A Complete User Authentication and Key Agreement Scheme Using Cancelable Biometrics and PUF in Multi-Server Environment

Hui Zhang, Weixin Bian, Biao Jie, Deqin Xu, and Jun Zhao

***Abstract*— With the current development and popularization of biometrics recognition technology, our biometrics and other identity information may be illegal bulk scalping, and there is the possibility of being used for false enrolment, network fraud and other illegal criminal activities. Although some network platforms based on biometrics recognition adopt multi-identity authentication, network hacking technology is also improving constantly. Therefore, we must not ignore the importance of biometrics data protection. To this end, we propose a complete user authentication protocol and key agreement scheme based on cancelable biometrics and physical unclonable function (PUF). Firstly, cancelable biometrics are generated by efficient biometrics fusion processing which called "PUF-TTM" (Template Transformation Method) using a PUF embedded into the device. Then based on Biometrics-as-a-Service (BaaS) model and secret sharing technology, a complete authentication protocol in multi-server environment is designed, and the robustness, effectiveness and security of our proposed scheme are ensured from the perspective of performance and security analysis.**

***Index Terms*— Cancelable biometrics, privacy preserving, authentication, physical unclonable functions, multi server.**

I. Introduction

As MORE and more applications are hosted on different servers, biometrics as remote authentication credentials are becoming more common. Compared with the traditional password-based authentication system, biometric authentication has obvious advantages [1]. Biometric characteristics can be used as the inherent identity of each person and uniquely identify each individual. It not only has the characteristics of durability and uniqueness, and can resist the random copying and malicious tampering of attackers, but also does not rely on the user's memory, so it is convenient and fast to use. However, along with this comes our consideration of the security and privacy of biometrics. Each biometric is unique, and once biometric data is illegally stolen or attacked, it will be permanently lost to the user. However, with the continuous improvement of network hacking technology, the popularization of multi-server environment and automatic identification technology, we need more secure strategies to protect biometrics data and resist various common attacks. Face recognition, as a popular way of biometric recognition, has the characteristics of real-time, accurate, stable, non-contact, and comprehensive infiltration into all aspects of our lives. And our face information, is not just a group of "face photos", behind it contains us such as ID number, bank card number and a series of sensitive information and our life and property safety. So, in this situation, all users are in a weak position, we need to use biometrics to complete the identity authentication, but we can't afford to lose them. Once our face information is lost, the security risks are immeasurable. This is also the reason why more and more researchers have invested in the field of biometric template protection in recent years.

Biometric template protection can be divided into Cancelable Biometrics (CB) and Biometrics Cryptosystem [2]. We will focus on the former here. The concept of CB was first proposed in 2007, and was later defined by Rathageb et al as a method comparison biometric templates in the transformation domain after intentional transformation and distortion of biological data [3]. According to the current situation of research in recent years, many scholars have made outstanding progress in this field, and proposed a series of template protection schemes to meet the requirements of non-invertibility, Unlinkability (Diversity), Revocability and Performance [4]–[8]. Non-invertibility refers to the fact that biometric features can easily generate the protected template, but it is difficult to restore the original biological information by inverse transformation of the protected biometric template. Unlinkability refers to the fact that there is no correlation between different biometric templates generated based on the same user's biometric. When a biometric template is attacked, the system can reissue a new protected biometric template for replacement, which is called Revocability. It is the performance requirement of CB to maintain the identification accuracy of the system while ensuring the security of biological information.

Existing remote biometric authentication schemes realize effective security and privacy protection, but most of them are based on single server environment, which cannot meet

Manuscript received February 18, 2021; revised August 20, 2021 and November 2, 2021; accepted November 3, 2021. Date of current version December 3, 2021. This work was supported in part by NSFC under Grant 61976006 and Grant 61902003 and in part by NSF_Anhui (AH) under Grant 2108085MF206. The associate editor coordinating the review of this manuscript and approving it for publication was Walter J. Scheirer. *(Corresponding author: Weixin Bian.)*

The authors are with the School of Computer and Information, Anhui Normal University, Wuhu 241002, China, and also with the Anhui Province Key Laboratory of Network and Information Security, Wuhu 241002, China (e-mail: bwx2353@ahnu.edu.cn).

Digital Object Identifier 10.1109/TIFS.2021.3128826

the current market demand and practical application [9]–[11]. When a user requests to obtain a variety of services provided by the server, multiple registration activities are required which greatly reduces the user experience and increases the risk of biological information leakage. On the other hand, with the popularity of cloud services, if the authentication scheme is still limited to the single-server environment, the biometric authentication system will eventually lose the trust and use of users. In this regard, we use the popular BaaS model to design a complete remote biometric authentication system based on PUF and cancelable biometrics. We propose a template transformation (PUF-TTM) in combination with the response of PUF to generate protected cancelable biometrics, use secret sharing technology to further protect biometrics template and transformation parameters, and secretly transmit information based on the newly proposed feature that PUF can share key, so as to securely complete user identity authentication.

A. Related Work

In 2015, Patel *et al.* [12] conducted a study based on cancelable biometrics, pointing out the importance of improving the protection of biometric templates. By 2019, Kumar [13] made a comprehensive overview of CB in terms of the advanced technologies in recent years. It can be seen that CB, as an emerging research field, has been favored by researchers from different research backgrounds. However, there is still much room for improvement in practicability and performance of the current research results. In 2010, Wang [14] pointed out that we were supposed to improve the protection of biometric templates on changeability and privacy protection, and systematically studied the face recognition method based on random transformation. This paper proposed a sort index number (SIN) approach in order to solve the variability and privacy protection problems of biometric identification system. As a representative cancelable biometrics scheme, Index-of-Max (IoM) generates revocable biometrics template by converting biometrics vector of real number domain to index domain hash code, which greatly enhances the concealment of biometrics information [7]. Recently, however, Atighehchi *et al.* [15] have pointed out that IoM is not as resistant to various attacks as originally claimed, and that this scheme is very vulnerable to both authentication and linking attacks. Compared with IoM, BioHashing, as an instance of random projection, uses the method of projection biometric vector to random subspace, and then binarization processing to generate irreversible binary code to achieve biometric template protection. However, if the transformed biometric and projection matrix are known to the attacker at the same time, all the protection barriers for biological data under this scheme will be broken [16], [17]. The recent rise of deep learning and cloud-based technologies has to some extent promoted the development and innovation of biometric template. Liu *et al.* [18] used deep learning to generate a cancelable template block based on the face and iris, and finished comparison in hash domain. Although the hash in privacy is one of the best, the biometrics are always affected by a lot of noise, causing biometrics are not exactly the same time, the accuracy of the certification result affected by negative. Yang *et al.* [19] using Binary Decision Diagrams (BDD) to generate safe, irreversible and revocable fingervein templates, which are then used as inputs to a Multi-Layer Exterior Learning Machine (ML-ELM) for training and prediction. While improving template protection, the recognition rate based on deep learning needs to be improved. Striking the right balance between performance and template security has always been our biggest challenge.

It is understood that remote biometric authentication system is often faced with four types of attacks, namely, spoofing attack on sensors, database attack, comparator attack and interception and eavesdropping on communication channels. In order to improve the security of authentication system, many authentication systems adopt multi-factor model to deal with various attacks [20], [21]. From the original password authentication scheme, it has gradually developed into multiple authentication factors combining smart card, biometric and other auxiliary information to improve the security and privacy of the system [22], [23]. Sarier [20] proposed an effective Multi-Factor Biometric Authentication (MFBA) protocol, which combined zero-knowledge proof and homomorphic encryption scheme to complete the comparison process in the encryption domain. The security concept of MFBA is defined as user privacy to ensure that user privacy can be realized even if the system is attacked by multiple attacks at the same time. However, in this scheme, the conversion parameters are stored in the smart card carried by the user, so the biological data may be easily recovered by attacker and the privacy of the user will be infringed. Yang *et al.* [22] broke the research bottleneck of the revocability of multi-biometric identification system and proposed a revocable multi-biometric identification system based on fingerprint and finger vein, which comprehensively evaluated and analyzed the comparison performance and safety strength under different fusion conditions. The smart card and secret sharing technology in our scheme can successfully resist the first two of the four attack modes mentioned above. Based on our proposed method, the template transformation method PUF-TTM generates revocable biometric templates and uses PUF shared key to secretly transmit information, which can prevent the attack of comparison model and communication channel.

Recently, smart devices and wireless communication technologies in the Internet of Things era have made rapid progress. First of all, the emergence of a new generation of cloud services enables biometrics to be transmitted as a service through the network to an independent organization to provide secure access, which greatly reduces the pressure on the hardware and management consumption of the demanding users. Alizadeh *et al.* [21] pointed out the feasibility of implementing multi-factor authentication in mobile cloud computing to solve practical problems with the help of centralized computing resources, while achieving more secure and efficient goals. Kaur and Khanna [25], based on Biometrics-as-a-Service (BaaS), a biometrics platform hosted in the cloud, designed a novel multi-server biometrics authentication scheme, which is different from the previous multi-factor authentication protocols. Kaur integrated the concept of CB into a complete authentication protocol, and used the secret sharing technology

to generate multiple shares to strengthen the protection of biological templates in the way of distributed storage, so as to further improve the credibility and security of the authentication system [24], [25]. Secret sharing technology, first proposed in 1979, applies to parties who must cooperate but do not fully trust each other. In 2002, Thien and Lin [26] used this technique to improve the security of stored secret images. Li and Hwang [1] proposed a secure biometric authentication model based on threshold secret sharing technology for the first time. The security of the scheme is guaranteed by the inherent non-repudiation of biometrics and the difficulty of public key cryptography, but the consideration of biometric template protection is ignored. Furthermore, inspired by the successful application of physical unclonable functions (PUFs) in IoT systems for remote authentication and establishing trust relationships between devices, PUF has also been used in remote biometric authentication schemes to improve design security [27], [28]. Arjona and Baturone [29] first proposed the XOR fusion of PUF and fingerprint features to generate protected biological templates. Gope *et al.* [30] proposed to use the user's biological fingerprint as PUF input directly to generate the biological key to complete user identity authentication, but then Bian *et al.* [10] pointed out that the method of biometric as PUF input was not feasible and could not get rid of the interference of noise. Bian *et al.* [10] and Zhao *et al.* [11] fully combine the characteristics of PUF and fuzzy extractors for biometric authentication in single server and multi-server environments respectively, but neither can resist perfect forward secrecy attack. In 2021, Chatterjee *et al.* [31] designed an anonymous authentication protocol (3PAA) using the physical unclonable function itself as user secret key, which solved some problems in existing schemes. But 3PAA scheme only uses PUF as the private key for user authentication, is unable to resist stolen device attack. A common shortcoming of the schemes mentioned above is that they do not consider the influence of physical unclonable function on CB. Physical unclonable function could meet the requirements of CB for non-invertibility, unlinkability and revocability. For this reason, the integration of physical unclonable function and cancelable biometrics makes sense. However, our scheme applies physical unclonable function features to generate cancelable biometric templates well, and ensures the security and privacy of biometric templates from the perspective of devices.

