User anonymity-based secure authentication protocol for telemedical server systems

Sunil Gupta*

Department of Cybernetics,
School of Computer Science and Engineering,
University of Petroleum and Energy Studies,
Dehradun, India
Email: s.gupta@ddn.upes.ac.in
*Corresponding author

Pradeep Kumar Arya

Department of Computer Science,
BML Munjal University,
Gurgaon, India
Email: pradeep.arya@bmu.edu.in

Hitesh Kumar Sharma

Department of Cybernetics,
School of Computer Science and Engineering,
University of Petroleum and Energy Studies,
Dehradun, India
Email: durgansh.sharma@ddn.upes.ac.in

Abstract: Telemedical server system enables a user to support the monitoring of health at home and access the medical facility over the network. Recently, many schemes have been proposed for providing security in the medical server system. Recently in year 2017, Limbasiya and Shivam proposed a scheme for medical applications using two-factor key verification. They claimed that the protocol provides security against all types of known active and passive attacks. In this paper we show that the Limbasiya and Shivam scheme suffers from user anonymity, replay and impersonation attack. The Limbasiya and Shivam scheme fails to provide low power consumption in terms of cryptographic computational operation and over head to the server. We propose a secure user anonymity-based authentication protocol to remove the weakness of former protocols. Our scheme is more effective in terms of mutual authentication and low power consumption. The performance analysis of our protocol shows less cryptographic computational cost and the server overload. The proposed protocol is tested and analysed using AVISPA security verification to confirm the secure and authentic protocol for telemedical server system.

Keywords: authentication; telemedical server; AVISPA; efficiency; smart card.

Reference to this paper should be made as follows: Gupta, S., Arya, P.K. and Sharma, H.K. (2023) 'User anonymity-based secure authentication protocol for telemedical server systems', *Int. J. Information and Computer Security*, Vol. 20, Nos. 1/2, pp.199–219.

Biographical notes: Sunil Gupta has over more than 18 years of experience in teaching and research in the field of computer science and engineering. He is working as a Professor in the University of Petroleum and Energy Studies (UPES). He is an active researcher in field of healthcare technology, cryptography and network security, cloud computing and internet of things.

Pradeep Kumar Arya completed his PhD in Computer Science and Engineering from the Anna University, India. He is an active researcher in field of cloud computing and security in sensor networks. He is an active team member of placement cell at the BML Munjal and mentor of Strokes Club.

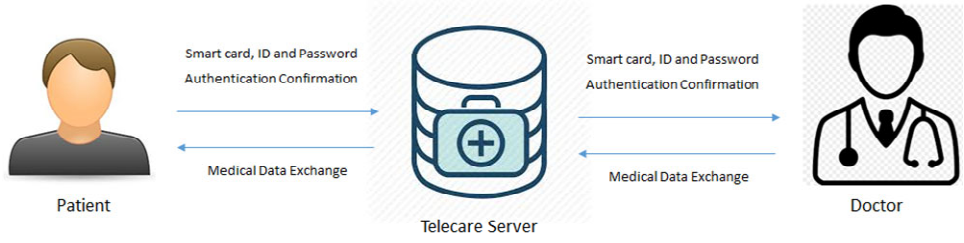
Hitesh Kumar Sharma is an Associate Professor in the Department of Cybernetics, SoCS, University of Petroleum and Energy Studies. He has published more than 50 research papers in international and national journals. He has authored two books. He has also filed and published two patents. His research area is network security and machine learning.

1 Introduction

In 21st century, technology made it possible to provide healthcare treatment from remote locations. The advancement in technologies like IoT, cloud computing, network security, etc. provide a strong support to telecare medicine information systems (TMISs) for remote healthcare. TMIS are intelligent systems which helps doctors to provide treatment remotely to their patient who are in rural areas and unable to visit hospitals. The patients store their medical reports and their treatments in TMIS repository and the doctor can access this repository to check the medical history of the patient. It helps the patient to save expense resulting from real time visits to the hospital, besides saving precious time. It also reduces overhead to the doctor and hospital to attend patient physically. Whenever patient requires medical treatment, he needs to authenticate himself/herself and provide his/her smart card details to a smart device. After authentication, patient needs to send his/her information to medical server via free network channel (Gubbi et al., 2013). The patients share their medical information with the server through a common network channel and this medical information is a very critical one, especially from a patient's perspective. In this case, privacy, security, confidentiality and integrity of their record are important for them. Since all this medical information is floating through a network and stored in a cloud server, the chance of a network attack to steal/temper/hack these records is highly possible. Attackers can also take control over the medical server and provide wrong treatment to the patient, which can cause a severe medical problem, not rule out a major medical emergency. Health is the most critical concern, but the security of such systems involved in remote medical treatment is as major an apprehension (Chen et al., 2011). In this view, so many authentication systems have been proposed for TMIS. However, these authentication systems have certain security issues and are prone to network attacks. To overcome these authentication issues, we have proposed an updated authentication model. The detailed authentication process is defined in the other sections

of the paper. There are three main blocks for TMIS patient, doctor and telemedical server. Figure 1 explains the basic authentication mechanism of TMIS.

Figure 1 Telemedical information system block diagram for user authentication (see online version for colours)



2 Related work

Lamport (1981) introduced an algorithm for authentication for accessing remote systems. In 2000, Hwang and Li suggested an authentication system for user by using Elgamals public key algorithm. In 2000, Sun defined an advanced scheme using a smart card for user authentication with more benefits over the authentication system proposed by Hwang and Li's (2000) in their scheme. In 2003, Wu and Chieu proposed an authentication based on smart card for remote users act as user friendly model. The shortcoming of Sun smart card-based model was resolved by Wu and Chieu (2003) in their model. Lee and Chiu (2005) reviewed the Mu and Chieu model and identified a forgery attack in their authentication system and proposed an improved model after fixing all security flaws and possible attacks. In 2006, Liao et al. came up with a one-factor authentication system using the Diffie-Hellman key exchange theory and they used hash function in to secure insecure networks and provide security for some general network attacks like stolen-verifier attack, replay attack, guessing attack and modification attack.

