IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 26, 2021, accepted September 6, 2021, date of publication September 9, 2021, date of current version September 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3111443

Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes

SUNGJIN YU[1,2], NAMSU JHO[1], AND YOUNGHO PARK[2,3], (Member, IEEE)
[1]Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[2]School of Electronics and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
[3]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 funded by Korean Government (Core Technology Research on Trust Data Connectome) under Grant 20ZR1300.

ABSTRACT Smart homes are an emerging paradigm of Internet of Things (IoT) in which users can remotely control various home devices via the internet anytime and anywhere. However, smart home environments are vulnerable to security attacks because an attacker can inject, insert, intercept, delete, and modify transmitted messages over an insecure channel. Thus, secure and lightweight authentication protocols are essential to ensure useful services in smart home environments. In 2021, Kaur and Kumar presented a two-factor based user authentication protocol for smart homes using elliptic curve cryptosystems (ECC). Unfortunately, we demonstrate that their scheme cannot resist security attacks such as impersonation and session key disclosure attacks, and also ensure secure user authentication. Moreover, their scheme is not suitable in smart home environments because it utilizes public-key cryptosystems such as ECC. Hence, we design a secure and lightweight three-factor based privacy-preserving authentication scheme for IoT-enabled smart home environments to overcome the security problems of Kaur and Kumar's protocol. We prove the security of the proposed scheme by using informal and formal security analyses such as the ROR model and AVISPA simulation. In addition, we compare the performance and security features between the proposed scheme and related schemes. The proposed scheme better provides security and efficiency compared with the previous schemes and is more suitable than previous schemes for IoT-enabled smart home environments.

INDEX TERMS Smart homes, privacy-preserving, authentication, security protocol.

I. INTRODUCTION

With the advances in 5G communication and portable device technologies, smart homes are emerging as an exciting new paradigm of Internet of Things (IoT) and also it has attracted a lot of attention from both scientific and academic communities. Smart homes [1]–[3] are networking environments in which smart devices such as smart curtains, smart washing machines, smart light bulbs, smart TV, and smart door locks/control mechanisms can communicate with other devices, and also are remotely controlled.

In smart home environments, users are able to enjoy new smart functionalities and services such as a high level of comfort, and improved quality of life using a portable device. For example, if a user opens the door and enters the home, the smart home system starts working and turns on the lights and boiler in the house. Moreover, the smart home can ensure convenient and efficient services to chronic diseases, disabled, and elderly people by identifying their health and behavioral patterns through smart devices. However, despite the multiple advantages of the smart home, it may cause serious privacy issues [4] since the collected data in smart devices are transmitted over an insecure channel. If collected data in smart devices is compromised, a malicious attacker can obtain the sensitive information of legitimate users, including daily habits and routines in the home, and also can utilize the information for criminal purposes. Moreover, the smart devices deployed in smart home environments are not suitable to apply public key cryptosystems (PKC) because it is resource-limited in terms of computation and communication overheads [5], [6]. Thus, secure and lightweight authentication and key agreement (AKA) schemes are essential to provide security and privacy for legitimate users [7]–[9].

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

In 2019, Shuai *et al.* [10] proposed a two-factor based anonymous authentication protocol for smart homes using elliptic curve cryptography (ECC). However, Kaur and Kumar [11] pointed out that Shuai *et al.*'s scheme [10] is vulnerable to replay, insider, session key disclosure, offline password guessing, and gateway bypass attacks. In 2021, Kaur and Kumar [11] presented cryptanalysis and improvement of a two-factor based authentication scheme for smart homes using ECC to enhance the security flaws of Shuai *et al.*'s scheme [11]. However, we prove that Kaur and Kumar's scheme [11] is still vulnerable to impersonation, session key disclosure attacks, and also cannot provide mutual authentication. Moreover, their scheme is not suitable for resource-limited devices because it utilizes ECC that generates high computation and communication overheads. Therefore, we design a secure and lightweight three-factor based privacy-preserving authentication scheme for IoT-enabled smart homes to resolve the security problems Kaur and Kumar's scheme [11]. The proposed AKA scheme additionally utilizes the fuzzy extractor mechanism to improve the security level of the two-factor AKA scheme. Even if two of the three factors are compromised, our AKA scheme is secure. Moreover, our scheme is suitable for resource-limited smart devices in smart home environments because it uses hash and XOR functions that generate low computation overheads.

A. CONTRIBUTIONS

The main contributions of the proposed AKA scheme are summarized as follows:

- We design a secure and lightweight three-factor based privacy-preserving user authentication scheme in IoT-enabled smart home environments to provide secure home services for legitimate users.
- The proposed AKA scheme resists various security attacks such as impersonation attack, and session key disclosure attack, and also provides the security functionalities such as mutual authentication, anonymity, and privacy.
- We perform formal (simulation) security of the proposed protocol using the Automated Verification of Internet Security Protocols and Applications (AVISPA) [12], [13], which evaluates security against various security attacks. Furthermore, we perform formal (mathematical) security analysis using the Real-or-Random (ROR) model [14] to evaluate the session key security of the proposed AKA scheme.
- We perform a comparative analysis of the proposed protocol and related schemes in terms of security features, computation costs, communication costs, and storage costs.

B. MOTIVATIONS

The major goal of this paper is to resolve the security weaknesses and inefficient efficiency present in Kaur and Kumar's scheme [11]. Their scheme does not provide the essential security functionalities such as session key disclosure attack, impersonation attack, and mutual authentication in IoT-enabled smart home environments. In addition, Kaur and Kumar's scheme [11] is not suitable for resource-constrained smart devices because it uses ECC, which generates high computation and communication overheads. These facts motivated us to propose a new secure and lightweight authentication protocol, which can provide the necessary security functionalities and effective efficiency and resolve security flaws that exist in IoT-enabled smart home environments. Thus, the proposed AKA scheme utilizes the fuzzy extractor mechanism to improve the security level of the two-factor AKA scheme and also ensures efficient performance because it utilizes only hash function and XOR operation that generate low computation and communication overheads.

C. ORGANIZATIONS

The structure of this paper is organized as follows. Section II presents the overview of related works for smart homes and Section III introduces the overview of the preliminaries. In Section IV, we review a detailed overview of Kaur and Kumar's scheme. In Section V and Section VI, we analyze the security flaws of Kaur and Kumar's scheme and proposes a secure and lightweight three-factor based privacy-preserving authentication scheme for IoT-enabled smart homes. Section VII presents the security analyzes of the proposed AKA scheme by using informal and formal security analysis. In Section VIII, we demonstrate the performance comparative analysis of the proposed AKA scheme with the previous schemes. Finally, we conclude this paper in Section IX.

II. RELATED WORKS

In the last few years, numerous AKA mechanisms have been presented to provide the security and privacy of users in various environments [1], [15]–[18]. In 2008, Jeong *et al.* [19] presented an AKA protocol to provide security in smart home environments using one-time password (OTP) and smart card. Jeong *et al.* [19] were claimed that their protocol ensures security from various security attacks. However, their protocol is vulnerable to potential security attacks such as smart card theft and insider attacks. In addition, their protocol is not provided mutual authentication between gateway and smart device and also is not achieved the untraceability and anonymity as the identity of the legitimate user is transmitted in plaintext over an open channel. Thus, their schemes [19] using smart card and OTP could not resist the various security attacks such as offline password guessing and smart card stolen attacks. In 2011, Vaidya *et al.* [20] presented a secure one-time password based AKA scheme using smart card in smart home environments. However, Kim *et al.* [21] proved that Vaidya *et al.*'s scheme [20] cannot resist offline password guessing attacks and does not ensure forward secrecy with smart card stolen attacks. Kim *et al.* [21] subsequently presented an enhanced AKA scheme to improve the security weaknesses of the Vaidya *et al.*'s scheme [20]. However, Kim *et al.*'s scheme [21] also fails to ensure user anonymity and untraceability of the smart device and legitimate user. These two-factor based AKA schemes for smart home cannot prevent various security attacks such as offline password guessing and smart card stolen attacks.

