Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **3**, May **2015**

An Efficient and Secure Biometrics-based One-Time Identity-Password Authenticated Scheme for E-coupon System towards Mobile Internet

Hongfeng Zhu, Yu Xia and Hui Li

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com, 593466728@qq.com, 876526606@qq.com

Received August, 2014; revised November, 2014

Abstract. *Authenticated key agreement protocols, aiming at solving the problems to set up a secure channel over public Internet, can achieve authentication of the corresponding participants and confidentiality of data transmission. Nowadays, most of the authenticated key agreement protocols pay close attention to security, efficiency and user friendly at the same time. One-time password-authenticated algorithm, which is that a hash chain can update by itself smoothly and securely through capturing the secure bit of the tip, has the feature of high-efficient. In addition, biometrics-based algorithm can make the scheme become more secure and user friendly. The combination of above-mentioned algorithms can lead to a high-practical scheme in the universal client/server architecture. Based on these motivations, the paper firstly proposed the new concept of one-time identity-password which means the identity and the password can be used only once. Then a new robust biometrics-based one-time identity-password (OTIP) authenticated key agreement protocol is given for E-coupon system. Security of the protocol is based on the biometric authentication and a secure one way hash function with the hash chain. At the same time the proposed protocol can not only refrain from many consuming algorithms, but is also robust to many kinds of attacks and owns much excellent features. Finally, we provide the secure proof and the efficiency analysis about our proposed scheme.*
Keywords: Authentication, Biometrics, One-time identity-password, E-coupon

1. **Introduction.** With the rapid development of mobile internet related to many service providers such as stock exchanging, commodity trading, and banking, many key agreement protocols have been studied widely. However, many authentication key agreement protocols used in M-commerce are designed for cable network and consume much communication rounds and computation costs , making them unfit for mobile internet surroundings. Furthermore, M-commerce is designed to satisfy user experience, especially for security and efficiency. So the paper purposes to design an authenticated key agreement scheme for E-coupon system which can achieve high-level security, high-efficiency and user friendly at the same time.

One time password (OTP) means that the password can be used only once. Nowadays, OTP has been widely used in the financial sector, telecommunications, online game field and so on. As a general rule, traditionally static password, for its security, can be easily stolen because of Trojan horse and keylogger program. It may also be cracked by brute force if an adversary spends enough time on it. Attackers can impersonate the legal user to communicate with the service server, and even modify the password of the legal user so that legal user cannot login the server. To address these conditions, OTP was developed

as a solution. It is an approach to effectively protect the safety of the users.
Lamport [1] firstly put forward a method of user password authentication using a one way function to encode the password in 1981. Obviously, due to the higher safety request of the user, many schemes based on this method [2-8] have been proposed. In 2000, Tang [2] proposed a strong directed OTP authentication protocol with discrete logarithm assumption. In 2010, based on the use of OTP in the context of password-authentication key exchange (PAKE), which can offer mutual authentication, session key exchange, and resistance to phishing attacks, Paterson et al. [3] proposed a general technique which allows for the secure use of pseudorandomly generated and time-dependent passwords. In 2011, Fuglerud et al. [4] proposed an accessible and secure authentication way to log in to a banking server, which used a talking mobile OTP client rather than dedicated OTP generators. Later, Li et al. [5] proposed a two-layer authentication protocol with anonymous routing on small Ad-hoc devices. In 2012, Mohan et al. [6] proposed a new method using OTP to ensure that authenticating to services, such as online shopping, was done in a very secure manner. In 2013, Huang et al. [7] proposed an effective simple OTP method that generates a unique passcode for each use. In Huangs method, OTP calculation used time stamps and sequence numbers. In addition, a two-factor authentication prototype for mobile phones using Huangs method has been used in practice for a year. In 2014, Xu et al. [8] proposed a self-updating OTP mutual authentication scheme based upon a hash chain for Ad hoc network. The updating process can be unlimited used without building a new hash chain.
However, these literatures [1-8] only care about covering the password with one-time password. In fact, the identity information is equally important. Because an adversary can retrive much useful information form the static identity by connecting with other information. Based on these motivations, the article presents a new simple biometrics-based one-time identity-password (OTIP) authenticated with key agreement protocol for mobile device using in E-coupon system between user and server to t mobile internet communication setting. Compared with previous related protocols, the proposed scheme has the following more practical advantages: (1) it firstly presents the concept of one-time identity-password. (2) it provides a kind of biometric authentication function securely [9], (3) it provides simple and robust session key agreement by adopting one-time identity-passowrd, (4) it provides secure one-time identity-password and biometrics and Seed update function by using biometrics update protocol, and (5) it can decrease the total calculated amount and communication rounds due to the hash chain and Xored operation, (6) it is secure against well-known kinds of attacks, (7) it is a high-efficiency and integrated E-coupon system.
The organization of the article is described as follows: some preliminaries are given in Section 2. Next, a biometrics-based one-time password-authenticated with key agreement scheme is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2. **Preliminaries.**

2.1. **One-way Hash Function.**

A secure cryptographic one-way hash function $h : a \to b$ has four main properties:
(1) The function h takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;
(2) The function h is one-way in the sense that given a , it is easy to compute $h(a) = b$.However, given b, it is hard to compute $h^{-1}(b) = a$;

(3) Given a , it is computationally infeasible to find a' such that $a' \neq a$,but $h(a') = h(a)$;
(4) It is computationally infeasible to find any pair a,a' such that $a' \neq a$,but $h(a') = h(a)$.

2.2. **Biometric authentication.** Each user has their unique biometric characteristics, such as voice, fingerprints, iris recognition and so on. These biometric characteristics have irreplaceable advantages: reliability, availability, non-repudiation and less cost. Therefore, biometric authentication has widely used. Fig.1 is the flow diagram of biometric characteristics collection and authentication. During the biometric collection phase, a biometric sample is collected, processed by a smart device, and stored which prepared for subsequent comparison (Fig.1). During the biometric authentication phase, the biometric system compares the stored sample with a newly captured sample (Fig.1). Obviously, smart device has powerful information confidentiality and flexible portability. When performing a biometric authentication process, a user inputs a smart device, and utilizes a simple finger touch or a glance at a camera to authenticate himself/herself [9, 11, 12].