In 2011, Wang et al. declared a secure authentication system with some unique features. It excludes the need to maintain password documentation, and does not necessitate the updation of the master key every time a new service provider joins the system (Wang et al., 2011). Pu et al. (2012) found some security problems regarding forward secrecy in the authentication model of Wang et al. (2011) and in turn proposed a new authentication model with better scheme to improve security features. In 2012, Wu et al. suggest a new model in which they reduced some exponential operators to minimise computing time, and also claimed that with reducing computing time their model is more effectively secure against any kind of network attack. After Wu et al. (2012) work, He et al. (2012) reviewed Wu et al.'s (2012) model and found weaknesses like an impersonation and privilege insider attack. To overcome these two major attacks in Wu et al. (2012) scheme, they proposed their own model. In 2012, Wei et al. analysed both models. Wei et al. (2012) proposed a new model to primarily remove these security issues. In 2013, Khan and Kumari identified that Wei et al. (2012) authentication scheme were weak against smartcard stolen, offline password guessing and DoS attack.

In 2013, Awasthi and Srivastava suggested a novel three factor authentication protocol for medical server system using biometric system and pseudorandom numbers.

Analysing their schemes, Tan (2014) caught an issue of user anonymity and a reflection attack in their work. Arshad and Nikooghadam (2014) identified DoS and replay attacks in Tan (2014) scheme. In 2015, Giri et al. reviewed Lee and Chiu (2005) authentication scheme for medical server and found an offline password guessing attack vulnerability. In same year, Amin and Biswas (2015) identified some flaws in authentication schemes of Giri et al. (2015). These flaws or weaknesses are: offline password guessing, privilege insider and user anonymity attacks.

In continuous effort to improve the security in earlier schemes, Bin Muhaya (2015) presented an improved scheme for authentication in telemedical system. Though, it was proved that Bin Muhaya's (2015) scheme also has a weakness for perfect secrecy and password guessing attacks. To remove the security flaws of Bin Muhaya (2015) authentication scheme the Arshad and Nikooghadam (2014) suggested a new key agreement and authentication protocol to provide user anonymity in telemedical system.

In 2017, Limbasiya and Shivam's (2017) revised Arshad and Nikooghadam (2014) authentication schemes precisely with the support of irreversible hash function, exclusive-or (XOR) operations and identified some vulnerabilities. Then, they introduced a novel authentication protocol to overwhelm the issues in previous schemes. In this paper, we have explored Limbasiya and Shivam (2017) protocol mathematically and found the weakness in terms of attacks and overhead protocol.

3 Analysis of Limbasiya and Shivam (2017) protocol

Limbasiya and Shivam (2017) identified some security attack issues, named as, impersonation and session key disclosure attacks. To remove the weakness, they advised an enhanced two-factor authentication mechanism after eliminating all security issues found in Arshad and Nikooghadam (2014). Proposed authentication system has three phases. First is registration phase, second is authentication, and third is updating of the password. The protocol used notations have been specified in Table 1. The step by step procedure of all three phases has been described in following section.

3.1 Registration phase

The registration phase consist mainly four stages. The flow of these four steps with mathematical formulas has been given in Table 2. It will be processed only once for each user. A new user can register directly to the system without intervention of an intermediate authentication system. Using a private communication channel a new user can register by executing the subsequent steps.

Step 1 *Ui:* User picks identification as IDi, and random number PWi, N_U. Computes $Mi = h(PWi \,||\, N_U)$ and sends a registration appeal message $\{IDi, Mi\}$ to the server through a private medium.

Step 2 *S:* Selects N_S and calculates $MIDi = h(IDi \,||\, N_S)$, $Ai = h(IDi \,||\, Yi \,||\, MIDi)$, $Pi = Ai \oplus Yi$, $Ni = Mi \oplus xi$.

Step 3 *S:* In this step, server will store IDi and $MIDi$ in its data centre, and $\{Ai, MIDi, Pi, Ni, h(\cdot)\}$ in SCi and provide the SCi information to the new user.

Step 4 *Ui:* Calculates $Bi = Ai \oplus h(IDi \,||\, PWi)$ and replaces Ai with Bi in the smart card: $SCi = \{Bi, MIDi, Pi, Ni, h(\cdot)\}$.

Table 1 Symbols and notation used in Limbasiya and Shivam (2017) system

Symbol	*Definition*
IDi	Identification of user
PWi	User password
N_U	A randomly generated nonce of user
N_S	A randomly generated nonce of server
xi	Server secret key
Yi	User's key for server
$MIDi$	Masked identity for user
T_2, T_3	Time measures at receiver end
T_1, T_4	Time measures at sender end
ΔT	The maximum delay allowed for transmission
SK	A session key with mutual agreement
$\|\|$	Operation for concatenation
$\oplus$	Operation for XOR
S	Server notation
Ui	User notation
SCi	Smart card for user
$h(\cdot)$	Hash function used for one-way

3.2 Authentication phase

The steps with calculation have been described in Table 3. All these steps are executed routinely and respective measurements are evaluated using the free channel:

Step 1 *Ui:* The user inserts the smart card SCi into the reader and inputs their identification and password as IDi and PWi. Then, computes $Ai = Bi \oplus h(IDi \,||\, PWi)$ where $Ai = h(IDi \,||\, Yi \,||\, MIDi)$, $Yi = Ai \oplus Pi$, $xi = Pi \oplus Ni$. A random number dC is generated and

$$QC = dCYi, V1 = h(IDi \,||\, Ai \,||\, QC \,||\, T1), K1 = dCxi = V1' = V1 \oplus (K1 \,||\, T1)$$

$MIDi' = MIDi \oplus h(K1)$ are evaluated. A request for login $\{MIDi', V1', QC, T1\}$ is given to the telemedical server.

