Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Analysis of User Authentication and Key Agreement Protocol for the Telecare Medicine Information System

Rupesh Kumar Verma[1], A. J. Khan[1] and Manoj Kumar Chande[2*]

[1]School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, C. G., India rupkv1993@gmail.com, khanaj@matsuniversity.ac.in

[2]Department of Applied Mathematics, Shri Shankaracharya Institute of Professional Management and Technology, Raipur, C. G., India

*Corresponding author. E-mail: manojkumarchande@gmail.com

ARTICLE INFO

Received: 08 Oct 2024

Revised: 21 Nov 2024

Accepted: 15 Dec 2024

ABSTRACT

The Telecare Medicine Information System (TMIS) is a steadily expanding medical service, offering remote access to health-care facilities and treatments to the patient via the internet. In recent times, Amintoosi and Nikooghadam have introduced a formally secure authentication and key management system for TMIS, relying on the utilization of the Elliptic Curve (EC) Cryptosystem. They assessed the protocol by Khatoon et al. and demonstrated its susceptibility to temporary information attacks specific to known sessions, highlighting its inability to offer flawless forward secrecy. As a remedy, they put forward an enhanced protocol based on elliptic curve cryptography (ECC). However, we found that the Amintoosi and Nikooghadam protocols are vulnerable to off-dictionary and replay attacks. In all authentication mechanisms, it is crucial to include regular password changes and a revocation process to uphold end-user security. Nonetheless, their protocol conspicuously lacks essential components, including phases for password changes, revocation, and re-registration. Consequently, we present an improved protocol that effectively mitigates all the vulnerabilities outlined in the protocols of Khatoon et al. and Amintoosi and Nikooghadam, while also incorporating essential features such as password updates, revocation procedures, and re-registration phases. The suggested protocol is subjected to formal analysis using the random oracle model, and compared to state-of -the-art protocols to demonstrate its suitability for TMIS

Keywords: Key Agreement Protocol, User Authentication, Elliptic Curve Cryptosystem (ECC), Random Oracle Model (ROM).

INTRODUCTION

The physician, patient, laboratory, as well as medical server use TMIS as a secure communication platform. They're connected and willing to provide information about their patients' treatments, drugs, and medical reports. The medical server must be accessed whenever a patient needs medical assistance. The medical server connects physicians for legitimate users in order to give health care assistance.

To get remote medical services, initially a patient signs up with the server. The TMIS maintains users records and serves as a communicating links among all the stake holders. TMIS is accessible through the internet, which exposes it to a range of security and privacy concerns due to unconstrained nature of internet. An adversary can access messages transmitted across a patient and a healthcare network in order to get confidential information about the patient.

As a consequence, patient confidentiality can be compromised, leading to the potential for irreversible harm.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Thus, it is imperative to implement a robust Mutual Authentication and Key Agreement (MAKA) mechanism to safeguard against unauthorized access to electronic health records stored in healthcare servers and to protect information transmitted between users.

Several Mutual Authentication and Key Agreement (MAKA) protocols have been introduced for telecare medicine information systems (TMIS). Notably, Amintoosi and Nikooghadam, in their recent work [1], introduced an ECC-based MAKA protocol specifically designed for TMIS. In their research, they conducted an analysis of Khatoon et al.'s protocol [2] and put forth an enhanced ECC-based alternative. However, we found that Amintoosi and Nikooghadam [1], protocol fails to resist off-dictionary attack and replay attack. Moreover, their protocol lacks critical elements, namely a password change phase, a revocation phase, and a re-registration phase, all of which are fundamental prerequisites for any authentication protocol.

As a consequence, we introduce an improved protocol that robustly defends against all the weaknesses identified in both Khatoon et al.'s [2]and Amintoosi and Nikooghadam's [1] protocols. We subject the proposed protocol to formal analysis using the ROM (Random Oracle Model) and compare it to state-of- the-art protocols, demonstrating its appropriateness for implementation in TMIS.

PRELIMINARIES

This section briefly discusses Elliptic Curve Cryptosystem (ECC) based two computationally hard problems and adversary capabilities.

Elliptic Curve Cryptosystem

Let's explore a situation in which both p and n are substantial prime numbers. Within this context, an elliptic curve, defined over a finite field denoted as F_p, consists of points that adhere to the equation:

$Ep(a, b)$: $y^2 = x^3 + ax + b \bmod p$, along with the point {0} considered an identity element. Given below are ECC based computational hard problems:

1) **The Elliptic Curve Discrete Logarithm Problem (ECDLP):** This problem states that it is computationally hard to find an integer x such that $P = xQ$, where P and Q are two distinct points on the given elliptic curve.

2) **The Elliptic Curve Diffie-Hellman Problem (ECDHP):** This problem states that it is computationally hard to find abQ, where aQ and bQ are two distinct points over the given elliptic curve.

