

Article

Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks

Alice May-Kuen Wong ¹, Chien-Lung Hsu ^{2,3,4,5,6,*}, Tuan-Vinh Le ² , Mei-Chen Hsieh ³ and Tzu-Wei Lin ²

¹ Department of Physical Medicine and Rehabilitation, Chang Gung Memorial Hospital, Taoyuan 33302, Taiwan; walice@adm.cgmh.org.tw

² Graduate Institute of Business and Management, Chang Gung University, Taoyuan 33302, Taiwan; tvle.cgu@gmail.com (T.-V.L.); d0640001@cgu.edu.tw (T.-W.L.)

³ Department of Information Management, Chang Gung University, Taoyuan 33302, Taiwan; meichen966@gmail.com

⁴ Healthy Aging Research Center, Chang Gung University, Taoyuan 33302, Taiwan

⁵ Department of Visual Communication Design, Ming Chi University of Technology, New Taipei 24301, Taiwan

⁶ Department of Nursing, Taoyuan Chang Gung Memorial Hospital, Taoyuan 33302, Taiwan

* Correspondence: clhsu@mail.cgu.edu.tw

Received: 21 March 2020; Accepted: 25 April 2020; Published: 29 April 2020



Abstract: The fifth generation (5G) mobile network delivers high peak data rates with ultra-low latency and massive network capacity. Wireless sensor network (WSN) in Internet of Thing (IoT) architecture is of prominent use in 5G-enabled applications. The electronic healthcare (e-health) system has gained a lot of research attention since it allows e-health users to store and share data in a convenient way. By the support of 5G technology, healthcare data produced by sensor nodes are transited in the e-health system with high efficiency and reliability. It helps in reducing the treatment cost, providing efficient services, better analysis reports, and faster access to treatment. However, security and privacy issues become big concerns when the number of sensors and mobile devices is increasing. Moreover, existing single-server architecture requires to store a massive number of identities and passwords, which causes a significant database cost. In this paper, we propose a three-factor fast authentication scheme with time bound and user anonymity for multi-server e-health systems in 5G-based wireless sensor networks. In our work, the three-factor authentication scheme integrating biometrics, password, and smart card ensures a high-security sensor-enabled environment for communicating parties. User anonymity is preserved during communication process. Besides, time bound authentication can be applied to various healthcare scenarios to enhance security. The proposed protocol includes fast authentication, which can provide a fast communication for participating parties. Our protocol is also designed with multi-server architecture to simplify network load and significantly save database cost. Furthermore, security proof and performance analysis results show that our proposed protocol can resist various attacks and bear a rational communication cost.

Keywords: 5G-based WSN; biometrics; multi-server; privacy protection; time bound

1. Introduction

The fifth generation (5G) mobile network is wireless communication technology supporting two-tier heterogeneous cellular networks (HetNets) with integrated access and backhaul (IAB).

As shown in Figure 1, the macro base stations (MBSs) in 5G architecture provide mm-wave backhaul to the small cell base stations (SBSs). Besides, the devices can access both MBSs and SBSs through direction communications [1–3]. 5G-enabled devices can also directly communicate with each other. Thus, 5G technology delivers high peak data rates with ultra-low latency and massive network capacity. The Narrow-Band Internet of Things (NB-IoT) system provides low power consumption, wide coverage, low cost, and large capacity, which are essential properties for 5G network [4]. Wireless sensor networks (WSNs) are a key technological building block of IoT, where each object (virtual or physical) can be sensed, identified, accessed, and interconnected via the Internet within a dynamic ubiquitous network [5,6]. WSN applications in distributed IoT architecture can be seen in various domains, such as healthcare [7–9], energy [10,11], industrial data acquisition and transmission system [12], mushroom humidity monitoring system [13], intelligent manhole cover monitoring system [14], intelligent station area recognition technology [15], smart car parking system [16], and so on.

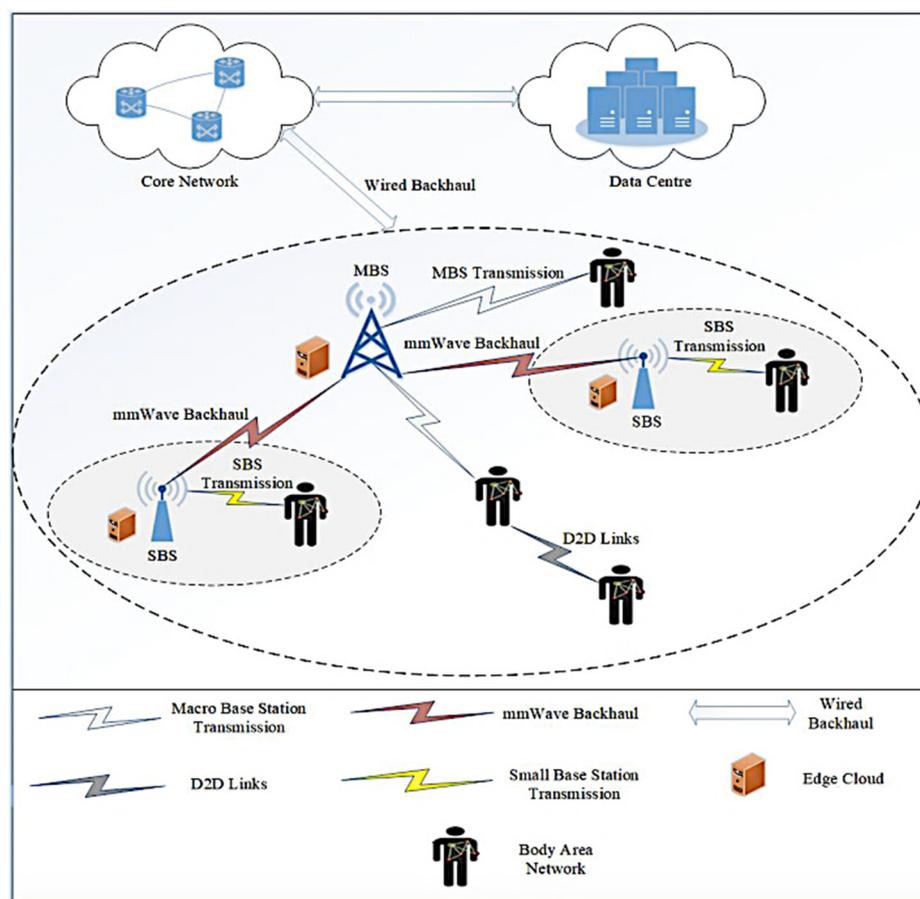


Figure 1. An overview of 5G-based smart healthcare architecture [1].

The use of IoT in electronic healthcare (e-health) management systems has attracted more and more attention because of its convenience, in which healthcare data are flexibly stored and shared among participating parties. Such a system is called IoMT (Internet of Medical Things) [17–19]. IoMT consists of various entities including healthcare centers, emergency centers, medical devices, and e-health users (including patients, physicians, pharmacists, medical researchers, etc.). A Wireless Body Area Network (WBAN) is composed by sensor/actuators nodes and hubs that operates in, on, or around a body (but not limited to human bodies) and supports a variety of medical and non-medical applications [20]. The 5G wireless system aims to support WBAN by increasing the interconnectivity of electronic devices [21].

In e-health systems enabled with 5G-based WSNs, users communicate with servers through a public channel; therefore, their information could be vulnerable to certain attacks, such as man-in-the-middle attack [22], replay attack [23], or impersonation attack [24]. User privacy is also a big issue, where sensitive information of the user may be revealed to the public during communication process. Additionally, existing authentication protocols are not consistent with certain scenarios in healthcare domains, for instance, medical examination appointment, since they were not designed with a time-based mechanism. In addition, most existing authentication protocols were designed with two-factor mechanism, which suffers from security risks when the attacker has obtained the password and smart card of the user. Furthermore, as the number of servers has increased remarkably to provide more services for the end user [25], a single-server architecture is unable to meet the needs of users. More registered servers will lead to more identities and passwords that the user must remember, which causes considerable database cost. Moreover, it is not secure for the users to use the same set of identities and passwords to register with different servers.

1.1. Main Contributions

To prevent an adversary from carrying out potential attacks, it is essential to design a robust authentication mechanism. In this paper, we propose a three-factor fast authentication scheme with time bound and user anonymity for multi-server e-health systems in 5G-based wireless sensor networks. Our scheme introduces three-factor authentication to address security issues of traditional authentications in e-health system. By means of the authentication protocol, the users must register with healthcare providers via a secure channel. After that, the users and the servers mutually authenticate and compute shared session keys via a public channel. Finally, the users can use these shared keys to get access to specific healthcare services. The contributions of our work can be summarized as follows.

- Three-factor authentication in the proposed protocol combines biometrics, password, and smart card for providing a high-security and privacy-preserving communication environment.
- Time-bound authentication helps in controlling user access, protecting sensitive information, and can be applied to many scenarios in healthcare such as access control to the users in WBANs, medical channel subscription, medical examination appointment, etc.
- Our work designs fast authentication to speed up the communication process.
- Our scheme is designed with multi-server architecture, which allows users to use a single password to obtain services from multiple servers. This advantage can simplify network workload and save a significant database cost.

1.2. Structure of the Paper

The rest of the paper is organized as follows. We present the literature review in Section 2. We briefly review Zhang et al.'s scheme [26] in Section 3. We describe system and security model in Section 4. We propose a three-factor authentication protocol with time bound and user anonymity for e-health systems in wireless body sensor networks in Section 5. Section 6 presents logical analysis of the proposed scheme using GNY logic. Section 7 presents verification proof of the proposed scheme using AVISPA tool. Section 8 presents semantic security analysis of our work. We present performance analysis of the proposed scheme in comparison with related works in Section 9. Section 10 presents implementation of the proposed scheme. Finally, some conclusions are given in Section 11.

2. Related Works

Today, the number of medical devices is increasing, making security problem in e-health cloud-based system more prominent. The associated security and privacy problems of the IoMT were presented in [27,28]. Besides, security and privacy issues in WSN for health and the environment have been addressed in several reviews [29–31] and surveys [32–34]. Among the recently proposed

cryptographic schemes for e-health systems, secure three-factor authentication mechanism [35–37] combining biometrics, password and smart card has recently attracted much attention.

Fan and Lin [38] proposed a three-factor authentication scheme based on biometrics. Their scheme can preserve the privacy of the biometric data of every user. Besides, Fan and Lin demonstrated the completeness of their proposed scheme with formal security analysis. Nevertheless, Fan and Lin's scheme is susceptible to many well-known attacks, such as stolen-verifier attack, online password guessing attack, modification attack, impersonation attack, man-in-the-middle (MITM) attack, stolen smart card attack, desynchronization attack, and denial of service (DoS) attack. Moreover, Fan and Lin's scheme cannot achieve user untraceability and requires a biometric data storage. Jiang et al. [39] proposed a robust privacy-preserving three-factor authentication protocol for e-health clouds. Remedying drawbacks in the predecessor scheme, Jiang et al. claimed that their proposed scheme can withstand various known attacks and provide more security features. However, we found that Jiang et al.'s scheme cannot resist replay attack, stolen smart card attack, desynchronization attack, and DoS attack. Recently, Zhang et al. [26] designed a dynamic authentication and three-factor key agreement with privacy protection for e-health. Although Zhang et al. stated that their scheme resists various well-known attacks, we found that Zhang et al.'s protocol is still vulnerable to DoS attack. Besides, Zhang et al.'s scheme suffers from storage burden of storing biometric data.

3. Review of Zhang et al.'s Scheme

Zhang et al. [26] designed a dynamic authentication and three-factor key agreement for the user and the server with privacy protection. Besides, the exact value of the biometric template remains unknown to the server. However, their scheme was found to have certain weaknesses. In this section, we present a brief review of Zhang et al.'s scheme and analyze its weaknesses.

