IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 17, 2021, accepted March 17, 2021, date of publication March 24, 2021, date of current version April 5, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3068723

Comments on "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes"

SUNGJIN YU[1,3], ASHOK KUMAR DAS[2], (Senior Member, IEEE), AND YOUNGHO PARK[3,4], (Member, IEEE)

[1]Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]School of Electronics and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
[4]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

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

This work was supported by the Electronics and Telecommunications Research Institute (ETRI) Grant by the Korean Government through the Core Technology Research on Trust Data Connectome under Grant 20ZR1300.

ABSTRACT Smart home is intended to be able to enhance home automation systems and achieves goals such as reducing operational costs and increasing comfort while providing security to mobile users. However, an attacker may attempt security attacks in smart home environments because he/she can inject, insert, intercept, delete, and modify transmitted messages over an insecure channel. Secure and lightweight authentication protocols are essential to ensure useful services in smart home environments. In 2020, Iqbal *et al.* presented an anonymous lightweight authentication protocol for software-defined networking (SDN) enabled smart home, called ALAM. They claimed that ALAM protocol could resist security threats, and also provide secure mutual authentication and user anonymity. This comment demonstrates that ALAM protocol is fragile to various attacks, including session key disclosure, impersonation, and man-in-the-middle attacks, and also their scheme cannot provide user anonymity and mutual authentication. We propose the essential security guidelines to overcome the security flaws of ALAM protocol.

INDEX TERMS Cryptanalysis, smart homes, key establishment, authentication, security protocol.

I. INTRODUCTION

With the advances in wireless technologies and portable devices, users can access various services via mobile device in smart home environments. The smart home allows useful services for the mobile users, including humidity of the house, automatic checking of the temperature, controlling light bulbs, and so on. In general, the smart home comprises several indoor smart devices, gateways, users, and controllers. Mobile users are registered in the controller, and they can access various services. However, these services are susceptible to potential attacks because sensitive messages are exchanged via an insecure channel. If the data collected by smart devices is compromised, a malicious attacker can obtain the private information of users, including habits and daily routines in smart home, and also utilize the information for criminal purposes. Therefore, a secure and lightweight authentication protocol is essential to provide mobile users with useful services in smart home environments.

In 2020, Iqbal *et al.* [1] designed an anonymous lightweight authentication protocol to provide secure services in smart home environments. They claimed that ALAM protocol could withstand security threats, such as desynchronization and replay attacks, and also ensure user anonymity and mutual authentication. However, this comment paper demonstrates that ALAM protocol suffers from many security threats, including impersonation, session key disclosure and man-in-the-middle (MITM) attacks. Moreover, ALAM protocol cannot also provide user anonymity and mutual authentication. Thus, we propose the necessary guidelines to overcome the security flaws of ALAM scheme [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Remigiusz Wisniewski.

The rest of this comment paper is organized as follows. In Section II and III, we review Iqbal *et al.*'s protocol and then show cryptanalysis of Iqbal *et al.*'s protocol, respectively. Section IV proposes some guidelines to overcome the security shortcomings of Iqbal *et al.*'s protocol. Finally, Section V summarizes and concludes the work.

A. ATTACKER MODEL

We present the widely-known Dolev-Yao (DY) model [2] to evaluate the security of ALAM protocol. The capabilities of an attacker in the DY model are as follows.

- Referring to DY model [2], a malicious adversary (MA) can replay, eavesdrop, modify, intercept, insert, and delete transmitted messages over an insecure channel.
- Software-defined networking (SDN) database modules and controllers are considered to be secure and cannot be compromised by MA. In other words, the controller's private key is not accessible to the MA [1].
- During a lost mobile device attack, MA obtains all secret credentials stored in mobile device by physical means, even if the mobile device has a certain degree of tamper resistance. Thus, MA can steal the legitimate user's mobile device and extract the secret credentials stored in memory by performing power analysis [3]–[5].
- After obtaining the secret credentials of the mobile device, MA may attempt various attacks such as "insider attack", "MITM attack", and "desynchronization attack", etc [6], [7].

