An efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features

Tsung-Hung Lin[1, *], Kuan-Han Chen[1]

ABSTRACT

In recent years, the Industrial Internet of Things has driven the development of smart manufacturing. Many machines have begun to be connected via the Internet and used for automated control and production. The Internet of Things integrates communication with various heterogeneous devices, which brings a lot of conveniences. Because of the convenience of IoT, people increasingly rely on these devices to obtain daily information, making devices connected to the Internet of Things vulnerable to cyberattacks. To ensure the integrity, security, and low latency of data transmission to avoid the production shutdowns in the Industrial Internet of Things, this article proposes an efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features. This scheme has robust security to protect data from being modified by the attacker and integrates the physical hardware features of the device into the key agreement schemes, replacing the previous method that only uses software calculations to achieve high-efficiency key calculation speed.

Keywords: Cyber Security, PUF, Key Agreement, IIoT.

I. INTRODUCTION

Internet of Things (IoT) is a technology that using the Internet to make devices that allow connecting to the Internet simply. Nowadays, mobile phones, tablets, and computers can use the Internet to communicate with each other; even those household appliances, which were considered unable to connect to the Internet in the past, can also start to communicate with each other through the Internet. IoT and the Internet have brought considerable convenience to people, and it can range from a Wireless Body Area Network (WBAN) from personal area to public infrastructure such as medical device, environmental control systems and industrial IoT systems, etc., can integrate communications heterogeneous devices through the Internet of Things.

In recent years, the Industrial Internet of Things (IIoT) has driven the development of smart manufacturing. Many machines have begun to connect through the Internet and are used for automated control and production. The confidentiality, integrity, and availability of data in the process of machine communication are important issues in today's IIoT environment. However, robust security authentication schemes ensure the consistency and correctness of session keys during the data transmission is also an important issue. When the factory administrator is remotely controlling the machine to produce products, the eavesdropping of malicious attackers in the communication is a considerable threat to the production line. Because malicious attackers can hack into the communication channel to steal the required information or introduce

[*] *Corresponding Author: Tsung-Hung Lin*
(E-mail: duke@ncut.edu.tw).
Author: Kuan-Han Chen
(E-mail: jasper86114@gmail.com).
[1]*Department of Computer Science and Information Engineering, National Chin-Yi University of Technology, No.57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan*

viruses during the communication process, causing the machine and system to paralyze and shutdown the production. So, when the machine and data are not adequately protected and leaked, the damage will be more serious than in the past. Ensuring the confidentiality, integrity, and availability of data in the proposed key agreement and establishing a secure authentication scheme method to resist massive, unpredictable, and complex attacks have become more critical.

In the past, people used biometrics, such as fingerprints, iris, palm prints, voice, or face, as a method of identity authentication because these features are unique to everyone, and they do not need to worry about losing or copying [1]. Similar to the biometric of human beings, Physical Unclonable Function (PUF) uses the physical factors of the device to identify the device. These features are also called the biometric of the device. Because they are easy to manufacture and the physical factors that occur during the manufacturing process are generated randomly, such as temperature and humidity during manufacturing, these factors cannot be predicted and controlled. They cannot wholly clone the same item, even if they re-produced again [2]. In 2001, Pappu et al. [3] stated that PUF used electrical to stimulate a system or device. The system or device will respond according to the stimulation and forming a Challenge-Response Pair (CRP) [3]. Therefore, PUF began to attract the attention of many cryptography experts and scholars in the field of cryptography and cyber security [4] and began to be used as encryption primitive [5], applying to many technologies, such as Low-cost identity authentication technology [6] [7] [8], key generation [9] [10] [11] and secure communication transmission protocol [2] [12], etc. Therefore, we want to use PUF technology to enhance the key agreement protocol in the current industrial IoT environment to ensure the integrity and security of data transmission.

Since we assume that every device used in the IIoT has a PUF scheme, the certification authority in the proposed scheme is a gateway server and can securely store the information about user and device, such as anonymous identity and CRPs. If the identity of the user and the device is public, the protection of the user and the device is not safe enough. A malicious attacker may carry out against a specific device or specific user (such as a factory supervisor) by Man-in-the-middle attacks and identity forgery. Therefore, the key agreement scheme in this article, the user and the device, need to be protected anonymously. Besides, even a short delay will affect the shutdown of the production line in the environment of IIoT. When the user is operating the device, it needs to have low latency. Furthermore, an ideal key agreement protocol also needs to has high computational efficiency in generating keys at each phase in real-time.

Summarizing the above arguments is to ensure the integrity and security in the IIoT and low latency and low computational cost to avoid production shutdowns. This article proposes an efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features and robust security to protect data from tampering. Besides, we use the physical characteristics of the device; instead of only using software calculations in the past, it has high efficiency in the key operation.

The rest of this article is arranged as follows. Section 2 is the related work of the IIoT key agreement and PUFs, Section 3 is an introduction to the authentication key agreement scheme we proposed in this article, and Section 4 will focus on the security of the authentication key agreement scheme analyzes in this article. Section 5 is the computation cost analysis of the proposed scheme and the conclusion given in Section 6.

II. RELATED WORK

This section will introduce the relevant literature and knowledge that will be used in an efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features, including key agreement technology in the IoT, High-efficiency authentication scheme, physical unclonable function and anonymity authentication scheme.

1. Key Agreement Technology of IIoT

Nowadays, Internet of Things technology is booming, and it has become a trend of modern technology development. Wireless Sensor Network (WSN) is one of the major technologies in IoT, which has a wide range of applications, from wireless human body areas composed of individuals, such as WBAN (Wireless Body Area Network), to large-scale public infrastructures, such as medical equipment, environmental control systems, and IIoT systems. Most scholars have begun to propose various authentication schemes related to IoT in recent years. In 2009, Das et al. [13] proposed a two-factor user authentication in wireless sensor networks and explained that it could resist stolen-verifier attack, replay attack, and password guessing attack [13], but Das et al.'s scheme still cannot resist offline password guessing attack and denial-of-service attack effectively. Therefore, in 2010, Vaidya et al. [14] proposed an improved two-factor user authentication to overcome the shortcomings of Das et al.'s scheme [14]. In fact, there have been many improved schemes proposed since then [15-18]. IoT technology allows people to connect with things for remote access and control. However, it brings much convenience to people’s daily lives; it poses a considerable threat to security and privacy due to IoT devices' heterogeneity because a variety of different devices need to be integrated.

