Computers, Materials & Continua
DOI:10.32604/cmc.2022.022706
Article

Tech Science Press

Efficient Joint Key Authentication Model in E-Healthcare

Muhammad Sajjad[1], Tauqeer Safdar Malik[1], Shahzada Khurram[2], Akber Abid Gardezi[3], Fawaz Alassery[4], Habib Hamam[5], Omar Cheikhrouhou[6] and Muhammad Shafiq[7,*]

[1]Department of Computer Science, Air University Multan Campus, Multan, 60000, Pakistan
[2]Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[3]Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan
[4]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia
[5]Faculty of Engineering, Moncton University, NB, E1A3E9, Canada
[6]CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax, 3038, Tunisia
[7]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, 38541, Korea
*Corresponding Author: Muhammad Shafiq. Email: shafiq@ynu.ac.kr
Received: 16 August 2021; Accepted: 27 September 2021

Abstract: Many patients have begun to use mobile applications to handle different health needs because they can better access high-speed Internet and smartphones. These devices and mobile applications are now increasingly used and integrated through the medical Internet of Things (mIoT). mIoT is an important part of the digital transformation of healthcare, because it can introduce new business models and allow efficiency improvements, cost control and improve patient experience. In the mIoT system, when migrating from traditional medical services to electronic medical services, patient protection and privacy are the priorities of each stakeholder. Therefore, it is recommended to use different user authentication and authorization methods to improve security and privacy. In this paper, our prosed model involves a shared identity verification process with different situations in the e-health system. We aim to reduce the strict and formal specification of the joint key authentication model. We use the AVISPA tool to verify through the well-known HLPSL specification language to develop user authentication and smart card use cases in a user-friendly environment. Our model has economic and strategic advantages for healthcare organizations and healthcare workers. The medical staff can increase their knowledge and ability to analyze medical data more easily. Our model can continuously track health indicators to automatically manage treatments and monitor health data in real time. Further, it can help customers prevent chronic diseases with the enhanced cognitive functions support. The necessity for efficient identity verification in e-health care is even more crucial for cognitive mitigation because we increasingly rely on mIoT systems.

Keywords: E-health systems; joint key authentication; mutual authentication

1 Introduction

The Internet of Things (IoT) is a network of low-power devices embedded with sensors, actuators, software, and network connections that can collect and exchange data autonomously [1]. The application of medical IoT (MIoT) systems in the industry has become increasingly prominent. For example, in 2020, 40% of IoT-related technologies have been used in healthcare to control costs, reduce inefficiencies, and save lives [2]. In the basic mIoT structure, the ID cards of the patients are connected to a secure cloud to store their credentials and electronic health records (EHR). Medical staff can more easily access this EHR on a tablet or desktop computer and put all important information in one place for easy sharing. In return, these EHR eliminate much life-saving inefficiency.

An open online communication atmosphere is self-doubt about IoT devices. In this regard, different healthcare providers, government agencies, insurance companies, patients and healthcare professionals, and many other stakeholders benefit directly or indirectly from the digital world [3,4]. Patient safety and vitality are the core goals of every stakeholder, but compared with traditional systems, mIoT are not trustworthy. There are many internal and external adversaries and hackers that may use various information and controls to forge legitimate users, or at least obtain valuable data from the database [5]. The security and confidentiality of the current wireless IoT requires data privacy, security, attack robustness, and self-maintenance. Moreover, the isolated user authentication structure is also of interest, which plays a vital role in the formation of communication through uncertain channels.

The mutual authentication between the user and the server using the three key factor protocol may help build a reliable mIoT system. However, this joint key authentication model is hectic for users in the delivery of health care services to the patients [6]. While granting system access rights, users must jointly use identity passwords, biometric templates, and smart cards. In real-time scenarios, users may encounter many problems when using the joint key factors. Sometimes forgotten passwords, damage or unclear biometric templates, or smart cards stolen, etc., preclude users from accessing the e-health system. In [7], surveys and interview responses indicate that users trust system authentication using mutual key factors, but there should be a reliable mechanism that allows users to authenticate and access electronic medical systems based on the criticality and type of users.

We investigate the following security and privacy issues to mIoT systems in general. First of all, agreements including data transmission, authorized use, and involving authorized users and their informed consent must be defined in clear and simple language. This will increase patient trust and consider all responsibilities related to patient data in detail so that responsibilities can be easily tracked [8,9]. Secondly, all data must be collected, managed and used fairly in accordance with data privacy regulations [10,11]. Without adequate security and privacy protection, all data must not be used [12]. Third, all interconnected IoT devices in a specific network should have sufficient capabilities to transmit and receive data through the underlying network without affecting the integrity of the data [13]. Fourth, the design of all participating devices must be able to provide comprehensive protection against certain network attacks, unauthorized system access, and unauthorized use. Last but not least, when deciding on the minimum security requirements for protecting data in a mIoT system, the lowest possible security, privacy, and system requirements must also be considered.

The main contributions of this paper are summarized as follows.

- We proposed an improved three-factor authentication scheme, eliminated the rigidity of inputting multiple key factors for authentication, and transformed the mIoT system into a reliable, flexible and convenient mutual key authentication scheme. Our proposed scheme effectively serves medical staff in various situations.

