A Robust Authentication Scheme for Telecare Medicine Information Systems

Kukki Arya
Vikrant Institute of Information Technology & Management, Gwalior (MP)

Abhinav Vidwansh
Vikrant Institute of Information Technology & Management, Gwalior (MP)

ABSTRACT
The Telecare Medicine Information System (TMIS) has established a connection between patients at home and doctors at a clinical center by using telecommunication systems and physiological monitoring devices. Authentication, security, patient's privacy protection and data confidentiality are important for patient or doctors accessing to Electronic Medical Records (EMR). Remote user authentication is desirable for TMIS to verify the correctness of communicating parties. The password based authentication schemes provide efficient and scalable solutions for remote user authentication. In this context, numerous schemes have been proposed to achieve these goals. However, these schemes are vulnerable to various attacks. Moreover, they are neither efficient nor user friendly. Specially, some schemes require the exponential computation or public key cryptography which leads to very low efficiency for smart card. This paper shows that recently proposed Zhian Zhu's scheme is incorrect. Moreover, it has insecure change of password, and no early wrong password detection and session key generation. To remedy, robust authentication scheme for TMIS has been proposed using one way hash function.

Keywords
Authentication, Hash function, Password, Smart card, TMIS.

1. INTRODUCTION
In last few decades, telecare medicine information systems enable health-care delivery services due to the increased availability of lower-cost telecommunications systems. These systems are moving towards an environment where automated patient medical records and electronically interconnected telecare facilities are prevalent. It has brought us a lot of conveniences. However, it may also reveal patient`s important information. Therefore, the security of TMIS is vital. TMIS needs a more secure and more efficient authentication scheme. A secure authentication scheme is essential to guarantee that only the authorized patients or users can access the service from TMIS [1, 2, 3].

In 2010, Wu et al. [4] proposed an efficient authentication scheme for TMIS. But, He et al. [5] pointed out that Wu et al.'s scheme [4] could not resist impersonation attack and insider attack. To improve security, He et al. [5] also proposed an improved scheme. Nevertheless, Wei et al. [6] demonstrated that both of Wu et al.'s scheme and He et al.'s scheme cannot achieve two-factor authentication. To overcome the weaknesses, Wei et al. suggested a better authentication scheme for TMIS and claimed that their scheme could withstand various potential attacks. However, Zhian Zhu [7] proved that this scheme is vulnerable to off-line password guessing attack. The author also proposed a new authentication scheme for TMIS. This paper shows that Zhian Zhu's scheme is incorrect. In the authentication phase, the server cannot validate the login request message of a user. Moreover, robust authentication scheme for TMIS has been proposed using one way hash function.

The rest of the paper is organized as follows. Here, section 2 demonstrates the weaknesses of Zhu's scheme. Section 3 presents our proposed secure and efficient scheme. Security analysis and performance comparison has been done in section 4. Finally, section 5 concludes the paper.

2. WEAK SPOTS PRESENT IN ZHIAN ZHU'S [7] SCHEME
This section demonstrates the security flaws present in Zhian Zhu's [7] scheme. It is found that this scheme is incorrect. At the time of login request creation, user inserts his smart card into the card reader and inputs his password PW_i. The smart card generates a random number w_i and computes

$$PW_i' = h(PW_i||N_i),$$

$$B_i' = B_i \oplus h(PW_i') = h(ID_i \oplus d) \oplus PW_i' \oplus h(PW_i'),$$

$$h_i = h(B_i'||w_i) = h((h(ID_i \oplus d) \oplus PW_i' \oplus h(PW_i'))||w_i) \quad (1)$$

$$X_i = (h_i||w_i)^e \bmod n$$

After computing the necessary parameters, user sends the login request $\{ID_i, X_i\}$ to the TMIS server. Upon receiving, server validates ID_i. If true, server computes

$$(h_i||w_i) = (X_i)^d \bmod n,$$

$$h_i' = h(h(ID_i \oplus d)||w_i) \quad (2)$$

It verifies whether received h_i and computed h_i' are equal or not. From eq. (1) and eq. (2), it is clear that h_i and h_i' are not equal. In addition, following are the limitations of this scheme:

- No secure change of password
- No early wrong password detection
- No session key generation

3. PROPOSED AUTHENTICATION SCHEME FOR TMIS AGAINST SMART CARD SECURITY BREACH
This section proposes authentication scheme using smart card. The given scheme has all the merits of Zhian Zhu's scheme and also provides security even if attacker gets user's smart card and extracts the stored data in it. The notations used throughout this paper are summarized in Table 1.

