N_i$, and $q_i$ as follows. Then, the gateway node $GW_i$ selects a random integer $e_i$ where $1 < e_i < q_i$ and $\gcd(e_i, q_i) = 1$, and makes it public. After that, the gateway node $GW_i$ computes $d_i$, where $1 < d_i < q_i$ and $e_id_i \equiv 1 \pmod{q_i}$ and keeps it secretly.

3.2. Gateway Node Registration Phase

In this phase, gateway node $GW_i$ interacts with remote server node $S$ for registration. To deal with the registration request submitted by the gateway node $GW_i$, the remote server node $S$ validates the gateway node $GW_i$’s legitimacy then issues the private key $S_i$ and certificate $\text{Cert}_{S_i} \rightarrow GW_i$ via a secure channel. Note that remote server node $S$ computes a private key by gateway node $GW_i$’s registration information. Figure 3. illustrates process of gateway node registration phase. Detailed descriptions are stated as follows:
Figure 3. Gateway node registration phase of proposed scheme.

Step 1: The gateway node GW\textsubscript{i} chooses an identifier ID\textsubscript{i} and submits to remote server node S.

Step 2: Upon receiving ID\textsubscript{i} from gateway node GW\textsubscript{i}, remote server node checks the format of ID\textsubscript{i}. If ID\textsubscript{i} is valid, remote server node S computes Si correspond to ID\textsubscript{i}, generates Cert\textsubscript{S→GW\textsubscript{i}} from Cert\textsubscript{HCA→S}, and sends (S\textsubscript{i}, Cert\textsubscript{S→GW\textsubscript{i}}) via secure channel to the gateway node GW\textsubscript{i}.

\begin{align*}
P_{i} &= H_{1}(ID_{i}) \\
S_{i} &= T_{S_{0}}(P_{i}) \mod p
\end{align*}

Step 3: The gateway node GW\textsubscript{i} chooses a random number s\textsubscript{i} as secret value and computed Q\textsubscript{i} and stores Cert\textsubscript{S→GW\textsubscript{i}} to complete gateway node registration phase.

\begin{equation}
Q_{i} = T_{s_{i}}(x) \mod p
\end{equation}

3.3. Constrained Node Registration Phase

The constrained node CN\textsubscript{ij} submits registration information to gateway node GW\textsubscript{i} in this phase. The gateway node GW\textsubscript{i} verifies the constrained node CN\textsubscript{ij}'s legitimacy then issues private key S\textsubscript{ij} and certificate Cert\textsubscript{GW\textsubscript{i}→CN\textsubscript{ij}} to complete this phase. Note that the gateway node GW\textsubscript{i} computes private key S\textsubscript{ij} by constrained node CN\textsubscript{ij}'s registration information. Figure 4. illustrates process of constrained node registration phase. Detailed descriptions are stated as follows:

Figure 4. Constrained node registration phase of proposed scheme.

Step 1: Constrained node CN\textsubscript{ij} chooses an identifier ID\textsubscript{ij} and a random number s\textsubscript{ij} as his own secret, computes Q\textsubscript{ij}, and sends (ID\textsubscript{ij}, Q\textsubscript{ij}) to gateway node GW\textsubscript{i}. 
\[ Q_{ij} = T_{s_{ij}}(x) \mod p \] (4)

Step 2: Upon receiving \( ID_{ij} \) from constrained node \( CN_{ij} \), gateway node \( GW_i \) checks the format of \( ID_{ij} \). If \( ID_{ij} \) is valid, gateway node \( GW_i \) computes private key \( S_{ij} \) correspond to \( ID_{ij} \), generates \( Cert_{GW_i \rightarrow CN_{ij}} \), and sends \( (S_{ij}, Cert_{GW_i \rightarrow CN_{ij}}) \) to constrained node \( CN_{ij} \) via secure channel.

\[ P_{ij} = H_2(Q_{ij}, ID_i) \] (5)

\[ S_{ij} = S_i T_{s_i}(P_{ij}) \mod p \] (6)

Step 3: The constrained node \( CN_{ij} \) stores \( (S_{ij}, Cert_{GW_i \rightarrow CN_{ij}}) \) to complete the constrained node registration phase.

3.4. Mutual Authentication and Key Agreement Phase

After the constrained node joins the remote server node alliance as a remote server node member, it can use the services not only provided by the registered services provider but also other services provider in the same remote server node alliance. When the constrained node applies for remote server node services, the gateway node and constrained node will execute mutual authentication to ensure the further interaction between the gateway node and constrained node is secure and validated. Figure 5. illustrates process of mutual authentication and key agreement phase. Detailed descriptions are stated as follows:

- **Step 1** Constrained node \( CN_{ij} \) chooses a random number \( a_{ij} \), computes \( \mu_{ij} \) and \( C_t \), and sends \( (C_t, ID_{ij}) \) to gateway node \( GW_i \).

\[ \mu_{ij} = T_{s_{ij}}(a_{ij}) \mod p \] (7)

\[ C_t = (T_{\epsilon_i}(\mu_{ij}||a_{ij}||Cert_{GW_i \rightarrow CN_{ij}}) \mod p)P_t \] (8)

**Figure 5.** Mutual authentication and key agreement phase of proposed scheme.
Step 2: Upon receiving \((C_t, ID_{ij})\), gateway node \(GW_t\) obtains \((\mu_j||a_{ij}||Cert_{GW_t-CN_{ij}})\) by decrypting \(P_t\) and verifies \(Cert_{GW_t-CN_{ij}}\) is valid. If \(Cert_{GW_j-CN_{ij}}\) is valid, gateway node \(GW_t\) progresses to steps below, or gateway node \(GW_t\) abandons request.

\[
(\mu_j||a_{ij}||Cert_{GW_t-CN_{ij}} = ) (T_d(C_t) \text{ mod } p) / P_t
\]

Step 3: Gateway node \(GW_t\) computes \((\omega), sk_{GW_t-CN_{ij}}, P_t, P_{ij}, P_t, K, MAC_{GW_t}\) and sends \((MAC_{GW_t}, \omega)\) to the constrained node \(CN_{ij}\).