3.1. Registration Phase

1. The user U_i first enters his/her identity ID_i , password PW_i , and biometric template B_i , and then generates a random number string r . Next, the user U_i computes $C_1 = h(ID_i || PW_i || h_{Bio}(B_i))$ and $C_2 = B_i \oplus r$. The user U_i then transmits (C_1, C_2) as a registration request to the server via a secure channel.
2. After receiving (C_1, C_2) , the server S uses private key k and C_2 to compute $M = h(h_{Bio}(C_2) || k)$. Then, the server S generates a random number string v , chooses $W_0 = \text{NULL}$, and calculates $W = h(h_{Bio}(C_2 \oplus v))$, $X = h(ID_{SC} || C_1 || M) \oplus v$ and $Y = M \oplus C_1$. The server S then stores $\{C_2, W_0, W\}$ in database, and writes $(ID_{SC}, h(\cdot), h_{Bio}(\cdot), X, Y)$ into smart card. After that, the server S sends the smart card to the user U_i via a secure channel.
3. After receiving smart card from the server, the user U_i computes $Z = r \oplus h_{Bio}(B_i)$. Finally, the user U_i stores Z in the smart card.

3.2. Login and Authentication Phase

1. The user U_i uses ID_i, PW_i, B_i , and smart card to login to the server S , and then generates a random number string u . After that, the user U_i calculates $C_1^* = h(ID_i || PW_i || h_{Bio}(B_i))$, $M^* = Y \oplus C_1^*$, $v^* = X \oplus h(ID_{SC} || C_1^* || M^*)$, $r^* = Z \oplus h_{Bio}(B_i)$, $C_3 = h_{Bio}(B_i \oplus r^* \oplus v^*)$, $C_4 = B_i \oplus r^* \oplus h(M^* || u)$, and $C_5 = u \oplus h_{Bio}(B_i \oplus r^*)$. Then, the user U_i transmits (C_3, C_4, C_5) to the server S .
2. The server S computes $W^* = h(C_3)$. After that, the server S searches W^* in the dynamic verification table and obtains C_2 . Otherwise, the medical server continues to search the column "dynamic string (W^0)" to see if a value is equal to W^* . If there is a match, the server S extracts the corresponding value C_2 and replaces W with the value of W^0 . Otherwise, the medical server S rejects the login request. Next, the server S generates random number string β and calculates $M' = h(h_{Bio}(C_2 || k))$, $u^* = C_5 \oplus h_{Bio}(C_2)$, and $B_i \oplus r^* = C_4 \oplus h(M' || u^*)$. Then, the server S checks if $B_i \oplus r^*$ and C_2 are within a bearable threshold [40], then computes $C_6 = \beta \oplus h(B_i \oplus r^*)$ and $C_7 = h((B_i \oplus r^*) || u^* || \beta)$. Next, the server S transmits (C_6, C_7) to the user U_i .

3. After receiving (C_6, C_7) , the user U_i computes $\beta_* = C_6 \oplus h(B_i \oplus r^*)$. Next, the user U_i checks if C_7 is equal to $h((B_i \oplus r^*) || u || \beta_*)$. If there is a match, the user U_i compute $C_8 = h(h_{Bio}(B_i \oplus r^* \oplus \beta_*) \oplus \beta_*)$, $X_{new} = h(IDSC || C_1^* || M^*) \oplus \beta_*$, and session key $SK = h(M^* || u || \beta_*)$. Thereafter, the user U_i transmits C_8 to server S .
4. After receiving C_8 , the server S compares C_8 with $h(h_{Bio}(B_i \oplus r^* \oplus \beta) \oplus \beta)$. If there is a match, the server S accepts $SK = h(M^* || u^* || \beta)$ as the session key. Next, the server S computes $W_{new} = h(h_{Bio}(C_2 \oplus \beta))$. Then, the server S replaces (W_0, W) by (W, W_{new}) and calculates $C_9 = h(SK || \beta)$. Then, the server S transmits C_9 to user U_i .
5. After receiving C_9 , the user U_i compares C_9 with $h(SK || \beta^*)$. If there is a match, the user U_i accepts SK as the session key. Finally, the user U_i replaces X by X_{new} in the smart card for the next login.

3.3. The Weaknesses

- Suffers from denial of service (DoS) attack: DoS attack is carried out by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users [41]. In this case, timestamp solution is employed to verify the validity of the message. Without the timestamp included in login request message (C_3, C_4, C_5) , Zhang et al.'s scheme is vulnerable to DOS attack.
- Suffers from a burden of biometric storage: The authentication based on biometric template requires a storage for storing biometric data. This additional storage does not make Zhang et al.'s scheme unsafe against insider attack since it does not consist of any information about passwords and the real biometric information in the database. However, it results in a significant cost that needs addressing.
- Lacks time-bound based access control: Time-based authentication is a good solution to prove an individual's identity and authenticity on appearance simply by detecting its presence at a scheduled time of day. Lacking this feature in the work, Zhang et al.'s scheme is not well suited for e-health since time bound is useful in many cases, e.g., medical examination appointment.
- Lacks multi-server environment: Multi-server architecture allows user to obtain services from multiple servers using a single password, which greatly saves database cost. Without introducing multi-server architecture, communication in Zhang et al.'s scheme is not prominently efficient.

4. System and Security Model

4.1. System Model

As shown in Figure 2, we propose a system model in which 5G-based smart healthcare network consists of various domains: community care domain, home care domain, and personal care domain. Sensors included in personal care domain are body wearable sensors and biometric sensor-enabled mobile device. They can provide a continuous health monitoring of a person without any constraint on his/her normal daily life activities [42]. Besides, home care domain includes some other sensors such as camera sensor, light sensor, etc. Community care domain includes temperature measuring sensor, sporting equipment, and other IoMT-enabled equipment.

Furthermore, within personal care domains, Wireless Body Sensor Network (WBSN) is a special case of the WBAN where all nodes in the network are sensors [43], which help in remotely collecting patient's health record data (temperature, motion detection, sound, etc.) [31,44–47]. Besides, this patient can use mobile device to collect sensing data produced by his/her body wearable sensors. This monitoring system provides an interesting and widely accepted technology, obtaining special attention because of its friendly services in the smart world. In home care domains, the user may also use this mobile device to access other sensor-enabled devices through SBS transmission, thereby having comprehensive control of their home based on the authority of the home care server. Additionally, in 5G networks, user devices and MBSs can conduct direct transmission for healthcare services as long as they have spectrum opportunities. Furthermore, in community care environments, sensors and

equipment are controlled by healthcare servers through SBSs. Thus, service providers can provide a continuity of care for the users.

In this system model, the user uses his/her mobile device and sensors to communicate with healthcare service provider and obtain specific services. Specifically, the user can login to home care server to query his/her own home care information. Besides, the user is able to upload his/her health data produced from wearable sensors to healthcare server. The user can also control light sensor, monitor sensor, and temperature measuring sensor from various healthcare domains. To accelerate the communication process, we design a fast authentication in the proposed scheme. The proposed scheme allows the communication between the user and the server to be carried out in a secure and privacy-preserved manner. Besides, Figure 2 also shows that our proposed multi-server environment allows the user to login to multiple healthcare service provider servers using a single password, thereby saving significant database cost and improving communication efficiency.

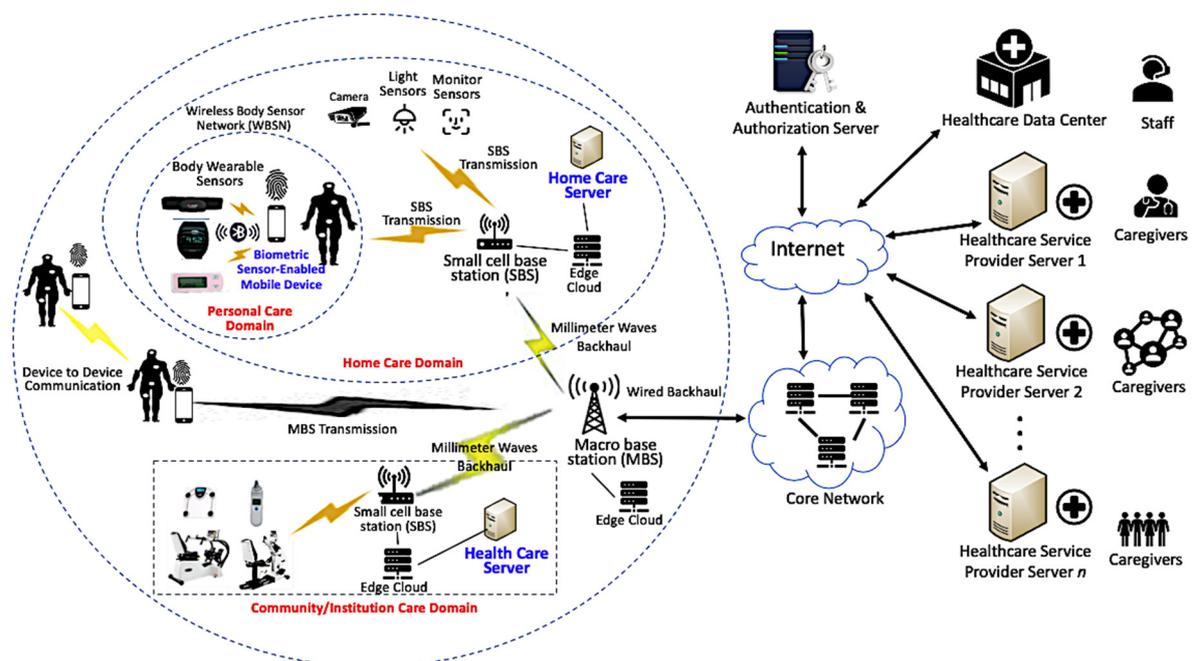


Figure 2. The proposed system model.

4.2. Security Model

Security risks in a public communication channel are common challenge for most of the wireless techniques. Data from the sensors and device in home domain are sensitive information and very likely to be compromised without a robust authentication mechanism. Besides, in home environment, data produced from these sensors are also very important and sensitive. For example, an adversary can impersonate the user to obtain the access to camera sensor, which strongly violates privacy of the user. In addition, in community care domain, sensor-enabled IoMT devices, for instance temperature measuring sensor, are likely vulnerable to security risks. The adversary may provide tampered information to the server after compromising these sensors.

Specifically, various attacks threatening the network access legitimacy are described as follows. *MITM attacks* is when the attacker compromises the transmitted message while the sender and the receiver believe that they are directly communicating with each other. *Impersonation attacks* happen when the attacker has obtained the identity of a user, and then attempts to impersonate him/her. *Replay attacks* let a malicious attacker intercept messages from the last communication session to derive the session key. In addition, the importance of user privacy protection in online communication is

prominent [48–50]. Solving the contradiction between user anonymity and authentication is still a big challenge in this research area.

For the security of the proposed scheme, the following essential requirements should be met to ensure a secure and privacy-preserved communication between the user and the server.

- Mutual authentication: Only the user with valid registered information can be successfully authenticated and is able to compute an exact session key to obtain service provided by the server. On the other hand, the server must be also authenticated as a legitimate party to provide true information for the user.
- Session key establishment: The purpose of this work is to allow the user and the server to securely negotiate a session key for the communication between them.
- User anonymity: We expect privacy of the user can be preserved during communication process.
- Biometric template anonymity: Three-factor mechanism includes biometric template in registration and authentication process. Our purpose is to not allow user's biometric template to be revealed to the public.
- Forward secrecy: Our work aims to prevent the attacker from using information from the past communication session to derive the key.

5. The Proposed Scheme

Our proposed scheme includes two roles: user U_i and server S_j . The purpose of the proposed protocol is to allow the user U_i and the server S_j to compute a shared session key in a secure and privacy-preserved manner. The user U_i first must register with the server S_j as a legitimate party. Next, the user U_i and the user S_j mutually authenticate based on their information, and then compute a session key via a public channel. The authentication process consists of four phases: initialization phase, registration phase, login and initial authentication phase, and fast authentication phase. Table 1 describes notations and cryptographic functions used in this paper.

Table 1. Notations used in the proposed scheme.

