Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 10, No. 03, September 2024.

AN IMPROVED AND EFFICIENT RSA-BASED AUTHENTICATION SCHEME FOR HEALTHCARE SYSTEMS

Fatty M. Salem[1], Nisreen F. Zaky[2], Elsayed M. Saad[2] and Hadeer A. Hassan Hosny[2]

(Received: 14-Feb.-2024, Revised: 5-Apr.-2024 and 26-Apr.-2024, Accepted: 8-May-2024)

ABSTRACT

Owing to the fast advancements of wireless communication, the telehealthcare platform makes it possible for patients to access healthcare services online. However, creating a secure and efficient authentication scheme for healthcare systems still presents a challenge. Several solutions have been introduced, but the majority of them are shortly found to be unable to meet some essential security standards. In this paper, we first revisit Dharminder et al.'s scheme and prove its failure to provide mutual authentication and pacient's untraceability and its vulnerability to impersonation attacks. Furthermore, we suggest an improved RSA-based authentication scheme to mitigate the deficiencies observed in Dharminder et al.'s schema. The proposed scheme can provide mutual authentication, patients' anonymity and untraceability and resist various types of attacks. Extensive evaluation on AVISPA proves the safeness of the proposed scheme against both passive and active attacks. Additionally, the proposed scheme is computationally and communicationally more efficient in comparison to other existing schemes.

KEYWORDS

Healthcare system, Authentication, Anonymity, Untraceability, Privacy.

1. INTRODUCTION

The Internet widespread utilization leads to creating a healthcare services' platform. The health records are transitioning from paper-based to electronic medical records that connect doctors and patients *via* medical servers. One widely used healthcare service is Telecare Medical Information System (TMIS) which provides healthcare services that are delivered to people at home [1].

In TMIS, all participants are registered by an established medical server, including nurses, doctors and patients. In general, it keeps electronic medical records of registered patients where a patient who has been registered can access the remote service whenever he/she wants and from any place. This system provides many advantages. First, due to the immediate communication offered by TMIS, healthcare services could be made available whenever and wherever. TMIS can overcome the limitations of time and distance. Second, TMIS servers allow access to patients' medical histories, which is extremely helpful for doctors in providing patients with the best possible medical care. Third, it requires less maintenance and can consolidate patient medical records from different healthcare providers.

Despite these benefits, TMIS may be susceptible to well-known attacks [2] due to its reliance on public networks. Therefore, a hacker can access messages sent over public channels and intercept, record, modify, delete and replay them. Furthermore, patient private information should be safeguarded to ensure user privacy. Therefore, to ensure the safety of TMIS, several security measures need to be achieved, such as mutual authentication, patient anonimity and untraceability and forward secrecy. Additionally, several attacks must be resisted, including insider attacks, attacks using stolen smart cards, offline password guessing attacks and attacks impersonating patients or servers.

For example, wearable health devices, such as fitness trackers and medical monitoring devices, represent a wealth of health data that can be vital for patient care. These devices often need to connect and transmit data to various healthcare platforms, ranging from personalized health applications to comprehensive healthcare systems. The challenge is to authenticate these devices to ensure transmitting data securely,

1. F. M. Salem (Corresponding Author) is with Department of Electronics and Communications Engineering, Faculty of Engineering, Helwan University, Helwan, Cairo, Egypt and with Faculty of Computing and Information Sciences, Egypt University of Informatics, New Administrative Capital, Cairo, Egypt. Email: faty_ahmed@h-eng.helwan.edu.eg
2. N. F. Zaky, E. M. Saad and H. A. Hassan Hosny are with Department of Computers and Systems Engineering, Faculty of Engineering, Helwan University, Helwan, Cairo, Egypt.

accurately attributed to the correct patient and smoothly integrating with the patients' health records in different systems.

1.1 Challenges and Basic Idea

The focus of this paper is on designing a healthcare authentication scheme and highlighting several challenges that must be addressed in developing a secure and efficient authentication model for healthcare systems [3]. The main challenges include:

- **Mutual Authentication and User Anonymity:** Previous schemes, including the one proposed by Dharminder et al. [4], have not succeeded in delivering mutual authentication and user anonymity. This is a significant gap, as mutual authentication ensures that both the user and the server verify each other's identity and user anonymity protects the identity of users accessing the system.
- **Resistance to Impersonation Attacks and Other Attacks:** This paper emphasizes the vulnerability of existing authentication systems to impersonation attacks, wherein an attacker masquerades as a legitimate user or server, along with other cyber threats, like impersonation attacks, replay attacks, insider attacks, stolen smart-card attacks and offline password-guessing attacks. These vulnerabilities expose sensitive patient data and system integrity to significant risks.
- **Efficiency in Computation and Communication Costs:** Another highlighted challenge is the need for an authentication scheme that prioritizes both security and efficiency in terms of computation and communication. Previous schemes suffer from high computational and communication costs, making them less practical for real-world applications.
- **Comprehensive Security Measures:** The review and analysis of various authentication schemes revealed a consistent challenge in developing an authentication system that effectively protects against diverse forms of attacks while maintaining the privacy and anonymity of users. This includes safeguarding against insider attacks, theft of smart cards and offline password guessing, as well as ensuring the freshness of session keys.

1.2 Motivation

The motivation behind this work stems from the critical analysis of existing authentication schemes for securing healthcare systems, especially the scheme proposed by Dharminder et al. [4]. The surge in healthcare services, facilitated by advancements in wireless communication, has highlighted significant security challenges, including the protection of sensitive patient data and the integrity of medical consultations. Existing systems, as exemplified by Dharminder et al.'s approach [4], failed in offering comprehensive security, lacking mutual authentication, user anonymity and resisting various types of attacks. Our motivation is driven by the urgent need to solve these vulnerabilities by proposing an authentication scheme for healthcare systems that is secure, efficient and feasible. Hence, we aim to contribute to the development of healthcare systems to ensure patient privacy, data integrity and service reliability, thus fostering trust and wider adoption of online healthcare services.

1.3 Our Contribution

This paper proposes an improved RSA [5] (Rivest-Shamir-Adleman)-based authentication scheme for healthcare systems. Specifically, the proposed scheme allows both patient and server to authenticate mutually; hence, they can agree on a secure shared session key. This paper's key contributions can be summarized as follows:

- We have looked over Dharminder et al.'s scheme in [4] and discovered that it lacks the ability to offer mutual authentication and untraceability and is incapable of withstanding both user and server impersonation attacks.
- An improved authentication scheme utilizing RSA encryption is proposed to address the security vulnerabilities present in Dharminder's scheme [4].
- The proposed scheme is created with two messages of exchange to ensure and speed up the session key agreement.
- A brief comparison is given between the proposed scheme and other current schemes. When

compared with similar schemes, the comparison suggests that the proposed scheme offers superior benefits in terms of security, computational costs and communication overheads.

- The proposed scheme has been subjected to security verification using the AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, confirming its security against both passive and active attacks.

1.4 Roadmap of This Article

The structure of this article is outlined as follows: Related work on the authentication of healthcare systems has been reviewed in Section 2. Some preliminaries used in the proposed scheme are provided in Section 3. The threat model is defined in Section 4. Dharminder et al.'s scheme is reviewed and cryptanalyzed in Section 5. Furthermore, Section 6 presents the proposed scheme. In Section 7, the analysis of the proposed scheme's security through both formal and informal methods is presented. Section 8 includes a performance evaluation of the proposed scheme. Finally, conclusions are prsenetd in Section 9.

2. RELATED WORK

Numerous authentication schemes have been suggested for healthcare systems to achieve authentication and preserve the privacy of patients. For example, in 2016, Li et al. [6] introduced an authentication scheme for an e-healthcare system based on the chaotic map. However, Madhusudhan & Nayak [7] explained that Li et al.'s scheme couldn't withstand user impersonation attacks, server impersonation attacks, password guessing attacks and man-in-the-middle (MIMT) attacks. In addition, Madhusudhan [7] elucidated that Li et al.'s scheme [6] established an insecure session key and can't guarantee user anonymity.

In [8], the authors introduced a secured data access/sharing system based on chaotic maps for an Internet of Things (IoT)-enabled cloud storage environment. During the data-storage phase, a secret key derived from the user's biometric information is utilized to encrypt the data, enabling the data owner to store it in encrypted form on a cloud server. After receiving consent from both parties, users can retrieve the data from the cloud server during the data-sharing phase. Additionally, the authors in [9] introduced a Chaotic Map-based Authentication Protocol for Crowdsourcing IoT (CMAP-IoT). In CMAP-IoT [9], the medical server keeps patient health information and the users must authenticate with the medical server before being able to access the data contained in the medical server. Nevertheless, this system lacks the ability to offer user anonymity while being susceptible to user impersonation attacks.