B. Contribution

In order to adapt to the trend of the current multi-server environment and the popularity of cloud service, we propose a complete remote biometric authentication system which can resist all kinds of attacks. Firstly, we propose a novel PUF-TTM method to build the cancelable biometric template based on facial images and realize distributed storage of transformation parameters and transformation templates by using secret sharing technology. Furthermore, we can generate different biometric templates for identity authentication without re-enrolment. Finally, we add the cancelable biometrics to a multi-server authentication system, complete the encryption of the transmitted information based on the configurable ring oscillator (CRO) PUF and verify the applicability of our proposed method through experiments, which not only protects the privacy of users, but also improves the credibility of the authentication system. Then, it's worth noting that the main contributions of this paper are summarized as follows:

(1) A novel generating method PUF-TTM of cancelable biometrics is designed based on physical unclonable function (PUF) and fuzzy extractor.

(2) A secure biometric authentication and key agreement scheme based on cancelable biometrics and secret sharing is proposed.

(3) Both user and device have their own unique biometrics feature, which can provide the key security properties.

(4) Designs a Biometrics-as-a-Service-based privacy-preserving computation framework which can be extended to other biometrics.

(5) A password free scheme for registration, login, authentication and secure session key establishment in multi-server environment.

The rest of the paper is organized as follows. The preliminary is provided in Section II. Proposed template protection process is introduced briefly in Section III. In Section IV we describe how to construct the proposed architecture for remote authentication. Experiments conducted and relevant analysis are given in Section V. In section VI, we make a security analysis and performance comparison of the proposed scheme, and in Section VII, we summarize our work.

II. Preliminary

A. BaaS

Biometrics-as-a-Service (BaaS), the final frontier of security, is a relatively new trend, referring to security technologies, systems and applications based on biometrics that are hosted in the cloud. BaaS meets the dual benefits of cloud computing and biometric security, and can be integrated into PC and mobile devices. Unlike traditional biometric services, which encrypt digital images and store them in secure locations on devices such as smartphones, BaaS stores authenticated data in the cloud. In our scheme, we design a privacy protection authentication scheme based on BaaS model, combined with PUF-TTM and secret sharing technology to further reduce and eliminate the possibility of biological data being stolen. On the one hand, it overcomes a potential challenge that biometrics differs from passwords: immutability. When biological information is maliciously attacked and stolen, we can flexibly generate a new biometric template by changing transformation parameters and shared values just like changing passwords. On the other hand, it can ignore the requirements of hardware infrastructure, the cost of system maintenance and other factors, get rid of the expensive and time-consuming process of software acquisition and integration, and easily solve the bottleneck problem of the realization of identity authentication function of the present Bring Your Own Device (BYOD) [32].

B. Fuzzy Extractor

The fuzzy extractor [10] is composed of a pair of functions, namely, $FE.Gen(\cdot)$ and $FE.Rec(\cdot)$. When the fingerprint F is

used as input to $FE.Gen(\cdot)$, a public auxiliary data P and a key C_i that does not need to be stored are generated, i.e., $(C_i, P) = FE.Gen(F)$. If F' and F prime are close enough, i.e., $\mathrm{dis}(F, F') \leq$ t, enter F' and P together into the function $FE.Rec(\cdot)$ to recover the key C_i, i.e., $C_i = FE.Rec(F', P)$. In this process, the fuzzy extractor overcomes the possible interference of noise in fingerprint and the insecurity of key storage. Unlike physical unclonable function, the fuzzy extractor allows the input to have a certain amount of noise, as long as the input is close enough to extract the same random string [33]. During enrolment, the C_i generated by the combination of fingerprint and fuzzy extractor is used as the input of the following physical unclonable function, which can not only replace a trusted random number mechanism in the system as a part of PUF-TTM, but also improve the security and privacy of the system from the perspective of multiple factors.

C. PUF

Physical unclonable function PUF, a hardware function that generates random values in the chip depending on the manufacturing process difference of ICs, is embedded in mobile devices to participate in the authentication as the "fingerprint" of the device. Based on the mathematical formula: $R = PUF(C)$ generates multiple challenge pairs of CRPs, where C is a set of possible challenges, and R, as the output of PUF, is the corresponding response set. Recently, Zhang and Qu [34], for the first time, proposed the concept that a shared key SK can be generated based on PUF. In our scheme, we choose the lightweight CRO PUF, which can not only protect the biological template, but also encrypt the information transmitted on the public channel with SK. Meanwhile, CRO PUF has the following four properties of all $(d, h, l, \lambda, \varepsilon)$-secure PUF:

(1) $P_r\left[d_H(PUF_m(C_i), PUF_m(C_i)) = 0\right] \geq 1 - \varepsilon$, $1 \leq m \leq M; 1 \leq i \leq N$

(2) $P_r\left[d_H(PUF_m(C_i), PUF_m(C_j)) > d\right] \geq 1 - \varepsilon$, $1 \leq m \leq M; 1 \leq i, j \leq N \wedge i \neq j$

(3) $P_r\left[d_H(PUF_m(C_i), PUF_n(C_i)) > d\right] \geq 1 - \varepsilon$, $1 \leq m, n \leq M \wedge m \neq n; 1 \leq i \leq N$

(4) $P_r\left[H_{-\infty}(PUF_m(C_i), PUF_n(C_j)) > \lambda\right] \geq 1 - \varepsilon$, $1 \leq m, n \leq M \wedge m \neq n; 1 \leq i, j \leq N \wedge i \neq j$.

Where d_H and $H_{-\infty}$ refer to the hamming distance and minimum entropy of two PUF outputs respectively, $PUF = \{PUF_1(\cdot), PUF_2(\cdot), \ldots, PUF_M(\cdot)\}$ represents the set PUFs, and $C = \{C_1, C_2, \ldots, C_N\}$ 𝔄 $s.t.\ \forall\ n\mathrm{C}_n \in \{0, 1\}^k$ said set of challenges. If you use the same C_i as input of the same PUF, will get the same response. If you use two even if there is a little different C_i and C_i input into the same PUF, get the response will also have very big difference. Likewise, if use the same C_j input to the different PUF, get the response will be different.

D. Secret Sharing

The concept of secret sharing, first proposed by Shamir [35] and Blakley [36] in 1979, refers to the reasonable distribution of secrets to multiple members for common management after encryption, so as to improve the secure storage of secrets. In this paper, we assume that t subsecret information $(K_0, K_1, K_2, K_3, \ldots, K_{t-1})$ is obtained after K is equally divided as a secret, and then embedded as a coefficient in the t-1 degree polynomial $f(x)$: $f(x) = K_0 + K_1x + K_2x^2 + \cdots + K_{t-1}x^{t-1}$. At the same time, there are n points in the two-dimensional plane with different x values satisfying $f(x_i) = y_i$, respectively: $(x_0, y_0), (x_1, y_1), \ldots, (x_{n-1}, y_{n-1})$. If we know any t of these n points, we can recover the coefficients of $f(x)$ using Lagrange interpolation, and get the secret K. But if you know at most t-1 of them, you will don't know anything about K. Where, the Lagrange interpolation polynomial is:

$$L(x) := \sum_{j=0}^{t-1} y_j \ell_j(x) \tag{1}$$

l_j(x) as the basic polynomial Lagrange, its expression is:

$$\ell_j(x) := \prod_{i=0, i\neq j}^{t-1} \frac{x - x_i}{x_j - x_i} \tag{2}$$

In our scheme, we apply secret sharing technology to generate multiple shares of biometric transformation parameters and transformation templates and store them separately in user token (smart card), remote database and application server database. Only when all shared servers are obtained can conversion parameters and conversion templates be recovered to complete remote biometric authentication of users. Specific secret sharing and secret recovery procedures are described in detail in Section III B and Section III C.

E. System Model

Our system model is shown in Fig.1. In the system, we assemble CRO PUF and face collector on mobile devices such as notebook, mobile phone, tablet and so on, and form the Endpoint UD with the user. Through the biometric authentication platform based on BaaS, the secure communication and identity authentication between users and multiple servers are completed, and the server is regarded as the trusted party.

III. Proposed Template Protection Process

As shown in Fig.2, the original face data of a user is subjected to a cancelable transformation to generate a transformed biometric template *Pf*. Since the direct use of the original biometric template information for authentication can easily reveal the user's private information, the proposal of the cancelable template protection scheme is very important. When a biometric template is under attack, we can generate a new, irreversible *Pf* by changing the transformation parameters. The process becomes invertible and unsafe if both the transformation template and the transformation parameters are intercepted by an attacker. Therefore, we propose a secret sharing algorithm to further improve the protection of transformation templates and parameters. For authentication, we first use the transformation parameters (K, C_i) and template *Pf* that shares used when they were recovered from enrolment, and then apply the same transformation parameters to the user's real-time biometric data to get the *Pf* ′ which is compared

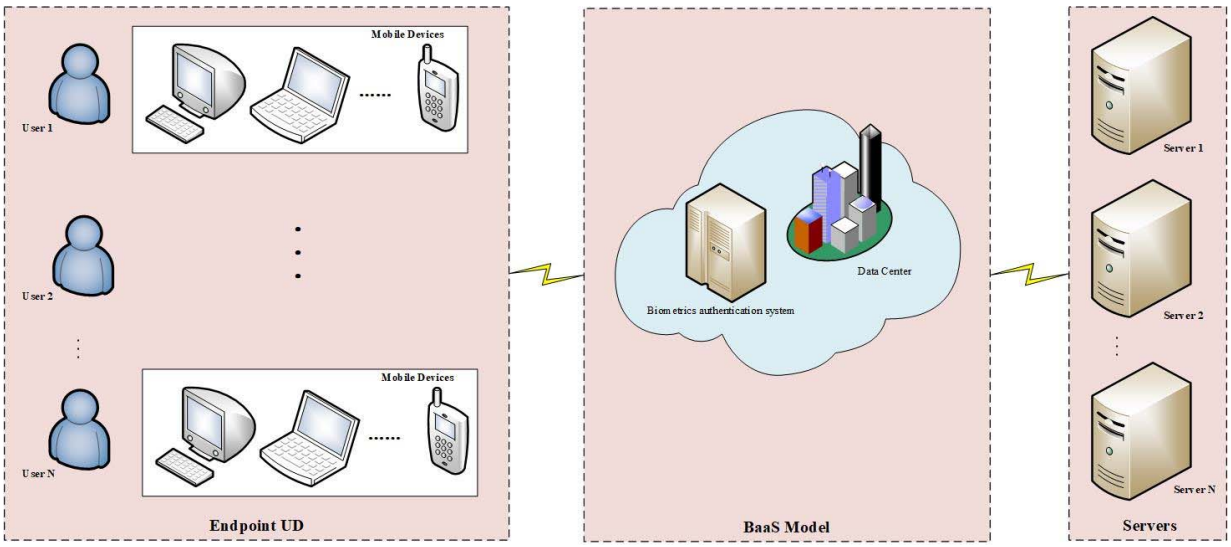


Fig. 1. System model.

