Comments and Replies

Comments on "Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment"

Sajid Hussain and Shehzad Ashraf Chaudhry

Abstract*—Very recently, Das *et al.* (IEEE Internet of Things Journal, pp. 4900–4913, 5(6), DOI: 10.1109/JIOT.2018.2877690, 2018) presented a biometric-based solution for security and privacy in Industrial Internet of Things architecture. Das *et al.* claimed that their protocol is secure against known attacks. However, this comment shows that their protocol is defenseless against stolen verifier, stolen smart device, and traceability attacks. The attacker having access to public parameters and any of the verifier and parameters stored in smart device can easily expose the session key shared among the user and the smart device. Moreover, their protocol fails to provide perfect forward secrecy. Finally, this article also provides some necessary guidelines on attack resilience for the authentication schemes based on merely the symmetric key primitives, which are overlooked by Das *et al.

***Index Terms*—Industrial Internet of Things (IIoT), insider attack, key establishment, perfect forward secrecy, secret key expose, stolen smart device, stolen verifier attack.**

I. Introduction

THE INDUSTRIAL Internet of Things (IIoT) is a system of interconnected smart devices equipped with sensors, actuators, and machinery to collect, interpret, and analyze data for making intelligent decisions without human intervention. Smart devices deal with sensitive data. The security and privacy are the main concerns for its productive realization as smart devices exchange information over public channel. Very Recently, Das *et al.* [1] presented a biometric-based authentication scheme to provide security and privacy in cloud-based IIoT Deployment. However, this comment shows that their protocol is defenseless against stolen verifier attack [7]–[9], which is a very realistic and common attack on authentication schemes [10], [11]. The attacker having access to public parameters and the verifier can easily expose the session key shared among the user and smart device. Moreover, their scheme is also defenseless against traceability and stolen smart device attacks and fails to provide perfect forward secrecy. For cryptanalysis purposes the common adversarial model in Section I-A is adopted. The rest of this article is organized as follows, in Section II a brief review of Das *et al.*'s scheme is presented, then it is cryptanalysis is presented in Section III. Some guidelines for attack resilience in symmetric key-based crypto-systems is provided in Section IV. Finally, the conclusion is given in Section V.

A. Adversarial Model

In this article, we consider the common adversarial model as mentioned in [2]–[4]. Where according to capabilities of the adversary $\mathcal{U}_{\mathcal{A}}$, following realistic assumptions are made.

1) $\mathcal{U}_{\mathcal{A}}$ fully controls the public communication channel. $\mathcal{U}_{\mathcal{A}}$ can capture, replay, modify, insert a new message, and can delete any message.
2) $\mathcal{U}_{\mathcal{A}}$ after getting registered with *GW* can get his own smart card and can extract information stored in that smart card [5], [6].
3) $\mathcal{U}_{\mathcal{A}}$ being insider can extract verifier table from *GW* database [7]–[11].

II. Review of the Scheme of Das *et al.*

This section briefly reviews Das *et al.* [1] scheme which comprises of three types of entity, the user U_i, the gateway node *GW*, and the smart device SD_j. The Gateway node *GW* mainly provides registration procedure to U_i and SD_j. The scheme of Das *et al.* consists of six phases, detailed as below.

A. Offline Smart Device Registration Phase

Following steps are followed to complete offline smart device registration phase.

Step OR 1: *GW* picks a unique identity ID_{SD_j} for every deployed smart device SD_j along with it's respective identity TID_{SD_j} and a unique secret key d_{SD_j}. The gateway node *GW* creates ID_{gw}, and temporary identity TID_{gw}, and k (unique master key) as well as d_{gw} (the secret key).

Manuscript received February 19, 2019; revised July 3, 2019; accepted July 28, 2019. Date of publication August 13, 2019; date of current version December 11, 2019. *(Corresponding author: Shehzad Ashraf Chaudhry.)*

S. Hussain is with the Department of Computer Science and Software Engineering, International Islamic University, Islamabad 54000, Pakistan (e-mail: sajid.mscs840@iiu.edu.pk).