- Our system guarantees anonymity and intractability, because it wraps the biometric template with a ropy high random number, and then stores the encrypted data in a dynamic table. Our system is flexible enough to allow users to select keys in real time.
- We conducted formal security analysis and prove that our system is robust against many attacks e.g., man-in-the-middle, replay, theft of authenticators, offline password guessing, and online password guessing.

The rest of this article is organized as follows. Section 2 summarizes the related work. Section 3 presents the proposed work. Section 4 discusses an informal safety analysis of the proposed work. Section 5 analyzes and evaluates the proposed work based on the variation of the situation. In the last section, we reached the conclusion.

2 Related Works

In general, the classic security and risk analysis measures (such as confidentiality, data integrity, availability, access control, and authentication) can be used to evaluate the security of the mIoT system. In recent years, many three-factor authentication systems have been introduced.

In [14], the authors introduced a low-computing three-factor authentication system by applying only the hash function. In [15], authors proposed a three-factor authentication structure and a public key and symmetric cryptographic system. However, the user authentication procedure becomes more cumbersome regarding identification, authentications and authorizations. In [6,16], we can find that some scholars have considered the dual factor of password and device retention. People who have both of these functions can login to the special system. Several user authentication mechanisms are in practice, among which identity passwords, biometric templates, smart cards, and mobile device factors are used individually or together for user authentication. In [11], the authors proposed a method to enhance IoT-based security by using the optimal homomorphic encryption authentication key, in which, a password-based method is used to protect IoT data, In the encryption process, the step size fire optimization algorithm is used to select the key authentication and the optimal key.

Biometric technology has become a common theme in the previous era. For isolated users, biometric authentication systems are becoming more common due to their biological characteristics such as fingerprint authentication, iris check, facial survey, handwritten signature verification, and keystroke checks to provide improved shelters [17]. In [18], the authors suggested that biometric-based authentication is a more reliable to remote user systems caromed to password-based authentication methods. However, each system has some advantages and disadvantages. For example, when using traditional ID/PWD authentication, password cracking, online/offline dictionary attacks, password guessing attacks, password leaks, and stolen verifier attacks are the most common problems reported by users [7]. Similarly, biometric template verifier attacks, vulnerabilities in smart card verification, and smart card theft attacks have also been reported in smart card user authentication [2]. An effective design of an authentication system based on mutual keys can overcome the limitations of classic systems.

3 Proposed Work

The joint key authentication (JKA) model is an auxiliary tool for e-health users in different situations. However, the rigidity of mutual key authentication is the main obstacle for users to access the e-medical system. We try to handle the real-time support of accessing the system by using different login cases to deal with the current scenario where they want to access the e-medical system. In the

suggested method, the application user can select any login case from the given login case options based on the current critical situation. The user interface helps them display a specific set of login credentials selected based on the login case. As shown in Fig. 1, there are four login cases designated by LC1–LC4. Each case consists of a mutual key and different login credentials. For example, the LC1 group has ID/PWD, biometrics and smart cards. Before proceed, we summarized the key symbols in Tab. 1. In our model, we discuss many strings that will be transmitted between the user and the healthcare server for authentication purposes. When the authentication process between the user and the healthcare server begins, the encrypted biometric identity will be stored along with the initial case and dynamic string.

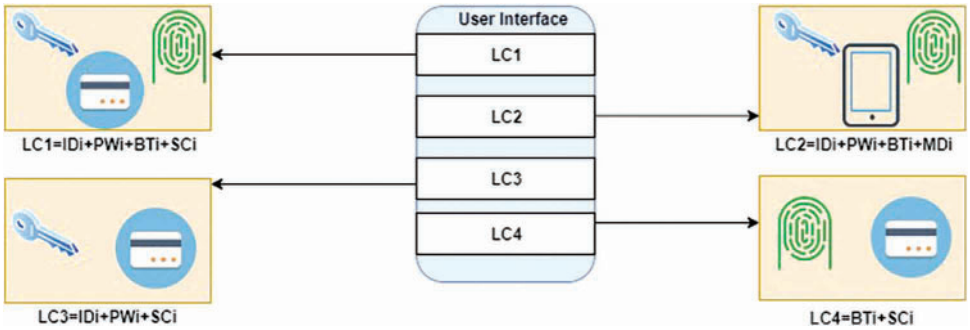

Figure 1: Joint key authentication scheme

Table 1: Summary of the symbols

Symbol	Description
U_i	User healthcare personnel
BT_i, BT_i^*	Biometric pattern or template of Ui
IDSC	Identity of smart card of Ui
IDmd	Identity of mobile device of Ui
di	Identity of user Ui
PWi	Password of user Ui
H(.)	Hash function
H∗(.)	Bio hash function
||	String concatenation sign
⊕	XOR operator
HS	HealthCare server
LCi	Login case of each user Ui
Rni	High entropy random no
LC(.)	Login case function string
Si	String of ith transmitted using transmission
Δ, t	Biometric and another factor matching algorithm

String concatenation is an important step to make key factors more secure. If someone steals the security key, he or she cannot reveal which part of the string identifies which key factor. In the proposed JKA model, the (||) symbol is used for string concatenation. Another point is that after concatenating the strings, one of the hashing techniques is applied to encrypt the entire string that cannot be easily reversed. Another function of the XOR ($\oplus$) operator is to protect the user's identity and ensure the user's privacy. The XOR operator has the lowest computational cost and is designed for all IoT medical equipment. In this regard, we discuss the following registration, authentication and session phases.

