This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

Digital Object Identifier

Remotely Access "My" Smart Home in Private: An Anti-tracking Authentication and Key Agreement Scheme

QIUYUN LYU[a], NING ZHENG[a], HUAPING LIU[b], CAN GAO[a], SI CHEN[c], JUNLIANG LIU[d]
[a]Hangzhou Dianzi University, Hangzhou, Zhejiang, China
[b]Oregon State University, Corvallis, OR 97331, USA
[c]Beijing Jiaotong University, Beijing, China
[d]MoreSec. Tech. Inc., Hangzhou, Zhejiang, China

Corresponding author: Ning Zheng (email:nzheng@hdu.edu.cn).

ABSTRACT Smart Home is one of the key applications of Internet of Things (IoT), which allows users to control the smart devices in their houses through the Internet. However, a smart home system also faces severe challenges in terms of privacy and confidentiality when users are allowed to remotely access it. Despite the recent research efforts on authentication schemes to improve the security aspects of Smart Home, there are still unsolved problems. On the one hand, most of the existing schemes focus on secure authentication and communication via a trusted third party without taking its privacy leakage into consideration. On the other hand, many protocols enable the users to directly authenticate themselves to a large number of smart devices in the smart home network, which is often inefficient and inconvenient. To cope with these issues, we propose a smart home system model based on Internet services like IFTTT (If This Then That) and design an anti-tracking mutual authentication scheme with a key agreement element in it. Specifically, our scheme introduces an IFTTT home gateway as the control commands executor and the security guard to allow a user to remotely access a smart home system privately. The proposed scheme employs an elliptic curves cryptography (ECC) algorithm, nonces, XOR and cryptographical hash functions to achieve mutual authentication with security features such as anonymity and perfect forward security. Security analysis and performance comparison results demonstrate that the proposed scheme achieves secure and private authentication.

INDEX TERMS Smart home, user authentication, anti-tracking, key agreement, BAN-logic.

I. INTRODUCTION

As smart devices and high speed networks continue to grow rapidly, the Internet of Things (IoT) has gained wide acceptance and popularity [1]. Smart Home is an e-merging key-element of the IoT [5]. The global smart home market is expected to grow from USD 76.6 billion in 2018 to USD 151.4 billion by 2024, at a CAGR of 12.02% [6].

Smart Home is an IoT-based system that allows a user to connect sensors, home appliances, and smart devices via the Internet to achieve remote monitoring of, remote access to, and remote control of a residential environment [7]. It brings users convenience and efficiency through providing various services such as energy conservation, secure monitoring, and healthcare. However, since users need to communicate over the public channel, i.e., the Internet, with resource limited smart devices, it is a significant challenge to ensure secure and private access to the smart home systems. For example, a smart device can be used to determine the activities and presence of an individual at a given time [8]; an adversary could remotely gain access to the monitoring system of a user's Smart Home [3]; and a user's profile, such as photos and identities, could leak out from the Smart Home application server [4].

To enhance the security of remote communications to Smart Homes, various authentication schemes have been developed. These schemes may be classified into three categories: *third party authentication*, *smart devices authentication*, and *home gateway authentication*. *Third party authentication* was the first proposed, which relies on a third server to authenticate a remote user to access a Smart Home [5, 20, 31]. For example, Vaidya *et al.* [20] and Jeong *et al.* [31] introduced an integrated authentication server (IAS) to authenticate a remote user and to send a ticket (including the session key with a home gateway) to him. The authenticated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

user sends the ticket to the home gateway and comes to an agreement on the session key. However, since IAS is shared among all users, it will be the first object that is subject to attacking by the adversaries. Also, the IAS is maintained by a third party which leaves additional vulnerabilities. To avoid the threats above, researchers have developed *smart devices authentication*, which focuses on authenticating a remote user by the smart devices directly with or without the help of a trusted third party [9-12]. The current generation of IoT devices in Smart Homes are vulnerable to attacks in a number of ways [13], such as reflection attack, domain name system (DNS) spoofing, distributed denial of service (DDOS) attacks based on Internet control message protocol (ICMP). Further, when a home has a large number of smart devices (e.g., more than 500), these devices' authentication inevitably becomes more vulnerable to attack [2]. These have led to *home gateway authentication schemes*, in which a home gateway authenticates a remote user for accessing smart devices [14]. The home gateway, as a security guard of smart devices in a smart home system, and as a private property of a user, generally achieves a stronger security. However, the scheme by Wazid *et al.* [14] places the security-base on the registration authority (RA) completely, leaving the home gateway alone on the Internet and making the remote users to change the session key with each smart device. Thus, this scheme must prevent attacks from the RA and the Internet, which has a low efficiency as the number of smart devices increases.

On the other end, a type of Internet services, IFTTT (IF This Then That), which acts as an interface between a user's phone and the smart home devices [5, 18, 32], has attracted significant attentions recently. IFTTT makes it convenient for a user to remotely manipulate the smart devices and configure the smart home through various IFTTT recipes. IFTTT recipes are the "If this (condition) then that (action)" statements, like "If a family member is at home, then turn on the air conditioner". Examples of some recipes are shown in Table 1 [5]. IFTTT provides an alternative way to save users' time and efforts on routine but repetitive activities [15], and is considered a promising framework for future Smart Homes [18]. However, in the current IFTTT framework [5, 18], a user's smart home system depends completely on the IFTTT server, in which the user's account and recipes are stored. Basically, schemes build on the IFTTT framework is a type of third party authentication schemes.

Note that existing research has developed tiptop authentication between smart devices and a home gateway within the home network [16, 21, 22]. Exploiting the convenience that IFTTT could provide, we propose an IFTTT-based Smart Home system in which an IFTTT home gateway is added as an independent security guard. Introducing an IFTTT home gateway into a Smart Home system is not a trivial task; it must sufficiently address three critical challenges: *1) Threats from a compromised IFTTT server.* An IFTTT server is an entity run by a third party. In traditional schemes, the third party server is often considered as a fully trusted entity that

TABLE 1: IFTTT recipes [5]

Smart devices	Trigger (If)	Action (Then)
Motion Sensors, Smart Lock, Smart Lights	User's arrival detected	Turn on
Motion Sensors, Smart Lock, User's device	User's departure detected, device's status: turned on	Notify user of the status of the devices
Temperature/Humidity Sensors, Air conditioner	Temperature too high/low	Set Temperature, Turn AC on/off
Sensors, User's device	Detects critical events	Notify user

is sufficiently secure to resist all kinds of attacks and has the ability and loyalty to process and store all secret information for smart devices and users. However, such assumptions are not necessarily true, since incidents of servers' leaking users' private data do occur frequently [37-39]. A compromised IFTTT server would be a significant privacy threat to the Smart Homes. *2) Security weakness from exposing an IFTTT home gateway to the Internet.* Because of cost and other practical considerations, the available resources of an IFTTT home gateway are not as abundant as those of a third party server. Consequently, authenticating a remote user using an IFTTT home gateway alone has a considerably weaker security than using a third party server. *3) Burdens due to requiring secure channels for registration.* In recent authentication schemes [9-10,14], the users, the home gateway and smart devices all take part in the registration phase, which requires some secure channels (communicating face-to-face could be considered a secure form). Current schemes assume that the registration rarely happens and thus neglect its associated burden, which could be significant for some cases. For example, a rental Smart Home needs much more registration than others since the house ownership changes more often.

The scheme proposed in this paper aims to address the issues discussed above. Specifically, an anti-tracking and mutual authentication scheme based on the IFTTT Smart Home system model is developed, in which the IFTTT server does not perform user registration or authentication as a trusted third party does; instead, an IFTTT home gateway authenticates remote users via an IFTTT server. The IFTTT Server cannot track the user, and the adversary cannot track the user and the ITFFF home gateway either. The contributions of the work in this paper are as follows.

1) To the authors' knowledge, this is the first work to propose a Smart Home system model in which a home gateway authenticates a remote user, aided by an IFTTT server.
2) To minimize the threat from a compromised IFTTT server, we design an anti-tracking and mutual authentication protocol. In this protocol, an IFTTT home gateway authenticates a remote user privately; the IFTTT server only maintains the home gateway pseudonym list and forwards the authentication messages for them.
3) To overcome the security weakness from exposing an

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

IFTTT home gateway to the Internet, in the proposed model, an IFTTT home gateway is placed behind an IFTTT server logically, in which a remote user sends protected authentication messages to an IFTTT server, and then the IFTTT server re-encrypts and forwards them to an IFTTT home gateway.

4) To avoid the complexity due to requiring secure channels for registration, we develop a remote registration method for the home gateway, and a method requires user registration be limited to a human visual range.
5) The security aspects of the proposed scheme are analyzed, and its performance is evaluated in practical scenarios.

The rest of this paper is organized as follows. Section II reviews related work. In Section III, we describe the system model, threat model, the design goals. The proposed scheme is described in Section IV. The security aspects of the proposed model are analyzed in Section V and a proof of the security with the Burrow-Abadi-Needham Logic (BAN-Logic) and Scyther tool is provided in Section VI. Section VII compares the performances of the proposed scheme and related existing schemes, followed by concluding remarks in Section VIII.

II. RELATED WORK

A. THIRD PARTY AUTHENTICATING A REMOTE USER

Authenticating a remote user via a third party is a common way for Smart Home systems. In 2008, Jeong *et al.* [31] introduced an integrated authentication server (IAS) to perform authentication, authorization and accounting (AAA) for Smart Homes. This scheme employs hash functions and symmetric encryption algorithms to achieve lightweight authentication. But it sends a user's identity in plaintext, which can be easily traced by an adversary. In 2011, Vaidya *et al.* [20] adopted the same system model as described in [31]. Lightweight authentication is achieved in a similar way, but the verification table is eliminated from the IAS to improve security. However, the user's identity is still transferred in plaintext. In 2018, Baruah *et al.* [5] proposed an IFTTT-based smart home system model. In this scheme, remote users logon to an IFTTT server to configure recipes and to remotely control the smart devices through the IFTTT server. It tackles the issues associated with a user's compromised device, but all the smart home devices being controlled by the IFTTT server could still be at risk of security breaches. The IAS and IFTTT server are shared among all the smart home users [5, 20, 31]. Thus, the IAS and IFTTT server could be the main targets of the adversaries, which may result in severe security problems. Furthermore, they are maintained by the third party, which adds additionally vulnerability.

