IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 9, 2021, accepted March 29, 2021, date of publication April 2, 2021, date of current version April 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3070641

An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments

TUAN-VINH LE[1], AND CHIEN-LUNG HSU[1,2,3,4,5], (Member, IEEE)
[1]Graduate Institute of Business and Management, Chang Gung University, Taoyuan 33302, Taiwan
[2]Department of Information Management, Chang Gung University, Taoyuan 33302, Taiwan
[3]Healthy Aging Research Center, Chang Gung University, Taoyuan 33302, Taiwan
[4]Department of Visual Communication Design, Ming Chi University of Technology, New Taipei 24301, Taiwan
[5]Department of Nursing, Taoyuan Chang Gung Memorial Hospital, Taoyuan 33044, Taiwan

Corresponding author: Chien-Lung Hsu (clhsu@mail.cgu.edu.tw)

This work was supported in part by the Chang Gung Memorial Hospital under Grant CMRPG5D0183 and Grant CMRPD3D0063; in part by the Ministry of Science and Technology in Taiwan under Grant MOST-105-2923-E-182-001-MY3, Grant MOST-107-2221-E-182-006, and Grant MOST-108-2221-E-182-011; in part by the Healthy Aging Research Center, Chang Gung University from the Featured Areas Research Center Program within the Framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan under Grant EMRPD1I0481, Grant EMRPD1H0421, Grant EMRPD1H0551, Grant EMRPD1K0461, and Grant EMRPD1K0481; and in part by the Ministry of Health and Welfare in Taiwan under Grant I1090604.

ABSTRACT Fifth generation (5G) mobile technology enables a new kind of network that provides high peak data rates, ultra-low latency communication and high user density. Electronic healthcare (e-health) allows the data to be stored and shared in a highly efficient and flexible manner. Group e-health services help in improving long-term results of the treatments due to its collaborative characteristic. The services including real-time remote patient monitoring and transmission of large health data files can be facilitated by e-health systems enabled with the 5G network. Since the communication channel is open, security and privacy in the system should be taken into account. Our work proposes a key distribution scheme for group healthcare services in 5G network environments. We construct various healthcare domains and apply the proposed scheme to the group services. The paper also introduces Single Sign-On (SSO), a cost-efficient solution, for multi-server architecture of the constructed system. Security and privacy of the scheme are enforced by a three-factor authentication mechanism (integrating smart card, password and biometrics) and strong user anonymity property. We provide security proof of the proposed scheme using various well-known tools including RoR model, BAN logic and AVISPA simulation. Results of various performance comparisons indicate that our scheme provides most functions and bears rational costs, compared with its related works.

INDEX TERMS 5G, group key distribution, e-health, privacy, SSO, three-factor authentication.

I. INTRODUCTION

Along with Internet of Things (IoT), Fifth Generation (5G) wireless technology is essential to various digitized applications. 5G technology provides high peak data rates with ultra-low latency and massive network capacity [1]. For obtaining such advances, unlike the previous generations (e.g., 4G), 5G is composed of two-tier heterogeneous cellular networks (HetNets) with integrated access and backhaul (IAB) [2]. Specifically, the network architecture is designed with macro base stations (MBSs) and small cell base stations (SBSs). Therein, the MBSs provide millimeters waves backhaul to the SBSs for extending the networks. The devices can access both MBSs and SBSs through directional transmissions [2], [3]. Moreover, 5G technology also supports device-to-device (D2D) communication in which mobile devices can communicate directly with each other to share radio access connection or exchange information [4]. There are various D2D communication topologies based on specific link establishments [5], [6]. At present, 5G applications have been introduced in various fields, such as energy [7]–[9], intelligent station area recognition technology [10], smart car parking system [11], healthcare [12], [13], etc.

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. InÁcio.

A. 5G WITH E-HEALTH SYSTEMS AND GROUP SERVICES

Electronic healthcare (e-health) has gained much attention since it allows health data to be flexibly stored and shared among multiple entities [14]. E-health systems enabled with

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

5G networks are able to support diverse applications with high reliability, information security, and seamless medical data transfer. Prominent uses cases include real-time remote monitoring for telemedicine, and transmission of large health data files. Since 5G provides the ultra-low latency, healthcare providers can monitor patients remotely and gather real-time data efficiently, without the worry of network blackouts, disconnections or lag time [15], [16]. It facilitates preventative care and other individually tailored healthcare provisions. Due to the high peak data rates supported by 5G, large data files in the systems can be efficiently transmitted between the users and providers for efficient patient treatments. For example, large image files created by Computerized Tomography (CT) or Magnetic Resonance Imaging (MRI) scans can quickly be transported to specialists for review [17], [18]. In addition, smart healthcare and the Internet of Medical Things (IoMT) [19]–[21] would be efficiently constructed due to the integration of 5G and e-health systems. Besides using individual services, multiple members of a family may join common healthcare services, for instance genetic testing [22]. In this way, they can conveniently know of the health status of the family members. Since families play an important role in promoting health and reducing the risk of illness [23], the services will significantly improve long-term results of medical treatments. The group health services can also be provided by healthcare teams at hospitals, healthcare institutions, or emergency centers. The whole treatment would be improved due to the collaborative work of the healthcare teams [24]–[26].

B. THE PROBLEMS

In a 5G-enabled healthcare environment, there are various e-health users [27], [28], including patients, physicians, pharmacists, medical researchers, caregivers, etc. The servers should be healthcare providers (e.g., hospitals), data center administrators, or medical professionals that provide services for specific users [29]. Since the users and servers carry out the communications throughout the open Internet, their sensitive information may be threatened to various attacks. Therefore, security and privacy of the e-health systems are of paramount importance [13], [30]. It requires a robust mechanism that can prevent possible security risks. Password-based or two-factor (integrating password and smart card) authentication schemes were proposed in many works to address the security issues [31], [32]. However, these are still not robust solutions. For example, in schemes designed with two-factor authentication, if the adversaries know of user' password, they can easily perform the attacks using a stolen smart card. With single-server architecture designed in a lot of works, the entities must store massive credentials (e.g., identities, passwords, etc.), for obtaining an increasing number of healthcare services [33]. Therefore, this architecture has been unable to meet the requirements of a convenient and cost-efficient communication.

C. RELATED WORKS AND MOTIVATION

Jiang *et al.* [34] proposed a remote biometrics user authentication scheme in a multi server environment. Odelu *et al.* [35] proposed a secure biometrics-based multi-server authentication protocol using smart cards. In addition, Park and Park [36] also designed a three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Qi *et al*. [37] introduced a biometrics-based authentication key exchange protocol for multi-server telecare medical information system (TMIS) without sharing the system private key with distributed servers. However, all [34]–[37] did not design their schemes with center-less authentication, where the registration center does not participate in the key agreement process. Moreover, Jiang *et al.* [34], Park and Park [36] and Qi *et al.* [37]'s schemes did not provide user untraceability, multi-server architecture and three-factor authentication, respectively. Another secure three-factor authentication scheme was proposed by Xu *et al.* [38] with a multi-server architecture. Besides, Hsu *et al.* [39] presented a three-factor fast authentication scheme with user anonymity for TMISs. Liu *et at*. [40] introduced their work with a biometric-based authentication scheme and privacy protection. According to Hsu *et al.* [39], Liu *et at*. [40] does not provide three-factor authentication, user anonymity, and user untraceability. Jiang *et al.* [41] presented a three-factor authentication scheme with privacy protection for e-health clouds. It is observed that Jiang *et al.* [41]'s scheme is not resilient to replay attacks, stolen smart card attacks and desynchronization attacks [39]. Moreover, Liu *et at*. [40] and Jiang *et al.* [41] cannot prevent Denial-of-Service (DoS) attacks. Jiang *et al.* [41] also did not introduce multi-server architecture in their proposed protocol. Wong *et al.* [42] proposed an efficient three-factor authentication protocol for multi-server e-health systems in 5G wireless sensor networks. However, the biometric noise was not discussed and addressed in their scheme. Specifically, the valid biometric templates of an individual may not be exactly the same with the one stored in the smart card. Since the biometrics is then computed in a hash function, the result should not pass the verification process. This is an important issue that needs addressing in the schemes designed with biometrics-based authentication. The issue can be remedied by various solutions [43], such as error-correcting codes, fuzzy commitments, fuzzy vaults, and biohash function. Among them, biohash function provides the noise tolerance with an efficient operation. Furthermore, all above-mentioned works did not propose the mechanism for group service communications.

Harn *et al.* [44] presented a novel design of group key distribution using only the logic exclusive-or (XOR) operation, and demonstrated its applications in various network models. A group key distribution scheme was introduced by [45] for a large size of group communication. In addition, Jiao *et al.* [46] proposed an efficient group key distribution protocol that can meet forward security and backward security. Tselikis *et al.* [47] proposed an

anonymous conference key distribution system, based on the elliptic curves, one-way hash functions and random pseudonyms. However, all the works of [44]–[47] introduced neither three-factor nor biometric-based authentication in their schemes. A secure authentication and group key distribution scheme for resource-limited Wireless Body Area Networks (WBANs) was proposed by Tan and Chung [48]. In their proposal, electrocardiogram (ECG) feature is applied as the unique synchronous factor for biometric authentication. Despite that, their scheme provided the identity authentication of the sensors, instead of the users with three-factor mechanism. Recently, Hsu and Le [49] proposed a group key distribution scheme with anonymous three-factor identification. The dynamic key distribution mechanism with complex steps in their work is not suitable to the group healthcare communication. Moreover, we found that their protocol did not address the biometric noise issue.

D. OUR CONTRIBUTIONS

In this paper, we propose an anonymous key distribution scheme for group healthcare services in 5G-enabled multi-server environments. Our scheme allows the servers to distribute a common key to a group of users for conducting group services. Main contributions of this paper can be presented as follows.

- We propose a 5G-enabled secure group communication model for various healthcare domains. The domains include personal care, home care and community care. Due to the proposed system model, the communications for group healthcare services can be efficiently facilitated by the high-speed 5G environments.
- The proposed scheme is designed with three-factor authentication integrating smart card, password, and biometrics, which provides a high security communication environment. User anonymity is also preserved during the communication process that is carried out via unreliable channels. Thus, the group key can be distributed in a secure and privacy-preserved manner. The common group key solution does not only enable group services, but also helps in saving the cost, due to the support of a single procedure (e.g., health data encryption) for all users. We employ Rabin cryptosystem in the scheme to achieve an efficient computation, since its encryption cost is much less than the one of Rivest-Shamir-Adleman (RSA) system.
- Our work introduces a single sign-on (SSO) solution [39], [40], [42] for group services in a multi-server environment. This solution allows users to use a single set of credentials stored in their smart cards to obtain services provided by multiple servers. It helps to significantly reduce the overhead, especially the storage cost. The SSO solution is achieved when the users store all information registered with multiple servers in the mobile devices [31], [39], [42].
- We provide a solid security proof of our scheme using various tools including Real-or-Random (RoR) model, Burrows-Abadi-Needham (BAN) logic, and Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation. In addition, we also demonstrate that our work is resilient to a lot of well-known attacks, such as DoS attacks, replay attacks, man-in-the-middle (MITM) attacks, etc.
- Our work presents an exhaustive performance analysis in terms of functions, communication cost, storage cost, and computation cost. The results of various comparisons indicate that the proposed scheme supports the most functions and bears rational costs, compared with the competitive ones.

