mathematics

MDPI

Article

Toward a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach

Tsu-Yang Wu [1], Qian Meng [1], Yeh-Cheng Chen [2], Saru Kumari [3] and Chien-Ming Chen [1,*]

[1] College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China; wutsuyang@gmail.com (T.-Y.W.); mq15753683129@163.com (Q.M.)
[2] Department of Computer Science, University of California, Davis, CA 001313, USA
[3] Department of Mathematics, Chaudhary Charan Singh University, Meerut 250004, India
* Correspondence: chienmingchen@ieee.org

Abstract: The extensive application of the Internet of Things (IoT) and artificial intelligence technology has greatly promoted the construction and development of smart cities. Smart home as the foundation of smart cities can optimize home lifestyles. However, users access the smart home system through public channels, and the transmitted information is vulnerable to attack by attackers, and the privacy and data security of the home user will be difficult to be guaranteed. Therefore, how to protect users' data and privacy security becomes critical. In this paper, we design a provably secure authentication scheme for the smart home environment, which ensures that only legitimate users can use smart devices. We use the informal model to verify the security of the scheme and formally analyze the security and correctness of the scheme through the Real or Random model. Finally, through the comparison of security and performance analysis, it is proven that our scheme has higher security under similar performance.

Keywords: IoT; smart city; smart home; authentication scheme

MSC: 68M25

Citation: Wu, T.-Y.; Meng, Q.; Chen, Y.-C.; Kumari, S.; Chen, C.-M. Toward a Secure Smart-Home IoT Access Control Scheme Based on Home Registration Approach. *Mathematics* **2023**, *11*, 2123. https://doi.org/10.3390/math11092123

Academic Editor: Antanas Cenys

Received: 27 March 2023
Revised: 22 April 2023
Accepted: 26 April 2023
Published: 30 April 2023

1. Introduction

The Internet of things (IoT) [1,2], cloud computing [3,4], big data [5,6], artificial intelligence [7,8], 5G and other technologies have promoted the construction and development of smart city. Smart city [9] covers all fields of life, such as smart transportation [10,11], smart healthcare [12], smart home, smart grid, etc., which are an indispensable part of smart city. As the foundation of smart city, smart home [13,14] is also the field closest to people's daily life. It can provide an information exchange function for families. People can operate and monitor smart home devices through the Internet and know what happens at home any time, improving people's comfort in life and optimizing people's lifestyles. The smart home environment includes various smart devices, such as refrigerators, cameras, curtains, etc. People can control smart devices through smartphones or tablets to enjoy their services. For example, users can view the camera remotely to understand what is happening at home; the users can control the temperature of the air conditioner through the smart phone.

A typical smart home architecture shown in Figure 1 consists of four entities: registration authority (RA), gateway, smart device, and users. RA is a trusted entity that mainly authorizes the gateway as the home registration center. Gateway is a semi-trusted entity that helps users to communicate with smart home devices and is responsible for registration. Smart device refers to all kinds of smart home appliances in the family, such as smart refrigerators, smart air conditioners, etc., where they are semi-trusted entities, and are connected to the gateway by wireless networks to provide users with various services. Only family members can register with the gateway to become legal users. In this

architecture, users need to connect the home devices via the gateway, and then operate the home devices through the smart home APP or voice assistant, such as adjusting the indoor temperature, switching lights, adjusting curtains, playing music, etc. Although the smart home has changed people's lives, it faces many security threats and challenges. For example, since smart home devices are connected to the Internet, malicious attackers can access users' private information by intercepting transmitted messages via open channels. Therefore, ensuring a secure smart-home IoT access control scheme is very important.

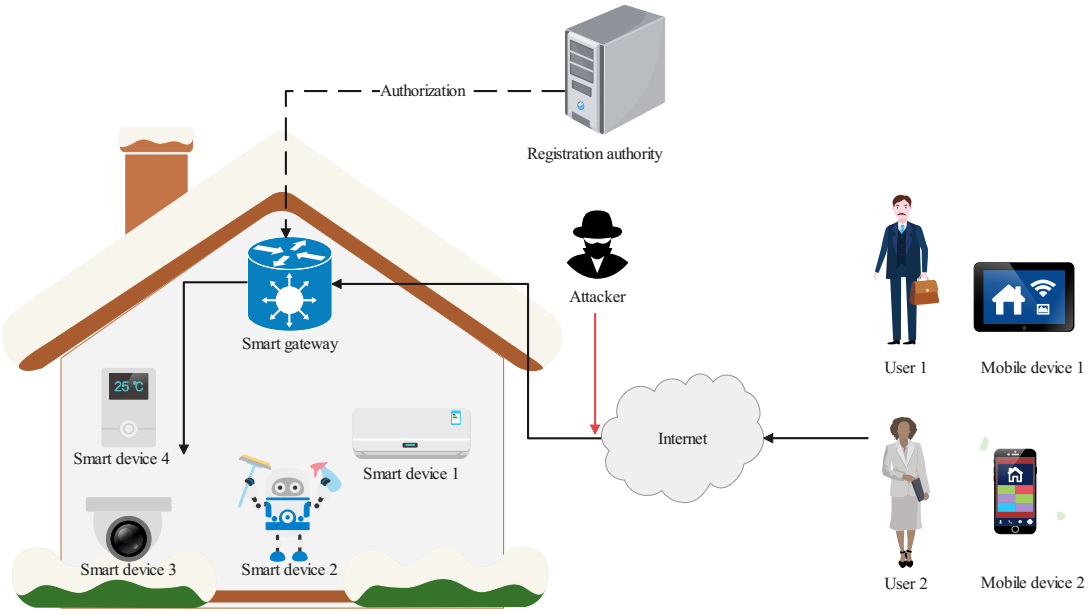

Figure 1. The architecture of smart home.

At present, some scholars protect users' privacy through differential privacy [15], quick response (QR) code [16] and other technologies, and many scholars have proposed many authentication and key agreement (AKA) schemes [13,17–24] to protect the confidentiality and security of transmitted information, but most of their schemes have various security problems, such as unable to achieve mutual authentication, unable to resist offline password guessing (OPG) attacks, insider attacks, impersonation attacks, etc. In order to protect and improve the security of information, Intel has proposed a new set of CPU instruction extensions called software guard extensions (SGX) [25,26] technology. It is a kind of hardware that can create a trusted execution environment (TEE) to protect code and data, which even high-level system software cannot access. The system will allocate a pre-reserved physical memory area for SGX technology, which is called enclave page cache (EPC), and the code and data are stored in a secure environment, called enclave. The application protected by SGX is divided into two parts: trusted part and untrusted part. The trusted part will run in the safe memory and conduct integrity measurement when loaded into Enclave to ensure the integrity and security of data. The program access address is in the Enclave and the physical address is in the EPC. Because the two achieve access control through a unique mapping relationship, it can ensure that external programs cannot access the enclave memory. SGX provides automatic generation functions Ecall and Ocall. Some privacy data is stored in Enclave memory through Ecall function. After confidential calculation is completed in Enclave, the calculated results are returned through Ocall function.

