BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 68, No. 4, 2020
DOI: 10.24425/bpasts.2020.134470

Multi-factor signcryption scheme for secure authentication using hyper elliptic curve cryptography and bio-hash function

VANI RAJASEKAR[1]*, J. PREMALATHA[2], and K. SATHYA[3]

[1] Dept of CSE, Kongu Engineering College, Perundurai, Erode, India
[2] Dept of IT, Kongu Engineering College, Perundurai, Erode, India
[3] Dept of CT/UG, Kongu Engineering College, Perundurai, Erode, India

Abstract. Among rapid development of wireless communication, technology cryptography plays a major role in securing the personal information of the user. As such, many authentication schemes have been proposed to ensure secrecy of wireless communication but they fail to meet all the required security goals. The proposed signcryption scheme uses multi-factor authentication techniques such as user biometrics, smart card and passwords to provide utmost security of personal information. In general, wireless devices are susceptible to various attacks and resource constraint by their very nature. To overcome these challenges a lightweight cryptographic scheme called signcryption has evolved. Signcryption is a logical combination of encryption and digital signature in a single step. Thereby it provides necessary security features in less computational and communication time. The proposed research work outlines the weaknesses of the already existing Cao et al.'s authentication scheme, which is prone to biometric recognition error, offline password guessing attack, impersonation attack and replay attack. Furthermore, the proposed study provides an enhanced multi-factor authentication scheme using signcryption based on hyper elliptic curve cryptography and bio-hash function. Security of the proposed scheme is analyzed using Burrows-Abadi-Needham logic. This analysis reveals that the proposed scheme is computational and communication-efficient and satisfies all the needed security goals. Finally, an analysis of the study results has revealed that the proposed scheme protects against biometric recognition error, password guessing attack, impersonation attack, DoS attack and dictionary attack.

Key words: signcryption, bio-hash function, hyper elliptic curve, cryptanalysis, authentication.

1. Introduction

Remote user authentication [1] is one of the most sought-after security features of controlled applications such as banking transactions, e-Passport, e-Aadhar, e-Voting, IoT applications and military applications. The main demand of such applications includes elevated levels of security with user anonymity and sender privacy. To date, many authentication schemes have been proposed based on passwords, identity based authentication and traditional certificate based, authentication yet most of them fail to provide the required security features at better computational and communicational cost. Meanwhile, it has been identified from the literature that authentication schemes based on signcryption [2] provide less computational and communicational cost. Many signcryption techniques have been proposed based on RSA, ElGamal, Schnorr and elliptic curve cryptography for encryption as well as SHA and Keccak Hashing to generate digital signatures. The proposed signcryption scheme based on hyper elliptic curve cryptography (HECC) for encryption and bio-hash function to generate digital signatures plays a major role in cryptographic primitives because of its smaller key size as compared with that of other cryptographic algorithms.

Recently authentication schemes have been further classified into three major categories as knowledge based, object based and biometry based ones. Each category has its own pros and cons. Knowledge based authentication schemes are known for their simplicity, efficiency and ease of use, but they are sensitive to malicious attacks due to password adoption. Object based authentication uses smart card technology, which contains cryptographic information about the users. The main drawback of this scheme is that the adversary has a chance to impersonate the legitimate user when the smart card is lost. Biometry based authentication has become the focal point for many researchers because the biometric traits of the users, such as finger prints, facial features, palm prints, iris features and retina features cannot be lost or forgotten by the users. Hence it remains a secure and efficient way for providing security. The proposed authentication technique combines the smart card, biometrics and password to provide efficient security and to protect against different attacks. The biometric device used in the proposed research is NEC's "Bio-IDiom". It is one of the most accurate biometric authentication devices deployed worldwide.

The main contribution of this paper is as follows: Section 2 briefly describes the related works carried out in the field of authentication along with the proposed light weight cryptographic

*e-mail: vanikecit@gmail.com

Manuscript submitted 2019-12-24, revised 2020-03-28, initially accepted for publication 2020-04-28, published in August 2020

method signcryption and hash function. Section 3 briefly describes the methodology and flaws of Cao et al.'s [3] scheme. Section 4 and 5 then discuss the proposed multi-factor authentication technique based on signcryption with HECC and bio-hash function. Section 6 is mainly devoted to formal security analysis on the proposed scheme using Burrows-Abadi-Needham (BAN) logic. Section 7 compares the various security features and efficiency (both computational cost and communicational cost) of proposed schemes with some existing ones.