B. SMART DEVICES AUTHENTICATING A REMOTE USER

Using smart devices to authenticate a remote user directly with or without the help of a third party has become a popular way recently [9, 11, 12]. In 2017, Ashibani *et al.* [12] proposed an identity-based signcryption to make the

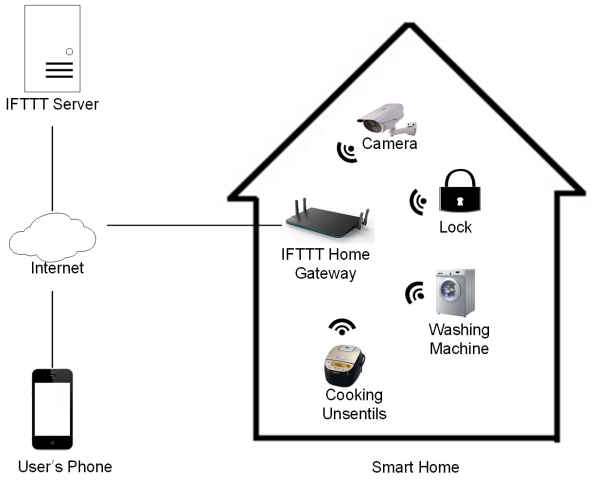


FIGURE 1: Smart Home system model.

authentication between an end-user's device and a smart home device secure. This scheme relies on ECC and bilinear pairing, but does not consider the feasibility of implementing these complex algorithms in resource limited smart devices. In 2018, Chifor *et al.* [9] proposed a fast identity online (FIDO) based authentication scheme between a user's phone and smart home IoT devices where a password-less authentication protocol is executed. This scheme uses the periodical siblings security scheme which is impractical for implementation in resource limited smart-home devices. Also a strict registration process of smart devices makes it difficult to use. In 2018, Ra *et al.* [11] developed an authentication scheme that uses a keyless signature infrastructure (KSI) to let a smart device authenticate a remote user. When there are a large number of smart devices, schemes that rely on smart devices to authenticate a remote user will face a major security issue. For example, Gartner predicted [2] that by 2022, a typical family home may have more than 500 smart devices, for which such schemes are unsuitable.

C. HOME GATEWAY AUTHENTICATING A REMOTE USER

Schemes in which a home gateway authenticates a remote user for smart devices aided by a third party have been proposed recently. A home gateway, as a private property of a user, can be fully controlled by a household, and it has much more resources than smart devices. Thus it can provide stronger security functions. In 2017, Wazid *et al.* [14] designed a protocol to let a home gateway authenticate a remote user and to build a session key between the user and a smart device. This scheme is based on the successful registration of all entities (a user, a home gateway, a smart device) to a trusted registration authority (RA). Thus, this scheme is not immune attacks from a compromised RA. Additionally, when a user accesses multiple smart devices, the home gateway must authenticate the user for each smart device and then get

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

the session key for each of them. Repeatedly authenticating the same user wastes resources and may result in long delay. Also, this scheme allows a user to directly connect to a home gateway. This process could be exploited by advanced adversaries to gather some information about the activities happening in the smart home through tracing the connection for a period of time.

D. HOME GATEWAY AUTHENTICATING SMART DEVICES

Smart devices authenticated by a home gateway is proposed for dealing with the attacks inside since a home network is an IoT-based local area network. In 2016, Kumar *et al.* [21] proposed a lightweight and secure session-key establishment scheme between a home gateway and smart devices. To enhance anonymity and security, in 2017, Kumar *et al.* [22] improved their scheme in [21] to achieve smart devices' anonymity. In 2017, Song *et al.* [16] proposed a secure authentication scheme between a home gateway and smart devices assisted by chaotic systems. This scheme achieves good security and has a high efficiency. But these schemes are insufficient to deal with issues associated with the remote users.

III. PROBLEM STATEMENT

A. SYSTEM MODEL

The system being proposed in this paper consists of four entities: *user's phone, IFTTT server, IFTTT home gateway and smart devices* at home, as shown in Fig. 1. A user uses his phone to remotely control his smart home system. An *IFTTT server* maintains all the IFTTT home gateways, finds the requested home gateway for a user, encrypts the request, and forwards the request to the IFTTT home gateway without requiring specific contents. An *IFTTT home gateway* authenticates the user and responds to the request, with encryption, to the IFTTT server. The server then decrypts it and forwards the decrypted request to the user without acquiring the specific contents. The *Smart devices* in the home network are managed by the IFTTT home gateway, and they form an independent self-governing system. Thus, if a user wants to control his home, he must be authenticated by the IFTTT home gateway via an IFTTT server, and he sends IFTTT recipes to the home gateway to control his home smart devices.

B. THREAT MODEL

The proposed scheme builds upon the Dolev-Yao threat model [17], in which any two parties could communicate over an insecure channel. The entities such as a user's phone and the IFTTT server are not considered to be trusted entities. It is assumed that the IFTTT server is interested in the user's information but strictly follows the authentication protocol. An adversary ($\mathcal{A}$) can eavesdrop the exchanged messages, and can also modify or delete the message contents during transmission.

- It is assumed that the standard cryptographic algorithms are secure and unbreakable. For example, the adversary is unable to forge valid hash values or to fabricate affirmed elliptic curve operations without getting a principal's private key. Besides, random numbers are generated (in default) by a function which converts the physical signal into the digitized signal from the network interface, and the hash functions produce pseudo random digest. Hence, it is assumed that the random numbers are unknown to an adversary.
- Assume $\mathcal{A}$ can launch active attacks with only part of the secret information. For example, $\mathcal{A}$ launches an attack with either a user's smart phone or his password and identity, but not both. Note that logically an IFTTT home gateway stays behind an IFTTT server, and these two entities have no motivation of cooperation to conduct any malicious activities since one is maintained by a house-owner and the other is run by a service provider. Hence, we assume $\mathcal{A}$ could either compromise an IFTTT server or impersonate an IFTTT home gateway, but not both at the same time.
- We also assume that the IFTTT home gateway and smart devices cannot be taken away by $\mathcal{A}$ since they are installed in home, but $\mathcal{A}$ can sniff the network flow and impersonate them. An IFTTT home gateway is assumed to be a trusted entity without any vulnerabilities from malicious attacks since it only connects to the designated IFTTT server with only one type of service (smart home control) via a protected mode (encrypted message).
- In developing the proposed scheme, we focus on a home gateway authenticating a remote user on behalf of the smart devices; communications between a gateway and smart devices are assumed to be secured by other schemes [16, 21, 22].

C. DESIGN GOALS

- **Full control.** By making users' own home gateways authenticate themselves in a private way, users retain full control of their Smart Homes.
- **Easy to install and transfer.** By having an IFTTT smart home gateway register to the IFTTT server via the Internet, and manage secure communications among the smart devices inside, this scheme lowers users' burden of Smart Home installation and house ownership exchange process. For Smart Home ownership exchanging, a new owner restarts a remote registration for his IFTTT home gateway and updates its users within human visual range. This way the scheme eliminates the complex and generally tedious tasks needed for the user, the home gateway, and the smart home devices.
- **Resistance to existing attacks.** Considering the possibility of a compromised user (or phone), a compromised IFTTT server, and existing network attacks from adversaries, we introduce multiple factors, such as a user's stored information (user name and password), last session key as context, nonces, utilize multi-technologies, like mutual authentication, ECC algorithm, pseudonym,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

TABLE 2: Notations

Nations	Description
S	IFTTT Server
HG_j	The jth IFTTT smart home gateway
U_i	The ith user
SP_i	The ith user's smart phone
x, P_s	IFTTT Server's ECC based private key and public key
x_j, P_{HG_j}	The jth IFTTT smart home gateway's ECC based private key and public key
uID_i	The ith user's identity
rID_j	Random number as the identity of HG_j
rC_j	Random number as the register code of HG_j
SN_j	HG_j 's preconfigured serial number.
k_{SH_j}	Session key shared between S and HG_j
k_{ij}^k	The ith user's kth key shared with HG_j, k=0,1 $\cdots$
T_i	Current timestamp, i=1,2 $\cdots$
ΔT	Maximum transmission delay
$H_1(\cdot), H_2(\cdot)$	Secure one way hash functions: $\{0,1\}^* \rightarrow \{0,1\}^k$
$E(\cdot), D(\cdot)$	Secure symmetric encryption primitive, such as AES
$m-$	Masked variable, for example, mk_{ij}^0 is masked version of k_{ij}^0

one time one session key, and keep the authenticating contents secret from the involved IFTTT server, to ensure the authentication scheme is secure against various attacks.

IV. PROPOSED SCHEME

In this section, we propose an anti-tracking mutual authentication scheme for an IFTTT-based Smart Home (see Fig. 1). We first build a secure channel between an IFTTT home gateway and the IFTTT server; then, we design a mutual authenticating protocol that allows the IFTTT home gateway and a remote user to authenticate each other aided by the IFTTT server. The IFTTT server cannot gain the authentication contents when it forwards the authenticating messages. The proposed scheme also achieves unlinkability since user accounts are not maintained in the IFTTT server, and logically the home gateway is hidden behind the IFTTT server. The proposed scheme has three phases: system initialization phase, registration phase, and authentication and key agreement phase. Notations adopted to describe the proposed protocol are listed in Table 2, the high-level registration and authentication process is shown in Fig. 2, and the details of the authentication process are showed in Table 3.

A. SYSTEM INITIALIZATION PHASE

IFTTT Server initialization: When an IFTTT Server (S) starts up, it chooses an elliptic curve E_p over a finite field F_p with a large prime number p, and a secure one-way hash function $H_1(\cdot)$. S also chooses a base point P with order n over E_p, and its private key x and computes $P_s = xP$ as its public key. And S keeps x in private, and publishes $\{p, E_p, P, P_s, n, H_1(\cdot)\}$.

IFTTT Home Gateway initialization: The home gateway (HG_j) is assumed to have been configured with public parameters $\{p, E_p, P, P_s, n, H_1(\cdot)\}$ and serial number (SN_j). When HG_j starts up, it chooses an elliptic curve E_{p_j} over a finite field F_{p_j} with a large prime number p_j, and a one-way hash function $H_2(\cdot)$. HG_j also chooses a base point P_j with order n_j and its private key x_j, and computes $P_{HG_j} = x_j P_j$ as its public key. And HG_j keeps x_j in private and stores public parameters $\{p_j, E_{p_j}, P_j, P_{HG_j}, n_j, H_2(\cdot)\}$.

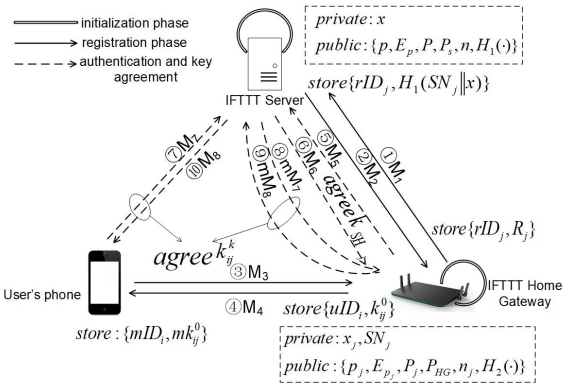


FIGURE 2: The high-level registration and authentication process.

B. REGISTRATION PHASE

The proposed scheme has two separate registration phases: home gateway registration phase and user registration phase. In the home gateway registration phase (see ①, ② in Fig. 2), an IFTTT home gateway registers to an IFTTT server to agree upon a pseudonym rID_j and the secret $H_1(SN_j||x)$; in the user registration phase (see ③, ④ in Fig. 2), a user registers to an IFTTT home gateway to configure the user identity (uID_i) and the initial authenticated session key (k_{ij}^0) within human visual range.

1) Home Gateway Registration (HGR) Phase

Step HGR1. HG_j generates random numbers rID_j, r_j and computes $mr1 = r_j P_s$ and $mr2 = r_j P$. HG_j computes $B_1 = H_1(mr1) \oplus SN_j$, $B_2 = H_1(mr1) \oplus rID_j, B_3 = H_1(mr2||SN_j||rID_j)$, then sends $M1 = \{mr2, B_1, B_2, B_3, T_1\}$ to S.