S. A. Chaudhry is with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 Istanbul, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/JIOT.2019.2934947

Step OR 2: For every smart device SD_j, GW computes $RID_{SD_j} = h(ID_{gw}||k)$ and temporary $TC_{SD_j} = h(RID_{SD_j}\|ID_{gw}\|d_{gw}\|RTS_{SD_j})$, where the registration time stamp of SD_j is RTS_{SD_j}.

Step OR 3: Then GW creates t-degree bivariate symmetric polynomial $f(x, y) = \sum_i^t, j =_0 a_{ij}x^i y^j \in GF(p)[x, y]$, from finite field $GP(p) = Z_p, Z_p = 0, 1, \ldots, p-1$ the coefficient $a'_{ij}s$ are selected where p is large prime of 160-bit prime number. So $f(x, y)$ is symmetric, then $f(x, y) = f(x, y)$. Then, polynomial share for SD_j as $f(TID_{S_j}, y) = \sum^{t_i}, j =_0 a_{ij}(TID_{SD_j})^i y^j$ computed by GW, which is t-degree uni-variate polynomial and $GP_(p)$ is again its coefficients. Then, GW have to compute its own polynomial $f(TID_{gw}, y) = \sum^{t_i}, j =_0 a_{ij}(TID_{SD_j})^i y^j$.

Step OR 4: Now, SD_j is preloaded with $d_{SD_j}, TC_{SD_j}, (TID_{SD_j}, RID_{SD_j}), f(TID_{SD_j}, y)$ in some area for deployment. The GW also stores $k, ID_{gw}, d_{gw}, TID_{gw}, f(TID_{gw}, y)$, and TID_{SD_j}, RID_{SD_j} relevant to every SD_j.

B. User Registration Phase

The user registration phase consists of the following steps to complete the registration of a user U_i at the Gateway Node GW.

Step REG 1: U_i chooses an identity ID_i and imprints biometric BIO_i at the biometric device terminal. A fuzzy extractor is used in this scheme for biometric verification. The fuzzy extractor function produce biometric secret bk_i on the input of biometric BIO_i produce $Gen(BIO_i) = (bk_i, pr_i)$.

Step REG 2: U_i selects a secret key d_i, computes $RID_i = h(ID_i\|d_i)$ and sends (RID_i) to GW for registration request.

Step REG 3: Upon reception, GW computes $TC_i = h(RID_i\|d_{gw}\|RTS_i)$, the temporary identity of user TID_i and computes it's own $TC_{gw} = h(ID_{gw}\|d_{gw})$ and smart card SC_i having $[TID_i, TC_i, h(TC_{gw})]$ is handed over to user U_i securely. The GW also saves $[TIDI_i, RID_i]$ in its database related to the registered user U_i.

Step REG 4: User U_i computes $Gen(BIO_i) = (bk_i, pr_i)$, $d'_i = d_i \oplus h(bk_i\|ID_i)$, $TC'_i = TC_i \oplus h(d_i\|bk_i\|ID_i)$, $RID'_i = RID_i \oplus h(bk_i\|d_i)$, $TC'_{gw} = h(TC_{gw}) \oplus h(RID_i\|bk_i\|d_i)$, and $RB_i = h(ID_i\|bk_i)$ from GW. $[TID_i, RB_i, RID'_i, d'_i, TC'_i, TC'_{gw}, h(.), Gen(.), Rep(.), pr_i, et]$ in SC_i's memory and then discard TC_i and $h(TC_{gw})$.

C. Key Management Phase

The main purpose of this phase is to establish a pairwise secret key between GW and device SD_j. This step is performed only once when smart device is deployed in the IIoT environment.

Step KM 1: SD_j sends it's TID_{SD_j} to GW through insecure channel.

Step KM 2: The gateway node also sends TID_{gw} to SD_j through insecure channel.