Symbols	Description
S_j	Server j
U_i	User i
ID_{S_j}	Identity of server j
ID_i	Identity of user i
PW_i	Password of user i
B_i	Biometric template of user i
x_j	Randomly selected string, the symmetric encryption key of the server S_j
p_j, q_j	Arbitrary big numbers, which are private keys of the server S_j
n_j	$n_j = p_j \cdot q_j$, the public key of the server S_j
σ, v	Randomly generated strings
b	Randomly generated value
T_1, T_2	Timestamp
t_1, t_2	Time bound
sk_{ij}	Session key established by the user and the server
$h(\cdot)$	One-way hash function
\oplus	Exclusive OR function
$SE(), SD()$	Symmetric encryption, decryption
$AD()$	Asymmetric decryption
$\square_{smart\ card}$	Store information into smartcard
\square_{usb}	Store information into USB

5.1. Initialization Phase

Our work employs Rabin cryptosystem [51], encryption process of which is extremely fast and easy (as long as encryption does not require computing a Jacobi symbol), while decryption of which (using

the Chinese remainder theorem) is roughly of the same speed as RSA decryption. In this phase, based on Rabin cryptosystem, initial parameters are generated to carry out whole authentication process.

1. Server: The server S_j chooses two arbitrary big numbers (p_j, q_j) , then compute $n_j = p_j \cdot q_j$, which satisfies $p_j \equiv q_j \equiv 3 \pmod{4}$, where p_j and q_j are private keys, and n_j is public key of the server S_j . The server S_j then randomly selects a string x_j as the symmetric encryption key of the server S_j . The server S_j then secretly stores (p_j, q_j, x_j) .
2. Smart card: The user has the smart card choose and store a random string σ .

5.2. Registration Phase

Before using the service, the user U_i must register with the server S_j via a secure channel. In this phase, the information of the user and the server are secretly stored. For that purpose, both sides perform the following steps to complete the registration phase. The procedure is shown in Figure 3.

1. The user U_i first enters identity ID_i , password PW_i and biometric template B_i , then computes $BB_i = h(PW_i||B_i)$ and $W = h(h(PW_i||\sigma)||h(ID_i \oplus ID_{S_j}) \oplus \sigma)$. Next, the user U_i transmits ID_i , W and BB_i to the sever S_j .
2. After receiving message (ID_i, W, BB_i) , the server S_j uses symmetric encryption key x_j to compute $y_{ij} = SE_{x_j}(h(x_j)||ID_{S_j}||ID_i||W||BB_i)$. Thereafter, the server S_j transmits (ID_i, n_j, y_{ij}) to the user U_i .

After receiving the message, the user U_i computes $\varepsilon_j = \sigma \oplus y_{ij}$. The user U_i then stores $(\sigma, ID_i, PW_i, B_i)$ and $(\varepsilon_j, ID_{S_j}, n_j)$ into smart card and flash drive, respectively.

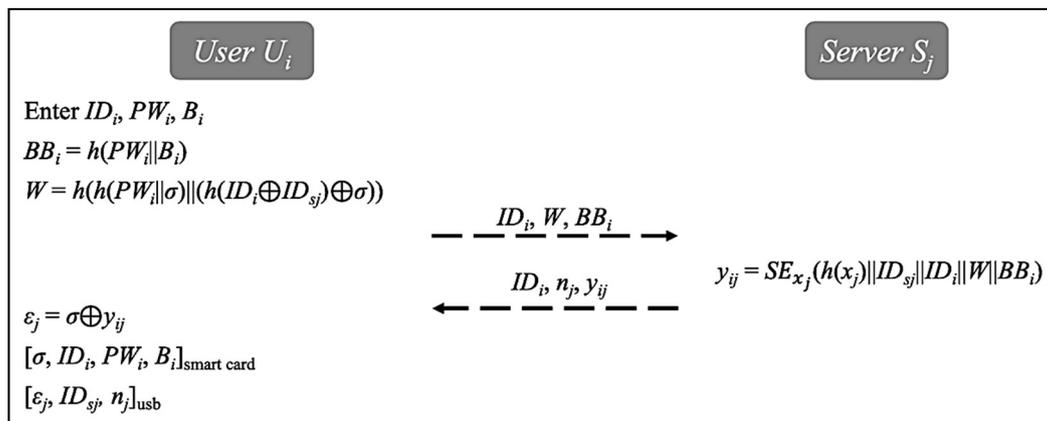


Figure 3. Registration phase.

5.3. Login and Initial Authentication Phase

If the user U_i wants to use service from healthcare provider, he/she has to communicate with the sever S_j to calculate a session key. Since this communication is carried out via a public channel, an authentication procedure is required to ensure they are legitimate parties. As shown in Figure 4, the user U_i and the server S_j perform the following steps to complete login and initial authentication phase.

1. The user U_i first inserts the smart card and enter PW_i^* and B_i^* . Next, the user U_i chooses a random string v , determines the number of authentications b , and computes $N = h^{(b)}(v)$, $BB_i^* = h(PW_i^*||B_i^*)$, $W' = h(h(PW_i^*||\sigma)||h(ID_i \oplus ID_{S_j}) \oplus \sigma)$, $y_{ij} = \sigma \oplus \varepsilon_j$, $\alpha = (BB_i^* \oplus W' \oplus T_1)$, and $k = (ID_{S_j}||ID_i||y_{ij}||N||\alpha||T_1)^2 \pmod{n_j}$. Then, the user U_i transmits k to the server S_j .
2. After receiving k , the server S_j uses private keys p_j, q_j to decrypt k then confirms the validity of the timestamp T_1 . Next, it uses symmetric key x_j to decrypt y_{ij} obtained from k . The server S_j then verifies $h(x_j)$, ID_i and ID_{S_j} . Thereafter, the server S_j computes $\alpha' = (BB_i \oplus W \oplus T_1)$. The server S_j

then compares α with α' . If there is a match, the server S_j calculates $\beta = h(N) \oplus T_2$ and new identity $ID_i^{new} = h(y_{ij} || ID_i || h(x_j))$. The server S_j then determines the time bound (t_1, t_2) , and choose two random strings a_s and b_s . Next, the server S_j computes $AT_a = h^{t_1-1}(h(ID_i^{new} || x_j || a_s))$, $AT_b = h^{z-t_2}(h(ID_i^{new} || x_j || b_s))$, session key $sk_{ij} = h(N \oplus y_{ij})$ and $Q = SE_{sk_{ij}}(\beta || ID_i^{new} || AT_a || AT_b || T_2)$. Then, the server S_j transmits (Q, t_1, t_2) to the user U_i .

3. After receiving (Q, t_1, t_2) , the user U_i computes $sk_{ij} = h(N \oplus y_{ij})$. Next, the user U_i uses session key sk_{ij} to decrypt Q and confirms the validity of the timestamp T_2 . Thereafter, the user U_i computes $\beta' = h(N) \oplus T_2$ and confirms β . If there is a match the user U_i accepts session key sk_{ij} . Finally, the user U_i stores (ID_i^{new}, AT_a, AT_b) and (t_1, t_2) in the smart card and flash drive, respectively.

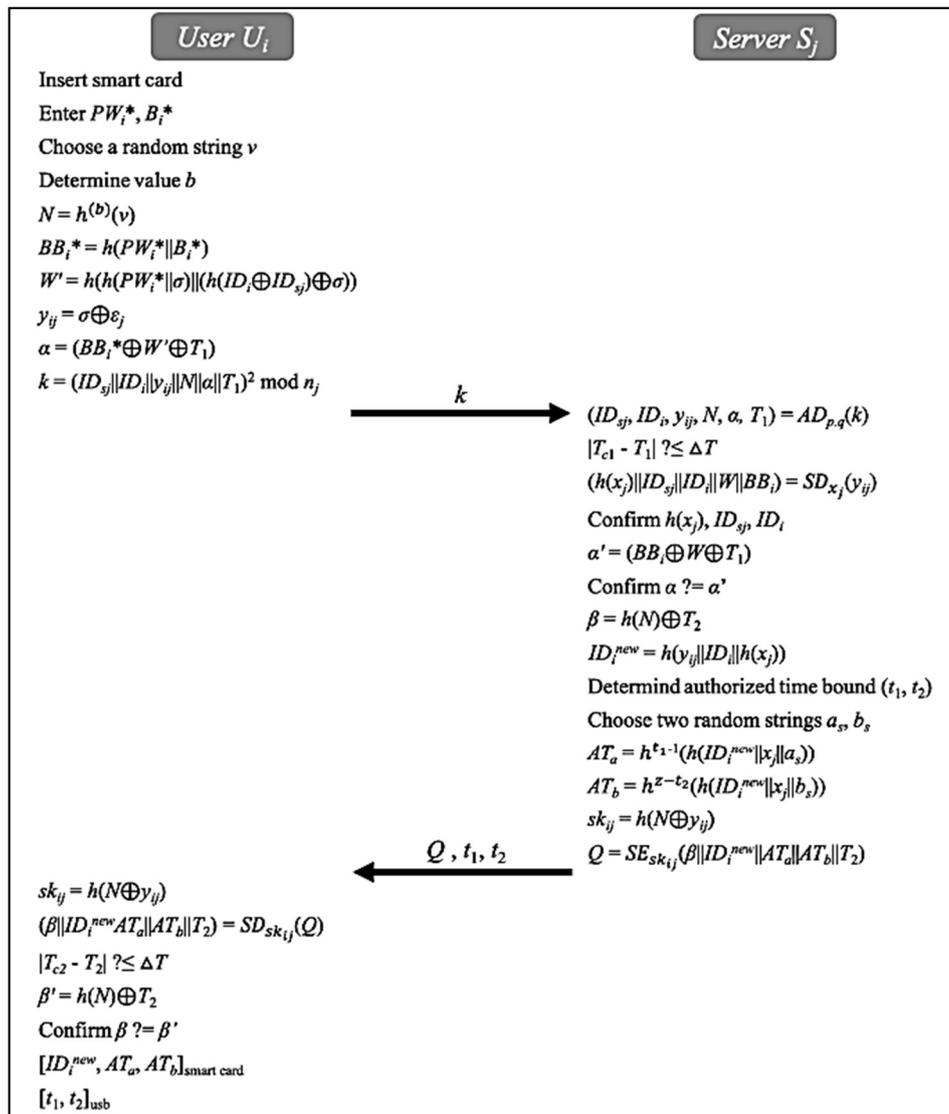


Figure 4. Login and initial authentication phase.

5.4. Fast Authentication Phase

As stated above, we design the fast authentication in our work to accelerate communication process. After the initial authentication, the user U_i and the server S_j are allowed to quickly authenticate each other based on an authorized time bound without computing a new session key. As shown in Figure 5, both sides perform the following steps to complete the fast authentication.

1. The user U_i enters ID_i^{new} , PW_i and B_i . The smart card confirms ID_i^{new} , PW_i , and B_i . Next, the user U_i computes $A_\gamma = h(h^{t-t_1}(AT_a)||h^{t_2-t}(AT_b))$. Then, the user U_i transmits A_γ to the server S_j .
2. After receiving A_γ , the server S_j calculates $X = h(ID_i^{new}||x_j||a_s)$, $Y = h(ID_i^{new}||x_j||b_s)$ and $A'_\gamma = h(h^{t-1}(X)||h^{z-t}(Y))$. Next, the server S_j compares A_γ with A'_γ . If there is no match, the server S_j will revoke the session key sk_{ij} ; otherwise, it computes $B_\gamma = SE_{sk_{ij}}(h(A'_\gamma \oplus ID_i^{new}))$. The server S_j then transmits B_γ to the user U_i .
3. After receiving B_γ , the user U_i computes $SE_{sk_{ij}}(h(A_\gamma \oplus ID_i^{new}))$, and then compares it with B_γ . If there is a match, the user U_i accepts sk_{ij} . Following this, the user U_i can still use the session key sk_{ij} to obtain the healthcare service in this communication session.

