Cloud-Aided Privacy Preserving User Authentication and Key Agreement Protocol for Internet of Things

Chenyu Wang[1], Ding Wang[2], Haowei Wang[2],
Guoai Xu[1],Jing Sun[1], Huaxiong Wang[3]

[1] Beijing University of Posts and Telecommunications
[2] Peking University
[3] Nanyang Technological University
xga@bupt.edu.cn, corresponding author

Abstract. With the exponential growth of interconnected devices, Internet of Things has played an indispensable part of our modern life. However, the constraint of the devices greatly limits the development of IoT and has become one of the major bottlenecks for the large-scale deployment of the devices. Cloud computing, as a technique for the analysis and storage of a large amount of heterogeneity data, is a key solution to this. However, the integrating of IoT and cloud computing also brings new security and privacy challenge. Therefore, an authentication mechanism must be provided to verify user's identity and ensure the data be accessed without authorization.However, we found most of the authentication schemes for IoT do not truly integrate the cloud computing thus are not suitable for IoT. To improve this unsatisfactory condition, we depicted the architecture of the cloud-assisted IoT environment, and for the first time designed a new secure and privacy preserving user authentication scheme for cloud-assisted IoT environment. Furthermore, we compared the proposed scheme with several related schemes from security functions and performance, the result showed the superiority of our scheme.

Keywords: Multi-factor user authentication, Internet of Things, Cloud Computing.

1 Introduction

Internet of Things (IoT) is a dynamic and global network with self configuring interconnected objects. It aims to let the things be able to be measured, connected, communicated and understood, and then further to make decisions or self-regulation intelligently. IoT is one of the most influential technologies and will play an important role in our further life without doubt. Internet of Things will digitize the real world and have a wide range of applications, like smart home, smart city, video surveillance and smart grid. According to [8], the number of the interconnected devices even exceeded the number of people

in 2011. Furthermore, this number was estimated to be 9 billion in 2012, and will reach the value of 24 billions by 2020 [3]. With the popularization of the interconnected devices, Internet of Things is bound to be one of the most essential techniques of our inter-connected world. Certainly, cloud computing, as a model for enabling ubiquitous, convenient, on-demand network to access to a shared configurable computing resources [16], is regarded as the most appropriate technology which can collaborate with IoT to maximize benefits of the both sides. The basic principle of cloud computing is to make the computation finished across a large number of distributed computers via virtualization technology. Therefore, cloud computing has become a promising technique for the future of information technology industry.

Consequently, integrating IoT and cloud computing has become an inevitable trend, many researchers have been devoted into it [1, 3, 9]. To IoT, cloud computing compensate its storage and computation constraints via providing virtually unlimited storage space and capabilities, furthermore, cloud computing can maximize the data collected from IoT to rich the services for users; to cloud computing, IoT extends its scope and perception of the real world via providing a large amount of data. The integrating of IoT and cloud computing will greatly improve the applications in smart city, smart home, environmental monitoring and smart grid.

However, we also should note the integrating of IoT and cloud computing brings benefits as well as new security challenges. In cloud computing environment, people already worry about their personal information being acquired by the third party or adversary with ulterior motives. When integrating IoT, such concerns on privacy protection will be more prominent since IoT brings the data from the real world to the cloud and more actions can be performed in the real world. Therefore, preventing the data from unauthorized access means a lot to user's privacy protection. Among the security measures, user authentication, as the first line to the security of the system, has attracted more and more attentions. Considering such an occasion where a user wants to access the data collected from the smart device directly, for example, the user wants to know his/her heartbeats from the wearable device, a more effective and secure method to achieve this is that the user and the smart device authenticate each other and then negotiate a session key to encrypt the communication with the help of cloud center and the gateway. The aim of the paper is to provide a secure authentication scheme for this occasion.

1.1 Related Works

In 2009, Das et al. [4] for the first time presented a smart card based user authentication scheme for real-time data access for wireless sensor network, while this scheme was shortly identified that it is vulnerable to serious security flaws [11, 12, 20] including offline dictionary attack, insider attack and impersonation attack. Since then, many authentication schemes for wireless sensor network are proposed [6, 10, 17, 21], while most of them have unsatisfactory aspects more or less. For example, Fan et al.'s scheme [6] cannot provide user anonymity and

forward secrecy; Jiang et al.s scheme [10] does not achieve forward secrecy too. Furthermore, these schemes more focus on wireless sensor network (the part of IoT), rather than take the whole big network (IoT) into consideration. Thus most of these schemes are not suitable for IoT.

Recently, with the prevalence of the idea of IoT, more and more user authentication schemes for IoT are presented. For example, in 2016, Farash et al. [7] introduced a user authentication and key agreement scheme for heterogeneous wireless sensor network for IoT, while their scheme then was found insecure against offline dictionary attack, no user anonymity and forward secrecy; in 2017, Wu et al. [27] also designed a temporary certificate based authentication scheme for IoT which suffers from impersonation attack, offline dictionary attack and no forward secrecy; in 2018, Wazid et al. [25] then presented a lightweight scheme for IoT again and proved it security with formal provable security, but unfortunately, their scheme is not secure against offline dictionary attack, no user anonymity and forward secrecy. Note that most schemes [5,14,19] including the above schemes though claimed to be designed for IoT environment, only have three participants: the user, the gateway and the sensor nodes, thus have many limitations and are not suitable for IoT environment according to our introduction above.