Step KM 3: SD_j computes $K_{sdjgw} = h(f(TID_{SD_j}, TID_{gw})\|RID_{SD_j})$ using polynomial $f(TID_{SD_j}, y)$ and pseudo identity RID_{SD_j} and then saves the K_{sdjgw} in the memory.

Step KM 4: Then, GW computes $K_{sdjgw} = h(f(TID_{gw}, TID_{SD_j})\|RID_{SD_j})$, $(= K_{sdjgw})$ by using saved polynomial share $f(TID_{gw}, y)$ and also RID_{SD_j} of SD_j in the database. So, $f(TID_{SD_j}, TID_{gw}) = f(TID_{gw}, TID_{SD_j})$, and then store the key K_{sdjgw} in the database.

D. User Login and Authentication phase

The login and authentication phase as shown in Fig. 1 is initiated by a legitimate user U_i. Following steps are performed between user U_i, Gateway GW, and smart device SD_j.

Step LA 1: User first inputs Smart card SC_i, biometric BIO'_i, and identity ID_i. SC_i retrieves the original BIO'_i as $bk_i = Rep(BIO'_i, pr_i)$, given by $HamDist(BIO'_i, BIO_i) \le et$. SC_i further calculates $RB'_i = h(ID_i\|bk_i)$ and checks $RB'_i \stackrel{?}{=} RB_i$ if not so SC_i ends the session. SC_i computes $d_i = d'_i \oplus h(bk_i\|ID_i)$, $TC_i = TC'_i \oplus h(d_i\|bk_i\|ID_i)$, $RID_i = RID'_i \oplus h(d_i\|bk_i)$ and $TC^*_{gw} = TC'_{gw} \oplus h(RID_i\|bk_i\|d_i) = h(TC_{gw})$. The current time stamp T_1 and random nonce r_u are generated by SC_i, and then SC_i computes $TID'_i = TID_i \oplus h(TC^*_{gw}\|T_1)$, $X_i = h(RID_i\|TID_i\|T_1) \oplus h(d_i\|TC_i\|r_u\|RID_i\|T_1)$, and $Y_i = RID_{SD_j} \oplus h(TC^*_{gw}\|RID_i\|T_1)$. Also, SC_i computes $Z_i = h(h(d_i\|TC_i\|r_u\|RID_i\|T_1)\|TC^*_{gw}\|RID_i)$ and sends message to GW as a login Request $Msg_1 = <TID'_i, X_i, Y_i, Z_i, T_1>$.

Step LA 2: Once M_{sg1} is received from U_i. GW first checks the maximum transmission delay $|\ T^*_1 - T_1\ | \le \triangle T$, after that GW computes $TID_i = TID'_i \oplus h(h(TC_{gw})\|T_1)$. GW calculates $V_{gw} = X_i \oplus h(RID_i\|TID_i\|T_1) = h(d_i\|TC_i\|r_u\|RID_i\|T_1)$, $RID_{SD_j} = Y_i \oplus h(h(TC_{gw})\|RID_i\|T_1)$ and $W_{gw} = h(V_{gw}\|h(TC_{gw})\|RID_i)$, if $W_{gw} \stackrel{?}{=} Z_i$, then GW successfully authenticates U_i. GW generates current time-stamp T_2 and computes $X_{gw} = V_{gw} \oplus h(K_{gwsdj}\|RID_{SD_j}\|T_2) = h(d_i\|TC_i\|r_u\|RID_i\|T_1) \oplus h(K_{gwsdj}\|RID_{SD_j}\|T_2)$, $Y_{gw} = h(RID_i\|T_1) \oplus h(K_{gwsdj}\|TID_{SD_j}\|RID_{SD_j}\|T_2)$ and $Z_{gw} = h(X_{gw}\|Y_{gw}\|K_{gwsdj}\|T_2)$. Message $M_{sg2} = <X_{gw}, Y_{gw}, Z_{gw}, T_2>$ by GW is sent to SD_j.