Step HGR2. S computes $mr1^* = x \cdot mr2$, and obtains SN_j^* and rID_j^* from B_1, B_2, Then it checks if $H_1(mr2||SN_j^*||rID_j^*) = B_3$ holds. If negative, then it terminates the process; otherwise, S concludes $SN_j^* = SN_j, rID_j^* = rID_j, mr1^* = mr1$, and S finds SN_j from its valid database. If SN_j exists, then S computes $B_4 = H_1(SN_j||x) \oplus SN_j \oplus rID_j \oplus mr1, B_5 = H_1(H_1(SN_j||x)||SN_j||rID_j||mr1)$ and sends $M2 = \{B_4, B_5\}$ back to HG_j. S stores rID_j as the identity of the home gateway and $H_1(SN_j||x)$ as its corresponding secret.

Step HGR3. When HG_j receives $M2$, it fetches $H_1^*(SN_j||x)$ from B_4 and then checks whether or not $H_1(H_1^*(SN_j||x)||SN_j||\ rID_j||mr1) = V_1$ holds. If positive, then HG_j gets $H_1^*(SN_j||x) = H_1(SN_j||x)$, fetches its unique hardware address MAC_j, and computes $R_j = H_1(SN_j||x) \oplus$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

$H_1(MAC_j)$; otherwise, it terminates the process. Finally, HG_j stores (rID_j, R_j).

2) User Registration (UR) Phase

Step UR1. When a user (U_i) registers to HG_j, it generates a random number rC_j as its registration code and displays it to U_i. Then it sends rID_j and the public parameters $\{p_j, E_{p_j}, P_j, P_{HG_j}, n_j, H_2(\cdot)\}$ to U_i's smart phone.

Step UR2. U_i chooses his password and username denoted as (PW_i, UN_i), and inputs PW_i, UN_i, rC_j on U_i's smart phone(SP_i) manually. Then SP_i retrieves its hardware address MAC_i and computes $w = H_2(PW_i||UN_i), u = H_2(UN_i \oplus MAC_i)$, $cp = wP_{HG_j}$, and $ep = wP_j$. SP_i computes $C_1 = u \oplus H_2(cp), C_2 = rC_j \oplus H_2(cp), C_3 = H_2(ep||u||rC_j), M_3 = \{ep, C_1, C_2, C_3\}$ and sends it to HG_j.

Step UR3. Upon receiving M_3, HG_j first computes $cp^* = x_j \cdot ep$. Then it obtains u^*, rC_j^* from C_1, C_2 and checks whether or not $H_2(ep||u^*||rC_j^*) = C_3$ holds. If negative, then the process terminates; otherwise, HG_j takes $rC_j^* = rC_j$ and $u^* = u$, then computes $uID_i = H_2(u), k_{ij}^0 = H_2(uID_i||rC_j)$, and stores $\{uID_i, k_{ij}^0\}$. At the same time, it sends $M_4 = \{H_2(uID_i||k_{ij}^0)\}$ back to SP_i.

Step UR4. Upon receiving M_4, SP_i computes uID_i, k_{ij}^0 as HG_j does, and checks M_4. If M_4 is valid, then SP_i computes $mID_i = w \oplus uID_i, mk_{ij}^0 = w \oplus k_{ij}^0$, and stores $\{mID_i, mk_{ij}^0\}$.

C. AUTHENTICATION AND KEY AGREEMENT PHASE

This process also has two separate phases: home gateway login phase and mutual authentication with key agreement phase. In the home gateway login phase (see ⑤, ⑥ in Fig. 2), an IFTTT home gateway logs onto an IFTTT server. After mutual authentication, the IFTTT home gateway and IFTTT server agree upon a session key (k_{SH_j}) and the IFTTT server marks it as online. In the mutual authentication with key agreement phase (see ⑦, ⑧, ⑨, ⑩ in Fig. 2), a user and an IFTTT home gateway perform mutual authentication via an IFTTT server, and they agree upon a new session key (k_{ij}^k) in a secret way, not only to the attackers but also to the IFTTT server. The last session key is involved in mutual authentication to prevent impersonation attack.

1) Home Gateway Login (HGL) Phase

Step HGL1. HG_j retrieves $H_1(SN_j||x)$ from R_j with $H_1(MAC_j)$, generates a random number r_j, computes $mr1 = r_jP_s, mr2 = r_jP, B_1 = H_1(mr1) \oplus rID_j, B_2 = H_1(mr1) \oplus H_1(SN_j||x), B_3 = H_1(mr2||H_1(SN_j||x)||rID_j||T_1), M_5 = \{mr2, B_1, B_2, B_3, T_1\}$, and sends M_5 to S.

Step HGL2. S first checks the timeliness of T_1 using the condition $|T_1 - T_1^*| \le \Delta T$, where the maximum transmission delay is denoted by ΔT and T_1^* is the reception time of M_5. If this condition holds, then S computes $mr1^* = x \cdot mr2$, and obtains $rID_j^*, H_1^*(SN_j||x)$ from B_1, B_2. S then checks whether or not $H_1(mr2||H_1^*(SN_j||x)||rID_j^*||T_1) = B_3$. If yes, then S gets $rID_j^* = rID_j, H_1^*(SN_j||x) = H_1(SN_j||x), mr_1^* = mr_1$, and S generates a random number r and computes $B_4 = H_1(mr1) \oplus r, B_5 = H_1(mr1||H_1(SN_j||x)||rID_j||r||T_2), k_{SH_j} = H_1(H_1(SN_j||x)||rID_j||r)$, and $M_6 = \{B_4, B_5, T_2\}$. S finally sends M_6 to HG_j and adds k_{SH_j} to its own database for this session key.

Step HGL3. HG_j checks the timeliness of T_2 via the condition $|T_2 - T_2^*| \le \Delta T$, where T_2^* is the reception time of M_6. If this condition holds, then HG_j fetches r^* and checks whether or not $H_1(mr1||H_1(SN_j||x)||rID_j||r^*||T_2) = B_5$ holds. If yes, then HG_j takes $r^* = r$, computes $k_{SH_j} = H_1(H_1(SN_j||x)||rID_j||r)$, and finally stores k_{SH_j} securely.

2) Mutual Authentication with Key Agreement (AUKA) Phase

As can be seen from the previous phases, S owns x in private and its public parameters $\{p, E_p, P, P_s, n, H_1(\cdot)\}$, and stores $\{rID_j, H_1(SN_j||x), k_{SH_j}\}$ in its database. HG_j has x_j in private and public parameters $\{p_j, E_{p_j}, P_j, P_{HG_j}, n_j, H_2(\cdot)\}$, and stores $\{uID_i, k_{ij}^0\}$ for $U_i, \{rID_j, R_j, k_{SH_j}\}$ for S, and also S's public parameters. U_i has (PW_i, UN_i) in its storage, and its SP_i stores $\{mID_i, mk_{ij}^0, rID_j\}$ and HG_j's public parameters.

This phase achieves the goal of mutual authentication with key agreement between HG_j and U_i aided by S. The authenticating messages between U_i and S are encrypted with the shared secrets between U_i and HG_j, and S just re-encrypts (or decrypts) and forwards the authentication messages and cannot trace the activities happening between U_i and HG_j. See Table 3.

Step AUKA1. U_i inputs its username (UN_i) and password (PW_i), SP_i computes $w = H_2(PW_i||UN_i)$, fetches uID_i, k_{ij}^k from $\{mID_i, mk_{ij}^k\}$ with w. SP_i generates random number r_i, and computes $c = r_i \cdot P_{HG_j}, e = r_i \cdot P_j$. Then it computes $O_1 = H_2(c) \oplus uID_i, O_2 = H_2(c) \oplus k_{ij}^k, O_3 = H_2(e||uID_i||rID_j||k_{ij}^k||T_1), M_7 = \{rID_j, e, O_1, O_2, O_3, T_1\}$ and sends M_7 to S.

Step AUKA2. S first checks the timeliness of T_1 through condition $|T_1 - T_1^*| \le \Delta T$, where the maximum transmission delay is denoted by ΔT and T_1^* is the reception time of M_7. If the condition holds, then S finds rID_j and forwards $mM_7 = \{E_{k_{SH_j}}(M_7), H_1(M_7)\}$ to HG_j.

Step AUKA3. Upon receiving mM_7, HG_j first computes $D_{k_{SH_j}}(E_{k_{SH_j}}(M_7))$ and checks $H_1(M_7)$; if it is valid, then HG_j checks the timeliness of T_1 through condition $|T_1 - T_1^{**}| \le \Delta T'$, where the maximum transmission delay is denoted by $\Delta T' (> 2\Delta T)$ and T_1^{**} is the reception time of mM_7. If this condition holds, then HG_j computes $c^* = x_j \cdot e$, and retrieves uID_i^*, k_{ij}^{k*} from O_1, O_2, and checks if $H_2(e||uID_i^*||rID_j||k_{ij}^{k*}||T_1) = O_3$ holds. If negative, then the process terminates; otherwise, HG_j takes $uID_i = uID_i^*, k_{ij}^k = k_{ij}^{k*}$ and checks if $\{uID_i, k_{ij}^k\}$ is in its valid database. If they are valid , then HG_j generates random number r_j, and computes $O_4 = H_2(c^*) \oplus r_j, O_5 = H_2(c^*||uID_i||rID_j||k_{ij}^k||r_j||T_2), M_8 = \{O_4, O_5, T_2\}$, and sends $mM_8 = \{E_{k_{SH_j}}(M_8), H_1(M_8)\}$ to S. It also computes $k_{ij}^{k+1} = H_2(uID_i||r_j||k_{ij}^k)$ and updates $k_{ij}^k = k_{ij}^{k+1}, k_{ij}^{old} = k_{ij}^k$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