A. ADVERSARY CAPABILITIES

The capabilities of the adversary A are as follows:

- A has comprehensive control over the channel of data transmission, allowing him to change, apprehend, remove, and send back any message [3]- [6].
- In polynomial time, A can enumerate all the values in $D_{pw} \times D_{id}$, here D_{pw} is password space and D_{id} is the identity space.
- A has access to all public parameters, including the user'sbiometrics. [7].
- A is unable to extract the private key of TMIS server.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AMINTOOSI AND NIKOOGHADAM PROTOCOL

The Amintoosi and Nikooghadam protocol is discussed briefly in this section. The full description of the protocol can be found in [1]. Here we only discuss registration and login and authentication phases of their protocol. Figure (1) illustrates the registration phase, whereas Figure (2), illustrates the login and authentication phase.

Patient U_i	**TMIS server S**
Chooses ID_i, PW_i	
Selects random number a_i	
$HID_i = h(ID_i \| a_i)$	
$A_i = h(ID_i \| PW_i \| a_i) \oplus ID_i$	
	$R_i = E_s(A_i \| HID_i)$
	$Q_i = A_i \oplus R_i$
	Stores $\{Q_i, E(\cdot)/\ D(\cdot)\}$and sends it securely to U_i.
$D_i = h(A_i \| HID_i)$	
Adds $\{D_i, a_i\}$ to SC, SC stores $\{Q_i, a_i, D_i, E(\cdot)/\ D(\cdot)\}$	

FIGURE 1. AMINTOOSI AND NIKOOGHADAM'S REGISTRATION PHASE

Patient U_i	**TMIS server S**
Insert SC and inputID_i^*, PW_i^*	
$HID_i^* = h(ID_i^* \| \| a_i)$,$A_i^* = h(ID_i^* \| \| PW_i^* \| \| a_i) \oplus ID_i^*$	
$D_i^* = h(A_i^* \| \| HID_i^*)$	
Verifies $D_i = D_i^*$	
Selects $c_i,\ d_i \in Z_p^*$ and T_i	
Computes $C_i = c_i P$, $Key_{1i} = C_i P = c_i aP$	
$E_i = E_{Key_{1i}} = (A_i, D_i, Q_i, T_1)$	
Sends $(C_i, E_i, d_i p, T_1)$	
	Selects T_2, Checks $\|T_2 - T_1\| < \Delta T$
	Computes $key'_{1i} = C_i P = c_i aP$
	Decrypts $D(key_{1i},)(E_i) = (A_i^*,\ D_i^*, Q_i^*, T_1^*)$
	Checks $T_1^* = T_1,\ R_i^* = A_i^* \oplus Q_i^*$
	Decrypts $D_s(R_i') = (A_i^*, HID_i^*)$
	$D_i^{**} = h(A_i^* \| \| HID_i^*)$
	Checks $D_i^* = D_i^{**}$, Selects $m_i \in Z_p^*$
	Computes $SK = h(m_i d_i p \| \| HID_i \| \| D_i)$ and $z_i = h(SK \| \| HID_i \| \| D_i)$
	Sends HID_i $(m_i p, z_i, T_2)$ to U_i
Checks $\|T_2 - T_1\| < \Delta T$	
Computes $SK = h(m_i d_i p \| \| HID_i \| \| D_i)$ and $z_i = h(SK \| \| HID_i \| \| D_i)$	
Checks $z_i^* = z_i$,	

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

FIGURE 2. AMINTOOSI AND NIKOOGHADAM'S LOGIN AND AUTHENTICATION PHASE

1. ANALYSIS OF AMINTOOSI AND NIKOOGHADAM PROTOCOL

This section emphasizes and illustrates the susceptibility of the Amintoosi and Nikooghadam protocol [1] to offline password guessing and replay attacks, underscoring its deficiency in terms of security in these specific areas.

A. Off-line Password Guessing Attack

In the event of a user's smart card being stolen or discovered by an adversary, the password can be deduced through the following means:

1. The adversary retrieves $\{Q_i, a_i, D_i, E(\cdot)/D(\cdot)\}$ from the smart card by using the differential power analysis proposed in [8] and [9].
2. The adversary selects a pair (ID_i^*, PW_i^*) from the Cartesian product $D_{ID} \times D_{PW}$, where D_{ID} and D_{PW} denote the identity space and the password space respectively.
3. The adversary inputs guessed (ID_i^*, PW_i^*) smart card computes $HID_i^* = h(ID_i^* || a_i)$, $A_i^* = h(ID_i^* || PW_i^* || a_i)$ and $D_i^* = h(A_i^* || HID_i^*)$. Then verifies $D_i^* = D_i$ if not, he/she repeats Steps 2 and 3 till succeeds.

An assailant can efficiently list all pairs (ID_i , PW_i) in the Cartesian product$D_{ID} \times D_{PW}$ within polynomial time as the user's identity and password exhibit have low entropy, as previously established [10]. Consequently, the described attack is feasible, rendering the Amintoosi and Nikooghadam [1] to off- line password guessing attacks.

