International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8805-8811

Three Party Authentication Scheme with Privacy in Telecare Medicine Information Systems

Hee Joo Park*

[*]Department of Cyber Security, Kyungil University, Kyungsan, Kyungbuk 712-701, Korea.

**Orcid ID: 0000-0002-1348-2999*

Abstract

Telecare medicine information systems (TMISs) provide patients at home, doctors at clinical centers and home health care agency with accessing electronic medical records securely, conveniently and efficiently. However, there are many security issues such as patient privacy and data integrity in TMISs. To support the issue, Lin et al. proposed two three party authentication schemes. First of all, this paper shows Lin et al.'s schemes have privacy problem, which is one of the most important issue in TMISs. Furthermore, we propose a new three party authentication scheme with privacy support in TMISs. Compare to the related schemes, the proposed scheme possesses higher security and privacy and has fewer transmissions. Thereby, it is suitable for the TMISs.

Keywords: Telecare medicine information system, Security, Privacy, Three party authentication.

INTRODUCTION

Telecare medical information systems (TMISs) are a good way to bring telemedicine directly into patients' homes. The medical server in TMISs should protect various private data and information of registered users, such as their names and electronic medical records. The main problem that researchers face when deploying TMIS is ensuring the security and privacy of important patient data [1-4]. Three party authentication schemes for data exchange in TMISs enable two users in hospitals and medical institutes negotiate a secure communication channel by establishing a secure session key via the help of the authentication server. Then these two entities can exchange medical data securely and conveniently as shown in Fig. 1.

Recently, many three party authentication schemes were proposed [5-]. Lee et al. proposed an efficient verifier based three party authentication scheme, which does not require server public key [5]. Wang et al. proposed a modified scheme in order to overcome the weakness in Lee et al.'s scheme [6]. Additionally, Kwon et al. proposed a round efficient and secure scheme, which does not provide key confirmation [7].

Especially focused on TMIS security, Wu et al. proposed a secure authentication scheme, which adds precomputation of exponentiation operations [8]. However, He et al. pointed out that Wu et al.'s scheme could not resist insider attacks and impersonation attacks [9]. Then, Wei et al. showed that He et al.'s scheme is vulnerable because it could not resist off-line password guessing attacks, and they also proposed an improved scheme [10]. Islam et al. found that Wu et al.'s scheme was still vulnerable to the privileged insider attack, off-line password guessing, and ephemeral secret leakage [11]. Lin et al. proposed a verifier based three party authentication scheme to provide high efficiency and security, along with low computation and transmission costs [12].

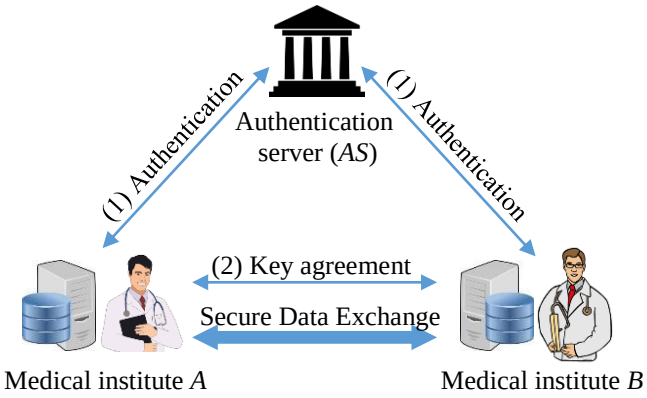

Figure 1: Three party authentication schemes in TMIS

The purpose of this paper is to propose a privacy enhanced authentication scheme based on Lin et al.'s authentication scheme. To do this, this paper first reviews Lin et al.'s authentication scheme in detail and shows it does not provide anonymity and untraceability. Then we will propose a new three party authentication scheme with privacy concern in TMIS. Analysis shows that the proposed scheme could efficiently solve the privacy concerns in Lin et al.'s scheme.

This paper is organized as follows. Section 2 reviews the related works focused on Lin et al.'s three party authentication scheme and pointed out the privacy issues on it. A new three party authentication scheme with privacy in TMIS is proposed to solve the privacy concerns in Lin

et al.'s scheme at Section 3. Analyses and conclusion are given in Sections 4 and 5, respectively.

RELATED WORKS

This section reviews Lin et al.'s three party authentication scheme without server public keys for data exchange in TMISs and withdraws privacy issues in it [12]. Table 1 lists the notations used throughout this paper.

