Engineering World
Open Access Journal
ISSN: 2692-5079

A Novel Approach for Patient Anatomized Authentication scheme using Smart Card in Telecare Medical Information System

Chintan Patel, Nishant Doshi

Abstract—In the Telecare Medical Information System (TMIS), a patient (aka *user*) and the server mutually authenticate each other and draws the prevalent session key over an insecure channel. The smart card of the patient contains the parameters predicated on the biometric data of the patient itself. Recently, in *J Med System*, Xie et al. (2014) show that Wen et al.'s scheme is vulnerable to off-line password guessing attack, perfect forward secrecy, and fails to provide patient anonymity and then proposed the biometric-based scheme to overcome these weaknesses. However, we show that Xie et al.'s scheme is still failing to withstand against perfect forward secrecy, key compromise impersonation resilience attack, and known key attack. Afterward, we proposed the scheme that not only secures against existing attacks but also achieves the constant computation time in every phase. Also, we added the *ID phase* and *Biometric Phase* for compromised users to change their credentials including biometric and stop the illegal use of compromised *user* ID or *Biometric* ID. To the best of our knowledge, our scheme is the first construction that provides security against the use of illegal/compromised *user* ID and *Biometric* ID.

Keywords—Telecare medicine, Connected Health Care, Biometric, Password, Authentication Protocol, Smart Card, Cryptanalysis.

I. Introduction

THE internet nowadays become the backbone for everyday's life. With a recent breakthrough in internet technology, the utilizer (from any remote location) can access different services viz. *Telecare Medical Information System*, *Connected Health Centers*, *Private Health Record System* and so on. For example, Telecare Medical Information System (TMIS) maintains the patient's record, which can help doctors diagnose, thus saving the expense and time for a needy patient. To avail of the service, the utilizer requires credentials from the remote server. The remote user authentication technique is useful to give the restricted access to legitimate users (aka *patients*) via remote access. The verification mechanism used by the server requires to stop the unauthorized user from accessing the network. The remote user authentication scheme is a simple, most acceptable, and widely adopted mechanism because of its low cost, user-friendly, simple implementation. The user authentication is the key component in the remote authentication scheme. Besides, verification of generated credentials is also playing an important role. The remote server requires to distinguish between the authorized requests and unauthorized/malicious requests. Failing to that leads to integrity as well as confidentiality to be broken. To handle this problem, the server maintains the identity and password of all authorized users. This mechanism is similar to that we use in our daily life like email access, ATM card usage, internet access. These systems are considered as *password based authentication* schemes. The remote server stores the identity ID and password (PWD) as a tuple in the secure table. Upon authentication requests from the user, the server checks the credentials against that of stored in the table. If it matches, then the user is allowed to do further communication; otherwise, the connection is terminated.

Through smart card-based verification, it delivers more security improvement. The Smart card takes as input identification and password and makes a login request to the server. The server authenticates the user by verifying them using the server's secret parameters. The smart card-based user authentication system's fundamental goal is to authenticate a valid cardholder with the right privileges directed by the issuer of the card.

In TMIS, the patient's anonymity is an important factor as the disease details of the respective patient can harm the patient [1], [2]. Indeed in [3], the authors proposed the dynamic ID-based password authentication scheme with patient anonymity where other schemes [4], [5], [6], [7], [8] fail to do so. However, in [9], [10], the authors shows that the scheme of [3] is susceptible to *password guessing attack,impersonation attack* and fails to provide *user anonymity*. For the ease of reading, in Figure 1, we have given the state-of-art survey for research in password-based authentication schemes [11], [12], [13], [14], [15], [16].

However, in real time patient (user) selects the weak password that is easy to guess and lead to the off-line password guessing attack. This can be prevented if there is provision to add the unique identity of user which not required to remember by user i.e. *Biometric* identity. Indeed in [17], the authors proposed the biometric based scheme for Telecare Medical Information system (TMIS). Thereafter, many researchers [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42] have worked in this area Very Recently, in [43], the authors showed that the scheme of [25] is vulnerable to *forward secrecy, off-line password guessing attack* and loss of *user anonymity*.

In this paper, we show that a uniqueness-and-anonymity-preserving user authentication scheme [43] is susceptible to *Perfect Forward Secrecy, Key Compromise Impersonation*

Chintan Patel is with the Department of Computer Science and Engineering, Pandit Deendayal Petroleum University, India
N. Doshi is with the Department of Computer Science and Engineering, Pandit Deendayal Petroleum University, India

Resilience Attack and *The Known Key Attack*. After that, we proposed our enhanced approach to deal with this.

A. *Our Contribution*

In this paper, we have done the crypt-analysis of the scheme of Xie et al. [43] and found it to be vulnerable for *perfect forward secrecy*, *key compromise impersonation resilience attack* and *known key attack*. Afterward, we have proposed a scheme to overcome these attacks. In real-time, like we lose our password, we can also lose our bi-metric identity i.e., in the accident, one can lose its bio-metric status like the thumb, eye, etc. Concerning this, in this paper, for the first time, we consider the phase in which the patient (or user) can change his/her bio-metric identity too.