B. RESEARCH CONTRIBUTIONS AND MOTIVATION

The major goal of this comment paper is to identify the security flaws present in ALAM scheme. ALAM does not ensure the required security functionalities such as "session key disclosure attack", "MITM attack", "impersonation attack", "mutual authentication", and "user anonymity" in smart home environments. These facts motivated us to come up with the necessary security guidelines which can ensure security functionalities and overcome security threats and flaws that exist in smart home environments.

II. REVIEW OF IQBAL *ET AL.*'S PROTOCOL

We review ALAM scheme [1] for a smart home environment. ALAM scheme consists of three phases: a) user registration, b) smart device registration and c) mutual authentication. The notations used in this comment are presented in Table 1.

TABLE 1. Notations.

Symbol	Description
MU_i	Mobile user
CT	Controller
SD_i	Smart device
U_{ID}	Identity of user
M_{ID}	Identity of mobile device
C_c	Counter of controller
k_{uc}	Shared secret key between controller and user
C_n, U_n	Random nonce of controller and user
CSP	Controller session parameter
SID	Session identifier
SD_{ID}	Identity of IoT smart device
$Auth.DB$	Database of authenticator manager
$Reg.DB$	Database of registration manager
$\triangle T$	Threshold difference in time
$E_K(), D_K()$	Encryption/decryption
$h()$	Hash function
$\oplus$	XOR operation

A. USER REGISTRATION PHASE

The mobile users (MU_i) must register with the SDN controller (CT) to receive smart home services. We show the user registration phase of ALAM protocol, and the detailed steps are as follows:

- **UR-1:** MU_i chooses user identity U_{ID}, and mobile identity M_{ID}. Then, MU_i sends $\{U_{ID}, M_{ID}\}$ to CT via a secure channel.
- **UR-2:** After getting message $\{U_{ID}, M_{ID}\}$, CT increases the value C_c and produces a transaction flow sequence number $C_c = TF_{seq}$ using a shared secret key k_{uc}. After that, CT generates a random nonce C_n and computes $CSP_{M_{ID}} = h(U_{ID} || M_{ID} || C_n)$ and $SID_u = E_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$. Then, CT sends $\{SID_u, k_{uc}\}$ to the mobile user over a secure channel. Finally, CT sends $\{SID_u, CSP_{M_{ID}}, k_{uc}, TF_{seq}\}$ to the $Reg.DB$ and $Auth.DB$.
- **UR-3:** Upon getting message $\{SID_u, k_{uc}\}$ from the CT, MU_i stores them in mobile memory.
- **UR-4:** After getting message $\{SID_u, CSP_{M_{ID}}, k_{uc}, TF_{seq}\}$, $Reg.DB$ and $Auth.DB$ also store them in secure database.

B. SMART DEVICE REGISTRATION PHASE

The smart device (SD_i) must register with the SDN controller to ensure useful home services. We present the smart device registration phase of ALAM protocol, and the detailed steps are as below.

- **SR-1:** SD_i chooses smart device identity SD_{ID} and then sends $\{SD_{ID}\}$ to the CT over a secure channel.
- **SR-2:** Upon getting message $\{SD_{ID}\}$, the CT generates controller identifier CID and random nonce C_m. CT then computes $CSP_{SD_{ID}} = h(SD_{ID} || C_m)$ and $SID_{SD_{ID}} = E_{k_c}(SD_{ID}, CSP_{SD_{ID}}, C_m)$. After that, the CT sends $\{SID_{SD_{ID}}, CID\}$ to the smart device SD_i over a secure channel. Finally, CT sends $\{SID_{SD_{ID}}, CSP_{SD_{ID}}\}$ to the $Reg.DB$ and $Auth.DB$.
- **SR-3:** After getting message $\{SID_{SD_{ID}}, CID\}$ from the CT, SD_i stores them in memory.
- **SR-4:** Upon getting message $\{SID_{SD_{ID}}, CSP_{SD_{ID}}\}$, $Reg.DB$ and $Auth.DB$ also store them in their secure database.