Table 1: Notations

Symbol	Description
p, g	A large prime p and a generator g in group Z_p^*
π_i, v_i	A password π_i and a verifier v_i of an entity i
$h(\cdot)$, $H(\cdot)$	Collision free one way hash functions
DID_i	A dynamic identifier of an entity i
$A \rightarrow B$: M	A sends message M to B through a common channel
M_i	A message i
$\oplus$	Exclusive OR operation

Lin et al.'s Three Party Authentication Scheme

Initially, A and B sends their verifiers to AS via s secure and verified channel to register their verifiers. For this, A shares verifier $v_A=g^{tA}$ mod p for password π_A and B shares verifier $v_B=g^{tB}$ mod p for password π_B with AS, respectively, where $t_A=H(A, AS, \pi_A)$ and $t_B=H(B, AS, \pi_B)$.

When entities want to communicate with each other, they needs to be authenticated with each other and to establish a secure channel by agreeing session key. For this, two entities A and B perform a mutual authentication with AS and each other with a key agreement. The detailed steps are as follows

Step 1. $A \rightarrow AS$: $[A, B, X_A]$

A selects $a \in_R Z_p^*$, computes $X_A=g^a$ mod p and sends $[A, B, X_A]$ to AS.

Step 2. $AS \rightarrow B$: $[X_A, X_{SA}, X_{SB}]$

AS selects c, $d \in_R Z_p^*$, and uses v_A and v_B to compute $X_{SA}=(v_A)^c \oplus v_A$ mod p and $X_{SB}=(v_B)^d \oplus v_B$ mod p. Then AS sends $[X_A, X_{SA}, X_{SB}]$ to B and computes g^c, g^d, $K_{SA}=(X_A)^c=g^{ac}$ mod p and $K_{SB}=(X_B)^d=g^{bd}$ mod p.

Step 3. $B \rightarrow A$: $[X_B, X_{SA}, V_{BS}, \mu_{BA}]$

B selects $b \in_R Z_p^*$, and computes $X_B=g^b$ mod p, $K_{BA}=(X_A)^b=g^{ab}$ mod p, $g^d=(X_{SB} \oplus v_B)^{tB-1}$ mod p, $K_{BS}=(g^d)^b=g^{bd}$ mod p, $V_{BS}=h(B, A, AS, X_B, X_A, g^d, K_{BS})$ and $\mu_{BA}=h(B, A, X_B, X_A, K_{BA})$, where $t_B=h(B, AS, \pi_B)$ and sends $[X_B, X_{SA}, V_{BS}, \mu_{BA}]$ to A.

Step 4. $A \rightarrow AS$: $[V_{AS}, V_{BS}, \mu_{AB}]$

A computes $g^c=(X_{SA} \oplus v_A)^{tA-1}$ mod p, $K_{AS}=(g^c)^a=g^{ac}$ mod p, $V_{AS}=h(A, B, AS, X_A, X_B, g^c, K_{AS})$ and $K_{AB}=(X_B)^a=g^{ba}$ mod p. If A successfully verifies μ_{BA}, A computes $\mu_{AB}=h(A, B, X_A, X_B, K_{AB})$ and sends $[V_{AS}, V_{BS}, \mu_{AB}]$ to AS.

Step 5. $AS \rightarrow B$: $[V_{SA}, V_{SB}, \mu_{AB}]$

If AS successfully verifies V_{AS} and V_{BS}, then computes $V_{SA}=h(AS, A, X_A, X_B, K_{SA})$ and $V_{SB}=h(AS, B, X_B, X_A, K_{SB})$ and sends $[V_{SA}, V_{SB}, \mu_{AB}]$ to A.

Step 6. $B \rightarrow A$: $[V_{SA}]$

If B successfully verifies μ_{AB} and V_{SB}, then sends $[V_{SA}]$ to A. Finally, A verifies V_{SA}.

Therefore, A and B have a common session key $SK=h(A, B, AS, K_{AB})=h(A, B, AS, K_{BA})$.