Among these authentication schemes for IoT, only a limited number of schemes evolve the cloud computing, for example, in 2018, Amin et al. [2] identified the importance of integrating of IoT and cloud computing and proposed an authentication scheme, while they not only cannot withstand various attacks, but also does not involve IoT elements; similar situation also happens on Shen et al.'s scheme [18]; in 2017, Wazid et al. [26] proposed a remote user authentication scheme for smart home environment with formal security proof, since the smart home is an important application of IoT, their scheme also can be regard as the one for IoT. Furthermore, in their scheme, a register server evolves which takes a part task of cloud center and can be reviewed as the cloud center directly when considering the cloud-assisted IoT environment. Therefore, we chose their scheme as a study case to explain the role of the cloud center in user authentication and identify challenges in the design of the scheme for cloud-assisted IoT environment.

In conclusion, from the related work of the remote multi-factor user authentication schemes for cloud-assisted IoT environment, we can see that: 1) designing a secure authentication scheme for IoT environment is difficult; 2) the authentication scheme for cloud-assisted IoT environment still lacks.

1.2 Motivations and Contributions

On one hand, the integrating of IoT and cloud computing enables a large number of application scenarios, and has been a foreseen trend. On the other hand, this new architecture also brings new security challenges, especially in privacy protection. User authentication as the first line of security is bound to attract many attentions. However, when reviewing the history of user authentication protocol for IoT or cloud computing related environment, it can be seen

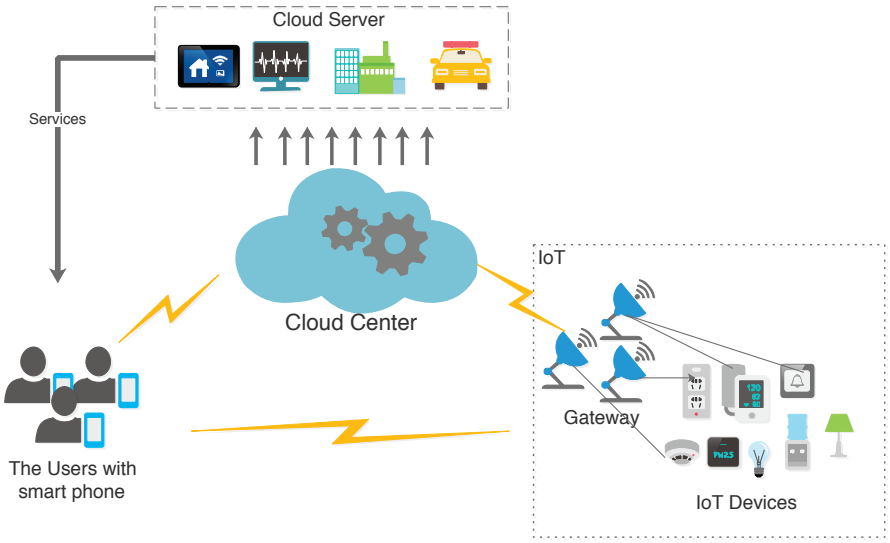

Fig. 1. Illustration of Cloud-assisted IoT architecture

that most of schemes are only designed for either cloud or IoT environment. Several schemes designed for the cloud-assisted IoT usually do not maximize the advantage of cloud computing, for example, the cloud center in their scheme just acts as a register center, and does not join in authentication process. In this case, the bottleneck of IoT in communication and computation cost still exists. To change this unsatisfactory situation, we first clearly depict the architecture of the cloud-assisted IoT environment, then for the first time propose a truly privacy preserving user authentication scheme for cloud-assisted IoT environment. In short, our contributions are summarized as follows:

1). Firstly, we depict the architecture of the cloud-assisted IoT environment, including the communication model of the user authentication.
2). Then, we for the first time design a truly secure and privacy preserving user authentication scheme for cloud-assisted IoT environment.
3). Finally, we analyze the security of the proposed scheme and compare it with several related schemes from security functions and performance, the result shows the superiority of our scheme.

1.3 The Organization of the Paper

The rest of the paper is organized as follows. Section II describes the system architecture and communication model; In Section III, we firstly review a recent scheme, then demonstrate the scheme suffers from many serious attacks; to provide a secure authentication scheme suitable for the IoT environment, we design a new scheme based on elliptic curve algorithm; its security and

performance analysis are given in Section IV and V, respectively. Finally, Section VI concludes the whole paper.

2 SYSTEM OVERVIEW

In this section, we provide an introduction to the cloud-aided Internet of Things environment. Note that the notations and abbreviations are described in Table 1. As shown in Fig. 1, the cloud-assisted IoT system may include four participants representing different stakeholders. The IoT consists of quantities of smart devices such as smart doorbells, smart locks and some gateways. The smart devices collect various data from the environment and can interconnect to each other to finish a common goal. The gateway is responsible for lightweight data processing, and it also collects data from the smart devices and upload them to the cloud center. Then the cloud center will do a series of complicated computations on the data from the real world to get some useful findings. Furthermore, based on these findings, the cloud center can also help the server provider to offer better and more precise services to the users.