\[
\omega_j = T_{st}(a_{ij}) \text{ mod } p
\]

\[
sk_{GW_t-CN_{ij}} = H_3(T_{st}(\mu_j) \text{ mod } p)
\]

\[
P_t = H_2(ID_t)
\]

\[
P_{ij} = H_2(Q_{ij}, ID_t)
\]

\[
P_t = H_1(ID_t)
\]

\[
K = (P_t||Q_0) \bigoplus (P_{ij}||Q_{ij}) \bigoplus (P_t||Q_{ij}) \bigoplus (sk_{GW_t-CN_{ij}}||\omega_j)
\]

\[
MAC_{GW_t} = h_K(P_t, P_{ij}, \mu_j)
\]

Step 4: Upon receiving \((MAC_{GW_t}, \omega)\), constrained node \(CN_{ij}\) computes \((sk'_{GW_t-CN_{ij}}, K')\) and verifies \(MAC_{GW_t}\). If result of verification is true, constrained node \(CN_{ij}\) computes \(MAC_{CN_{ij}}\) and sends \(MAC_{CN_{ij}}\) to gateway node \(GW_t\).

\[
sk'_{GW_t-CN_{ij}} = H_3(T_{st}(\omega) \text{ mod } p)
\]

\[
K' = (P_t||Q_0) \bigoplus (P_{ij}||Q_{ij}) \bigoplus (P_t||Q_{ij}) \bigoplus (sk'_{GW_t-CN_{ij}}||\omega_j)
\]

\[
h_{K'}(P_t, P_{ij}, \mu_j) = MAC_{GW_t}
\]

\[
MAC_{CN_{ij}} = h_{sk'_{GW_t-CN_{ij}}}(P_{ij}, P_t, \omega_j)
\]

Step 5: Upon receiving \(MAC_{CN_{ij}}\), gateway node \(GW_t\) verifies \(MAC_{CN_{ij}}\). If the result of verification is true, mutual authentication and key agreement is completed.

\[
h_{sk_{GW_t-CN_{ij}}}(P_{ij}, P_t, \omega_j) = MAC_{CN_{ij}}
\]

3.5. Anonymous Identity Distribution Phase

If the constrained node needs an anonymous identity for some remote server node services, the gateway node will generate an anonymous identity and the corresponding private key for constrained node according to the registration information. Note that anonymous identity will compute by adding constrained node’s ID to ensure their connection. Figure 6. illustrates process of anonymous identity distribution phase. Detailed descriptions are stated as follows:

Step 1: Gateway node \(GW_t\) generates a random number \(t_i\), uses session key \(sk_{GW_t-CN_{ij}}\) to encrypt \(ID_{ij}\) and \(t_i\), and generates and sends pseudonym \(aID_{ij}\) to constrained node \(CN_{ij}\).

\[
aID_{ij} = E_{sk_{GW_t-CN_{ij}}}(ID_{ij}||t_i)
\]

Step 2: Upon receiving \(aID_{ij}\), constrained node \(CN_{ij}\) computes \(P_{aID_{ij}}\) and \(Q_{aID_{ij}}\) and sends \(Q_{aID_{ij}}\) to gateway node \(GW_t\).

\[
P_{aID_{ij}} = H_1(ID_{ij}||aID_{ij})
\]
\[ Q_{aID_j} = E_{sk_{GW_t-CN_{ij}}} (ID_t || aID_j) \]  

(24)

Figure 6. Anonymous identity distribution phase of proposed scheme.

Step 3: After receiving \( Q_{aID_j} \), gateway node \( GW_t \) decrypts \( Q_{aID_j} \) with \( sk_{GW_t-CN_{ij}} \) and checks \( P_{aID_j} \). If it holds, gateway node \( GW_t \) computes \( aS_{ij} \) and encrypts \( aS_{ij} \) with \( sk_{GW_t-CN_{ij}} \). Then, gateway node \( GW_t \) encrypts \( (C, P_t) \) to \( MAC'_{GW_t} \) and sends \( MAC'_{GW_t} \) to constrained node \( CN_{ij} \).

\[
(ID_t || aID_j) = D_{sk_{GW_t-CN_{ij}}} (Q_{aID_j})
\]  

(25)

\[
H_1(ID_t || aID_j) = P_{aID_j}
\]  

(26)

\[
aS_{ij} = S_t T_s(P_t) \mod p
\]  

(27)

\[
C = E_{sk_{GW_t-CN_{ij}}} (aS_{ij})
\]  

(28)

\[
MAC'_{GW_t} = E_{sk_{GW_t-CN_{ij}}} (C, P_t)
\]  

(29)

Step 4: Upon receiving \( MAC'_{GW_t} \), gateway node \( GW_t \) verifies \( MAC_{CN_{ij}} \). If result of verification is true, gateway node \( GW_t \) obtain \( aS_{ij} \) by decrypting \( C \), and anonymous identity distribution phase is completed.

\[
(C, P'_t) = D_{sk_{GW_t-CN_{ij}}} (MAC'_{GW_t})
\]  

(30)

\[
H_1(ID_t) = P'_t
\]  

(31)
\[ a_{Sij} = D_{sk_{GW_t \leftrightarrow CN_{ij}}} (C) \]  

### 3.6. Anonymous Signature and Verification Phase

Gateway node \( GW_t \) (verifier) receives and verifies message with signature generated by anonymous private key \( a_{Sij} \) using verification function. Figure 7 illustrates process of anonymous signature and verification phase. Detailed descriptions are stated as follows:

#### Step 1: Constrained node \( CN_{ij} \) (Signer)

1. Choose a random number \( R_y \in \mathbb{Z}_q^* \), computes \((W_{ij}, V_{ij}, t_{ij})\) for further computation.

\[ W_{ij} = T_{R_y}(x) \mod p \]  
\[ V_{ij} = H_1(W_{ij} || aID_{ij} || aS_{ij}) \]  
\[ t_{ij} = R_y V_{ij} \mod p \]

2. Choose a random number \( L_y \in \mathbb{Z}_p^* \) (\( L_{ij,g} \) is the \( g \)th bit of \( L_y \))

#### Step 2: Constrained node \( CN_{ij} \) (Signer)

3. \( O_y = \prod_{p=1}^{61} Q'_{g-1} \)