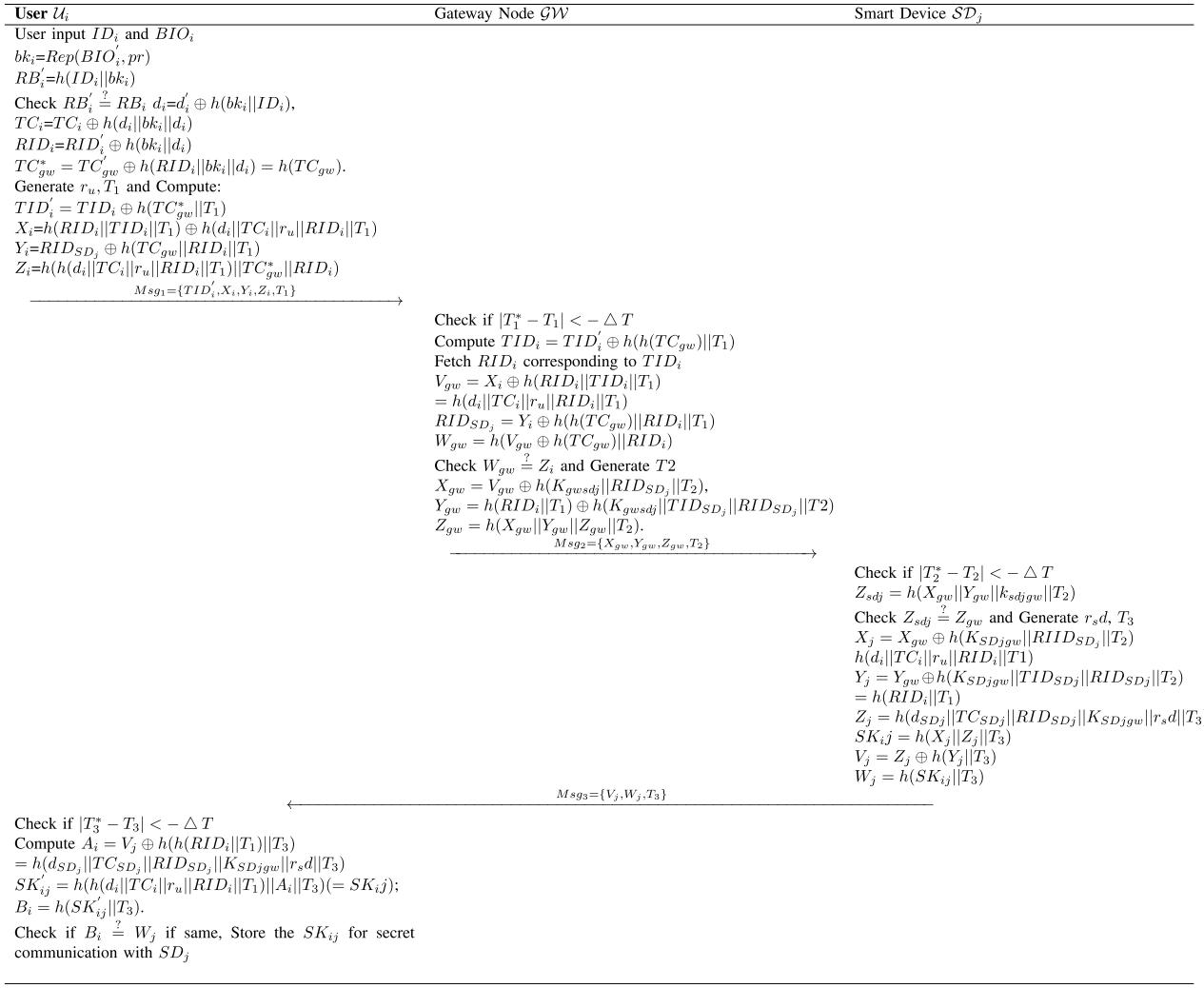

Fig. 1. Das *et al.*'s scheme.