To ensure the secure transmission of remote control data, we propose a scheme based on SGX, which can help our scheme effectively resist insider attacks. Our main contributions are as below:

(1) We propose a new framework that features the ability to be registered within a family. Different from the past, we authorize the smart gateway as a home registration

center by the registration authority (RA), so that users and smart devices can complete registration at home, which also facilitates the addition of future members and devices. This process can be completed only at home.

(2) According to our survey, this is the first paper to apply SGX to smart home environments. Using SGX can be effective to prevent insider attacks.

(3) We demonstrate the security of the proposed scheme using Real-Or-Random (RoR) model and informal security analysis. Furthermore, we compare the proposed scheme with other existing schemes, and the results reveal that our scheme offers higher security with similar performance.

The remainder of the paper is arranged as follows. Section 2 is related work, Section 3 is the proposed scheme, the security analysis is in Section 4, and Section 5 is the performance comparison. Our conclusion is in Section 6.

2. Related Work

Numerous authentication and key agreement (AKA) schemes have been put forward to ensure the secure transmission of information in smart home systems. Some authentication schemes are listed in Table 1. Jeong et al. [27] devised an authentication scheme based on home network environment. The author proved that their scheme is secure, but the user's identity is immediately transmitted on the public channel, which does not realize user anonymity, and is unable to withstand tracking attacks. Vaidya et al. [28] proposed a lightweight AKA scheme for secure remote access to the home network. However, Kim et al. [29] demonstrated that their scheme is unable to provide user anonymity, mutual authentication, and cannot resist OPG attacks. Later, Kim et al. [29] put forward an enhanced scheme based on Vaidya et al. [28]. Li et al. [30] put forward a lightweight AKA scheme for the home energy management system. The wireless node and the control center completed authentication and established session key, but the user and the control center lacked the authentication process. Han et al. [31] devised an authentication scheme to solve the problem of secure pairing of consumer electronic products in the smart home environment, but their scheme requires manufacturers to be online all the time is unrealistic. Santoso and Vun [32] devised a secure two-factor AKA scheme, which uses elliptic curve cryptography (ECC) technology and is suitable for the smart home environment based on the IoT. Kumar et al. [33] also proposed a lightweight scheme for this environment and realized the establishment of session key between gateway and smart device. However, other scholars have proved that anonymity and untraceability cannot be provided.

Ashibani and Mahmoud [34] designed an identity-based AKA scheme. The scheme uses ECC and pairing operations with high computational complexity, which can realize secure mutual authentication between users and smart devices. However, they ignore that smart devices have limited computing power. In order to solve the above problems, Wazid et al. [35] designed a lightweight remote user authentication scheme. The home gateway helps user and smart device complete authentication and establish session key, and proves that their scheme is secure. Unfortunately, Shuai et al. [13] discovered that Wazid et al.'s [35] scheme cannot withstand desynchronization attacks, and when the gateway is damaged, the user authentication table in the gateway is easy to be leaked. Users' privacy is very easy to disclose. Shuai et al. [13] devised an AKA scheme using ECC. However, Kuar et al. [19] have demonstrated that their scheme cannot resist OPG, insider, and session key disclosure (SKD) attacks. Kaur et al. [19] proposed a two factor authentication scheme, but Yu et al. [17] stated that it cannot withstand simulated attacks and provide mutual authentication. Chifor et al. [36] devised an authentication scheme that can provide fast online identity authentication and realize password free authentication between users and smart devices. Ghosh et al. [37] designed a secure multi-level authentication scheme, which can resist many common attacks. Dey and Hossian [38] designed an authentication scheme using the public key cryptosystem and asserted that their scheme was resistant to various common attacks. However, Gaba et al. [39] found that their scheme is unable to resist smart device stolen (SDS) attacks, and could not guarantee anonymity

and confidentiality. Then, Gaba et al. [39] designed an ECC-based authentication scheme to ensure the positioning security of household devices. Naoui et al. [40] designed an authentication framework based on the user's configuration file, request time, location and other context information. Poh et al. [41] proposed a scheme to protect data privacy. However, Irshad et al. [42] proved that their scheme could not achieve the confidentiality of user authentication parameters. They propose a new two-factor AKA scheme that ensures perfect froward secrecy (PFS) by using a circular fuzzy extractor. Banerjee et al. [43] designed a lightweight anonymous AKA scheme suitable for this environment. Unfortunately, AL-Turjman and Deebak [44] discovered that their scheme could not provide identity protection and traceability. Zou et al. [18] devised a more secure scheme. Yu et al. [17] devised a three factor AKA scheme, but Alzahrani et al. [45] found that Yu et al.'s scheme [17] cannot provide mutual authentication. Piraytesh et al. [21] proposed a hyperelliptic curve cryptosystem-based AKA scheme in smart home, which they claim ensures good performance. Guo et al. [22] designed an AKA scheme based on smart home, and introduced fog nodes into the scheme to process the data of smart devices faster.

At present, some scholars have applied SGX to other environments to design schemes. Sun et al. [25] used SGX to design schemes to better protect dynamic identity authentication. Liu et al. [26] devised an AKA scheme that applies SGX to wireless sensor networks (WSNs). The scheme also uses dynamic authentication certificate (DAC) to ensure more effective secure communication.

Table 1. The summary of authentication schemes.

Schemes	Advantages	Shortcomings
Shuai et al. [13]	(1) Provides mutual authentication (2) Can resist impersonation attacks	(1) Cannot resist insider attacks (2) Cannot resist SKD attacks (3) Cannot resist OPG attacks
Yu et al. [17]	(1) Can provide user anonymity (2) Can resist PFS attacks	(1) Cannot provide mutual authentication
Zou et al. [18]	(1) Can resist SDS attacks (2) Provides mutual authentication	–
Kaur et al. [19]	(1) Can resist OPG attacks (2) Provides user anonymity	(1) Cannot resist impersonation attacks (2) Cannot provide mutual authentication
Vaidya et al. [28]	(1) Can resist SKD attacks (2) Provides PFS	(1) Cannot provide user anonymity (2) Cannot provide mutual authentication (3) Cannot resist OPG attacks
Santoso and Vun [32]	(1) Provides user anonymity (2) Provides PFS	–
Wazid et al. [35]	(1) Can resist insider attacks (2) Provides PFS (3) Can resist OPG attacks	(1) Cannot resist desynchronization attacks
Banerjee et al. [43]	(1) Provides PFS (2) Can resist OPG attacks	(1) Cannot provide user anonymity and untraceability

3. The Proposed Scheme

In this section, we introduce the proposed scheme in detail, the network model of this scheme is shown in Figure 2. The proposed scheme includes three phases: authorization gateway, registration, and access and control. The notations used in the paper are listed in Abbreviations.