E. PAPER STRUCTURE

The rest of the paper is organized as follows. Section II, we provide technical preliminaries of the proposed scheme. Section III, we present the system construction, formal security model and security goals. Section IV, we provide the design details of the proposed scheme. Section V and Section VI present security analysis and security simulation of our work, respectively. Performance evaluation and the comparisons are provided in Section VII. Finally, we draw some conclusions and discuss several future works in the last section of the paper.

II. TECHNICAL PRELIMINARIES

In this section, we briefly describe Rabin cryptosystem, advanced encryption standard, one-way hash function and biohash function.

A. RABIN CRYPTOSYSTEM

Rabin cryptosystem is an asymmetric encryption method, which relies on intractability of the integer factorization problem assumption (IFPA) [50], [51]. The cryptosystem consists of three algorithms: key generation, encryption and decryption. Although Rabin's decryption speed is roughly the same as the one of RSA, its encryption speed is much faster since it is computed using a modular squaring. Algorithms of the Rabin system are described as follows.

- *Key generation*: Two distinct primes (p, q) are randomly selected as the private keys of the system, in which $p \equiv q \equiv 3 \ mod \ 4$. The corresponding public key is computed by $n = p.q$.
- *Encryption*: Let $m \in (0, \ldots, n-1)$ be a plaintext, we can compute a ciphertext $c = m^2 \ mod \ n$.
- *Decryption*: Applying the Chinese Remainder Theorem (CRT), we can decrypt c by computing $m = \sqrt{c} \ mod \ n$. The private key (p, q) are necessary to efficiently factor N. m can be entirely recovered by adding some predefined padding.

Definition 1 (IFPA): Suppose there is a positive composite integer n (n is sufficiently large, for instance 1024 bits) and two distinct primes (p, q), where $n = p.q$. It is computationally hard is to derive and from the given n.

B. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES) [52] is a symmetric encryption technique that provides high degree

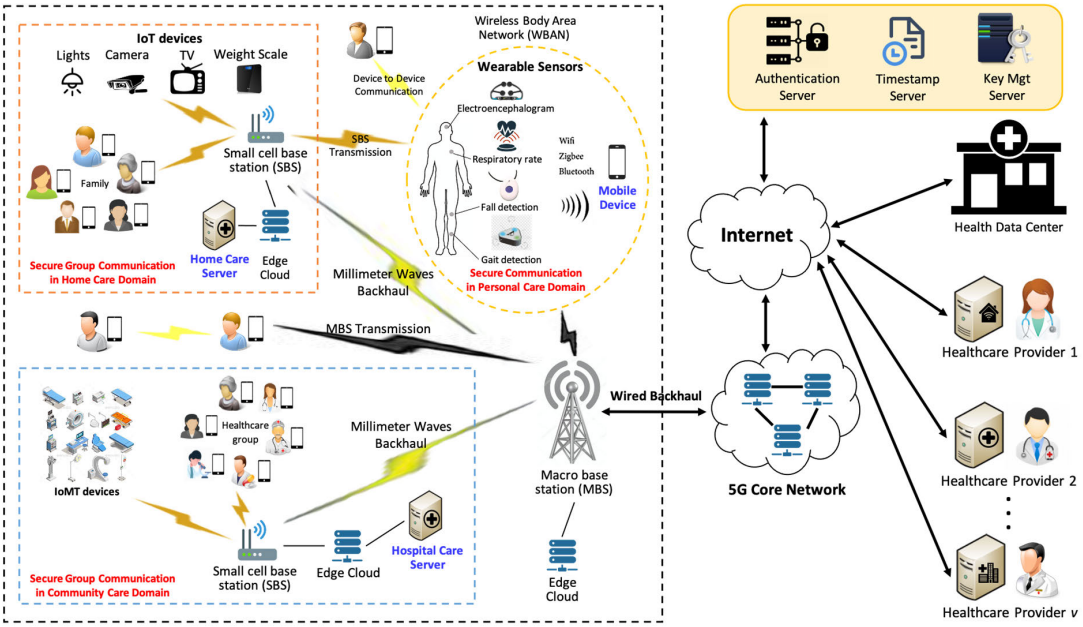

FIGURE 1. Our proposed system model.

of security. The AES encryption converts data into an unintelligible form, called ciphertext. Conversely, the decryption converts this ciphertext into its original form, called plaintext. AES algorithm is capable of generating block ciphertexts of 128 bits, with three different key sizes, namely, 128, 192 and 256 bits.

C. ONE-WAY HASH FUNCTION

One-way hash function is a cryptographic function that provides irreversibility and collision resistance to the hashed data. Given an arbitrary-length message m and a hash function $h(\cdot)$, some characteristics of the function are described in the following definitions [51].

Definition 2: A fixed-size output $C = h(m)$ should be produced.

Definition 3: It is easy to compute $C = h(m)$, but it is computationally hard to find m from the given C.

Definition 4: It is computationally hard to find $n \neq m$ with $h(n) = h(m)$.

Definition 5: It is computationally hard to find any pair (m, m) with $h(m) = h(n)$.

D. BIOHASH FUNCTION

Biohash function is designed to map an individual's biometrics to a specific binary string that provides the tolerance of noise [43]. The biohash function holds the same security with the one-way hash functions.

Definition 6: Suppose B_i and B_i' are respectively the original and the newly input biometric templates of an individual. The input B_i' is not exactly the same with B_i, but within a bearable threshold. Given the biohash function H_{Bio}, we have $H_{Bio}(B_i) = H_{Bio}(B_i')$.

III. PROBLEM STATEMENT

In this section, we provide a system model of the proposed scheme and its formal security model. Some important security goals are also discussed.

A. SYSTEM CONSTRUCTION

Our proposed system model includes three healthcare domains [42], namely, personal care, home care and community care, in a 5G-enabled multi-server environment, as shown in Figure 1. E-health users U_i and service provider servers S_j are two main roles in our construction. U_i can receive services from multiple S_j only with a single login enabled by the SSO solution.

A personal care domain consists of various wearable sensors (electroencephalogram, respiratory rate, fall detection, gait detection, etc.) installed in U_i's body, within a WBAN [39]. The sensors are used to collect the health data, thus providing a continuous health monitoring on U_i without any constraint on their normal daily life activities [42]. With the support of wireless technologies (for instance, Bluetooth), sensing data is then transmitted to U_i's mobile device for further communications. Personal care is the sub-domain of the home or community care domains.

In a home care domain, U_i registers with S_j using the smart card, password and biometrics. After a mutual authentication, S_j distributes a secret group key to U_i. Based on this key, sensing data from the personal care domain is encrypted and securely uploaded to the systems for the remote monitoring. This communication can quickly be carried out by the help of 5G networks for the real-time process. In this case, S_j should be private doctors or family medical professionals. S_j can also use the key to encrypt the healthcare related data including treatment details or medical testing results,

then send it to U_i. In this way, everyone in the family is able to query and access health data of their own and of the other family members since they have a common group key. In smart homes, there may be various IoT devices that can connect to the network, such as smart light, camera, TV, etc. U_i can set the group key as a key used to conveniently control these devices, even though U_i is not available at home. In the 5G network, U_i communicates with S_j through either SBSs or MBSs as long as they have spectrum opportunities. The service providers may employ edge servers to achieve better response times and transfer rates [31]. U_i can also use mobile devices to directly communicate with each other for the sharing of access connection or additional information. Furthermore, communications between U_i and S_j in our scheme are time stamped for the purpose of security, which is discussed later in subsequent sections.

The communications in a community care domain are similar to the one in the home care domains. However, the setting of communicating entities should be different. We take the communication of a healthcare group in hospital as an example. Members in the group (patients, doctors, pharmacists, researchers, etc.) should be the users U_i. S_j may be a hospital. administrator or a medical doctor who is the leader of the healthcare team. After U_i receives the distributed group key, they are able to obtain the similar services provided by S_j. As a doctor, pharmacist or researcher in a healthcare team, U_i can monitor patients' health status and provide prescriptions, verify the correctness of the prescriptions, or analyze the data sent by S_j, respectively [39]. U_i, as a CT or MRI specialist, may also communicate the large image files of the patients with S_j (as another specialist) for expedited reviews and treatments, due to high-speed data transmission of the 5G network. In smart hospitals, there may be modern IoMT devices used for specific treatments. U_i of the team can also utilize the group key distributed by the administrator to operate (turn on, control or turn off) these connected devices. Similarly, U_i in this domain can perform the D2D communications for additional purposes.

B. FORMAL SECURITY MODEL

Since the communication between U_i and S_j is carried out via an open channel, their transmitted information may be threatened to various risks. In a three-factor authentication-based group key distribution environment, an adversary A can perform various attacks on a challenger $\mathbb{C}$ by making the following queries [40].

- *Send*($\mathbb{C}$, M_{sg}): This is an active attack. A requests message M_{sg} to $\mathbb{C}$, and $\mathbb{C}$ replies to A based on the rules of our scheme.
- *Execute*(U_i, S_j): This is a passive attack. A eavesdrops the communicated messages of U_i and S_j.
- *Reveal*($\mathbb{C}$): This query reveals the group key distributed by $\mathbb{C}$ to A.
- *Corrupt*(U_i, a): $\mathbb{C}$ returns U_i's password, biometrics, and parameters stored in the smart card and mobile device to A, based on a value $a \in \{1, 2, 3\}$.

TABLE 1. Notations and cryptographic functions used in our scheme.

Notations	Description
S_j	Healthcare server j
U_i	User i
ID_{S_j}	Identity of S_j
ID_i	Identity of U_i
PW_i	Password of U_i
B_i	Biometrics of U_i
p_j, q_j	Private keys of S_j
n_j	Public key of S_j
s_j	Secret key of S_j
t	Timestamp
$\oplus$	XOR function
$h(.), H(.)$	Secure one-way hash functions
H_{Bio}	Secure biohash function
$AE(.)$, $AD(.)$	Rabin encryption, decryption algorithm
$SE(.)$, $SD(.)$	AES encryption, decryption algorithm
$[.]_{SC_i}$	Store values in U_i's smart card
$[.]_{MD_i}$	Store values in U_i's mobile device
$[.]_{DB_j}$	Store values in S_j's database

- *Test*($\mathbb{C}$): A requests $\mathbb{C}$ for the group key, $\mathbb{C}$ flips a coin b and probabilistically replies to A.