3.1 Registration Phase

For the registration phase, there are four different login cases in the proposed method. These cases are grouped by different key factors, which will be involved in the future login process. The detailed login process for each login case (LC) is given in the Tabs. 2 and 3. User U_i choose ID, PW imprint biometric template and random number, take hash value by applying $S_1 = H(ID_i||PW_i||H^*(BT_i))$. Then, the biometric identity is encrypted with random number 1, $S_2 = BT_i \oplus rn_1$ and hash value of Identity and Password encrypted of random number 1, $S_3 = H(ID_i \oplus PW_i) \oplus rn_1$. Thereafter, the hash value of ID, PW and Random no encrypted with S_2 and save value in S_4 string. After that four string S_1, S_2, S_3 and, S_4 send to healthcare server (HS). The HS use its private information master key hsgenerateID_{sc} for Smart Card and ID_{md} for mobile device. Concatenation $S_2$with master key hs and extract hash value, $M = H(H^*(S_2)||$ hs). Select random no rn_2 and then hash and encrypt $LC = H(H^*(S_2) \oplus rn_2)$ finally compute X_1 of hash value concatenation of smart card id, Master key and random no 1 for smart card, $X_1 = H(ID_{sc}||S_1||\ M\ ) \oplus rn_2$. Similarly, compute X_2 of hash value concatenation of mobile device $X_2 = H(ID_{md}||S_1||\ M\ ) \oplus rn_2$ encrypt master key with $S_1\ \ Y = M \oplus S_1$ store $\{S_2,\ \ LC_0, LC_1\}$ into HS.

Table 2: Login cases 1 and 2 in the registration phase

Login case 1 (IDi/PWi + BTi + SCi)	Login case 2 (IDi/PWi + BTi + MDi)
User Ui Input IDi, PWi, Imprint BT_i^* choose random integer rn_3.Insert smart card and compute following strings.	User Ui Input IDi, PWi, Imprint BT_i^* choose random integer rn_3. Attach mobile device with terminal and compute following strings.
$S_1^* = H(ID_i\|\|PW_i\|\|H^*(BT_i^*))$	$S_1^* = H(ID_i\|\|\ PW_i\|\|H^*(BT_i^*)\ )$
$M^* = Y \oplus H(S_1^*)$	$M^* = Y \oplus H(S_1^*)$
$rn_2^* = X_1 \oplus H(ID_{sc}\|\|S_1^*\|\|M^*)$	$rn_2^* = X_2 \oplus H(ID_{md}\|\|S_1^*\|\|M^*)$
$rn_1^* = Z \oplus H^*(S_2)$	$rn_1^* = Z \oplus H^*(S_2)$
$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$	$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$
$S_6 = BT_i^* \oplus rn_1^* H(M^*\|\|rn_3)$	$S_6 = BT_i^* \oplus rn_1^* H(M^*\|\|rn_3)$
$S_7 = rn_3 \oplus H^*(BT_i^* \oplus rn_1^*)$	$S_7 = rn_3 \oplus H^*(BT_i^* \oplus rn_1^*)$
$\{S_5, S_6, S_7\}$ login request send to *HS*	$\{S_5, S_6, S_7\}$ login request send to *HS*

3.2 Authentication Phase

Upon receiving $\{S_5, S_6, S_7\}$ login request message from Ui, HS search LC^* from user Login case table and obtain S2. First of all, searches the column dynamic string LC and if it equal to LC^*; then extract corresponding value S_2 searches the column dynamic string LC_0 and extract corresponding value S2 finally replace LC with LC_0. Otherwise, HS reject U_i login request. Suppose, S_2 has been

extracted after successful comparison of dynamic strings then HS generate a random number rn4, store some strings into smart card and mobile device $\frac{\{ID_{sc},H(.),H^*(.),X_1,Y,S_3,S_4\}}{\text{write into Smart Card}}$ and $\frac{\{ID_{md},\ H(.),H^*(.),X_2,\ Y,S_3,S_4\}}{\text{write into Mobile Device}}$ and finally, encrypt biometric template with random number 1 and save into smart card and mobile device. Then, compute $M' = H(H^*(S_2)||\ hs) rn_3^* = S_7 \oplus H^*(BT_i^* \oplus rn_1^*)$ and $BT_i^* \oplus rn_1^* = S_6 \oplus H(M^*||rn_3)$ and compare $BT_i^* \oplus rn_1^*$ and S_2 within bearable threshold. Session terminates if $BT_i^* \oplus rn_1^*$ threshold greater than proposed value compute S8 and S9 and send to Ui $S_8 = rn_4 \oplus H(BT_i^* \oplus rn_1^*) S_9 = H((BT_i^* \oplus rn_1^*)||rn_3^*||rn_4$. When $\{S_8, S_9\}$ is received from healthcare server HS, $rn_4^* = S_8 \oplus H(BT_i^* \oplus rn_1^*) S_9 = H((BT_i^* \oplus rn_1^*)||rn_3^*||rn_4^*)$ verifies the above string hold the value or not?

