An Improvement of Sood, *et al.*'s Authentication Scheme using Smart Card

Kwang Cheul Shin[1] and Jung Gil Cho[2*]

[1]*Division of Industrial Management Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea*
[2]*Division of Computer Science Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea*
[1]*skcskc12@sungkyul.ac.kr,* [2]*jkcho@sungkyul.ac.kr*
**Corresponding Author: jkcho@sungkyul.ac.kr*

Abstract

In 2004, Das, et al.'s proposed the dynamic ID-based remote user authentication scheme to protect the user's anonymity. However, in 2005, Chein, et al.'s and Liao, et al.'s demonstrated that Das, et al.'s scheme failed to protecting user's anonymity. In addition, they showed that it was susceptible to guessing attack, so that it might expose the password to the remote system. In 2006, Liou, et al.'s proposed a new scheme which aimed to resolve the security vulnerabilities of Das, et al's scheme such as mutual authentication and malicious server attacks. However, in 2010, Sood, et al.'s demonstrated that Liou, et al's scheme is susceptible to impersonal attack, malicious user attack, man in the middle attack and offline password guessing attack. To resolve those vulnerabilities, Sood, et al.'s proposed new scheme. However, as a result of analysis of the new scheme proposed by Sood, et al., it is still vulnerable to malicious legal user attack and various attacks such as forgery, insider and database. In this paper, we propose an improvement to the Sood, et al.'s scheme in order to resolve such problems.

Keywords: *Authentication, Smart Card, Forgery Attack, Anonymity*

1. Introduction

A password authentication scheme is mostly used for verifying user identity based on smart card. The password authentication is a simple and easy to use authentication scheme to verify the legitimate user when logging in to remote system.

Smart card has been used as a popular tool because of its convenience, low cost, efficiency and popularity. Also smart card authentication schemes have been widely deployed to verify the legitimacy of remote user's login request [1-4].

Currently, the researches related to authentication protocol design are being actively carried out [5-9].

In 2004, Das, *et al.*'s [10] proposed the dynamic ID-based remote user authentication scheme preventing an attacker from knowing the user's identity. This scheme has the advantage that users can select and update the password as they want. Another advantage would be that there is no need to maintain password verification table storing password and identifier (ID) in the server.

Das et al.'s proposed new scheme and claimed that their scheme is secure against stolen verifier attack, replay attack, forgery attack, insider attack and identity theft.

However, in 2005, Chien, *et al.*'s [11] pointed out that Das, *et al.*'s scheme fails to protect the user's anonymity and Liao, *et al.*'s [12] and Das et al.'s schemes are vulnerable to guessing attack and might potentially expose the user's password.

In 2006, Liou, *et al.*'s [13] proposed enhanced scheme to resolve the vulnerabilities caused by mutual authentication and malicious server attack of Das, *et al.*'s scheme.

However, in 2010, Sood, *et al.*'s [14] demonstrated that Liou, *et al.*'s scheme is susceptible to impersonal attack, malicious user attack, man in the middle attack and offline password guessing attack. To resolve those vulnerabilities, Sood, *et al.*'s proposed new scheme.

In this paper, we will demonstrate that Sood, *et al.*'s scheme is still vulnerable to malicious legal user attack and various attacks including forgery, insider and database. To solve these problems, we will propose a more improved and more secure scheme.

2. Review of Sood et al.'s Scheme

In this section, we briefly review Sood, *et al.*'s scheme which consists of four parts. registration phase, login phase, authentication phase and password change phase.

2.1. Notations

Ui	ith user
Pi	The password of Ui
IDi	The identity of Ui
S	The remote server
sk	Session Key
C	The client
h(.)	A one-way hash function
yi	Random Number Selected by Server S
$\oplus$	Bitwise Xor operation
$\|\|$	Concatenation
$\Rightarrow$	A secure channel
$\rightarrow$	A common channel

2.2. Registration phase

A user Ui has to submit his unique identity IDi and password Pi to the server S for registration over a secure communication channel.