Definition 7: Let $Adv_{\mathbb{C}}^{5G-AGKDS}$ be the advantage of A in breaking the semantic security system, then $Adv_{\mathbb{C}}^{5G-AGKDS} = \left|2Pr\left[b' = b\right] - 1\right|$, where $5G - AGKDS$ denotes the proposed scheme, and b' denotes the guessed bit.

C. SECURITY GOALS

Since user privacy and the healthcare data are very sensitive and important, possible attacks can induce big consequences, such as financial loss, system obstruction, etc. It may also directly affect the treatment process and quality of the healthcare services [39]. We therefore determine some essential security goals of the proposed scheme below, so that S_j can securely distribute the group key to U_i.

- *Mutual authentication*: U_i must be authenticated as a legitimate user to receive the group key distributed by S_j. Likewise, U_i must also authenticate S_j to verify its legitimacy for the true services.
- *Robustness against well-known attacks*: The proposed scheme should be resilient to various well-known security attacks, typically, replay attacks and MITM attacks.
- *User anonymity and untraceability*: Identity of U_i must be preserved during the communication carried out via an open channel. In addition, any two past messages sent by the same U_i should not be identified.
- *Forward secrecy*: Our work aims to prevent A from using information of the current communication session to derive the secret group key distributed in the past sessions.

IV. OUR PROPOSED SCHEME

Our proposed scheme allows the servers to distribute secure common keys to the groups of users, so that they can enjoy the group healthcare services. The procedure includes four

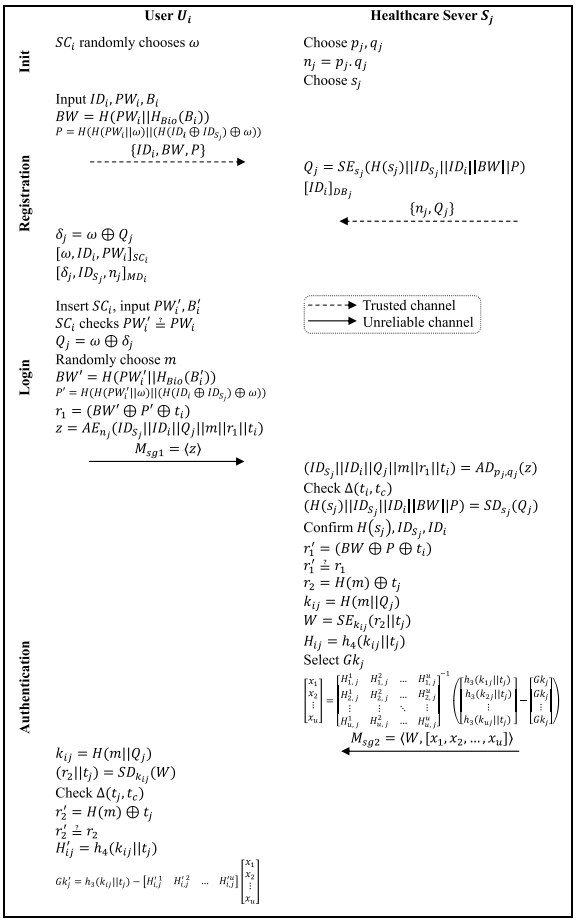

FIGURE 2. Procedure of the proposed scheme.

phases: initialization, registration, login, and authentication. After the system initialization, the registration (key predistribution) procedure is conducted in a trusted channel, whereas the login procedure and authentication procedure are carried out via an unreliable channel. Table 1 describes some notations and functions used in the scheme. The design details are depicted in Figure 2.

A. INITIALIZATION PHASE

In this phase, system parameters are generated in order to be used to carry out the entire communication process. To this end, S_j first selects two large primes (p_j, q_j) as private keys, and computes $n_j = p_j.q_j$ as the corresponding public key, which satisfies $p_j \equiv q_j \equiv 3(mod\ 4)$. Next, S_j randomly selects s_j as its secret symmetric key. S_j secretly stores $[(p_j, q_j), s_j]$ in DB_j. In user side, SC_i randomly selects and stores a string ω.

B. REGISTRATION PHASE

U_i must register with S_j for using its services. To this end, U_i and S_j perform the following steps to complete the registration procedure.

Step R1 : U_i enters his/her identity ID_i, password PW_i and biometrics B_i. U_i then computes $BW = H(PW_i||H_{Bio}(B_i))$ and $P = H(H(PW_i||\omega)||(H(ID_i \oplus ID_{S_j}) \oplus \omega))$. Next, U_i sends (ID_i, B, P) to S_j.

Step R2 : Upon receiving (ID_i, BW, P), S_j uses encryption key s_j to compute $Q_j = SE_{s_j}(H(s_j)||ID_{S_j}||ID_i||BW||P)$. Then, S_j sends (n_j, Q_j) to U_i.

Step R3 : Upon receiving message (n_j, Q_j), U_i computes $\delta_j = \omega \oplus Q_j$. Finally, U_i stores their credentials $\{\omega, ID_i, PW_i\}$ and server-related parameters $\{\delta_j, ID_{S_j}, n_j\}$ in SC_i and MD_i respectively.

C. LOGIN PHASE

In this procedure, U_i inserts SC_i, and enters password PW_i' and biometrics B_i'. PW_i' is first checked by SC_i. U_i then computes $Q_j = \omega \oplus \delta_j$, and randomly chooses a number m. Next, U_i computes $BW' = H(PW_i'||H_{Bio}(B_i'))$, $P' = H(H(PW_i'||\omega)||(H(ID_i \oplus ID_{S_j}) \oplus \omega))$, $r_1 = (BW' \oplus P' \oplus t_i)$, and a ciphertext $z = AE_{n_j}(ID_{S_j}||ID_i||Q_j||m||r_1||t_i)$. Thereafter, U_i sends message $M_{sg1} = \langle z \rangle$ to S_j.

D. AUTHENTICATION PHASE

Upon the login request from U_i, S_j and U_i carry out the following two steps to complete the authentication procedure, which allows U_i to obtain a secret group key distributed by S_j.

Step A1 : Upon receiving M_{sg1}, S_j uses its private keys (p_j, q_j) to decrypt z and confirms the validity of the timestamp t_i. Next, S_j uses s_j to decrypt Q_j (obtained from message z) and verifies $h(s_j)$, ID_i and ID_{S_j}. If they are valid, S_j computes $r_1' = (BW \oplus P \oplus t_i)$, then checks if r_1 (obtained from z) and r_1' are identical. If there is a match, S_j calculates $r_2 = H(m) \oplus t_j$, $k_{ij} = H(m||Q_j)$, and a ciphertext $W = SE_{k_{ij}}(r_2||t_j)$. Next, S_j computes $H_{ij} = h_4(k_{ij}||t_j)$, chooses group key Gk_j, and calculates a set of coefficients $(x_1, x_2, \ldots, x_u)$ as follows, in which u is the total number of users in a group communication.

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_u \end{bmatrix} = \begin{bmatrix} H_{1,j}^1 & H_{1,j}^2 & \ldots & H_{1,j}^u \\ H_{2,j}^1 & H_{2,j}^2 & \ldots & H_{2,j}^u \\ \vdots & \vdots & \ddots & \vdots \\ H_{u,j}^1 & H_{u,j}^2 & \ldots & H_{u,j}^u \end{bmatrix}^{-1} \times \left(\begin{bmatrix} h_3(k_{1j}||t_j) \\ h_3(k_{2j}||t_j) \\ \vdots \\ h_3(k_{uj}||t_j) \end{bmatrix} - \begin{bmatrix} Gk_j \\ Gk_j \\ \vdots \\ Gk_j \end{bmatrix} \right) \quad (1)$$

Then, S_j sends message $M_{sg2} = \langle W, [x_1, x_2, \ldots x_u] \rangle$ to U_i.

Step A2 : Upon receiving M_{sg2}, U_i computes $k_{ij} = H(m||Q_j)$ to decrypt W. U_i checks the validity of the timestamp t_j. Next, U_i computes $r_2' = H(m) \oplus t_j$ and compares it with r_2. If there is a match, U_i computes $H_{ij}' = h_4(k_{ij}||t_j)$. Finally, U_i obtains the group key distributed by S_j by calculating the following

TABLE 2. Symbols used in RoR model-based security proof.

Symbols	Description
l_h	Key size of hash values
l_r	Key size of random numbers
l_b	Key size of biometric template
q_h	Total number of the hash oracle queries
q_s	Total number of the *Send* queries
q_e	Total number of the *Execute* queries
L_H	List storing hash oracle outputs
L_A	List storing random oracle results
L_M	List storing transmitted messages of U_i and S_j

calculation.

$$Gk'_j = h_3(k_{ij}||t_j) - \left[H'^1_{i,j} \;\; H'^2_{i,j} \;\; \dots \;\; H'^u_{i,j} \right] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_u \end{bmatrix} \quad (2)$$

In this way, each user of the same groups obtains a common secret key for using specific group services provided by the healthcare servers.

V. SECURITY ANALYSIS

This section provides security proof of our scheme using RoR model and BAN logic. In addition, we also discuss some further security features of the scheme.

A. FORMAL SECURITY PROOF USING ROR MODEL

Formal security proof of the proposed scheme is proven using widely-accepted ROR model [39], [40]. The model includes various queries (*Send*, *Execute*, *Reveal*, *Corrupt* and *Test*) that can be made by A to guess the shared secret key of U_i and S_j. The proof in RoR consists of a number of games, in which A can attack the scheme in various ways by the increased probability. The purpose is to demonstrate the total probability of A in successfully attacking the proposed scheme is negligible. Table 2 provides some notations used in the proof. Based on the formal security model specified in Section III-B, we prove the security of our work as follows.

Definition 8: Let $Adv_A^{IFPA}(T_A)$ be the advantage of A in breaking the IFPA. Based on Definition 1, we have that $Adv_A^{IFPA}(T_A)$ is negligible for A with the running time T_A.

Definition 9: The value $max\left\{C'.q_s^{s'}, q_s\left(\frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\}$ is negligibly small, where C', s' are zipf parameters and ε_{bm} is the probability of false positive of biometrics [39].

Theorem 1: With $Adv_{\mathbb{C}}^{5G-AGKDS}$, $Adv_A^{IFPA}(t_A)$ and the notations defined in Definition 7, Definition 8 and Table 2 respectively, we have that A only has a negligible probability, in the following equation, in breaking our scheme. Our work therefore is semantically secure.

$$\begin{aligned} Adv_{\mathbb{C}}^{5G-AGKDS} \leq & \frac{3q_s + q_e}{2^{l_r}} + \frac{q_h^2 + 12q_h}{2^{l_h}} \\ & + 2max\left\{C'.q_s^{s'}, q_s\left(\frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\} \\ & + 2q_h(q_s + q_e + 1)Adv_A^{IFPA}(T_A) \end{aligned} \quad (3)$$

TABLE 3. Simulation of *Send* and *Execute* oracle queries.