B. Replay Attack

In this attack, the attacker captures a session's contents and then sends the same message to impersonate a session participant and get unfair privileges. In Amintoosi and Nikooghadam [1] protocol, we suppose that adversary intercept the message (m_ip, z_i, T_2) and send it to the legal user with current timestamp T^*. Then user will compute *SK*, z_i and will pass the verification equation $z_i = z^*$ as it is independent of timestamp. Hence, the user will authenticate the adversary as the legal server and will start secure communication with it.

C. Absence of Password Change Phase and Smart Card Revocation Phase

For security reasons, passwords should be changed on a regular basis. Also, any smart-card-based authentication protocol must include a revocation phase to ensure the end user's security. However, for a lost or stolen smart card the protocol [1] does have a revocation phase. In the formulation of any authentication protocol, the incorporation of a revocation phase is typically advisable. This phase enables the user to block a lost or stolen smart card to prevent any potential misuse and facilitates the request for a replacement smart card. As a result, the inclusion of a smart card revocation phase is considered advantageous in authentication protocols.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

PROPOSED PROTOCOL

The section provides an overview of the registration, login and authentication, password change, revocation, and re-registration phases of the modified protocol. The suggested protocol is capable of withstanding a wide range of known threats while also providing the necessary security features. The TMIS server initiates the protocol by selecting an elliptic curve denoted as E over a finite field F_p along with a large ordered base point B. Subsequently, the server generates a private key represented as a random number, denoted as s, drawn from the set of non-zero integers modulo q. This private key s is kept confidential. Additionally, the server publishes$(E, B, P, k, h_o(\cdot), h(\cdot))$, while retaining the secrecy of s. In this context, $h_o(\cdot)$ and $h(\cdot)$ denote cryptographically secure one-way hash functions. A comprehensive list of the various notations used in the proposed protocol can be found in Table I.

1. **Patient Registration Phase:** Figure (3) illustrate the registration phase involving interactions between the user and the TMIS server, with detailed steps described below:

Notation	Description
E	Elliptic curve defined within a finite field denoted as F_p..
P	Large prime.
B	Base point B of the elliptic curve E with a substantial order k.
ID_p	Identity of the patient.
T_p	Time stamp of ID_p.
S	The secret key of TMIS server denotes as S.
(h_o, h)	Cryptographic secure hash function.
T_s	Time stamps of S.
→	Represents insecure / open network.
⟹	Represents secure network.

TABLE I NOTATIONS EMPLOYED IN THE SUGGESTED PROTOCOL

(a) Patient ⟹Server: $\{ID_p, RPW_p\}$. The patient selects an identity ID_p, a password PW_p of their preference. The smart card generates a random number r_p and calculates $PWP_p = h_o(ID_p \| r_p \| PW_p)$. Subsequently, it securely transmits the registration message $\{ID_p, RPW_p\}$ to the medical server.

(b) Server⟹Patient: $\{DID_p, B_p, E, P, n, h(\cdot)\}$. Upon receipt of the message $\{ID_p, RPW_p\}$, the server checks for the existence of ID_p in its database. If it is found, the server request for new identity.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Otherwise, it computes $A_p = h(ID_p \| s)$ and $B_p = RPW_p \oplus A_p$ .Then, it randomly select r_s and computes $DID_p = E_s(ID_p \| r_s)$ and securely send message $\{E, P, n, h(\cdot), DID_p, B_p\}$ to the user. The server records $(ID_p \| r_s \| List)$ in its database. The list keeps track of how many times a

user has failed to register, and if that number surpasses a specified threshold value, the user'sregistration is suspended until the userre-registers.

c) Patient $\Longrightarrow$ smartcard:$\{DID_p, B_p, E, P, n, h(\cdot), Ver_p\}$: The mobile device computes $A_p = RPW_p \oplus B_p$, $Ver_p = h(ID_p \| h(ID_p) \| s)$ and stores $\{DID_p, B_p, E, P, n, h(\cdot), Ver_p\}$ in its memory.

2) Log in and Authentication Phase: Figure (4) illustrates the login, mutual authentication, and key agreement phase. After a successful registration, the patient can log in and authenticate using the following process:

(a) Patient → Server: $M_1 = \{DID_p, \alpha P, V_p, T_p\}$.The patient enters ID'_p and PW'_p. The device's memory fetches T_p and B_p. Then it computes $RPW'_p = h(ID'_p \| r_p \| PW'_p)$, $A'_p = RPW'_p \oplus B_p$ and $Ver'_p = h(ID_p \| h(ID_p \| s))$. Then verifies $Ver'_p = Ver_p$ if equality do-not holds, it ends the interaction else randomly generates $\alpha \in Z_q^*$ and calculates $V_p = h(DID_p \| \alpha P \| A_p \| T_p)$ and sends message $M_1 = \{DID_p, \alpha P, V_p, T_p\}$ to the server via an open network. The number of wrong password submissions must be limited by the system.