Table 1. Notations used in this paper

Symbols	Their Meaning
U_i	Patient or User
S	Server at TMIS
SC	Smart Card
ID_i	Identifier of U_i
PW_i	Password of U_i
X_s	Secret key of S
P	Large prime number such that (p-1) has at least one large prime factor
G	Primitive element over Finite Field GF(p)
$\oplus$	Bitwise XOR operation
h(•)	Cryptographic one way hash function
N_u	Random nonce generated by U_i
N_s	Random nonce generated by S
SKey	Shared session key

Before going through the inner details of the proposed scheme, the flow diagram (as shown in Fig. 1) is given to show the activities and actions in order to describe the workflow.

3.1 Registration Phase

To avail the facilities or services provided by the TMIS server, each user has to first register with it. In this phase, U_i chooses ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to S over a secure channel. Upon receiving the registration request, S computes

$$\alpha_i = h(X_s)$$

$$\beta_i = \alpha_i \oplus h(ID_i||h(PW_i))$$

and issues a smart card over secure channel to U_i by storing the necessary parameters $\{\alpha_i, \beta_i, h(\bullet)\}$ into smart card memory.

3.2 Login and Authentication Phase

The login and authentication phase is shown in Fig. 2. In this phase, when a legal user wants to login into the TMIS and access some EMR data or services, he or she has to insert the smart card to the terminal and keys in ID_i' and PW_i'. The terminal computes $\beta_i' = \alpha_i \oplus h(ID_i'||h(PW_i'))$ and verifies whether β_i (stored in the smart card memory) and β_i' are equal or not. If true, U_i is the legitimate bearer of smart card otherwise, rejects the login request. Then, the terminal generates a random nonce N_u, computes

