Comments on “ITSSAKA-MS: An Improved Three-Factor Symmetric-Key Based Secure AKA Scheme for Multi-Server Environments”

SUNGJIN YU AND YOUNGHO PARK, (Member, IEEE)

1School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
2School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT Multi-server technology is widely utilized due to its enormous applicability in fields such as telecare medicine information system (TMIS), online shopping, remote surveillance, online banking, etc. However, a malicious attacker can perform various security attacks in the multi-server environments because he/she can easily modify, insert, inject, delete, and intercept exchanged messages over a public channel. Thus, secure authentication and key agreement (AKA) schemes are indispensable to provide useful services in multi-server environments. In 2020, Ali et al. presented a three-factor symmetric key based secure AKA scheme for privacy and security in multi-server environments. Ali et al. claimed that their scheme can prevent various security attacks, and also ensure secure authentication. However, this comment shows that Ali et al.’s scheme suffers from many drawbacks, including session key exposure, man-in-the-middle (MITM), and masquerade attacks. Moreover, their scheme fails to ensure mutual authentication. Thus, we suggest the necessary security guidelines to resolve the security threats of Ali et al.’s scheme.

INDEX TERMS Cryptanalysis, multi-server environment, authentication, key establishment, security protocol.

I. INTRODUCTION

With the development in portable device and wireless communication, users can access useful services through smart devices at anytime and anywhere in multi-server environments. Multi-server technology has become a promising alternative with its extensive applications of networks and has been used in various fields, including telecare medicine information system (TMIS), online shopping, remote surveillance, online banking, and so on. Multi-servers allow legitimate users to access various services from multiple servers through wireless communication. Generally, a multi-server comprises of the user, the trusted registration center (RC), and a group of servers. Once the user is registered in RC, they are able to access application servers that have registered in the RC. However, in multi-server environments, an attacker can perform various security attacks because all messages are transmitted over a public channel. Thus, secure and efficient authentication and key agreement (AKA) scheme is indispensable to ensure secure services for legitimate users in multi-server environments.

In 2020, Ali et al. [1] designed a biometric-based secure AKA scheme to provide secure services in multi-server environments. Ali et al. claimed that their scheme is able to resist various security threats such as impersonation, replay, session key exposure, and insider attacks. Moreover, they claimed that their scheme can ensure secure mutual authentication, anonymity, and perfect forward secrecy. However, this comment shows that their scheme is vulnerable to session key exposure, man-in-the-middle (MITM) and masquerade attacks, and also does not provide mutual authentication. Therefore, we suggest the some guidelines to resolve the security threats of Ali et al.’s scheme.

The outline of this comment is summarized as follows. Section II briefly reviews Ali et al.’s scheme and then Section III presents cryptanalysis for Ali et al.’s scheme. In Section IV, we suggest guidelines to resolve the security flaws of Ali et al.’s scheme. Finally, the entire work is summarized in Section V.
A. ADVOCACY MODEL

We present the attack assumptions comprising the well-known Dolev-Yao (DY) threat model [2] to examine the security of SMAP-IoV. In the DY model, the capabilities of a malicious adversary are as follows:

- Referring to the DY model [2], a malicious attacker (MA) is able to eavesdrop, modify, replay, inject, or delete transmitted messages over a public channel.
- MA can steal the legal user’s smart card and extract the stored secret credentials in memory by performing power analysis [3]–[5].
- MA can be a legitimate and privileged insider, which is able to reveal the verifier table stored in the RC database [1].
- After getting the secret credentials of the smart card, an adversary may attempt potential attacks such as “MITM”, “masquerade”, “off-line password guessing” attacks and so on [6]–[8].

B. MOTIVATION AND CONTRIBUTION

The major aim of this comment is to identify the security drawbacks present in the protocol of Ali et al. Consequently, Ali et al.’s scheme fails to ensure the required security functionalities such as “session key exposure attack”, “MITM attack”, “masquerade attack”, and “mutual authentication”, which are considered to be major requirements in multi-server environments. These facts motivated us to come up with security guidelines, which can provide security functionalities and resolve security flaws and threats that exist in multi-server environments.

II. REVIEW OF THE ALI et al.’s SCHEME

We briefly review Ali et al.’s AKA scheme for multi-server environments. Ali et al.’s scheme [1] is composed of three processes: user registration, server registration, authentication, and key establishment. The symbols utilized in this article are summarized in Table 1.