(b) Server → Patient: $M_2 = \{\beta P, V_s, F, T_s\}$. Upon receiving the message, the server checks the freshness of T_p. If it is determined to be sale not fresh, the server rejects the request. Conversely, if it is fresh, the server decrypts DID_p as $(ID_p \| r_s) = D_s(DID_p)$ and retrieves ID_p, r_s list from the database. The value of List is first checked to determine if it is below the threshold value. If it is higher the server aborts the session, else computes $A_p = h(ID_p \| s)$ checks whether the V_p obtained is equal to $h(DID_p \| \alpha P \| A_p \| T_p)$. If unequal, denies therequest and sets List = List + 1; else, randomly generates $\beta \in z_p^*$, $r_s^{new}$and computes $DID_p^{new} = E_s(ID_p \| r_s^{new})$ and session key as $SK = h(ID_p \| \alpha\beta P \| A_p)$,$V_s = h(DID_p^{new} \| SK \| T_s)$ and $F = DID_p^{new} \oplus h(SK)$. Then, the server sends $M_2 = \{\beta P, V_s, F, T_s\}$ to the patient via an open network.

(c) Upon receiving the message, the device checks the freshness of T_s, if fresh it computes $SK = h(ID_p \| \alpha\beta P \| A_p)$, $DID_p^{new} = F \oplus h(SK)$. Then checks whether the received $V_s = h(DID_p^{new} \| SK \| T_s)$. If unequal, it's aborted the interaction; else, accepts thesession key and replaces DID_p with DID_p^{new}.

3) Password Change Phase - The following are the steps for changing a user's password:

(a) The patients inputs ID'_p and PW'_p. The device retrieves $r_p$and B_p from its memory and then computes $RPW'_p = h(ID'_p \| r_p \| PW'_p)$, $A'_p = RPW'_p \oplus B_p$ and $Ver'_p = h(ID_p \| h(ID_p \| s))$. Then verifies $Ver'_p = Ver_p$.

(b) If it's a legitimate user, the smart card prompts for new password PW_p^{new} and computes $B_p^{new} = B_p \oplus PRW_p \oplus h(ID'_p \| r_p \| PW_p^{new})$ and replaces B_p with B_p^{new}.

4) Revocation Phase – If a user's card is compromised in the following way, the user's account can be revoked:

(a) T he user performs the authentication procedure by following the steps outlined in the section 2.

(b) Patient → Server: $M_1 = \{DID_p, \alpha P, V_p, T_p, revoke - request\}$.

(c) The server authenticates the user after receiving the revocation request. If the user is legal, the server raises the value of List above the threshold value and revokes the card. After that, unless the user re-registers, no one can use the card to log onto the network.

5) Re-Registration Phase – The following steps can be taken by a user to re-register:

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Patient U_i	TMIS Server S
Computes $PRW_p = h_o(ID_p \parallel r_p \parallel PW_p)$	
Transmit (ID_p, RPW_p) to S	
Checks ID_p	
If exists, the compute	
$A_p = h(ID_p \parallel s)$ $B_p = RPW_p \oplus A_p$	
Select $r_s$and compute $DID_p = E_s(ID_p \parallel r_s)$	
Send $\{DID_p, B_p, E, P, k, h(\cdot)\}$	
	Compute $A_p = RPW_p \oplus B_p$,
	$Ver_p = h(ID_p \parallel h(ID_p) \parallel s)$ and stores
	$\{DID_p, B_p, E, P, n, h(\cdot), Ver_p\}$

Figure 3 – Registration Phase

Patient U_i	TMIS Server S
Input ID'_p and PW'_p	
Computes $RPW'_p = h(ID'_p \,\|\| r_p \| \| PW'_p)$	
$A'_p = RPW'_p \oplus B_p$	
$Ver'_p = h(ID_p \| \| h(ID_p \parallel s))$	
Checks $Ver'_p = Ver_p$	
If invalid, abort else selects $\alpha \in Z_q^*$ and fresh	
T_p	

