symmetry

MDPI

*Article*

# Geometric Authentication Mechanism for Enhancing Security in IoT Environment

**Ming-Chin Chuang [1,*] and Chia-Cheng Yen [2]**

[1] Department of Computer Science and Information Engineering, China University of Technology, Taipei City 116, Taiwan
[2] Department of Computer Science, University of California, Davis, CA 95616, USA; ccyen@ucdavis.edu
* Correspondence: speedboy@cute.edu.tw

**Abstract:** In the Internet of things (IoT) environment, many applications access services through remote methods. In this paper, we designed a new geometric authentication mechanism to enhance security. The solution is based on geometric characteristics to achieve rapid authentication at low computational cost. In addition, we use the user's biometrics to improve the security level of the system. Our solution meets the following security features: anonymity, resistance to forgery attacks and replay attacks, fast error detection, resistance to offline password guessing attacks, resistance to server overload attacks, mutual authentication, session key agreement, and flexibility in users choosing and changing their passwords easily.

**Keywords:** authentication; geometric; biometrics; anonymity; Internet of things (IoT)

check for updates

**Citation:** Chuang, M.-C.; Yen, C.-C. Geometric Authentication Mechanism for Enhancing Security in IoT Environment. *Symmetry* **2021**, *13*, 1369. https://doi.org/10.3390/sym13081369

Academic Editor: Christos Volos

Received: 7 July 2021
Accepted: 26 July 2021
Published: 28 July 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

Wireless and mobile communication systems have become increasingly popular. Many service providers are beginning to propose convenient Internet of things (IoT) services and cloud applications for users. People usually use mobile devices to access all kinds of services, e.g., web-browsing, remote monitoring, and multimedia applications anytime and anywhere. Figure 1 shows an example where the user logs in to the IoT gateway (IGW) to access or control IoT devices remotely. There is no doubt that an authentication mechanism is essential to protect valid users against different types of attacks. Remote user authentication schemes are the easiest and most practical authentication mechanisms for nonsecure networks.

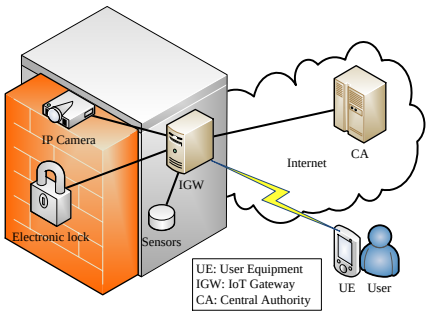



**Figure 1.** Remote access via gateway in IoT environment.

However, previous authentication schemes suffer from high computational cost and insufficient security. Some schemes use asymmetric cryptography, which results in high computational cost. Most schemes use ID/password-based authentication, but the security robustness of these schemes is insufficient. Therefore, we propose a new three-factor (i.e., smart device, biometrics, and password) remote user authentication scheme for improving the performance and enhancing security in the IoT environment in this paper.

The contributions of this paper are as follows.

- Lightweight authentication: The computational performance of our scheme is better than the traditional authentication schemes (e.g., asymmetric or symmetric encryption scheme) because our scheme uses only a hash function and arithmetic.
- Three-factor authentication: A higher-entropy password increases the difficulty in brute forcing it. Many papers have proven that the three-factor authentication scheme has better security (i.e., higher password entropy) and robustness.
- Reduced IGW computing load: Many authentication methods require full participation of the IGW. However, in an IoT environment, the number of IoT devices is large. Therefore, previous schemes are not suitable for use in an IoT environment because the IGW easily suffers from the single-point failure problem due to a distributed denial-of-service (DDoS) attack. In our scheme, GAME supports the fast error detection process on the client side. If the user access is illegal, the smartphone immediately detects an error event and then rejects the login. In this way, the computational load of the IGW can be effectively reduced.

The remainder of this paper is organized as follows. Section 2 describes some related work. In Section 3, we describe the proposed scheme in detail. The security analyses and comparisons are presented in Section 4. Then, in Section 5, we summarize our conclusions.

## 2. Related Work

This section includes three parts: user requirements, system requirements, and existing authentication schemes.

### *2.1. User Requirements*

Since the designed authentication system must be user-friendly, the following requirements must be taken into account for users:

1. Secure and simple password selection and modification: The system should enable users to select and modify their passwords easily and securely. This means that the user can change their password without the help of a trusted third party after having ensured the legality of the cardholder.
2. Registration only once: The user must register only once with the Central Authority (CA) and may then access a variety of application servers. Additionally, the single registration may reduce the network load and the CA overhead.
3. Anonymity: User privacy has been increasingly brought to the attention of industry and academia. Therefore, anonymous authentication implies verifying that a user is not using the real identity to perform the authentication procedure.