Simulation of *Execute*(U_i , S_j) query occurs in succession with simulation of *Send*($\mathbb{C}$, M_{sg}) queries, described as follows. U_i transmits $Msg_1 =< z >$ to S_j , and S_j sends $Msg_2 =< W, [x_1, x_2, \dots x_u] >$ to U_i, we have: $<\{ID_{S_j}||ID_i||Q_j||m||r_1||t_i\}_{n_j}> \leftarrow$ *Send*(U_i , *start*), $< \{r_2||t_j\}_{k_{ij}}$, $[x_1, x_2, \dots x_u] > \leftarrow$ *Send*(S_j , $<\{ID_{S_j}||ID_i||Q_j||m||r_1||t_i\}_{n_j}>$) Finally, $Msg_1 =< \{ID_{S_j}||ID_i||Q_j||m||r_1||t_i\}_{n_j} >$ and $Msg_2 =< \{r_2||t_j\}_{k_{ij}}, [x_1, x_2, \dots x_u] >$ are returned.
Based on the rules of our scheme, *Send* query is executed in the following. • Upon *Send*(U_i, *start*) query, $\mathbb{C}$ replies to A as follows. Compute ID_{S_j}, ID_i, Q_j, r_1; choose m Output $Msg_1 =< \{ID_{S_j}||ID_i||Q_j||m||r_1||t_i\}_{n_j} >$. • Upon *Send*($S_j$, $<\{ID_{S_j}||ID_i||Q_j||m||r_1||t_i\}_{n_j}>$), $\mathbb{C}$ replies to A as follows. Decrypt z, check t_i, decrypt Q_j, check $H(s_j), ID_{S_j}, ID_i$ and r_1, and compute r_2 , k_{ij} and $\{r_2||t_j\}_{k_{ij}}$. The communication session will terminate if one of the verifications does not hold. Select Gk_j and compute $[x_1, x_2, \dots x_u]$. Output $Msg_2 =< \{r_2||t_j\}_{k_{ij}}, [x_1, x_2, \dots x_u] >$. • $\mathbb{C}$'s response to *Send*(U_i, $<\{r_2||t_j\}_{k_{ij}}, [x_1, x_2, \dots x_u]>$) is as follows. Compute k_{ij}, decrypt $\{r_2||t_j\}_{k_{ij}}$, check t_j and r_2, and compute Gk'_j. If one of the checks does not hold, terminate the session; otherwise, accept Gk'_j. After the group key is distributed, $\mathbb{C}$ terminates the session.

Proof: Our proof consists of six games: G_0, G_1, G_2, G_3, G_4 and G_5. We define $Succ_i$ ($i = 0, 1, 2, 3, 4, 5$) as the events where A succeeds in guessing the bit b with the *Test* query. The success probabilities are denoted by $Pr[Succ_i]$ accordingly.

- Game G_0: In the RoR model, this initial game is identical to the actual scheme. The coin b is flipped to start the game. Based on Definition 7, we have,

$$Adv_{\mathbb{C}}^{5G-AGKDS} = |2Pr\,[Succ_0] - 1| \quad (4)$$

- Game G_1: In this game, we simulate all the queries including *Hash*, *Send*, *Execute*, *Reveal*, *Corrupt*, and *Test*. Table 3 presents the *Send* and *Execute* queries based on the rule of the proposed scheme. Thus, G_1 creates three lists, namely, L_H, L_A and L_M. Since G_0 and G_1 are indistinguishable, we can obtain,

$$Pr\,[Succ_1] = Pr\,[Succ_0] \quad (5)$$

- Game G_2: Collision probability of hash oracle and random oracle queries are considered in this game, for all transmitted messages between U_i and S_j. Based on the birthday paradox, we have the probability of hash queries is at most $\frac{q_h^2}{2^{l_h+1}}$. In the login and authentication phases, there are two messages M_{sg1} and M_{sg2} with a randomly generated number m. It has the maximum collision probability as $\frac{q_s+q_e}{2^{l_r+1}}$. Overall, we can obtain,

$$|Pr\,[Succ_2] - Pr[Succ_1]\,| \leq \frac{q_s + q_e}{2^{l_r+1}} + \frac{q_h^2}{2^{l_h+1}} \quad (6)$$

TABLE 4. Comparison on functions.

Functions	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[49]	Ours
Provides three-factor authentication	√	√	√	×	√	√	×	√	√	√	√
Provides solution for biometric noise	√	√	√	√	√	√	√	√	×	×	√
Provides group key distribution	×	×	×	×	×	×	×	×	×	√	√
Provides group healthcare communications	×	×	×	×	×	×	×	×	×	×	√
Provides RoR provable security proof	√	×	×	×	√	√	√	×	×	×	√
Provides AVISPA/ProVeri security simulation	×	√	×	×	×	√	×	×	√	√	√
Provides user anonymity	√	√	√	√	√	√	×	√	√	√	√
Provides user untraceability	×	√	√	√	√	√	×	√	√	√	√
Provides forward secrecy	√	√	√	√	√	√	√	√	√	√	√
Provides multi-server architecture	√	√	×	√	√	√	√	×	√	√	√
Provides center-less authentication	×	×	×	×	√	√	√	√	√	√	√
Resists DoS attacks	√	√	√	√	√	√	×	×	√	√	√
Resists online password guessing attacks	√	√	√	√	√	√	√	√	√	√	√
Resists offline password guessing attacks	√	√	√	√	√	√	√	√	√	√	√
Resists impersonation attacks	√	√	√	√	√	√	√	√	√	√	√
Resists replay attacks	√	√	√	√	√	√	√	×	√	√	√
Resists MITM attacks	√	√	√	√	√	√	√	√	√	√	√
Resists tampering attacks	√	√	√	√	√	√	√	√	√	√	√
Resists desynchronization attacks	√	√	√	√	√	√	√	×	√	√	√
Resists insider attacks	√	√	√	√	√	√	√	√	√	√	√
Resists lost smart card/device attacks	√	√	√	√	√	√	√	×	√	√	√

- Game G_3: In this game, we calculate the collision probabilities of all remaining oracle queries with specific messages. To this end, two cases corresponding with two communication rounds are considered as follows.
  Case 1: This case considers the query $Send(S_j, Msg_1)$. Msg_1 is computed from two hashes (BW', P') and two other values (Q_j, r_1), which totally results in a probability at most $4\frac{q_h}{2^{l_h}}$. In addition, the random number m contained in this message has the probability as $\frac{q_s}{2^{l_r}}$.
  Case 2: We consider $Send(U_i, Msg_2)$ query in this case. Similarly, Msg_2 contains r_2 and k_{ij}, which should be known to A, for performing the attacks. The corresponding probability is up to $2\frac{q_h}{2^{l_h}}$.
  Due to the indistinguishability of G_2 and G_3, we can obtain the following total probability,

$$|Pr\,[Succ_3] - Pr[Succ_2]\,| \leq 6\frac{q_h}{2^{l_h}} + \frac{q_s}{2^{l_r}} \tag{7}$$

- Game G_4: This game considers the *Corrupt* query in which A performs guessing attacks on users' passwords and biometrics. We have the probabilities of guessing PW_i and B_i are at most $C'.q_s^{s'}$ and $\max\{q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\}$ respectively [40]. In addition, A is able to break the security system with the most probability as $q_h Adv_A^{IFPA}(t_A)$. Since G_3 and G_4 are identical, we have,

$$|Pr\,[Succ_4] - Pr\,[Succ_3]\,| \leq \max\{C'.q_s^{s'}, q_s(\frac{1}{2^{l_b}}, \varepsilon_{bm})\} + q_h Adv_A^{IFPA}(T_A) \tag{8}$$

- Game G_5: We consider the perfect forward secrecy feature of our work in this final game. Based on the old messages communicated between U_i and S_j, A similarly executes *Execute*, *Send*, and hash oracle queries. We simulate this game using the advantage of the *IFPA* assumption. The *Test* query is also executed to return the real group key for each instance. Since G_4 and G_5 are indistinguishable without this attack, we can obtain,

$$|Pr[Succ_5] - Pr[Succ_4]| \leq q_h(q_s + q_e)Adv_A^{IFPA}(T_A) \tag{9}$$

After executing all above games, A guesses the bit b' for obtaining Gk_j with the probability as follows.

$$Pr\,[Succ_5] = \frac{1}{2} \tag{10}$$

Based on Equations (5), (10), and the triangle inequality, we can obtain,

$$\begin{aligned} |Pr\,[Succ_0] - \frac{1}{2}| &= |Pr\,[Succ_1] - Pr[Succ_5]\,| \\ &\leq |Pr\,[Succ_1] - Pr\,[Succ_2]| \\ &\quad + |Pr\,[Succ_2] - Pr\,[Succ_3]| \\ &\quad + |Pr\,[Succ_3] - Pr\,[Succ_4]| \\ &\quad + |Pr\,[Succ_4] - Pr\,[Succ_5]\,| \end{aligned} \tag{11}$$

Based on Equations (4)-(11), we can achieve,

$$\begin{aligned} \frac{1}{2}Adv_{\mathbb{C}}^{5G-AGKDS} &= |Pr\,[Succ_0] - \frac{1}{2}| \\ &\leq \frac{q_s + q_e}{2^{l_r+1}} + \frac{q_h^2}{2^{l_h+1}} + 6\frac{q_h}{2^{l_h}} + \frac{q_s}{2^{l_r}} \\ &\quad + max\left\{C'.q_s^{s'}, q_s\left(\frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\} \\ &\quad + q_h Adv_A^{IFPA}(T_A) \\ &\quad + q_h(q_s + q_e)Adv_A^{IFPA}(T_A) \end{aligned} \tag{12}$$

Multiplying both sides of Equation (12) by a factor of 2, we can obtain the final result as follows,

$$\begin{aligned} Adv_{\mathbb{C}}^{5G-AGKDS} &\leq \frac{3q_s + q_e}{2^{l_r}} + \frac{q_h^2 + 12q_h}{2^{l_h}} \\ &\quad + 2max\left\{C'.q_s^{s'}, q_s\left(\frac{1}{2^{l_b}}, \varepsilon_{bm}\right)\right\} \\ &\quad + 2q_h(q_s + q_e + 1)Adv_A^{IFPA}(T_A) \end{aligned} \tag{13}$$

Since Equations (3) and (13) are consistent, it is indicated that A only has a negligible success probability in breaking the proposed scheme. Our work therefore is semantically secure, and Theorem 1 is proven.

B. AUTHENTICATION PROOF USING BAN LOGIC

In this section, we use BAN logic [31], [39], [53] to provide authentication proof of our work. BAN logic provides the rules used for analyzing authentication protocols. Based on these rules and logic analysis, we can indicate that communicating parties believe the authenticated parameter is a secret shared key only known by them. The notations used in this proof are defined as follows.

