On The Security of PACMAN: Privacy-Preserving Authentication Scheme for Managing Cybertwin-Based 6G Networking

Myeonghyun Kim
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Republic of Korea
kimmyeong123@knu.ac.kr

Seunghwan Son
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Republic of Korea
sonshawn@knu.ac.kr

Youngho Park
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Republic of Korea
parkyh@knu.ac.kr

Kilhoum Park
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Republic of Korea
khpark@ee.knu.ac.kr (Corresponding author)

***Abstract*—Cybertwin-based cloud-centric networks are attracting considerable attention as new multiaccess edge computing network architecture in 6G networks. However, the sensitive data transmitted between the cybertwin and users/things via wireless communication can be intercepted and hijacked by malicious attackers, resulting in security threats and privacy concerns owing to leakage or abuse. Therefore, secure authentication and key agreement schemes are essential to ensure secure communication in cybertwin-based networks. In 2021, Soleymani *et al.* presented a privacy-preserving authentication scheme for managing cybertwin-based 6G netoworking (PACMAN). Soleymani *et al.* claimed that their scheme can satisfy privacy-preserving requirements and resist security threats. However, we demonstrates that PACMAN fails to achieve privacy-preserving requirement. Thus, we suggest the necessary security guidelines to achieve privacy-preserving and resolve the security risks of PACMAN.**

***Index Terms*—Cryptanalysis, cybertwin, authentication, privacy-preserving, security**

I. Introduction

With the development of 6G network technology as well as smart device and applications technology in the industry, a vast number of sensor nodes/smart devices have been embedded in industrial applications, and the degree of interconnection and amount of data processed have multiplied [1]. Therefore, research on a new network architecture based on cybertwin that can provide three functions such as the communication assistant, behavior logger and digital assets in the edge server is currently underway to improve the flexibility and scalability of the integrated 6G industrial network [2]–[5]. Cybertwin regarded as a new multiaccess edge computing technique to create digital representation of humans or devices in the edge server can obtain necessary services from service providers, and provide services to users/things. However, because wireless communication is used to transmit data between the cybertwin and users/things in a cybertwin-based network architecture, the data are susceptible to potential security threats and privacy breaches [6]–[9]. Therefore, authentication and key agreement are required for secure service delivery in cybertwin-based network architecture.

In 2022, Soleymani *et al.* [10] designed an authentication protocol with a privacy-preserving based on digital signature and authenticated key exchange (termed PACMAN) to generate and share the session key for secure communication in the cybertwin-based network architecture. They claimed that PACMAN can resist security threats while preserving privacy. However, this paper demonstrates that PACMAN fails to satisfy the privacy-preserving requirements. Unlike the claim of Soleymani *et al.*, malicious adversaries who obtain the same secret credential distributed to the participants in the system can extract the private keys of other participants and extract the real identities of authorized users.

II. Review of Soleymani *et al.*'s scheme

A. Initialization phase

The trusted authority (TA) generates the system parameters $\{p, q, E_q(a, b), G, P, P_{pub}, h\}$ and publishes them in the network for all entities, where $pandq$ are primes, $E_q(a, b)$ is a nonsingular elliptic curve, G is the group of order q, $P(\in G)$ is the generator, s and $P_{pub} = s \cdot P$ are the master private key and the public key of TA, respectively, and $h : \{0, 1\}^* \rightarrow Z_q^*$ is a secure one-way hash function.

B. Registration Phase

The registration of cybertwin and user is achieved by TA.

This study was supported by the BK21 Four project funded by the Ministry of Education, Korea (4199990113966).