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

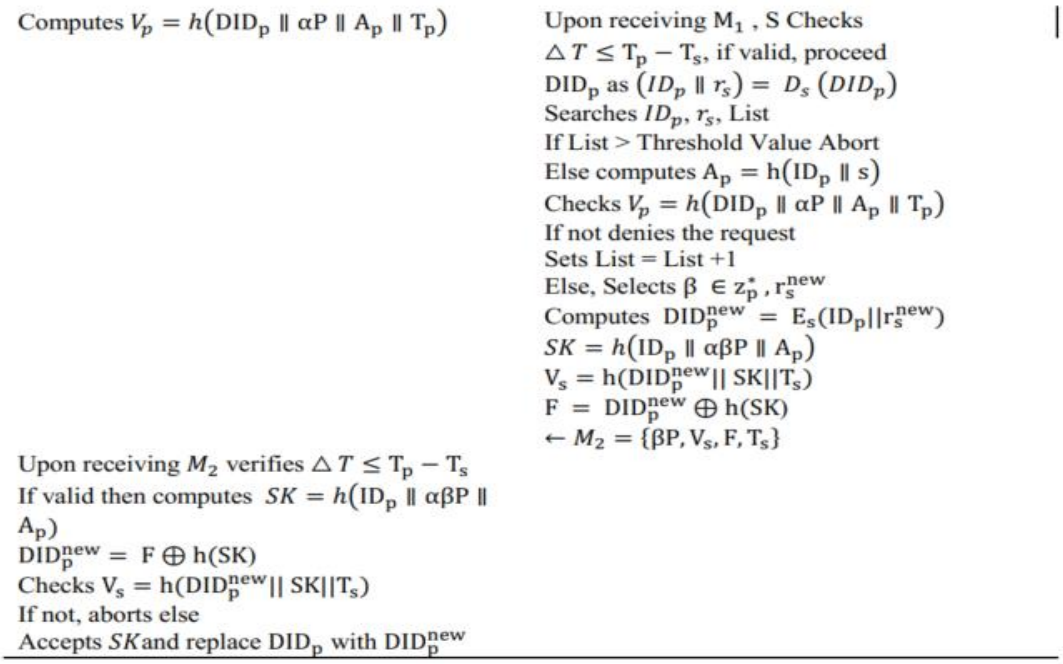

Figure 4 Login, Authentication and Key Agreement Phase

SECURITY ANALYSIS

This section provides both a formal and an informal security analysis of the enhanced protocol. For the formal security analysis, the Real-or-Random (ROR) model, as defined by Abdalls et al. [11], is employed. The subsequent subsections detail the ROR model.

A. Security Analysis Using Random Oracle Model

The protocol involves two participants, a patient P and the server S.

- Instance: $\prod_S^t$ represents the instance t of the server S and $\prod_P^u$ represents any instant u of the user U_i . They are termed oracles.
- Session Identifier (SID): Any oracle's SID is the ordered concatenation of all the messages it has communicated i.e. all the sent and received messages.
- Open Oracle: If the accepted session key is exposed by an oracle $\prod^t$ in any state, it is said to be open.
- Partner Oracle: Two oracles are partners if they are in same state and have same SID.
- Fresh Oracle: If an oracle and its partner oracle have not been opened or corrupted, they are considered fresh.
- Adversary: The adversary has access to all communications and could perform the following queries:

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Execute $(\prod^t, \prod^u,)$: This query initiates an eavesdropping attack with the aim of intercepting any communication between two authorized users.
- Send $(\prod^t, m)$: This query executes an active attack by sending a message m to a participant instance $\prod^t$ and recording its response.
- Corrupt SC($\prod^t$): This query reveals the information stored in the smart card.
- Test($\prod^t$): This query assesses the semantic security of the session key SK based on the indistinguishability principle within the framework of the ROR model, as outlined in [11]. In this experiment, the adversary sends a test query to a new oracle at any given moment. To commence the experiment, a fair and impartial coin c is flipped. If the result is 1, it signifies the generation of a session key at random; conversely, if the outcome is any other value, it corresponds to the agreed-upon session key of the test oracle.

The semantic security is defined in the following way:

> Definition 6.1: Adversary, referred to as A, as well as the challenger, to differentiate between the genuine session key of the instance and a session key generated at random. The adversary is permitted to perform a sequence of Test queries on either the user or server instance. The results of these Test queries must consistently align with the random bit c. At the conclusion of the experiment, the adversary A returns a bit. A is the winner if c'= c. Let *Succ* represent the scenario in which A wins the game. The A's probability in winning the challenge is $Adv_P^{ake} = 2|Pr[Succ] - 1|$. A protocol P is considered secure if the advantage of an adversary Adv_P^{ake} is less than or equal to a sufficiently small value $\eta > 0$.

Lemma 6.2 (Difference Lemma): [11] Let's assume that $Succ_1$, $Succ_2$ and $Succ_3$, represent events within a given probability distribution. Additionally if we have the condition that

$Succ_1 \wedge Succ_3 \Leftrightarrow Succ_2$, then the following inequality holds:

$|Pr[Succ_1] - Pr[Succ_2]| \leq Pr[Succ_3]$.

The following theorem establishes the semantic security of the proposed protocol.

Theorem 6.3: Let's suppose that the adversary A operates within a polynomial time frame of t in the context of the proposed protocol P while utilizing a random oracle. Additionally, let D denote a password dictionary space uniformly distributed. The probability of adversary A successfully compromising the security of the session key in protocol P is given by:

$$Adv_P^{AKAP} \leq \frac{q_h^2}{|Hash|} + \frac{2q_{send}}{|D|} + 2Adv^{ECDHP}(t).$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Here q_h denotes Hash query frequency, $|Hash|$ is the hash function's range space, q_{send} denotes send query frequency, $|D|$ is the size of dictionary space, and $Adv^{ECDHP}(t)$ is A's advantage in breaking the ECDH.

