A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards

Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami

***Abstract*— Recently, in 2014, He and Wang proposed a robust and efficient multi-server authentication scheme using biometrics-based smart card and elliptic curve cryptography (ECC). In this paper, we first analyze He–Wang's scheme and show that their scheme is vulnerable to a known session-specific temporary information attack and impersonation attack. In addition, we show that their scheme does not provide strong user's anonymity. Furthermore, He–Wang's scheme cannot provide the user revocation facility when the smart card is lost/stolen or user's authentication parameter is revealed. Apart from these, He–Wang's scheme has some design flaws, such as wrong password login and its consequences, and wrong password update during password change phase. We then propose a new secure multi-server authentication protocol using biometric-based smart card and ECC with more security functionalities. Using the Burrows–Abadi–Needham logic, we show that our scheme provides secure authentication. In addition, we simulate our scheme for the formal security verification using the widely accepted and used automated validation of Internet security protocols and applications tool, and show that our scheme is secure against passive and active attacks. Our scheme provides high security along with low communication cost, computational cost, and variety of security features. As a result, our scheme is very suitable for battery-limited mobile devices as compared with He–Wang's scheme.**

***Index Terms*— Security, authentication, smart card, revocation and re-registration, BAN logic, AVISPA.**

I. INTRODUCTION

WITH the rapid development of the wireless communication networks and e-commerce applications, such as e-banking and transaction-oriented services [1], there is a growing demand to protect the user credentials privacy. In the recent couple of decades, more and more transactions for the mobile devices have been implemented on the Internet or wireless networks due to the portability property of mobile devices, such as laptops, smart cards and smart phones [2]. Thus, the authentication protocols become the trusted components in a communication system. In order to protect the sensitive information against a malicious adversary, a variety of security services such as mutual authentication, user credentials privacy and SK-security need to be considered [3], [4]. We also consider the following two real-life scenarios for the smart card based authentication schemes in which the registered users may revoke and re-register with the same identity [5]–[8]: (i) when unexpectedly the secret token of a legal user is revealed and (ii) if the smart card of a legal user is stolen or lost. Hence, the authentication schemes must support the user revocation and re-registration with the same identity. The user revocation and re-registration with the same identity may cause the user impersonation attack, when an authentication scheme distributes the static secret tokens. Therefore, designing an efficient approach to tackle the problem of user revocation while supporting a strong user untraceability becomes a challenging problem [9]–[11]. As a result, the user revocation and re-registration with the same identity is identified as a fundamental security functionality for the smart card-based authentication schemes.

A. Security Requirements of Authentication Schemes

According to [3], [4], and [12], in the basic adversarial model, a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ can have a full control over all the authentic messages. Hence, the adversary $\mathcal{A}$ can read, modify or delete all the authentic messages transmitted between users and server. In addition, $\mathcal{A}$ can have access to the secret information via the session exposure attacks. Thus, an authentication scheme should satisfy the following security properties.

1) **SK-security:** An authentication scheme should guarantee the security of the session key, called the session key security (SK-security), in the following two cases:
   (i) The leakage of a session key or session-specific temporary information will have no effects on the security of other sessions.
   (ii) The leakage of the crucial long-term secrets, such as the private keys of users or servers, which are used across the multiple sessions, will not necessarily compromise the secret information from all past sessions, known as the perfect forward secrecy.
2) **User credentials privacy:** It ensures that $\mathcal{A}$ cannot derive a user credentials, such as authentication parameter, user password and identity.
3) **Secure mutual authentication:** It ensures that an authentication scheme must provide the secure mutual authentication with the presence of the shared secret credentials.

Manuscript received November 17, 2014; revised March 4, 2015 and May 22, 2015; accepted May 26, 2015. Date of publication June 1, 2015; date of current version July 22, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Shantanu D. Rane.

V. Odelu and A. Goswami are with the Department of Mathematics, IIT Kharagpur, Kharagpur 721302, India (e-mail: odelu.phd@maths.iitkgp.ernet.in; goswami@maths.iitkgp.ernet.in).

A. K. Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: iitkgp.akdas@gmail.com; ashok.das@iiit.ac.in).

This paper has supplementary downloadable material at http://ieeexplore.ieee.org, provided by the authors. The material is 139.7 KB in size.

Digital Object Identifier 10.1109/TIFS.2015.2439964

B. Related Work

After conception of Lamport's seminal authentication scheme in 1981 [13], several two-party authentication schemes have been proposed in the literature (for example, [1], [6]–[11]). In a single-server environment, a user needs to register with each server separately. However, it is impossible to directly apply two-party authentication methods devised for a single server environment to a multi-server environment. To handle this problem, several multi-server authentication schemes (for example [14]–[19]) have been proposed in the literature. Yoon and Yoo [20] proposed a multi-server authentication scheme using the biometrics-based smart card and ECC. However, Kim et al. [21] pointed out that if the smart card is lost, Yoon-Yoo's scheme cannot prevent the offline password guessing attack. Further, they proposed an enhanced scheme in order to withstand the security flaw found in Yoon-Yoo's scheme. Later, He [22] proved that Yoon-Yoo's scheme is insecure against the privileged insider attack and impersonation attack. He [22] showed that their proposed attacks are also valid for Kim et al.'s scheme. Recently, He and Wang [23] proposed a robust biometrics-based authentication scheme for multi-server environment in order to withstand these security issues, and claimed that their scheme is secure against all possible known attacks. However, in this paper, we show that He-Wang's scheme fails to prevent known session temporary information attack, and as a result, their scheme cannot prevent the reply attack and impersonation attack. In addition, we show that their scheme cannot provide the strong user anonymity.

With the rapid progress in the biometric technology, the market share is increasingly shifting towards the biometric techniques [24]. The biometrics-based authentication systems are designed to withstand attacks when employed in security-critical e-commerce applications such as e-banking and transaction-oriented services [25]. Recent study shows that the elliptic curve cryptography (ECC) is suitable for the battery-limited devices [26]. In this paper, we propose a novel and secure biometrics-based multi-server authentication mechanism using ECC for the battery-limited devices.

C. Our Contributions

Our contributions in this paper are outlined below.

- In our scheme, a session key is only available to the communicating parties (user and server), and it is unknown to either the registration center or others.
- Our scheme provides user credentials privacy even if the session-specific temporary information are unexpectedly leaked. But most of the existing schemes do not provide credentials privacy including the recently proposed He-Wang's scheme.
- Our scheme provides the SK-security, whereas He-Wang's scheme has several drawbacks when the session temporary information are leaked to the adversary.
- Our scheme efficiently supports the password change phase. However, He-Wang's scheme has some design flaws, such as wrong password login and its consequences, and wrong password update during password change phase.
- In our scheme, the registration center (RC) authenticates the user and server separately whenever they want to establish the session key. On the other hand, in He-Wang's scheme, the RC cannot identify the user and the server separately. Thus, in He-Wang's scheme, a legal malicious server may act as a legal user and enjoy the services from the other servers.
- Our scheme efficiently supports the basic security property of the revocation and re-registration with the same identity due to the usage of random number in computation of authentication parameter of a legal user. On the other hand, most of the existing schemes do not support revocation and re-registration with the same identity including He-Wang's scheme.
- In our scheme, the registration center RC stores the user identity information to avoid many users to register with the same identity and thus, our scheme prevents the many logged-in users attack.
- Our scheme provides high security along with a variety of features as compared to He-Wang's scheme. Therefore, our scheme is very suitable for the battery-limited mobile devices as the ECC is more efficient for the battery-limited devices.

D. Threat Model

We assume that an adversary can retrieve the sensitive information stored in the smart-card memory using the power analysis attacks [27], [28]. Furthermore, we use the Dolev-Yao threat model [29], in which the two communicating parties communicate over an insecure public channel. We use the similar threat model for our scheme where the communicating channels are insecure and the end-points cannot in general be trustworthy.

E. Organization of the Paper

The rest of the paper is organized as follows. In Section II, we briefly discuss some mathematical preliminaries to review and analyze He-Wang's scheme [23] and our proposed scheme. We then review the recently proposed He-Wang's scheme in Section III. In Section IV, we show that He-Wang's scheme is vulnerable to various attacks. We also point out some design flaws of He-Wang's scheme in this section. In Section V, we present a novel and secure biometrics-based efficient multi-server authentication scheme using smart cards in order to withstand the flaws found in He-Wang's scheme. We analyze the security of our scheme through the rigorous informal and formal security analysis and verification in Section VI. In Section VII, we compare the performance and security of our scheme with He-Wang's scheme. Finally, we conclude the paper in Section VIII.

II. MATHEMATICAL PRELIMINARIES

In this section, we briefly discuss the mathematical preliminaries to review and analyze He-Wang's scheme [23].

A. Elliptic Curve Over a Prime Field $GF(p)$

A non-singular elliptic curve $y^2 = x^3+ax+b$ over the finite field $GF(p)$ is the set E_p of all the solutions $(x, y) \in Z_p \times Z_p$ to the congruence $y^2 = x^3+ax+b \pmod p$, where $a, b \in Z_p$ are constants such that $4a^3+27b^2 \neq 0 \pmod p$, together with a special point $\mathcal{O}$ called the point at infinity or zero point, $Z_p = \{0, 1, \ldots, p-1\}$ and $p > 3$ be a prime. The set of elliptic curve points, E_p forms an abelian group under addition modulo p operation [30].

Let G be a base point on E_p, whose order be n, that is, $nG = G + G + \ldots + G (n \text{ times}) = \mathcal{O}$. Assume that $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are two points on elliptic curve $y^2 = x^3+ax+b \pmod p$. Then $R = (x_R, y_R) = P+Q$ is computed as follows [30]:

$$x_R = (\delta^2 - x_P - x_Q)(\text{mod}\, p),$$
$$y_R = (\delta(x_P - x_R) - y_P)(\text{mod}\, p),$$

where

$$\delta = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} (\text{mod}\, p), & \text{if } P \neq Q \\ \dfrac{3{x_P}^2 + a}{2y_P} (\text{mod}\, p), & \text{if } P = Q. \end{cases}$$

In elliptic curve cryptography, the scalar multiplication is defined as the repeated additions. For example, if $P \in E_p$, then $4P$ is computed as $4P = P + P + P + P$.

Definition 1 [Elliptic Curve Discrete Logarithm Problem (ECDLP)]: Computing $Q = kP$ is relatively easy for given $k \in Z_p$ and $P \in E_p$. However, given $P \in E_p$ and $Q \in E_p$, it is computationally hard to compute the scalar k such that $Q = kP$.