TABLE 3: Proposed mutual authentication with key agreement

User(U_i)/Smart phone (SP_i) $< mID_i, mk_{ij}^k, rID_j, H_2(\cdot), P_{HG_j}, P_j >$	IFTTT Server (S) $< rID_j, k_{SH_j}, H_1(\cdot) >$	IFTTT Home Gateway (HG_j) $< uID_i, k_{ij}^k, k_{SH_j}, H_1(\cdot), H_2(\cdot) >$
Input PW_i, UN_i. Compute $w = H_2(PW_i \| UN_i)$, $uID_i = w \oplus mID_i$, $k_{ij}^k = w \oplus mk_{ij}^k$ generate r_i, and compute $c = r_i \cdot P_{HG_j}$, $e = r_i \cdot P_j$, $O_1 = H_2(c) \oplus uID_i$, $O_2 = H_2(c) \oplus k_{ij}^k$, $O_3 = H_2(e \| uID_i \| rID_j \| k_{ij}^k \| T_1)$, $M_7 = \{rID_j, e, O_1, O_2, O_3, T_1\}$ Send M_7 to S. $\longrightarrow$ (via open channel)	Check if $\|T_1 - T_1^*\| \le \Delta T$? If so, retrieve k_{SH_j} with rID_j. Compute $mM_7 = \{E_{k_{SH_j}}(M_7), H_1(M_7)\}$ Send mM_7 to HG_j. $\longrightarrow$ (via open channel)	Compute $M_7' = D_{k_{SH_j}}(E_{k_{SH_j}}(M_7))$, Cheek $H_1(M_7') = H_1(M_7)$? If so, check $\|T_1 - T_1^{**}\| \le \Delta T'$? If so, compute $c^* = x_j \cdot e$, $uID_i^* = O_1 \oplus H_2(c^*)$, $k_{ij}^{k*} = O_2 \oplus H_2(c^*)$. Check if $H_2(e \| uID_i^* \| rID_j \| k_{ij}^{k*} \| T_1) = O_3$? If so, $uID_i = uID_i^*, k_{ij}^k = k_{ij}^{k*}$ Check if uID_i, k_{ij}^k in its valid database? If so, generate r_j, Compute $O_4 = H_2(c^*) \oplus r_j$, $O_5 = H_2(c^* \| uID_i \| rID_j \| k_{ij}^k \| r_j \| T_2)$, $M_8 = \{O_4, O_5, T_2\}$, $k_{ij}^{k+1} = H_2(uID_i \| r_j \| k_{ij}^k)$. Updates $k_{ij}^k = k_{ij}^{k+1}, k_{ij}^{old} = k_{ij}^k$, $\longleftarrow$ Send $mM_8 = \{E_{k_{SH_j}}(M_8), H_1(M_8)\}$ to S. (via open channel)
Check if $\|T_2 - T_2^{**}\| \le \Delta T'$? If so, compute $r_j^* = O_4 \oplus H_2(c)$. Check $H_2(c \| uID_i \| rID_j \| k_{ij}^k \| r_j^* \| T_2) = O_5$? If so, $c = c^*, r_j^* = r_j$ Compute $k_{ij}^{k+1} = H_2(uID_i \| r_j \| k_{ij}^k)$, Update $k_{ij}^k = k_{ij}^{k+1}$.	Compute $M_8' = D_{k_{SH_j}}(E_{k_{SH_j}}(M_8))$, Check $H_1(M_8') = H_1(M_8)$? If so, check $\|T_2 - T_2^*\| \le \Delta T$? $\longleftarrow$ If so, forward M_8 to SP_i. (via open channel)	

Step AUKA4. S computes $D_{k_{SH_j}}(E_{k_{SH_j}}(M_8)$, gets M_8 and checks $H_1(M_8)$. If it holds, then S checks the timeliness of T_2 through condition $|T_2 - T_2^*| \le \Delta T$, where T_2^* is the reception time of mM_8. If the condition holds, then S forwards M_8 to SP_i.

Step AUKA5. SP_i first checks the timeliness of T_2 through condition $|T_2 - T_2^{**}| \le \Delta T'$, where T_2^{**} is the reception time of M_8. If the condition holds, then SP_i fetches r_j^* from M_8 with $H_2(c)$ from O_4, and checks whether or not $H_2(c \| uID_i \| rID_j \| k_{ij}^k \| r_j^* \| T_2) = O_5$. If yes, then SP_i takes $c = c^*, r_j^* = r_j$, computes $k_{ij}^{k+1} = H_2(uID_i \| r_j \| k_{ij}^k)$, and updates $k_{ij}^k = k_{ij}^{k+1}$. Finally, SP_i computes $mID_i = w \oplus uID_i, mk_{ij}^k = w \oplus k_{ij}^k$, and updates $\{mID_i, mk_{ij}^k\}$. At this point, the mutual authentication with key agreement procedure finishes and SP_i sends remote control messages or receives responses from HG_j directly with k_{ij}^k.

V. SECURITY ANALYSIS

In this section, we prove that the proposed scheme can withstand the following known attacks.

A. USER ANONYMITY

Proof. In the proposed scheme, on the one hand, the IFTTT Server (S) does not maintain any user's (U_i) identity database. On the other hand, suppose the adversary $\mathcal{A}$ eavesdrops the messages $\{rID_j, e, O_1, O_2, O_3, T_1\}$ and $\{O_4, O_5, T_2\}$ from public channel, but O_1 varies for each authentication, and the space complexity of O_1 is $O(2^{160})$ taking the hash digest with 160 bits in length into consideration. O_4, O_5 are nonce-embedded messages and rID_j is the IFTTT Home Gateway's (HG_j) pseudo-identity, $\mathcal{A}$ cannot map rID_j to a specific U_i, or map rID_j to a specific home gateway IP address. Therefore, the proposed scheme provides the user anonymity.

B. TRACEABILITY

Proof. As mentioned above, $\mathcal{A}$ can sniff the channel and gather $\{rID_j, e, O_1, O_2, O_3, T_1\}, mM_8, mM_7$, and $\{O_4, O_5, T_2\}$, but $\mathcal{A}$ cannot trace U_i or locate HG_j. Firstly, mM_8, mM_7 are encrypted messages between S and HG_j. Thus $\mathcal{A}$ cannot distinguish the current pair of $U_i \leftrightarrow HG_j$ since a single S serves a huge number of HG_j. Secondly, S only maintains the logged-on HG_j's pseudo-identity without embedded user information and the only user identity related O_1 varies during each authentication, $\mathcal{A}$ cannot trace user and locate HG_j. Thus, the proposed scheme prevents U_i and HG_j from being traced by the attacker.

C. STOLEN SMART PHONE ATTACK

Proof. Suppose the smart phone SP_i of U_i is lost or stolen by an adversary $\mathcal{A}$. $\mathcal{A}$ can extract all information $\{rID_j, mID_i, mk_{ij}^0, p_j, E_{p_j}, P_j, P_{HG_j}, n_j, H_2(\cdot)\}$ stored in SP_i. Noting that $w = H_2(PW_i \| UN_i), uID_i = w \oplus mID_i, k_{ij}^k = w \oplus mk_{ij}^k$, to correctly retrieve uID_i, k_{ij}^k, $\mathcal{A}$ needs to know both UN_i and PW_i. In the proposed scheme, both the UN_i and PW_i are of 128 bits long and are chosen randomly by a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

user. Consequently, the space complexity of UN_i and PW_i as a whole is $O(2^{256})$; it is computationally infeasible for $\mathcal{A}$ to guess. Therefore, the proposed scheme is secure against such an attack.

D. USER IMPERSONATION ATTACK

Proof. Assuming that an adversary $\mathcal{A}$ has the correct UN_i and PW_i and that he obtains rID_j by sniffing the network. $\mathcal{A}$ tries to impersonate a legitimate user (U_i) to launch the authentication protocol. $\mathcal{A}$ must provide the correct uID_i, k_{ij}^k to HG_j, but it is impossible without (U_i)'s phone. In addition, even if $\mathcal{A}$ obtains the correct uID_i with brute-force, he still fails to follow the dynamically changing k_{ij}^k since the legitimate user updates it each session. Consequently, the scheme resists user impersonation attack.

E. MUTUAL AUTHENTICATION

Proof. In our scheme, HG_j authenticates U_i by verifying if $uID_i = uID_i^*, k_{ij}^k = k_{ij}^{k*}$ hold, and U_i authenticates HG_j by verifying if $c = c^*, r_j^* = r_j$ hold. In addition, when HG_j logs onto S, S authenticates HG_j by verifying if $rID_j^* = rID_j, H_1^*(SN_j||x) = H_1(SN_j||x)$ hold, and HG_j authenticates S by verifying if $r^* = r, mr1^* = mr1$ hold. Consequently, the proposed scheme achieves mutual authentication.

F. DESYNCHRONIZATION ATTACK

Proof. Updating the session keys by both the user (U_i) and the home gateway (HG_j) may cause desynchronization. In the proposed scheme, HG_j first verifies U_i and updates their session key. If $\mathcal{A}$ intercepts M_8 or mM_8 and drops them, then it will not introduce desynchronization error since HG_j stores both the new session key $k_{ij}^k = k_{ij}^{k+1}$ and the old session key $k_{ij}^{old} = k_{ij}^k$. Then U_i can restart the authentication procedure and pass the verification with k_{ij}^{old}. This shows that the proposed scheme is safe from desynchronization attacks.

G. PERFECT FORWARD SECURITY

Proof. Assuming that the private key x_j of HG_j is compromised, and that the adversary $\mathcal{A}$ obtains k_{ij}^k, k_{ij}^{old}, $\mathcal{A}$ cannot fetch the random number r_j and k_{ij}^{old-2} in the previous session since it is not stored anywhere. Thus $\mathcal{A}$ cannot compute the correct $k_{ij}^{old-1} = H_2(uID_i||r_j||k_{ij}^{old-2})$. Further, assuming that the adversary $\mathcal{A}$ also obtains U_i's PW_i, UN_i and calculates the correct uID_i, k_{ij}^k, but he still has no way to recover any of the correct keys $\{k_{ij}^0, k_{ij}^1, \ldots, k_{ij}^{k-2}\}$. Accordingly, the proposed scheme achieves a perfect forward security.

H. REPLAY ATTACK

Proof. If $\mathcal{A}$ simply replays $M_7 = \{rID_j, e, O_1, O_2, O_3, T_1\}$ with nothing modified, then S first uses the maximum delay time ΔT to check if T_1 in a valid time-limit. If it fails, then $\mathcal{A}$ fails; otherwise, if $\mathcal{A}$ fortunately passes the check, then HG_j checks T_1 again with $\Delta T'$. Thus $\mathcal{A}$ hardly has a chance to attack with practical $\Delta T, \Delta T'$. Even if $\mathcal{A}$ passes the second check, he cannot calculate the correct session key without c, uID_i, k_{ij}^k. Moreover, even if $\mathcal{A}$ replays $M_7 = \{rID_j, e, O_1, O_2, O_3, T_1\}$ by modifying $T_1^\sharp$ to pass the twice time-limit checks, he cannot pass the check $H_2(e||uID_i^*||rID_j||k_{ij}^{k^*}||T_1^\sharp) = O_3$. Thus, our scheme is resistant to a replay attack.

I. COMPROMISED IFTTT SERVER ATTACK

Proof. Consider a scenario where the IFTTT Server is compromised by an adversary $\mathcal{A}$, who tries to track U_i's activity and gather U_i's remote control commands (or S itself is curious about U_i while abiding by the protocol). In our scheme, firstly, the mutually authenticated session key between U_i and HG_j is unknown to S. Secondly, when U_i launches a new authentication procedure via S, he provides nothing about U_i's identity information but HG_j's pseudo-identity rID_j, which is a random number. Thirdly, after finishing the authentication, remote control commands that U_i sends to HG_j are encrypted by the new session key, and are also unknown to S. Accordingly, the proposed scheme ensures U_i's privacy and the security of remote access to smart home system under a compromised IFTTT server attack.

J. HOME GATEWAY IMPERSONATION ATTACK

Proof. Suppose an adversary $\mathcal{A}$ gets the valid rID_j through sniffing the network. He then tries to impersonate a legitimate IFTTT home gateway (HG_j) to log onto S and perform attacks. $\mathcal{A}$ can easily get S's public parameters $\{p, E_p, P, P_s, n, H_1(\cdot)\}$; however, he has to fetch $H_1(SN_j||x)$. Note that $R_j = H_1(SN_j||x) \oplus H_1(MAC_j)$. So $H_1(SN_j||x)$ is stored as a masked value and it is impossible to fetch it without cracking the hardware of HG_j. In other words, the proposed scheme has a good resistance to the home gateway impersonation attack.