A. USER REGISTRATION PROCESS

All users $U_i$ must register with the registration center $RC$ in order to receive useful services. We present the user registration process of Ali et al.’s scheme and the detailed steps are as below:

**UR 1:** $U_i$ selects $ID_i$, $PW_i$, and imprints $BIO$. Then, $U_i$ calculates $CID_i$ = $h(ID_i)$ and sends it to $RC$ over a secure channel.

**UR 2:** After obtaining message $\{CID_i\}$, the RC chooses a random number $R_i$ and temporary identity $TID_i$. After that, RC computes $Auth = h(K_{RC}|||CID_i||R_i)$, $K_i = h(CID_i||R_i)$, and $R_1 = E_{K_{RC}}(Auth, R_1, CID_i)$. Finally, RC stores $\{R_i, K_i, TID_i\}$ in the SC and sends it to $U_i$.

**UR 3:** After obtaining smart card $SC$, the $U_i$ calculates $Gen(BIO) = (\sigma, \tau_i)$, $A_i = h(ID_i)||PW_i||\sigma_i$, $R_i^* = R_i \oplus h(PW_i||\sigma_i)$, $K_i^* = K_i \oplus h(PW_i||\sigma_i)$, $TID_i^* = TID_i \oplus h(PW_i||\sigma_i)$ and replaces $\{K_i, R_i, TID_i\}$ with $\{K_i^*, R_i^*, TID_i^*, Gen(.), Rep(.), \tau, \tau_i\}$ in SC.

| Symbol | Itemize |
|--------|---------|
| $U_i$  | User    |
| $RC$   | Registration center |
| $S_j$  | Server |
| $ID_i, PW_i$ | Identity and password of $U_i$ |
| $SID_j$ | Identity of $S_j$ |
| $Gen(.)$, $Rep(.)$ | Fuzzy extractors |
| $SC$ | Smart card |
| $K_{RC}, K_{S_j}$ | Secret key of $RC$ and $S_j$ |
| $\sigma, \tau$ | Biometric secret key and public reproduction |
| $t$ | Error tolerance threshold |
| $SK$ | Session key between $S_j$ and $U_i$ |
| $T_i$ | Timestamp |
| $E_K(.)$, $D_K(.)$ | Encryption/Decryption |
| $\oplus$ | XOR operation |
| $||$ | Concatenation operation |

B. SERVER REGISTRATION PROCESS

All servers $S_j$ must register with the RC in order to provide various services. Each server $S_j$ chooses a identity $SID_j$ and sends it to $RC$. Then, $RC$ computes $S_{priv} = h(SID_j||K_{RC})$ and sends it to $S_j$. Finally, $S_j$ stores $\{S_{priv}\}$ in database.

C. AUTHENTICATION AND KEY AGREEMENT PROCESS

In this process, $U_i$ requests authentication to $S_j$ in order to establish the session key $SK$. We describe the AKA protocol of Ali et al.’s scheme in Fig. 1 and the detailed steps of this process are as follows:

**AK 1:** $U_i$ inserts $SC$ and inputs $ID_i$ and $PW_i$. Then, $U_i$ imprints $BIO$, computes $Rep(BIO, \tau_i) = \sigma_i$, $A_i^* = h(ID_i)||PW_i|||\sigma_i$, and checks $A_i^* \neq A_i$. If the condition is valid, $U_i$ calculates $R_i = R_i^* \oplus h(PW_i|||\sigma_i)$, $K_i = K_i^* \oplus h(PW_i|||\sigma_i)$, $TID_i = TID_i^* \oplus h(PW_i|||\sigma_i)$, $CID_i^* = h(ID_i)$, $R_2 = R_2 \oplus CID_i^*$, $TID_i^* = TID_i \oplus CID_i^*$, $T_i^* = T_i \oplus CID_i^*$, and $W_i = h(CID_i^*||K_i||T_i)$. After that, $U_i$ transmits the message $M_1 = \{R_i, R_i^*, SID_j, W_i, T_i^*, TID_i^*\}$ to $RC$ over an insecure channel.