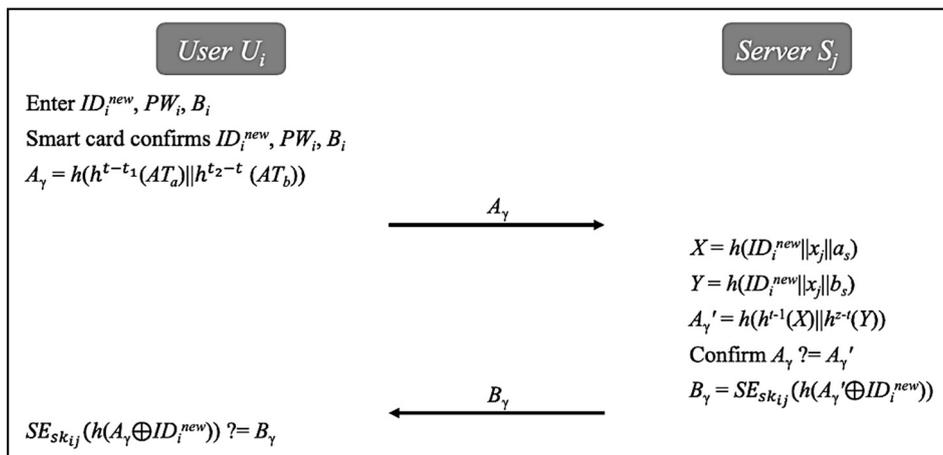


Figure 5. Fast authentication phase.

6. Logical Analysis Using GNY Logic

In this section, we prove security completeness and correctness of our proposed protocol through logical roles of GNY (Gong–Needham–Yahalom) logic [52]. GNY logic has been widely used to formally analyze the completeness of a cryptographic protocol. The proposed scheme is presented in logic as follows.

Message k

$U_i \rightarrow S_j$: ($\{ID_{S_j}, ID_i, \{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, H^{(b)}(\sigma), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1), T_1\}_{\text{mod } n_i}$)

Message (Q, t_1, t_2)

$S_j \rightarrow U_i$: ($\{F(H(N), T_2), H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j)), H^{t_1-1}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, a_s), H^{t_2-t_2}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, b_s)\}, T_2\}_{sk_{ij}, t_1, t_2}$)

6.1. Logical Rules Used in Our Proof

- (I1) $\frac{P \triangleleft^* \{X\}_K, P \triangleright K, P \models P \stackrel{K}{\leftarrow} Q, P \models \emptyset(X), P \models \#(X, K)}{P \models Q \sim X, P \models Q \sim \{X\}_K, P \models Q \triangleright K}$: Suppose that for principal P all of the following conditions hold: (1) P receives a formula consisting of a X encrypted with key K and marked with a not-originated-here mark; (2) P possesses K ; (3) P believes K is a suitable secret for himself and Q ; (4) P believes formula X is recognizable; and (5) P believes that K is fresh or that X is fresh. Then, P is entitled to believe that: (1) Q once conveyed X ; (2) Q once conveyed the formula X encrypted with K ; and (3) Q possesses K .

- (I₂) $\frac{P \triangleleft^* \{X, \langle S \rangle\}_{+K}, P \ni (-K, S), P \equiv \overset{+K}{\leftarrow} P, P \equiv P \overset{S}{\leftarrow} Q, P \equiv \emptyset(X, S), P \equiv \#(X, S, +K)}{P \equiv Q \sim (X, \langle S \rangle), P \equiv Q \sim \{X, \langle S \rangle\}_{+K}, P \equiv Q \ni +K}$: Suppose that for principal P all of the following conditions hold: (1) P receives a formula consisting of X concatenated with S , encrypted with a public key, and marked with a not-originated-here mark; (2) P possesses S and the corresponding private key; (3) P believes the public key is his own; (4) P believes S is a suitable secret for himself and Q ; (5) P believes that X concatenated with S is recognizable; and (6) P believes that at least one of S , X , or $+K$ is fresh. Then, P is entitled to believe that: (1) Q once conveyed the formula X concatenated with S ; (2) Q once conveyed the formula X concatenated with S and encrypted with the public key; and (3) Q possesses the public key.
- (I₇) $\frac{P \equiv Q \sim (X, Y)}{P \equiv Q \sim X}$: P believes Q once conveyed a formula consisting of X , and then P is entitled to believe Q once conveyed X .
- (J₁) $\frac{P \equiv Q \Rightarrow C, P \equiv Q \equiv C}{P \equiv C}$: P believes that Q is an authority on some statement C and that Q believes in C , and then P should believe in C as well.
- (F₁) $\frac{P \equiv \#(X)}{P \equiv \#(X, Y), P \equiv \#(F(X))}$: P believes message X is fresh, which means P can believe that any (X, Y) including message X is fresh, and then P believes $F(X)$, which is computed from message X , is also fresh.
- (T₁) $\frac{P \triangleleft^* X}{P \triangleleft X}$: When P obtains a non-original value $*X$, it means P may obtain the original X .
- (T₃) $\frac{P \triangleleft \{X\}_K, P \ni K}{P \triangleleft X}$: P uses secret key K to encrypt, decrypt to obtain message X .
- (T₄) $\frac{P \triangleleft \{X\}_{+K}, P \ni -K}{P \triangleleft X}$: P uses private key $-K$ to decrypt, uses public key $+K$ to encrypt, and obtains the message X .
- (P₁) $\frac{P \triangleleft X}{P \ni X}$: P can see the message X , indicating that P really possesses the message X .
- (P₄) $\frac{P \ni X}{P \ni H(X)}$: If P possesses X , then it possesses $H(X)$.
- (R₁) $\frac{P \equiv \emptyset(X)}{P \equiv \emptyset(X, Y), P \equiv \emptyset(F(X))}$: P believes message X is recognizable, indicating that P can believe that any (X, Y) including message X is recognizable, and P believes that any $F(X)$ computed from message X is also recognizable).
- (R₂) $\frac{P \equiv \emptyset(X), P \ni K}{P \equiv \emptyset(\{X\}_K), P \equiv \emptyset(\{X\}_{K^{-1}})}$: P believes message X is recognizable and P possesses the shared secret key K , and then P believes anything computed using the shared secret key is recognizable.
- (R₄) $\frac{P \equiv \emptyset(X), P \ni -K}{P \equiv \emptyset(\{X\}_{-K})}$: P believes the message X is recognizable and P possesses private key $-K$, then P believes any message computed using private key is recognizable.

6.2. Assumptions of the Proposed Protocol

- (A₁) $S_j \ni p_j, q_j$: The server S_j possesses private keys p_j and q_j .
- (A₂) $S_j \ni x_j$: The server S_j possesses secret key x_j .
- (A₃) $S_j \ni N$: The server S_j possesses message N .
- (A₄) $S_j \equiv \emptyset(H(x_j))$: The server S_j believes that $H(x_j)$ is recognizable.
- (A₅) $S_j \equiv \emptyset(\alpha)$: The server S_j believes that α is recognizable.
- (A₆) $U_i \equiv \#(T)$: The user U_i believes that timestamp T is fresh.
- (A₇) $S_j \equiv (U_i \overset{N}{\leftarrow} S_j)$: The server S_j believes that N is a suitable secret for the user U_i and the server S_j .
- (A₈) $U_i \ni N$: The user U_i possesses N .
- (A₉) $U_i \ni y_{ij}$: The user U_i possesses the key y_{ij} .
- (A₁₀) $U_i \equiv \emptyset(v)$: The user U_i believes that v is recognizable.
- (A₁₁) $S_j \equiv U_i \Rightarrow (U_i \overset{N}{\leftarrow} S_j)$: The server S_j believes that the user U_i has jurisdiction over N , which is a suitable secret for the user U_i and the server S_j .
- (A₁₂) $S_j \equiv \#(T)$: The server S_j believes that timestamp T is fresh.

6.3. Goals

- Message content authentication: It proves the authenticity of transmitted message.

Goal 1: Prove the authenticity of message k :

$$S_j \models \emptyset \left(\{ID_{S_j}, ID_i, \{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, H^{(b)}(v), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1, T_1\}_{\text{mod } n_j} \right) \quad (G1)$$

Only the server S_j can read message k transmitted by the user U_i .

Goal 2: Prove the authenticity of the message (Q, t_1, t_2) :

$$U_i \models \emptyset \left(\{F(H(N), T_2), H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j)), H^{t_1-1}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, a_s)), H^{z-t_2}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, b_s)), T_2\}_{sk_{ij}, t_1, t_2} \right) \quad (G2)$$

Only the user U_i can read message (Q, t_1, t_2) transmitted by the server S_j .

- Message origin authentication: It proves that the received message is transmitted by the legitimate parties.

Goal 3: Prove the origin of message k :

$$S_j \models U_i \sim \left(\{ID_{S_j}, ID_i, \{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, H^{(b)}(v), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1, T_1\}_{\text{mod } n_j} \right) \quad (G3)$$

The server S_j can verify that only the user U_i can generate message k received by the server S_j .

Goal 4: Prove the origin of message (Q, t_1, t_2) :

$$U_i \models S_j \sim \left(\{F(H(N), T_2), H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma)), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j)), H^{t_1-1}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, a_s)), H^{z-t_2}(H(H(\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}, ID_i, H(x_j))), x_j, b_s)), T_2\}_{sk_{ij}, t_1, t_2} \right) \quad (G4)$$

The user U_i can verify that only the server S_j can generate message (Q, t_1, t_2) received by the user U_i .

- Key agreement and confirmation: They prove that the session key is secret and shared only by the legitimate parties.

Goal 5: Key Agreement of $U_i \rightarrow S_j$:

$$U_i \models S_j \ni sk_{ij} \quad (G5)$$

The user U_i believes that only the server S_j can obtain the shared session key sk_{ij} .

Goal 6: Key Confirmation of $U_i \rightarrow S_j$:

$$U_i \models S_j \equiv (U_i \stackrel{sk_{ij}}{\leftrightarrow} S_j) \quad (G6)$$

The user U_i believes that the user server S_j is convinced of the shared session key sk_{ij} established between them.

Goal 7: Key Agreement of $S_j \rightarrow U_i$:

$$S_j | \equiv (U_i \stackrel{sk_{ij}}{\leftrightarrow} S_j) \quad (G7)$$

The server S_j believes that a shared session key sk_{ij} between it and the user U_i has been established.

Goal 8: Key Confirmation of $S_j \rightarrow U_i$:

$$S_j | \equiv U_i | \equiv (U_i \stackrel{sk_{ij}}{\leftrightarrow} S_j) \quad (G8)$$

The server S_j believes that the user U_i has already obtained the shared session key sk_{ij} .

Since S_j knows of message k , we have that:

$$S_j \triangleleft *(\{ID_{S_j}, ID_i, y_{ij}, N, \alpha, T_1\}_{\text{mod } n_j}) \quad (1)$$

According to T_1 , we have that:

$$S_j \triangleleft (\{ID_{S_j}, ID_i, y_{ij}, N, \alpha, T_1\}_{\text{mod } n_j}) \quad (2)$$

According to Equation (2), A_1 , and T_4 , the server S_j can use private keys p_j and q_j to decrypt k ; we have that:

$$S_j \triangleleft (ID_{S_j}, ID_i, y_{ij}, N, \alpha, T_1) \quad (3)$$

According to Equation (3), A_2 , and T_3 , the server S_j can use secret key x_j to decrypt $y_{ij} = \{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}$; we have that:

$$S_j \triangleleft (ID_{S_j}, ID_i, H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i), H^{(b)}(v), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1, T_1) \quad (4)$$

According to (4) and P_1 , we have that:

$$S_j \ni ID_i, ID_{S_j}, H(x_j), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1) \quad (5)$$

According to (5), A_4 , A_5 , and R_1 , we have that:

$$S_j | \equiv \emptyset (ID_i, ID_{S_j}, H(x_j), F(H(PW_i^*, B_i^*), H(H(PW_i^*, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), T_1)) \quad (6)$$

According to Equation (6), S_j can believe $H(x_j)$ is truly recognizable. According to A_2 and R_4 , the server S_j possesses x_j and can identify $H(x_j)$. Therefore, the server S_j believes y_{ij} (encrypted using x_j) is recognizable. We have that:

$$S_j | \equiv \emptyset (y_{ij}) \iff S_j | \equiv \emptyset (\{H(x_j), ID_{S_j}, ID_i, H(H(PW_i, \sigma), F(H(F(ID_i, ID_{S_j})), \sigma))), H(PW_i, B_i)\}_{x_j}) \quad (7)$$

According to Equations (6) and (7), A_5 , and R_1 , (G1) is realized by our protocol.