Remark: Here $|Hash||D|$ are sufficiently large.

Proof 6.3: An adversary A is given five incremental attacks of A in G_i, $0 \le i \le 4$. The advantage

Adv^{AKAP} of A is breaking the semantic security of P is deduced by difference between games G_i. The adversary A's success in guessing the bit c in the game G_i is indicated by Wik_i. The suggested protocol spans games G_0 to G_4. . The conclusion of the proof will demonstrate that the adversary A possesses a negligible advantage when it comes to compromising the session key security of the proposed protocol P.

- Game G_0: Game G: This represents a genuine adversarial attack on the random oracle protocol P. At the commencement of this scenario, a bit c is chosen. Using the definition 6.1 we obtain

$$Adv_P^{AKAP}(A) = 2|Pr[Succ] - 1| \quad (1)$$

- Game G_1: Eavesdropping attack is modelled by this game. The adversary A eavesdrop $M_1 = \{DID_p, \alpha P, V_p, T_p\}$ and $M_2 = \{\beta P, V_s, F, T_s\}$ transmitted during mutual authentication and key agreement phase. Initially, the adversary initiates an execute query, followed by a test query, in which it tries to ascertain whether the output corresponds to a legitimate session key SK or if it is simply a random value. In the proposed protocol, the session key is calculated as $SK = h(ID_p \| \alpha\beta P \| A_p)$. The computation of SK necessitates the secret credentials ID_p, α, β and A_p all of which are unfamiliar to the adversary A. Consequently, the chances of adversary A succeeding in this game through an eavesdropping attack remain unaltered. The probability of G_0 and G_1 is then the same. As a result, we get the following equation:

$$Pr[Succ_0] = Pr[Succ_1] \quad (2)$$

- Game G_2: In G_2 oracles Send and Hash, as well as the oracles Execute $(\prod^t, \prod^u, \prod^u)$ and Test, are used to simulate G_2. The attacker A engages in an active attack, attempting to

deceive the authenticated participants by sending forged messages. To achieve collisions, the adversary A persistently makes continuous hash queries. As all monitored messages $M_1 = \{DID_p, \alpha P, V_p, T_p\}$ and $M_2 = \{\beta P, V_s, F, T_s\}$ are linked to the random numbers , α, β and the time stamp T_p and T_s, the messages will always be random. As a result, querying the *Send* oracle will result in no collisions. The following equation is derived using the birthday paradox [12]:

$$|Pr[Succ] = Pr[Succ]| \le \frac{q_h^2}{|Hash|} \quad (3)$$

- Game G_3: This game simulates the *Corrupt MD* oracle. In order to acquire the password, the adversary A employs a dictionary attack, making use of the parameters stored within the mobile device. Nevertheless, in the proposed protocol, the quantity of unsuccessful login attempts is limited

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

to a finite value. Consequently, we deduce the following expression:

$$| Pr[Succ_0] = Pr[Succ_1]| \leq \frac{q_{send}}{2^l|D|} \quad (4)$$

- Game G_4: In this situation the adversary strives to obtain the accurate session key SK that is jointly utilized by both the patient and the server. It's worth noting that $SK = h(ID_p \| \alpha\beta P \| A_p)$, computing $\alpha\beta P$ from the captured αP in M_1 and βP in M_2 equals calculating the ECDHP in polynomial time t. Thus, we obtain:

$$| Pr[Succ_0] = Pr[Succ_1]| \leq Adv_A^{ECDHP}(t) \quad (5)$$

The value of c is not revealed to any adversary, and all session keys are generated randomly and are independent of each other. As a result, it is evident that

$$Pr[Succ_4] = \frac{1}{2} \quad (6)$$

Equation (1) and (2) yield the following results:

$$Adv_A^{AKPK}(t) = \left| Pr[Succ_0] - \frac{1}{2} \right| = \left| Pr[Succ_1] - \frac{1}{2} \right| \quad (7)$$

Equation (6) and (7) yield the following outcomes:

$$\frac{1}{2} Adv_A^{AKPK}(t) = \left| Pr[Succ_0] - \frac{1}{2} \right| = |Pr[Succ_1] - Pr[Succ_4]| \quad (8)$$