Definition 2 [Computational Diffie-Hellman Problem (CDHP)]: Given $P, xP, yP \in E_p$, it is computationally hard to compute $xyP \in E_p$ without the knowledge of $x \in Z_p^*$ or $y \in Z_p^*$, where $Z_p^* = \{a | 0 < a < p, \gcd(a, p) = 1\} = \{1, 2, 3, \ldots, p-1\}$.

Definition 3 (Collision-Resistant One-Way Hash Function): A collision-resistant one-way hash function $H : X \to Y$, where $X = \{0, 1\}^*$ and $Y = \{0, 1\}^n$, is considered as a deterministic algorithm that takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$, and outputs a binary string $y \in \{0, 1\}^n$ of fixed-length n [31], [32]. If $Adv_{\mathcal{A}}^{HASH}(t)$ is an adversary (attacker) $\mathcal{A}$'s advantage in finding collision, we then have

$$Adv_{\mathcal{A}}^{HASH}(t) = Pr[(x, x') \Leftarrow_R \mathcal{A} : x \neq x', H(x) = H(x')],$$

where $Pr[E]$ denotes the probability of a random event E, and $(x, x') \Leftarrow_R \mathcal{A}$ denotes the pair (x, x') is selected randomly by $\mathcal{A}$. In this case, the adversary $\mathcal{A}$ is allowed to be probabilistic and the probability in the advantage is computed over the random choices made by the adversary $\mathcal{A}$ with the execution time t. A hash function $H(\cdot)$ is called collision-resistant, if $Adv_{\mathcal{A}}^{HASH}(t) \leq \epsilon$, for any sufficiently small $\epsilon > 0$.

B. Biometrics and Fuzzy Extractor

A metric space is a set Υ with a distance function $dis : \Upsilon \times \Upsilon \to R^+ = [0, \infty)$ [34]. An example of a metric space is the Hamming metric, $\Upsilon = \Gamma^n$, which is defined over some alphabet Γ^n (for example, $\Gamma = \{0, 1\}$) and $dis(\omega, \omega')$ is the number of positions in which the strings ω and ω' differ. The statistical distance is the distance between two probability distributions A and B defined by $SD(A, B) = \frac{1}{2} \sum_v |Pr[A = v] - Pr[B = v]|$. Further, the min-entropy $H_\infty(A)$ of a random variable A is $-log(max_a Pr[A = a])$.

A fuzzy extractor $(\Upsilon, m, l, t, \epsilon)$ extracts a nearly l-bit random string σ from its biometric characteristic input ω in an error-tolerant way [34], where m is the min-entropy of any distribution W on metric space Υ and t the error tolerance threshold. If an input changes but it remains close to ω, then the extracted σ remains the same. To assist in recovering σ from the biometric characteristic input ω', a fuzzy extractor outputs an auxiliary string θ. However, σ remains uniformly random for a given θ. The fuzzy extractor is given by the following two procedures, called the probabilistic generation procedure (Gen) and the deterministic reproduction procedure (Rep):

- Gen is a probabilistic generation procedure, which on (biometric characteristic) input $\omega \in \Upsilon$, outputs an extracted string $\sigma \in \{0, 1\}^l$ and auxiliary string θ. For any distribution W on metric space Υ of min-entropy m, if $\langle \sigma, \theta \rangle \leftarrow Gen(\omega)$, the statistical distance $SD(\langle \sigma, \theta \rangle, \langle U_l, \theta \rangle) \leq \epsilon$, where U_l denotes the uniform distribution on l-bit binary strings and ϵ is the statistical distance between two given probability distributions $\langle \sigma, \theta \rangle$ and $\langle U_l, \theta \rangle$ with $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$ [34].
- Rep is a deterministic reproduction procedure that allows to recover σ from the corresponding auxiliary string θ and any vector ω' close to ω. For all $\omega, \omega' \in \Upsilon$ satisfying $dis(\omega, \omega') \leq t$, if $\langle \sigma, \theta \rangle \leftarrow Gen(\omega)$, then $Rep(\omega', \theta) = \sigma$.

The fuzzy extractor $(\Upsilon, m, l, t, \epsilon)$ is efficient, if Gen and Rep run in polynomial time in representation size of a point in Υ. $(\Upsilon, m, l, t, \epsilon)$ is secure if it is difficult to recover σ from a closed biometric input ω' with the auxiliary string θ [23].

The uniqueness property of a biometric allows its applications in authentication protocols. As compared to the low-entropy passwords, the biometric keys have more advantages such as biometric keys cannot be lost or forgotten, biometric keys are hard to forge or distribute, biometric keys are difficult to copy or share, and as a result, guessing the biometric keys is a hard problem [24], [35]–[39]. As pointed out in [34], a strong fuzzy extractor $(\Upsilon, m, l, t, \epsilon)$ can extract at most $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$ nearly random bits. Thus, the probability to guess the biometric key data $\sigma \in \{0, 1\}^l$ by an attacker is approximately $\frac{1}{2^l}$, where $l = m - 2\log(\frac{1}{\epsilon}) + O(1)$ [34].

C. Case Study on Biometrics Modality

In this section, we provide a particular case study involving biometric trait based on various parameters. In Table I, a comparison of various biometric technologies is provided based on seven factors [33]. Universality is a factor by which we mean that every person using a system should possess the trait. By uniqueness, we mean the trait should be sufficiently different for individuals in the relevant population such that

TABLE I

COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES BASED ON [33]

Biometric identifier	I_1	I_2	I_3	I_4	I_5	I_6	I_7
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Note: I_1 : Universality; I_2 : Distinctiveness; I_3 : Permanence; I_4 : Collectability; I_5 : Performance; I_6 : Acceptability; I_7 : Circumvention; L : Low; M : Medium; H : High.

they can be distinguished from one another. Permanence is a factor which relates to the manner in which a trait varies over time. Collectability (also called measurability) relates to the ease of acquisition or measurement of the trait. Performance is another factor which relates to the accuracy, speed, and robustness of technology used. Acceptability means how well individuals in the relevant population accept the technology. Finally, circumvention relates to the ease with which a trait might be imitated using an artifact or substitute. As pointed out in [33], the applicability of a specific biometric technique depends heavily on the requirements of the application domain. It is also pointed out that there is no single technique, which can outperform all the others in all operational environments. Each biometric technique is admissible and there is no optimal biometric characteristic. From this table, it is observed that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in some applications such as tele-banking applications, the voice-based technique may be preferred, because it can be integrated seamlessly into the existing telephone system [33].

In a biometric verification system, there are two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person (called false match or false accept) and (ii) mistaking two biometric measurements from the same person to be from two different persons (called false nonmatch or false reject) [33]. Jain et al. [33] reported the state-of-the-art error rates of three popular biometric traits, namely fingerprint, face and voice, which are shown in Table II. Note that accuracy estimates of various biometric systems are dependent on a number of test conditions. They also pointed out that there is plenty of scope for improvement in biometrics. Thus, based on the application and environment, we can choose a biometric trait, which can be very suitable for the battery-limited mobile devices.

III. REVIEW OF HE-WANG'S SCHEME

In this section, we review the recently proposed He-Wang's scheme [23]. For the convenience, in this paper we use the notations listed in Table III.

TABLE II

STATE-OF-THE-ART ERROR RATES ASSOCIATED WITH VARIOUS BIOMETRIC SYSTEMS [33]

	Test	Test parameter	FNMR	FMR
Finger-print	FVC 2002 [40]	Users mostly in the age group 20-39	0.2%	0.2%
Face	FRVT 2002 [41]	Enrollment and test images were collected in indoor environment and could be on different days	10%	1%
Voice	NIST 2000	Test dependent	10-20%	2-5%

Note: FNMR: False nonmatch rate; FMR: False match rate.

TABLE III

NOTATIONS USED IN THIS PAPER

Symbol	Description
RC	The registration center
k	The master secret key of RC
n, p	Two sufficiently large prime number
F_p	A finite field of order p
E_p	A non-singular elliptic curve over a field $GF(p)$
G	The additive group consisting of points on E_p
P	A generator of G with order n
P_{pub}	The public key of RC, where $P_{pub} = kP$
S_j	The j^{th} server
SID_j	Identity of server S_j
k_j	Private key of S_j
U_i	The i^{th} user
ID_i and pw_i	Identity and password of U_i, respectively
k_i	Authentication parameter (secret token) of U_i
SC_i	Smart card of the user U_i
Ω	Symmetric-key cryptography
$E_k(\cdot)/D_k(\cdot)$	Symmetric encryption/decryption using the key k
$H(\cdot)$	A cryptographic hash function
$M_1 \| M_2$	Data M_1 concatenates with data M_2
$M_1 \oplus M_2$	XOR operation of M_1 and M_2
$X \to Y : \langle M \rangle$	X sends message M to Y

Initially, the registration center RC selects a non-singular elliptic curve E_p over a finite field $GF(p)$, a base point $P \in G$, where p is a large prime and G is an additive cyclic group of order n consisting of points on E_p. The RC selects its private key k and computes its public key $P_{pub} = kP$. Note that P is made public by the RC.

A. Registration Phase

This phase consists of the server registration phase and the user registration phase. This phase is summarized in Table IV.

1) Server Registration Phase: In this phase, a server S_j chooses its identity SID_j and sends it to the RC via a secure channel. Upon receiving this request, the RC computes $k_j = H(SID_j||k)$ and then sends it to S_j via a secure channel. After receiving k_j from the RC, S_j keeps it secret.

2) User Registration Phase: In this phase, a user U_i sends a request and obtains the smart-card SC_i with authentication parameter as follows:

Step R1: U_i chooses his/her identity ID_i, password pw_i and imprints his/her personal biometric impression B_i at the sensor. Then U_i computes $(\sigma_i, \theta_i) = Gen(B_i)$ and sends the registration request $Reg = \{ID_i, H(pw_i||\sigma_i)\}$ to RC via a secure channel.

TABLE IV

REGISTRATION PHASE OF HE-WANG'S SCHEME

Server S_j	Registration center RC
$\xrightarrow{\{SID_j\}}$ (via a secure channel)	Computes $k_j = H(SID_j\|\|k)$.
Keeps k_j as secret.	$\xleftarrow{\{k_j\}}$ (via a secure channel)
User U_i	Registration center RC
Inputs ID_i, pw_i, B_i. Computes $(\sigma_i, \theta_i) = Gen(B_i)$. $\xrightarrow{Reg = \{ID_i, H(pw_i\|\|\sigma_i)\}}$ (via a secure channel)	Computes $k_i = H(ID_i\|\|k)$, $z_i = k_i \oplus H(pw_i\|\|\sigma_i)$. Stores z_i into smart card, SC_i. $\xleftarrow{SC_i = \{z_i\}}$ (via a secure channel)
Stores θ_i into SC_i.	