Privacy Issue of Lin et al.'s Scheme

Within many kinds of privacy right, patient privacy for TMIS is calling more and more attentions. As natural existence, the privacy is part of the social life, the patient's state of illnesses and physical condition is regarded as the private information, hence it needs to be achieved the right privacy [13-14]. TMIS has duty to protect the patients' privacy. Privacy in TMISs comprises anonymity and unlinkability. They could be defined as follows

- Anonymity : it means the electronic medical records must be hidden from insurance providers, researchers, management staff, and any other related personnel who have no appropriate access privileges
- Unlinkability : it indicates that multiple electronic medical records cannot be linked to the same owner to prevent the profiling of a patient

In the course of having or being part of a medical practice, any entity in TMIS may learn information they wish to share with the medical or research community. If this information is shared or published, the privacy of the patients must be respected. Likewise, participants in TMIS that are outside the realm of direct patient care have a right to privacy as well. In this way, the application must

guarantee a well defined degree of privacy with precisely formulated and verified rules.

However, Lin et al.'s scheme could not provide anonymity nor unlinkability due to the exposure of TMIS entities identities. Especially, step 1 of Lin et al.'s scheme requires $A \rightarrow AS$: [A, B, X_A] where A and B are identifiers of the entities in TMIS. Thereby, we can conclude that Lin et al.'s scheme does not provide privacy.

NEW THREE PARTY AUTHENTICATION SCHEME WITH PRIVACY SUPPORT

In this section, we propose a new three party authentication scheme with privacy support in TMIS to solve the problems in Lin et al.'s scheme. The proposed scheme uses dynamic identifier DID_i instead of real identifier to provide anonymity and untraceability. For this, the proposed scheme uses a server side verification table as shown in Table 2. It uses two dynamic identifiers, which are the current one, DID_i and the previous one $PDID_i$.

Table 2: Verification Table

Verifier	Dynamic Identifier	Previous Dynamic Identifier
v_A	DID_A	$PDID_A$
v_B	DID_B	$PDID_B$

Initial Registration

For the system parameter setup, initially, *AS* chooses a large prime number p and a primitive root g in a group Z_p^*. All registrations are carried out by *AS* via a secure channel. A and B send their verifiers with their dynamic identities to *AS* for the registration. For this, A shares the verifier $v_A=g^{tA} \bmod p$ for password π_A and $DID_A=h(A, v_A, 0)$ and B shares the verifier $v_B=g^{tB} \bmod p$ for password π_B and $DID_B=h(B, v_B, 0)$ with *AS*, respectively, where $t_A=H(A, AS, \pi_A)$ and $t_B=H(B, AS, \pi_B)$. *AS* stores v_A and DID_A for A and v_B and DID_B for B.

Authentication and Key Agreement

When entities want to communicate with each other, they needs to be authenticated with each other and to establish a secure channel by agreeing a session key. For this, two entities A and B perform a mutual authentication with *AS* and each other with a key agreement. The detailed steps are as follows:

Step 1. $A \rightarrow B$: [DID_A, X_A, V_{AS}]

A selects $a \in_R Z_p^*$, computes $X_A=g^a \bmod p$ and $V_{AS}=h(DID_A, AS, X_A, v_A)$, and sends [$DID_A$, X_A, V_{AS}] to B.

Step 2. $B \rightarrow AS$: [DID_A, X_A, DID_B, X_B, V_{BS}]

B selects $b \in_R Z_p^*$, and computes $X_B=g^b \bmod p$ and $V_{BS}=h(DID_B, AS, X_B, v_B, V_{AS})$, and sends [$DID_A$, X_A, DID_B, X_B, V_{BS}] to *AS*.

Step 3. $AS \rightarrow B$: [X_{SA}, V_{SA}, X_{SB}, V_{SB}]

AS uses v_A and v_B to verify V_{BS} and finishes the request if it fails the verification. Otherwise, *AS* compute $X_{SA}=(X_A)^c \oplus v_A \bmod p$, $X_{SB}=(X_B)^d \oplus v_B \bmod p$, $V_{SA}=h(DID_A, AS, (X_A)^c, v_A)$ and $V_{SB}=h(DID_B, AS, (X_B)^d, v_B)$. Then *AS* sends [$X_{SA}$, V_{SA}, X_{SB}, V_{SB}] to B.