Step 2 *S:* After getting $\{MIDi', V_1, Q_C, T_1\}$, the telemedical server checks $T_2 - T_1 \leq \Delta T$. The server then calculates $K_1^* = d_C xi = \dfrac{QCxi}{Yi}$, $V1 = V_1' \oplus h\left(K_1^* \,||\, T_1\right)$, $MIDi = MIDi' \oplus h(K1^*)$ and checks for $h(IDi \,||\, h(IDi \,||\, Yi \,||\, MIDi) \,||\, Q_C \,||\, T1) = ?V1$. Then, the server generates a number randomly d_S, and calculates $Q_S = d_S Yi$, $K_2 = h(dSQ_CT_3) = h(dSdCYiT_3)$, where T_3 is the measured time at server end when K_2 is calculated and $V2 = h(QS \,||\, V2 \,||\, K2)$. Finally, the server generates

the its session key $SK_S = h(IDi \| K_2)$ and sent back a challenge message to user$\{Q_S, V_2, T_3\}$.

Step 3 *Ui:* After getting the challenge communication from the telemedical server *S*, the *Ui* checks $T_4 - T_3 \leq \Delta T$. The user then calculates the values $dS = QSYi$, $K_2^* = h(dCQS) = h(d_S d_C Yi T_3)$ and checks * $h(QS \| V1 \| K2^*) = ?V2$. Then, the user side session key $SKU = h(IDi \| K2^*)$ is calculated. Finally, the $SKU = ?SKS$ is compared and if it is equal then server authenticates the session, if it is not found equal, server will terminate the session forcefully.

Table 2 Review of Limbasiya and Shivam (2017) registration phase

User		*Telemedical server*
Selects *identification, password and nonce as IDi, PWi and* N_U		
Calculates $Mi = h(PWi \| N_U)$		
	$\{IDi, Mi\}$ → Secure channel	
		Chooses *NS*
		Computes…
		$MIDi = h(IDi \| NS)$
		$Ai = h(IDi \| Yi \| MIDi)$
		$Pi = Ai \oplus Yi$
		$Ni = Mi \oplus xi$
		$SCi = \{Ai, MIDi, Pi, Ni, h(\cdot)\}$
		Stores *IDi* and *MIDi* in the database
	$\{SCi\}$ ← Secure channel	
Calculates $Bi = Ai \oplus h(IDi \| PWi)$		
Replace *Ai* and *Bi* in *SCi*		
$SCi = \{Bi, MIDi, Pi, Ni, h(\cdot)\}$		

Table 3 Authentication phase of Limbasiya and Shivam (2017)

User	*Telemedical server*
Inserts the user smart card into the reader	
Enters identification and password, *IDi* and *PWi*	
$SCi = \{Bi, MIDi, Pi, Ni, h(\cdot)\}$	
Computes…	
$Ai = Bi \oplus h(IDi \| PWi)$	
Where $Ai = h(IDi \| Yi \| MIDi)$	

Table 3 Authentication phase of Limbasiya and Shivam (2017) (continued)

User		*Telemedical server*
Computes…		
$Yi = Ai \oplus Pi$		
$xi = Pi \oplus Ni$		
Generates a random number dC		
Computes…		
$QS = dCYi$		
$V1 = h(IDi \| Ai \| QC \| T1)$		
$K1 = dCxi$		
$V_1' = V_1 \oplus h(K_1 \| T_1)$		
$MIDi' = MIDi \oplus h(K_1)$		
	$\{MIDi, V_1', Qc, Ti\}$ →	
		Checks $T_2 - T_1 \leq \Delta T$
		Computes…
		$K_1^* = d_C xi = \frac{QCxi}{Yi}$
		$V_1' = V_1 \oplus h(K_1 \| T_1)$
		$MIDi = MIDi' \oplus h(K_1^*)$
		Checks…
		$h(IDi \| h(IDi \| Yi \| MIDi) \| QC \| T_1 = ?V_1$
		Generates random number dS
		Computes…
		$Q_S = d_S Yi$
		$K_2 = h(d_S Q_C T_3) = h(d_S d_C Yi T_3)$
		$V_2 = h(Q_S \| V_1 \| K_2)$
		$SK_S = h(IDi \| K_2)$
	← $\{Q_s, V_2, T_3\}$	
Checks		
$T_4 - T_3 \leq \Delta T$		
$d_S = Q_S Yi$		
$K_2^* = hj(d_C Q_S) = h(d_C d_S Yi T_3)$		
Verifies $h(Q_S \| V_1 \| K_2^*) = ?V_2$		
Calculates *		
$SK_U = h(IDi \| K_2^*)$		
Checks $SKU = ?\ SKS$		

3.3 User password update phase

If a user needs to update the current password for any reason, than the third phase will be used and the steps defined for updating password will be processed:

Step 1 Do the same Step 1 of Section 3.2 of the authentication phase.

Step 2 Do the same Step 2 of Section 3.2 of the authentication phase.

Step 3 Upon getting the challenge $\{Q_S, V_2, T_3\}$ from the server, the user calculates $K_2^* = h(d_C Q_S) = h(d_C d_S Y i T_3)$ and verifies whether $h(Q_S \| V_1 \| K_2^*)$ matches the received V_2 or not. If it is not matched, the process get terminate. If it get match with the value, the smart card calculates $B_i^{new} = Ai \oplus h(IDi \| PW_i^{new})$ and updates Bi with B_i^{new} in SC_i.