Therefore, some experts and scholars have begun to research the security architecture, framework [19] [20], and key agreement [13-22], which are related to the Internet of Things. In 2019, Mohammad et al. [23] reviewed some authentication key agreement protocols used to protect IoT, compared them in terms of security and performance, and believed that lightweight and mutual authentication are the essential elements to ensure the security of IoT [23].

2. Physically Unclonable Function (PUFs)

In recent years, many scholars have proposed to use biometric (face, iris, fingerprints, etc.) as an authentication method and improved the security of accounts or passwords through these unguessable and forged biometric. However, with the development of the Internet of Things technology, to enhance the security of devices, Physical Unclonable Function (PUF) has begun to be proposed by experts and scholars. PUF is a hardware primitive that uses physical factors while devices were manufacturing to produce unpredictable results. Because of its physical property, the response of PUF cannot be perfectly cloned or duplicate. A set of CRPs generate by PUF can be used to identify the unique feature. Therefore, any tampering behavior of the PUF structure can be easily detected; silicon PUF uses the randomness caused by physical factors while manufacturing to generate a unique response of the device [3]. Silicon PUF is currently the most widely used type of PUF. In the related literature, many experts and scholars have proposed several architectures using silicon PUF, which can be divided into two categories: memory-based PUF and delay-based PUF. Memory-based PUF is like Static Random-Access Memory PUF (SRAM PUF). The initial value of SRAM is random and unpredictable to achieve the PUF function, while delay-based PUF, such as RO PUF and Arbiter PUF, unlike memory-based PUF, change the threshold voltage of electronic components to increase the slight delay and deviation in the path to obtain the corresponding response [12].

3. High-Efficiency Authentication Scheme

In the past, many scholars have researched the identity authentication protocol using the Traditional Public Key Cryptosystem (TPKC) [24] [25] [26], but the authentication method based on TPKC requires a complicated exponential operation. So, the required computational cost is too high to achieve low latency; therefore, an authentication method based on Elliptic Curve

Cryptography (ECC) was subsequently proposed because the key size generated by ECC is smaller than that of TPKC, and it can be realized better computational performance [2] [27]. However, in the ECC-based authentication schemes, the speed of verifying the public key is very slow, which cannot achieve the high computational efficiency, which required by the ideal key agreement protocol, and cannot be used in an actual IIoT environment.

In order to achieve a high computational efficiency key agreement protocol that can be used in the actual IIoT environment, we use PUF, Hash Function, and Exclusive-OR gate (XOR) as the key generation method and compare with the authentication protocol based on TPKC and ECC, it can have lower computational cost and high computational efficiency.

4. Anonymity Authentication Scheme

In the IoT's communication authentication process, the anonymity of users and devices is one of the essential features. To prevent specific users and devices from being tracked and attacked by malicious attackers, many anonymous-related authentication schemes have also been used successively [8] [28]. However, many authentication schemes use the same anonymous identity in each session phase, and they will still be eavesdropped on by malicious attackers under long-term use. Therefore, we have the proposed method designs a one-time random number for users and devices that will update their identity authentication every time to ensure the anonymous identity of the users and the devices and avoid eavesdropping, operating, or controlling by malicious attackers.

III. PROPOSED METHOD

This section discusses an efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features that we proposed in this article. The authentication scheme of PUF is shown in Figure 1, the certificate authority (CA) will give challenges for the device, and the device will derive responses back to CA. The proposed authentication scheme consists of three phases: user registration, device registration, and Identity authentication key agreement. The definition of symbols used in the scheme proposed in this article is shown in Table 1.

1. User registration phase

In the user registration phase, the user needs to register with CA through the following steps, as shown in Figure 2. CA is a gateway server in the proposed scheme and can securely store the information list of users and devices.

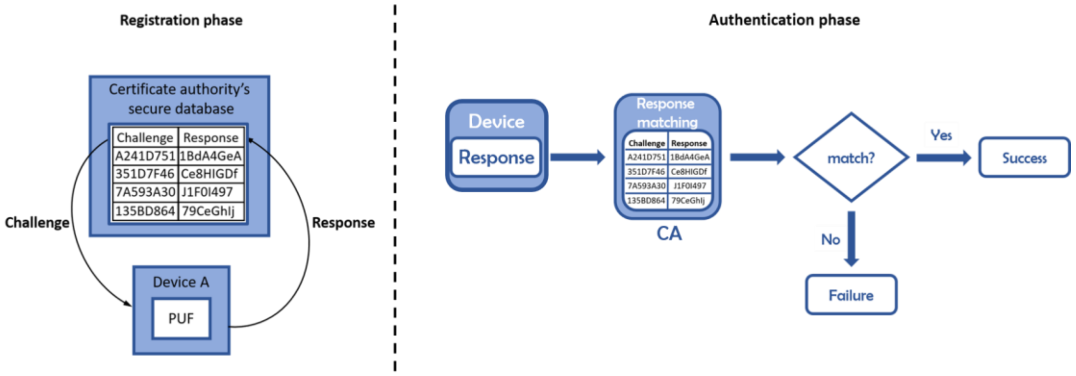
(1) The user U_i enters his biometric BIO_i and sends it to CA via a secure channel.

(2) CA generates $H(BIO_i)$ from the user's biometric BIO_i through the one-way hash function $H(.)$ for biometrics, and then calculates $AID_i = d_s \oplus H(BIO_i) \oplus U_i$, d_s is the secret key of the certification authority, and SU_i is the serial number of the user i and start from 0. After the calculation, the certification authority will one-way hash AID_i with $h(.)$ to get $h(AID_i)$, and store $h(AID_i)$ and SU_i in the database.

(3) CA returns the user's anonymous identity AID_i to U_i to complete the user registration phase.