2. Related works

Amin et al. [4] developed a two-factor remote user authentication scheme based on RSA along with some mathematical operations such as $+$, $-$, $*$, %, /. From their results analysis, it has been identified that their schemes reduce computational and communicational cost by 40% but they fail to provide the necessary security features such as non-repudiation and forward secrecy, and they do not protect against password guessing attacks, dictionary attacks and impersonation attacks, either. A more recent signcryption technique which is based on elliptic curve cryptography (ECC) was developed by Baojun et al. [5]. It has been shown in their scheme that it has reduced computational and communicational cost by 50% as compared to signcryption which is based on RSA and Schnorr. However, from the results it has been identified that their scheme fails to provide forward secrecy and it is sensitive to dictionary attacks and impersonation attacks. The security requirement needed for generating digital signatures is to protect against the chosen cipher text attack (CCA). CCA is defined as the attack type in which the adversary has no knowledge about the cipher text but an n number of messages may be queried to the system in order to identify the cipher text. Protection against CCA attack is referred as non-malleability, i.e. if any adversary tries to modify the digital envelope, then the receivers should inform the sender about the attack that happens. The whole mechanism is defined by Zhang [6].

Wenbo et al. [7] developed a new authentication protocol for wireless sensor networks based on elliptic curve cryptography. Since sensor networks are limited by computing power, developing remote user authentication provides paramount security. Similarly, Choi and Lee [8] have developed enhanced multi-factor authentication based on the bio-hash function. From the literature study, it has been identified that their scheme is sensitive to the biometric recognition fault with a higher false acceptance rate, false rejection rate and equal error rate. The proposed scheme has analyzed and identified that, if signcryption is included in the authentication scheme with HECC and bio-hash function, it provides enhanced security as compared to that of existing schemes. The result analysis also reveals that the proposed scheme is computationally and communicationally efficient. Lu et al. [9] have identified that the Arshad et al. [10] scheme is vulnerable to offline password guessing attacks. It has also been shown that their scheme is vulnerable to impersonation attacks which cause the secret features of the user to be disclosed to the adversary. Lidong et al. [11] had proposed an efficient and secure three-factor based authenticated key exchange scheme using an elliptic curve cryptosystem. Although this scheme uses three-factor secure authentication strategy, it fails to avoid the biometric recognition error, masquerading attacks and mutual authentication.

Kamran et al. [12] identified the various levels of attacks that can be involved in the biometric system. They are: 1. Illegal interception of legitimate data and submission of data again to the user biometric system. 2. Fake biometric traits of the user presented to the system. 3. Feature extraction process circumvented by malicious codes that may replace legitimate features of user with fraudulent ones. 4. Fusion level or score level modified by intruder results in the increasing false acceptance rate (FAR) and false rejection rate (FRR), thereby reducing efficiency of the biometric system.

2.1. Usefulness of bio-hash function. The bio-hash function or symmetric hash function is defined as the hash function's certain class that is invariant to the order in which input pattern is given to the hash function. Thus the bio-hash function can overcome the biometric recognition error and is more advantageous than the traditional way of hash function. Sometimes the traditional hash function may be altered by the intruder. To overcome this risk, the proposed approach uses the bio-hash function which utilizes biometric traits of individuals. From the study it has also been identified that general hash function sometimes results in recognition error, and slight changes result in large differences in hash value. Novel technical characteristics are as follows:

1. Same biometric traits of user will have same hash output and varying biometric traits will never produce similar hash output
2. Partial biometric traits can be matched if they contain sufficient minutiae for matching even though it may have missing core and delta.
3. Any rotation and translation of original biometric template will never have any impact on output hash values.