(ⅰ) C $\Rightarrow$ S : IDi, Pi

The Server S computes the security parameters Ai=h(x||yi), Bi=h(IDi||Pi)$\oplus$Pi$\oplus$h(x||yi), Ci=h(x||yi)$\oplus$h(Pi) and Di=h(IDi||Pi)$\oplus$h(x).

The server S chooses the value of yi corresponding to each user in such a way that the value of Ai must be unique for each user.

The server S stores yi$\oplus$x and IDi$\oplus$h(x) corresponding to Ai in its database. Then the server S issues the smart card containing security parameters(Bi, Ci, Di, h()) to the user Ui through a secure communication channel.

(ⅱ) S $\Rightarrow$ C: Smart card

2.3. Login phase

A user Ui inserts his smart card into card reader to login on to the server S and submits his identity IDi^* and password Pi^*.

The smart card computes $h(x||yi)=Bi \oplus h(IDi^*||Pi^*) \oplus Pi^*$, $Ci^*=h(x||yi) \oplus h(Pi^*)$ and compares Ci^* with the stored value of Ci in its memory to verifies the legality of the user Ui.

(ⅰ) Smart card checks Ci^* ?=Ci

After verification, the smart card computes $h(x)=Di \oplus h(IDi||Pi)$, $CIDi=h(x||yi) \oplus h(h(x)||T)$ and $Mi=h(h(x)||h(x||yi)||T)$, where T is current date and time of the input device. Then the smart card sends login request message(CIDi, Mi, T) to the service provider server S.

(ⅱ) S→C: CIDi, Mi, T.

2.4. Authentication phase

After receiving the login request message from the client C, the service provider server S checks the validity of time stamp T by checking $(T'-T) <= \delta T$, where T' is current date and time of the server S and δT is expected time interval for a transmission delay.

The server S computes $Ai^*=CIDi \oplus h(h(x)||T)$ and finds Ai corresponding to Ai^* in its database and then extracts $yi \oplus x$ and $IDi \oplus h(x)$ corresponding to Ai from its database.

Now the server S computes yi from $yi \oplus x$ and IDi from $IDi \oplus h(x)$ because the server S knows the value of x.

Then the server S computes $Mi^*=h(h(x)||Ai||T)$ and compares Mi^* with the received value of Mi.

(ⅰ) Server S checks Mi^* ?=Mi

If they are not equal, the server S rejects the login request and terminates this session. Otherwise, the server S acquires the current time stamp T'' and computes $Vi=h(Ai||h(x)||T||T'')$ and sends the message (Vi, T'') back to the smart card of the user Ui.

(ⅱ) S→C: Vi, T''

On receiving the message (Vi, T''), the user Ui's smart card checks the validity of time stamp T' by checking $(T'''-T') <= \delta T$, where T''' is current date and time of the smart card. Then the smart card computes $Vi^*=h(h(x||yi)||h(x)||T||T'')$ and compares it with the received value of Vi.

This equivalency authenticates the legality of the service provider server S and the login request is accepted else the connection is interrupted. Finally, the client C and server S agree on the common session key as $sk=h(IDi||h(x||yi)||h(x)||T||T'')$.

2.5. Password Change phase

The client C can change his password without the server's help. The user Ui inserts his smart card into a card reader and enters his identity IDi^* and password Pi^* corresponding to his smart card.

The smart card computes $h(x||yi)=Bi \oplus h(IDi^*||Pi^*) \oplus Pi^*$, $Ci^*=h(x||yi) \oplus h(Pi^*)$ and compares Ci^* with the stored value of Ci in its memory to verified the legality of the user. Once the legality of card holder is verified then the client can instruct the smart card to change his password.

Afterwards, the smart card asks the card holder to resubmit a new password Pi^{new} and then smart card computes $Bi^{new}= h(IDi||Pi^{new}) \oplus Pi^{new} \oplus h(x||yi)$, $Ci^{new}=h(x||yi) \oplus h(Pi^{new})$ and

Di^{new}=Di⊕h(IDi||Pi)⊕h(IDi||Pi^{new}). Thereafter, smart card updates the value of Bi, Ci and Di stored in its memory with Bi^{new}, Ci^{new} and Di^{new}.