Step LA 3: Upon reception of $M_{sg}2$, SD_j checks the maximum transmission delay $|T_2^{*} - T_2| \leq \triangle T$. Then SD_j compute $Z_{sdj} = h(X_{gw}\|Y_{gw}\|K_{sdjgw}\|T_2)$ by using pairwise key $K_{sdjgw}(= K_{gwsdj})$ with GW and then verifies $Z_{sdj} \stackrel{?}{=} Z_{gw}$, if so then SD_j authenticates GW. Then SD_j creates random nonce r_{sd} and time-stamp T_3 and computes $X_j = X_{gw} \oplus h(K_{sdjkw}\|\mathrm{RID}_{\mathrm{SD}_j}\|T_2) = h(d_i\|TC_i\|r_u\|\mathrm{RID}_i|T_1)$, $Y_j = Y_{gw} \oplus h(K_{sdjgw}\|\mathrm{TID}_{\mathrm{SD}_i}\|\mathrm{RID}_{\mathrm{SD}_j}\|T_2) = h(\mathrm{RID}_i\|T_1)$, $Z_j = h(d_{\mathrm{SD}_j}\|TC_{\mathrm{SD}_j}\|\mathrm{RID}_{\mathrm{SD}_j}\|K_{sdjgw}\|r_{sd}\|T_3)$, and session key $SK_{ij} = h(X_j\|Z_j\|T_3)$, $V_j = Z_j \oplus h(Y_j\|T_3)$ and $W_j = h(SK_{ij}\|T_3)$. Then, message $\mathrm{Msg}_3 = <V_j, W_j, T_3>$ is sent by SD_j to U_i.

Step LA 4: Upon reception of message $M_{sg}3$, user U_i checks transmission delay $|T_3^{*} - T_3| \leq \triangle T$. SC_i computes $A_i = V_j \oplus h(h(\mathrm{RID}_i\|T_1)\|T_3) = h(d_{\mathrm{SD}_j}\|TC_{\mathrm{SD}_j}\|\mathrm{RID}_{\mathrm{SD}_j}\|K_{sdjgw}\|r_{sd}\|T_3)$, and shared session key by smart devices SD_j, $\mathrm{SK}_{ij}' = h(h(d_i\|\mathrm{TC}_i\|r_u\|\mathrm{RID}_i\|T_1)\|A_i\|T_3)$ $(= \mathrm{SK}_{ij})$, $B_i = h(\mathrm{SK}_{ij}'\|T_3)$. U_i checks $B_i \stackrel{?}{=} W_j$. U_i rejects the session key in case of failure. At the last user U_i and smart devices SD_j store the computed session key for future secure communication.

III. Weaknesses of Das *et al.*'s Scheme

This section shows that the authentication scheme for cloud-based IIoT by Das *et al.* [1] is vulnerable to traceability, stolen-verifier, and stolen smart device attacks. Moreover, this section also shows that their scheme does not provide perfect forward secrecy.

A. Traceability Attack

Let $\mathcal{U}_\mathcal{A}$ be a dishonest but legal user registered with the system and by using his own smart card and biometrics $\mathcal{U}_\mathcal{A}$ computes

$$\mathrm{TC}_{gw}^{*} = h(\mathrm{TC}_{gw}). \tag{1}$$

Let another user U_i initiate a login request by sending message $\mathrm{Msg}_1 = \{\mathrm{TID}_i', X_i, Y_i, Z_i, T_1)\}$, $\mathcal{U}_\mathcal{A}$ intercepts the message and

compute

$$\mathrm{TID}_i = \mathrm{TID}'_i \oplus h(TC^*_{gw}||T_1) \quad (2)$$

where TID_i remains same for all sessions, therefore $\mathcal{U}_\mathcal{A}$ has launched successful traceability attack.