Step R2: After receiving the registration request Reg from U_i, the RC computes $k_i = H(ID_i||k)$, $z_i = k_i \oplus H(pw_i||\sigma_i)$ and stores z_i into a smart-card SC_i. Finally, the RC issues SC_i to U_i face to face (via a secure channel).

Step R3: After receiving SC_i, U_i stores θ_i into its memory.

B. Authentication and Key Establishment Phase

In this phase, U_i and S_j mutually authenticate each other and establish the session key. The login and authentication and key establishment phases of He-Wang's scheme are summarized in Table V.

Step A1: U_i inserts SC_i into a card reader, and inputs pw_i, ID_i and imprints personal biometrics B_i' at the sensor. U_i then generates a random number $x \in Z_n^*$ and computes $Rep(B_i', \theta_i) = \sigma_i$, $k_i = z_i \oplus H(pw_i||\sigma_i)$, $X = xP$, $K_1 = xP_{pub}$, $CID_i = ID_i \oplus H(K_1)$, and $h_1 = H(ID_i||SID_j||k_i||X||K_1)$. Finally, U_i sends the message $M_1 = \{CID_i, X, h_1\}$ to S_j via a public channel.

Step A2: After receiving the message M_1, S_j randomly chooses $y \in Z_n^*$ and computes $Y = yP$, $K_2 = yP_{pub}$, $h_2 = H(CID_i||X||h_1||SID_j||k_j||Y||K_2)$, and $CSID_j = SID_j \oplus H(K_2)$. Finally, S_j sends the message $M_2 = \{CID_i, X, h_1, CSID_j, Y, h_2\}$ to the RC via a public channel.

Step A3: Upon receiving M_2 from S_j, RC computes $K_3 = kY (= K_2)$, $SID_j = CSID_j \oplus H(K_2)$, and $k_j = H(SID_j||k)$. Then RC checks whether $h_2 = H(CID_i||X||h_1||SID_j||k_j||Y||K_3)$ holds or not. If it does not hold, the RC terminates the session. Otherwise, RC computes $K_4 = kX (= K_1)$, $ID_i = CID_i \oplus H(K_4)$, and $k_i = H(ID_i||k)$. RC then checks whether $h_1 = H(ID_i||SID_j||k_i||X||K_4)$ holds or not. If it does not hold, it terminates the session. Otherwise, RC computes $TID_i = ID_i \oplus H(Y||K_3||k_j)$, $h_3 = H(ID_i||TID_i||X||SID_j||Y||k_j)$, $TSID_j = SID_j \oplus H(X||K_4||k_i)$, and $h_4 = H(ID_i||X||K_4||SID_j||Y||k_i)$. Finally, RC sends the message $M_3 = \{TID_i, h_3, TSID_j, h_4\}$ to S_j via a public channel.

Step A4: After receiving M_3 from RC, S_j computes $ID_i = TID_i \oplus H(Y||K_2||k_j)$ and checks whether ID_i is valid or not. If it is not valid, S_j terminates the session. Otherwise, S_j checks whether the condition $h_3 = H(ID_i||TID_i||X||SID_j||Y||k_j)$ holds or not. If it does not hold, S_j terminates the session. Otherwise, S_j computes the session key $SK = yX = xyP$ and $h_5 = H(ID_i||SID_j||X||Y||SK||h_4)$. Finally, S_j sends $M_4 = \{TSID_j, Y, h_4, h_5\}$ to U_i via a public channel.

Step A5: Upon receiving M_4 from S_j, U_i computes $SID_j = TSID_j \oplus H(X||K_1||k_i)$ and then checks whether $h_4 = H(ID_i||X||K_4||SID_j||Y||k_i)$ holds or not. If it does not hold, U_i stops the session. Otherwise, U_i computes the session key $SK = xY = xyP$, and checks whether $h_5 = H(ID_i||SID_j||X||Y||SK||h_4)$ holds or not. If it does not hold, U_i terminates the session. Otherwise, U_i computes $h_6 = H(SID_j||ID_i||X||Y||SK||h_4)$ and sends $M_5 = \{h_6\}$ to S_j via a public channel.

Step A6: After receiving M_5 from U_i, S_j checks whether the condition $h_6 = H(SID_j||ID_i||X||Y||SK||h_4)$ holds or not. If it holds true, S_j confirms that U_i is legitimate. Otherwise, S_j stops the session immediately.

C. Password Change Phase

In this phase, U_i changes his/her password as follows:

Step P1: U_i inserts SC_i into a card reader and inputs pw_i, ID_i and imprints personal biometrics B_i' at the sensor. U_i also inputs the new password pw_i^{new}.

Step P2: SC_i then computes $Rep(B_i', \theta_i) = \sigma_i$, $k_i = z_i \oplus H(pw_i||\sigma_i)$, and $z_i^{new} = k_i \oplus H(pw_i^{new}||\sigma_i)$. Finally, SC_i replaces z_i with z_i^{new}.

IV. CRYPTANALYSIS ON HE-WANG'S SCHEME

In this section, we show that He-Wang's scheme [23] is vulnerable to various well-known attacks, which are outlined in the following subsections.

A. Known Session-Specific Temporary Information Attack

Assume that the session random number x chosen by U_i is unexpectedly revealed to the PPT adversary $\mathcal{A}$. Then, He-Wang's scheme has the following drawback:

- Since U_i and S_j compute a session key SK as $SK = xY = xyP$, $\mathcal{A}$ can compute the session key SK using known session random number x.
- $\mathcal{A}$ intercepts the message $M_1 = \{CID_i, X, h_1\}$ sent to the server S_j (in Step A1 of the authentication and key establishment phase), and checks whether xP matches with X. If it matches, $\mathcal{A}$ confirms that x corresponds to M_1 and computes K_1 and ID_i as $K_1 = xP_{pub}$ and $ID_i = CID_i \oplus H(K_1)$ (this may cause user anonymity violation). The adversary $\mathcal{A}$ sends reply message M_1 to S_j without any modifications. In this case, neither S_j nor RC can identify the message M_1 as a replied one. From the message $M_4 = \{TSID_j, Y, h_4, h_5\}$, the adversary $\mathcal{A}$ knows Y and h_4, and he/she can compute SK as $SK = xY$ using x and then compute the valid $h_6 = H(SID_j||ID_i||X||Y||SK||h_4)$ for S_j without knowledge of U_i's authentication parameter k_i. As a result, $\mathcal{A}$ can successfully impersonate the legal user U_i.

TABLE V

LOGIN, AND AUTHENTICATION AND KEY ESTABLISHMENT PHASES OF HE-WANG'S SCHEME

User U_i	Server S_j	Registration center RC
Inputs ID_i, pw_i, B_i' into SC_i. Chooses a random $x \in Z_n^*$. Computes $\sigma_i = Rep(B_i', \theta_i)$, $k_i = z_i \oplus H(pw_i\|\|\sigma_i)$, $X = xP$, $K_1 = xP_{pub}$, $CID_i = ID_i \oplus H(K_1)$, $h_1 = H(ID_i\|\|SID_j\|\|k_i\|\|X\|\|K_1)$. $\xrightarrow{M_1 = \{CID_i, X, h_1\}}$ (via a public channel)		
	Chooses a random $y \in Z_n^*$. Computes $Y = yP$, $K_2 = yP_{pub}$, $h_2 = H(CID_i\|\|X\|\|h_1\|\|SID_j\|\|k_j\|\|Y\|\|K_2)$, $CSID_j = SID_j \oplus H(K_2)$. $\xrightarrow{M_2 = \{CID_i, X, h_1, CSID_j, Y, h_2\}}$ (via a public channel)	
		Computes $K_3 = kY\ (= K_2)$, $SID_j = CSID_j \oplus H(K_2)$, $k_j = H(SID_j\ \|\|k)$. Checks $h_2 =^?$ $H(CID_i\|\|X\|\|h_1\|\|SID_j\|\|k_j\|\|Y\|\|K_3)$. accept/reject? Computes $K_4 = kX\ (= K_1)$, $ID_i = CID_i \oplus H(K_4)$, $k_i = H(ID_i\|\|k)$. Checks $h_1 =^? H(ID_i\|\|SID_j\|\|k_i\|\|X\|\|K_4)$. accept/reject? Computes $TID_i = ID_i \oplus H(Y\|\|K_3\|\|k_j)$, $h_3 = H(ID_i\|\|TID_i\|\|X\|\|SID_j\|\|Y\|\|k_j)$, $TSID_j = SID_j \oplus H(X\|\|K_4\|\|k_i)$, $h_4 = H(ID_i\|\|X\|\|K_4\|\|SID_j\|\|Y\|\|k_i)$. $\xleftarrow{M_3 = \{TID_i, h_3, TSID_j, h_4\}}$ (via a public channel)
	Computes $ID_i = TID_i \oplus H(Y\|\|K_2\|\|k_j)$. Checks the validity of ID_i. accept/reject? Checks $h_3 =^? H(ID_i\|\|TID_i\|\|X\|\|SID_j\|\|Y\|\|k_j)$. accept/reject? Computes the session key $SK = yX = xyP$, $h_5 = H(ID_i\|\|SID_j\|\|X\|\|Y\|\|SK\|\|h_4)$. $\xleftarrow{M_4 = \{TSID_j, Y, h_4, h_5\}}$ (via a public channel)	
Computes $SID_j = TSID_j \oplus H(X\|\|K_1\|\|k_i)$. Checks $h_4 =^? H(ID_i\|\|X\|\|K_4\|\|SID_j\|\|Y\|\|k_i)$. accept/reject? Computes the session key $SK = xY = xyP$. Checks $h_5 =^? H(ID_i\|\|SID_j\|\|X\|\|Y\|\|SK\|\|h_4)$. accept/reject? Computes $h_6 = H(SID_j\|\|ID_i\|\|X\|\|Y\|\|SK\|\|h_4)$. $\xrightarrow{M_5 = \{h_6\}}$ (via a public channel)		
	Checks $h_6 =^? H(SID_j\|\|ID_i\|\|X\|\|Y\|\|SK\|\|h_4)$. accept/reject?	

- One more drawback is that the RC cannot identify the user U_i and the server S_j separately when they want to establish the session key. In this case, a legal server S_j may act as legal user [42] and enjoy the services from the other servers S_l's.

As a result, He-Wang's scheme cannot provide strongly the SK-security. The SK-security is very essential in the security-critical applications.