In the past few years, many researchers have been proposed symmetric/asymmetric-based AKA schemes for smart homes [22]–[24] to overcome the above-mentioned security flaws. In 2011, Vaidya *et al.* [25] proposed an ECC-based secure and lightweight AKA scheme for smart home networks. However, their scheme [25] suffered from insider, impersonation, and offline password guessing attacks. In 2015, Santoso *et al.* [26] presented a secure AKA scheme using ECC in smart home environments. However, Santoso *et al.*'s scheme [26] is insecure against stolen verifier and insider attacks. In 2019, Shuai *et al.* [10] presented a two-factor based lightweight AKA mechanism for smart home with provable security using ECC. However, Kaur and Kumar [11] proved that Shuai *et al.*'s scheme [10] is insecure against insider, replay, session key disclosure, gateway bypass, and offline password guessing attacks. In 2020, Wazid *et al.* [27] presented the symmetric key cryptography and hash function based efficient AKA scheme for smart homes. However, Lyu *et al.* [28] claimed that Wazid *et al.*'s scheme [27] cannot resist compromised server and desynchronization attacks. These symmetric/asymmetric-based AKA schemes for smart homes are still cannot various security attacks, and also not suitable for the resource-limited smart devices in smart home environments since it requires high computational costs.

In 2021, Kaur and Kumar [11] proposed an enhanced two-factor based AKA scheme in smart home environments to overcome the security problems of Shuai *et al.*'s scheme [10]. They were claimed that their protocol can resist potential security attacks and also guarantees user anonymity, privacy, and mutual authentication. However, we proved that Kaur and Kumar's scheme also is vulnerable to impersonation and session key disclosure attacks, and does not achieve mutual authentication. Moreover, their scheme is not suitable for resource-constrained devices because it utilizes public-key cryptosystems such as ECC. Thus, we design a secure and lightweight three-factor based privacy-preserving AKA scheme for IoT-enabled smart homes to resolve the security flaws Kaur and Kumar's scheme [11].

III. PRELIMINARIES

We introduce the overview of the preliminaries to enhance the readability of this article.

A. THREAT MODEL

This section presents the widely-known Dolev-Yao (DY) model [29] to demonstrate the security of the proposed AKA scheme. In the DY model, the capabilities of a malicious adversary are as follows.

- In this model, a malicious adversary (*MA*) can insert, delete, eavesdrop, replay, modify transmitted messages over an insecure channel.
- If a smart card of the legitimate user is stolen, its secret credentials can be extracted by *MA* using power-analysis attacks [30]–[32].
- The smart devices can be tampered, and physically captured by *MA* in the registration phase. Thus, *MA* can extract the secret credentials stored in its memory [33]–[35].
- *MA* can attempt offline identity and offline password guessing attacks. Thus, *MA* can guess the real identity and password of the legitimate user simultaneously.
- After getting the secret credentials of the smart device and smart card, *MA* may try potential security attacks such as offline guessing, session key disclosure, impersonation, and privileged insider attacks [36], [37].

B. FUZZY EXTRACTOR

This section introduces the basic concepts of the fuzzy extractors [38]. The fuzzy extractors are a cryptographic method using user biometric to perform a secure authentication and it consists of the two operations as the generator $Gen(\cdot)$ and reproduction $Rep(\cdot)$ which are denoted as follows:

1. $Gen(\cdot)$: Given a user's biometric input BIO, $Gen(\cdot)$ selects a biometric secret key $\gamma_i \in \{0, 1\}^l$ and a public reproduction parameter $\beta_i \in \{0, 1\}^*$, which is a probabilistic function.
2. $Rep(\cdot)$: Given a noisy biometric input BIO, $Rep(\cdot)$ reproduces γ_i using value β_i, which is public reproduction related with BIO.

C. SYSTEM MODEL

This section introduces the system model for IoT-enabled smart homes in Figure 1. The proposed system model consists of four entities: the registration authority, user, gateway, and smart device. The detailed descriptions of each entity are as follows:

- Registration authority (RA): The registration authority is a trusted authority and is responsible for the registration of participants.
- Gateway: The gateway manages the collected data in smart devices to provide useful home services for legitimate users. In addition, the gateway is a powerful entity and serves as a bridge between the smart device and legitimate user.
- User: The authorized user by the registration authority can access useful home services through the gateway using a portable device at anytime and anywhere.
- Smart Devices: The smart devices (e.g. sensors and things) deployed in smart homes are resource-limited, collect a large amount of real-time data and transmit the collected data to the legitimate user.

IV. REVIEW OF KAUR AND KUMAR's SCHEME

We review Kaur and Kumar's scheme [11] for smart homes. Their scheme consists of three phases: 1) initialization,

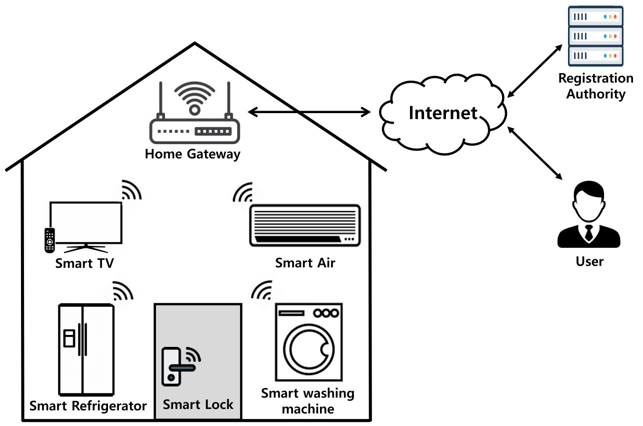

FIGURE 1. System model for IoT-enabled smart homes.

2) registration and 3) mutual authentication. The symbols used in this paper are as shown in Table 1.

TABLE 1. Symbols.

Symbol	Description
U_i	User
SD_j	Smart device
GW	Gateway
RA	Registration authority
ID_i, PW_i	U_i's identity and password
SID_j, GID_i	Identity of SD_j and GW_i
T_i	Timestamp
v	Fuzzy verifier
SK	Session key
K_G	GW's master key
X_{GU}	Common secret key between U_i and GW
X_{GS}	Common secret key between SD_j and GW
$h(\cdot)$	Hash function
$\oplus$	XOR operation
$\|\|$	Concatenation operations

A. INITIALIZATION PHASE

The registration authority RA performs the initialization tasks as follows:

- **IP-1:** RA selects an elliptic curve E on the basic field F_p and forms an additive group AG of the order p generated by G.
- **IP-2:** After that, RA generates a private key z and public key $PK = z \cdot G$ and also selects a master key K_G for GW.
- **IP-3:** RA stores z and K_G in the memory of GW, and then loads system public parameters $\{E(F_p), AG, G, PK, h(\cdot)\}$ in GW and SD_j, which are publicly known to all U_i.
- **IP-4:** Finally, RA selects the identities of SD_j and also stores it in the memory of SD_j.

B. REGISTRATION PHASE

This phase includes the user and smart device registration phases. The detailed descriptions are as below:

1) USER REGISTRATION PHASE

U_i performs the following steps with RA to register in the system.

- **URP-1:** U_i chooses a ID_i and a PW_i and generates a random number r. After that, U_i calculates $RID_i = h(ID_i||r)$, $RPW_i = h(PW_i||r)$, and transmits it to RA via a secure channel.
- **URP-2:** RA verifies whether RID_i chosen by U_i is already assigned or not. If it is already assigned U_i is asked to select a new identity. Otherwise, RA computes $X_{GU} = h(RID_i||K_G)$ and $B_1 = X_{GU} \oplus RPW_i$. Then, RA keeps track of number of attempts taken in T while logging in which initially have the zero value in it. RA stores the credential $\{B_1, T\}$ in smart card (SC) and trasmits it to U_i.
- **URP-3:** U_i computes $B_2 = r \oplus h(ID_i||PW_i)$ and $B_3 = h(RID_i||RPW_i) \bmod v$ which v is fuzzy verifier whose value is $2^4 \leq v \leq 2^8$. Finally, U_i stores $\{B_2, B_3\}$ in memory of smart card.

2) SMART DEVICE REGISTRATION PHASE

SD_j performs the following steps with RA to register in the system.

- **SDRP-1:** SD_j selects a SID_j and transmits it to RA via a secure channel.
- **SDRP-2:** RA verifies whether SID_j already assigned to other SD_j or not. If SD_j is already assigned registration request is terminated. Otherwise, RA computes $X_{GS} = h(SID_j||K_G)$ and transmits it to SD_j.
- **SDRP-3:** Finally, SD_j stores X_{GS} in memory of SD_j.