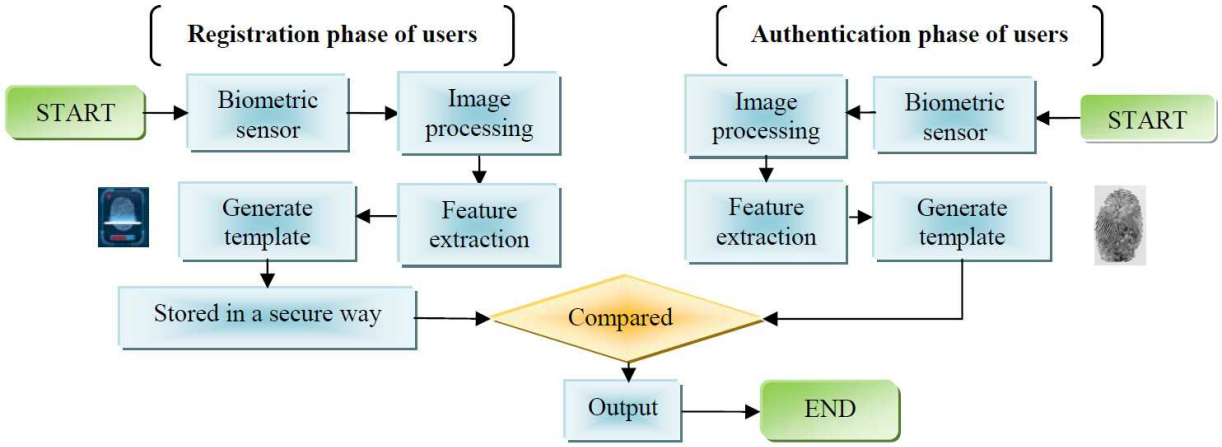

FIGURE 1. The flow diagram of Biometric characteristics collection and authentication

2.3. **Hard-Core Predicate and Hash Chain.** General speaking, a polynomial-time predicate b is called a hard-core of a function f if each efficient algorithm, given $f(x)$,can guess $b(x)$ with success probability that is only negligibly better than one-half.

Definition 2.1. (Hard-Core Predicate) *A polynomial-time-computable predicate* $b : \{0,1\}^* \to \{0,1\}^n$ *is called a hard-core of a function* f *for each probabilistic polynomial-time algorithm* $A^{\sim}$*, each positive polynomial* $p(\cdot)$*, and all sufficiently large* n *has* $\Pr[A^{\sim}(f(U_n)) = b(U_n)] \leq \frac{1}{2} + \frac{1}{p(n)}$*.* U_n *is a random variable uniformly distributed in* $\{0,1\}^n$*.*

Definition 2.2. (Hash Chain) *Select a cryptographic secure hash function* h *with secure parameter* $k : \{0,1\}^* \to \{0,1\}^k$*. Pick a seed* s *randomly and apply* h *recursively* N *times to an initial seed* s *to generate a hash chain. The tip* ω *of the chain equals* $h^N(s)$*.*
$\omega = h^N(s) = h(h^{N-1}(s)) = \underbrace{h(h(h(...h(s))))}_{N \quad Times}$

2.4. **RSA Cryptography.** Rivest, Shamir, and Adleman first designed the RSA cryptography system in 1977. Subsequently, several other researchers began to use the RSA system to accomplish the applications of digital signature and data encryption. In the RSA system,we can generate two keys - a public key and a private key. The keys can easily be built between Entity C as follows:
C first chooses two different large prime numbers p, q and computers $n = pq$. Then, C

generates e that satisfies $\gcd(e,(n))=1$, where $\varphi(n)=(p-1)(q-1)$. Finally C can get d from computing $ed \equiv 1 \mathrm{mod} \varphi(n)$.
As mentioned above, (n,e) is the public key and (p,q,d) is the private key. To protect the integrity of the message, the signer can use the private key to sign the message as $(m)^d$ and the verifier can use the signature and public key to check the integrity of the message m as $((m)^d)^e=(m)^{ed} \mathrm{mod} n=m$.

3. **The Proposed Protocol.** In this section, biometrics-based one-time identity-password authenticated key agreement scheme is proposed which consists of three phases: the user registration phase, authenticated key agreement phase and the Seed and one-time password update phase (because the temporary identity is updated in every authenticated key agreement phase). But firstly some notations are given which used in the proposed scheme.

3.1. **Notations.** The concrete notation used hereafter is shown in Table 1.

Table 1. Notations

Symbol	Definition
ID_A,ID_S,ID_{TTP}	The identity of a user and the shop and the TTP server, respectively
TID_{A_t}	The temporary identity of Alice
R_{A_x}, R_{S_x}	nonces
B	the biometric sample of user
τ	predetermined threshold for biometric verification
$d()$	symmetric parametric function
h	A secure one-way hash function
$Seed$	An initial seed to generate a hash chain by the TTP server
$\|\|$	concatenation operation
$\oplus$	XORed operation
z	E-coupon
t	the reverse counter of the chosen hash chain by the server

3.2. **User registration phase.** Concerning the fact that the proposed scheme mainly relies on the design of one-time identity-password, it is assumed that the user can register at his appointed server in some secure way or by secure channel. The same assumption can be set up for the TTP server. Fig.2 illustrates the user registration phase.
Step 1. When a user Alice wants to be a new legal user, she chooses her identity ID_A at liberty and sends it to the trusted third party TTP with some her necessary information.
Step 2. Upon receiving the request from Alice, TTP selects a Seed, a random number R_{TTP_0} and setting a secure parameter N.Then TTP initialize the temporary identity TID_{A_0} and computes $h(R_{TTP_0})$,
$Seed_{A-TTP} \oplus R_{TTP_0}$ and sends $\{N, Seed_{A-TTP}, TID_{A_0}\}$ to Alice via a secure channel.
Step 3. Upon receiving the message $\{N, Seed_{A-TTP}, TID_{A_0}\}$, Alice inputs her personal biometric image sample B at the mobile device. Then Alice computes $p_t = h^{N-t}(h(B) \oplus Seed_{A-TTP} \oplus h(ID_A||ID_{TTP}))$ and submits $\{p_0\}$ to TTP via a secure channel. Finally Alices mobile device stores $\{TID_{A_0}, Seed_{A-TTP}, B, h, d(), \tau, p_t(0 \le t < N)\}$ securely, where $d(\cdot)$ is a symmetric parametric function and τ is predetermined threshold for biometric authentication. The parameter t is the reverse counter of the chosen hash chain: when $t=0$, the $h^N()$ of hash chain is the first instance used in the proposed protocol. When $t=N-1$,

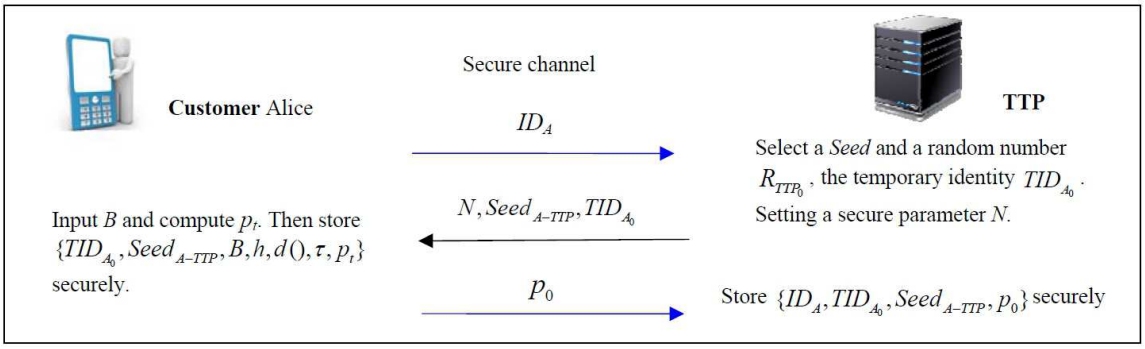

FIGURE 2. User registration phase (Customer Alice as an example)

the $h^{N-(N-1)}() = h()$ of hash chain is the last used instance in our proposed protocol.
Step 4. Upon receiving the message $\{p_0\}$, TTP stores $\{ID_A, TID_{A_0}, Seed_{A-TTP}, p_0\}$ securely.
Remark: In brief, the SHOP S can be as a user to registration on the TTP server. The only difference comparison with the customer Alice registration on the TTP server is the notationss subscripts, such as $Seed_{S-TTP}$,ID_S, TID_{S_0} and so on.