2.2. Signcryption. The proposed signcryption scheme is based on hyper elliptic curve cryptography with bio-hash function to generate digital signatures. The hyper elliptic curve over genus $g \geq 2$ curve is given by Eq. (1).

$$y^2 + h(x)y = f(x) \bmod q\,, \tag{1}$$

where h(x) is a polynomial where the degree of $h(x) \leq g$ and $f(x)\varepsilon F[x]$ is a polynomial, which is known as a monic polynomial in general. The degree of f(x) should be less than or equal to $2g+1$. The Mumford representation of divisor D is represented in Eq. (2). HECC is more efficient than elliptic curve cryptography (ECC) because of its smaller key size, and it is more secure as it provides forward secrecy and all necessary security requirements.

$$D = (a(x), b(x)) = \left\{ \sum_{i=0}^{g} x^i a_i \sum_{i=0}^{g-1} x^i b_i \right\} \varepsilon j_c\left(F_q\right). \tag{2}$$

- Choose a large prime number q where $q > 2^{80}$.
- Consider C to be the hyper elliptic curve defined over prime field and specified as Fq.
- Choose a divisor D of large prime n, where $n \geq 2^{80}$.
- Let da be the private key of the sender where $da\varepsilon 0, 1, 2, \ldots, p-1$.
- Calculate public key of the sender as $p_a = d_a D$.
- Let db be the receiver's private key where $db\varepsilon 0,\ 1,\ 2,\ \ldots,\ p-1f$.
- Compute receiver's public key as $p_b = d_b D$.
- Consider m to be the secret message to be sent to the receiver.
- Let E_k and D_k denote encryption and decryption.
- Let the signcrypted tuple be (C, r, S).
- Let Bi be the biometric template of the user.
- Let $H_{Bi}(.)$ represent the bio-hash function.

A. Signcryption based on HECC and bio-hashing

- Select a random number k, where $k = 1, 2, 3, \ldots, n-1$.
- Calculate $k1 = H(kD)$.
- Calculate $k2 = H(kp_b)$.
- Let cipher text $C = E_{k2}(m)$.
- Let R be calculated by $R = H_{Bi}(m||k2)$.
- Calculate $S = (k/(R + d_a)) \bmod n$.
- Compute $r = RD$.
- The signcrypted tuple after this process is (C, r, S).

B. Unsigncryption based on HECC and bio-hashing

- Calculate $k1 = H_{Bi}(S(p_a + r))$.
- Calculate $k2 = H_{Bi}(S(d_b(p_a + r))$.
- Let m be identified by decryption as $m = D_{k2}(c)$.
- Compute R as $R = H_{Bi}(m||k2)$.
- Check $r = RD$ and if both are equal, accept the message or reject the message.

2.3. BAN logic. (Burrows-Abadi-Needham) BAN logic was first identified by Burrows et al. [13]. It is a set of rules for analyzing and defining the information exchange protocols. It helps users identify whether the information is exchanged in a trustworthy manner, secured against eavesdropping; it also helps eradicate vulnerability and tampering of information. It has noticeably drawn favorable attention of many researchers due to its simplicity of use and efficiency in formal analysis of various authentication schemes. The BAN logic includes three sequences: a) Verification of message origin; b) Verification of message freshness and c) Verification of the origin's trustworthiness.

3. Review of Cao et al.'s authentication scheme

The Cao et al.'s scheme is reviewed before cryptanalysis is conducted on their scheme. This scheme contains 3 phases: 1. Registration phase; 2. Password change phase and 3. Login and authentication phase. The parameter to be considered for the authentication scheme is given in Table 1.

Table 1
Notions and their descriptions

No.	Parameter used	Description
1	C_i	Client/User
2	S_i	Server/Receiver
3	Bi	Biometric template of client
4	Id_i	Client's identity
5	Pw_i	Client's password
6	$H_{Bi}(.)$	Bio-hash function
7	h(.)	General Keccak hash function
8	r_C	Random number generated by client
9	r_S	Random number generated by server
10	K_C	Secret key generated by client
11	K_S	Secret key generated by server
12	N_i	Counter number
13	t_i	Time stamp value of ith tuple
14	$\oplus$	Bitwise XOR operation
15	$\|\|$	Concatenation operator
16	(C, r, S)	Signcrypted tuple
17	bk	Session key used by client and server

A. Registration phase

In this phase, the client has to register with the server.

1. C_i selects Id_i, Pw_i, and imprints his own biometric template Bi to generate the secret key value K_C. The C_i sends the $(Pw_i \oplus K_C)$ and $(Bi \oplus K_C)$ to S_i through a secure communication channel.
2. S_i calculates $f_i = h(Bi \oplus K_C)$, $r_i = h(Pw_i \oplus K_C) \oplus f_i$ and $e_i = h(Id_i||K_S) \oplus r_i$.
3. Thus the server will make a new entry for the client with its Id_i, N_i, and $Ed_i = h(Id_i||N_i)$ in its database.
4. S_i calculates $v_i = h(Pw_i \oplus Bi||K_S)$.