B. *Paper Organization*

The paper is organized as follows. Section 2 and 3 deals with the review and cryptanalysis of the scheme [43] respectively. In section 4, we have given the proposed scheme with five phase. In section 5, we have given the in-depth analysis for prevention of different attacks using the proposed scheme. In section 6, we have given the performance analysis by comparing our scheme with existing schemes. Conclusion and references are at the end.

II. Scheme and Cryptanalysis of Xie et al.[43]

A. *Xie et al. scheme:*

We follow the notations given in Table 1. In Table 1, the e, d, n, p, q are generated in the same way as in the RSA cryptosystem. The *Initialization Phase,* of Xie et al.'s scheme is given in Figure 1. In Figure 2, the user U is communicating with server S during *Login and Authentication Phase*, while in the description (pp. 4 in [43]), the smart card reader is communicating with server S. Therefore, in this section we have modeled the scheme as given in the description, where the line between the user and smart card reader is secure. In contrast, the line between smart card reader and server is insecure.

B. *Cryptanalysis of Xie et al. scheme*

*1) **Perfect Backward/Forward Secrecy**:* A scheme is said to be secure against perfect backward / forward secrecy attack if long term secrets of involving parties (i.e. user and server) doesn't compromised the past and future sessions. In the scheme [43], attacker $\mathbb{A}$ gets the ID_i, PW_i, B_i and smart card. Based on this and record of previous sessions, $\mathbb{A}$ gets the $r_1, r_2, NID_{ij}, NID'_{ij}$. Afterward using trial method as in [43], attacker checks if $NID' = h(r_1||r)$ for different values of r. After getting these values, attacker can compute the sk of that session. The same procedure can be carried out for future sessions.

TABLE I
Notation Table

Notation	Meaning
U_i	ith user
S	Remote server
ID_i	Identity of user U_i
P_i	Password of user U_i
b_i	Random seed generated by U_i
$H(\cdot)$	Secure collusion resistant one way hash function
$h(\cdot)$	Secure collusion resistant one way Biometric hash function as in [44]
p, q	Large prime numbers
n	$n = pq$
$\|\|$	The string concatenation operation
$\oplus$	The bitwise XOR operation
e, d	e is a prime number and d is an integer, where $ed = 1\ mod\ (p-1)(q-1)$
y_i	A random value corresponding to user U_i
x	Master secret of remote server S
g	Generator for group G_p with prime order p

*2) **Key Compromise Impersonation Resilience Attack**:* A scheme is said to be secure against key compromised impersonation resilience attack if a valid user can not impersonate as another user. In the scheme [43], the attacker $\mathbb{A}$ compromise the data of patient P1 (with ID_i) and masquerade as patient P2 (with ID_j) to the server. Assume that $\mathbb{A}$ has the ID_i, PW_i, B_i, and smart card of patient P1. $\mathbb{A}$ calculates $RPW'_i = H(B_i||ID_j||PW_i)$ and update the existing f_i with $f'_i = H(RPW'_i)$. At the end of normal (as in the scheme of [43]) protocol run, smart card reader assumes that it had SK with the server for ID_j while the server assumes that it had SK with smart reader card for ID_i.

*3) **The Known Key Attack**:* A scheme is said to be secure against the known key attack if compromising the user's secret key for time T doesn't compromise the past and future sessions. In the scheme [43], attacker $\mathbb{A}$ gets the data of patient P1 for time T of some session with server S. Based on this, $\mathbb{A}$ will try to compromise the past and future sessions between P1 and server. Assume that $\mathbb{A}$ has the ID_i, PW_i, B_i, and smart card of patient P1. $\mathbb{A}$ calculates $RPW_i = H(B_i||ID_i||PW_i)$ and $e_i = RPW_i \oplus TID_i$. Afterward, for any future communication, $\mathbb{A}$ can use the e_i to get the secret values and launch the MITM attack between the smart card reader (SCR) and server S during *Login and Authentication* as follows. In this attack, we follow the notation $A \rightarrow B(C)$ that shows the message sent from A to B but received by attacker C.

- $U_i \rightarrow SCR$:
  ID_i, PW_i, B_i+ smart card
- SCR Compute RPW_i=$H(B_i|(|ID_i|)|PW_i)$. Check if $f_i = H(RPW_i)$ matches. Generate random a. Computes e_i=$RPW_i \oplus TID_i = H(ID_i||X_s)$, r_1=$a \cdot P$, $ctr_(U_i)'$=$ctr_(U_i) + 1$, M_1=$E_(e_i)(r_1||ctr_(U_i)')$, M_2=$H(ID_i|(|r_1|)|ctr_(U_i)'||NID_i)$
- $SCR \rightarrow S(\mathbb{A})$: $M_1, M_2, ctr_(U_i)', NID_i$
- $\mathbb{A}$: Gets $D_{(e_i)}(M_1) = r_1, ctr_(U_i)$. Generate a'_1, Computes r'_1=$a'_1 \cdot P$, $ctr_(U_i)'$=$ctr_(U_i) + 1$, M'_1=$E_(e_i)(r'_1||ctr_(U_i)')$, M_2=H$(ID_i||r'_1||ctr_(U_i)'||NID_i)$
- $\mathbb{A} \rightarrow S$: $M'_1, M'_2, ctr_(U_i)', NID_i$.