VI. SECURITY PROOF WITH BAN-LOGIC AND SCYTHER

This section analyzes the security of the proposed scheme with Burrow *et al.* [35] BAN-logic and the Scyther tool [40]. We prove that the proposed scheme allows the user to securely establish a session key with the IFTTT home gateway.

A. BAN LOGIC NOTATIONS AND POSTULATES

Suppose that A & B are symbols for principals, X & Y are symbols of statements, P and P_s are the symbols of an elliptic curve base point and the public key, respectively. The logic notations of BAN-logic are listed in Table 4.

The BAN-logic postulates used in this scheme are as follows:

R1: Message-meaning rule1: $\frac{A|\equiv \stackrel{P,P_s}{\longrightarrow} B, A|\sim \ll y \diamond P \gg, A \triangleleft (<< y \diamond P_s \gg)_X}{A|\equiv B|\sim X}$. That is, if A believes that B has P as a base point and P_s as a public key of an elliptic curve, and A sends the result of y multiplied by P, and receives the result of X XOR the hashed $\ll y \diamond P_s \gg$, then A believes B once said X.

TABLE 4: BAN-Logic notations

Symbol	Description
$A\|\equiv X$	*A believes a statement X*
$A \triangleleft X$	*A receives X .*
$A\|\sim X$	*A sends X .*
$\mathrm{A} \Rightarrow \mathrm{X}$	*A controls X .*
$\xrightarrow{P,P_s} A$	*A has P_s as a public key and P as* a base point of an elliptic curve
$\sharp(\mathrm{X})$	*X is fresh .*
$A \overset{X}{\longleftrightarrow} B$	*X is a secret known only to A and B .*
$\ll x \diamond P \gg$	A number x multiplies a point P in an elliptic curve.
$(X)_Y$	X XOR Y .
[X,Y]	X attaches Y .
< X >	*X is hashed .*

R2: Message-meaning rule2: $\frac{A \triangleleft \ll y \diamond P \gg, A \triangleleft (<\ll y \diamond P_s \gg>)_{A \overset{X}{\longleftrightarrow} B}}{A|\equiv B|\equiv A \overset{X}{\longleftrightarrow} B}$. That is, A receives the result of y multiplied by P as well as the result of X XOR the hashed $\ll y \diamond P_s \gg$, where X is a secret known only to A and B, then A believes that B trusts the fact that A and B share X.

R3: Nonce-verification rule: $\frac{A|\equiv\sharp(X), A|\equiv B|\sim X}{A|\equiv B|\equiv X}$. That is, if A believes the freshness of X and that B once said X, then A believes that B trusts X.

R4: Deducing rule1: $\frac{A|\equiv B|\equiv X, A|\equiv A \overset{Y}{\longleftrightarrow} B}{A|\equiv B|\equiv A \overset{<[X,Y]>}{\longleftrightarrow} B}$. That is, if A believes that B trusts X, and that Y is the secret known only to A and B, then A believes that B trusts that A and B share the hashed value of $[X, Y]$. Alternatively, the rule can be: $\frac{A|\equiv\sharp(X), A|\equiv B|\equiv A \overset{Y}{\longleftrightarrow} B, B|\equiv A|\sim X}{A|\equiv B|\equiv A \overset{<[X,Y]>}{\longleftrightarrow} B}$. That is, if A believes the freshness of X, and A believes B trusts that Y is the secret known only to A and B, and also B believes A sends X, then A believes B trusts that A and B share the hashed value of $[X, Y]$.

R5: Deducing rule2: $\frac{A|\equiv B \Rightarrow X, A|\equiv A \overset{Y}{\longleftrightarrow} B}{A|\equiv B \Rightarrow <[X,Y]>}$. That is, if A believes that B controls X, and that Y is the secret known only to A and B, then A believes that B controls the hashed value of $[X, Y]$.

R6: Jurisdiction rule: $\frac{A|\equiv B \Rightarrow X, A|\equiv B|\equiv X}{A|\equiv X}$. That is, if A believes that B controls X, and A believes that B trusts X, then A believes X.

R7: Believe rule: $\frac{A|\equiv\sharp(X), A|\equiv A \overset{Y}{\longleftrightarrow} B, A|\equiv B|\equiv A \overset{Y}{\longleftrightarrow} B}{A|\equiv A \overset{<[X,Y]>}{\longleftrightarrow} B}$. That is, if A believes the freshness of X, and that Y is the secret known only to A and B, and A believes B trusts that A and B share Y, then A believes that A and B share the hashed value of $[X, Y]$.

B. SECURITY PROOF WITH BAN-LOGIC

For convenience, let U, H be denoted as U_i, HG_j respectively; let k, SNX be denoted as the shared key k_{SH_j} and $H_1(SN_j||x)$ between HG_j and S; and let nsk, osk be denoted as k_{ij}^k, k_{ij}^{old} between U_i and HG_j; and also let P_s, P_H be denoted as S's public key and HG_j's public key.

The proposed scheme has two login phases: HG_j logs onto S and U_i logs onto HG_j via S. Each of them executes the key agreement process, and the latter phase (U_i's) is based on the session key of HG_j's login. To make the description more clear, we first combine HG_j's login phase and U_i's login phase to one formalized scheme. We also simplify U_i's login messages by not explicitly describing the messages sent by S, since S only executes encryption or decryption and forwards messages with the session key shared with HG_j. The key elements of messages are idealized without including the timestamps, since their checks do not affect the proof. To highlight the key points, we adopt the same symbol <> for $H_1(\cdot), H_2(\cdot)$ and r_j for HG_j's random number in the two login phases. Although they have the same symbol, they are used in different session without introducing chaos.

The formalized idealized scheme together with the security goals are described next. Initial premises are provided before the proof procedure.

Formalized Idealized Scheme:

With the above BAN-Logic notations, we formalize and idealize M5, M6, M7 and M8 in Fig. 2 into Message1, Message2, Message3 and Message4, respectively, without including the timestamps. Also we introduce two symbols for the shared secrets for simplicity.

Message1: $H \rightarrow S : \ll r_j \diamond P \gg, (<\ll r_j \diamond P_s \gg>)_{rID_j}, (<\ll r_j \diamond P_s \gg>)_{SNX}, <\ll r_j \diamond P \gg ||SNX||rID_j>$

Message2: $S \rightarrow H : (<\ll x \diamond r_j \diamond P \gg>)_r, < x \ll x \diamond r_j \diamond P \gg ||SNX||rID_j||r >$

Message3: $U \rightarrow S \rightarrow H : rID_j, \ll r_i \diamond P_j \gg, (<\ll r_i \diamond P_H \gg>)_{uID_i}, (<\ll r_i \diamond P_H \gg>)_{osk}, <\ll r_i \diamond P_j \gg ||uID_i||rID_j||osk >$

Message4: $H \rightarrow S \rightarrow U : (<\ll x_j \diamond r_i \diamond P_j \gg>)_{r_j}, <\ll x_j \diamond r_i \diamond P_j \gg ||uID_i||rID_j||osk||r_j >$

Symbol1: $k =< [SNX, rID_j, r] >$

Symbol2: $nsk =< [uID_i, r_j, osk] >$

Security Goals:

If the proposed scheme is secure, then both S and H believe that they negotiate and share k after authentication, and both U and H believe that they negotiate and share nsk after authentication. The goals with BAN-Logic notations are as follows.

Goal1 . $H| \equiv S| \equiv H \overset{k}{\leftrightarrow} S$

Goal2 . $H| \equiv H \overset{k}{\leftrightarrow} S$

Goal3 . $S| \equiv H| \equiv H \overset{k}{\leftrightarrow} S$

Goal4 . $S| \equiv H \overset{k}{\leftrightarrow} S$

Goal5. $U| \equiv H| \equiv U \overset{nsk}{\leftrightarrow} H$

Goal6. $U| \equiv U \overset{nsk}{\leftrightarrow} H$

Goal7. $H| \equiv U| \equiv U \overset{nsk}{\leftrightarrow} H$

Goal8. $H| \equiv U \overset{nsk}{\leftrightarrow} H$

Initial premises:

The parameters at the system initialization and registration phases are summarized and formalized into the following initial premises with BAN-Logic notations.

A1: $H| \equiv \xrightarrow{P,P_s} S$

A2: $H| \equiv H \overset{SNX,rID_j}{\longleftrightarrow} S$

A3: $S| \equiv H \overset{SNX),rID_j}{\longleftrightarrow} S$

A4: $S| \equiv \sharp(r)$

A5: $H| \equiv \mathrm{S} \Rightarrow r$

A6: $U| \equiv \xrightarrow{P_j,P_H} H$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

A7: $U| \equiv U \overset{uID_i,osk}{\longleftrightarrow} H$
A8: $H| \equiv U \overset{uID_i,osk}{\longleftrightarrow} H$
A9: $H| \equiv \sharp(r_j)$
A10: $U| \equiv H \Rightarrow r_j$

Using BAN-Logic rules, we prove that H and S successfully share a common session key k and that U and H securely negotiate a common new session key nsk.

S1. Message1 shows that H sends $\ll r_j \diamond P \gg$ to S, that is $H| \sim\ll r_j \diamond P \gg$. Message2 shows that H receives the message $(<\ll x \diamond r_j \diamond P_j \gg>)_r$. According to ECC algorithm, we have $\ll x \diamond r_j \diamond P \gg = \ll r_j \diamond P_s \gg$, thus we get $H \triangleleft (<\ll r_j \diamond P_s \gg>)_r$. With A1, we use R1 to obtain

$$H| \equiv S| \sim r.$$

S2. S1, A4, and R3 lead to the result:

$$H| \equiv S| \equiv r.$$

S3. From S2, A2, and R4, we obtain

$$H| \equiv S| \equiv H \overset{<[SNX,rID_j,r]>}{\longleftrightarrow} S,$$

and with Symbol1, we have:

$$H| \equiv S| \equiv H \overset{k}{\leftrightarrow} S \ (Goal1).$$

In other words, the IFTTT home gateway believes that the IFTTT server trusts the secret k between them.

S4. From A5, A2 and Symbol 1, using R5 we have:

$$H| \equiv S \Rightarrow k.$$

S5. From S4 and Goal1, with R6, we have:

$$H| \equiv H \overset{k}{\leftrightarrow} S. \ (Goal2)$$

This means that the IFTTT home gateway believes the secret k is shared with the IFTTT server.

S6. From Message1, A2, A3, we obtain:

$$S \triangleleft \ll r_j \diamond P \gg, S \triangleleft (<\ll r_j \diamond P_s \gg>)_{H \overset{SNX,rID_j}{\longleftrightarrow} S}.$$

S7. From S6 and R2, we have:

$$S| \equiv H| \equiv H \overset{SNX,rID_j}{\longleftrightarrow} S.$$

S8. S1, S7, A4, together with R4 and Symbol1 lead to:

$$S| \equiv H| \equiv H \overset{k}{\leftrightarrow} S \ \ (Goal3).$$

In other words, the IFTTT server believes that the IFTTT home gateway trusts the secret k between them.

S9. From S7, A4, A3, with R7 and Symbol1, We have :

$$S| \equiv H \overset{k}{\leftrightarrow} S \ \ (Goal4),$$

which means that the IFTTT server believes the secret k is shared with the IFTTT home gateway.