The server sends a smart card to the client. It contains $< Ed_i, f_i, e_i, N_i, h(.) >$.

B. Password change phase

This phase is executed when C_i is in need of changing the password or when the user lost their smart card.

1. C_i submits Id_i, $(Pw_i \oplus K'_C)$, $(Bi \oplus K'_C)$ to S_i where K'_C is the newly generated random number for the client,
2. S_i calculates $v'_i = h(h(Pw_i) \oplus h(Bi) \oplus K_S)$ and compares v_i with v'_i. If they are not equal, then this phase will be terminated.
3. Otherwise, S_i computes $N_{i\,new} = N_i + 1$ and then computed the following:
   $f_{i\,new} = h(Bi \oplus K'_C)$,
   $r_{i\,new} = h(Pw_i \oplus K'_C) \oplus f_{i\,new}$ and
   $e_{i\,new} = h(Id_i||K_S) \oplus r_{i\,new}$.

4. The server will send a smart card to the client. It contains $< \mathrm{Ed_i}, \mathrm{f_{i\,new}}, \mathrm{e_{i\,new}}, \mathrm{N_{i\,new}}, \mathrm{h}(.) >$ and $\mathrm{C_i}$ stores the newly generated random number $\mathrm{K'_C}$ on the smart card.

C. Login and authentication phase

The steps involved where $\mathrm{C_i}$ starts logging in with $\mathrm{S_i}$

1. $\mathrm{C_i}$ imprints their biological information into the smart card and it computes $\mathrm{h(Bi \oplus K_C)}$ where $\mathrm{K_C}$ is stored on the client's smart card. $\mathrm{C_i}$ proceeds only if $\mathrm{h(Bi \oplus K_C)}$ matches $\mathrm{f_i}$.
2. $\mathrm{C_i}$ then assigns $\mathrm{Id_i}$ and $\mathrm{Pw_i}$ to the smart card, and it then computes the following:
   - $\mathrm{r_i = h(Pw_i \oplus K_C) \oplus f_i}$,
   - $\mathrm{m1 = e_i \oplus r_i}$,
   - $\mathrm{m2 = m1 \oplus r_c}$,
   - $\mathrm{m3 = h(m1 \| r_c)}$,
   - $\mathrm{Ed_i = h(Id_i \| N_i)}$.
3. $\mathrm{C_i}$ sends the login request $< \mathrm{Ed_i, m2, m3} >$ to $\mathrm{S_i}$.
4. $\mathrm{S_i}$ checks for $\mathrm{Ed_i}$ and $\mathrm{Id_i}$ in the database entry for authentication phase.
5. If $\mathrm{Id_i}$ is valid, then $\mathrm{S_i}$ computes the following:
   - $\mathrm{m4 = h(Id_i \| K_S)}$ and $\mathrm{m5 = m2 \oplus m4}$,
   - $\mathrm{m6 = m4 \oplus r_S}$ and $\mathrm{m7 = h(m4 \| r_S)}$.

   $\mathrm{S_i}$ sends $< \mathrm{m6, m7} >$ to $\mathrm{C_i}$.
6. $\mathrm{C_i}$ computes m8 and checks if $\mathrm{m7 = h(m1 \| m8)}$. If it is equal, $\mathrm{C_i}$ calculates m9.
   - $\mathrm{m8 = m6 \oplus m1}$ and $\mathrm{m9 = h(m1 \| r_C \| m8)}$,

   $\mathrm{C_i}$ sends $< \mathrm{m9} >$ to $\mathrm{S_i}$.
7. $\mathrm{S_i}$ receives $< \mathrm{m9} >$ and checks whether it is equal to m10. If it is, the login request is successful and $\mathrm{S_i}$ sends $< \mathrm{m10} >$ to $\mathrm{C_i}$
   - $\mathrm{m10 = h(m4 \| m5 \| r_S)}$.
8. on receiving $< \mathrm{m10} >$, $\mathrm{C_i}$ will verify $< \mathrm{m10} >$r with the following and will consider $\mathrm{S_i}$ as a legal server
   - $\mathrm{m10 = h(m1 \| m8 \| r_C)}$.

4. Cryptanalysis on Cao et al.'s authentication scheme

The proposed scheme has based cryptanalysis on Cao et al.'s scheme, which is specified as follows.