Table 3: Login cases 3 and 4 in the registration phase

Login case 3 (Idi/PWi + SCi)	Login case 4 (SCi + BTi)
User Ui input IDi, PWi choose random integer rn_3. Insert smart card and compute following strings.	Imprint BT_i^* choose random integerrn_3. Insert smart card and compute strings:
$S_3 \oplus rn_1 = H(ID_i \oplus PW_i)$	$rn_1 = S_3 \oplus H(ID_i \oplus PW_i)$
$\triangle(H(ID_i \oplus PW_i), \quad H(ID_i^* \oplus PW_i^*)) =$	$S_2 = H(ID_i \oplus PW_i \oplus rn_1) \oplus S_4$
	$S_2^* = BT_i^* \oplus rn_1, \triangle (S_2^*, S_2) \leq)$
$S_1^* = H(ID_i^*\|\|PW_i^*\|\|H^*(BT_i))$	$S_1^* = H(ID_i\|\|PW_i\|\|H^*(BT_i^*))$
$M^* = Y \oplus S_1^*$	$M^* = Y \oplus S_1^*$
$rn_2^* = X_1 \oplus H(ID_{sc}\|\|S_1^*\|\|M^*)$	$rn_2^* = X_1 \oplus H(ID_{sc}\|\|S_1^*\|\|M^*)$
$rn_1^* = Z \oplus H^*(S_2)$	$rn_1^* = Z \oplus H^*(S_2)$
$S_5 = H^*(BT_i \oplus rn_1^* \oplus rn_2^*)$	$S_5 = H^*(BT_i^* \oplus rn_1^* \oplus rn_2^*)$
$S_6 = BT_i \oplus rn_1^* H(M^*\|\|rn_3)$	$S_6 = BT_i^* \oplus rn_1^* H(M^*\|\|rn_3)$
$S_7 = rn_3 \oplus H^*(BT_i \oplus rn_1^*)$	$S_7 = rn_3 \oplus H^*(BT_i^* \oplus rn_1^*)$
$\{S_5, S_6, S_7\}$ login request send to HS	$\{S_5, S_6, S_7\}$ login request sends to HS

3.3 Session Phase

The session key is an important stage to maintain insecure communication between the parties. This session makes the future communication after a successful login between the user and the healthcare server secure. We describe the entire process string and follow how the dynamic string is passed. The session key communication between the user and the smart card is as follows.

- After Successful verification user computes remaining strings to build session key agreement $SesK_u = H(M^*||rn_3||rn_4^*)$.
- $X_{new1} = H(ID_{sc}||S_1^*||M^*) \oplus rn_4^*$.
- Ui send string S10 to HS for confirmation, $S_{10} = H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4^*) \oplus rn_4^*)$.
- After receiving S10 from Ui and match with string $H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4) \oplus rn_4)$.
- Session accept by the HS if these two values same, $SesK_{hs} = H(M'||rn_3^*||rn_4)$.
- Computes $LC_{new} = H(H^*(S_2 \oplus rn_4)$ and replace (LC0, LC) with (LC, LCnew).
- For HS sends to user Ui for next login $S_{11} = H(SesK_{hs}||rn_4)$ for confirmation.
- When receive confirmation from HS user Ui compare S11 with $H(SesK_u||rn_4)$. If user fail to compare in time or does not S11 in time, terminate the session.
- Replace X1 with Xnew1 into smart card for every next login.

We now describe the session key communication between user and mobile device in the following.

- After successful verification user computes remaining strings to build session key agreement, $\mathrm{SesK_u} = \mathrm{H(M^*||\ rn_3||rn_4^*)}$
- $X_{new2} = H(ID_{md}||S_1^*||M^*) \oplus rn_4^*$
- Ui Send S10 to HS for confirmation.
- $S_{10} = H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4^*) \oplus rn_4^*$
- After receiving S10 from Ui and match with string $H(H^*(BT_i^* \oplus rn_1^* \oplus rn_4) \oplus rn_4)$
- Session Accept by the HS if these two values same.
- $SesK_{hs} = H(M'||rn_3^*||rn_4)$
- Computes $LC_{new} = H(H^*(S_2 \oplus rn_4)$ and replace (LC0, LC) with (LC, LCnew)
- For HS sends to user Ui for next login $S_{11} = H(SesK_{hs}||rn_4)$ for confirmation.
- When receive confirmation from HS user Ui compare S11 with $H(SesK_u||rn_4)$. If user fail to compare in time or does not received S11 in time, terminate the session.
- Replace X2 with Xnew2 into mobile device for every next login.

4 Informal Security Analysis

We use AVISPA (Automatic Verification of Internet Security Protocols and Applications) and HLPSL tools [19] to analyze our authentication schemes in official languages. AVISPA is a collection of protocol analysis technologies and libraries to ensure robustness, scalability and security, and standardize security protocols. HLPSL is a role-based language, which indicates the continuity of the activities of each contract member in the module. We have expressed the security goals in HLPSL. We show the objectives of the special occasions in the HLPSL as well. For example, the mystery of sec m Key, sec v Key indicates that if the gatecrasher accepts the mysterious respect, it is not for him and another person has effectively attacked the convention. HLPSL adapts to the determination of the target certainty determined by verification to observe whether the master node correctly believes that the proposed peer is available in the current session, have reached a specific state. Internally, the attack conditions are determined based on short-lived basic principles (as health attributes), but macros use security goals as often as possible, namely mysterious and unique verification types.