B. Impersonation Attack

In He-Wang's scheme [23], during the registration phase of a user U_i, the registration center RC computes the authentication parameter k_i of U_i using the identity ID_i of U_i and secret key k of RC as $k_i = H(ID_i||k)$. Clearly, the authentication parameter is static and the registration phase has no ability to detect re-registration with the old identity. Thus, the user U_i can not re-register with the same identity ID_i in future for the following two genuine cases:

- when U_i's smart-card SC_i is lost/stolen, and
- unexpectedly U_i's authentication parameter k_i is revealed.

Hence, the PPT adversary $\mathcal{A}$ can easily obtain the authentication parameter by performing re-registration with the legal user U_i's identity ID_i because the RC does not maintain any user identity information table. Moreover, the servers' authentication parameters are also static and the RC does not maintain any identity information of the servers. Therefore, the second case is also applicable to the servers. As a result, $\mathcal{A}$ can obtain the authentication parameter of a legal user (or a server), and then successfully impersonate the user (or a server). Moreover, the server is a semi-trusted party and He-Wang's authentication scheme cannot protect the user's identity from the server. It also causes the user's anonymity violation. As a result, He-Wang's scheme fails to protect user impersonation attack.

C. Wrong Password Login and Its Consequences

According to Khan and Kumari [10], during the authentication and key establishment phase if a legal user U_i enters his/her wrong password, the authentication test will fail and then it causes denial of service to the legal user U_i. In the login phase of He-Wang's scheme [23], the smart cart SC_i sends the message M_1 without verifying the correctness of the user U_i's credentials ID_i, pw_i and biometrics B_i'. Even if U_i mistakenly enters his/her wrong password, say

$pw_i'(pw_i' \neq pw_i)$, then SC_i still computes $k_i' = z_i \oplus H(pw_i'||\sigma_i)$ instead of $k_i = z_i \oplus H(pw_i||\sigma_i)$. In this case, U_i will send a wrong login request message M_1' instead of valid message M_1. Thus, the authentication test fails and as a result, He-Wang's scheme [23] falls under the denial-of-service (DoS) to the legal user U_i, which must not happen in sensitive applications. Moreover, an adversary can create denial of service problem by keep on sending the login request message using the legal user U_i's smart-card SC_i and wrong credentials.

D. Drawback in Password Change Phase

In the password change phase of He-Wang's scheme [23], a legal user U_i inputs ID_i, old password pw_i^{old}, biometrics B_i^* and new password pw_i^{new} into the smart card SC_i. As discussed in Section IV-C, even if U_i enters his/her wrong password pw_i' instead of old correct password $pw_i^{old}(pw_i' \neq pw_i^{old})$, SC_i still computes $k_i' = z_i \oplus H(pw_i'||\sigma_i)$ and updates z_i with $z_i' = k_i' \oplus H(pw_i^{new}||\sigma_i)$, where $k_i' \neq k_i$, using the wrong computed k_i' without verifying the validity of old password pw_i^{old}. After updating SC_i with wrong password entry, U_i will never pass the authentication test and the repetition of authentication may cause prolonged/permanent failures to login. As a result, the wrong password update may also cause the denial-of-service to the legal users in such a specific case.

E. No Provision for Revocation and Re-Registration

In order to provide the strong security to the user, revocation of lost/stolen smart-card is one of the fundamental security requirement of smart-card based authentication schemes. If a legal user U_i's smart-card SC_i is lost or stolen, there must be some mechanism to prevent the misuse of lost/stolen smart-card SC_i. Otherwise, an adversary $\mathcal{A}$ can impersonate the legal user U_i as the registration phase has no ability to detect the re-registration with old identity. To cope with this problem, the smart-card based authentication schemes need to store the identity information table in the RC's database, based on which the invalid smart-card will be detected [5]. However, most of the existing multi-server authentication schemes including He-Wang's scheme do not consider the fundamental security feature for revocation and re-registration in their schemes in the multi-server environment.

V. THE PROPOSED SCHEME

In this section, we propose a new biometrics-based multi-server authentication protocol using smart card and ECC, which withstands the security pitfalls of He-Wang's scheme (discussed in Section IV). Our scheme consists of the six phases, namely, initialization phase, registration phase, login phase, authentication and key agreement phase, password change phase, and revocation and re-registration phase.

A. Initialization Phase

In this phase, the registration center RC selects a non-singular elliptic curve E_p over a finite filed $GF(p)$, a base point $P \in G$, where p is a large prime and G is an additive cyclic group of order n consisting of points on E_p, a secure collision-resistant one-way hash function $H(\cdot)$, and a symmetric-key cryptosystem Ω. Also, the RC chooses its private key k which is assumed to be 2048-bit, and then computes its public key P_{pub} as $P_{pub} = kP$. Finally, the RC declares its public parameters $\{p, E_p, P, P_{pub}, n, H(\cdot), \Omega\}$.

TABLE VI

REGISTRATION PHASE OF OUR SCHEME

Server S_j	Registration center RC
$\xrightarrow{\{SID_j\}}$	Checks SID_j. Generates r_j.
(via a secure channel)	Computes $k_j = H(SID_j\|\|k\|\|r_j)$, Computes signature s_j as $s_j = H(k\|\|r_j\|\|k_j\ \|\|SID_j)$. Stores $\{H(SID_j\|\|k), r_j\}$ into $\mathcal{T}$.
Keeps k_j as secret.	$\xleftarrow{\{k_j, s_j\}}$
Declares $\{SID_j, s_j\}$ as public.	(via a secure channel)
User U_i	Registration center RC
Inputs ID_i, pw_i, B_i into SC_i.	
Computes $(\sigma_i, \theta_i) = Gen(B_i)$.	Checks Reg. Generates r_i.
$\xrightarrow{Reg = \{ID_i, H(pw_i\|\|\sigma_i)\}}$	Computes $k_i = H(ID_i\|\|k\|\|r_i\|\|$
(via a secure channel)	$H(ID_i\|\|k))$, $z_i = k_i \oplus H(pw_i\|\|\sigma_i)$, $s_i = H(k_i\|\|ID_i\|\|H(pw_i\|\|\sigma_i))$. Stores $\{H(ID_i\|\|k), r_i\}$ into $\mathcal{T}$.
	$\xleftarrow{\{z_i, s_i\}}$
Stores $\{z_i, s_i, \theta_i\}$ into SC_i.	(via a secure channel)

B. Registration Phase

In order to avoid a new user registration with the existing legal user identity, we use an identity verifier table, say $\mathcal{T}$ in our scheme. The registration phase of our scheme is summarized in Table VI.

1) Server Registration Phase: In this phase, a server S_j chooses his/her unique identity SID_j and sends the registration request $\{SID_j\}$ to RC via a secure channel. After receiving this request, RC checks whether the hash value $H(SID_j||k)$ matches with any one of the entries in the identity-verifier table $\mathcal{T}$. If it matches, RC rejects the request by declaring it as invalid. Otherwise, RC randomly generates a number r_j and computes $k_j = H(SID_j||k||r_j)$. RC also computes the signature s_j on SID_j corresponding to r_j as $s_j = H(k||r_j||k_j||SID_j)$ and stores $\{H(SID_j||k), r_j\}$ into its identity-verifier table $\mathcal{T}$. Finally, RC sends $\{k_j, s_j\}$ to S_j via a secure channel. After receiving $\{k_j, s_j\}$ from RC, S_j keeps k_j as secret and declares the information $\{SID_j, s_j\}$, which are publicly available to all the legal users.

2) User Registration Phase: Assume that the smart card has been pre-configured with public parameters $\{p, E_p, P, P_{pub}, n, \Omega, H(\cdot)\}$ before given to a user U_i and a built-in fingerprint scan component is embedded into the card reader. A user U_i sends a request and obtains the smart-card, say SC_i, and then registers to RC using the following steps:

Step R1: U_i first inserts the received smart card SC_i into the card reader, inputs his/her unique identity ID_i, chosen password pw_i and imprints the personal biometrics B_i at the sensor. Then U_i computes $(\sigma_i, \theta_i) = Gen(B_i)$ and sends the registration request $Reg = \{ID_i, H(pw_i||\sigma_i)\}$ to the registration center RC via a secure channel.

Step R2: Upon receiving the request message Reg, RC checks whether the hash value $H(ID_i||k)$ matches with any existing entry in the identity-verifier table $\mathcal{T}$. If it matches, RC rejects the request by declaring it as invalid. Otherwise, RC generates a random number r_i and computes $k_i = H(ID_i||k||r_i||H(ID_i||k))$, $z_i = k_i \oplus H(pw_i||\sigma_i)$ and $s_i = H(k_i||ID_i||H(pw_i||\sigma_i))$. Further, RC updates its identity-verifier table $\mathcal{T}$ with the new entry $\{H(ID_i||k), r_i\}$. Finally, RC sends $\{z_i, s_i\}$ to U_i via a secure channel.

Step R3: After receiving $\{z_i, s_i\}$ from RC, U_i stores $\{z_i, s_i, \theta_i\}$ into the smart card SC_i.

Remark 1: In order to avoid the many-logged-in-user attack, one can use the table entry for a user U_i *as* $\{H(ID_i||k), r_i, status\}$, *where* $status \in \{-1, 0, 1\}$ *and* $status = 0$ *if the user is active and not logged-in;* $status = 1$ *if the user is active and logged-in; and* $status = -1$ *if the user is inactive. The status inactive is used when the user is revoked his/her account for some security reasons.*

C. Login Phase

In order to login to a server S_j, the user U_i needs to execute the following steps:

Step L1: U_i inserts his/her smart card SC_i into a card reader and inputs pw_i', ID_i' and imprints the personal biometrics B_i' at the sensor. Then, SC_i computes $\sigma_i' = Rep(B_i', \theta_i)$ and $k_i' = z_i' \oplus H(pw_i'||\sigma_i')$ and checks whether $H(k_i'||ID_i'||H(pw_i'||\sigma_i'))$ matches with s_i stored in the smart card SC_i. If it does not match, SC_i rejects the entered credentials and terminates the session.

Step L2: SC_i then randomly chooses a one-time secret $x_i \in Z_n^*$ and a random nonce n_1. In order to avoid the known session-specific temporary information attack, SC_i computes $X = xP$, $K_1 = xP_{pub}$ using $x = H(x_i||k_i||n_1)$ instead of directly using the session random number x_i. Further, SC_i computes $C_1 = E_{K_{1x}}[ID_i, SID_j, s_j, n_1]$, and $h_1 = H(ID_i||SID_j||s_j||n_1||k_i||X||K_1)$, where K_{1x} represents the x-coordinate of the ECC point K_1. Finally, U_i sends the message $M_1 = \{C_1, X, h_1\}$ to the server S_j via a public channel.

D. Authentication and Key Establishment Phase

In this phase, both U_i and S_j execute the following steps to mutually authenticate each other and agree on a session key in order to communicate over insecure public channels later.