3.3. **Issue e-coupon phase.** Shop S has the biometric sample B*, and her mobile device (Seed, B, h, d(),τ,pt,$\tau, TID_{A_{t-1}}$). TTP securely kept the secret information $Seed_{S-TTP}$, pt-1,$TID_{S_{t-1}}, ID_S$. This concrete process is presented in the Fig. 3.
Step 1. If Shop S wishes to establish a session key with TTP, she imprints biometric B^* at the mobile device with her IDS. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, which means Shop S will get a connection refused response. If $d(B^*, B) < \tau$, which means Shop S will get a connection accepted response. Then the mobile device selects random R_{S_t} (the same length with $Seed_{S-TTP}$) and e-coupon z, then computes:$C_1 = E_{Seed_{S-TTP}}(R_{S_t}||ID_S||ID_{TTP}||z)$. After that, the mobile device sends $m_1 = \{TID_{S_{t-1}}, C_1\}$ to the TTP.
Step 2. After receiving the message $m_1 = \{TID_{S_{t-1}}, C_1\}$ from S, TTP will do the following tasks:
(1) Using $TID_{S_{t-1}}$tofind$Seed_{S-TTP}$andp_{t-1} and decrypt C_1toget$R_{S_t}||ID_{TTP}||ID_S||z$.
(2) Selects random R_{TTP_t} and computes $M_{t_1} = N - t$,$M_{t_2} = Seed_{S-TTP} \oplus h(R_{S_t}||R_{TTP_t})$, $M_{t_3} = h(h(R_{S_t}||R_{TTP_t})) \oplus p_{t-1}$,$M_{t_4} = h(h(R_{S_t}||R_{TTP_t})||TID_{S_{t-1}}) \oplus TID_{S_t}$, $K_{S-TTP} = h(h(R_{S_t}||R_{TTP_t})||ID_S||ID_{TTP})$.
(3)Use d to sign z and ID_S.Compute$C_2 = E_{K_{S-TTP}}\left(z||h(z||ID_S)^d||ID_S||ID_{\text{TTP}}\right)$. Store ID_S, z and $h(z||ID_S)^d$ into database and publish e. Finally TTP sends the message $m_2 = \{M_{t_i}(i = 1, 2, 3, 4), C_2\}$ to S.
Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, C_2\}$, S will check if $h(M_{t_2} \oplus Seed_{S-TTP}) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, S terminates it simply. Otherwise that means S authenticates TTP in this instance. Then S computes $m_3 = p_t \oplus h(R_{S_t}||R_{TTP_t})$, $TID_{S_t} = M_{t_4} \oplus h((M_{t_2} \oplus Seed_{S-TTP})||TID_{S_{t-1}})$,$K_{S-TTP} = h(h(R_{S_t}||R_{TTP_t})||ID_S||ID_{TTP})$ and deletes p_t.
UseK_{S-TTP}todecryptC_2andverifyID_SandID_{TTP}. Finally S replaces $TID_{S_{t-1}}$byTID_{S_t} and sends $m_3 = p_t \oplus h(R_{S_t}||R_{TTP_t})$ to TTP .
Step 4. After receiving m_3 , TTP computes $p_{t-1}^{\sim} = h(m_3 \oplus h(R_{S_t}||R_{TTP_t}))$ and verifies