- $M| \equiv X$: M believes statement X.
- $M \triangleleft X$: M sees statement X.
- $\#(X)$: The formula X is fresh.
- $M| \sim X$: M once said statement X.
- (X, Y): X or Y is one part of the formula (X, Y).
- $M \Longrightarrow X$: M has jurisdiction over statement X.
- $\langle X \rangle_Y$: This represents X combined with the formula Y.
- $M \overset{K}{\leftrightarrow} N$: The shared key K is known only to M and N, and it is used for their communication.
- $M \overset{X}{\Longleftrightarrow} N$: Formula X is a secret known only by M and N. Only M and N can use X to authenticate each other.

According to the procedures of the BAN logic, the proposed scheme should satisfy the following goals of the authentication.

Goal 1: $S_j| \equiv (U_i \overset{k_{ij}}{\leftrightarrow} S_j)$. S_j believes k_{ij} is a secret value sent by U_i, and k_{ij} is a shared value between them.

Goal 2: $U_i| \equiv (U_i \overset{Gk_j}{\leftrightarrow} S_j)$. U_i believes Gk_j is a secret group key distributed by S_j, and Gk_j is a shared key between them.

Our scheme includes two messages described as follows.

$$M_{sg1}.U_i \rightarrow S_j : (AE_{n_j}(ID_{S_j}||ID_i||Q_j||m||r_1||t_i)).$$
$$M_{sg2}.S_j \rightarrow U_i : (SE_{k_{ij}}(r_2||t_j), [x_1, x_2, \ldots x_u]).$$

The idealized form of the messages in the BAN logic is given below.

$$M_{sg1}.U_i \rightarrow S_j : (\langle ID_{S_j}, ID_i, Q_j, m, r_1, t_i \rangle_n).$$
$$M_{sg2}.S_j \rightarrow U_i : (\langle r_2, t_j \rangle_{k_{ij}}, \langle x_1, x_2, \ldots x_u \rangle).$$

Some logical rules of the BAN logic used in our scheme are given as follows.

- R1 (seeing rule): $\frac{M \overset{X}{\Longleftrightarrow} N, N \triangleleft \langle X \rangle_K}{M| \equiv N| \sim X}$;
- R2 (interpretation rule): $\frac{M| \equiv N| \sim (X,Y)}{M| \equiv N| \sim X}$;
- R3 (freshness rule): $\frac{M| \equiv \#(X)}{M| \equiv \#(X,Y)}$;
- R4 (verification rule): $\frac{M| \equiv \#(X), M| \equiv N| \sim X}{M| \equiv N| \equiv X}$;
- R5 (jurisdiction rule): $\frac{M| \equiv N \Longrightarrow X, M| \equiv N| \equiv X}{M| \equiv X}$;
- R6 (additional rule): $\frac{M| \equiv (X,Y)}{M| \equiv X}$.

Based on the logic, we also make the following assumptions of the proposed scheme.

- A1: $S_j| \equiv U_i \overset{n}{\Longleftrightarrow} S_j$;
- A2: $S_j| \equiv \#(t_i)$;
- A3: $S_j| \equiv U_i \Longrightarrow (Q_j, t_i)$;
- A4: $U_i \Longrightarrow (m, \omega, \delta_j)$;
- A5: $U_i| \equiv \#(t_j)$;
- A6: $U_i| \equiv S_j \Longrightarrow ((t_j, (x_1, x_2, \ldots x_u))$.

Based on the above-mentioned assumptions and logical rules, we analyze the procedure of the proposed scheme and provide the authentication proof as follows.

- E_1 : According to the message M_{sg1}, we can have, $S_j \triangleleft (\langle ID_{S_j}, ID_i, Q_j, m, r_1, t_i \rangle_n)$.
- E_2 : According to R1 and A1, we have, $S_j| \equiv U_i| \sim (ID_{S_j}, ID_i, Q_j, m, r_1, t_i)$.
- E_3 : Based on R2, we can obtain, $S_j| \equiv U_i| \sim (Q_j, m, t_i)$.
- E_4 : We have, $S_j| \equiv \#(Q_j, m, t_i)$, according to R3 and A2.
- E_5 : Based on R4, we obtain, $S_j| \equiv U_i| \equiv (F, Q_j, t_i)$.
- E_6 : According to R5, A1 and A3, we have, $S_j| \equiv (Q_j, m, t_i)$.
- E_7 : Based on R6 and E_6, we obtain, $S_j| \equiv Q_j$ and $S_j| \equiv m$.
- E_8 : From E_7 and $k_{ij} = H(m||Q_j)$, we can obtain, $S_j| \equiv (U_i \overset{k_{ij}}{\longleftrightarrow} S_j)$. (**Goal 1**)
- E_9 : Based on A4, $k_{ij} = H(m||(\omega \oplus \delta_j))$ and E_8, we obtain, $U_i| \equiv k_{ij}$ and $U_i| \equiv U_i \overset{k_{ij}}{\Longleftrightarrow} S_j$.
- E_{10} : According to the message M_{sg2}, we have, $U_i \triangleleft (\langle r_2, t_j \rangle_{kij}, \langle x_1, x_2, \ldots x_u \rangle)$.
- E_{11} : Based on R1 and E_9, we obtain, $U_i| \equiv S_j| \sim (r_2, t_j, (x_1, x_2, \ldots x_u))$.
- E_{12} : Based on R2, we have, $U_i| \equiv S_j| \sim (t_j, (x_1, x_2, \ldots x_u))$.
- E_{13} : According to R3 and A5, we can obtain, $U_i| \equiv \#(t_j, (x_1, x_2, \ldots x_u))$.
- E_{14} : We have, $U_i| \equiv S_j| \equiv (t_j, (x_1, x_2, \ldots x_u))$, based on R4.
- E_{15} : We obtain, $U_i| \equiv (t_j, (x_1, x_2, \ldots x_u))$, based on R5 and A6.
- E_{16} : Based on R6 and E_{15}, we have, $U_i| \equiv t_j$ and $U_i| \equiv (x_1, x_2, \ldots x_u)$.
- E_{17} : According to E_9, E_{16} and

$$Gk_j = h_3(k_{ij}||t_j) - \left[h_4(k_{ij}||t_j)_1 \; h_4(k_{ij}||t_j)_2 \; \ldots \; h_4(k_{ij}||t_j)_u\right] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_u \end{bmatrix},$$

we can obtain, $U_i| \equiv (U_i \overset{Gk_j}{\longleftrightarrow} S_j)$ (**Goal 2**)

Thus, the proposed scheme achieves both **Goal 1** and **Goal 2**, which ensures that both U_i and S_j mutually authenticate each other.

C. DISCUSSION ON SOME OTHER FEATURES

We provide semantic analysis of our scheme in terms of some more security features. The detailed discussion is presented in the following.

1) PROVIDES ROBUST MUTUAL AUTHENTICATION

Upon the received message M_{sg1}, S_j decrypts Q_j and verifies $H\left(s_j\right), ID_{S_j}, ID_i$. Moreover, S_j also check the value $r_1 = (BW' \oplus P' \oplus t_i)$ by $r_1' \stackrel{?}{=} r_1$. On the other hand, the value $r_2 = H(m) \oplus t_j$ sent by the server is also checked by U_i. Since r_1 and r_2 are only correctly computed by the legitimate user and server respectively, the mutual authentication is robust. The group key Gk_j will not be accepted unless the above checks hold. Thus, conclusion is established.

2) PROVIDES USER ANONYMITY

The user identity ID_i included in P' and z is protected by the one-way hash function h and Rabin encryption respectively. ID_i is kept secret to U_i and S_j only, and it is not revealed to the public during the authentication process. Therefore, user anonymity is achieved in our scheme.

3) PROVIDES USER UNTRACEABILITY

In the proposed scheme, the ciphertexts are computed using the random number m. In addition, the timestamps t_i, t_j included in the messages are different in every session. As such, A cannot identify any two past messages sent by the same U_i. Therefore, our work achieves user untraceability.

4) PROVIDES FORWARD SECRECY

In login phase of the scheme, the nonce k_{ij} is computed using a random number m. Moreover, the group key Gk_j is also a randomly selected value. Suppose A has obtained these parameters in the current communication session, he/she is still not able to compromise the group keys of the past sessions. Thus, our scheme provides perfect forward secrecy.

5) RESISTS DOS ATTACKS

Our scheme provides smart card verification. SC_i will checks PW_i', and reject it if the verification is not successful. Therefore, A is not able to use its candidate passwords (and biometrics) to flood S_j. Moreover, timestamp t_i is also checked after z is decrypted. Retransmitting z repeatedly to make S_j disrupted will not work efficiently in this case. Hence, the proposed scheme can avoid DoS attacks.

6) RESISTS ONLINE PASSWORD GUESSING ATTACKS

A may attempt to guess a candidate password and input it to the system, in order to initialize the login request. However, A's candidate password will easily be checked and declined by SC_i's verification. Thus, the conclusion is established.

7) RESISTS OFFLINE PASSWORD GUESSING ATTACKS

Suppose A has somehow obtained the hash values computed by U_i, then tries to guess PW_i. In our scheme, PW_i is included in $BW = H(PW_i||H_{Bio}(B_i))$ and $P = H(h(PW_i||\omega)||(h(ID_i \oplus ID_{S_j}) \oplus \omega))$. A attempts to compute the hash values B and P and compare them with the ones he has obtained. However, A does not know of the biometrics B_i and the random parameter ω. Therefore, A is not able to compute the desired hash values for guessing the correct PW_i. Thus, our work resists offline password guessing attacks.

8) RESISTS IMPERSONATION ATTACKS

This attack happens when the attacker has obtained the identity ID_i and tries to impersonate U_i. Even if ID_i is revealed to A, our work is still safe due to the resistance to password guessing attacks. Moreover, since A does not know of the parameter ω, they cannot compute the correct values B, P to impersonate U_i. The conclusion is therefore established.

9) RESISTS REPLAY ATTACKS

In the proposed scheme, S_j can verify whether the message $\langle z \rangle$ is resent by checking the timestamp t_i. Similarly, U_i can check the validity of the message $\langle W, [x_1, x_2, \ldots x_n] \rangle$ by confirming the timestamp t_j. Therefore, it is not possible for A to perform the replay attacks on the current communication session using the intercepted message from the last session. Hence, replay attacks are prevented in our work.

10) RESISTS MITM ATTACKS

In the login phase of our scheme, A can use the public key n_j of S_j to generate a candidate login request message z'. In this case, A may act as a middle man to change the correspondence between U_i and S_j who trust they are straightforwardly communicating with each other. However, without the knowledge of s_j or $H(s_j)$, the attacker cannot pass the verification of S_j. Moreover, as stated, since our scheme can resist offline password guessing attacks and impersonation attacks, A is not able to compute the correct z. Therefore, MITM attacks are completely resisted in the proposed scheme.