2.6. Scheme Analysis

• Server S Secret Information h(x‖yi), h(x)'s Vulnerabilities

In Sood, *et al.*'s scheme, server S computes Ai, Bi, Ci and Di at the registration phase. However, the design of server S has vulnerability of potentially exposing secret information h(x‖yi), h(x) in the process of calculation.

When a user initially requests the server to register by sending IDi and Pi via a secure communication channel, server S computes Ai, Bi, Ci and Di with the use of random number (yi) chosen by the server and IDi and Pi of the user. S stores those values (Bi, Ci, Di) in smart card and then issues the smart card to the user to transmit the data.

In this process, the vulnerability resides in the fact that a legal smart card user(member) can discover h(x‖yi) and h(x) from the value of Bi, Ci, and Di.

The h(x) is the same value for each legitimate smart card user(member) and h(x‖yi) is different for each user depending on the random number y. Now it is demonstrated that how malicious legal user obtains h(x‖yi) of other legal user.

At login phase, the legal user sends CIDi, Mi, T to server.

The legal but malicious user can disguise(or impersonate) his or her identity as the user Ui who is a legal user by means of sniffing. First, the malicious legal user knows h(x) by extracting the value Di from smart card. To obtain h(x‖yi), the malicious legal user computes a following equation using CIDi and T intercepted.

$$h(x||yi) = CIDi \oplus h(h(x)||T)$$

Here the malicious legal user could obtain the value of h(x‖yi) and then generate Mi using the value of h(x‖yi) as follows.

$$Mi=h(h(x)||h(x||yi)||T)$$

Therefore, the disguise attack is possible because the legal but malicious user knows CIDi, Mi, T, h(x‖yi) and h(x).

• Forgery(or impersonation) attack

All the legal user(member) find h(x) by computing h(x)=Di⊕h(IDi||Pi) from Di=h(IDi||Pi)⊕h(x). The malicious legal user is a user who is already registered to server S in a legitimate way. The malicious legal user can eavesdrop on the CIDi, Mi and T from the login message of other legal user.

Now he can perform the forge attack as follows:

Because he knows h(x) and T, he computes $h(x||yi)_{M(Malicious)}$ using CIDi, h(x) and T, and computes CID_M and M_M using $h(x||yi)_M$ as follows.

$CID_M=h(x||yi)_M \oplus h(h(x)||T_M)$, $M_M=h(h(x)||h(x||yi)_M||T_M)$, where T_M is the current date and time of the malicious legal user.

Malicious legal user sends (CID_M, M_M, T_M) to server. In this case, T_M is valid because it was computed by the malicious legal user with the current time and date.

Upon receiving the login request message from the malicious legal user, server will carry out the verification process.

Server will check the freshness of T_M by means of $T'-T_M <= \delta T$, where T' is the S's current date and time.

To obtain IDi⊕h(x) and yi⊕x generated and stored at registration phase, Ai can be computed as follows.

Ai=h(x||yi)=CID_M⊕h(h(x)||T_M), yi⊕x and IDi⊕h(x) corresponding to A from its database, yi from yi⊕x, IDi from IDi⊕h(x).

Computes : M^*=h(h(x)||h(x||yi)||T_M)

Compares :

M_M=?M^* if the verification is correct the authenticity of malicious legal user is assured, it is obvious that S will accept the login request message.

S computes Vi=h(A||h(x)||T||Ts) where Ts is the current date and time of S.

S sends (Vi, Ts) to U's smart card, and then malicious legal user intercepts verification message [Vi, Ts] of the legal user.

The malicious legal user can easily find other legal peer member's ID by using social engineering attack or shoulder surfing.

Malicious legal user computes the session key sk=h(IDi||h(x||yi)||h(x)||T||Ts). Therefore it is obvious that Sood et al.'s scheme cannot resist the forge(or impersonation) attack.