In 2017, Ankita Chaturvedi et al. [10] reviewed several authentication schemes [11]-[14], but they found that these schemes [11]-[14] are unable to detect input correctness, leading to Denial of Service (DoS) scenarios and any error made during the password-changing process prevents the user from logging in with the same smart card. Chaudhry et al. introduced an enhancement to the two-factor authentication protocol [15], yet Shuming Qiu et al. [16] pointed out that Chaudhry et al.'s scheme [15] is unable to withstand offline password-guessing attacks, MIMT attacks and user/server impersonation attacks. To address these shortcomings, Qiu et al. [16] developed a scheme to defend against all known attacks and presented an elliptic curve-based mutual authentication scheme for TMIS.

Li et al. [17] have introduced a mutual-authentication scheme that is both secure and anonymous for two-hop wireless body-area networks. However, upon reviewing Li et al.'s scheme [17], still Koya and Deepthi [18] found vulnerabilities, including critical escrow issues and susceptibility to sensor node impersonation attacks. Additionally, they noted that the assumption regarding the reliability of the hub node is unrealistic. In addition, Kompara et al. [19] explained that Li et al.'s scheme [17] is ineffective and can't offer untraceability. Therefore, a new authentication scheme has been proposed in [19], employing only two types of operations: the cryptographic hash function and the XOR operation. This is aimed at reducing computational complexity and transmission costs. However, Rehman et al. [20] elucidated that Kamparaa et al.'s scheme [19] can't achieve anonymity and untraceability and can't resist impersonation attacks and sensor-node impersonation attacks. On the other hand, Rehman et al.'s scheme [20] is still susceptible to desynchronization attacks.

Lee et al. introduced a mutual authentication scheme for remote users using smart cards [21]. However, Radhakrishnan et al. [22] clarified that Lee et al.'s scheme [21] is susceptible to identity-guessing

attacks, password-guessing attacks, insider attacks, stolen smart-card attacks and DoS attacks. Mishra et al. [23] proposed an authentication method for TMIS utilizing biometrics and nonce. Still, Zhang et al. [24] elucidated that Mishra et al.'s scheme [23] is vulnerable to replay and MIMT attacks and can't achieve forward secrecy. Additionally, A three-factor authenticated TMIS technique based on chaotic maps was presented by Zhang et al. [24] to address the shortcomings of Mishra et al.'s scheme [23]. It is obvious that in schemes [9][22][24], users are at risk of identity and password guessing, as well as stolen smart-card attacks. Kim et al. [25] introduced a lightweight authentication method that ensures anonymity through biometric-based authentication, aiming at maintaining the freshness of the message requests' keys.

In 2020, Dharminder et al. [4] reviewed Radhakrishnan et al. [22] and found that it can't achieve unlinkability and resist identity-guessing attacks, password-guessing attacks and stolen smart-card attacks. Hence, an authentication method was presented by Dharminder et al. [4] to solve the weakness of the schemes in [9][22][24]. However, our findings indicate that Dharminder et al.'s scheme [4] fails to offer mutual authentication and untraceability and is susceptible to user and server impersonation attacks, as we will demonstrate later. In addition, Soni et al. [26] elucidated that Dharminder et al.'s scheme [4] requires more computation cost and communication overhead. To guarantee low latency, a mutual-authentication architecture based on fog computing for healthcare was described by Singh et al. [27] using RSA; however, Singh et al.'s scheme [27] is susceptible to Greatest Common Divisor (GCD)-based attacks.

In [28], an authentication protocol utilizing Radio Frequency Identification (RFID) and El-Gamal cryptosystem has been proposed to safeguard patients' privacy in TMIS. The scheme can defend against several types of attacks, including tag impersonation, location tracking, replay, de-synchronization and DoS attacks. In [29], Khan et al. introduced a lightweight RFID protocol to protect patient privacy by employing pseudonyms instead of real IDs. An anonymous patient monitoring system has been proposed by Amin et al. [30] using wireless medical-sensor networks. Still, Ali et al. [31] found that Amin et al.'s scheme [30] can't resist offline password-guessing attacks, user impersonation attacks and known session-key temporary-information attacks. Moreover, to solve these problems, Ali et al. [31] suggested a mechanism with three-factor authentication of Amin et al.'s scheme [30] using symmetric encryption and hash functions to offer authentication. However, Ali et al.'s scheme [31] can't offer perfect forward secrecy nor resist desynchronization attacks, guessing attacks and insider attacks.

Sharma et al. [32] recommend implementing an authentication scheme for cloud-based healthcare systems; however, Canetti and Krawczyk [33] demonstrated that Sharma et al.'s scheme [32] is susceptible to privileged insider attacks. Recently, an anonymity-preserving user-authentication method has been presented by Masud et al. [34] and its primary goal is to ensure users' anonymity, but Masud's scheme [34] can't achieve anonymity of communicating parties and can't resist insider attacks and desynchronization attacks. In [35], a three-factor authentication protocol has been proposed for consumer USB mass-storage devices. However, Renuka et al. [36] identified that the scheme in [35] fails to guarantee user anonymity and forward/backward secrecy and is unable to withstand session-specific temporary attacks. Moreover, the scheme in [35] can't enable users to change their password. Sonia et al. [37] suggested a remote authentication scheme consisting of three factors for a patient monitoring system; however, Sonia et al.'s plan [37] contains serious faults, according to Xu et al. [38], including sensor-node capture assault, lack of forward secrecy and loss of three-factor security. Table 1 summarizes the existing relevant schemes on the security of healthcare systems.

A lot of authors claimed that their schemes are secure and proved the security of their proposed schemes using various methods of formal security proof; however, Wang et al. [39]-[40], found that formal security proof has its limitations and for the formally proven schemes, informal analysis of these schemes proved their failure of offering several essential security requirements and their vulnerabilities to various types of attack. This is why we first reviewed and analyzed Dharminder et al.'s scheme and then proposed an improved authentication scheme to overcome the shortcomings of Dharminder et al.'s scheme.

3. PRELIMINARIES

This section will review some basic information essential for this study.

Table 1. Summary of related work.

Ref.	Countermeasure	Advantages	Disadvantages
[4]	RSA-based Authentication	Can achieve anonymity, forward secrecy and withstand replay attacks and man-in-middle attacks.	Can't achieve mutual authentication and untraceability and can't withstand impersonation attacks.
[9]	Chaotic-map Encryption	Can achieve mutual authentication and withstand DoS attacks, replay attacks and insider attacks.	Unable to offer user anonymity and susceptible to user impersonation attacks.
[10]	Identity-based Key Establishment	Can withstand offline password-guessing attacks and DoS attacks.	Can't resist man-in-the-middle attacks, replay attacks, insider attacks and stolen-verifier attacks.
[15]	Elliptic-curve Cryptography	Can offer mutual authentication while maintaining user anonymity.	Unable to withstand offline-password-guessing attacks, user/server impersonation attacks and MIMT attacks.
[16]	Elliptic-curve Cryptography	Capable of achieving mutual authentication and forward secrecy.	Can't resist insider attacks.
[19]	Hash Function and XOR Operation	Can achieve mutual authentication and reduce computation complexity and transmission costs.	Can't achieve anonymity and untraceability and can't resist impersonation attacks and sensor-node impersonation attacks.
[22]	Diffie-Hellman Problem and Hash Functions	Can offer mutual authentication, forward secrecy and guarantee user's anonymity and untraceability.	Can't resist man-in-the-middle attacks, replay attacks and insider attacks.
[30]	Hash Function and XOR Operation	Can offer mutual authentication and user's anonymity and untraceability.	Unable to withstand offline password-guessing attacks, user impersonation attacks and known session-key temporary-information attacks.
[32]	Hash Function and XOR Operation	Can offer mutual authentication, forward secrecy, data integrity and user's anonymity and untraceability.	Unable to withstand privileged inside attacks.
[34]	Hash Function and XOR Operation	Can provide mutual authentication and data privacy and resist against impersonation attacks, replay attacks and MIMT attacks.	Can't achieve anonymity of communicating parties and can't resist insider attacks and desynchronization attacks.
[36]	Fuzzy Extractor	Can offer mutual authentication, forward secrecy, anonymity, robustness to replay attacks and impersonation attacks.	Can't withstand offline password-guessing attacks, insider attacks and smart-card loss attacks.
[37]	Rabin Cryptosystem and Chaotic Maps	Can offer mutual authentication, forward secrecy and user's anonymity and untraceability.	Can't resist against sensor-node capture attacks and suffer lack of forward secrecy and loss of three-factor security.