B. Stolen-Verifier Attack

Let $\mathcal{U}_\mathcal{A}$ be an insider of Gateway node (GW), $\mathcal{U}_\mathcal{A}$ based on his privileges steals verifier table from *GW* database. $\mathcal{U}_\mathcal{A}$ may get TID_i and corresponding RID_i. Now, based on the verifier information pair $\{\mathrm{TID}_i, \mathrm{RID}_i\}$ and the extracted $TC^*_{gw} = h(TC_{gw})$, $\mathcal{U}_\mathcal{A}$ can compute the session key shared between a user U_i and a smart device SD_j as follows.

Step SVA 1: U_i initiates login request by sending $\mathrm{Msg}_1 = <\mathrm{TID}'_i, X_i, Y_i, Z_i, T_1>$ to *GW*.

Step SVA 2: $\mathcal{U}_\mathcal{A}$ intercepts the message and computes

$$\mathrm{TID}_i = \mathrm{TID}'_i \oplus h(\mathrm{TC}_{gw}||T_1). \quad (3)$$

$\mathcal{U}_\mathcal{A}$ using stolen verifier, extracts corresponding RID_i, and computes

$$V_{gw} = X_i \oplus h(\mathrm{RID}_i||\mathrm{TID}_i||T_1) \quad (4)$$

$$= h(d_i||TC_i||r_u||\mathrm{RID}_i||T_1). \quad (5)$$

Step SVA 3: *GW* after verification of U_i credentials directs $\mathrm{Msg}_2 = <X_{gw}, Ygw, Z_{gw}, T_2>$ to SD_j.

Step SVA 4: SD_j after validation of Msg_2 sends $\mathrm{Msg}_3 = <V_j, W_j, T_3>$ to U_i. $\mathcal{U}_\mathcal{A}$ intercepts the message.

Step SVA 5: U_i computes session key $\mathrm{SK}_{ij} = h(h(d_i||TC_i||r_u||\mathrm{RID}_i||T_1)||A_i||T_3)$.

Step SVA 6: $\mathcal{U}_\mathcal{A}$ computes

$$A_i = V_j \oplus h(h(\mathrm{RID}_i||T_1)||T_3) \quad (6)$$

Step SVA 7: Finally, $\mathcal{U}_\mathcal{A}$ computes the session key

$$\mathrm{SK}_{ij} = h\big(V_{gw}||A_i||T_3\big). \quad (7)$$

The session key computed by U_i and SD_j is same as computed by $\mathcal{U}_\mathcal{A}$ in (7). Therefore, the shared secret key has been compromised using stolen verifier attack.

C. Stolen Smart Device Attack

Let $\mathcal{U}_\mathcal{A}$ manages to get $TC_{\mathrm{SD}_j}, (\mathrm{TID}_{\mathrm{SD}_j}, \mathrm{RID}_{\mathrm{SD}_j}), f(\mathrm{TID}_{\mathrm{SD}_j,y})$ stored in smart device, then $\mathcal{U}_\mathcal{A}$ can easily compute $Y_j = Y_{gw} \oplus h(K_{sdjgw}||TC_{\mathrm{SD}_j}||\mathrm{RID}_{\mathrm{SD}_j}||T_2)$, $Z_j = V_j \oplus h(Y_j||T_3)$ and $X_j = X_{gw} \oplus h(K_{sdjgw}||\mathrm{RID}_{\mathrm{SD}_j}||T_2)$. Finally, $\mathcal{U}_\mathcal{A}$ can compute the session key $\mathrm{SK} = h(X_j||Z_j||T_3)$. Therefore, Das *et al.*'s scheme is vulnerable to stolen smart device attack.

D. Non Provision of Perfect Forward Secrecy

In Das *et al.*'s scheme, an adversary $\mathcal{U}_\mathcal{A}$ can easily compute $\mathrm{RID}_{\mathrm{SD}_j} = h(\mathrm{ID}_{gw}||k)$, $TC_{\mathrm{SD}_j} = h(\mathrm{RID}_{\mathrm{SD}_j}||\mathrm{ID}_{gw}||d_{gw}||\mathrm{RTS}_{\mathrm{SD}_j})$, $Y_j = Y_{gw} \oplus h(K_{sdjgw}||TC_{\mathrm{SD}_j}||\mathrm{RID}_{\mathrm{SD}_j}||T_2)$, $Z_j = V_j \oplus h(Y_j||T_3)$, $X_j = X_{gw} \oplus h(K_{sdjgw}||\mathrm{RID}_{\mathrm{SD}_j}||T_2)$, and $SK = h(X_j||Z_j||T_3)$, if the GW node's secret keys k and d_{gw} are compromised. Therefore, Das *et al.*'s scheme fails to provide perfect forward secrecy.

