A Novel Three-Factor Authentication Protocol for Multiple Service Providers in 6G-Aided Intelligent Healthcare Systems

TUAN-VINH LE¹, CHUNG-FU LU¹, CHIEN-LUNG HSU²,³,⁴,⁵,⁶,⁷, TRUNG K. DO⁸, YEN-FANG CHOU⁷, AND WEI-CHENG WEI⁴

¹Department of Information Management, Chihlee University of Technology, New Taipei City 220305, Taiwan
²Graduate Institute of Management, Chang Gung University, Taoyuan 33302, Taiwan
³Master of Science Degree Program in Innovation for Smart Medicine, Chang Gung University, Taoyuan 33302, Taiwan
⁴Department of Information Management, Chang Gung University, Taoyuan 33302, Taiwan
⁵Healthy Aging Research Center, Chang Gung University, Taoyuan 33302, Taiwan
⁶Department of Visual Communication Design, Ming Chi University of Technology, New Taipei City 24301, Taiwan
⁷Department of Nursing, Taoyuan Chang Gung Memorial Hospital, Taoyuan 33044, Taiwan
⁸Department of Economics, Danang Architecture University, Danang 50217, Vietnam

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

This work was supported by the Ministry of Science and Technology, Taiwan, under Grant MOST-110-2221-E-182-049 and Grant MOST-110-2218-E-218-001-MBK.

ABSTRACT 6G technology is now attracting many scientific researchers due to its prominent features including high mobility, high data rate, high operating frequency, and ultra-low end-to-end delay. Compared to the 5G, 6G has certain advantages that can transform smart healthcare to a new advanced intelligent healthcare system, where multiple issues and concerns of the services (e.g., slow ambulance response) are effectively resolved. In such a communication system, patients and service providers communicate with each other via an open internet channel. Since the healthcare data is important and very sensitive, security and privacy in the healthcare network become prominent. In this paper, we introduce a 6G-aided intelligent healthcare environment. Our work also proposes a solution called Centerless User-Controlled Single Sign-On (CL-UCSSO) for achieving a convenient and cost-saving communication in a multi-server system constructed. A three-factor mechanism (combining smart card, password and biometrics) and time bound property are integrated to design the protocol with fast authentication that allows patients and providers to efficiently establish secure communications. Security proof of the proposed protocol is provided using well-known verification tools including RoR model, AVISPA simulation and BAN logic. Results of performance comparisons on various aspects show that our work provides more functionalities and incurs less cost compared with the related works.

INDEX TERMS 6G-IoE, CL-UCSSO, fast authentication, intelligent healthcare, multi-server, patient privacy, time bound.

I. INTRODUCTION
5G communication technology has been successfully deployed in many countries and had a big impact on our society with diverse application scenarios [1]. However, for revolutionizing our daily life with higher quality of service (QoS) and quality of life (QoL), it still has certain drawbacks. For instance, holographic communication cannot be supported by 5G due to lower data rate [2], [3]. 6G technology is now attracting many scientific researchers due to its prominent features including high mobility, high data rate, high operating frequency and ultra-low end-to-end delay [2], [4]. Using the terahertz (THz) signal, 6G will provide a bandwidth three-time higher than the one of 5G [5], [6]. New Radio Lite (NR-Lite) of the 5G will be replaced by Intelligent Radio (IR) for intelligent communications [7]. More detailed comparisons between 5G and 6G were specifically discussed in [8]. 6G is expected to be fully backed by the satellite. In the core network, the Internet of Things (IoT) architecture will soon be replaced by the
Internet of Everything (IoE). From 2030 onward, 6G is also expected to revolutionize information management systems in various fields [9]. At present, 6G technologies have already been started for timely development in several countries, such as United States, China, Japan, Finland, etc. [10]–[12].

The current smart healthcare systems still cannot provide perfect medical services due to some unavoidable problems in terms of time and space. Ambulance service is taken as an example. In many cases, patients died in ambulance before reaching the hospital or even before the ambulances reached the spot. The reason is that we still lack an intelligent healthcare system with efficient accident detection mechanism [2]. This system requires a real-time detection that can provide services on time and on the spot. Intelligent healthcare is implemented partially till date with traditional smart systems. Moreover, the rural connectivity is still a challenge for the 5G as well as healthcare [13]. 6G technology is proposed with strict requirements for healthcare that address all connection issues and fully support an intelligent environment, which cannot be achieved by the 5G. The requirements include data rate of $\geq 1$ Tbps, operating frequency of $\geq 1$ THz, end-to-end delay of $\leq 1$ ms, reliability of $10^{-9}$, mobility of $\geq 1000$ km/h and wavelength of $\leq 300\mu$m [4]. These advantages truly support intelligent healthcare driven by artificial intelligence (AI) technology that enables various intelligent entities (IE) [14]. Services in the intelligent healthcare would include telesurgery, patient monitoring in Wireless Body Sensor Networks (WBSNs), holographic communications, augmented/virtual reality (AR/VR), etc. [2]. Hospital-to-Home (H2H) services will be implemented using mobile hospitals established by intelligent vehicles. These services are especially important when potential epidemic or pandemic (for instance, COVID-19) outbreaks. Furthermore, Computed Tomography (CT) or Magnetic Resonance Imaging (MRI) services will be more efficiently provided using intelligent equipment. With the above strict requirements and advantages supporting various technologies including IE, AI, IoE, real-time mechanism, etc., 6G will completely transform the current smart healthcare to the new advanced intelligent healthcare. It would further construct a new communication environment called Intelligent Internet of Medical Things (IoMT) [15].

Since communications in the 6G-aided intelligent healthcare systems are carried out via public internet channels and the health data is extremely sensitive, security and privacy issues are prominent concerns. Adversaries may perform various attacks (e.g., man-in-the-middle (MITM) attacks, etc.), which violate patient privacy or directly obstruct the healthcare systems [16]. In addition, legitimacy of the doctors (healthcare providers) in the communications also needs to be taken into account for avoiding fraud services. Two-factor authentication mechanism integrating user’s password and smart card was discussed in many works to prevent possible risks [17], [18]. Nevertheless, the mechanism may not be robust once the adversaries effectuate password guessing attacks or stolen smart card attacks [16]. Along with the advent of intelligent systems and the need of healthcare, there would be an increasing number of medical services provided by multiple providers. The healthcare providers may include doctors, pharmacists, pathologists or data scientists who manage respective servers in the systems. Under this circumstance, the design of single-server architecture has been unable to meet the needs of users where they may want to use a massive number of services [17]. Thus, it is needed to design a more secure and functional authentication protocol that can efficiently address all the concerns. In addition, the protocol should also be designed with reasonable costs consumed.

A. RELATED WORKS

Based on Rabin cryptosystem [19], Jiang et al. [20] introduced a three-factor authentication protocol internet-integrated wireless sensor networks, which addresses the drawbacks of the two-factor mechanism. Another research proposed by Shuai et al. [21] also employed the Rabin system to design a secure password-based authentication protocol with forward secrecy for industrial IoT (IIoT). Recently, Lin and Hsu [22] proposed an authenticated key agreement protocol for 5G-based telemedicine systems. Their work did not provide user anonymity as the identity is masked during the authentication phase via open channel. Lin et al. [23] proposed a smart card-based authentication scheme with multi-server architecture and user privacy protection for 5G-IoT healthcare systems. The public parameter $N_i$ for user verification in the first communication round of their scheme is revealed to the public while no timestamp is employed. Their work therefore is not robust to Denial of Service (DoS) attacks. Meshram et al. [24] introduced a smart card and password-based user authentication protocol based on extended chaotic maps. In the authentication procedure of their protocol, the server further stores an additional value $SB_i$. Therefore, the work may be vulnerable to desynchronization attacks. Although the works of [23] and [24] can achieve user anonymity, both did not provide user untraceability because the messages in their schemes contains some constant values. Based on these values, adversaries may guess identity of the user. Furthermore, Lin et al. [23] is not free from stolen smart card attacks since users’ private credentials are directly stored in the card without being masked. Similarly, the work proposed by Le and Hsu [16] only prevents the smart card capture attacks partially as the adversaries can perform power analysis to obtain passwords of the users [25]. In this way, multiple attacks can be performed once they obtain users’ biometrics. Thus, three-factor authentication mechanism in their work will become ineffective. Le and Hsu [16] also did not provide password update solution to enhance the security. This solution was proposed in another anonymous three-factor authentication protocol introduced by Xu et al. [26]. Dharminder et al. [27] introduced a construction of authenticated key exchange protocol based on Rivest-Shamir-Adleman (RSA) encryption [28] for healthcare services. Thakare and Kim [29] presented a cryptographic protocol for user authentication in IoT environments.
Besides, Tanveer et al. [30] proposes an anonymous and reliable authentication protocol for smart grid systems. All above-mentioned works, except [26] and [16], did not design their protocols with three-factor authentication. Moreover, only [26] and [16] achieves user untraceability during the communication in the protocols. Multi-server architecture, a solution that affiliates communications among multiple users and multiple servers, was only introduced in the proposals of [16], [23], [26].

B. CONTRIBUTIONS

In this article, we propose a user anonymity-preserving three-factor authentication protocol for multi-server intelligent healthcare systems enabled by 6G communication technology. Specifically, our work allows the patients and the servers to mutually authenticate each other, so that they can securely establish a reliable shared session key. Efficiency of the communication in the proposed work is also taken into account. Main contributions of this paper can be summarized as follows.