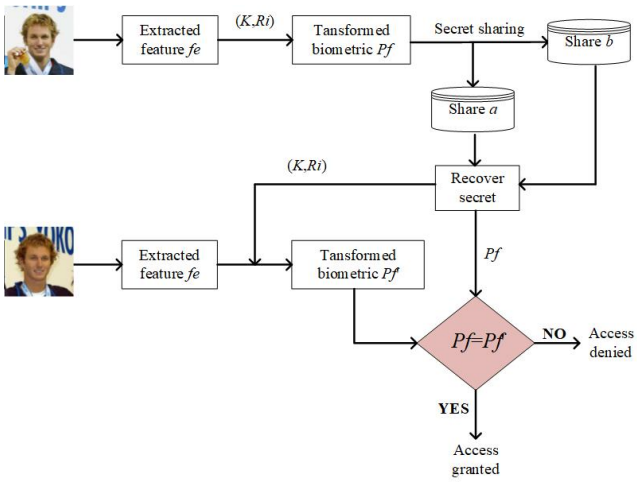


Fig. 2. Overview of the proposed transformation process.

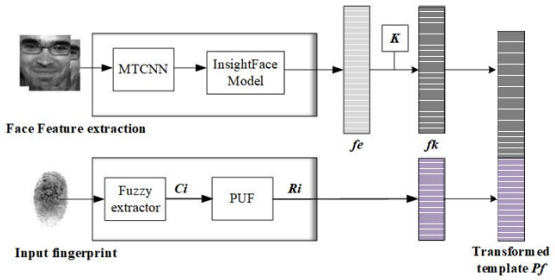


Fig. 3. Process of biometrics template transformation method (PUF-TTM).

against *Pf* to grant or deny access. In this process, template protection is mainly determined by three parts, namely, template transformation process, secret sharing process and secret recovery process. The details of each section are as follows.

A. Template Transformation Method With PUF (PUF-TTM)

Based on the current popular face recognition algorithm, we use the model provided by InsightFace to extract features from the face data set of LFW, and obtained 512-dimension feature vectors *fe*. For the original feature vectors *fe,* we use the proposed template transformation method with PUF (PUF-TTM) to obtain the cancelable biometric template *Pf*, as shown in Fig. 3. The detailed steps are described below.

Step1: All face images are firstly aligned and cropped to 112×112 by MTCNN and then are supposed to send to InsightFace model to generate the 512-dimention embeddings. Let *fe* be a 1-D feature vector belong to each face image and then to be transformed.

Step2: Generate a user-specific random matrix K (512×512) whose width and height are similar to the feature vector *fe* and salt *fe* with K as $fk = fe \times K$ to get the salted vector *fk* which is going to be binalized.

Step3: Input the user's fingerprint feature into fuzzy extractor in order to generate a device-specific challenge *Ci* of the specific user and then input to CRO PUF to get a response *Ri* which doesn't need to be stored.

Step4: Generate the transformed template *Pf* by concatenating the values corresponding to the two vectors *fk* and R_i.

B. Secret Sharing for Template and Parameters Protection

A single technique based on secret sharing is proposed here for implementing distributed storage of transformation templates and transformation parameters using equations of quadratic polynomials and straight lines. K and *Ci* in this case are the parameters we use to generate the transformation templates. We divide K into three parts to get k_1, k_2, k_3, and then there are 5 secret information (k_1, k_2, k_3, C_i, Pf) who are supposed to be shared to enhance the protection of biological data. A step wise procedure of the proposed secret sharing is shown in Fig. 4 and described below.

Step 1. Establish the general equation of a line l_1 using the keys k_1, k_2 and k_3 as $l_1 : y = k_1\ x^2 + k_2 x + k_3$.

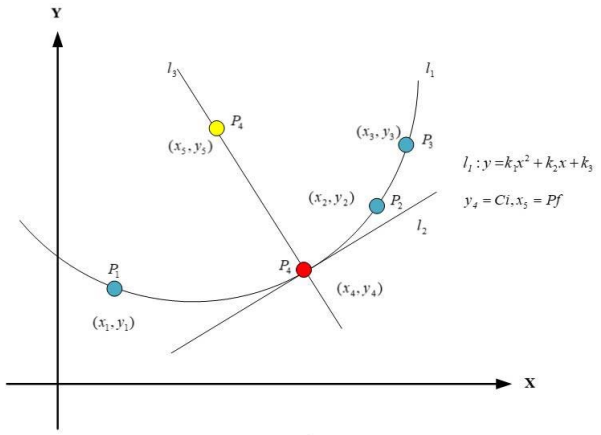


Fig. 4. Concept of secret sharing using three lines.

Let P be an innocuous image such that on reshaping its dimension is equal to that of Pf. We get three secrets S_1, S_2, S_3 by exporting P as a password using key derivation function 2 (PBKD2). Let $x_1 = S_1$, $x_2 = S_2$, $x_3 = S_3$, then y_1, y_2 and y_3 are evaluated using the line l_1 defined above. This step outputs six shares, namely $S_1 = x_1$, $S_2 = x_2$, $S_3 = x_2$, $S_4 = y_1$, $S_5 = y_2$, $S_6 = y_3$ that are mapped as three points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $P_3(x_3, y_3)$ on the line l_1.

Step 2. Define a point $P_4(x_4, y_4)$ on the line l_1 whose y-coordinate is defined using transformation parameter C_i and a random share S_7, i.e. $y_4 = C_i + S_7$. Evaluate its x-coordinate as $x_4 = \left(\sqrt{k_2^2 + 4k_1y_4 - 4k_1k_3} - k_2\right)/2k_1$ using the equation of line l_1. The obtained value is stored as $S_8 = x_4$.

Step 3. Let l_2 be the tangent line of l_1 at the point P_4. Establish an equation of line as l_2: $y = k_4x + b$ whose slope k_4 is equal to $2k_1x_4 + k_2$, intercept b is equal to $y_4 - k_4x_4$.

Step 4. Let l_3 be the normal line of l_2 crossing the point P_4. Establish an equation of line as l_3: $y = k_5x + d$ whose slope k_5 is equal to $x_4 = 1/-k_4$ because of the equation $k_4k_5 = -1$, intercept d is equal to $y_4 - k_5x_4$.

Step 5. Map the reference template Pf as the x-coordinate of a point l_3, i.e. $x_5 = Pf$. Obtain its y-coordinate as $y_5 = k_5x_5 + d$ using the equation of line l_3 and stored as share $S_9 = y_5$.

Finally, in order to share five pieces of transformation parameters secretly nine secret shares are created as S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8 and S_9. Shares S_1, S_2, S_3, S_4, S_5, S_6 are generated for the coefficients k_1, k_2, k_3 of polynomial l_1, while shares S_7, S_8, S_9 are generated for C_i and Pf.

C. Secret Recovery Process for Biometric Authentication

According to the shares we can recover the five needed secrets. The secret recovery process for biometric authentication is given below.

Step 1. Map three points P_1, P_2, P_3 using the first six shares $S_1 = x_1$, $S_2 = x_2$, $S_3 = x_2$, $S_4 = y_1$, $S_5 = y_2$, $S_6 = y_3$ and Lagrange's interpolation to find the equation of line l_1. The coefficients of the line l_1 reveals the first three secrets k_1, k_2, k_3.

Step 2. Define x-coordinate of the point P_4 lying on l_1 as $x_4 = S_8$. Using the equation of l_1 evaluate its y-coordinate $y_4 = k_1x_4^2 + k_2x_4 + k_3$ which is equal to the transformation parameter $C_i + S_7$.

Step 3. Determine the second line l_2 of the tangent line at the point P_4, by using the first line l_1 and P_4, the equation of line l_2 is established whose normal line at the point P_4 is the last line l_3.

Step 4. Recover reference template $Pf = x_5$ by determining the y-coordinate of the point P_5 lying on l_3 as $y_5 = S_9$.

IV. Proposed Architecture for Remote Authentication

Given that there are few authentication schemes involving cancelable biometrics in a multi-service environment, we propose a novel BaaS-based remote multi-server biometric authentication scheme using the PUF of the device and secret sharing technology. Our authentication approach involves three entities, namely: (i) user-the entity which is authenticating using the biometric identity, (ii) device-the entity which is equipped with an image sensor, Fuzzy extractor and a CRO-PUF, (iii) multi-server-the entity which authenticates the user using secret shares and cancelable biometrics template before allowing the user to perform any services of server. We form a combination of a user and a device as Endpoint UD terminal, and use a cloud-based service called as Biometrics-as-a-Service (BaaS) to complete user identity authentication.

A complete cancelable biometrics-based authentication framework is developed in this work by using PUF-TTM and secret sharing scheme discussed above for multi-server environment. Using Fuzzy extractor, PUF and random number mechanism, PUF-TTM can generate multiple different pseudo-identities for the same biometric sample of users, which can be used to obtain multiple services provided by servers in a multi-server environment. Among them, PUF is a lightweight cryptographic primitive that takes a string of bits as an input challenge and generates a unique response based on the process variations occurring in the semiconductor manufacturing process. It can be used as a device-unique "fingerprint" like a human's fingerprint to uniquely identify the identity of each device. Combined with the user's fingerprint, the challenge C_i of PUF is generated by using the user's fingerprint as input of the fuzzy extractor, which gets rid of the disadvantage that the information stored in the device is vulnerable to attack. The challenge pair (CRPs) of CRO-PUF and random number generation mechanism are combined as transform parameters of cancelable biometrics. CRO-PUF is sufficient for the generation of transformation keys, although it is weak PUF which generates only a small amount of CRPs. The application of secret sharing technology realizes the secure management of biometric template and transformation parameters, which enables users to use their biometrics safely in a multi-server environment. While the current method of generating a cancelable biometric is irreversible, the process becomes meaningless once both the transformation parameters and the transformation template are captured by an attacker. So how to manage the transformation parameters of the

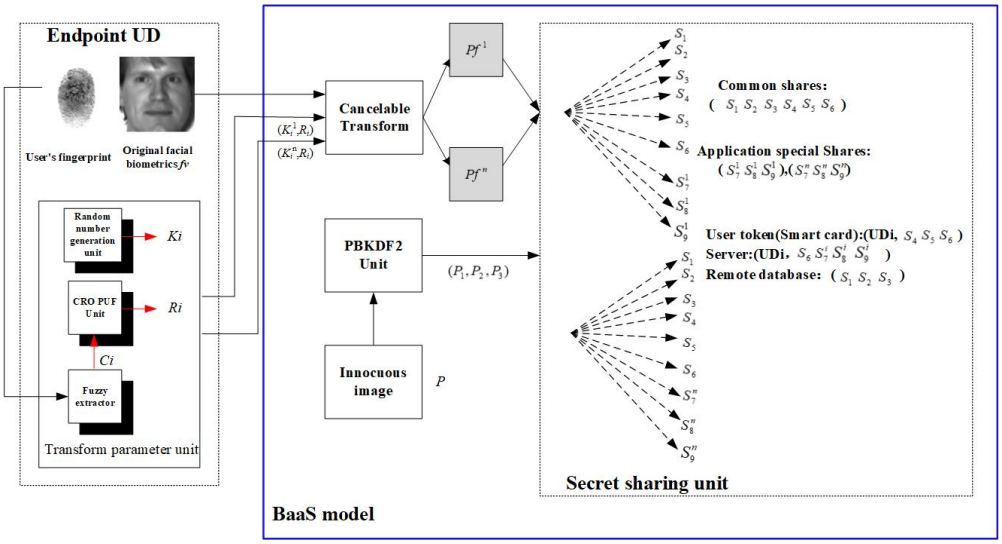


Fig. 5. Enrollment process using PUF and secret sharing for the proposed multi-server architecture over a BaaS model.

biological template is a crucial issue. We use secret sharing technology to generate multiple shares of biological transformation templates and transformation parameters, which are stored separately in the system and remote database. This not only solves the security vulnerability caused by directly storing biometric data, but also makes it a huge challenge for attackers to recover secrets through distributed storage of shares. Our scheme mainly includes verifying the authenticity and legitimacy of users and devices, establishing session key and updating the database. The specific enrolment and authentication process is described below.