C. MUTUAL AUTHENTICATION PHASE

In this phase, U_i and SD_j must establish a common session key with the help of GW to access secure home services. We describe the detailed mutual authentication phase of Kaur and Kumar's scheme [11] as follows:

- **MAP-1:** U_i first enters ID_i and PW_i and calculates $r^* = h(ID_i||PW_i) \oplus B_2$, $RPW_i^* = h(PW_i||r^*)$, $RID_i^* = h(ID_i||r^*)$, $B_3^* = h(RID_i^*||RPW_i^*) \bmod v$ and verifies if $B_3^* \stackrel{?}{=} B_3$. If the condition is correct, U_i generates a random numbers x_1 and c, and selects the identity SID_j of SD_j with whom U_i wants to connect. U_i calculates $X_{GU} = RPW_i \oplus B_1$, $B_4 = c \cdot G$, $B_5 = c \cdot PK$, $PID_i = RID_i \oplus B_5$, $N_1 = (x_1||SID_j) \oplus X_{GU} \oplus T_1$, and $W_1 = h(RID_i||x_1||X_{GU}||N_1)$. Then, U_i transmits $\{PID_i, B_4, N_1, W_1, T_1\}$ to GW over a public channel.
- **MAP-2:** On getting the messages from U_i, GW computes $B_5^* = z \cdot B_4$, $RID_i^* = PID_i \oplus B_5^*$, $X_{GU} = h(RID_i^*||K_G)$, $(x_1^*||SID_j) = N_1 \oplus X_{GU} \oplus T_1$, and $W_1^* = h(RID_i^*||x_1^*)||X_{GU}||N_1)$ and checks if $W_1^* \stackrel{?}{=} W_1$. If it is valid, GW generates a random number x_2 and calculates $X_{GS} = h(SID_j||K_G)$, $N_2 = X_{GS} \oplus T_2 \oplus (RID_i||GID_i||x_1||x_2)$, and $W_2 = h(RID_i||GID_i||X_{GS}||x_1||x_2)$. After that, GW sends $\{N_2, W_2, T_2\}$ to SD_j.
- **MAP-3:** SD_j computes $(RID_i||GID_i||x_1||x_2) = N_2 \oplus X_{GS} \oplus T_2$ and $W_2^* = h(RID_i||GID_i||X_{GS}||x_1||x_2)$, and then checks if $W_2^* \stackrel{?}{=} W_2$. If the condition is valid, SD_j

generates a random number x_3 and computes a session key $SK = h(RID_i||GID_i||SID_j||x_1||x_2||x_3)$, $N_3 = x_3 \oplus X_{GS} \oplus T_3$, and $W_3 = h(x_3||X_{GS}||SK)$. After that, SD_j tnrasmits $\{N_3, W_3, T_3\}$ to GW over a public channel.

- **MAP-4:** On getting the messages from SD_j, GW computes $x_3 = N_3 \oplus X_{GS} \oplus T_3$, $SK = h(RID_i|| GID_i||SID_j||x_1||x_2||x_3)$, and $W_3^* = h(x_3||X_{GS}||SK)$, and verifies if $W_3^* \stackrel{?}{=} W_3$. If it is valid, GW computes $N_4 = (GID_i||x_2||x_3) \oplus X_{GU} \oplus T_4$ and $W_4 = h(X_{GU}||SK||x_2||x_3)$, and then sends $\{N_4, W_4, T_4\}$ to U_i.
- **MAP-5:** U_i computes $(GID_i||x_2||x_3) = N_4 \oplus X_{GU} \oplus T_4$, $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$, and $W_4^* = h(X_{GU}||SK||x_2||x_3)$ and checks if $W_4^* \stackrel{?}{=} W_4$. If it is valid, the mutual authentication between U_i and SD_j is successful, and also a common session key is established between them.

V. CRYPTANALYSIS OF KAUR AND KUMAR's SCHEME

In this section, we perform the cryptanalysis of Kaur and Kumar's scheme [11]. Kaur and Kumar [11] claimed that their scheme can prevent various security attacks, and also provide mutual authentication. Unfortunately, we prove that their scheme cannot resist potential security attacks such as impersonation and session key disclosure attacks, and also does not ensure mutual authentication.

A. IMPERSONATION ATTACK

Referring to Section III-A, if MA captures SD_j, MA can extract the secret parameters $\{SID_j, X_{GS}\}$ stored in its memory. In addition, MA can insert, delete, eavesdrop, replay, and modify the exchanged messages over an insecure channel. The detailed descriptions of this attack are as below.

- **Step 1:** MA computes $(RID_i||GID_i||x_1||x_2) = N_2 \oplus X_{GS} \oplus T_2$. Then, MA generates a new random number x_{MA}, $SK_{MA} = h(RID_i||GID_i||SID_j||x_1||x_2||x_{MA})$, $N_{MA3} = x_{MA} \oplus X_{GS} \oplus T_3$, and $W_{MA3} = h(x_{MA}||X_{GS} ||SK_{MA})$. After that, MA transmits $\{N_{MA3}, W_{MA3}, T_3\}$ to GW over a public channel.
- **Step 2:** After obtaining the messages, GW computes $x_{MA} = N_{MA3} \oplus X_{GS} \oplus T_3$, $SK = h(RID_i|| GID_i||SID_j||x_1||x_2||x_{MA})$, $W_{MA3}^* = h(x_{MA}||X_{GS}||SK_{MA})$, and checks if $W_{MA3}^* \stackrel{?}{=} W_{MA3}$. If the condition is valid, GW generates a timestamp T_4 and computes $N_{MA4} = (GID_i||x_2||x_{MA3}) \oplus X_{GU} \oplus T_4$, and $W_{MA4} = h(X_{GU}||SK_{MA}||x_2||X_{MA3})$. Then, GW sends $\{N_{MA4}, W_{MA4}, T_4\}$ to U_i.
- **Step 3:** U_i computes $(GID_i||x_2||x_{MA3}) = N_{MA4} \oplus X_{GU} \oplus T_4$, $SK_{MA} = h(RID_i||GID_i||SID_j||x_1||x_2||x_{MA3})$, and $W_{MA4}^* = h(X_{GU}||SK_{MA}||x_2||x_{MA3})$, and verifies if $W_{MA4}^* \stackrel{?}{=} W_{MA4}$. If it is correct, MA impersonate as SD_j successfully and also shares the common session key SK_{MA} with U_i successfully.

B. SESSION KEY DISCLOSURE ATTACK

In this attack, MA can calculate a session key $SK = h(RID_i||GID_i||SID_j||x_1||x_2||x_3)$ between U_i and SD_j. According to Section III-A, MA can extract the secret parameters $\{SID_j, X_{GS}\}$ stored in SD_j. Then, MA computes $(RID_i||GID_i||x_1||x_2) = N_2 \oplus X_{GS} \oplus T_2$ and $x_3 = N_3 \oplus X_{GS} \oplus T_3$. MA can calculate a session key $SK = h(RID_i||GID_i||SID_j||x_1||x_2||x_3)$ successfully. Therefore, Kaur and Kumar's scheme is insecure to session key disclosure attacks.

C. MUTUAL AUTHENTICATION

Kaur and Kumar claimed that their scheme provides mutual authentication among U_i, GW, and SD_j. However, according to Section V-A and V-B, MA can calculate the authentication request message $W_2 = h(RID_i||GID_i||X_{GS}||x_1||x_2)$ and response message $W_3 = h(x_3||X_{GS}||SK)$ successfully. Thus, Kaur and Kumar's scheme does not provide a secure mutual authentication.

VI. PROPOSED SCHEME

We design a secure and lightweight three-factor based privacy-preserving AKA scheme for IoT-enabled smart homes to enhance the security weaknesses of Kaur and Kumar's scheme [11]. The proposed AKA scheme consists of four phases: 1) initialization, 2) registration, 3) mutual authentication, and 4) password and biometric update. The detailed descriptions are as follows:

A. INITIALIZATION PHASE

In the proposed scheme, the pre-configured during manufacturing production or reconfigured during maintenance, a master key is assumed to be pre-shared in the tamper-resistant memory of the security module such as the trusted platform module (TPM). Before GW and SD_j are deployed in smart home environments, RA first generates a master key K_G and then stores it in the tamper-resistant memory of GW. SD_j chooses a SID_j and sends it to RA via a secure channel. Then, RA checks whether SID_j. If it is correct, RA stores it in the tamper-resistant memory of GW and then generates a master key K_{SD} of SD_j and stores it in the tamper-resistant memory of SD_j.

B. REGISTRATION PHASE

This phase includes the user and smart device registration phases. The detailed descriptions are as below:

1) USER REGISTRATION PHASE

U_i must register with RA to access the useful home services.