A. Offline password guessing attack

In Cao et al.'s scheme, offline password attack can be possible in the following cases. Let us assume that m2 and m3 are identified by the intruder and he can identify $\mathrm{f_i}$, K_c, h(.) and $\mathrm{e_i}$ from the stolen smart card. The attacker then identifies $\mathrm{m1 = (e_i \oplus r_i)}$, $\mathrm{m2 = (m1 \oplus r_c)}$ and $\mathrm{m3 = h(m1 \| r_c)}$. The value of m3 can also be identified as $\mathrm{m3 = h(e_i \oplus r_i \| m1 \oplus m2)}$. As $\mathrm{r_i}$ is already known to m3, it can be given as $\mathrm{m3 = h(e_i \oplus h(Pw_i \oplus K_C) \oplus f_i \| m1 \oplus m2)}$. In the above case, the attacker already knows all values except $\mathrm{Pw_i}$, whereas the attacker can easily identify $\mathrm{Pw_i}$ because of its low entropy.

B. Biometric recognition fault

In Cao et al.'s scheme, there is potential for biometric recognition fault due to usage of general hash function. In general hash technique, a small change in input results in great variation in output hash value. When users imprint their biometrics, there is a possibility of false acceptance rate (FAR) and false rejection rate (FRR), therefore when $\mathrm{C_i}$ inputs biometrics, there is a chance to generate false $\mathrm{Bi'}$. The false $\mathrm{Bi'}$ results in very large variation inf'_I, which causes the login phase to fail. Even though a legitimate user imprints their own biometrics, it results in biometric recognition fault.

C. Tracking attack

From the login message $< \mathrm{Ed_i, m2, m3} >$, $\mathrm{Ed_i}$ can be a fixed value for some smart cards. From the $\mathrm{Ed_i}$ it is easy to determine the value of $\mathrm{Id_i}$. An adversary can eavesdrop on the client login message $< \mathrm{Ed_i, m2, m3} >$ to obtain the login pattern and usage pattern of $\mathrm{C_i}$. Hence it is identified that Cao et al.'s scheme is sensitive to tracking attacks. Because of such attacks, it can never achieve user intractability.

D. Slow wrong password detection

It is defined as the process in which Cao et al.'s scheme is slow in detecting the wrong password. In this scheme, the smart card is not capable of identifying the wrong password entry when the user logs in. The wrong password can be detected only during the authentication phase when $\mathrm{S_i}$ verifies the similarities in m3 and $\mathrm{h(m4 \| m5)}$. Let us assume that $\mathrm{C_i}$ selects the wrong password $\mathrm{Pw'_i}$ where the smart card will never identify that this is a wrong password as it computes $< \mathrm{r'_i, m'2, m'3, m'1, Ed_i} >$. It sends the login message $< \mathrm{Ed_i, m'2, m'3} >$ to $\mathrm{S_i}$. Where $\mathrm{S_i}$ will not immediately identify the wrong password, first it checks for valid $\mathrm{Ed_i}$ then it computes $\mathrm{m4 = h(Id_i \| K_S)}$ and $\mathrm{m'5 = m'2 \oplus m4}$. Because m′3 is same as $\mathrm{h(m4 \| m'5)}$, $\mathrm{S_i}$ may eventually conclude that $\mathrm{C_i}$ has input the wrong password hence the slow wrong password detection time is more in Cao et al.'s scheme.