A. Enrollment Phase

The enrollment protocol is executed between the Endpoint UD and cloud-based BaaS and the process is illustrated in Fig.5. For each registered user, we assign a unique identity UD_{i} to the combination of the user and the device they are using. After the registration request is issued, the user provides the preprocessed and feature extracted biometric data *fv*, which is subjected to the proposed PUF-TTM using user-specific transformation parameters $(K_i,\ R_i)$ generated from the random number generation unit, Fuzzy extractor and CRO-PUF embedded in the client device. And then different transformed templates can be obtained by changing any parameter for the same biometric sample. Let the transformation parameter R_i be fixed here and assign different K_i for each application., different transformed templates $Pf^1, Pf^2, \ldots, Pf^{\mathrm{n}}$ are generated from $(K_i^1, R_i), (K_i^2, R_i) \ldots (K_i^{\mathrm{n}}, R_i)$.

We then use the secret sharing technique to hide the transformation parameters and the transformation template, and then discard the original biological information *fv* directly after generating the shares without saving processing. According to the secret sharing process we proposed in Section III B, We use an innocuous image signal P as the input of PBKDF2 to get a secret, and then we divide it into three parts to form three secrets, says P_1, P_2, P_3. For the first parameter K_i (K_{i1}, K_{i2}, K_{i3}), six output shares are generated with the proposed secret sharing approach over a BaaS model. Similarly, three output shares S_7^i, S_8^i, S_9^i are generated from the parameter R_i and transformed template Pf^i stored on each application server SV_i.

It is worth noting that the shares (S_1, S_2, S_3, S_4, S_5, S_6) are used as common shares and (S_7^i, S_8^i, S_9^i) are referred as the specific shares of each application server. To further improve the protection of biometric data in a multi-server environment, shares are stored separately. The common shares S_1, S_2, S_3 are stored over remote databases, while the shares S_4, S_5, S_6 and user-specific identity UD_{i} are stored in user token, eg. smart card. And the other shares S_7^i, S_8^i, S_9^i are provided to application servers with UD_{i} and S_6. Once registered, users can use their smart cards and real-time biometric information to prove their legal identity to the application server and complete the next full authentication process. Due to the CRO-PUF embedded in user devices, we can obtain the shared key *SK* for authentication in multi-server environment according to the PUF-based key sharing proposed for the first time recently in the Internet of Things security.

B. Login and Authentication Phases

Fig.6 shows the login, authentication and key agreement procedures for our proposed architecture. First a user attempting to login an application server SV_j via his/her own devices, he/she has to provide a smart card with registration information $\{UD_{\mathrm{i}}, S_4, S_5, S_6\}$ and enter real-time facial information Bio_i through biometric extractor, and then the shared key *SK* generated by CRO PUF is used for secret information exchange between UD_i and SV_j. SV_j uses the secret recovery process mentioned above to restore the user's biometric transformation template *Pf* and parameters (*Ki*, *Ri*). Then the transformation parameters are passed to UD_i in encrypted state and applied to the real-time biometrics of the user to obtain *Pf*', which is used to calculate the session key sk_{ij}, and finally the data of the application server is matched to make the decision to reject or accept.

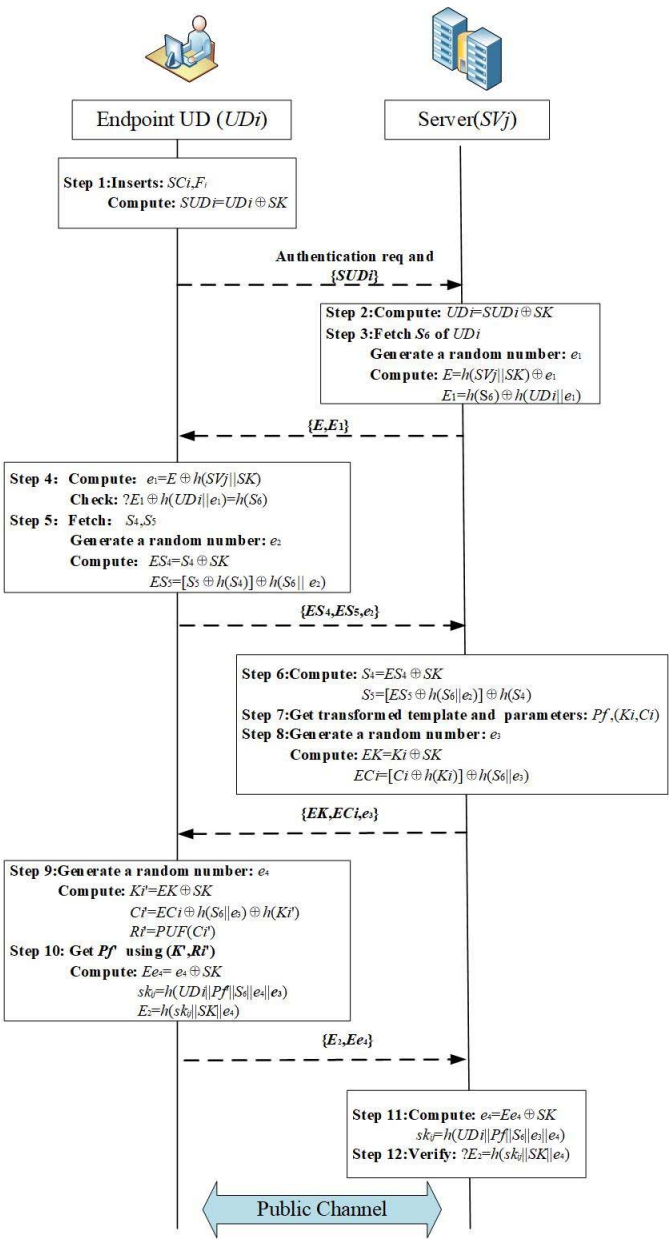


Fig. 6. Login, authentication and key agreement phases for the proposed architecture.

Step 1: Using the UD_i entered by user and pre-shared key SK, Endpoint UD_i first computes $SUD_i = UD_i \oplus SK$ in order to encrypt the transmitted identity, and then UD_i sends the message $\{SUD_i\}$ and authentication request to SV_j.

Step 2: SV_j first decodes UD_i by computing $UD_i = SUD_i \oplus SK$ followed by fetching common shares of UD_i from its database.

Step 3: SV_j computes $E_1 = h(S_6) \oplus h(UD_i)$ after fetching S_6 of UD_i and subsequently generates a random number e_1 and then sends a response message $\{E_1, e_1\}$ to UD_i.

Step 4: Upon receipt of the message in step 3, UD_i first verifies whether the result of $E_1 \oplus h(UD_i)$ is equal to $h(S_6)$ because only real server has the right secret S_6. If not, UD_i terminates the session.

Step 5: UD_i fetches the common shares S_4, S_5 from its database and generates a random number e_2. Also, it computes $ES_4 = S_4 \oplus SK$ and $ES_5 = [S_5 \oplus h(S_4)] \oplus h(S_6||e_2)$ for the next encrypted transmission. And then UD_i is asked to send the message $\{ES_4, ES_5, e_2\}$.

Step 6: Upon receiving UD_i's message $\{ES_4, ES_5, e_2\}$, SV_j first decodes S_4 by computing $S_4 = ES_4 \oplus SK$ and then decodes S_5 by computing $S_5 = [ES_5 \oplus h(S_6||e_2)] \oplus h(S_4)$.

Step 7: Upon decoding S_4 and S_5, the reference template Pf and transformation parameters (K_i, C_i) are recovered for further processing combining the shares S_1, S_2, S_3 fetched from the remote database and S_6, S_7^i, S_8^i, S_9^i fetched from the database of application server SV_j.

Step 8: Subsequently SV_j generates a random number e_3 used to encrypt transformation parameters. Next, SV_j computes $EK = K_i \oplus SK$ and $EC_i = [C_i \oplus h(K_i)] \oplus h(S_6||e_3)$ which are submitted to UD_i.

Step 9: UD_i first generates a random number e_4 and obtains K_i' and C_i' by computing $K_i' = EK \oplus SK$ and $C_i' = [EC_i \oplus h(S_6||e_3)] \oplus h(K_i)$. And then the challenge C_i' is input to PUF and get R_i' using $R_i' = PUF(C_i')$.

Step 10: UD_i generates the transformation template Pf' from the user's real-time biometric sample Bio_i using the transformation parameters (K_i', C_i'). Then UD_i computes $Ee_4 = e_4 \oplus SK$ and the session key sk_{ij} is established by computing $sk_{ij} = h(UD_i||Pf'||S_6||e_4||e_3)$. Finally, UD_i computes $E_2 = h(sk_{ij}||SK||e_4)$ and sends the composite massage $\{E_2, Ee_4\}$ to SV_j.

Step 11: Upon receiving the message from UD_i, SV_j first decodes e_4 by computing $e_4 = Ee_4 \oplus SK$, then computes $sk_{ij} = h(UD_i||Pf||S_6||e_4||e_3)$ in order to achieve the session key.

Step 12: Finally, SV_j verifies whether the key-hash response $h(sk_{ij}||SK||e_4)$ is equal to E_2. If not, SV_j will terminate this session.