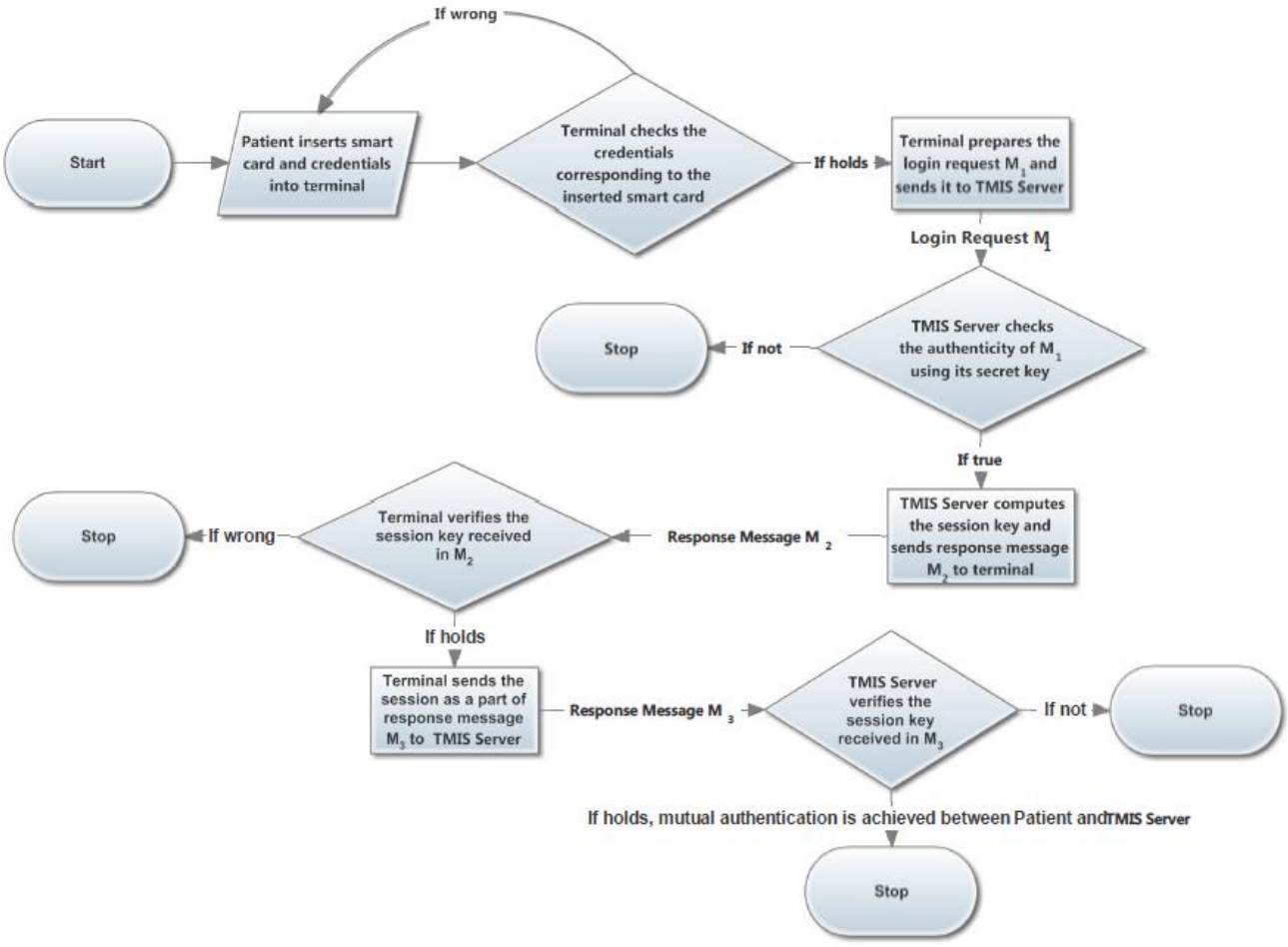

Fig 1: Flow diagram of proposed authentication scheme for TMIS

$$\gamma_i = N_u \oplus \alpha_i$$

$$LA_1 = h(PW_i') \oplus h(\alpha_i||N_u)$$

$$LA_2 = h(PW_i') \oplus \alpha_i$$

$$LA_3 = h(LA_2||N_u||\beta_i)$$

and sends the login request $M_1 = \{ID_i, LA_1, LA_3, \gamma_i\}$ to the server S. Upon receiving the login request M_1; S first checks the validity of ID_i to accept/reject the login request. If true, S computes

$$\alpha_i = h(X_s)$$

$$N_u = \gamma_i \oplus \alpha_i$$

$$h(PW_i') = LA_1 \oplus h(\alpha_i||N_u)$$

$$LA_2' = h(PW_i') \oplus \alpha_i$$

$$\beta_i' = \alpha_i \oplus h(ID_i'||h(PW_i'))$$

$$LA_3' = h(LA_2'||N_u||\beta_i')$$

and checks whether LA_3 and LA_3' are equal or not. If they are not equal then rejects the login request otherwise generates a random nonce N_s, computes

$$\gamma_s = N_s \oplus \alpha_i$$

$$SKey = h(ID_i||LA_2'||N_u||N_s||\beta_i')$$

$$LA_4 = h(SKey||\alpha_i||\beta_i'||N_u||N_s)$$

and sends the response message $M_2 = \{ID_i, LA_4, \gamma_s\}$ to the terminal U_i. After getting the message M_2 from S, terminal computes

$$N_s = \gamma_s \oplus \alpha_i$$

$$SKey = h(ID_i||LA_2||N_u||N_s||\beta_i')$$

$$LA_4' = h(SKey||\alpha_i||\beta_i'||N_u||N_s)$$

and verifies whether LA_4 and LA_4' are equal or not. If it holds, S is authentic and the session key is fresh otherwise, terminates the session. Subsequently, terminal computes