ISSN: 2692-5079

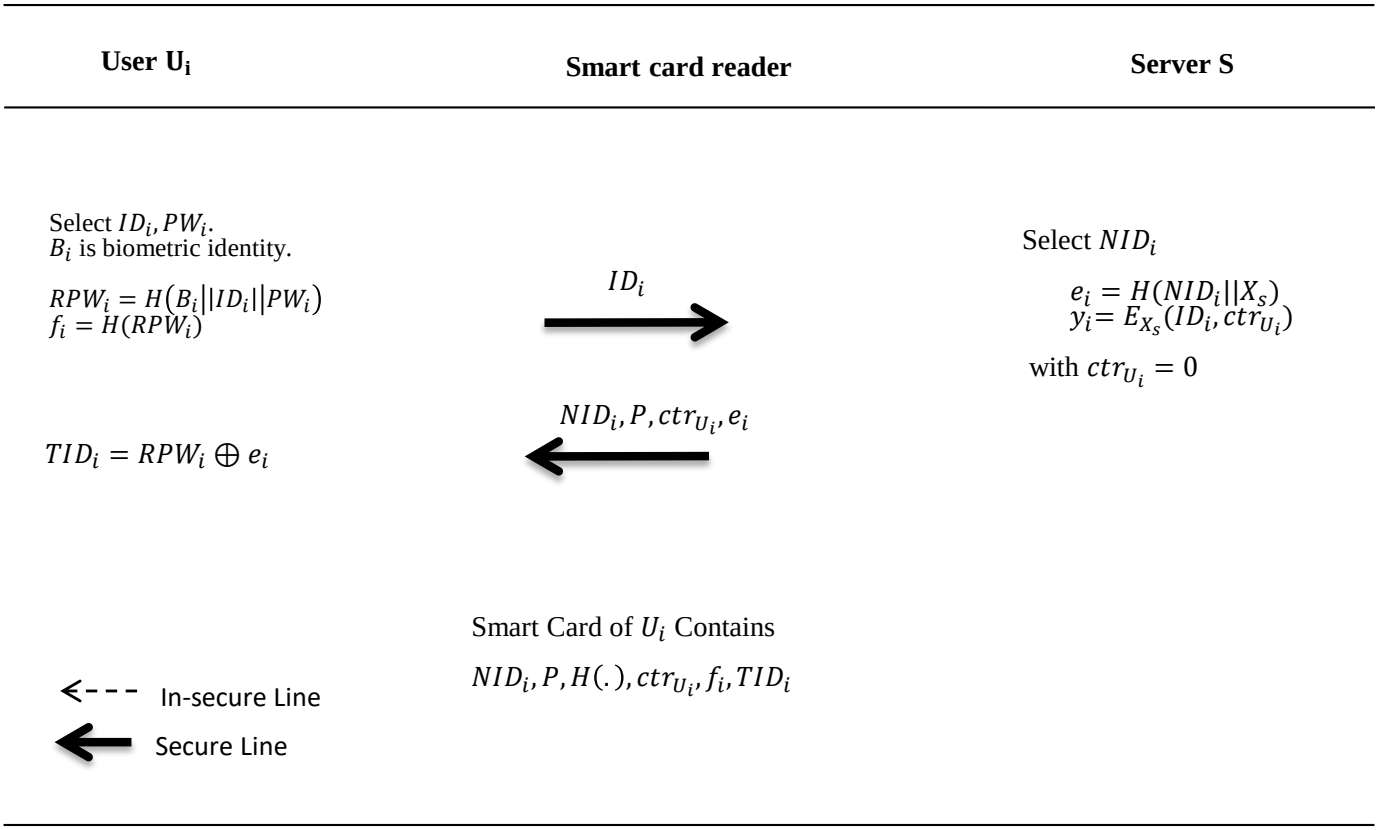

Fig. 1. Initialization Phase of Xie et al. scheme [43]

- S : Find y_i from NID_i, Computes $D_{X_s}(y_i) = ID_i, ctr_(U_i)$, Computes $H(ID_i, X_s)$. Gets $D_(H(ID_i||X_s))$, (M_1')=$r_1', ctr_(U_i)$. Check if $ctr_(U_i)' > ctr_(U_i)$ and $H(ID_i||r_1'||ctr_(U_i)'||NID_i) = M_2$. Selects random b, NID_i', $r_2 = b \cdot P$, $r = b \cdot r_1' = b \cdot a_1' \cdot P$, $M_3 = H(r_1'||r) \oplus NID_i'$, $M_4 = H(r_2||r_1'||r||NID_i')$.
- $S \rightarrow U_i(\mathbb{A})$: M_3, M_4, r_2
- $\mathbb{A}$: Computes as follows. $r = a_1' \cdot r_2 = b \cdot a_1' \cdot P$, $NID_i' = H(r_1'||r) \oplus M_3$, $M_5 = H(NID_i'||r)$, $SK_(\mathbb{A} \leftrightarrow S) = H(r_2||r_1'||r||ctr_(U_i)')$.
- $\mathbb{A} \rightarrow S$: M_5
- $\mathbb{A}$: It also computes parameters for U_i. Selects b' and existing NID_i', $r_2' = b' \cdot P$, $r' = b' \cdot r_1 = b' \cdot a_1 \cdot P$, $M_3' = H(r_1||r') \oplus NID_i'$, $M_4' = H(r_2'||r_1||r'||NID_i')$.
- $\mathbb{A} \rightarrow SCR$: M_3', M_4', r_2'.
- S : Check if $M_5 = H(NID_i'||r)$, $SK_{\mathbb{A} \leftrightarrow S} = H(r_2||r_1'||r||ctr_(U_i)')$.
- SCR : Compute as follows. $r' = a \cdot r_2' = b' \cdot a \cdot P$ $NID_i' = H(r_1||r') \oplus M_3'$, Check if $M_4' = H(r_2'||r_1||r'||NID_i')$, $M_5' = H(NID_i'||r')$, $SK_(\mathbb{A} \leftrightarrow U_i)$= $H(r_2'||r_1||r'||ctr_(U_i)')$, Update $NID_i \leftrightarrow NID_i'$ and $ctr_(U_i) \leftrightarrow ctr_(U_i)'$.
- $SCR \rightarrow U_i$:
- $SK_{(\mathbb{A} \leftrightarrow U_i)}+$ Smart Card.