- **URP-1:** U_i generates a random number a_i and enters a unique ID_i and PW_i, and imprints biometric BIO. Then, U_i computes $Gen(BIO) = \langle \gamma_i, \beta_i \rangle$, and $RID_i = h(ID_i||\gamma_i)$, and $RPW_i = h(PW_i||\gamma_i)$ and transmits $\{RID_i, RPW_i, a_i\}$ to RA over a secure channel.
- **URP-2:** RA computes $X_{GU} = h(RID_i||K_G||a_i)$ and $A_1 = X_{GU} \oplus h(a_i||RPW_i)$. Then, RA sends $\{X_{GU}\}$ to the GW via a secure channel. Then, GW computes $L_i = h(GID_i||K_G) \oplus X_{GU}$ and stores $\{L_i\}$ in secure database. Finally, RA stores $\{A_1\}$ in the smart card and issues the smart card to U_i via a secure channel.

- **URP-3:** U_i computes $K_i = h(ID_i||PW_i||\gamma_i)$, $A_2 = E_{K_i}(A_1)$, $A_3 = a_i \oplus h(RID_i||RPW_i)$, and $A_4 = h(RID_i||RPW_i||a_i)$. After that, U_i eliminates $\{A_1\}$ in the smart card and then stores $\{A_2, A_3, A_4\}$ in the smart card. As a result, the smart card containts the secret parameters $\{A_2, A_3, A_4\}$.

2) SMART DEVICE REGISTRATION PHASE

SD_j performs the following steps with RA to provide the useful home services.

- **SDRP-1:** SD_j generates a random number b_j and computes $PID_j = h(SID_j||b_j)$. Then, SD_j transmits $\{b_j, PID_j\}$ to RA over a secure channel.
- **SDRP-2:** RA computes $X_{GS} = h(PID_j||K_G||b_j)$. After that, RA stores $\{PID_j, b_j\}$ in secure database of GW and transmits $\{X_{GS}\}$ to SD_j via a secure channel.
- **SDRP-3:** SD_j computes $B_1 = h(SID_{SD}||K_{SD}) \oplus b_j$ and $B_2 = h(K_{SD}||b_j) \oplus X_{GS}$. Finally, SD_j stores $\{B_1, B_2\}$ in the memory.

C. MUTUAL AUTHENTICATION PHASE

The registered U_i and SD_j must establish a common session key with the help of GW to utilize secure home services. Figure 2 shows the mutual authentication phase of the proposed AKA scheme and also the detailed processes are as follows:

- **MAP-1:** U_i inputs ID_i, PW_i and imprints BIO. Then, U_i computes $\gamma_i = Rep(BIO, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i = h(PW_i||\gamma_i)$, $K_i = h(ID_i||PW_i||\gamma_i)$, and retrieves $\{A_2\}$ in mobile devices. After that, U_i computes $A_1 = D_{K_i}(A_2)$, $a_i = A_3 \oplus h(RID_i||RPW_i)$, $X_{GU} = A_1 \oplus h(a_i||RPW_i)$ and $A_4^* = h(RID_i||RPW_i||a_i)$, and checks whether $A_4^* \stackrel{?}{=} A_4$. If the condition is valid, U_i generates a random nonce r_U, and a timestamp T_1. Then, U_i selects a identity SID_j of the SD_j and computes $M_1 = (SID_j|||r_U) \oplus X_{GU}$, $M_2 = RID_i \oplus h(X_{GU}||r_U)$, and $M_{UG} = h(RID_i||X_{GU}||r_U)$. After that, U_i transmits $\{M_1, M_2, M_{UG}\}$ to GW over a public channel.
- **MAP-2:** After getting the messages from U_i, GW retrieves $\{L_i\}$ in secure database and computes $X_{GU} = h(GID_i||K_G) \oplus L_i$, $(SID_j||r_U) = M_1 \oplus X_{GU} \oplus T_1$, $RID_i = M_2 \oplus h(X_{GU}||r_U||T_1)$, and $M_{UG}^* = h(RID_i||X_{GU}||r_U||T_1)$. Then, GW_i verifies if $M_{UG}^* \stackrel{?}{=} M_{UG}$. After that, GW generates a r_{GW} and a T_2. Then, GW computes $X_{GS} = h(SID_j||K_G)$, $M_3 = (RID_i||GID_i||r_U||r_{GW}) \oplus h(SID_j||X_{GS}||T_2)$ and $M_{GS} = h(RID_i||GID_i||X_{GS}||r_U||r_{GW}||T_2)$. Then, GW transmits $\{M_3, M_{GS}, T_2\}$ to SD_j.
- **MAP-3:** On getting the messages from GW, SD_j retrieves $\{B_1, B_2\}$ in the memory and computes $b_j = B_1 \oplus h(PID_j||K_{SD})$, $X_{GS} = B_2 \oplus h(K_{SD}||b_j)$, $(RID_i||GID_i||r_U||r_{GW}) = M_3 \oplus h(SID_j||X_{GS}||T_2)$ and $M_{GS}^* = h(RID_i||GID_i||X_{GS}||r_U||r_{GW}||T_2)$, and checks if $M_{GS}^* \stackrel{?}{=} M_{GS}$. If it is valid, SD_j generates a r_{SD} and T_3. After that, SD_j generates a random nonce r_{SD} and a timestamp T_3. Then, SD_j computes $M_4 = r_{SD} \oplus h(X_{GS}||RID_i||GID_i||T_3)$, $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$, and $M_{SG} = h(SID_j||r_{SD}||X_{GS}||SK||T_3)$. Finally, SD_j transmits $\{M_4, M_{SG}, T_3\}$ to GW via a public channel.
- **MAP-4:** After getting the messages from SD_j, GW computes $r_{SD} = M_4 \oplus h(X_{GS}||RID_i||GID_i||T_3)$, $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$, $M_{SG}^* = h(SID_j||r_{SD}||X_{GS}||SK||T_3)$, and checks if $M_{SG}^* \stackrel{?}{=} M_{SG}$. If the condition is correct, GW generates a timestamp T_4 and computes $M_5 = (GID_i||r_{GW}||r_{SD}) \oplus h(RID_i||X_{GU}||r_U||T_4)$ and $M_{GU} = h(RID_i||GID_i||r_U|| r_{GW}||SK||T_4)$. Finally, GW transmits $\{M_5, M_{GU}, T_4\}$ to U_i.
- **MAP-5:** On getting the messages from GW, U_i computes $(GID_i||r_{GW}||r_{SD}) = M_5 \oplus h(RID_i||X_{GU}||r_U||T_4)$, $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$, and $M_{GU}^* = h(RID_i||GID_i||r_U||r_{GW}||SK||T_4)$, and checks if $M_{GU}^* \stackrel{?}{=} M_{GU}$. if it is valid, the mutual authentication between U_i and SD_j is successful, and also a common session key is established between them.

D. PASSWORD AND BIOMETRIC UPDATE PHASE

If an authorized user wants a new password and biometric, and biometric, U_i can easily update their own old password and old biometric. The detailed descriptions are as follows:

PBUP-1: U_i first inputs a identity ID_i, a old password PW_i^{old}, and imprints a old biometric BIO^{old}.

PBUP-2: After that, SC computes $\gamma_i = Rep(BIO^{old}, \beta_i)$, $RID_i = h(ID_i||\gamma_i)$, $RPW_i^* = h(PW_i^{old}||\gamma_i)$, $K_i = h(ID_i||PW_i^{old}||\gamma_i)$, and retrieves $\{A_2\}$ in mobile device. After that, SC computes $A_1 = D_{K_i}(A_2)$, $a_i = A_3 \oplus h(RID_i||RPW_i^*)$, $X_{GU} = A_1 \oplus h(a_i||RPW_i^*)$, and $A_4^* = h(RID_i||RPW_i^*||a_i)$, and checks whether $A_4^* \stackrel{?}{=} A_4$. If it is not valid, SC cancele the current session, otherwise SC requests a new password PW_i^{new} and a new biometric BIO^{new} to U_i.

PBUP-3: Then, U_i inputs a new password PW_i^{new} and a new biometric BIO^{new} in SC.