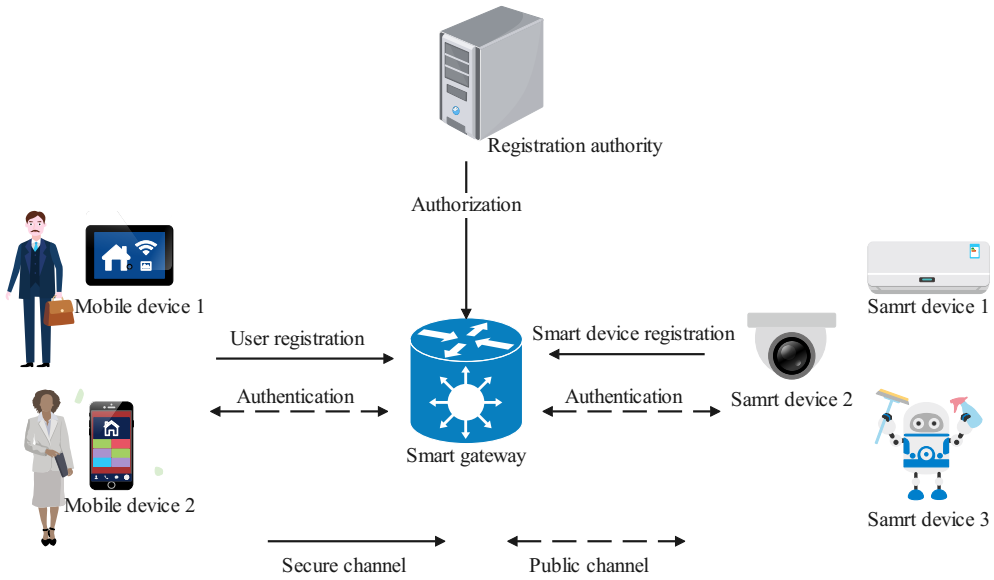

Figure 2. Network model of smart home.

3.1. Authorization Gateway Phase

RA selects ID_k, r_k, computes the temporary identity $PID_k = h(ID_k \parallel r_k)$ of GW, and transmits $\{ID_k, PID_k\}$ to GW; GW stores $\{PID_k\}$ in memory. Then, GW selects F_p, G, P, x. Then, GW computes $X = x \cdot P$, stores $\{(PID_k, ID_k, x)\}$ in SGX, and publish $\{E(F_p), G, P, X\}$.

3.2. Registration Phases

At this phase, users and smart devices register with the gateway as a legal entity, and all registration information is transmitted on the secure channel.

3.2.1. User Registration Phase

(1) U_i chooses identity ID_i, password PW_i and biometrics B_i, and then transmits the ID_i to the GW;
(2) GW selects random number a_i, computes $HID_i = h(ID_i \parallel a_i)$, and sends HID_i to U_i;
(3) U_i calculates $Gen(B_i) = (\sigma_i, \tau_i)$, $Auth_i = h(ID_i \parallel PW_i \parallel \sigma_i)$, and stores $Auth_i, HID_i, \tau_i$ in their own mobile device. Table 2 shows the detailed process.

Table 2. User registration phase.

U_i		GW
Select ID_i, PW_i, B_i		
	$\xrightarrow{\{ID_i\}}$	
		Select a_i
		Compute $HID_i = h(ID_i \parallel a_i)$
	$\xleftarrow{\{HID_i\}}$	
Compute $Gen(B_i) = (\sigma_i, \tau_i)$		
$Auth_i = h(ID_i \parallel PW_i \parallel \sigma_i)$		
Store $\{Auth_i, HID_i, \tau_i\}$ in mobile device		

3.2.2. Smart Device Registration Phase

(1) D_j chooses its own identity SID_j and transmits it to the GW;
(2) GW selects random number r_j, computes $PID_j = h(SID_j \parallel r_j)$, stores PID_j in memory, and stores $\{(PID_j, ID_j)\}$. Finally, it sends PID_j to D_j;
(3) D_j stores PID_j in its own memory.

3.3. Access and Control Phase

The GW assists the U_i and the D_j in completing identity authentication and establishing a session key. Messages between devices are also transmitted through public channels. The detailed process is shown in Table 3.

(1) U_i enters ID_i, PW_i, B_i, calculates $\sigma_i = Rep(B_i, \tau_i)$, $Auth_i' = h(ID_i \parallel PW_i \parallel \sigma_i)$, and verifies $Auth_i' \stackrel{?}{=} Auth_i$. If the verification passes, this shows that the U_i is legitimate; Otherwise, the session terminates. U_i selects d_1, d_2, T_1, computes $C_1 = d_1 \cdot P$, $C_2 = d_1 \cdot x$, $C_3 = d_2 \oplus C_2 \oplus SID_j$, $C_4 = ID_i \oplus h(SID_j \parallel d_2)$, $V_1 = h(C_2 \parallel ID_i \parallel T_1)$. At last, U_i transmits message $M_1 = \{PID_k, PID_j, C_1, C_3, V_1, T_1\}$ to GW.
(2) When the GW obtains message M_1, it validates the timestamp's correctness. Next, GW sends PID_j, PID_k to the SGX interface. SGX match SID_j and x according to PID_j, PID_k. Then, GW computes $C_2' = x \cdot C_1$, $d_2' = C_3 \oplus C_2' \oplus SID_j$, $ID_i = C_4 \oplus h(SID_j \parallel d_2)$, $V_1' = h(C_2 \parallel ID_i \parallel T_1)$, and verifies $V_1' \stackrel{?}{=} V_1$. If the verification passes, GW selects T_2, computes $C_5 = ID_i \oplus d_2 \oplus h(SID_j \parallel T_2)$, $V_2 = h(SID_j \oplus d_2 \oplus T_2)$, and sends message $M_2 = \{C_5, V_2, T_2\}$ to the S_j.
(3) Upon receiving the M_2, S_j verifies the timestamp $|T - T_2| \leqq \Delta T$, then computes $ID_i \oplus d_2 = C_5 \oplus h(SID_j \parallel T_2)$, $V_2' = h(ID_i \oplus d_2 \parallel T_2)$, and verifies $V_2' \stackrel{?}{=} V_2$. If the verification is successful, it selects T_3, d_3, and computes $SK_{ji} = h(SID_j \oplus d_3 \parallel ID_i \oplus d_2)$, $C_6 = d_3 \oplus h(ID_i \oplus d_2 \parallel SID_j)$, $V_3 = h(SID_j \parallel T_3)$, $V_4 = h(SK_{ji} \parallel d_3 \parallel SID_j)$, and transmits the $M_3 = \{C_6, V_3, T_3, V_4\}$ to GW.
(4) When GW receives the M_3, it verifies the T_3. Next, GW computes $V_3' = h(SID_j \parallel T_3)$, and verifies $V_3' \stackrel{?}{=} V_3$. If the verification is successful, it proves that S_j is a legitimate device. Then it selects the timestamp T_4, and then send $M_4 = \{C_6, V_4, T_4\}$ to the U_i.
(5) After receiving the message M_4, U_i computes $d_3 = C_6 \oplus h(ID_i \oplus d_2 \parallel SID_j)$, $SK_{ij} = h(SID_j \oplus d_3 \parallel ID_i \oplus d_2)$, $V_4' = h(SK_{ij} \parallel d_3 \parallel SID_j)$, and verifies $V_4' \stackrel{?}{=} V_4$. If the two values are the same, U_i will use the SK_{ij} to transmit information with S_j.

Table 3. Login and authentication phase.