C. MUTUAL AUTHENTICATION PHASE

In this phase, a mobile user MU_i requests authentication to the SDN controller to receive secure service. We describe

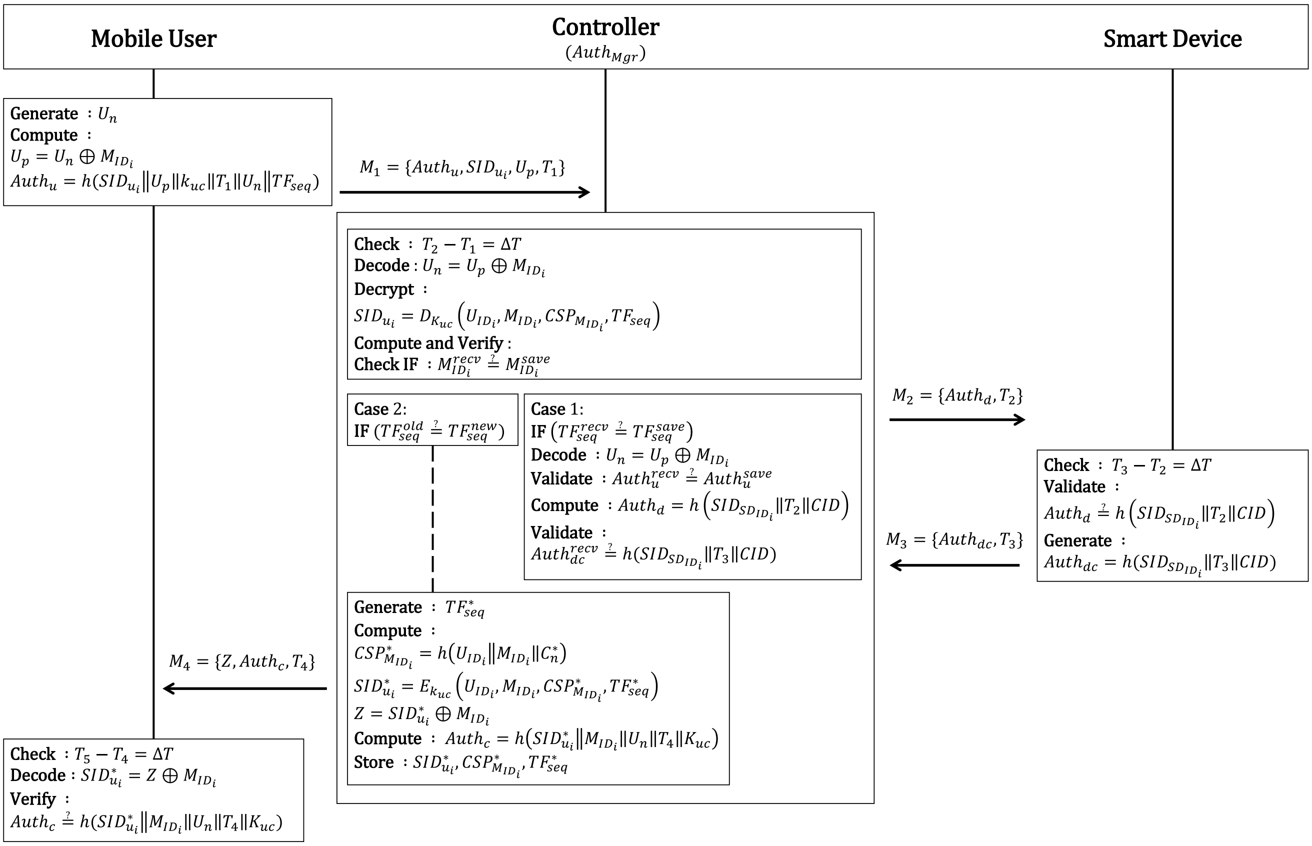

FIGURE 1. **Mutual authentication phase of Iqbal *et al.*'s scheme.**

the authentication phase of ALAM protocol as summarized in Fig. 1 and the detailed steps of this phase are as follows.