Step AK1: Upon receiving the login message M_1, the server S_j chooses a random nonce n_2 and computes $C_2 = E_{H(k_j||h_1)}[n_2]$ and $h_2 = H(C_1||X||h_1||SID_j||k_j||s_j||n_2)$. S_j then sends the message $M_2 = \{C_1, X, h_1, C_2, h_2\}$ to RC via a public channel.

Step AK2: After receiving the message M_2 from S_j, RC computes $K_2 = kX(= K_1)$ and obtains ID_i, SID_j, s_j, and n_1 by decrypting C_1 using K_{2x}, where K_{2x} is the x-coordinate of the ECC point K_2. RC checks the freshness of n_1, and also checks validity of SID_j and ID_i by checking $H(SID_j||k)$ and $H(ID_i||k)$, respectively, in the table $\mathcal{T}$. If these are not valid, RC immediately terminates the session. Otherwise, RC retrieves r_j and r_i corresponding to SID_j and ID_i, respectively, from $\mathcal{T}$. Next, RC computes $k_i = H(ID_i||k||r_i||H(ID_i||k))$ and $k_j = H(SID_j||k||r_j)$, and then checks whether the conditions $h_1 = H(ID_i||SID_j||s_j||n_1||k_i||X||K_2)$ and $s_j = H(k||r_j||k_j||SID_j)$ hold or not. If these do not hold, RC stops the session. Otherwise, RC confirms that the received credentials (SID_j, s_j) of S_j are valid. RC then computes $n_2 = D_{H(k_j||h_1)}(C_2)$ and authenticates the server S_j by checking the condition $h_2 = H(C_1||X||h_1||SID_j||k_j||s_j||n_2)$. If the authentication fails, the RC terminates the session. Otherwise, RC computes $k_{i,j} = H(k_i||K_2||n_1)$, $C_3 = E_{H(k_j||h_1||n_2)}\ [SID_j||k_{i,j}]$ (the identity ID_i of U_i is kept anonymous to S_j), and $h_3 = H(k_j||h_2||C_3||SID_j||k_{i,j}||X||n_2)$. Finally, RC sends the message $M_3 = \{C_3, h_3\}$ to S_j via a public channel.

In order to check the freshness of the random nonce n_1 by the RC, we adopt the following strategy as suggested in [35] and [43]. The RC can store n_1 corresponding to the value $H(ID_i||k)$ in the table $\mathcal{T}$. When the RC receives the next message, say $M_2' = \{C_1', X', h_1', C_2', h_2'\}$, it computes $K_2' = kX'(= K_1)$ and obtains ID_i, SID_j, s_j, and n_1' by decrypting C_1' using K_{2x}', where K_{2x}' is the x-coordinate of the ECC point K_2'. The RC then checks the value of n_1' corresponding to $H(ID_i||k)$ with the stored value n_1 in the table $\mathcal{T}$. If there is a match, the RC ensures that the message is not a fresh one. Otherwise, the RC treats the received message as a fresh message and updates n_1 with n_1' in the table $\mathcal{T}$. Note that the old n_1 can be kept for some time by the RC so that if an adversary replays the same old message again containing n_1, it can be detected as old message.

Step AK3: After receiving the message M_3 from RC, S_j obtains SID_j and $k_{i,j}$ by decrypting C_2 using $H(k_j||h_1||n_2)$ and then checks whether the condition $h_3 = H(k_j||h_2||C_3||SID_j||k_{i,j}||X||n_2)$ holds or not. If it does not hold, S_j terminates the session. Otherwise, S_j confirms that the secrets $k_{i,j} = H(k_i||K_2||n_1)$ and X are shared by the legal user U_i, and $k_{i,j}$ is only known to RC, U_i and S_j. Then, S_j randomly chooses $y \in Z_p^*$ and computes $Y = yP$, $SK = H(yX||k_{i,j}||s_j)$, and $h_4 = H(SID_j||s_j||h_1||k_{i,j}||X||Y||SK)$. Finally, S_j sends the message $M_4 = \{Y, h_4\}$ to U_i via a public channel.

Step AK4: Upon receiving the message M_4 from S_j, U_i computes $SK = H(yX||k_{i,j}||s_j)$, where $k_{i,j} = H(k_i||K_1||n_1)$ and checks whether the condition $h_4 = H(SID_j||s_j||h_1||k_{i,j}||X||Y||SK)$ holds or not. If it does not hold, U_i terminates the session. Otherwise, U_i authenticates S_j as the hash value $k_{i,j}$ is only known to RC, U_i and S_j. U_i then computes $h_5 = H(SID_j||k_{i,j}||X||Y||SK)$ and sends the confirmation message $M_5 = \{h_5\}$ to S_j via a public channel.

Step AK5: After receiving the message M_5 from U_i, S_j checks whether the condition $h_5 = H(SID_j||k_{i,j}||X||Y||SK)$ holds or not. If it holds, S_j confirms that U_i is a valid user. Otherwise, S_j terminates the session immediately.

Finally, after mutual authentication, both user U_i and server S_j agree on the common session key SK. The login and authentication and key establishment phases of our scheme are summarized in Table VII.

TABLE VII

LOGIN, AND AUTHENTICATION AND KEY ESTABLISHMENT PHASES OF OUR SCHEME

User U_i	Server S_j	Registration center RC
Inputs ID_i', pw_i', B_i' into SC_i. Computes $\sigma_i' = Rep(B_i', \theta_i)$, $k_i' = z_i' \oplus H(pw_i' \vert\vert \sigma_i')$. Checks $s_i =^? H(k_i' \vert\vert ID_i' \vert\vert H(pw_i' \vert\vert \sigma_i'))$. accept/reject? Chooses $x_i \in Z_n^*$, n_1. Computes $x = H(x_i \vert\vert k_i \vert\vert n_1)$, $K_1 = xP_{pub}$, $X = xP$, $C_1 = E_{K_{1x}}[ID_i, SID_j, s_j, n_1]$, $h_1 = H(ID_i \vert\vert SID_j \vert\vert s_j \vert\vert n_1 \vert\vert k_i \vert\vert X \vert\vert K_1)$. $\xrightarrow{M_1 = \{C_1, X, h_1\}}$ (via a public channel)	Chooses n_2 and computes $C_2 = E_{H(k_j \vert\vert h_1)}[n_2]$, $h_2 = H(C_1 \vert\vert X \vert\vert h_1 \vert\vert SID_j \vert\vert k_j \vert\vert s_j \vert\vert n_2)$. $\xrightarrow{M_2 = \{C_1, X, h_1, C_2, h_2\}}$ (via a public channel)	Computes $K_2 = kX\ (= K_1)$, $[ID_i, SID_j, s_j, n_1] = D_{K_{2x}}(C_1)$. Checks validity of ID_i, n_1, SID_j. accept/reject? Computes k_i and k_j. Checks validity of h_1 and s_j. accept/reject? Computes $n_2 = D_{H(k_j \vert\vert h_1)}(C_2)$. Checks validity of h_2. accept/reject? Computes $k_{i,j} = H(k_i \vert\vert K_2 \vert\vert n_1)$, $C_3 = E_{H(k_j \vert\vert h_1 \vert\vert n_2)}[SID_j \vert\vert k_{i,j}]$, $h_3 = H(k_j \vert\vert h_2 \vert\vert C_3 \vert\vert SID_j \vert\vert k_{i,j} \vert\vert X \vert\vert n_2)$. $\xleftarrow{M_3 = \{C_3, h_3\}}$ (via a public channel)
	Computes $[SID_j \vert\vert k_{i,j}] = D_{H(k_j \vert\vert h_1 \vert\vert n_2)}(C_3)$. Checks validity of h_3. accept/reject? Chooses $y \in Z_p^*$. Computes $Y = yP$, $SK = H(yX \vert\vert k_{i,j} \vert\vert s_j)$, $h_4 = H(SID_j \vert\vert s_j \vert\vert h_1 \vert\vert k_{i,j} \vert\vert X \vert\vert Y \vert\vert SK)$. $\xleftarrow{M_4 = \{Y, h_4\}}$ (via a public channel)	
Computes $k_{i,j} = H(k_i \vert\vert K_1 \vert\vert n_1)$, $SK = H(xY \vert\vert k_{i,j} \vert\vert s_j)$. Checks validity of h_4. accept/reject? Computes $h_5 = H(SID_j \vert\vert k_{i,j} \vert\vert X \vert\vert Y \vert\vert SK)$. $\xrightarrow{M_5 = \{h_5\}}$ (via a public channel) Computes $SK = H(yX \vert\vert k_{i,j} \vert\vert s_j)$	Checks $h_5 =^? H(SID_j \vert\vert k_{i,j} \vert\vert X \vert\vert Y \vert\vert SK)$. accept/reject? Computes $SK = H(xY \vert\vert k_{i,j} \vert\vert s_j)$	

E. Password Change Phase

In this phase, U_i can change his/her password pw_i without further contacting the RC using the following steps:

Step P1: U_i inserts his/her smart card SC_i into a card reader and inputs pw_i', ID_i' and imprints personal biometrics B_i' at the sensor. SC_i computes $\sigma_i' = Rep(B_i', \theta_i)$ and $k_i' = z_i' \oplus H(pw_i'||\sigma_i')$, and then checks whether the condition $s_i = H(k_i'||ID_i'||H(pw_i'||\sigma_i'))$ holds or not. If it does not hold, SC_i rejects the entered credentials. Otherwise, SC_i asks U_i for a new password.

Step P2: U_i enters his/her chosen new password, say pw_i^{new} into the smart card SC_i.

Step P3: SC_i then computes $z_i^{new} = k_i \oplus H(pw_i^{new}||\sigma_i)$ and $s_i^{new} = H(k_i||ID_i||H(pw_i^{new}||\sigma_i))$. Finally, SC_i replaces z_i and s_i with z_i^{new} and s_i^{new}, respectively.

Remark 2: In the case of all three factors (smart card, password and biometrics) are required, the authentication mechanism should be more efficient [44]. For identifying wrong password entry, He-Wang's scheme requires $6T_M$, where T_M denotes an elliptic curve scalar multiplication operation. However, in our scheme, the password verification is done by the smart card SC_i locally. Moreover, we can achieve the three-factor authentication by removing the hash value s_i from the smart-card SC_i and then, the identification of a wrong password would require only $3T_M$ operations in our scheme. In that case, the password change will not be possible locally.