Usually, the users do not communicate with the IoT network directly. Once the users want to access a certain resource, he/she can get the information from the cloud center. Furthermore, to enjoy the service provided by the cloud server, the users also only need to authenticate with the cloud center or the cloud server, without IoT networks. However, considering such a scenario, where the users want to know the real-time data from the smart devices, such as his/her heartbeats, then it is inefficient and impossible to get these data from cloud center, since the smart devices usually upload the data within certain time interval. Under this situation, to ensure the user can securely access the data, it is necessary to let the user and the target smart device authenticate each other, and negotiate a secret session key. Then the user and the smart device can transmit sensitive information with the session key securely. Note that, we recommend to let the cloud center join in this authentication since it can greatly alleviate the storage and computation load of the gateway (even the smart devices). If the cloud center does not join in the authentication and just acts as a register center, then to verify the legitimation of the user, the gateway has to store some information related to the user and do more computation to finish the authentication, which will limit the scale of the IoT networks. Therefore, an ideal authentication process in the scenario mentioned above is: firstly, the user initiates an access request to the cloud center; secondly, the cloud center verifies the legitimation of the user, and forwards the request to the gateway; thirdly, the gateway authenticates the cloud center, then transmits the message to the target smart devices; fourthly, the smart devices verify the gateway and give a response to it; fifthly, the gateway checks the response and gives it to the cloud center; sixthly, after testing the response, the cloud center transmits it to the user; seventhly, the user verifies the response and computes the session key shared with the smart device to finish the authentication successfully.

Table 1. Notations and Abbreviations

Symbol	Description	Symbol	Description
U_i	i^{th} user	x/y	secret key of $CloCen$
S_j	j^{th} sensor node	X_{S_j}	secret key of GWN for S_j
x_{G_k}	secret key of GWN_k	X_{G_k}	secret key of CC for GWN_k
GWN_k	k^{th} gateway	K_{GWN-U_i}	secret key of GWN for U_i
$CloCen.$	the cloud center	K_{GWN-S_j}	secret key of GWN for S_j
$\mathcal{A}$	the adversary	$\oplus$	bitwise XOR operation
SK	the session key	$\rightarrow$	a common channel
ID_i	identity of U_i	$\Longrightarrow$	a secure channel
SID_j	identity of S_j	$h(\cdot)$	one-way hash function
GID_j	identity of S_j	$Gen(\cdot)/Rep(\cdot)$	fuzzy extractor
PW_i/Bio_i	password/biometrics of U_i	$\|$	concatenation operation

3 PROPOSED SCHEME

According to our analysis in Section 2, making the cloud center join in the authentication benefits improving the performance and network capacity of the system. While in some schemes like [26], the cloud center (register center) only is responsible for registering, or rather, assigning some parameters to other participants, which almost does not take the advantages of cloud computing. Therefore, these schemes are not so suitable for the further smart home environment with larger-scale smart devices. To present a more suitable communication framework and overcome the identified weaknesses, we propose a new enhanced user authentication scheme which is a cloud-assisted Internet of Things network with larger-scale smart devices. In our scheme, the cloud center acts as the trust bridge among the other three participants and undertake most complicated computations. For security consideration, to provide truly multi-factor security, we follows Wang et al.'s suggestion [22] to deploy a public key algorithm; to achieve forward secrecy, we let the sensor node do two elliptic curves point multiplication [15]; and since temporary certificate based schemes usually have desynchronization attack, we adopt the public key algorithm to achieve the similar function like user anonymity. All in all, our scheme is processed as follows:

3.1 Smart device and Gateway Registration Phase

Since we consider the As we mentioned before, in practice, the gateway and the sensor nodes may be provided by a company, and the cloud center may be provided by another company. In this network, the gateway acts as an interface between the wireless sensor networks and the internet. Therefore, on one hand, the cloud center should distribute a secret key to the gateway as their authenticated credentials; on the other hand, the gateway and the sensor nodes should keep their own secret key to stop their data from unauthorized access by the third party (the cloud center). Similarly, for the security consideration, we let the cloud center own two secret keys (x and y), one for the users, the other for the gateways. Furthermore, our scheme is built on an elliptic curve E