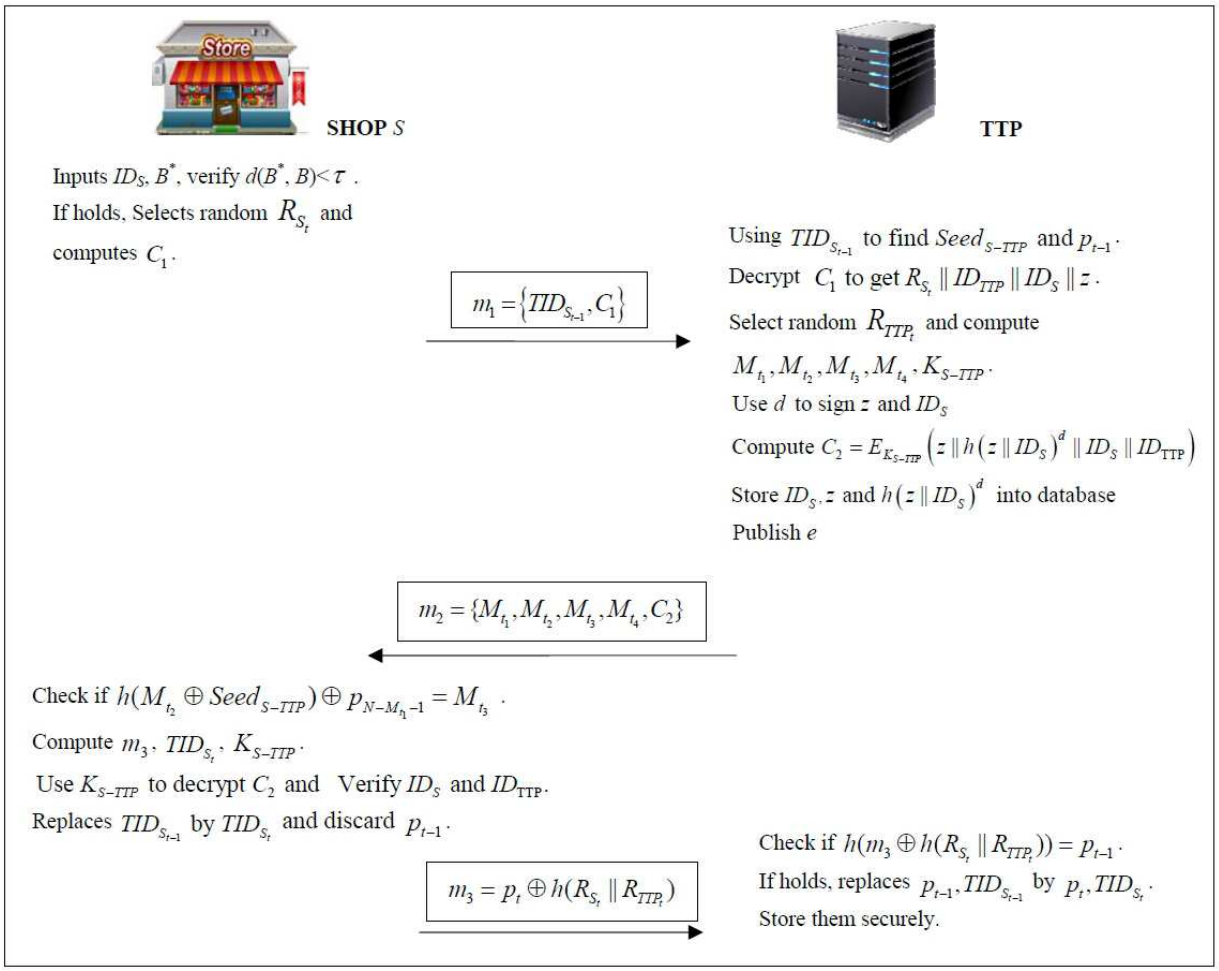

FIGURE 3. Issue e-coupon phase in our proposed scheme

whether $p_{t-1}^{\sim} = p_{t-1}$ or not. If it does not hold, TTP terminates it. Otherwise, TTP replaces $p_{t-1}, TID_{S_{t-1}}$ by p_t, TID_{S_t} and stores them securely.

3.4. **Download e-coupon phase.** Alice has the biometric sample B^*, and her mobile device ($Seed_{A-TTP}$, B, h, $d()$,τ, p_t, τ,$TID_{A_{t-1}}$). S securely kept the secret information ($Seed_{A-TTP}$, p_{t-1}, $TID_{A_{t-1}}$,ID_A). This concrete process is presented in the following Fig. 4.

Step 1. If Alice wishes to download e-coupon from TTP, she imprints biometric B^* at the mobile device with her ID_A. Then the biometric authentication process of mobile device compares the newly captured B^* with the stored B. If $d(B^*, B) \geq \tau$, which means Alice will get a connection refused response. If $d(B^*, B) < \tau$, which means Alice will get a connection accepted response. Then the mobile device selects random R_{A_t} (the same length with Seed) and computes $C_1 = E_{Seed_{A-TTP}}(R_{A_t}||ID_A||ID_{TTP})$. After that, the mobile device sends $m_1 = \{TID_{A_{t-1}}, C_1\}$ to the TTP.

Step 2. After receiving the message $m_1 = \{TID_{A_{t-1}}, C_1\}$ from Alice, TTP will do the following tasks:

(1) Using $TID_{A_{t-1}}$tofind$Seed_{A-TTP}$andp_{t-1} and decrypt C_1togetR_{A_t}.

(2) Selects random R_{TTP_t} and computes $M_{t_1} = N-t$,$M_{t_2} = Seed_{A-TTP} \oplus h(R_{A_t}||R_{TTP_t})$,$M_{t_3} = h(h(R_{A_t}||R_{TTP_t})) \oplus p_{t-1}$,$M_{t_4} = h(h(R_{A_t}||R_{TTP_t})||TID_{A_{t-1}}) \oplus TID_{A_t}$,$K_{A-TTP} = h(h(R_{A_t}||R_{TTP_t})||ID_A||ID_{TTP})$.

(3) UseID_Stofind$z$and$h(z||ID_S)^d$, $C_2 = E_{K_{A-TTP}}(z||h(z||ID_S)^d||ID_A||ID_{\text{TTP}})$. Finally TTP sends the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, C_2\}$ to Alice.

Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, C_2\}$, Alice will check if $h(M_{t_2} \oplus Seed_{A-TTP}) \oplus p_{N-M_{t_1}-1} = M_{t_3}$. If the equation does not hold, Alice terminates it simply. Otherwise that means Alice authenticates TTP in this instance. Then Alice computes $m_3 = p_t \oplus h(R_{A_t}||R_{TTP_t})$, $TID_{A_t} = M_{t_4} \oplus h((M_{t_2} \oplus Seed_{A-TTP})||TID_{A_{t-1}})$, $K_{A-TTP} = h(h(R_{A_t}||R_{TTP_t})||ID_A||ID_{TTP})$ and deletes p_t. Alice uses K_{A-TTP} to decrypt C2 to verify ID_AandID_{TTP}. Then Alice gets $z$and$h(z||ID_S)^d$. Next Alice replaces $TID_{A_{t-1}}$byTID_{A_t} and sends $m_3 = p_t \oplus h(R_{A_t}||R_{TTP_t})$ to TTP. Finally Alice can use the E-coupon $z$and$h(z||ID_S)^d$ at anytime.

Step 4. When TTP obtains m_3,TTP computes $p_{t-1}^{\sim} = h(m_3 \oplus h(R_{A_t}||R_{TTP_t}))$ and verifies whether $p_{t-1}^{\sim} = p_{t-1}$ or not. If it does not hold, TTP terminates it. Otherwise, TTP replaces p_{t-1} by p_t to store p_t securely.