F. Revocation and Re-Registration Phase

In this phase, we explain the user revocation and re-registration with the same identity when his/her authentication key is compromised or the smart-card is lost/stolen. In these two cases, a user U_i can revoke his/her account and re-register without changing his/her identity ID_i. For revocation of U_i's account, the registration center RC verifies his/her personal identities such as PAN card, date of birth, passport, or any authorized identities, and then simply removes the random number r_i from the table $\mathcal{T}$. Thus, after revocation of U_i's account, RC rejects the login request as the corresponding random number r_i is not presented in $\mathcal{T}$ and then it cannot authenticate the user U_i. In the case of re-registration of U_i with the same identity ID_i, RC verifies $\mathcal{T}$ whether the identity ID_i is valid, that is, whether the user U_i is already registered, but the status is inactive. If it is valid, RC executes the registration phase to reactivate U_i's account.

Remark 3: Assume that the secret key k_j of the server S_j is unexpectedly revealed to an attacker $\mathcal{A}$. The server S_j can revoke its account and re-register to the RC with the same identity SID_j in order to obtain a fresh secret k_j^{fresh} without any difficulty because the RC can choose a fresh random *number r_j^{fresh}, and compute a secret key k_j^{fresh} and signature s_j^{fresh} using r_j^{fresh}. Therefore, our scheme also provides the server re-registration when its secret key is revealed, whereas He-Wang's scheme cannot support it.*

VI. SECURITY ANALYSIS OF OUR SCHEME

In this section, we analyze our scheme using the widely-accepted BAN logic [45] and show that our proposed scheme provides secure authentication. After that we discuss informally the possible attacks on our scheme. Furthermore, we simulate our scheme for the formal security verification using the widely-accepted and used AVISPA tool to show that our scheme is secure against active attacks, such as the man-in-the-middle-attack and reply attack.

A. Authentication Proof Based on the BAN Logic

The notations used in the BAN logic are as follows:

- $P \mid\equiv X$: Principal P believes a statement X, or P is entitled to believe X.
- $\#(X)$: Formula X is fresh.
- $P \mid\Rightarrow X$: Principal P has jurisdiction over statement X.
- $P \lhd X$: Principal P sees the statement X.
- $P \mid\sim X$: Principal P once said the statement X.
- (X, Y) : Formula X or Y is one part of formula (X, Y).
- $\{X\}_K$: Formula X encrypted under the key K.
- $\langle X\rangle_Y$: Formula X combined with the formula Y.
- $P \overset{K}{\longleftrightarrow} Q$: P and Q may use the shared key K to communicate. The key K is good, in that it will never be discovered by any principal except P and Q.
- $P \overset{X}{\rightleftharpoons} Q$: Formula X is secret known only to P and Q, and possibly to principals trusted by them.

Rules: We have the following four rules:

Rule(1). Message-meaning rule: $\frac{P\mid\equiv P\overset{K}{\longleftrightarrow}Q,\, P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$ and $\frac{P\mid\equiv P\overset{Y}{\rightleftharpoons}Q,\, P\lhd\langle X\rangle_Y}{P\mid\equiv Q\mid\sim X}$.

Rule(2). Nonce-verification rule: $\frac{P\mid\equiv\#(X),\, P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$.

Rule(3). Jurisdiction rule: $\frac{P\mid\equiv Q\mid\Rightarrow X,\, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$.

Rule(4). Freshness-conjuncatenation rule: $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$.

Goals: According to the analytic procedures of the BAN logic, the proposed protocol must satisfy the following test goals in order to prove the system is secure:

$$G_1 : S_j \mid\equiv U_i \overset{k_{i,j}}{\rightleftharpoons} S_j;\ G_2 : U_i \mid\equiv S_j \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_j;$$
$$G_3 : U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_j;\ G_4 : S_j \mid\equiv U_i \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_j;$$
$$G_5 : S_j \mid\equiv U_i \overset{SK}{\longleftrightarrow} S_j.$$

Generic form: The generic form of our scheme is given below:

From message M_1, $U_i \rightarrow S_j$: $\{ID_i, SID_j, s_j, n_1\}_{K_1}$, $X = xP$, $\langle ID_i||SID_j||s_j||n_1||X||K_1\rangle_{k_i}$.

From message M_2, $S_j \rightarrow RC$: $\{ID_i, SID_j, s_j, n_1\}_{K_1}$, $X = xP, \langle ID_i||SID_j||s_j||n_1||k_i||X||K_1\rangle_{k_i}, \{n_2\}_{H(k_j||h_1)}$, $\langle C_1||X||h_1||SID_j||s_j||n_2\rangle_{k_j}$.

From message M_3, $RC \rightarrow S_j$: $\{SID_j||k_{i,j}\}_{H(k_j||h_1||n_2)}$, $X = xP$, $\langle h_2||C_3||SID_j||k_{i,j}||X||n_2\rangle_{k_j}$.

From message M_4, $S_j \rightarrow U_i$: $Y = yP$, $\langle SID_j||s_j||h_1||X||Y||SK\rangle_{k_{i,j}}$.

From message M_5, $U_i \rightarrow S_j$: $\langle SID_j||X||Y||SK\rangle_{k_{i,j}}$.

Idealized form: The arrangement of the proposed protocol to the idealized form is as follows:

Message M_1:

$$U_i \rightarrow S_j : \langle ID_i, SID_j, s_j, n_1, X, U_i \overset{K_1}{\longleftrightarrow} RC\rangle_{U_i \overset{k_i}{\longleftrightarrow} RC}$$

Message M_2:

$$S_j \rightarrow RC : \langle C_1, X, h_1, SID_j, s_j, n_2\rangle_{S_j \overset{k_j}{\longleftrightarrow} RC}$$

Message M_3:

$$RC \rightarrow S_j : \langle h_2, C_3, SID_j, U_i \overset{k_{i,j}}{\rightleftharpoons} S_j, X, n_2\rangle_{S_j \overset{k_j}{\longleftrightarrow} RC}$$

Message M_4:

$$S_j \rightarrow U_i : \langle SID_j, s_j, h_1, X, Y, U_i \overset{SK}{\longleftrightarrow} S_j\rangle_{U_i \overset{k_{i,j}}{\rightleftharpoons} S_j}$$

Message M_5:

$$U_i \rightarrow S_j : \langle SID_j, X, Y, U_i \overset{SK}{\longleftrightarrow} S_j\rangle_{U_i \overset{k_{i,j}}{\rightleftharpoons} S_j}$$

Hypotheses: The following assumptions about the initial state are made to analyze the proposed protocol:

$H_1 : U_i \mid\equiv \#(n_1)$, $U_i \mid\equiv \#(xP)$; $H_2 : S_j \mid\equiv \#(n_2)$, $U_j \mid\equiv \#(yP)$; $H_3 : U_i \mid\equiv U_i \overset{k_i}{\longleftrightarrow} RC$; $H_4 : RC \mid\equiv U_i \overset{k_i}{\longleftrightarrow} RC$;

$H_5 : U_i \mid\equiv U_i \overset{k_{i,j}}{\rightleftharpoons} S_j$; $H_6 : S_j \mid\equiv S_j \overset{k_j}{\longleftrightarrow} RC$;

$H_7 : RC \mid\equiv S_j \overset{k_j}{\longleftrightarrow} RC$; $H_8 : U_i \mid\equiv RC \mid\Rightarrow S_j \mid\sim X$;

$H_9 : S_j \mid\equiv RC \Mapsto U_i \mid\sim X$; $H_{10} : U_i \mid\equiv S_j \mid\Rightarrow U_i \overset{SK}{\longleftrightarrow} S_j$;

$H_{11} : S_j \mid\equiv U_i \mid\Rightarrow U_i \overset{SK}{\longleftrightarrow} S_j$;

$H_{12} : S_j \mid\equiv RC \mid\Rightarrow U_i \overset{k_{i,j}}{\longleftrightarrow} S_j$.

The idealized form of the proposed protocol is analyzed based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

From message M_2, we have

$$S_1 : RC \lhd \langle C_1, X, h_1, SID_j, s_j, n_2\rangle_{S_j \overset{k_j}{\longleftrightarrow} RC}.$$

From H_7, S_1 and *Rule*(1), we have,

$$S_2 : RC \mid\equiv S_j \mid\sim \langle C_1, X, h_1, SID_j, s_j, n_2\rangle.$$

From message M_1, we have,

$$S_3 : RC \lhd \langle ID_i, SID_j, s_j, n_1, X, U_i \overset{K_1}{\longleftrightarrow} RC\rangle_{U_i \overset{k_i}{\longleftrightarrow} RC}.$$

From H_3, S_3 and *Rule*(1), we also have,

$$S_4 : RC \mid\equiv U_i \mid\sim \langle ID_i, SID_j, s_j, n_1, X, U_i \overset{K_1}{\longleftrightarrow} RC\rangle.$$

From message M_3, we have,

$$S_5 : S_j \lhd \langle h_2, C_3, SID_j, U_i \overset{k_{i,j}}{\rightleftharpoons} S_j, X, n_2\rangle_{S_j \overset{k_j}{\longleftrightarrow} RC}.$$

From H_6, S_5 and *Rule*(1), we obtain,

$$S_6 : S_j \mid\equiv RC \mid\sim \langle h_2, C_3, SID_j, U_i \overset{k_{i,j}}{\rightleftharpoons} S_j, X, n_2\rangle.$$

From H_2, S_6, $Rule(2)$ and $Rule(4)$, we get,

$$S_7 : S_j \mid\equiv RC \mid\equiv U_i \overset{k_{i,j}}{\rightleftharpoons} S_j.$$

Again, from H_{12}, S_7 and $Rule(3)$, we have,

$$S_8 : S_j \mid\equiv U_i \overset{k_{i,j}}{\rightleftharpoons} S_j (\textbf{Goal } G_1).$$

From message M_4, we get,

$$S_9 : U_i \lhd \langle SID_j, s_j, h_1, X, Y, U_i \xleftrightarrow{SK} S_j \rangle_{U_i \overset{k_{i,j}}{\rightleftharpoons} S_j}.$$

From H_5, S_9 and $Rule(1)$, we get

$$S_{10} : U_i \mid\equiv S_j \mid\sim \langle SID_j, s_j, h_1, X, Y, U_i \xleftrightarrow{SK} S_j \rangle.$$

From H_1, S_{10}, $Rule(2)$ and $Rule(4)$, we have,

$$S_{11} : U_i \mid\equiv S_j \mid\equiv U_i \xleftrightarrow{SK} S_j (\textbf{Goal } G_2).$$

From H_{10}, S_{11} and $Rule(3)$, we obtain,

$$S_{12} : U_i \mid\equiv U_i \xleftrightarrow{SK} S_j (\textbf{Goal } G_3).$$

From message M_5, we get,

$$S_{13} : S_j \lhd \langle SID_j, X, Y, U_i \xleftrightarrow{SK} S_j \rangle_{U_i \overset{k_{i,j}}{\rightleftharpoons} S_j}.$$

From S_8, S_{13} and $Rule(1)$, we also get,

$$S_{14} : S_j \mid\equiv U_i \mid\sim \langle SID_j, X, Y, U_i \xleftrightarrow{SK} S_j \rangle.$$

From H_2, S_{14}, $Rule(2)$ and $Rule(4)$, we obtain,

$$S_{15}{:}S_j \mid\equiv U_i \mid\equiv U_i \xleftrightarrow{SK} S_j (\textbf{Goal } G_4)$$

Finally, from H_{11}, S_{15}, and $Rule(3)$, we have,

$$S_{16} : S_j \mid\equiv U_i \xleftrightarrow{SK} S_j (\textbf{Goal } G_5).$$

B. Other Possible Attacks

In this section, we show informally that our scheme has the ability to resist the various possible known attacks.