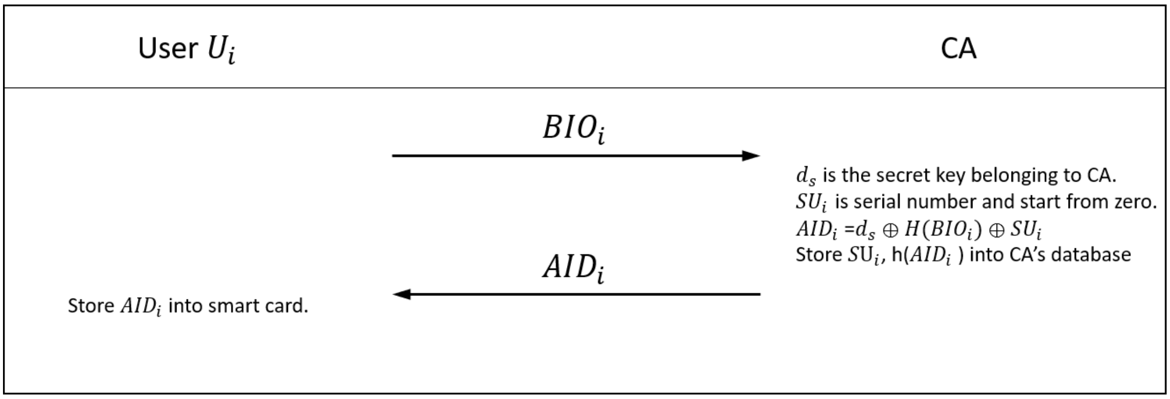
Table 1. Definition of symbols used in proposed scheme

Symbol	Description
CA	Certificate authority
d_s	The secret key used by CA
U_i	The i_{th} user
N_p	The p_{th} device
BIO_i	The biometric of the i_{th} user
ID_p	The ID of p_{th} device
AID_i	Temporary identity of the i_{th} user
TID_p	Temporary identity of the p_{th} device
SU_i	The serial number for the i_{th} user which generated by CA
SD_p	The serial number for the p_{th} device which generated by CA
$h(.)$	One-way hash function
$H(.)$	One-way hash function of biometric



Challenge	Response
A241D751	1BdA4GeA
351D7F46	Ce8HIGDf
7A593A30	J1F0I497
135BD864	79CeGhIj

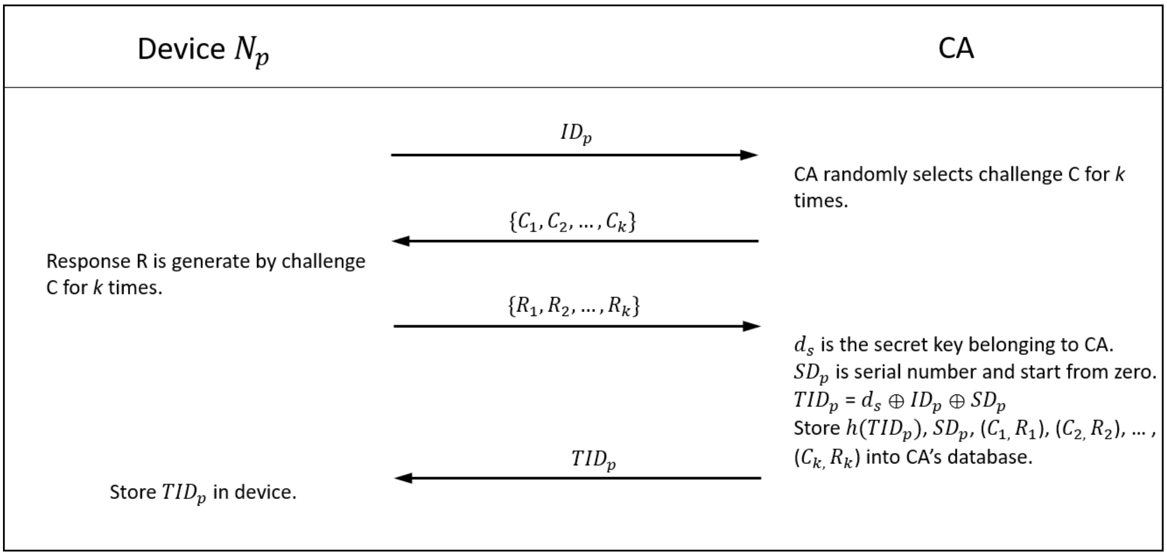
Figure 1. The authentication scheme of PUF.



d_s is the secret key belonging to CA.
SU_i is serial number and start from zero.
AID_i =$d_s \oplus H(BIO_i) \oplus SU_i$
Store SU_i, h(AID_i) into CA's database

Store AID_i into smart card.

Figure 2. Proposed user registration phase.



CA randomly selects challenge C for *k* times.

Response R is generate by challenge C for *k* times.

d_s is the secret key belonging to CA.
SD_p is serial number and start from zero.
TID_p = $d_s \oplus ID_p \oplus SD_p$
Store $h(TID_p)$, SD_p, (C_1, R_1), (C_2, R_2), … , (C_k, R_k) into CA's database.

Store TID_p in device.

Figure 3. Proposed device registration phase.