S10. Message3 shows that U sends $\ll r_i \diamond P_j \gg$ to H, that is $U| \sim\ll r_i \diamond P_j \gg$. Message4 shows that U receives $(<\ll x_j \diamond r_i \diamond P_j \gg>)_{r_j}$. According to ECC algorithm, We have $\ll x_j \diamond r_i \diamond P_j \gg = \ll r_i \diamond P_H \gg$, thus we get $U \triangleleft (<\ll r_i \diamond P_H \gg>)_{r_j}$. With A6, we use R1 to obtain

$$U| \equiv H| \sim r_j.$$

S11. S1, A9, and R3 lead to:

$$U| \equiv H| \equiv r_j.$$

S12. From S11, A7 and R4, we obtain:

$$U| \equiv H| \equiv U \overset{<[uID_i,osk,r_j]>}{\longleftrightarrow} H,$$

and with Symbol2, we have:

$$U| \equiv H| \equiv U \overset{nsk}{\leftrightarrow} H \ \ (Goal5).$$

In other words, the user believes that the IFTTT home gateway trusts the secret nsk between them.

S13. From A10, A7 and Symbol2, by using R5, we obtain:

$$U| \equiv H \Rightarrow nsk.$$

S14. From S13 and Goal1, with R6, we have:

$$U| \equiv U \overset{nsk}{\leftrightarrow} H \ \ (Goal6),$$

which means that the user believes the secret nsk is shared with the IFTTT home gateway.

S15. From Message3, A7, A8, we can obtain:

$$H \triangleleft \ll r_i \diamond P_j \gg, H \triangleleft (<\ll r_i \diamond P_H \gg>)_{U \overset{uID_i,osk}{\longleftrightarrow} H}.$$

S16. From S15 and R2, we have:

$$H| \equiv U| \equiv H \overset{uID_i,osk}{\longleftrightarrow} U.$$

S17. From S10, S16, A9, with R4 and Symbol2, we get:

$$H| \equiv U| \equiv U \overset{nsk}{\leftrightarrow} H \ \ (Goal7).$$

In other words, the IFTTT home gateway believes that the user trusts the secret nsk between them.

S18. From S16, A9, A8, with R7 and Symbol2, We have:

$$H| \equiv U \overset{nsk}{\leftrightarrow} H, \ \ (Goal8)$$

which means that the IFTTT home gateway believes the secret nsk is shared with the user.

C. SECURITY PROOF WITH SCYTHER

In this section, the Scyther tool is applied to perform a formal analysis of the proposed model. Scyther is an automatic security protocol verification tool, commonly used to identify potential attacks and vulnerabilities. It has been used to verify numerous security protocols. Here the Scyther tool is used to evaluate the following properties of proposed scheme: secrecy, replay attack resistance, man-in-the-middle attack resistance, and reflection attack resistance. Since the user registration protocol is securely performed using a face-to-face method, the Scyther tool is used to evaluate the other three protocols: home gateway registration protocol, home gateway login protocol, and mutual authentication with key agreement protocol.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

Fig. 3 illustrates the results obtained from Scyther's analysis of the home gateway registration protocol. The results clearly show that home gateway registration in the proposed scheme is secure.

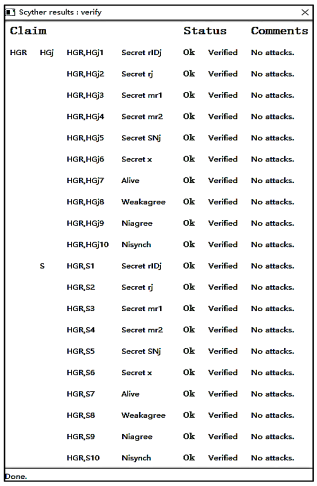


FIGURE 3: Analysis results using Scyther tool for home gateway registration protocol.

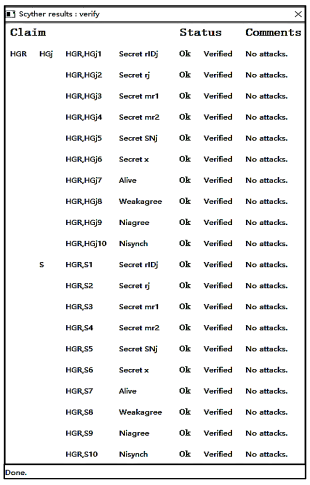
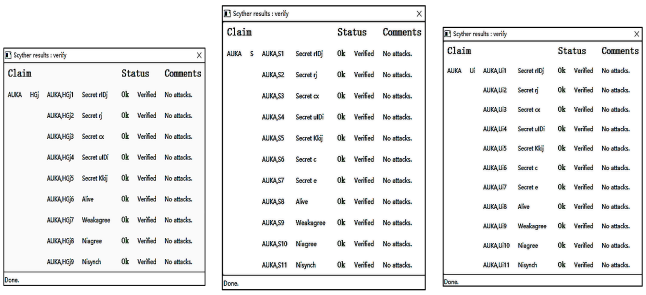


FIGURE 4: Analysis results using Scyther tool for home gateway login protocol.

Results from Scyther analysis of home gateway login protocol between the IFTTT home gateway and the IFTTT server are shown in Fig. 4. No attacks were observed.

Scyther is finally used to analyze the mutual authentication with key agreement protocol between the user and the IFTTT home gateway via the IFTTT server, and the results are shown in Fig. 5. These results show that Scyther has not found any weaknesses or potential attacks against the proposed scheme.



(a) AUKA-HG_j (b) AUKA-S (c) AUKA-U_i

FIGURE 5: Analysis results using Scyther tool for mutual authentication with key agreement protocol.

We repeated the Scyther verification twenty times, using both the manually defined claims and Scyther's automatically generated claims, and the results remained the same. The Scyther testing codes are provided in the Appendices.

VII. PERFORMANCE COMPARISON

In our proposed system model, the scheme without the security techniques follows the same three phases: system initialization phase, registration phase and authentication phase. However, it stores and checks the user name and password directly, which takes negligible computational time compared with the proposed scheme.

In this section, the proposed scheme is compared with related schemes: Baruah *et al.* [5], Wazid *et al.* [14], Jeong *et al.* [31], Vaidya *et al.* [20], and Zhang *et al.* [24] during the authentication and key agreement phase. Since the system initialization and registration phases are not frequent, the costs involved in these phases are not discussed. The computational costs are shown in in Table 5. Similar notations as used by Wazid *et al.* [14] are adopted here: $T_h, T_E/T_D, T_{fe}, T_{P_a}, T_{P_m}, T_{mac}$ denote, respectively, the computational time for hash function (using SHA-1 hashing algorithm), symmetric encryption/decryption, a fuzzy extractor, an elliptic curve point addition, an elliptic curve point multiplication, and message authentication code (MAC). It is also assumed that the bitwise XOR operation time is negligible, and is thus not considered as part of the performance parameters. Parameters used in the experiments [14,33,34] are: $T_h = T_{mac} = 0.32ms, T_{fe} = T_{P_m} = 17.1ms$, and $T_E/T_D = 5.6ms$. Based on the results in [36], one elliptic curve point addition is nearly 11.7 times faster than one elliptic curve point multiplication; thus, $T_{P_a} = 1.46ms$. The scheme by Baruah *et al.* [5] adopts totally different computation. Thus, in the comparison, the computation time published in [5] will be used. The computational cost of the proposed scheme is higher than that of the schemes developed by Wazid *et al.* [14], Jeong *et al.* [31], ad Vaidya *et al.* [20], because we introduce the ECC algorithm to enhance security. Since the added computation is required on a user's phone and home gateway which has sufficient computational resources, it is still practical to implement. The three-party authentication in the proposed scheme is faster than Zhang *et al.* [24]'s scheme, which is designed for two parties based on ECC.

The communication cost of various existing schemes and the proposed scheme are compared in Table 6. Similar assumptions to the ones made in [14] are adopted here: the identities are of 128-bit long; random nonces are 128 bits; elliptic curve points are 128 bits; timestamps are 32 bits; a plaintext/ciphertext block in symmetric encryption/decryption (using AES-CBC algorithm) is 128 bits, and the hash digest is 160 bits. Since the schemes by Jeong *et al.* [31], and Vaidya *et al.* [20] need to connect a third party to get an authenticated ticket and use it to connect the home gateway to prove and fetch services, it is better to include the ticket proving process. Specifically, in our scheme, messages of the authentication phase are $M_7 = \{rID_j, e, O_1, O_2, O_3, T_1\}, M_8 = \{O_4, O_5, T_2\}, mM_7 = \{E_{kS_{H_j}}(M_7), H_1(M_7)\}, mM_8 = \{E_{kS_{H_j}}(M_8), H_1(M_8)\}$. The costs of $O_1 \sim O_5$ are 160 bits; thus M_7, M_8, mM_7 and mM_8 are 896 bits, 352bits, 1056bits, and 512bits, respectively. As a result, the total communication cost of our scheme turns out to be (896+352+1056+512)=2816 bits. Note that both the two-party authentication scheme by Zhang *et al.* [24], and the proposed scheme adopt the ECC algorithm. Our proposed scheme has higher communication cost because

TABLE 6: Comparison of communication cost

Auth. scheme	Total message	Total cost (bits)
Baruah *et al.* [5]	5	241K
Wazid *et al.* [14]	4	3232
Jeong *et al.* [31]	4	2464
Vaidya *et al.* [20]	5	3524
Zhang *et al.* [24]	2	896
Ours	4	2816

a third party is introduced to enhance security and privacy (see Table 7). Our scheme has a higher communication cost than the schemes by Jeong *et al.* [31] because we need extra masking information to resist the attack from the involved compromised third party (the IFTTT server).

TABLE 7: Comparison of security and privacy features

	Baruah *et al.* [5]	Wazid *et al.* [14]	Jeong *et al.* [31]	Vaidya *et al.* [20]	Zhang *et al.* [24]	Ours
SF1	N	Y	N	N	Y	Y
SF2	Y	Y	N	N	Y	Y
SF3	Y	Y	Y	Y	N	Y
SF4	Y	Y	Y	Y	Y	Y
SF5	Y	Y	Y	Y	Y	Y
SF6	-	N	-	N	Y	Y
SF7	Y	Y	N	Y	Y	Y
SF8	Y	Y	Y	Y	Y	Y
SF9	N	N	N	N	-	Y
SF10	N	Y	Y	Y	-	Y

Note: SF1: provides user anonymity; SF2: provides un-traceability; SF3: resists stolen smart phone attack; SF4: resists user impersonation attack; SF5: provides mutual authentication; SF6: resists desynchronization attack; SF7: provides perfect forward security; SF8: resists replay attack; SF9: resists compromised server attack; SF10: resists home gateway impersonation attack.

The security and privacy features of of the proposed and existing schemes are compared in Table 7. The scheme by Baruah *et al.* [5] does not provide user anonymity and cannot resist the compromised server attack and the home gateway impersonation attack. The scheme by Wazid *et al.* [14] is vulnerable to the desynchronization attacks and compromised server attacks. Both the schemes by Jeong *et al.* [31] and Vaidya *et al.* do not provide a user with anonymity and untraceability, and are also insecure to compromised server attacks. The scheme by Jeong *et al.* [31] does not achieve perfect forward security and the scheme by Vaidya *et al.* [20] is vulnerable to desynchronization attacks. The scheme by Zhang *et al.* [24] achieves more security and privacy features than the above schemes, but it lacks a way to prevent a stolen smart phone attack. Overall, the proposed scheme provides better security and privacy than existing schemes.