1) Privileged Insider Attack: As in He-Wang's scheme, in the registration phase of our scheme, a legal user U_i sends the identity ID_i and the pseudo-password $H(pw_i||\sigma_i)$ instead of sending the direct password pw_i in plaintext. Due to the difficulty of inverting one-way hash function $H(\cdot)$ and guessing biometrics B_i of the user U_i, it is computationally hard for the insider to derive the password pw_i. Hence, our scheme is secure against the privileged insider attack.

2) Password Guessing Attack: In our scheme, the password pw_i of a user U_i is involved in $z_i = k_i \oplus H(pw_i||\sigma_i)$ and $s_i = H(k_i||ID_i||H(pw_i||\sigma_i))$, which are stored in the smart card SC_i. Assume that an adversary $\mathcal{A}$ has the lost/stolen smart card SC_i of the user U_i. Then, using the power analysis attacks [27], [28], $\mathcal{A}$ can extract all the information from SC_i including z_i and s_i. However, guessing password pw_i without knowing the biometric B_i and identity ID_i is a computationally infeasible problem for $\mathcal{A}$. Since biometrics keys cannot be lost/forgotten, it is hard to forge and also it is difficult to copy [24], [35], $\mathcal{A}$ has no ability to derive the password pw_i from the stolen/lost smart card SC_i. Thus, our scheme is secure against offline password guessing attack through the stolen/lost smart card attack.

3) Strong User Anonymity: In our scheme, the identity ID_i of a legal user U_i is included in $C_1 = E_{K_{1x}}[ID_i, SID_j, s_j, n_1]$ of the message M_1, where $K_1 = H(x_i||k_i||n_1)P_{pub} = kX$. An adversary $\mathcal{A}$ requires either the pair (k_i, x_i) or secret key k of the RC to compute K_1. The adversary $\mathcal{A}$ has no ability to compute the identity ID_i, even if he/she knows the temporary information x_i and n_1 without knowledge of either k_i or k due to the difficulty of solving ECDLP and CDHP (provided in Definitions 1 and 2). Moreover, ID_i is not revealed to a server S_j, instead the user U_i shares $k_{i,j}$ through the RC. Thus, our scheme provides the strong user anonymity property.

4) Mutual Authentication: From the goals G_2-G_5 in Section VI-A, it is proved that in our scheme, a user U_i and a server S_j mutually authenticate each other. Also, the registration center RC authenticates both U_i and S_j based on their identities. Therefore, our scheme achieves the mutual authentication.

5) Server Spoofing Attack: To impersonate a server S_j to the user U_i and the RC, an adversary $\mathcal{A}$ needs to generate the valid $C_2 = E_{H(k_j||h_1)}[n_2]$ and $h_2 = H(C_1||X||h_1||SID_j||k_j||s_j||n_2)$ for the message M_2 to get $C_3 = E_{H(k_j||h_1||n_2)}[SID_j||k_{i,j}]$ for the message M_3. It is clear that the attacker $\mathcal{A}$, in this case, cannot succeed without having the valid tuple $\langle SID_j, k_j, s_j \rangle$ due to the difficulty of inverting a one-way hash function $H(\cdot)$. As a result, our scheme has the ability to resist the server spoofing attack.

6) Stolen Verifier Attack: In the registration phase of our scheme, the RC stores the identity information $\{H(ID_i||k), r_i\}$ of a legal user U_i. Since it is masked with RC's secret key k using a secure one-way hash function $H(\cdot)$, deriving ID_i is computationally infeasible. Hence, our scheme is secure against stolen verifier attack.

7) Perfect Forward Secrecy: Perfect forward secrecy ensures that an adversary $\mathcal{A}$ cannot compute the session keys generated in previous sessions, even if he/she gets all participants' secret keys. In our scheme, the session key $SK = H(yX||k_{i,j}||s_j) = H(yH(x_i||k_i||n_1)P||k_{i,j}||s_j)$ is computed using the session random numbers x_i, n_1 and y chosen by U_i and S_j. Thus, even if all participants' secret keys compromised, it is computationally infeasible for the adversary $\mathcal{A}$ to compute SK without knowing x_i, n_1 and y due to the collision-resistant property of the one-way hash function $H(\cdot)$ (provided in Definition 3) and the difficulty to solve ECDLP (provided in Definition 1). As a result, our scheme provides the perfect forward secrecy.

8) Known Session-Specific Temporary Information Attack: Our scheme successfully prevents this attack as follows. From the goal G_1, we achieve $U_i \overset{k_{i,j}}{\rightleftharpoons} S_j$, where $k_{i,j} = H(k_i||K_1||n_1) = H(k_i||H(x_i||k_i||n_1)P_{pub}||n_1) = H(H(ID_i||k||r_i||H(ID_i||k))||kX||n_1)$. Clearly, even if an attacker $\mathcal{A}$ knows the temporary information x_i and n_1, he/she cannot compute $k_{i,j}$ without having the knowledge of either k_i or k. In this way, our scheme overcomes the drawbacks found in He-Wang's scheme. Moreover, without revealing the identity ID_i of the user U_i to the server S_j, S_j authenticates U_i through the registration center RC, whereas He-Wang's scheme reveals the identity ID_i to the server S_j and with the known session-specific temporary information, the adversary $\mathcal{A}$ is successful in the reply attack.

9) Reply Attack: Suppose an adversary $\mathcal{A}$ intercepts the message $M_1 = \{C_1, X, h_1\}$, where $X = xP$, $C_1 = E_{K_{1x}}[ID_i, SID_j, s_j, n_1]$ and $h_1 = H(ID_i||SID_j||s_j||n_1||k_i||X||K_1)$, and replies this message to the server S_j. However, the adversary $\mathcal{A}$ cannot compute the valid $h_5 = H(SID_j||k_{i,j}||X||Y||SK)$ without knowing k_i, x_i and n_1. Therefore, $\mathcal{A}$ cannot succeed by replying with the intercepted message M_1. Hence, our scheme protects the replay attack.

10) Impersonation Attack: An adversary $\mathcal{A}$ does not have any means to get a user (or server) information in order to authenticate at the RC and also to establish a session key with the server (or the user). Moreover, the RC authenticates a user U_i and a server S_j separately as the server S_j needs to provide two valid factors SID_j and s_j along with the secret key k_j. Thus, our scheme has the ability to prevent the impersonation attack.

11) Man-in-the-Middle Attack: In this attack, an attacker $\mathcal{A}$ may try to impersonate a valid user U_i or server S_j by intercepting the messages. However, in our scheme the RC authenticates both U_i and S_j separately, and also U_i and S_j authenticate each other with the presence of the trusted RC. Hence, our scheme is secure against man-in-the-middle attack.

C. Simulation for Formal Security Verification Using AVISPA Tool

In addition to the informal and formal security analysis, we provide the simulation results for our scheme using the widely-accepted and used AVISPA (Automated Validation of Internet Security Protocols and Applications) tool [46], [47]. It is a tool for the automated validation of Internet security-sensitive protocols and applications. It consists of the following four backends: (a) On-the-fly-Model-Checker (OFMC), (b) Constraint Logic based Attack Searcher (CL-AtSe), (c) SAT-based Model-Checker (SATMC), and (d) Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). The implementation of our scheme in HLPSL (High Level Protocol Specification Language) used in AVISPA, and the details of AVISPA architecture and HLPSL are provided in the supplementary material. We have simulated our scheme using the widely-accepted OFMC backend [48] for the formal security verification, and the results are shown in Figure 1. The results clearly demonstrate that our scheme is secure.