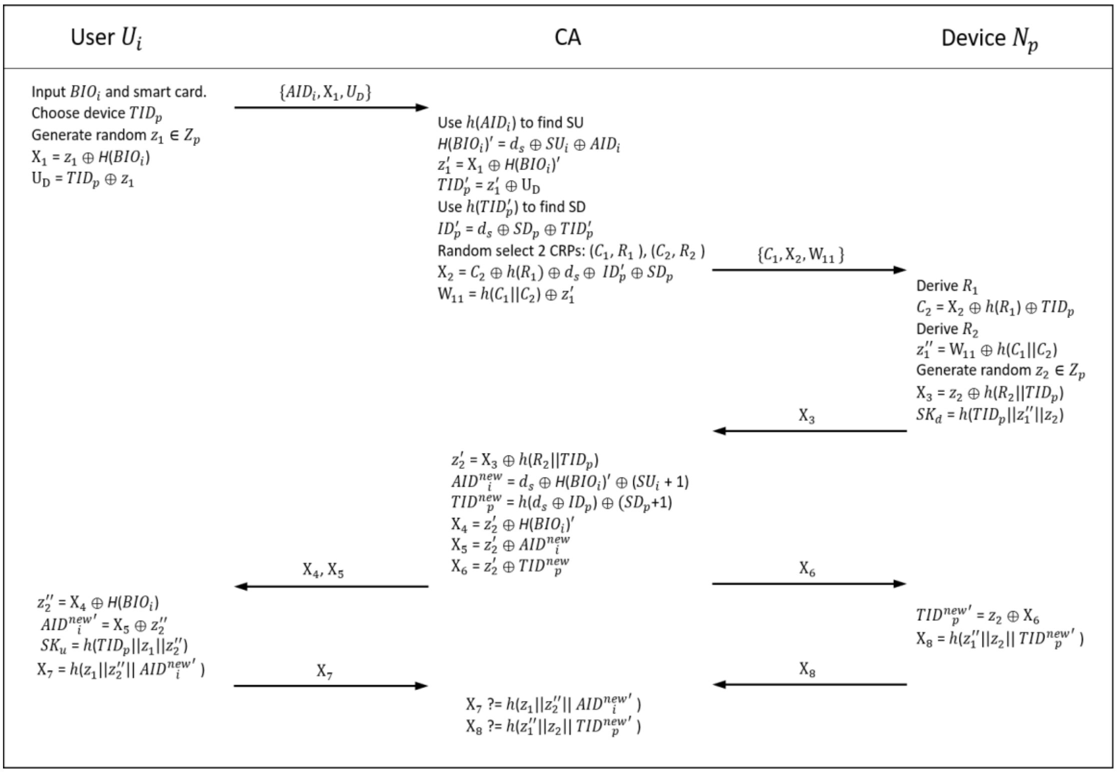

User U_i
CA
Device N_p
Input BIO_i and smart card.
Choose device TID_p
Generate random $z_1 \in Z_p$
$X_1 = z_1 \oplus H(BIO_i)$
$U_D = TID_p \oplus z_1$
$\{AID_i, X_1, U_D\}$
Use $h(AID_i)$ to find SU
$H(BIO_i)' = d_s \oplus SU_i \oplus AID_i$
$z_1' = X_1 \oplus H(BIO_i)'$
$TID_p' = z_1' \oplus U_D$
Use $h(TID_p')$ to find SD
$ID_p' = d_s \oplus SD_p \oplus TID_p'$
Random select 2 CRPs: (C_1, R_1), (C_2, R_2)
$X_2 = C_2 \oplus h(R_1) \oplus d_s \oplus ID_p' \oplus SD_p$
$W_{11} = h(C_1||C_2) \oplus z_1'$
$\{C_1, X_2, W_{11}\}$
Derive R_1
$C_2 = X_2 \oplus h(R_1) \oplus TID_p$
Derive R_2
$z_1'' = W_{11} \oplus h(C_1||C_2)$
Generate random $z_2 \in Z_p$
$X_3 = z_2 \oplus h(R_2||TID_p)$
$SK_d = h(TID_p||z_1''||z_2)$
X_3
$z_2' = X_3 \oplus h(R_2||TID_p)$
$AID_i^{new} = d_s \oplus H(BIO_i)' \oplus (SU_i + 1)$
$TID_p^{new} = h(d_s \oplus ID_p) \oplus (SD_p+1)$
$X_4 = z_2' \oplus H(BIO_i)'$
$X_5 = z_2' \oplus AID_i^{new}$
$X_6 = z_2' \oplus TID_p^{new}$
X_4, X_5
X_6
$z_2'' = X_4 \oplus H(BIO_i)$
$AID_i^{new'} = X_5 \oplus z_2''$
$SK_u = h(TID_p||z_1||z_2'')$
$X_7 = h(z_1||z_2''||AID_i^{new'})$
$TID_p^{new'} = z_2 \oplus X_6$
$X_8 = h(z_1''||z_2||TID_p^{new'})$
X_7
X_8
X_7 ?= $h(z_1||z_2''||AID_i^{new'})$
X_8 ?= $h(z_1''||z_2||TID_p^{new'})$

Figure 4. Proposed identity authentication key agreement phase.

2. Device registration phase

In the device registration phase, the device needs to register with CA through the following steps, as shown in Figure 3.

(1) The device N_p sends ID_p to CA through a secure channel.

(2) Randomly select *k* times of challenge, and send TID_p to the device Np.

(3) To send back k responses to CA.

(4) CA calculates TIDp = ds ⊕ IDp ⊕ SDp, where ds is the secret key of CA, and SDp is the serial number of the device p starts from 0 and store the h(TIDp), SDp, (C1, R1), ... , (Ck, Rk) in the CA's database.

(5) The device N_p stores TID_p to complete the registration phase of the device.

3. Identity authentication key agreement phase

After the user and device registration phase, it will go in the identity authentication and key agreement phase. At this phase, the user can connect to CA through the Internet for identity authentication and key agreement. The key will be generated through the schemes which we designed, and then the user can communicate with the device, as shown in Figure 4.

(1) The user U_i uses a smart card and enters his biometric BIO_{i} and selects the device N_p which U_i wants to connect with. The user U_i will randomly generate a one-time random number $z_1 \in Z_{\mathrm{p}}$, and use z_1 and $H(BIO_i)$ to calculate $X_i = z_1 \oplus H(BIO_i)$ and use TID_p and z_1 calculate $U_D = TID_p \oplus z_1$, and then send $\{AID_i, X_1, U_D\}$ to the certification authority (CA).

(2) When the certification authority receives $\{AID_i, X_1, U_D\}$, AID_i calculates $h(AID_i)$ through $h(.)$ and uses $h(AID_i)$ to find the serial number SU_i of the user U_i. The certification authority (CA) uses the secret key d_s and the serial number SU_i to calculate $H(BIO_i)' = \mathrm{d}_s \oplus SU_i \oplus AID_i$, and then calculates $z_1' = X_1 \oplus H(BIO_i)'$, $TID_p' = z_1' \oplus U_D$, calculate $h(TID_p')$ to find out the serial number of the device Np in the certification authority(CA) database SDp, and randomly select two

CRP-(C1, R1), (C2, R2) from the CA database, and finally calculate X2 = $C2 \oplus h(R2) \oplus ds \oplus IDp' \oplus SDp$ and W11 = $h(C1 \| C2) \oplus z1'$, send {$C1$, X2, W11} to the device Np.