In Tab. 4, we show the security performance comparison of our proposed scheme with the existing authentication schemes. We compare the different prepositions (from P1 to P14) in the following.

Table 4: Performance comparison with existing authentication schemes

Security propositions	Yeh et al. [12]	Wu et al. [16]	Amin et al. [18]	Li et al. [14]	Zhang et al. [1]	Our
P1	N/A	Y	Y	Y	Y	Y
P2	Y	N	N	N	Y	Y
P3	NA	Y	N	N	N	Y
P4	Y	N	Y	Y	Y	Y
P5	Y	Y	Y	Y	Y	Y
P6	Y	Y	N	Y	Y	Y
P7	N	Y	Y	Y	Y	Y

(Continued)

Table 4: Continued

Security propositions	Yeh et al. [12]	Wu et al. [16]	Amin et al. [18]	Li et al. [14]	Zhang et al. [1]	Our
P8	N	Y	N	N	Y	Y
P9	N/A	Y	Y	Y	Y	Y
P10	N	Y	N	Y	Y	Y
P11	N	Y	Y	Y	Y	Y
P12	N	Y	Y	Y	Y	Y
P13	N	Y	Y	N	Y	Y
P14	N	N	N	N	N	Y

Note: N = NO, Y = Yes, N/A = Not Applicable.

P1: The proposed method prevents offline password guessing attacks.

Proof: Our solution resists offline password or dictionary attacks, that is, if adversary A wants to obtain the password when logging in from one of the login cases (LCi), IDi and PWi are not found, because the transmission message {S5 . . . S11} has no information about the user Ui (IDi and PWi). Unfortunately, if A is from a smart card {IDsc, H(.), H ∗ (.), X1, Y, S3, S4} or from a mobile device {IDmd, H(.), H ∗ (.), X1, Y, S3, S4} But S1 cannot be calculated because the values of Y and M and the string encrypted with high-entropy random numbers cannot be obtained. The substrings stored in SC and MD will be decrypted when one of the missing substrings is obtained from the healthcare server. This is why the proposed method can prevent offline guessing attacks.

P2: Our proposed method guarantees for biometric protection.

Proof: User Ui's biometric template BTi protective wrapper has high entropy random number RN1 and is stored in smart card and mobile device $Z = rn_1 \oplus H(H^*(S_2))$, $S_4 = H(ID_i \oplus PW_i \oplus rn_1) \oplus S_2$ strings. And as $S_2 = BT_i \oplus rn_1$ biometric identity is stored in the database of the healthcare server. If attacker A accesses the stored biometric character string, but cannot extract the biometric template without knowing RN1.

P3: Proposed method statement for user anonymity and untrace capabilities.

Proof: Ui stores biometric identities in a database and calculates S5, S6, S7 for every login. When there is no RN3 and RN4 login password dynamically and randomly during the authentication phase, the reason behind this value will change in each session and can be retained. The user's ability is anonymous and untraceable by adversary A.

P4: Proposed method preserves server from internal/insider attack.

Proof: An internal attack is completely invalid in this scenario, because the database table has no Ui identity information. The healthcare server only stores the biometric template identity BTi. If adversary A unfortunately steals a database table and accesses biometric information, but the information is of no use to him/her and cannot access the identity and password of user Ui. Internal attacks are also known as insider attacks [20].

P5: Proposed method resists stolen verifier attack.

Proof: The database table is composed of three attribute names biometric identity S2, login case LC0 and LC. If adversary A successfully steals the database table and tries to guess the key (hs) of the healthcare server and calculates S2' = S6 ⊕ h (h ((h ∗ (S2) ||hs') ||S7 ⊕ h ∗ (S2)) the verification

code but in vain, because the threshold level of the biometric template is an unbearable threshold level. Secondly, trying to find the server master key has no results, because the master key is extracted from a high-entropy random number.

P6: Proposed method prevents replay attacks.

Proof: Only when the communication between the user Ui and the healthcare server HSi does not have proper identity verification, a replay attack is possible. In order to avoid this type of threat, the user Ui and the server HS communicate {S5 . . . S11} through mutual authentication and session key negotiation. The values of RN3 and RN4 will change for each next user. Suppose that attacker A captures the communication message between Ui and HSi, and sends any message to HSi and is identified because the value of the session key does not match.

P7: Proposed method protects impersonation attacks.

Proof: An impersonation attack occurs when an unauthorized user sends a message to the recipient on behalf of an authorized user. This happens when the adversary tracks the identity of the user Ui, but the solution we proposed in our method is to save the biometric information in the database and communicate through messages with biometric identities, which is impossible for the adversary.

P8: Proposed method resists desynchronization attacks.

Proof: When there is a communication gap between Ui and HSi, a desynchronization attack will occur. In our proposed method, HSi constructs the session key S10 and sends it to Ui when Ui receives the session key message from HSi in time, and then calculates its S11 based on the HSi message. Otherwise, HSi terminates the session and restarts the login and identity verification process. The proposed scheme ensures synchronization and resists such attacks.

P9: Proposed method guarantees known session key security.

Proof: When the key parameters of Ui and HSi are the same, the security of the known session key still exists. In our method, SesKui = SesKhs is calculated for each user and each login session. The new values of M and RN3 and RN4 high-entropy random numbers are used, and are known by Ui and HSi. Therefore, the proposed method guarantees what is called session key security.