E. Client impersonation attack

In Cao et al.'s authentication scheme, $\mathrm{C_i}$ can be authenticated to $\mathrm{S_i}$ only by means of $\mathrm{Id_i}$ and smart card before accessing the biometrics of the user. From the public login message $< \mathrm{Ed_i, m2, m3} >$ an attacker can easily identify the $\mathrm{f_i}$, $\mathrm{K_c}$, h(.) and $\mathrm{e_i}$. The attacker computes $\mathrm{r_i = h(Pw_i \oplus K_C) \oplus f_i}$ from $\mathrm{Pw_i}$, $\mathrm{K_i}$, and $\mathrm{f_i}$. He impersonate the legitimate user without accessing the user's biometrics Bi and computes the following: $\mathrm{m1 = (e_i \oplus r_i)}$ and $\mathrm{m'2 = (m1 \oplus r'_c)}$ and $\mathrm{m'3 = h(m1 \| r'_c)}$. After $\mathrm{S_i}$ receives the login message $< \mathrm{Ed_i, m'2, m'3} >$, it checks the legitimacy but it cannot identify the forged m9 and original message m9 because the attacker computes $\mathrm{m9 = h(Id_i \| K_S)}$ using $\mathrm{r_i}$ and $\mathrm{e_i}$. $\mathrm{S_i}$ will send the $< \mathrm{Ed_i}$, m6, m7 $>$ to $\mathrm{C_i}$ which again is used by the adversary to compute $\mathrm{m8 = m6 \oplus m1}$ and if $\mathrm{m7 = h(m1 \| m8)}$ then $\mathrm{m'9 = h(m1 \| r_C \| m8)}$. In the next step $\mathrm{S_i}$ checks if the received m′9 is same as that of $\mathrm{m'10 = (m4 \| m'5 \| r_S)}$ whereas an attacker is not able to differentiate between m′9 and m9 because the attacker uses accurate values of $\mathrm{m1 = h(Id_i \| K_S)}$ and $\mathrm{r'_C}$ for calculating $< \mathrm{Ed_i, m'2, m'3} >$.

The attacker can be authenticated successfully by the server S_i due to the values of Ed_i, r_i, and e_i identified through a password guessing attack.

F. Server impersonation attack

C_i can be authenticated to S_i by means of $< Ed_i,\ m2,\ m3 >$. Let us assume that an attacker is intercepting this login message and calculates $m'6 = m'4 \oplus r_S$ and $m'7 = h(m'4 \| r_S)$. S_i then sends the $< m'6, m'7 >$ to C_i. It then computes $m'8$ and checks if $m7 = h(m1 \| m8)$. The attacker cannot differentiate between m7 and $m'7$ because of legitimate values used by the attacker. Therefore the adversary can be authenticated successfully to C_i which results in server impersonation attack. C_i then calculates m9 and sends to S_i which again continues to calculate m10 and finally the attacker will be completely authenticated to C_i.

G. Id guessing attack

Cao et al.'s scheme used Ed_i to protect the value of Id_i used in the login message. The attacker can guess the Id_i in two ways. From the stolen smart card, the attacker acquires the value of Ed_i from which the value of Id_i can be calculated as $Ed_i = h(Id_i \| N_i)$. From the above formula the attacker knows all the values except Id_i and due to the low entropy, Id_i can also be easily identified resulting in Id guessing attack.

H. Lack of session key agreement

Session key or symmetric key is generally used to establish secure communication between the authenticating parties. In Cao et al.'s authentication scheme C_i and C_i finally authenticate each other based on m9 and m10, where $m9 = h(m1 \| r_C \| m8)$ and $m10 = h(m4 \| m5 \| r_S)$. Secure communication is not established in this scheme because no session key is available in m9 and 10. To ensure high level of security for encryption in communication session, a session key is necessary. Hence the login and authentication phase should be modified in such a way as to include session key agreement.

I. Sensitivity to DoS attack

DoS attack is defined as the case where the attacker makes the network resource or service unavailable to legitimate users. There is vast possibility for DoS attack in Cao et al.'s authentication scheme. Consider a case where the attacker collects the previous login message $< Ed_i, m'2, m'3 >$ from C_i and sends it to S_i without any modification. S_i receives $< Ed_i, m'2, m'3 >$ and computes the value of m4, m5 and m6 without checking the freshness. S_i then sends the $< Ed_i, m6, m7 >$ to the attacker. With the help of this communication, the adversary can be able to conduct a DoS attack on the legitimate server resulting in legitimate user not being able to avail or use the resources.

5. Multi-factor authentication scheme based on signcryption

The proposed method includes 3 phases such as: 1. Registration phase; 2. Password change phase and 3. Login and Authentication phase.

A. Registration phase

C_i establishes communication with S_i using the secure channel, as shown in Fig. 1.