• Insider's attack

Sood et al.'s scheme has pitfall of insider's attack of server S. In the registration phase, user's password will be revealed to the remote system as the user submits his IDi and password Pi, if the user uses password to access several servers for his convenience, the insider of the remote system can impersonate Ui to access other servers [15].

• Steal information from database

In the Sood, *et al.*'s scheme, S maintains a database, where security information is stored but not encrypted. The information stored in database includes A=(x||yi), user's ID(IDi⊕h(x)) and server's random number y(yi⊕x). Due to the vulnerability of secret information, h(x||yi) and h(x), of server S, it is easy to a attack database. Even if the adversary can obtain the information of database, he or she cannot recover yi from yi⊕x and IDi from IDi⊕h(x) of each user. However, if the adversary is the malicious legal user, he or she can recover yi from yi⊕x and IDi from IDi⊕h(x) of each user, because he or she already knows h(x||yi) and h(x), which means he or she can easily find h(x||yi) from the database. So Sood, *et al.*'s scheme cannot resist to steal the information from a database attack.

3. Propose Scheme

Improvement ideas:

The vulnerabilities of Sood et al.'s scheme(DB attack and forgery attack) stem from the fact that the legal user can easily compute the values of h(x||yi) and h(x) as computed by server S. Therefore the scheme should be designed to prevent the adversary or even the legal user from computing h(x||yi) and h(x) easily.

In this section, We describes a new remote user authentication scheme which resolves the above security flaws of Sood, *et al.*'s [14] scheme.

The improved scheme is also divided into four phase: registration, login, authentication, and password change phases.

3.1. Registration phase

The user Ui sends the registration request to the remote server S:

step 1 : C ⇒ S : IDi, h(Pi)
(ⅰ) Ui chooses a password Pi and computes h(Pi). He submits IDi and h(Pi) to S through a secure channel.
(ⅱ) S then chooses a secret number yi(for only user Ui),
computes Ai=h(x ‖ yi)⊕h(x), Bi=h(IDi ‖ h(Pi))⊕Ai, and Ci=h(Pi)⊕h(Bi ‖ yi), where x is the secret key of S.
(ⅲ) S stores yi⊕x and IDi⊕h(x) corresponding to h(x ‖ yi)=Ai⊕h(x) in a database.
(ⅳ) S stores parameters (h(), Bi, Ci) into a smart card, then sends the smart card and yi to Ui through the secure channel.
step 2 : S ⇒ C : Smart card

3.2. Login phase

When a user Ui wants to login the remote server S, He/she inserts the smart card to the terminal and keys the IDi, password Pi and yi, then the smart card will perform the following steps.

Step 1 : Password check : h(Bi ‖ yi)=?Ci⊕h(Pi), accept or reject. After verification, the smart card computes : CIDi=h(IDi⊕h(Pi))⊕Bi⊕T) and Di=h(T ‖ IDi ‖ yi), where T is the current date and time. C's smart card sends CIDi, Di, T to S.

Step 2 : S ⇒ C : CIDi, Di, T

3.3. Authentication phase

When the remote server S receives the login request CIDi, Di, T at time T', server authenticates the client C as follows:

Step 1 : S verifies if (T'-T)≤δT. If it holds, S accepts C the login request, where δT is an expected valid time interval.
And then S obtains $h(x‖yi)^*$ by computing $h(x‖yi)^*$=CIDi⊕T⊕h(x).

With the calculated value of $h(x‖yi)^*$, S finds the same value by searching the values stored in database of S. With the use of secret key x of S, S identifies yi and IDi from the yi⊕x and IDi⊕h(x), yi⊕x and IDi⊕h(x) corresponding to $h(x ‖ yi)^*$ from its database.

Extracts yi from yi⊕x and ID from IDi⊕h(x), and computes Di^*=h(T ‖ IDi ‖ yi) compares Di^*=?Di if the verification is correct the authenticity of client is assured.

If they are not equal, the server S rejects the login request and terminates this section. Otherwise, the server S acquires the current time stamp T" and computes Ei=h(T" ‖ IDi ‖ yi) and sends the message (Ei, T") back to the smart card of the user Ui.