P10: Proposed method ensures full forward secrecy.

Proof: Full forward secrecy guarantee means that message secrecy is maintained and dynamically changed during each transmission between Ui and HSi. The entire communication will be free from the adversary attack. The value is stored in in the smart card SCi or mobile device. If the opponent already knows the PWi and the key hs and tries to calculate M and S1 but he/she only knows the current message, if he/she has biometric information only. Otherwise this operation cannot be performed.

P11: Proposed method works on perfect mutual authentication.

Proof: Perfect mutual authentication means that a complete handshake process occurs and then data communication is started between between Ui and HSi. In our scheme, the strings S8 and S9 are used for authentication between Ui and HSi. It is verified that Ui and HSi share common SesKu and SesKhs, and update Xnew1 and Xnew2 to smart cards or mobile devices. At the same time, LC0 also updates the new value to the database table.

P12: Proposed method provides resistance against man-in-the-middle attack.

Proof: Our defense against man-in-the-middle attacks is that we prevent desynchronization attack factors. When we pass authentication messages between Ui and HSi, we focus on confirmation

messages S10 and S11. If one of them is blocked for any reason, the session is terminated and restarted. Start the login and authentication process. This thing eradicated the clues of man-in-the-middle attacks.

P13: Proposed method defined by formal security proof.

Proof: Our solution has been formally proven by using the formal Internet security verification AVISPA tool and tested for multiple security attacks. The HLPSL is used to define secure and reliable authentication protocols. AVISPA clearly verifies that the proposed method is safe from active and passive attacks. We used the HLPSL names On-the-Fly Model Checker (OFMC) and Constraint-Logic-Based-Attack Searcher (CL-ATSE) two back-end and abstract-based methods, and displayed the results in a specified format as shown in Fig. 2.

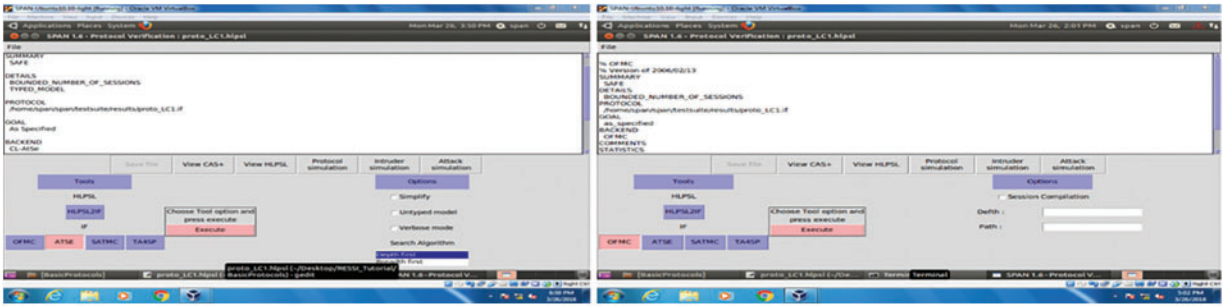

Figure 2: Security validation by OFMC and CL-ATSE

P14: Proposed method protects smart card or mobile device lost attacks.

Proof: When the smart card SCi or mobile device MDi is lost or stolen by adversary A, our proposed method will protect the identity verification process and secret information from offline or online guessing attacks. For complete authentication, the adversary cannot calculate S1 = h(IDi||PWi||h(BTi)) and M = h(h ∗ (S2) ||hs) because he/she has no information about the secret master key HSi and HSi are values generated by a one-way hash function.

5 Situation and Execution Cost Variant Analysis

We compared our model with the existing authentication schemes in Tab. 5 for various situations. We will discuss all these cases one by one as follows. C1: The user's biometric model is infected due to injuries in the medical field, and the biometric template (fingerprint, thumb scan, iris, etc.) of the application user may be affected by the injury. Its physical properties have changed, and its templates cannot be scanned. In this case, our proposed authentication method provides an alternative to login case (LC) and uses other login credentials, ignores the infected biometric pattern, and immediately handles the authentication process. In the proposed JKA model, the user can use ID, PW and smart card to access his or her system.

Table 5: Situation variant comparison of the proposed scheme with the existing schemes

Security propositions	Yeh et al. [12]	Wu et al. [16]	Amin et al. [18]	Li et al. [14]	Zhang et al. [1]	Our
C1	NS	NS	NS	NS	NS	S
C2	NS	NS	NS	NS	NS	S
C3	NS	NS	NS	NS	NS	S
C4	NS	NS	NS	NS	NS	S
C5	NS	NS	NS	NS	NS	S
C6	NS	NS	NS	NS	NS	S
C7	NS	NS	NS	NS	NS	S
C8	NS	NS	NS	NS	NS	S
C9	NS	NS	NS	NS	NS	S
C10	NS	NS	NS	NS	NS	S
C11	NS	NS	NS	NS	NS	S
C12	NS	NS	NS	NS	NS	S
C13	NS	NS	NS	NS	NS	S

Note: NS = Not Supportive; S = Supportive.