Since the user U_i knows of message (Q, t_1, t_2) , we have that:

$$U_i \triangleleft *(\{\beta, ID_i^{new}, AT_a, AT_b, T_2\}_{sk_{ij}}, t_1, t_2) \quad (8)$$

Based on rule T_1 , we have that:

$$U_i \triangleleft (\{\beta, ID_i^{new}, AT_a, AT_b, T_2\}_{sk_{ij}}, t_1, t_2) \quad (9)$$

Based on A_8 and A_9 , we have that:

$$U_i \ni F(N, y_{ij}) \quad (10)$$

Based on (10) and rule P_4 , the user U_i can possess the shared secret key sk_{ij} ; we have that:

$$U_i \ni H(F(N, y_{ij})) \iff U_i \ni sk_{ij} \quad (11)$$

Based on Equations (9) and (11), and rule T_3 , U_i can use the shared key sk_{ij} to decrypt $Q = \{\beta, ID_i^{new}, AT_a, AT_b, T_2\}_{sk_{ij}}$; we have that:

$$U_i \triangleleft (\beta) \iff U_i \triangleleft F(H(N), T_2) \iff U_i \triangleleft F(H(H^{(b)}(v)), T_2) \quad (12)$$

Based on Equation (12), A_{10} , and rule R_1 , we have that:

$$U_i \mid \equiv \emptyset(H^{(b)}(v)) \iff U_i \mid \equiv \emptyset(N) \quad (13)$$

Based on Equation (13) and R_1 , we have that:

$$U_i \mid \equiv \emptyset(F(H(N), T_2)) \iff U_i \mid \equiv \emptyset(\beta) \quad (14)$$

Based on Equations (11) and (14), and rule R_2 , U_i can possess sk_{ij} and identify β . Since the user U_i believes message Q encrypted using sk_{ij} is recognizable, (Q, t_1, t_2) is truly the message which is encrypted using sk_{ij} possessed by the user U_i . Hence, the proposed scheme realizes (G2).

According to (1), (3), A_4 , A_5 , A_{12} , F_1 , and I_2 , (G3) is achieved.

Based on Equations (8), (10) and (11), A_3 , A_6 , F_1 , and I_1 , (G4) is achieved.

Based on (G4) and rule I_7 , our scheme realizes (G5).

Since the users U_i believes the server S_j is legitimate and has jurisdiction, we have $U_i \mid \equiv S_j \mid \Rightarrow S_j \mid \equiv *$. Based on (G4), (G6) is realized.

Based on (G3), A_{11} , and rule J_1 , (G7) is realized.

Since the server S_j believes the user U_i is legitimate and has jurisdiction, we have $S_j \mid \equiv U_i \mid \Rightarrow U_i \mid \equiv *$. Based on (G3), our proposed scheme realizes (G8).

7. Security Analysis Using AVISPA Tool

7.1. Overview of AVISPA

Automated Validation of Internet Security Protocols and Applications (AVISPA) [53] is a widely accepted tool used for the analysis of large-scale Internet security-sensitive protocols and applications. AVISPA tool executes the simulated protocol specified by HLPSL language [54]. For verifying cryptographic protocol, AVISPA 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). In this paper, using AVISPA tool and Security Protocol Animator (SPAN), we provide a security proof for the proposed scheme. Figure 6 shows the interface of the SPAN with AVISPA tool.

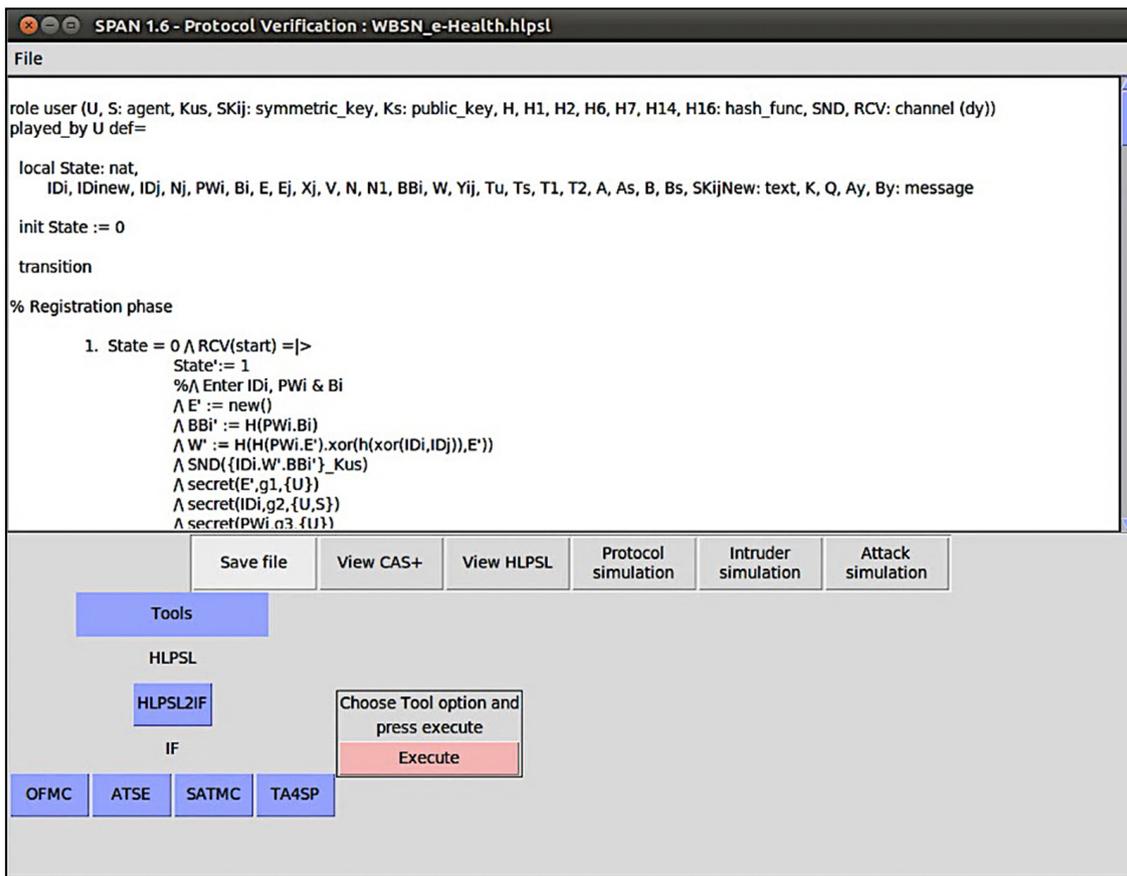


Figure 6. Security Protocol Animator for AVISPA.

7.2. The Verification

The proposed protocol is verified using the OFMC and CL-AtSe backends. In AVISPA, our scheme includes two roles: user U and server S. The HLPSP specifications of the user U and the sever S are shown in Boxes 1 and 2, respectively. Besides, session role, environment role and goals are also specified in HLPSP, as shown in Box 3. For verification of the proposed scheme, we consider seven secrecy goals and three authentication goals as follows.

- secrecy_of g1: E' is kept secret to the user U.
- secrecy_of g2: IDi is kept secret to the user U and the server S.
- secrecy_of g3: PWi is kept secret to the user U.
- secrecy_of g4: Bi is kept secret to the user U.
- secrecy_of g5: Xj is kept secret to the server S.
- secrecy_of g6: As' is kept secret to the server S.
- secrecy_of g7: Bs' is kept secret to the server S.
- authentication_on u_s_v: The server S authenticates the user U based on V received from the message of the user U.
- authentication_on u_s_tu: The server S authenticates the user U based on Tu received from the message of the user U.
- authentication_on s_u_ts: The user U authenticates the server S based on Ts received from the message of the server S.

Box 1. The HLPSe specification of the user.

```

role user (U, S: agent, Kus, SKij: symmetric_key, Ks: public_key, H, H1, H2, H6, H7, H14,
          H16: hash_func, SND, RCV: channel (dy))

played_by U def=
local State: nat,
IDi, IDinew, IDj, Nj, PWi, Bi, E, Ej, Xj, V, N, N1, BBi, W, Yij, Tu, Ts, T1, T2, A, As, B, Bs, SKijNew: text, K, Q, Ay, By: message
init State := 0
transition
% Registration phase
1. State = 0/\ RCV(start) =>
State' := 1
%\ Enter IDi, PWi & Bi
/\ E' := new()\ BBi' := H(PWi.Bi)\ W' := H(H(PWi.E).xor(h(xor(IDi,IDj)),E'))
/\ SND({IDi.W'.BBi'}_Kus)
/\ secret(E',g1,{U})\ secret(IDi.g2,{U,S})\ secret(PWi.g3,{U})\ secret(Bi.g4,{U})
2. State = 1/\ RCV({IDi.Nj.{H(Xj)}.IDj.IDi.H(H(PWi.E).xor(h(xor(IDi,IDj)),E)).H(PWi.Bi)}_Xj')_Kus) =>
State' := 2
/\ Ej' := xor(E,({H(Xj)}.IDj.IDi.W.BBi}_Xj))
%\ Store E, IDi, PWi & Bi in the smart card %\ Store Ej', IDj, & Nj in the USB
% Login and initial authentication phase
3. State = 0/\ RCV(start) =>
State' := 1
%\ Insert smart card %\ Enter PWi* & Bi*
/\ V' := new()
%\ Suppose b = 3
/\ N' := H(H(H(V')))\ BBi' := H(PWi.Bi)\ W' := H(H(PWi.E).xor(h(xor(IDi,IDj)),E))\ Yij' := xor(E,Ej)\ Tu' := new()\ A' :=
xor(xor(BBi',W'),Tu')\ K' := {IDi.IDj.Yij'.N'.A'.Tu'}_Ks
/\ SND(K')
/\ witness(U,S,u_s_v,V')\ witness(U,S,u_s_tu,Tu')
/\ secret(IDi.g2,{U,S})\ secret(PWi.g3,{U})\ secret(Bi.g4,{U})
4. State = 1/\ RCV({B'.H(Yij.IDi.H(Xj)).H6(H(H(Yij.IDi.H(Xj)).Xj.As')).H14(H(H(Yij.IDi.H(Xj)).Xj.Bs')).Ts'}_SKij).T1'.T2') =>
State' := 2
/\ SKij' := H(xor(N,Yij))
%\ Confirm Ts' %\ Confirm B %\ Store IDinew, ATa, ATb in the smart card %\ Store T1, T2 in the USB
/\ request(S,U,s_u_ts,Ts')
% Fast authentication phase
5. State = 0/\ RCV(start) =>
State' := 1
%\ Enter IDinew, PWi & Bi %\ Suppose Tlogin = 8
/\ Ay' := H(H1(H6(H(H(Yij.IDi.H(Xj)).Xj.As))))\ H(H2(H14(H(H(Yij.IDi.H(Xj)).Xj.Bs))))
/\ SND(Ay')
6. State = 1/\ RCV({H(xor(Ay',IDinew))}_SKij) =>
State' := 2
%\ Confirm By'
end role

```

After executing the tool, as shown in Boxes 4 and 5 respectively, the analysis results of the proposed protocol using the OFMC and CL-AtSe backends confirm that the stated secrecy and authentication properties are satisfied for a bounded number of sessions as specified in the environment role. Thus, our scheme can resist various well-known attacks.