3.1 RSA-based Cryptosystem

This sub-section will concentrate on revisiting the fundamental definition and properties of the RSA Cryptosystem [5].

First, choose two primes, p and q and compute the modulus $n = p \times q$ and the Euler totient function $\varphi(n) = (p-1) \times (q-1)$. To generate the public and private keys, select an integer e such that $gcd(e, \varphi(n)) = 1$ and compute $d \equiv e^{-1} \, mod \, \varphi(n)$. The public key is denoted by e, while the private key is represented by d. Encryption and decryption using the RSA algorithm are outlined as follows:

1. In RSA encryption, the sender encrypts a message m using the receiver's public key e as follows:
$c = m^e \, mod \, n$.

2 . When the receiver receives the cipher text c, the receiver decrypts it using the receiver's private key d as $m = c^e \ mod \ n$.

3.2 Hash Function

An algorithm is a hash function that maps various-length inputs into a fixed-length output known as a hash value or hash code. The mathematical function condenses the message to a predetermined size and is a one-way function, making it challenging for attackers to recognize and decrypt the message. Cryptographic hashes come in various forms; for instance, SHA-1 (Secure Hash Algorithm 1) is a commonly utilized hash function that accepts an input and produces a 160-bit hash value. The cryptographic hash function provides many security services like message authentication and integrity and implements digital signatures. There are numerous aspects of the cryptographic hash function:

- Non-reversibility or one-way function: A strong hash should make reconstructing the original message from the hash output complex.
- Diffusion or avalanche effect: A half of the hash should also be changed if one piece of the original password is changed. In other words, if one bit in the initial message changes, the encrypted message should also vary.
- Determinism: The hash value or enciphered text generated by a particular message must always be the same.
- No collision: It would be difficult to find two distinct messages resulting in the same ciphertext.

4. THREAT MODEL

As the authentication protocol is executed over a public channel, the attacker utilizes several advantages or capabilities during the execution of the authentication protocol. We present some widely accepted assumptions as follows:

- An attacker can intercept, modify, delete and replay the exchanged messages.
- The smart card can be stolen or lost.
- An attacker may get the smart card and obtain its stored information.
- An attacker can run an impersonation attack if the user's password on the smart card is revealed.
- An attacker could be a legitimate user or a legitimate server.

5. REVIEW OF DHARMINDER ET AL.'S SCHEME

A review and cryptanalysis of Dharminder et al.'s scheme [4] are illustrated below.

5.1 Dharminder et al.'s Scheme

Three phases of the scheme introduced by Dharminder et al. are reviewed below:

- **Registration Phase**

User U_i registers to server S_j through secure channel as follows:

1.U_i selects Id_i and PW_i, generates a random b and computes $A_i = h(PW_i||b)$. Afterwards, U_i sends $\{Id_i, A_i\}$ to S_j.
2. After receiving $\{Id_i, A_i\}$, S_j calculates:

$Cid_i = h(Id_i||d)$

$A_u = Cid_i \oplus h(A_i||Id_i)$

$B_u = h(Cid_i||A_i||Id_i)$

3. U_i stores $\{A_u, B_u, e, n, h(.), h(Id_i \oplus PW_i) \oplus b\}$ in its Smart Card (SC).

- **Login Phase**

A legal U_i user starts in the login phase as:

1. U_i enters SC, inputs Id_i and PW_i and recovers $b = h(Id_i \oplus PW_i) \oplus b \oplus h(Id_i \oplus PW_i)$. Then, U_i calculates $A_i = h(PW_i||b)$ and $Cid_i = A_u \oplus h(A_i||Id_i)$ and verifies $h(Cid_i||A_i||Id_i) = B_u$.

2. After performing the verification, U_i selects a random $N_u \in Z_n^*$ and calculates $V_1 = h(A_i || Id_i)$, $V_2 = (Cid_i || A_u)^e$ and $V_3 = h(Cid_i || N_u || T_u)$, where T_u is the current timestamp of U_i.
3. Finally, U_i sends $M_1 = \{V_1, V_2, V_3, T_u\}$ to S_j.

- **Authentication Phase**

In the authentication phase, S_j obtains $M_1 = \{V_1, V_2, V_3, T_u\}$ from U_i and proceeds as follows:

1. S_j verifies T_u and computes:
   $V_2^d = (Cid_i || A_u)$
   $h(A_i || Id_i) = Cid_i \oplus A_u$
   $V_1 \oplus h(A_i \| Id_i) = N_u$
2. S_j calculates $V_3^* = h(Cid_i || T_u)$; if $V_3^* = V_3$, it authenticates U_i.
3. S_j selects a random value N_u and calculates:
   $SK_s = h(N_s || N_u || T_u || T_s)$
   $V_4 = N_s \oplus N_u \oplus Cid_i$
4. Then, S_j sends $M_2 = \{V_4, T_s\}$ to U_i.
5. After receiving $M_2 = \{V_4, T_s\}$, U_i verifies T_s and calculates $N_S^* = V_4 \oplus N_u \oplus Cid_i$.
6. Then, U_i computes $V_4^* = N_S^* \oplus N_u \oplus Cid_i$, if $V_4^* = V_4$, it authenticates S_j.
7. Finally, U_i computes a common session key $Sk_U = h(N_s || N_u || T_u || T_s) = Sk_s$.

5.2 Cryptanalysis of Dharminder et al.'s Scheme

Dharminder et al.'s scheme [4] will be analyzed below.

- **Impersonation Attack**

The attacker can potentially impersonate both the user and the server, as analyzed below**:**

User Impersonation Attack: To impersonate the user, let's consider that the adversary possesses the Id_i of a legal user U_i and also has access to the stored smart-card values $\{A_u, B_u, e, n, h(.), h(Id_i \oplus PW_i) \oplus b\}$, the adversary can generate any A_i^*, A_u^* and N_u^* and compute $Cid_i^* = A_u^* \oplus h(A_i^* || Id_i)$, $V_1^* = h(A_i^* || Id_i)$, $V_2^* = (Cid_i^* || A_u^*)^e$ and $V_3^* = h(Cid_i^* || N_u^* || T_u)$ and send $\{V_1^*, V_2^*, V_3^*, Tu\}$ to the sever.

After receiving $M_1 = V_1^*, V_2^*, V_3^*, Tu\}$, the server S_j computes:

$V_2^d = (Cid_i^* || A_u^*)$
$h(A_i^* || Id_i) = Cid_i^* \oplus A_u^*$
$N_u^* = V_1^* \oplus h(A_i^* || Id_i)$
$V_3' = h(Cid_i^* || N_u || T_u)$

It is evident that $V_3' = V_3^*$, which makes the server S_j identify the adversary as a legal user; hence, the adversary succeeds in masquerading to be a legal user.

Server Impersonation Attack: Furthermore, the attacker can act as the legal server by sending $M_2 = \{V_4^*, T_s\}$ and the user U_i will verify T_s and compute $N_S' = V_4^* \oplus N_u \oplus Cid_i$; then, U_i will compute V_4' as $V_4' = N_S^* \oplus N_u \oplus Cid_i$ using N_S^* which is computed using V_4^* itself; hence, for any value for V_4^*, when U_i compares V_4 with V_4', they will be equals and U_i will accept communication with the adversary as the legal server. Therefore, Dharminder et al.'s protocol can't achieve user authentication or server authentication.

- **Lack of Authentication**

Before providing any service, mutual authentication requires the server to verify the user and the user to authenticate the server. Furthermore, no illegal users or servers will be allowed to impersonate legal users or servers.

Mutual authentication can't be attained in Dharminder et al.'s scheme, leading to the problem of impersonating the user and the server. An attacker A can spoof a legal user and a legal server through the login process, as shown previously. This contradicts the process of mutual authentication for the scheme and limits the proper mutual authentication.