The triangular inequality gives the following

$$|Pr[Succ_1] - Pr[Succ_4]| \leq |Pr[Succ_1] - Pr[Succ_2]| + |Pr[Succ_2] - Pr[Succ_4]|$$

$$\leq |Pr[Succ_1] - Pr[Succ_2]| + |Pr[Succ_2] - Pr[Succ_3]|$$

$$+|Pr[Succ_3] - Pr[Succ_4]| \quad (9)$$

By combining equations (3), (4), (5), and (9), we obtain the following:

$$|Pr[Succ_1] - Pr[Succ_4]| \leq \frac{q_h^2}{2|Hash|} + \frac{q_{send}}{|D|} + Adv_A^{ECDHP}(t) \quad (10)$$

Equation (8) & (10) result in the following outcome:

$$\frac{1}{2} Adv_A^{AKPK}(t) \leq \frac{q_h^2}{2|Hash|} + \frac{q_{send}}{|D|} + Adv_A^{ECDHP}(t) \quad (11)$$

Therefore the desired conclusion is obtained by multiplying both sides of (11) by a factor of two:

$$Adv_A^{AKPK}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2|D|} + 2Adv_A^{ECDHP}(t) \quad (12)$$

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The following section delves into the security properties offered by the proposed protocol.

- **Resist Known-Session-Specific Temporary Information Attack**: The proposed protocol resists this attack i.e., even if an adversary has the random variablesα and/or β, he/she cannot calculate session key $SK = h(ID_p \| \alpha\beta P \| A_p)$. To compute SK the adversary must use the server's secret key s which is not accessible to the attacker. Consequently, adversary will be unable to compute the session key SK and the proposed protocol will be resistant to known-session specific temporary information attacks.

Resist Off-line Dictionary Attack and DOS Attack: In accordance to the range space of |HASH| and the size of |D| are sufficiently large. Furthermore in the login phase, the card validates $Ver_p' = Ver_p$ and if equality do-not holds, it aborts the session. Additionally, the system imposes a limit on the number of incorrect password inputsto a finite number. All these ensure that protocol canresist off-line dictionary attack and DOS attack.

- **Resist Replay Attack:** Each message $M_1$and M_2issupplied with timestamps T_p and T_s respectively, during the exchanges between the patient and the server. As a result, even if an adversary could record and replay messages sent between two entities, those messages would fail to pass the authentication mechanism of the parties involved.
- **Resist Privileged Insider and Stolen Smart Card Attack:** Let an insider who knows registration information ID_p and RPW_p of a legitimate user turns as an adversary and reads the stolen smart card information by using power analysis methods [13]. However, A cannot obtain any useful information from it as all the obtained parameters are safeguard using either one-way hash function or symmetric encryption.
- **Resist Man-in-the-middle Attack:** Messages M_1 and M_2 can be obtained by the attacker A in the suggested protocol. Then A can try to change or fake these communications in the hopes of one of the counterparts accepting them. A must then computes V_p and V_s to ensure that the counterparts authenticate him/her. However, due to the difficulties of ECDHP, A is unable to deduce these messages without (ID_p, r_s, B_p) As a result, the proposed protocol's authentication mechanism thwart man-in-the-middle attacks.
- **Resist User Impersonation Attack:** In this attack, an attacker impersonates as a legal participant. As explained in above attack due to hardness of ECDHP and mutual authentication mechanism, A cannot be validated by the intended participant. Consequently, the proposed protocol can effectively resist user impersonation attacks.
- **Resist Server Impersonation Attack:** A attempts to impersonate as server. Any user's communication $M_1 = \{DID_p, \alpha P, V_p, T_p\}$ could be intercepted by a malicious insider. Then S/he tries to compute $M_2 = \{\beta P, V_s, F, T_s\}$ to prove that they are the server. But the attacker cannot compute $A_p = h(ID_p \| s)$, since the server's private key s, is unknown. As a result, he won't be able to compute valid M_2 and thus won't be able to impersonate as server.
- **Provides User Anonymity and Un-traceability:** In order to obtain ID_p from the expression $DID_p = E_s(ID_p \| r_s)$, having access to r_s be essential, and this information is solely held by

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the server. Furthermore the login message $M_1 = \{DID_p, \alpha P, V_p, T_p\}$ is dynamic because it includes the random number α. As a result, the proposed protocol offers user anonymity and untrace ability.

- **Provides Perfect Forward Secrecy:** If the attacker, even with knowledge of the long-term key, is unable to compute the session key SK, the protocol is deemed to offer perfect forward secrecy. In the proposed protocol, due to the computational difficulty of the ECDHP, even if an adversary possesses the server's private key s, they will still be incapable of calculating the session key $SK = h(ID_p \| \alpha\beta P \| A_p)$.

PERFORMANCE ASSESSMENT AND COMPARATIVE ANALYSIS

In this section, we perform a performance comparison between the proposed protocol and those by Sharif et al. [14], Ravan bakhsh and Nazari [15], and Arshad and Nikooghadam [16], with particular attention to the computational costs involved in the login authentication and key agreement phases. The evaluation primarily revolves around assessing the computational expenses associated with the operations performed within each phase of the respective protocols. As referenced in He et al. [7], Table II provides an overview of various computational complexities and their corresponding execution times in seconds.