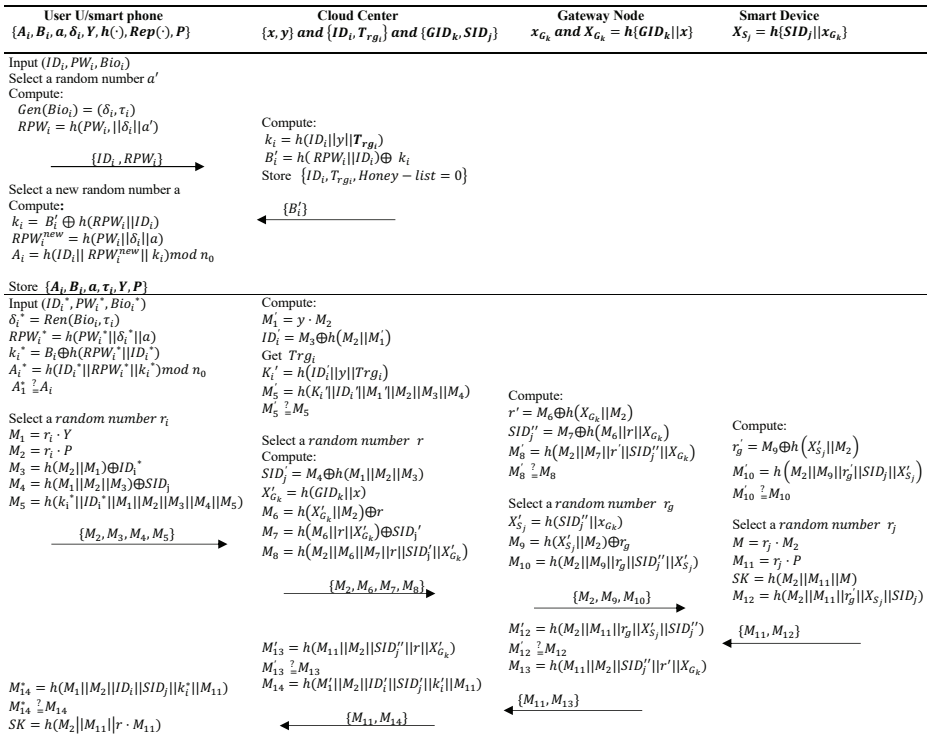

Fig. 2. The User Registration and Authentication Phase of the Proposed Scheme

(generated by P with a large prime order q) over prime finite field F_p, the public key $Y = yP$. Accordingly, in our scheme, the smart device and the gateway can register to the cloud-assisted Internet of Things system as follows:

The gateways register to the cloud center:

Step 1. $GWN_k \Longrightarrow CloCen$: registration request.
Step 2. $CloCen \Longrightarrow GWN_k$: $\{GID_k, X_{G_k} (= h(GID_k||x))\}$.
Step 3. GWN_k keeps $X_{G_k} = h(x||GID_k)$.

The smart device register to the gateway as follows:

Step 1. $S_j \Longrightarrow GWN_k$: registration request.
Step 2. $GWN_k \Longrightarrow S_j$: $\{SID_j, X_{S_j} = h(SID_j||x_{G_k})\}$, where x_{G_k} is the secret key of the gateway.
Step 3. S_j keeps $X_{S_j} = h(SID_j||x_{G_k}$.

3.2 User Registration Phase

Step 1. $U_i \Longrightarrow CloCen$: $\{ID_i, RPW_i\}$.
U_i selects its identity ID_i and password PW_i, enters the biometric Bio_i, then the smart phone computes: $Gen(Bio_i) = (\delta_i, \tau_i)$, $RPW_i = h(PW_i||\delta_i||a')$, where a' is a random number chosen by the phone.

Step 2. $CloCen \Longrightarrow U_i$: $\{A_i, B_i, Y, n_0, h(\cdot), Gen(\cdot)\}$.
The cloud center first picks the timestamps T_{rg_i}, computes $k_i = h(ID_i||y||T_{rg_i})$, $B_i' = h(RPW_i||ID_i) \oplus k_i$, and stores $\{ID_i, T_{rg_i}, Hoeny-list = NULL\}$.

Step 3. the smart phone selects a new random number a to avoid privilege insider attack, and computes: $k_i' = B_i' \oplus h(RPW_i||ID_i)$, $RPW_i^{new} = h(PW_i||\delta_i||a)$, $A_i = h(ID_i||RPW_i^{new}||k_i) \bmod n_0$, $B_i = h(RPW_i^{new}||ID_i) \oplus k_i$, keeps $\{A_i, B_i, a, \tau_i, Y, n_0, h(\cdot), Rep(\cdot)\}$ in its database.

3.3 Login Phase

Step 1. $U_i \longrightarrow CloCen$: $\{M_2, M_3, M_4, M_5\}$.
U_i inputs $\{ID_i^*, PW_i^*, Bio_i^*\}$, the smart phone computes: $\delta_i^* = Rep(Bio_i^*, \tau_i)$, $RPW_i^* = h(PW_i^*||\delta_i^*||a)$, $k_i^* = B_i \oplus RPW_i^*$, $A_i^* = h(ID_i^*||RPW_i^*||k_i^*) \bmod n_0$, then verifies U_i via comparing A_i^* with A_i. If they are not equal, the smart phone rejects the request, otherwise, selects a random number, and computes: $M_1 = r_iY$, $M_2 = r_iP$, $M_3 = h(M_2||M_1) \oplus ID_i^*$, $M_4 = h(M_1||M_2||M_3) \oplus SID_j$, $M_5 = h(k_i^*||ID_i^*||M_1||M_2||M_3||M_4)$.