- **AP-1:** MU_i generates a random nonce U_n and a timestamp T_1, computes $U_p = U_n \oplus M_{ID}$ and $Auth_u = h(SID_u \,||U_p \,||k_{uc} \,||T_1 \,||U_n \,||TF_{seq})$, and the sends the message $M_1 = \{Auth_u, SID_u, U_p, T_1\}$ to the CT over an insecure channel.
- **AP-2:** Upon getting the message M_1, the CT checks timestamp $T_2 - T_1 = \Delta T$ and decodes $U_n = U_p \oplus M_{ID}$. The CT decrypts $SID_u = D_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$ and checks $M_{ID}^{recv} \stackrel{?}{=} M_{ID}^{save}$. If it is valid, CT can come across two scenarios. In the following, we discuss the following two cases.

Case 1.

- **AP-3:** If $TF_{seq}^{recv} \stackrel{?}{=} TF_{seq}^{save}$, MU_i will always be true in authentication request after registration and decodes $U_n = U_p \oplus M_{ID}$. Then, CT verifies $Auth_u^{recv} \stackrel{?}{=} Auth_u^{save}$. If it is valid, CT generates a timestamp T_2 and computes $Auth_d = h(SID_{SD_{ID}} \,||T_2 \,||CID)$. After that, CT sends the message $M_2 = \{Auth_d, T_2\}$ to the SD_i over an insecure channel.
- **AP-4:** Upon getting the message M_2, SD_i checks $T_3 - T_2 = \Delta T$ and computes $Auth_d^* = h(SID_{SD_{ID}} \,||T_2 \,||CID)$, and checks $Auth_d^* \stackrel{?}{=} Auth_d$. If it is correct, SD_i computes $Auth_{dc} = h(SID_{SD_{ID}} \,||T_3 \,||CID)$ and sends the message $M_3 = \{Auth_{dc}, T_3\}$ to the CT via an open channel.
- **AP-5:** Upon getting the message M_3, CT computes $Auth_{dc}^* = h(SID_{SD_{ID}} \,||T_3 \,||CID)$ and verifies $Auth_{dc}^* \stackrel{?}{=} Auth_{dc}$. If it is valid, SD_i is authenticated successfully.

Case 2.

- **AP-6:** CT either the received $Auth_{dc}$ from the SD_i in M_3 is checked or if the received TF_{seq} from the MU_i is old, whereas CT is waiting for new TF_{seq}^{new}. Then, CT verifies $TF_{seq}^{old} \stackrel{?}{=} TF_{seq}^{new}$. If it is valid, CT generates TF_{seq}^* and updates $\{TF_{seq}\}$ with $\{TF_{seq}^*\}$, and stores both values in secure database. After that, CT generates a random nonce C_n^* and computes $CSP_{M_{ID}}^* = h(U_{ID} \,||M_{ID} \,||C_n^*)$. CT also chooses a timestamp T_4 and generates $SID_u^* = E_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}^*, TF_{seq}^*)$, $SID_u^* \oplus M_{ID}$, and $Auth_c = h(SID_u^* \,||M_{ID} \,||U_n \,||T_4 \,||k_{uc})$. Finally, CT sends the message $M_4 = \{Auth_c, Z, T_4\}$ to the MU_i via insecure channel.
- **AP-7:** After getting the message M_4, MU_i checks $T_5 - T_4 = \Delta T$ and decrypts $SID_u = D_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$. Then, MU_i computes the session key $SID_u^* = Z \oplus M_{ID}$, the authentication message $Auth_c^* = h(SID_u^* \,||M_{ID} \,||U_n \,||T_4 \,||k_{uc})$ and verifies $Auth_c^* \stackrel{?}{=} Auth_c$. If it is valid, MU_i is mutually authenticated successfully.

III. CRYPTANALYSIS OF IQBAL *ET AL.*'S PROTOCOL

This comment paper is about "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes" that is presented by Iqbal *et al.* [1]. Iqbal *et al.* claimed that ALAM scheme could resist various attacks and also ensure user anonymity and mutual authentication. However, we demonstrate that ALAM scheme is vulnerable to "impersonation", "MITM", and "session key disclosure" attacks. Furthermore, we show that ALAM protocol fails to ensure "user anonymity" and "mutual authentication".