4. \( b_{ij} = H_1(Q, W_{ij}, M) \)

5. \( Y_{ij} = L_{ij} b_{ij} t_{ij} \mod p \)

6. \( \eta_{ij} = T_{Y_{ij}}(x) \mod p \)

7. \( \sigma_{ij} = (Q, W_{ij}, Y_{ij}) \)

#### Step 3: Gateway node \( GW_t \) (Verifier)

8. Upon receiving signature \( \sigma_{ij} \), gateway node \( GW_t \) verifies signature \( \sigma_{ij} \). If \( \eta'_{ij} \) holds, signature is accepted.

\[ \eta'_{ij} = O_y T_{b_{ij}}(W_{ij}) T_{b_{ij}v_{ij}}(aS_{ij}) \mod p \]
4. Security Analysis

We present formal verification using BAN logic [54] and theoretical analyses to prove that proposed scheme can achieve security properties and resist potential common attacks.

4.1. Formal Verification Using BAN Logic

BAN logic has become a widely accepted and well-known logical methodology for analyzing security of schemes [54–65]. The goal of BAN logic is to verify the exchanged information and the belief relationship among communicating parties and analyze protocols by deriving beliefs to proof that honest and legitimate parties can correctly execute and complete a protocol. We apply BAN logic [54] to prove the authenticity of our scheme. The notations used in BAN logic [54] analysis are defined as follows. P and Q are principles, X and Y are statements, C is channel, r and w are set of readers and writers respectively, and K is encryption key. P ⊨ X denotes that P believes X; P ⊨ ¬X denotes that P once said X. C(X) means that X is transited via channel C; r(C) and w(C) denotes as the set of readers and writers of C respectively. P ⊢ X means that P sees C(X). X is transited via C and can be observed by P, and P must be a reader of C to read X. P ⊢ X | C means that P sees X via C. (X)k denotes that X is encrypted with the key K. P ⊢X Q means that P and Q can establish a secure communication channel by using K. The logical postulates in BAN logic [54] are described using rules below.

Rule 1. \( P \equiv C(X) \) \( P \in r(C) \) \( P \in w(C) \): If P receives and reads X via C, then P believes that X has arrived on C and P sees X.

Rule 2. \( P \equiv (X, Y) \) \( P \in r(C, Y) \) : If P sees a hybrid message (X, Y), then P sees X and Y separately.

Rule 3. \( P \equiv (w(C) = (P, Q)) \): If P believes that C can only be written by P and Q, then P believes that if P receives X via C, then Q said X.

Rule 4. \( P \equiv (Q \sim (X, Y)) \) : If P believes that Q said a hybrid message (X, Y), then P believes that Q has said X and Y separately.

Rule 5. \( P \equiv (^\sim_s \langle \text{ECMDH(secret)} \rangle P, P \equiv ^\sim_s \langle \text{ECMDH(public)} \rangle Q) \): If P believes that \( s_{ij} \) is its extended chaotic maps-based Diffie–Hellman secret and that \( \omega_i \) is the extended chaotic maps-based Diffie–Hellman component from Q, then P believes that \( s_{GW_{ij} + CN_{ij}} \) is the symmetric key shared between P and Q.

Rule 6. \( P \equiv (Q \sim X), P \equiv #(X) \): If P believes that another Q said X and P also believes that X is fresh, then P believes that Q has recently said X.

Rule 7. \( P \equiv #(X) \) \( P \equiv \Phi_1 \) \( P \equiv \Phi_1 \): If P believes that a part of a mixed message X is fresh, then it believes that the whole message (X, Y) is fresh.

Rule 8. \( P \equiv (\Phi_1 \rightarrow \Phi_2), P \equiv \Phi_1 \) \( P \equiv \Phi_2 \): If P believes that \( \Phi_1 \) implies \( \Phi_2 \) and P believes that \( \Phi_1 \) is true, then P believes that \( \Phi_2 \) is true.

The proposed scheme is described in logic as below.

Step 1. \( GW_{i} < (^\sim_s \langle \text{ECMDH(public)} \rangle CN_{ij}, C_{GW_{ij}, CN_{ij}}((P_{ij}, P_{ij}, \omega_{ij})_{k})) \)

Step 2. \( CN_{ij} < (^\sim_s \langle \text{ECMDH(public)} \rangle GW_{ij}, C_{CN_{ij}}(C_{GW_{ij}, CN_{ij}}(P_{ij}, P_{ij}, \omega_{ij})))_{k}) \)

Table 2 lists used assumptions, where A and B are CN_{ij} and GW_{ij}, but A ≠ B.

| Assumptions | Definitions |
|-------------|-------------|
| A1. \( A \in r(C_{A, B}) \) | A can read from the channel \( C_{A, B} \). |
| A2. \( A \equiv (w(C_{A, B}) = \{A, B\}) \) | A believes that A and B can write on \( C_{A, B} \). |
| A3. \( A \equiv (B \sim \Phi \rightarrow \Phi) \) | A believes that B only says what it believes. |
| A4. \( A \equiv #(N_{A}) \) | A believes that \( N_{A} \) is fresh. |
| A5. \( A \equiv ^\sim_s \langle \text{ECMDH(secret)} \rangle A \) | A believes that \( s_{ij} \) is its extended chaotic maps-based Diffie–Hellman secret. |
Based on the assumptions and logical analyses, the proposed scheme must realize goals in Table 3.