### *2.2. System Requirements*

Given that a remote authentication system is susceptible to attack by adversaries, our goal is to design a system that is robust enough to resist such attacks. From related studies [1,2], the following key requirements are identified for secure authentication:

1. Efficiency: Due to the limited computing power of mobile devices, the communication and computing costs on mobile devices must be lightweight.
2. Integrity: The system must ensure the integrity of the message. This means that, when the data is modified, the system will find out and authentication fails.
3. Session key protocol: After the authentication process, a session key will be generated between the mobile device and the IGW to provide secure communication and achieve forward secrecy.
4. Mutual authentication: The IGW must verify that the user is legitimate, and the user must also ensure that the IGW is not forged. Therefore, the authentication system needs a mutual authentication process.

5. No verification table: In most applications, the CA stores the user's password table, which can cause the verifier to be stolen. Therefore, the design solution should avoid maintaining password verification tables for users.

### *2.3. Existing Authentication Schemes*

Wu [3] first proposed a remote login authentication scheme based on geometric methods in 1995. However, some studies [4,5] found that Wu's scheme was vulnerable to replay attacks and offline password guessing attacks. Chien et al. [5] proposed a modified authentication scheme to solve these problems, but [6,7] showed that the modified scheme [5] was still vulnerable to offline password guessing attacks. In addition, it is easy for illegal users to forge valid login requests under the revised scheme. Later, [7] proposed an improved scheme to overcome these drawbacks. The common disadvantage of all the above schemes is that they do not consider user privacy. However, privacy issues are now receiving more and more attention from industry and academia. To this end, we propose an anonymous remote user authentication scheme based on geometric methods [8]. However, our previous work did not take into account session key agreement and mutual authentication.

Many studies [9–18] combined a user's biometrics with a password and a smart device to design a remote user authentication scheme to improve the security level (i.e., a secret key that has a value of high entropy [14]). In 2002, Lee et al. [9] proposed a fingerprint-based remote user authentication scheme using smart cards. However, a large number of subsequent studies [10–12] pointed out that this scheme cannot resist server spoofing attacks and masquerading attacks. Although Lin and Lai [12] combined password and fingerprint into super passwords and provided an offline password change scheme, Mitchell and Tang [13] proposed that the password change process is fragile because the smart card does not have enough information to check the correctness of the old passwords. Then, Fan and Lin [14] proposed a three-factor authentication scheme that combines a password with smart card and biometrics to provide high-security remote authentication. Khan et al. [15] proposed an improved scheme to enhance the security. However, this scheme was proven to be vulnerable to parallel session attacks [16,17], where an attacker who does not know the password of a legitimate user can pretend to be a user by eavesdropping on the communication between the user and the server to generate a valid login message in some way. Later, Li and Hwang [18] proposed an efficient biometric-based remote user authentication scheme using smart cards. Unfortunately, these biometric-based solutions [9–18] only support a single server environment, which is a limitation because there are multiple application servers on the Internet. Recently, Chuang and Chen [1] proposed a biometrics-based multi-server authentication scheme. However, Mishra et al. [19] revealed that the scheme in [1] is prone to masquerading, smart card theft, and server spoofing attacks. Afterward, Mishra et al. designed a more secure three-factor authentication scheme. Later, Lu et al. [20,21] pointed out that the solution [19] could be attacked by server masquerading and spoofing. Recently, many studies [22–28] proposed a lightweight authentication scheme for the IoT environment. However, these solutions still have weaknesses, especially in terms of computing and communication costs, which are higher than the solution we proposed. Banerjee et al. [29] proposed an anonymous and robust authentication scheme for IoT-based smart homes. However, [2] pointed out that Banerjee et al.'s scheme [29] does not ensure identity protection, traceability, or session secret key negotiation. Xiang and Zheng [30] presented a situation-aware device authentication scheme in smart home environments. They claimed that their solution can withstand various security threats and ensure mutual authentication and data integrity. However, Oh et al. [31] proved that this scheme cannot guarantee secure mutual authentication and is vulnerable to smart device theft, impersonation, and session key disclosure attacks.

## 3. Proposed Scheme

In this section, we describe our geometric authentication mechanism for enhancing security, called GAME, in an IoT environment. GAME is a lightweight authentication scheme. Moreover, we combine biometric technology and a password to enhance the level of security. The proposed geometric authentication mechanism involves four procedures: registration, login, authentication, and changing passwords. The notation used throughout this paper is listed in Table 1.

