HOSTED BY

ELSEVIER

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

ORIGINAL ARTICLE

Secure server-server communication for dual stage biometrics – based password authentication scheme

Mythili Boopathi [a,*], M. Aramudhan [b]

[a] School of Information Technology, Vellore Institute of Technology, Vellore 632014, India
[b] Department of Information Technology, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal 609603, India

Received 17 April 2016; revised 27 July 2016; accepted 23 January 2017

KEYWORDS

Authentication;
Security;
Server;
Biometric;
Protocol

Abstract The distributed environment insists the protection of servers, while information sharing is achieved. The conventional biometrics-based password authentication mechanisms use single server, which can be compromised easily. The dual stage authentication mechanism has been already proved for its security over the single stage authentication mechanism in our previous work. In this paper, the protocol is improved to establish communication between the authentication server and the master server through a secure link. Since the hashed messages are prone to collision attacks, the proposed scheme uses elliptic curve cryptography-based ciphers for establishing connection at the initial stage. The security analysis of the proposed authentication scheme with secure server – server communication link reveals the robustness and the security features, which are offered over our previous as well as the conventional authentication mechanisms.

1. Introduction

Protecting the network servers from any unsafe user is largely indispensable, in case of the distributed environment [3]. As per the current literature and the real-time situations, the passwords are found to serve as the primary authentication approach in almost all applications [1,23,28]. From its existence in 1981, the researchers have centred their theme around this approach, particularly during the past ten years [5,6,10,19,21,22]. Password authentication using smart card is one among the two-factor authentication techniques of the distributed environment, which is effortless with increased level of robustness [2]. The smart card-dependent password authentication method involves a total of three phases, wherein the user as well as the server is busily indulged in the execution of crucial tasks. The registration phase forms the initial phase, in which the server renders a smart card to the user. The personal details that pertain to the user are contained in the smart card to allow its utilization during the authentication period. Either the user or the server, who is involved in the registration phase, is given the freedom of making a choice on the initial password. Once the registration phase gets finished, the user enters the log-in phase and umpteen number of access to the server can be made as per his/her wish. The availability of an appropriate smart card and its associated password is highly essential to succeed the log-in phase. Hence, the approach involving both the smart card and the password is found to undergo a two-factor authentication. When the password changing phase is performed, the user can alter his/her

* Corresponding author.
E-mail address: mythiliboopathi2016@gmail.com (M. Boopathi).
Peer review under responsibility of Faculty of Engineering, Alexandria University.

http://dx.doi.org/10.1016/j.aej.2017.01.031
1110-0168 © 2017 Faculty of Engineering, Alexandria University. Production and hosting by Elsevier B.V.

Nomenclature

RC	Registration centre
MS	Master Server
AS	Authentication Server
U_i	*ith* user
k	Secret key of RC
F_p	A finite field of order p
E_p	A non-singular elliptic curve over a field $GF(p)$
n, p	Large prime numbers
$H(\cdot)$	One way hash function
T	Identity verifier table
ID_i'	Identity of *ith* user
pw'	Password of *ith* user
B_i'	Biometric information of *ith* user
SC_i	Smart card of *ith* user
$REP(\cdot)/GEN(\cdot)$	Probabilistic generation function and deterministic reproduction function for the fuzzy extractor
$\oplus/\|\|$	XOR operator/Concatenation operator
$Z_n^*/Z_p^*/Z_k^*$	A plane of real integers
P_{pub}	Public key of the RC
SID_j	Identity of the *jth* server
$D_A(B)/E_A(B)$	Symmetric key decryption/encryption of B using the key A
r_i/r_j	An arbitrary integer
M_k/M_{pub}	Secret key and public key of the master server
M_a/M_b	Elliptic curve constants a and b for MS

password and the smart card details with complete independence [3].

The smart card-based password authentication scheme was put forth in 1999 itself [11]. It is after 1999, the researchers have been intensively attracted towards the smart card-based password authentication mechanism [12] due to the improved robust nature that is experienced over the sole password-based authentication mechanism [13]. Yet, the researchers of present day have concentrated much on the basic vulnerabilities that exist in the smart-card-based password authentication mechanism to support real-time applications [14]. Various numbers of works related to robustness improvement in the smart card-based-password authentication mechanism can be found in the literature in a span of last ten years [15–18]. One such is the work of Juang et al. [17], wherein the authentication procedure of the log-in phase in the smart-card-based password authentication scheme is performed swiftly through the inclusion of a pre-computation phase. Incorporation of the pre-computation phase has lessened the restrictions that are associated with the computational power, in addition to enhancing the authentication efficiency [17].

Previously, we have addressed the security challenges in the state-of-the-art authentication mechanism that uses a single server only. Hence, our previous article has introduced a dual stage biometrics-based password authentication mechanism using smart cards that use two servers for authentication. This paper enhances the security of the dual stage authentication mechanism further through establishing a secure server – server connection, so that the probability of compromising the server can be further reduced. The security enhancement is demonstrated using the security analysis of the proposed authentication scheme. The rest of the paper is organized as follows: Section 2 reviews the state-of-the-art authentication mechanisms that are reported in the literature and Section 3 distinguishes the existing single stage authentication mechanism and the proposed dual stage authentication mechanism. Section 4 explains the proposed authentication mechanism with secure server – server communication link and Section 5 performs the security analysis on the proposed scheme. Section 6 investigates the robustness of the proposed authentication scheme with as well as without secure server – server communication link and the single stage authentication mechanism. Section 7 concludes the paper with the possible future work.

2. Literature review

Li et al. [25,26] have made an attempt to put forth a dynamic identity-based authentication protocol, which is used in favour of smart card, in 2012 itself. Yet, Shunmuganathan et al. [24] have pinpointed few demerits in the dynamic identity-based protocols of [25,26] such as the susceptibility of the protocol towards forgery attack, offline password guessing attack, poor reparability and stolen smart-card attack. They have also dealt with a secure remote user authentication scheme, which is relevant to the multi-server environment. The uniqueness of their scheme is that the data contained in the smart card undergoes a logical way of security, in addition to preserving the identity's dynamicity through password randomization at all sessions. They have stated that their scheme exhibited improved robustness in opposing the replay attack, forgery attack, spoofing attack, offline-password guessing attack and stolen smart-card attack [24]. In 2012, Islam and Biswas have also suggested an enhanced scheme for password authentication and updation. But, their scheme was also adversely affected due to insider attacks, stolen-verifier and offline password guessing. Therefore, Li [27] has presented an advanced smart card-based password authentication and update scheme. Their scheme was an extended version of their previous work, rendering user privacy at a largely satisfactory level.