VIII. CONCLUSION

We have presented an IFTTT-based smart home system model and an anti-tracking mutual authentication scheme in this paper. The proposed system model keeps an IFTTT home gateway behind the IFTTT server logically and authenticates a remote user independently. The proposed registration procedure facilitates users to securely configure smart homes, especially in the house ownership exchanging process. The authentication protocol combines multiple factors: user's memory (password), previous session key, serial number and hardware address of the home gateway, to mutually verify the actual communication entities. It achieves anonymity and untraceability aided by the ECC algorithm and nonces. Security analysis, proof of BAN-logic and result of Sytcher tool show that our scheme achieves better security and privacy than existing schemes. Performance comparison result reveals that the proposed scheme is suitable for implementation in practice.

ACKNOWLEDGEMENT

The authors would like to acknowledge Profs. S. Li and M. Xu, Drs. T. Cui and M. Gao for their useful discussions and suggestions. This work was supported by the 2018 Discipline Construction of Zhejiang Provincial Key University Cyberspace Security (No. GK188800225009), the cyberspace security Major Program in National Key Research and Development Plan of China under grant No. 2016YFB0800201, Natural Science Foundation of China under grant No. 61572165, 61702150 and 61803135, the State Key Program of Zhejiang Province Natural Science Foundation of China under grant No. LZ15F020003, the Key Research and Development Plan Project of Zhejiang Province under grant No. 2017C01065 and 2017C01062, and the Scientific Research fund of Zhejiang Provincial Education Department under grant No.Y201737924.

REFERENCES

[1] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges", *Future Generation Computer Systems,* vol. 82, pp. 395-411, 2018.

[2] Michael Shanler, "Predicts 2015: The Rise of Digital R&D Innovation for Manufacturers", Available: https://www.gartner.com/doc/2941518?ref=SiteSearch\&sthkw=a\%20typical\%20family\%20home\%20could\%20contain\%20more\%20than\%20500\%20smart\%20devices\%20by\%202022\%2C\&fnl=search\&srcId=1-3478922254.

[3] Katherine Albrecht, Liz Mcintyre "Privacy Nightmare: When Baby Monitors Go Bad" *IEEE Technology and Society Magazine*, vol. 34, no. 3, pp.14-19, 2015.

[4] Brian Barret, "Hack Brief: Hacker Strikes Kids' Gadget Maker VTech

TABLE 5: Comparison of computational cost

Auth. scheme	User or client	HG or device or server	Third party	Total cost	Total time
Baruah *et al.* [5]	0.00098ms	80.02ms	0.00465ms	-	80.026ms
F Wazid *et al.* [14]	$9T_h + 1T_D + 1T_{fe}$	$5T_h + 1T_D$	$8T_h + 2T_E$	$22T_h + 4T_E/T_D + T_{fe}$	46.54ms
Jeong *et al.* [31]	$4T_h + 3T_D/T_E$	$1T_h + 3T_E/T_D$	$6T_h + 2T_E$	$11T_h + 8T_E/T_D$	48.3ms
Vaidya *et al.* [20]	$10T_h + T_D$	$4T_H + 1T_D$	$6T_h + 2T_E$	$20T_H + 4T_E/T_E$	28.8ms
Zhang *et al.* [24]	$2T_{pm} + 1T_{Pa} + 3T_H + 2T_{mac}$	$3T_{pm} + 1T_{Pa} + 4T_H + 2T_{mac}$	-	$5T_{pm} + 2T_{Pa} + 7T_H + 4T_{mac}$	91.94ms
Ours	$6T_h + 2T_{pm}$	$4T_H + 2T_E/T_D + 1T_{pm}$	$2T_H + 2T_E/T_D$	$12T_H + 3T_{pm} + 4T_E/T_D$	77.54ms

Note:$T_H = T_{mac}$*= 0.32ms,* $T_{fe} = T_{pm}$*=17.1ms,* T_E/T_D *=5.6ms, and* T_{Pa}*=1.46ms.*

to Steal 5 Million Accounts", Available: https://www.wired.com/2015/11/vtech-childrens-gadget-maker-hack-5-million-accounts/.

[5] B. Baruah and S. Dhal, "A Two-factor Authentication Scheme Against FDM Attack in IFTTT Based Smart Home System," *COMPUTERS & SECURITY*, vol. 77, pp. 21-35, 2018.

[6] "Smart Home Market by Product (Lighting Control, Security & Access Control, HVAC, Entertainment, Smart Speaker, Home Healthcare, Smart Kitchen, Home Appliances, and Smart Furniture), Software & Services, and Region - Global Forecast to 2024" Available: https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html. Accessed in January,2019.

[7] B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes", *Sensors*, vol. 18, pp. 1-17, 2018.

[8] Q. Do, B. Martini, K.-K. R. Choo, "Cyber-physical Systems Information Gathering: A Smart Home Case Study," *Computer Networks,* vol. 138, pp. 1-12, 2018.

[9] B.-C. Chifor, I. Bica, V.-V. Patriciu, F. Pop, "A Security Authorization Scheme for Smart Home Internet of Things devices," *Future Generation Computer Systems*, vol. 82, pp. 740-749, 2018.

[10] J. Shen, C. Wang, T. Li *et al.*, "Secure Data Uploading Scheme for A Smart Home System," *Information Sciences,* vol. 453, pp. 186-197, 2018.

[11] G. - J. Ra and I. - Y. Lee, "A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments," *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, vol. 12, no. 2, pp. 892-905, Feb. 2018.

[12] Y. Ashibani, Q. H. Mahmoud, "An Efficient and Secure Scheme for Smart Home Communication using Identity-Based Signcryption," in Proc. IEEE 36TH INTERNATIONAL PERFORMANCE COMPUTING AND COMMUNICATIONS CONFERENCE (IPCCC), 2017.

[13] V. Sivaraman, H. Habibi, Gharakheili *et al.*, "Smart IoT Devices in the Home Security and Privacy Implications" *IEEE TECHNOL AND SOCLETY MAGAZINE*, pp. 71-79, Jun. 2018.

[14] M. Wazid, A. k. Das, V. Odelu *et al.*, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," *IEEE Transactions on Dependable and Secure Computing,* pp. 1-15, 2017.

[15] A. Coskun, G. Kaner, I. Bostan, "Is Smart Home a Necessity or a Fantasy for the Mainstream User? A Study on Users' Expectations of Smart Household Appliances," *International Journal of Design*, vol. 12, no. 1, pp. 7-20, 2018.

[16] T. Song, R. Li, B. Mei, J. Yu *et al.*, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," *IEEE INTERNET OF THINGS JOURNAL,* vol. 4, no. 6, pp. 1844-1852, Dec. 2017.

[17] D. Dolev and A. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory,* vol. 29, no. 2, pp. 198-208, 1983.

[18] Available: http://IFTTT.com.

[19] M. Wazid, A. K. Das, V. Odelu *et al.*, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks," *IEEE INTERNET OF THINGS JOURNAL.* vol. 5, no. 1, pp. 269-282, Feb. 2018.

[20] Binod Vaidya, Jong Hyuk Park, "Robust One-time Password Authentication Scheme Using Smart Card for Home Network Environment," *IEEE Computer Communications,* vol. 34, no. 2011, pp. 326-33, 2011.

[21] Pardeep Kumar, Andrei Gurtov,etc., "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," *IEEE Sensors Journal*, vol.16, no.1, pp. 254-264, 2016.

[22] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous Secure Framework in Connected Smart Home Environments," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* vol. 12, no. 4, pp. 968-979, Apr. 2017.

[23] S.S Leong ,Nicholas C.H.Vun, "Design and Implementation of an Authentication Protocol For Home Automation Systems," *IEEE Trans on Consumer Electronics,* vol. 44,no. 3,pp. 911-921, 1998.

[24] W Zhang, D Lin, H Zhang, C Chen, X Zhou, "A Lightweight Anonymous Mutual Authentication with Key Agreement Protocol on ECC", in Proc. of 2017 IEEE Trustcom/BigDataSE/ICESS.2017.

[25] J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity Based IoT Device Authentication," in Proc. IEEE INFOCOM - IEEE Conference on Computer Communications, 2017.

[26] M. Alaa, A. A. Zaidan, B. B. Zaidan *et al.*, "A Review of Smart Home Applications Based on Internet of Things," *Journal of Network and Computer Applications,* vol. 97, pp. 48-65, 2017.

[27] Sunwoo Kim, Jeonghyuk Yoon, "An Exploratory Study on Consumer's Needs on Smart Home in Korea", *DUXU 2016*, Part III, LNCS 9748, pp. 337-345, 2016.

[28] A. Burrows, D. Coyle,and R. G.-Hill, "Privacy, Boundaries and Smart Homes for Health: An Ethnographic Study," *Health & Place,* ,vol. 50, pp. 112-118, 2018.

[29] E. Park, S. Kim, Y. S. Kim, S. J. Kwon, "Smart Home Services as the Next Mainstream of the ICT Industry: Determinants of the Adoption of Smart Home Services," *Univ Access Inf Soc,* vol. 17, pp. 175-190, 2018.

[30] S. U. Rehman and V. Gruhn, "An Approach to Secure Smart Homes in CyberPhysical Systems/Internet-of-Things," in Proc.Fifth International Conference on Software Defined Systems (SDS), pp. 126-129, 2018.

[31] J. Jeong, M.Y. Chung, H. Choo, "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks," in Proc. 41st Annual Hawaii International Conference on System Sciences (HICSS'08), 2008.

[32] E. Tsui, W.M. Wang and Farzad Sabetzadeh, "Enacting Personal Knowledge Management & Learning With Web Services Interoperability Tools," in Proc. IEEE CCIS, pp. 492-494, 2014.

[33] D. He, N. Kumar, J. H. Lee, and R. S. Sherratt, "Enhanced Three Factor Security Protocol for Consumer USB Mass Storage Devices," *IEEE Transactions on Consumer Electronics,* vol. 60, no. 1, pp. 30-37, 2014.

[34] C. C. Lee, C. T. Chen, P. H. Wu, and T. Y. Chen, "Three-factor Control Protocol Based on Elliptic Curve Cryptosystem for Universal Serial Bus Mass Storage Devices," *IET Computers & Digital Techniques,* vol. 7, pp. 48-55, 2013.

[35] M.Burrow, M.Abadi, R.Needham, "A Logic of Authentication," *ACM Trans. Comput. SYst*, vol. 8, no. 1, pp. 18-36, 1990.

[36] S. QIU, G. XU, H. AHMAD and L. WANG, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," *IEEE Access,* vol. 6, pp. 7452-7463, 2018.

[37] Swati Khandelwal, "Uh oh, Yahoo! Data Breach May Have Hit Over 1 Billion Users," Accessed on: Sep. 30, 2016, [Online]. Available: https://thehackernews.com/2016/09/yahoo-data-breach-billion.html.

[38] Lee Mathews, "Equifax Data Breach Impacts 143 Million Americans," Accessed on: Sep. 7, 2017, [Online]. Available: https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#fb01eee356f8.