(3) After the device Np receives {$C1$, X2, W11}, it will derive R1 from C1, and then calculate $C2$ = X2 $\oplus h(R1) \oplus TIDp$, derive R2 by C2, calculate $z1'$ = W11 $\oplus h(C1 \| C2)$, and generate a one-time random number $z2 \in Zp$, finally calculate X3 = $z2 \oplus h(R2 \| TIDp)$and $SKp = h(TIDp \| z1'' \| z2)$, and send X3 to the certification authority.

(4) When the certification authority receives X3, it uses X3 to calculate $z2'$= X3 $\oplus h(R2 \| TIDp)$, and calculates $AID\ inew = ds \oplus$ H(BIOi)' $\oplus$ (SUi + 1) and $TID\ pnew = h(ds \oplus IDp) \oplus (SDp + 1)$, and finally calculates X4 = $z2' \oplus$ H(BIOi)' , X5 = $z2' \oplus AIDinew$ and X6 = $z2' \oplus$ TIDinew, sending X4, X5 to user Ui, and sending X6 to the device Np.

(5) After the user Ui receives X4 and X5, it calculates $z2''$ = X4 $\oplus$ H($BIOi$) by X4 and use X5 to calculates AIDinew = X5 $\oplus z2''$, SKu = $h(TIDp \| z1 \| z2'')$, finally, calculate X7 = $h(z1 \| z2'' \| AIDinew')$, and send X7 to the certification authority (CA).

(6) When the user Ui receives X4 and X5, the device Np will receive X6, and X6 is used to calculate $TIDpnew'$ = $z2 \oplus$ X6. After that, device will calculate X8 = $h(z1'' \| z2 \| TIDpnew')$and send X8 to the certification authority(CA).

(7) Finally, after the certification authority (CA) receives X7 and X8, it will verifies whether X7 ?= h(z1 ‖ z2” ‖ AIDinew) and X8 ?= $h(z1'' \| z2 \| TIDpnew')$ is correct or not. If X7 and X8 have verify, the certification authority (CA) will update $h(AID_i) = h(AID_i^{new})$, $SU_i = SU_i + 1$, and $h(TID_p) = h(TID_p^{new})$, $SD_p = SD_p + 1$ to complete the key agreement.

User U_i

$$\begin{aligned}
SK_u &= h(TID_p||z_1||z_2''), z_1 \in Z_p \\
z_2'' &= \mathrm{X}_4 \oplus H(BIO_i) \\
&= z_2' \oplus H(BIO_i)' \oplus H(BIO_i) \\
&= z_2' \oplus H(BIO_i)' \oplus H(BIO_i) \\
&= \mathrm{X}_3 \oplus h(R_2||TID_p) \oplus H(BIO_i)' \oplus H(BIO_i) \\
&= z_2 \oplus h(R_2||TID_p) \oplus h(R_2||TID_p) \oplus H(BIO_i)' \oplus H(BIO_i) \\
&= z_2
\end{aligned}$$

Figure 5. The session key calculation of user.

Device N_p

$$\begin{aligned}
SK_d &= h(TID_p||z_1||z_2''), z_2 \in Z_p \\
z_1'' &= \mathrm{W}_{11} \oplus h(C_1||C_2) \\
&= z_1' \oplus h(C_1||C_2) \oplus h(C_1||C_2) \\
&= \mathrm{X}_1 \oplus H(BIO_i)' \\
&= z_1 \oplus H(BIO_i) \oplus H(BIO_i)' \\
&= z_1
\end{aligned}$$

Figure 6. The session key calculation of device.