In the scheme of Xie et al. [43], using only password change phase, this attack can be prevented upon detection. Whereas, in our scheme patient can run any of the three algorithm (i.e. ID change, Password change and Bio-metric change) to avoid this attack upon detection. Thus, our scheme gives more options to patient as to that of [43].

III. The Proposed Scheme

The proposed algorithms/phases of our approach are as follows.

1. ***Initialization Phase:*** server generates the public and private parameters for the system. Then server sends the required parameters to the smart card reader via a secure channel.
2. ***Registration Phase :*** User generates ID, password P, random b and sent them to the server. The server computes the parameters and gives the smart card to the user. This phase is carried out over a secure channel.
3. ***Login Phase:*** The user gives the smart card, ID to the card reader, and gets back the credentials for the *Verification phase* if authenticated otherwise session expires. This phase is carried out on an insecure channel.
4. ***Verification Phase :*** User gives the credentials obtained from *Login Phase* for particular time. Server S gives the parameters for computing session key SK if the user

ISSN: 2692-5079

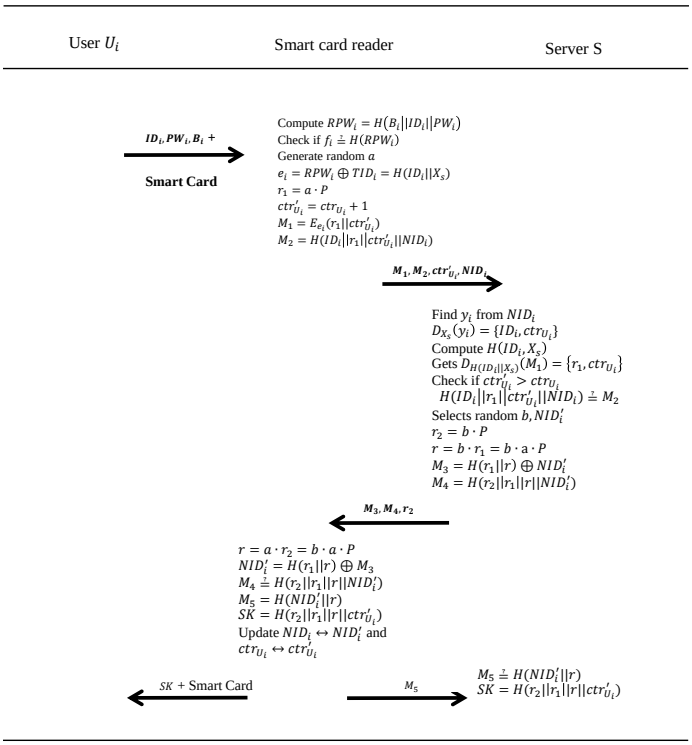

Fig. 2. Login and Authentication Phase of Xie et al. scheme [43]

authenticates within a particular time span otherwise reject. This phase is carried out on an insecure channel.

5. ***Password Change :*** User requests to re-issue smart card for ID and new password P' to server S. This phase is carried out on a secure channel.
6. ***ID Change:*** Due to some reason, if the user is compromised, he may ask for new ID' to S. S issues the smart card with parameters to the user. This phase is carried out on a secure channel.
7. ***Biometric ID Change:*** Due to some reason, if the user's biometric is lost, then he may ask for new Bio_i to S. S issues the smart card with parameters to the user. It is clear that it is nothing but some digital information that is used to match with the corresponding owner, and this can be changed by changing the algorithm to transform the biometric data captured to this digital information. This phase is carried out on a secure channel.

In the proposed scheme, we assume that there are three categories of parties involved, namely server S, smart card reader and user U_i.

A. *Initialization phase*

Step 1: Server S generates e, d, n (as in Table 1). S sends $H(.), H(d)$ and (e, n) to the smart card reader securely.

B. *Registration Phase*

Step 1: User U_i establishes the secret channel through any security mechanism.

Step 2: User U_i with identity ID_i, password PW_i and biometric identity Bio_i. U_i generates random seed r_U and computes $b_i = h(r_U \oplus Bio_i), P_i = h(PW_i||Bio_i)$ and send to S.

Step 3: Server checks for authentication and uniqueness of ID_i in internal database. If any of these checks fail then return to *Step R1*.