Step 2 : S ⇒Smart card : Ei, T”

Upon receiving the login response message Ei, T”, U’s smart card carries out the following operations.

Checks the validity of T”.

Computes : Ei^{*}=h(T” ‖ IDi ‖ yi)

Compares : Ei^{*}=?Ei if the verification is correct the authentication of S is assured.

Finally, Ui and S computes the session key sk=h(T ‖ T” ‖ IDi ‖ yi)

3.4. Password change phase

When Ui wants to change the password, Ui inserts his smart card to the card reader of a terminal, and inputs his IDi^{*}, Pi^{*}, yi, and then the smart card carries out the following operations:

Computes :

h(Bi ‖ yi)=?Ci⊕h(Pi^{*})

Request to Ui a new password Pi_{new}

Computes :

Ai=Bi⊕h(IDi ‖ h(Pi))

Bi_{new}=h(IDi ‖ h(Pi_{new}))⊕Ai, and Ci=h(Pi_{new})⊕h(Bi_{new} ‖ yi)

and updates the values Bi and Ci stored in its memory with Bi_{new}, Ci_{new}.

4. Scheme Analysis

Smart card uses embedded microprocessor to perform the required operations specified in protocol, cooperating with smart card reader machine.
Messerges, *et al.*‘s [16]pointed out that all existing smart cards cannot prevent the information stored in them from being extracted by techniques such as monitoring their power consumption.

In this respect, smart card can be stolen by attacker, so that the stored information can be extracted. In this section, we are going to demonstrate that our scheme is secure against this.

- **Forgery(impersonation) attack:**

This attack attempts to forge the message by using information acquired from the target authentication scheme. When forging the message, the attacker disguises his or her identity as a legal user.

The attacker attempts to modify login request messages (CIDi, Di, and T) to ($CIDi_M$, Di_M, T_M), where T_M is the attacker's current date and time, so as to succeed in the authentication phase. However, the attacker needs to obtain IDi of Ui, Pi and yi of server's random number, and x of server's secret key, in order to compute valid parameters of CIDi and Di. Otherwise, the attempts would be rejected at authentication phase step 1. Additionally, the disguise attack is impossible because yi and h(x) are being protected by the user Ui and server S.

• Stolen smart card attack:

If the attacker steels the smart card, he/she could extract $Bi=h(IDi \| h(Pi)) \oplus Ai$, and $Ci=h(Pi) \oplus h(Bi \| yi)$ from smart card memory. In this case, the attacker should guess correct values of IDi, Pi and yi altogether at the same time.

Table 1. Functionality comparison of scheme and Sood, *et al.*'s

Feature	Sood et al.'s Scheme	Proposed Scheme
User's Anonymity	Yes	Yes
Mutual authentication	Yes	Yes
Insider attack	No	Yes
Malicious legality user attack	No	Yes
Forge(impersonation) attack	No	Yes
Stolen smart card attack	Yes	Yes
Database attack	No	Yes

Yes : stands for achieved, No : non-achieved

• Malicious legal user attack:

Malicious legal user attacker can compute A_M as follows, using his/her own ID_M, password P_M, and B_M stored in smart card, $A_M=B_M \oplus h(ID_M \| h(P_M))$.

However, it is impossible for the attacker to discover x and y because A_M is computed as a result of operating($\oplus$) between $h(x \| y)$ and $h(x)$, that is $h(x \| y) \oplus h(x)$, where $h(x \| y)$ means string concatenation of secret key x of server S and random number y, and $h(x)$ gets hash value of x applying hash function to x.

Here the value of x and y are significantly important. If those value are easily revealed by the nature of scheme, the value of $yi \oplus x$ and $IDi \oplus h(x)$ stored in database can also be easily discovered by the attacker.

On the other hand, the attacker attempts to compute $h(x \| y)$ and $h(x)$ by intercepting login request messages (CIDi, Di, Ti) of the user Ui and authentication response messages (E, T) from the server S. In this case, the attacker needs to know password Pi for the legal user. However, the attacker cannot compute A_M and cannot discover x and yi. Hence the malicious legal user attack is impossible.