4 Weakness of Limbasiya and Shivam (2017) protocol

This section shows that Limbasiya and Shivam (2017) scheme is vulnerable to user anonymity attack, replay attack and user impersonation attack. The scheme provides low performance in terms of computational cost and overhead of the telemedical server.

4.1 User anonymity and replay attacks

If the intruder is able to enter in between the communication, he/she may be able to find out the detail of smart card as $SCi = <A_i, MID, Pi, Ni, h(\cdot)>$ by which the intruder may easily know the identification of the user as follows:

1 Intruder knows MID and hash function by which he/she able to find out the identification 'ID_1' of the user and nonce N_s.

2 When the user goes to login phase the intruder is easily able to calculate A_i as he/she knows B_i, ID.

3 When the user inputs the password, he is able to calculate

$$A_i = B_i \oplus h(ID1 \| PW)$$

By which intruder is easily able to calculate

$$Y_i = A_i \oplus P_i$$

$$X_i = P_i \oplus N_i$$

So intruder is able to know the server key of user and server secret key. This may leak the information of user and intruder may easily falsify the information that shows a user anonymity attack.

4 The user anonymity attack forces an intruder for replay attack as he/she get the information of user and network. He/she easily eavesdrops the message and replay the message.

4.2 Impersonation attack

As an intruder is able to know the $Y_i = A_i \oplus P_i$ and $X_i = P_i \oplus N_i$. This shows that intruder knows the secret key of user and server. The intruder now acts as a legitimate server and gives false information to the user and takes all the user data.

Intruder may also behave as hidden server and provide itself as a legitimate medical server. He/she may able to capture all the information of user and provider, which may impact on user data and the network of the system.

4.3 Low performance of Limbasiya and Shivam (2017) scheme

The server has extra overhead to generate pre-user server key and servers per user secret key for each users. This may increase the computational step and need more energy to generate the keys. This increases the extra overhead to server for generating these secret values for each user and store into the database of the server. The comparison chart in Limbasiya scheme also shows that the performance in terms of user registration and authentication phase is less as related to other scheme. The time required for registration phase is 0.0063 ms and for authentication phase it is 0.0237 ms. These values seem high in comparison with other schemes of cryptographic operations.

5 Proposed work

To improve the weakness of Limbasiya and Shivam (2017) protocol, we have proposed a new user anonymity-based authentication protocol consisting of four stages namely server setup stage, user registration stage, authentication stage and password change stage.

5.1 Server setup stage

The telemedical servers setup the parameter in offline mode as follows:

Step 1 The server primary initialises the prime number p and q such that p is a primitive root of q.

Step 2 The server selects a private key 'd' such that $d < q$ and keep the key as secret and a use one way hash function $h(\cdot)$ for message authentication. Where one-way hash function is a mathematical function which converts a variable-length input string into a fixed-length unique binary-sequence which is difficult to invert. One-way hash function generates same hash value for same input but if there is even a small change in input string then the generated output hash value would have huge change. It is computationally difficult to obtain original string from its hash value.

5.2 User registration stage

The user U_i, want associate with a server should registers as follows. Table 4 shows the symbol and notation used in the proposed protocol. Table 5 explicate the registration stage.

Step 1 Every user has to choose their own identity IU_i and password PU_i.

Step 2 The user generates a random number r_i where $i = 2, 3, \ldots, n$ for each set of login to the server.

Step 3 User U_i computes masked password $MPU_i = h(PU_i \| r)$ and send $<MPU_i, IU_i>$ to the server for the login.

Step 4 The server compute $\alpha = \dfrac{1}{qd + h(IUi) - MPU_i \bmod p}$ and stores user identity IU_i and MPU_i in its own database. The medical server send a smart card SC_i to user contain the information as

$$< MPU_i, \alpha, h(), p > .$$

Step 5 The smart card computes the different value of α as α' where

$$\alpha' = (\alpha + MPU_i)^{ri} - MPU_i$$

where r_i is the random number generated by the user at every set of registration.

So, $\alpha' = (\alpha + MPU_i)^{ri} - MPU_i$ and compute $A = q^i \bmod p$ and store these value in the smart card SC_i so smart card contain

$$SC_i = \{\alpha', A, MPU_i, h(), p\}$$

Table 4 Symbol and notation used in proposed protocol

Symbol	*Definition*
IUi	User identity
PUi	User password
MPUi	User masked password
ri	Random number selected by user
d	Private key of server
p, *q*	Prime numbers
SK	A session key with mutual agreement
$\|\|$	Operation for concatenation
$\oplus$	Operation for XOR
S	Server notation
SCi	Smart card for user
$h(\cdot)$	Hash function used for one-way

Table 5 User registration stage of the proposed protocol

User U_j		**Server**
User choose		
Identification and its own password		
IU_i, PU_i		
Generate random no_r_i		
Compute		
$MPU_i = h(PU_i \| r)$		
	$<MPU_i, IU_i>$ →	
		Compute $\alpha = \frac{1}{qd + h(IUi) - MPUi \bmod p}$
		Send smart card SC_i
		$SCi = <MPU_i, \alpha, h(), p>$
		Store IU_i and PU_i in its own database
	← $<SC_i>$	
Compute		
$\alpha' = (\alpha + MPU_i)^{ri} - MPU_i$		
Compute		
$A = q_i^r \bmod p$		
Store $Sc_i = \{\alpha', A, MPU_i, h(), p\}$		

5.3 User login and authentication stage

Once a user U_i needs a login to the server, he/she enters with their user name IU_j and password PU_j. The authentication process starts as follows. Table 6 explicates the user login and authentication stage of the proposed protocol.