Step 4. $B \rightarrow A$: [X_{SA}, V_{SA}, X_B, V_{BA}, V_B]

B computes $(X_B)^d=X_{SB} \oplus v_B$ and verify V_{SB}. Only if the verification is successful, B computes $K_{BA}=(X_A)^b=g^{ab} \bmod p$, $V_{BA}=h(X_A, X_B, K_{BA}, V_{SA})$ and $V_B=h(X_A, X_B, (X_B)^d, v_B)$, and sends [$X_{SA}$, V_{SA}, X_B, V_{BA}, V_B] to A.

Step 5. $A \rightarrow AS$: [V_A, V_B]

A computes $(X_A)^c=X_{SA} \oplus v_A$ and verify V_{SAB}. Only if the verification is successful, A computes $K_{AB}=(X_B)^a=g^{ba} \bmod p$ and verify V_{BA}. If the verification is successful, A computes $V_A=h(X_A, X_B, (X_A)^c, v_A)$ and sends [V_A, V_B] to *AS*. Finally, *AS* verifies V_A and V_B.

Therefore, A and B have a common session key $SK=h(DID_A, DID_B, AS, K_{AB})=h(DID_A, DID_B, AS, K_{BA})$. Only after the success of this phase, A updates DID_A with $h(DID_A, v_A, (X_A)^c)$ and B updates DID_B with $h(DID_B, v_B, (X_B)^d)$ and *AS* does the same operations as A and B right after they update $PDID_i$ with DID_i, respectively.

Fig. 2 shows the overview of authentication and key agreement for the proposed three party authentication scheme with privacy support.