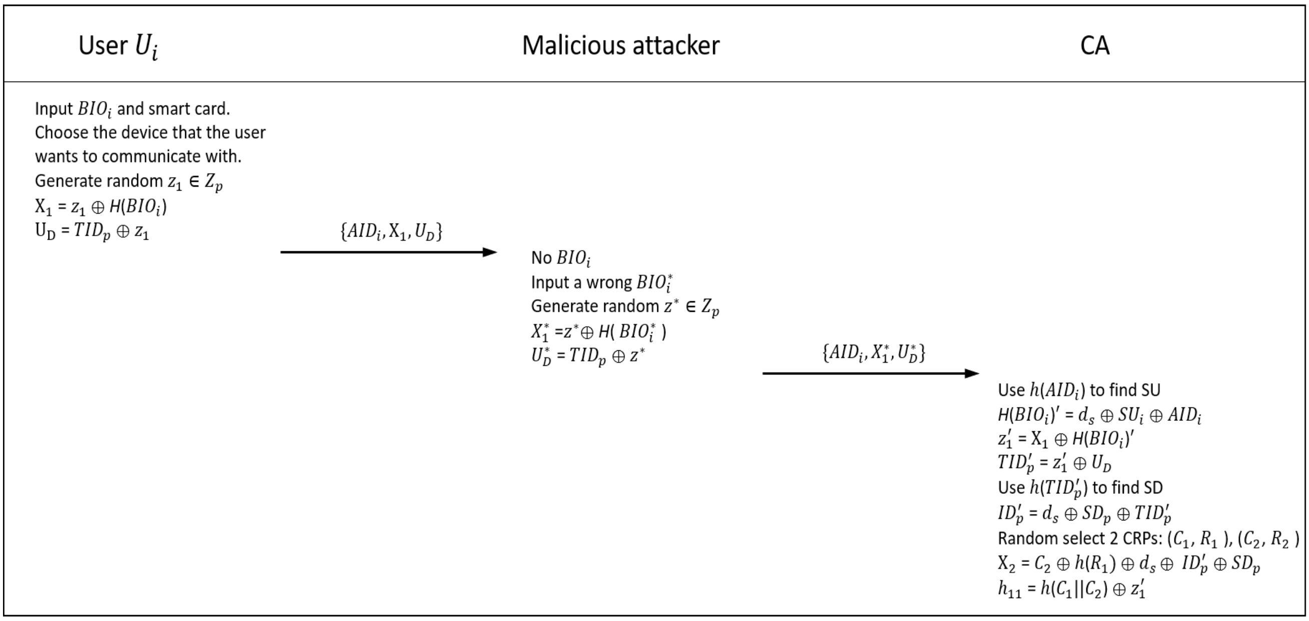

User U_i
Malicious attacker
CA
Input BIO_i and smart card.
Choose the device that the user wants to communicate with.
Generate random $z_1 \in Z_p$
$X_1 = z_1 \oplus H(BIO_i)$
$U_D = TID_p \oplus z_1$
$\{AID_i, X_1, U_D\}$
No BIO_i
Input a wrong BIO_i^*
Generate random $z^* \in Z_p$
$X_1^* = z^* \oplus H(BIO_i^*)$
$U_D^* = TID_p \oplus z^*$
$\{AID_i, X_1^*, U_D^*\}$
Use $h(AID_i)$ to find SU
$H(BIO_i)' = d_s \oplus SU_i \oplus AID_i$
$z_1' = X_1 \oplus H(BIO_i)'$
$TID_p' = z_1' \oplus U_D$
Use $h(TID_p')$ to find SD
$ID_p' = d_s \oplus SD_p \oplus TID_p'$
Random select 2 CRPs: (C_1, R_1), (C_2, R_2)
$X_2 = C_2 \oplus h(R_1) \oplus d_s \oplus ID_p' \oplus SD_p$
$h_{11} = h(C_1 || C_2) \oplus z_1'$

Figure 7. A man-in-the-middle attack in proposed schemes.

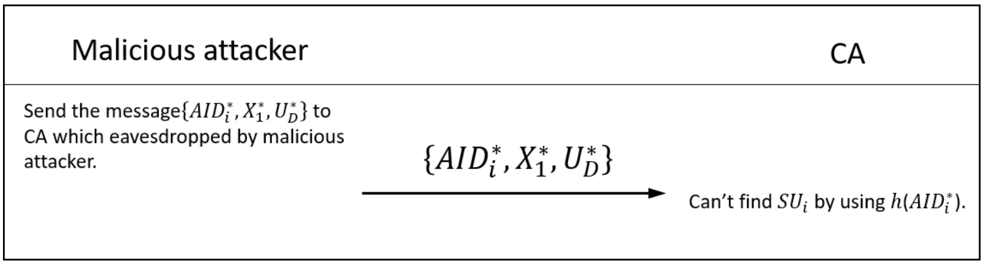

Malicious attacker
CA
Send the message$\{AID_i^*, X_1^*, U_D^*\}$ to CA which eavesdropped by malicious attacker.
$\{AID_i^*, X_1^*, U_D^*\}$
Can't find SU_i by using $h(AID_i^*)$.

Figure 8. Replay attack between user and CA.

IV. SECURITY ANALYSIS

In this section, we discuss the security analysis of the proposed schemes. In order to meet the characteristics of IIoT, this article illustrates availability and integrity.

Besides, to ensure secure and confidential communication between the user side and the device side during the key agreement process. This study provides proofs to ensure users' and devices' anonymity and be able to counter man-in-the-middle attacks (MITM) effectively. The proposed scheme also provides evidence that it can resist identity impersonation attacks, replay attacks, stolen-verifier attacks (SV attacks), and internal privilege attacks. It also illustrates that the proposed protocol has perfect forward secrecy and session key security.

1. Data integrity and availability

The critical thing in IIoT is data integrity and availability to ensure correct transmission. The data integrity means that after the key agreement is successfully complete, the user and device can get a symmetric key that others cannot know, so they can encrypt, decrypt and transmit data securely like a secure tunnel ensuring the integrity of the data.

During the data transmission process, it must be ensured that the data is correct during the agreement and has not been tampered with by malicious attackers. Therefore, the conference key generated by the user and the device during the key agreement phase must be the same. Therefore, we will prove that when the user U_i, certification authority CA, and the device N_p has not lost any data, the session keys generated by both parties are the same, as shown in Figure 5 and Figure 6.

2. The anonymity of users and devices

With the rapid development of the Internet of Things, it has connected computers and communication devices in the past and a series of other gadgets used in our daily lives. Nowadays, people's identities and privacy need to be protected, but device identities protection is gradually becoming important. In the key agreement schemes proposed in this article, in addition to the use of anonymous user identity *AID* and device identity *TID*, the user and device are given new *AID*s and *TID*s after each key agreement phase to avoid long-term use. Use the same identity for key agreement, causing specific users and devices to be tracked and attacked by malicious attackers.

3. Man-in-the-middle attack

Man-in-the-middle attack means that while a user or a device is communicating, a malicious attacker establishes the connection between the two parties and conducts eavesdropping, thereby obtaining or tampering with the data between the two parties. The communication can operate normally as usual. Therefore, it is difficult to detect a man-in-the-middle attack.

When a malicious attacker wants to eavesdrop on the key agreement process through a man-in-the-middle attack, the process is shown in Figure 7.

Usually, the user performs calculations and sends the message $\{AID_i, X_1, U_D\}$ to the certification authority. Since the malicious attacker has been eavesdropping in the middle, the message $\{AID_i, X_1, U_D\}$ will be sent to the malicious attacker first. However, the malicious attacker does not have the user's BIO_i^*, so the malicious attacker cannot know z_1 through X_1, and can only generate fake biometric BIO_i^* through forgery, calculate the fake message X_1^*, and fake U_D, and finally send it to the certification authority. When certification authority receives $\{AID_i, X_1^*, U_D*\}$, because BIO_i^* is not the correct user's biometrics, it will cause the user, malicious attacker and certification authority 's messages to be asymmetry, leading to authentication errors.

If a malicious attacker intercepts the message X_3 that the device N_p send to the certification authority, because the malicious attacker does not know the R_2, which generated by the device N_p, he cannot know the value of $h(R_2 || TID_p)$. Because z_2' is calculated by $X_3 \oplus h(R_2 || TID_p)$, it will cause the z_2 of the user, malicious attacker and certification authority to be asymmetry, leading to authentication errors.