Step 1 User U_i login to telemedical server using its smart card SC_j having known parameter stored $<\alpha', A>$.

Step 2 Smart card takes input of user password PU_j and computes

$$MPU_i = h(PU_i \| r_i)$$

$\alpha^* = \alpha' + MPU_i \bmod p$ and compute $B = h(A \| \alpha^* \| IU_i)$ and send $<IU_i, B, A>$ to the telemedical server.

Step 3 Once receiving B, the telemedical server uses its own private key 'd' to calculate $\alpha^{**} = A^{(d+h(IUi)-1} \bmod p$, then server check $B' = h(A \| \alpha^{**} \| IU_i)$.

If $B' = B$, the computation holds true else terminate the session.

Step 4 Telemedical server generates a random number r_j and calculate session key $S_k = h(\alpha^{**} \| r_j)$, $h_1 = h(S_k \| r_j)$ and send r_j and h_1 to the remote user.

Step 5 The user U_i, accept the value r_j and h_1 and user α^* and r_j to compute $S_k' = h(\alpha^* \| r_j)$ and user check $H_1' = h(S_k' \| r_j)$.

If find $h_1' = h$, the computation holds true otherwise terminate the session.

User calculate $_{h2} = h_1(IU_i \| S_k')$ and send h_2 to the server.

Step 6 The server receive h_2 and compute the value $h_3 = h(TU_i \| S_k)$ and compare with $h_2 = h_3$ if computation holds true the communication taken palace and user can access the server resources.

Table 6 User login and authentication stage of the proposed protocol

User		**Medical server**
Enter IU_j and PU_j		
Smart card parameter		
<α′, A>		
Compute		
$MPU_i = h(PU_i \| r_i)$		
$\alpha^* = \alpha' + MPU_i \bmod p$		
$B = A \| \alpha^* \| IU_I)$		
	<IU_i, B, A> →	
		Calculate
		$\alpha^{**} = A^{(d+h(IUi)-1} \bmod p$
		$B' = h(A\| \alpha^{**} \| IU_i)$
		Check B′ = B
		If it holds true
		Generate random number r_j
		Calculate
		$S_k = h(\alpha^{**} \| r_j)$
		$h_1 = h(S_k \| r_j)$
	← <r_j, h_1>	
Compute		
$S_k' = h(\alpha^* \| r_j)$ and user check		
$H_1' = h(S_k' \| r_j)$		
Check		
$h_1' = h$		
If hold true		
Calculate		
$h_2 = h_1(IU_1 \| S_k')$		
	<h_2> →	
		Calculate
		$h_3 = h(IU_i \| S_k)$
		Check $h_3 = h_2$
		If hold true
		Communication start

5.4 Password change stage

Once a user U_i needs to modify the password, then he/she may put his/her sum old password and then enter the new password using following steps:

Step 1 User computes $MPU_i = h(PU_i \| r_i)$ and computes new as $NMPU_i = h(NPU_i \| r_i)$.

Step 2 User computes $\alpha_{new} = \alpha + MPU_i - NMPU_i \bmod p$.

Step 3 $\alpha'_{new} = \alpha' + MPU_i + MPU_i - NMPU_i \bmod p$.

Step 4 Substitute the value of α with new value of α_{new} and substitute the value of α' to new value of α'_{new} and this will make a password change.

6 Security analysis of the proposed protocol

The analysis shows that our proposed protocol provides security against user impersonation attack, replay attack, man in middle attack (MIMA), insider attack, smart card stolen attack, password guessing and anonymity attack.

6.1 Property 1: the proposed work provide the protection against impersonation attack

In the proposed protocol, the telemedical server uses the identity of the user U_i to calculate 'α'. If an intruder wants to do any impersonation attack using this data, he has to do and face all problem of discrete logarithm and it is practically impossible to calculate 'α' using identification only. As we know

$$\frac{1}{qd + h(IU_i) - MPU_i \bmod p}$$

Here, p is prime number and it is a primitive root of q. This is infeasible to find out the value of p and q. So the proposed scheme can provide better security against impersonation attack.

6.2 Property 2: the proposed work provides protection against replay attack

In the proposed scheme, we use random value r_j and r_i for login and authentication process. If any intruder is able to know $<IU_i, B, A>$ and want to use them for login to server. Here, intruder has no knowledge of r_i and r_j. So the intruder will not be able to compute h_1 and h_2. If servers are not able to receive h_3 and computation holds false, this may have an impact on the communication link, so there will be no possibility of replay attack in the communication.

6.3 Property 3: the proposed work provides the protection against the MIMA

In this attack, an intruder intercepts the communication link and shows itself as a legitimate user. In the proposed protocol, the intruder will not be able to generate the r_j,

h_1 and h_2. So he/she cannot compute the valid h_3 so the MIMA is not possible in our proposed work.

6.4 Property 4: the proposed work provides the protection against the insider attack

In our protocol, the user U_i does not directly send the password to the telemedical server. The user U_i changes the entered password to the masked password as $MPU_i = h(PU_i \| r)$ where r is the random number generated by pseudo-random number generator, which is not using any confirmation table so the proposed protocol is safe against the insider attack.

6.5 Property 5: the proposed work provides the protection against smart card stolen attack

In the proposed scheme, the mutual authentication is through the secret key 'd' where value of $d < q$ and q is the prime number. If the intruder is able to store the smart card he/she may not able to modify the password or any user information stored in the server database. In our protocol, server does not need any prior information from smart card. Therefore, if any of the information is stolen and modified, it may not have an impact on the user and server database. So the scheme is secure against stolen attack.