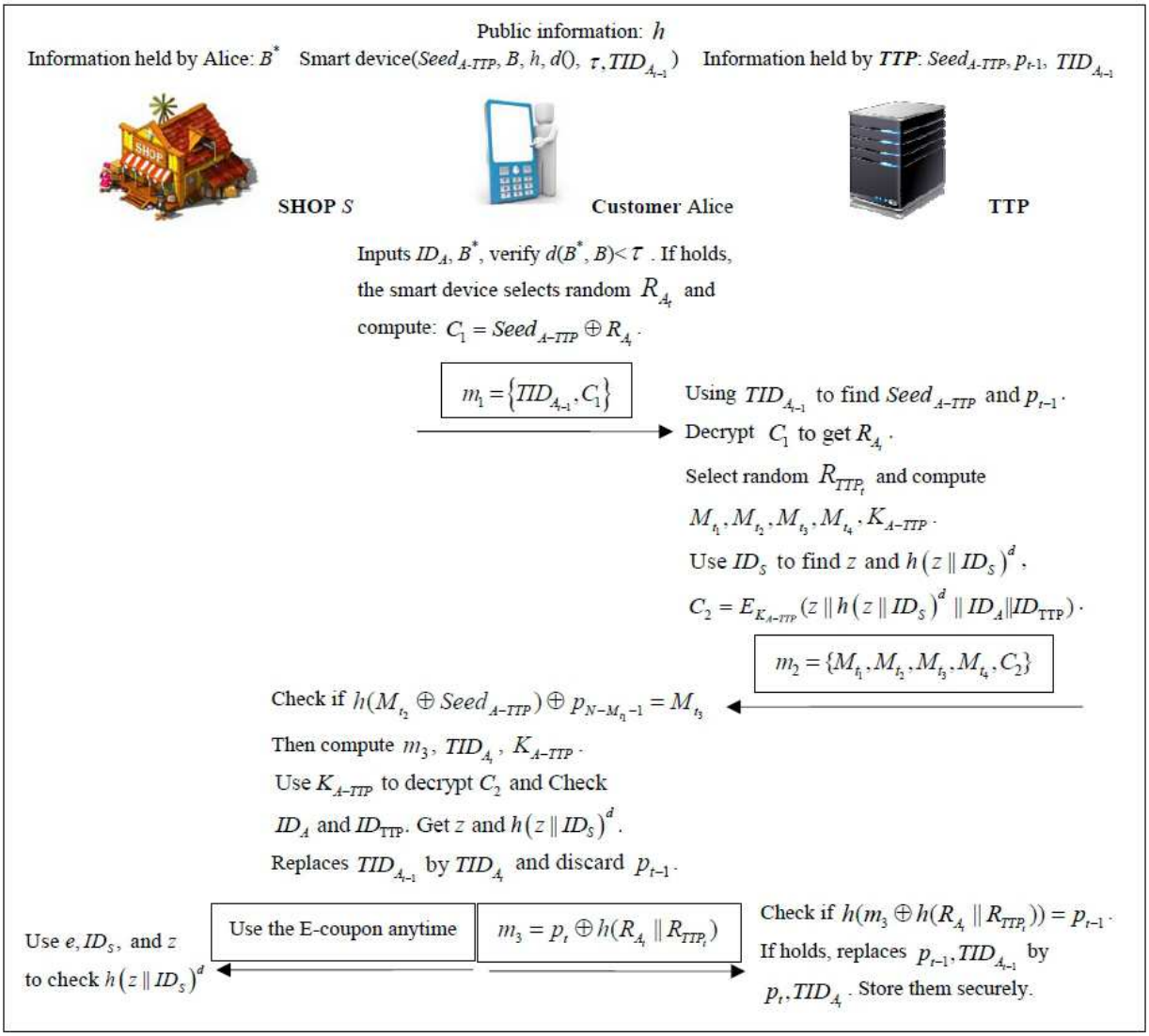

FIGURE 4. Download e-coupon phase in our proposed scheme

3.5. **The Seed and one-time password update phase.** Fig.5 illustrates biometrics and password update phase. The steps are mobile device compares the newly captured

B^* with the stored B. If performed during the Seed and one-time password update phase as follows.

Step 1. When t = N-1, a user (Alice or Shop S) and TTP need to update the Seed and one-time password at the same time. The user imprints biometric B^* at the mobile device. Then the biometric authentication process of $d(B^*, B) \geq \tau$, which means the user will get a connection refused response. If $d(B^*, B) < \tau$, which means the user will get a connection accepted response. Then the user inputs her ID_A, and the mobile device selects random $R_{A_{N-1}}$ (the same length with Seed) and computes: $R_{A_{N-1}} \oplus Seed$. After that, the mobile device sends $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$ to TTP.

Step 2. After receiving the message $m_1 = \{TID_{A_{N-2}}, R_{A_{N-1}} \oplus Seed\}$ from the user, TTP will do the following tasks:

(1) Compute $R_{A_{N-1}} = R_{A_{N-1}} \oplus Seed \oplus Seed$;

(2) Selects random $R_{TTP_{N-1}}, Seed^{\sim}$ and computes $M_{t_1} = N - t = N = N - N + 1 = 1$, $M_{t_2} = Seed \oplus h(R_{A_{N-1}}||R_{TTP_{N-1}})$,$M_{t3} = h(h(R_{A_{N-1}}||R_{S_{TTP-1}})) \oplus p_{t-1}$, $M_{t_4} = h(h(R_{A_{N-1}}||R_{TTP_{N-1}})||TID_{A_{N-2}}) \oplus TID_{A_0}^{\sim}$ and $M_{t_5} = Seed \oplus Seed^{\sim}$.

Finally TTP sends the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$ to the user.

Step 3. After receiving the message $m_2 = \{M_{t_1}, M_{t_2}, M_{t_3}, M_{t_4}, M_{t_5}\}$, the user will check

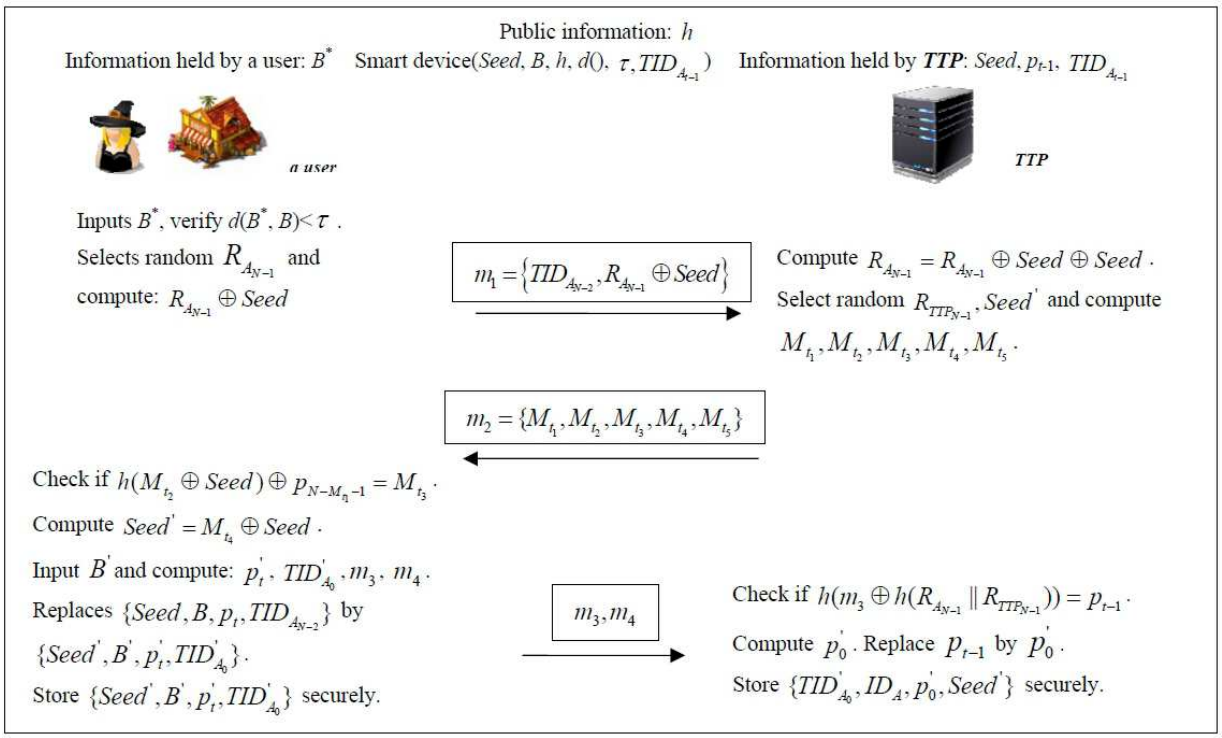

FIGURE 5. The Seed and one-time integrated information update phase (when t = N-1)