Though the previous works can be regarded as more viable to the security threats, a hard platform that performs cryptanalysis still exists. A small number of researchers have tried to offer benchmarks, which aid in characterizing the protocol's robust nature for protecting it from the security threats [2]. As an example, consider the work of Huang et al. [3]. They have examined the literature and discovered two probable adversaries, who know the pre-set data in the smart card as well as the data that continuously changes as time slots pass by. At last, they have suggested few ideas for tackling the security threats of similar kind during the execution of the smart card-based password authentication mechanisms. The prevailing authentication mechanisms are certainly improved due to their

Please cite this article in press as: M. Boopathi, M. Aramudhan, Secure server-server communication for dual stage biometrics – based password authentication scheme, Alexandria Eng. J. (2017), http://dx.doi.org/10.1016/j.aej.2017.01.031

investigation on the security threats. In the same way, Wang et al. [2] have accounted for the barriers that offer hindrance in achieving two-factor authentication schemes. Some other researchers have also given discussions on the security threats with regard to the three-factor authentication schemes. Yeh et al. [31] have made an analysis on the already available three-factor authentication schemes and suggested few issues that are related to privacy and lack of robustness against the insider attacks as well as the stolen – verifier attacks. They have put forward an authentication technique, which relies on the elliptic curve cryptography that exploits three-factor authentication for the biometric systems. Nevertheless, Yu et al. [30] have tried to overcome the issues concerned with the two-factor authentication scheme to propose a generic outline, supporting the three-factor authentication. Odelu [29] has put efforts to utilize up to seven factors for imparting an effective authentication scheme, which employs both the elliptic curve cryptography (ECC) and the biometrics – based smart card. They have examined the performance with respect to robustness and authenticity through the use of Burrows-Abadi-Needham (BAN) logic.

2.1. Security issues

The smart card-based password authentication mechanism supports a number of applications that include e-health, e-governance, e-commerce and e-banking. But, their liability to usability [9], privacy matters [8] and security threats [7] still persists. The passwords that are related to the smart cards can never be generated using tough entropy, as in the rest of the password authentication mechanisms [1,4]. Therefore, the smart card-based password authentication mechanism is restricted because of these reasons [20].

In the former researches, the authentication factor was set as one. But, numerous factors are considered in the researches of present day [29]. Further, the biometrics-based authentication mechanisms involve one authentication stage or employ one server alone. The total system will be subjected to destruction or security threats in such cases, if the adversary takes control over that particular single server. Usually, the communication is established in a distributed environment that contains more number of deregulated users. Hence, the chances for compromising the server are high.

3. Notable biometrics-based password authentication mechanism using smart cards

3.1. Single stage authentication mechanisms

He-Wang has introduced the most well-known single stage multi-server authentication protocol, which rely on both the smart card authentication and the biometrics password [32]. This protocol encloses a total of two phases. Registration of the users as well as the servers with the RC takes place in the initial phase. On the contrary, the second phase enables user login and user authentication from the server through the aid of RC. As a consequence, the sharing of keys among the server and the user happens to set up a most reliable and safer communication link. Therefore, the initial phase is termed as registration phase and the second phase is termed as login, authentication and key establishment phase. The complete discussion of the protocol is dealt in [32]. The protocol's security and key sharing are accomplished in [32] through the utilization of information hashing and ECC approaches. Though the biometrics-based login goes hand in hand with the smart card authentication and password login, the He-Wang's scheme is prone to severe attacks such as the known session – specific temporary information attack and the impersonation attack [29]. Therefore, Vanga Odelu et al. have tried to improvise the robustness against similar kind of well-known attacks. Odelu's scheme [29] involves a total of six phases, which are orderly initialization phase, registration phase, login phase, authentication and key establishment phase, password change phase and revocation and re-registration phase. The initialization phase characterizes the non-singular elliptic curve E_p over a finite field $GF(p)$, a secure one-way hash function $H(\cdot)$ that is devoid of collision and a symmetric key cryptosystem. It is the RC that makes a choice of the private key to decide on the public key, which is then publicly shared. The private key is always maintained secret. During the execution of the registration phase, the servers along with the users register to the RC with the help of the credentials such as user ID, server ID, password and biometric details of users. The RC carries out a small number of protective measures before storing their details in the identity verifier table T.

3.2. Dual stage authentication mechanisms

The dual stage authentication mechanism is found to own two stages of authentication, in accordance with its name. Hence, it differs from a single stage authentication mechanism. As indicated in Fig. 1, the two-stage authentication is accomplished with the inclusion of two servers in the protocol. The literature strongly aids the notion of dual server to mitigate the attacks occurring due to the compromising of server, in addition to imparting improved robustness. For instance, Yang et al. [33] have pointed out few offline dictionary attacks influencing the single server-based authentication mechanism. In addition, they have stated the reasons for why the two server-based authentication mechanisms are necessitated. Moreover, they have concluded that the real-time applications cannot employ or function using multiple servers. Hence, two servers are employed. Usually, one server is to authenticate and the other is to control the remaining server. In our earlier work, we have introduced the dual stage authentication mechanism, which is an enhancement over the Vanga Odelu's scheme [29]. The phases involved in this work include initialization phase, registration phase, login phase and authentication and key establishment phase. This scheme is found to be devoid of password change phase as well as revocation and re-registration phase, since the main goal was to render improved robustness during authentication. The two servers that are deployed in our schemes have been named as the Master Server (MS) and the Authentication Server (AS). These servers, when employed, allow the total user communication to take place with complete control. During the execution of registration phase, the MS undergoes registration with the RC and maintains the credentials in a secret manner such that the AS is also not rendered with the details contained in MS. When considering the authentication and key establishment phase, two types of communication are established. One communication is set up between the MS and the AS as well as the

