Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8669941, 12 pages
https://doi.org/10.1155/2022/8669941

Research Article

SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes

Bander A. Alzahrani,[1] **Ahmed Barnawi**,[1] **Abdullah Albarakati**,[1] **Azeem Irshad**,[2] **Muhammad Asghar Khan**,[3] **and Shehzad Ashraf Chaudhry**[4]

[1]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[2]*Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan*
[3]*Hamdard Institute of Engineering & Technology, Islamabad 44 000, Pakistan*
[4]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

Correspondence should be addressed to Shehzad Ashraf Chaudhry; ashraf.shehzad.ch@gmail.com

Received 23 November 2021; Accepted 13 January 2022; Published 12 February 2022

Academic Editor: Hasan Ali Khattak

Being one of the finest applications of the IoT, smart homes (SHs) with an aim to improve quality of life are taking over the traditional lifestyles. The entities within a SH communicate with each other and with the environment including the users to transform daily life seamlessly enjoyable and easy. However, owing to the public communication infrastructure, the advantages of SH are subject to security and privacy issues. Recently, Yu et al. presented a privacy and security solution for SH environment. The scheme of Yu et al. is based on lightweight symmetric key functions. Although the scheme of Yu et al. exhibits the lightweight property, it is proven in this paper that their scheme cannot provide mutual authentication due to a crucial design fault. An improved scheme using symmetric key functions for SH (SKIA-SH) is proposed in this paper. The security of the proposed scheme is furnished through formal BAN logic followed by brief discussion on security attribute provision of the proposed SKIA-SH. The comparisons show that the proposed SKIA-SH provides the required security on the cost of slight increase in computation and communication costs. The simulation results show that the SKIA-SH completes an authentication round by exchanging 216 bytes in just 5.34 ms.

1. Introduction

The smart home (SH) is an emerging concept, and with the aid of 6G/IoT smart infrastructure, the SH concept is gradually overtaking traditional living styles. SH is a communication setup among the daily useable devices like lightbulbs, televisions, door lock, monitoring cameras, washing machines, and so on. The smart devices (SDs) within a SH interact with each other and with the users to provide seamless services and for transforming daily life more and more easy and enjoyable. The services include automatic door lock and unlock, switching on and off the lights and air conditioners, suspicious activity alarming, etc. In addition, the SH concept can be very useful for patients and elderly people through activity and health-related monitoring and support. The SDs in a SH communicate over the wireless insecure channel and the public Internet. Due to communication over insecure channels, the advantages of the SH are subject to several privacy and security issues [1, 2]. Such security and privacy issues can enable an entity with malicious intentions also called as an attacker to expose user-related sensitive data including the daily routines, habits, and so on, and this information can be used with wicked intentions. In addition, the SDs are lightweight devices, and deploying public key-based infrastructure (PKI) is not a viable solution for the SH environments as PKI can pose high computation and communication costs on the low powered SDs [3–5]. Therefore, symmetric key-based authentication schemes suit the SH environments [6–8].

Recently, many authentication schemes were proposed using symmetric and PKI-based cryptographic primitives. Some of the recently proposed schemes were proposed to

secure smart home (SH) environments [9, 10]. In 2021, Ali et al. explained the pitfalls of clogging attack and designed an elliptic curve-based authentication scheme to resist clogging attack. Physical capturing is also among the crucial class of attacks [11], and physical capturing of a smart device can lead to exposure of private information of the device and it can also lead to exposure of related and communicative devices present in the smart IoT environments. Irshad et al. [12] also proved that the authentication scheme of Tsai and Lo [13] lacks required security against server forgery and impersonation attack. Moreover, Maitra et al. [14] also proposed an improvement over Lee et al.'s ElGamal-based authentication method [15]. In 2020, Ali Khan et al. [16] and Wei et al. [17] proposed two separate methods to secure smart grid and USB mass storage communication, respectively. However, these schemes were proved insecure and impractical in [18, 19]. Using elliptic curve cryptography (ECC), Vaidya et al. [9] presented their designed authentication scheme for SH. Despite their claim of security and lightweight property, the scheme presented in [9] is prone to several attacks including user forgery, privileged insider (PI), and password guessing (PG) attacks. Santoso and Vun [10] also proposed an authentication scheme for smart devices in the SH environments. Yu et al. [20] in their recent study claimed that the scheme presented in [10] has weaknesses against PI and stolen verifier (SV) attacks. Wazid et al. [21] also proposed an authentication scheme, and in 2019, Lyu et al. [22] claimed that Wazid et al.'s scheme is prone to desynchronization and related attacks. Another authentication scheme was also proposed by Lyu et al. [22]. After that, in the same year, Shuai et al. [23] presented another authentication scheme. The scheme of Shuai et al. was also structured upon ECC, and despite the claims presented in [23], in 2021, Kaur and Kumar [24] simulated the insecurity of the scheme of Shuai et al. against PI, replay, session key exposure, and related attacks. Kaur and Kumar [24] also presented an improved authentication scheme using ECC and claimed that their ECC-based scheme not only extends security but is also lightweight. However, in 2021, Yu et al. [20] proved that the scheme presented by Kaur and Kumar is prone to several weaknesses including exposure of session key and insecurity against impersonation attack. Moreover, Yu et al. also claimed that the scheme of Kaur and Kumar cannot provide mutual authentication.

1.1. Motivations and Contributions. Very recently in 2020, Yu et al. [20] presented their designed authentication scheme for smart home. The scheme of Yu et al. was built on lightweight symmetric key operations (SKOs). They claimed that due to avoidance of PKI and usage of only SKO, their scheme not only is lightweight but also provides privacy and security to the SH devices. In this study, we analyze that in contrast to the claims of Yu et al., the scheme of Yu et al. cannot extend authentication among SH devices due to a crucial design flaw of their scheme. Hence, their scheme is not practical, and to fill the gap, we proposed a symmetric key-based improved lightweight authentication scheme for smart homes (SKIA-SH).

1.2. System Architecture. A standard smart home (SH) as adopted from Yu et al.'s scheme [20] is depicted in Figure 1. The authentication entities in a SH network consist of user/s with mobile device/s, the gateway, and the smart devices (SDs). The users can control the SDs remotely, and before deployment, the registration authority registers users and SDs and deploys secret and public parameters on the memory of users and SDs. The user monitors the working of SDs, and SDs communicate with user/s through the facilitation of gateways. The entities (smart devices) of a SH network are equipped with Wi-Fi and connect with each other and with gateway through public wireless channel. Moreover, the user connects with smart devices through gateway, and the channel used between a user and a gateway is the public Internet, which allows the communication administered remotely and globally. The communication of the entities of a SH through public wireless and Internet channels calls for a secure channel through authentication and key establishment between user/s and the gateway. The authentication and key exchange protect the information exchange through public wireless channel.

1.3. Adversarial Model. In a smart home (SH) communication architecture, one or more users communicate with smart devices (SDs) through facilitation of the gateway and on the public wireless channel. Therefore, SH is an attractive environment for malicious adversaries to launch several attacks including impersonation and forgery. As per the common adversary model DY [25], an adversary has the capabilities to listen to the channel and can read, modify, and jam a message exchanged between the entities of the SH [26, 27]. Moreover, the adversary can generate and send a fake message to any entity, whereas the current de facto adversary model CY [28] is adopted in this paper and in several other proposals [29, 30]. The CK adversary model considers a more strong attacker, where in addition to adversarial capabilities of DY model, the attacker can either compromise the long-term or short-term secrets both but not at the same time [31, 3232]. The CY model suggests to construct the session keys using both the long and short-term secrets and the session keys should be independent to each other.

2. Revisiting Yu et al.'s Scheme

In the following subsections, we revisit the scheme of Yu et al. [20], which provides the authentication among the IoT-based smart devices and the user with the help of gateway. The scheme is based on lightweight symmetric key operations. Before moving to the description of the Yu et al.' scheme, Table 1 is provided to explain the notations used throughout the whole paper.