**Table 1.** Notation.

| Symbol | Description |
|---|---|
| $BIO_i$ | Biometric information of user $i$ |
| $ID_i$ | The public identification of a user $i$ |
| $AID_i$ | The alias of user $i$ |
| $SID_j$ | The public identification of an IGW $j$ |
| $(x_0,y_0)$ | A secret point stored in the IoT gateway (IGW) and the central authority (CA) |
| $r_i$ | A random number $i$ |
| $T$ | The current timestamp |
| $\oplus$ | The bitwise XOR operator |
| $h(\ )$ | A one-way collision-resistant hash function |
| $\|\ \|$ | The combination of strings |
| $PW_i$ | The password of user $i$ |
| $P$ | A large prime |
| $SK_{ij}$ | The session key between $i$ and $j$ |

### 3.1. Registration Procedure

Before logging in to access the service, the user must complete the registration process, which needs to be executed through a secure channel. Figure 2 shows the user registration procedure, while the steps are outlined below.

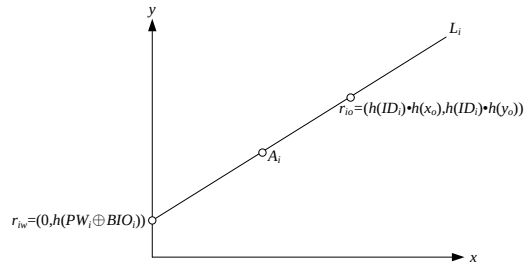



**Figure 2.** Registration procedure.

Step 1: The user sends their registration information to the central authority (CA) through a secure communication channel. The registration information includes their identification $ID_i$, password $PW_i$, and biometric information $BIO_i$.

Step 2: After the CA receives the user's data, it selects a large prime number $P$, calculates $V_i = h^2(PW_i \oplus BIO_i)$ and defines two points ($r_{iw}$ and $r_{io}$), which are $(0, h(PW_i \oplus BIO_i))$ and $(h(ID_i) \cdot h(x_0), h(ID_i) \cdot h(y_0))$. Next, the CA establishes a line $L_i$ through $r_{iw}$ and $r_{io}$, and then calculates the midpoint between $r_{iw}$ and $r_{io}$, which is represented by $A_i$. The secret point $(x_0,y_0)$ is a secret point stored in the trusted platform module (TPM) of the IGW and the CA. Note that the CA selects a different secret point for each IGW.

Step 3: The CA stores the parameters $\{h(ID_i), h(\ ), P, A_i, V_i\}$ in the NFC-SIM card of the mobile phone and provides them to the user via a secure channel.

### 3.2. Login Procedure

The user logs in from the mobile phone. This login process is the first checkpoint. If the user access is illegal, the mobile phone immediately detects an error event (e.g., wrong user password or failed biometric identification), and then reports the error. When the number of input errors exceeds three, the card is locked, as shown in Figure 3.




(**a**) (**b**)

**Figure 3.** (**a**) PIN code lock. (**b**) The device is locked after three incorrect inputs.

Step 1: The user enters their $ID_i$ and $PW_i$ on the mobile phone. Then, the mobile phone scans their biometric information $BIO_i$ on the sensor.

Step 2: The mobile phone checks $h(ID_i)$ and verifies whether $h^2(PW_i \oplus BIO_i)$ is equal to $V_i$. If this information is verified, the phone calculates $r_{iw} = (0, h(PW_i \oplus BIO_i))$ and reconstructs the line $L_i$ through $r_{iw}$ and $A_i$.

Step 3: The mobile phone calculates the point between $r_{iw}$ and $A_i$, represented by $B_i$, generates a new point $r_{iT}$, which is equal to $(0, h(h(PW_i \oplus BIO_i) \oplus h(T)))$, and then uses $r_{iT}$ and $B_i$ to generate a new line $L_{WT}$.

Step 4: The mobile phone selects a point $C_i$ on the $L_{WT}$ line, which is different from $r_{iT}$ and $B_i$, generates a random number $r_i$, and then calculates the alias $AID_i$, $AID_i = r_i \cdot h(ID_i)$.

Step 5: The user sends an authentication message $\{AID_i, A_i, C_i, T\}$ to the IGW through a normal wireless network.

### 3.3. Authentication Procedure

After the IGW receives the login request message, the IGW starts the authentication process to verify the user's request message, as shown in Figures 4 and 5. The steps of the certification process are described below.