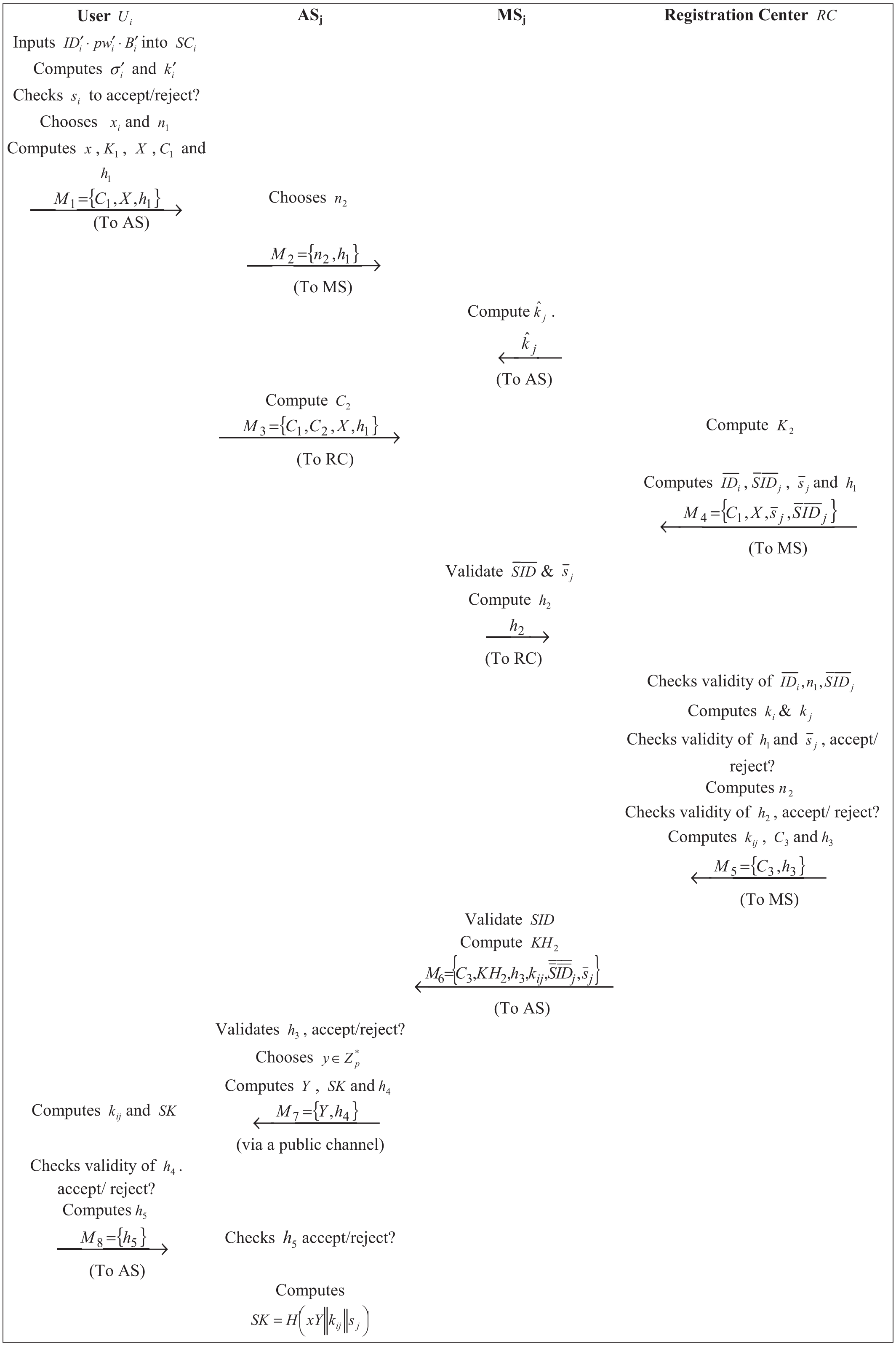
User U_i
AS$_j$
MS$_j$
Registration Center RC
Inputs $ID_i' \cdot pw_i' \cdot B_i'$ into SC_i
Computes σ_i' and k_i'
Checks s_i to accept/reject?
Chooses x_i and n_1
Computes x, K_1, X, C_1 and h_1
$M_1=\{C_1,X,h_1\}$
(To AS)
Chooses n_2
$M_2=\{n_2,h_1\}$
(To MS)
Compute $\hat{k}_j$.
$\hat{k}_j$
(To AS)
Compute C_2
$M_3=\{C_1,C_2,X,h_1\}$
(To RC)
Compute K_2
Computes $\overline{ID}_i$, $\overline{SID}_j$, $\bar{s}_j$ and h_1
$M_4=\{C_1,X,\bar{s}_j,\overline{SID}_j\}$
(To MS)
Validate $\overline{SID}$ & $\bar{s}_j$
Compute h_2
h_2
(To RC)
Checks validity of $\overline{ID}_i,n_1,\overline{SID}_j$
Computes k_i & k_j
Checks validity of h_1 and $\bar{s}_j$, accept/ reject?
Computes n_2
Checks validity of h_2, accept/ reject?
Computes k_{ij}, C_3 and h_3
$M_5=\{C_3,h_3\}$
(To MS)
Validate SID
Compute KH_2
$M_6=\{C_3,KH_2,h_3,k_{ij},\overline{\overline{SID}}_j,\bar{s}_j\}$
(To AS)
Validates h_3, accept/reject?
Chooses $y \in Z_p^*$
Computes Y, SK and h_4
Computes k_{ij} and SK
$M_7=\{Y,h_4\}$
(via a public channel)
Checks validity of h_4.
accept/ reject?
Computes h_5
$M_8=\{h_5\}$
(To AS)
Checks h_5 accept/reject?
Computes
$SK = H\left(xY \| k_{ij} \| s_j\right)$

Figure 1 The dual stage biometrics-based password authentication mechanism, without any secure server-server communication link.

RC. The other communication takes place among the AS and the user, the MS and the RC. Hence, no communication link is established directly from the MS to the user or vice versa. The adversarial nature of the channel can be tackled with this setup, since the AS is prevented from directly accessing the server details.

3.3. Single stage vs dual stage authentication mechanisms

The communication link that is established between the participants of single stage and dual stage authentication mechanism is illustrated in Fig. 2. In the single stage authentication mechanism, the server establishes both the transmitting and the receiving communication between the user and the RC. As a result, the server is vulnerable to attacks and it can be compromised by the servers. In the dual stage authentication mechanism, the AS communicates with the user and RC, whereas the MS communicates with the AS and the RC. Fig. 2 further infers that the MS is not permitted to communicate with the user and hence, it cannot be harmed by attackers. The AS is only permitted to send information to the RC and not to receive information from RC. Hence, a hacked AS cannot harm RC. However, our previous authentication scheme has initiated the authentication and key establishment phase by transmitting a sensible nonce n_2 from the AS to the MS that can be hacked, if the server – server communication link is weak. This issue is overcome in the proposed dual stage authentication mechanism by establishing a secure server – server communication link.

4. Secure server – server communication-enabled dual stage authentication mechanism

The proposed authentication mechanism resembles our previous dual stage authentication mechanism with a change in the message to be transmitted from the AS to the MS in the step AK1. Prior to the initiation of login, authentication and key establishment phase, a server link establishment phase is included to enable the message from step AK1 that is protected by ECC. The rest of the steps of login, authentication and key establishment phase, the initialization phase and the registration phase (see Fig. 3) are similar with those of our previous scheme. The server link establishment phase and the authentication phases are detailed below as per Fig. 4.

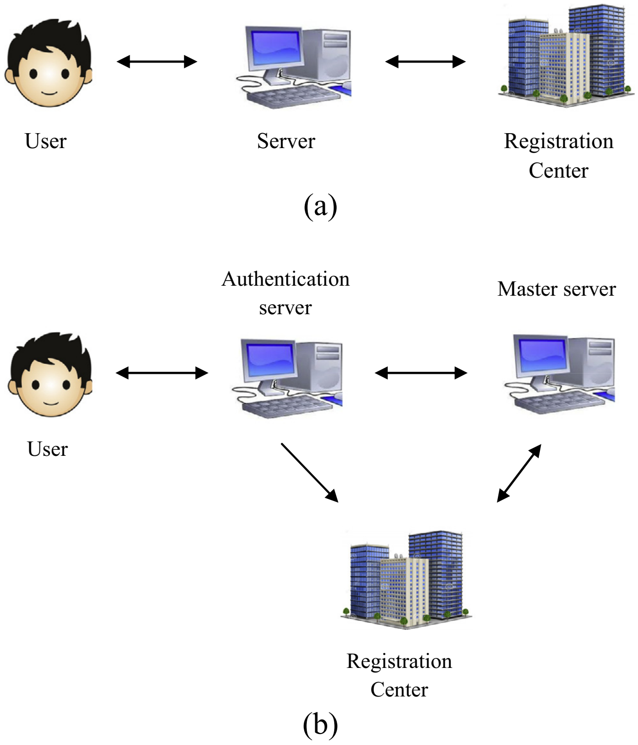

Figure 2 Communication links associated with (a) single stage authentication mechanism and (b) dual stage authentication mechanism.