- **Cybertwin:** Each cybertwin CT_j registered by the TA has a unique ID_j, private key SK_j, public key $PK_j = SK_j \cdot P$, and master secret key X_j.
- **User:** User U_i has a private key SK_i and public key PK_i. For each user, TA selects the real identity ID_i, password PW_i and sends the encrypted message $Z_i = Enc_{PK_i}\{Y_i, SNG_{SK_{TA}}(Y_i)\}$ to the user, where $Y_i = \{ID_i, PW_i, s\}$. After receiving Z_i, U_i decrypts the Z_i to obtain $\{ID_i, PW_i, s\}$ and checks the signature $SNG_{SK_{TA}}(Y_i)$ using PK_{TA}, where s is used later in the authentication phase. Furthermore, U_i employes the fuzzy extractor and biometric data BIO_i to extract R_i, $P_i = Gen(BIO_i)$ as its biometric information stored in the mobile device. Then, U_i selects a random number r_i and computes $HPW_i = h(PW_i||r_i)$. Finally, U_i securely submits the registration request $\{ID_i, PW_i, R_i\}$ to its cybertwin host. Upon receiving this request, its cybertwin CT_j checks whether ID_i is in the database. If it exists, the user needs to choose a new identity. Otherwise, CT_j computes $B_1 = h(ID_i||PW_i||R_i)$, $B_2 = h(ID_i||X_j)$, $B_3 = h(PW_i||R_i) \oplus B_2$. Finally, The CT_j sends $\{B_1, B_3, X\}$ to U_i, securely. Once the parameters are received from CT_j, U_i stores $\{P_i, r_i, B_1, B_3, X, Gen(), Rep()\}$ into the mobile device.

C. Authentication Phase

In this phase, U_i requests authentication to its cybertwin CT_j in order to establish the session key SK_{U-CT}. The detailed steps of this phase are as follows.

- **Step 1:** U_i inputs the identity ID_i and password PW_i and imprints biometric information BIO_i in its device. It calculates $R_i = Rep(BIO_i, P_i)$, $B_1' = h(ID_i||h(PW_i||r_i)||R_i)$ and checks the $B_1' = B_1$. If it is not valid, the login request is rejected. Otherwise, if it is valid, U_i selects a random number $x_i \in Z_q^*$ and computes $B_2 = B_3 \oplus h(HPW_i||R_i)$, $D_1 = x_i \cdot P$, $D_2 = x_i \cdot PK_j$, $PID_i = ID_i \oplus h(D_2)$, $D_3 = h(B_2||D_2)$ and signature $\sigma_i = SK_i + s \cdot h(PID_i||M_1)$, where $M_1 = \{D_1, D_3, T_1\}$ and T_1 denotes the current timestamp. Then, U_i sends $\{PID_i, M_1, \sigma_i\}$ to its cybertwin host CT_j.
- **Step 2:** CT_j assesses $\sigma_i \cdot P = PK_i + P_pub \cdot h(PID_i||M_1)$ and checks whether the T_1 is fresh. If it is valid, CT_j computes $D_2' = SK_j \cdot D_1$, $ID_i' = PID_i \oplus h(D_2')$ and checks whether ID_i is in the database. If it holds, CT_j computes $B_2' = h(ID_i||X_j)$ and $D_3' = h(B_2'||D_2')$ and checks $D_3' = D_3$. if $D_3' \neq D_3$, the request is terminated. Otherwise, CT_j generates $x_j \in Z_q^*$ and computes $D_4 = x_j \cdot P$, $SK_{U-CT} = h(D_1||D_4||x_j \cdot D_1)$, $D_5 = h(ID_i'||D_1||D_4||B_2')$ and signature $\sigma_j = SK_j + s \cdot h(ID_j||M_2)$, where $M_2 = \{D_4, D_5, T_2\}$ and T_2 denotes the current timestamp. Then, CT_j sends $\{ID_j, M_2, \sigma_j\}$ to U_i.
- **Step 3:** U_i assesses $\sigma_j \cdot P = PK_j + P_pub \cdot h(ID_j||M_2)$ and checks whether the T_2 is fresh. If it is valid, U_i calculates $D_5' = h(ID_i||D_1||D_4||B_2)$ and checks $D_5' \stackrel{?}{=} D_5$. If it holds, U_i calculates $SK_{U-CT}' = h(D_1||D_4||x_i \cdot D_4)$.