- We introduce a 6G-IoE intelligent healthcare application in a multi-provider environment. In particular, 6G helps in transforming smart healthcare (aided by the traditional 5G technology) to the intelligent one truly driven by AI. In the proposed model, healthcare services are provided by multiple servers along with the help of intelligent objects, in a real-time manner.
- We design the protocol with three-factor mechanism (something you know, something you have and biometrics (something you are)), which assures a high security for the authentication. Rabin cryptosystem is employed in the protocol, which improve the performance of the RSA’s encryption process. A perfect user privacy is achieved with forward secrecy of the session keys, user anonymity, user untraceability and message unlinkability. The generated session keys are used to secure the real time healthcare services that are achieved by the advantages of 6G discussed in Section I. Fast authentication is proposed for allowing users and servers to quickly compute additional shared session keys for subsequent communications within a short time. This solution is carried out with fewer steps and simplified computation after the initial authentication. Therefore, it can accelerate the communication processes and is suited for AI-driven low-power devices in the 6G network [31]. In our work, the users can update their password to assure a higher security. We also considered biometrics update function in the protocol. However, the biometrics is a unique identity of each individual; and in healthcare scenario, an account should belong to a single person only for privacy preservation. Updating biometrics (especially face or iris) is nearly equivalent to adding a new user. Instead, the user can create new account for this purpose. Therefore, biometrics change is not needed in the proposed work. The designed protocol is much less complex without this function, but with a similar security assured.
- As mentioned, multi-server architecture is employed in the proposed architecture with multiple healthcare service providers. The number of servers depends directly upon the number of services that a patient wants to use. Our protocol allows the users to store a single set of credentials registered with multiple servers in a smart card. They only need to enter the credentials once per session then choose specific servers from the list in the device for using multiple services. In this way, a User-Controlled Single Sign-On (UCSSO) function is achieved. It significantly alleviates storage cost and computation cost. The proposed UCSSO is designed without the participant of registration center. This solution also reduces communication cost, as well as security risks where adversaries may attack the center to compromise the whole system. A secure and efficient centerless (CL)-UCSSO is established. When the proposed CL-UCSSO is implemented for the multi-server architecture, the number of users may drastically increase due to its convenience and functionality. Since the introduced 6G-aided network provides tremendously high bandwidth, massive patients in the proposed protocol can simultaneously communicate with multiple servers in an efficient manner.
- In healthcare scenarios, a user may use services provided by multiple servers. Each provider may provide services with different working times. For instance, a remote doctor provides a daily service from 9:00 to 12:00; working time of a local doctor is from 14:00 to 18:00; while a nurse starts the work at 11:00 every day. Thus, a time-bound-based authentication is introduced in our work, which facilitates communications of the allotted services in such scenarios. Time-allotted services provide a more efficient healthcare process. This solution also addresses bottleneck issues in online communications when massive patients may request the services at the same time. In addition, this authentication function increases the protocol security because some time-bound-related parameters (specified later in Section IV) are kept secret to the users only.
- Security certificate of our protocol is provided using three formal verification tools: Real-or-Random (RoR) model, Automated Validation of Internet Security Protocols and Applications (AVISPA) software, and Burrows-Abadi-Needham (BAN) logic. Moreover, a further informal analysis is also included to explain various well-known security attacks (e.g., replay attacks, MITM attacks, etc.) that can be prevented by our protocol.
- A comprehensive performance comparison of our work and the related works is presented, in terms of various aspects including functionality, computation cost, communication cost, and storage cost. The analytical results indicate that our protocol consumes less energy and...
lower cost but provides more functionalities, compared with its competitive works.

C. PAPER ORGANIZATION

The remainder of this article is structured as follows. Section II, we provide some preliminaries employed in the proposed protocol. Section III, we present the system construction including architecture model and adversarial capabilities. Section IV, we specifically present the proposed protocol. Security analysis and performance evaluation of our work are provided in Section V and Section VI, respectively. Finally, we conclude the work and discuss some future research directions in the last section of the article.

II. PRELIMINARIES

We discuss some important technical preliminaries including biohash function, time bound, security assumption and formal security model, used in our proposal.

A. BIOHASH FUNCTION

Biohash function is designed to map the biometrics of an individual to a specific binary string that provides the tolerance of noise [32]. It provides the same security features with the traditional one-way hash functions [33]. Compared to other ideas (e.g., fuzzy extractor) that address biometrics noise issue, biohash function bears a much less computation cost [32].

Definition 1: Suppose $BIO$ and $BIO'$ are the original and the newly input biometric templates of an individual, respectively. Therein, $BIO'$ is not completely identical to $BIO$, but the difference is still within a bearable threshold. With the given biohash function $h_{bio}$, we can obtain: $h_{bio}(BIO) = h_{bio}(BIO')$.

B. TIME BOUND PROPERTY

We define the time bound used for the authentication in the proposed protocol as follows.

Definition 2: Suppose we have time points $t, t_1, t_2 \in \{1, 2, \ldots, 24\text{ (hours)}\}$ where $(t_1, t_2)$ is a time bound, and $t_1 \leq t_2$; $A = h^{t_1-1}(\square)$ and $B = h^{24-t_2}(\triangle)$ where $\square$ and $\triangle$ are some arbitrary values, $h$ is a one-way hash function. The value $T = h(h^{t_1-1}(A)||h^{t_2-t_1}(B)) = h(h^{t_1-1}(h^{t_1-1}(\square))||h^{t_2-t_1}(h^{24-t_2}(\triangle)))$ exists when and only when $t_1 \leq t \leq t_2$.

C. SECURITY ASSUMPTIONS

Security assumptions used in our protocol are defined as follows.

Definition 3 (Integer Factorization Problem): Suppose there is a positive composite integer $n$ and two distinct primes $(p, q)$, where $n = p \cdot q$. The value $n$ must be sufficiently large, e.g., 1024 bits. The Integer Factorization Problem (IFP) explains that it is mathematically hard to retrieve $p$ and $q$ from the given $n$.

Definition 4 (Minimum Trust): Each healthcare server is accepted as trustworthy, because users (patients) register their secret information to gain services from them.

D. FORMAL SECURITY MODEL

We employ Real-or-Random (RoR) model for a formal security proof in our work. RoR model is a well-known tool used to analyze the advantage of adversaries in breaking cryptographic protocols [34]. Suppose there exits two parties, patient $P$ and healthcare server $S$, carrying out their communication via an open channel. An adversary $A$ can make the following various queries to perform the attacks, where $C$ is a protocol challenger and $M$ is a communicated message.

- Send($C, M$): This active attack allows $A$ to request $M$ to $C$, and $C$ replies to $A$ in accordance with the rules of the protocol.
- Execute($P, S$): In this passive attack, eavesdrops the transmitted messages between $U$ and $S$.
- Reveal($C$): attempts to retrieve the secret session key computed by $C$ to $A$.
- Corrupt ($P, a$): In a protocol with three-factor authentication, this query returns $P$’s password (if $a = 1$), biometrics (if $a = 2$), and parameters stored in a smart card and an intelligent device (if $a = 3$) to $A$.
- Test($C$): $A$ requests $C$ for the secret session key $c$ probabilistically replies to $A$ based on the outcome of a tossed coin $b$.

Definition 5: Let $Adv_{\text{GHC}}^{\text{SGHC}}$ be the advantage of running in polynomial time in breaking the semantic security system of our work; $\text{GHC}$ and $b'$ denotes the proposed protocol (for 6G healthcare services) and the guessed bit of session keys, respectively. We can obtain, $Adv_{C}^{\text{SGHC}} = |2Pr[b' = b] - 1|$.

III. SYSTEM CONSTRUCTION

We describe the system model of the proposed protocol in this section. It primarily presents the communications enabled in a 6G-aided intelligent healthcare system. In addition, adversarial capabilities are also discussed.

A. ARCHITECTURE MODEL

The proposed model includes two main entities, namely, patient $P_i$ and healthcare provider $S_j$, who are communicating in a multi-server environment. As shown in Figure 1, $P_i$ can
carry out the CL-UCSSO that uses a single set of credentials (stored in the smart card) to directly gain services from multiple $S_j$, without the participation of a central party. The services include medical treatment, prescription, H2H, MRI, CT scan, etc. They may be provided by local doctors in a hospital or by remote doctors. We take the patient monitoring service carried out through the WBSN as an example. The network consists of multiple medical sensors (e.g., respiratory rate, fall detection, etc.) worn by $P_i$ [35]. The sensors collect various health data and transmit it to $P_i$’s mobile device with the support of a wireless technology (e.g., Wi-Fi, ZigBee or Bluetooth). Then, the sensing data is securely transmitted to $S_j$ via the IR signal of the 6G network for further communications. The service provides a continuous real-time monitoring on $P_i$ without any constraints on patients’ normal daily life activities [36]. With extremely high data rate, the 6G also provides faster speed of data transfer (especially large image files produced by MRI or CT scanners) for timely treatments. In addition, healthcare data may be stored for further services such as pathology or data analysis. It is noted that the mobile devices (of $P_i$), MRI, and CT machines (equipped for respective services at the hospital) and so on are AI-enabled intelligent entities. Other than smart functionalities of a traditional device, they have ability to automatically launch healthcare services when noticing unusual symptoms from $P_i$. For instance, the mobile device would launch a H2H service on a fall or a respiratory depression detected. Whereas the MRI machine would automatically communicate with the most appropriate doctor for the service once it finds abnormal signal intensity on the images. For securing the communication between $P_i$ and $S_j$, the proposed protocol allows them to establish an authenticated session key used to encrypt the communicated messages. To this end, $P_i$ chooses a device to register with $S_j$ using smart card, password and biometrics for achieving a three-factor authentication mechanism. Time bound property is also integrated to authenticate $P_i$ at specific time points of services. We further design a fast procedure of key negotiation after the initial authentication process, so that $P_i$ and $S_j$ can quickly compute the multiple new shared keys. This solution significantly accelerates communication process and reduces computational load on low-power devices in the proposed 6G-IoE healthcare environment.