4. Replay attack

A malicious attacker captures a certain transmitted message and uses the obtained message to repeatedly send it to the certification authority, which is called replay attack. When a malicious attacker intends to use replay attack, as shown in Figure 8, AID_i^*, X_i^* and $U_D{}^*$ are the messages stolen by the malicious attacker. Due to the schemes in this article, each time, the SU_i and SD_p used by users and devices are different, resulting in different AID_i and TID_p at each stage. Even if a malicious user steals a message through eavesdropping, the certification authority still cannot pass the old AID_i and TID_p to find out the corresponding SU_i and SD_p, and will reject the request which sent by the malicious attacker. And in this article, we use two random pairs of CRPs as the method to generate X_2 and W_{11}. Even if a malicious attacker steals the message sent from the previous certification authority to the device, he still cannot use the old R_1 and R_2 to verified successfully, so replay attacks between the device and CA can be prevented in this scheme, as shown in Figure 9.

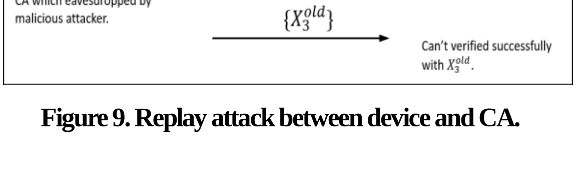

Malicious attacker
CA
Send the message $\{X_3^{old}\}$ to CA which eavesdropped by malicious attacker.
$\{X_3^{old}\}$
Can't verified successfully with X_3^{old}.

Figure 9. Replay attack between device and CA.

5. Identity impersonation attack

Identity impersonation attacks are when an attacker pretends to be a trusted user to deceive the system. When a malicious attacker intends to deceive CA through a fake identity, because the malicious user doesn't know the correct biometric BIO_i of the original user, the malicious attacker enters the fake biometric BIO_i^* and sends {AID_i , X_i^*,C_p} to CA, when CA receives {AID_i, X_i^*,C_p}, because of the $H(BIO_i^*)$ does not match $H(BIO_i)$, the malicious attacker calculated z_1^* will not be equal to z_1 calculated by CA. In addition, when a malicious user wants to crack the session key SK through z_1 and z_2, since z_2 is also encrypted and protected by the original user's biometrics, the malicious user still cannot crack the session key SK.

When a malicious attacker wants to send data by impersonating a fake device, because the malicious attacker does not know the response message sent by the device to the certification authority, he cannot correctly respond to the challenge from the certification authority, resulting in authentication errors. Therefore, the schemes in this article can resist the fake Pretend to attack.

6. Stolen-Verifier attack

In the authentication schemes proposed in this article, the CA verification table contains the user's serial number SU_i, the device serial number SD_p, the k pieces CRPs of the device, and $h(AID_i)$ and $h(TID_p)$ which have been hash. When a malicious attacker obtains the verification table stored in CA through some methods, he wants to use the information in the verification table to impersonate the user and obtain $h(AID_i)$ and $h(TID_p)$, but because the hash function has irreversible characteristics, it cannot obtain the user's AID and the device's TID, but also cannot obtain $H(BIO_i)$ which protected by d_s and SU_i, and can protect ID_p by using ds and SD_p; therefore, the schemes in this article can resist stolen-verifier attack.

7. Insider attack

Internal personnel enable them to use the system legally. The purpose is to allow personnel to perform their duties. However, insider attacks refer to the internal personnel who used these permissions to circumvent any security controls they know through their legal authentication. Moreover, they disguise other legitimate users to get the private key d_s of CA. Since the private key d_s is only known by CA, it cannot be obtained by legitimate internal users. In addition, the device in this article uses PUF's CRP to verify its identity with the certification authority, and other devices cannot know the CRP of other devices through their own CRP. So, the schemes in this article can resist insider attacks.

8. Perfect forward secrecy and session key security

In cryptography, perfect forward secrecy means that when a malicious attacker obtains the session key of a particular session through some methods, it is necessary to protect the session key generated in the past and the future from being leaked, even if the session key in the past is leaked, the encrypted ciphertext still has confidentiality and will not be cracked by malicious attackers.

The schemes in this article, one-time random numbers z_1 and z_2 are used and randomly generated by both the user and the device, and within the valid time of the session key, the malicious attacker cannot calculate the session key SK, which we calculate with the one-way hash function, so the schemes in this article provide perfect forward secrecy and session key security.

V. COMPUTATION COST ANALYSIS

This section will discuss the computation costs of the proposed authentication and key agreement schemes in this article. To better understand the symbols of computation costs, the symbols are defined in table 2. The execution time of T_X, $T_{HF,}$ and T_{PUF} are 0.0007ms, 0.009ms, and 1ns, respectively.

Table 2. Proposed notations of computation costs.

Notation	Describe
T_{HF}	The execution time of one-way hash function
T_X	The execution time of exclusive-or function
T_{PUF}	The execution time of physical unclonable function

Table 3. The proposed computation costs.

User	CA	Device
$4T_X + 2T_{HF}$	$18T_{X+}6T_{HF+}3T_{PUF}$	$5T_X + 5T_{HF} + 3T_{PUF}$

In the proposed efficient IIoT cyber security authentication schemes using PUF circuit features for fast seamless adaptive key agreement, there are two operations that will be calculated by the user, including 4 times T_X and 2 times T_{HF}. The certification authority in the proposed process of identity authentication and key agreement will calculate with three operations, including 18 times T_X, 6 times T_{HF} and 3 times T_{PUF}. In the proposed process of identity authentication and key agreement, the device uses 5 times T_X, 5 times T_{HF} and 3 times T_{PUF}. The computation costs in the proposed schemes are shown in Table 3. Therefore, the efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features proposed in this article has low computational costs.

VI. CONCLUSION

The Industrial Internet of Things drives the development of smart manufacturing. Many machines are connected with the Internet for automated control. However, it is necessary to have robust security authentication schemes to ensure the consistency and correctness of session key when the data transmission and to ensure that it will not be modified by the malicious attacker during the process in today's IIoT environment, so many scholars have proposed a lot of authentication schemes related to IoT. In the past, people used biological characteristics as a method to achieve identity authentication. Nowadays, not only humans but also device identity authentication has become important as well. Like the biological characteristics of human beings, the physical factors of the devices are different when manufactured. Physical Unclonable Function (PUF) uses the physical factor to identify the device. Because malicious attackers have a great chance of performing man-in-the-middle attacks and identity forgery against a specific device or specific user, we need to protect the user and the device. Therefore, PUF-based authentication schemes have been proposed. Unlike the past, we proposed a PUF-based authentication scheme that can protect the device not only by PUF but also anonymized the identity of the device.