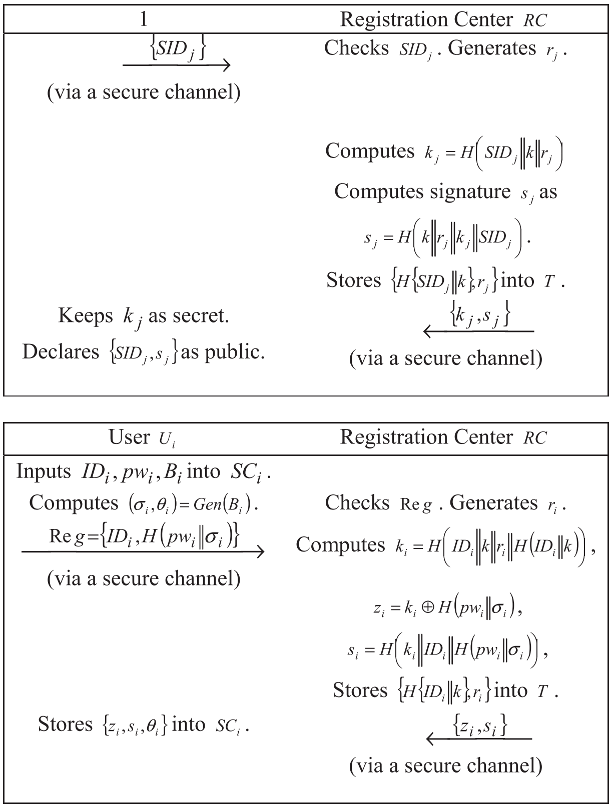
1
Registration Center RC
$\{SID_j\}$
(via a secure channel)
Checks SID_j. Generates r_j.
Computes $k_j = H\left(SID_j \| k \| r_j\right)$
Computes signature s_j as
$s_j = H\left(k \| r_j \| k_j \| SID_j\right)$.
Stores $\{H\{SID_j \| k\}, r_j\}$ into T.
Keeps k_j as secret.
$\{k_j, s_j\}$
Declares $\{SID_j, s_j\}$ 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 $\mathrm{Re}\,g$. Generates r_i.
$\mathrm{Re}\,g = \{ID_i, H(pw_i \| \sigma_i)\}$
Computes $k_i = H\left(ID_i \| k \| r_i \| H(ID_i \| k)\right)$,
(via a secure channel)
$z_i = k_i \oplus H(pw_i \| \sigma_i)$,
$s_i = H\left(k_i \| ID_i \| H(pw_i \| \sigma_i)\right)$,
Stores $\{H\{ID_i \| k\}, r_i\}$ into T.
Stores $\{z_i, s_i, \theta_i\}$ into SC_i.
$\{z_i, s_i\}$
(via a secure channel)

Figure 3 User and MS registration with RC in the proposed scheme.

4.1. Server link establishment

The server link establishment initiates the process for establishing a secure communication link between the AS and the MS. In this process, the MS generates M_k from Z_k^* and performs the elliptic curve operation. The prime field is determined as E_p and it allows the selection of M_P and M_p. Elliptic curve multiplication is performed between M_k and M_P to determine M_{pub} such that $M_{pub} = M_k M_P$. The MS keeps M_k as its secret key and M_{pub} as its public key. Moreover, it discloses the elliptic curve parameters such as M_a, M_b, M_p and M_P to the AS via a secure channel.

4.2. User login

With user login, the user is facilitated to enter all the associated credentials of him/her to the AS using just two steps, as dealt in the login phase described in [29].

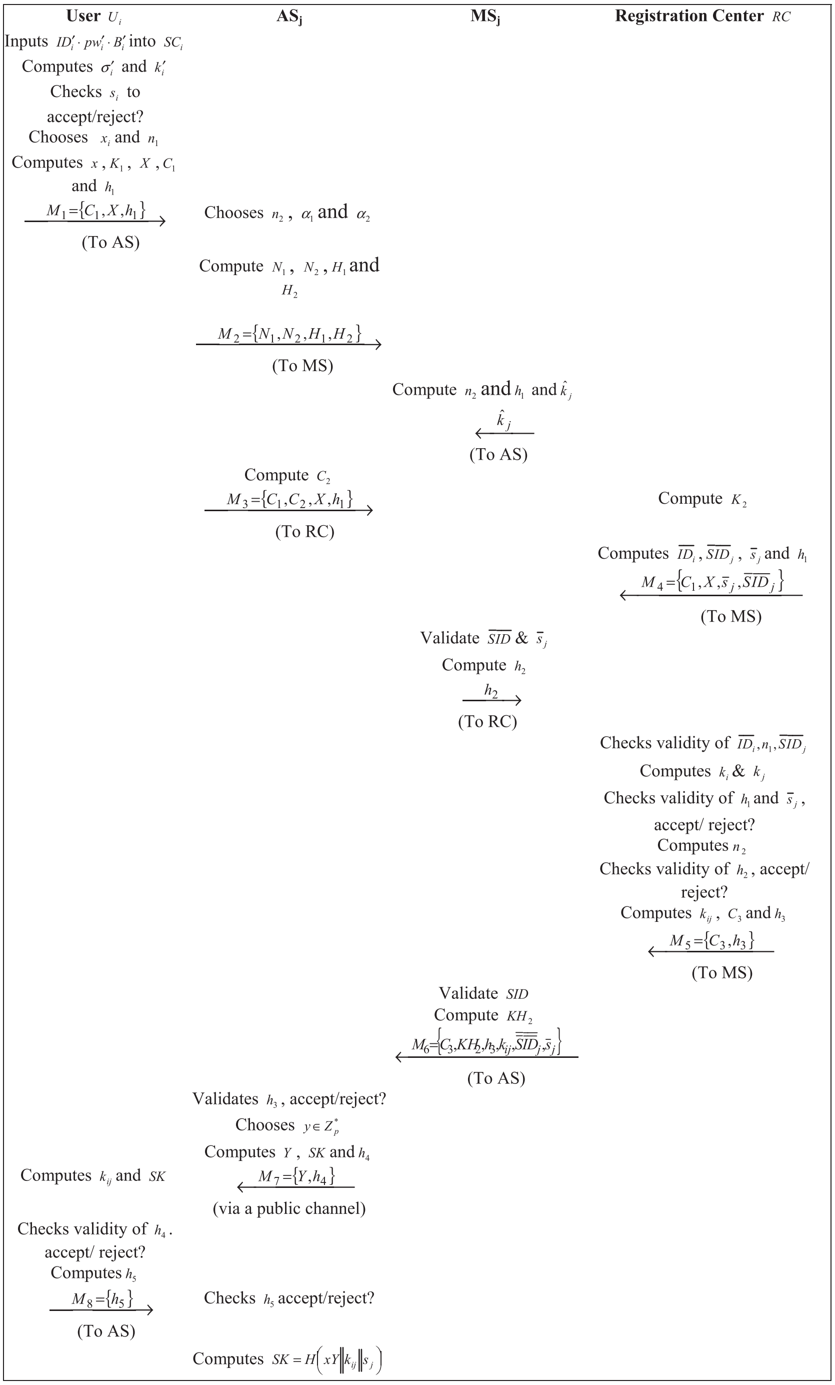
User U_i
$\mathrm{AS_j}$
$\mathrm{MS_j}$
Registration Center RC
Inputs $ID_i' \cdot pw_i' \cdot B_i'$ into SC_i
Computes σ_i' and k_i'
Checks s_i to accept/reject?
Chooses x_i and n_1
Computes x, K_1, X, C_1 and h_1
$M_1=\{C_1,X,h_1\}$
(To AS)
Chooses n_2, α_1 and α_2
Compute N_1, N_2, H_1 and H_2
$M_2=\{N_1,N_2,H_1,H_2\}$
(To MS)
Compute n_2 and h_1 and $\hat{k}_j$
$\hat{k}_j$
(To AS)
Compute C_2
$M_3=\{C_1,C_2,X,h_1\}$
(To RC)
Compute K_2
Computes $\overline{ID}_i$, $\overline{SID}_j$, $\bar{s}_j$ and h_1
$M_4=\{C_1,X,\bar{s}_j,\overline{SID}_j\}$
(To MS)
Validate $\overline{SID}$ & $\bar{s}_j$
Compute h_2
h_2
(To RC)
Checks validity of $\overline{ID}_i, n_1, \overline{SID}_j$
Computes k_i & k_j
Checks validity of h_1 and $\bar{s}_j$, accept/ reject?
Computes n_2
Checks validity of h_2, accept/ reject?
Computes k_{ij}, C_3 and h_3
$M_5=\{C_3,h_3\}$
(To MS)
Validate SID
Compute KH_2
$M_6=\{C_3,KH_2,h_3,k_{ij},\overline{\overline{\overline{SID}}}_j,\bar{s}_j\}$
(To AS)
Validates h_3, accept/reject?
Chooses $y \in Z_p^*$
Computes Y, SK and h_4
$M_7=\{Y,h_4\}$
(via a public channel)
Computes k_{ij} and SK
Checks validity of h_4. accept/ reject?
Computes h_5
$M_8=\{h_5\}$
(To AS)
Checks h_5 accept/reject?
Computes $SK = H(xY \| k_{ij} \| s_j)$