$$LA_5 = h(SKey||\alpha_i||N_s||\beta_i')$$

and sends $M_3 = \{ID_i, LA_5\}$ to the server S. Once the message M_3 is received, S computes

$$LA_5' = h(SKey||\alpha_i||N_s||\beta_i')$$

and verifies whether LA_5 and LA_5' are equal or not. If it holds, mutual authentication is achieved between U_i and S. Both the parties agree upon a common shared session key $SKey = h(ID_i||LA_2||N_u||N_s||\beta_i) = h(ID_i||LA_2||N_u||N_s||\beta_i')$ for further communication.

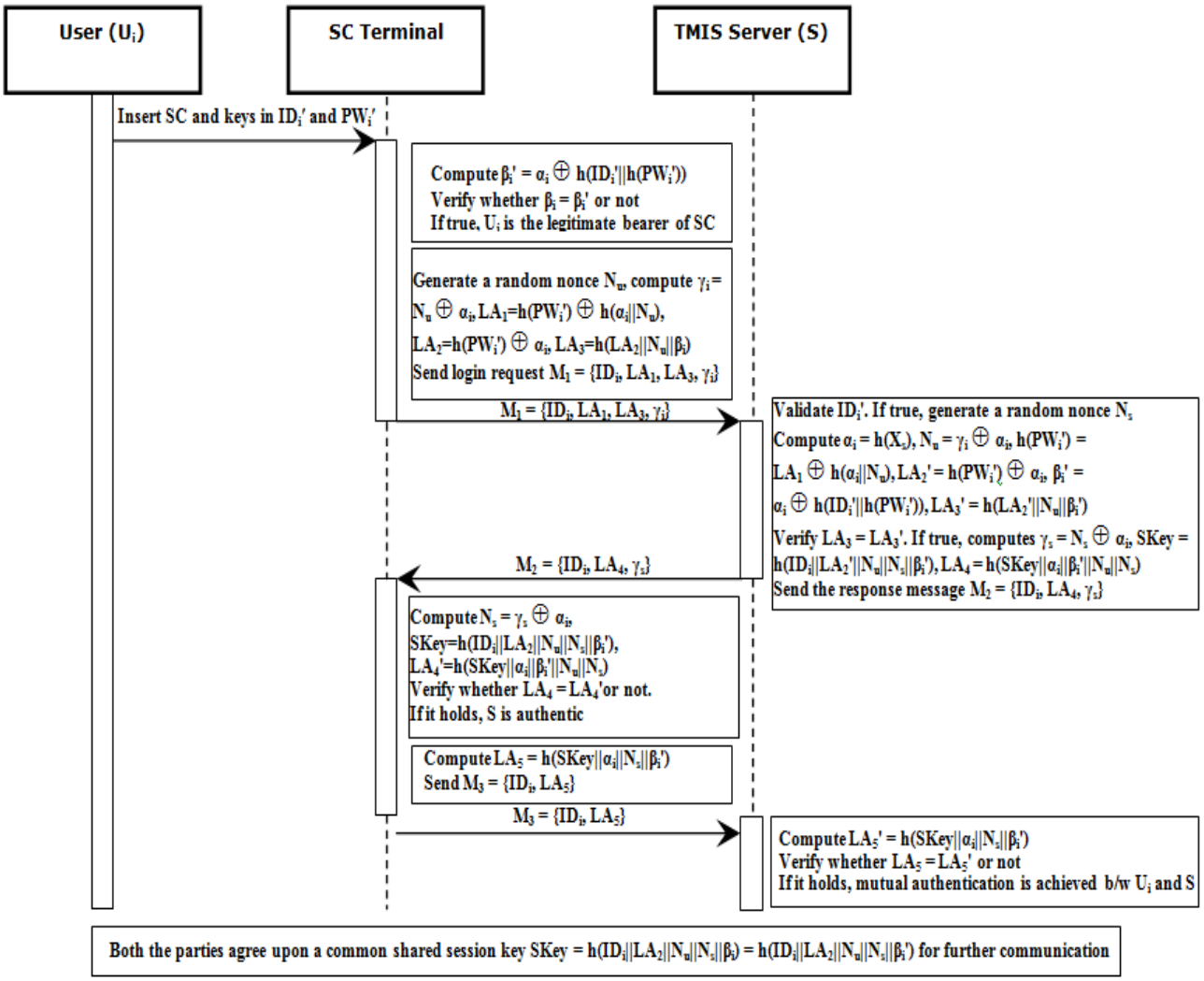

Fig 2: Login and Authentication phase of proposed smart card authentication scheme

3.3 Password Updating Phase

This phase is invoked when U_i wants to change the password. For this, U_i inserts the smart card to the terminal and keys in ID_i' and PW_i'. The terminal computes

$$\beta_i' = \alpha_i \oplus h(ID_i'||h(PW_i'))$$

and verifies whether β_i and β_i' are equal or not. If true, U_i is the authorized owner of smart card. Now, the terminal prompts U_i to enter a new password. U_i enters new password PW_{inew}. The terminal computes

$$\beta_{inew} = \alpha_i \oplus h(ID_i'||h(PW_{inew}))$$

and stores β_{inew} in place of β_i in the smart card memory. Thus, U_i can change the password without any assistance from S. To resist online-password guessing attack, the scheme limits the number of attempts up to limited number of times.

4. SECURITY ANALYSIS

An ideal authentication scheme must support both mutual authentication and session key establishment. This section discusses an in-depth security analysis of proposed authentication scheme for TMIS. It considers the following potential attacks, i.e. impersonation attack, offline and online password guessing attacks, replay attack, privileged insider attack and attack on perfect forward secrecy. It is assumed that (i) the attacker has the potential to eavesdrop any communicated message transmitted between U_i and S and (ii) the attacker may extract all secrets stored in the smart card memory by physically monitoring its power consumption. Finally, it gives functionality comparison of proposed scheme with previous authentication schemes used in TMIS.

4.1 Guarding against Potential Attacks and provides Essential Features