In order to ensure the integrity and security of data transmission in the Industrial Internet of Things, and to avoid the short delay in communication and has the low computational cost, we replaced the key agreement in the past, which used pure software calculation methods by using the circuit features of the device. The physical features of PUF are integrated into the key agreement schemes to achieve high-efficiency key operation and low computation costs to protect the user and the device; an efficient adaptive key agreement scheme for IIoT cyber security authentication using PUF circuit features is proposed.

REFERENCES

[1] Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An introduction to biometric authentication systems, *Biometric Systems (pp. 1-20). Springer*, London.

[2] Braeken, A. PUF Based Authentication Protocol for IoT. *Symmetry* 2018, 10, 352. https://doi.org/10.3390/sym10080352

[3] PAPPU, Ravikanth, et al. Physical one-way functions. *Science*, 2002, 297.5589: 2026-2030.

[4] Lanxiang Chen, A framework to enhance security of physically unclonable functions using chaotic circuits, *Physics Letters* A,Volume 382, Issue 18, 2018, Pages 1195-1201, ISSN 0375-9601.

[5] Guajardo∗ J. (2011) Physical Unclonable Functions (PUFs). In: van Tilborg H.C.A., Jajodia S. (eds) *Encyclopedia of Cryptography and Security. Springer*, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_912.

[6] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, USA,

2007, pp. 9-14.

[7] W. Che, F. Saqib and J. Plusquellic, "PUF-based authentication," *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Austin, TX, USA, 2015, pp. 337-344, doi: 10.1109/ICCAD.2015.7372589.

[8] Tahavori, Mahdi, and Farokhlagha Moazami. "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid." *Peer-to-Peer Networking and Applications 13 (2020)*: 1616-1628.

[9] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching," *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, San Diego, CA, USA, 2011, pp. 128-133, doi: 10.1109/HST.2011.5955010.

[10] J. Delvaux, D. Gu, D. Schellekens and I. Verbauwhede, "Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 889-902, June 2015, doi: 10.1109/TCAD.2014.2370531.

[11] Maes, Roel, Anthony Van Herrewege, and Ingrid Verbauwhede. "PUFKY: A fully functional PUF-based cryptographic key generator." *International Workshop on Cryptographic Hardware and Embedded Systems. Springer*, Berlin, Heidelberg, 2012.

[12] Barbareschi, Mario, Alessandra De Benedictis, and Nicola Mazzocca. "A PUF-based hardware mutual authentication protocol." *Journal of Parallel and Distributed Computing 119 (2018)*: 107-120.

[13] M. L. Das, "Two-factor user authentication in wireless sensor networks", *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086-1090, March 2009, doi: 10.1109/TWC.2008.080128.

[14] Vaidya, B., Makrakis, D., & Mouftah, H. T. (2010). Improved two-factor user authentication in wireless sensor networks. *IEEE 6th international conference on wireless and mobile computing, networking and communications (WiMob)*, 2000 (pp. 600–606)

[15] Hsieh, W. B., & Leu, J. S. (2014). A Robust User Authentication Scheme sing Dynamic Identity in Wireless Sensor Networks. *Wireless personal communications*, 77(2), 979-989.

[16] H. Garg and M. Dave, "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777334.

[17] Turkanović, Muhamed, Boštjan Brumen, and Marko Hölbl. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion." *Ad Hoc Networks 20 (2014)*: 96-112.

[18] Chen, Tien-Ho, and Wei-Kuan Shih. "A robust mutual authentication protocol for wireless sensor networks." *ETRI journal 32.5 (2010)*: 704-712.

[19] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel and D. Mosse, "Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes," *2012 Eighth International Conference on Intelligent Environments*, Guanajuato, 2012, pp. 206-213, doi: 10.1109/IE.2012.57.

[20] Beheshti-Atashgah, Mohammad, et al. "Security and Privacy-preserving in e-health: a new framework for patient." *Internet of Things (2020)*: 100290.

[21] D. Shin, K. Yun, J. Kim, P. V. Astillo, J. Kim and I. You, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks," *IEEE Access*, vol. 7, pp. 142531-142550, 2019, doi: 10.1109/ACCESS.2019.2943929.

[22] Zhang, Yinghui, et al. "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things." *Journal of Network and Computer Applications 123 (2018)*: 89-100.

[23] Z. Mohammad, A. Abusukhon and T. A. Qattam, "A Survey of Authenticated Key Agreement Protocols for Securing IoT," *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, Amman, Jordan, 2019, pp. 425-430, doi: 10.1109/JEEIT.2019.8717529.

[24] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM 21.2 (1978)*: 120-126.

[25] Shamir, Adi. "Identity-based cryptosystems and signature schemes." *Workshop on the theory and application of cryptographic techniques. Springer*, Berlin, Heidelberg, 1984.

[26] Nalla, Divya, and K. Chandrasekhar Reddy. "Signcryption scheme for Identity-based Cryptosystems." *IACR Cryptol. ePrint Arch. 2003 (2003)*: 66.

[27] Chandrasekar, A., V. R. Rajasekar, and V. Vasudevan. "Improved authentication and key agreement protocol using elliptic curve cryptography." *International Journal of Computer Science and Security 3.4 (2009)*: 325-333.

[28] Alshahrani, Mohammed, and Issa Traore. "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain." *Journal of information security and applications 45 (2019)*: 156-175.

Tsung-Hung Lin (Orcid: 0000-0002-5601-4415) received the Ph.D. degree in Computer Science and Information Engineering from the National Chung Cheng University, Taiwan, R.O.C. He joined the faculty of Department of Computer Science and Information Engineering at National Chin-Yi University of Technology, Taiwan, R.O.C., and has been as a full professor. His research interests include Industry Cyber Security, Artificial Intelligence, Machine Learning, Big Data, Cloud Computing, IoT applications, Steganography, and Wireless Sensor Network.

Kuan-Han Chen received the BEng degree in Information and Communication Engineering from the Chaoyang University of Technology, Taiwan, R.O.C. He is currently working toward the MEng degree in Department of Computer Science and Information Engineering at National Chin-Yi University of Technology, Taiwan, R.O.C. His research interests include Industry Cyber Security, Internet of Things, Steganography, and information security.