Box 2. The HLPSSL specification of the server.

```

role server (U, S: agent, Kus, SKij: symmetric_key, Ks: public_key, H, H1, H2, H6, H7, H14,
            H16: hash_func, SND, RCV: channel (dy))

played_by S def=
local State: nat,
IDi, IDinew, IDj, Nj, PWi, Bi, E, Ej, X, Y, Xj, V, N, N1, BBi, W, Yij, Tu, Ts, T1, T2, A, As, B, Bs, ATa, ATb, SKijNew: text, K, Q, Ay,
By: message
init State := 0
transition
% Registration phase
1. State = 0/\ RCV((IDi.H(H(PWi.E')).xor(h(xor(IDi,IDj))),E')).H(PWi.Bi))_Kus) =>
State' := 1
/\ Yij' := {H(Xj).IDj.IDi.H(H(PWi.E')).xor(h(xor(IDi,IDj))),E')).H(PWi.Bi)}_Xj
%/\ Store IDj
/\ SND({IDi.Nj.Yij'}_Kus)
/\ secret(Xj,g5,{S})
% Login and initial authentication phase
2. State = 0/\ RCV((IDi.IDj.Yij'.H(H(H(V')))).A'.Tu')_Ks) =>
State' := 1
%/\ Confirm Tu' %/\ Use Xj to decrypt Yij %/\ Confirm H(Xj), IDsj & IDi
/\ A' := xor(xor(BBi.W).Tu') %/\ Confirm A
/\ Ts' := new()/\ B' := xor(H(H(H(H(V')))),Ts')/\ IDinew' := H(Yij.IDi.H(Xj))/\ T1' := new()/\ T2' := new()/\ As' := new()/\ Bs' :=
new()
%/\ Z =24, suppose T1=7, T2=10
/\ ATa' := H6(H(IDinew'.Xj.As'))/\ ATb' := H14(H(IDinew'.Xj.Bs'))/\ SKij' := H(xor(H(H(H(V'))),Yij'))/\ Q' :=
{B'.IDinew'.ATa'.ATb'.Ts'}_SKij'
/\ SND(Q'.T1'.T2')
/\ witness(S,U,s_u_ts,Ts')
/\ secret(As',g6,{S})/\ secret(Bs',g7,{S})
/\ request(U,S,u_s_v,V')/\ request(U,S,u_s_tu,Tu')
% Fast authentication phase
3. State = 0/\ RCV(H(H1(H6(H(H(Yij.IDi.H(Xj)).Xj.As')))).H(H2(H14(H(H(Yij.IDi.H(Xj)).Xj.Bs'))))) =>
State' := 1
/\ X' := H(IDinew.Xj.As)/\ Y' := H(IDinew.Xj.Bs)/\ Ay' := H(H7(X').H16(Y'))
%/\ Confirm Ay
/\ By' := {H(xor(Ay',IDinew))}_SKij
/\ SND(By')
end role

```

Box 3. The HLPSSL specification of the session role, environment role and goals.

```

role session (U, S: agent, Kus, SKij: symmetric_key, Ks: public_key, H, H1, H2, H6, H7, H14,
            H16: hash_func) def=

local SU, RU, SS, RS: channel (dy)
composition
user (U,S,Kus,SKij,Ks,H,H1,H2,H6,H7,H14,H16,SU,RU)/\ server (U,S,Kus,SKij,Ks,H,H1,H2,H6,H7,H14,H16,SS,RS)
end role
role environment() def=
const u, s: agent,
kus, skij, kui: symmetric_key,
ks, ki: public_key,
h, h1, h2, h6, h7, h14, h16: hash_func,
u_s_v, u_s_tu, s_u_ts, g1, g2, g3, g4, g5, g6, g7: protocol_id
intruder_knowledge = {u,s,ks,ki,inv(ki)}
composition
session(u,s,kus,skij,ks,h,h1,h2,h6,h7,h14,h16)/\ session(u,i,kui,kui,ks,h,h1,h2,h6,h7,h14,h16)/\
session(i,s,kui,kui,ks,h,h1,h2,h6,h7,h14,h16)
end role
goal
secrecy_of g1, g2, g3, g4, g5, g6, g7authentication_on u_s_v, u_s_tu, s_u_ts
end goal
environment()

```

Box 4. The results of the OFMC back-end.

```

% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/WSN_e-Health.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.70 s
visitedNodes: 163 nodes
depth: 6 plies

```

Box 5. The result of the CL-AtSe back-end.

```

SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/span/span/testsuite/results/WSN_e-Health.if
GOAL
As Specified
BACKEND
CL-AtSe
STATISTICS
Analysed : 2 states
Reachable : 0 states
Translation: 0.09 s
Computation: 0.00 s

```

8. Semantic Security Analysis

Resistance to online password guessing attack: In this case, the attacker has obtained some relevant parameters and tries to guess the password to initiate login request. Nevertheless, the server can easily observe this attack by verifying the validity of the value α of the request message k . Thus, online password guessing attack is resisted in our protocol.

Resistance to offline password guessing attack: The attacker attempts to collect all offline information to guess the correct password. However, the attacker does not have the private key of the server, thus he cannot decrypt message k . Similarly, the attacker does not have sk_{ij} , thus he is not able to decrypt message Q . Moreover, since the messages are changed in every single login, the attacker cannot use the stolen information of the previous login to compromise the current login. Besides, PW_i is not available to the public and is computed only when the user inserts the smart card. Hence, our protocol is safe against offline password guessing attack.

Resistance to impersonation attack: In our protocol, the attacker cannot carry out impersonation attack without knowing password PW_i (owing to password guessing attack resistance as stated above) and string number σ . Therefore, the attacker cannot compute the correct W and α to impersonate the user with the candidate login message. Hence, our work is free from impersonation attack.

Resistance to replay attack: Our protocol includes timestamp T_1 in login message $k = (ID_{S_j} \| ID_i \| y_{ij} \| N \| \alpha \| T_1)^2 \bmod n_j$; therefore, the server S_j can easily check the validity of the message k . In addition, the user U_i can verify the validity of the message Q by checking the timestamp T_2 . Furthermore, all the messages are calculated using random number strings, which are used just once in every communication session. Thus, our protocol fully resists replay attack.

Resistance to DoS attack: As stated above, our protocol uses timestamp to prevent attacker from intercepting user's message and then retransmitting it repeatedly to disrupt the server. The message $k = (ID_{S_j} \| ID_i \| y_{ij} \| N \| \alpha \| T_1)^2 \bmod n_j$ includes timestamp T_1 to prevent the attacker from retransmitting login requests to the sever. Therefore, the proposed protocol is secure from DoS attack.

Resistance to modification attack: This attack happens when the attacker intercepts the login message k and transmits a modified one to the sever. The value k is a ciphertext computed using public key n_j , which is only decrypted using the private key p_j and q_j of the server. Moreover, the attacker is still blocked by timestamp T_1 (due to the resistance to replay attack and DoS attack stated above) even when he has compromised the message k . Similarly, the message Q is protected by the session key sk_{ij} and the timestamp T_2 . Therefore, the proposed scheme can resist modification attack.

Resistance to insider attack: Since the proposed scheme does not require storage for storing the biometric data, it is not possible for a malicious legal user (attacker) to impersonate legitimate user without the correct biometric characteristic B_i . In addition, verification table is not required in our scheme. Thus, our scheme can fully prevent insider attack.

Resistance to MITM attack: In our protocol, the attacker cannot compromise message k and sends a login request to the sever since he/she is not able to compute the correct $h(x_j)$ for server verification without secret key x_j . Moreover, the attacker also cannot calculate the correct k due to the resistance to password guessing attack and impersonation attack as stated. Hence, the attacker cannot act as a middleman and our scheme is free from man-in-the-middle attack.

Resistance to stolen smart card attack: Suppose the smart card has been stolen and the attacker has obtained the values σ , ID_i , PW_i , and B_i . However, since the attacker does not know of the identity of the server, he cannot compute W' . Besides, the attacker is unable to compute y_{ij} from σ and ε_j unless he/she steals smart card and flash drive respectively at the same time. As a result, it is not possible for the attacker to compute the correct α and k for verification. Therefore, the proposed protocol is safe against stolen smart card attack.

Resistance to desynchronization attack: In login and initial authentication phase, the server uses sk_{ij} to encrypt acknowledgment message β and then send β to the user. The server will check the validity of the message β before accepting the session key sk_{ij} . Similarly, in fast authentication phase, the session key sk_{ij} is accepted only when A_γ and B_γ have been confirmed. The user will delete the session key and restart whole process if the confirmations are not successful. Thus, desynchronization attack is resisted in our scheme.

Provision of biometric data anonymity: In the registration phase, biometric data B_i and password PW_i are computed using one-way hash function. Biometric data will not be available to public since the hash is an irreversible value. Hence, the proposed scheme provides biometric data anonymity for the user.

Provision of forward secrecy: The attacker attempts to use information from the past communication session to derive the key. Suppose the attacker has obtained the random strings v and b , he/she is not able to compute the session key without the values σ and ε_j stored in the smart card and flash drive. Therefore, the proposed protocol achieves forward secrecy.

Provision of user anonymity and untraceability: The identity ID_i is only included in the message $W = h(h(PW_i \| \sigma) \| (h(ID_i \oplus ID_{S_j}) \oplus \sigma))$. Owing to the one-way hash function, the identity ID_i is not available to the public during communication process. In other words, the identity ID_i is kept secret to the user U_i and the server S_j . In addition, the attacker cannot identify any two past protocol runs initiated by the same user since the value k is computed using random number v . Therefore, the proposed scheme achieves strong user anonymity and untraceability.

Compared with previous works, Table 2 shows that our scheme is free from DoS attack, which is a vulnerability to all others. Fan and Lin [38] and Jiang et al. [39] are not secure against stolen smart card attack and desynchronization attack. Besides, Fan and Lin [38] and Zhang et al. [26] suffer from storage burden of storing biometric data in their proposed schemes. Jiang et al. [39] is not free from resist replay attack. Fan and Lin [38] is not able to resist online password guessing attack, modification attack, impersonation attack and man-in-the-middle attack. Besides, Fan and Lin [38] does not provide user untraceability. Especially, only our work provides time bound solution and fast authentication.

Table 2. Comparison of security properties.

	Fan and Lin [38]	Jiang et al. [39]	Zhang et al. [26]	Ours
Resistance to online password guessing attack	X	O	O	O
Resistance to offline password guessing attack	O	O	O	O
Resistance to impersonation attack	X	O	O	O
Resistance to replay attack	O	X	O	O
Resistance to DoS attack	X	X	X	O
Resistance to modification attack	X	O	O	O
Resistance to insider attack	O	O	O	O
Resistance to MITM attack	X	O	O	O
Resistance to stolen smart card attack	X	X	O	O
Resistance to desynchronization attack	X	X	O	O
No storage burden of biometric data	X	O	X	O
Provision of biometric data anonymity	O	O	O	O
Provision of forward secrecy	O	O	O	O
Provision of fast authentication	X	X	X	O
Provision of time-bound authentication	X	X	X	O
Provision of user anonymity	O	O	O	O
Provision of user untraceability	X	O	O	O

9. Performance Analysis

In this section, we provide a performance analysis to compare our scheme with its predecessor schemes. Specifically, we make a comparison with the logarithm to base 2 of the running time of each scheme. The value $\log_2 x$ is used to compare the efficiency of the protocols where x is the rough estimation of running time (Table 3) when n (number of servers) increases from 1 to 1000. When n gradually increases, Figure 7 shows that our scheme is more efficient than the predecessor schemes. Even in single-server architecture (where $n = 1$), our scheme is more efficient than Fan and Lin [38] and Jiang et al [39].

Table 3. Comparison of computational complexities.