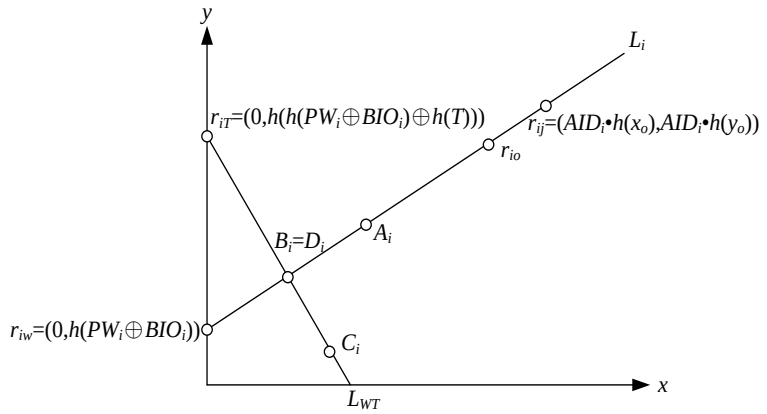



**Figure 4.** Diagram of user login and authentication phases.

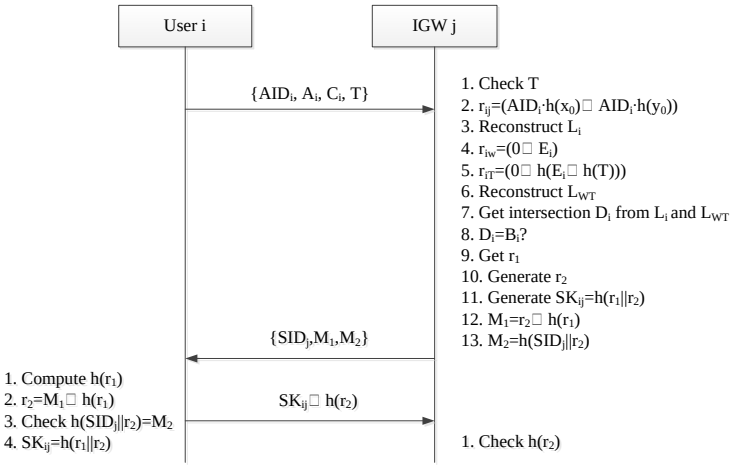



**Figure 5.** Message flow of authentication phase.

Step 1: The IGW first checks the timestamp. It rejects the login message if the difference between $T'$ and $T$ is larger than the threshold.

Step 2: The IGW computes point $r_{ij} = (AID_i \cdot h(x_0), AID_i \cdot h(y_0))$ and then reconstructs the line $L_i$ by $r_{ij}$ and $A_i$.

Step 3: The IGW computes the intersection point $r_{iw}$ of $L_i$ and the $y$-axis, defines $r_{iw} = (0, E_i)$, and then computes $r_{iT} = (0, h(E_i \oplus h(T)))$.

Step 4: The IGW uses $r_{iT}$ and $C_i$ to reconstruct the line $L_{WT}$ and computes the intersection point $D_i$ of $L_i$ and $L_{WT}$.

Step 5: The IGW accepts the login request if the value of $D_i$ is equal to the middle point $B_i$ of $A_i$ and $r_{iw}$. Otherwise, the request is rejected.

Step 6: When the authentication is successful, the IGW can deduce $r_1$ through $r_{io}$ and $r_{ij}$ on the $L_i$ line. $r_{ij} = (AID_i \cdot h(x_0), AID_i \cdot h(y_0)) = (r_1 \cdot h(ID_i) \cdot h(x_0), r_1 \cdot h(ID_i) \cdot h(y_0)) = r_1(h(ID_i) \cdot h(x_0), h(ID_i) \cdot h(y_0)) = r_1 \cdot r_{io}$.

Step 7: Then, the IGW generates the random number $r_2$, computes the session key $SK_{ij} = h(r_1 || r_2)$, and generates the messages $M_1$ and $M_2$; $M_1 = r_2 \oplus h(r_1)$ and $M_2 = h(SID_j || r_2)$.

Step 8: The IGW sends the message $\{SID_j, M_1, M_2\}$ to the user.

Step 9: After the mobile phone receives the message, it calculates $h(r_1)$, takes out $r_2$, and then checks whether $h(SID_j || r_2)$ is equal to $M_2$. If it is correct, the session key $SK_{ij} = h(r_1 || r_2)$ is generated, and the encrypted message $SK_{ij} \oplus h(r_2)$ is sent to the IGW.

Step 10: After the IGW receives the message, it uses the session key $SK_{ij}$ to decrypt the encrypted message, obtains $h(r_2)$, and then verifies whether it is correct. If it is correct, the mutual authentication is completed. Otherwise, access is denied.

### *3.4. Password Change Procedure*

In our method, when the user wants to change their password, they do not need the help of the CA. Figure 6 shows the lines and points used in the user password change procedure.

Step 1: The user keys in their $ID_i$ and $PW_i$, and then the mobile phone scans their biometric feature $BIO_i$ at the sensor.