III. Cryptanalysis of Soleymani *et al.*'s scheme

A. Adversary Model

We present the widely-known Dolev-Yao (DY) model [11]–[14] to evaluate the security of PACMAN. The adversary Adv can have the following capabilities based on the DY threat model.

- An Adv can replay, eavesdrop, modify, intercept, insert, and delete the transmitted messages through an insecure channel.
- An Adv can physically capture the user's mobile device to deduce sensitive data through power analysis attacks. [15]–[17].
- An Adv can attempt various attacks, such as insider, impersonation, man-in-the-middle, and replay attacks.

B. Leakage of private key

Referring to Section III-A, Adv can extract the secret data $\{s\}$ stored in a mobile device. Subsequently, Adv can extract the private key of U_i and CT_j from public messages by using s. The detailed steps are as follows.

Leakage of U_i's private key:

- **Step 1:** Adv obtains the $\{PID_i, D_1, D_3, T_1, \sigma_i\}$ transmitted through an insecure channel.
- **Step 2:** Adv can extract the U_i's private key SK_i by calculating
  $\sigma_i - s \cdot h(PID_i||D_1||D_3||T_1)$
  $= SK_i + s \cdot h(PID_i||D_1||D_3||T_1) - s \cdot h(PID_i||D_1||D_3||T_1)$
  $= SK_i$.

Leakage of CT_j's private key:

- **Step 1:** Adv obtains the $\{ID_j, D_4, D_5, T_2, \sigma_j\}$ transmitted through an insecure channel.
- **Step 2:** Adv can extract the CT_j's private key SK_j by calculating
  $\sigma_j - s \cdot h(ID_j||D_4||D_5||T_2)$
  $= SK_j + s \cdot h(ID_j||D_4||D_5||T_2) - s \cdot h(ID_j||D_4||D_5||T_2)$
  $= SK_j$.

In addition to this key leakage problem, all system entities that know the secret value s can obtain the private key of other legitimate entities in the same way as abovementioned. Therefore, Soleymani *et al.*'s assertion that privacy-preserving can be achieved because third parties cannot obtain private information about legitimate users or CTs is incorrect.

C. Leakage of user's real identity

Referring to Section III-B, Adv can calculate the private key SK_j. Subsequently, Adv can extract the user's real identity from the user's pseudo-identity PID_i. The detailed steps are as follows.

- **Step 1:** Adv obtains the $\{PID_i, D_1, D_3, T_1, \sigma_i\}$ transmitted through an insecure channel.
- **Step 2:** Adv can extract the U_i's real identity ID_i by calculating
  $PID_i \oplus h(D_i \cdot SK_j)$
  $= ID_i \oplus h(D_2) \oplus h(D_i \cdot SK_j)$

$= ID_i \oplus h(D_i \cdot SK_j) \oplus h(D_i \cdot SK_j)$
$= ID_i$.

Therefore, Soleymani *et al.*'s assertion that privacy-preserving can be achieved because third parties are unable to extract the real identity from the user's pseudo-identity is incorrect.

IV. Guidelines on privacy perseving enhancement

In Section III, we demonstrate that PACMAN fails to ensure the praivcay preserving. Thus, we suggest the necessary guidelines to enhance the privacy-preserving of PACMAN.

- **Guideline 1.** In the PACMAN scheme, the U_i's mobile device used s, which is stored in its memory, to sign the messages. However, referring to Section III, Adv can extract the private key and real identity of users from the messages transmitted through a insecure channel. Thus, PACMAN should store masked secret credentials with password and/or biometric information using XOR and hash function operations to increase the security level of the systems, while preventing the leakage of secret credentials to external adversaries.
- **Guideline 2.** In the PACMAN scheme, all entities receive the same secret credential from the TA. However, referring to Section III, Adv and participants in the system can extract the private key and real identity of the authorized users. Therefore, TA should issue a unique secret credential to each registering entity to prevent the privacy breaches caused by the use of the same credential.
- **Guideline 3.** All participants must securely encrypt and transmit the messages using symmetric keys, because Adv can replay, eavesdrop, modify, intercept, insert, and delete the transmitted messages during authentication phase.