	Fan and Lin [38]	Jiang et al. [39]	Zhang et al. [26]	Ours
Registration phase	$2T_{SED} + T_H + T_X$	$4T_H + 3T_X$	$7T_H + 5T_X$	$T_{SED} + 5T_H + 3T_X$
Login and authentication phase	$5T_{SED} + 2T_{ASED} + 2T_H + T_X$	$4T_{PM} + 4T_{SED} + 10T_H + T_X$	$23T_H + 22T_X$	$2T_{SED} + 9T_H + 2T_X$
Password update phase	—	$12T_H + 4T_X$	—	—
Total time complexities	$7T_{SED} + 2T_{ASED} + 3T_H + 2T_X$	$4T_{PM} + 4T_{SED} + 26T_H + 8T_X$	$30T_H + 27T_X$	$3T_{SED} + 14T_H + 5T_X$
Total rough estimation (ms)	1106.41n	300.14n	15.135n	33.125n

n , number of servers; T_E , time for performing an exponentiation operation; T_{PM} , time for performing an elliptic curve point multiplication operation; T_{SED} , time for performing a symmetric encryption/decryption operation; T_{ASED} , time for performing an asymmetric encryption/decryption operation; T_H , time for performing a hash function operation; T_X , time for performing an exclusive-or operation; According to Banerjee et al. [55]: $T_E \approx 522$ ms; $T_{PM} \approx 63.075$ ms; $T_{SED} \approx 8.7$ ms; $T_{ASED} \approx 522$ ms; $T_H \approx 0.5$ ms; and $T_X \approx 0.005$ ms.

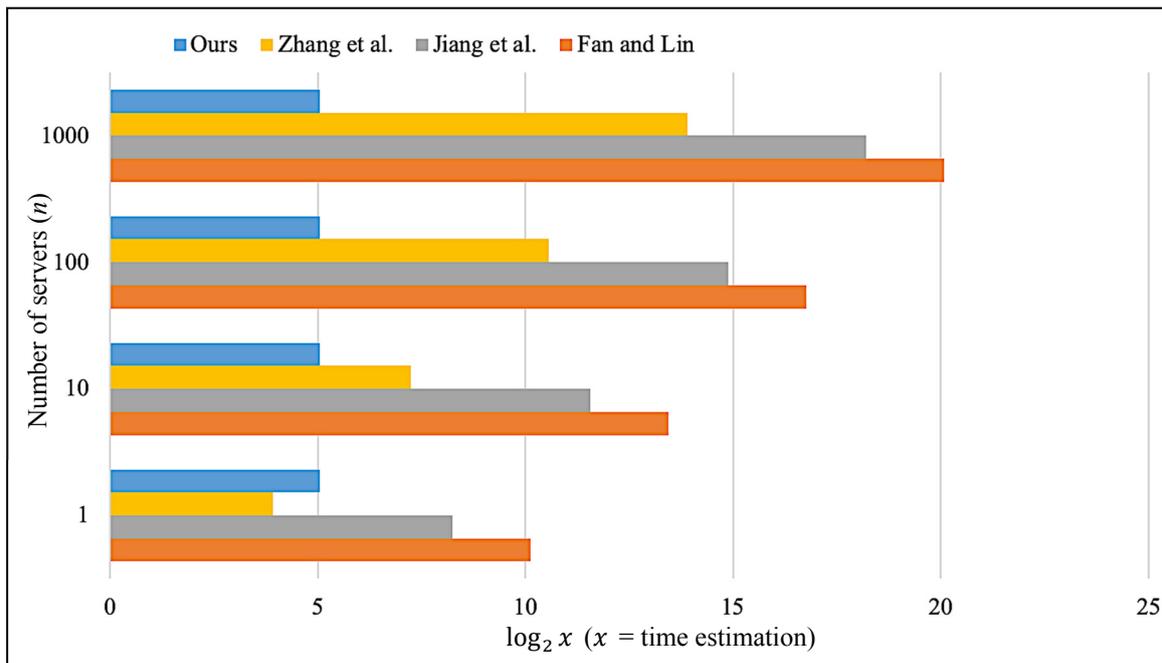


Figure 7. Running time of different schemes.

10. Implementation of the Proposed Scheme

Consistent with the proposed system model presented in Figure 2, we present possible scenarios in a 5G-based multi-server-based healthcare system. The user can use his/her biometric sensor-enabled mobile device and body wearable sensors to obtain services from multiple servers.

- *Scenario 1:* The user can use the smart card, password, and sensor device to login to Home Care Server (S_1) of Service Provider 1 to query his/her healthcare status. In addition, the user can login to healthcare data center to upload personal health information. Furthermore, the user can also login to Service Provider 2 (S_2) and compute a session key to obtain remote healthcare services with caregivers.
- *Scenario 2:* With the help of continuous care across the domains, the user can login to Healthcare Service Provider 3 (S_3) to upload health sensing data produced by the wearable sensors. Besides, when the user gets in community care domain, he/she can login to its healthcare server to compute session keys for using IoMT-devices through a 5G wireless network.

Furthermore, after registering with S_1 , S_2 , and S_3 , the user possesses (PW_i, σ_i, B_i) and then stores them in the smart card. The public parameters $(\epsilon_1, ID_{s1}, n_1)$, $(\epsilon_2, ID_{s2}, n_2)$, and $(\epsilon_2, ID_{s2}, n_2)$ of S_1 , S_2 , and S_3 , respectively, are stored in the flash drive. Consistent with user anonymity property of our proposed scheme, privacy of the user (ID_i) is preserved during this communication process. Besides, using the proposed scheme, the communication between the user and the servers is safe against possible attacks specified in Section 7. For example, the attacker cannot steal the smart card (containing (PW_i, σ_i, B_i)) and the flash drive (containing $(\epsilon_1, ID_{s1}, n_1)$) at the same time, thus the stolen smart card attack is resisted. If these three services are provided by a single healthcare institution, overhead of the proposed system is still only 33.125 ms (according to Table 3), which costs less than the methods of Zhang et al. (45.405 ms), Jiang et al. (900.42 ms), and Fan and Lin (3319.23 ms).

In addition, if service providers would like to give some discounts to specific users for their particular contribution, for instance valuable health data, the servers may use time-bound authentication solution introduced in our work for this purpose. Only authenticated users within an authorized time bound are able to get the discounts from the providers. In a hospital, time-bound authentication is also useful for physicians to set up examination schedules for specific patients.

Furthermore, we use the Go programming language to develop a system interface, where the user uses smart card to register for using services provided by Linkou Chang Gung Memorial hospital. Multi-server architecture can be designed with single sign-on (SSO) [56]. SSO solution allows the users to access multiple applications of the same authentication provider using single identity and password. First, the user makes a registration with the server (Figure 8, and then uses registered information (including the identity *d0540011*) to login to the system (Figure 9). We allow the user to create specific servers by himself/herself in this simulation. As shown in Figure 10, the user has used the smart card to create Billing server. The user can query server information in the next step. As shown in Figure 11, several servers including *CGMH*, *CGMH_blockchain*, *Blockchain*, *GOOGLE*, *EHR*, and *Billing* have been created. Next, the user uses his/her identity, password, and an additional ID (*01011992*) to register with the desired server, for instance Billing server (Figure 12). Finally, the user can check his/her account in which specific servers (*Blockchain*, *CGMH*, *Billing*, and *EHR*) and identities (*01011992* and *29071991*) are listed with the corresponding extra passwords automatically generated by SSO-enabled system (Figure 13). By this mechanism, the user is able to obtain data from multiple services provided by the hospital.

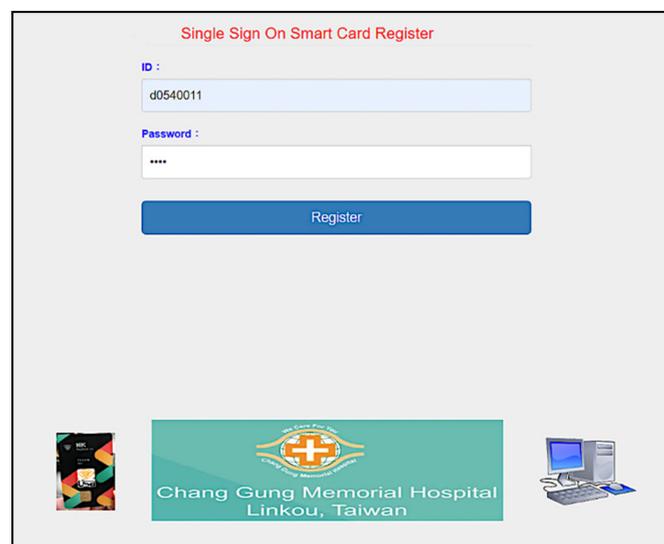


Figure 8. User registration.

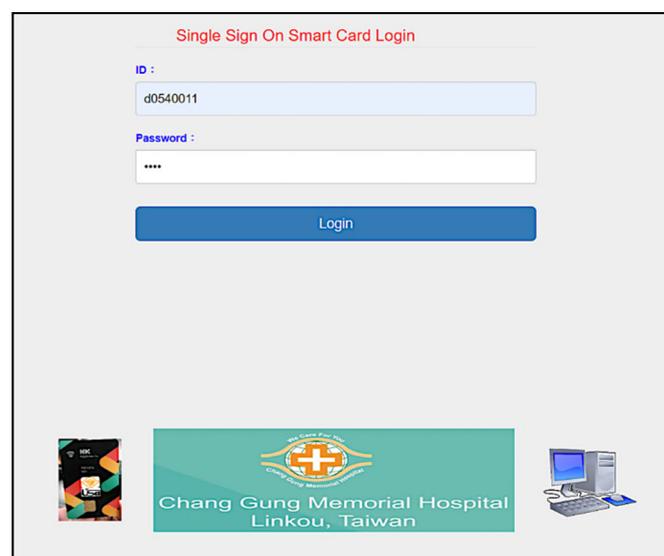


Figure 9. User login.

Single Sign On Create Server

Smartcard ID :
d0540011

Smartcard Password :

Server Name :
Billing

Register



Chang Gung Memorial Hospital
Linkou, Taiwan

Figure 10. Server creation.

Single Sign On Registration Phase

Smartcard ID
[Empty]

Smartcard Password
[Empty]

ID
[Empty]

Server :
CGMH
CGMH_blockchain
Blockchain
GOOGLE
EHR
Billing



Chang Gung Memorial Hospital
Linkou, Taiwan

Figure 11. Server query.

Single Sign On Registration Phase

Smartcard ID
d0540011

Smartcard Password

ID
01011992

Server :
Billing

Register



Chang Gung Memorial Hospital
Linkou, Taiwan

Figure 12. Registration with specific server.

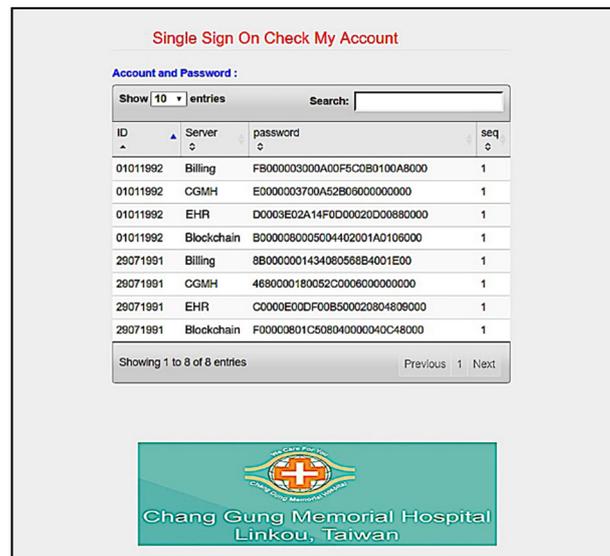


Figure 13. Account checking.

11. Conclusions

The use of 5G-enabled WSN applications in IoT architecture has gained a lot of attention from the scientific community. E-health system allows e-health users to store and share their data in a more convenient way compared to the traditional healthcare system. By the support of 5G technology, healthcare data produced from sensor nodes are efficiently transited in e-health system for efficient services, better analysis reports, and faster access to treatment. In this paper, we propose a three-factor fast authentication scheme with time bound and user anonymity for multi-server e-health systems in 5B-based wireless sensor networks. Three-factor authentication scheme combining biometrics, password, and smart card ensures a high security communication for participating parties in sensor-enabled environments. User anonymity is preserved during authentication process of our protocol. Besides, the proposed protocol introduces a fast authentication for accelerating communication process. This protocol is also designed with multi-server architecture that helps save database cost and alleviate network load. In addition, time-bound authentication introduced in the proposed protocol is suitable for various scenarios in healthcare. Security proof and performance analysis results show that our work can resist more attacks and bear a rational computational cost compared to its predecessor works.