Figure 4 Proposed dual stage biometrics-based password authentication mechanism with secure server – server communication link.

Step L1: The user (U_i) places his/her smart card (SC_i) on a card reader and enters pw_i', ID_i' for imprinting the private biometrics B_i' at the sensor. As the next step, SC_i makes a computation of σ_i' and k_i' with the expressions in Eqs. (1) and (2), in a respective way. Subsequently, $H(k_i' \| ID_i' \| H(pw_i' \| \sigma_i'))$ and s_i that the smart card SC_i contains are tested for matching. A no match allows SC_i to discard all the credentials that are provided and causes the session to get ceased.

$$\sigma_i' = REP(B_i', \theta_i) \tag{1}$$

$$k_i' = z_i' \oplus H(pw_i' \| \sigma_i') \tag{2}$$

$$X = xP \tag{3}$$

$$K_1 = xP_{pub} \tag{4}$$

Step L2: Next, SC_i makes an arbitrary selection of the one-time secret $x_i \in Z_n^*$ along with an arbitrary nonce n_1. Prevention of the known session-specific temporary information attack is possible, if SC_i determines K_1 and X with the help of Eqs. (4) and (3), respectively.

Please cite this article in press as: M. Boopathi, M. Aramudhan, Secure server-server communication for dual stage biometrics – based password authentication scheme, Alexandria Eng. J. (2017), http://dx.doi.org/10.1016/j.aej.2017.01.031

In addition, these calculations employ x from Eq. (5), rather than utilizing the session random number x_i in a straightforward manner. Moreover, SC_i allows the computation of C_1 and h_1 through Eqs. (6) and (7), respectively. Here, K_{1x} stands for the x-coordinate of the ECC point K_1. In the end, U_i starts transmitting the message $M_1 = \{C_1, X, h_1\}$ to the server S_j by means of a public channel.

$$x = H(x_i \| k_i \| n_1) \tag{5}$$

$$C_1 = E_{K_{1x}} \lfloor ID_i, SID_j, s_j, n_1 \rfloor \tag{6}$$

$$h_1 = H(ID_i \| SID_j \| s_j \| n_1 \| k_i \| X \| K_1) \tag{7}$$

4.3. Authentication and key establishment

Step AK1: Once the AS receives M_1, it selects the nonce (n_2), α_1 and α_2 to compute N_1, N_2, H_1 and H_2 using Eqs. (8)–(11), respectively. Using these values, M_2 is constructed and forwarded to the MS. The various products that are involved include the following.

$$N_1 = \alpha_1 M_P \tag{8}$$

$$N_2 = n_2 + \alpha_1 M_{pub} \tag{9}$$

$$H_1 = \alpha_2 M_P \tag{10}$$

$$H_2 = h_1 + \alpha_2 M_{pub} \tag{11}$$

Step AK2: The MS receives N_1, N_2, H_1 and H_2 before determining n_2 and h_1 using Eqs. (13) and (15), respectively. In accordance with the value of h_1 and Eq. (16), the MS calculates the value of $\overset{\frown}{k}_j$. This obtained value of $\overset{\frown}{k}_j$ is then conveyed to the AS.

$$n'_2 = N_2 - N_1 M_k \tag{12}$$

$$n_2 = n'_{2x} \tag{13}$$

$$h'_1 = H_2 - H_1 M_k \tag{14}$$

$$h_1 = h'_{1x} \tag{15}$$

$$\overset{\frown}{k}_j = H(k_j \| h_1) \tag{16}$$

Step AK3: $\overset{\frown}{k}_j$ serves as the encryption key for the AS to perform encryption of the nonce n_2 and therefore, the computation of C_2 can be proceeded as stated below. The AS forms M_3 once again with the aid of C_1, C_2, h_1 and X before transmitting it to the RC.

$$C_2 = E_{\overset{\frown}{k}_j}(n_2) \tag{17}$$

Step AK4: With the details in M_3 and as per Eq. (18), the RC computes K_2. Later, Eq. (19) supports in the computation of $\overline{ID}_i, \overline{SID}_j, \bar{s}_j$ and n_1. As the next step, the RC forms M_4 through considering the values of $C_1, X, \bar{s}_j$ and $\overline{SID}_j$ before sending it to the MS.

$$K_2 = KX \tag{18}$$

$$[\overline{ID}_i, \overline{SID}_j, \bar{s}_j, n_1] = D_{K_{2x}}(C_1) \tag{19}$$

Step AK5: On receiving the $\overline{SID}_j$ and $\bar{s}_j$, the MS checks them against SID_j and s_j that reside in it, after the completion of the registration phase. Authentication of the AS and the establishment of communication will be achieved, only when there exists a matching between the parameters. The MS would then compute h_2 in accordance with Eq. (20) and transmits it to RC, immediately after the authentication of AS.

$$h_2 = H(C_1 \| X \| h_1 \| \overline{SID}_j \| k_j \| \bar{s}_j \| n_2) \tag{20}$$