**AK 2:** After getting message $\{M_1\}$, the RC calculates $(Auth, R_1, CID_i) = D_{K_{RC}}(R_i)$ and checks the condition $|T_1 - T_i| \leq \Delta T$. If it is correct, RC computes $W_i = h(CID_i)||h(CID_i||K_{RC}||T_1)$. $Auth^* = h(K_{RC}||CID_i||R_1)$ and checks $W_i^* = W_i$ and $Auth^* \neq Auth$. If the condition is correct, RC computes $TID_1 = TID_i^* \oplus CID_i$, $R_2 = R_2 \oplus CID_i$ and generates a timestamp $T_2$. After that, RC calculates $K_j = h(SID_j||K_{RC})$, $W_{RC} = h(K_j||T_2)$, and $Y_{RC} = h(SID_j||CID_i||R_2||\tau_i)$, and encrypts $GR_{RC} = E_{K_j}(TID_1, W_{RC}, Y_{RC}, T_1, T_2)$. Finally, RC transmits the message $M_2 = \{GR_{RC}, SID_j\}$ to $S_j$.

**AK 3:** After obtaining message $\{M_2\}$, the $S_j$ decrypts $(TID_i, W_{RC}, Y_{RC}, T_1, T_2) = S_{priv}(GR_{RC})$ and validates the condition $|T_2 - T_1| \leq \Delta T$. If the condition is equal,
S. Yu, Y. Park: Comments on ITSSAKA-MS

FIGURE 1. Authentication and key agreement process of Ali et al.’s scheme.

| User ($U_i$) | Registration center ($RC$) | Server ($S_j$) |
|--------------|---------------------------|----------------|
| Computes $W_{RC}^* = h(S_{priv_i}||T_2)$ and checks $W_{RC}^* \neq W_{RC}$. If it is valid, $S_j$ generates a $T_3$ and calculates $SK = h(Y_{RC}||SID_j||T_3)$, and directly transmits the message $M_3 = \{W_{S_j}, T_3, TID_j\}$ to the $U_i$ over an insecure channel. |
| $T_i$ $= T_i \oplus CID_i$ |
| $[T_3 - T_i] \leq \Delta T$ |
| $W_{S_j}^* = h(Y_{RC}||SID_j||T_3)$ |
| $W_{S_j}$ $= h(SK||T_3)$ |
| Checks $W_{S_j}^* \neq W_{S_j}$. If true, save the session key |

$S_j$ computes $W_{S_j}^* = h(S_{priv_j}||T_2)$ and checks $W_{S_j}^* \neq W_{RC}$. If it is valid, $S_j$ generates a $T_3$ and calculates $SK = h(Y_{RC}||SID_j||T_3)$, and directly transmits the message $M_3 = \{W_{S_j}, T_3, TID_j\}$ to the $U_i$ over an insecure channel.

- **AK 4:** After getting message $\{M_3\}$, the $U_i$ checks the freshness of condition $[T_3 - T_i] \leq \Delta T$. If the condition is correct, $U_i$ computes $Y_i = h(Y_{RC}||CID_i^*||R_2||T_3)$, $SK = h(Y_{RC}||SID_j||T_3)$, and $W_{S_j}^* = h(SK||T_1||T_3)$. After that, $U_i$ validates the condition $W_{S_j}^* = W_{S_j}$ If it is equal, $U_i$ and $S_j$ establish $SK$ successfully and then save the $SK$ for future communication.

### III. CRYPTANALYSIS OF ALI ET AL.’S SCHEME

This comment is about “ITSSAKA-MS: An Improved Three-Factor Symmetric-Key Based Secure AKA Scheme for Multi-Server Environments”, that is proposed by Ali et al. [1]. They claimed that their scheme can prevent various security attacks, and also ensure secure authentication. However, we prove that AKA scheme for multi-server environment by Ali et al.’s scheme [1] is susceptible to “session key exposure”, “MITM”, “smart card theft”, and “masquerade” attacks. In addition, we also demonstrate that their scheme fails to provide mutual authentication.

### A. MASQUERADE ATTACK

A MA may attempt to masquerade legal users through stolen smart card. According to Section I-A, we assume that MA can extract the stored secret credential $\{K_i^*, R_i^*, TID_i^*, Gen(), Rep(), \tau, t\}$ in SC. Moreover, MA can eavesdrop, modify, replay, inject, or delete the exchanged messages via a public channel. Consequently, MA can perform the impersonation as the following detailed steps.