2.1. Initialization. During manufacturing, the TP generates a private key K_{GR} and stores it in the memory of GK_r. Moreover, all the IoT-based smart devices SD_q: $\{q = 1, 2, \ldots, n\}$ are assigned unique identities ID_{sq}: $\{q = 1, 2 \ldots n\}$. The TP also generates and stores the secret keys

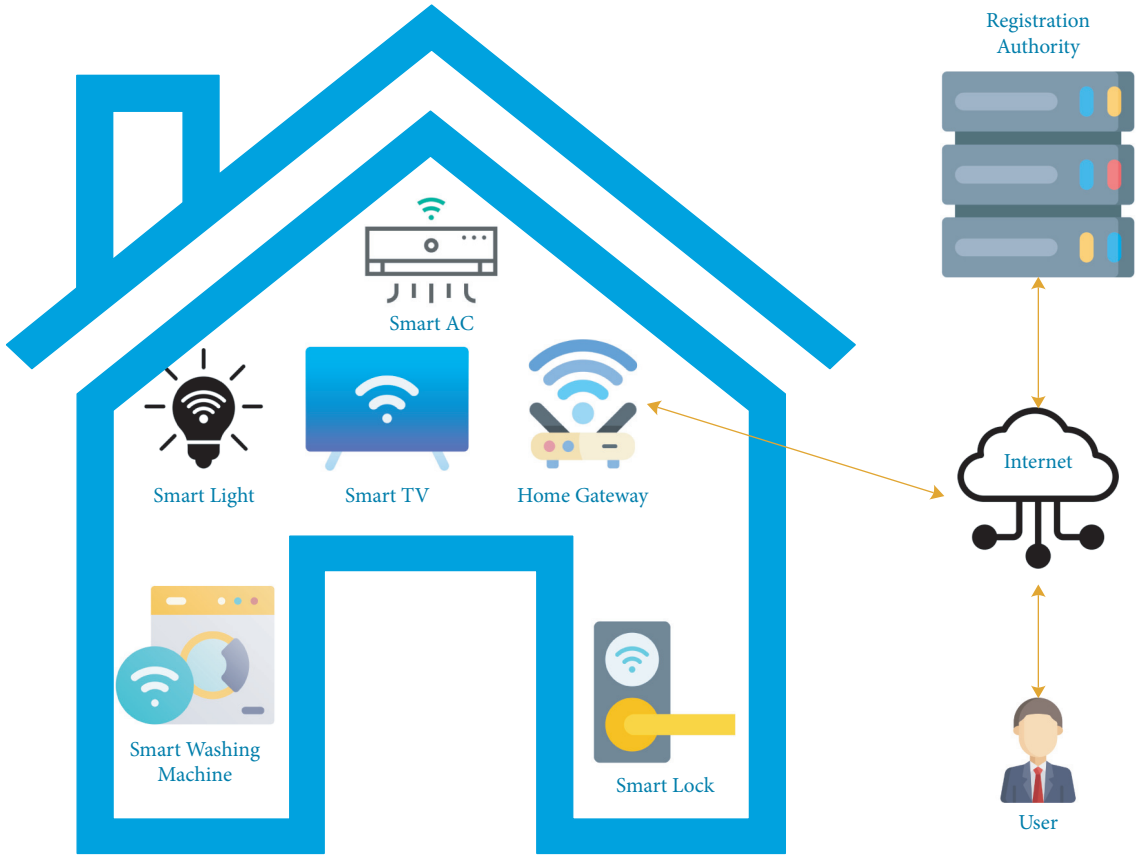

Figure 1: Smart home environment.

Table 1: Symbol guide.

Symbols	Explanations
GK_r	Gateway
SD_q	IoT device
U_p	p^{th} user
TP	Trusted third party
ID_{sq}	Identity of SD_q
ID_{up}	Identity of U_p
GID_{gr}	Identity of GK_r
β_{up}, γ_{up}	Fuzzy parameters
K_{GR}	Private key of GK_r
K_{UP}	Private key of U_p
K_{SQ}	Private key of SD_q
X_{pr}	Shared secret key among U_p and GK_r
X_{qr}	Shared secret key among SD_q and GK_r
$\oplus, H(.)$	XOR and hash operations

K_{SQ}: $\{q = 1, 2 \ldots n\}$ and stores it in the memory of each if SD_q: $\{q = 1, 2 \ldots n\}$.

2.2. User Registration. To initiate a registration request, the user U_p generates α_{up}, selects ID_{up} and PW_{up}, computes $Gen(Bio_{up}) = (\gamma_{up}, \beta_{up})$, $RID_{up} = h(ID_{up} \| \gamma_{up})$, and $RPW_{up} = h(PW_{up} \| \gamma_{up})$, and sends $\{RID_{up}, RPW_{up}, \alpha_{up}\}$ to TP through a private channel. The TP computes $X_{pr} = h(RID_{up} \| K_{GR} \| \alpha_{up})$, $A_1 = X_{PR} \oplus h(\alpha_{up} \| RPW_{up})$ and sends X_{pr} to GK_r. The GK_r now computes $L_{up} = h(GID_{gr} \| K_{GR}) \oplus X_{pr}$. The GK_r stores L_{up} into its own memory and the TP sends A_1 to U_p. U_p now computes $K_{UP} = h(ID_{up} \| PW_{up} \| \gamma_{up})$, $A_2 = E_{K_{UP}}(A_1)$, $A_3 = \alpha_{up} \oplus h(RID_{up} \| RPW_{up})$, and $A_4 = h(RID_{up} \| RPW_{up} \| \alpha_{up})$ and deletes A_1 and stores $\{A_2, A_3, A_4\}$ in the memory of SD_q.

2.3. Smart Device Registration. A SD_q generates α_{sq}, computes $PID_{sq} = h(SD_q \| \alpha_{sq})$, and sends the duo $\{PID_{sq}, \alpha_{sq}\}$ to TP. The TP now computes $X_{pr} = h(PID_{sq} \| K_{GR} \| \alpha_{sq})$ and stores $\{PID_{sq}, \alpha_{uq}\}$ in GK_r's database and sends X_{pr} to SD_q. The SD_q now computes $B_1 = h(SID_{sq} \| K_{SQ}) \oplus \alpha_{sq}$ and $B_2 = h(K_{SQ} \| \alpha_{sq}) \oplus X_{qr}$ and stores B_1, B_2 in its own memory.

2.4. Authentication. As summarized in Figure 2, the user U_p initiates authentication phase by entering the pair of his own identity and password $\{ID_{up}, PW_{up}\}$. The user terminal device computes $\gamma_{up} = Rep(Bio_{up}, \beta_{up})$, $RID_{up} = h(ID_{up} \| \gamma_{up})$, $RPW_{up} = h(PW_{up} \| \gamma_{up})$, and $K_{UP} = h(ID_{up} \| PW_{up} \| \gamma_{up})$. Now U_p extracts A_2, using K_{UP} decrypts A_2, and gets $A_1 = D_{K_{UP}}(A_2)$. U_p further computes $\alpha_{up} = A_3 \oplus h(RID_{up} \| RPW_{up})$ and $X_{pr} = A_1 \oplus h(\alpha_{up} \| RPW_{up})$. Now, U_p checks the equality $A_4 =_? h(RID_{up} \| RPW_{up} \| \alpha_{up})$, and if it holds, U_p selects/generates $\{T_1, r_{up}\}$ and proceeds with the authentication phase through execution of the following steps:

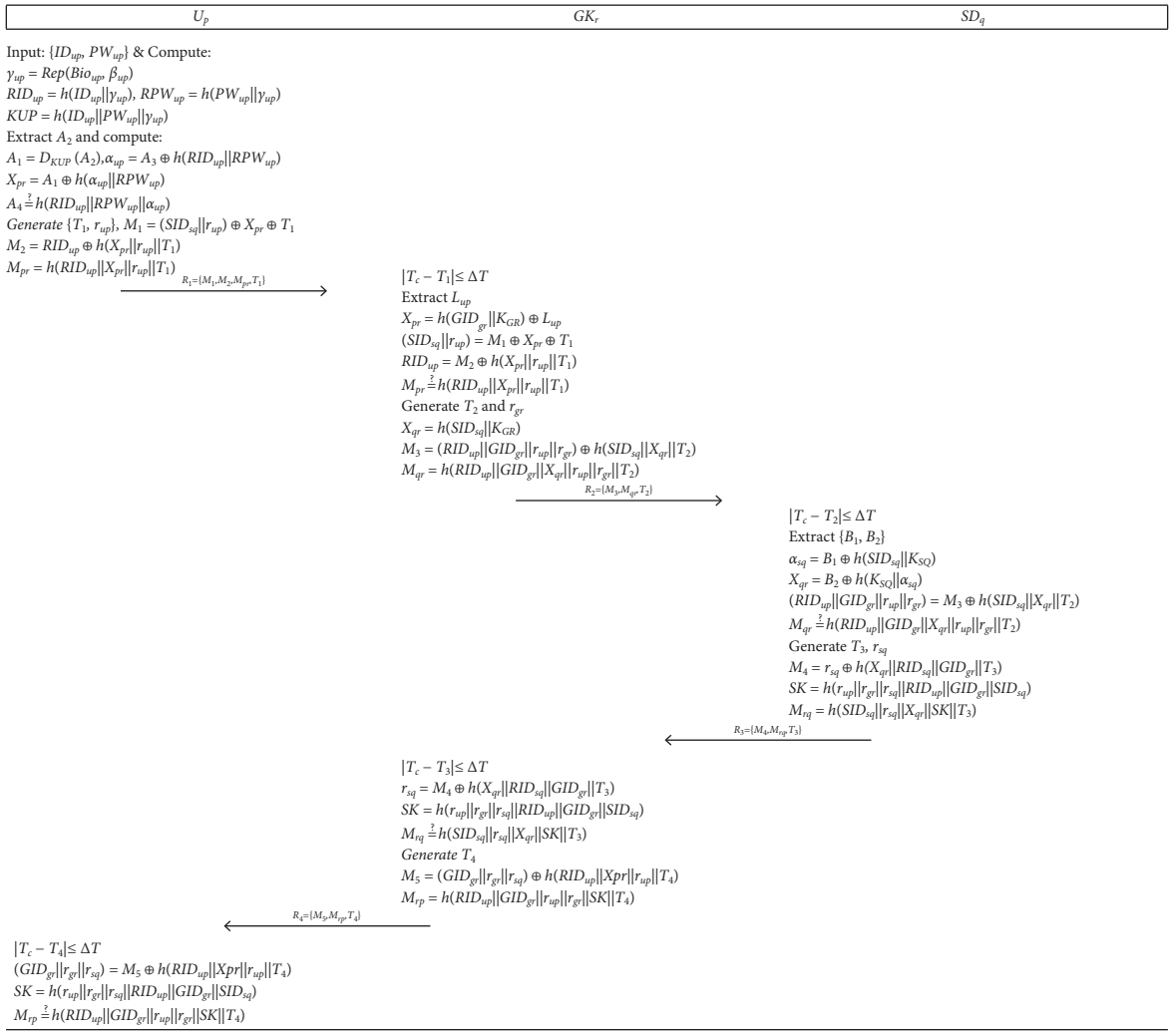

Figure 2: The scheme of Yu et al.

AY 1: $\mathbf{U_p} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_1 = \{\mathbf{M}_1, \mathbf{M}_2, \mathbf{M_{pr}}, \mathbf{T}_1\}$.

U_p computes $M_1 = (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1$, $M_2 = \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and $M_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \mathrm{Vert} | r_{\mathrm{up}} \| T_1)$ and sends request message $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

AY 2: $\mathbf{GK_r} \longrightarrow \mathbf{SD_q}$: $\mathbf{R}_2 = \{\mathbf{M}_3, \mathbf{M_{qr}}, \mathbf{T}_2\}$.

GK_r on receiving $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ checks $|T_c - T_1| \leq \Delta T$, where T_c is current timestamp recorded at GK_r and ΔT is the allowable time delay. On the successful validation of timestamp, GK_r extracts L_{up} and computes $X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}$, $(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1$, and $\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$. Now, GK_r checks validity of $M_{pr} =_? h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and if it holds, GK_r selects/generates $\{T_2, r_{gr}\}$. Now, GK_r computes $X_{\mathrm{qr}} = h(\mathrm{SID_{sq}} \| K_{\mathrm{GR}})$, $M_3 = (\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}}) \oplus h(\mathrm{SID_{sq}} \| X_{\mathrm{qr}} \| T_2)$, and $M_{\mathrm{qr}} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{\mathrm{qr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| T_2)$. GK_r completes this step by sending $R_2 = \{M_3, M_{qr}, T_2\}$ to SD_q.

AY 3: $\mathbf{SD_q} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_3 = \{\mathbf{M}_4, \mathbf{M_{rq}}, \mathbf{T}_3\}$.

SD_q on receiving $R_2 = \{M_3, M_{qr}, T_2\}$ checks $|T_c - T_2| \leq \Delta T$, and on successful validation of timestamp, SD_q extracts $\{B_1, B_2\}$ from its memory and computes $\alpha_{\mathrm{sq}} = B_1 \oplus h(\mathrm{SID_{sq}} \| K_{\mathrm{SQ}})$, $X_{\mathrm{qr}} = B_2 \oplus h(K_{\mathrm{SQ}} \| \alpha_{\mathrm{sq}})$, and $(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}}) = M_3 \oplus h(\mathrm{SID_{sq}} \| X_{\mathrm{qr}} \| T_2)$. Now, SD_q checks validity of $M_{qr} =_? h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{\mathrm{qr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| T_2)$, and if it holds, SD_q selects/generates $\{T_3, r_{\mathrm{sq}}\} M_4 = r_{\mathrm{sq}} \oplus h(X_{\mathrm{qr}} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$, $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$, and $M_{\mathrm{rq}} = h(\mathrm{SID_{sq}} \| r_{\mathrm{sq}} \| X_{\mathrm{qr}} \| \mathrm{SK} \| T_3)$. SD_q now sends $R_3 = \{M_4, M_{rq}, T_3\}$ to GK_r.

AY 4: $\mathbf{GK_r} \longrightarrow \mathbf{U_p}$: $\mathbf{R}_4 = \{\mathbf{M}_5, \mathbf{M_{rp}}, \mathbf{T}_4\}$.

GK_r on receiving $R_3 = \{M_4, M_{rq}, T_3\}$ checks $|T_c - T_3| \leq \Delta T$, and on successful validation of timestamp, GK_r computes $r_{\mathrm{sq}} = M_4 \oplus h(X_{\mathrm{qr}} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$ and $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. Now, GK_r checks validity of $M_{rq} =_? h(\mathrm{SID_{sq}} \| r_{\mathrm{sq}} \| X_{\mathrm{qr}} \| \mathrm{SK} \| T_3)$. On successful validation, GK_r generates $\{T_4\}$ and computes $M_5 = (\mathrm{GID_{gr}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}}) \oplus h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_4)$ and $M_{rp} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| \mathrm{SK} \| T_4)$. Now, GK_r sends $R_4 = \{M_5, M_{rp}, T_4\}$ to U_p.

AY 5: U_p on receiving $R_4 = \{M_5, M_{rp}, T_4\}$ checks $|T_c - T_4| \leq \Delta T$, and on successful validation of timestamp, U_p computes $(\mathrm{GID_{gr}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}}) = M_5 \oplus h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_4)$ and session key $\mathrm{SK} = h(r_{\mathrm{up}} \| r_{\mathrm{gr}} \| r_{\mathrm{sq}} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. U_p checks the validity of $M_{rp} =_? h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{\mathrm{up}} \| r_{\mathrm{gr}} \| \mathrm{SK} \| T_4)$. On successful validation, U_p considers SD_q and GK_r authenticates and keeps SK as the session key for future secure communication.

3. Weaknesses of Yu et al.'s Scheme

In this section, it is shown that the scheme of Yu et al. [20] cannot provide mutual authentication among the smart devices (SDs) of a smart home (SH). Specifically, in Yu et al.'s scheme, once GK_r receives the authentication request, it cannot recognize the user requesting the authentication. Therefore, the process may stop here and the scheme of Yu et al. cannot complete a round of authentication process. The following explanation of an authentication round of the scheme of Yu et al. can clarify the scheme's incorrectness:

(1) U_p first completes a login by entering his password, identity, and biometrics, and the user device computes and sends request message $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

$$\begin{aligned} M_1 &= (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1, \\ M_2 &= \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1), \\ M_{\mathrm{pr}} &= h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1). \end{aligned} \tag{1}$$

Now, U_p sends $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ to GK_r.

(2) GK_r on receiving $R_1 = \{M_1, M_2, M_{pr}, T_1\}$, checks $|T_c - T_1| \leq \Delta T$. On successful validation of T_1, GK_r extracts L_{up} from its database and computes

$$X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}, \tag{2}$$

$$(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1, \tag{3}$$

$$\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1). \tag{4}$$

(3) GK_r computes the shared key X_{pr} through equation (2), and for this, GK_r needs to extract L_{up}, from the database stored on the memory of GK_r. The database has the entries of the form $\{\mathrm{ID_{up}}, L_{\mathrm{up}}\}$: p: $1, 2 \ldots m$, if there are m users. To extract L_{up} from the database, GK_r first needs to recognize the specific user U_p with identity $\mathrm{ID_{up}}$. However, GK_r does not recognize U_p because it does not receive identity or any other user-related information in the request message R_1. Therefore, GK_r cannot extract L_{up} and equations (2), (3), and (4) cannot be resolved. Due to this incorrectness, the scheme of Yu et al. cannot complete even a round of authentication process.

4. SKIA-SH: Proposed Scheme

In this section, we present the improved scheme over Yu et al.'s scheme. For designing improved scheme, we take the initialization phase of Yu et al. as it was designed by Yu et al. Furthermore, the smart device registration phase is also taken as it is. The proposed scheme amends some steps in user registration and authentication phases to provide a scalable and correct mechanism for the provision of secure channel among a user and a smart device. The proposed symmetric key-based improved authentication scheme for smart homes (SKIA-SH) is described below.