Step 4: Server generates random seed y_i. Compute the secret parameters as follows: N_i=$y_i \oplus H(d||H(d))$, C_i= $ID_i \oplus H(y_i||d)$. B_i=H($y_i||ID_i||d||P_i||b_i$), A_i= $P_i \oplus H(y_i||ID_i||d)$, D_i= $b_i \oplus H(P_i||y_i||d)$. Finally server S gives the smart card containing $(N_i, C_i, B_i, A_i, D_i)$ to U_i securely.

C. *Login Phase*[1]

Step 1: User U_i inserts his smart card into the card reader. Card reader extracts N_i, C_i and computes the login credentials for current time stamp T.

Step 2: Smart card generates the random seed N_u and compute the following parameters. E_i= $y_i \oplus H(d||H(d)) \oplus H(N_u||H(d))$, F_i= $ID_i \oplus H(y_i||d) \oplus H(N_u)$, G_i=${N_u}^e \bmod n$, , M_i=$H(N_u||H(d)||T)$, Smart card reader gives E_i, F_i, G_i, M_i, T to U_i.

D. *Verification Phase*

Step 1: User U_i sends $E_i, F_i, G_i, M_i, B_i, A_i, D_i, T$ and random seed N_v to server S. Here, U_i saves N_v till the session key SK is agreed.

Step 2: S takes the current time stamp T' and checks if $T' - T \leq \triangle t$, where $\triangle t$ is predefined fixed time decided by S from beginning of the system. If not then discard the request.

Step 3: S gets N_u by doing ${G_i}^d \bmod n$.

Step 4: S extracts y_i, ID_i, P_i, b_i from E_i, F_i, A_i and D_i respectively as follows. $y_i = E_i \oplus H(d||H(d)) \oplus H(N_u||H(d))$, $ID_i = F_i \oplus H(y_i||d) \oplus H(N_u)$, $P_i = A_i \oplus H(y_i||ID_i||d)$, $b_i = D_i \oplus H(P_i||y_i||d)$.

Step 5: S computes $B^* = H(y_i||ID_i||d||P_i||b_i)$ and compares with received B_i. If they are same than continued otherwise session is expire. S generates random seed Z and compute the following J_i=$Z \oplus H(P_i||b_i||N_v)$, L_i=$H(Z||P_i||ID_i||T||T'||N_v)$ and the session key SK=$H(Z||P_i||b_i||T||T')$., S sends J_i, L_i, T' to U_i.

Step 6: U_i gets $Z = J_i \oplus H(P_i||b_i)$ and computes $L' = H(Z||P_i||ID_i||T||T'||N_v)$ from Z and secret parameters. Compare L' with L_i. If they match then compute session key $SK = H(Z||P_i||b_i||T||T')$ otherwise discard the session.

[1]This phase don't require ID_i,b_i,P_i as we requires ID_i,b_i,P_i in session key SK, the off-line password guessing attack (i.e. attacker having smart card of user) is not successful.

E. *Password Change* [2]

Step 1: User U_i wants to change the password $P_i = h(PW_i||Bio_i)$ to $P_j = h(PW_j||Bio_i)$.
Step 2: U_i sends $N_i, C_i, B_i, A_i, D_i, ID_i, P_i, P_j$ and b_i to S.
Step 3: S computes ID_i, P_i and b_i from N_i, C_i, A_i, D_i and compare with received ID_i, P_i, b_i. If anyone of them failed to match then discard the request.
Step 4: S computes ${B_i}^{new} = H(y_i||ID_i||d||P_j||b_i), {D_i}^{new} = b_i \oplus H(P_j||y_i||d)$ and sends it to U_i.

F. *ID Change phase*

Let us assume that U_i with ID_i is compromised due to some reason. In this case, U_i requests for new ID_i' to S. Then S authenticates U_i and proceeds as follow.

Step 1: S adds ID_i in the forge ID list. S will check this list in every phase to avoid the attacks.
Step 2: U_i gives ID_i',P_i',b_i' to S.
Step 3: S checks if $ID_i{}'$ is already in internal database (containing assigned IDs in system) or not. If present then ask for new parameters otherwise continue.
Step 4: Server S generates y_i' and computes N_i'= $y_i' \oplus H(d||H(d))$,C_i'= $ID_i' \oplus H(y_i'||d)$, B_i'=$H(y_i'||ID_i'||d||P_i'||b_i'$, A_i'= $P_i' \oplus H(y_i'||ID_i'||d)$, $D_i' = b_i' \oplus H(P_i'||y_i'||d)$. Finally S gives the smart card containing $(N_i', C_i', B_i', A_i', D_i')$ to U_i securely.

G. *Biometric ID Change phase*

Step 1: User U_i wants to change the Biometric identity Bio_i to Bio_i'. This phase happens on secure channel.
Step 2: U_i sends $N_i, C_i, B_i, A_i, D_i, ID_i, P_i, b_i$ and b_i' to S, where $b_i' = h(Bio_i' \oplus r_U)$.
Step 3: S computes ID_i, P_i and b_i from N_i, C_i, A_i, D_i and compare with received ID_i, P_i, b_i. If anyone of them failed to match then discard the request.
Step 4: S computes ${B_i}^{new} = H(y_i||ID_i||d||P_j||b_i'), {D_i}^{new} = b_i' \oplus H(P_j||y_i||d)$ and sends it to U_i.