11) RESISTS TAMPERING ATTACKS

This attack happens when A blocks the login request $\langle z \rangle$ generated by legitimate users, modifies the contents, and sends a tampered one to S_j. However, A cannot tamper with z since this ciphertext is only successfully decrypted using the private keys p_j and q_j, which are only known to S_j. Therefore, our scheme resists data tampering attacks.

12) RESISTS DESYNCHRONIZATION ATTACKS

In the proposed scheme, the parameters BW, P and timestamps t_i, t_j are used to compute the acknowledgement values r_1 and r_2. They will be deleted after the communication sessions finish. No redundant parameters are stored by U_i and S_j. Therefore, the conclusion is established.

13) RESISTS INSIDER ATTACKS

This attack happens when a privileged insider in the server side acts as A and uses the information of the targeted U_i to carry out the attack. In our scheme, S_j may know of the parameters ID_i, BW, P. Nevertheless, A cannot use ID_i to perform the attacks since as stated our work can resist impersonation attacks. Moreover, as stated, it is also not possible for A to carry out the offline password guessing attacks based on BW and P. In addition, biometric databases and verification tables are all not required in our work. The proposed scheme can therefore withstand insider attacks.

14) RESISTS LOST SMART CARD ATTACKS

Suppose SC_i is lost and A somehow obtains it. In our scheme, B_i is not directly stored in SC_i. Moreover, SC_i can protect secret values from unauthorized disclosure [39]. Therefore, A is not able to obtain the information (ω, ID_i, PW_i) stored in SC_i to perform the attacks even if A can obtain SC_i and MD_i at the same time. Hence, our work is free from lost smart card attacks.

VI. FORMAL SECURITY VERIFICATION USING AVISPA SIMULATION TOOL

We provide security verification of the proposed scheme using the widely accepted AVISPA tool, which was frequently used in a lot of relevant works [31], [42], [54]. Unlike RoR model and BAN logic, AVISPA is a push-button software for the automated validation of cryptographic protocols and applications. Specifically, it is employed to formally verify the resilience of the protocols to replay attacks and MITM attacks, based on predetermined goals. The tool executes a simulation specified by the High-Level Protocol Specification Language (HLPSL) [55]. In our simulation, Security Protocol Animator (SPAN) is integrated with AVISPA tool, which helps to interactively build message sequence charts of the protocol execution. The AVIPSA tool includes four backends: On-the-fly Model-Checker (OFMC), Constraint Logic based Attack Searcher (CL-AtSe), SAT-based ModelChecker (SATMC) and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). At present, both SATMC and TA4SP back-ends do not support algebraic properties of modular exponentiation and XOR operator, which are required in the proposed scheme. We therefore only report the simulation results under OFMC and CL-AtSe backends. The OFMC backend can be employed not only for efficient falsification of protocols, but also for verification for a bounded number of sessions, without bounding the messages an intruder can generate. Whereas in the CL-AtSe approach, each protocol step is modeled by constraints on the intruder's knowledge (server's public key, intruder's own keys, etc.).

Consistent with the construction of the proposed scheme, we include two main roles in the simulation: User U and E-Health Server S. Each role is fully specified using HLPSL codes. Since including the codes within the text is too cumbersome, only some important notations and operations are provided as follows. "*Trust*" is a symmetric key used to enable the communication in a trusted channel at the registration stage. "*REncrypt*" is specified as a public key (of Rabin cryptosystem) used by U to compute the message Z in the login phase. In the authentication phase, S uses the corresponding private key "*inv*(*REncrypt*)" to decrypt the message and verifies the login request. The decryption using "*inv*(*REncrypt*)" is an operation automatically executed by the tool. We define "*Gkj*" as the group key that is securely distributed by S. Suppose there are three users using a group service provided by S, the parameters $[x_1, x_2, \ldots, x_u]$ in M_{sg2} are simulated using "$X1$", "$X2$" and "$X3$". These parameters are then sent to U for group key calculation. Note that based on requirement of the HLPSL, the first letter of each parameter in the specification of main roles must be capitalized. In addition, since the language only supports concatenation, XOR and exponentiation, the mathematical operators including subtraction, addition, multiplication and division in the scheme are defined as hash functions in the simulation.

Other than two basic roles U and S, roles *session* and *environment* are also required by the tool. Specifically, the role *session* indicates all components used in a single communication session, including cryptographic keys (e.g., *Trust*, *REncrypt*, etc.), communication channel (*Receive* and *Send* channels between U and S), mathematical operators, main roles (U and S), etc. The role *environment* specifies specific sessions that we want to simulate in the tool, where the intruder impersonates U or S. For this purpose, an extra role named *intruder* denoted by "*i*" is included in the specification. The intruder "*i*" is also assigned with its own keys (symmetric key *kui*, public asymmetric key *ki*, and private asymmetric key *inv*(*ki*)), so that it can carry out possible attacks on the simulated scheme. In the role *environment*, all letters of each parameter are written in lower case.

AVISPA tool simulates the protocols with two kinds of goals, namely, secrecy goal and authentication goal. The former one is to preserve the secret parameters and registered credentials. The latter one is to verify if the newly generated parameters in the login and authentication phase are truly sent by legitimate parties. Following this, six secrecy goals considered for the verification of our scheme are described as follows.

1) "*sj*": is the secret symmetric key of the server, and it is kept secret to S only.
2) "*w*": represents parameter ω in the scheme (since the tool does not support this symbol), which is generated in the registration phase. It is kept secret to U only.
3) "*idi*": is the identity of U, which is kept secret to U and S. This goal is to enable the user privacy in our scheme.
4) "*pwi*": is the user password, which is a secret known by U only.
5) "*bi*": is the user biometrics, and it is kept secret to U only.
6) "*kij*": is the secret value computed by both U and S. It is kept secret to them only and is used for securely distributing the group key.

We also consider three authentication goals between U and S, which are specified in the following.

1) "*m*": is a random value selected by U in the login phase. It should be authenticated to be sent by a legitimate user.
2) "*ti*": is a timestamp generated by U, which is not identical in every communication session. Its validity should be authenticated by S.
3) "*tj*": is a timestamp generated by S. U should ensure that this parameter is sent by a legitimate server.

After executing the tool, the results demonstrate the proposed scheme has passed the AVISPA verification under

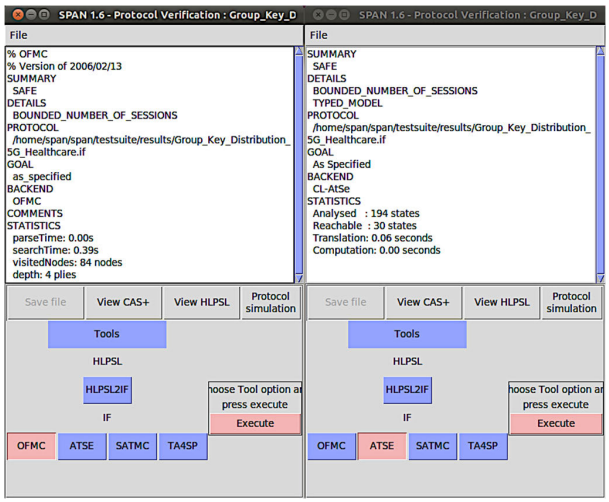

FIGURE 3. Verification results of OFMC and CL-AtSe backends.

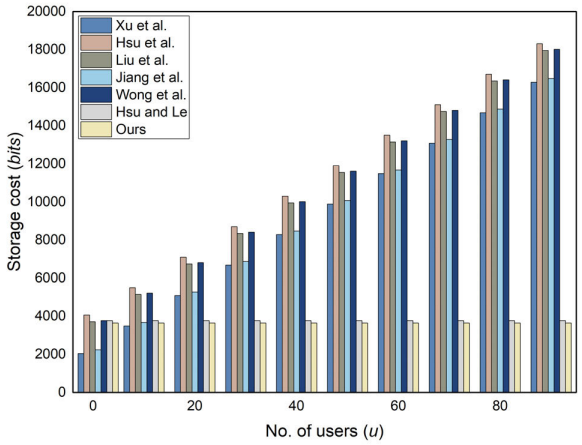

FIGURE 4. Storage costs of different schemes.

OFMC and CL-AtSe backends, as shown in Figure 3. The stated secrecy and authentication goals are satisfied for the specified sessions. Thus, the proposed scheme is safe against relay attacks and MITM attacks.

VII. PERFORMANCE ANALYSIS

We evaluate the performance of our work and compare it with the predecessor schemes in terms of functions, communication cost, storage cost, and computation cost.

A. FUNCTIONS

In Table 4, we provide the comparison results on functions of our scheme and some relevant schemes discussed in Section I-A. We use symbol $\surd$ to denote that the scheme achieves the specific function. Also, symbol $\times$ denotes that the function is not achieved by the scheme. It is observed that our work provides the most functional scheme compared with the competitive ones. In particular, only the proposed work supports secure group communications in 5G healthcare environments. Group key distribution mechanism with three-factor authentication is only introduced in ours and Hsu and Le [49]'s schemes.

TABLE 5. Comparison on communication cost.

Schemes	Total rounds	Total cost (bits) of a single user and servers
Xu *et al.* [38]	$3u + \frac{u!}{(u-2)!}$	$1344 + \frac{160u!}{(u-2)!}$
Hsu *et al.* [39]	$2u + \frac{u!}{(u-2)!}$	$1344 + \frac{160u!}{(u-2)!}$
Liu *et al.* [40]	$3u + \frac{u!}{(u-2)!}$	$2912 + \frac{160u!}{(u-2)!}$
Jiang *et al.* [41]	$2uv + \frac{v.u!}{(u-2)!}$	$1152v + \frac{160v.u!}{(u-2)!}$
Wong *et al.* [42]	$2u + \frac{u!}{(u-2)!}$	$1344 + \frac{160u!}{(u-2)!}$
Hsu and Le [49]	$2u$	$1312 + 160u$
Ours	$2u$	$1280 + 160u$

u: no. of users, v: no. of servers.