Table 3. Goals of the proposed scheme.

| Goals | Definitions |
|-------|-------------|
| G1. CN\textsubscript{ij} | Constrained node CN\textsubscript{ij} believes that \( s_k_{GW_{i+CN_{ij}}} = H_3(T_{\mu} mod p) \) is a symmetric key shared between participants CN\textsubscript{ij} and GW\textsubscript{i}. |
| G2. GW\textsubscript{i} | Gateway node GW\textsubscript{i} believes that \( s_k_{GW_{i+CN_{ij}}} = H_3(T_{\mu} mod p) \) is a symmetric key shared between participants CN\textsubscript{ij} and GW\textsubscript{i}. |
| G3. CN\textsubscript{ij} | Constrained node CN\textsubscript{ij} believes that \( S_i \) is convinced of \( s_k_{GW_{i+CN_{ij}}} = H_3(T_{\mu} mod p) \). |
| G4. GW\textsubscript{i} | Gateway node GW\textsubscript{i} believes that \( U \) is convinced of \( s_k_{GW_{i+CN_{ij}}} = H_3(T_{\mu} mod p) \). |

To accomplish the Goal 1, we have Equations (42) and (43). Equations (42) and (43) must hold because of Rule 5 and A5.\[ CN_{ij} \equiv (\rightarrow_{ECMDH(secret)} CN_{ij}) \tag{42} \]
\[ CN_{ij} \equiv (\rightarrow_{ECMDH(public)} GW_i) \tag{43} \]

Next, we have Equations (44) and (45) which must hold because of A3 and Rule 8 to accomplish Equation (43).
\[ CN_{ij} \equiv (\rightarrow_{ECMDH(public)} GW_i, C_{CN_{ij}}, GW_i(P_{ij}, P_t, \omega_t, s_k_{GW_{i+CN_{ij}}}, \omega_t) \rightarrow (\rightarrow_{ECMDH(public)} GW_i)) \tag{44} \]
\[ CN_{ij} \equiv (GW_i \sim \omega_{ij} \rightarrow_{ECMDH(public)} GW_i) \tag{45} \]

We have Equation (46) which must hold because of Rule 6 and 7 and A4 to accomplish Equation (45).
\[ CN_{ij} \equiv \#(\rightarrow_{ECMDH(public)} GW_i) \tag{46} \]

We have Equations (47)–(49) which must hold because of Rule 1, 2, and 3, and A1 and A2 to accomplish Equation (46).
\[ CN_{ij} \in r(C_{GW_i}, CN_{ij}) \tag{47} \]
\[ CN_{ij} \equiv (w(C_{GW_i}, CN_{ij}) \equiv \{CN_{ij} \setminus GW_i\}) \tag{48} \]
\[ CN_{ij} \equiv \omega_i \rightarrow_{ECMDH(public)} GW_i \tag{49} \]

We have the proposed scheme realizes that G1 is achieved by using Rule 5. Similarly, we have that the proposed scheme realizes G2 by using the same arguments of G1.

We have Equations (50) and (51) which must hold because of Rule 3 and A3 to accomplish G3.
\[ CN_{ij} \equiv (GW_i \sim (CN_{ij} \leftrightarrow GW_i) \rightarrow GW_i) \equiv (CN_{ij} \leftrightarrow GW_i) \tag{50} \]
\[ CN_{ij} \equiv (GW_i \sim (CN_{ij} \leftrightarrow GW_i)) \tag{51} \]

We have Equations (51) and (52) which must hold because of Rule 6 and 7 and A4 to accomplish Equation (51).
\[ CN_{ij} \equiv \#(CN_{ij} \leftrightarrow GW_i) \tag{52} \]
We have Equations (47), (48), and (53) which must hold because of Rule 1, 2, and 3, and A1 and A2 to accomplish Equation (53).

\[
CN_{ij} \leftrightarrow_{CN_{ij}, GW_i} (CN_{ij} \leftrightarrow GW_i)
\]  

(53)

Thus, the proposed scheme realizes G3 is achieved. Similarly, using the same arguments of G3, the proposed scheme realizes G4. Therefore, the proposed scheme realizes G1, G2, G3, and G4.

4.2. Theoretical Analyses

We present theoretical analyses to prove that proposed scheme can achieve security properties and resist potential common attacks.

4.2.1. Security of Secret Key

We assume that adversary wants to get the master secret key obtained by remote server node, gateway node GW_i and constrained node CN_{ij}, such like Q_i = T_{s_0}(x) \bmod p and Q_i = T_{s_i}(x) \bmod p. The adversary must have to solve the question based on CMDLP. If an adversary wants to get the gateway node GW_i’s secret key by compute S_i = T_{s_i}(P_i) \bmod p = T_{s_0}(H_1(ID_i)) \bmod p, adversary needs to solve the question based on CMDLP. On the other hand, the gateway node GW_i generates the secret key for the constrained node CN_{ij}, by performing S_{ij} = S_i T_{s_i}(P_{ij}) \bmod p = T_{s_0}(H_1(ID_i)) T_{s_i}(H_2(Q_{ij}, ID_i)) \bmod p. The gateway node GW_i use private key S_i and its own secret s_i in the computing process, hence only gateway node GW_i can know the constrained node CN_{ij}’s secret key.

4.2.2. Session Key Confirmation and Security of Session Key

We provide session key confirmation which can guarantee the correctness of the encryption key in the session through message authentication code MAC_{GW_i} and MAC_{CN_{ij}}. If the adversary wants to obtain a session key sk_{GW_i++CN_{ij}}, the adversary has to solve CMDHP even with knowledge of \omega_i. Moreover, session key sk_{GW_i++CN_{ij}} is not the same every time because of random number a_{ij}.

4.2.3. Mutual Authentication

In the authentication process, constrained node CN_{ij} and gateway node GW_i compute their session key K by public parameters (ID_i, ID_{ij}, Q_{ij}, X, ID_f, Y). In addition, each party generates message authentication code MAC_{GW_i} and MAC_{CN_{ij}} by K and sk_{GW_i++CN_{ij}} respectively to verify their validity. Moreover, because the feature of HIDC, gateway node GW_i can realize constrained node CN_{ij} comes from which cloud services provider by public parameter ID_{ij}.

4.2.4. Device Anonymity

After mutual authentication phase, constrained node CN_{ij} can obtain pseudonym private key aS_{ij} corresponding to pseudonym identity alID_{ij} from supplier gateway node GW_i. The pseudonym identity alID_{ij} involve not only constrained node CN_{ij}’s ID_{ij} but also time stamp t_s, that is to ensure every time the constrained node can obtain different pseudonym identity to avoid attack by remove the linkage between the real identity and pseudonym identity. Besides, alID_{ij} is computed by a supplier with its own secret. That is, only the supplier who gave alID_{ij} to the constrained node CN_{ij} can recover the constrained node’s real identity.