Step 2: The mobile phone checks $h(ID_i)$ and verifies whether $h^2(PW_i \oplus BIO_i)$ is equal to $V_i$. If the information is verified, the user can key in their new password $PW_i^*$. The mobile phone sets the point $r_{iw} = (0, h(PW_i \oplus BIO_i))$, calculates the point $r_{io} = 2A_i - r_{iw}$, computes the new point $r_{iw}^* = (0, h(PW_i^* \oplus BIO_i))$, computes the new point $A_i^* = (r_{iw}^* + r_{io})/2$, and calculates the new $V_i^* = h^2(PW_i^* \oplus BIO_i)$. It then replaces the stored $A_i$ and $V_i$ with $A_i^*$ and $V_i^*$, respectively.

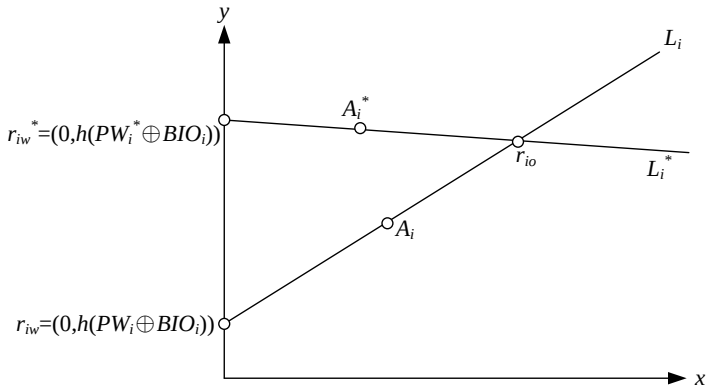



**Figure 6.** User password change phase.

## 4. Analysis

### *4.1. Definition*

- A fragile key has a very low entropy value (e.g., only a password is used to protect access), and an attacker can guess the user's password within polynomial time. On the contrary, a strong key usually has a high entropy value (e.g., password plus biometric information and mobile phone), such that the attacker cannot guess the user password within polynomial time [14]. Additionally, any two people cannot have the same biometric information.
- In this research, the hash function is a one-way collision-free hash function (e.g., SHA-512 [32]). When the value of x is given, this hash function can easily calculate h(x). However, if the value of h(x) is given, it is difficult to push back x without incurring a high computational cost.
- During the login process, this secure hardware has retrial restrictions to prevent attackers from using brute force cracking techniques to guess the user's password.

### *4.2. Security Analysis*

1. Higher security level: Many papers have already proven that the security of the three-factor authentication scheme is stronger than the security of the two-factor authentication scheme.
2. Anonymity and identity protection: In the login procedure, the user's original name is converted into an alias (e.g., $AID_i = r_i \cdot h(ID_i)$). The generation of the alias is based on a random number (i.e., Step 4 of the login procedure). The random number generated by each login process is different. Therefore, the attacker cannot know the original identity of the user without knowing the random number $r_i$. In addition, our anonymity mechanism is a dynamic identity process. In the registration phase, the SIM card does not store the identity of the user. Therefore, the attacker cannot retrieve the user identity, even if the attacker obtains the SIM card. In GAME, we use a hash function to protect the identity of the user (i.e., $h(ID_i)$).
3. Resistance to replay attack: In the login procedure, the login request is rejected if an attacker resends $\{AID_i, A_i, C_i, T'\}$ to the IGW. Since $T'$ is inconsistent with the T in $C_i$, it is different from $C_i'$. Thus, our method can resist replay attacks. In the authentication procedure, GAME can still resist replay attacks since the message contains the random number. The random number generated is different each time. Therefore, the authentication process will not succeed if an attacker intercepts and replays the authentication message.
4. Choose and change passwords easily: Users can select and modify passwords without participating in the CA, which is very convenient for users. Note that this procedure can still be considered a security issue. When users modify their passwords, they must succeed in verification before they execute the password change procedure.