3.4 Authentication Phase

1. $CloCen \longrightarrow GWN_k$: $\{M_2, M_6, M_7, M_8\}$.
The cloud center first do some computations to checks the valid of U_i: computes $M_1' = yM_2$, $ID_i' = M_3 \oplus h(M_2||M_1')$, retrieves T_{rg_i} with the computed ID_i', and continue computes $k_i = h(ID_i'||y||T_{rg_i})$, $M_5' = h(k_i'||ID_i'||M_1'||M_2||M_3||M_4)$, then authenticates the user U_i with M_5'.
If $M_5' \neq M_5$, the cloud center thinks U_i is an adversary, thus rejects the session, and sets $Honey-list = Honey-list+1$, once $Honey-list$ exceeds a preset value (such as 10), suspends U_i's account; otherwise, computes $SID_j' = M_4 \oplus h(M_1||M_2||M_3)$, and according to SID_j selects corresponding gateway GWN_k, computes $X_{G_k}' = h(x||GID_k)$, $M_6 = h(X_{G_k}'||M_2) \oplus r$, $M_7 = h(M_6||r||X_{G_k}') \oplus SID_j'$, $M_8 = h(M_2||M_6||M_7||r||SID_j'||X_{G_k}')$, where r is a random number chosen by $CloCen$.
2. $GWN_k \longrightarrow S_j$: $\{M_2, M_9, M_{10}\}$.
The gateway first computes $r' = M_6 \oplus h(X_{G_k}||M_2)$, $SID_j'' = M_7 \oplus h(M_6||r||X_{G_k})$, $M_8' = h(M_2||M_7||r'||\ SID_j'||X_{G_k})$, then checks whether $M_8' \stackrel{?}{=} M_8$ to authenticate $CloCen$.
If $M_8' \neq M_8$, GWN_k exits the session, otherwise, selects a random number r_g, and computes: $X_{S_j}' = h(SID_j''||x_{G_k})$, $M_9 = h(X_{S_j}'||M_2) \oplus r_g$, $M_{10} = h(M_2\ ||M_9||r_g||SID_j''||X_{S_j}')$.
3. $S_j \longrightarrow GWN_k$: $\{M_{11}, M_{12}\}$.
The smart device computes $r_g' = M_9 \oplus h(X_{S_j}||M_2)$, $M_{10}' = h(M_2||M_9||\ r_g'||SID_j||X_{S_j})$. If $M_{10}' \neq M_{10}$, the smart device rejects the access, otherwise computes $M = r_jM_2$, $M_{11} = r_jP$, $SK = h(M_2||M_{11}||M)$, $M_{12} = h(M_2||M_{11}||r_g'||X_{S_j}||SID_j)$.

4. $GWN_k \longrightarrow CloCen$: $\{M_{11}, M_{13}\}$.
   The gateway computes $M'_{12} = h(M_2||M_{11}||r_g||X'_{S_j}||SID''_j)$, compares M'_{12} with M_{12} to authenticate S_j. If the equation does not hold, terminates the session, otherwise computes $M_{13} = h(M_{11}||M_2||SID''_j||r'||X_{G_k})$.
5. $CloCen \longrightarrow U_i$: $\{M_{11}, M_{14}\}$.
   The cloud center computes $M'_{13} = h(M_{11}||M_2||SID''_j||r||X'_{G_k})$. If $M'_{13} \neq M_{13}$, ends the session, otherwise, computes $M_{14} = h(M'_1||M_2||ID'_i||SID'_j||k'_i||M_{11})$.
6. The smart phone computes $M^*_{14} = h(M_1||M_2||ID_i||SID_j||k^*_i||M_{11})$, if $M^*_{14} == M_{14}$, the smart phone accepts $SK = h(M_2||M_{11}||r_iM_{11})$ as the session key, the authentication process finishes successfully. Otherwise, the smart phone terminates the session.

3.5 Password Change Phase

To achieve user friendliness, we allow the user to change his/her password locally as following steps:

Step 1. $U_i \longrightarrow smartphone$: $\{ID^*_i, PW^*_i, Bio^*_i, PW^{new}_i\}$.
Step 2. The smart phone computes $\delta^*_i = Rep(Bio^*_i, \tau_i)$, $RPW^*_i = h(PW^*_i||\delta^*_i||a)$, $k^*_i = B_i \oplus RPW^*_i$, $A^*_i = h(ID^*_i||\ RPW^*_i||k^*_i)$ mod n_0.
If $A^*_i \neq A_i$, rejects the request; otherwise computes $RPW^{new}_i = h(PW^{new}_i||\delta^*_i||a)$, $A^{new}_i = h(ID^*_i||RPW^{new}_i||k^*_i)$ mod n_0, $B^{new}_i = h(RPW^{new}_i\ ||ID_i) \oplus k_i$, and then replaces $\{A_i, B_i\}$ with $\{A^{new}_i, B^{new}_i\}$.

3.6 Re-registration Phase

Once the user's account has been suspended, he/she can re-register to the system with the same identity as follows:

Step 1. $U_i \Longrightarrow CloCen$: $\{ID_i, RPW_i, revoke - requst\}$, where $Gen(Bio_i) = (\delta_i, \tau_i)$, $RPW_i = h(PW_i||\delta_i||a')$.
Step 2. $CloCen \Longrightarrow U_i$: $\{A^{new}_i, B^{new}_i, Y, h(\cdot), Gen(\cdot)\}$.
The cloud center first finds ID_i from the database, if it does not exist, rejects the request; otherwise, picks the timestamps $T^{new}_{rg_i}$, computes $k_i = h(ID_i||y||T^{new}_{rg_i})$, $B^{new}_i = h(RPW_i||ID_i) \oplus k^{new}_i$, and stores $\{ID_i, T^{new}_{rg_i}, Hoeny - list = NULL\}$.
Step 3. the smart phone selects a random number a^{new}, computes: $k^{new}_i = B'_i \oplus h(RPW_i||ID_i)$, $RPW^{new}_i = h(PW_i||\delta_i||a^{new})$, $A^{new}_i = h(ID_i||\ RPW^{new}_i||k^{new}_i)$ mod n_0, $B^{new}_i = h(RPW^{new}_i||ID_i) \oplus k^{new}_i$, keeps $\{A^{new}_i, B^{new}_i, a^{new}, \tau_i, Y, n_0, h(\cdot), Rep(\cdot)\}$ in its database.