- **Lack of Unlinkability (Untraceability)**

Achieving linkability means that the attacker can't relate two messages to the same user; hence, the user's activities can't be traced in the system. As we see in equation $V_2 = (Cid_i||A_u)^e$, the value of V_2 is constant as it consists of Cid_i and A_u, which are encrypted by the fixed public key e and Cid_i consists of $\{A_u, A_i, Id_i, PW_i, b\}$ which are also fixed values. Consequently, V_2 remains constant in every communication applied between both the user and the server, allowing the equation mentioned above to link the user's message, thereby simplifying user identification.

6. THE PROPOSED SCHEME

To solve the flaws of Dharminder et al.'s scheme [4], we introduce a new authentication scheme utilizing RSA encryption with initialization to generate the server's public and private keys, as discussed in Section 2. The notations required for the proposed scheme are depicted in Table 2. The proposed scheme comprises four phases outlined as follows:

Table 2. Index of notations.

Notation	Interpretation
Id_i	User *i* identity
PW_i	User *i* password
e	Server *j* public key
d	Server *j* private key
T_u, T_s	Fresh timestamps
Sk_s	Session key computed by server *j*
S_{KU}	Session key computed by user *i*
$h(.)$	Hash function
$\oplus$	XOR operation
$\|\|$	Concatenation operation

6.1 Registration Phase

User U_i registers to server S_j through a secure channel as described in Figure 1 and illustrated as follows:

1. U_i selects Id_i, PW_i and a random number b, calculates $A_i = h(PW_i \,||\, b)$ and sends $\{Id_i, A_i\}$ to S_j.

2. S_j Computes:
$Cid_i = h(Id_i||d)$
$A_u = Cid_i \oplus h(A_i||Id_i)$
$B_u = h(Cid_i||A_i||Id_i)$
2. Then, S_j stores (Id_i, A_i, Cid_i) in its database and stores $\{A_u, B_u, e, n, h(.), h(Id_i \oplus PW_i) \oplus b\}$ in SC for U_i.

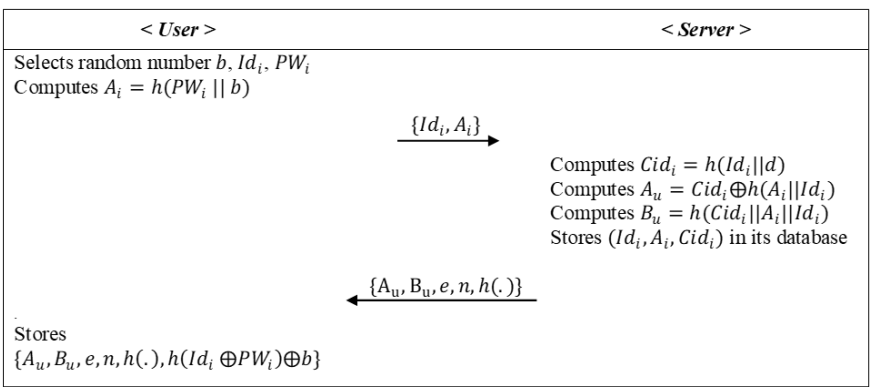


Figure 1. Registration phase.

6.2 Login Phase

In the login phase (described in Figure 2), a valid U_i progresses as follows:

1. First, a legal user U_i enters Sc, inputs Id_i and PW_i and recovers $b = h(Id_i \oplus PW_i) \oplus b \oplus h(Id_i \oplus PW_i)$.
2. U_i calculates $A_i = h(PW_i||b)$, $Cid_i = A_u \oplus h(A_i||Id_i)$ and performs verification for $h(Cid_i||A_i||Id_i) = B_u$.
3. After verification, U_i chooses a random number $N_u \in Z_n^*$ and calculates $V_1 = (Id_i||Cid_i||A_u||N_u||T_u)^e$, where T_u is the current timestamp of U_i.
4. Then, U_i Sends $M_1 = \{V_1, T_u\}$ to S_j.

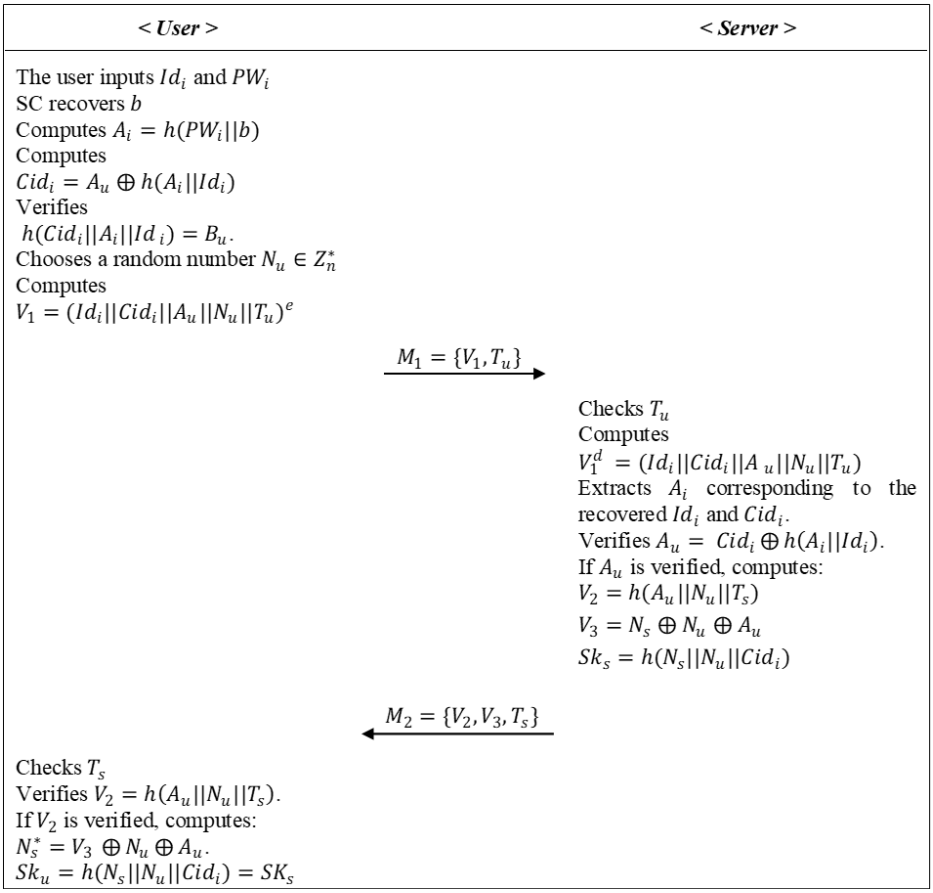


Figure 2. Login and authentication process.

6.3 Authentication Phase

Valid U_i proceeds in the authentication phase as follows:

1. Upon receiving $M_1 = \{V_1, T_u\}$ from U_i , S_j verifies T_u and calculates $V_1^d = (Id_i||Cid_i||A_u||N_u||T_u)$, extracts A_i corresponding to the recovered Id_i and Cid_i and verifies $A_u = Cid_i \oplus h(A_i||Id_i)$.
2. If A_u is verified, S_j computes:

   $V_2 = h(A_u||N_u||T_s)$
   $V_3 = N_s \oplus N_u \oplus A_u$
   $Sk_s = h(N_s||N_u||Cid_i)$
   Finally, S_j sends $M_2 = \{V_2, V_3, T_s\}$ to U_i.
3. Upon receiving $M_2 = \{V_2, V_3, T_s\}$, U_i checks T_s and verifies $V_2 = h(A_u||N_u||T_s)$.
4. If V_2 is verified, U_i computes $N_s^* = V_4 \oplus N_u \oplus A_u$.
5. Finally, U_i computes the session key $Sk_u = h(N_s||N_u||Cid_i) = SK_s$.

6.4 Password-change Phase

A legal user inputs Id_i, PW_i and a new password PW_i^{new}. Then, SC calculates $A_i = h(PW_i||b)$, $Cid_i = A_u \oplus h(A_i||Id_i)$ and verifies $h(Cid_i||A_i||Id_i) = B_u$. If verified, SC calculates the values $A_i^{new} = h(PW_i^{new}||b)$, $cid_i^{new} = A_u \oplus h(A_i^{new}||Id_i)$ and $h(cid_i^{new}||A_i^{new}||Id_i) = B_u^{new}$ and replaces B_u with B_u^{new}.

7. SECURITY ANALYSIS OF THE PROPOSED SCHEME

Here, we will conduct a brief security analysis of the proposed scheme. Furthermore, we utilized AVISPA [41] to simulate the proposed method for formal security verification.