V. Conclusion

We analyze the security vulnerabilities of Privacy-preserving authentication scheme for managing cybertwin-based 6G networking proposed by Soleymani *et al.* We have demonstrated that the scheme does not satisfy the privacy-preserving requirements as claimed and does not guarantee the security of the private key. Furthermore, a malicious adversary (who steals secret information from a mobile device) or an insider of the system can easily steal sensitive information about other entities, posing a potential security risk. Therefore, we have presented the necessary guidelines to achieve privacy-preservation and resolve the security risks of Soleymani *et al.*'s scheme.

References

[1] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7204-7212, Oct. 2021.

[2] Q. Yu, J. Ren, Y. Fu, Y. Li, and W. Zhang, "Cybertwin: An origin of next generation network architecture," *IEEE Wireless Commun.*, vol. 26, no. 6,pp. 111–117, Dec. 2019.

[3] Q. Yu, J. Ren, H. Zhou, and W. Zhang, "A cybertwin based network architecture for 6G," *in Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Levi, Finland, 2020, pp. 1-5.

[4] D. K. Jain, S. K. S. Tyagi, S. Neelakandan, M. Prakash, and L. Natrayan, "Metaheuristic optimization-based resource allocation technique for cybertwin-driven 6G on IoE environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4884-4892, Jul. 2022.

[5] W. Qi and H. Su, "A cybertwin based multimodal network for ECG patterns monitoring using deep learning," *IEEE Trans. Ind. Informat.*,, vol. 18, no. 10, pp. 6663-6670, Oct. 2022.

[6] G. Li, C. Lai, R. Lu, and D. Zheng, "SecCDV: A security reference architecture for cybertwin-driven 6G V2X," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4535-4550, May 2022.

[7] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "BDTwin: An integrated framework for enhancing security and privacy in cybertwin-driven automotive industrial internet of things," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17110-17119, Sep.2022.

[8] M. Kim, J. Lee, J. Oh, D. Kwon, K. Park, Y. Park, and K. H. Park, "A secure batch authentication scheme for multiaccess edge computing in 5G-enabled intelligent transportation system," *IEEE Access*, vol. 10, pp. 96224-96238, 2022.

[9] S. Son, D. Kwon, J. Lee, S. Yu, N. -S. Jho, and Y. Park, "On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain," *IEEE Access*, vol. 10, pp. 75365-75375, 2022.

[10] S. A. Soleymani, S. Goudarzi, M. H. Anisi, Z. Movahedi, A. Jindal, and N. Kama, "PACMAN: Privacy-preserving authentication scheme for managing cybertwin-based 6G networking," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4902-4911, Jul. 2022.

[11] 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.

[12] J. Oh, J. Lee, M. Kim, Y. Park, K. Park, and S. Noh, "A secure personal health record sharing system with key aggregate dynamic searchable encryption," *Electronics*, vol. 11, no. 9, p. 3199, Oct. 2022.

[13] M. Kim, J. Lee, J. Oh, K. Park, Y. Park, and K. Park, "Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers," *Appl. Energy*, vol. 322, p. 119445, Sep. 2022.

[14] M. Wang, L. Rui, Y. Yang, Z. Gao, and X. Chen, "A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 3, pp. 2664-2676, Sep. 2022.

[15] 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.

[16] J. Lee, G. Kim, A. K. Das, and Y. Park, "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2412-2425, Jul.-Sep. 2021.

[17] S. Yu, A. K. Das, and Y. Park, "Comments on "ALAM: Anonymous lightweight authentication mechanism for SDN enabled smart homes"," *IEEE Access*, vol. 9, pp. 49154-49159, Mar. 2021