B. COMMUNICATION COST

In this subsection, comparison on communication cost of different schemes is considered based on the total communication rounds and the length of communicated messages. Since the schemes proposed by [34]–[37] were not designed with the center-less authentication, they are not included in this comparison. For a strong security, we assume the length of asymmetric encryptions/decryptions (for instance Rabin cryptosystem) is 1024 bits. Symmetric encryption/decryptions have the block length of 256 bits. The identities, passwords and biometrics have the same length of 128 bits. 160 bits is the length of the random numbers and hash values. In addition, elliptic curve point multiplications and time timestamps are with the length of 320 bits and 32bits respectively. Unlike in our and Hsu and Le [49]'s schemes, in order to achieve the group communication feature, users in the other schemes are assumed to communicate with each other in the groups of two. This assumption is consistent with the support of D2D communications in the proposed 5G-enabled environments. In this way, a user can share the session key to all remaining users for achieving the group services. For example, in Wong *et al.* [42]'s scheme, the number of communication rounds in the scheme is $2u$. The users need additional $2C_2^u = 2\frac{u!}{2!(u-2)!} = \frac{u!}{(u-2)!}$ rounds for the D2D communication. Therefore, the total rounds are $2u + \frac{u!}{(u-2)!}$. The corresponding communication cost is $1344 + \frac{160u!}{(u-2)!}$, in which each session key is a hash value. Following this, communication costs of Liu *et al.* [40], Hsu *et al.* [39] and Xu *et al.* [38] are $2912 + \frac{160u!}{(u-2)!}$, $1344 + \frac{160u!}{(u-2)!}$ and $1344 + \frac{160u!}{(u-2)!}$, respectively. Since Jiang *et al.* did not design their scheme with multi-server architecture, computation result of its cost is $1152v + \frac{160v.u!}{(u-2)!}$. Whereas with group key distribution property, our and Hsu and Le [49]'s schemes only bear the costs of $1280 + 160u$ and $1312 + 160u$, respectively. Table 5 specifically tabulates the comparison results. It is easily observed that when u and v gradually increase, our scheme achieves the most efficient communication compared with the others.

C. STORAGE COST

Storage costs of different schemes are calculated based on the parameters provided in Section VII-B. We consider the

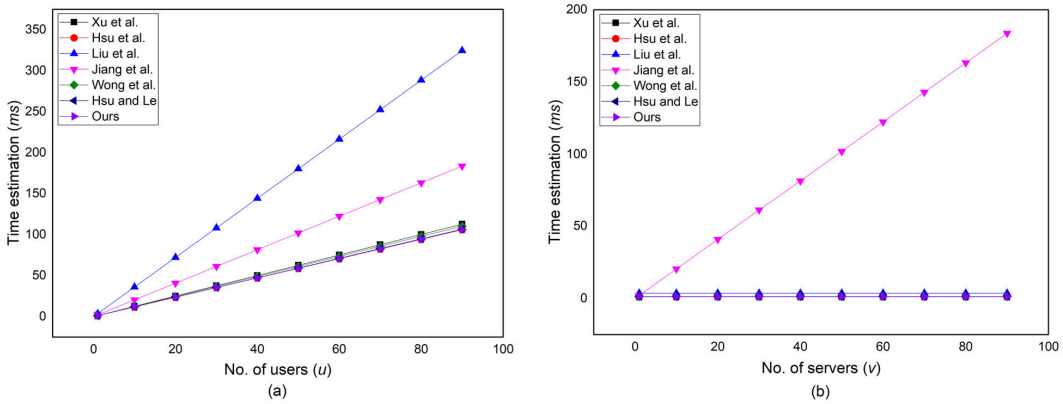

FIGURE 5. Computation cost of different schemes in two scenarios: a) a single server provides service for multiple users; and b) a single user receives services provided by multiple servers.

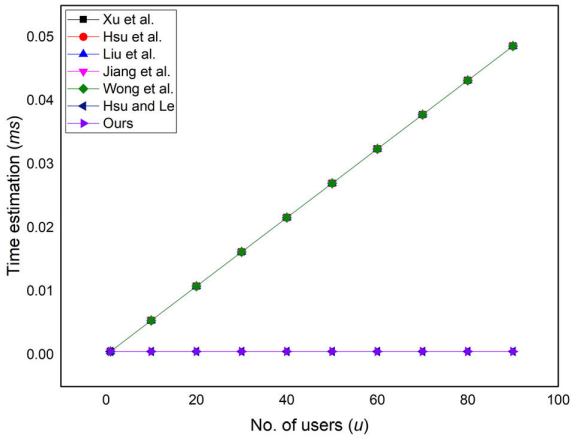

FIGURE 6. Additional computation costs of different schemes for a specific healthcare application.

TABLE 6. Comparison on storage cost.

Schemes	User side (bits)	Server side (bits)
Xu *et al.* [38]	$480 + 160u$	1408
Hsu *et al.* [39]	$1952 + 160u$	1952
Liu *et al.* [40]	$1216 + 160u$	2336
Jiang *et al.* [41]	$1120 + 160u$	960
Wong *et al.* [42]	$1952 + 160u$	1664
Hsu and Le [49]	1952	1824
Ours	1824	1824

u: no. of users.

storage for the parameters stored by the user and the server in the system initialization phase and registration phase. In addition, consistent with the scenario specified in Section VII-B, the users have to temporarily store the shared session keys received from the D2D communications. Therefore, an extra cost of the temporary storage is included for the user side. The costs will drastically increase when massive users simultaneously login to the system. Whereas, in our and [49]'s schemes, the users do not need to share and store the session keys due to the group key property. Table 6 tabulates the comparison on the storage cost of different schemes. The comparison results are also depicted in Figure 4. We can see that the proposed scheme bears the least storage cost when u increases, compared with the other schemes. Our work is even more efficient in the SSO-enabled multi-server environments.

TABLE 7. Notations used in the analysis on computation cost.

Notations	Description
T_{PM}	Time of computing an elliptic curve point multiplication
T_{SED}	Time of computing a symmetric encryption/decryption
T_H	Time of computing a hash function
T_{FE}	Time of computing a fuzzy extractor operation
T_{PA}	Time of computing an elliptic curve point addition
T_{SM}	Time of computing a scalar multiplication
T_M	Time of computing a modular squaring
T_{QR}	Time of computing a square root modulo N

D. COMPUTATION COST

This subsection provides the comparison of our work with the others in terms of computation cost. Table 7 provides the notations we use in this analysis. Since XOR operations consume a negligible computation cost [39], we do not include it in the time estimation. In Table 8, we present the results of this comparison for the single user and server in specific schemes. We also use the setting of [39] to do some experiments on the schemes. Based on the data retrieved from Table 8, we depict the results of the experiments in Figure 5 with two different scenarios. In Figure 5a, a single server provides service for multiple users. Figure 5b shows the scenario that a single user receives services provided by multiple servers. Since the cost difference of most schemes is not big (except Liu *et al.* [40]'s and Jiang *et al.* [41]'s schemes), the figures appear with superimposed plot lines. The cost of Jiang *et al.* [41]'s scheme drastically increases in direct proportion to the number of servers (as shown in Figure 5b), since multi-server architecture is not available in their work. In both scenarios, we can observe that the proposed work is the most efficient scheme when the numbers of users and serves gradually increase.

Furthermore, we discuss an additional computation cost when applying all schemes in a specific healthcare application. Employing the group key distribution scheme, the server only needs to use a single group session

TABLE 8. Comparison on computation cost.

Schemes	Time estimation of U_i	Time estimation of S_j
Xu *et al.* [38]	$3T_{SM} + 9T_H$ $\approx 0.62721ms$	$3T_{SM} + 6T_H$ $\approx 0.62514ms$
Hsu *et al.* [39]	$T_M + T_{SED} + 6T_H$ $\approx 0.00537ms$	$T_{QR} + 2T_{SED} + 3T_H$ $\approx 1.17215ms$
Liu *et al.* [40]	$T_{FE} + 3T_{PM} + 4T_H$ $\approx 2.03476ms$	$3T_{PM} + 3T_H + 4T_{PA}$ $\approx 1.5723ms$
Jiang *et al.* [41]	$2T_{PM} + 2T_{SED} + 6T_H$ $\approx 1.02122ms$	$2T_{PM} + 2T_{SED} + 4T_H$ $\approx 1.01984ms$
Wong *et al.* [42]	$T_M + T_{SED} + 7T_H$ $\approx 0.04953ms$	$T_{QR} + 2T_{SED} + 7T_H$ $\approx 1.17491ms$
Hsu and Le [49]	$T_M + T_{SED} + 12T_H$ $\approx 0.00951ms$	$T_{QR} + 2T_{SED} + 9T_H$ $\approx 1.17629ms$
Ours	$T_M + T_{SED} + 9T_H$ $\approx 0.00744ms$	$T_{QR} + 2T_{SED} + 5T_H$ $\approx 1.17353ms$

According to [39]: $T_{PM} \approx T_{FE} \approx 0.508ms$, $T_{SED} \approx 0.00054ms$, $T_M \approx T_H \approx 0.00069ms$, $T_{PA} \approx 0.0069ms$, $T_{SM} \approx 0.207ms$, and $T_{QR} \approx 1.169ms$.

key to encrypt the health data once. Therefore, it significantly reduces the cost. Since our scheme provides this mechanism, the additional cost should only be $0.00054ms$, in which a single server provides the services for multiple users of a healthcare group. In case of using a key agreement scheme for this service, the server has to encrypt the data multiple times for the corresponding multiple users. For example, in Wong *et al.* [42], the cost will be $0.00054u\ ms$. In this way, we can determine the costs of all remaining schemes. Figure 6 depicts the comparison result, which shows that computation in our and Hsu and Le [49]'s schemes is the most efficient.

VIII. CONCLUSION

E-health systems enabled with 5G network architecture provide fast and seamless access to patient's data, thus achieving rapid medical analysis reports for groups of the patients. However, security and privacy are prominent concerns in the systems. In this paper, we have proposed an anonymous key distribution scheme for group healthcare services in 5G-enabled multi-server environments with SSO solution. The proposed scheme with secure three-factor authentication and user anonymity is a good fit to the group communications in 5G architecture environments for various healthcare domains. We achieve a solid security proof of the proposed scheme using the RoR model, BAN logic and AVISPA simulation. Our work is demonstrated to withstand various well-known security attacks. Compared with the related works, the proposed scheme is the most functional one and bears the least cost.

In future works, access control to the health data for the groups with specific attributes will be considered. We would also consider integrating e-health systems with a consortium blockchain architecture, in the scenarios of collaborative healthcare programs between multiple providers. The solution can help to preserve the integrity of some sensitive data.

ACKNOWLEDGMENT

The authors would like to thank anonymous referees for their constructive suggestions.

REFERENCES

[1] J. Cao, P. Yu, M. Ma, and W. Gao, "Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1561–1575, Apr. 2019.

[2] C. Saha and H. Dhillon, "Millimeter wave integrated access and backhaul in 5G: Performance analysis and design insights," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 12, pp. 2669–2684, Dec. 2019.

[3] A. Ahad, M. Tahir, and K.-L.-A. Yau, "5G-based smart healthcare network: Architecture, taxonomy, challenges and future research directions," *IEEE Access*, vol. 7, pp. 100747–100762, 2019.

[4] P. K. Barik, C. Singhal, and R. Datta, "An efficient data transmission scheme through 5G D2D-enabled relays in wireless sensor networks," *Comput. Commun.*, vol. 168, pp. 102–113, Feb. 2021.

[5] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, May 2014.