C. Revocation Phase

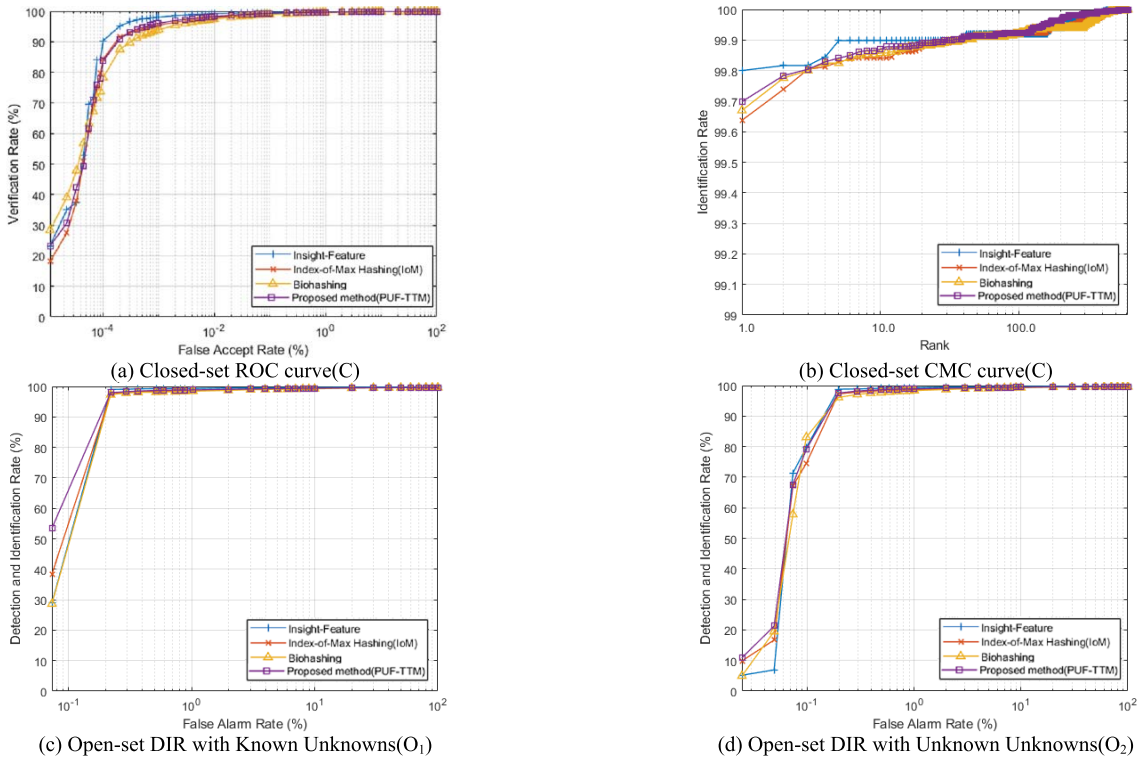
In order to meet the revocability requirement of biometric template protection, our system needs to provide the necessary revocability mechanism to resist malicious attacks and user token loss. Protected biometric template is based on the user's face, fingerprint, fuzzy extractor, PUF and secret sharing technology to create a joint cooperation, none is missing. When the revoke command is issued, on the one hand, the user can generate a new protected biometric template by re-enrolling through the enrolment protocol, on the other hand, the method we proposed can realize the revoke of the biometric template without the trouble of the user re-enrolling. When the user token (smart card) is lost, we can update S_1, S_2, and S_3 in the remote database by changing one or more shares in S_4, S_5 or S_6 without affecting the shared information in the application server. When an application server's database is maliciously attacked, we can use the same strategy to change only the value of the shared S_7, S_8 and S_9 will be updated, and the public share will work just fine.

V. Experimental Results

Based on the popular large face data set LFW [37], we evaluate our scheme in terms of performance, unlinkability and revocability, and **compare the computational costs in**

TABLE I
COMPARISON OF CANCELABLE BIOMETRIC SCHEMES ON LFW

CB scheme	Dataset	Biometric trait	Feature size	Technique	Irreversibility	Revocability
Biohashing	LFW	Deep facial feature	512 real-valued vectors	Random projection	Random projection	Using new random projection key
IoM hashing				Ranking based hashing	Multiple random projection	Using new random projection key
Proposed method(PUF-TTM)				PUF-based fusion	1. User-specific transform parameters 2. PUF's property	1. Using new transform parameters 2. Using new secrets sharing



(a) Closed-set ROC curve(C)

(b) Closed-set CMC curve(C)

(c) Open-set DIR with Known Unknowns(O_1)

(d) Open-set DIR with Unknown Unknowns(O_2)

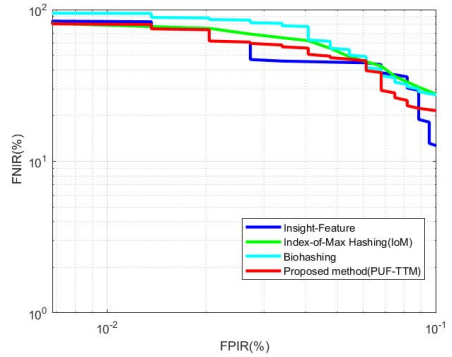
Fig. 7. Comparison between different methods. The (a) ROC curves and the (b) CMC curves for the closed-set evaluation on probe set C, as well as the open-set DIR curves for (c) probe set O_1 and (d) probe set O_2 are given for all four evaluated methods.

all phases with some famous schemes, which clearly and intuitively highlight the advantages of our scheme. LFW is a data set for unconstrained face recognition, which is composed of 13,233 facial images of 5749 celebrities collected from the network. Each person may contain more than 1 to 3 facial images. This data set has been applied to many researches on cancelable biometrics schemes. According to the partition method on LFW dataset put forward by Gunther, M. *et al.*, our data can be divided into three categories: training set, gallery set and four different probe sets (C, O_1, O_2, O_3) [38]. The gallery set contains face images of users known to the system, while the samples in probe sets are presented to the system for recognition. Among them, probe C corresponds to different face samples of the user in the gallery set, and the rest of probe sets contain different samples in the presence and absence (which can be called imposters) of the gallery. We first preprocess all the face images using MTCNN to detect the face area and cut them into 112×112 images after alignment, and then input them to the latest face deep model InsightFace for feature extraction, thus obtaining 512-dimension embeddings. Based on the proposed PUF-TTM, we carry out the irreversible transformation, and finally get the cancelable biometric template of human face.

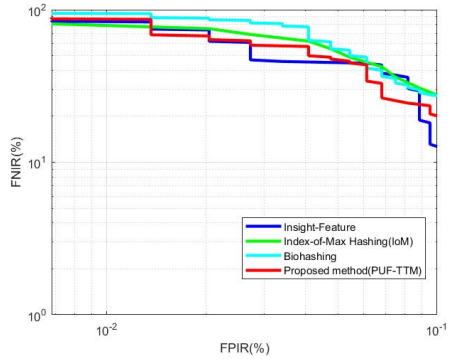
A. Performance Evaluation

In order to ensure the security of the original biological data and achieve good face verification performance, we studied the performance of a variety of popular cancelable biometrics schemes in the open and closed sets for the LFW data set, and based on the cosine similarity completes the comparison of pairs of deep feature vectors in the transform domain. In the Closed-set identification, we use the standard face recognition performance evaluation curve: Cumulative Match Characteristic (CMC) curve and Receiver Operating Characteristic (ROC) curve for experiments. The Detection and

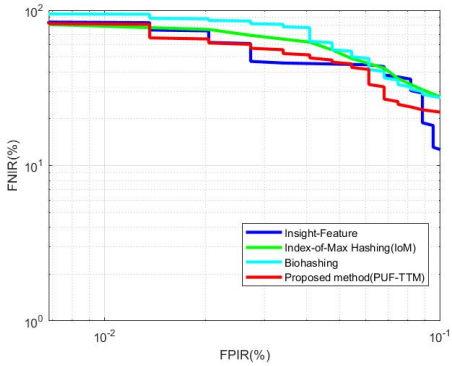
Identification Rate (DIR) curve and Detection-Error Trade-off (DET) curve are used in the open-set identification [39]. Among them, the detection and recognition rate refer to the score that the prob samples are correctly detected and recognized in the gallery, and the false alarm rate refers to the score that false alarms for the imposters, which is different from the false accept rate in the ROC curve. A false alarm occurs when the top match score of an imposter is above the threshold set by the system. DET curve: shows the False Positive Identification Rate (FPIR) and the False Negative Identification Rate (FNIR) with the change threshold both changes. The closer the curve of the image is to the lower left corner, the better the recognition performance is. Table I shows the comparison results of the commonly used Biohashing, IoM hashing schemes and our scheme. We can visually see that our proposed scheme is more reliable and efficient than other schemes, ensuring the irreversibility and revocability of the biometric scheme from many aspects. In terms of irreversibility, we combine user-specific transformation parameters and the uniqueness of PUF to perform irreversible conversion of biological characteristics; for revocability, we use new transformation parameters and secret sharing to resist attacks. In order to further evaluate the performance of proposed scheme, we have drawn Fig. 7 and Fig. 8 to compare the performance of the schemes mentioned above. From the results, we can see that our scheme always approaches the experimental results of the original insight feature and is higher than other schemes. It achieves a good balance between template security and performance maintenance.



(a) DET curve on the probe set O_1



(b) DET curve on the probe set O_2



(c) DET curve on the probe set O_3

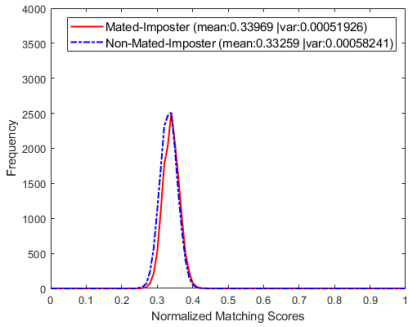
Fig. 8. Recognition performance evaluation for all four evaluated methods on different probe sets (O_1, O_2, O_3).

B. Unlinkability and Revocability

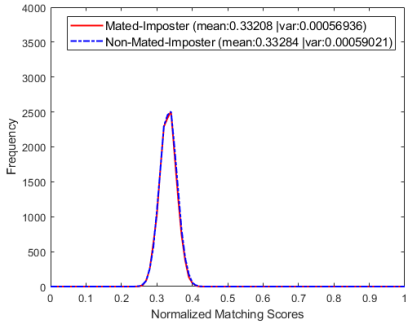
In order to verify that the template protection scheme we proposed meets the requirements of unlinkability and revocability, we select the first 10 images of 158 users with more than 10 face images in the LFW dataset to form a small dataset LFW10, and based on this conduct experimental analysis. We use two kinds of scores for evaluation defined by Gomez-Barrero *et al.* [40], namely Mated-imposter score and Non-mated importer score. Mated-imposter score refers to the comparison score of the same user's face image based on different conversion parameters, and the Non-mated importer score refers to the comparison score of different users' biometric templates using different parameters for PUF-TTM. Fig. 9 shows the fractional distribution in the case of only changing parameter K and changing all parameters. It can be seen from the figure that in these two cases, the two distributions show obvious overlap and close to the same. To further evaluate this overlap, we compute the global measure $D_{\leftrightarrow}^{sys}$ defined in [40] which can evaluate overall linkability of the system. If $D_{\leftrightarrow}^{sys} = 0$, shows that our scheme is absolutely no link; if $D_{\leftrightarrow}^{sys} = 1$, the opposite. Calculation results show that the value of $D_{\leftrightarrow}^{sys}$ in our scheme is almost close to zero. Overall, our analysis and results indicate that the proposed scheme supports unlinkability. Even if the attacker can obtain all the comparison scores of the compromised biometric templates from different applications, it is impossible to distinguish them from the same principal. This is because this property ensures that there is no correlation between the updated biometric templates of the same user and the compromised one. We plot the fraction distribution of genuine, imposter and Mated-imposter, as shown in Fig.10. We can clearly see that the fraction distributions of Mated-imposter and imposter are extremely similar, with similar mean and variance, while the distributions of Mated-imposter and genuine are obviously different. Therefore, the revocable nature of our scheme is established. When the system suffers a malicious attack, we can replace the compromised template by republishing a brand new protected biometric template.