3.7 Dynamics Node Addition Phase

The dynamics smart devices addition phase is similar to the smart device registration phase in Section. 3.1, so we do not repeat here.

4 Security Analysis

From the perspective of a real adversary, we give an informal analysis of the proposed scheme in this section.

4.1 User Anonymity

To preserve user anonymity, the scheme should stop a user from computing the identity and tracking the user. For identity protection, we transmit the identity ID_i in a form of $h(M_2||M_1) \oplus ID_i$, where M_1 is only known to the user and the cloud center with x, thus besides them, nobody can compute ID_i; for user untraceability, all the parameters transmitted in open channel are dynamically changing with the random numbers chosen by the four participants. Therefore, our scheme achieves user anonymity.

4.2 Forward Secrecy

Forward secrecy requires that the compromise of the whole system does not affect the previous session. Supposing the long term secret key x and y are exposed, then the adversary also eavesdrops the parameters M_2 and M_{11} consisted of the session key, while for the rest parameter M where $M = r_j M_2 = r_i M_{11}$. Note that r_j and r_i are not transmitted in the open channel and are only known to the smart device and the user, respectively. Therefore, the adversary can only directly compute the value of M with M_2 and M_{11}, that is, the adversary has to solve the Elliptic Curve Computational Diffie-Hellman (ECCDH) problem. Since the ECCDH problem cannot be solved within polynomial time, the adversary is bound to fail to compute M. Thus, our scheme achieves forward secrecy.

4.3 Mutual Authentication

Mutual authentication requires each participant to verify the other one's identity. In the proposed scheme, the cloud center authenticates the user through $M_5 = h(k_i||ID_i||M_1||M_2||M_3||M_4)$, k_i is their preset fixed shared secret and (M_1, M_2) is a pair of ciphertext and plaintext in public key algorithm. Thus k_i and M_1 are only known to the user and the cloud center, the authentication is effective; similarly, the user authenticates the cloud center with the same key parameters; then cloud center is authenticated by the gateway via M_8 which consists of their shared secret key X_{G_k}; the smart device and the gateway authenticate each other via M_{12} and M_{10}, respectively. In consequence, the proposed scheme achieves mutual authentication.

4.4 Privileged Insider Attack

Privileged insider attack requires the legitimate cloud center administrator to gain no advantage in attacking the security of the scheme. To achieve this goal, we let the user send $\{ID_i, RPW_i = h(PW_i||\delta_i||a)\}$ to the cloud center when he/she registers to avoid exposing sensitive information. Under this circumstance, the administrator of cloud center cannot gain any useful information since the password PW_i is protected by two parameters.

4.5 Smart Card Loss Attack

In [24], the smart card loss attack here refers to an adversary conduct attack with the help of parameters from the smart phone. In our scheme, if the adversary acquires $\{A_i, B_i, a, \tau_i, Y, h(\cdot), Rep(\cdot)\}$ in the phone, on one hand, if he/she wants to change the password without being noticed by the smart phone, then he/she has to construct correct $A_i = h(ID_i||RPW_i||k_i) \bmod n_0$ to pass the verification of the smart phone. Since the knowledge of $\{A_i, B_i, a, \tau_i, Y, n_0, h(\cdot), Rep(\cdot)\}$ makes no help to compute A_i, the adversary cannot change the password; on the other hand, if the adversary wants to guess the password correctly, he/she may either use A_i or M_5 as the verification parameter to test the correctness of the guessed password. To A_i, even the adversary with the biometric finds such a password and identity satisfying $h(ID_i^*||RPW_i^*||k_i) \bmod n_0 == A_i$, he/she still is not sure whether the password is right, since there are $|\mathcal{D}_{pw}| * |\mathcal{D}_{id}| \setminus n_0 \approx 2^{32}$ candidates of $\{ID_i, PW_i\}$ pair when $n_0 = 2^8$ and $|\mathcal{D}_{pw}| = |\mathcal{D}_{id}| = 2^6$ [23]. To further determine the correctness of the guessed password, the adversary has to conduct an online verification, which will be stopped by $Honey - list$; to M_5, as we explained before, M_5 consists of not only the preset secret shared parameter k_i which can be deduced from user's password and biometric, but also a dynamically changing M_1 which can only be known to the real user who selects r_i and the cloud center who knows y, in other words, the adversary though can "compute" k_i with the guessed password, cannot "compute" M_1, therefore, the adversary fails to construct such a M_5^* and then verifies it correctness with M_5 from the open channel. In conclusion, our scheme is secure against this attack.

4.6 Impersonation Attack

Firstly, we consider user impersonation attack. Note that in this attack, the adversary does not acquire the information from the smart card. On one hand, the adversary cannot gain user's password via offline dictionary attack according to our analysis of "smart card loss attack"; on the other hand, the adversary cannot directly construct such a valid access request $\{M_2, M_3, M_4, M_5\}$, where M_5 consists of k_i which can only be computed via user's sensitive information like the password, biometric and the smart phone or the long term secret y and verifier table, that is the adversary cannot impersonate the user.