4.1. SKIA-SH: User Registration. To initiate a registration request, the user U_p generates α_{up}, selects $\mathrm{ID_{up}}$ and $\mathrm{PW_{up}}$, computes $\mathrm{Gen}(\mathrm{Bio_{up}}) = (\gamma_{\mathrm{up}}, \beta_{\mathrm{up}})$, $\mathrm{RID_{up}} = h(\mathrm{ID_{up}} \| \gamma_{\mathrm{up}})$, and $\mathrm{RPW_{up}} = h(\mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$ and sends $\{\mathrm{RID_{up}}, \mathrm{RPW_{up}}, \alpha_{\mathrm{up}}\}$ to TP through a private channel. TP computes $X_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| K_{\mathrm{GR}} \| \alpha_{\mathrm{up}})$ and $A_1 = X_{\mathrm{PR}} \oplus h(\alpha_{\mathrm{up}} \| \mathrm{RPW_{up}})$ and sends X_{pr} to GK_r. GK_r now computes $L_{\mathrm{up}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus X_{\mathrm{pr}}$ and $\mathrm{PID_{up}} = h(\mathrm{ID_{up}} \| \alpha_{\mathrm{up}} \| X_{\mathrm{pr}})$. GK_r stores L_{up} and $\mathrm{PID_{up}} = h(\mathrm{ID_{up}} \| \alpha_{\mathrm{up}} \| X_{\mathrm{pr}})$ into its own memory, and TP sends $\{A_1, \mathrm{PID_{up}}\}$ to U_p. U_p now computes $K_{\mathrm{UP}} = h(\mathrm{ID_{up}} \| \mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$, $A_2 = E_{K_{\mathrm{UP}}}(A_1)$, $A_3 = \alpha_{\mathrm{up}} \oplus h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}})$, and $A_4 = h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}} \| \alpha_{\mathrm{up}})$, deletes A_1, and stores $\{A_2, A_3, A_4, \mathrm{PID_{up}}\}$ in the memory of SD_q.

4.2. SKIA-SH: Authentication. The user U_p initiates authentication phase as shown in Figure 3, by entering the pair of his own identity and password $\{\mathrm{ID_{up}}, \mathrm{PW_{up}}\}$. The user terminal device computes $\gamma_{\mathrm{up}} = \mathrm{Rep}(\mathrm{Bio_{up}}, \beta_{\mathrm{up}})$, $\mathrm{RID_{up}} = h(\mathrm{ID_{up}} \| \gamma_{\mathrm{up}})$, $\mathrm{RPW_{up}} = h(\mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$, and $K_{\mathrm{UP}} = h(\mathrm{ID_{up}} \| \mathrm{PW_{up}} \| \gamma_{\mathrm{up}})$. Now U_p extracts A_2, using K_{UP} decrypts A_2, and gets $A_1 = D_{K_{\mathrm{UP}}}(A_2)$. U_p further computes $\alpha_{\mathrm{up}} = A_3 \oplus h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}})$ and $X_{\mathrm{pr}} = A_1 \oplus h(\alpha_{\mathrm{up}} \| \mathrm{RPW_{up}})$. Now, U_p checks the equality $A_4 =_? h(\mathrm{RID_{up}} \| \mathrm{RPW_{up}} \| \alpha_{\mathrm{up}})$, and if it holds, U_p selects/generates $\{T_1, r_{\mathrm{up}}\}$ and proceeds with the authentication phase through execution of the following steps:

AP 1: $\mathbf{U_p} \longrightarrow \mathbf{GK_r}$: $\mathbf{R_1} = \{\mathbf{M_1}, \mathbf{M_2}, \mathbf{M_{pr}}, \mathbf{T_1}\}$.

U_p computes $M_1 = (\mathrm{SID_{sq}} \| r_{\mathrm{up}}) \oplus X_{\mathrm{pr}} \oplus T_1$, $M_2 = \mathrm{RID_{up}} \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and $M_{\mathrm{pr}} = h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \mathrm{Vert} | r_{\mathrm{up}} \| T_1)$ and sends request message $R_1 = \{M_1, M_2, M_{\mathrm{pr}}, \mathrm{PID_{up}}, T_1\}$ to GK_r.

AP 2: $\mathbf{GK_r} \longrightarrow \mathbf{SD_q}$: $\mathbf{R_2} = \{\mathbf{M_3}, \mathbf{M_{qr}}, \mathbf{T_2}\}$.

GK_r on receiving $R_1 = \{M_1, M_2, M_{\mathrm{pr}}, \mathrm{PID_{up}}, T_1\}$ checks $|T_c - T_1| \leq \Delta T$, where T_c is current timestamp recorded at GK_r and ΔT is the allowable time delay. On successful validation of timestamp, GK_r, extracts L_{up} as per the $\mathrm{PID_{up}}$ from its database where the entries are of the form $\{\mathrm{PID_{up}}, \mathrm{ID_{up}}, L_{\mathrm{up}}\}$ and computes $X_{\mathrm{pr}} = h(\mathrm{GID_{gr}} \| K_{\mathrm{GR}}) \oplus L_{\mathrm{up}}$, $(\mathrm{SID_{sq}} \| r_{\mathrm{up}}) = M_1 \oplus X_{\mathrm{pr}} \oplus T_1$, and $\mathrm{RID_{up}} = M_2 \oplus h(X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$. Now, GK_r checks validity of $M_{pr} =_? h(\mathrm{RID_{up}} \| X_{\mathrm{pr}} \| r_{\mathrm{up}} \| T_1)$, and if it holds, GK_r selects/

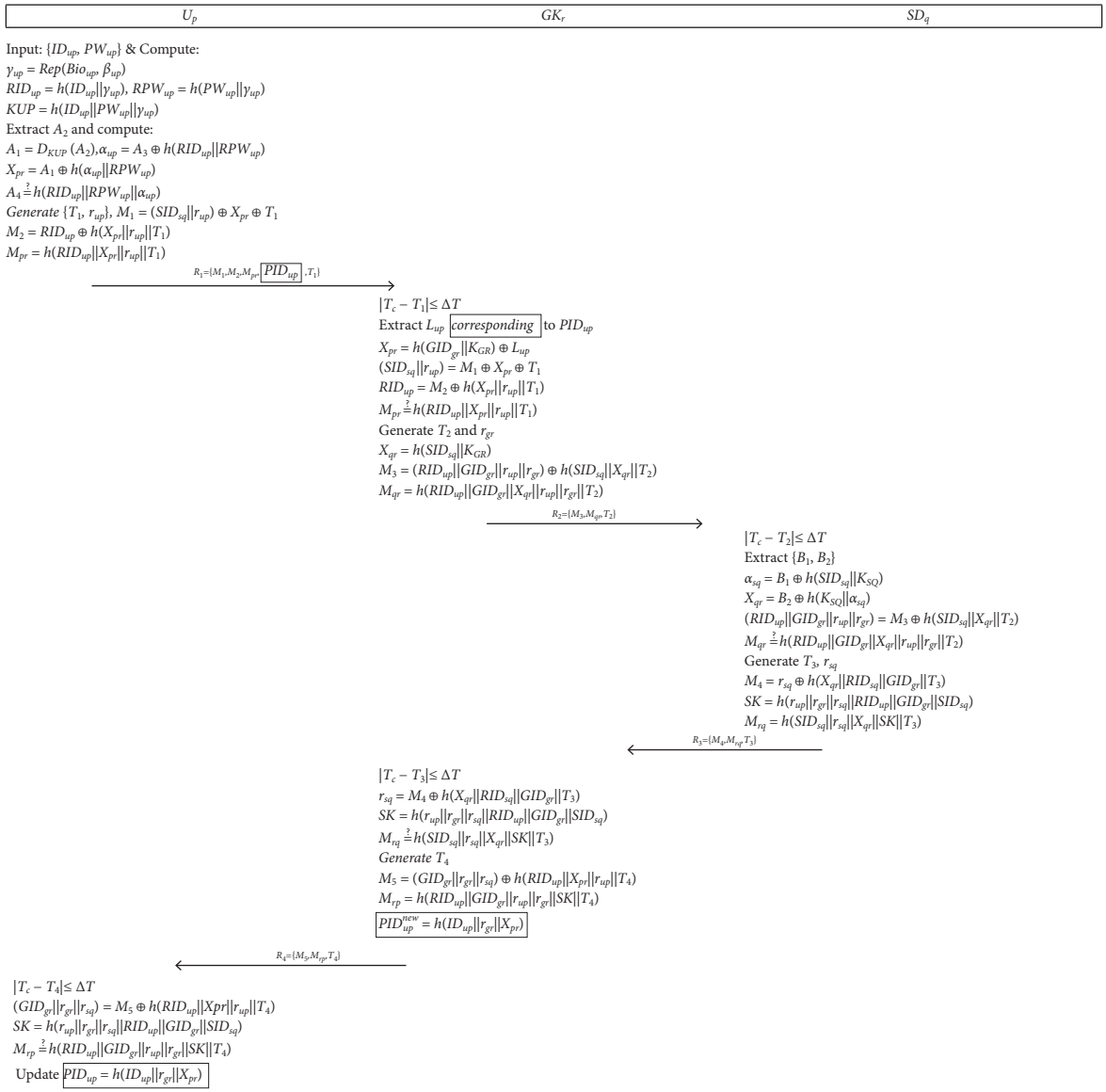

Figure 3: SKIA-SH: the proposed scheme.

generates $\{T_2, r_{gr}\}$. Now, GK_r computes $X_{qr} = h(\mathrm{SID_{sq}} \| K_{GR})$, $M_3 = (\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr}) \oplus h(\mathrm{SID_{sq}} \| X_{qr} \| T_2)$, and $M_{qr} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{qr} \| r_{up} \| r_{gr} \| T_2)$. GK_r completes this step by sending $R_2 = \{M_3, M_{qr}, T_2\}$ to SD_q.