7.1 Informal Security Analysis of the Proposed Scheme

This sub-section presents an informal security analysis of the proposed scheme. First, we will set up the achievement of the fundamental security needs and the suggested scheme's resistance to various forms of attacks in healthcare systems, as user impersonation, server impersonation, secure session key, insider attacks, stolen smart-card attacks and offline password-guessing attacks.

Mutual Authentication: When both the user and the server can authenticate each other successfully, the system is considered to have achieved mutual authentication.

On the server side, S_j computes $V_1^d = (Id_i||Cid_i||A_u||N_u||T_u)$ using its private key d to extract A_i correlating to the recovered Id_i and Cid_i and determines whether or not A_i already exists in its database from the registration phase and checks if $A_u = Cid_i \oplus h(A_i||Id_i)$. Suppose the extracted A_i exists in the server's database and A_u is verified. In that case, U_i is authenticated to S_j as only user U_i can compute valid Cid_i, which depends on A_i calculated using the user's password PW_i.

On the user side, U_i checks whether $V_2 = h(A_u||N_u||T_s)$. If V_2 is verified, S_j is then authenticated to U_i, as only server S_j can extract A_u and N_u from the transmitted message V_1 by decrypting V_1 using the server's private key d, known only to the server S_j.

Consequently, the proposed scheme enables the exchange of mutually-authenticated information between the server and the user. Hence, the suggested scheme can achieve mutual authentication.

User Anonymity: The proposed scheme can maintain the user's anonymity by concealing the user's identity, Id_i by concatenating it with the random number N_u and hiding it in $V_1 = (Id_i||Cid_i||A_u||N_u||T_u)^e$; therefore, the attacker is unable to access or obtain the user's identity Id_i as it requires the attacker to decrypt V_1 using the server's private key d. Additionally, the user's identity Id_i is not included in (V_2, V_3) in the transmitted message $M_2 = \{V_2, V_3, T_s\}$ from the server S_j.

User Untraceability: The proposed scheme can ensure the user's untraceability, as the user and server generate new random values (N_u, N_s) and fresh timestamps (T_u, T_s) in each session to compute $V_1 = (Id_i||Cid_i||A_u||N_u||T_u)^e$, $V_2 = h(A_u||N_u||T_s)$ and $V_3 = N_s \oplus N_u \oplus A_u$. As a result, in each session, the transmitted messages $M_1 = \{V_1, T_u\}$ and $M_2 = \{V_2, V_3, T_s\}$ provide new values which prohibit the attacker from relating the sent messages from the same user to each other or tracing its activities.

Forward Secrecy: Let's suppose that the attacker can acquire both the user's password PW_i-and the shared key between the user and the server $Sk_u = h(N_s||N_u||Cid_i) = SK_s$ and can intercept the transmitted message $M_1 = \{V_1, T_u\}$. Even in this situation, without knowledge of the random numbers (N_u, N_s), the attacker cannot disclose the previously transmitted messages. Furthermore, due to the RSA factorization issue, calculating the private key d of the server is difficult.

Secure Session Key: In this plan, the shared session key $Sk_u = h(N_s||N_u||Cid_i) = SK_s$ is computed based on random numbers N_u and N_s generated by the user and the server. Hence, the attacker can obtain the session key if he can retrieve the values of N_u and N_s; this needs disclosing the server's private key d, which is very hard due to the computational difficulty of factoring large integers. As a result, the session key in the proposed scheme is highly secure.

User Impersonation Attack: The attacker must create a legitimate value V_1 to successfully impersonate a legitimate user. For example, in order to succeed in generating $V_1 = (Id_i||Cid_i||A_u||N_u||T_u)^e$, it

requires the attacker to successfully compute $A_i = h(PW_i||b)$ and $Cid_i = A_u \oplus h(A_i||Id_i)$. This is because Cid_i depends on A_i, calculated using the password PW_i which is known only to the user U_i. Therefore, the proposed scheme is devised to mitigate user impersonation attacks.

Impersonation Attack: For the attacker to impersonate the server successfully, specific actions must be taken; it requires the attacker to generate valid values of V_2 and V_3. For instance, achieving $V_2 = h(A_u||N_u||T_s)$ and $V_3 = N_s \oplus N_u \oplus A_u$ necessitates the attacker obtaining A_u and N_u by decrypting V_1 using the server's private key d, which is exclusively known to the server S_j. However, it is known that getting the private key d of the server is a challenging process due to the factorization problem in RSA. Therefore, the suggested scheme can effectively prevent server impersonation attacks.

Replay Attack: The timestamps of the user and server (T_u, T_s) are inserted in each transmitted message. Additionally, with each login message $M_1 = \{V_1, T_u\}$, the user U_i selects a fresh random number N_u to provide $V_1 = (Id_i||Cid_i||A_u||N_u||T_u)^e$ and the server selects a fresh random number N_s to calculate $V_3 = N_s \oplus N_u \oplus A_u$. Moreover, these random numbers are used to compute the session key $Sk_u = h(N_s||N_u||Cid_i) = SK_s$. Hence, the proposed scheme can resist replay attacks.

Insider Attack: A malicious insider cannot obtain a server's password, since U_i sends $h(PW_i \,||\, b)$ instead of PW_i to server S_j through a secure channel. Hence, a malicious insider cannot acquire the PW_i of user U_i due to the one-way property of the hash function.

Stolen Smart-card Attack: As the smart card typically does not store A_i, the attacker can't elicit Id_i from Cid_i or PW_i from A_i. Nevertheless, the message V_1 is randomized using the random number N_u and protected by encrypting V_1 utilizing the server's public key e. Additionally, the identity is protected by hashing the identity Id_i concatenated with the private key d of the server, as $(Cid_i = h(Id_i||d))$.

Offline Password Guessing: To guess PW_i, we need to know A_i, which is not saved on the smart card and if the attacker is aware of the values that the user has saved on his smart card $\{A_u, B_u, e, n, h(.), h(Id_i \oplus PW_i) \oplus b\}$, the password can't be guessed, as the hash and xor functions protect the password. Additionally, the attacker can't obtain the password from the transmitted messages over the public channel, as (V_1, V_2, V_3) no longer include A_i. Therefore, the password is protected.

7.2 Simulation for Conducting Formal Security Verification Using AVISPA Tool

In this sub-section, the security properties of the proposed system will be verified using the AVISPA [41] simulation tool. The simulation is carried out using a language for high-level protocol specifications (HLPSL). The user's role is defined in HLPSL (High Level Protocol Specification Language) specification, as depicted in Figure 3. The user and server communicate by transmitting and receiving messages through channels using the Snd() and Rcv() operations. A channel(dy) type declaration indicates that the channel is designed for the DolevYao threat model. Lastly, Ui authenticates the server S, as per the declaration request (Ui, S, user_server_nu, Nu). Additionally, the server's role is specified in the HLPSL specification, as illustrated in Figure 4. The role specifications for session, goal and environment in HLPSL are depicted in Figure 5.

The simulation results are presented using the back-ends Constraint-logic-based Attack Searcher (CL-AtSe) and On-the-Fly Model-Checker (OFMC) [42]. Figures 6 and 7 validate that under both back-ends, CL-AtSe (Constraint-logic-based Attack Searcher) and OFMC (On-the-fly Model-Checker), the suggested scheme is deemed SAFE. This suggests that the proposed scheme is capable of resisting both passive and active attacks, including replay and MITM attacks.

8. PERFORMANCE EVALUATION

In this section, the security and performance of the proposed scheme are compared to those of other relevant schemes, including those proposed by Chaturvedi et al. [10], Qiu et al. [16], Radhakrishnan et al. [22], Renuka et al. [36] and Dharminder et al. [4]. Table 3 illustrates the estimated computation time [43] for each cryptographic function, facilitating performance comparison.