Step AK6: In this step, a second stage validation on $\overline{SID}_j$ as well as $\bar{s}_j$ is accomplished for assuring the authenticity of MS. This validation procedure is carried out through ensuring whether $H(\overline{SID}_j \| k)$ exists in T or not. The presence of $H(\overline{SID}_j \| k)$ in T indicates a valid MS. Else, an invalid session is imagined to exist and the ceasing of the session takes place. In the same manner, the validation of the user is accomplished through the use of $H(\overline{ID}_i \| k)$. Existence of an authentic user as well as the MS allows the RC to compute k_i and k_j with the aid of Eqs. (21) and (22), respectively. Next, the RC performs the validation of h_1 and $\bar{s}_j$, as Eqs. (23) and (24) are satisfied in order. If the received h_1 and $\bar{s}_j$ succeeds the validation procedure, the RC uses Eq. (25) to compute n_2. Once again the received h_2 undergoes validation using Eq. (26) and supports in the computation of k_{ij} using Eq. (27). Depending on k_{ij} and using Eqs. (28) and (29), the computation of C_3 and h_3 takes place in a respective manner. Later, these values help in the construction of the message M_5 that is to be transmitted to the MS.

$$k_i = H(\overline{ID}_i \| k \| r_i \| H(ID \| k)) \tag{21}$$

$$k_j = H(\overline{SID}_j \| k \| r_j) \tag{22}$$

$$h_1 = H(\overline{ID}_i \| \overline{SID}_j \| \bar{s}_j \| n_1 \| k_i \| X \| k_2) \tag{23}$$

$$\bar{s}_j = H(k \| r_j \| k_j \| \overline{SID}_j) \tag{24}$$

$$n_2 = D_{H(k_j \| h_1)}(C_2) \tag{25}$$

$$h_2 = H(C_1 \| X \| h_1 \| \overline{SID}_j \| K_j \| s_j \| n_2) \tag{26}$$

$$k_{ij} = H(k_i \| K_2 \| n_1) \tag{27}$$

$$C_3 = E_{H(k_j \| h_1 \| n_2)}[\overline{SID}_j \| k_{ij}] \tag{28}$$

$$h_3 = H(k_j \| h_2 \| C_3 \| SID_j \| k_{ij} \| X \| \| s_j \| n_2) \tag{29}$$

Step AK7: The validation of $\overline{SID}_j$ is once more done through the computation of $\overline{\overline{SID}}_j$ in accordance with Eq. (30). Then, the matching between $\overline{SID}_j$ and the stored $\overline{SID}_j$ is analysed to authenticate the AS, paving way for any adversary attacks to be prohibited. If a valid $\overline{SID}_j$ is encountered, the MS forms M_6 with $C_3, h_3, k_{ij}, \overline{\overline{SID}}_j, \bar{s}_j$ and KH_2 and conveys it to the AS. Computation of $\overline{\overline{SID}}_j, k_{ij}$ and KH_2 is made as per Eqs. (30)–(32), in order.

$$\overline{\overline{SID}}_j = D_{H(k_j \| h_1 \| n_2)}(C_{3x}) \tag{30}$$

$$k_{ij} = D_{H(k_j \| h_1 \| n_2)}(C_{3y}) \tag{31}$$

$$KH_2 = (k_j \| h_2) \tag{32}$$

Please cite this article in press as: M. Boopathi, M. Aramudhan, Secure server-server communication for dual stage biometrics – based password authentication scheme, Alexandria Eng. J. (2017), http://dx.doi.org/10.1016/j.aej.2017.01.031

Step AK8: The AS performs validation of h_3 yet again with the help of Eq. (33). Once h_3 is valid, Y, SK and h_4 can be found as stated in Eq. (34)–(36). Then, the AS utilizes Y and h_4 to form the message M_7 for transmitting it to the user.

$$h_3 = H(KH_2\|C_{3X}\|C_{3Y}\|\overline{SID}_j\|K_{ij}\|X\|n_2) \tag{33}$$

$$Y = yP \tag{34}$$

$$SK = H(yX\|k_{ij}\|s_j) \tag{35}$$

$$h_4 = H(\overline{SID}_j\|s_j\|h_1\|k_{ij}\|X\|Y\|SK) \tag{36}$$

Step AK9: The user achieves the computation of k_{ij} as stated in Eq. (37) and confirms whether h_4 is valid or not by exploiting Eq. (36). On finding a valid h_4, the user uses Eq. (38) to calculate h_5 and transmits it as the message M_8 to the AS.

$$k_{ij} = H(k_i\|K_1\|n_1) \tag{37}$$

$$h_5 = H(SID_j\|k_{ij}\|X\|Y\|SK) \tag{38}$$

Step AK10: Eventually, the AS uses Eq. (38) for checking the received h_5 to finalize the key SK that is given as follows:

$$SK = H(xY\|k_{ij}\|s_j) \tag{39}$$

5. Security analysis

5.1. Collision attack

Generally, the collision attack attempts to produce an input that can result in a hash value corresponding to another input. Under such circumstances, both the single stage authentication mechanisms and our dual stage authentication mechanism are vulnerable to the security threats. For instance, h_1 of login phase, h_2, h_3, h_4 and h_5 of authentication and key establishment phase can be determined without knowing the hashing message. Since we mainly focus on the security threats between the AS and the MS, we investigate the possibility of avoiding collision attack between the server links. So, the AS encrypts h_1 using ECC and sends to the MS. Though h_1 is a hashed message, it has been encrypted as curve points to avoid the collision attack. Since h_1 is forwarded to the MS by the AS in our previous scheme, collision attacks can easily occur.

5.2. Chosen – prefix collision attack

It is a variant of collision attack through which a similar hashed message can be obtained from the concatenated two hashing messages, when either of the prefixes is known. For instance, $h_1 = H(\overline{ID}_i\|\overline{SID}_j\|\bar{s}_j\|n_1\|k_i\|X\|k_2)$ can be obtained by just knowing any of the concatenated messages, let us say n_1. Hence, the insecure server – server link can be vulnerable to this variant of collision attack too. In the proposed scheme, there is no hashed message to be transferred from the AS to the MS in Step AK1.

5.3. Other attack models

Similar to our previous scheme, the current scheme is also robust against the known plaintext attack (KPA), the chosen – plaintext attack (CPA), the chosen cipher text attack (CCA1) and the adaptive chosen cipher text attack (CCA2). The KPA [35] of the proposed scheme is handled by leaving the computation of C_2 and h_2 to the MS. Since $\widehat{k}_j$ is unavailable in step AK1, the CPA is successfully weakened in the proposed scheme.

C_3 of the proposed authentication scheme is not prone to CCA1 and CCA2 due to the decryption process and server validation. As the property of [29] is derived in the proposed authentication mechanism, it is found to be robust against few other attack models such as server spoofing, stolen verifier attack, known session-specific temporary information attack, reply attack, impersonation attack and man-in-the-middle attack.