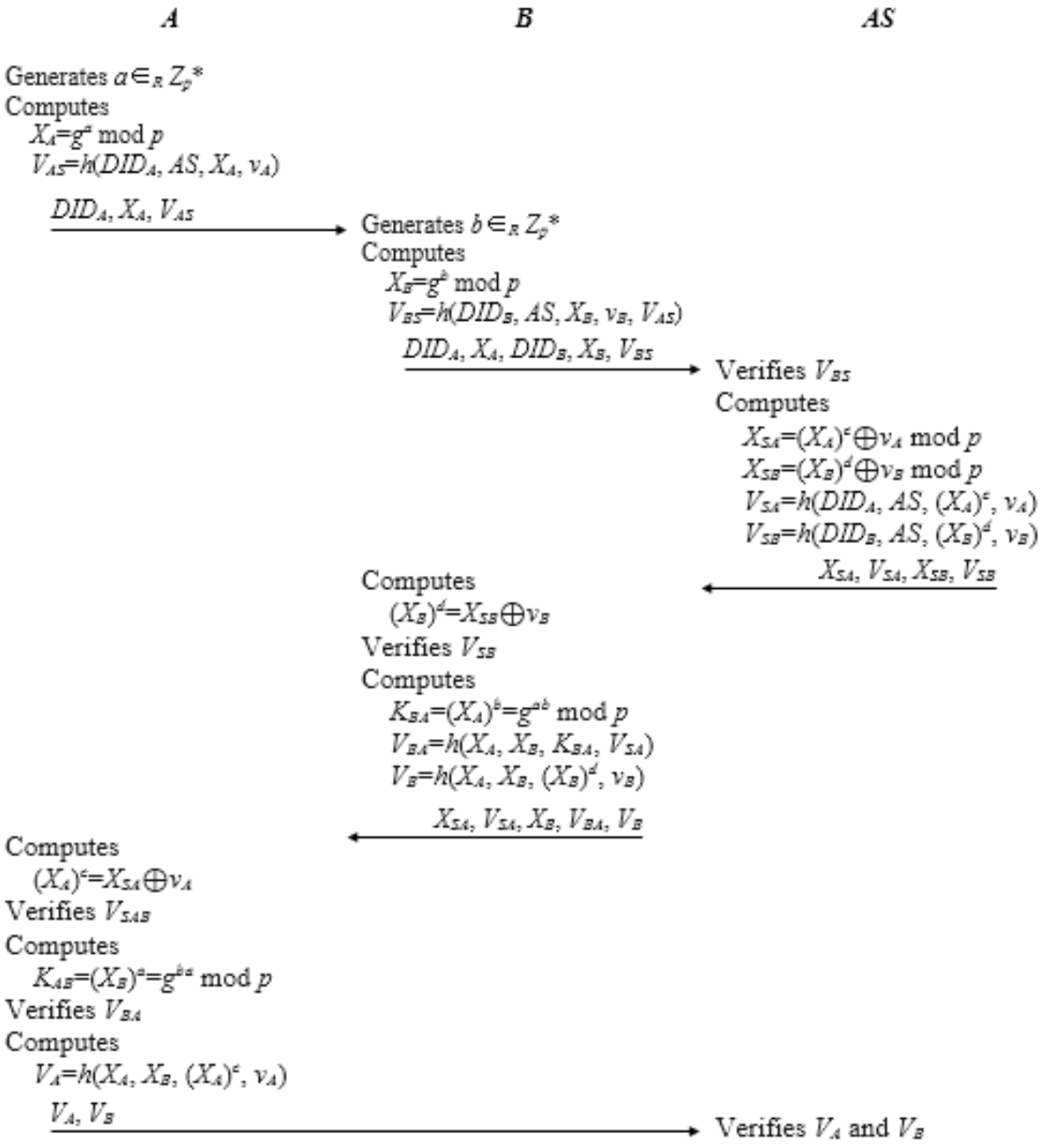

Figure 2: New Three Party Authentication Scheme with Privacy Support

ANALYSES

This section discusses security analysis and performance analysis by comparing the proposed scheme with Wang et al.'s scheme and Lin et al.'s scheme in [6, 12].

Security Analysis

Although it is important to provide a formal security proof on any cryptographic schemes, the formal security proof of security schemes remains one of the most challenging issues for cryptography research. Until now, a simple, efficient and convincing formal methodology for correctness analysis on authentication schemes is still an important subject of research and an open problem. Because of these reasons, most security schemes have been demonstrated with a simple proof. Therefore, we follow the approaches used in [15-16] for comparison purpose.

We will analyze the security of the proposed scheme to verify the overall security and privacy requirements as follows.

Definition 1 (Modified Hash Problem) Let $a, b, c \in Z_p$, and $d=h(a, b, c, d)$. If a can be evaluated from given d and c, then we say the modified hash problem is solved, which could be defined as the probability of $\Pr(a|b,c,d)=\varepsilon_1$.

Theorem 1 (Data Integrity) In the proposed authentication scheme, if an adversary can change V_i to V_i' successfully, then the modified hash problem can be solved.

Proof: In the proposed scheme, assume an adversary tries to change V_{AS} to V_{AS}' from eavesdropped messages. Let RO_1 be a random oracle: Input DID_A, AS, X_A, v_A to output V_{AS}', such that $V_{AS}'=h(DID_A, AS, X_A, v_A)$. In definition 1, let $DID_A \leftarrow b$, $AS \leftarrow c$ and $X_A \leftarrow d$ be input parameter of RO_1 and obtain output V_{AS}. Let $a \leftarrow V_{AS}$, then a is evaluated. Therefore, $\Pr(V_{AS}|DID_A,AS,X_A) \leq \Pr(a|b,c,d)=\varepsilon_1)$, which means the modified hash equal problem can be solved if RO_1 exists.

Theorem 2 (Anonymity) In the proposed authentication scheme, if an adversary can obtain A from DID_A, then the modified hash problem can be solved.

Proof: In the proposed scheme, assume an adversary tries to evaluate identifier A from the eavesdropped DID_A. Let RO_2 be a random oracle with input DID_A to output A, which is $RO_2(DID_A) \Rightarrow A$). In definition 1, let $DID_A \leftarrow d_1$ be input parameter of RO_2 and obtain output A. Let $a \leftarrow A$, then a is evaluated. Therefore, $\Pr(A|DID_A) \leq \Pr(a|d)=\varepsilon_1)$, which means the modified hash equal problem can be solved if RO_2 exists.

Definition 2 (Discrete Logarithm Problem) Let $a \in Z_c^*$, and g is a group generator of Z_c^*. If a can be evaluated from given $b=g^a \bmod c$, then we say the discrete logarithm problem is solved, which could be defined as the probability of $\Pr(a|b,c)=\varepsilon_2$.

Theorem 3 (Verifier Safety) In the proposed authentication scheme, if an adversary can obtain t_A from v_A, then the discrete logarithm problem can be solved.

Proof: In the proposed scheme, an adversary steals a copy of the verifier v_A for the user assume an adversary tries to derive t_A from v_A from eavesdropped messages. Let RO_3 be a random oracle: Input v_A and p to output t_A, which is $RO_3(v_A, p) \Rightarrow t_A$). In definition 2, let $g^{tA} \leftarrow b$ and $p \leftarrow c$ be input parameter of RO_3 and obtain output t_A. Let $a \leftarrow t_A$, then a is evaluated. Therefore, $\Pr(t_A|g^{tA},p) \leq \Pr(a|b,c)=\varepsilon_2)$, which means the discrete logarithm problem can be solved if RO_3 exists.