B. ADVERSARIAL CAPABILITIES

Possible attacks in the healthcare systems can induce tremendous consequences, such as patient privacy violation, financial loss, system obstruction, etc. The attacks may also directly affect the treatment process and reduce the quality of medical services [35]. In the proposed work, we have observed various potential risks, and assume that $A$ has the following capabilities to break the security system [37], [38].

- $A$ has the control over the public communication channel where they can intercept, delete, insert or replay any transcripts conveyed between $P_i$ and $S_j$.
- $A$ may steal $P_i$’ smart card and intelligent device, then perform power analysis attacks to extract the secret parameters.
- $A$ attempts to attack the ciphertexts communicated between $P_i$ and $S_j$ in the past once they have obtained the session key in current communication session.
A. SYSTEM INITIALIZATION

Our protocol employs Rabin cryptosystem for an efficient computation as its encryption operation (based on modular squaring operation) is much faster than the RSA cryptosystem [21]. $S_j$ chooses two arbitrary large primes $p_j, q_j$ as server’s private keys, then compute the corresponding public key $n_j = p_j q_j$, where $p_j \equiv q_j \equiv 3 \pmod{4}$. Based on the IFP assumption specified in Definition 3, it is computationally hard to derive $p_j$ and $q_j$ from $n_j$. $S_j$ also randomly selects $x_j$ as its master secret key.

B. REGISTRATION

This phase is conducted via a secure channel, in which $P_i$ registers with $S_j$ as a legitimate patient for using the service. As shown in Fig. 2, both sides perform the following steps to complete the registration procedure.

Step R1: $P_i$ first inputs the identity $ID_i$, password $PW_i$ and imprints the biometrics $B_i$. $P_i$ chooses a random number $\sigma$, and computes $W = h(h(ID_i[|\sigma])h(PW_i[|\sigma]))$ and $PB = h(ID_i[|h_{bio}(B_i)])$. Next, $P_i$ transmits $\{ID_i, W, PB\}$ to $S_j$.

Step R2: Upon receiving $\{ID_i, PB, W\}$, $S_j$ chooses a symmetric encryption algorithm (e.g., Advanced Encryption Standard (AES) [39]) then uses the secret key $x_j$ to compute $z_j = SE_{x_j}(h(x_j))|ID_i|W|PB)$. Next, $S_j$ determines a time bound $(t_1, t_2)$, and computes $TB_1 = h^{t_1−1}(h(ID_i)|x_j|W))$ and $TB_2 = h^{t_2−1}(h(ID_i)|x_j|PB))$. $S_j$ then stores $ID_i$ in its database $DB_j$, and sends $\{n_j, z_j, t_1, t_2, TB_1, TB_2\}$ to $P_i$.

Step R3: Upon receiving the above message, $P_i$ computes $V = h(\sigma)|PW_i|PB)$ and $\varepsilon_j = \sigma \oplus z_j$. Next, $P_i$ stores $\{\varepsilon_j, n_j, t_1, t_2, TB_1, TB_2\}$ and $\{\sigma, V\}$ in the device $HD_i$ and the card $SC_i$, respectively. $SC_i$ can be either a traditional or a contactless smart card.

C. LOGIN AND AUTHENTICATION

In this phase, $P_i$ is allowed to login and mutually authenticate with $S_j$ for using its service. A fast authentication procedure is then provided so that $P_i$ can quickly perform the mutual authentication with $S_j$ to compute the new session keys. Each fast authentication is carried out based on the parameters from the previous session, without the complex procedure of the initial process. This phase consists of three procedures including login, initial authentication and fast authentication, which are carried out via an open channel. The whole phase is depicted in Fig. 3.

1) LOGIN

$P_i$ inserts $SC_i$, inputs $ID_i^*, PW_i^*$, and imprints $B_i^*$. $SC_i$ computes $PB^{*\varepsilon} = h(ID_i^*|h_{bio}(B_i^*))$ and checks $V = h(\sigma)|PW_i^*|PB^{*\varepsilon})$. $P_i$ chooses a server $S_j$ and computes $A_1 = h(h^{t_1−1}(TB_1))|h^{t_2−1}(TB_2)|PB^{*\varepsilon})$. Thereafter, $P_i$ randomly chooses a number $r$ and an integer $v$ then computes $F = h^r(r)$, $z_j = \sigma \oplus \varepsilon_j$, a ciphertext $C_1 = (A_1||F||z_j||ID_i^*|T_i)^v modn$. $P_i$ transmits the login request message $C_1$ to $S_j$.

2) INITIAL AUTHENTICATION

There are two steps in this procedure in which $P_i$ and $S_j$ mutually authenticate each other for an initial shared session key.

Step IA1: Upon the received message, $S_j$ uses its private keys $p_j, q_j$ to decrypt $C_1$ and obtains $\{A_1, F, z_j, ID_i^*, T_i\}$. $S_j$ checks if the timestamp $T_i$ is valid. If the check holds, $S_j$ uses $x_j$ to decrypt $z_j$, and confirms $ID_i^* = ID_i$ and $h(x_j)$. Next, $S_j$ computes $X = h(ID_i)|x_j|W)$ and $Y = h(ID_i)|x_j|PB)$ to check $A_1 = h(h^{t_1−1}(X))|h^{t_2−1}(Y)|PB)$. If there is a match, $S_j$ computes $A_2 = h(F)|T_i$, a session key $SK = h(F)|z_j)$, and a ciphertext $C_2 = SE_{SK}(A_2||T_i)$. $C_2$ is transmitted to $P_i$ for the next step.
Step IA2: Upon the received $C_2$, $P_i$ computes $SK = h(F||z_j)$ and uses it to decrypt $C_2$. $P_i$ checks the timestamp $T_j$ and $A_2 = h(F'||T_j)$. If the checks hold, a session key $SK$ is established between $P_i$ and $S_j$.

### 3) FAST AUTHENTICATION

Based on the parameters $r$, $v$, $F$ and session key $SK$ in the previous sessions, $P_i$ and $S_j$ can quickly authenticate and compute new shared session keys.

**Step FA1:** $P_i$ enters $ID_i'$, $PW_i'$ and imprints $B_i'$. $SC_i$ computes $PB^* = h(ID_i' || h_{bio}(B_i'))$ and checks $V \doteq h(\sigma|PW_i'||PB^*)$. Then $P_i$ computes $F_e = h^{(v-\epsilon)}(r)$ where $\epsilon$ runs from 1 to $v$. If $\epsilon > v$, the initial authentication is recalled, otherwise, $P_i$ computes a ciphertext $\alpha_e = SE_{SK}(F_e)$. Next, $P_i$ transmits $\alpha_e$ to $S_j$.

**Step FA2:** Upon receiving the message, $S_j$ uses $SK$ to decrypt $\alpha_e$ and checks $h(F_e) \doteq F$. If there is a match, $F$ is replaced by $F_e$ for the next fast authentication. Thereafter, $S_j$ computes a new session key $SK_{new} = h(F_i||SK)$ and uses it to generate a ciphertext $\beta_e = SE_{SK_{new}}(F_e)$. $\beta_e$ is transmitted to $P_i$ for the next step.

![FIGURE 3. Login and authentication phase of the proposed protocol.](image1)

![FIGURE 4. Password update phase of the proposed protocol.](image2)
TABLE 2. Simulation of hash, reveal, test, corrupt, execute and send oracle queries.

| Query                  | Simulation Details                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Hash                   | If the record \((m_i, h(m_i))\) is found in the list \(L_h\), return \(h(m_i)\); otherwise, choose \(a' \in Z_p^*\) and add \((m_i, h'(m_i))\) into \(L_h\). A similar procedure is performed for \(L_s\), in which the query is initiated by \(A\). |
| Corrupt                | If \(C\) is in an accepted state, the session key formed by \(C\) is returned.                                                                                                                                     |
| Execute                | The query \(C\) is simulated as follows.                                                                                                                |
| Send                   | If \(a = 1\): the query outputs \(P_i\)'s password \(PW_i\). If \(a = 2\): the query outputs \(P_i\)'s biometrics \(B_i\). If \(a = 3\): the query outputs parameters stored in \(P_i\)'s smart card or intelligent device. |
| Send                   | The query \(C\) is simulated as follows.                                                                                                                |

Definition 9: Let \(\text{Adv}^{\text{IFP}}_A(t_A)\) be the advantage of \(A\) in breaking the IFP assumption. Since the assumption holds, \(\text{Adv}^{\text{IFP}}_A(t_A)\) is defined as a negligible probability with the execution time \(t_A\).