The process of logging in and authenticating is a critical phase of any authentication scheme. Therefore, we will focus on this phase. The proposed scheme relies on several hash functions, H, modular exponentiation for encryption/decryption using RSA, elliptic-curve point multiplication and a simple

```
role user(Ui:agent,S:agent,H,Mul:hash_func,SKas:symmetric_key,
SND,RCV:channel(dy))
played_by Ui
def=
local State:nat,
IDi,Ai,PWi,Cidi,Au,Bu,E,N,B,Nu,Ns,P,SKu,SKs,Q,D: text,
V1,V2,V3,Tu,Ts: message,
Inc: hash_func
const user_server, server_user,subs_1,subs_2,subs_3 : protocol_id
init State := 0
transition
1. State=0 /\ RCV(start)=|>
State':= 1 /\ B':=new() /\ Ai':=H(PWi.B) /\ SND({IDi.Ai}_SKas)
2. State=1 /\ RCV({Au'.Bu'.E'.N'.xor((H(xor(IDi,PWi))),B)}_SKas)
=|>
State':=2 /\ Nu':= new() /\ Tu':= new()/\ Ai':=H(PWi.B)
/\ Cidi':=xor(Au',H(Ai'.IDi))
/\ secret(PWi,subs_1,Ui)
/\ V1':=exp((IDi.Cidi'.Au'.Nu.Tu'),E)
/\ SND(V1'.Tu')
/\ witness(Ui,S,user_server_nu,Nu)
3. State= 2 /\ RCV(V2.V3.Ts)=|>
State':= 3 /\ Ns':=xor(V3,Nu,Au) /\ request(Ui,S,user_server_nu,Nu)
/\ SKu':=H(Ns.Nu.Cidi)
end role
```

Figure 3. Role of user Ui in HLPSL.

```
role server(Ui:agent,S:agent,H,Mul:hash_func,SKas:symmetric_key,
SND,RCV:channel(dy))
played_by S
def=
local State:nat,
IDi,Ai,PWi,Cidi,Au,Bu,E,N,B,Nu,Ns,P,SKu,SKs,Q,D: text,
V1,V2,V3,Tu,Ts: message,
Inc: hash_func
const user_server, server_user,subs_1,subs_2,subs_3 : protocol_id
init State := 0
transition
1. State=0 /\ RCV({IDi'.Ai'}_SKas) =|> State':=1 /\ P':=new() /\
Q':=new() /\ E':=new() /\ N':=Mul(P,Q) /\ Cidi':= h(IDi'.D) /\
Ts':=new()
/\ Au':=xor(Cidi,H(Ai)) /\ Bu':=H(cidi.Ai.IDi')
/\ secret(D,subs_2,S) /\ secret({Ai,Cidi,E,IDi,Ns},subs_3,{Ui,S})
/\ SND({Au'.Bu'.E'.N'}_SKas)
2. State=1 /\ RCV(V1,Tu) =|> State':=2 /\ IDi' :=exp(V1,D) /\
Au':=exp(V1,D) /\ Cidi':=exp(V1,D) /\ Nu':=exp(V1,D)
/\ witness(S,Ui,server_user_ns,Ns) /\ V2':=H(Au'.Nu'.Ts) /\
V3':=xor(Ns,Nu',Au') /\ SKs':=H(Ns.Nu'.Cidi')
end role
```

Figure 4. Role of server S in HLPSL.

```
role session(Ui:agent,S:agent,H,Mul:hash_func,SKas:symmetric_key)
def=
local SI,SJ,RI,RJ: channel(dy)
composition
user(Ui,S,H,Mul,SKas,SI,RI) /\ server(Ui,S,H,Mul,SKas,SJ,RJ)
end role
role environment()
def=
const ui:agent,s:agent,h,mul:hash_func,skas:symmetric_key,
v1,v2,v3,idi,ai,cidi,au,bu,e,n,p,q,sku,sks,b: text,
user_server_nu, server_user_ns, subs_1,subs_2,subs_3 : protocol_id
intruder_knowledge ={ui,s,h,mul,v1,v2,v3,idi,ai,cidi,au,bu,e,n}
composition
session(ui,s,h,mul,skas) /\ session(ui,s,h,mul,skas)
end role
goal
secrecy_of subs_1
secrecy_of subs_2
secrecy_of subs_3
authentication_on user_server_nu
authentication_on server_user_ns
end role
```

Figure 5. The proposed HLPSL scheme's role specifications for the session, goal and environment.

```
%OFMC
%Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/ home/span/span/testsuite/results/Tmis.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.03s
visitedNodes: 13 nodes
depth: 4 plies
```

Figure 6. The proposed scheme simulation results based on the OFMC back-end.

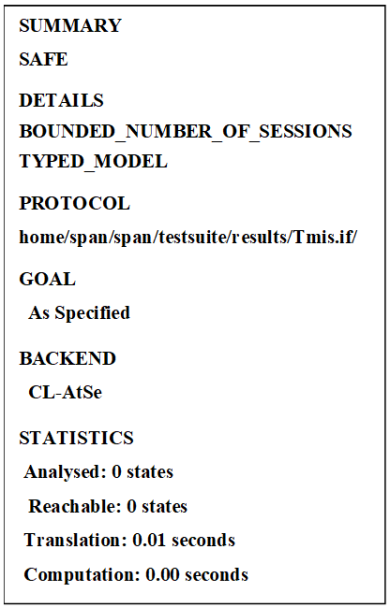


Figure 7. The proposed scheme's outputs based on the CL-AtSe back-end.

XOR function. However, compared to other cryptographic operations, the cost of concatenation (||) and XOR (⊕) operations is negligible.

The scheme is convenient for low-power devices, as the cryptographic techniques are straightforward. In addition, the proposed scheme employs SHA-1 as a hash function for computation-cost evaluation. The SHA-1 algorithm receives messages of varying sizes divided into blocks; each block has an input of 512 bits and provides an output of 160 bits.

Table 3. Notations and approximate computation times.

Notation	Description	Approximate computation time (in seconds)
t_h	Time of hash function	0.00032
t_{me}	Time of modular exponentiation	0.0192
t_{ecm}	Time of elliptic-curve point multiplication	0.0172

8.1 Computation Cost

The computational expense of implementing the proposed scheme is detailed in Table 4.

Table 4. The proposed scheme's computation cost.

Computation Cost	User	Server	Total
Registration phase	$1t_h$	$3t_h$	$4t_h$
(ms)	0.32	0.96	1.28
Login and Authentication phase	$5t_h + 1t_{me}$	$3t_h + 1t_{me}$	$8t_h + 2t_{me}$
(ms)	20.8	20.16	40.96
Total computation cost	$6t_h + 1t_{me}$	$6t_h + 1t_{me}$	$12t_h + 2t_{me}$
(ms)	21.12	21.12	42.24

For user U_i : In the registration phase, user U_i executes one hash function, which takes 0.32 ms. Throughout the login and authentication phase, the user and server perform 5 hash functions and one modular exponentiation which require 20.8 ms. Thus, the user consumes a total of 21.12 ms.

For server S_j : In the registration phase, the server S_j executes 3 hash functions which need 0.96 ms. While in login and authentication, the server performs 3 hash functions and 1 modular exponentiation

which require 20.16 ms. Hence, the server consumes a total of 21.12 ms.

As depicted in Table 4, the total time needed to complete the registration phase is 1.28 ms, while the real-time needed to complete the login and authentication phase is 40.96 ms.

8.2 Security and Performance Assessment

In this sub-section, we compare the security and performance of our proposed scheme with those of recent existing schemes. Performance is evaluated based on communication and computational costs.

8.2.1 Security Comparison

For security comparison, we put forward a list of 10 independent criteria of security evaluation as follows:

- SEC1. Mutual authentication: The server must verify the user's identity before offering any service and the user should verify the server's identity to trust and accept the offered services.
- SEC2: User anonymity: The user must act or communicate in the system without stating his name or identity.
- SEC3: User untraceability: The attacker couldn't be able to relate any two messages to the same user; hence, the user's activities in the system can't be traced.
- SEC4: Forward secrecy: Even if one or more of the generated session keys are compromised, the data from other sessions is protected.
- SEC5: Session-key agreement: The user and server can agree on a shared session-key to ensure secure data transmission.
- SEC6: Resistance to impersonation attack: The scheme prevents the attacker from joining and/or accessing the system as a legitimate user or server.
- SEC7: Resistance to replay attack: The scheme prevents the attacker from retransmitting previously transmitted messages as a legitimate user or server.
- SEC8: Resistance to insider attack: The attack can be executed by an authorized user to access the system. However, when changing or obtaining the user's information from the server, the scheme prevents the attacker from compromising both the user's privacy and the integrity of the system.
- SEC9: Resistance to stolen smart-card attack: If the attacker captures the user's stolen smart card, the scheme prevents it from recovering the password or impersonating the user.
- SEC10: Resistance to offline password-guessing attack: The scheme prevents the attacker from guessing the password.