C. Computational Performance Comparisons

To further evaluate the performance of our scheme, we have carried out a detailed analysis of the computational costs in



(a) Only changing the parameter: K



(b) Change all parameters：(K,Ci)

Fig. 9. Unlinkability analysis by changing (a) only the parameter K, $\boldsymbol{D_{\leftrightarrow}^{sys}} = \mathbf{0.01}$. and (b) all parameters (K, Ci), $\boldsymbol{D_{\leftrightarrow}^{sys}} = \mathbf{0.00}$. on LFW10.

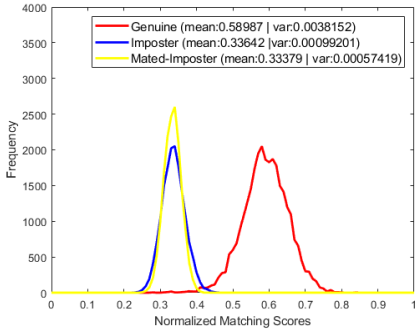


Fig. 10. Revocability analysis by the distribution of genuine, imposter and Mated-imposter scores on LFW10.

all phases between the proposed scheme and other relevant schemes. The comparison results are summarized in Table II. Among them, T_{PUF} represents the time cost for PUF-based operations, T_h is the time complexity of the hash function. And the time of *FE.Gen*() and *FE.Rec*() are denoted by T_{FEG} and T_{FER} respectively, the time of scalar multiplication operation is expressed as T_{SM}. Based on the experimental results in literature [10], [31], we found that a hash operation at the user and server was 0.026ms and 0.011ms respectively; each PUF operation takes 0.13ms at the user's device; each *FE.Gen*(·) operation takes 2.67ms at user's device and *FE.Rec*(·) operation takes 3.35ms at the server; each SM operation takes 3.5ms. Therefore, our scheme has a total time delay of 0.463ms in the mutual authentication stage. The result shows that the computational cost of our scheme is less than most schemes. Specially, we can see from the fourth part of the proposed remote authentication architecture that we

TABLE II
COMPUTATIONAL COST COMPARISONS

Schemes	Authentication		Total
	User	Server	
[10]	$11T_h + 1T_{FEG} + 1T_{FER} + 1T_{PUF}$	$7T_h + 1T_{FER}$	$18T_h + 1T_{FEG} + 2T_{FER} + 1T_{PUF}$
[11]	$14T_h + 1T_{FER} + 1T_{PUF}$	$13T_h$	$27T_h + 1T_{FER} + 1T_{PUF}$
[31]	$3T_h + 5T_{PUF} + 16T_{SM}$	$1T_h + 8T_{SM}$	$4T_h + 5T_{PUF} + 24T_{SM}$
[32]	$1T_h + 2T_{PUF}$	$1T_h$	$2T_h + 2T_{PUF}$
Ours	$9T_h + 1T_{PUF}$	$9T_h$	$18T_h + 1T_{PUF}$

TABLE III
BASIC NOTATIONS OF BAN LOGIC

Notations	Meanings
#(X)	Formula X is fresh
$A \mid\equiv X$	Principal A believes the message X
$A \lhd X$	Principal A sees the message X
$A \mid\sim X$	Principal A once said the message X
$A \mid\Rightarrow X$	Principal A has jurisdiction over the message X
$A \overset{K}{\longleftrightarrow} B$	K is the shared key between A and B
$A \overset{X}{\Leftrightarrow} B$	Formula X is a secret known only to A and B
$\{X,Y\}_K$	X and Y are encrypted with the key K
$\langle X \rangle_Y$	Formula X is combined with Y

only involve the operations with low time consumption such as *hash, XOR* and PUF. All the above results have shown the validity and superiority of our scheme for remote user authentication.

VI. SECURITY ANALYSIS

A. Formal Security Analysis Using Burrows-Abadi-Needham (BAN) Logic

We use Burrows-Abadi-Needham (BAN) logic [41] to analyze the security of our proposed scheme, from the definition of basic conformity and reasoning logic, related assumptions and goals, to detailed explanations of the specific reasoning process, so as to draw a conclusion whether the agreement meets our expected goals. Based on our proposal, we conduct formal analysis with *UDi* and *SVj* as the main body.

1) The Basic Symbols and Rules of Inference: As shown in Table III, the basic symbols and definitions involved in BAN logic are explained, and several basic logical inference rules are listed below, which will help us to analyze our own schemes with theoretical basis later.

R1. Message-meaning rule: $\frac{A \mid\equiv A \overset{K}{\leftrightarrow} B, A \lhd \{X\}_K}{A \mid\equiv B \mid\sim X}$ and $\frac{A \mid\equiv A \overset{Y}{\Leftrightarrow} B, A \lhd \{X\}_Y}{A \mid\equiv B \mid\sim X}$

R2. Nonce-verification rule: $\frac{A \mid\equiv \#(X), A \mid\equiv B \mid\sim (X)}{A \mid\equiv B \mid\equiv X}$

R3. Jurisdiction rule: $\frac{A \mid\equiv B \Rightarrow X, A \mid\equiv B \mid\equiv X}{A \mid\equiv X}$

R4. Belief rule: $\frac{A \mid\equiv (X), A \mid\equiv (Y)}{A \mid\equiv (X, Y)}$

R5. Fresh rule: $\frac{A \mid\equiv \#(X)}{A \mid\equiv \#(X, Y)}$

2) Relevant Assumptions and Goals: For our proposed scheme, we use BAN logic language to make relevant assumptions, i.e. A1-A8, and preset the goals realized between *UDi* and *SVj*, i.e. G1-G4.

A1: $SV_j \left| \equiv \#(e_1), SV_j \right| \equiv \#(e_3)$ A2: $UD_i \left| \equiv \#(e_2), UD_i \right| \equiv \#(e_4)$

A3: $UD_i| \equiv UD_i \overset{SK}{\leftrightarrow} SV_j$ A4: $SV_j| \equiv UD_i \overset{SK}{\leftrightarrow} SV_j$

A5: $UD_i| \equiv UD_i \overset{Pf}{\Leftrightarrow} SV_j$ A6: $SV_j| \equiv UD_i \overset{Pf}{\Leftrightarrow} SV_j$

A7: $UD_i| \equiv SV_j \Rightarrow UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ A8: $SV_j| \equiv UD_i \Rightarrow UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$

G1: $UD_i \left| \equiv SV_j \right| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ G2: $UD_i| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$

G3: $SV_j \left| \equiv UD_i \right| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ G4: $SV_j| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$

3) Inference Proof: Based on the above assumptions and goals, we use the following steps to prove that the proposed scheme achieves secure authentication and session key negotiation between *UDi* and *SVj*. Firstly, we summarize the information passed on the common channel during the authentication process, as follows:

Message1: $UD_i \rightarrow SV_j$: $<SUDi>$

Message2: $SV_j \rightarrow UD_i$: $< E, E_1 >$

Message3: $UD_i \rightarrow SV_j$: $<ES_4, ES_5, e_2 >$

Message4: $SV_j \rightarrow UD_i$: $<EK, ECi, e_3 >$

Message5: $UD_i \rightarrow SV_j$: $< E_2, Ee_4 >$

Two pieces of information emerge from this combination:

Message1: $UD_i \rightarrow SV_j$: $< SUDi, ES_4, ES_5, e_2, E_2, Ee_4 >$

Message2: $SV_j \rightarrow UD_i$: $< E, E_1, EK, ECi, e_3 >$

The basic symbols of BAN logic are used to formalize Message1 and Message2 as:

Message1: $SV_j \lhd < SUDi, ES_4, ES_5, e_2, E_2, Ee_4 >$ that is:

M1: $SV_j \mathrm{SV_j} \lhd \{UDi, S_4, S_5, e_4\}_{\mathrm{SK}}, \{sk_{ij}\}_{Pf}$

Message2: $UD_i \lhd < E, E_1, EK, ECi, e_3 >$ that is:

M2: $UD_i \lhd \{UDi, Ki, Ci, S_6\}_{SK,Pf}$

Based on the previous work, the specific logical analysis process is as follows:

According to information M1, Message-meaning rule R1 and hypothesis A4, A6, we can get:

S1. $SV_j| \equiv UD_i| \sim UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$

According to S1 and inference rule R2, we can get:

S2. $SV_j| \equiv UD_i| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ (**G3**)

Based on S2 and Jurisdiction rule R3, assumption A8, we get:

S3. $SV_j| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ (**G4**)

From M2, a series of assumptions A1, A2, A3, A5, $sk_{ij} = h(UD_i||Pf'||S_6||e_4||e_3)$, and inference rule R1, we get:

S4. $UD_i \left| \equiv SV_j \right| \sim UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$

Based on S4 and R2, we get:

S5. $UD_i \left| \equiv SV_j \right| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ (**G1**)

Finally, according to S5 and hypothesis A7, inference rule R3 can be applied to obtain:

S6. $UD_i| \equiv UD_i \overset{sk_{ij}}{\leftrightarrow} SV_j$ (**G2**)

B. Formal Security Analysis Using Real-Or-Random (ROR) Model

We are using the Real-Or-Random model proposed by Abdalla *et al.* [42] which proves that the session key security is preserved by the proposed protocol.

1) Real-Or-Random (ROR) Model: In our proposed user authentication and key agreement scheme, there are three parties involved, namely the Endpoint UD of the user and device, the application server SV and cloud-based BaaS. Specific to a session, respectively instantiated as UD_i, SV_j, $BaaS$.

a) Participants: The instances u, t and v of UD_i, SV_j, $BaaS$ are denoted as Π^u_{UDi}, Π^t_{SVj} and Π^v_{BaaS} respectively which are called oracles.

b) Partnering: We denote that the two instances are partnered if they hold the same non-null session key sk_{ij} in the communication. As an instance Π^u_{UDi}'s partner, Π^t_{SVj} is called the partner IDpid^u_{UDi} of Π^u_{UDi}. And sk_{ij} is token to be the partial transcript of authentication process between Π^u_{UDi} and Π^t_{SVj}.

c) Freshness: Π^u_{UDi} or Π^t_{SVj} is treated as fresh if the session key sk_{ij} is not leaked to every adversary via the following given *Reveal*() query.

d) Adversary: An adversary $\mathcal{A}$ can control the communication between Π^u_{UDi} and Π^t_{SVj} through the following query access, so as to achieve active and passive attack on protocol, such as eavesdropping, intercepting, deleting, modifying, forging and injecting other messages.