The following notations are used in the proof.
- \(h\): Length of each hash value.
- \(s\): Length of each random number.
- \(l\): Length of each biometrics value.
- \(q_h\): Total hash oracle queries.
- \(q_e\): Total \(\text{Send}\) queries.
- \(q_s\): Total \(\text{Execute}\) queries.
- \(L_H\): List of hash oracle outputs.
- \(L_S\): List of random oracle results.
- \(L_T\): List of transcripts communicated between \(P_i\) and \(S_j\).
- \(e_h\): Probability of biometrics false positive.
- \(C', s'\): Zipf parameters.

Definition 10: The value \(\max \left\{ C', q_e, q_s \left(\frac{1}{2^s}, e_h\right) \right\}\) is sufficiently small, so that \(A\) cannot guess the credentials of \(P_i\) [35].

Theorem 1: The proposed protocol is semantically secure because \(A\) only has the following negligible probability in breaking our security system.

\[
\text{Adv}^{\text{GHC}}_{\text{C}} \leq \frac{3q_s + q_e}{2^s} + \frac{q_s^2 + 10q_h}{2^h} + 2\max \left\{ C', q_e, q_s \left(\frac{1}{2^s}, e_h\right) \right\} + 2q_h(q_s + q_e + 1)\text{Adv}^{\text{IFP}}_A(t_A)
\]

Proof: We includes a number of six games in the proof including \(G_0, G_1, G_2, G_3, G_4, G_5, G_6\), in which probability of \(A\) gradually increases. The purpose of \(A\) is to obtain the bit \(b\) with the \(\text{Test}\) query after each of the games is finished. The success probabilities are denoted by \(Pr[S_i]\) where \(i = 0, 1, 2, 3, 4, 5\) are the events in respective games. In the games, \(A\) sets a simulator \(B\) to play the role of \(C\).

\(G_0\): This is the starting game. We assume this game is identical to the real protocol in random oracles. \(B\) tosses the coin \(b\) to start the game. We can obtain,

\[
\text{Adv}^{\text{GMECMH}}_{\text{C}} = |2Pr[S_0] - 1|
\]

\(G_1\): This game simulates all the queries specified in the model. Simulation of the queries are presented in Table 2 in accordance with the rule of the proposed protocol. In this way, the game creates three lists: \(L_H, L_A\) and \(L_T\). Due to the indistinguishability of \(G_0\) and \(G_1\), we have,

\[
Pr[S_1] = Pr[S_0]
\]

\(G_2\): We consider collision probability of the hash oracle and random oracle queries in this game, for all communicated transcripts between \(P_i\) and \(S_j\) in the login and initial authentication phases, there are two randomly generated numbers \(r\) and \(v\) included in two messages \(C_1\) and \(C_2\). Since \(v\) is an integer equal to the number of fast authentications, it should be an easy-to-find value. Therefore, we only consider \(r\) as a random number for the random oracle queries. Its collision probability is at most \(\frac{q_s+q_e}{2^{s+1}}\). Since \(G_1\) and \(G_2\) are indistinguishable, we can obtain,

\[
|Pr[S_2] - Pr[S_1]| \leq \frac{q_s + q_e}{2^{s+1}} + \frac{q_s^2}{2^{h+1}}
\]

\(G_3\): \(G_3\) is similar to \(G_2\) but the queries are executed for specific transcripts sent by \(P_i\) or \(S_j\). The game includes two cases of two corresponding communicated messages (\(C_1\) and \(C_2\)) as follows.

Case 1: This case considers the query \(\text{Send}(S_j, C_1)\). The messages \(C_1\) is computed from two hashes \((A_1, F)\) and another value \(z\), which totally results in a probability at most \(3\frac{2^h}{2^s}\). Note that we do not consider \(ID_{C_1}^x\) in \(C_1\) for the hash oracle as the identities are not hard to retrieved. Moreover, \(ID_{C_1}^x\) is stored in server's database and may be compromised.
by a privileged insider. In addition, the random number \( r \) contained in \( C_4 \) has the probability as \( \frac{q_h}{2^l} \).

**Case 2:** The query \( \text{Send}(P_1, C_2) \) is considered in this case. The values \( A_2 \) and \( SK \) contained the messages \( C_2 \) should be known to \( A \) for performing the attacks. The maximum probability is up to \( 2 \frac{q_h}{2^l} \).

Overall, we can obtain the following total probability,

\[
|Pr \{ S_3 \} - Pr \{ S_2 \} | \leq \frac{5 q_h}{2^l} + \frac{q_s}{2^l} \tag{5} 
\]

**G4:** We consider guessing attacks executed by \( A \) in this game. Three cases are presented as follows.

**Case 1:** In this case, \( A \) makes the \( \text{Corrupt}(P_1, 1) \) query to guess \( U_i \)'s password. Thereafter, \( A \) executes the \( \text{Send}(S_j, C_1) \) query for the attacks. Thus, the probability is at most \( (C', q_s') \).

**Case 2:** \( A \) executes the \( \text{Corrupt}(P_1, 2) \) query to retrieve \( P_i \)'s biometrics in this case. Since also makes the \( \text{Send}(S_j, C_1) \) query in this case, the maximum probability is up to \( \max\{q_h(\frac{1}{2^l}, \varepsilon_{bm})\} \).

**Case 3:** In this case, \( A \) attempts to break the IFP assumption (using \text{Hash} oracle queries) to compromise the message \( C_4 \). Its collision probability is at most \( q_hAdv_A^{IFP}(t_A) \).

Since \( G_3 \) and \( G_4 \) are identical without above attacks, we obtain,

\[
|Pr \{ S_4 \} - Pr \{ S_3 \} | \leq \max\{C', q_s', q_h(\frac{1}{2^l}, \varepsilon_{bm})\} + q_hAdv_A^{IFP}(t_A) \tag{6} 
\]

**G5:** In this final game, the forward secrecy property of the proposed work is considered. Based on the old transcripts sent by \( P_1 \) and \( S_j \), \( A \) makes \( \text{Execute}, \text{Send}, \text{and Hash} \) oracle queries to compromise the protocol. The game is simulated using the advantage in breaking the IFP assumption. Thereafter, the \text{Test} query is made to return the real session key to \( A \). Without considering the attack in this game, \( G_4 \) and \( G_5 \) are indistinguishable. Thus, we have,

\[
|Pr \{ S_5 \} - Pr \{ S_4 \} | \leq q_h(q_s + q_e)Adv_A^{IFP}(t_A) \tag{7} 
\]

After executing all the games, \( A \) guesses the bit \( b' \) with the probability of the \text{Test} query as follows.

\[
Pr \{ S_5 \} = \frac{1}{2} \tag{8} 
\]

According to Equations (3), (8), and applying the triangular inequality, we obtain,

\[
|Pr \{ S_0 \} - \frac{1}{2} | = |Pr \{ S_1 \} - Pr \{ S_2 \} | \\
\leq |Pr \{ S_1 \} - Pr \{ S_3 \} | \\
+ |Pr \{ S_2 \} - Pr \{ S_1 \} | \\
+ |Pr \{ S_3 \} - Pr \{ S_4 \} | \\
+ |Pr \{ S_4 \} - Pr \{ S_5 \} | \tag{9} 
\]

Based on Equations (2)-(9), we can achieve the following equation,

\[
\frac{1}{2} Adv_C^{SGMH} = |Pr \{ S_0 \} - \frac{1}{2} | 
\]

The final result can easily be obtained as follows,

\[
Adv_C^{SGMH} \leq 3q_s + q_e + \frac{q_h^2 + 10q_h}{2^l} + 2q_h(q_s + q_e)Adv_A^{IFP}(t_A) \tag{11} 
\]

Therefore, we claim Theorem 1, and the proposed protocol is semantically secure.

**B. FORMAL SECURITY VALIDATION USING AVISPA**

In this section, the widely accepted AVISPA simulation [16], [17] is employed to validate the security of the proposed protocol. It is a push-button tool that automatically verifies the resistance of cryptographic protocols to MITM attacks and replay attacks. The simulation is executed using the High-Level Protocol Specification Language (HLPSL) [40]. In our setting, AVISPA tool is installed with the Security Protocol Animator (SPAN), in order to build an interactive message sequence charts and friendly user interface.

Two main roles, Patient \( P \) and Server \( S \), are included in the simulation, which are fully specified using HLPSL code. Some important definitions and operations are described as follows. Since the communication in registration phase is carried out in a trusted channel, we define TrustedChannel as a symmetric key used to protect communicated messages. The registered information and user credentials are then stored by both sides in a secure manner. PublicKey is defined as a public key of Rabin cryptosystem. \( P \) uses PublicKey to compute the ciphertext \( C_1 \), which protects the parameters \{A1, F, Zj, IDi’, Ti\} in the login phase. Upon receiving \( C_1 \), S uses the corresponding private key inv(PublicKey), which is generated automatically by the tool, to decrypt \( C_1 \) and verifies \( P \)'s login request. After the user authentication, a session key \( SK \) is computed by \( S \). \( SK \) is used to compute the ciphertext \( C_2 \) for securely transmitting the parameters \{A2, Tj\} to \( P \), in order that \( P \) can complete the mutual authentication and key agreement. Note that some mathematical operators (e.g., subtraction) used in the protocol are specified as hash functions, as the HLPSL only supports XOR, concatenation and exponentiation operations.