[6] R. Chevillon, G. Andrieux, and J.-F. Diouris, "Energy optimization of D2D communications using relay devices and data entropy," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[7] W. Li, Q. Zhang, Q. Zhang, F. Guo, S. Qiao, S. Liu, Y. Luo, Y. Niu, and X. Heng, "Development of a distributed hybrid seismic–electrical data acquisition system based on the narrowband Internet of Things (NB-IoT) technology," *Geosci. Instrum., Methods Data Syst.*, vol. 8, no. 2, pp. 177–186, Aug. 2019.

[8] D. A. Raj and S. Kayalvizhi, "NB-IoT based water meter," *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 635–637, 2019.

[9] A. Israr, Q. Yang, W. Li, and A. Y. Zomaya, "Renewable energy powered sustainable 5G network infrastructure: Opportunities, challenges and perspectives," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102910.

[10] Z. Liu, Z. Dai, P. Yu, Q. Jin, H. Du, Z. Chu, and D. Wu, "Intelligent station area recognition technology based on NB-IoT and SVM," in *Proc. IEEE 28th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2019, pp. 1827–1832.

[11] M. Praveen and V. Harini, "NB-IoT based smart car parking system," in *Proc. Int. Conf. Smart Struct. Syst. (ICSSS)*, Mar. 2019, pp. 1–5.

[12] H. N. Qureshi, M. Manalastas, S. M. A. Zaidi, A. Imran, and M. O. Al Kalaa, "Service level agreements for 5G and beyond: Overview, challenges and enablers of 5G-healthcare systems," *IEEE Access*, vol. 9, pp. 1044–1061, 2021.

[13] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet Things J.*, early access, Nov. 30, 2020, doi: 10.1109/JIOT.2020.3041042.

[14] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Inf. Sci.*, vol. 527, pp. 493–510, Jul. 2020.

[15] Y. Zhang, G. Chen, H. Du, X. Yuan, M. Kadoch, and M. Cheriet, "Real-time remote health monitoring system driven by 5G MEC-IoT," *Electronics*, vol. 9, no. 11, p. 1753, Oct. 2020.

[16] A. Kumar, M. A. Albreem, M. Gupta, M. H. Alsharif, and S. Kim, "Future 5G network based smart hospitals: Hybrid detection technique for latency improvement," *IEEE Access*, vol. 8, pp. 153240–153249, 2020.

[17] K. Karako, P. Song, Y. Chen, and W. Tang, "Realizing 5G- and AI-based doctor-to-doctor remote diagnosis: Opportunities, challenges, and prospects," *BioSci. Trends*, vol. 14, no. 5, pp. 314–317, 2020.

[18] D. Li, "5G and intelligence medicine—How the next generation of wireless technology will reconstruct healthcare?" *Precis. Clin. Med.*, vol. 2, no. 4, pp. 205–208, Dec. 2019.

[19] L. Haoyu, L. Jianxing, N. Arunkumar, A. F. Hussein, and M. M. Jaber, "An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability," *Future Gener. Comput. Syst.*, vol. 98, pp. 69–77, Sep. 2019.

[20] K. Sowjanya, M. Dasgupta, and S. Ray, "Elliptic curve cryptography based authentication scheme for Internet of medical things," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102761.

[21] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T. Qiu, and R. Y. K. Kwok, "Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 463–478, Feb. 2021.

[22] C. Jujjavarapu, J. Anandasakaran, L. M. Amendola, C. Haas, E. Zampino, N. B. Henrikson, G. P. Jarvik, and S. D. Mooney, "ShareDNA: A smartphone app to facilitate family communication of genetic results," *BMC Med. Genomics*, vol. 14, no. 1, p. 10, Dec. 2021.

[23] Y. M. Ortiz, M. Suárez-Villa, and M. Y. Expósito, "Importance and recognition of the family in health care: A reflection for nursing," *Nursing Care Open Access J.*, vol. 3, pp. 307–309, Oct. 2017.
[24] C. G. N. Voorend, N. C. Berkhout-Byrne, Y. Meuleman, S. P. Mooijaart, W. J. W. Bos, and M. van Buren, "Perspectives and experiences of patients and healthcare professionals with geriatric assessment in chronic kidney disease: A qualitative study," *BMC Nephrol.*, vol. 22, no. 1, p. 9, Dec. 2021.
[25] S. Marlow, T. Bisbey, C. Lacerenza, and E. Salas, "Performance measures for health care teams: A review," *Small Group Res.*, vol. 49, no. 3, pp. 306–356, Jun. 2018.
[26] Z. Ezziane, M. Maruthappu, L. Gawn, E. A. Thompson, T. Athanasiou, and O. J. Warren, "Building effective clinical teams in healthcare," *J. Health Org. Manage.*, vol. 26, no. 4, pp. 428–436, Aug. 2012.
[27] K. Sowjanya and M. Dasgupta, "A ciphertext-policy attribute based encryption scheme for wireless body area networks based on ECC," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102559.
[28] R. P. Singh, M. Javaid, A. Haleem, R. Vaishya, and S. R. Ali, "Internet of medical things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," *J. Clin. Orthopaedics Trauma*, vol. 11, no. 4, pp. 713–717, 2020.
[29] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *J. Med. Syst.*, vol. 43, no. 10, p. 320, Oct. 2019.
[30] N. A. Azeez and C. V. der Vyver, "Security and privacy issues in E-health cloud-based system: A comprehensive content analysis," *Egyptian Informat. J.*, vol. 20, no. 2, pp. 97–108, Jul. 2019.
[31] C.-L. Hsu, T.-V. Le, C.-F. Lu, T.-W. Lin, and T.-H. Chuang, "A privacy-preserved E2E authenticated key exchange protocol for multi-server architecture in edge computing networks," *IEEE Access*, vol. 8, pp. 40791–40808, 2020.
[32] A. Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar, and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *J. Inf. Secur. Appl.*, vol. 51, Apr. 2020, Art. no. 102443.
[33] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12557–12574, 2019.
[34] P. Q. W. Z. Jiang Wen Li Jin and H. Zhang, "An anonymous and efficient remote biometrics user authentication scheme in a multi server environment," *Frontiers Comput. Sci.*, vol. 9, no. 1, pp. 142–156, 2015.
[35] V. Odelu, A. Kumar Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.
[36] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 2123, 2016.
[37] M. Qi, J. Chen, and Y. Chen, "A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC," *Comput. Methods Programs Biomed.*, vol. 164, pp. 101–109, Oct. 2018.
[38] D. Xu, J. Chen, and Q. Liu, "Provably secure anonymous three-factor authentication scheme for multi-server environments," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 2, pp. 611–627, 2019.
[39] C.-L. Hsu, T.-V. Le, M.-C. Hsieh, K.-Y. Tsai, C.-F. Lu, and T.-W. Lin, "Three-factor UCSSO scheme with fast authentication and privacy protection for telecare medicine information systems," *IEEE Access*, vol. 8, pp. 196553–196566, 2020.
[40] W. Liu, X. Wang, W. Peng, and Q. Xing, "Center-less single sign-on with privacy-preserving remote biometric-based ID-MAKA scheme for mobile cloud computing services," *IEEE Access*, vol. 7, pp. 137770–137783, 2019.
[41] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for E-health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, Oct. 2016.
[42] A. M.-K. Wong, C.-L. Hsu, T.-V. Le, M.-C. Hsieh, and T.-W. Lin, "Three-factor fast authentication scheme with time bound and user anonymity for multi-server E-health systems in 5G-based wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2511, Apr. 2020.
[43] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for E-Health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.
[44] L. Harn, C. Hsu, and Z. Xia, "Lightweight and flexible key distribution schemes for secure group communications," *Wireless Netw.*, vol. 27, no. 1, pp. 129–136, Jan. 2021.
[45] L. Harn, C. Hsu, and Z. Xia, "Lightweight group key distribution schemes based on pre-shared pairwise keys," *IET Commun.*, vol. 14, no. 13, pp. 2162–2165, Aug. 2020.
[46] R. Jiao, H. Ouyang, Y. Lin, Y. Luo, G. Li, Z. Jiang, and Q. Zheng, "A computation-efficient group key distribution protocol based on a new secret sharing scheme," *Information*, vol. 10, no. 5, p. 175, May 2019.
[47] C. Tselikis, C. Douligeris, L. Maglaras, and S. Mitropoulos, "On the conference key distribution system with user anonymity," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102556.
[48] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.
[49] C.-L. Hsu and T.-V. Le, "A time bound dynamic group key distribution scheme with anonymous three-factor identification for IoT-based multi-server environments," in *Proc. 15th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*, Aug. 2020, pp. 59–65.
[50] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorizations," Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. MIT/LCS/TR-212, 1979.
[51] M. Shuai, L. Xiong, C. Wang, and N. Yu, "A secure authentication scheme with forward secrecy for industrial Internet of Things using rabin cryptosystem," *Comput. Commun.*, vol. 160, pp. 215–227, Jul. 2020.
[52] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, and E. Roback, "Announcing the advanced encryption standard (AES)," National Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. FIPS 197, 2001.
[53] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2884–2895, Aug. 2018.
[54] C.-L. Hsu, W.-X. Chen, and T.-V. Le, "An autonomous log storage management protocol with blockchain mechanism and access control for the Internet of Things," *Sensors*, vol. 20, no. 22, p. 6471, Nov. 2020.
[55] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, 2005, pp. 1–17.

TUAN-VINH LE received the M.S. degree in business administration from the Department of Business Administration, National Formosa University, Taiwan. He is currently pursuing the Ph.D. degree with the Graduate Institute of Business and Management, Chang Gung University, Taiwan. He has some publications in IEEE Access, *Sensor*, and *Journal of Internet Technology*. His research interests include information security, communication system security, applied cryptography, cryptographic protocol, and blockchain. As an international student, he was granted a Full Scholarship for his M.S. degree in business administration from National Formosa University, in 2014, and a Full Scholarship for his Ph.D. degree in business and management from Chang Gung University, in 2016. He was a Session Chair of MD2020 and a Reviewer of IEEE Access.

CHIEN-LUNG HSU (Member, IEEE) received the M.S. and Ph.D. degrees in information management from the National Taiwan University of Science and Technology, in 1997 and 2002, respectively. From August 2009 to May 2012, he was the Director of the Chinese Cryptology and Information Security Association (CCISA), Taiwan. From August 2012 to July 2013, he was a Visiting Scholar with the Department of Electrical Engineering and Computer Science, University of Central Florida, USA. From August 2013 to August 2016, he was the Chair of the Department of Information Management, Chang Gung University, Taiwan. He is currently a joint Professor with the Department of Information Management, Graduate Institute of Business and Management, Chang Gung University. His research interests include smart home, smart healthcare, mobile commerce, computer and communication security, information security, applied cryptography, digital right management, auto identification technology, and user centered service. He received lots of honors, awards, certificates in terms of information security for his research, and has a great number of publications in his research related fields.