We have made the assumption that an identity or timestamp consists of 32 bits, a nonce is 64 bits in length, an elliptic curve (EC) point spans 320 bits, and the output of a hash function is 256 bits for communication-related costs. The computational overhead of the proposed protocol, as well as other relevant protocols, is condensed in Table III. As indicated by Table III, the suggested protocol demonstrates greater efficiency compared to existing protocols.

Notation	Description
T_E	Modular exponentiation execution time ~ 0.063075 *Sec.*
T_M	The Elliptic curve scalar point multiplication execution time, 0.522 *Sec.*
T_H	The simple hash function execution time ~ 0.0005 *Sec.*
T_F	The fuzzy extractor execution time, ~ 0.063075 *Sec.*
T_S	The symmetric key encryption and decryption execution time ~ 0.0087 Sec.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE II DEFINITION AND EXECUTION TIME OF VARIOUS OPERATIONS UNIT

Protocols	Login Authentication and Key agreement Phase		Total	Communication Cost (bits)
	Patient	Server		
Amintoosi [1]	$2T_M + T_S + 5T_H$ ~ 1.0552	$2T_M + 2T_S + 3RD$ ~ 1.0629	2.1181	1280
Sharif [14]	$2T_M + 7T_H$ ~ 1.0475	$2T_M + 2T_S + 57$ ~ 1.0649	2.1124	1376
Ravanbaksh [15]	$T_F + 3T_M + 7T_H$ ~ 1.6332	$3T_M + 4T_H$ ~ 1.568	3.2010	1248
Arshad [16]	$2T_M + 7T_H$ ~ 1.0475	$2T_M + 7T_H$ ~ 1.0475	2.0950	1632
Proposed	$2T_M + 6T_H$ ~ 1.047	$2T_M + 2T_S + 5T_H$ ~ 1.0639	2.1109	1216

TABLE III COMPUTATIONAL OVERHEAD COMPUTATION

CONCLUSION

We propose an authentication and key agreement technique for a TMIS that is both secure and efficient. All of the problems in the Amintoosi and Nikooghadam [1] are eliminated with this enhanced protocol. The suggested protocol is subjected to formal analysis as well as heuristic analysis, to establish that it meets all of the security requirements and compared to state- of -the-art protocols to demonstrate its suitability for TMIS. As a result, the suggested protocol increases security and efficiency while simultaneously eliminating vulnerabilities.

REFERENCES

[1] Amintoosi, H., & Nikooghadam, M. (2019, October). A novel provably-secure ECC-based authentication and key management protocol for telecare medical information systems. In *2019 9th International Conference on Computer and Knowledge Engineering (ICCKE)* (pp. 85-90). IEEE.

[2] Khatoon, S., Rahman, S. M. M., Alrubaian, M., & Alamri, A. (2019). Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment. IEEE access, 7, 47962-47971.

[3] Dolev, D., & Yao, A. (1983). On the security of public key protocols. IEEE Transactions on information theory, 29(2), 198-208.

[4] Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., & Shalmani, M. T. M. (2008). On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. In Advances in Cryptology–CRYPTO 2008: 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings 28 (pp. 203-220). Springer Berlin Heidelberg.

[5] Wang, D., & Wang, P. (2016). Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE transactions on dependable and secure computing*, *15*(4), 708-722.

[6] Wang, D., He, D., Wang, P., & Chu, C. H. (2014). Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Transactions on Dependable and*

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Secure Computing, *12*(4), 428-442.

[7] He, D., & Wang, D. (2014). Robust biometrics-based authentication scheme for multiserver environment. *IEEE Systems Journal*, *9*(3), 816-823.

[8] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE transactions on computers*, *51*(5), 541-552.

[9] Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19* (pp. 388-397). Springer Berlin Heidelberg.

[10] Bonneau, J. (2012, May). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE symposium on security and privacy* (pp. 538-552). IEEE.

[11] Abdalla, M., Fouque, P. A., & Pointcheval, D. (2005). Password-based authenticated key exchange in the three-party setting. In *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8* (pp. 65-84). Springer Berlin Heidelberg.

[12] Boyko, V., MacKenzie, P., & Patel, S. (2000). Provably secure password-authenticated key exchange using Diffie-Hellman. In *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19* (pp. 156-171). Springer Berlin Heidelberg.

[13] Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19* (pp. 388-397). Springer Berlin Heidelberg.

[14] Ostad-Sharif, A., Abbasinezhad-Mood, D., & Nikooghadam, M. (2019). An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. *International journal of communication systems*, *32*(5), e3913.

[15] Ravan bakhsh, N., & Nazari, M. (2018). An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems. *Multimedia Tools and Applications*, *77*(1), 55-88.

[16] Ravan bakhsh, N., & Nazari, M. (2018). An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems. *Multimedia Tools and Applications*, *77*(1), 55-88.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.