The tool simulates cryptographic schemes with two security properties: secrecy and authentication. The secrecy property is to protect the secret parameters and user credentials in the registration phase. In this way, some secrecy goals considered for the verification of our protocol are described as follows.
• secrecy_of xj: Xj is the master secret key of the server. Therefore, it is specified to be kept secret to S only.
• secrecy_of o: since symbol o (the random value chosen by P in the registration phase) is not supported in the
  HLPcsl, we use O to represent it. O is kept secret to P.
• secrecy_of idi: IDi is the identity of the patient. To achieve user anonymity in the public channel, IDi is specified to be kept secret to P and S.
• secrecy_of pwi: PWi is the password of the patient. Therefore, it must be a secret known by P only.
• secrecy_of bi: Bi is the biometrics of the patient. It therefore is specified to be a secret known by P only.

In addition, the security of the time bound (T1, T2) should also be considered. However, it is not computationally hard to derive these values. The secrecy of {TB1, TB2} is primarily dependent on the security of {Xj, O, IDi, PWi, Bi} rather than {T1, T2}. Thus, we do not include the time bound in the specification of secrecy goals. Furthermore, the authentication property of the tool is provided to verify the legitimacy of the new random parameters generated in the login and authentication phase. We have the following goals of the mutual authentication between P and S considered in the simulation.

• authentication_on r: S authenticates P based on the randomly selected value R.
• authentication_on ti: S authenticates P based on the timestamp Ti generated by P.
• authentication_on tj: P authenticates S based on the timestamp Tj generated by S.

In addition to the basic roles P and S, Session and Environment roles are required in the simulation. Session role specifies all components used in a communication session by both P and S. The components include roles/agents (P and S), different keys (TrustedChannel, PublicKey and SK), mathematical and cryptographic operations, and communication channel established for P (SP, RP) and S (SS, RS). In Environment role, other than some similar parameters defined in Session role, there exists a protocol_id that denotes all constants associated with the stated security goals. The composition in this role specifies all communication sessions with the participation of an intruder i. The role also defines intruder knowledge including {p, s, publickey, ki (intruder’s own public key), inv(ki) (intruder’s own private key), ski (intruder’s symmetric key)}, so that the intruder can perform possible attacks on both P and S.

There are four backends for the verification results in the AVIPSA tool including Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP), SAT-based ModelChecker (SATMC), On-the-fly Model-Checker (OFMC), and Constraint Logic based Attack Searcher (CL-AtSe). Among them, the SATMC backend and TA4SP back-end do not support algebraic properties of modular exponentiation and XOR operator, which are required in the proposed protocol. Therefore, we execute the validation operation under the OFMC and CL-AtSe backends only. The OFMC approach is employed for efficient falsification of protocols and verification of a bounded number of communication sessions, without considering the generated messages of intruders. On the other hand, each step of the simulated protocol is modeled by constraints on the intruder’s knowledge in the CL-AtSe backend. After fully translating the protocol into HLPcsl language with sufficient specification, we run the tool using above two suitable backends. Based on the results shown in Figure 5, the stated secrecy goals and authentication goals are satisfied for specific communication sessions specified in the environment role. It is indicated that the simulated protocol has passed the verification. Thus, MITM attacks and replay attacks are prevented in our work.

C. AUTHENTICATION PROOF USING BAN LOGIC

BAN logic has been a well-known tool employed to provide mutual authentication proof of cryptographic protocols in many works [16], [17], [35]. Based on these rules provided by the tool and relevant logic analysis, we aim to prove that Pi and Si believe the session key computed is a secret shared value only known to them. The notations we use for the proof in this section are defined as follows.

• A |≡ X: A believes statement M.
• A ⊨ M: A sees statement M.
• (#M): The formula M is fresh.
• A |∼ M: A once said statement M.
• (M, N): M or N is one part of the formula (M, N).
• A ⊢ M: A has jurisdiction over statement M.
• (M)N: This represents M combined with the formula N.
• A ⊨ M K: B The shared key K is known only to A and B, and it is used for their communication.
• A ⊨ M B: Formula M is a secret known only by A and B. Only A and B can use M to authenticate each other.

Based on principle of the BAN logic, the following authentication goals should be satisfied for the proof.

Goal 1: Si |≡ (Sj SK Pj). Sj believes SK is a secret value sent by Pi, and SK is a shared key negotiated by them. (G1).

Goal 2: Pi |≡ (Pi SK Sj). Uj believes SK is a secret group key distributed by Sj, and Gkj is a shared key between them. (G2).

FIGURE 5. Validation results under OFMC and CL-AtSe backends.
In the login and authentication phase of our protocol, there are two communicated messages described as follows.

**Message 1 (C1).** $P_1 \rightarrow S_j : (AE_{\sigma_i}((A_1 || F || z_j || ID_1 || T_1)))$.

**Message 2 (C2).** $S_j \rightarrow P_i : (SE_{SK}(A_2 || T_j))$.

The idealized form of these messages used the proof procedure of the BAN logic is given below.

$C_1. P_1 \rightarrow S_j : ((A_1 || F || z_j || ID_1 || T_1)_a)$.  
$C_2. S_j \rightarrow P_i : ((A_2 || T_j)_b)$.  

Some logical rules of the tool that are used in our proposed protocol are specified as follows.

- **Seeing rule (R1):** $A_1 \in C P B \Rightarrow R_1(a) \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.
- **Interpretation rule (R2):** $A_1 \in B \Rightarrow M \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.  
- **Freshness rule (R3):** $A_1 \in B \Rightarrow M \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.  
- **Verification rule (R4):** $A_1 \in B \Rightarrow M \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.  
- **Jurisdiction rule (R5):** $A_1 \in B \Rightarrow M \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.  
- **Additional rule (R6):** $A_1 \in B \Rightarrow M \Rightarrow \frac{A_1 \leftarrow B \Rightarrow M}{A_1 \leftarrow B \Rightarrow M}$.

Consistent with the idealized form, the following assumptions are made for the proof of our protocol.

- **Assumption 1 (A1):** $S_j \equiv P_i \Rightarrow S_j$.
- **Assumption 2 (A2):** $S_j \equiv (T_i)$.  
- **Assumption 3 (A3):** $S_j \equiv P_i \Longrightarrow (A_1, T_i)$.  
- **Assumption 4 (A4):** $P_i \Longrightarrow (r, \sigma, \varepsilon)$.  
- **Assumption 5 (A5):** $P_i \equiv #(T_i)$.  
- **Assumption 6 (A6):** $P_i \equiv S_j \Longrightarrow (A_2, T_j)$.

Based on the above rules and assumptions, we analyze the procedure of our protocol and perform the mutual authentication proof in the following.

- **S1:** According to the message $C_1$, we have, $S_j \leftarrow ((A_1 || F || z_j || ID_1 || T_1)_a)$.  
- **S2:** Based on R1 and A1, we have, $S_j \equiv P_i \Rightarrow (A_1 || F || z_j || ID_1 || T_1)$.
- **S3:** Based on R2, we can obtain, $S_j \equiv P_i \Rightarrow (A_1 || F || z_j || T_1)$.
- **S4:** According to R3 and A2, we obtain, $S_j \equiv #((A_1 || F || z_j || T_1))$.  
- **S5:** Based on R4, we obtain, $S_j \equiv P_i \Rightarrow (A_1 || F || z_j || T_1)$.  
- **S6:** According to R5 and A3, we have, $S_j \equiv (A_1 || F || z_j || T_1)$.  
- **S7:** Based on R6, we obtain, $S_j \equiv A_1, S_j \equiv F, S_j \equiv z_j$, and $S_j \equiv T_1$.  
- **S8:** From $SK = h(F || z_j)$, we can obtain, $S_j \equiv (S_j \leftarrow P_i)$.  

Thus, the protocol achieves both $G1$ and $G2$. Hence, it is ensured that both $P_i$ and $S_j$ mutually authenticate each other.

**D. SEMANTIC ANALYSIS**

Various security features achieved by the proposed protocol are further discussed and explained in this section. The details are as follows.

1) **ROBUST MUTUAL AUTHENTICATION**

Upon receiving the login request message $C_1$ from $P_i$, $S_j$ decrypts $z_j$ and confirms $(ID_r, h(x_j))$. If they pass the confirmation, $S_j$ then verifies the acknowledgement value of $P_i$ by $A_1 = h(h^{-1}(X) || M_k || PB)$. In the server side, $P_i$ also checks the acknowledgement value $A_2$ of $S_j$ before they confirm the shared session key. If the verifications of $A_1$ and $A_2$ do not hold, the communication session will terminate without establishing a shared key. Therefore, a robust mutual authentication is achieved in our work.

2) **PERFECT FORWARD Secrecy**

Suppose $A$ has somehow obtained a session key in the current session and attempts to use it to attack the past communications between $P_i$ and $S_j$. In each communication session, the session key $SK$ is a nonce computed using the random number $r$ and by multiple operations of the hash function. Therefore, it is not possible for $A$ to use that key to perform the attacks. Hence, the conclusion is established.