if $h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1} = M_{t3}$. If the equation does not hold, the user terminates it simply. Otherwise that means the user authenticates TTP in this instance. The user inputs biometric image sample $B^{\sim}$and then mobile device computes

$$p_t^{\sim} = h^{N-t}(h(B^{\sim}) \oplus Seed^{\sim} \oplus h(ID_A))$$

,

$$TID_{A_0}^{\sim} = M_{t_4} \oplus h((M_{t_2} \oplus Seed)||TID_{A_{N-2}})$$

, $m_3 = p_t \oplus h(R_{A_{N-1}}||R_{TTP_{N-1}})$ and $m_4 = p_0^{\sim} \oplus h(R_{A_{N-1}}||R_{TTP_{N-1}})$. Next the user sends to TTP. Finally the users mobile device will replaces $\{Seed, B, p_t, TID_{A_{N-2}}\}$ by $\{Seed^{\sim}, B^{\sim}, p_t^{\sim}, TID_{A_0}^{\sim}\}$ and stores $\{Seed^{\sim}, B^{\sim}, p_t^{\sim}, TID_{A_0}^{\sim}\}$ securely.

Step 4. When TTP obtains m_3, m_4, TTP computes $p_{t-1}^{\sim} = h(m_3 \oplus h(R_{A_{N-1}}||R_{TTP_{N-1}}))$ and verifies whether $p_{t-1}^{\sim} = p_{t-1}$ or not. If it does not hold, TTP terminates it. Otherwise, TTP computes $p_0^{\sim} = m_4 \oplus h(R_{A_{N-1}}||R_{TTP_{N-1}})$ to replace p_{t-1} by $p_0^{\sim}$ for storing $\{TID_{A_0}^{\sim}, ID_A, p_0^{\sim}, Seed^{\sim}\}$ securely.

4. **Security Consideration.** The section analyzes the security of our proposed protocol. The structure of analysis security just sees the Figure 6. Let us assume that there are two secure components, including a secure one-way hash function and a secure symmetric encryption. Stored information, especially for seed, can be reserved in a secure way. Assume that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. The definitions and analysis of the security requirements [18-20] will be illustrated in this section.

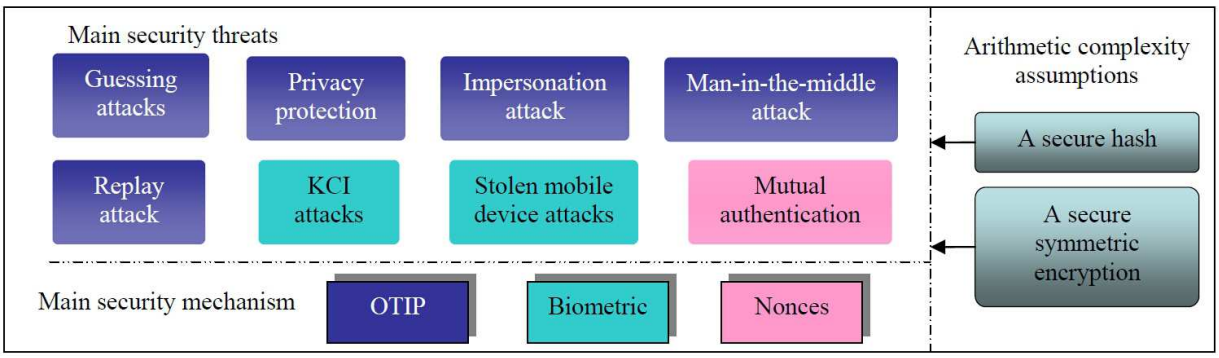

FIGURE 6. The structure of analysis security

Remark: Because there is no session key in our proposed scheme, so some security threats (such as known-key security, perfect forward secrecy and session key security and so on) need not to analyze. We can draw a conclusion that the proposed scheme provided One-time identity-password feature which can wipe out many attacks relating the static identity and static password. At the same time, our proposed protocol prevents the KCI attacks owing to OTIP mechanism.

4.1. **Security threats can be wiped out owing to shift static identity-password to dynamic identity-password. (1) Off-line dictionary/guessing attacks**

In an off-line dictionary/guessing attack, an attacker random chooses a word from a dictionary or guesses a password and verifies his choose or guess, but he does not need to participate in any communication phase because he has already downloaded the nessesary information.

In our proposed scheme of the authenticated key exchange phase, the off-line dictionary/guessing attack will not affect, because there is no fixed password at all. Furthermore, the mobile device authenticated Alice only by Alices personal biometric image sample B .Therefore, the proposed scheme can resist guessing attacks.

(2) Privacy protection

Our proposed protocol can protect users privacy because we firstly adopt the one-time identity-password. For example, the message $m_1 = \{TID_{S_{t-1}}, C_1\}$, there is two information: one is a temporary identity used only one, the other is a cipher text. So an adversary

cannot get any useful information about users or the TTP during the transmitting procedure. And for others transmitted messages, there is also no useful information about users or the TTP. Therefore, the proposed scheme can provide privacy protection.

(3) Impersonation attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.

An adversary cannot impersonate anyone of the user or TTP. First of all, owing to adopt one-time identity-password idea, an adversary cant launch an impersonation attack because he doesnt know the identity of the user at all. Even if the adversary eavesdropping on the line year by year, he get the temporary identities which are nothing but some random numbers.

Even if the adversary get the real identity of a user in a certain way (such as social engineering), he also cant launch an impersonation attack. Because the users and TTP all choose the random numbers (R_{S_t}, R_{TTP_t}) to protect sensitive information and keep messages fresh, there is no way for an adversary to have a chance to carry out impersonation attack.

(4) Man-in-the-middle attack

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

First of all, an adversary cant launch a man-in-the-middle attack because he doesnt know the identity of the user at all. The adversary doesnt know how to become the middle man between the two hiding men.

Even if the adversary get the real identity of a user in a certain way (such as social engineering), and he also cant launch a man-in-the-middle attack. Because $m_i (1 \leq i \leq 3)$ contain the secret Seed and the nonces, a man-in-the-middle attack cannot succeed.

(5) Replay attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Any replay attack cant be carried out, because the temporary identity can be used only once.

4.2. **Immune to the security threats owing to adopt biometrics authentication.**

(6) Key Compromise Impersonation Attacks (KCI attacks)

An adversary is said to impersonate a party B to another party A if B is honest and the protocol instance at A accepts the session with B as one of the session peers but there exists no such partnered instance at B [17]. In a successful KCI attack, an adversary with the knowledge of the long-term private key of a party A can impersonate B to A.