Then, we talk about the cloud center impersonation attack. According to our protocol, both the user and the gateway will authenticate the cloud center via M_{14} and M_8, thus to impersonate the cloud center, the adversary has to compute M_{14} and M_8 correctly. However, to compute these two parameters, the adversary has to know k_i and X_{G_k} simultaneously. Since the two parameters are not transmitted directly or with "$\oplus$" operation in the open channel, the adversary cannot get them when he/she is not a legitimate participant, that is the adversary cannot impersonate the cloud center.

As for the gateway and the smart device, similarly to our analysis above, the gateway and the smart device authenticate each other with X_{S_j} who is not transmitted directly or with "$\oplus$" operation in the open channel, the adversary cannot get X_{S_j} except that he/she captures the smart device. But when the

Table 2. Performance comparison among relevant authentication schemes

Ref.	Evaluation Criteria [24]												Computational Cost in Login & Authentication			
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	User	Cloud	Gateway	Device
ours	√	√	√	√	√	√	√	√	√	√	√	√	$3T_P + T_B + 8T_H$	$T_P + 10T_H$	$7T_H$	$2T_P + 4T_H$
[14]	√	√	√	×	×	×	√	√	√	√	√	√	$3T_P + T_B + 7T_H$	-	$T_P + 6T_H$	$2T_P + 4T_H$
[25]	√	√	√	×	×	√	√	×	√	√	×	×	$T_B + 13T_H + 2T_S$	-	$5T_H + 4T_S$	$4T_H + 2T_S$
[2]	√	√	√	×	×	×	√	√	√	√	√	×	$9T_H$	$10T_H$	-	$4T_H$
[13]	√	√	√	×	√	×	√	×	×	×	√	×	$2T_P + T_B + 7T_H$	-	$T_P + 9T_H$	$4T_H$
[26]	√	√	√	×	×	×	√	×	√	√	√	×	$T_B + 9T_H + T_S$	-	$11T_H + 2T_S$	$7T_H + T_S$

T_E, T_P, T_B, T_H, T_S denote the operation time for modular exponentiation, elliptic curve point multiplication, fuzzy extracting biometric data, hash, and symmetric encryption, respectively, Some lightweight operations like exclusive-OR and $\|$ are omitted.
$C1$: No password verifier table; $C2$: Password friendly; $C3$: No password exposure; $C4$: No lost smart card attack; $C5$: Resistance to known attacks; $C6$: Sound repairability; $C7$: Provision of key agreement; $C8$: No clock synchronization; $C9$: Timely typo detection; $C10$: Mutual authentication; $C11$: User anonymity; $C12$: Forward secrecy.

adversary has captured the device, it is not appropriate to consider smart device impersonation attack anymore. Thus, the adversary cannot impersonate the smart device. Then, to the gateway, the cloud center also authenticates it via X_{G_k} which cannot be acquired to the adversary as we mentioned above, that is $\mathcal{A}$ cannot impersonate the gateway.

In conclusion, our scheme can well withstand against impersonation attack.

De-synchronization Attack We use the random number and the public key algorithm to achieve user anonymity and prevent replay attack, the participants are not required to keep the consistency of the clock synchronize or some temporary certificate related parameters. Therefore, our scheme can withstand against de-synchronization attack.

5 PERFORMANCE ANALYSIS

To check the performance of our proposed scheme, we compared it with several related schemes in this section. Note that, here we follow Wang et al.'s 12 independent criteria [24] as shown in Table **??**. Though their criteria are proposed for wireless sensor networks, also suitable for cloud-assisted IoT. On one hand, the WSN is a significant part of Internet of Things, the security threats and requirements of WSN also apply to the cloud-assisted IoT environment. On the other hand, compared with WSN, the cloud-assisted IoT environment has two different aspects, one is the user's terminate device (smart card VS. smart phone), the other is the participation of the powerful cloud center. When considering the security, the parameters in the smart card and the smart phone both can be extracted by the adversary, so this difference has no essential affect on the 12 criteria. As for the cloud center, it is assumed to be trusted, thus also makes no change to the criteria. In conclusion, Wang et al.'s 12 criteria also apply to the cloud-assisted IoT environment.

From Table 2, it is easy to see that our scheme is more suitable to the cloud-assisted Internet of Things environment: our scheme satisfies all the attributes proposed by Wang et al. [24], also shows its competitiveness in computation cost.

Other schemes all have several security flaws more or less, the best one can only provide 9 attributes. When considering the computational cost, it should note that the limitation of the IoT network is the gateway and the sensor nodes/ smart device. Since the cloud center has powerful capacity, and smart phone only works for one terminate user, while one gateway may connect thousands of smart devices or sensor nodes and serve for thousands of users, and under this circumstance, reducing the computational cost on gateway is even more significant than that on the sensor nodes or smart device. With the help of the cloud, our scheme greatly release the computation cost of the gateway, which means that our scheme can accommodate more network nodes, while other schemes, though claimed to be applicable to the IoT environment, are not well suited for IoT due to the limitations of gateways and sensor nodes. The only one that uses cloud computing to help the authentication is Amin et al.'s scheme [2], but unfortunately, this scheme does not take into account the important components (i.e. wireless sensor network) of the IoT. As for the computational cost on the sensor nodes/ smart phone, our scheme performs not bad among these schemes armed with public key algorithm. Although, these schemes without deploying public key algorithm cost less, but definitely fail to achieve a secure authentication according to [23]. In conclusion, our scheme is more suitable for the Internet of Things environment.