AP 3: $\mathbf{SD_q} \longrightarrow \mathbf{GK_r}$: $\mathbf{R}_3 = \{\mathbf{M}_4, \mathbf{M_{rq}}, \mathbf{T}_3\}$.

SD_q on receiving $R_2 = \{M_3, M_{qr}, T_2\}$ checks $|T_c - T_2| \leq \Delta T$, and on successful validation of timestamp, SD_q extracts $\{B_1, B_2\}$ from its memory and computes $\alpha_{sq} = B_1 \oplus h(\mathrm{SID_{sq}} \| K_{SQ})$, $X_{qr} = B_2 \oplus h(K_{SQ} \| \alpha_{sq})$, and $(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr}) = M_3 \oplus h(\mathrm{SID_{sq}} \| X_{qr} \| T_2)$. Now, SD_q checks validity of $M_{qr} \stackrel{?}{=} h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| X_{qr} \| r_{up} \| r_{gr} \| T_2)$, and if it holds, SD_q selects/generates $\{T_3, r_{sq}\}$ $M_4 = r_{sq} \oplus h(X_{qr} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$, $SK = h(r_{up} \| r_{gr} \| r_{sq} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$, and $M_{rq} = h(\mathrm{SID_{sq}} \| r_{sq} \| X_{qr} \| SK \| T_3)$. SD_q now sends $R_3 = \{M_4, M_{rq}, T_3\}$ to GK_r.

AP 4: $\mathbf{GK_r} \longrightarrow \mathbf{U_p}$: $\mathbf{R}_4 = \{\mathbf{M}_5, \mathbf{M_{rp}}, \mathbf{T}_4\}$.

GK_r on receiving $R_3 = \{M_4, M_{rq}, T_3\}$ checks $|T_c - T_3| \leq \Delta T$, and on successful validation of timestamp, GK_r computes $r_{sq} = M_4 \oplus h(X_{qr} \| \mathrm{RID_{sq}} \| \mathrm{GID_{gr}} \| T_3)$ and $SK = h(r_{up} \| r_{gr} \| r_{sq} \| \mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| \mathrm{SID_{sq}})$. Now, GK_r checks validity of $M_{rq} \stackrel{?}{=} h(\mathrm{SID_{sq}} \| r_{sq} \| X_{qr} \| \mathrm{SK} \| T_3)$. On successful validation, GK_r generates $\{T_4\}$ and computes $M_5 = (\mathrm{GID_{gr}} \| r_{gr} \| r_{sq}) \oplus h(\mathrm{RID_{up}} \| X_{pr} \| r_{up} \| T_4)$, $M_{rp} = h(\mathrm{RID_{up}} \| \mathrm{GID_{gr}} \| r_{up} \| r_{gr} \| \mathrm{SK} \| T_4)$ and $\mathrm{PID_{up}^{new}} = h(\mathrm{ID_{up}} \| r_{gr} \| X_{pr})$. GK_r stores $\mathrm{PID_{up}^{new}}$ in its database in some temporary variable alongside $\{\mathrm{PID_{up}}, \mathrm{ID_{up}}, L_{up}\}$, where

PID_{up} is the old identity. GK_r keeps identity pair $\{PID_{up}, PID_{up}^{new}\}$ until it receives next authentication to avoid any identity de-synchronization, and on next successful login, both identities are updated. Finally, GK_r sends $R_4 = \{M_5, M_{rp}, T_4\}$ to U_p.

AP 5: U_p on receiving $R_4 = \{M_5, M_{rp}, T_4\}$ checks $|T_c - T_4| \leq \Delta T$, and on successful validation of timestamp, U_p computes $(GID_{gr} \| r_{gr} \| r_{sq}) = M_5 \oplus h(RID_{up} \| X_{pr} \| r_{up} \| T_4)$ and session key $SK = h(r_{up} \| r_{gr} \| r_{sq} \| RID_{up} \| GID_{gr} \| SID_{sq})$. U_p checks the validity of $M_{rp} =_? h(RID_{up} \| GID_{gr} \| r_{up} \| r_{gr} \| SK \| T_4)$. On successful validation, U_p computes $PID_{up}^{new} = h(ID_{up} \| r_{gr} \| X_{pr})$ and updates PID_{up} with PID_{up}^{new} and considers SD_q and GK_r authenticates and keeps SK as the session key for future secure communication.

5. Formal Security Analysis through BAN

We present the formal security analysis of the proposed scheme through employing the Burrows–Abadi–Needham logic (BAN) logic [33]. In this BAN logic analysis, we discuss the security evaluation with an emphasis on mutual authenticity among legal participants, protection of session key, and the key distribution among the participants.

(i) $S| \equiv : X$the principle S believes X.

(ii) $S \triangleleft X$: S sees X.

(iii) $S| \sim X$: S once said X and believes that X is true.

(iv) $S| \Rightarrow X$: S has jurisdiction over X.

(v) $(\#(X))$: X is not replayed and is fresh.

(vi) (X, X'): X and X' are parts of a hash digest message.

(vii) $\langle X, X' \rangle_k$: X and X' are exchanged using mutually agreed key k.

(viii) $S \leftrightarrow_K S'$: the communication among S and S' is secured using K as the key.

Some rules that are used in the analysis are given below:

R_1: message meaning rule:

$$\frac{S| \equiv S \xrightarrow{K} S', S \triangleleft \langle X \rangle_{X'}}{S| \equiv S'| \sim X}. \tag{5}$$

R_2: nonce verification rule:

$$\frac{S| \equiv \#(X), S| \equiv S'| \sim X}{S| \equiv S'| \equiv X}. \tag{6}$$

Rule 3: jurisdiction rule:

$$\frac{S| \equiv S' \Rightarrow X, S| \equiv S'| \equiv X}{S| \equiv X}. \tag{7}$$

Rule 4: freshness conjunction rule:

$$\frac{S| \equiv \#(X)}{S| \equiv \#(X, X')}. \tag{8}$$

Rule 5: belief rule:

$$\frac{S| \equiv (X), S| \equiv (X')}{S| \equiv (X, X')}. \tag{9}$$

Rule 6: session key rule:

$$\frac{S| \equiv \#(X, S|) \equiv S' \equiv X}{S| \equiv S \leftrightarrow_K S'}. \tag{10}$$

(i) G-1: $GK_r| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(ii) G-2: $GK_r| \equiv U_p| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(iii) G-3: $U_p| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(iv) G-4: $U_p| \equiv GK_r| \equiv (GK_r \leftrightarrow_{SK} U_p)$.

(v) G-5: $SD_q| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

(vi) G-6: $U_p| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

The idealized form of the communication messages is given below:

(vii) R_1: $U_p \longrightarrow GK_r$: M_1, M_2, M_{pr}, T_1: $\{\langle SID_{sq}, r_{up}, T \rangle_{1X_{pr}}, \langle RID_{up} \rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, \backslash\backslash r_{up}, T_1)_{X_{pr}}, T_1\}$.

(viii) R_2: $GK_r \longrightarrow SD_q$: M_3, M_{qr}, T_2: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr} \rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

(ix) R_3: $SD_q \longrightarrow GK_r$: M_4, M_{rq}, T_3: $\{\langle r_{sq} \rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

(x) R_4: $GK_r \longrightarrow U_p$: M_5, M_{rp}, T_4: $\{\langle GID_{gr}, r_{gr}, r_{sq} \rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, GID_{gr}, \backslash\backslash r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

To prove the model, we construct the following premises.