VII. PERFORMANCE COMPARISON

In this section, we only compare the performance of our scheme with He-Wang's scheme [23], because we have pointed out the security pitfalls of He-Wang's scheme and then proposed a new scheme to withstand those security pitfalls found in their scheme.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web−interface−computation/
  ./tempdir/workfilewa2NHD.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 81.41s
  visitedNodes: 4622 nodes
  depth: 9 plies
```

Fig. 1. The result of the analysis using OFMC backend of our scheme.

TABLE VIII

COMPARISON OF COMMUNICATION COST

	He-Wang [23]	Ours
Server registration phase	192 bits	352 bits
User registration phase	192 bits	512 bits
Login and authentication phases	3520 bits	2944 bits

As in [23], we also assume that the length of the identity ID_i, the output size of hash function $H(\cdot)$ (for example, SHA-1 [49]), and an elliptic curve point $P = (P_x, P_y)$ are 32 bits, 160 bits, and 320 bits, respectively. In addition, we assume that the block size of symmetric encryption/decryption (for example, AES [50]) is 128 bits and a random number/nonce is 128 bits. The communication cost for the server registration phase for sending the identity SID_j and receiving the pair (k_j, s_j) is $32 + (160 + 160) = 352$ bits. To separately identify a server S_j at the RC, our scheme requires extra 160 bits for s_j in the server registration phase. The communication cost for the user registration phase for sending the pair $(ID_i, H(pw_i||\sigma_i))$ and receiving the pair (z_i, s_i) becomes $(32 + 160) + (160 + 160) = 512$ bits. Since the user U_i receives the smart card SC_i before the registration, our scheme requires extra 320 bits to receive z_i and s_i instead of receiving SC_i as in He-Wang's scheme. During the login phase, and authentication and key agreement phase, our scheme requires $(3 \times 128) + 320 + 160 = 864$ bits, $(3 \times 128) + 320 + 160 + 128 + 160 = 1152$ bits, $128 + 160 = 288$ bits, $320 + 160 = 480$ bits, and 160 bits for the messages $M_1 = \{C_1, X, h_1\}$, $M_2 = \{C_1, X, h_1, C_2, h_2\}$, $M_3 = \{C_3, h_3\}$, $M_4 = \{Y, h_4\}$ and $M_5 = \{h_5\}$, respectively. Therefore, the total communication cost required in the login phase, and authentication and key agreement phase of our scheme is 2944 bits, whereas He-Wang's scheme requires 3520 bits. Since the user and server registration phases are one-time, our scheme significantly reduces the communication cost in the login phase, and authentication and key agreement phase as compared to He-Wang's scheme as shown in Table VIII.

We have compared the computational costs of our scheme with He-Wang's scheme in Table IX. Let T_H, T_Ω and T_M denote the time to execute a one-way hash function, a symmetric key encryption/decryption and an elliptic curve point multiplication, respectively. According to the results reported in [51], $T_H \approx 0.0023ms$, $T_\Omega \approx 0.0046ms$ and $T_M \approx 2.226ms$. From Table IX, we see that the computational costs required during the login phase, and authentication and

TABLE IX

COMPARISON OF COMPUTATIONAL COST

	He-Wang [23]	Ours
User (U_i)	$3T_M + 7T_H$	$3T_M + 7T_H + 1T_\Omega$
Server (S_j)	$3T_M + 5T_H$	$2T_M + 6T_H + 2T_\Omega$
RC	$2T_M + 9T_H$	$1T_M + 11T_H + 3T_\Omega$
Total cost	$8T_M + 21T_H$	$6T_M + 24T_H + 6T_\Omega$
Total execution time	$17.8563ms$	$13.4388ms$

TABLE X

COMPARISON OF FUNCTIONALITY FEATURES

	He-Wang [23]	Ours
Provides mutual authentication	Yes	Yes
Requires identity-verification table	No	Yes
Server spoofing attack resistance	Yes	Yes
Stolen verifier attack resistance	Yes	Yes
Privileged insider attack resistance	Yes	Yes
Password guessing attack resistance	Yes	Yes
Stolen/lost smart card attack resistance	Yes	Yes
Provides strong user anonymity	No	Yes
Provides perfect forward secrecy	Yes	Yes
Known session-specific temporary information attack resistance	No	Yes
Provides SK-security	No	Yes
Impersonation attack resistance	No	Yes
Reply attack resistance	No	Yes
Man-in-the-middle attack resistance	Yes	Yes
Provision for revocation and re-registration	No	Yes
Free from denial of service attack	No	Yes
Wrong password login	Yes	No
Drawback in password change phase	Yes	No

key establishment phase of our scheme for the user U_i, server S_j and RC are $3T_M + 7T_H + 1T_\Omega$, $2T_M + 6T_H + 2T_\Omega$, and $1T_M + 11T_H + 3T_\Omega$, respectively. The total computational cost is then $6T_M + 24T_H + 6T_\Omega$. According to the execution time for different operations given in [51], the approximate time to execute our scheme is $13.4388ms$, whereas He-Wang's scheme requires $17.8563ms$. Thus, our scheme also significantly reduces the computational costs during the login phase, and authentication and key agreement phase as compared to those for He-Wang's scheme.

Finally, in Table X, we have shown the functionality analysis of our scheme with He-Wang's scheme. It is observed that our scheme outperforms as compared to He-Wang's scheme as our scheme supports extra features listed in this table and is also more secure than He-Wang's scheme. As a result, our scheme is much suitable for practical applications as compared to the recently proposed He-Wang's scheme.

VIII. CONCLUSION

In this paper, we have first reviewed the recently proposed He-Wang's scheme and then shown that their scheme is vulnerable to the known session-specific temporary information attack and thus, their scheme fails to prevent reply attack and cannot provide strong user anonymity. Also, we have demonstrated the drawbacks in He-Wang's scheme while distributing the static authentication parameters and with the wrong password entry. To withstand these drawbacks, we have proposed a novel and efficient multi-server authentication protocol using biometric-based smart card and ECC. We have shown that our scheme is secure and provides more functionalities as compared to He-Wang's scheme. Using the BAN logic, we have proved that our scheme provides secure authentication through the formal security analysis. We have further simulated our scheme for the formal security verification using the widely-accepted AVISPA tool, and shown that our scheme is secure. In addition, through the informal security analysis, we have shown that our scheme is secure against various known attacks. Our scheme thus provides high security along with low communication cost, computational cost, and offers a variety of features. As a result, our scheme is particularly suitable for battery-limited mobile devices.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the Associate Editor for providing constructive and generous feedback.

REFERENCES

[1] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2004–2013, Nov. 2013.

[2] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 1, pp. 337–368, First Quarter 2014.

[3] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology*. Innsbruck, Austria: Springer-Verlag, 2001, pp. 453–474.

[4] M. Bellare, R. Canetti, and H. Krawczyk, "A modular approach to the design and analysis of authentication and key exchange protocols," in *Proc. 30th Annu. ACM Symp. Theory Comput. (STOC)*, 1998, pp. 419–428.

[5] E. Brickell and J. Li, "Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 345–360, May/Jun. 2012.

[6] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1767–1775, Jul. 2014.

[7] D. Wang, D. He, P. Wang, and C. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Comput.*, to be published.

[8] S. Wu, Y. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," *Secur. Commun. Netw.*, vol. 5, no. 2, pp. 236–248, 2012.

[9] S. Kumari and M. K. Khan, "Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme,'" *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 3939–3955, 2014.

[10] M. K. Khan and S. Kumari, "Cryptanalysis and improvement of 'an efficient and secure dynamic ID-based authentication scheme for telecare medical information systems,'" *Secur. Commun. Netw.*, vol. 7, no. 2, pp. 399–408, 2014.

[11] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 431–436, Feb. 2011.

[12] L. Wu, Y. Zhang, and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," *Comput. Standards Interf.*, vol. 31, no. 2, pp. 286–291, 2009.

[13] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[14] L.-H. Li, I.-C. Lin, and M.-S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," *IEEE Trans. Neural Netw.*, vol. 12, no. 6, pp. 1498–1504, Nov. 2001.

[15] T.-Y. Chen, C.-H. Ling, and M.-S. Hwang, "Weaknesses of the Yoon–Kim–Yoo remote user authentication scheme using smart cards," in *Proc. IEEE Workshop Electron., Comput. Appl.*, Ottawa, ON, Canada, May 2014, pp. 771–774.

[16] W.-S. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 251–255, Feb. 2004.

[17] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Comput. Standards Interf.*, vol. 31, no. 6, pp. 1118–1123, 2009.

[18] T.-Y. Chen, C.-C. Lee, M.-S. Hwang, and J.-K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *J. Supercomput.*, vol. 66, no. 2, pp. 1008–1032, 2013.

[19] J.-L. Tsai, N.-W. Lo, and T.-C. Wu, "A new password-based multi-server authentication scheme robust to password guessing attacks," *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 1977–1988, 2013.

[20] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, 2013.

[21] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in *Proc. 12th Int. Conf. Comput. Sci. Appl. (ICCSA)*, Salvador, Brazil, 2012, pp. 391–406.

[22] D. He. (2011). "Security flaws in a biometrics-based multi-server authentication with key agreement scheme," IACR Cryptol. ePrint Arch., Tech. Rep. 2011/365, pp. 1–9. [Online]. Available: http://eprint.iacr.org/2011/365.pdf

[23] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, to be published.

[24] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Commun. ACM*, vol. 43, no. 2, pp. 90–98, 2000.

[25] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[26] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 62–67, Feb. 2004.

[27] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, vol. 1666. Santa Barbara, CA, USA, 1999, pp. 388–397.

[28] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[29] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[30] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.

[31] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, Dec. 2010, Art. ID 33.

[32] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Designs, Codes Cryptogr.*, vol. 38, no. 2, pp. 259–277, 2006.

[33] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[34] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology*. Interlaken, Switzerland: Springer-Verlag, 2004, pp. 523–540.

[35] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Inf. Secur.*, vol. 5, no. 3, pp. 145–151, 2011.

[36] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012.

[37] Q. Zhang, Y. Yin, D.-C. Zhan, and J. Peng, "A novel serial multimodal biometrics framework based on semisupervised learning techniques," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1681–1694, Oct. 2014.

[38] K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 771–780, Dec. 2010.

[39] M. A. Pathak, B. Raj, S. D. Rane, and P. Smaragdis, "Privacy-preserving speech processing: Cryptographic and string-matching frameworks show promise," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 62–74, Mar. 2013.

[40] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," in *Proc. 16th Int. Conf. Pattern Recognit. (ICPR)*, Quebec City, QC, Canada, 2002, pp. 811–814.

[41] P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. *FRVT 2002: Overview and Summary*. [Online]. Available: https://epic.org/privacy/surveillance/spotlight/1105/nist0303.pdf, accessed Feb. 2015.

[42] R.-C. Wang, W.-S. Juang, and C.-L. Lei, "User authentication scheme with privacy-preservation for multi-server environment," *IEEE Commun. Lett.*, vol. 13, no. 2, pp. 157–159, Feb. 2009.

[43] X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 73–79, 2011.

[44] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[45] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[46] *AVISPA: Automated Validation of Internet Security Protocols and Applications*. [Online]. Available: http://www.avispa-project.org/, accessed Jan. 2013.

[47] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, "An novel three-party authenticated key exchange protocol using one-time key," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 498–503, 2013.

[48] D. Basin, S. Mödersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, 2005.

[49] *FIPS PUB 180-1, Secure Hash Standard*, U.S. Dept. Commerce, Nat. Inst. Standards Technol., Washington, DC, USA, Apr. 1995.

[50] National Institute of Standards and Technology (NIST), U.S. Department of Commerce. (Nov. 2001). *FIPS PUB 197, Advanced Encryption Standard*. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, accessed Nov. 2010.

[51] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 2, pp. 1005–1023, Second Quarter 2014.

Vanga Odelu received the M.Tech. degree in computer science and data processing from IIT Kharagpur, India, in 2011, where he is currently pursuing the Ph.D. degree with the Department of Mathematics. He has authored 18 papers in international journals and conferences. His research interests include cryptography, network security, and hierarchical access control.

Ashok Kumar Das received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Assistant Professor with the Center for Security, Theory and Algorithmic Research of the International Institute of Information Technology, Hyderabad, India. He has authored over 70 papers in international journals and conferences in his research areas. His current research interests include cryptography, wireless sensor network security, proxy signature, hierarchical access control, data mining, and remote user authentication. He received the Institute Silver Medal from IIT Kharagpur.

Adrijit Goswami received the M.Sc. and Ph.D. degrees from Jadavpur University, India, in 1985 and 1992, respectively. In 1992, he joined IIT Kharagpur, India, where he is currently a Professor with the Mathematics Department. He has authored over 105 papers in international journals and conferences in his research areas. His research interests include cryptography and network security, inventory management under fuzzy environment, optimization, database systems, distributed and object-oriented databases, and data mining.