A. IMPERSONATION ATTACK

MA may attempt to impersonate legitimate user. Referring to Section I-A, MA can extract the secret credentials $\{SID_u, k_{uc}\}$ stored in mobile device. Moreover, MA can replay, intercept, modify, eavesdrop, insert, and delete transmitted messages over an insecure channel. The detailed steps of this attack are as follows.

- **Step 1:** MA first calculates $D_{k_{uc}}(SID_u) = (U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$ and $U_n = U_p = M_{ID}$. Then, MA generates a new random nonce A_n, and calculates $U_{MA} = A_n \oplus M_{ID}$ and $Auth_{MA} = h(SID_u \,||U_{MA} \,||k_{uc} \,||T_1 \,||A_n \,||TF_{seq})$. After that, MA sends the message $M_{MA1} = \{Auth_{MA}, SID_u, U_{MA}, T_1\}$ to the CT over an insecure channel.
- **Step 2:** After getting the message M_{MA1}, the CT checks the timestamp $T_2 - T_1 = \triangle T$ and decodes $A_n = U_{MA} \oplus M_{ID}$. Then, CT decrypts $SID_u = D_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$ and verifies $M_{ID}^{recv} \stackrel{?}{=} M_{ID}^{save}$. If it is correct, CT can come across two scenarios. Both situations are provided below.

Case 1.

- **Step 3:** If $TF_{seq}^{recv} \stackrel{?}{=} TF_{seq}^{save}$, the CT decodes $A_n = U_{MA} \oplus M_{ID}$. Then, CT verifies $Auth_{MA}^{recv} \stackrel{?}{=} Auth_{MA}^{save}$. If it is valid, CT generates a timestamp T_2 and computes $Auth_d = h(SID_{SD_{ID}} \,||T_2 \,||CID)$. After that, CT sends $M_2 = \{Auth_d, T_2\}$ to the SD_i over an insecure channel.
- **Step 4:** Upon getting the message M_2, SD_i checks $T_3 - T_2 = \triangle T$ and computes $Auth_d^* = h(SID_{SD_{ID}} \,||T_2 \,||CID)$, and checks $Auth_d^* \stackrel{?}{=} Auth_d$. If it is correct, SD_i computes $Auth_{dc} = h(SID_{SD_{ID}} \,||T_3 \,||CID)$ and sends the message $M_3 = \{Auth_{dc}, T_3\}$ to the CT via insecure channel.
- **Step 5:** After getting the message M_3, CT computes $Auth_{dc}^* = h(SID_{SD_{ID}} \,||T_3 \,||CID)$ and verifies $Auth_{dc}^* \stackrel{?}{=} Auth_{dc}$. If it is correct, SD_i is authenticated successfully.

Case 2.

- **Step 6:** CT verifies $TF_{seq}^{old} \stackrel{?}{=} TF_{seq}^{new}$. If it is valid, CT generates TF_{seq}^* and updates $\{TF_{seq}\}$ with $\{TF_{seq}^*\}$, and stores both values in secure database. After that, CT generates a random nonce C_n^* and computes $CSP_{M_{ID}}^* = h(U_{ID} \,||M_{ID} \,||C_n^*)$. CT also chooses a timestamp T_4 and generates $SID_u^* = E_{k_{uc}}(U_{ID}, M_{ID}, CSP_{M_{ID}}^*, TF_{seq}^*)$, $SID_u^* \oplus M_{ID}$, and $Auth_{cMA} = h(SID_u^* \,||M_{ID} \,||A_n \,||T_4 \,||k_{uc})$. Finally, CT sends the message $M_4 = \{Auth_{cMA}, Z, T_4\}$ to the MU_i via public channel.
- **Step 7:** After getting the message M_4, MA checks $T_5 - T_4 = \triangle T$ and computes session key $SID_u^* = Z \oplus M_{ID}$, authentication message $Auth_{cMA}^* = h(SID_u^* \,||M_{ID} \,||A_n \,||T_4 \,||k_{uc})$, and verifies $Auth_{cMA}^* \stackrel{?}{=} Auth_{cMA}$. If it is valid, MA is authenticated successfully.