IV. Security and Performance Analysis

A. *Security analysis*

The security of our scheme is based on the collision resistance hash function and the integer factorization problem (as in the RSA scheme). Here we analyze the security of the proposed scheme against different attacks. Based on the techniques from [3], [20], [21], [23], an adversary $\mathbb{A}$ or user U_i can extract the parameters from the smart card.

*1) **User Anonymity**:* Assume that the adversary $\mathbb{A}$ has eavesdrop the communication in *Login Phase* and get E_i, F_i, G_i, M_i and T. However, for every request, smart reader chooses different N_u and $\mathbb{A}$ cannot determine N_u due to the integer factorization problem (if we assume that $\mathbb{A}$ have n, e). Therefore, our scheme resists against user anonymity attacks.

*2) **Off-line Password Guessing Attack**:* Assume that the adversary $\mathbb{A}$ has eavesdrop the communication in *Login Phase* and get E_i, F_i, G_i, M_i and T. In addition, we assume that $\mathbb{A}$ has smart card so that $(N_i, C_i, B_i, A_i, D_i)$. However, $\mathbb{A}$ needs to guess ID_i, P_i and b_i at the same time to get the value of session key SK after *Verification Phase*. This is not possible due to randomness of all parameters in real time scenario. Therefore, our proposed protocol is secure against offline password guessing attack.

*3) **Stolen Verifier Attack**:* If we assume that $\mathbb{A}$ have $H(d)$ due to smart card compromise attack, even then $\mathbb{A}$ cannot guess the value of d due to property of secure collusion resistance hash function. Therefore, our proposed protocol is secure against the stolen verifier attack. In most of the attacks, the scheme of [43] requires the hardness of guessing two parameters ID_i and P_i, while our proposed scheme requires guessing of three parameters ID_i, P_i and b_i. Therefore, our scheme achieves more security hardness against $\mathbb{A}$.

*4) **Key Compromise Impersonation Resilience Attack**:* As $\mathbb{A}$ (with valid parameters for ID_j) does not have value of ID_i, P_i and b_i, it cannot fabricate E_i, F_i, G_i, M_i. On the reverse side, from the values E_i, F_i, G_i, M_i values, $\mathbb{A}$ never get ID_i,P_i and b_i in polynomial time. Therefore, $\mathbb{A}$ cannot masquerade as U_i to S. Therefore our proposed protocol is secure against user impersonation attack.

*5) **Server Masquerading Attack**:* The malicious server (not having d) value cannot compute SK, as it does not have the value of ID_i, P_i, b_i and N_u corresponding to U_i. Therefore, the proposed protocol is secure against server masquerading attack.

*6) **Replay Attack and Parallel Session Attack**:* Due to the freshness of login credentials for time stamp T. $\mathbb{A}$ is not able to make a reply attack after $\triangle t$ time. If $\mathbb{A}$ start many parallel sessions with S within the same time window, even then $\mathbb{A}$ cannot guess the session key SK as ID_i,P_i and b_i are unknown to $\mathbb{A}$. Therefore, our proposed protocol is secure against a replay attack and parallel session attack.

*7) **Mutual Authentication**:* In *Verification Phase*, a user having valid ID_i, P_i and b_i can only able to compute session key and validate from L_i from S. $\mathbb{A}$ cannot have these values as it cannot have any secret parameters. S will authenticate U_i from B_i value of the smart card. It is already shown that $\mathbb{A}$ cannot masquerade as U_i or cannot do offline password guessing attack. Therefore, the proposed protocol is secure against mutual authentication attack.

*8) **Denial of Service Attack**:* Assume that the adversary $\mathbb{A}$ got the smart card of user U_i and so that the values $(N_i, C_i, B_i, D_i, A_i)$. In *Password Change* phase, S computes the ID_i, P_i and b_i then compare with user-provided values of ID_i, P_i and b_i. As $\mathbb{A}$ does have this value and is not able to guess all three values within polynomial time, S denies the request of *Password Change*. If $\mathbb{A}$ crosses the threshold number of requests, then the server automatically locks the smart card for the predefined time duration. Therefore, our proposed protocol is secure against the denial of service attack. Besides, we have used the Bio Hash [44] function h to protect against the denial of service attack as we are using biometric identity Bio_i. Additionally, if the attacker replies to

[2]As we are using the secret parameter d in the user's smart card for improved security, ID/Password/Bio_password change phase must be carried out by server only

the message at T'', it can only work till $\leq \triangle t$ time. Thus the attacker has only a small amount of time to launch the attack. In modern-day servers, "'captcha"' is used to stop automatic requesting.

*9) **Online Password Guessing Attack**:* In this attack, $\mathbb{A}$ uses the dictionary-based words to consider as ID_i, P_i and b_i and launch the attack. However, in the proposed protocol, $\mathbb{A}$ needs to get the smart card and guess ID_i, P_i, and b_i values to make this attack. Nevertheless, guessing of these three parameters is not possible in polynomial time. Therefore, our proposed protocol is secure against online password guessing attack.