Execute(Π^t, Π^u): This query is like modelling an eavesdropping attack executed by $\mathcal{A}$ to obtain the messages transmitted between Π^u_{UDi} and Π^t_{SVj}.

Reveal(Π^t): The current session key sk_{ij} generated by Π^t (and its partner) will reveal to adversary by this query.

Send(Π^t, m): This query is modeled as an active attack. By the query, $\mathcal{A}$ will run this query to send a message m to a participant instance Π^t and receives a response message.

CorruptUserToken(Π^u_{UDi}): It corresponds to a user token(smart card) loss/stolen attack wherein $\mathcal{A}$ can get all the sensitive secret information stored in the user token.

Test(Π^t): It is about modeling the semantic security of sk_{ij} established between Π^u_{UDi} and Π^t_{SVj} following the indistinguishability style in this ROR model. Before we start the experiment, a coin c needs to be flipped whose value is the output of *Test*() query and kept secret from the adversary $\mathcal{A}$. When the query is executed by $\mathcal{A}$ and the established session key sk_{ij} is fresh, the instance Π^t returns sk_{ij} if c $= 1$ or a random number in the same domain if c $= 0$; else, it returns null.

e) Semantic security of the session key: In the ROR model, $\mathcal{A}$ is challenged in distinguishing between an instance's real sk_{ij} and a random key. Thus $\mathcal{A}$ is allowed to query numerous *Test*() query to the instance of Π^u_{UDi} or Π^t_{SVj}. The output of *Test*() query needs to be consistent with respect to the random bit c. Finally, $\mathcal{A}$ returns a guessed bit c'. and $\mathcal{A}$ will be successful in the game if c' $=$ c. Let E denote the event in which the $\mathcal{A}$ wins the game. It follows that the gain of $\mathcal{A}$ in breaching the semantic security of our proposed authenticated key-agreement (AKE) protocol, say

P is as follows:

$$Adv_P^{AKE} = |2.Pr\ [E] - 1| \tag{3}$$

where $Pr[X]$ stands for the probability of some event X. We say P is a secure multi-server scheme in the ROR sense when $Adv_P^{AKE} \leq \varphi$, for φ is negligible.

f) Random oracle: As in [43], each participant and $\mathcal{A}$ are provided with a one-way hash function h that is modeled by a random oracle, say *Hash*. And then the *Hash* oracle is simulated by a two-tuple (a, b) table of binary strings. If a hash query $h(a)$ is made, the *Hash* oracle returns b when a is present in the table; else, it returns a uniform random string b and the pair (a, b) is kept safe in the corresponding table.

2) Security Proof: Theorem 1 given below provides the semantic security of our proposed scheme under the ROR model.

Theorem 1: Assume that $\mathcal{A}$ is an adversary running in polynomial time t alongside our scheme P in random oracle, D denotes a uniformly distributed password dictionary and k denotes the number of bits present in the biometric key. And then, the advantage of A in breaking the session key security of P is:

$$Adv_P^{AKE} \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{k-1}|D|} \tag{4}$$

where q_h, q_s, $|Hash|$ and $|D|$ are the number of *Hash* queries, *Send* queries, the range space of hash function h and the size of D.

Proof: We follow a sequence of four games defined as Gi $(i = 0, 1, 2, 3)$ which is similar to that in [11], [43]. Let Ei be an event wherein $\mathcal{A}$ guesses the bit c in game Gi correctly. These games are detailed below.

Game G_0: This corresponds to the actual attack by the adversary $\mathcal{A}$ alongside the proposed scheme P. In this game, the bit c needs to be chosen at the begin of G_0. Hence, it follows that:

$$Adv_P^{AKE} = |2.Pr\ [E_0] - 1| \tag{5}$$

Game G_1: Under this game G_1, $\mathcal{A}$ querys the *Execute*(Π^t, Π^u) oracle to implement the eavesdropping attacks. $\mathcal{A}$ querys the *Test* oracle at the end of G_1. The output of *Test* query is used to decide whether $\mathcal{A}$ could derive the actual session key sk_{ij} between *UDi* and *SVj*. In the proposed protocol, the session key is computed by *UDi* and *SVj* as $sk_{ij} = h(UD_i||Pf||S_6||e_4||e_3)$, where *UDi* is the unique identification of Endpoint UD, *Pf* is a cancelable biometric template which is only known to *UDi* and *SVj*, S_6 is a share secret only known to the real server, e3 and e4 are two random numbers generated by *SVj* and *UDi* respectively and they are encrypted before the public channel transmission. By intercepting information on a public channel, $\mathcal{A}$ cannot obtain the critical message needed to compute the session key. In other words, the chance of winning game G_1 by eavesdropping attack is not increased and it is equivalent to the game G_0. It then follows that:

$$Pr[E_1] = Pr[E_0]. \tag{6}$$

Game G_2: Unlike G_1, we add *Send* and *Hash* oracles to simulate active attacks in this game G_2. Let $\mathcal{A}$ make numerous *Hash* queries to find whether there is a collision. In our scheme, Message1 and Message2 are the information passed on the common channel during the authentication process. Message1 $\{SUDi, ES_4, ES_5, e_2, E_2, Ee_4\}$ contains pre-shared secret key *SK*, the key authentication information *Pf*, the share S_6 only known to real server, the random numbers e_2 and e_4. And Message2 $\{E, E_1, EK, ECi, e_3\}$ also contains pre-shared secret key *SK*, the key authentication information *Ki*, the share S_6 only known to real server, the random numbers e_1 and e_3. Due to the random numbers attached in each message, there is no collision when $\mathcal{A}$ queries the *Send* oracle. According to the birthday paradox results, it follows that:

$$|Pr[E_1] - \Pr[E_2] \leq \frac{q_h^2}{2.|Hash|} \tag{7}$$

Game G_3: This game simulates the *CorruptUserToken* oracle and it models the user token(smart card) lost/stolen attack. The adversary $\mathcal{A}$ can get the message $\{UD_i, S_4, S_5, S_6\}$ from the user token, but nothing of value came out of it. What is stored in the user token is only a partial share based on the biometric template and transformation parameters, which is useless to an attacker who does not know the biometric key. Assuming our scheme applies a strong fuzzy extractor mechanism for extracting at k random bits, the probability of guessing biometric key by $\mathcal{A}$ is approximated as $\frac{1}{2^k}$. If the frequency of wrong password insertion is kept to a definite limit by the system, it follows that:

$$|\Pr[E_2] - \Pr[E_3]| \leq \frac{q_s}{2^k.|D|} \tag{8}$$

Note that the session key all the random oracles are simulated in the game G_3. In order to win the game after querying the *Test* query, A is only left to guess the bit c and we infer that:

$$\Pr[E_3] = \frac{1}{2} \tag{9}$$

According to (5) and (6), we firstly get:

$$\frac{1}{2}Adv_P^{AKE} = \left|Pr\ [E_0] - \frac{1}{2}\right| = \left|Pr\ [E_1] - \frac{1}{2}\right| \tag{10}$$

Based on (9) and triangular inequality formula, then we can get:

$$\begin{aligned}\left|Pr\ [E_1] - \frac{1}{2}\right| &= |Pr\ [E_1] - Pr\ [E_3]| \\ &\leq |Pr\ [E_1] - Pr\ [E_2]| + |Pr\ [E_2] - Pr\ [E_3]|\end{aligned} \tag{11}$$

From (7) and (8), we obtain:

$$\left|Pr\ [E_1] - \frac{1}{2}\right| \leq \frac{q_h^2}{2.|Hash|} + \frac{q_s}{2^k.|D|} \tag{12}$$

That is:

$$\frac{1}{2}Adv_P^{AKE} \leq \frac{q_h^2}{2.|Hash|} + \frac{q_s}{2^k.|D|} \tag{13}$$

To sum up, we can get the following formula, which proves that our scheme can achieve the session key security.

$$Adv_P^{AKE} \leq \frac{q_h^2}{|Hash|} + \frac{q_s}{2^{k-1}.|D|} \tag{14}$$

C. Informal Security Analysis

Based on some common security attributes, and assuming that the public communication channel can be controlled by an attacker, we conducted a detailed informal analysis of the proposed scheme, which more scientifically proved that our scheme can perfectly realize the biological information security and privacy and have enough reference significance.

1) User Anonymity: We use the newly proposed CRO PUF to generate a lightweight key-sharing protocol that generates shared keys for resource-constrained devices to encrypt the original IDs of the communicating parties and the secret information exchanged. At each login, different SUD_i can be realized based on the characteristics of personalized configuration of the hardware structure and selection of different RO challenges. Get rid of the commonly used random number mechanism, and realize the anonymity of users from the perspective of hardware.

2) Freshness of Session Key: We combine the relevant registration information with random numbers to calculate the session key sk_{ij}. The existence of random numbers makes the session key generated every time a connection is established completely different. This feature guarantees the freshness of the session key of our proposed scheme.

3) Database Attacks: We propose a template transformation method (PUF-TTM) to convert the original biological information to generate CB, and then use secret sharing technology to manage CB and conversion parameters, and store them in the user token (smart card), system server and remote server in the form of multiple secret shares. When an attacker tries to steal user privacy by attacking the database, all efforts may be in vain. First of all, the attacker needs to obtain access to all databases and get all the shares to recover the biometric template CB, which is difficult for the attacker to achieve in the case of using distributed databases. Secondly, even if the attacker successfully recovers the conversion template and conversion parameters, he cannot restore the original biometric template. We have performed irreversible conversion of the original biological template, and the attacker can only pass the identity verification if he has real biological information and equipment at the same time. Obviously, the realization of these conditions is extremely difficult, so our scheme successfully resisted database attacks.

4) Impersonation Attacks:

a) Server impersonation attacks: In our solution, *UDi* will first verify the authenticity of *SVj*'s identity. Because only the real server knows the specific information of the share S_6, *UDi* first decrypts the random number e_1 generated by the server, and then verifies whether the XOR result of E_1 and $h(UD_i||e_1)$ is equal to $h(S_6)$ to successfully resist server impersonation attack. Even if an attacker tries to pretend to be a legitimate server, generate a random number instead of e_1, and send the response message $\{E,\ E_1\}$ to *UDi*, he cannot successfully pass the verification and obtain the useful information.

b) User impersonation attacks: The attacker may obtain the user token and biometric through covert means and pretend to be a legitimate user to try to gain access to the server. In the proposed scheme, tamper resistant smart cards are combined with a revocation mechanism. If the user's token is lost, the system can easily issue new token information for it. Therefore, an attacker cannot complete mutual authentication by pretending to be a user or a server.