• Insider attack:

In this registration phase, user submits h(Pi) to the remote server. So, even an insider cannot know the password of a user. Hence, our scheme defends insider attack.

• Database attack:

Database stores the user information $yi \oplus x$, $IDi \oplus h(x)$ and $h(x \| yi)$ which are computed by server S. To acquire the user information from the database, the attacker should know yi and secret key x of server S. Using those data, the attacker can compute $h(x \| yi)$ which is a vital information to find the matched information in database. In the proposed scheme, the only way to do this is to extract Bi and Ci from the smart card and intercept CIDi and Di from the

login request message. However, it is impossible in our proposed scheme because all those parameters are the operating result in an integrated way.
The functionality comparison of the proposed scheme with the relevant smart card based authentication schemes is summarized in Table 1

5. Computation Cost Analysis of Proposed Scheme

In this section, comparisons between Sood, *et al.*'s scheme [14], and our proposed scheme are shown in Table 2.

An efficient authentication scheme must take communication and computation cost into consideration during user's authentication.

Assume that the identity IDi, password Pi, x and yi, one way hash function values are all 128-bit long.

Let TH, TE and TS denote the time complexity for hash function, exponential operation and symmetric key encryption respectively.

Generally, time complexity associated with these operations can be roughly expressed as TS≥TE≥TH.

In the proposed scheme, the parameters stored in smart card are Bi, Ci and the memory needed in the smart card is 256(=2*128) bits. The communication cost of authentication includes the capacity of transmitting message involved in the authentication scheme.

The capacity of transmitting message (CIDi, Mi, T) and (Vi, T") is 640(=5*128) bits.

The computation cost of registration is the total time of all operations executed in the registration phase.

In registration scheme, Ui computes h(Pi) that requires 1TH and S computes Ai, Bi, and Ci that requires 4TH.

Table 2. Cost comparison of scheme and Sood, *et al.*'s

Feature	Sood et al. scheme			Our scheme		
	Smart card	**system**	**Operation process**	**Smartcard**	**System**	**operation process**
Memory space		384 bits			256 bits	
Communication cost	5*128 bits			5*128 bits		
registration phase		4TH	7 Times		4TH	3 Times
login phase	4TH		6 Times	3TH		3 Times
authentication phase	2TH	4TH	7 Times	2TH	4TH	4 Times
			4 Times			3 Times
password change phase		5TH	6 Times		4TH	3 Times

In login phase, Ui computes h(Bi ‖ yi) that requires 1TH, h(Pi) requires 1TH, CIDi requires 1TH, computes Di that requires 1TH.

In authentication phase, S computes h(x) that requires 1TH, Di* requires 1TH, Ei* requires 1TH, and computes sk that requires 1TH. In the same phase, Ui computes Ei* that requires 1TH, sk requires 1TH,

We can see that the number of hash operation is decreased by only two in our scheme compared with Sood, *et al.*'s scheme

6. Conclusion

Sood, *et al.*'s demonstrated that Liou, *et al*.'s scheme is susceptible to impersonal attack, malicious user attack, man in the middle and offline password guessing attack. Sood, *et al.*'s scheme was proposed to resolve the problems discovered in Liou, *et al*.'s scheme. However this study pointed out that the Sood, *et al.*'s scheme is still susceptible to malicious legal user attack, forgery attack and insider attack.

In this paper, I demonstrate that the improvement authentication scheme proposed by Sood, *et al.*'s is still vulnerable to malicious legal user attack, and steal information from a database attack, insider attack, forgery(impersonation) attack.

I am proposed for improvement to the scheme in order to solving such problems. This paper proposed an improvement to the scheme in order to solve such problems.
The proposed scheme is simplified, fast and efficient because only one way hash functions and XOR operations are used in its implementation more than Sood, *et al.*'s scheme.