6 CONCLUSION

To satisfy the exponential growth of interconnected devices and the demanding on large amounts of data processing, integrating of IoT and cloud computing has become an inevitable trend in the future. However, under this condition, we found most of the authentication schemes for IoT do not really integrate the cloud computing thus are not suitable for IoT. Thus, we firstly depict the architecture of the cloud-assisted IoT environment, and propose a new secure and privacy preserving user authentication scheme for cloud-assisted IoT, analyze its security and compare it with several related schemes, the result shows the superiority of our new scheme.

Acknowledgments

This work was supported by the National Key Research and Development Plan of China under Grant No.2018YFB0803605, and by the National Natural Science Foundation of China under Grant No.61802006, and by China Postdoctoral Science Foundation under Grants No.2018M640026 and No.2019T120019.

References

1. Alhakbani, N., Hassan, M.M., Hossain, M.A., Alnuem, M.: A framework of adaptive interaction support in cloud-based internet of things (iot) environment. In: Proc. IDCS (Internet and Distributed Computing System). pp. 136–146 (2014)

2. Amin, R., Kumar, N., Biswas, G., Iqbal, R., Chang, V.: A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment. Future Gener. Comput. Sys. 78, 1005–1019 (2018)
3. Botta, A., De Donato, W., Persico, V., Pescapé, A.: Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Sys. 56, 684–700 (2016)
4. Das, M.L.: Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 8(3), 1086–1090 (2009)
5. Dhillon, P.K., Kalra, S.: Secure multifactor remote user authentication scheme for internet of things environments. Int. J. Commun. Syst. 30(16), e3323 (2017)
6. Fan, R., He, D., Pan, X., Ping, L.: An efficient and dos-resistant user authentication scheme for two-tiered wireless sensor networks. J. Zhejinag Univ. Sci. C 12(7), 550–560 (2011)
7. Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Netw. 36, 152–176 (2016)
8. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): A vision, architectural elements, and future directions. Future Gener. Comput. Sys. 29(7), 1645–1660 (2013)
9. Hossain, M.S., Muhammad, G.: Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Comput. Netw. 101, 192–202 (2016)
10. Jiang, Q., Zeadally, S., Ma, J., He, D.: Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access 5, 3376–3392 (2017)
11. Khan, M., Alghathbar, K.: Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. Sensors 10(3), 2450–2459 (2010)
12. Kumar, P., Gurtov, A., Ylianttila, M., Lee, S., Lee, H.: A strong authentication scheme with user privacy for wireless sensor networks. ETRI J. 35(5), 889–899 (2013)
13. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K., Choo, K.K.R.: A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J. Netw. Comput. Appl. 103, 194–204 (2018)
14. Li, X., Niu, J., Bhuiyan, M.Z.A., Wu, F., Karuppiah, M., Kumari, S.: A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things. IEEE Trans. Ind. Inform. 14(8), 3599–3609 (2018)
15. Mal, C., Wang, D., Zhao, S.: Security flaws in two improved remote user authentication schemes using smart cards. Int. J. Commun. Syst. 27(10), 2215–2227 (2012)
16. Mell, P., Grance, T., et al.: The nist definition of cloud computing. NatI. Inst. Stand. Technol 53(6), 50 (2009)
17. Reddy, A.G., Das, A.K., Yoon, E.J., Yoo, K.Y.: A secure anonymous authentication protocol for mobile services on elliptic curve cryptography. IEEE Access 4, 4394–4407 (2016)
18. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y.: Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J. Netw. Comput. Appl. 106, 117–123 (2018)
19. Srinivas, J., Das, A.K., Wazid, M., Kumar, N.: Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things (2018), doi: 10.1109/TDSC.2018.2857811

20. Sun, D., Li, J., Feng, Z., Cao, Z., Xu, G.: On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Pers. Ubiquitous Comput. 17(5), 895–905 (2013)
21. Wang, C., Xu, G., Sun, J.: An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. Sensors 17(12), 2946 (2017)
22. Wang, D., Wang, P.: On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. Comput. Netw. 73(C), 41–57 (2014)
23. Wang, D., Wang, P.: Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. Depend. Secur. Comput. 15(4), 708–722 (2018)
24. Wang, D., Li, W., Wang, P.: Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Ind. Inform. 14(9), 4081–4092 (2018)
25. Wazid, M., Das, A.K., Khan, M.K., Al-Ghaiheb, A.D., Kumar, N., Vasilakos, A.: Design of secure user authenticated key management protocol for generic iot networks. IEEE Internet of Things J. 5(1), 269–282 (2018)
26. Wazid, M., Das, A.K., Odelu, V., Kumar, N., Susilo, W.: Secure remote user authenticated key establishment protocol for smart home environment (2017), doi:10.1109/TDSC.2017.2764083
27. Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K.K.R., Wazid, M., Das, A.K.: An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment. J. Netw. Comput. Appl. 89, 72–85 (2017)