Definition 3 (Modified Hash Equal Problem) Let a_i, b_i, $c_i \in Z_p$, and $d_i=h(a_i, b_i, c_i)$. If $Equal(a_1, a_2)$ can be evaluated from given b_1, b_2, c_1 and c_2, then we say the modified hash equal problem is solved, where $Equal(x, y)$ is 1 if $x=y$, otherwise 0. The probability could be defined as $\Pr(Equal(a_1, a_2)|b_1,b_2,c_1,c_2)=\varepsilon_3$.

Theorem 3 (Untraceability) The proposed scheme can resist against tracking attacks.

Proof: In the proposed scheme, an adversary tries to evaluate $Equal(A^{(i)}, A^{(j)})$ to track the entity A from eavesdropped $DID_A^{(i)}$, $DID_A^{(j)}$, $(X_A)^{c(i)}$ and $(X_A)^{c(j)}$. Let RO_4 be a random oracle: input $DID_A^{(i)}$, $DID_A^{(j)}$, $(X_A)^{c(i)}$ and $(X_A)^{c(j)}$ to output $Equal(A^{(i)}, A^{(j)})$, which is RO_4 ($DID_A^{(i)}$, $DID_A^{(j)}$, $(X_A)^{c(i)}$, $(X_A)^{c(j)}) \Rightarrow Equal(A^{(i)}, A^{(j)})$. In definition 3, let $DID_A^{(i)} \leftarrow b_1$, $DID_A^{(j)} \leftarrow b_2$, $(X_A)^{c(i)} \leftarrow c_1$ and $(X_A)^{c(j)} \leftarrow c_2$ be input parameters of RO_4 and obtain output $Equal(A^{(i)}, A^{(j)})$. Let $Equal(a_1, a_2) \leftarrow Equal(A^{(i)}, A^{(j)})$, then $Equal(a_1, a_2)$ is evaluated. Therefore, $\Pr(Equal(A^{(i)},A^{(j)})|DID_A^{(i)},DID_A^{(j)},(X_A)^{c(i)},(X_A)^{c(j)}) \leq \Pr(Equal(a_1,a_2)|b_1,b_2,c_1,c_2) =\varepsilon_3)$, which means the modified hash equal problem can be solved if RO_4 exists.

Table 3: Security and privacy comparison

Property / Scheme	PR1	PR2	PR3	PR4	PR5
Wang et al.'s in [6]	Secure	Provide	Partially	N/A	N/A
Lin et al.'s in [12]	Secure	Secure	Provide	N/A	N/A
Proposed scheme	Secure	Secure	Provide	Provide	Provide

* PR1 : stolen verifier attack, PR2 : integrity, PR3 : authentication, PR4 : anonymity, PR5 : untraceability

Performance Analysis

Table 4 shows the performance comparisons of the related authentication schemes with the proposed scheme. The first line shows the comparison for modular exponentiation operations. We only require half number of operations compared with the other two. Especially, this is very important factor for the performance concern because the modular exponentiation operation is one of heavy operations in the authentication scheme.

The subsequent comparison items are XOR operations and random numbers. All Wang et al.'s scheme, Lin et al.'s scheme and the proposed scheme have the same computational XOR operations and random numbers. However, the proposed scheme requires many operations for hash operations than Wang et al.'s scheme and Lin et al.'s scheme due to providing anonymity for each entities.

For the transmission rounds Wang et al.'s scheme and the proposed scheme requires less cost than Lin et al.'s

scheme. Additionally, the proposed scheme provides more security and privacy properties and requires fewer exponentiation operations than Wang et al.'s scheme and Lin et al.'s scheme.

Table 4: Computation and communication overhead comparison

Scheme Properties	Wang et al.'s [6]			Lin et al.'s [12]			Proposed scheme		
	A	B	S	A	B	S	A	B	S
Exponentiation	4	4	6	4	4	6	2	2	2
XOR	1	1	2	1	1	2	1	1	2
Random number	1	1	2	1	1	2	1	1	2
Hash	3	3	4	4	4	4	6	6	6
Transmission rounds	5			6			5		

Therefore, compared to Wang et al.'s scheme and Lin et al.'s scheme, the proposed scheme requires less operational cost and fewer messages in communication, and provides more security and privacy properties. The proposed scheme thus is superior to related schemes.