*10) **Perfect Forward Secrecy**:* Assume that a long time secret key d of the server is compromised. Even then, $\mathbb{A}$ cannot get the previous SKs as N_u and Z are different for every SKs. Even more, our proposed protocol requires y_i, which is unique for each U_i. So that $\mathbb{A}$ needs to ID_i, P_i, and b_i to get the compromise of the system and previous communications. As given in the above attacks, this is not possible in polynomial time. Therefore, our proposed protocol is secure against forwarding secrecy attack.

*11) **Man-in-Middle Attack**:* We assume that $\mathbb{A}$ will be in between S and U_i and intercepts all messages that send across insecure channel. As $\mathbb{A}$ cannot know ID_i, P_i and b_i, it cannot launch any attack against U_i. Therefore, the proposed protocol is secure against the Main-In-Middle attack.

*12) **Denning Sacco Attack / The Known Key Attack**:* In this attack, we assume that $\mathbb{A}$ had intercepted all messages over an insecure channel. Besides, $\mathbb{A}$ has the SK for time T by somehow. However, $\mathbb{A}$ still cannot launch any attack or get future secret because in $J_i = Z \oplus H(P_i||b_i||N_v)$ is different for every session key due to randomness in Z and N_v. That means $\mathbb{A}$ cannot launch any attack without the knowledge of secret parameters. Therefore, our proposed protocol is secure against denning the Sacco attack.

*13) **Insider Attack**:* Users have a common tendency to make the same password at various places. Therefore, in an insider attack, if any system admin (or server S) knows the password PW_i of user i, it can compromise the other accounts of the same user. However, our proposed scheme is withstood against this attack as we are merging the biometric password with a text password and taking the hash of it. Therefore, S will not be able to know the text password in its normal form, and thus our scheme is secure against insider attack.

B. Performance analysis

In this section, we have given the performance analysis of our proposed scheme against existing schemes. Let T_{Hash}, T_{Mul} and T_{Enc} be the time requires to perform *one-way collusion resistance hash function, scalar multiplication on a elliptic curve* and *symmetric encryption/decryption function*. The time required for each operation is given in Table 2. In Table 2, we considered U_i as the number of operations by the user and smart card reader. The results from Table 2 shows that our scheme much less time as to that of existing schemes. The detailed analysis of proposed scheme against existing scheme is given in Table 3.

TABLE II
TIME REQUIRED FOR VARIOUS CRYPTOGRAPHIC OPERATIONS [45], [46]

Operation	Time in ms (milliseconds)
T_{Hash}	0.5
T_{Mul}	63.075
T_{Enc}	8.7

TABLE III
PERFORMANCE ANALYSIS OF PROPOSED SCHEME

Scheme	U_i	S	Total
[22]	$6T_{Hash}$	$4T_{Hash}$	$10T_{Hash} \approx 5ms$
[23]	$10T_{Hash}$	$7T_{Hash}$	$17T_{Hash} \approx 8.5ms$
[25]	$2T_s + 9T_{Hash}$	$2T_s + 6T_{Hash}$	$4T_s + 15T_{Hash} \approx 42.3ms$
[47]	$3T_{Mul} + 6T_{Hash}$	$3T_{Mul} + 4T_{Hash}$	$6T_{Mul}+10T_{Hash} \approx 380ms$
[48]	$3T_{Mul} + 6T_{Hash}$	$3T_{Mul} + 4T_{Hash}$	$6T_{Mul}+10T_{Hash} \approx 380ms$
[43]	$2T_{Mul}+T_{Enc}+ 7T_{Hash}$	$2T_{Mul} + 2T_{Enc} + 6T_{Hash}$	$4T_{Mul} + 3T_{Enc} + 13T_{Hash} \approx 280ms$
This scheme	$6T_{Hash}$	$8T_{Hash}$	$14T_{Hash} \approx 7ms$

V. CONCLUSION

In this paper, we have shown the scheme of [43] is vulnerable to *perfect forward secrecy, key compromise impersonation resilience attack*, and *known key attack*. Besides, due to costly scalar operations, the time requires by [43] is much more. Therefore, in this paper, we proposed the scheme to not only withstand against the mentioned attacks but also requires reduced cost as to that of [43]. Besides, we added two novel phases in the existing TMIS scheme for a biometric-based authentication scheme using smart card viz.ID change and Biometric change. Our system is a typical scenario of single authority i.e., one server generates smart cards for all the users. Thus, compromising the server's secret key d can compromise the entire system, but it is remote possibilities. One can extend our scheme to multi-authority to avoid this.

REFERENCES

[1] C. Lambrinoudakis and S. Gritzalis, "Managing medical and insurance information through a smart-card-based information system," *Journal of Medical Systems*, vol. 24, no. 4, pp. 213–234, 2000.
[2] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 12, pp. 34–41, Jan 2008.
[3] M. Das, A. Saxena, and V. Gulati, "A dynamic id-based remote user authentication scheme," *Consumer Electronics, IEEE Transactions on*, vol. 50, pp. 629–631, May 2004.
[4] Z.-Y. Wu, Y. Chung, F. Lai, and T.-S. Chen, "A password-based user authentication scheme for the integrated epr information system," *Journal of Medical Systems*, vol. 36, no. 2, pp. 631–638, 2012.
[5] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.
[6] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2012.
[7] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597–3604, 2012.
[8] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3833–3838, 2012.

[9] A. K. Awasthi, ""comment on "a dynamic id-based remote user authentication scheme"," *Transaction Cryptology*, vol. 1, pp. 15–17, May 2004.