4.2.5. Traceability of Anonymity

Server node S can audit transmission history by recovering anonymous ID alID_{ij}. The gateway node GW_i decrypts alID_{ij} with secret s_i to recover anonymous real identity by performing (ID_{ij}||t_1) = D_{sk_{GW_i++CN_{ij}}}(alID_{ij}).
4.2.6. Unforgeability

If the adversary wants to forge validated anonymous identity, adversary has to acquire gateway node $GW_i$’s secret $s_i$ and private key $S_i$. The adversary has to solve CMDLP if adversary wants to compute gateway node $GW_i$’s secret $s_i$ and private key $S_i$ from public parameter $Q_i$.

4.2.7. Without Assistance of Registration Center

Ying and Nayak [4] and Ul Haq et al. [5] proposed scheme for multi-server 5G networks which included a registration center (RC) in their system structures. RC is a third party for both sides of communication, and two parties have to go through registration phase to RC before communication. Privilege attack or malicious insider attack may occur if the adversary is in RC, and risk of message leakage may happen. If privilege attack or malicious insider attack happen in telemedicine system, patience privacy may be damaged. Moreover, system structure including RC in 5G networks is no difference from the one in conventional networks. In proposed scheme, we introduced hierarchical system structure which is suitable for 5G networks without RC or trusted third party.

4.2.8. Non-Repudiation and Security of Signature

When constrained node $CN_{ij}$ executes signature function based on Chebyshev chaotic maps with anonymous private key $aS_{ij}$ to generate signature $\sigma_{ij}$. Gateway node $GW_t$ can verify $\eta_{ij}$. As the result, non-repudiation can be achieved. We apply signature Meshram et al.’s ID-based online short signature scheme [45] in anonymous signature and verification phase, and security of signature has been proven using Bellar et al.’s method [69].

4.2.9. Resistant to Bergamo et al.’s Attack

Bergamo et al.’s attack [70] is based on two conditions: Attackers can obtain related elements $(x, a_{ij}, \mu_{ij}, \omega_t)$ or several Chebyshev polynomials pass through the same point due to the periodicity of cosine function. In the authenticated key exchange phase of the proposed scheme, attackers cannot obtain any of the related elements $(x, a_{ij}, \mu_{ij}, \omega_t)$ because they are encrypted in transmitted messages and only the user and server can retrieve the decryption key. Moreover, the proposed protocol utilizes the extended Chebyshev polynomials, in which the periodicity of the cosine function is avoided by extending the interval of $x$ to $(-\infty, +\infty)$ [40]. As a result, our scheme can resist the attack proposed by Bergamo et al. [70].

5. Performance Analysis

We present comparisons of Yan et al.’s [30], Hu et al.’s [71], Ying and Nayak’s [4], Ul Haq et al.’s [5], and proposed schemes concerning security requirements and computational complexity comparison.

5.1. Security Requirements Comparison

As shown in Table 4, proposed scheme provides all listed security requirements. Yan et al.’s [30] and Hu et al.’s [71], and proposed schemes utilize hierarchical system structure. Yan et al.’s [30] and Ying and Nayak’s [4] only achieve one security requirement. Hu et al.’s [71] scheme achieves mutual authentication and anonymity, and Ul Haq et al.’s [5] scheme achieves mutual authentication, session key confirmation, and anonymity. None of mentioned previous schemes achieve traceability of anonymity, unforgeability, and non-repudiation except proposed scheme.

5.2. Computational Complexity Comparison

We present a computational complexity comparison of our scheme with Yan et al.’s [30], Hu et al.’s [71], Ying and Nayak’s [4], and Ul Haq et al.’s [5] schemes in Table 5. We can ignore the time taken for computing XOR operation because the value is too low to influence the result. Hu et al.’s [71], Ying and Nayak’s [4], and Ul Haq et al.’s [5] schemes take more
computational cost than Yan et al.’s [30] and ours. Hu et al.’s scheme [71] takes the most computational cost, and the reason may be that Hu et al.’s scheme [71] is the only scheme which performs exponentiation operations among them. Ying and Nayak’s [4] and Ul Haq et al.’s [5] schemes take more computational cost than Yan et al.’s [30] and ours because Ying and Nayak’s [4] and Ul Haq et al.’s [5] schemes perform more not only one-way hash function operations but elliptic curve point multiplications. The results have proven that performing an elliptic curve point multiplication takes more time than a Chebyshev chaotic maps operation, and, compared to RSA and ECC, Chebyshev polynomials can offer smaller key size and faster computation [42,43,72–74]. However, Yan et al.’s scheme [30] performs only two elliptic curve point multiplications in total while our scheme performs six Chebyshev chaotic maps operations. For the above reason, Yan et al.’s scheme [30] takes less time than our scheme. Although Yan et al.’s scheme [30] is more efficient than our scheme by a narrow margin, Yan et al.’s scheme [30] cannot provide key confirmation because of lacking session key agreement, and neither can Ying and Nayak’s scheme [4]. Moreover, Yan et al.’s scheme [30] cannot provide mutual authentication, anonymity, traceability of anonymity, unforgeability, and non-repudiation. Figure 8. illustrates computational complexity of receiver/gateway node with varying number of devices.

| Security Requirements       | Yan et al. [30] | Hu et al. [71] | Ying and Nayak [4] | Ul Haq et al. [5] | Ours |
|-----------------------------|-----------------|----------------|--------------------|-------------------|-----|
| Mutual authentication       | X               | O              | X                  | O                 | O   |
| Session key confirmation    | X               | X              | X                  | O                 | O   |
| Anonymity                   | O               | O              | X                  | X                 | O   |
| Traceability of anonymity   | O               | X              | X                  | X                 | O   |
| Unforgeability              | O               | O              | O                  | O                 | O   |
| Non-repudiation             | O               | X              | O                  | O                 | O   |
| Without RC                  | O               | X              | X                  | X                 | O   |

Table 4. Security requirements comparison.