Because there is no password at all and the mobile device authenticated user only by users personal biometric image sample B, the key compromise impersonation attacks will fail.

(7) Stolen mobile device attacks

Anyone gets the mobile device in some way to execute some kinds of attacks.

It is very clear that the proposed scheme provides biometrics authentication. Anyone including an adversary cannot pass the biometric verification. Therefore, the proposed scheme can resist stolen mobile device attacks.

4.3. **Resist the security threat owing by nonces. (8) Mutual authentication**

Mutual authentication refers to two parties authenticating each other suitably and simultaneously.

If $h(M_{t_2} \oplus Seed) \oplus p_{N-M_{t_1}-1}$ equals M_{t_3} , which means that TTP was already authenticated by the user. Because only TTP can retrive the users random number by secret Seed.
If $h(m_3 \oplus h(R_{A_t}||R_{S_t}))$ equals p_{t-1}, which means that the user was already authenticated by TTP. Because only the user can retrive the $h(R_{A_t}||R_{S_t})$ by the secret Seed.

5. **Efficiency Analysis.** In our proposed protocol, no time-consuming modular exponentiation and scalar multiplication on elliptic curves are needed.

TABLE 2. Computational cost of our proposed scheme and comparisons with [10].

Phase	**Entity**	**Cryptography operation[10] (2014)**					**Our Proposed Scheme**				
		S	As	Ch	H	BA	S	As	Ch	H	BA
User registration	Shop	0	0	0	2	0	0	0	0	$N+2$	1
	Alice	0	0	0	2	0	0	0	0	$N+2$	1
	TTP	0	0	0	2	0	0	0	0	$N+2$	1
Issue e-coupon	Shop	2	0	3	2	0	2	0	0	5	1
	TTP	3	1	2	0	0	2	1	0	5	0
Download e-coupon	Alice	2	0	3	2	0	1	0	0	5	1
	TTP	3	0	2	0	0	1	0	0	4	0
	Shop	0	1	0	0	0	0	1	0	0	1
App recondition	Alice	0	0	0	2	0	0	0	0	0	1
	TTP	1	0	1	2	0	0	0	0	0	0
Password renovation	User(Alice and Shop)	0	0	0	3	0	0	0	0	$N+5$	1
	TTP	1	0	0	3	0	0	0	0	4	0
Total		14	2	13	22	0	6	2	0	3N+32	7

Table 2 shows the computational cost of our proposed scheme and the comparisons between our proposed scheme and Chang and Suns scheme of [10]. Therefore, as in Table 2, we can draw a conclusion that the proposed scheme has the lowest computational costs and is well suited to the mobile devices applications. Here, the operations used in our proposed scheme include symmetric encryption/decryption (S), asymmetric encryption/decryption (As), Chebyshev chaotic maps operation (Ch), the one-way hash function (H), and biometric authentication (BA).
Fig.7 illustrates the concrete values with the N changing between our proposed scheme and Chang and Suns scheme of [10]. We compared the computation of symmetric encryption/decryption, Chebyshev chaotic maps operation and the one-way hash function. There are two reasons to exclude asymmetric encryption/decryption and biometric authentication: one side, its the same calculation times with asymmetric encryption/decryption for our protocol and the literature [10]. On the other side, the computation process of biometric authentication adopts dedicated hardware which can make biometric authentication complete quickly with a good user experience.
So we divided the total computations into two steps:
(1) The first step including user registration phase and password renovation phase which can only be used once. $(10T_H + 1T_{CH} + 3T_S)$ is the computations of [10] and $(13T_H + 3NT_H)$ is the computations of our proposed scheme. Where T_H, T_{CH}, T_S means

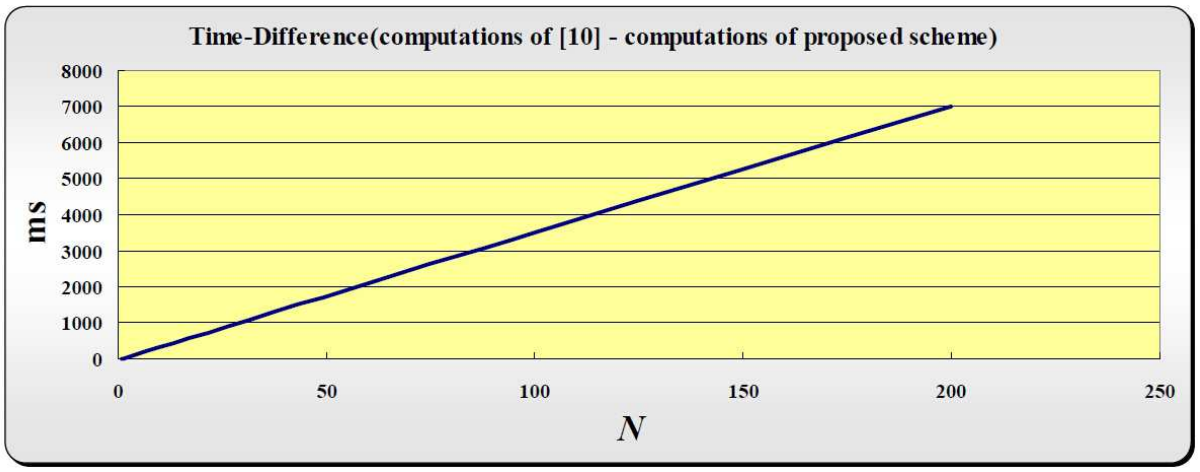

FIGURE 7. Total difference between the amount of computations between literature [10] and our proposed scheme

he time for executing the hash function, Chebyshev chaotic maps operation and symmetric encryption/decryption.
(2) The second step including Issue e-coupon phase, Download e-coupon phase and App recondition phase which can be used $(N-1)$ times.$(8T_H+11T_{CH}+11T_S)$ is the computations of [10] and $(19T_H+6T_S)$ is the computations of our proposed scheme at a time. So the difference of total calculated amount between literature [10] and our proposed scheme is:

$$\begin{aligned}
&Total_{time-difference} = Total_{\text{computations of [10]}} - Total_{\text{computations of our protocol}} \\
&=(10T_H + 1T_{CH} + 3T_S) - (13T_H + 3NT_H) + (N-1)[(8T_H + 11T_{CH} + 11T_S) - \\
&(19T_H + 6T_S)] \\
&=N(11T_{CH} + 5T_S - 14T_H) - 10T_{CH} - 2T_S + 8T_H
\end{aligned}$$