U_i	GW	D_j
Input ID_i, PW_i, B_i		
Compute $\sigma_i = Rep(B_i, \tau_i)$		
$Auth_i' = h(ID_i \parallel PW_i \parallel \sigma_i)$		
Check $Auth_i' \stackrel{?}{=} Auth_i$		
Select d_1, d_2, T_1		
$C_1 = d_1 \cdot P$		
$C_2 = d_1 \cdot X$		
$C_3 = d_2 \oplus C_2 \oplus SID_j$		
$C_4 = ID_i \oplus h(SID_j \parallel d_2)$		
$V_1 = h(C_2 \parallel ID_i \parallel T_1)$		
$\xrightarrow{M_1=\{PID_k, PID_j, C_1, C_3, C_4, V_1, T_1\}}$		

Table 3. *Cont.*

U_i	GW	D_j
	$\lvert T - T_1 \rvert \leqq \Delta T$ Send PID_j, PID_k to SGX Match SID_j, x according PID_j, PID_k Compute $C_2' = x \cdot C_1$ $d_2' = C_3 \oplus C_2' \oplus SID_j$ $ID_i = C_4 \oplus h(SID_j \parallel d_2)$ $V_1' = h(C_2 \parallel ID_i \parallel T_1)$ Check $V_1' \stackrel{?}{=} V_1$ Select T_2 $C_5 = ID_i \oplus d_2 \oplus h(SID_j \parallel T_2)$ $V_2 = h(SID_j \oplus d_2 \oplus T_2)$ $\xrightarrow{M_2=\{C_5,V_2,T_2\}}$	
		$\lvert T - T_2 \rvert \leqq \Delta T$ Compute $ID_i \oplus d_2 = C_5 \oplus h(SID_j \parallel T_2)$ $V_2' = h(ID_i \oplus d_2 \parallel T_2)$ Check $V_2' \stackrel{?}{=} V_2$ Select T_3, d_3 $SK_{ji} = h(SID_j \oplus d_3 \parallel ID_i \oplus d_2)$ $C_6 = d_3 \oplus h(ID_i \oplus d_2 \parallel SID_j)$ $V_3 = h(SID_j \parallel T_3)$ $V_4 = h(SK_{ji} \parallel d_3 \parallel SID_j)$ $\xleftarrow{M_3=\{C_6,V_3,T_3,V_4\}}$
	$\lvert T - T_3 \rvert \leqq \Delta T$ Compute $V_3' = h(SID_j \parallel T_3)$ Check $V_3' \stackrel{?}{=} V_3$ Selects T_4 $\xleftarrow{M_4=\{C_6,V_4,T_4\}}$	
$\lvert T - T_4 \rvert \leqq \Delta T$ Computes $d_3 = C_6 \oplus h(ID_i \oplus d_2 \parallel SID_j)$ $SK_{ij} = h(SID_j \oplus d_3 \parallel ID_i \oplus d_2)$ $V_4' = h(SK_{ij} \parallel d_3 \parallel SID_j)$ Check $V_4' \stackrel{?}{=} V_4$ if ture svaes the SK_{ij} for future communication		

4. Security Analysis

4.1. Formal Analysis

We use RoR model to formally analyze the scheme to prove the security of the proposed scheme. The steps of proof will be described in detail below.

RoR Model

RoR model [46,47] simulates the probability of an attacker cracking the scheme in polynomial time through different rounds of games and judges the security of the proposed scheme by whether the attacker can calculate the session key.

Our proposed agreement has three participants: U_i, GW, and D_j. We define $\Pi_{U_i}^x$, Π_{gw}^y, and $\Pi_{d_j}^z$ to represent the user instance, the gateway instance, and the smart device instance, respectively. Based on the ROR model, $\mathcal{A}$ needs to follow the following capabilities in each game.

(1) $Execute(O)$: This query is a passive attack and can enable $\mathcal{A}$ to eavesdrop on messages sent by entities, where $O = \{\Pi_{U_i}^x, \Pi_{GW}^y, \Pi_{D_j}^z\}$.

(2) $Send(O, M_i)$: $\mathcal{A}$ can send the message M_i send it to O and obtain the response from O.

(3) $Hash(string)$: This query means that $\mathcal{A}$ can obtain the hash of a certain string.
(4) $CorruptMobiledevice(\Pi_{U_i}^{x})$: $\mathcal{A}$ executing this query can obtain data in the mobile device.
(5) $Test(O)$: $\mathcal{A}$ flips a coin c to guess the real session key. In the case of $c = 1$, the $\mathcal{A}$ can obtain the session key, otherwise the attacker obtains a random string.

Theorem 1. *In RoR model, $\mathcal{A}$ can break the proposed scheme in polynomial time is $Adv_{\mathcal{A}}^{\mathcal{P}}(\xi) \leq= \frac{q_h^2}{|Hash|} + 2Adv_{\mathcal{A}}^{ECDHP}(\xi) + \frac{q_s}{2^{l-1}|D|}$. Here, $|Hash|$ indicates the range space of the hash function; $Adv_{\mathcal{A}}^{ECDHP}(\xi)$ indicates the advantage of cracking elliptic curve Diffie-Hellman problem (ECDHP); q_s refers to the Send query; l indicates the bit length of biological information; $|D|$ refers to the space size of the password dictionary.*

Proof. We defined 4 games GM_0-GM_3 to simulate $\mathcal{A}$'s attack process. During the proof process, $succ_A^{GM_i}(\xi)$ is defined as the probability that $\mathcal{A}$ can successfully compute the session key in each game, $Adv_{\mathcal{A}}^{\mathcal{P}}$ indicates that the $\mathcal{A}$ can break the advantage of scheme $\mathcal{P}$. The following is the specific process of the game.

GM_0: In GM_0, $\mathcal{A}$ needs to select a bit c to start the game simulating the real attack. So we have

$$Adv_{\mathcal{A}}^{\mathcal{P}}(\xi) = |2Pr[Succ_{\mathcal{A}}^{GM_0}(\xi)] - 1|. \tag{1}$$

GM_1: GM_1 adds the $Execute()$ query to GM_0. At GM_1, $\mathcal{A}$ intercepts the $M_1 = \{PID_k, PID_j, C_1, C_3, C_4, V_1, T_1\}$, $M_2 = \{C_5, V_2, T_2\}$, $M_3 = \{C_6, V_3, V_4, T_3\}$ and $M_4 = \{C_6, V_4, T_4\}$. When this query ends, $\mathcal{A}$ will execute $Test()$ query to compute the session key $SK_{ij} = \{SID_j \oplus d_3 \parallel ID_i \oplus d_2\}$. SID_j, d_3, ID_i and d_2 are confidential to $\mathcal{A}$. Therefore, there is no difference between GM_1 and GM_0.

$$Pr[Succ_{\mathcal{A}}^{GM_1}(\xi)] = Pr[Succ_{\mathcal{A}}^{GM_0}(\xi)]. \tag{2}$$