PBUP-4: After that, SC computes $\gamma_i^{new} = Rep(BIO^{new}, \beta_i^{new})$, $RPW_i^{new} = h(PW_i^{new}||\gamma_i^{new})$, $K_i^{new} = h(ID_i||PW_i^{new}||\gamma_i^{new})$, $A_2^{new} = E_{K_i^{new}}(A_1)$, $A_3^{new} = a_i \oplus h(RID_i^{new}||RPW_i^{new})$, and $A_4^{new} = h(RID_i^{new}|| RPW_i^{new}||a_i)$. Finally, SC replaces $\{A_2^{new}, A_3^{new}, A_4^{new}\}$ with $\{A_2, A_3, A_4\}$ in the memory.

VII. SECURITY ANALYSIS

We assess the security of the proposed AKA scheme by utilizing informal security and formal security analyzes, including ROR model and AVISPA.

A. INFORMAL SECURITY ANALYSIS

The security of the our scheme is proved by performing the informal security analysis. We demonstrate that our scheme

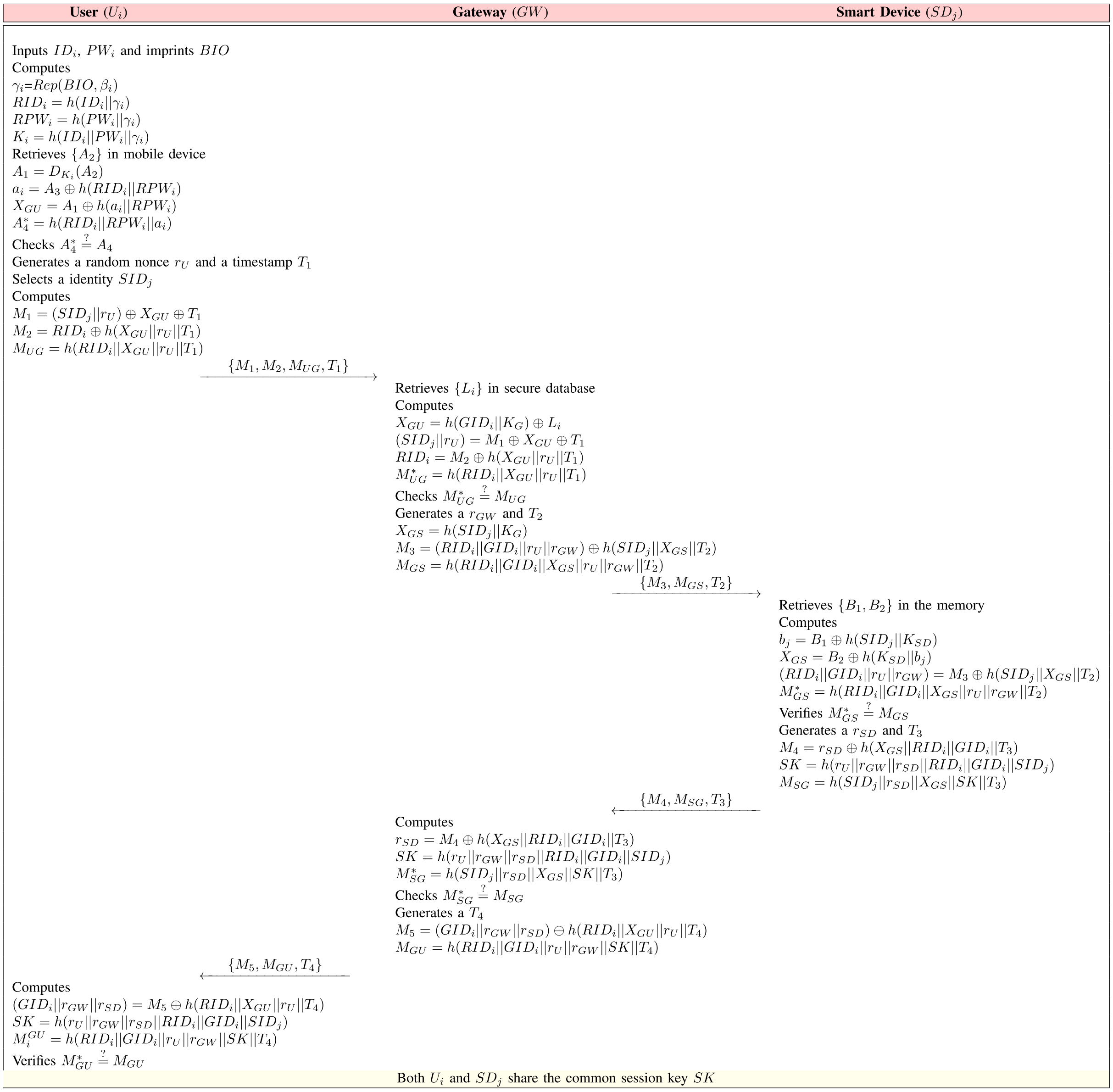

FIGURE 2. **Authentication and key agreement phase of our scheme.**

can withstand various security attacks, and also ensure user anonymity and mutual authentication.

1) IMPERSONATION ATTACK

When MA wants to masquerade a legal U_i, MA must calculate the authentication request messages $\{M_1, M_2, M_{UG}, T_1\}$ and response messages $\{M_5, M_{GU}, T_4\}$. However, it is difficult to generate the authentication request and response messages because MA does not know a secret key X_{GU}, a random nonce r_U, and a pseudo-identity RID_i. Therefore, our protocol prevents impersonation attacks since MA cannot generate the authentication request message and response of the legal user successfully.

2) SESSION KEY DISCLOSURE ATTACK

Referring to Section III-A, we assume that MA can steal the smart card and extract all secret credentials $\{A_2, A_3, A_4\}$ in the memory. In the proposed AKA scheme, MA should obtain the random nonces $\{r_U, r_{GW}, r_{SD}\}$ to generate session key $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$ successfully. However, MA cannot calculate a SK because X_{GU} and X_{GS} are masked with GW's master key K_G and random numbers $\{a_i, b_j\}$ by using hash function. Moreover, the random nonces $\{r_U, r_{GW}, r_{SD}\}$ cannot be obtained since MA does not know the secret keys $\{X_{GU}, X_{GS}\}$, Hence, the proposed AKA scheme is resilient against session key disclosure attacks.

3) SMART DEVICE CAPTURE ATTACK

Assuming that the smart device is physically captured by MA, MA can extract all secret parameters $\{B_1, B_2\}$ in the memory, where $B_1 = h(SID_j||K_{SD}) \oplus b_j$ and $B_2 = h(K_{SD}||b_j) \oplus X_{GS}$. However, MA cannot calculate X_{GS} without knowing the SD's master key K_{SD}, identity SID_j, and random number b_j. And also, MA cannot calculate a session key SK since MA does not know a SD_j's secret key X_{GS}, a GW's master key K_G, and a SD_j's real identity SID_j. Thus, the proposed AKA scheme is secure against smart device capture attacks.

4) REPLAY ATTACK

Suppose that MA intercepts all exchanged messages $\{M_1, M_2, M_{UG}, T_1\}$, $\{M_3, M_{GS}, T_2\}$, $\{M_4, M_{SG}, T_3\}$, and $\{M_5, M_{GU}, T_4\}$ in authentication phase. If MA resends all exchanged messages in the previous session, our scheme checks the validation of the current timestamp. Moreover, all messages are protected with the random nonces $\{r_U, r_{GW}, r_{SD}\}$ and secret keys $\{X_{GU}, X_{GS}\}$. Hence, the proposed AKA scheme is resilient against replay attacks.

5) MAN-IN-THE-MIDDLE (MITM) ATTACK

Assuming that MA eavesdrops all transmitted messages $\{M_1, M_2, M_{UG}, T_1\}$, $\{M_3, M_{GS}, T_2\}$, $\{M_4, M_{SG}, T_3\}$, and $\{M_5, M_{GU}, T_4\}$, then MITM attacks may be possible. However, MA cannot generate the authentication request and response messages since all messages are masked with the secret keys $\{X_{GU}, X_{GS}\}$, random nonces $\{r_U, r_{GW}, r_{SD}\}$, and identities $\{RID_i, SID_j, GID_i\}$ using hash function. Therefore, the proposed AKA scheme is secure against MITM attacks.

6) OFFLINE PASSWORD GUESSING ATTACK

Suppose that smart card is stolen or lost, MA can extract the sensitive information $\{A_2, A_3, A_4\}$ stored in the memory, where $A_2 = E_{K_i}(A_1)$, $A_3 = a_i \oplus h(RID_i||RPW_i)$, and $A_4 = h(RID_i||RPW_i||a_i)$. Consequently, MA is computationally infeasible to derive the real password of the legitimate user from $\{A_2, A_3, A_4\}$ without the knowledge of γ_i and RPW_i.