5) Replay Attacks: The secret sharing technology and revocation mechanism ensure the ability of the proposed scheme to resist replay attacks. First, the conversion template and conversion parameters are generated by the proposed method to generate multiple shares, and then stored in multiple databases in a distributed manner, combined with random number encryption, and transmitted on a public channel. Secondly, our revocation mechanism can generate new shared data to complete user authentication by changing only one share

6) Man-in-Middle Attacks (MIMA): The mutual authentication process of *UDi* and *SVj* involves the transmission of Message1 and Message2, and the attacker will try to intercept and tamper with them. Among them, SK is the shared secret of *UDi* and *SVj*, and *Pf* is the key authentication information that only *UDi* and *SVj* know. Any information obtained by the attacker on the public channel cannot decode the original data, nor can it piece together information about the user's biological characteristics and privacy related snippets. This shows that our scheme is immune to Man-in-Middle attacks.

7) Cross-Matching Attacks: When any user uses the same biometrics to apply for the services of different servers, not only are different pseudo-identities assigned to each server, which can prevent cross-matching between different servers, but also generate different shares based on CB and store them in different databases. CB can be recovered only if a certain amount of shares are obtained, except that the attacker cannot obtain any useful information.

8) Insider Attacks: All secret information is not directly stored in the database. On the one hand, the original biological information is not stored, we complete the biological template comparison in the transformation domain; on the other hand, we distributed storage and sharing based on secret sharing technology. Any malicious insider cannot obtain secret information.

9) Online and Offline Password Guessing Attacks: Our scheme does not involve the use of passwords. We combine facial and fingerprint information to propose a template transformation method PUF-TTM to generate irreversible, revocable, unlinkable and performance-maintained biometric templates, and manage transformation templates and transformation parameters based on secret sharing technology. Therefore, for an attacker, any online or offline password guessing technology is useless. Our scheme perfectly resists all offline and online password guessing attacks.

10) Perfect Forward Secrecy Attacks: When the long-term key is intercepted by the attacker, if the attacker cannot calculate the current or previous session key, it means that the proposed scheme supports forward secrecy. In our

scheme, our session key is calculated based on the transformation template, shares and random numbers, namely $sk_{ij} = h(UD_i||Pf||S_6||e_4||e_3)$, if you don't know $\{UD_i, Pf, S_6, e_4, e_3\}$ cannot calculate sk_{ij}. In addition, Pf is only known by UD_i and SVj, and even if the attacker intercepts all the information on the public channel, sk_{ij} cannot be calculated. In summary, our scheme has perfect forward secrecy.

11) Ephemeral Secret Leakage (ESL) Attacks: Limited by the computing power of mobile devices, many protocols use precomputation technique to store random numbers ahead of time. This makes the protocol vulnerable to ESL attacks. An adversary can decrypt a user's private key by combining the ephemeral secrets (or random values) with intercepted exchanges on a public channel. But our protocol does not have that problem. On the one hand, the proposed protocol is a password free scheme for registration, login, authentication and secure session key establishment in multi-server environment. Authentication based on cancelable biometrics and PUF is our strength. Only legitimate users who have both can pass the server authentication. On the other hand, our registration phase occurs in a cloud-based multi-server interaction with the Endpoint UD, where encrypted data is distributed and stored using secret sharing technology. This makes it impossible for an adversary to obtain the ephemeral secrets (or random values) associated with the session key. Even intercepting the exchange is futile. Therefore, our protocol is secure under the ESL attack.

VII. Conclusion

In this paper, we use PUF-TTM and secret sharing technology to propose a complete BaaS-based multi-server user authentication and key agreement scheme, which achieves more effective biometric template protection and higher security performance. Inspired by the recent success of lightweight authentication systems in the Internet of Things, we introduce PUF into our scheme. On the one hand, we use the properties of PUF to design a template transformation method (PUF-TTM) to generate cancelable biometrics(CB), and combine secret sharing technology to store biological templates and related parameters, on the other hand, ensure the legitimacy of the device during the authentication process, and integrate the device response and biological information in a novel way, which not only protects user privacy, but also further improves the credibility of the biometric authentication system in a multi-server environment. In terms of security and performance analysis, we have carried out security analysis from various aspects and scientific evaluation based on BAN logic, and compared the current research scheme to highlight the innovation and performance advantages of our scheme, ensuring that our proposed scheme can perfectly meet the requirements of non-invertibility, Unlinkability (Diversity), Revocability and Performance. In future work, we will continue to advance research in this field.

References

[1] C. T. Li and M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *Int. J. Innov. Comput., Inf. Control*, vol. 6, no. 5, pp. 2181–2188, 2010.

[2] B. Choudhury, P. Then, B. Issac, V. Raman, and M. K. Haldar, "A survey on biometrics and cancelable biometrics systems," *Int. J. Image Graph.*, vol. 18, no. 1, Jan. 2018, Art. no. 1850006.

[3] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, Dec. 2011.

[4] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on biohashing," in *Proc. Int. Conf. Secur. Cryptogr. (SECRYPT)*, Reykjavik, Iceland, 2013, pp. 1–8.

[5] N. D. Butt, "Helper data scheme for 2D cancelable face recognition using bloom filters," in *Proc. Int. Conf. Syst.*, Dubrovnik, Croatia, 2014, pp. 271–274.

[6] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools Appl.*, vol. 75, no. 23, pp. 16333–16361, Dec. 2016.

[7] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.

[8] K. Gupta, G. S. Walia, and K. Sharma, "Novel approach for multimodal feature fusion to generate cancelable biometric," *Vis. Comput.*, vol. 37, no. 6, pp. 1401–1413, Jun. 2021.

[9] S. Ibjaoun, A. A. El Kalam, V. Poirriez, A. A. Ouahman, and M. de Montfort, "Analysis and enhancements of an efficient biometric-based remote user authentication scheme using smart cards," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov. 2016, pp. 1–8.

[10] W. Bian, P. Gope, Y. Cheng, and Q. Li, "Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme," *Future Gener. Comput. Syst.*, vol. 109, pp. 45–55, Aug. 2020.

[11] J. Zhao *et al.*, "A secure biometrics and PUFs-based authentication scheme with key agreement for multi-server environments," *IEEE Access*, vol. 8, pp. 45292–45303, 2020.

[12] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[13] N. Kumar, "Cancelable biometrics: A comprehensive survey," *Artif. Intell. Rev.*, vol. 53, no. 5, pp. 3403–3446, Jun. 2020.

[14] Y. Wang, "Changeable and privacy preserving face recognition," Ph.D. dissertation, Univ. Toronto, Toronto, ON, Canada, 2010.

[15] K. Atighehchi, L. Ghammam, K. Karabina, and P. Lacharme, "A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing," 2019, *arXiv:1910.01389*.

[16] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[17] A. D. Algarni, G. M. El Banby, N. F. Soliman, F. E. A. El-Samie, and A. M. Iliyasu, "Efficient implementation of homomorphic and fuzzy transforms in random-projection encryption frameworks for cancellable face recognition," *Electronics*, vol. 9, no. 6, p. 1046, Jun. 2020.

[18] Y. Liu, J. Ling, Z. Liu, J. Shen, and C. Gao, "Finger vein secure biometric template generation based on deep learning," *Soft Comput.*, vol. 22, no. 7, pp. 2257–2265, Apr. 2018.

[19] W. Yang, S. Wang, J. Hu, G. Zheng, J. Yang, and C. Valli, "Securing deep learning based edge finger vein biometrics with binary decision diagram," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4244–4253, Jul. 2019.

[20] N. D. Sarier, "Practical multi-factor biometric remote authentication," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Washington, DC, USA, Sep. 2010, pp. 1–6.

[21] M. Alizadeh, W. H. Hassan, and T. Khodadadi, "Feasibility of implementing multi-factor authentication schemes in mobile cloud computing," in *Proc. 5th Int. Conf. Intell. Syst., Modeling Simulation*, Langkawi, Malaysia, Jan. 2014, pp. 615–618.

[22] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.

[23] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," *Future Gener. Comput. Syst.*, vol. 85, pp. 76–87, Aug. 2018.

[24] K. M. S. Soyjaudah, G. Ramsawock, and M. Y. Khodabacchus, "Cloud computing authentication using cancellable biometrics," in *Proc. Africon*, Sep. 2013, pp. 1–4.

[25] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Gener. Comput. Syst.*, vol. 102, pp. 30–41, Jan. 2020.
[26] C. C. Thien and J. C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, 2002.
[27] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jul. 2019.
[28] U. Javaid, M. N. Aman, and B. Sikdar, "Defining trust in IoT environments via distributed remote attestation using blockchain," in *Proc. 21st Int. Symp. Theory, Algorithmic Found., Protocol Design Mobile Netw. Mobile Comput.*, New York, NY, USA, Oct. 2020, pp. 321–326.
[29] R. Arjona and I. Baturone, "A dual-factor access control system based on device and user intrinsic identifiers," in *Proc. 42nd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Florence, Italy, Oct. 2016, pp. 4731–4736.
[30] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 4957–4968, Sep. 2019.
[31] U. Chaterjee, D. Mukhopadhyay, and R. S. Chakraborty, "3PAA: A private PUF protocol for anonymous authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 756–769, 2021.
[32] Y. Zheng, Y. Cao, and C.-H. Chang, "UDhashing: Physical unclonable function-based user-device hash for endpoint authentication," *IEEE Trans. Ind. Electron.*, vol. 66, no. 12, pp. 9559–9570, Dec. 2019.
[33] D. Chang, S. Garg, M. Hasan, and S. Mishra, "Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3152–3167, 2020.
[34] J. Zhang and G. Qu, "Physical unclonable function-based key sharing via machine learning for IoT security," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 7025–7033, Aug. 2020.
[35] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[36] G. R. Blakley, "Safe guarding cryptographic keys, managing requirements knowledge," in *Proc. IEEE Comput. Soc. Int. Workshop*, New York, NY, USA, Jun. 1979, p. 313.
[37] G. B. Huang *et al.*, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," in *Proc. Workshop Faces Real-Life Images, Detection, Alignment, Recognit.*, E. Learned-Miller, A. Ferencz, and F. Jurie, Eds. Marseille, France, 2008, pp. 1–14.
[38] M. Gunther, S. Cruz, E. M. Rudd, and T. E. Boult, "Toward open-set face recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Honolulu, HI, USA, Jul. 2017, pp. 71–80.
[39] P. J. Phillips, P. Grother, and R. Micheals, "Evaluation methods in face recognition," in *Handbook of Face Recognition*. London, U.K.: Springer, 2011, pp. 551–574.
[40] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.
[41] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A, Math. Phys. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[42] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Pract. Public Key Cryptogr. (PKC)*, in Lecture Notes in Computer Science, Berlin, Germany, 2005, pp. 65–84.
[43] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.