References

[1] L. Lamport, "Password authentication with insecure communication", communications of the ACM, vol. 24, no. 11, **(1981)**, pp. 770-772.
[2] M. S. Hwang, C. C. Lee and Y. L. Tang, "A Simple remote User Authentication Scheme. Mathematical and Computer Modelling, vol. 36, **(2002)**, pp. 103-107.
[3] C. M. Chen and W. C. Ku, "Stolen-verifier attack on two new strong-password authentication protocol", IEICE Transactions on communications E85-B, **(2002)** November pp. 2519-2521.
[4] C. C. Lee, M. S. Hwang and W. P. Yang, "A Flexible Remote User Authentication Scheme using Smart Cards", ACM Operating System Review, vol. 36, no. 4, **(2002)**, pp. 23-29.
[5] Y. Y. Wang, J. Y. Kiu, F. X. Xiao and J. dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", Computer Communications, vol. 32, **(2009),** pp. 583-585.
[6] Y. P. Liao and S. S. Wang, "A secure dynamic ID-based remote user authentication scheme for multi-server environment", Computer Standards & Interfaces, vol. 31, **(2009)**, pp. 24-29.
[7] C. S. Bindu, P. C. S. Reddy and B. Satyanarayana, "Improved Remote User Authentication Scheme Preserving User Anonymity", IJCSNS, vol. 8, no. 3, **(2008)** March.
[8] Q. Xie, J. -K. Wang, D. -R. Chen and X. -Y. Wang, "A novel user authentication scheme using smart card", College of Computer Science. Zhejiang University. Hangzhou, 310027, P R China, and Graduate School. Hangzhou Normal University, **(2008)**.
[9] J. Xu, W.Zhu and D. Feng, "An improved smart card based password authentication scheme provable security", Computer Standard & Interface, vol. 31, **(2009)**, pp. 723-728.
[10] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication Scheme", IEEE Transactions on Consume Electronics, vol. 50, no. 2, **(2004)** May, pp. 629-631.
[11] H. Y. Chien and C. H. Chen, "A Remote Authentication Scheme Preserving User anonymity", In proceeding of Advanced Information networking and Applications, vol. 2, **(2005)** March, pp. 245-248.
[12] I. E. Liao, C. C. Lee and M. S. Hwang, "Security Enhancement for a Dynamic ID-Based Remote User Authentication Scheme", In Proceeding of Conference on Next Generation Web Services Practice, **(2005)** July, pp. 437-440.
[13] Y. P. Liou, J. Lin and S. S. Wang, "A New Dynamic ID-Based Remote User Authentication Scheme using Smart Cards", In Proceedings of 16th Information Security Conference, Taiwan, **(2006)** July, pp. 198-205.
[14] S. K. Sood, A. K. Sarje and K. Singh, "An Improvement of Liou, *et al.*'s authentication scheme using smart

cards", International Journal of Computer Applications, vol. 1, no. 8, **(2010)**, pp. 16-23.
[15] W. C. Ku, C. M. Chen and H. L. Lee, "Cryptanalysis of a variant of peyravian-Zunic's password authentication scheme", *IEEE Transactions on Communications*, vol. E86-B, no. 5, **(2003)** May, pp. 1682-1684.
[16] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining Smart Card Security under the Threat of Power Analysis Attack", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)** May, pp. 541-552.

Authors

Kwang Cheul Shin

Division of Industrial Management Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, skcskc12@sungkyul.edu

Education & Work experience: 2003, Ph.D. degree in Information and Communication Engineering, Sung kyunkwan University. Currently: Professor in Dept. of Industrial Management Engineering, Sungkyul University. Tel: 82-031-467-8916

Jung Gil Cho

Division of Computer Science Engineering, Sungkyul University, #147-2, Anyang 8 dong, Manan-gu, Anyang-si, Gyeonggi-do 430-742, Korea, jkcho@sungkyul.ac.kr

Education & Work experience: 2003, Ph.D. degree in Computer Science Engineering, Chungbuk National University. Currently: Professor in Dept. of Computer Science Engineering, Sungkyul University. Tel: 82-031-467-8916