5. Fast error detection: In our method, the fast error detection process is performed only on the client side and does not require the IGW to assist in authentication. Therefore, this stage does not consume network transmission resources and IGW computing resources. In the login and password change process, if an attacker tries to guess the password or enters wrong biometric data, the mobile phone can immediately detect the input error (i.e., Step 2 in the login procedure and Step 2 in the password change procedure), and then perform error reporting and lock the card.
6. Resistance to offline password guessing attacks: In previous studies, if an attacker captured consecutive login messages $\{AID_{i1}, A_i, C_{i1}, T_1\}$ and $\{AID_{i2}, A_i, C_{i2}, T_2\}$ at the time points of $T_1$ and $T_2$, they could try to guess the user's $PW_i$ and use the retrieved information to verify their guess. Then, they may calculate the point $r_{iw}{}' = (0,h(PW_i{}'\oplus BIO_i))$ and calculate the intermediate point $B_i{}'$ between $r_{iw}{}'$ and $A_i$. In addition, the attacker can calculate this $r_{iT1'} = (0,h(h(PW_i{}'\oplus BIO_i)\oplus h(T_1)))$ and construct the line $L_{WT1'}$ passing through the two points of $C_{i1}$ and $r_{iT1'}$. Similarly, the attacker can calculate the point $r_{iT2'}$ and the construction line $L_{WT2'}$. Next, they can compare $B_i{}'$ with the intersection of $L_{WT1'}$ and $L_{WT2'}$, $B_i{}''$. If the values are equal, this means that the password $PW_i{}'$ guessed by the attacker is correct. However, in our method, the attacker cannot retrieve these values (i.e., $r_{iw}{}'$, $r_{iT1'}$, and $r_{iT2'}$) because the attacker does not have the user's biometric $BIO_i$. Thus, our method can resist offline password guessing attacks.
7. Resistance to forgery attacks: Although the attacker can intercept the login message $\{AID_i, A_i, C_i, T\}$, they cannot forge a valid login message $\{AID_i, A_i, C_i{}', T'\}$ to pass the authentication process. This is because the attacker does not know $h(PW_i\oplus BIO_i)$ and, thus, cannot calculate the point $B_i$ and the corresponding point $r_{iT}{}' = (0, h(h(PW_i\oplus BIO_i)\oplus h(T')))$. Of course, the attacker will not be able to correctly re-establish the line $L_{WT}$. Therefore, our solution can resist forgery attacks.
8. Resistance to stolen smart device: When the attacker steals the smart device of a user, the attacker still cannot be authenticated successfully. This is because the attacker cannot provide valid biometric identification in login phase. Moreover, the biometric information of the user is not directly stored on the smart device.
9. Resistance to server overloading attacks: In previous methods, the entire authentication procedure was executed on the server, making the server vulnerable to overload attacks. Assuming that the user's mobile phone is stolen by an attacker, in the previous method, the attacker could deduce the user's identity through intercepted messages. Even if the attacker types in the wrong password, a large number of malicious authentication request messages can be generated on the server. These malicious authentication request messages will cause server computing overload. However, this situation cannot happen with our method, because (i) our method supports the authentication of biometric information, and (ii) our method supports fast error detection. Therefore, when the user enters the wrong ID, password, or biometric message, the mobile phone will not generate a malicious authentication request message to the server.
10. Mutual authentication: A mutual authentication procedure is supported by our authentication method. The server needs to verify that the user is legitimate, and the user also needs to ensure that the server is not forged. When mutual authentication is successful, the security of the overall system can be ensured.
11. Session key generation: After the authentication process, a session key is generated between the user and the IGW to provide secure communication. The IGW responds with a message $\{SID_j, M_1, M_2\}$ to the mobile phone. After the mobile phone receives the message, it calculates $h(r_1)$, takes out $r_2$, and then checks whether $h(SID_j||r_2)$ is equal to $M_2$. If it is correct, the session key $SK_{ij} = (r_1||r_2)$ is generated, and the encrypted message $SK_{ij}\oplus h(r_2)$ is sent to the IGW. The session key is generated from two random numbers through a hash function; thus, each session key is different and cannot be pushed back.

### *4.3. Comparison with Other Schemes*

We compared our scheme with related existing schemes [28–30]. Table 2 shows the comparisons of security features. Obviously, the proposed scheme provides the most security properties.

**Table 2.** Comparisons of security features.

| | GAME | Shuai et al. [28] | Banerjee et al. [29] | Xiang and Zheng [30] |
|---|---|---|---|---|
| Three-factor | Y | N | Y | N |
| Identity protection | Y | Y | Y | N |
| Anonymity | Y | Y | N | N |
| Resistance to replay attacks | Y | Y | Y | Y |
| Choose and change passwords easily | Y | Y | Y | Y |
| Fast error detection | Y | Y | Y | Y |
| Resistance to offline password guessing attacks | Y | N | Y | Y |
| Resistance to forgery attacks | Y | Y | Y | Y |
| Resistance to stolen smart device | Y | - | N | N |
| Resistance to server overloading attacks | Y | Y | Y | Y |
| Session key agreement | Y | Y | N | N |
| Mutual authentication | Y | Y | N | N |

Y: secure; N: insecure; -: not considered.