Consequently, ALAM protocol is vulnerable to the impersonation attack, because MA can impersonate as a mobile user, and establish successfully a session key with the CT on behalf of the mobile user MU_i.

B. SESSION KEY DISCLOSURE ATTACK

In Section III-A, this comment paper demonstrated that MA can impersonate a mobile user MU_i and calculate a session key $SID_u^* = Z \oplus M_{ID}$ as follows. Referring to Section I-A, MA can extract secret credentials stored in mobile device, and intercept the exchanged messages between MU_i, CT, and SD_i via an insecure channel. In addition, MA calculates $D_{k_{uc}}(SID_u) = (U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$, and $U_n = U_p = M_{ID}$. After getting message $\{M_4\}$, the MA computes the session key $SID_u = Z \oplus M_{ID}$ and authentication message $Auth_c^* = h(SID_u^* \,||M_{ID} \,||U_n \,||T_4 \,||k_{uc})$. Consequently, ALAM protocol cannot withstand the session key disclosure attack because MA can generate $SID_u = Z \oplus M_{ID}$ between MU_i and CT successfully.

C. MITM ATTACK

ALAM scheme cannot withstand MITM attack, because MA can compute the authentication request message M_1. According to Section III-A, the MA computes $D_{k_{uc}}(SID_u) = (U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$ and $U_n = U_p = M_{ID}$. After that, MA computes session key $SID_u^* = Z \oplus M_{ID}$ and authentication message $Auth_{cMA}^* = h(SID_u^*||M_{ID}||A_n||T_4||k_{uc})$ successfully. Thus, ALAM scheme cannot resist to MITM attack.

D. USER ANONYMITY AND MUTUAL AUTHENTICATION

Iqbal *et al.* claimed that ALAM scheme ensures authentication between the MU_i, CT, and SD_i. However, referring to Section III-A and III-C, the MA can compute $D_{k_{uc}}(SID_u) = (U_{ID}, M_{ID}, CSP_{M_{ID}}, TF_{seq})$. Thus, MA can obtain the real identity U_{ID} and M_{ID} of the legitimate user and mobile device. Moreover, MA can compute the authentication request message M_1 and response message M_4 successfully. Thus, ALAM scheme cannot ensure user anonymity and mutual authentication.

IV. GUIDELINES ON ATTACKS RESILIENCE

In ALAM scheme [1], the major security issue is that the shared secret (long-term) key is stored in mobile device without any cryptographic methods. Because of this problem, an adversary can extract and obtain secret credentials using power analysis. According to Section III, we proved that ALAM scheme is vulnerable to various attacks, including "session key disclosure", "MITM", and "impersonation" attacks. In addition, their scheme fails to provide "user anonymity" and "mutual authentication". Thus, we propose the necessary guidelines to overcome the security flaws of ALAM scheme as also suggested in [8].

- **Guideline 1.** ALAM scheme adopts the two-factor authentication mechanism using the secret credentials and mobile device. However, referring to Section III, the *MA* is able to impersonate as a mobile user. Thus, ALAM should store the masked secret credentials with password and/or biometric using hash function and bitwise XOR operation to enhance the security level. This will increase the security level of the system.
- **Guideline 2.** In ALAM scheme, the mobile device can use the physical unclonable function (PUF) to prevent physical attacks. PUF-based authentication schemes can resist smart device physical capture attack because an attacker *MA* cannot access the PUF function even by stealing the smart device [9]–[11].
- **Guideline 3.** ALAM scheme may cause serious security problems in the future because the shared secret (long-term) key is not updated. Therefore, ALAM scheme should periodically update the shared secret (long-term) key to improve the security of the system.
- **Guideline 4.** All participants should securely encrypt and send messages using symmetric keys, because the attacker *MA* can modify, intercept, delete, and insert the exchanged messages during the mutual authentication phase.