Table 5 presents a comparison between the proposed scheme and other related schemes, focusing on key aspects of online privacy and security, such as authentication, anonymity, untraceability and forward secrecy in healthcare systems. In Table 5, the symbols "√" and "X" indicate whether the scheme meets the relevant security features or not.

Table 5. Security comparison.

Scheme	Chaturvedi et al. [10]	Qiu et al. [16]	Radhakrihnan et al. [22]	Renuka et al. [36]	Dharminder et al. [4]	The Proposed Scheme
SEC1	√	√	√	√	×	√
SEC2	√	√	√	√	√	√
SEC3	√	√	√	√	×	√
SEC4	√	√	√	√	√	√
SEC5	√	√	√	√	√	√
SEC6	√	√	√	√	×	√
SEC7	×	√	×	√	√	√
SEC8	×	×	×	×	√	√
SEC9	√	√	√	×	√	√
SEC10	√	√	√	×	√	√

8.2.2 Computation-cost Comparison

Table 6 displays the computational cost of the proposed scheme in comparison with those of the relevant authentication schemes. The results indicate that the login and authentication phase of the proposed scheme requires $8t_h + 2t_{me}$, amounting to 40.96 ms. Consequently, it is suggested that the computational expense of the proposed scheme is lower than Chaturvedi et al.'s scheme [10] and Renuka et al.'s scheme [36], while it shares the same computation cost as Dharminder et al.'s scheme [4].

The proposed scheme exhibits a slightly higher computation cost compared to Qiu et al.'s scheme [16]. However, this slight increase is justified, as the proposed scheme is capable of resisting insider attacks, a vulnerability present in Qiu et al.'s scheme [16]. In contrast to Radhakrishnan et al.'s scheme [22], the proposed scheme incurs a higher cost, which is reasonable, given that the proposed scheme can defend against several types of attacks, including replay attacks, MITM assaults, stolen-verifier attacks and insider attacks.

Table 6. Computation-cost comparison.

Schemes	User computation cost	Server computation cost	Total cost
Chaturvedi et al. [10]	$7t_h + 1t_{me}$	$4t_h + 1t_{me}$	$11t_h + 2t_{me}$
(ms)	21.44	20.48	41.92
Qiu et al. [16]	$6t_h + 1t_{ecm}$	$5t_h + 1t_{ecm}$	$11t_h + 2t_{ecm}$
(ms)	19.12	18.8	37.92
Radhakrihnan et al. [22]	$9t_h$	$7t_h + 1t_{me}$	$16t_h + 1t_{me}$
(ms)	2.88	21.44	24.32
Renuka et al. [36]	$7t_h + 3t_{ecm}$	$5t_h + 3t_{ecm}$	$12t_h + 6t_{ecm}$
(ms)	53.84	53.2	107.04
Dharminder et al. [4]	$6t_h + 1t_{me}$	$2t_h + 1t_{me}$	$8t_h + 2t_{me}$
(ms)	21.12	19.84	40.96
The Proposed Scheme	$5t_h + 1t_{me}$	$3\ t_h + 1t_{me}$	$8\ t_h + 2t_{me}$
(ms)	20.8	20.16	40.96

8.2.3 Communication-cost Comparison

Let's consider the bit sizes as follows: 160 bits for a random number and the user's identity, 32 bits for the timestamp, 320 bits for the elliptic-curve point and 160 bits for the hash output (if SHA_1 is applied as h(·)). İn the proposed scheme, the message $M_1 = \{V_1, T_u\}$ needs 1024+32 = 1056 bits and the message $M_2 = \{V_2, V_3, T_s\}$ needs 160 + 160 + 32 = 352 bits. Thus, the proposed scheme requires a communication cost of 1056 + 352 = 1408 bits for the two messages sent between the user U_i and the sender S_j .

Table 7 demonstrates that the proposed scheme's and other related systems' communication costs are comparable. For example, the schemes in [10], [16], [22], [36] and [4] require 1248, 1280, 1888, 1184 and 1568 bits, respectively, whereas the proposed scheme takes 1408 bits. Furthermore, compared to Chaturvedi et al.'s scheme [10], Qiu et al.'s scheme [16] and Renuka et al.'s scheme [36], the communication cost of the proposed scheme is a little increased; the suggested scheme can meet all security standards, whereas the other schemes can't, hence this is justifiable.

Table 7. Communication-cost comparison.

Scheme	Communication Cost	
	No. of Messages	Cost (in bits)
Chaturved et al. [10]	2	1248
Qiu et al. [16]	3	1280
Radhakrihnan et al. [22]	2	1888
Renuka et al. [36]	2	1184
Dharminder et al. [4]	2	1568
The Proposed Scheme	2	1408

Based on the mentioned results and analysis, the proposed scheme provides enhanced security services and resilience against attacks compared to related schemes in [10][16][22][36][4]. Additionally, the proposed scheme demonstrates a comparable computational cost to other related schemes which lack the security services achieved by our proposed scheme. These advantages position the proposed scheme as a more suitable choice for healthcare systems.

From the results mentioned above and the analysis, the proposed scheme achieved more security services and resisted more attacks than the related schemes in [10][16][22][36][4]. Moreover, the proposed scheme has a comparable computation cost to other related schemes which failed to achieve the security services offered by our proposed scheme. These advantages enhance the suitability of the proposed scheme for healthcare systems.

9. CONCLUSIONS

In this paper, we conducted a thorough review and analysis of Dharminder et al.'s scheme, revealing its inability to ensure authentication, user untraceability and vulnerability to both user-impersonation attacks and server impersonation attacks. We developed an improved RSA-based authentication scheme to address these critical security flaws and provide authorized access to healthcare services. The proposed scheme offers mutual authentication, user anonymity, untraceability and forward secrecy. Additionally, it is resilient against a range of attacks, including stolen smart-card attacks, user and server impersonation attacks, password-guessing attacks, insider attacks and offline password-guessing attacks. The security analysis of the proposed scheme, supported by simulations using the AVISPA tool, confirms the proposed scheme's superior security over existing schemes. Additionally, through performance evaluation, we illustrated that the proposed scheme requires 61.7% and 2.3% lower computation costs than Renuka et al.'s scheme and Chaturvedi et al.'s scheme, respectively. This research not only addressed vital security gaps in the authentication schemes of healthcare systems, but also introduced an improved and secure scheme that is both computationally and communicationally more efficient. The proposed improvement is pivotal for the secure and effective implementation of healthcare systems, ensuring the protection of sensitive patient information and facilitating the reliable delivery of medical services.

REFERENCES

[1] J. Srinivas, D. Mishra and S. Mukhopadhyay, "A Mutual Authentication Framework for Wireless Medical Sensor Networks," J. of Medical Systems, vol. 41, pp. 1-10, 2017.

[2] D. Mishra et al., "Cryptanalysis and Improvement of Yan et al.'s Biometric-based Authentication Scheme for Telecare Medicine Information Systems," J. of Medical Systems, vol. 38, pp. 1-12, 2014.

[3] A. Kumar et al.,"A Novel Privacy-preserving Blockchain-based Secure Storage Framework for Electronic Health Records," Journal of Information and Optimization Sciences, vol. 43, pp. 549-570, 2022.

[4] D. Dharminder, D. Mishra and X. Li, "Construction of RSA-based Authentication Scheme in Authorized Access to Healthcare Services," J. of Medical Systems, vol. 44, pp. 1-9, 2020.

[5] R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM, vol. 21, pp. 120-126, 1987.

[6] C.T. Li et al., "A Secure Dynamic Identity and Chaotic Maps-based User Authentication and Key Agreement Scheme for E-Health Care Systems," J. of Medical Systems, vol. 40, pp. 1-10, 2016.

[7] R. Madhusudhan and C. S. Nayak, "A Robust Authentication Scheme for Telecare Medical Information Systems," Multimedia Tools and Applications, vol. 78, pp. 15255-15273, 2019.

[8] M. Tanveer et al., "CADF-CSE: Chaotic Map-based Authenticated Data Access/Sharing Framework for IoT-enabled Cloud Storage Environment," Physical Communication, vol. 59, p. 102087, 2023.

[9] M. Tanveer et al., "CMAP-IoT: Chaotic Map-based Authentication Protocol for Crowdsourcing Internet of Things," Arabian J. for Science and Engineering, vol. 49, pp. 3453–3466, 2024.

[10] A. Chaturvedi, D. Mishra and S. Mukhopadhyay, "An Enhanced Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems," Computer and Information Sciences, vol. 29, pp. 54-62, 2017.