4.1.1 Impersonation Attack

In this scheme, the login request contains $M_1 = \{ID_i, LA_1, LA_3, \gamma_i\}$, where $LA_1 = h(PW_i') \oplus h(\alpha_i||N_u)$, $LA_2 = h(PW_i') \oplus \alpha_i$, $LA_3 = h(LA_2||N_u||\beta_i)$. Hence, to attacker needs the value of α_i, N_u and β_i' to forge which are not a part of any of the transmitted messages between user U_i and the server S.

4.1.2 Offline and Online Password Guessing Attacks

Usually, users have a tendency to choose weak passwords which are simple to recollect. As a result, these easy-to-remember passwords are potentially susceptible to password guessing attacks. In the proposed scheme, PWi is not employed in the computation of any of the communicated message parameters. It implies that the password and the messages are completely independent. Consequently, the attacker is unable to extract PW_i from the eavesdropped login and response messages transmitted between S and U_i. In this scheme, $h(PW_i)$ is used only in the calculation of LA_1. Attackers need the value of α_i and N_u to check whether each of their guessed passwords is correct or not. To resist online password guessing attack, the smart card will be locked if U_i enters wrong password more than limited number of times.

4.1.3 Replay Attack

An adversary may attempt to act as an authentic administrator by resending previously intercepted messages. This scheme employs random nonce N_u and N_s which are totally different from session to session. As a result, attackers cannot enter the system by resending the previously transmitted messages to impersonate U_i. Hence, attacker has no way to mount replay attack and the presented scheme is free from this vulnerability.

4.1.4 Privileged Insider Attack

For remembrance, many users employ same password to access different servers. Nevertheless, a privileged insider of server can get this password and then try to utilize it for personal benefit. During the registration phase of the proposed scheme, U_i sends $h(PW_i)$ to S instead of PW_i in a plain text in order to resist insider attack. Hence, this scheme provides security against privileged insider attack.