It is worth to note that we do not claim that the guidelines suggested by us as a full-proof solution to the pointed-out drawback of ALAM scheme. However, it will definitely increase the complexity of the malicious adversary *MA*.

Iqbal *et al.* would have put best efforts to design a secure protocol for smart home applications. However, they would not have viewed their protocol from the point of view that we have analyzed and proved it. Thus, this comment paper will lead to the design of more secure and efficient authentication protocols for smart home applications.

V. CONCLUSION

This comment paper refers to "ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes" presented by Iqbal *et al.* We proved that their scheme is vulnerable to potential attacks such as "impersonation", "MITM", and "session key disclosure" attacks. Moreover, their scheme cannot also provide "user anonymity" and "mutual authentication" functionality requirements. After stealing secret credentials stored in mobile device, an adversary can compute the session key between a legitimate user and the controller. Thus, we presented some guidelines to enhance the security flaws of ALAM protocol. Consequently, we can thwart the pointed out security problems not only in ALAM protocol, but we believe that these will be also helpful in other future authentication protocols.

REFERENCES

[1] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, "ALAM: Anonymous lightweight authentication mechanism for SDN enabled smart homes," *IEEE Internet Things J.*, early access, Sep. 15, 2021, doi: 10.1109/JIOT.2020.3024058.

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

[3] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K.-R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[4] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.

[5] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Future Gener. Comput. Syst.*, vol. 91, pp. 475–492, Feb. 2019.

[6] S. J. Yu, J. Y. Lee, Y. H. Park, Y. H. Park, S. W. Lee, and B. H. Chung, "A secure and efficient three-factor authentication protocol in global mobility networks," *Appl. Sci.*, vol. 10, no. 10, pp. 3565–3588, 2020.

[7] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Netw.*, vol. 177, pp. 107333–107349, Aug. 2020.

[8] S. Yu and Y. Park, "Comments on 'ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments'" *IEEE Access*, vol. 8, pp. 193375–193379, 2020.

[9] Y. Zheng, Y. Cao, and C.-H. Chang, "UDhashing: Physical unclonable function-based user-device hash for endpoint authentication," *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9559–9570, Dec. 2019.

[10] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107593.

[11] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Physically secure lightweight anonymous user authentication protocol for Internet of Things using physically unclonable functions," *IEEE Access*, vol. 7, pp. 85627–85644, 2019.

SUNGJIN YU received the B.S. degree in electronics engineering from Daegu University, in 2017, and the M.S. degree in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2019, respectively, where he is currently pursuing the Ph.D. degree in electronics and electrical engineering. He is currently a Researcher with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. His research interests include blockchain, authentication, information security, VANET, FANET, Internet of Vehicles, and Internet of Drones.

ASHOK KUMAR DAS (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research interests include cryptography, network security, blockchain, security in the Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing, intrusion detection, and AI/ML security. He has authored over 240 papers in international journals and conferences in the above areas, including over 205 reputed journal articles. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON SMART GRID, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), *Computers and Electrical Engineering*, *Computer Networks*, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE ACCESS, IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, *IEEE Communications Magazine*, *IEEE Consumer Electronics Magazine*, *Computer Methods and Programs in Biomedicine*, *Future Generation Computer Systems*, *Expert Systems with Applications*, *Computer Standards and Interfaces*, and *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is also on the Editorial Board of the *International Journal of Internet Technology and Secured Transactions* (Inderscience), *KSII Transactions on Internet and Information Systems*, and *IET Communications*. He is also a Guest Editor for *Computers and Electrical Engineering* (Elsevier), *ICT Express* (Elsevier), the Special Issue on *Big data and Internet of Things* in e-healthcare, the Special Issue on *Blockchain Technologies*, and Applications for 5G Enabled IoT. He has served as a program committee member for many international conferences. He also severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN 2019), Avila, Spain, in June 2019.

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 information security, computer networks, and multimedia.