GM_2: GM_2 adds $Send()$ and $Hash()$ operations to the game. $\mathcal{A}$ wants to tamper with the message stolen on the public channel, but the authentication values V_1, V_2, V_3, V_4 are all based on hash functions, and the authentication values are composed of random numbers and dot product. Since random numbers are different, hash functions do not collide. In addition, since the $\mathcal{A}$ cannot obtain the x of GW and cannot solve the ECDHP, the $\mathcal{A}$ cannot calculate $C_2^* = x \cdot C_1$. Therefore, based on $Adv_{\mathcal{A}}^{ECDHP}(t)$ and birthday paradox, we can obtain

$$|Pr[Succ_{\mathcal{A}}^{GM_2}(\xi)] - Pr[Succ_{\mathcal{A}}^{GM_1}(\xi)]| \leq \frac{q_h^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDHP}(t). \tag{3}$$

GM_3: GM_3 adds $CorruptMobiledevice()$ operation, which can be used by $\mathcal{A}$ to obtain user information $\{V_1, HID_i, \tau_i\}$. In addition, $\mathcal{A}$ selects a low entropy password based on the password dictionary to guess the correct password of U_i, and the probability that $\mathcal{A}$ would correctly predict the biological key is $\frac{1}{2}$. Suppose the system allows the $\mathcal{A}$ to enter a limited number of wrong passwords, we have

$$|Pr[Succ_{\mathcal{A}}^{GM_3}(\xi)] - Pr[Succ_{\mathcal{A}}^{GM_2}(\xi)]| \leq \frac{q_s}{2^l|D|}. \tag{4}$$

Finally, $\mathcal{A}$ guesses bit b through the $Test()$ operation to win the game. So we can obtain

$$Pr[Succ_{\mathcal{A}}^{GM_3}(\xi)] = \frac{1}{2}. \tag{5}$$

According to $GM_0 - GM_3$, we have

$$\begin{aligned}\frac{Adv_{\mathcal{A}}^{\mathcal{P}}(\xi)}{2} &= |Pr[Succ_{\mathcal{A}}^{GM_0}(\xi)] - \frac{1}{2}| \\ &= |Pr[Succ_{\mathcal{A}}^{GM_0}(\xi)] - Pr[Succ_{\mathcal{A}}^{GM_3}(\xi)]| \\ &= |Pr[Succ_{\mathcal{A}}^{GM_1}(\xi)] - Pr[Succ_{\mathcal{A}}^{GM_3}(\xi)]| \\ &\leq \sum_{i=0}^{2} |Pr[Succ_{\mathcal{A}}^{GM_{i+1}}(\xi)] - Pr[Succ_{\mathcal{A}}^{GM_i}(\xi)]| \\ &= \frac{q_h^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDHP}(\xi) + \frac{q_s}{2^l|D|}\end{aligned} \tag{6}$$

Therefore, we can obtain

$$Adv_{\mathcal{A}}^{\mathcal{P}}(\xi) \leq= \frac{q_h^2}{|Hash|} + 2Adv_{\mathcal{A}}^{ECDHP}(\xi) + \frac{q_s}{2^{l-1}|D|} \tag{7}$$

□

4.2. Informal Analysis

4.2.1. Impersonation Attack

Suppose that $\mathcal{A}$ attempts to impersonate a legitimate user and communicate with other entities communicate to establish a session key. Because RA is only responsible for registration and does not store any entity information, he cannot impersonate users by obtaining RA information. If $\mathcal{A}$ obtains the information $\{PID_k, PID_j\}$ stored in the gateway and intercepts the information $\{PID_k, PID_j, C_1, C_3, V_1, T_1\}$ on the public channel to compute $V_1 = h(C_2 \parallel ID_i \parallel T_1)$, but because it cannot obtain $\{x, SID_j\}$, he cannot compute $C_2' = x \cdot C_1$, and $ID_i = C_4 \oplus h(SID_j \parallel d_2)$, so he cannot successfully compute V_1, and he cannot be authenticated through the gateway. Therefore, $\mathcal{A}$ cannot impersonate a legitimate user. In the same way, $\mathcal{A}$ tries to become a legitimate smart device, but because he cannot obtain the SID_j, he cannot compute the $V_3 = h(SID_j \parallel T_3)$, so he cannot successfully compute V_3, and he cannot be authenticated through the gateway. So our scheme is immune to impersonate attack.

4.2.2. Session Key Disclosure (SKD) Attack

Suppose $\mathcal{A}$ intercepts the messages $M_1 - M_4$, and attempts to calculate $SK = h(SID_j \oplus d_3 \parallel ID_i \parallel d_2)$, but the x, SID_j are private and $\mathcal{A}$ cannot obtain these values. Therefore, $\mathcal{A}$ cannot compute $C_2 = x \cdot C_1$, $d_2 = C_3 \oplus C_2' \oplus SID_j$, and $ID_i = C_4 \oplus h(SID_j \parallel d_2)$ through values of PID_j, C_1, C_6. Obviously, he cannot calculate SK. Thus, our scheme is immune to SKD attack.

4.2.3. Smart Device Stolen (SDS) Attack

Suppose $\mathcal{A}$ obtains the $PSID_j$ stored in the smart home device, intercepts C_1 and C_4, and tries to compute $C_2 = x \cdot C_1$, $ID_i = C_4 \oplus h(SID_j \parallel d_2)$, because the smart device only stores the pseudo identity PID_j of the device, the attacker cannot obtain x, d_2, so he cannot compute C_2, ID_i, so he cannot calculate the $SK = h(SID_j \oplus d_3 \parallel ID_i \parallel d_2)$. Thus, our scheme can resist the SDS attack.

4.2.4. Privacy and Anonymity

$\mathcal{A}$ can identify the real identity of U_i and D_j according to the intercepted public channel information. In our proposed scheme, we use hash function and random number to hide the real identity of U_i and D_j, thus providing anonymity for them. In each session, because the random number is different, even if $\mathcal{A}$ can intercept the pseudo identity of U_i and D_j, he cannot identify the real identity of their real identities. Therefore, our scheme can protect the entity's privacy from being disclosed.

4.2.5. Mutual Authentication

The gateway authenticates user and smart device using V_1 and V_3, respectively. Although $\mathcal{A}$ can eavesdrop on these two values, $\mathcal{A}$ cannot correctly compute and change the verification value because he cannot obtain x, SID_j, and cannot compute $C_2 = x \cdot C_1$, $ID_i = C_4 \oplus h(SID_j \parallel d_2)$. Similarly, although the verification value V_3 is transmitted on the public channel, $\mathcal{A}$ cannot obtain the SID_j. He cannot correctly calculate and change V_3. As long as a changes any of the verification values, it will be detected immediately and the session will be terminated. So our scheme can realize mutual authentication.

5. Security and Performance Comparison

We use the proposed scheme to compare the existing schemes [13,17,48] in terms of security, computing cost and communication cost, and the detailed introduction and comparison results are described below.

5.1. Security Comparison

The proposed scheme is compared with the three schemes regarding security, and the comparison results are listed in Table 4. Shuai et al.'s scheme [13] is unable to withstand OPG, insider, and SKD attacks. The scheme of Yu et al. [17] cannot realize mutual authentication; Kaur et al. [19] cannot withstand impersonation attack and violated mutual authentication. The proposed scheme and Zou et al.'s scheme [18] can resist common attack.

Table 4. Comparisons of security.