IV. Discussion on Attack Resilience

This section describes some necessary guidelines on attack resilience overlooked by Das *et al.* during design phase of their biometric-based authentication scheme for IIoT structured over the symmetric key primitives.

1) The Gateway node should not store any verifier table and if it is necessary; to resist any stolen verifier attack, the verifier should be stored in encrypted form.
2) Every user must have one or more unique parameters for authentication purposes, i.e., the login request may not be formed on generic parameters.
3) To achieve anonymity and to resist traceability attack in a cryptographic system based merely on the symmetric key primitives, either the user may store a long range of unlinked pseudo identities or gateway node after each successful login request should send a new identity to the user for next login.
4) The session key should comprise of some randomly generated nonpublic parameters and that too from each user and smart device to provide perfect forward secrecy as well as to provide resistance to smart device stolen attack.

V. Conclusion

In this comment, we have shown that Das *et al.*'s biometric-based authentication scheme for IIoT is vulnerable to traceability, stolen verifier, and stolen smart device attacks. A legal but dishonest user of the system can easily launch traceability attack. Moreover, the dishonest user after stealing the verifier table and/or parameters stored in smart device can compute any session key shared among smart device and users. We have also shown that Das *et al.*'s scheme fails to provide perfect forward secrecy. Finally, we have provided some guidelines on attack resilience for the authentication schemes based on merely the symmetric key primitives.

Acknowledgment

The authors would like to thank the anonymous reviewers and the Editor Prof. I. Bisio for their valuable recommendations to improve the quality, correctness, presentation, and readability of this article.

References

[1] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018. doi: 10.1109/JIOT.2018.2877690.

[2] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the power of power analysis in the real world: A complete break of the KEELOQ code hopping scheme," in *Advances in Cryptology—CRYPTO* (LNCS 5157), D. Wagner, Ed. Heidelberg, Germany: Springer, 2008, pp. 203–220.

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

[4] X. Cao and S. Zhong, "Breaking a remote user authentication scheme for multi-server architecture," *IEEE Commun. Lett.*, vol. 10, no. 8, pp. 580–581, Aug. 2006.

[5] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[6] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO*. Heidelberg, Germany: Springer, 1999, pp. 388–397.
[7] C.-M. Chen and W.-C. Ku, "Stolen-verifier attack on two new strong-password authentication protocols," *IEICE Trans. Commun.*, vol. 85, no. 11, pp. 2519–2521, 2002.
[8] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2018.
[9] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.
[10] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 4, pp. 633–645, Jul./Aug. 2018.
[11] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1621–1631, Jun. 2018.

Sajid Hussain received the M.S. degree from International Islamic University, Islamabad, Pakistan, in 2018.

His current research interests include computer networking, network security, network communication, information security, cryptography, elliptic/hyper elliptic curve cryptography, encryption, and authentication.

Shehzad Ashraf Chaudhry received the master's and Ph.D. degrees (with Distinction) from International Islamic University, Islamabad, Pakistan, in 2009 and 2016, respectively.

He is currently with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey. He has authored over 75 scientific publications appeared in different international journals and proceedings, including 55 in SCI/E journals. With an H-index of 20 and an I-10 index of 35, his work has been cited over 1175 times. He has also supervised over 35 graduate students in their research. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystem, and next generation networks. He occasionally writes on issues of higher education in Pakistan.

Dr. Chaudhry was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientists in Pakistan. He has served as a TPC member of various international conferences and is an Active Reviewer of many ISI indexed journals.