(xi) κ_1: $U_p| \equiv \#(T_1)$.

(xii) κ_2: $GK_r| \equiv \#T_2$.

(xiii) κ_3: $SD_q| \equiv \#T_3$.

(xiv) κ_4: $U_p| \equiv (U_p \leftrightarrow_{X_{Pr}} GK_r)$.

(xv) κ_5: $U_p| \equiv (U_p \leftrightarrow_{SK} SD_q)$.

(xvi) κ_6: $GK_r| \equiv (GK_r \leftrightarrow_{L_{up}} U_p)$.

(xvii) κ_7: $GK_r| \equiv GK_r \leftrightarrow_{X_{qr}} SD_q$.

(xviii) κ_8: $SD_q| \equiv (SD_q \leftrightarrow_{SK} U_p)$.

(xix) κ_9: $SD_q| \equiv SD_q \leftrightarrow_{SK} GK_r$.

(xx) κ_{10}: $U_p| \equiv GK_r| \Rightarrow (U_p \leftrightarrow_{M_{rp}} GK_r)$.

(xxi) κ_{11}: $GK_r| \equiv U_p| \Rightarrow (U_p \leftrightarrow_{M_{pr}} GK_r)$.

(xxii) κ_{12}: $SD_q| \equiv U_p| \Rightarrow (U_p \leftrightarrow_{r_{up}} SD_q)$.

(xxiii) κ_{13}: $GK_r| \equiv SD_q| \Rightarrow (SD_q \leftrightarrow_{M_{rq}} GK_r)$.

(xxiv) κ_{14}: $SD_q| \equiv GK_r| \Rightarrow (U_p \leftrightarrow_{r_{gr}} GK_r)$.

(xxv) κ_{15}: $U_p| \equiv SD_q| \Rightarrow (U_p \leftrightarrow_{r_{sq}} GK_r)$.

Next we use the designed idealizations in the following formulations. Considering R_1 and R_2 of the idealized formalization:

(i) R_1: $U_p \longrightarrow GK_r$: M_1, M_2, M_{pr}, T_1: $\{\langle SID_{sq}, r_{up}, T_1 \rangle_{X_{pr}}, \langle RID_{up} \rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, r_{up}, \backslash\backslash T_1)_{X_{pr}}, T_1\}$.

(ii) R_2: $GK_r \longrightarrow SD_q$: M_3, M_{qr}, T_2: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

Employing seeing rule for R_1 and R_2, we get

(i) F_1: $GK_r \backslash lh\ dM_1, M_2, M_{pr}, T_1$: $\{\langle SID_{sq}, r_{up}, T_1\rangle X_{pr}, \backslash\backslash \langle RID_{up}\rangle_{h(X_{pr}, r_{up}, T_1)}, (RID_{up}, r_{up}, T)_{1X_{pr}}, T_1\}$.

(ii) F_2: $SD_q \backslash lh\ d\ M_3, M_{qr}, T_2$: $\{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

According to $F_1, F_2, \kappa_8, \kappa_9$, and message meaning rule, we have

(iii) F_3: $GK_r| \equiv U_p \sim \{\langle SID_{sq}, r_{up}, T_1\rangle_{X_{pr}}, \langle RID_{up}\rangle \backslash\backslash \_h(X_{pr}, r_{up}, T_1), (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

(iv) F_4: $SD_q| \equiv GK_r \sim \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

(v) Employing F_3, κ_1, freshness conjucatenation, and nonce verification rules, we have

(vi) F_5: $GK_r| \equiv U_p \equiv \{\langle SID_{sq}, r_{up}, T_1\rangle_{X_{pr}}, \langle RID_{up}\rangle \backslash\backslash \_h(X_{pr}, r_{up}, T_1), (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

On applying F_4, κ_2, freshness conjucatenation, and nonce verification rules, we get

(i) F_6: $SD_q| \equiv GK_r \equiv \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle \backslash\backslash \_h(SID_{sq}, X_{qr}, T_2)\}$.

After applying F_5, κ_{12}, and jurisdiction rule,

(ii) F_7: $GK_r| \equiv \{\langle SID_{sq}, r_{up}, T\rangle_{1X_{pr}}, \langle RID_{up}\rangle_{h(X_{pr}, r_{up}, T_1)}, \backslash\backslash (RID_{up}, r_{up}, T_1)_{X_{pr}}, T_1\}$.

Using F_6, κ_{14}, and jurisdiction rule,

(i) F_8: $SD_q| \equiv \{\langle RID_{up}, GID_{gr}, r_{up}, r_{gr}\rangle_{h(SID_{sq}, X_{qr}, T_2)}\}$.

After applying F_5, F_7, and session key rule, we get

(i) F_9: $GK_r| \equiv GK_r \leftrightarrow_{SK} U_p$ (G-1).

Using $F_5, F_7, \kappa_6, \kappa_8$, and nonce verification rule, we get

(i) F_{10}: $SD_q| \equiv SD_q \leftrightarrow_{SK} U_p$ (G-5).

Using R_3 of the idealized form:

(i) R_3: $SD_q \longrightarrow GK_r$: M_4, M_{rq}, T_3: $\{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

By applying seeing rule for R_3, we get

(i) F_{11}: $GK_r \triangleleft M_4, M_{rq}, T_3$: $\{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

Employing F_{11}, κ_7, and message meaning rule, we get

(i) F_{12}: $GK_r| \equiv SD_q \sim \{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, \backslash\backslash (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

On applying $F_{12}, \kappa_3, \kappa_{13}$, freshness conjucatenation, and nonce verification rules, we have

(i) F_{13}: $GK_r| \equiv SD_q| \equiv \{\langle r_{sq}\rangle_{h(X_{qr}, RID_{sq}, GID_{gr}, T_3)}, \backslash\backslash (SID_{sq}, r_{sq}, X_{qr}, T_3)_{SK}, T_3\}$.

(ii) $U_p| \equiv (GK_r \leftrightarrow_{SP} U_p)$ (G-3).

(iii) $U_p| \equiv GK_r| \equiv (GK_r \leftrightarrow_{SP} U_p)$ (G-4).

Next, using R_4 idealized form:

(i) R_4: $GK_r \longrightarrow U_p$: M_5, M_{rp}, T_4: $\{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, GID_{gr}, r_{up}, \backslash\backslash r_{gr}, T_4)_{SK}, T_4\}$.

By using seeing rule for R_4, we get

(i) F_{14}: $U_p \triangleleft M_5, M_{rp}, T_4$: $\{\langle GID_{gr}, r_{gr}, r_{sq}\rangle \backslash\backslash \_h\ RID_{up}, X_{pr}, r_{up}, T_4, (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By using $F_{14}, \kappa_4, \kappa_5, \kappa_{11}$, and message meaning rule, we have

(i) F_{15}: $U_p| \equiv GK_r \sim \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, \backslash\backslash (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By applying $F_{15}, \kappa_2, \kappa_3$, freshness conjucatenation, and nonce verification rules, we have

(i) F_{16}: $U_p| \equiv GK_r| \equiv \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, \backslash\backslash (RID_{up}, GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

By applying $F_{16}, \kappa_4, \kappa_{10}, \kappa_{15}$, and jurisdiction rule, we get

(i) F_{17}: $U_p| \equiv \{\langle GID_{gr}, r_{gr}, r_{sq}\rangle_{h(RID_{up}, X_{pr}, r_{up}, T_4)}, (RID_{up}, \backslash\backslash GID_{gr}, r_{up}, r_{gr}, T_4)_{SK}, T_4\}$.

Through F_{17}, we apply the session key rule as

(i) F_{18}: $GK_r \equiv U_p| \equiv GK_r \leftrightarrow_{SK} U_p$ (G-2).

By applying $F_{18}, \kappa_2, \kappa_{14}$, we use the session key rule as

(i) F_{19}: $U_p| \equiv SD_q \leftrightarrow_{SK} U_p$ (G-6).

This BAN logic analysis proves sufficiently that our contributed model achieves the targeted goals by attaining mutual authenticity among the legal entities of the system.

5.1. Informal Security Analysis. An informal security discussion on the security features of the proposed scheme is provided in the following.

5.1.1. Mutual Authentication. In the proposed scheme, all participating entities such as U_p, GK_r, and SD_q mutually authenticate one another. GK_r authenticates U_p after extracting L_{up}, computing X_{pr}, and verifying M_{pr} factor with a fresh timestamp T_1. Similarly, GK_r authenticates SD_q after computing and evaluating the correctness of M_{rq} parameter. No malicious entity may compute r_{sq} factor without applying the shared secret X_{qr}. Likewise, U_p authenticates GK_r and SD_q on account of verification of M_{rp} factor. U_p knows that no adversary may calculate the constituent factors including SK, GID_{gr}, r_{gr}, and r_{sq} in further computing M_{rp} without using the shared secret X_{pr}. Finally, SD_q endorses both U_p and GK_r entities after verification of M_{qr} parameter. SD_q verifies the validity of RID_{up}, GID_{gr}, r_{up}, and r_{gr} factors due to the shared secret X_{qr}.