### *4.4. Computation Analysis*

We measured the computation time required for various operations. As hardware, we use the UP Board IoT gateway (Raspberry Pi compatible) developed by AAEON as the test platform [33], as shown in Figure 7. The operating system was a 64 bit Windows 10, the memory was 4 GB, and the CPU was an Intel Atom 1.44 GHz. Table 3 shows the measured calculation time of each operation. Since the proposed method only uses arithmetic operations, XOR operations, and hash functions, the calculation time is much shorter than the RSA authentication method. Table 4 compares the computational costs of the proposed scheme and those of other schemes. $T_m$, $T_R$, $T_h$, $T_a$, and $T_s$ denote the execution times of an ECC point multiplication, fuzzy extractor function, hash function, and an arithmetic and symmetric key encryption/decryption, respectively. The scheme in [30] featured the lowest computational cost, but it suffered from many attacks.



**Figure 7.** AAEON UP Board (IoT gateway).

**Table 3.** Computational time.

| Operation | Microseconds |
|---|---|
| RSA 1024 encryption | 6709 |
| RSA 1024 decryption | 280 |
| RSA 1024 signature | 7100 |
| RSA 1024 verification | 270 |
| ECC point multiplication | 75 |
| AES 256 encryption | 1.6 |
| AES 256 decryption | 1.6 |
| Fuzzy extractor function | 7 |
| SHA-1 | 1 |
| SHA-512 | 1.2 |
| Arithmetic | 0.5 |

**Table 4.** Comparison of computational cost with other schemes.

| | GAME | Shuai et al. [28] | Banerjee et al. [29] | Xiang and Zheng [30] |
|---|---|---|---|---|
| Total | $20T_h + 1T_R + 8T_a$ | $3T_m + 16T_h$ | $26T_h + 1T_R$ | Low security risk: $11T_h$High security risk: $11T_h + 4T_s$ |
| Computational cost | 31 ms | 230 ms | 33 ms | Low security risk: 14 msHigh security risk: 19 ms |

## 5. Conclusions

Since most of the authentication schemes are based on ID/password, security is obviously insufficient. In this paper, we proposed an anonymous remote user authentication mechanism based on geometric methods, whereby we used a combination of password and user's biometric information to provide a more secure authentication mechanism. Moreover, GAME only uses arithmetic operations and hash functions; thus, the computational complexity of the method is extremely low, and the calculation time is much shorter than that of traditional asymmetric encryption authentication methods. Therefore, our method is very suitable for application services on mobile devices in an IoT environment. Lastly, the proposed method satisfies the following security properties: it is anonymous, can resist forgery attacks, can resist repeated attacks, can quickly detect errors, can resist offline password guessing attacks, can resist server overload attacks, and can enable easy selection and modification of the password.

**Author Contributions:** Conceptualization, M.-C.C.; methodology, M.-C.C. and C.-C.Y.; software, C.-C.Y.; investigation, M.-C.C.; resources, M.-C.C.; data curation, C.-C.Y.; writing—original draft preparation, M.-C.C.; writing—review and editing, M.-C.C. and C.-C.Y.; supervision, M.-C.C. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Ministry of Science and Technology, R.O.C., under grants MOST 107-2221-E-163-001-MY3.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## References