Security Properties	Shuai et al. [13]	Kaur et al. et al. [19]	Yu et al. [17]	Zou et al. [18]	Ours
Impersonation attack	✓	×	✓	✓	✓
Temporary value disclosure attack	✓	✓	✓	✓	✓
OPG attack	×	✓	✓	✓	✓
Insider attack	×	✓	✓	✓	✓
SDS attack	✓	✓	✓	✓	✓
SKD attack	×	✓	✓	✓	✓
Mutual authentication	✓	×	×	✓	✓

5.2. Computation Costs Comparison

We use an IQOO9 mobile phone to emulate U_i and S_j and a Lenovo desktop computer to emulate the GW. The mobile phone's processor is a snapdragon 8-core processor with 12G of running memory and the Lenovo desktop computer's CPU is the Intel(R) Core(TM)i5-8500 CPU@ 3.00 GHz with 16G of running memory. The software used on the computer is IntelliJ idea 2020.3, and the program is written using JAVA and cryptographic library JPBC-2.0.0 [49]. In Table 5, we select four main operations: hash function T_h, point scalar multiplication T_m, symmetric decryption T_{de}, and symmetric encryption T_{dn}. We ran various operations 100 times on the mobile phone and computer to take the average running time. In Table 6, we based on the results in Table 5 to show the comparison of computation costs between our and recently proposed schemes [13,17–19]. For example, our scheme requires $7T_h + 2T_m$ for U_i. The cost is $7 \times 0.0023 + 2 \times 0.6349 = 1.2859$ ms.

In Table 6, and Figure 3, the costs of [13,17,19] for U_i are less than our scheme. Our scheme requires an additional 0.1971 ms than [17] and 0.0023 ms than [13,19]. In fact, the two values are reasonable in practice. More importantly, the three schemes have some security weaknesses mentioned in Table 4. Overall, our scheme provides both security and efficiency for U_i.

In Table 6, and Figure 4, the costs of [13,17,19] for S_j are less than our scheme. Our scheme requires an additional 0.0069 ms than [13,19] and 0.0023 ms than [17]. In fact, the two values are reasonable in practice. More importantly, the three schemes have some security weaknesses mentioned in Table 4. Overall, our scheme provides both security and efficiency for S_j.

Table 5. Computation costs of complex operations.

Operations	Symbolic	Mobile Phone (ms)	Computer (ms)
Hash function	T_h	0.0023	0.00103
Point scalar multiplication	T_m	0.6349	0.545
Symmetric Decryption	T_{de}	0.0612	0.0127
Symmetric Encryption	T_{en}	1	0.1833

Table 6. Computation costs.

Scheme	U_i (ms)	S_j (ms)	GW (ms)
Shuai et al. [13]	$6T_h + 2T_m = 1.2836$	$3T_h = 0.0069$	$7T_h + T_m = 0.5522$
Kaur et al. [19]	$6T_h + 2T_m = 1.2836$	$3T_h = 0.0069$	$7T_h + T_m = 0.5522$
Yu et al. [17]	$T_{de} + T_m + 12T_h = 1.0888$	$7T_h = 0.0161$	$11T_h = 0.0113$
Zou et al. [18]	$6T_h + 3T_m = 1.9185$	$5T_h + 2T_m = 1.2813$	$6T_h + T_m = 0.5518$
Ours	$7T_h + 2T_m = 1.2859$	$6T_h = 0.0138$	$5T_h + T_m = 0.5501$

5.3. Communication Costs Comparison

In Table 7, we show the communication costs between our and recently proposed schemes [13,17–19]. Note that the lengths of symmetric encryption and decryption $|E|$, hash functions $|H|$, timestamp T, integer $|Z_p^*|$, identify $|ID|$ and ECC $|G|$ are defined by 256 bits, 256 bits, 128 bits, 160 bits, 32 bits, and 320 bits, respectively. Here, the total communication costs of our scheme are computed by $2|ID| + |G| + 5|Z_p^*| + 3|T| + 5|H| = 2 \times 32 + 320 + 5 \times 160 + 3 \times 128 + 5 \times 256 = 2348$ bits. The communication costs of Shuai et al.'s scheme [13] requires $3|Z_p^*| + 4|H| + |G| = 3 \times 128 + 4 \times 256 + 5 \times 320 = 1824$ bits, Kaur et al.'s scheme [19] requires $5|Z_p^*| + 4|H| + |G| + 3|T| = 5 \times 128 + 4 \times 256 + 320 + 3 \times 128 = 2400$ bits, Yu et al.'s scheme [17] requires $4|Z_p^*| + 4|H| + 3|T| = 4 \times 128 + 4 \times 256 + 3 \times 128 = 2048$ bits, Zou et al.'s scheme [18] requires $3|ID| + 3|G| + 2|Z_p^*| + 3|T| + 10|H| = 3 \times 32 + 3 \times 320 + 2 \times 160 + 3 \times 128 + 10 \times 256 = 3944$ bits. Finally, the results in Table 7 are depicted in Figure 5. It can be seen that Zou et al.'s scheme [18] has the highest communication cost, Shuai et al.'s scheme [13] has the lowest communication cost, and our scheme is lower than Zou et al.'s scheme [18], slightly higher than Kaur et al.'s scheme [19].

Table 7. Communication costs.

Scheme	Communication Costs (bits)	Length (bits)
Shuai et al. [13]	$3\|Z_p^*\| + 4\|H\| + \|G\|$	1824
Kaur et al. [19]	$5\|Z_p^*\| + 4\|H\| + \|G\| + 3\|T\|$	2400
Yu et al. [17]	$4\|Z_p^*\| + 4\|H\| + 3\|T\|$	2048
Zou et al. [18]	$3\|ID\| + 3\|G\| + 2\|Z_p^*\| + 3\|T\| + 10\|H\|$	3944
Ours	$2\|ID\| + \|G\| + 5\|Z_p^*\| + 3\|T\| + 5\|H\|$	2848

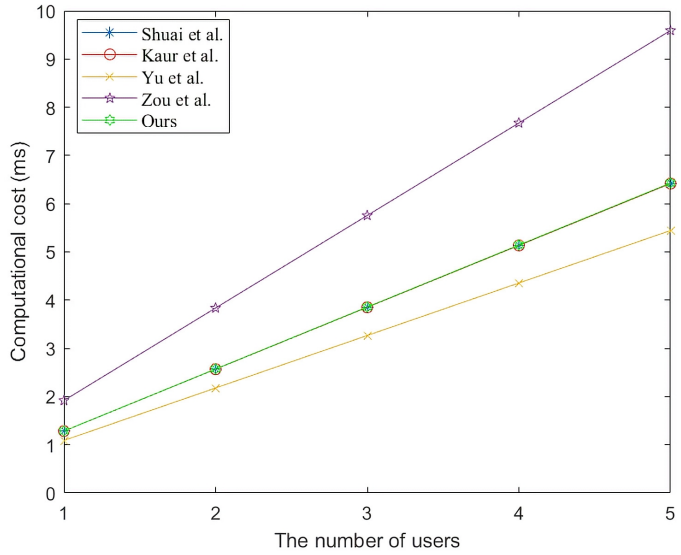

Figure 3. The computation cost of users [13,17–19].