CONCLUSION

A three party authentication scheme without server public keys for data exchange in was proposed by Lin et al. over TMISs. However, this paper showed that Lin et al.'s scheme has lack of privacy issues focused on anonymity and unlinkability. To solve the privacy weaknesses, this paper proposed a new three party authentication scheme with privacy concern to solve the problems in Lin et al.'s scheme. Compared to the related authentication scheme, the proposed scheme provides higher security and privacy, and has lower computational cost. .

REFERENCES

[1] M. U. Aslam, A. Derhab, K. Saleem, H. Abbas, M. Orgun, W. Iqbal, B. Aslam, A Survey of Authentication Schemes in Telecare Medicine Information Systems, Journal of Medical Systems, vol. 41:14 (2017) DOI:10.1007/s10916-016-0658-3.

[2] K. S. Rao, V. N. Mandhala, D. Bhattacharyya, An Association Rule hiding Algorithm for Privacy Preserving Data Mining, International Journal of Control and Automation, vol. 7, no. 11 (2014) pp. 393-404.

[3] R. S. Tolentino, S. Park, A Study on U-Healthcare System for Patient Information Management over Ubiquitous Medical Sensor Networks, International Journal of Advanced Science and Technology, vol. 18 (2010) pp. 1-11.

[4] R. Shahriyar, F. Bari, G. M. Akbar, Intelligent Mobile Health Monitoring System, International Journal of Control and Automation, vol. 2, no. 3 (2009) pp. 13-28.

[5] S. W. Lee, H. Kim, K. Y. Yoo, Efficient verifier-based key agreement protocol for three parties without server's public key, Applied Mathematics and Computation, vol. 167, no. 2 (2005) pp. 996-1003.

[6] R. C. Wang, K. R. Mo, Security enhancement on efficient verifier-based key agreement protocol for three parties without server's public key, International Mathematical Forum, vol. 20 (2006) pp. 965-972.

[7] J. O. Kwon, I. R. Jeong, K. Sakurai, D. H. Lee, Efficient verifier-based password-authenticated key exchange in the three-party setting, Computer Standards & Interfaces, vol. 29, no. 5 (2007) pp. 513-520.

[8] Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee, Y. Chung, A Secure Authentication Scheme for Telecare Medicine Information Systems, Journal of Medical Systems, vol. 36, no. 3 (2012) pp. 1529-1535.

[9] D. B. He, J. H. Chen, R. Zhang, A more secure authentication scheme for telecare medicine information systems, Journal of Medical Systems, vol. 36, no. 3 (2012) pp. 1989-1995.

[10] J. H. Wei, X. X. Hu, W. F. Liu, An improved authentication scheme for telecare medicine information systems, Journal of Medical Systems, vol. 36, no. 6 (2012) pp. 3597-3604.

[11] S. K. Islam, G. P. Biswas, Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system, Journal of King Saud University – Computer and Information Sciences, vol. 27, no. 2 (2015) pp. 211-221.

[12] T. H. Lin, T. F. Lee, Secure Verifier-Based Three-Party Authentication Schemes without Server Public Keys for Data Exchange in Telecare Medicine Information Systems, Journal of Medical Systems, vol. 38:30 (2014) DOI:10.1007/s10916-014-0030-4.

[13] J. Wang, Z. Zhang, K. Xu, Y. Yin, P. Guo, A Research on Security and Privacy Issues for Patient related Data in Medical Organization System, International Journal of Security & Its Applications, vol. 7, no. 4 (2013) pp. 287-298.

[14] Y. Song, L. Li, J. Zhang, J. Yang, A Method for Individualized Privacy Preservation, International Journal of Security & Its Applications, vol. 7, no. 6

(2013) pp. 109-116.

[15] R. Amin, G. P. Biswas, A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS, Journal of Medical Systems, vol. 39, no. 3 (2015) pp. 1-17.

[16] S. Y. Chiou, Z. Ying, J. Liu, Improvement of a privacy authentication scheme based on cloud for medical environment, Journal of Medical Systems, vol. 40, no. 4 (2016) pp. 1-15.