3) **USER ANONYMITY, USER UNTRACEABILITY AND MESSAGE UNLINKABILITY**

The identity $ID_i$ of $P_i$ is protected in the ciphertext $C_1$. Both of the messages conveyed between $P_i$ and $S_j$ do not publicly contain $ID_r$. Therefore, $ID_r$ cannot be revealed to $A$ during the communication. It is a secret known by $P_i$ and $S_j$ only. Both $C_1$ and $C_2$ are nonce values and they are completely different in every communication session. $A$ is not able to identify any two transcripts conveyed by the same patient $P_i$. Furthermore, $A$ cannot find any constants when linking $C_1$ with $C_2$ for the purpose of tracing $P_i$. Thus, the proposed protocol achieves user anonymity, user untraceability and message unlinkability.

4) **RESISTANCE TO PASSWORD GUESSING ATTACKS**

In this case, $A$ enters a guessed password (along with an identity and biometrics) to the system for the purpose of login. Nevertheless, $SC_i$ will check the value $V$ and easily decline $A_i$’ candidate password. Suppose the value $W$ has been obtained by $A$, then attempts $A$ to guess $P_i$’s password based on this hash value. However, other than $PW_j$, $W$ also contains the identity $ID_i$ and random number $\sigma$. Without $ID_i$ and $\sigma$, it is not possible for $A$ to compute a hash value $W'$ and compare it with $W$ for guessing the correct password. Consequently, our work can resist both online and offline password guessing attacks. Furthermore, password update function is...
also provided in the proposed protocol, which enhances the security of $PW_i$.

5) RESISTANCE TO IMPERSONATION ATTACKS
Suppose $A$ has somehow obtained $ID_i$ then use it for computing a login request, in order to impersonate $P_i$. Due to the stated resistance to password guessing attacks, $PW_i$ cannot be revealed to $A$. Moreover, $B_i$ is kept secret to $P_i$ only. Even though $A$ knows of $ID_i$, it is not possible for $A$ to compute $W$ and $PB$ without $PW_i$ and $B_i$. In addition, $A$ also lacks the correct $A_1$ and $z_j$ for forging the ciphertext $C_1$. Hence, impersonation attacks are resisted in the proposed protocol.

6) RESISTANCE TO MITM ATTACKS
In the login procedure, $A$ can directly use $n_j$ to encrypt a candidate message and forge $C_1$. In this way, $A$ acts as a middle man to change the conveyed messages between $P_i$ and $S_j$ while $P_i$ and $S_j$ totally do not notice the attack. Nevertheless, since $A$ does not know of $x_j$ and the value $h(x_j)$ for the verification, $S_j$ will easily reject the above login request. In addition, as stated, the proposed protocol can prevent password guessing attacks and impersonating attacks. Therefore, it is not possible for $A$ to calculate a correct $C_1$. $A$ may also block $C_1$, modifies its contents, and sends a tampered message to $S_j$. $A$ is not able to perform this act since they do not know of the private keys $p_j$ and $q_j$ to decrypt and tamper with $C_1$. Hence, our protocol is completely free from MITM attacks.

7) RESISTANCE TO REPLAY ATTACKS
$A$ may intercept and resend $C_1$ to $S_j$ for performing a replay attack on the subsequent communication sessions. In our protocol, timestamp $T_i$ is employed to verify if $C_1$ is resent. In other words, $T_i$ assures $C_1$ is used only once for the purpose of login. In a similar way, timestamp $T_j$ can be used to check the validity of the message $C_2$ sent to $P_i$. Moreover, the acknowledgement values $A_1$ and $A_2$ are also used to check the legitimacy of $P_i$ and $S_j$ respectively. Therefore, the conclusion is established.

8) RESISTANCE TO DESYNCHRONIZATION ATTACKS
In the proposed protocol, the acknowledgements $A_1$ and $A_2$ are computed based on the values $PB$, $X$, $Y$ and timestamp $T_j$, which are deleted after the communication. $P_i$ and $S_j$ do not further store any redundant parameters after each session finishes. Therefore, the proposed work does resist desynchronization attacks.

9) RESISTANCE TO INSIDER ATTACKS
Due to the Definition 2, $S_j$ is assumed to be a trusted entity during the registration of $P_i$. In the database of $S_j$, only the identity $ID_i$ of $P_i$ is stored after the registration procedure. If a privileged insider acts as $A$ to perform an attack on a target patient using $ID_i$, they will not be successful due to the prevention of impersonation attacks as discussed. In addition, our work does not require biometrics database as well as password table in the protocol. Thus, our protocol can withstand insider attacks.

10) RESISTANCE TO STOLEN SMART CARD ATTACKS
Suppose $A$ somehow has stolen $SC_i$ from $P_i$. Then, $A$ performs a power analysis attack and obtain all values stored in $SC_i$. In the proposed protocol, password $PW_i$ and biometrics $B_i$ are not directly stored in $SC_i$. Even though $A$ is able to obtain $HD_i$ and $SC_i$ at the same time and pass the verification of $SC_i$, they still cannot compute a valid $C_1$ without these important parameters. Hence, our protocol can prevent stolen smart card attacks.

11) RESISTANCE TO DoS ATTACKS
In each login phase of the proposed protocol, $SC_i$ always checks the legitimacy of $P_i$ based on their input values. Specifically, $SC_i$ will verify $V$ and immediately terminate the session if the verification does not hold. Therefore, $A$ is not able to flood the system with subsequent computation steps. In addition, $S_j$ also verify the freshness of timestamp $T_j$ right after decrypting $C_1$. Repeatedly retransmitting $C_1$ to make $S_j’s$ services disrupted would not work efficiently for $A$ once the resource in the server side is redundant. Since the risk of DoS attacks in the design is low, $T_j$ is put inside $C_1$ to reduce communication cost. The conclusion is established.

VI. PERFORMANCE ANALYSIS
In this section, we present a detailed comparative study of our protocol and some recent related protocols discussed in Section I-A, which are the most similar ones to ours. The performance comparison includes various aspects, namely, functionality, storage cost, communication cost, and computation cost.

A. FUNCTIONS
We tabulate the comparison results of various functions achieved by different protocols in Table 3. Symbol √/ denotes that the protocol achieves a specific function. We also use symbol × to denote that the function is not achieved by the protocol. Symbol – means the function is not available in the protocol. It is observed that the proposed protocol provides the supports of more security properties and functionalities compared with the competitive ones. In particular, only our work introduces fast authentication and time-bound authentication solutions in the proposed 6G-IoE intelligent healthcare environment.

B. STORAGE AND COMMUNICATION COST
We define some parameters used in the comparisons as follows. The lengths of asymmetric encryptions or decryptions (e.g., RSA cryptosystem) and Chebyshev polynomials are assumed to be 1024 bits for assuring strong security. Symmetric encryptions and decryptions have a 256-bit length of each block. Each identity, password and biometrics has a similar length of 128 bits. 160 bits is the length of a single random number and hash value. The elliptic curve point
TABLE 3. Comparison on functionality.

| Functions                        | [16] | [22] | [23] | [24] | [26] | [27] | [29] | [30] | Ours |
|----------------------------------|------|------|------|------|------|------|------|------|------|
| Resist online password guessing attacks | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist offline password guessing attacks | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist impersonation attacks      | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist MITM attacks               | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist replay attacks             | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist desynchronization attacks  | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist insider attacks            | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist stolen smart card attacks  | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Resist DoS attacks                | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide mutual authentication     | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide perfect forward secrecy    | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide patient anonymity         | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide patient untraceability    | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide message unlinkability     | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide three-factor authentication| ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide mathematical security proof | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide security simulation with ProVer/AVISPA | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide fast authentication        | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide time bound authentication  | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provides password update function  | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide UCSSO solution            | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide center-less authentication | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |
| Provide 6G-IoE intelligent healthcare application | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   | ⌂   |

multiplication operation and timestamp are with the length of 320 bits and 32 bits, respectively. The storage cost is the total length of the parameters that \( P_i \) and \( S_j \) store after registration phase. For instance, in our protocol, \( P_i \) stores \( \{\varepsilon_j, n_j, t_1, t_2, TB_1, TB_2\} \) and \( \{\sigma, V\} \) in their device and card respectively, which incurs a total length of 1920 bits. \( S_j \) only stores \( ID_i \) of each \( P_i \) in their database, the length of which is 128 bits. Storage cost of all other protocols can be computed in a similar way. Table 4 presents the costs of different protocols. It is observed that our work consumes the least storage cost. Since ours, Lin et al. [23] and Le and Hsu [16] employ SSO solution in the protocols, the cost in the \( P_i \)'s side will not increase in direct proportion to the number of servers. Suppose \( s \) is the total number of servers, Figure 6 further describes the comparison results on the storage cost.

In terms of communication cost, in the initial authentication, when \( P_i \) enters \( ID_i^*, PW_i^*, B_i^* \) (from \( HD_i \)) to \( SC_i \), it bears a cost of 384 bits. After the verification, \( SC_i \) sends \( \sigma, PB^* \) back to \( P_i \) for further computations. This process consumes a cost of 320 bits. The total is 384 bits + 320 bits = 704 bits. Similarly, in fast authentication phase, these communications only bear a total cost of 384 bits. We also consider the total communication rounds and the length of all transcripts conveyed between \( P_i \) and \( S_j \) in each authentication session. In our work, the transcripts include \( (C_1, C_2) \) and \( (\alpha, \beta) \) in the initial and fast authentication procedures, which consume

FIGURE 6. Storage costs of different protocols.