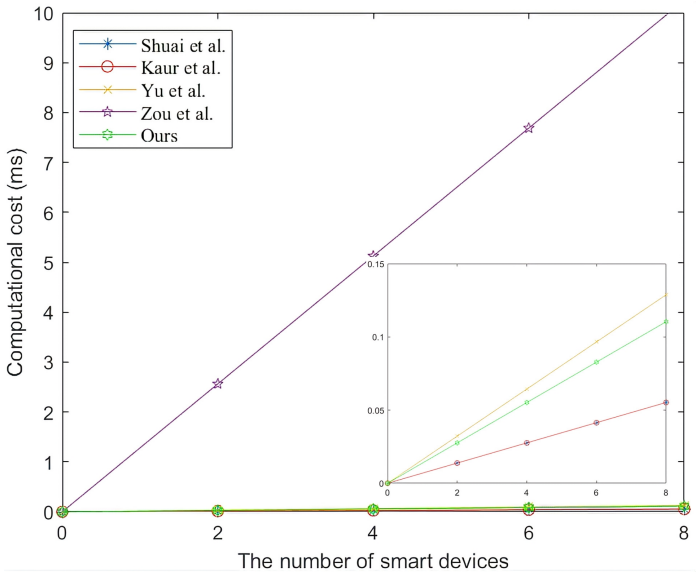

Figure 4. The computation cost of smart devices [13,17–19].

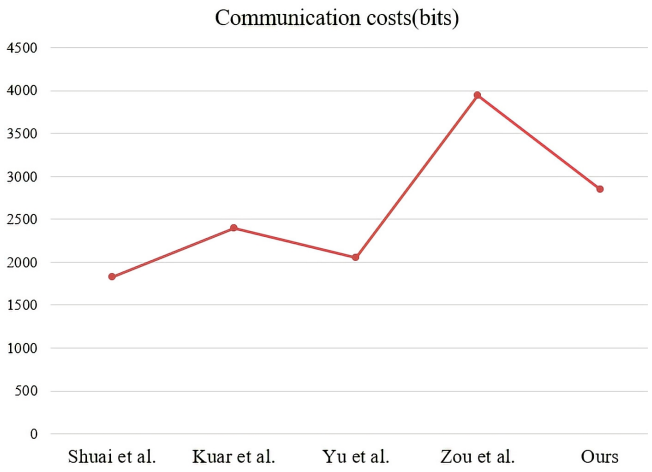

Figure 5. The results of communication costs [13,17–19].

6. Conclusions

As the foundation of smart cities, smart homes are closer to people's lives, so ensuring the security of data transfers between entities is critical. In this paper, we propose an AKA scheme suitable for smart home environments and use the combination of SGX and gateway to prevent insider attacks effectively. Moreover, we also prove the proposed scheme's security through informal security analysis and the RoR model. Finally, we compare the proposed scheme with existing schemes regarding security, computation, and communication costs. Based on the comparison results, our scheme performs better and is more suitable for this environment. In the future, smart home authentication schemes should incorporate multiple approaches such as multi-factor authentication and biometrics. Additionally, users should set strong passwords for smart home devices and limit the number of people who can access smart devices. We will continue to improve the smart home authentication scheme to meet the growing security needs.

Author Contributions: Conceptualization, T.-Y.W.; methodology, T.-Y.W. and Q.M.; software, Y.-C.C.; formal analysis, S.K.; investigation, C.-M.C.; writing—original draft preparation, T.-Y.W., Q.M., Y.-C.C., S.K. and C.-M.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data is included in the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
SGX	Software guard extensions
TEE	Trusted execution environment
EPC	Enclave page cache
ROR	Real-or-random
AKA	Authentication and key agreement
OPG	Offline password guessing
SKD	Session key disclosure
PFS	Perfect froward secrecy
SDS	Smart device stolen
Notations	**Meanings**
U_i	The i-th user
ID_i	Identity of U_i
PW_i	U_i's password
PID_i	Pseudo identity of U_i
RA	The registration authority
x	RA's secret key
GW	The gateway
ID_k	The k-th user
PID_k	GW's pseudo identity
D_j	The j-th smart device
SID_j	D_j's identity
PID_j	D_j's pseudo identity
SK_{ij}, SK_{ji}	The session key

References

1. Wu, T.Y.; Guo, X.; Chen, Y.C.; Kumari, S.; Chen, C.M. SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing. *Symmetry* **2022**, *14*, 1393. [CrossRef]
2. Mei, Q.; Yang, M.; Chen, J.; Wang, L.; Xiong, H. Expressive Data Sharing and Self-Controlled Fine-Grained Data Deletion in Cloud-Assisted IoT. *IEEE Trans. Dependable Secur. Comput.* 2022, *early access*. [CrossRef]