[11] Q. Jiang, J. Ma, Z. Ma and G. Li, "A Privacy-enhanced Authentication Scheme for Telecare Medical Information System," Journal of Medical Systems, vol. 37, pp. 1-8, 2013.

[12] D. Mishra, "On the Security Flaws in ID-based Password Authentication Schemes for Telecare Medical Information Systems," J. of Medical Systems, vol. 39, pp. 1-16, 2015.

[13] X. Xu, P. Zhu and Q. Wen, "A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems," J. of Medical Systems, vol. 38, pp. 1-17, 2014.

[14] Z. Zhu, "An Efficient Authentication Scheme for Telecare Medicine Information Systems," J. of Medical

Systems, vol. 36, pp. 3833-3838, 2012.
[15] S. A. Chaudhry, K. Mahmoud, H. Naqvi and M. K. Khan, "An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography," J. of Medical Systems, vol. 39, pp. 1-11, 2015.
[16] S. Qiu, G. XU, H. Ahmad and L. Wang, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," IEEE Access, vol. 6, pp. 7452-7463, 2017.
[17] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah and V. Gupta, "Anonymous Mutual Authentication and Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks," Computer Networks, vol. 129, pp. 429-443, 2017.
[18] A. M. Koya and P. P. Deepthi, "Anonymous Hybrid Mutual Authentication and Key Agreement Scheme for Wireless Body Area Network," Computer Networks, vol. 140, pp. 138-151, 2018.
[19] M. Komparaa, SK.H. Islam and M. Hölbl, "A Robust and Efficient Mutual Authentication and Key Agreement Scheme with Untraceability for WBANs," Computer Networks, vol. 148, pp. 196-213, 2019.
[20] Z. U. Rehman, S. Altaf and S. Iqbal, "An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN," IEEE Access, vol. 8, pp. 175385-175397, 2020.
[21] T. F. Lee et al., "Secure and Efficient Password-based User Authentication Scheme Using Smart Cards for the Integrated EPR Information System," J. of Medical Systems, vol. 37, pp. 1-7, 2013.
[22] N. Radhakrishnan and M. Karuppiah, "An Efficient and Secure Remote User Mutual Authentication Scheme Using Smart Cards for Telecare Medical Information Systems," Informatics in Medicine Unlocked, vol. 16, p. 100092, 2019.
[23] D. Mishra et al., "Security Enhancement of a Biometric-based Authentication Scheme for Telecare Medicine Information Systems with Nonce," J. of Medical Systems, vol. 38, pp. 1-11, 2012.
[24] 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 J. of Biomedical and Health Informatics, vol. 21, pp. 465-475, 2016.
[25] K. Kim, J. Ryu, Y. Lee and D. Won, "An Improved Lightweight User Authentication for the Internet of Medical Things," Sensors, vol. 23, no. 3, p. 1122, 2023.
[26] M. Soni and D. K. Singh, "Privacy-preserving Secure and Low-cost Medical Data Communication Scheme for Smart Healthcare," Computer Communications, vol. 194, pp. 292-300, 2022.
[27] S. Singh and V. K. Chaurasiya, "Mutual Authentication Framework Using Fog Computing in Healthcare," Multimedia Tools and Applications, vol. 81, pp. 31977-32003, 2022.
[28] F. Salem and R. Amin, "A Privacy-preserving RFID Authentication Protocol Based on El-Gamal Cryptosystem for Secure TMIS," Information Sciences, vol. 527, pp. 382-393, 2020.
[29] M. A. Khan, S. Ullah, T. Ahmad, K. Jawad and A. Buriro, "Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol," Sensors (Basel), vol. 23, no. 12, p. 5518, 2023.
[30] R. Amin et al., "A Robust and Anonymous Patient Monitoring System Using Wireless Medical Sensor Networks," Future Generation Computer Systems, vol. 80, pp. 483-495, 2018.
[31] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li and F. Wu, "An Enhanced Three-factor Based Authentication Protocol Using Wireless Medical Sensor Networks for Healthcare Monitoring," J. of Ambient Intelligence and Humanized Computing, vol. 15, pp. 1165-1186, 2018.
[32] G. Sharma and S. Kalra, "A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services," Iranian J. of Science and Technology Trans. of Electrical Eng., vol. 43, pp. 619–636, 2019.
[33] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," Proc. of Advances in Cryptology, Part of the Book Series: Lecture Notes in Computer Science, vol. 2332, pp. 337-351, Springer Berlin Heidelberg, 2002.
[34] M. Masud et al., "Lightweight and Anonymity-preserving User Authentication Scheme for IoT-based Healthcare," IEEE Internet of Things J., vol. 9, pp. 2649 - 2656, 2021.
[35] D. He and N. Kumar, "Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices," IEEE Trans. on Consumer Electronics, vol. 60, no. 1, pp. 30-37, 2014.
[36] K. M. Renuka, S. Kumari and X. Li, "Design of A Secure Three-factor Authentication Scheme for Smart Healthcare," J. of Medical Systems, vol. 43, pp. 1-12, 2019.
[37] P. Sonia, A. K. Pal and S.H. Islam, "An Improved Three-factor Authentication Scheme for Patient Monitoring Using WSN in the Remote Healthcare System," Computer Methods and Programs in Biomedicine, vol. 182, p. 105054, 2019.
[38] G. Xu et al., "Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks," IEEE Access, vol. 8, pp. 47282-47294, 2020.
[39] D. Wang et al., "Anonymous Two-factor Authentication in Distributed Systems: Certain Goals are Beyond Attainment," IEEE Trans. on Dependable and Secure Computing, vol. 12, no. 4, pp. 228-442, 2015.
[40] Q. Wang and D. Wang, "Understanding Failures in Security Proofs of Multi-factor Authentication for Mobile Devices," IEEE Trans. on Information Forensics and Security, vol. 18, pp. 597-612, 2022.
[41] A. Armando et al., " AVISPA: Automated Validation of Internet Security Protocols and Applications," pp. 281-285, [Online], Available: http://www.avispa-project.org/, Accessed in January 2024.

[42] D. Basin, S. Mödersheim and L. Vigano, "OFMC: A symbolic Model Checker for Security Protocols," Int. J. of Information Security, vol. 4, pp. 181–208, 2005.

[43] J. Srinivas et al., "Anonymous Lightweight Chaotic Map-based Authenticated Key Agreement Protocol for Industrial Internet of Things," IEEE Trans. on Dependable and Secure Computing, vol. 17, no. 6, pp. 1133-1146, 2018.

ملخص البحث:

نتيجةً للتّقدُّم الهائل في الاتّصالات اللّاسلكية، فإنّ منصّات الرّعاية الصّحية عن بُعد جعلت من الممكن للمرضى تلقّي الرّعاية الصّحية اللّازمة عن بُعد دون الحاجة إلى الحضور إلى مراكز الرّعاية الصّحية. ومع ذلك، يبقى إيجاد خطّة تحقُّق آمنة وفعّالة لأنظمة الرّعاية الصّحية من أبرز التّحدّيات. وقد اقتُرحت حلول عديدة لهذه المشكلة، لكنها ظلّت في معظمها قاصرةً عن تأمين الأمان المطلق والحماية من الهجمات السّيبرانية.

في هذه الورقة، بدأنا أوّلاً بدراسة وتحليل أحد الحلول المقترحة في المرجع [4] لبيان إخفاقه في توفير التّحقُّق المتبادل وضمان سرّية معلومات المريض وعدم تتبُّعهِ، إلى جانب هشاشة ذلك الحلّ المقترح للهجمات. بعد ذلك، نقترح خطّةً محسّنة وفعّالة لمعالجة أوجُه القصور في الخطّة المقترحة في المرجع [4].

ويمكن للخطّة المقترحة في هذه الدّراسة أن تؤمّن التّحقُّق المتبادل، وأن تحافظ على خصوصية المريض وعلى سرّية معلوماته، إلى جانب ضمان عدم تتبُّعه من قبل المهاجمين والمتطفّلين الإلكترونيين، مع توفير الحصانة اللّازمة لنظام الرّعاية الصّحية من الهجمات والاختراقات على اختلاف أنواعها. من ناحيةٍ أخرى، تتميّز الخطّة المقترحة في هذه الدّراسة بالفعالية مقارنة بمثيلاتها القائمة من حيث تكلفة الحسابات وتكلفة الاتّصالات.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).