TABLE 4. Comparison on storage cost of each entity.

| Protocols            | \( P_i \) side (bits) | \( S_j \) side (bits) |
|----------------------|-----------------------|-----------------------|
| Le and Hsu [16]      | 1824                  | 1824                  |
| Lin et al. [23]      | 2176                  | 128                   |
| Meshram et al. [24]  | 1664                  | 608                   |
| Xu et al. [26]       | 1248                  | 960                   |
| Dharminder et al. [27]| 1504                  | 160                   |
| Thakare and Kim [29] | 480                   | 608                   |
| Ours                 | 1920                  | 128                   |

TABLE 5. Comparison on communication cost.

| Protocols            | Cost btw \( SC_i \) and \( P_i \) | Cost btw \( P_i \) and \( S_j \) | Rounds btw \( P_i \) and \( S_j \) | Round trip time in 6G |
|----------------------|----------------------------------|----------------------------------|----------------------------------|-----------------------|
| Le and Hsu [16]      | 544 bits                         | 1440 bits                        | 2                                | < 2 ms                |
| Lin et al. [23]      | 544 bits                         | 5736 bits                        | 3                                | < 3 ms                |
| Meshram et al. [24]  | 1760 bits                        | 3072 bits                        | 2                                | < 2 ms                |
| Xu et al. [26]       | 1024 bits                        | 1344 bits                        | 3                                | < 3 ms                |
| Dharminder et al. [27]| 1472 bits                        | 1568 bits                        | 2                                | < 2 ms                |
| Thakare and Kim [29] | -                                | 1440 bits                        | 3                                | < 3 ms                |
| Ours                 | Initial authentication           | 794 bits                         | 2                                | < 2 ms                |
|                      | Fast authentication              | 384 bits                         | 2                                | < 2 ms                |
TABLE 6. Comparison on computation cost of a single session.

| Protocols | Time complexities of $P_i$ side | Time estimation of $P_i$ side (ms) | Time complexities of $S_j$ side | Time estimation of $S_j$ side (ms) | Total time estimation (ms) |
|-----------|---------------------------------|------------------------------------|---------------------------------|------------------------------------|--------------------------|
| Le and Hsu [16] | $T_M + T_{SED} + 9T_H$ | $\approx 0.00744$ | $T_QB + 2T_{SED} + ST_{H}$ | $\approx 1.17353$ | $\approx 1.18097$ |
| Lin et al. [23] | $2T_{CM} + 2T_{SED} + 7T_H$ | $\approx 0.06353$ | $2T_{CM} + 2T_{SED} + ST_{H}$ | $\approx 0.06215$ | $\approx 0.12568$ |
| Meshram et al. [24] | $2T_{CM} + 11T_H$ | $\approx 0.06521$ | $2T_{CM} + 9T_H$ | $\approx 0.06383$ | $\approx 0.12904$ |
| Xu et al. [26] | $T_{FE} + 4T_{PM} + 9T_H$ | $\approx 2.54621$ | $3T_{PM} + 5T_H$ | $\approx 1.52745$ | $\approx 4.07366$ |
| Dhamminder et al. [27] | $T_{SED} + 5T_{H}$ | $\approx 1.17245$ | $T_{ASED} + 3T_{H}$ | $\approx 1.71070$ | $\approx 2.34352$ |
| Thakare and Kim [29] | $4T_{PM} + T_{PM} + 2T_{H}$ | $\approx 2.04028$ | $5T_{PM} + 2T_{PM} + 6T_{H}$ | $\approx 2.55794$ | $\approx 4.59822$ |
| Ours | Initial authentication | $T_M + T_{SED} + 9T_H$ | $\approx 0.00744$ | $T_QB + 2T_{SED} + 8T_{H}$ | $\approx 1.17560$ | $\approx 1.18304$ |
| | Fast authentication | $2T_{SED} + 5T_{H}$ | $\approx 0.00453$ | $2T_{PM} + 2T_{H}$ | $\approx 0.00246$ | $\approx 0.00699$ |

Based on [16, 23], $T_{CM} \approx 0.02881ms$, $T_{PE} \approx 0.508ms$, $T_{PM} \approx 0.508ms$, $T_{FA} \approx 0.0069ms$, $T_{SED} \approx 0.00054ms$, $T_{ASED} \approx 1.169ms$, $T_M \approx 0.0069ms$, $T_{QH} \approx 1.169ms$, and $T_{H} \approx 0.00069ms$.

a total length of 1280 bits and 512 bits, respectively. The number of communication rounds between $P_i$ and $S_j$ are 2 in both procedures. In 6G networks, the end-to-end communication latency is less than 1 ms [4], [41]. Therefore, the round-trip times for each session in the proposed protocol are estimated to be less than 2 ms. Detailed comparison on communication cost of different protocols is provided in Table 5. We can observe that the proposed protocol is one of the most efficient ones with the initial authentication. When the fast authentication is performed, it bears the least cost. Since most of the protocols are designed based on smart card mechanism for achieving a high security, such communication costs with the round-trip times required should be reasonable.

C. COMPUTATION COST

We assume the time of computing an XOR operation is negligible since it is extremely fast. According to [32], the execution times of a biohash function and a one-way hash function are similar. For the sake of simplicity, they are assumed to be the same one. We denote the following cryptographic functions and operations for the evaluation on computation cost.

- $T_{CM}$: Time of computing a Chebyshev chaotic polynomial mapping.
- $T_{FE}$: Time of computing a fuzzy extractor operation.
- $T_{PM}$: Time of computing an elliptic curve point multiplication.
- $T_{PA}$: Time of computing an elliptic curve point addition.
- $T_{SED}$: Time of computing a symmetric encryption or decryption.
- $T_{ASED}$: Time of computing an asymmetric encryption or decryption.
- $T_M$: Time of computing a modular squaring.
- $T_{QR}$: Time of computing a square root modulo $N$.
- $T_{H}$: Time of computing a hash function.

As we know the execution time of a hash function is also very fast. Whereas the number of fast authentications $v$ and the time points $t$, $t_1$, $t_2$ in our proposal should not be very large. Therefore, the costs of computing $h^{(v-\epsilon)}$, $h^\epsilon$, $h^\epsilon$, $h^{(v-1)}$, $h^{2\epsilon-1}$, $h^{2\epsilon-1}$ and $h^{2\epsilon-1}$ are assumed to be similar. The results of comparison on computation cost of different protocols in a single communication are tabulated in Table 6. Suppose all time bounds set by servers are the same and $v$ is set to 5. Figure 7 depicts the comparison of the proposed work and the related works with the data retrieved from Table 6 for the first 20 communication sessions. The results show that our protocol with fast authentication achieves the highest efficiency.

Furthermore, we describe a scenario where a single patient is using services provided by multiple servers. Since our work introduces the UCSSO, some computations in the protocol, such as $PB^* = h(ID^*||h_{bio}(B^*))$ and $V = h(\sigma||PW^*||PB^*)$, are only operated once for the communications with multiple servers. It significantly enhances the efficiency of the protocol. We also calculate the computation costs of the other protocols and depict the comparison results in Figure 8. It shows that the initial authentication procedure in our protocol bears an acceptable computation cost considering the superior to the others in terms of functions and security properties, discussed in Section VI-A. When it comes to the fast authentication procedure, we obviously achieve an efficient communication with the least cost consumed. It is a good fit for 6G-IoE healthcare environments where resource-constrained devices should only consume little computation energy.
The authors would like to thank anonymous referees for their technology for some communications in the healthcare world. In addition, data immutability enabled by blockchain providing non-repudiation of the health data in the quantum A post-quantum signature scheme may be integrated for biohash function and XOR operation employed in the design. BAN logic. A performance evaluation on various aspects various tools, namely, RoR model, AVISPA simulation, and unlinkability. We provide security proof of the protocol using user privacy is achieved with forward secrecy of session keys efficiently establish healthcare communications. A perfect plagued protocol allows patients and providers to securely and ing a cost-efficient communication in the system. The proposed protocol allows patients and providers to securely and efficiently establish healthcare communications. A perfect user privacy is achieved with forward secrecy of session keys computed, user anonymity, user untraceability and message unlinkability. We provide security proof of the protocol using various tools, namely, RoR model, AVISPA simulation, and BAN logic. A performance evaluation on various aspects indicates that our work achieves most functionalities and incurs least cost compared with its predecessor works.

In future works, we will consider further improving the efficiency of the work with only one-way hash function, biohash function and XOR operation employed in the design. A post-quantum signature scheme may be integrated for providing non-repudiation of the health data in the quantum world. In addition, data immutability enabled by blockchain technology for some communications in the healthcare systems would also be an interesting research direction.