7) PERFECT FORWARD SECRECY

The security for perfect forward secrecy means that the past session key SK will not be disclosed even if the long-term secret key of communication entities is revealed. However, if GW's master key K_G and SD_j's secret key K_{SD} are compromised, MA cannot compute the session key $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$ without knowledge of SID_j, b_j, X_{GU}, and X_{GS}. Thus, our protocol is resilient to perfect forward secrecy.

8) ANONYMITY AND UNTRACEABILITY

Assuming that MA intercepts all transmitted messages during AKA phase. MA is impossible to compute the U_i's identity ID_i, pseudo-identity RID_i, the SD_j's identity SID_j and pseudo-identity PID_j without knowing secret credentials $\{X_{GU}, X_{GS}\}$. Hence, the proposed scheme provides anonymity for U_i and SD_j. Moreover, the timestamps and random nonces are different in any session, that is the transmitted messages in each session are unique and dynamic, so MA cannot trace U_i and SD_j from different sessions. Therefore, the proposed AKA scheme achieves untraceability for U_i and SD_j.

TABLE 2. Queries and descriptions.

Queries	Descriptions
$Execute(\mathcal{P}_U^{t_1}, \mathcal{P}_{GW}^{t_2}, \mathcal{P}_{SD}^{t_3})$	Based on $Execute$ query, MA performs the active/passive attacks by eavesdropping all messages between each participants via a public channel.
$CorruptSC(\mathcal{P}_U^{t_1})$	This query is modeled as the smart card stolen attacks, where MA is able to extract the secret parameters stored in SC.
$Send(\mathcal{P}^t, Msg)$	Based on $Send$ query, MA is able to send the message Msg to the P^t, and also receive the response message accordingly.
$Test(\mathcal{P}^t)$	In this query, an unbiased coin c is tossed prior to starting of the games. If MA obtains the condition $c = 1$ using $Test()$ query, it denotes a SK between $P_U^{t_1}$ and $P_{SD}^{t_2}$ is fresh. If MA gets the condition $c = 0$, it denotes a SK is not fresh, otherwise MA gets a null value ($\perp$).
$Reveal(\mathcal{P}^t)$	Based on $Reveal$ query, MA reveals a SK established between $P_U^{t_1}$ and $P_{SD}^{t_2}$.

9) MUTUAL AUTHENTICATION

In our scheme, all parties perform mutual authentication successfully, After obtaining the message $\{M_1, M_2, M_{UG}, T_1\}$, GW checks $M_{UG}^* \stackrel{?}{=} M_{UG}$. If it is valid, GW authenticates U_i. Upon getting the message $\{M_3, M_{GS}, T_2\}$ from GW, the SD_j verifies $M_{GS}^* \stackrel{?}{=} M_{GS}$. If the condition is equal, SD_j authenticates GW. After getting the message $\{M_4, M_{SG}, T_3\}$, GW checks $M_{SG}^* \stackrel{?}{=} M_{SG}$. If it is correct, GW authenticate SD_j. Upon obtaining the message $\{M_5, M_{GU}, T_4\}$ from GW, the U_i verifies $M_{GU}^* \stackrel{?}{=} M_{GU}$. If the condition is valid, U_i authenticates GW. Consequently, all parties in our scheme are mutually authenticated since MA cannot generate the transmitted authentication messages $\{M_{UG}, M_{GS}, M_{SG}, M_{GU}\}$ successfully.

B. FORMAL SECURITY ANALYSIS

The security of the proposed AKA scheme is proved by using formal security analysis such as ROR model and AVISPA simulation.

1) ROR MODEL

This section evaluates a SK security of the proposed AKA protocol from MA by performing ROR model [14]. We first briefly introduce the ROR model prior to demonstrate SK security for our protocol.

In our scheme, there are three participants: the user $P_U^{t_1}$, gateway $P_{GW}^{t_2}$, and smart device $P_{SD}^{t_3}$, where $P_U^{t_1}$, $P_{GW}^{t_2}$, and $P_{SD}^{t_3}$ are instances t_1^{th} of U_i, t_2^{th} of GW_j, and t_3^{th} of SD_j, respectively. In Table 2, we introduce overviews of each query such as $Execute()$, $CorruptSC()$, $Send()$, $Reveal()$, and $Test()$ to perform ROR model. In addition, we use an one-way hash function $Hash$ as the random oracle and also utilize Zipf's law [39] to prove SK security.

Theorem. Adv_{MA}^{AKA} denotes the advantages of MA in violating SK security for our protocol. Then, we have the following inequality.

$$Adv_{MA}^{AKA} \leq \frac{q_h^2}{|Hash|} + 2\{C \cdot q_{send}^s, \frac{q_s}{2^{l_b}}\}$$

Hash, q_h, and q_{send} are the number of *Hash* queries, the range space of the hash function $h(\cdot)$, and *Send*() query respectively. Furthermore, C, s, and l_b are the Zipf's parameters [39].

Proof. We describe a sequence of four games denoted by GM_i $(i = 0, 1, 2, 3)$ played by MA. We indicate that Adv^{AKA}_{MA,GM_i} is the probability of MA winning the GM_i. All games are described as belows:

Game GM_0: This game represents the real security attacks executed by MA against the proposed AKA scheme. MA must guess a bit c correctly to win the game. We obtain the following result:

$$Adv^{AKA}_{MA} = |2 \cdot Adv^{AKA}_{MA,GM_0} - 1| \quad (1)$$

- **Game** GM_1: This game is modeled that MA simulates eavesdropping attacks in which exchanged messages are intercepted during AKA process performing *Execute*(). After getting exchanged messages, MA performs *Reveal*() and *Test*() queries to check whether it is a SK or a random number. MA needs secret credentials such as K_G, X_{GU}, and X_{GS} to derive $SK = h(r_U||r_{GW}||r_{SD}||RID_i||GID_i||SID_j)$. Hence, MA does not at all help in increasing the winning probability of this game by intercepting on the exchanged messages. Based on this game, the following is obtained:

$$Adv^{AKA}_{MA,GM_1} = Adv^{AKA}_{MA,GM_0} \quad (2)$$

- **Game** GM_2: This GM_2 is considered as the active/passive attacks, where simulations of *Send*() and *Hash*() queries are included. In GM_2, the MA is able to intercept all transmitted messages $\{M_1, M_2, M_{UG}, T_1\}$, $\{M_3, M_{GS}, T_2\}$, $\{M_4, M_{SG}, T_3\}$, and $\{M_5, M_{GU}, T_4\}$ during AKA process. However, all exchanged messages are safeguarded utilizing the hash function $h(\cdot)$. Furthermore, the random nonces r_U, r_{GW}, and r_{SD} are not revealed from the exchanged messages since the random nonces are also protected by hash function $h(\cdot)$. By applying the birthday paradox, we obtain the following result:

$$|Adv^{AKA}_{MA,GM_2} - Adv^{AKA}_{MA,GM_1}| \leq \frac{q_h^2}{2|Hash|} \quad (3)$$

- **Game** GM_3: This game is modeled by using *CorruptSC*(). In GM_3, the MA is able to extract the secret credentials $\{A_2, A_3, A_4\}$ in the SC memory using power-analysis attacks. Generally, the legitimate user uses the low-entropy password. Using stored secret credentials $\{A_2, A_3, A_4\}$ of the SC, MA may attempt to extract the password PW_i by performing offline password guessing attack. However, in our scheme, MA cannot obtain the PW_i of the legitimate user correctly via *Send*() query without the biometric information γ_i and secret credential RPW_i. Moreover, the probability of guessing the l_b bits of the biometric secret key b_i is approximately $\frac{1}{2^{l_b}}$. Hence, GM_2 and GM_3 are indistinguishable if the offline password/biometric guessing attacks are not present. Based on this game, the following is obtained:

$$|Adv^{AKA}_{MA,GM_3} - Adv^{AKA}_{MA,GM_2}| \leq \{C \cdot q^s_{send}, \frac{q_s}{2^{l_b}}\} \quad (4)$$

After GM_{0-3} are played successfully, MA tries to guess the correct bit c to win the game by using *Test*(). Therefore, we obtain the following result:

$$Adv^{AKA}_{MA,GM_3} = \frac{1}{2} \quad (5)$$

By applying Eq. (1), (2) and (5), we get the following result:

$$\begin{aligned}\frac{1}{2}Adv^{AKA}_{MA} &= |Adv^{AKA}_{MA,GM_0} - \frac{1}{2}| \\ &= |Adv^{AKA}_{MA,GM_1} - \frac{1}{2}| \\ &= |Adv^{AKA}_{MA,GM_1} - Adv^{AKA}_{MA,GM_3}| \quad (6)\end{aligned}$$