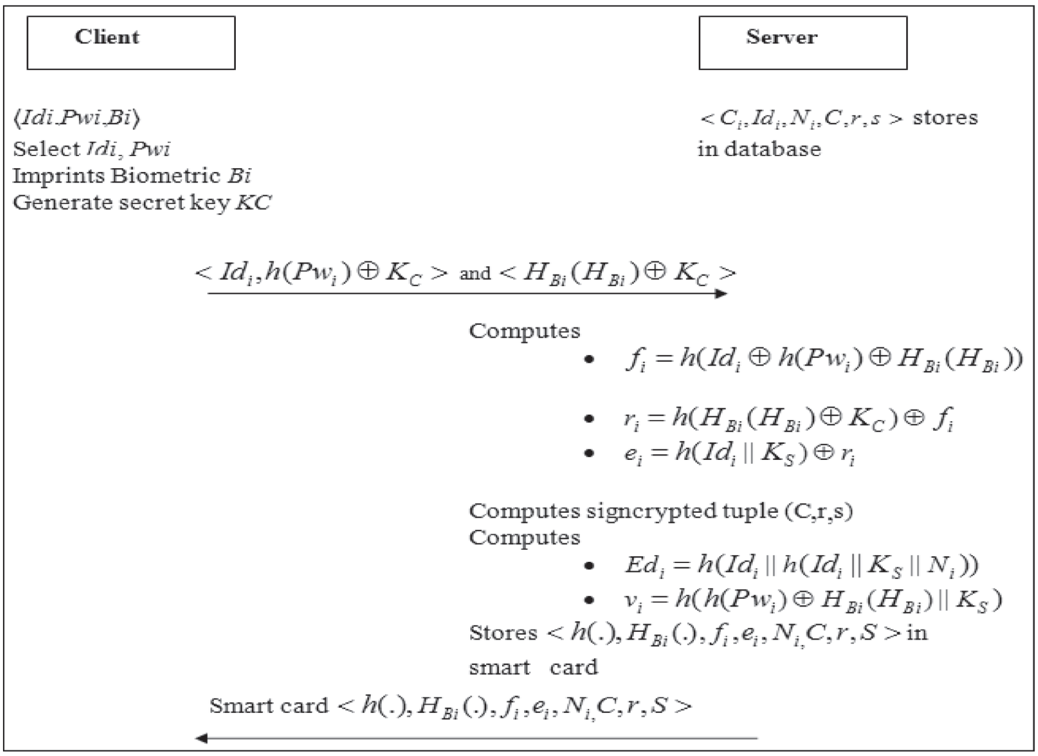

Fig. 1. Registration phase

Step 1: C_i choses Id_i, Pw_i, imprints the user biometric data Bi and then generates the secret key of client as K_C. It calculates $< Id_i, h(Pw_i) \oplus K_C >$ using general hash function. Then, by means of bio-hash function, it computes $< H_{Bi}(Bi) \oplus K_C >$ and sends to S_i using a secure communication channel.

Step 2: On receiving this, S_i computes the following:

- $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$,
- $r_i = h(H_{Bi}(Bi) \oplus K_C) \oplus f_i$,
- $e_i = h(Id_i \| K_S) \oplus r_i$.

Step 3: S_i also calculates the signcrypted tuples (C, r, S) for the given information from the C_i and it creates an entry and stores $< C_i, Id_i, N_i, C, r, S >$ in the database.

Step 4: S_i also computes the Ed_i as follows and stores it in the database for the corresponding C_i

- $Ed_i = h(Id_i \| h(Id_i \| K_s \| N_i)$,
- $v_i = h(h(Pw_i) \oplus H_{Bi}(Bi) \| K_s)$.

Step 5: S_i sends the smart card to C_i. The values in the smart card are $< h(.)$, $H_{Bi}(.)$, f_i, e_i, $N_i, C, r, S >$.

B. Password change phase

In the proposed method, this phase will be executed when the legitimate user's smart card is lost. In case of a need to change the password, the user has to send the old password Pw_i and new password $Pw_{i\,new}$. The flow of this process is described in Fig. 2.

Step 1: C_i selects Id_i, Pw_i, Pw_{inew} and the user imprints the biometric Bi and generates the new secret key of client as K'_C. It then calculates $< Id_i$, $h(Pw_i) \oplus K'_C >$, $< h(Pw_{i\,new}) \oplus K'_C >$, $< H_{Bi}(Bi) \oplus K'_C >$ and sends this newly calculated values to S_i.

Step 2: After receiving this, the server checks for all the entries of C_i in the database. It then computes $v'_i = h(h(Pw_i) \oplus H_{Bi}(Bi) \| K_s)$ and compares v_i with v'_i.