4.1.5 Attack on Perfect Forward Secrecy

It is essential for both the communicating parties to establish a session key to be used for protecting their subsequent communications. Perfect Forward Secrecy (PFS) tells that even though the current session key is revealed it does not facilitate the attacker to compromise the session keys of earlier sessions. In the proposed scheme, the session key, $SKey = h(ID_i||LA_2||N_u||N_s||\beta_i) = h(ID_i||LA_2||N_u||N_s||\beta_i')$, is totally different among sessions due to the employment of randomly generated nonce N_u and N_s. Even if an attacker gets X_s, server's secret key, there is no way to get any information about present session key or previous session keys. Hence, the scheme provides PFS.

4.1.6 It allows users to choose and change the password freely as well as securely

It is difficult to memorize the system generated passwords. Hence, the scheme must provide the facility to choose the password. To extend efficiency, password can be changed freely at any time without any interaction with the server or the verifier. In the proposed scheme, U_i can choose and change the password securely by proving authenticity at the smart card level itself without any assistance from S. It eliminates the role of S throughout password change phase. Password change at the U_i side strengthens the security.

4.1.7 It provides early wrong password detection

To check whether or not the requested entity is a legitimate bearer of smart card, entered password must be verified at the smart card level prior to login request creation. In order to forestall Denial-of-Service attack, the proposed scheme quickly verifies the legitimacy of the users at the time of creating login request by comparing β_i' with the stored β_i. It creates a login request only when smart card finds entered password correct. Hence, it avoids unnecessary burden on the TMIS server.

4.2 Functionality comparison of proposed scheme with previous authentication schemes used in TMIS

In order to measure the functionality of proposed scheme, it is compared with the previous authentication schemes used in TMIS (see Table 2 and Table 3). It can be clearly seen that the given scheme keeps all the previous advantages and achieves the security and functionality requirements.

In order to analyze the computational complexity of the schemes, we define t_s, t_e, t_{inv}, t_h and t_m be the time cost of one scalar multiplication in a group, one modular exponentiation in Z_p, one inverse operation in Z_q, one hash operation and one modular multiplication in Z_q, respectively. As mentioned in [8, 11], the time cost of all operations satisfies the following: $T_s \approx 29t_h$, $t_h \approx t_m$ and $t_e \approx t_{inv} \approx 240t_m$.

Table 2. Comparison of proposed scheme with existing authentication schemes used in TMIS

Security Properties	**Proposed Scheme**	**Zhian Zhu's Scheme [7]***	**Wei et al.'s Scheme [6]**	**He et al.'s Scheme [5]**	**Wu et al.'s Scheme [4]**
User is allowed to choose and change the password	Yes	Yes	Yes	Yes	Yes
Secure change of password	Yes	***No***	***No***	***No***	***No***
Provides mutual authentication	Yes	Yes	Yes	Yes	Yes
Provides early wrong password detection	Yes	***No***	***No***	***No***	***No***
Provides session key generation	Yes	***No***	Yes	Yes	Yes
Resists impersonation attack	Yes	Yes	Yes	Yes	***No***
Resists guessing attack	Yes	Yes	***No***	***No***	***No***
Resists replay attack	Yes	Yes	Yes	Yes	Yes
Resists privileged insider attack	Yes	Yes	Yes	Yes	***No***