By applying Eq. (4), (5) and (6), we obtain the following result using the triangular inequality:

$$\begin{aligned}\frac{1}{2}Adv^{AKP}_{MA} &= |Adv^{AKP}_{MA,GM_1} - Adv^{AKP}_{MA,GM_3}| \\ &\leq |Adv^{AKP}_{MA,GM_1} - Adv^{AKP}_{MA,GM_2}| \\ &\quad +|Adv^{AKP}_{MA,GM_2} - Adv^{AKP}_{MA,GM_3}| \\ &\leq \frac{q_h^2}{2|Hash|} + \{C \cdot q^s_{send}, \frac{q_s}{2^{l_b}}\}. \quad (7)\end{aligned}$$

Multiplying both sides of Eq. (7) by the factor of two, the following result is obtained:

$$Adv^{AKA}_{MA} \leq \frac{q_h^2}{|Hash|} + 2\{C \cdot q^s_{send}, \frac{q_s}{2^{l_b}}\}$$

2) AVISPA SIMULATION

In the past few years, numerous studies using AVISPA simulation have been proposed [40]–[42]. AVISPA simulation is a role-based security validation tool that demonstrates whether the authentication protocol is secure against potential security attacks based on DY model [29]. This simulation mechanism is implemented using High-Level Protocol Specification Language (HLPSL) [43] to generate input format (IF) of the back-ends, including Constraint Logic-based Attack Searcher (CL-AtSE), SAT-based Model Checker (SATMC), Tree Automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP), and On-the-Fly Model Checker (OFMC). IF is provided as the input to one of the four back-ends, which produces the output format (OF). In addition, OF indicates the security of the proposed AKA scheme.

To analyze the security of the AKA scheme, we express based on a rule-oriented HLPSL. The detailed HLPSL specifications for AVISPA can be found in [12], [13]. The specification roles for the user U_i, the gateway GW, and the smart device SD, and the mandatory roles for the environments, sessions, and security goals are implemented in HLPSL. Because XOR operations are not supported for

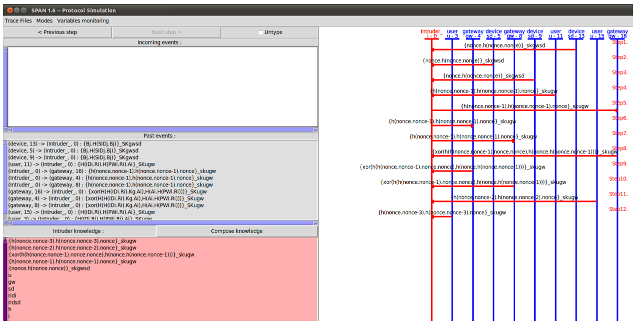

FIGURE 3. AVISPA results using SPAN.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL

  /home/span/span/testsuite/results/AVISPA_sjyu.if

GOAL
  As_Specified

BACKEND
  OFMC

COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.30s
  visitedNodes: 1040 nodes
  depth: 9 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  /home/span/span/testsuite/results/AVISPA_sjyu.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 63 states
  Reachable  : 63 states
  Translation: 0.03 seconds
  Computation : 0.01 seconds
```

FIGURE 4. AVISPA results using OFMC and CL-AtSe.

TA4SP and SATMC back-ends, AVISPA simulation results for two back-ends are not included. We simulate the proposed AKA scheme using the Security Protocol ANimator (SPAN) as shown in Figure 3. In addition, we demonstrate that our scheme resists replay and MITM attacks using OFMC and CL-AtSe back-ends as shown in Figure 4.

VIII. PERFORMANCE ANALYSIS

This section analyzes the comparative analysis of our scheme with the related schemes [10], [11], [27] in terms of the computation, communication, and storage costs, and security features.

A. COMPUTATION COSTS

We evaluate the computation costs of the proposed AKA with related schemes [10], [11], [27] in terms of MU_i, GW, and SD_j during AKA process. According to [11], [44], the execution times of each operation are acquired based on a desktop with a Windows 8 Intel(R) Core TM I7-4710HQ 2.50 GHZ, 8 GB Memory. Moreover, the software development environment was implemented using Visual C++ 2010, MIRACL C/C++ Library. We denote the execution times of the following parameters based on [44]. T_{ed}, T_{ecc}, and T_h denote the execution times for symmetric encryption/decryption ($\approx$ 0.0215 ms), ECC point multiplication ($\approx$ 0.4276 ms), and hash function ($\approx$ 0.0052 ms), respectively. Moreover, It is also assumed that the execution time for fuzzy extractor T_{fe} is equal to T_{ecc} presented in [11]. In Table 3, we show the comparison results of the computation overhead and execution times between the proposed AKA scheme and those of related schemes. Consequently, our protocol has the lowest computation overhead of those compared with the previous schemes [10], [11], [27].

B. COMMUNICATION COSTS

We analyze the communication costs of the proposed AKA with previous schemes [10], [11], [27] during AKA process. We assume the communication costs of the following parameters based on Shuai *et al.*'s scheme [10]. The length of timestamp, random nonce, secret key, hash function, message authentication code, identity, pseudo-identity, symmetric encryption/decryption, and ECC point multiplication are as 32 bits, 160 bits, 160 bits, 160 bits, 160 bits, 128 bits, 128 bits, 256 bits, and 320 bits, respectively. In Table 4, we show the comparison results of the communication cost between the proposed scheme and previous schemes. Consequently, the proposed AKA scheme provides a superior communication cost compared with the related schemes [10], [11], [27].

C. STORAGE COSTS

We compare the storage costs for the basis of bytes stored in smart card of the proposed AKA and related schemes [10], [11], [27]. We assume the storage costs of the following parameters. We assume that the bits for the length of the secret parameters presented in Section VIII-B are equal to the storage costs. Table 5 presents the comparison results of the storage cost between the proposed scheme and previous schemes. Although the storage cost of the proposed AKA is somewhat higher than Kaur and Kumar [11], it ensures

TABLE 3. A comparative summary: computation costs.

Schemes	User	Gateway (GW)	Smart device (SD)	Total costs	Execution times
Shuai *et al.* [10]	$6T_h + 2T_{ecc}$	$7T_h + T_{ecc}$	$3T_h$	$16T_h + 3T_{ecc}$	1.366 ms
Wazid *et al.* [27]	$11T_h + T_{ed} + T_{fe}$	$11T_h + 2T_{ed}$	$7T_h + T_{ed}$	$29T_h + 4T_{ed} + T_{fe}$	0.6644 ms
Kaur and Kumar [11]	$6T_h + 2T_{ecc}$	$7T_h + T_{ecc}$	$3T_h$	$16T_h + 3T_{ecc}$	1.366 ms
Our scheme	$11T_h + T_{fe} + T_{ed}$	$11T_h$	$7T_h$	$29T_h + T_{fe} + T_{ed}$	0.5999 ms

TABLE 4. A comparative summary: communication costs.

Nodes	Shuai *et al.* [10]	Wazid *et al.* [27]	Kaur and Kumar [11]	Our scheme
User to GW	768 bits	480 bits	800 bits	512 bits
GW to SD	320 bits	448 bits	352 bits	352 bits
SD to GW	320 bits	512 bits	352 bits	352 bits
GW to user	320 bits	828 bits	352 bits	352 bits
Total costs	1728 bits	2268 bits	1856 bits	1568 bits

TABLE 5. A comparative summary: storage costs.

Schemes	Storage costs
Shuai *et al.* [10]	512 bits
Wazid *et al.* [27]	640 bits
Kaur and Kumar [11]	384 bits
Our scheme	480 bits

TABLE 6. A comparative summary: security features.

Feature	Shuai *et al.* [10]	Wazid *et al.* [27]	Kaur and Kumar [11]	Our scheme
SFT_1	×	×	○	○
SFT_2	×	○	○	○
SFT_3	×	○	○	○
SFT_4	○	○	×	○
SFT_5	×	○	○	○
SFT_6	×	○	×	○
SFT_7	×	○	○	○
SFT_8	○	○	×	○
SFT_9	×	○	○	○
SFT_{10}	○	○	○	○
SFT_{11}	○	○	○	○

○: Resistance of security features; ×: Non-resistance of security features; SFT_1: Replay attack; SFT_2: Offline password guessing attack; SFT_3: Gateway bypass attack; SFT_4: User impersonation attack; SFT_5: User device stolen attack; SFT_6: Session key disclosure attack; SFT_7: Insider attack; SFT_8: Mutual authentication; SFT_9: User anonymity; SFT_{10}: User untraceability; SFT_{11}: Perfect forward secrecy.

superior security, computation cost, and communication cost than other related schemes [10], [27].

D. SECURITY FEATURES

This section evaluates the security features of the proposed AKA scheme compared to previous schemes [10], [11], [27]. Table 6 shows that previous schemes suffer from various security attacks, including offline password guessing, replay, and impersonation attacks, and so on, and also does not provide mutual authentication and user anonymity. In contrast, the proposed AKA scheme resists various security attacks, and also provides forward secrecy, mutual authentication, and user anonymity. Hence, the proposed AKA scheme offers more security and functionality features compared with previous schemes [10], [11], [27].

IX. CONCLUSION

We proved that Kaur and Kumar *et al.*'s scheme is insecure to various security attacks such as impersonation and session key disclosure attacks, and also does not ensure mutual authentication. We design a lightweight three-factor based privacy-preserving authentication scheme for IoT-enabled smart homes to overcome the security flaws of Kaur and Kumar *et al.*'s scheme. We demonstrated that the proposed AKA scheme resists various security threats, and also allows user anonymity, untraceability, and mutual authentication. We then proved using well-known accepted AVISPA simulation and ROR model that the proposed AKA scheme is secure against various security attacks. Moreover, we compared the computation, communication, and storage costs of the proposed AKA scheme with other related schemes. Thus, the proposed AKA scheme improved security and privacy, and also ensured the low computation, communication, and storage costs compared with the other related schemes using only fuzzy extractor, hash, and XOR functions, which generate low computation and communication costs. Our scheme is suitable for IoT-enabled smart home environments because it is more secure and lightweight than existing schemes.

REFERENCES

[1] K. Han, T. Shon, and K. Kim, "Efficient mobile sensor authentication in smart home and WPAN," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 591–596, May 2010.
[2] T. D. Mendes, R. Godina, E. M. Rodrigues, J. C. Matias, and J. P. Catalão, "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," *Energies*, vol. 8, no. 7, pp. 7279–7311, 2015.
[3] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors J.*, vol. 16, no. 1, pp. 254–264, Jan. 2016.
[4] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technol. Soc. Mag.*, vol. 37, no. 2, pp. 71–79, Jun. 2018.
[5] P. Gope, H. SK Islam, M. S. Obaidat, R. Amin, and P. Vijayakumar, "Anonymous and expeditious mobile user authentication scheme for GLOMONET environments," *Int. J. Commun. Syst.*, vol. 31, no. 2, pp. 1–18, 2017.
[6] R. Amin, S. K. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018.
[7] V. K. Yadav, A. Anand, S. Verma, and S. Venkatesan, "Private computation of the Schulze voting method over the cloud," *Cluster Comput.*, vol. 23, no. 4, pp. 2517–2531, Dec. 2020.
[8] N. Andola, Raghav, V. K. Yadav, S. Venkatesan, and S. Verma, "SpyChain: A lightweight blockchain for authentication and anonymous authorization in IoD," *Wireless Pers. Commun.*, vol. 119, no. 1, pp. 343–362, Jul. 2021.
[9] V. K. Yadav, S. Verma, and S. Venkatesan, "Linkable privacy-preserving scheme for location-based services," *IEEE Trans. Intell. Transp. Syst.*, early access, May 5, 2021, doi: 10.1109/TITS.2021.3074974.
[10] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Comput. Secur.*, vol. 86, pp. 132–146, Sep. 2019.
[11] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *J. Inf. Secur. Appl.*, vol. 58, pp. 102787–102798, 2021.
[12] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Feb. 16, 2021. [Online]. Available: http://www.avispa-project.org/
[13] *SPAN: A Security Protocol Animator for AVISPA*. Accessed: Feb. 16, 2021. [Online]. Available: http://www.avispa-project.org/
[14] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography*. Les Diablerets, Switzerland: Springer, 2005, pp. 65–84.
[15] S. Kumari, A. K. Das, M. Wazid, X. Li, F. Wu, K. K. R. Choo, and M. K. Khan, "On the design of a secure user authentication and key agreement scheme for wireless sensor networks," *Concurrency Comput. Pract. Exper.*, vol. 29, no. 23, pp. 1–24, 2017.
[16] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "eDAAAS: Efficient distributed anonymous authentication and access in smart homes," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 12, pp. 1–11, 2016.
[17] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.
[18] M. Bilal and S. G. Kang, "An authentication protocol for future sensor networks," *Sensors*, vol. 17, no. 5, p. 979, 2017.
[19] J. Jeong, M. Y. Chung, and H. Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Waikoloa, HI, USA, Jan. 2008, pp. 294–301.
[20] B. Vaidya, S.-S. Yeo, J. J. P. C. Rodrigues, and J. H. Park, "Robust one-time password authentication scheme using smart card for home network environment," *IEEE Comput. Commun.*, vol. 34, no. 3, pp. 326–336, Mar. 2011.
[21] H. J. Kim and H. S. Kim, "AUTH_HOTP-HOTP based authentication scheme over home network environment," in *Proc. Int. Conf. Comput. Sci. Appl.*, 2011, pp. 622–637.

[22] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Proc. 5th Int. Conf. Comput. Intell., Commun. Syst. Netw.*, Madrid, Spain, Jun. 2013, pp. 1–6.
[23] J. Shen, C. Wang, X. Chen, X. Huang, Z.-H. Zhan, and T. Li, "Secure data uploading scheme for a smart home system," *Inf. Sci.*, vol. 453, pp. 186–197, Jul. 2018.
[24] U. Satapathy, B. K. Mohanta, D. Jena, and S. Sobhanayak, "An ECC based lightweight authentication protocol for mobile phone in smart home," in *Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS)*, Rupnagar, India, Dec. 2018, pp. 1–6.
[25] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2011, pp. 787–788.
[26] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *Proc. Int. Symp. Consum. Electron.*, 2015, pp. 1–2.
[27] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Dec. 2020.
[28] 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.
[29] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[30] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Int. Conf. Adv. Cryptol.*, Berlin, Germany, 1999, pp. 388–397.
[31] 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.
[32] S. J. Yu, K. S. Park, and Y. H. Park, "A secure lightweight three-factor authentication scheme for IoT in cloud computing environment," *Sensors*, vol. 19, no. 16, pp. 3598–3618, 2019.
[33] K. Park, S. Noh, H. Lee, A. K. Das, M. Kim, Y. Park, and M. Wazid, "LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical Internet of Things," *IEEE Access*, vol. 8, pp. 119387–119404, 2020.
[34] S. J. Yu, K. S. Park, J. Y. Lee, Y. H. Park, Y. H. Park, S. W. Lee, and B. H. Chung, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, pp. 1758–1784, 2020.
[35] S. J. Yu and Y. H. Park, "SLUA-WSN: Secure and lightweight three-factor-based user authentication protocol for wireless sensor networks," *sensors*, vol. 20, no. 15, pp. 4143–4169, 2020.
[36] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.
[37] P. Soni, A. K. Pal, and H. SK Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.
[38] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Tech.*, Interlaken, Switzerland, 2004, pp. 523–540.
[39] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[40] S. J. Yu, J. Y. Lee, K. K. Lee, K. S. Park, and Y. H. Park, "Secure authentication protocol for wireless sensor networks in vehicular communications," *Sensors*, vol. 18, no. 10, pp. 3191–3214, 2017.
[41] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.
[42] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046–107062, 2020.
[43] D. V. Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, Tallinn, Finland, 2005, pp. 1–17.
[44] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyan, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, 2016.

SUNGJIN YU received the B.S. degree in electronics engineering from Daegu University and the M.S. degree in electronics engineering from Kyungpook National University, Daegu, South Korea, in 2017, and 2019, respectively, where he is currently pursuing the Ph.D. degree with 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, the Internet of Vehicles, and the Internet of Drones.

NAMSU JHO received the B.S. degree in mathematics from Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 1999, and the Ph.D. degree in mathematics from Seoul National University, South Korea, in 2007. Since 2007, he has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, as a Principal Researcher. His research interests include cryptography and information theory.

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, Corvallis, OR, 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.