6.6 Property 6: the proposed work provides the protection against password attack

The proposed protocol provides the mutual authentication between user and telemedical server therefore only authentic user password can pass the server authentication, so any attempt by the intruder at guessing the password will be detected by the server. In our scheme, the password is converted into masked password using a random number generator. It is not feasible for the intruder to generate the masked password using the same hash value. Consequently, the protocol is safe against password attack.

7 Performance analysis of the proposed protocol

The performance analysis defines the security feature and the computational cost of proposed protocol and the other related works, Zhu (2012), Bin Muhaya (2015) and Limbasiya and Shivam (2017). Table 7 shows the assessment of the security feature among different authentication schemes. The proposed protocol is safe against all types of known active and passive attack.

Table 8 shows the computation cost of cryptographic operations of related work. Our scheme provides less computational cost related to other protocol. According to the data available in Xu and Wu (2015), the execution time required for the hash function T_H is 0.004 ms and time for XOR operation T_{XOR} is 0.13 sec while the time required for the execution of exponential function T_{expo} is 0.16 ms, these value are calculated by using C/C++ library in MI RACL. Table 9 shows the efficiency of proposed protocol in term of time effectiveness and the energy consumption. The proposed protocol takes 0.192 ms to complete the execution process and requires 4.6 MJ of energy consumption. We use the

formula $E = U * I * t$ for calculating the energy consumption for the mica motes the value of $I = 8$ mA and $U = 3.0$ V at active mode. Table 9 shows the significant improvement in the proposed protocol. Figure 2 shows the total execution time and the energy consumption of the different authentication protocol.

Table 7 Assessment of security features among related authentication schemes

Security feature	*Zhu (2012)*	*Bin Muhaya (2015)*	*Limbasiya and Shivam (2017)*	*Proposed*
Impersonation attack	X	X	X	√
Replay attack	X	X	X	√
Denial of service (DoS)	X	√	√	√
User password guessing	X	√	X	√
Man in middle	√	X	√	√
Insider attack	X	X	√	√
Smart card stolen	X	√	X	√
Server password attack	X	X	X	√
User anonymity	X	X	X	√
Session key attack	X	√	√	√
Mutual authentication	√	X	√	√
Key security	-	√	√	√
Perfect forward secrecy	-	√	√	√

Figure 2 Comparison of total execution time and energy consumption of the authentication protocols (see online version for colours)

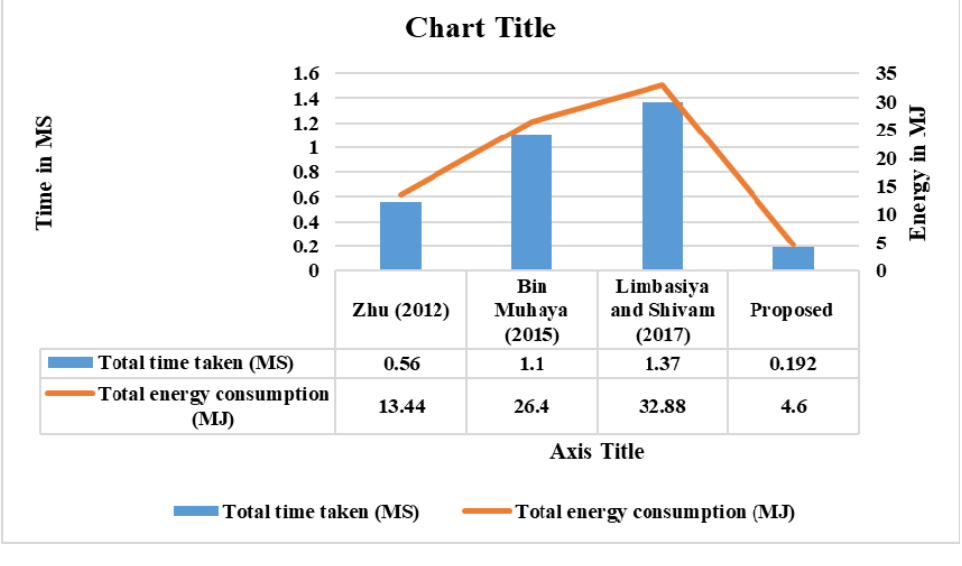


Table 8 Computation cost comparison of proposed protocol with related work

Protocol	*User registration stage*	*User login and authentication*
Zhu (2012)	$2T_H + 2T_{XOR}$	$8T_H + 2T_{XOR}$
Bin Muhaya (2015)	$3T_H + 3T_{XOR}$	$12T_H + 5T_{XOR}$
Limbasiya and Shivam (2017)	$4T_H + 3T_{XOR}$	$15T_H + 7T_{XOR}$
Proposed	$2T_H + T_{expo}$	$6T_H$

Note: Where T_H – time for execution of one way hash function, T_{XOR} – time for execution of XOR operation and T_{expo} – time for execution of exponential operation.