5.1.2. Anonymity and Untraceability. The proposed scheme remains anonymous due to the fact that U_p does not send its real identity ID_{up} in plaintext on insecure channel. To achieve this property, it computes RID_{up} by taking hash of

real identity ID_{up} along with high entropy random integer γ_{up}. Moreover, this hidden identity is submitted to GK_r under the cover of shared secret X_{pr}. An adversary may eavesdrop M_2 message from open channel; however, it may not extract either RID_{up} or the hidden identity ID_{up} from M_2. Similarly, our scheme is untraceable since no adversary can distinguish or trace the similarity among messages of various sessions of the same user. Thus, our scheme supports anonymity and untraceability for the user U_p.

5.1.3. Impersonation Attacks. Our scheme is resistant to U_p as well as GK_r impersonation attacks. The adversary may attempt to impersonate as U_p and for this, it can replay $R_1 = \{M_1, M_2, M_{pr}, T_1\}$ or can modify R_1 and send the R_1 to GK_r, the later may come to know the possibility of the impersonation attack if the M_{pr} is not satisfied. Similarly, if an adversary attempts to initiate GK_r impersonation attack towards U_p by manipulating the R_4 message, U_p may come to know about any forgery on part of adversary by constructing session key SK and verifying the M_{rp} equation. Hence, the proposed scheme resists any possibility of impersonation attack.

5.1.4. Replay Attack. The attacker may eavesdrop the contents exchanged on the public channel, and it can replay the eavesdroped contents. The proposed scheme may resist replay attack successfully since it employs timestamps $T_1 - T_4$ to ensure the freshness of each constructed and submitted message $R_1 - R_4$, respectively. An adversary may not compute fresh messages $R_1 - R_4$ without accessing the shared secrets X_{pr} as well as X_{qr} which are possessed by the legitimate entities of the system.

5.1.5. Stolen Verifier Attack. The proposed scheme is immune to stolen verifier attack by a possible malicious attacker. In our scheme, even if the adversary comes to know about the users' verifiers such as L_{up}, the adversary must need private key K_{GR} to compute X_{pr} and recover further information. It is too hard to guess the private secret key K_{GR} of GK_r for polynomial time adversary. Thus, our scheme is resistant to stolen verifier attack.

5.1.6. Man in the Middle Attack. In our scheme, if an attacker attempts to act as a malicious intermediary among U_p, GK_r, and SD_k entities by manipulating the messages $R_1 - R_4$, it will be detected in the verification procedures such as M_{pr}, M_{qr}, M_{rp}, and M_{rq} of respective entities. It is obvious from the subsection related to resistance from impersonation attacks that if an attacker attempts to replay or modify the parameters of intermediate messages, it will not succeed in these malicious attempts. Hence, our scheme can resist man in the middle attack successfully.

5.1.7. Perfect Forward Secrecy. The proposed scheme supports perfect forward secrecy because even if the private secret key K_{GR} of GK_r is revealed to the adversary, the latter will not be able to compute X_{pr} without accessing the parameter L_{up} which is stored in the repository of GK_r. Thus, the adversary may not compute current, previous, or future session keys, in case the long-term private secret of GK_r is exposed to the adversary.

5.1.8. SD_q Physical Capture. In proposed scheme, if the device SD_q is physically captured by the adversary while the latter extracts B_1 and B_2 from the memory of device, it will not be able to recover the shared secret X_{qr} for lacking access to the private key of SD_q. Moreover, even if the adversary is able to access the SD_q's private key, it will only be able to compute the session key of a particular device while the rest of the smart devices SD_q in the system will remain protected and the attacker will not be able to compute their session keys.

6. Comparisons

In the following subsections, we provide the comparisons of the proposed SKIA-SH and relevant schemes of Wazid et al. [21], Shuai et al. [23], Kaur and Kumar [24], and Yu et al. [20].

6.1. Security Features. The security attribute provision of the proposed SKIA-SH and related schemes [20, 21, 23, 24] is shown in Table 2. Referring to Table 2, except the proposed SKIA-SH scheme, all the related schemes presented in [20, 21, 23, 24] entail one or more weaknesses: the scheme of Yu et al. [20] has a faulty design and it cannot provide mutual authentication between a user and smart devices (SDs), which is proved in Section 3 of this paper. The scheme of Kaur and Kumar [24] has weaknesses against session key disclosure attack and it cannot provide mutual authentication between a user and SDs. The scheme of Shuai et al. [23] cannot resist offline password guessing, insider, replay, and session disclosure attacks, whereas, the scheme of Wazid et al. cannot provide forward secrecy and it cannot resist replay and de-synchronization attacks. Only proposed SKIA-SH provides requisite security attributes and is well suited for smart home (SH) environments.

6.2. Computation Cost. In this section, using a real-time experiment, we provide a comparative computation cost of our SKIA-SH and some of the recent schemes [20, 21, 23, 24]. We conducted the experiment using three devices and corresponding underneath hardware and softwares: ① A Xiaomi Redmi-Note-8 equipped with 4 GB RAM and with an Octa-core 2.01-GHz mprocessor and v-9 andriod MUI-V.11.0.7 operating system, the smart phone simulates a user/mobile-device, ② for GK_r, we adopted an Elite-Book HP 8460P equipped with 4 GB RAM and intel ③ 2.7 GHz mprocessor and th OS used is Ubuntune V.LTS-16, ④ the smart device SD_q is simulated through a Cortex:A53-ARMv8, Pi-B+, 64 bit: SoC, 1 GB: LPDDR2 SDRAM and 1.4 GHz mprocessor. Among other operations, the biohashing/fuzzy extraction T_{fb} is approximated with an elliptic-curve point multiplication T_{em}. The notations and

Table 2: Security features.

Schemes	Our scheme	[20]	[24]	[23]	[21]
MAP	✓	×	×	✓	✓
UAP	✓	✓	✓	✓	✓
SVP	✓	✓	✓	✓	✓
DSN	✓	✓	✓	✓	×
UIA	✓	✓	✓	✓	✓
RAP	✓	✓	✓	×	×
SKD	✓	✓	×	×	✓
PCA	✓	✓	✓	✓	✓
FSP	✓	✓	✓	✓	×
IAP	✓	✓	✓	×	✓
MMP	✓	✓	✓	✓	✓
OPG	✓	✓	✓	×	✓

Note. MAP: mutual authentication provision; UAP: user anonymity and privacy; PSV: stolen verifier protection; DSN: resistance to de-synchronization attack; UIA: user impersonation attack; RAP: replay attack protection; SKD: session key disclosure attack; PCA: protection from physical capture of smart device; FSP: forward secrecy provision; IAP: insider attack protection; MMP: man in middle attack; OPG: offline password guessing attack; ✓: attribute provision; ×: attribute non-provision.

Table 3: Running time.

Entity ⟶	U_p	GK_r	SD_q
↓ Operation			
T_{em}/T_{fb}	5.116	0.926	4.107
T_e	0.017	0.008	0.013
T_h	0.009	0.004	0.006

Note. T_{em}: point multiplication over ECC; T_{fb}: fuzzy extraction/biohashing; T_e: AES-128 block encryption/decryption operation; T_h: secure one-way hash operation.

Table 4: Comparisons of computation and communication costs.

Protocol	U_p	GK_r	SD_q	RT	Bytes ex.
Wazid et al. [21]	$1T_{fb} + 8T_h + 6T_e$	$7T_h + 11T_e$	$5T_h + 11T_e$	≈5.493 ms	376
Shuai et al. [23]	$1T_{fb} + 6T_h + 2T_{em}$	$7T_h + 1T_{em}$	$3T_h$	≈16.374 ms	208
Kaur and Kumar [24]	$1T_{fb} + 6T_h + 2T_{em}$	$8T_h + 1T_{em}$	$3T_h$	≈16.378 ms	224
Yu et al. [20]	$1T_{fb} + 12T_h + 1T_e$	$11T_h$	$7T_h$	≈5.327 ms	196
Proposed	$1T_{fb} + 13T_h + 1T_e$	$12T_h$	$7T_h$	≈5.34 ms	216

Note. RT: running time (ms); ex: exchange.

their corresponding running times on each device according to the conducted experiment are shown in Table 3. To furnish a round of authentication, U_p executes $1T_{fb} + 13T_h + 1T_e$ operations, in addition to $12T_h$ and $7T_h$ executed by GK_r and SD_q. The total running time (RT) on U_p side is ≈5.25 ms, the RT on GK_r is ≈0.048 ms, and the RT on SD_q through the experiment is ≈0.042 ms. Therefore, total RT of the proposed SKIA-SH is ≈5.34 ms. The RT to execute an authentication round of Yu et al.'s scheme is ≈5.327. Similarly, the RT of the schemes of Shuai et al., Kaur and Kumar, and Wazid et al. is ≈16.374, ≈16.378, and ≈5.493, respectively.