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

REFERENCES
[1] M. Z. Noohani and K. U. Magsi, “A review Of 5G technology: Architecture,” Secur. wide Appl., vol. 7, pp. 3440–3471, 2020.
[2] S. Nayak and R. Patgiri, “6G communication technology: A vision on intelligent healthcare,” in Health Informatics: A Computational Perspective in Healthcare, R. Patgiri, A. Biswas, and P. Roy, Eds. Singapore: Springer, 2021, pp. 1–18.
[3] S. Minglan, Z. Chaoying, L. Qiaoqiao, L. Baolin, and W. Jianxin, “Holographic communication technology,” Proc. SPIE, vol. 11933, pp. 437–441, Oct. 2021.
[4] S. Chen, Y.-C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, “Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed,” IEEE Wireless Commun., vol. 27, no. 2, pp. 218–228, Apr. 2020.
[5] Z. Chen, X. Ma, B. Zhang, Y. Zhang, Z. Niu, N. Kuang, W. Chen, L. Li, and S. Li, “A survey on terahertz communications,” China Commun., vol. 16, no. 2, pp. 1–35, 2019.
[6] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, “6G: Opening new horizons for integration of comfort, security, and intelligence,” IEEE Wireless Commun., vol. 27, no. 5, pp. 126–132, Oct. 2020.
[7] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J.-A. Zhang, “The roadmap to 6G: AI empowered wireless networks,” IEEE Commun. Mag., vol. 57, no. 8, pp. 84–90, Aug. 2019.
[8] S. Alrahai, J. Shaye, M. Behjati, R. Nordin, N.F. Abdullah, A. Abu-Samah, and D. Nandi, “Revolution or evolution? Technical requirements and considerations towards 6G mobile communications,” Sensors, vol. 22, no. 3, p. 762, Jan. 2022.
[9] Z. Qadir, H. S. Munawar, N. Saeed, and K. N. Le, “Towards 6G Internet of Things: Recent advances, use cases, and open challenges,” 2021, arXiv:2111.06596.
[10] S. Minglan, Z. Chaoying, B. Shihada, and M.-S. Alouini, “What should 6G be?” Nature Electron., vol. 3, no. 1, pp. 20–29, Jan. 2020.
[11] T. Nakamura, “5G evolution and 6G,” in Proc. IEEE Symp. VLSI Technol., Jun. 2020, pp. 1–5.
[12] M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, “6Genesis flagship program: Building the bridges towards 6G-enabled wireless smart society and ecosystem,” in Proc. IEEE 10th Latin Amer. Conf. Commun. (LATINCOM), Nov. 2018, pp. 1–9.
[13] E. Yuacoub and M.-S. Alouini, “A key 6G challenge and opportunity—Connecting the base of the pyramid: A survey on rural connectivity,” Proc. IEEE, vol. 108, no. 4, pp. 533–582, Apr. 2020.
[14] S. Nayak and R. Patgiri, “6G communication: Envisioning the key issues and challenges,” EAI Endorsed Trans. Internet Things, vol. 6, no. 24, Feb. 2021, Art. no. 166959.
[15] S. Verma, S. Kaur, M. A. Khan, and P. S. Sehdev, “Toward green communication in 6G-enabling wireless Internet of Things,” IEEE Internet Things J., vol. 8, no. 7, pp. 5408–5415, Apr. 2021.
[16] T. V. Le and C. L. Hsu, “An anonymous key distribution scheme for group healthcare services in 5G-enabled multi-server environments,” IEEE Access, vol. 9, pp. 53408–53422, 2021.
[17] 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.
[18] 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.
[19] M. O. Rabin, “Digitalized signatures and public-key functions as intractable as factorizations,” Massachusetts Inst. Technol., Cambridge, M.I.T., USA, Tech. Rep., 1979.
[20] Q. Jiang, S. Zeadally, J. Ma, and D. He, “Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks,” IEEE Access, vol. 5, pp. 3376–3392, 2017.
[21] 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.
[22] T.-W. Lin and C.-L. Hsu, “FAIDM for medical privacy protection in 5G telemedicine systems,” Appl. Sci., vol. 11, no. 3, p. 1155, Jan. 2021.
[23] T.-W. Lin, C.-L. Hsu, T.-V. Le, C.-F. Lu, and B.-Y. Huang, “A smartcard-based user-controlled single sign-on for privacy preservation in 5G IoT telemedicine systems,” Sensors, vol. 21, no. 8, p. 2880, Apr. 2021.
[24] C. Meshram, R. W. Ibrahim, L. Deng, S. W. Shende, S. G. Meshram, and S. K. Barve, “A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment,” Soft Comput., vol. 25, no. 15, pp. 10037–10051, Aug. 2021.
[25] S. Mangard, E. Oswald, and T. Popp, “Power analysis attacks: Revealing the secrets of smart cards,” Tech. Rep., 2007.
[26] D. Xu, J. Chen, and Q. Liu, “Provably secure anonymous three-factor authentication scheme for multi-server environments,” J. Ambient Intell. Hum. Comput., vol. 10, no. 2, pp. 611–627, Feb. 2019.
[27] D. Dharminder, D. Mishra, and X. Li, “Construction of RSA-based authentication scheme in authorized access to healthcare services,” J. Med. Syst., vol. 44, no. 1, pp. 1–9, Jan. 2020.
[28] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[29] A. Thakare and Y.-G. Kim, “Secure and efficient authentication scheme in IoT environments.” Appl. Sci., vol. 11, no. 3, p. 1260, Jan. 2021.

[30] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, “ARAP-SG: Anonymous and reliable authentication protocol for smart grids,” IEEE Access, vol. 9, pp. 143366–143377, 2021.

[31] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, “Artificial-Intelligence-Enabled intelligent 6G networks,” IEEE Netw., vol. 34, no. 6, pp. 272–280, Nov. 2020.

[32] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, “A robust biometrics and cryptography-based three-factor authentication scheme for global mobility networks in 5G-based wireless sensor networks,” IEEE Trans. Ind. Electron., vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[33] S. Al-Kuwari, J. Davenport, and R. Bradford, “Cryptographic hash functions: Recent design trends and security notions,” in Proc. IACR, 2011, p. 565.

[34] 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.

[35] 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.

[36] 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.

[37] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, “A robust biometrics based three-factor authentication scheme for global mobility networks in smart city,” Future Gener. Comput. Syst., vol. 83, pp. 607–618, Jun. 2018.

[38] D. Wang and P. Wang, “Two birds with one stone: Two-factor authentication with security beyond conventional bound,” IEEE Trans. Dependable Secure Comput., vol. 4, no. 4, pp. 708–722, Jul./Aug. 2016.

[39] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, and L. E. Bassham, “Announcing the advanced encryption standard (AES),” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2001.

[40] D. Von Oheimb, “The high-level protocol specification language HLPSL developed in the EU project AVISPA,” in Proc. APPSEM Workshop, 2005, pp. 1–17.

[41] M. Alsabah, M. A. Naser, B. M. Mahmmod, S. H. Abdullhusain, M. R. Eissa, A. Al-Baidhani, N. K. Noordin, S. M. Sait, K. A. Al-Utaibi, and F. Hashim, “6G wireless communications networks: A comprehensive survey,” IEEE Access, vol. 9, pp. 148191–148243, 2021.

**TUAN-VINH LE** received the Ph.D. degree in management from the Graduate Institute of Management, Chang Gung University, Taiwan, in 2021. He is currently an Assistant Professor with the Department of Information Management, Chihlee University of Technology, Taiwan. He has authored or coauthored multiple articles in the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, SENSORS, JOURNAL OF INTERNET TECHNOLOGY, LIBRIS: INTERNATIONAL JOURNAL OF LIBRARIES AND INFORMATION STUDIES, and INTERNATIONAL JOURNAL OF ELECTRONIC COMMERCE STUDIES. His research interests include information security, communication system security, cryptography, and blockchain.

Dr. Le is currently a certified EC-Council Instructor and an Active Reviewer of several journals IEEE ACCESS and CONNECTION SCIENCE. He was granted full scholarships for his M.S. degree from the National Formosa University, in 2014, and the Ph.D. degree from Chang Gung University, in 2016.

**CHUNG-FU LU** received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in information management from the National Taiwan University of Science and Technology, Taiwan, in 1991, 1993, and 2011, respectively. He is currently an Associate Professor with the Department of Information Management, Chihlee University of Technology, Taiwan. His current research interests include cryptography, information security, network security, wireless sensor networks, smart home systems, and mobile commerce.

Dr. Lu was the Chair of the Department of Information Management, Chihlee University of Technology, from 2018 to 2022.

**CHIEN-LUNG HSU** 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 with 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, Orlando, FL, USA. He is currently a Joint Professor with the Department of Information Management and the Graduate Institute of Management, Chang Gung University, Taiwan. His research interests include smart healthcare, computer security, information security, cryptography, digital right management, and auto identification technology. He has a great number of publications related to the research interests.

Dr. Hsu was listed in the World’s Top 2% Scientists 2020. From August 2013 to August 2016, he was the Chair of the Department of Information Management, Chang Gung University.

**TRUNG K. DO** received the Ph.D. degree in finance from the National Central University, Taoyuan, Taiwan. He is currently a Senior Lecturer with the Department of Economics, Danang Architecture University, Danang, Vietnam. His articles have been published in Journal of Banking and Finance, Corporate Governance: An International Review, Finance Research Letters, Research in International Business and Finance, and International Journal of Finance and Economics. His research interests include corporate finance and fintech security.

**YEON-FANG CHOU** is currently pursuing the Ph.D. degree with the School of Nursing, Taipei Medical University, Taiwan. She is currently a Nursing Supervisor with the Department of Nursing, Taoyuan Chang Gung Memorial Hospital. Her research interests include healthcare and rehabilitation.

**WEI-CHENG WEI** received the M.S. degree from the Department of Information Management, Chang Gung University, Taiwan. He is currently an Information Security Management Consultant with Mobilon Information Service Company Ltd., Taiwan. His research interests include information security management, user privacy, and medical equipment management.

* * *