| Scheme                      | Yan et al. [30] | Hu et al. [71] | Ying and Nayak [4] | Ul Haq et al. [5] | Ours |
|-----------------------------|-----------------|----------------|--------------------|-------------------|-----|
| Sender/constrained node     | $2T_h + T_{ecc}$ | $2T_e + T_{ecc}$ | $8T_h + 5T_{ecc}$ | $6T_h + 5T_{ecc}$ | $3T_{ch} + 3T_h$ |
|                            | = 128.18$T_h$   | = 2214.16$T_h$ | = 638.8$T_h$      | = 636.8$T_h$      | = 129.12$T_h$ |
| Receiver/gateway note       | $2T_h + T_{ecc}$ | $2T_{ecc}$ | $4T_h + 5T_{ecc}$ | $4T_h + 5T_{ecc}$ | $3T_{ch} + 6T_h$ |
|                            | = 128.18$T_h$   | = 252.32$T_h$  | = 634.8$T_h$      | = 634.8$T_h$      | = 132.12$T_h$ |
|                            | $4T_h + 2T_{ecc}$ | $2T_e + 3T_{ecc}$ | $12T_h + 10T_{ecc}$ | $10T_h + 10T_{ecc}$ | $6T_{ch} + 9T_h$ |
|                            | = 256.36$T_h$  | = 2466.48$T_h$ | = 1273.6$T_h$     | = 1271.6$T_h$     | = 261.24$T_h$ |

Table 5. Computational complexity comparison.

$T_{ch}$: Time for performing a Chebyshev chaotic maps operation; $T_{ecc}$: Time for performing an elliptic curve point multiplication; $T_{sym}$: Time for performing a symmetry encryption operation; $T_e$: Time for performing an exponentiation operation; $T_h$: Time for performing a one-way hash function operation; $T_{ch} = 42.04T_h$; $T_{ecc} = 126.16T_h$; $T_{sym} = 17.4T_h$; $T_e = 1044T_h$; $T_h = 0.006$ ms.
6. Conclusions

5G networks has an efficient effect in energy consumption and provides quality of experience and amount of devices communication, and 5G will change connected services and devices through higher reliability, connectivity, and cloud storage. IoT applying 5G infrastructure changes application scenario in many fields especially real-time communication between machines, data, and people. IoT with 5G environment provides solutions of network layer, including enhancing quality of service, router and jamming control, and resource optimization, to solve challenges of smart medical healthcare. Medical privacy is important in smart medical healthcare because data leaking brings potential harm to patients and hospital. We propose a FAIDM for medical privacy protection in 5G telemedicine systems which provides federated identity management which provide a secure way to protect medical privacy. To achieve privacy preservation, we provide anonymous identity to constrained nodes for reducing exposure of personal private data. Our scheme provides features below. (i) Proposed scheme provides federated identity management which can manage identity of devices in a hierarchical structure efficiently. (ii) Identity authentication will be achieved by mutual authentication between devices and SBSs/MBSs. (iii) The proposed scheme provides session key to secure transmitted data which is related to privacy of patients. (iv) The proposed scheme provides anonymous identities for devices in order to reduce the possibility of leaking transmitted medical data and real information of device and its owner. (v) If one of devices transmit abnormal data, the proposed scheme provides traceability of anonymous identities for servers of medical institute to check specific device. (vi) the proposed scheme provides anonymous signature for non-repudiation of devices, and records of signatures can be used for periodical audit of medical institute.