[10] W. C. Ku and S. T. Chang, ""impersonation attack on a dynamic id based remote user authentication scheme using smart cards"," *IEICE Trans. Commun.*, vol. E88, no. B, pp. 2165–2167, 2005.

[11] Y. yan Wang, J. yong Liu, F. xia Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 32, no. 4, pp. 583 – 585, 2009.

[12] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305 – 309, 2011. Special Issue of Computer Communications on Information and Future Communication Security.

[13] H.-M. Chen, J.-W. Lo, and C.-K. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3907–3915, 2012.

[14] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 37, no. 2, 2013.

[15] F. Wen and D. Guo, "An improved anonymous authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 38, no. 5, 2014.

[16] F. Wen, "A more secure anonymous user authentication scheme for the integrated epr information system," *Journal of Medical Systems*, vol. 38, no. 5, 2014.

[17] A. Awasthi and K. Srivastava, "A biometric authentication scheme for telecare medicine information systems with nonce," *Journal of Medical Systems*, vol. 37, no. 5, 2013.

[18] A. Das and A. Goswami, "An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function," *Journal of Medical Systems*, vol. 38, no. 6, 2014.

[19] D. Mishra, S. Mukhopadhyay, S. Kumari, M. Khan, and A. Chaturvedi, "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce," *Journal of Medical Systems*, vol. 38, no. 5, 2014.

[20] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. Khan, "Cryptanalysis and improvement of yan et al.s biometric-based authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 6, 2014.

[21] X. Yan, W. Li, P. Li, J. Wang, X. Hao, and P. Gong, "A secure biometrics-based authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 37, no. 5, 2013.

[22] Y.-F. Chang, S.-H. Yu, and D.-R. Shiao, "A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 2, 2013.

[23] A. Das and A. Goswami, "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 3, 2013.

[24] K.-W. Kim and J.-D. Lee, "On the security of two remote user authentication schemes for telecare medical information systems," *Journal of Medical Systems*, vol. 38, no. 5, 2014.

[25] F. Wen, "A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 6, 2013.

[26] Z. Cai, H. Yan, P. Li, Z.-A. Huang, and C. Gao, "Towards secure and flexible ehr sharing in mobile health cloud under static assumptions," *Cluster Computing*, vol. 20, pp. 2415–2422, Sept. 2017.

[27] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," *Soft Computing*, vol. 20, pp. 3243–3255, Aug 2016.

[28] H. Yan, X. Li, Y. Wang, and C. Jia, "Centralized duplicate removal video storage system with privacy preservation in iot," *Sensors*, vol. 18, no. 6, 2018.

[29] L. Yang, Z. Han, Z. Huang, and J. Ma, "A remotely keyed file encryption scheme under mobile cloud computing," *Journal of Network and Computer Applications*, vol. 106, pp. 90 – 99, 2018.

[30] J. Xu, L. Wei, Y. Zhang, A. Wang, F. Zhou, and C. zhi Gao, "Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures," *Journal of Network and Computer Applications*, vol. 107, pp. 113 – 124, 2018.

[31] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[32] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li, "A novel security scheme based on instant encrypted transmission for internet of things,," *Security and Communication Networks*, vol. 2018, pp. 10179–10188, 2018.

[33] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial iot," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.

[34] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An id-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[35] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 2201–2210, Aug 2014.

[36] H. Tian and J. Li, "A short non-delegatable strong designated verifier signature," *Frontiers of Computer Science*, vol. 8, pp. 490–502, Jun 2014.

[37] W. Chen, H. Lei, and K. Qi, "Lattice-based linearly homomorphic signatures in the standard model," *Theoretical Computer Science*, vol. 634, pp. 47 – 54, 2016.

[38] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Information Sciences*, vol. 387, pp. 165 – 179, 2017.

[39] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Computing*, vol. 22, pp. 2257–2265, Apr 2018.

[40] Q. Liu, G. Wang, F. Li, S. Yang, and J. Wu, "Preserving privacy with probabilistic indistinguishability in weighted social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, pp. 1417–1429, May 2017.

[41] Z. Chen, L. Peng, C. Gao, B. Yang, Y. Chen, and J. Li, "Flexible neural trees based early stage identification for ip traffic," *Soft Computing*, vol. 21, pp. 2035–2046, Apr 2017.

[42] H. Shen, C. Gao, D. He, and L. Wu, "New biometrics-based authentication scheme for multi-server environment in critical systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, pp. 825–834, Dec 2015.

[43] Q. Xie, W. Liu, S. Wang, L. Han, B. Hu, and T. Wu, "Improvement of a uniqueness-and-anonymity-preserving user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 38, no. 9, 2014.

[44] L. Nanni and A. Lumini, "Random subspace for an improved biohashing for face authentication," *Pattern Recognition Letters*, vol. 29, no. 3, pp. 295 – 300, 2008.

[45] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803 – 2814, 2008. Mobility Protocols for ITS/VANET.

[46] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Computer Communications*, vol. 35, no. 2, pp. 188 – 195, 2012.

[47] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Novel anonymous authentication scheme using smart cards," *Industrial Informatics, IEEE Transactions on*, vol. 9, pp. 2004–2013, Nov 2013.

[48] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 3, 2014.