C2: Due to any substance, the user's biometric pattern is not clear. In the healthcare field, the biometric templates (fingerprints, thumb scans, iris, etc.) of app users may be affected by the use of fingerprints or substances on their thumbs. Its physical properties include any substance, such as oil, carbon, dust, etc. In this case, the authentication method we recommend is supported. The user can use ID, password and smart card to access his/her system.

C3: The user's biometric model does not meet the tolerable threshold level. In this case, the user printed a biometric pattern, but the machine had a technical failure and could not capture a clear fingerprint or iris image. For this reason, the BTi image result exceeded the acceptable threshold level. This is why our proposed method allows users to log in to the system using ID/PW and smart card, and extract the previous biometric pattern after comparing ID/PW.

C4: If the user has forgotten the ID or PW or both, but he/she can choose to use a biometric template and smart card to access the system. In this way, the user and the system are also very easy. Compared with ID and PW, system access via biometric cards and smart cards is highly secure.

C5: If the user believes that his/her ID and PW are compromised. Then, biometrics and smart card authentication is another option for him/her to access the system.

C6: Lost/stolen smart card. In this case, the user has lost or stolen his/her smart card, but the user wants to access the system immediately. The method we propose supports him/her to use another source called a mobile device to access the system. Because at the time of registration, the same authentication $\underset{\text{write into Smart Card}}{\{ID_{sc}, H(.), H^*(.), X_1, Y, S_3, S_4\}}$ and $\underset{\text{write into Mobile Device}}{\{ID_{md}, H(.), H^*(.), X_1, Y, S_3, S_4\}}$ strings are stored in smart cards and mobile devices, so it is a suitable substitute for smart cards. Second, only use the mobile device in login scenario 2, where the user wants to access the system without using a smart card. All authentication strings are extracted and matched from the mobile device.

C7: If the smart card of the user is damaged. Our system supports him/her to get access by using another source called mobile device. Because at the time of registration, same authentication strings stored into smart card and mobile device so that it would be suitable alternative of smart card.

C8: If the smart card reader device cannot read the card. Our system then guides the user to use his/her mobile device and access the system.

C9: If the user has lost or stolen his/her mobile device, but the user wants to access the system immediately. The method we propose supports him/her to use another source called a smart card to access the system. Because the same authentication string is stored in the smart card and the mobile device at the time of registration, it is a suitable substitute for the mobile device.

C10: If the mobile device of the user is damaged. Our system then supports user to use another source called a smart card to access the system. Because in the registration time, the same authentication string is stored in the smart card and the mobile device, so it is a suitable substitute for the mobile device.

C11: If the mobile device is not detected by the system or the user cannot read the authentication information from the mobile device. Our system prioritizes the use of smart cards to access the system in the case of LC1, LC3 and LC4.

C12: Implement organizational policies and standards. Our proposed method is flexible to customize security features for organizations to define their system authentication policies individually. Our systems are dynamically shaped according to organizational standards.

C13: Our proposed system supports organizations that set login factors based on the current economic situation. Sometimes, compared with mobile devices, it is expensive to issue a smart card for each employee, or sometimes it is not economical to use a biometric machine, then the solution we propose will run dynamically as needed.