Author Contributions: Conceptualization, C.-L.H. and T.-W.L.; methodology, C.-L.H. and T.-W.L.; security analysis, T.-W.L.; writing—original draft preparation, T.-W.L.; writing—review and editing, T.-W.L.; supervision, C.-L.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministry of Science and Technology, Taiwan, grant number MOST 108-2221-E-182-011, Healthy Aging Research Center, Chang Gung University, Taiwan, grant number EMRPD1K0461 and EMRPD1K0481, and Chang Gung University, Taiwan, grant number PARPD3K0011.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This study did not report any data.
Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahad, A.; Tahir, M.; Yau, K.L.A. 5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions. IEEE Access 2019, 7, 100747–100762. [CrossRef]
2. Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems. IEEE Internet Things J. 2020, 7, 16–32. [CrossRef]
3. Kakkar, A. A survey on secure communication techniques for 5G wireless heterogeneous networks. Inf. Fusion 2020, 62, 89–109. [CrossRef]
4. Ying, B.; Nayak, A. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. J. Netw. Comput. Appl. 2019, 131, 66–74. [CrossRef]
5. Haq, I.U.; Wang, J.; Zhu, Y. Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. J. Netw. Comput. Appl. 2020, 161, 102660. [CrossRef]
6. Anwar, S.; Prasad, R. Framework for Future Telemedicine Planning and Infrastructure using 5G Technology. Wirel. Pers. Commun. 2018, 100, 193–208. [CrossRef]
7. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. 2020, 135. [CrossRef]
8. Rao, K. The Path to 5G for Health Care. IEEE Future Netw. 2018. Available online: https://futurenetworks.ieee.org/images/files/pdf/applications/5G--Health-Care030518.pdf (accessed on 20 July 2020).
9. World Health Statistics 2017: Monitoring Health for the SDGs (Sustainable Development Goals); World Health Organization: Geneva, Switzerland, 2017.
10. Lloret, J.; Parra, L.; Taha, M.; Tomás, J. An architecture and protocol for smart continuous eHealth monitoring using 5G. Comput. Netw. 2017, 129, 340–351. [CrossRef]
11. Chen, M.; Yang, J.; Zhou, J.; Hao, Y.; Zhang, J.; Youn, C.H. 5G-Smart Diabetes: Toward Personalized Diabetes Diagnosis with Healthcare Big Data Clouds. IEEE Commun. Mag. 2018, 56, 16–23. [CrossRef]
12. Fan, K.; Jiang, W.; Li, H.; Yang, Y. Lightweight RFID Protocol for Medical Privacy Protection in IoT. IEEE Trans. Ind. Inform. 2018, 14, 1656–1665. [CrossRef]
13. Murugan, A.; Chechare, T.; Muruganathan, B.; Ganesh Kumar, S. Healthcare information exchange using blockchain technology. Int. J. Electr. Comput. Eng. 2020, 10, 421–426. [CrossRef]
14. Lin, W.-Y.; Zhang, X.; Song, H.; Omori, K. Health information seeking in the Web 2.0 age: Trust in social media, uncertainty reduction, and self-disclosure. Comput. Hum. Behav. 2016, 56, 289–294. [CrossRef]
15. Park, Y.J.; Chung, J.E.; Shin, D.H. The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. Am. Behav. Sci. 2018, 62, 1319–1337. [CrossRef]
16. Lupton, D. The thing-power of the human-app health assemblage: Thinking with vital materialism. Soc. Theory Health 2019, 17, 125–139. [CrossRef]
17. Libert, T. Privacy implications of health information seeking on the web. Commun. ACM 2015, 58, 68–77. [CrossRef]
18. Gandy, O.H., Jr.; Nemorin, S. Toward a political economy of nudge: Smart city variations. Int. J. Adv. Comput. Sci. Technol., A. Revolutionizing healthcare with IoT and cognitive, cloud-based telemedicine. Acta Polytech. Hung. 2019, 16, 163–181. [CrossRef]
19. Park, Y.J.; Shin, D.D. Contextualizing privacy on health-related use of information technology. Comput. Hum. Behav. 2020, 105, 106204. [CrossRef]
20. Marciniak, R. Role of new IT solutions in the future of shared service model. Pollack Period. 2013, 8, 187–194. [CrossRef]
21. Garai, Á.; Péntek, I.; Adamkó, A. Revolutionizing healthcare with IoT and cognitive, cloud-based telemedicine. Acta Polytech. Hung. 2019, 16, 163–181. [CrossRef]
22. Zriqat, E.; Altamimi, A.M. Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. Int. J. Adv. Comput. Sci. Appl. 2016, 7, 229–236.
23. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. In United States Statutes at Large; Office of the Federal Register: Washington, DC, USA, 1996; Volume 110, pp. 1936–2103.
24. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation): 2012/0011 (COD); Council of the European Union: Brussels, Belgium, 2013.
25. Pramanik, P.K.D.; Pareek, G.; Nayar, A. Security and privacy in remote healthcare: Issues, solutions, and standards. In Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare; Elsevier: Amsterdam, The Netherlands, 2019; pp. 201–225. [CrossRef]
26. Devaraj, S.J. Emerging paradigms in transform-based medical image compression for telemedicine environment. In Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare; Elsevier: Amsterdam, The Netherlands, 2019; pp. 15–29. [CrossRef]
27. The European Union Agency for Cybersecurity. ICT Security Certification Opportunities in the Healthcare Sector; European Union Agency For Network and Information Security: Attiki, Greece, 2019.
28. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 1985; Volume 196, pp. 47–53.
29. Gentry, C.; Silverberg, A. Hierarchical id-based cryptography. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2002; Volume 2501, pp. 548–566.
30. Yan, L.; Rong, C.; Zhao, G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2009; Volume 5931, pp. 167–177.
31. Park, Y.; Sur, C.; Rhee, K.-H. A Privacy-Preserving Location Assurance Protocol for Location-Aware Services in VANETs. Wirel. Pers. Commun. 2011, 61, 779–791. [CrossRef]
32. Shen, V.R.L.; Huang, W.C. A Time-Bound and Hierarchical Key Management Scheme for Secure Multicast Systems. Wirel. Pers. Commun. 2015, 85, 1741–1764. [CrossRef]
33. Fremantle, P.; Aziz, B. Cloud-based federated identity for the Internet of Things. Ann. Des Telecommun. Ann. Telecommun. 2018, 73, 415–427. [CrossRef]
34. Santos, M.L.B.A.; Carneiro, J.C.; Franco, A.M.R.; Teixeira, F.A.; Henriques, M.A.A.; Oliveira, L.B. FLAT: Federated lightweight authentication for the Internet of Things. Ad Hoc Netw. 2020, 107. [CrossRef]
35. Mishkovski, I.; Kocarev, L. Chaos-Based Public-Key Cryptography. In Chaos-Based Cryptography: Theory, Algorithms and Applications; Kocarev, L., Lian, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 27–65. [CrossRef]
36. Yoon, E.J.; Jeon, I.S. An Efficient and Secure Diffie–Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map. Commun. Nonlinear Sci. Numer. Simul. 2011, 16, 2383–2389. [CrossRef]