1. Chuang, M.-C.; Chen, M.C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Syst. Appl.* **2014**, *41*, 1411–1418. [CrossRef]
2. AL-Turjman, F.; Deebak, D.B. Seamless authentication: For IoT-big data technologies in smart industrial application systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 2919–2927.
3. Wu, T.-C. Remote login authentication scheme based on a geometric approach. *Comput. Commun.* **1995**, *18*, 959–963. [CrossRef]
4. Hwang, M.-S. Cryptanalysis of a remote login authentication scheme. *Comput. Commun.* **1999**, *22*, 742–744. [CrossRef]
5. Chien, H.-Y.; Jan, J.-K.; Tseng, Y.-M. A modified remote login authentication scheme based on geometric approach. *J. Syst. Softw.* **2001**, *55*, 287–290. [CrossRef]
6. Chang, C.-C.; Lin, I.-C. Cryptanalysis of the modified remote login authentication scheme based on a geometric approach. *Informatica* **2005**, *16*, 37–44. [CrossRef]
7. Ku, W.-C.; Chang, S.-T.; Chen, H.-H.; Tsaur, M.-J. Weakness and simple improvement of a password authentication scheme based on geometric approach. In Proceedings of the IEEE Conference on Local Computer Networks (LCN), Sydney, Australia, 17 November 2005; pp. 472–473.
8. Chuang, M.-C.; Lee, J.-F. An anonymous remote user authentication scheme based on a geometric approach for wireless networks. In Proceedings of the IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet), Xianning, China, 16–18 April 2011; pp. 1015–1018.
9. Lee, J.K.; Ryu, S.R.; Yoo, K.Y. Fingerprint-based remote user authentication scheme using smart cards. *Electron. Lett.* **2002**, *38*, 554–555. [CrossRef]
10. Ku, W.; Chang, S.; Chiang, M. Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. *Electron. Lett.* **2005**, *41*, 240–241. [CrossRef]
11. Chang, C.-C.; Lin, I.-C. Remarks on fingerprint-based remote user authentication scheme using smart cards. *ACM SIGOPS Oper. Syst. Rev.* **2004**, *38*, 91–96. [CrossRef]
12. Lin, C.-H.; Lai, Y.-Y. A flexible biometrics remote user authentication scheme. *Comput. Stand. Interfaces* **2004**, *27*, 19–23. [CrossRef]
13. Mitchell, C.J.; Tang, Q. Security of the Lin-Lai Smart Card Based User Authentication Scheme, Technical Report. 2005. Available online: http://www.rhul.ac.uk/mathematics/techreports (accessed on 1 May 2021).
14. Fan, C.-I.; Lin, Y.-H. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. *IEEE Trans. Inform. Forensics Secur.* **2009**, *4*, 933–945. [CrossRef]
15. Khan, M.K.; Zhang, J. An efficient and practical fingerprint-based remote user authentication scheme with smart cards. In *Springer Lecture Notes in Computer Science, Proceedings of the International Conference on Information Security Practice and Experience, Hangzhou, China, 11–14 April 2006*; Springer: Berlin, Germany, 2006; pp. 260–268.
16. Khan, M.K.; Zhang, J.; Wang, X. Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos Solitons Fractals* **2008**, *35*, 519–524. [CrossRef]
17. Xu, J.; Zhu, W.; Feng, D. Improvement of a fingerprint-based remote user authentication scheme. In Proceedings of the IEEE International Conference on Information Security and Assurance (ISA), Busan, Korea, 24–26 April 2008; pp. 87–92.
18. Li, C.-T.; Hwang, M.-S. An efficient biometrics-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* **2010**, *33*, 1–5. [CrossRef]
19. Mishra, D.; Das, A.K.; Mukhopadhyay, S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Syst. Appl.* **2014**, *41*, 8129–8143. [CrossRef]
20. Lu, Y.; Li, L.; Yang, X.; Yang, Y. Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. *PLoS ONE* **2015**, *10*, e0126323. [CrossRef]
21. Lu, Y.; Li, L.; Peng, H.; Yang, Y. A biometrics and smart cards-based authentication scheme for multi-server environments. *Secur. Commun. Netw.* **2015**, *8*, 3219–3228. [CrossRef]
22. Dammak, M.; Boudia, O.R.M.; Messous, M.A.; Senouci, S.M.; Gransart, C. Token-based lightweight authentication to secure IoT networks. In Proceedings of the IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4.
23. Gupta, A.; Tripathi, M.; Shaikh, T.J.; Sharma, A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Comput. Netw.* **2019**, *149*, 29–42. [CrossRef]
24. Lyu, Q.; Zheng, N.; Liu, H.; Gao, C.; Chen, S.; Liu, J.J.I.A. Remotely access "My" smart home in private: An antitracking authentication and key agreement scheme. *IEEE Access* **2019**, *7*, 41835–41851.
25. Ma, M.; He, D.; Wang, H.; Kumar, N.; Choo, K.-K.R. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. *IEEE Internet Things J.* **2019**, *6*, 8065–8075. [CrossRef]
26. Renuka, K.M.; Kumari, S.; Zhao, D.; Li, L. Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems. *IEEE Access* **2019**, *7*, 51014–51027. [CrossRef]
27. Li, X.; Peng, J.; Obaidat, M.S.; Wu, F.; Khan, M.K.; Chen, C. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Syst. J.* **2019**, *14*, 39–50. [CrossRef]
28. Shuai, M.; Yu, N.; Wang, H.; Xiong, L. Anonymous authentication scheme for smart home environment with provable security. *Comput. Secur.* **2019**, *86*, 132–146. [CrossRef]

29. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Park, Y. An efficient, anonymous and robust authentication scheme for smart home environments. *Sensors* **2020**, *20*, 1215. [CrossRef]
30. Xiang, A.; Zheng, J. A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks. *Electronics* **2020**, *9*, 989. [CrossRef]
31. Oh, J.; Yu, S.; Lee, J.; Son, S.; Kim, M.; Park, Y. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors* **2021**, *21*, 1–24.
32. NIST, U.S. *Department of Commerce. Secure Hash Standard, U.S. Federal Information Processing Standard (FIPS)*; NIST, U.S. Department of Commerce: Gaithersburg, MD, USA, 2002.
33. AAEON. Available online: http://www.aaeon.com/tw/ (accessed on 1 March 2021).