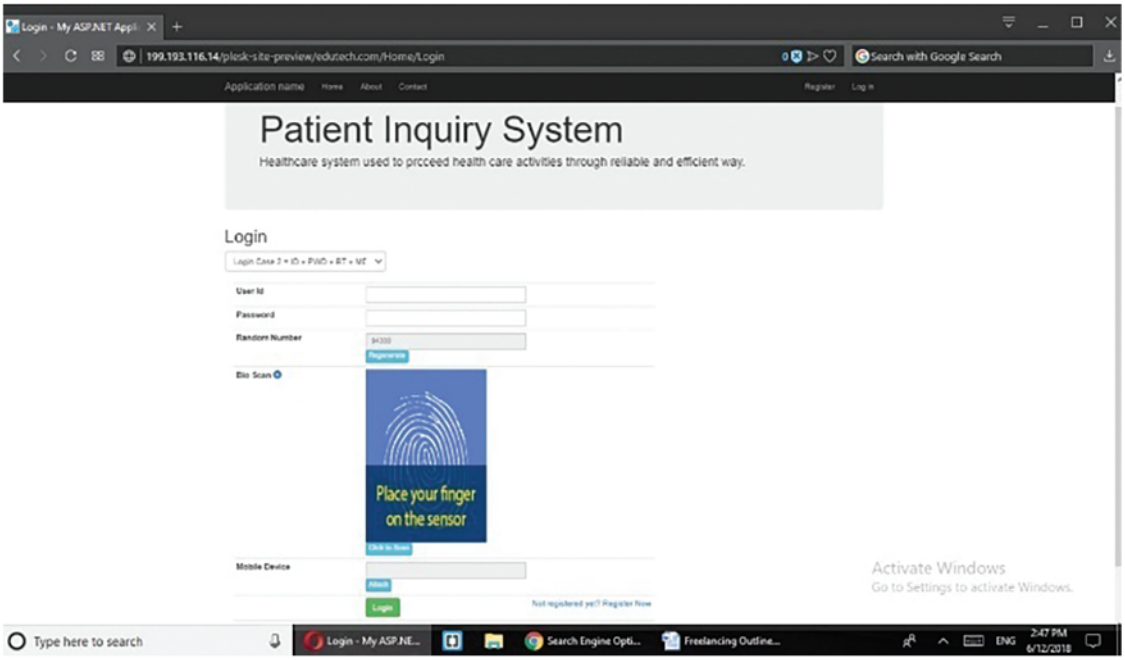

Figure 3: Registration interface

We have investigated the operating costs of the proposed system and compared it with existing solutions. To this end, we developed a prototype at the local intermediate health center, as shown in Fig. 3. We considered the time and space costs used in the login and authentication phases of login case 2. The prototype is a framework with Android library functions and MS SQL SERVER in a Web-based application developed in ASP.NET MVC 5. The execution time is shown in Tab. 6, which is the average of 100 results. The parameter selection to measure the execution cost is based on the consumption of the highest running time, so only the cost of Hash and Bio-hash operations that take a lot of running time is calculated, not the exclusive OR operation of encryption and decryption. Due to the efficient execution time and flexible operation in various situations, our proposed scheme is superior to other schemes.

Table 6: Execution cost comparison of the proposed scheme with the existing schemes

Authentication schemes	Hash & Bio Hash opr.	Other operations used in algorithm	Average execution time (ms)
Yeh et al.	3Thsh	4Tsm + 12Tadd	3.4508
Wu et al.	12Thsh + 1Tb-hsh	4Tsm + 4Tsk	3.2252
Amin et al.	10Thsh + 1Tb-hsh	-	0.0819
Li et al.	10Thsh + 1Tb-hsh	4Tme	6.6610
Zhang et al.	19Thsh + 4Tb-hsh	-	0.0989
Our	18Thsh + 4Tb-hsh	-	0.0978

6 Conclusions

We propose a mutual authentication scheme, which provides a dynamic solution for the selection of multiple factors when accessing the electronic health system. The proposed scheme is more flexible to handle the real-time situation of medical staff and patients who want easier access to the system. The dynamic behavior of the proposed scheme selects different key factors, which are economical for organizations that want to adopt cheap and reliable authentication mechanisms. This cost-reduction strategy can encourage medical institutions and personnel to accept the certification scheme proposed for modern electronic medical systems. We verified the security features of the proposed scheme through informal analysis. We have investigated the proposed scheme of the existing model according to the implementation cost and various situations. Due to the lightweight operation of the bio-hash operation with modular exponential function, our scheme has lower computational cost. For future work, it is necessary to find simpler and more convenient ways to use the proposed authentication scheme to integrate all devices, such as (smart card readers, mobile devices, and biometric scanners).

Acknowledgement: We deeply acknowledge Taif University for supporting this study through Taif University Researchers Supporting Project Number (TURSP-2020/150), Taif University, Taif, Saudi Arabia.

Funding Statement: This work was supported by Taif University (in Taif, Saudi Arabia) through the Researchers Supporting Project Number (TURSP-2020/150).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Zhang, Y. Zhang, S. Tang and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2795–2805, 2018.

[2] L. Zhang, S. Zhu and S. Tang, "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 2, pp. 465–475, 2016.

[3] X. Li, Q. Wen and W. Li, "A three-factor based remote user authentication scheme: Strengthening systematic security and personal privacy for wireless communications," *Wireless Personal Communications*, vol. 86, no. 3, pp. 1593–1610, 2015.

[4] Q. Jiang, M. K. Khan, X. Lu, J. Ma and H. Debiao, "A privacy preserving three-factor authentication protocol for e-health clouds," *Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[5] J. Ling and G. Zhao, "An improved anonymous password authentication scheme using nonce and bilinear pairings," *International Journal of Network Security*," vol. 17, no. 6, pp. 787–794, 2015.

[6] L. L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *Journal of Medical Systems*, vol. 39, no. 2, pp. 1–9, 2015.

[7] J. L. Fernández-Alemán, I. C. Señor, P. A. O. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, 2013.

[8] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 20, pp. 1–15, 2014.

[9] M. S. Farash and M. A. Attari, "Cryptanalysis and improvement of a chaotic map-based key agreement protocol using chebyshev sequence membership testing," *Nonlinear Dynamics*, vol. 76, no. 2, pp. 1203–1213, 2014.

[10] X. L. Li, Q. Y. Wen, W. M. Li, H. Zhang and Z. P. Jin, "Secure privacy-preserving biometric authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 11, pp. 1–8, 2014.

[11] J. S. Yu, G. L. Wang, Y. Mu and W. Gao, "An efficient generic framework for three-factor authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302–2313, 2014.

[12] L. H. Yeh, T. H. Chen, K. J. Hu and W. K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Information Security*, vol. 7, no. 3, pp. 247–252, 2013.

[13] E. J. Yoon and K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *Journal of Supercomputing*, vol. 63, no. 1, pp. 235–255, 2013.

[14] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[15] C. -I. Fan and Y. -H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 933–945, 2009.

[16] F. Wu, L. Xu, S. Kumari and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Computers & Electrical Engineering*, vol. 45, pp. 274–285, 2015.

[17] C. L. Brown, "Health-care data protection and biometric authentication policies: Comparative culture and technology acceptance in China and in the United States," *Review of Policy Research*, vol. 29, no. 1, pp. 141–159, 2012.

[18] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan and X. Li, "Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems," *Journal of Medical Systems*, vol. 39, no. 11, pp. 1–21, 2015.

[19] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.
[20] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.