37. Yoon, E.J.; Yoo, K.Y. Cryptanalysis of Group Key Agreement Protocol Based on Chaotic Hash Function. Ieice Trans. Inf. Syst. 2011, 94, 2167–2170. [CrossRef]
38. Broumandnia, A. Image encryption algorithm based on the finite fields in chaotic maps. J. Inf. Secur. Appl. 2020, 54. [CrossRef]
39. Musanna, F.; Kumar, S. Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quantum Inf. Process. 2020, 19. [CrossRef]
40. Zhang, L. Cryptanlysis of the Public Key Encryption Based on Multiple Chaotic Systems. ChaosSolitons Fractals 2008, 37, 669–674. [CrossRef]
41. Chain, K.; Kuo, W.-C. A new digital signature scheme based on chaotic maps. Nonlinear Dyn. 2013, 74, 1003–1012. [CrossRef]
42. Tahat, N.; Hijazi, M.S. A new digital signature scheme based on chaotic maps and quadratic residue problems. Appl. Math. Inf. Sci. 2019, 13, 115–120. [CrossRef]
43. Tahat, N.; Alomari, A.K.; Al-Freedi, A.; Al-Hazimeh, O.M.; Al-Jamal, M.F. An Efficient Identity-Based Cryptographic Model for Chebyshev Chaotic Map and Integer Factoring Based Cryptosystem. J. Appl. Secur. Res. 2019, 14, 257–269. [CrossRef]
44. Tahat, N.; Tahat, A.A.; Albadarneh, R.B.; Edwan, T.A. Design of identity-based blind signature scheme upon chaotic maps. Int. J. Online Biomed. Eng. 2020, 16, 104–118. [CrossRef]
45. Meshram, C.; Li, C.T.; Meshram, S.G. An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput. 2019, 23, 747–753. [CrossRef]
46. Meshram, C.; Lee, C.; Meshram, S.G.; Meshram, A. OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network. IEEE Access 2020, 8, 80063–80073. [CrossRef]
47. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects. In Security Architecture and Procedures for 5G System; (Release 17); The 3rd Generation Partnership Project (3GPP): Sophia Antipolis CEDEX, France, 2020.
48. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects. In System Architecture for the 5G System (5GS); Stage 2 (Release 16); The 3rd Generation Partnership Project (3GPP): Sophia Antipolis CEDEX, France, 2020.
49. National Health Service Business Services Authority. Available online: https://www.nhsbsa.nhs.uk/exemption-certificates (accessed on 8 September 2020).
50. European Commission. European Interoperability Certificate Governance: A Security Architecture for Contact Tracing and Warning Apps, 1st ed.; European Commission: Brussels, Belgium, 2020.
51. American Hospital Association Certification Center. Available online: https://www.aha.org/career-resources/certification-center (accessed on 8 September 2020).
52. Pharmaceuticals and Medical Devices Agency. Available online: https://www.pmda.go.jp/english/ (accessed on 8 September 2020).
53. Healthcare Certification Authority. Available online: https://hca.nat.gov.tw/Default.aspx (accessed on 8 September 2020).
54. Burrows, M.; Abadi, M.; Needham, R. A logic of Authentication. ACM Trans. Comput. Syst. (TOCSI) 1990, 8, 18–36. [CrossRef]
55. Ali, R.; Pal, A.K.; Kumari, S.; Karuppiah, M.; Conti, M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Gener. Comput. Syst. 2018, 84, 200–215. [CrossRef]
56. Barman, S.; Das, A.K.; Samanta, D.; Chattopadhyay, S.; Rodrigues, J.J.P.C.; Park, Y. Provably Secure Multi-Server Authentication Protocol Using Fuzzy Commitment. IEEE Access 2018, 6, 38578–38594. [CrossRef]
57. Challa, S.; Das, A.K.; Odulu, V.; Kumar, N.; Kumari, S.; Khan, M.K.; Vasilakos, A.V. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Comput. Electr. Eng. 2018, 69, 534–554. [CrossRef]
58. Chatterjee, S.; Roy, S.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Vasilakos, A.V. Secure Biometric-Based Authentication Scheme Using Chebyshev Chaotic Map for Multi-Server Environment. *IEEE Trans. Dependable Secur. Comput.* 2018, 15, 824–839. [CrossRef]
59. Dodangeh, P.; Jahangir, A.H. A biometric security scheme for wireless body area networks. *J. Inf. Secur. Appl.* 2018, 41, 62–74. [CrossRef]
60. Li, C.T.; Lee, C.C.; Weng, C.Y. Security and efficiency enhancement of robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks. *J. Inf. Sci. Eng.* 2018, 34, 155–170. [CrossRef]
61. Liu, X.; Li, Y.; Qu, J.; Lu, L. EL-AKA: Energy-Efficient and Lightweight Multi-Server Authentication and Key Agreement Protocol Based on Dynamic Biometrics. *Wirel. Pers. Commun.* 2018, 100, 767–785. [CrossRef]
62. Sahoo, S.S.; Mohanty, S.; Majhi, B. An Improved and Secure Two-factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment. *Wirel. Pers. Commun.* 2018, 101, 1307–1333. [CrossRef]
63. Sharma, V.; You, I.; Leu, F.Y.; Atiquzzaman, M. Secure and efficient protocol for fast handover in 5G mobile Xhaul networks. *J. Netw. Comput. Appl.* 2018, 102, 38–57. [CrossRef]
64. Sutrala, A.K.; Das, A.K.; Kumar, N.; Reddy, A.G.; Vasilakos, A.V.; Rodrigues, J.J.P.C. On the design of secure user authenticated key management scheme for multigateway-based wireless sensor networks using ECC. *Int. J. Commun. Syst.* 2018, 31. [CrossRef]
65. Tan, Z. Secure Delegation-Based Authentication for Telecare Medicine Information Systems. *IEEE Access* 2018, 6, 26091–26110. [CrossRef]
66. Mandal, S.; Mohanty, S.; Majhi, B. Cryptanalysis and Enhancement of an Anonymous Self-Certified Key Exchange Protocol. *Wirel. Pers. Commun.* 2018, 99, 863–891. [CrossRef]
67. Qiu, Y.; Ma, M. Secure Group Mobility Support for 6LoWPAN Networks. *IEEE Internet Things J.* 2018, 5, 1131–1141. [CrossRef]
68. Xu, G.; Qu, S.; Ahmad, H.; Xu, G.; Guo, Y.; Zhang, M.; Xu, H. A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography. *Sensors* 2018, 18, 2394. [CrossRef]
69. Bellare, M.; Namprempre, C.; Neven, G. Security proofs for identity-based identification and signature schemes. *J. Cryptol.* 2009, 22, 1–61. [CrossRef]
70. Bergamo, P.; D’Arco, P.; de Santis, A.; Kocarev, L. Security of Public-key Cryptosystems Based on Chebyshev Polynomials. *IEEE Trans. Circuits Syst. I Regul. Pap.* 2005, 52, 1382–1393. [CrossRef]
71. Hu, C.; Liu, P.; Guo, S.; Xu, Q. Anonymous hierarchical identity-based encryption with bounded leakage resilience and its application. *Int. J. High Perform. Comput. Netw.* 2017, 10, 226–239. [CrossRef]
72. Zhu, H. Secure chaotic maps-based group key agreement scheme with privacy preserving. *Int. J. Netw. Secur.* 2016, 18, 1001–1009.
73. Lin, T.W.; Hsu, C.L. Anonymous group key agreement protocol for multi-server and mobile environments based on Chebyshev chaotic maps. *J. Supercomput.* 2018, 74, 4521–4541. [CrossRef]
74. Guo, X.; Sun, D.; Yang, Y. An Improved Three-Factor Session Initiation Protocol Using Chebyshev Chaotic Map. *IEEE Access* 2020, 8, 111265–111277. [CrossRef]