In Chang et al. [10] scheme, they coded a C language program of hash function, they input a 512-bit random string and implemented the program 10,000 times in a Window 7 workstation with an AMD Phenom^{TM}II X4 945 processor running at 3.00GHZ, 8192MB of RAM, and a 7200 RPM Western Digital WD5000AAKS-22V1A0465 GB ATA drive. They showed that the average time for one hash value was 0.605ms. In [15], Lee showed that one hash function operation was about one time faster than one Chebyshev chaotic maps operation. We can draw a conclusion that the average time for one Chebyshev chaotic maps operation was about 1.21ms. In addition, according to [16], we can come to a conclusion that one hash function operation is about 10 times faster than a symmetric encryption/decryption. So a symmetric encryption/decryption operation was about 6.05ms. Moreover, the computational cost of XOR operation could be ignored when compared with other operations.
So we have $1T_S \approx 10T_H, 1T_{CH} \approx 2T_H$. Then we have:

$$\begin{aligned}
&Total_{time-difference} = Total_{\text{computations of [10]}} - Total_{\text{computations of our protocol}} \\
&=N(11T_{CH} + 5T_S - 14T_H) - 10T_{CH} - 2T_S + 8T_H \\
&\approx N(22T_H + 50T_H - 14T_H) - 20T_H - 20T_H + 8T_H \\
&= (58N - 32)T_H
\end{aligned}$$

That means our proposed scheme (even if N = 1) has much more efficient than the literature [10]. With the N increases linearly, our proposed schemes cost of computation will

decrease linearly comparing with the literature of [10]. As for store space, our proposed scheme just need 62.5K (assume $p_t = 128bits$, and $N = 500$).It is can be ignored at present contrasting to the TeraBit storage.
Table 3 compares the functionalities and system efficiency of our proposed protocol and other, related coupon schemes [10-14]. The results of the comparisons show that our proposed scheme provides more functionalities, and is more suit for user-friendliness system.

TABLE 3. Comparisons between the related protocols and our proposed protocol

	[10] (2014)	**[11] (2007)**	**[12] (2007)**	**[13] (2008)**	**[14] (2013)**	**Our scheme**
System completeness	√√√	√	√	√	√	√√√
Digital signature	PKI-based	PKI-based	PKI-based	N/A	N/A	PKI-based
	√√	×	√√	×	×	√√
Efficiency	CMs-based	Exp-based	Exp-based	Hash-based	XOR-based	Chain-based
	√√	√	√√	√√√	√√√√	√√√
Communi cationrounds						
Reg	2	4	4	2	2	3
Auth	3	5	4	2	2	3
Privacy protection	√√	×	×	×	√	√√√√
×:Weak;√:Ordinary;√√:Good;√√√:Very Good;√√√√:Excellent N/A not applicable,Exp exponential, XOR exclusiveOR,CMs chaotic maps, Reg registration,Auth authentication						

6. **Conclusion.** The paper proposed a novel and complete biometrics-based and one-time identity-password authentication scheme for e-coupon systems. There are many advantages about our protocol which described as follow: Firstly, from the standpoint of a security analysis, our scheme uses biometrics method and dynamic ID-password to achieve high-level security. Then, along with one-time password, we insert the dynamic ID which can consume the almost negligible computations, communications and size of memory. It is efficient method at least cost. Next, the core ideas of the proposed scheme are the features of security and efficiency in the mobile device and servers side, and the feature of user friendly for the users side. Finally, through comparing with recently related work, our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications.

REFERENCES

[1] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.
[2] S. H. Tang, Directed one-time password authentication scheme based upon discrete logarithm, *Journal of Circuits, Systems and Compute*, vol. 10, no. 3, pp. 173-180, 2000.
[3] K. G. Paterson, G. Kenneth and D. Stebila, One-time-password-authenticated key exchange, *Information Security and Privacy: Proceedings of 15th Australasian Conference*, pp. 264-281, 2010.
[4] K. Fuglerud and O. Dale, Secure and inclusive authentication with a talking mobile one-time-password client,*Security and Privacy, IEEE*, vol.9, no. 2, pp. 27-34, 2011.

[5] C. T. Li and M. S. Hwang, A lightweight anonymous routing protocol without public key en/decryptions for wireless Ad Hoc networks, *Information Sciences*, vol. 181, no. 23, pp. 5333-5347, 2011.

[6] R. Mohan and N. Partheeban, Secure multimodal mobile authentication using one time password,*Informational Journal of Recent Technology and Engineering*, vol. 1, no. 1, pp. 131-136, 2012.

[7] Y. Huang, Z. Huang, H.R. Zhao and X.J. Lai, A new one-time password method. *Informational Conference on Electronic Engineering and Computer Science*, pp 32-37, 2013.

[8] F. Xu, X. Lv, Q. Zhou and X. Liu, Self-updating one-time password authentication protocol for ad hoc network,*Transactions on Internet and Information Systems*, vol. 8, no. 5, pp. 1817-1827, 2014.

[9] C. T. Li, M. S. Hwang , An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

[10] C. C. Chang, C. Y. Sun, A Secure and Efficient Authentication Scheme for E-coupon Systems. *Wireless Personal Communications*, vol. 77, no. 4, pp: 2981-2996, 2014.

[11] M. Aigner, S. Dominikus, and M. Feldhofer, A system of secure virtial coupons using NFC technology, *InProceedings of IEEE International Conference on Pervasive Computing and Communication Workshops*,New York, U.S.A, pp. 362366, 2007.

[12] S. Dominikus, and M. Aigner, mCoupons: An application for near field communication (NFC), *In-Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshop*,Ontario, Canada, pp. 421428, 2007.

[13] H. C. Hsiang, and W. K. Shih, Secure mCoupons scheme using NFC,*Proceedings of the International Conference on Business and Information*,Seoul, Korea, 2008.

[14] S. W. Park, and I. Y. Lee, Efficient mCoupon authentication scheme for smart poster environments based on low-cost NFC,*International Journal of Security and its Applications*, vol. 7, no. 5, pp. 131138, 2013.

[15] B. Schneier,*Applied cryptography, protocols, algorithms, and source code in C* (2nd ed.)New York, USA: Wiley, 1996.

[16] C. C. Lee, A simple key agreement scheme based on chaotic maps for VSAT satellite communications,*International Journal of Satellite Communications and Networking*,Published online: 21 June 2013.

[17] J. Katz, and S. J. Shin, Modeling insider attacks on group key-exchange protocols, In: *Proceedings of the 12th ACM Conference on Computer and Communications SecurityCCS05, ACM*, pp. 180189, 2005.

[18] L. H. Li , I. C. Lin , and M. S. Hwang, A remote password authentication scheme for multi-server architecture using neural networks,*IEEE Transactions on Neural Networks*, vol. 12, no. 6, pp. 14981504, 2001.

[19] I. C. Lin, M. S. Hwang, and L. H. Li, A new remote user authentication scheme for multi-server architecture,*Future Generation Computer Systems*, vol. 19, no. 1, pp. 1322, 2003.

[20] B. Wang, M. Ma, A smart card based efficient and secured multi-server authentication scheme,*Wireless Personal Communications*, vol. 68, no. 2, pp. 361-378, 2013.