- **Step 1:** MA first computes $h(PW_i||\sigma_i) = R_i^* \oplus R_i$, $K_i = K_i^* \oplus h(PW_i||\sigma_i)$, $TID_i = TID_i^* \oplus h(PW_i||\sigma_i)$, $CID_i^* = TID_i \oplus TID_i^*$, $R_2 = R_2^* \oplus CID_i^*$, $T_1 = T_1^* \oplus CID_i^*$, and $W_i = h(CID_i^*||K_i||T_2)$. After that,
MA generates a random nonce R_MA and calculates \( R_M^* = R_M \oplus CID^* \). Then, MA transmits the message \( M_{MA1} = \{ R_i, R_M^*, SID_j, W_i, T_1^*, TID^*_j \} \) to RC.

**Step 2:** Upon obtaining the message \( \{ M_{MA1} \} \), the RC calculates \( Auth(R_1, CID_i) = D_{K_{RC}}(R_1) \) and \( T_i = T_1^* \oplus CID_i \), and checks the condition \( |T_i - T_c| \leq \Delta T \). If it is correct, RC computes \( W_i^* = h(CID_i)[h(CID_i)[K_{RC}||T_i]] \), \( Auth^* = h(K_{RC}||CID_i||R_{MA}) \), and checks \( W_i^* \neq W_i \) and \( Auth^* \neq Auth \). If the condition is correct, RC computes \( TID_i = TID^*_j \oplus CID_i, R_{MA} = R_M^* \oplus CID_i \) and generates a timestamp \( T_2 \). Then, RC computes \( K_j = h(SID_j||K_{RC}) \), \( W_{RC} = h(K_j||T_2) \), and \( Y_{MA} = h(SID_j||R_{MA}||T_1) \), and encrypts \( G_{RC} = E_k(TID_i, W_{RC}, Y_{MA}, T_1, T_2) \). Finally, RC transmits the message \( M_{MA2} = \{ G_{RC}, SID_j \} \) to SJ.

**Step 3:** Upon receiving message \( \{ M_{MA2} \} \), the SJ decrypts \( TID_i, W_{RC} \) and checks \( W_{RC}^* \neq W_{RC} \). If it is valid, SJ generates a \( T_3 \) and calculates \( SK_{MA} = h(Y_{MA}||SID_j||T_3) \), \( W_{MA} = h(SK_{MA}||T_1||T_3) \), and directly sends the message \( M_{MA3} = \{ W_{MA}, T_3, TID_i \} \) to U1.

**Step 4:** Upon receiving message \( \{ M_{MA3} \} \), the MA computes \( Y_{MA} = h(SID_j||CID^*_j||R_{MA}||T_1) \), \( SK_{MA} = h(Y_{MA}||SID_j||T_3) \), and \( W_{MA} = h(SK_{MA}||T_1||T_3) \).

Consequently, Ali et al.’s scheme is fragile to the masquerade attack because the MA can impersonate as a legitimate user successfully.

### B. SESSION KEY EXPOSURE ATTACK

Referring to Section III-A, we demonstrate that MA can masquerade legitimate user U1 and computes the session key \( SK = h(Y_{RC}||SID_j||T_3) \) as follows. According to Section I-A, MA is able to extract stored secret parameters in SC, and intercept the transmitted data between U1, RC, and SJ over a public channel. If so, MA computes \( h(PW_i||\sigma_i) = R_i^* \oplus R_i, TID_i = TID^* \oplus h(PW_i||\sigma_i), CID_i^* = TID^*_j \oplus TID^*_j, R_2 = R_2^* \oplus CID_i^* \), and \( T_1 = T_1^* \oplus CID_i^* \). After getting message \( \{ M_3 \} \), the MA calculates \( Y_i = h(SID_j)||CID_i^*||R_2^*||T_1 \) and \( SK = h(Y_i||SID_j||T_3) \) successfully. As a result, Ali et al.’s scheme is susceptible to the session key exposure attack because MA can successfully generate \( SK = h(Y_i||SID_j||T_3) \) between U1 and SJ.