Table 9 Time taken and energy consumption of proposed protocol

Protocol phase	*Zhu (2012)*	*Bin Muhaya (2015)*	*Limbasiya and Shivam (2017)*	*Proposed*
Total cost	$10T_H + 4T_{XOR}$	$15T_H + 8T_{XOR}$	$19T_H + 10T_{XOR}$	$T_H + T_{XOR}$
Total time taken	0.56 MS	1.1 MS	1.37 MS	0.192 MS
Total energy consumption	13.44 MJ	26.4 MJ	32.88 MJ	4.6 MJ

Figure 3 HLPSL code for user role in the proposed protocol

```
role user (Ui,S:agent,
Smk:symmetric_key,
H:hash_func,
Snd,Rcv:channel(dy))
played_by Ui
def=
local State: nat,Hsc:hash_func,
IUi,PUi,MPUi,Ri,MPUi:text,
Aj,Dj,P,Bj,Hl,C,Ri,Rg:text,
Sk,Skp:text
const alice_bob_Ri,alice_bob,alice_bob,
bob_alice,bob_alice,
subl,sub2,sub3,sub4,sub5:protocol_id
init State :=  0
transition
%Registration phase
1. State=0/\Rcv(start) =|>
State' :=1/\Ri' :=new()
      /\PIUi' :=H(IUi.Ri')
      /\Snd({PIUi'}_Smk)
      /\secret ({ IUi},subl,Ui)
%server S send smart card Sm (Rj,Hl) securely
2.  State =1/\Rcv({H(H(IUi.Ri).Bj')
.Hsc(P'.Q').Aj'}_Smk) =|>
% Login and authentication phase
State' :=2 /\ secret ({ Bj', P' ,Q'}. sub2, {S})
       /\MPUi':=H(PUi.Ri)
      /\Wj' :=H(H(IUi.Ri).Bj')
      /\Ri' :=new()
      /\Fj' :=exp((H(IUi.Ri).MPUi'.Ri'.
H(H(IUi.MPUi).Bj')),Aj')
      /\Dj':=H(MPUi'.Ri'.Wj)
      /\Ej' :=H(H(IUi.Ri).MPUi'),Ri')
/\Snd(Dj'.Ej'.Fj')
/\witness(Ui,S,alice_bob,Ri')
/\witness(Ui,S,alice_bob)
3. State=2/\ Rcv((Ri',Rg').
H(H(H(IUi.Ri).H(PUi.Ri).Ri'.Rg')
.H(H(IUi.Ri).Bj').Rg')=|>
State' :=3/\
      /\Sk' :=H(H(IUi.Ri).H(PUi.Ri).Ri'
.Rg')
      /\Skp' :=H(Sk'.H(H(IUi.Ri).Bj')
.H(IUi.Ri))
      /\Snd(Skp)
      /\witness(Ui,S,alice_bob)
      /\request(S,Ui,bob_alice)
      /\request(S,Ui,bob_alice_Ri,Ri')
end role
```

8 Proof of proposed protocol using automated validation of internet security protocol and application

Automated validation of internet security protocol and application (AVISPA) (Armando et al., 2006) uses the 2006/04 2013 version of HLPSL, which supports the authentication and specified goals. Figure 6 and Figure 7 show the results of the AVISPA simulation of proposed protocol. The backend use is OFMC and CL-At sec for execution of protocol.

Figure 4 HLPSL code for server role of the proposed protocol

```
role server (Ui,S:agent,
Smk:symmetric_key,
H:hash_func,
Snd,Rcv:channel(dy))
played_by S
def=
local State: nat,Hsc:hash_func,
IUi,PUi,MPUi,Ri,MPUi:text,
Aj,Dj,P,Bj,Hl,C,Ri,Rg:text,
Sk,Skp:text
const alice_bob_Ri,alice_bob,alice_bob,
bob_alice,bob_alice,
sub1,sub2,sub3,sub4,sub5:protocol_id
init State :=  0
transition
%Registration phase
1. State=0/\Rcv(start) =|>
State' :=1/\P':=new()
/\Q':=new()
/\Aj':=new()
/\N':=Hsc(P',Q')
/\Bj':=inv(Aj')
/\Wj':=H(H(IUi.Ri).Bj')
      /\Snd({Wj'.N'.Aj'}_Smk)
      /\secret ({ IUi},sub1,Ui)
      /\secret({Bj',P',Q'},sub2,{S})
%Login and authentication phase
2.  State =1/\Rcv(H(H(PUi.Ri).Ri'
.H(h(IUi.Ri).Bj').
exp((H(IUi.Ri).H(PUi.Ri).Ri'
.H(H(IUi.Ri).Bj'),Aj)
.xor(H(H(IUi.Ri).H(PUi.Ri)),Ri')) =|>
% Login and authentication phase
State' :=2 /\Rg' :=new()
      /\T2' :=new()
      /\Xt' := (Ri',Rg')
      /\Sk':=H(H(IUi.Ri).H(PUi.Ri)
.Ri'.Rg')
      /\Lj' :=H(Sk'.H(H(IUi.Ri).Bj')
.Rg')
/\Snd(Xt'.Lj)
/\witness(S,Ui, bob_alice)
/\witness(S,Ui,bob_alice_Rg,Rg')
3. State=2/\ Rcv (H(H(IUi.Ri).H(PUi.Ri)
.Ri'.Rg')
.H(H(IUi.Ri).Bj').H(IUi.Ri))=|>
State' :=3/\request(Ui,S, alice_bob')
      /\request(Ui,S, alice_bob_Ri,Ri')
      /\request(Ui,S, alice_bob')

end role
```

Figure 3, Figure 4 and Figure 5 shows the role specification of user, server, session and environment used for simulation using HLPSL code. The analyser checks the security attacks in the given protocol. The simulation back-end has knowledge of all intruder among with legitimate nodes. The result analysis shows that the proposed protocol is safe against all type of known attacks.