Author Contributions: Conceptualization, A.M.-K.W., C.-L.H., and T.-V.L.; protocol, C.-L.H. and M.-C.H.; GNY logic, C.-L.H., M.-C.H., and T.-V.L.; AVISPA tool, C.-L.H. and T.-V.L.; semantic security analysis, T.-V.L. and T.-W.L.; performance analysis, T.-V.L. and T.-W.L.; implementation, C.-L.H. and T.-V.L.; supervision, C.-L.H.; and funding acquisition, A.M.-K.W. and C.-L.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by Chang Gung Memorial Hospital under Grant Nos. CMRPG5D0183 and CMRPD3D0063 and Ministry of Science and Technology in Taiwan under Grant Nos. MOST-105-2923-E-182-001-MY3, MOST-107-2221-E-182-006, and MOST-108-2221-E-182-011. This work was also funded in part by 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 Nos. EMRPD1I0481, EMRPD1H0421, and EMRPD1H0551.

Acknowledgments: We would like to thank Chang Gung University, Chang Gung Memorial Hospital, the Ministry of Science and Technology (MOST), and the Ministry of Education (MOE) in Taiwan.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahad, A.; Tahir, M.; Yau, K.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]

2. Panwar, N.; Sharma, S.; Singh, A.K. A survey on 5G: The next generation of mobile communication. *Phys. Commun.* **2016**, *18*, 64–84. [[CrossRef](#)]
3. Saha, C.; Dhillon, H. Millimeter Wave Integrated Access and Backhaul in 5G: Performance Analysis and Design Insights. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1. [[CrossRef](#)]
4. Cao, J.; Yu, P.; Ma, M.; Gao, W. Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. *IEEE Intern. Things J.* **2019**, *6*, 1561–1575. [[CrossRef](#)]
5. Renuka, K.; Kumar, S.; Kumari, S.; Chen, C.M. Cryptanalysis and Improvement of a Privacy-Preserving Three-Factor Authentication Protocol for Wireless Sensor Networks. *Sensors* **2019**, *19*, 4625. [[CrossRef](#)] [[PubMed](#)]
6. Porambage, P.; Schmitt, C.; Kumar, P.; Gurtov, A.; Ylianttila, M. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014.
7. Manatarinat, W.; Poomrittigul, S.; Tantatsanawong, P. Narrowband-Internet of Things (NB-IoT) System for Elderly Healthcare Services. In Proceedings of the 2019 5th International Conference on Engineering, Applied Sciences and Technology (ICEAST), Luang Prabang, Laos, 2–5 July 2019.
8. Zhu, Y.; Jia, G.; Han, G.; Zhou, Z.; Guizani, M. An NB-IoT-based smart trash can system for improved health in smart cities. In Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019.
9. Shi, Y.; Zhao, Y.; Xie, R.; Han, G. Designing a Structural Health Monitoring System for the Large-scale Crane with Narrow Band IoT. In Proceedings of the 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal, 6–8 May 2019.
10. Li, W.; Zhang, Q.; Zhang, Q.; Guo, F.; Qiao, S.; Liu, S.; Luo, Y.; Niu, Y.; Heng, X. 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.* **2019**, *8*, 177–186. [[CrossRef](#)]
11. Raj, D.A.; Kayalvizhi, S. Nb-iot based water meter. *Int. J. Recent Technol. Eng.* **2019**, *7*, 635–637.
12. Zhang, R.; Cui, S.; Zhao, C. *Design of a Data Acquisition and Transmission System for Smart Factory Based on NB-IoT*; Springer: Singapore, 2020; pp. 875–880.
13. Sun, C.; Cao, Y. *Design of Mushroom Humidity Monitoring System Based on NB-IoT*; Springer: Cham, Switzerland, 2020; pp. 281–289.
14. Guo, X.; Liu, B.; Wang, L. Design and Implementation of Intelligent Manhole Cover Monitoring System Based on NB-IoT. In Proceedings of the 2019 International Conference on Robots & Intelligent System (ICRIS), Haikou, China, 15–16 June 2019.
15. Liu, Z.; Dai, Z.; Yu, P.; Jin, Q.; Du, H.; Chu, Z.; Wu, D. Intelligent station area recognition technology based on NB-IoT and SVM. In Proceedings of the 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), Vancouver, BC, Canada, 12–14 June 2019.
16. Praveen, M.; Harini, V. NB-IOT based smart car parking system. In Proceedings of the 2019 International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 14–15 March 2019.
17. Chávez-Ángeles, M.G. The ecological semantics of the IoMT: Modelling cyborgs networks for health policy. *Inform. Med. Unlocked* **2018**, *12*, 138–142. [[CrossRef](#)]
18. Haoyu, L.; Jianxing, L.; Arunkumar, N.; Hussein, A.F.; Jaber, M.M. An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. *Future Gener. Comput. Syst.* **2019**, *98*, 69–77. [[CrossRef](#)]
19. Sodhro, A.H.; Pirbhulal, S.; Sangaiah, A.K. Convergence of IoT and product lifecycle management in medical health care. *Future Gener. Comput. Syst.* **2018**, *86*, 380–391. [[CrossRef](#)]
20. Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless Body Area Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1658–1686. [[CrossRef](#)]
21. Huang, X.; Gao, X.; Yan, Z. Security protocols in body sensor networks using visible light communications. *Int. J. Commun. Syst.* **2016**, *29*, 2349–2363. [[CrossRef](#)]
22. Callegati, F.; Cerroni, W.; Ramilli, M. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Secur. Priv.* **2009**, *7*, 78–81. [[CrossRef](#)]
23. Malladi, S.; Alves-Foss, J.; Heckendorn, R. On Preventing Replay Attacks on Security Protocols. In *Proceeding International Conference on Security and Management*; University of Idaho: Moscow, ID, USA, 2002.

24. Adams, C. *Impersonation Attack*, in *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Ed.; Springer: Boston, MA, USA, 2005; p. 286.
25. Kumar, A.; Om, H. An improved and secure multiserver authentication scheme based on biometrics and smartcard. *Digit. Commun. Netw.* **2018**, *4*, 27–38. [[CrossRef](#)]
26. Zhang, L.; Zhang, Y.; Tang, S.; Luo, H. Privacy Protection for E-Health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement. *IEEE Trans. Ind. Electron.* **2018**, *65*, 2795–2805. [[CrossRef](#)]
27. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [[CrossRef](#)]
28. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [[CrossRef](#)]
29. Zhang, G.; Poon, C.; Zhang, Y.-T. A Review on Body Area Networks Security for Healthcare. *ISRN Commun. Netw.* **2011**, *2011*. [[CrossRef](#)]
30. Aftab, M.U.; Ashraf, O.; Irfan, M.; Majid, M.; Nisar, A.; Habib, M.A. A Review Study of Wireless Sensor Networks and Its Security. *Commun. Netw.* **2015**, *7*, 8. [[CrossRef](#)]
31. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamshirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [[CrossRef](#)]
32. Gope, P. *Security and Privacy in Wearable Body Sensor Networks*, in *Wearable Sensors*; IOP Publishing: Bristol, UK, 2017; pp. 7-1–7-13.
33. Khan, R.A.; Pathan, A.-S.K. The state-of-the-art wireless body area sensor networks: A survey. *Int. J. Distrib. Sensor Netw.* **2018**, *14*, 1550147718768994. [[CrossRef](#)]
34. Chaudhary, S.; Singh, A.; Chatterjee, K. Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey. *Int. J. Comput. Intell. IoT* **2019**, *2*.
35. Sahoo, S.S.; Mohanty, S. A Lightweight Biometric-based Authentication Scheme for Telecare Medicine Information Systems Using ECC. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT, Bangalore, India, 10–12 July 2018.
36. Hirtan, L.; Krawiec, P.; Dobre, C.; Batalla, J.M. Blockchain-based approach for e-health data access management with privacy protection. In Proceedings of the IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, Limassol, Cyprus, 11–13 September 2019.
37. Aghili, S.F.; Mala, H.; Shojafar, M.; Peris-Lopez, P. LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT. *Future Gener. Comput. Syst.* **2019**, *96*, 410–424. [[CrossRef](#)]
38. Fan, C.; Lin, Y. Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics. *IEEE Trans. Inform. Forensics Secur.* **2009**, *4*, 933–945. [[CrossRef](#)]
39. Jiang, Q.; Khan, M.K.; Lu, X.; Ma, J.; He, D. A privacy preserving three-factor authentication protocol for e-Health clouds. *J. Supercomput.* **2016**, *72*, 3826–3849. [[CrossRef](#)]
40. Zhang, L.; Zhu, S.; Tang, S. Privacy Protection for Telecare Medicine Information Systems Using a Chaotic Map-Based Three-Factor Authenticated Key Agreement Scheme. *IEEE J. Biomed. Health Inform.* **2016**, *21*, 465–475. [[CrossRef](#)]
41. US-CERT. *Understanding Denial-of-Service Attacks*; Department of Homeland Security: Washington, DC, USA, 2019.
42. Negra, R.; Jemili, I.; Belghith, A. Wireless Body Area Networks: Applications and Technologies. *Procedia Comput. Sci.* **2016**, *83*, 1274–1281. [[CrossRef](#)]
43. Li, H.; Tan, J. Heartbeat-Driven Medium-Access Control for Body Sensor Networks. *IEEE Trans. Inform. Technol. Biomed.* **2010**, *14*, 44–51.
44. Vandana, T.S.; Venkateshwarlu, S.; Teja, C.V.R. Exploration of an Intelligent and Secure Wireless Body Area Networks for Health Monitoring. *Int. J. Recent Technol. Eng.* **2019**, *8*. [[CrossRef](#)]
45. Elhayatmy, G.; Dey, N.; Ashour, A.S. Internet of Things Based Wireless Body Area Network in Healthcare. In *Internet of Things and Big Data Analytics toward Next-Generation Intelligence*; Dey, N., Hassanien, A., Bhatt, C., Ashour, A., Satapathy, S., Eds.; Springer: Cham, Switzerland, 2018.
46. Ghamari, M.; Janko, B.; Sherratt, R.S.; Harwin, W.; Piechockic, R.; Soltanpur, C. A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments. *Sensors* **2016**, *16*, 831. [[CrossRef](#)]

47. Shah, A.M.; Abdelmaboud, A.; Mahmood, K.; ul Hassan, M.; Saeed, M.K. eHealth WBAN: Energy-Efficient and Priority-Based Enhanced IEEE802.15.6 CSMA/CA MAC Protocol. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 82–87. [[CrossRef](#)]
48. Rehman, O.; Javaid, N.; Bibi, A.; Khan, Z.A. Performance Study of Localization Techniques in Wireless Body Area Sensor Networks. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25 June 2012.
49. Smith, H.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Quart.* **2011**, *35*, 989–1015. [[CrossRef](#)]
50. Buchanan, T.; Paine, C.; Joinson, A.N.; Reips, U.D. Development of measures of online privacy concern and protection for use on the Internet. *J. Am. Soc. Inform. Sci. Technol.* **2007**, *58*, 157–165. [[CrossRef](#)]
51. Rabin, M.O. *Digitalized Signatures and Public-Key Functions as Intractable as Factorizations*; Massachusetts Institute of Technology: Cambridge, MA, USA, 1979.
52. Gong, L.; Needham, R.; Yahalom, R. Reasoning about belief in cryptographic protocols. In Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 7–9 May 1990.
53. The AVISPA Team. Automated Validation of Internet Security Protocols and Applications (AVISPA 1.1). 2006. Available online: <http://www.avispa-project.org> (accessed on 29 April 2020).
54. Von Oheimb, D. The high-level protocol specification language HLPSP developed in the EU project AVISPA. In Proceedings of the APPSEM 2005 Workshop, Munich, Germany, 12–15 September 2005.
55. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Park, Y.; Tanwar, S. Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Networks. *IEEE Access* **2018**, *6*, 20673–20693. [[CrossRef](#)]
56. Nongbri, I.; Hadem, P.; Chettri, S. A Survey on Single Sign-On. *Procedia Technol.* **2018**, *6*, 134–139.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).