### C. MITM ATTACK

Ali et al. claimed that their scheme can withstand MITM attack because MA is unable to calculate the correct login request message \( M_1 = \{ R_i, R_2^*, SID_j, W_i, T_1^*, TID^*_j \} \) without secret parameters \( \{ CID_i, R_2, K_j \} \). However, referring to Section III-A, MA calculates \( h(PW_i||\sigma_i) = R_i^* \oplus R_i, K_j = K_j^* \oplus h(PW_i||\sigma_i), TID_i = TID^*_j \oplus h(PW_i||\sigma_i), CID_i^* = TID^*_j \oplus TID^*_j, R_2 = R_2^* \oplus CID_i^* \), and \( T_1 = T_1^* \oplus CID_i^* \). Consequently, MA can impersonate as a legitimate user and generates the correct session key \( SK = (Y_i||SID_j)||T_3 \). Therefore, Ali et al.’s scheme is insecure against smart card theft attack.

### D. SMART CARD THEFT ATTACK

Ali et al.’s scheme claimed that the knowledge of attained parameters should not be enough for the malicious adversary to attain useful information to masquerade a legal user. However, according to Section III-A, MA can impersonate as a legitimate user and generate the correct session key \( SK = (Y_i||SID_j)||T_3 \). Therefore, Ali et al.’s scheme is insecure against smart card theft attack.

### E. MUTUAL AUTHENTICATION

In Ali et al.’s scheme [1], they claimed that their scheme allows mutual authentication between the U1, RC, and SJ. However, according to Section III-C, MA can calculate the correct login request message \( M_1 \) and authentication response message \( M_3 \) successfully. Consequently, Ali et al.’s scheme does not provide secure mutual authentication.

### IV. GUIDELINE ON ATTACK RESILIENCE

In Section III, we demonstrate that Ali et al.’s scheme suffers from many drawbacks, including session key exposure, MITM, and masquerade attacks. Moreover, their scheme fails to ensure mutual authentication. Therefore, we suggest the necessary guidelines to resolve the security threats of Ali et al. scheme.

- All participants must securely encrypt and transmit the messages using a symmetric key because a malicious attacker can easily insert, delete, intercept, and modify the transmitted messages during the AKA phase.
- The session key \( SK \) must consist of some randomly generated parameters such as random nonce and secret credential.
- In case of lost or stolen smart card, a malicious attacker can impersonate as a legitimate user or can change the password of the user. Thus, AKA scheme must store the secret credentials in encrypted form to prevent smart card theft attack.

### V. CONCLUSION

This comment refers to “ITSSAKA-MS: An Improved Three-Factor Symmetric-Key Based Secure AKA Scheme for Multi-Server Environments,” presented by Ali et al. We have shown that Ali et al.’s scheme is fragile to well-known attacks such as masquerade, MITM and smart card theft attacks, and also does not ensure mutual authentication. Furthermore, a malicious attacker after stealing parameters stored in the smart card or the verifier table can calculate a session key shared between the user and server. Thus, we have presented the necessary guidelines to resolve the security drawbacks of Ali et al.’s scheme. In this way, we can thwart the pointed out security problems not only in Ali et al.’s scheme but also in future designs of other authentication schemes.
REFERENCES

[1] Z. Ali, S. Hussain, R. H. U. Rehman, A. Munshi, M. Liaqat, N. Kumar, and S. A. Chaudhry, “ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments,” IEEE Access, vol. 8, pp. 107993–108003, 2020.

[2] D. Dolev and A. Yao, “On the security of public key protocols,” IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[3] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Advances in Cryptology. Berlin, Germany: Springer, 1999, pp. 388–397.

[4] S. J. Yu, K. S. Park, and Y. H. Park, “A secure lightweight three-factor authentication scheme for IoT in cloud computing environment,” Sensors, vol. 19, no. 16, p. 3598, 2019.

[5] S. Hussain and S. A. Chaudhry, “Comments on ‘Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,’” IEEE Internet Things J., vol. 6, no. 6, pp. 10936–10940, Dec. 2019.

[6] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, “A dynamic privacy-preserving key management protocol for V2G in social Internet of Things,” IEEE Access, vol. 7, pp. 76812–76832, 2019.

[7] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, “IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment,” IEEE Access, vol. 8, pp. 167875–167886, 2020.

[8] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, “On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks,” IEEE Access, vol. 8, pp. 107046–107062, 2020.

SUNGJIN YU received the B.S. degree in electronics engineering from Daegu University, in 2017, and the M.S. degree from Kyungpook National University, Daegu, South Korea, in 2019, where he is currently pursuing the Ph.D. degree in electronics engineering. His research interests include blockchain, VANET, information security, post-quantum cryptography, and authentication.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. His research interests include multimedia, computer networks, and information security.

* * *