Figure 5 Session and environmental HLPSL code for the proposed protocol

```
role session(Ui, S:agent,
Smk :symmetric_key,
H:hash_func)
def=
local SI,SJ,RI,RI:channel(dy)

composition
      user(Ui,S,Smk,H,SI,RI)
      /\server(Ui,S,Smk,H,SJ,RI)
end role



role enviroment()
def=
const Ui,S:agent,
smk:symmetric_key,
h,hsc:hash_func,
iUi,pUi,fj,MPUi,piUi:text,
aj,bj,Ri,rg,xt,p,q,ej,n:text,
dj,ri,cj,wj,lj,sk,skp:text,
alice_bob_Ri,alice_bob,
alice_bob,Ui_S,Ui_S_Ri,S_Ui,
Ui_S,S_Ui_rg,
bob_alice,bob_alice_rg,
subl,sub2: protocol_id
intruder_knowledge = {Ui,S,h,hsc,piUi,
aj,dj,ej,fj,lj,skp}
composition
session(Ui,S,smk,h)
/\session(t,S,smk,h)
/\session(Ui,t,smk,h)
end role

goal
      secrecy_of subl
      secrecy_of sub2
      authentication_on Ui_S
      authentication_on Ui_S_Ri
      authentication_on S_Ui
      authentication_on Ui_S
      authentication_on S_Ui_rg
end goal

enviroment()
```

Figure 6 Result analysis of proposed protocol using OFMC

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/simulation_medical_server.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.63s
  visitedNodes: 24 nodes
  depth: 4 plies
```

Figure 7 Result analysis of proposed protocol using CL-AtSe

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/simulation_medical_server.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 3 states
  Reachable  : 0 states
  Translation: 0.07 seconds
  Computation: 0.01 seconds
```

9 Conclusions

This paper proposed a secure authentication protocol for telemedical server and provides user anonymity protection. The proposed protocol removes the weakness of the Limbasiya and Shivam (2017) protocol and provides conflict against user anonymity, replay attack and impersonation attack. The protocol removes the overhead problem of server for using two secret keys, one for user and another for server. We propose a secure system by using smart card to access the telemedical server remotely. The proposed protocol provides mutual authentication between the user and the medical server. The protocol is simulated using AVISPA and it result shows the protocol is safe against all type of known active and passive attacks.

References

Amin, R. and Biswas, G.P. (2015) 'An improved RSA based user authentication and session key agreement protocol usable in TMIS', *Journal of Medical Systems*, Vol. 39, No. 8, pp.1–14.

Armando, A., Basin, D., Cuellar, J., Rusinowitch, M. and Vigano, L. (2006) 'AVISPA: automated validation of internet security protocols and applications', *ERCIM News*.

Arshad, H. and Nikooghadam, M. (2014) 'Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 38, No. 12, pp.1–12.

Awasthi, A.K. and Srivastava, K. (2013) 'A biometric authentication scheme for telecare medicine information systems with nonce', *Journal of Medical Systems*, Vol. 37, No. 5, pp.1–4.

Bin Muhaya, F.T. (2015) 'Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medicine information system', *Security and Communication Networks*, Vol. 8, No. 2, pp.149–158.

Chen, T.H., Hsiang, H.C. and Shih, W.K. (2011) 'Security enhancement on an improvement on two remote user authentication schemes using smart cards', *Future Generation Computer System*., Vol. 27, No. 4, pp.377–380.

Giri, D., Maitra, T., Amin, R. and Srivastava, P.D. (2015) 'An efficient and robust RSA-based remote user authentication for telecare medical information systems', *Journal of Medical Systems*, Vol. 39, No. 1, pp.1–9.

Gubbi, J., Buyya, R. and Marusic, S. (2013) 'Internet of things (IoT): a vision, architectural elements, and future directions', *Future Generation Computer System*, Vol. 29, No. 7, pp.1645–1660.

He, D., Chen, J. and Zhang, R. (2012) 'A more secure authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 36, No. 3, pp.1989–1995.

Hwang, M.S. and Li, L.H. (2000) 'A new remote user authentication scheme using smart cards', *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 1, pp.28–30.

Khan, M.K. and Kumari, S. (2013) 'An authentication scheme for secure access to healthcare services', *Journal of Medical Systems*, Vol. 37, No. 4, pp.1–12.

Lamport, L. (1981) 'Password authentication with insecure communication', *Communications of the ACM*, Vol. 24, No. 11, pp.770–772.

Lee, N.Y. and Chiu, Y.C. (2005) 'Improved remote authentication scheme with smart card', *Computer Standards Interfaces*, Vol. 27, No. 2, pp.177–180.

Liao, I.E., Lee, C.C. and Hwang, M.S. (2006) 'A password authentication scheme over insecure networks', *Journal of Computer and System Sciences*, Vol. 72, No. 4, pp.727–740.

Limbasiya, T. and Shivam, S. (2017) 'A two-factor key verification system focused on remote user for medical applications', *Int. J. Critical Infrastructures*, Vol. 13, Nos. 2/3, pp.133–151.

Pu, Q., Wang, J. and Zhao, R. (2012) 'Strong authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 36, No. 4, pp.2609–2619.

Sun, H.M. (2000) 'An efficient remote use authentication scheme using smart cards', *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp.958–961.

Tan, Z. (2014) 'A user anonymity preserving three- factor authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 38, No. 3, pp.1–9.

Wang, R.C., Juang, W.S. and Lei, C.L. (2011) 'Provably secure and efficient identification and key agreement protocol with user anonymity', *Journal of Computer and System Sciences*, Vol. 77, No. 4, pp.790–798.

Wei, J., Hu, X. and Liu, W. (2012) 'An improved authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 36, No. 6, pp.3597–3604.

Wu, S.T. and Chieu, B.C. (2003) 'A user friendly remote authentication scheme with smart cards', *Computers Security*, Vol. 22, No. 6, pp.547–550.

Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C. and Chung, Y. (2012) 'A secure authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 36, No. 3, pp.1529–1535.

Xu, L. and Wu, F. (2015) 'Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care', *J. Med. Syst.*, Vol. 39, No. 2, p.10.

Zhu, Z. (2012) 'An efficient authentication scheme for telecare medicine information systems', *Journal of Medical Systems*, Vol. 36, No. 6, pp.3833–3838.