6. Performance analysis

6.1. Robustness

The level of security is examined here to reveal out the proposed scheme's robustness in tackling the collision attacks and four other familiar attacks such as CCA2, CPA, KPA and CCA1 [35]. Usually, the proposed scheme imparts improved robustness against guessing attack, privileged insider attack, stolen verifier attack, password server spoofing, reply attack, known session-specific temporary information attack, man-in-the-middle attack and impersonation attack. Table 1 summarizes the robustness that the proposed scheme offers against such type of attacks through making a comparison with He-wang's scheme [32], Vanga Odelu's scheme [29] and our prior scheme. Our earlier scheme does not have secure link between the AS and the MS, whereas such secure link has been established in the proposed scheme. As per Table 1, no scheme is found to fail in rendering robustness against privileged password guessing attack, insider attack, stolen verifier attack, server spoofing attack and man-in-the-middle attack. The two proposed schemes of ours that involve and do not involve a secure server link and Vanga Odelu's scheme [29] impart increased robustness against the impersonation attack, known as the session-specific temporary information attack, and the reply attack. On the contrary, He-wang's scheme suffers greatly due to these attacks [29]. When considering the attacks such as CCA1, KPA, CPA and CCA2, high level of robustness was achieved only with our schemes. On the other hand, the remaining two schemes were found to exhibit higher vulnerability towards the security threats. Our scheme with a secure server – server link is found to be robust against the collision attacks, whereas the rest of the schemes are vulnerable.

6.2. Security features

The analysis on robustness is alone not sufficient. A small number of other features are to be considered to validate the supremacy of the proposed scheme over the traditional schemes as well as our prior scheme that does not incorporate a secure server-server link. Table 2 compares the features that are related to the proposed scheme against that of the previously available schemes. In the proposed protocol, the validation of the server identities was made four times for making sure that the server is free from any sort of hacking. Of these

Please cite this article in press as: M. Boopathi, M. Aramudhan, Secure server-server communication for dual stage biometrics – based password authentication scheme, Alexandria Eng. J. (2017), http://dx.doi.org/10.1016/j.aej.2017.01.031

Table 1 Robustness of the proposed scheme, our previous scheme and the conventional schemes against various attack models.

Attack models	He-Wang's scheme [31]	Vanga Odelu's scheme [29]	Proposed scheme	
			Without secure server-server link	WITH secure server-server link
Server spoofing attack	Yes	Yes	Yes	Yes
Stolen verifier attack	Yes	Yes	Yes	Yes
Privileged insider attack	Yes	Yes	Yes	Yes
Password guessing attack	Yes	Yes	Yes	Yes
Man-in-the-middle attack	Yes	Yes	Yes	Yes
Known session-specific temporary information attack	No	Yes	Yes	Yes
Impersonation attack	No	Yes	Yes	Yes
Reply attack	No	Yes	Yes	Yes
KPA	No	No	Yes	Yes
CPA	No	No	Yes	Yes
CCA1	No	No	Yes	Yes
CCA2	No	No	Yes	Yes
Collision attack	No	No	No	Yes
Chosen – prefix collision attack	No	No	No	Yes

Table 2 Comparison of security features between the proposed scheme, our previous scheme and the conventional schemes.

Security features	He-Wang's scheme [31]	Vanga Odelu's scheme [29]	Proposed scheme	
			Without secure server-server link	With secure server-server link
Provides mutual authentication	Yes	Yes	Yes	Yes
Provides perfect forward secrecy	Yes	Yes	Yes	Yes
Requires identity-verification table	No	Yes	Yes	Yes
Provides strong user anonymity	No	Yes	Yes	Yes
Provides SK-security	No	Yes	Yes	Yes
Multi-stage server validation	No	No	Yes	Yes
Protection against server compromise	No	No	Yes	Yes
Server credential protection	No	No	Yes	Yes
Secure server link	No	No	No	Yes
Protection against hashing function	No	No	No	Yes

four validations, the RC involves two validations for validating the AS as well as the MS. The remaining two validations are performed in the MS to check the AS. Consequently, the MS or the RC can itself decide whether the server is compromised or suffering from attacks. In Vanga Odelu's scheme, the validation of the server identity is achieved single time. On the contrary, He-Wang's scheme never does any such validation. So, the traditional authentication schemes would certainly fail to detect the server compromise or attacks. In the proposed scheme, the MS only contains the user credentials. In addition, the user is prohibited from communicating with the MS directly and the MS performs user authentication via the AS only.

Hence, the server attacks, which are caused through unprotected channel that exists between the server and the user, are greatly reduced. The credentials are maintained with improved security in the MS, though the AS is prone to attacks. The RC detects any sort of hacking in the MS and prevents the connection establishment of the AS with it or the MS. Therefore, the proposed scheme can afford improved safety towards the user credentials without server compromise. Though the server credentials remain secure, a vulnerable link can demolish the security of the protocol. This problem can be overcome in the proposed scheme with secure server – server link by exploiting the ECC concepts. As a result, the security of the server – server link has been ensured. Moreover, adequate protection has been given to the hashed message of step AK1.

6.3. Computational complexity

As per [34], a one-way hash function, a symmetric key encryption/decryption process and an elliptic curve point scalar multiplication roughly take about 0.0023 ms, 0.0046 ms and 2.226 ms, in order. The comparison of the computational costs of the traditional schemes against the proposed scheme has been made in accordance with it and is listed in Table 3. The complexity analysis reveals a non-satisfactory performance of the proposed scheme with secure server – server link because it has consumed 22.37 ms, which is higher than all the authen-

Table 3 Comparison of computing costs incurred by the proposed scheme and the conventional schemes.

Security operations	He-Wang's scheme [31]				Vanga Odelu's scheme [29]				Proposed scheme with secure server – server link					Proposed scheme with secure server – server link				
	User (U_i)	Server (S_j)	RC	Execution Time (ms)	User (U_i)	Server (S_j)	RC	Execution Time (ms)	User (U_i)	AS	MS	RC	Execution Time (ms)	User (U_i)	AS	MS	RC	Execution Time (ms)
Elliptic curve scalar multiplication	3	3	2	17.81	3	2	1	13.36	3	2	0	1	13.36	3	4	2	1	22.26
One way hash function	7	5	9	0.05	7	6	11	0.06	9	4	2	18	0.08	9	4	2	18	0.08
Symmetric key encryption/decryption	–	–	–	–	1	2	3	0.03	1	1	1	3	0.03	1	1	1	3	0.03
Total time (ms)	6.69	6.69	4.47	17.86	6.70	4.45	2.27	13.45	6.7	4.47	0.01	2.28	13.47	6.7	8.92	4.46	2.28	22.37

tication schemes. However, the security concern is considered seriously because the hashing function plays a key role in all the authentication mechanisms. From Table 3, it is evident that the proposed schemes perform 33 hashing functions, the Vanga Odelu's scheme [29] performs 24 hashing functions and the He-wang's scheme [32] performs 21 hashing functions. The role of hashing functions in the authentication schemes is higher than any other security functions. While the collision attack takes place, other schemes become prone to them. In contrast, the proposed scheme is robust against the collision attacks, though the computational complexity resulting from the usage of ECC is more.

7. Conclusion and future work

This paper has attempted to establish a secure connection between the dual servers, which are associated with our previous dual stage biometrics-based password authentication mechanism using smart cards. Since the collision attacks break the security of the hashed messages that are to be transferred between the AS and the MS, the proposed secure connection establishment process has deployed the ECC-based cipher texts. As a result, the proposed dual stage authentication mechanism has become robust against such collision attacks. This has been demonstrated in the security analysis. The proposed authentication mechanism has also been proved for its security over the server-server communication link, privacy for server credentials and challenges that are posed for server compromise. Yet, the computational complexity of the proposed scheme with secure server – server communication link has been found to be higher than that experienced in our previous dual stage authentication as well as the conventional single stage authentication mechanisms. Hence, the future work is focussed towards reducing the computational complexity, without compromising the security against the collision attacks.