[39] Seung Lee, "Facebook: 87 million users affected by Cambridge Analytica data collection," Accessed on: Apr. 4, 2018, [Online]. Available: https://www.mercurynews.com/2018/04/04/facebook-87-million-users-affected-by-cambridge-analytica-data-collection/.

[40] C. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols", in Proc. CAV-20th International Conference on Computer Aided Verification, pp. 414-418, 2008.

APPENDICES:

Algorithm 1 code of Scyther for the home gateway registration protocol

```
hashfunction H1;
usertype Timestamp;

protocol HGR(HGj,S){
    role HGj{
        fresh rIDj : Nonce;
        fresh rj : Nonce;
        fresh mr1 : Nonce;
        fresh mr2 : Nonce;
        fresh SNj : Nonce;
        fresh x : Nonce;

        fresh B1 : Function;
        fresh B2 : Function;
        fresh B3: Function;
        fresh B4 : Function;
        fresh B5: Function;
        fresh M1: Function;
        fresh M2: Function;
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access


```
        fresh Ts : Timestamp;

        send_1(HGj, S, mr2, B1(H1(mr1), SNj),
B2(H1(mr1),rIDj), B3(H1(mr2), SNj, rIDj), TsM1(S));
        recv_2(S, HGj, B4(H1(SNj, x),SNj, rIDj, m-
r1),B5(H1(SNj, x),SNj, rIDj, mr1)M2(HGj));

        claim(HGj,Secret,rIDj);
        claim(HGj,Secret,rj);
        claim(HGj,Secret,mr1);
        claim(HGj, Secret, mr2);
        claim(HGj,Secret,SNj);
        claim(HGj,Secret,x);
        claim(HGj,Alive);
        claim(HGj,Weakagree);
        claim(HGj,Niagree);
        claim(HGj,Nisynch);
    };

    role S {
        fresh rIDj : Nonce;
        fresh rj : Nonce;
        fresh mr1 : Nonce;
        fresh mr2 : Nonce;
        fresh SNj : Nonce;
        fresh x : Nonce;

        fresh B1 : Function;
        fresh B2 : Function;
        fresh B3: Function;
        fresh B4 : Function;
        fresh B5: Function;
        fresh M1: Function;
        fresh M2: Function;

        fresh Ts : Timestamp;

        recv_1(HGj, S, mr2, B1(H1(mr1), SNj),
B2(H1(mr1), rIDj), B3(H1(mr2), SNj,rIDj), TsM1(S));
        send_2(S, HGj, B4(H1(SNj, x), SNj, rIDj, mr1),
B5(H1(SNj, x), SNj, rIDj, mr1)M2(HGj));

        claim(S, Secret, rIDj);
        claim(S, Secret, rj);
        claim(S, Secret, mr1);
        claim(S, Secret, mr2);
        claim(S, Secret, SNj);
        claim(S, Secret, x);
        claim(S, Alive);
        claim(S, Weakagree);
        claim(S, Niagree);
        claim(S, Nisynch);
    };
};
```

Algorithm 2 code of Scyther for the home gateway login protocol

```
hashfunction H1;
usertype Timestamp;

protocol HGL(HGj,S){
    role HGj{
        fresh rIDj : Nonce;
        fresh rj : Nonce;
        fresh mr1 : Nonce;
        fresh mr2 : Nonce;
        fresh SNj : Nonce;
        fresh x : Nonce;
        fresh r : Nonce;

        fresh B1 : Function;
        fresh B2 : Function;
        fresh B3: Function;
        fresh B4 : Function;
        fresh B5: Function;
        fresh M5: Function;
        fresh M6: Function;

        fresh Ts : Timestamp;

        send_1(HGj, S, mr2, B1(H1(mr1), rIDj),
B2(H1(mr1), H1(SNj, x)), B3(H1(mr2,H1(SNj, x), T-
s))M5(S));
        recv_2(S, HGj, B4(H1(mr1), r), B5(H1(mr1,
H1(SNj, x), rIDj, r, Ts), Ts)M6(HGj));

        claim(HGj,Secret,rIDj);
        claim(HGj,Secret,rj);
        claim(HGj,Secret,mr1);
        claim(HGj,Secret,mr2);
        claim(HGj,Secret,SNj);
        claim(HGj,Secret,x);
        claim(HGj,Secret,r);
        claim(HGj,Alive);
        claim(HGj,Weakagree);
        claim(HGj,Niagree);
        claim(HGj,Nisynch);
    };

    role S {
        fresh rIDj : Nonce;
        fresh rj : Nonce;
        fresh mr1 : Nonce;
        fresh mr2 : Nonce;
        fresh SNj : Nonce;
        fresh x : Nonce;
        fresh r : Nonce;

        fresh B1 : Function;
        fresh B2 : Function;
```

```
            fresh B3: Function;
            fresh B4 : Function;
            fresh B5: Function;
            fresh M5: Function;
            fresh M6: Function;

            fresh Ts : Timestamp;

            recv_1(HGj, S, mr2, B1(H1(mr1), rIDj), B2(H1(mr1), H1(SNj, x)), B3(H1(mr2, H1(SNj, x), T-s))M5(S));
            send_2(S, HGj, B4(H1(mr1), r), B5(H1(mr1, H1(SNj,x), rIDj, r, Ts), Ts)M6(HGj));

            claim(S,Secret,rIDj);
            claim(S,Secret,rj);
            claim(S,Secret,mr1);
            claim(S,Secret,mr2);
            claim(S,Secret,SNj);
            claim(S,Secret,x);
            claim(S,Secret,r);
            claim(S,Alive);
            claim(S,Weakagree);
            claim(S,Niagree);
            claim(S,Nisynch);
        };
};
```

Algorithm 3 code of Scyther for the mutual authentication with key agreement protocol

```
hashfunction H1;
hashfunction H2;
usertype Timestamp;

protocol AUKA(HGj,S,Ui){
    role HGj{
        fresh rj : Nonce;
        fresh cx : Nonce;
        fresh uIDi : Nonce;
        fresh rIDj : Nonce;
        fresh Kkij : Nonce;
        fresh EKSHi : Function;
        fresh O4: Function;
        fresh O5: Function;
        fresh M7: Function;
        fresh mM7: Function;
        fresh mM8: Function;

        fresh Ts : Timestamp;

        recv_2(S, HGj, EKSHi(M7), H1(M7), Tsm-M7(HGj));
        send_3(HGj, S, EKSHi(O4(H2(cx), rj), O5(H2(cx, uIDi, rIDj, Kkij, rj, Ts)), Ts),H1(O4(H2(cx), rj), O5(H2(cx, uIDi, rIDj, Kkij, rj, Ts)), Ts)mM8(S));

        claim(HGj,Secret,rIDj);
        claim(HGj,Secret,rj);
        claim(HGj,Secret,cx);
        claim(HGj,Secret,uIDi);
        claim(HGj,Secret,Kkij);
        claim(HGj,Alive);
        claim(HGj,Weakagree);
        claim(HGj,Niagree);
        claim(HGj,Nisynch);
    };

    role S{
        fresh rIDj : Nonce;
        fresh uIDi : Nonce;
        fresh c : Nonce;
        fresh e : Nonce;
        fresh Kkij : Nonce;
        fresh rj : Nonce;
        fresh cx : Nonce;

        fresh O1 : Function;
        fresh O2 : Function;
        fresh O3: Function;
        fresh O4: Function;
        fresh O5: Function;
        fresh mM8: Function;
        fresh EKSHi : Function;
        fresh mM7: Function;
        fresh M7: Function;
        fresh M8: Function;
        fresh Ts : Timestamp;

        recv_1(Ui, S, rIDj, e, O1(H2(c), uIDi), O2(H2(c), Kkij), O3(H2(e, uIDi, rIDj, Kkij, Ts))M7(S));
        send_2(S, HGj, EKSHi(M7), H1(M7), Tsm-M7(HGj));
        recv_3(HGj, S, EKSHi(O4(H2(cx), rj), O5(H2(cx, uIDi, rIDj, Kkij, rj, Ts)), Ts), H1(O4(H2(cx), r-j),O5(H2(cx,uIDi,rIDj,Kkij,rj,Ts)), Ts)mM8(S));
        send_4(S, Ui, O4(H2(cx), rj), O5(H2(cx, uIDi, rIDj, Kkij, rj, Ts)), TsM8(Ui));

        claim(S,Secret,rIDj);
        claim(S,Secret,rj);
        claim(S,Secret,cx);
        claim(S,Secret,uIDi);
        claim(S,Secret,Kkij);
        claim(S,Secret,c);
        claim(S,Secret,e);
        claim(S,Alive);
        claim(S,Weakagree);
        claim(S,Niagree);
        claim(S,Nisynch);
    };

    role Ui{
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2907602, IEEE Access

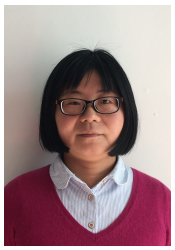

```
            fresh rIDj : Nonce;
            fresh uIDi : Nonce;
            fresh c : Nonce;
            fresh e : Nonce;
            fresh Kkij : Nonce;
            fresh cx : Nonce;
            fresh rj : Nonce;

            fresh O1 : Function;
            fresh O2 : Function;
            fresh O3: Function;
            fresh O4 : Function;
            fresh O5: Function;
            fresh M7: Function;
            fresh M8: Function;

            fresh Ts : Timestamp;

            send_1(Ui, S, rIDj, e, O1(H2(c), uIDi),
O2(H2(c), Kkij), O3(H2(e, uIDi, rIDj, Kkij, Ts))M7(S));
            recv_4(S, Ui, O4(H2(cx), rj), O5(H2(cx, uIDi,
rIDj, Kkij, rj, Ts)), TsM8(Ui));

            claim(Ui,Secret,rIDj);
            claim(Ui,Secret,rj);
            claim(Ui,Secret,cx);
            claim(Ui,Secret,uIDi);
            claim(Ui,Secret,Kkij);
            claim(Ui,Secret,c);
            claim(Ui,Secret,e);
            claim(Ui,Alive);
            claim(Ui,Weakagree);
            claim(Ui,Niagree);
            claim(Ui,Nisynch);
      };
};
```



QIUYUN LYU is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China. She received the bachelor's and master's degrees from Chang'an University, in 2000 and 2003, respectively. She is an associate professor of the School of Cyberspace, Hangzhou Dianzi University. Her current research interests include privacy enhancing technology, authentication protocol.

NING ZHENG is the vice president of Hangzhou Dianzi University, Hangzhou, China. He has authored over 70 referred journal and conference papers. His research interests are privacy enhancing information management system and network information security.

HUAPING LIU received the B.S. and M.S. degrees in electrical engineering from Nanjing University of Posts and Telecommunications, Nanjing, China, in 1987 and 1990, respectively, and the Ph.D. degree in electrical engineering from New Jersey Institute of Technology, Newark, Since September 2001, he has been with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, where he is currently a professor. His research interests include privacy enhancing technology in communication systems and multiuser communications.

CAN GAO is currently pursuing the bachelor's degree with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China. Her research interests are authentication, privacy and smart homes.

SI CHEN is currently pursuing the master's degree with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing, China. Her research interests are identity authentication, privacy protection and smart homes.

JUNLIANG LIU is an expert in security department of MoreSec. Tech. Inc., Hangzhou, China. His current research interests include protocol security analysis, privacy enhancing technology, authentication protocol design.