3. Zhang, J.; Li, M.; Chen, Z.; Lin, B. Computation offloading for object-oriented applications in a UAV-based edge-cloud environment. *J. Supercomput.* **2022**, *78*, 10829–10853. [CrossRef]
4. Wu, T.Y.; Meng, Q.; Kumari, S.; Zhang, P. Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments. *Sensors* **2022**, *22*, 3858. [CrossRef] [PubMed]
5. Wang, S.; Chen, Z.; Zhu, W.; Wang, F.Y. Deep random walk of unitary invariance for large-scale data representation. *Inf. Sci.* **2021**, *554*, 1–14. [CrossRef]
6. Cheng, H.; Shi, Y.; Wu, L.; Guo, Y.; Xiong, N. An intelligent scheme for big data recovery in Internet of Things based on multi-attribute assistance and extremely randomized trees. *Inf. Sci.* **2021**, *557*, 66–83. [CrossRef]
7. Pan, J.S.; Lv, J.X.; Yan, L.J.; Weng, S.W.; Chu, S.C.; Xue, J.K. Golden eagle optimizer with double learning strategies for 3D path planning of UAV in power inspection. *Math. Comput. Simul.* **2022**, *193*, 509–532. [CrossRef]
8. Zou, W.; Guo, L.; Huang, P.; Lin, G.; Mei, H. Linear time algorithm for computing min-max movement of sink-based mobile sensors for line barrier coverage. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6175. [CrossRef]
9. Hundera, N.W.; Jin, C.; Geressu, D.M.; Aftab, M.U.; Olanrewaju, O.A.; Xiong, H. Proxy-based public-key cryptosystem for secure and efficient IoT-based cloud data sharing in the smart city. *Multimed. Tools Appl.* **2022**, *81*, 29673–29697. [CrossRef]
10. Chaudhry, S.A. Combating identity de-synchronization: an improved lightweight symmetric key based authentication scheme for IoV. *J. Netw. Intell.* **2021**, *6*, 12.
11. Wu, T.; Guo, X.; Chen, Y.; Kumari, S.; Chen, C. Amassing the security: An enhanced authentication protocol for drone communications over 5G networks. *Drones* **2021**, *6*, 10. [CrossRef]
12. Wu, T.Y.; Meng, Q.; Yang, L.; Kumari, S.; Nia, M.P. Amassing the Security: An Enhanced Authentication and Key Agreement Protocol for Remote Surgery in Healthcare Environment. *Comput. Model. Eng. Sci.* **2023**, *134*, 317–341. [CrossRef]
13. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146. [CrossRef]
14. Kong, H.; Lu, L.; Yu, J.; Chen, Y.; Tang, F. Continuous authentication through finger gesture interaction for smart homes using WiFi. *IEEE Trans. Mob. Comput.* **2020**, *20*, 3148–3162. [CrossRef]
15. Zhao, J.; Chen, Y.; Zhang, W. Differential privacy preservation in deep learning: Challenges, opportunities and solutions. *IEEE Access* **2019**, *7*, 48901–48911. [CrossRef]
16. Pan, J.S.; Sun, X.X.; Chu, S.C.; Abraham, A.; Yan, B. Digital watermarking with improved SMS applied for QR code. *Eng. Appl. Artif. Intell.* **2021**, *97*, 104049. [CrossRef]
17. Yu, S.; Jho, N.; Park, Y. Lightweight three-factor-based privacy-preserving authentication scheme for iot-enabled smart homes. *IEEE Access* **2021**, *9*, 126186–126197. [CrossRef]
18. Zou, S.; Cao, Q.; Wang, C.; Huang, Z.; Xu, G. A robust two-factor user authentication scheme-based ECC for smart home in IoT. *IEEE Syst. J.* **2021**, *16*, 4938–4949. [CrossRef]
19. Kaur, D.; Kumar, D. Cryptanalysis and improvement of a two-factor user authentication scheme for smart home. *J. Inf. Secur. Appl.* **2021**, *58*, 102787. [CrossRef]
20. Ge, M.; Kumari, S.; Chen, C.M. AuthPFS: A Method to Verify Perfect Forward Secrecy in Authentication Protocols. *J. Netw. Intell.* **2022**, *7*, 734–750.
21. Pirayesh, J.; Giaretta, A.; Conti, M.; Keshavarzi, P. A PLS-HECC-based device authentication and key agreement scheme for smart home networks. *Comput. Netw.* **2022**, *216*, 109077. [CrossRef]
22. Guo, Y.; Zhang, Z.; Guo, Y. SecFHome: Secure remote authentication in fog-enabled smart home environment. *Comput. Netw.* **2022**, *207*, 108818. [CrossRef]
23. Nyangaresi, V.O. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *J. Syst. Archit.* **2022**, *133*, 102763. [CrossRef]
24. Yakubu, B.M.; Khan, M.I.; Khan, A.; Jabeen, F.; Jeon, G. Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home. *Digit. Commun. Netw.* 2023, *in press*. [CrossRef]
25. Sun, H.; Xiao, S. DNA-X: Dynamic network authentication using SGX. In Proceedings of the 2nd International Conference on Cryptography, Security and Privacy, Guiyang, China, 16–19 March 2018; pp. 110–115. [CrossRef]
26. Liu, X.; Guo, Z.; Ma, J.; Song, Y. A secure authentication scheme for wireless sensor networks based on DAC and Intel SGX. *IEEE Internet Things J.* **2021**, *9*, 3533–3547. [CrossRef]
27. Jeong, J.; Chung, M.Y.; Choo, H. Integrated OTP-based user authentication scheme using smart cards in home networks. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, HI, USA, 7–10 January 2008; p. 294. [CrossRef]
28. Vaidya, B.; Park, J.H.; Yeo, S.S.; Rodrigues, J.J. Robust one-time password authentication scheme using smart card for home network environment. *Comput. Commun.* **2011**, *34*, 326–336. [CrossRef]
29. Kim, H.J.; Kim, H.S. AUTH HOTP-HOTP based authentication scheme over home network environment. In Proceedings of the International Conference on Computational Science and Its Applications, Santander, Spain, 20–23 June 2011; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6784, pp. 622–637.
30. Li, Y. Design of a key establishment protocol for smart home energy management system. In Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, 5–7 June 2013; pp. 88–93. [CrossRef]

31. Han, K.; Kim, J.; Shon, T.; Ko, D. A novel secure key paring protocol for RF4CE ubiquitous smart home systems. *Pers. Ubiquitous Comput.* **2013**, *17*, 945–949. [CrossRef]
32. Santoso, F.K.; Vun, N.C. Securing IoT for smart home system. In Proceedings of the 2015 International Symposium on Consumer Electronics (ISCE), Madrid, Spain, 24–26 June 2015; pp. 1–2. [CrossRef]
33. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2015**, *16*, 254–264. [CrossRef]
34. Ashibani, Y.; Mahmoud, Q.H. An efficient and secure scheme for smart home communication using identity-based signcryption. In Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–7. [CrossRef]
35. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Susilo, W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 391–406. [CrossRef]
36. Chifor, B.C.; Bica, I.; Patriciu, V.V.; Pop, F. A security authorization scheme for smart home Internet of Things devices. *Future Gener. Comput. Syst.* **2018**, *86*, 740–749. [CrossRef]
37. Ghosh, N.; Chandra, S.; Sachidananda, V.; Elovici, Y. SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT. *IEEE Internet Things J.* **2019**, *6*, 10773–10785. [CrossRef]
38. Dey, S.; Hossain, A. Session-key establishment and authentication in a smart home network using public key cryptography. *IEEE Sens. Lett.* **2019**, *3*, 1–4. [CrossRef]
39. Gaba, G.S.; Kumar, G.; Monga, H.; Kim, T.H.; Kumar, P. Robust and lightweight mutual authentication scheme in distributed smart environments. *IEEE Access* **2020**, *8*, 69722–69733. [CrossRef]
40. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Lightweight and secure password based smart home authentication protocol: LSP-SHAP. *J. Netw. Syst. Manag.* **2019**, *27*, 1020–1042. [CrossRef]
41. Poh, G.S.; Gope, P.; Ning, J. PrivHome: Privacy-preserving authenticated communication in smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1095–1107. [CrossRef]
42. Irshad, A.; Usman, M.; Chaudhry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-loop-driven low-cost and secure biometric user access to server. *IEEE Trans. Reliab.* **2020**, *70*, 1014–1025. [CrossRef]
43. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Park, Y. An efficient, anonymous and robust authentication scheme for smart home environments. *Sensors* **2020**, *20*, 1215. [CrossRef] [PubMed]
44. Fadi, A.T.; Deebak, B.D. Seamless authentication: For IoT-big data technologies in smart industrial application systems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2919–2927.
45. Alzahrani, B.A.; Barnawi, A.; Albarakati, A.; Irshad, A.; Khan, M.A.; Chaudhry, S.A. SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8669941. [CrossRef]
46. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3386, pp. 65–84.
47. Wu, T.Y.; Meng, Q.; Yang, L.; Guo, X.; Kumari, S. A provably secure lightweight authentication protocol in mobile edge computing environments. *J. Supercomput.* **2022**, *78*, 13893–13914. [CrossRef]
48. Xiang, A.; Zheng, J. A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks. *Electronics* **2020**, *9*, 989. [CrossRef]
49. De Caro, A.; Iovino, V. jPBC: Java pairing based cryptography. In Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC), Kerkyra, Greece, 28 June–1 July 2011; pp. 850–855. [CrossRef]