References

[1] Hung-Min Sun, Yao-Hsin Chen, Yue-Hsun Lin, OPass: a user authentication protocol resistant to password stealing and password reuse attacks, IEEE Trans. Inform. Forensics Secur. 7 (2) (2012) 651–663.

[2] Ding Wang, Debiao He, Ping Wang, Chao-Hsien Chu, Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment, IEEE Trans. Dependable Secure Comput. 12 (4) (2015) 428–442.

[3] Xinyi Huang, Xiaofeng Chen, Jin Li, Yang Xiang, Xu Li, Further observations on smart-card-based password-authenticated key agreement in distributed systems, IEEE Trans. Parallel Distrib. Syst. 25 (7) (2014) 1767–1775.

[4] L. Lamport, Password authentication with insecure communication, Commun. ACM 24 (11) (1981) 770–772.

[5] K.K.R. Choo, C. Boyd, Y. Hitchcock, The importance of proofs of security for key establishment protocols: formal analysis of Jan-Chen, Yang-Shen-Shieh, Kim-Huh-Hwang-Lee, Lin-SunHwang, and Yeh-Sun protocols, Comput. Commun. 29 (15) (2006) 2788–2797.

[6] C. Lee, M. Hwang, I. Liao, Security enhancement on a new authentication scheme with anonymity for wireless environments, IEEE Trans. Ind. Electron. 53 (5) (2006) 1683–1687.

[7] M. Bond, O. Choudary, S. Murdoch, Chip and skim cloning EMV cards with the pre-play attack, in: Proc. IEEE S&P 2014, IEEE Computer Society, 2014, pp. 1–15.

[8] D. Wang, P. Wang, On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions, Comput. Netw. 42 (2014) 41–57.

[9] N. Gunson, D. Marshall, H. Morton, M. Jack, User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking, Comput. Secur. 30 (4) (2011) 208–220.

[10] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, Xuemin Shen, BECAN: A Bandwidth-Efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 23 (1) (Jan. 2012) 32–43.

[11] W.H. Yang, S.P. Shieh, Password authentication schemes with smart cards, Comput. Sec. 18 (8) (1999) 727–733.

[12] H. Chien, J. Jan, Y. Tseng, An efficient and practical solution to remote authentication: smart card, Comput. Sec. 21 (4) (2002) 372–375.

[13] W.C. Ku, S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 50 (1) (2004) 204–207.

[14] E.J. Yoon, E.K. Ryu, K.Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Trans. Consum. Electron. 50 (2) (2004) 612–614.

[15] C.I. Fan, Y.C. Chan, Z.K. Zhang, Robust remote authentication scheme with smart cards, Comput. Sec. 24 (8) (2005) 619–628.

[16] T.F. Cheng, J.S. Lee, C.C. Chang, Security enhancement of an IC-card-based remote login mechanism, Comput. Netw. 51 (9) (2007) 2280–2287.

[17] W.S. Juang, S.T. Chen, H.T. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron. 55 (6) (2008) 2551–2556.

[18] D.Z. Sun, J.P. Huai, J.Z. Sun, J.X. Li, J.W. Zhang, Z.Y. Feng, Improvements of Juang's password-authenticated key agreement scheme using smart cards, IEEE Trans. Ind. Electron. 56 (6) (2009) 2284–2291.

[19] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H. Deng, A generic framework for three-factor authentication: preserving security and privacy in distributed systems, IEEE Trans. Parallel Distrib. Syst. 22 (8) (2011) 1390–1397.

[20] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.

[21] N. Saxena, N.S. Chaudhari, EasySMS: a protocol for end-to-end secure transmission of SMS, IEEE Trans. Inform. Forensics Sec. 9 (7) (2014) 1157–1168.

[22] M. Martinez-Diaz, J. Fierrez, Galbally, The DooDB graphical password database: data analysis and benchmark results, IEEE Access 1 (2013) 596–605.

[23] H. Nicanfar, P. Jokar, K. Beznosov, V.C.M. Leung, Efficient authentication and key management mechanisms for smart grid communications, IEEE Syst. J. 8 (2) (2014) 629–640.

[24] S. Shunmuganathan, R.D. Saravanan, Y. Palanichamy, Secure and efficient smart-card-based remote user authentication scheme for multiserver environment, Can. J. Electr. Comput. Eng. 38 (1) (2015) 20–30.

[25] Y.X. Li, J. Ma Xiong, W. Wang, An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards, J. Network Comput. Appl. 35 (2) (2012) 763–769.

[26] Xiong Li, Jian Ma, Wendong Wang, Yongping Xiong, Junsong Zhang, A novel smart card and dynamic ID based remote user authentication scheme for multi-server environment, Math. Comput. Model. 58 (1–2) (2013) 85–95.

[27] Chun-Ta Li, A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card, IET Inf. Secur. 7 (1) (2013) 3–10.

[28] S.K. Hafizul Islam, G.P. Biswas, Design of improved password authentication and update scheme based on elliptic curve cryptography, Math. Comput. Model. 57 (11–12) (2013) 2703–2717.

[29] V. Odelu, A.K. Das, A. Goswami, A secure biometrics-based multi-server authentication protocol using smart cards, IEEE Trans. Inform. Forensics Sec. 10 (9) (2015) 1953–1966.

[30] Jiangshan Yu, Guilin Wang, Yi Mu, Wei Gao, An efficient generic framework for three-factor authentication with provably secure instantiation, IEEE Trans. Inform. Forensics Sec. 9 (12) (2014) 2302–2313.

[31] Hsiu-Lien Yeh, Tien-Ho Chen, Kuei-Jung Hu, Wei-Kuan Shih, Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data, IET Inf. Secur. 7 (3) (2013) 247–252.

[32] D. He, D. Wang, Robust biometrics-based authentication scheme for multiserver environment, IEEE Syst. J. (2014), http://dx.doi.org/10.1109/JSYST.2014.2301517.

[33] Yanjiang Yang, Robert H. Deng, Feng Bao, A practical password-based two-server authentication and key exchange system, IEEE Trans. Dependable Secure Comput. 3 (2) (2006) 105–114, http://dx.doi.org/10.1109/TDSC.2006.16. April-June.

[34] H. Kilinc, T. Yanik, A survey of sip authentication and key agreement schemes, IEEE Commun. Surv. Tutorials 16 (2) (2014) 1005–1023.

[35] Niels Ferguson, Bruce Schneier, Introduction to cryptography: attacks, in: Carol A. Long, Practical Cryptography (Hardcover ed.), Wiley Publishing Inc., 2003, pp. 30–32. ISBN 0-471-22894-X.

Please cite this article in press as: M. Boopathi, M. Aramudhan, Secure server-server communication for dual stage biometrics – based password authentication scheme, Alexandria Eng. J. (2017), http://dx.doi.org/10.1016/j.aej.2017.01.031