6.3. Communication Cost. This section shows the comparisons of our SKIA-SH and the schemes of [20, 21, 23, 24], and for computation cost (CC) comparisons, we adopted SHA-1 with 20-byte output size. The identities and time stamps are kept 8 bytes and 4 bytes, respectively. The random numbers are taken 20 bytes long, and the adopted encryption/decryption algorithm AES-128 also takes 16-byte input and 16-byte output. The size of a coordinate of elliptic curve point (ECP) is 20 bytes and the total length of an ECP is 20 + 20 = 40 bytes. The SKIA-SH (proposed scheme) completes an authentication round by exchanging four (4) messages: ① message sent by U_p to GK_r is $R_1 = \{M_1, M_2, M_{pr}, PID_{up}, T_1\}$. R_1 costs {20 + 20 + 20 + 20 + 4} = 84 bytes. ② Message sent by GK_r to SQ_q is $R_2 = \{M_3, M_{qr}, T_2\}$. R_2 costs {20 + 20 + 4} = 44 bytes. ③ Message sent by SQ_q to GK_r is $R_3 = \{M_4, M_{rq}, T_3\}$, and R_3 costs {20 + 20 + 4} = 44 bytes. ④ Likewise, the message sent by GK_r to U_p is $R_4 = \{M_5, M_{rp}, T_4\}$, and R_4 costs {20 + 20 + 4} = 44 bytes. Therefore, total bytes exchanged during a round of authentication cycle are {84 + 44 + 44 + 44} = 216 bytes. The communication cost of the Yu et al.'s scheme is {64 + 44 + 44 + 44} = 196 bytes. Similarly, the communication cost of the scheme of Shuai et al., Kaur and Kumar, and Wazid et al. is 208 bytes, 224 bytes, and 376 bytes, respectively. The computation and communication cost comparisons are also depicted in Table 4.

7. Conclusion

In this article, we highlighted the need of secure and communication between the smart devices and users through the facilitation of the gateway in the smart home (SH) settings of the IoT. We then reviewed a very recent authentication scheme of Yu et al. We proved that the symmetric key-based efficient and secure authentication scheme entails a critical design flaw, and owing to the explored design flaw, the scheme of Yu et al. cannot complete a cycle of authentication process. An improved scheme free of design flaws and based on only symmetric key function for SH (SKIA-SH) is proposed to mitigate the security and efficiency issues of the SH environments. The security of the SKIA-SH is substantiated through BAN logic. Moreover, we provided a brief discussion of the security attribute provision of the proposed SKIA-SH. To measure the performance, we set up a real-time experiment, and the results show that the SKIA-SH is more secure while it has slight over computation and communication costs when compared with original scheme of Yu et al. The SKIA-SH accomplishes the authentication among a user and a smart device involving gateway in 5.34 ms and by exchanging 216 bytes. As a future work, we intend to extend the proposed method to work in a building area network to provide central and apartment-based services.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, under grant no. RG-3-611-41. The authors, therefore, acknowledge with thanks the DSR for technical and financial support.

References

[1] V. Sivaraman, H. H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[2] T.-Y. Wu, Z. Lee, L. Yang, and C.-M. Chen, "A provably secure authentication and key exchange protocol in vehicular ad hoc networks," *Security and Communication Networks*, vol. 2021, Article ID 9944460, 17 pages, 2021.

[3] P. Gope, H. Islam, M. S. Obaidat, R. Amin, and P. Vijayakumar, "Anonymous and expeditious mobile user authentication scheme for glomonet environments," *International Journal of Communication Systems*, vol. 31, no. 2, pp. 1–18, 2017.

[4] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 80, pp. 483–495, 2018.

[5] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "Lake-6sh: lightweight user authenticated key exchange for 6lowpan-based smart homes," *IEEE Internet of Things Journal*, vol. 1, 2021.

[6] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. B. Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IOT environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, 2021.

[7] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "Ramp-iod: a robust authenticated key management protocol for the internet of drones," *IEEE Internet of Things Journal*, vol. 1, 2021.

[8] F. Wu, L. Xiong, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with IOT notion," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1120–1129, 2021.

[9] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Proceedings of the IEEE International Conference Consumer Electronics (ICCE)*, pp. 787-788, Las Vegas, NV, USA, January 2011.

[10] F. K. Santoso and N. C. H. Vun, "Securing IOT for smart home system," in *Proceedings of the International Symposium on Consumer Electronics*, Madrid, Spain, June 2015.

[11] S. A. Chaudhry, A. Irshad, J. Nebhen, and A. K. Bashir, "An anonymous device to device access control based on secure certificate for internet of medical things systems," *Sustainable Cities and Society*, vol. 75, Article ID 103322, 2021.

[12] A. Irshad, M. Sher, H. F. Ahmad, and B. A. Alzharani, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 12, pp. 5529–5552, 2016.

[13] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE systems journal*, vol. 9, no. 3, pp. 805–815, 2015.

[14] T. Maitra, M. S. Obaidat, R. Amin, S. H. Islam, S. A. Chaudhry, and D. Giri, "A robust elgamal-based password-authentication protocol using smart card for client-server communication," *International Journal of Communication Systems*, vol. 30, no. 11, Article ID e3242, 2017.

[15] Y.-C. Lee, Y.-C. Hsieh, P.-J. Lee, and P.-S. You, "Improvement of the ElGamal based remote authentication scheme using smart cards," *Journal of Applied Research and Technology*, vol. 12, no. 6, pp. 1063–1072, 2014.

[16] A. Ali Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "Palk: password-based anonymous lightweight key agreement framework for smart grid," *International Journal of Electrical Power & Energy Systems*, vol. 121, 2020 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061519340621, Article ID 106121.

[17] J. Wei, W. Liu, and X. Hu, "Secure control protocol for universal serial bus mass storage devices," *IET Computers & Digital Techniques*, vol. 9, no. 6, pp. 321–327, 2015.

[18] S. A. Chaudhry, "Correcting "palk: password-based anonymous lightweight key agreement framework for smart grid"," *International Journal of Electrical Power & Energy Systems*, vol. 125, Article ID 106529, 2021.

[19] M. F. Ayub, S. Shamshad, K. Mahmood, S. H. Islam, R. M. Parizi, and K.-K. R. Choo, "A provably secure two-factor authentication scheme for usb storage devices," *IEEE*

Transactions on Consumer Electronics, vol. 66, no. 4, pp. 396–405, 2020.

[20] S. Yu, N. Jho, and Y. Park, "Lightweight three-factor-based privacy- preserving authentication scheme for iot-enabled smart homes," *IEEE Access*, vol. 9, pp. 126186–126197, 2021.

[21] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 391–406, 2020.

[22] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely access "my" smart home in private: an anti-tracking authentication and key agreement scheme," *IEEE Access*, vol. 7, pp. 41835–41851, 2019.

[23] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, vol. 86, no. 132–146, 2019.

[24] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *Journal of Informatics*, vol. 58, pp. 2787–10279, 2021.

[25] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[26] C.-M. Chen and S. Liu, "Improved secure and lightweight authentication scheme for next-generation IOT infrastructure," *Security and Communication Networks*, vol. 2021, Article ID 6537678, 13 pages, 2021.

[27] L. Xiong, L. Tian, M. S. Obaidat, and F. Wu, "A lightweight privacy-preserving authentication protocol for vanets," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3547–3557, 2020.

[28] C. Ran and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, Springer, Innsbruck, Austria, June 2001.

[29] T.-Y. Wu, L. Yang, M. Qian, X. Guo, and C.-M. Chen, "Fog-driven secure authentication and key exchange scheme for wearable health monitoring system," *Security and Communication Networks*, vol. 2021, Article ID 8368646, 14 pages, 2021.

[30] Z. Ali, S. A. Chaudhry, and K. Mahmood, "A clogging resistant secure authentication scheme for fog computing services," *Computer Networks*, vol. 185, Article ID 107731, 2021.

[31] M. A. Saleem, S. H. Islam, S. Mahmood, and M. Hussain, "Provably secure biometric-based client-server secure communication over unreliable networks," *Journal of Information Security and Applications*, vol. 58, Article ID 102769, 2021.

[32] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2014.

[33] M. Burrows, M. Abadi, and R. Michael Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.