Table 3. Comparison of proposed scheme in terms of computational complexity

		Proposed Scheme	**Zhu's Scheme [7]***	**Wei et al.'s Scheme [6]**	**He et al.'s Scheme [5]**	**Wu et al.'s Scheme [4]**
Registration phase	Smart card	t_h	t_h	t_h	t_h	0
	Server	$2t_h$	t_h	$t_e \approx 240t_h$	$t_e+t_{inv}+t_h \approx 481t_h$	$3t_e+t_{inv}+2t_m \approx 962t_h$
Login and authentication phase	Smart card	$7t_h$	$t_e+4t_h \approx 244t_h$	$t_e+6t_h+T_s \approx 275t_h$	$t_e+t_{inv}+5t_h+t_m \approx 486t_h$	$4t_h+3t_m \approx 7t_h$
	Server	$7t_h$	$t_e+4t_h \approx 244t_h$	$t_e+t_{inv}+5t_h+T_s \approx 514t_h$	$t_e+t_{inv}+4t_h \approx 484t_h$	$t_e+4t_h \approx 244t_h$
Password update	Smart card	$4t_h$	$2t_h$	$2t_h$	$t_e+t_{inv}+2t_h+t_m \approx 483t_h$	$2t_e+2t_{inv}+2t_m \approx 962t_h$

5. CONCLUSION

Recently, Zhian Zhu [7] proposed an efficient authentication scheme for TMIS. The author claimed that the scheme provides mutual authentication and is able to resist privileged insider attack, password guessing attack, impersonation attack, stolen verifier attack, replay attack and man-in-the-middle attack. Nevertheless, this paper demonstrated that the scheme presented by Zhian Zhu [7] is incorrect. In addition, it has insecure change of password, and no early wrong password detection and session key generation. To remedy, robust authentication scheme for TMIS has been proposed which has the following merits:

- Users can choose their own passwords and need not to remember server generated passwords.
- They can change their passwords freely at the smart card level without any assistance from the server.
- The scheme provides security against impersonation attack, online and offline password guessing attack, replay attack and privileged insider attack.
- The scheme offers early wrong password detection, mutual authentication, secure session key establishment and overcomes the time synchronization problem.

Security analysis proves that the proposed scheme is highly secure and can be used for practical applications. Moreover, comparative result has also been presented on the basis of various security features provided and vulnerabilities present in the existing authentication schemes proposed for TMIS.

6. REFERENCES

[1] Adamsk, T., Winiecki, W., Entity identification algorithms for distributed measurement and control systems with asymmetry of computational power, Prz Elektrotechniczn,(2008),No. 05

[2] Cheng, X.R., Li, M.X., The authentication of the grid monitoring system for wireless sensor networks, Prz Elektrotechniczn, (2013),No.01a

[3] Pejaś, J., El Fray , I., Ruciński, A., Authentication protocol for software and hardware components in distributed electronic signature creation system, Prz Elektrotechniczn, (2012),No.10b

[4] Wu, Z. Y., Lee, Y. C., Lai, F., Lee H. C., and Chung, Y., "A secure authentication scheme for telecare medicine information systems", Journal of Medical Systems (Springer). DOI: 10.1007/s10916-010-9614-9, 2010.

[5] He, D. B., Chen, J. H., and Zhang, R., "A more secure authentication scheme for telecare medicine information systems", Journal of Medical Systems (Springer). DOI:10.1007/s10916-011-9658-5, 2011.

[6] Wei, J., Hu, X., Liu, W., "An Improved Authentication Scheme for Telecare Medicine Information Systems", Journal of Medical Systems (Springer). DOI:10.1007/s10916-012-9835-1, 2012.

[7] Zhian Zhu, "An Efficient Authentication Scheme for Telecare Medicine Information Systems", Journal of Medical Systems (Springer). DOI: 10.1007/s10916-012-9856-9, 2012.

[8] Fan, Ch.-I. Sun, Huang, W. Z., Vincent, S.-M.,Provably secure randomized blind signature scheme based on bilinear pairing,Comput Math Appl, 2010, No.60,285–293

[9] Koblitz, N., Menezes, A.J., Vanstone, S.A.,The state of elliptic curve cryptography, Design Code Cryptogr, (19)2000, No.2-3, 173–193

[10] Xue,K.M.,Hong, P.L., Security improvement on an anonymous key agreement protocol based on chaotic maps, Commun Nonlinear Sci Numer Simulat, 2012, No.17, 2969–2977

[11] Menezes, A., Van Oorschot, P. C., Vanstone, S. Handbook of Applied Cryptography, CRC Press, USA, 1997.