Step 3: S_i also calculates the signcrypted tuples (C, r, S) for the given information from the C_i and then it sets the $N_{i\,new} = N_i + 1$ and the remaining values are calculated:

- $f_{i\,new} = h(Id_i \oplus h(Pw_{i\,new}) \oplus H_{Bi}(Bi))$,
- $r_{i\,new} = h(H_{Bi}(Bi) \oplus K'_C) \oplus f_{i\,new}$,
- $e_{i\,new} = h(Id_i \| K_S) \oplus r_{i\,new}$.

Step 4: S_i also computes the Ed_{inew} as follows and stores it in the database for the corresponding C_i:

- $Ed_{i\,new} = h(Id_i \| h(Id_i \| K_s \| N_{i\,new})$.

Step 5: S_i sends the new smart card to C_i. The values in the smart card are $< h(.), H_{Bi}(.), f_{i\,new}, e_{i\,new}, N_{i\,new}, C, r, S >$.

C. Login and authentication phase

This phase is executed when C_i authenticates to server S_i, as shown in Fig. 3. In the login phase, the smart card checks the legitimacy of the user using Id_i, Pw_i and Bi. The login phase will be executed by C_i as follows.

Step 1: C_i inputs the Id_i, Pw_i; and imprints biometric Bi using any biometric device. It computes $h(Pw_i)$ using traditional hash function and computes $H_{Bi}(Bi)$ using bio-hash function. Then smart card verification will be performed as follows:

- $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$.

Step 2: If f_i is verified correctly by the smart card, C_i generates the value of timestamp as t_1 and generates a random number as r_C.

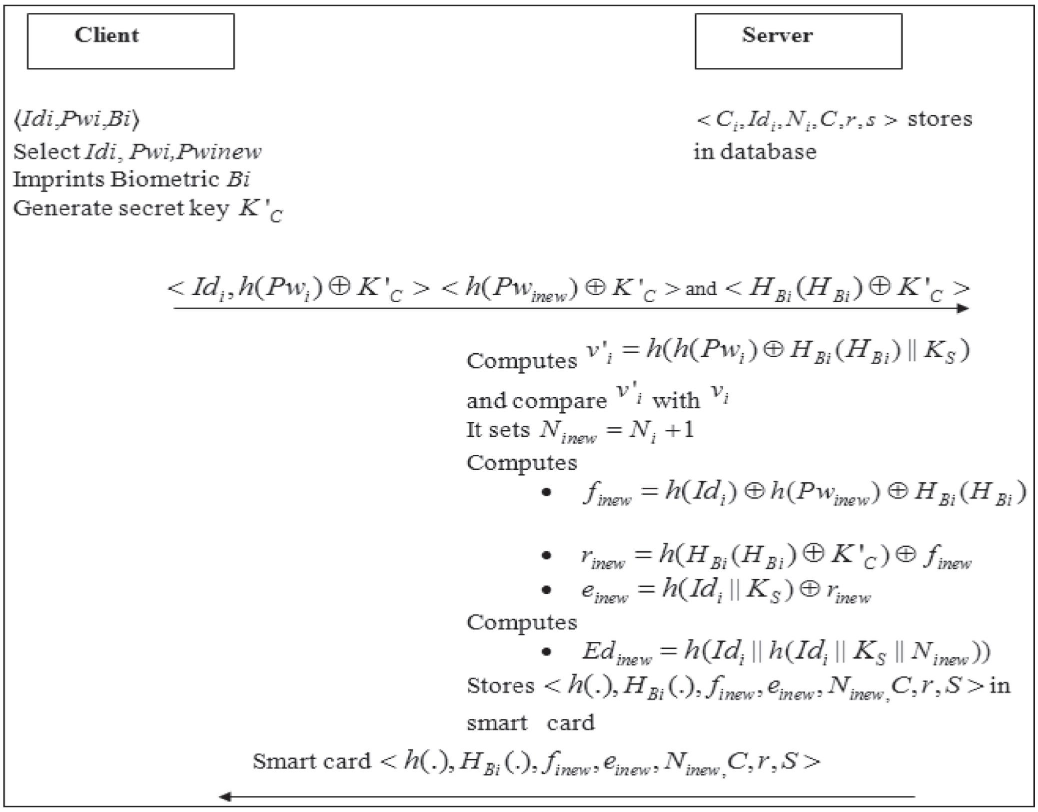

Fig. 2. Password change phase

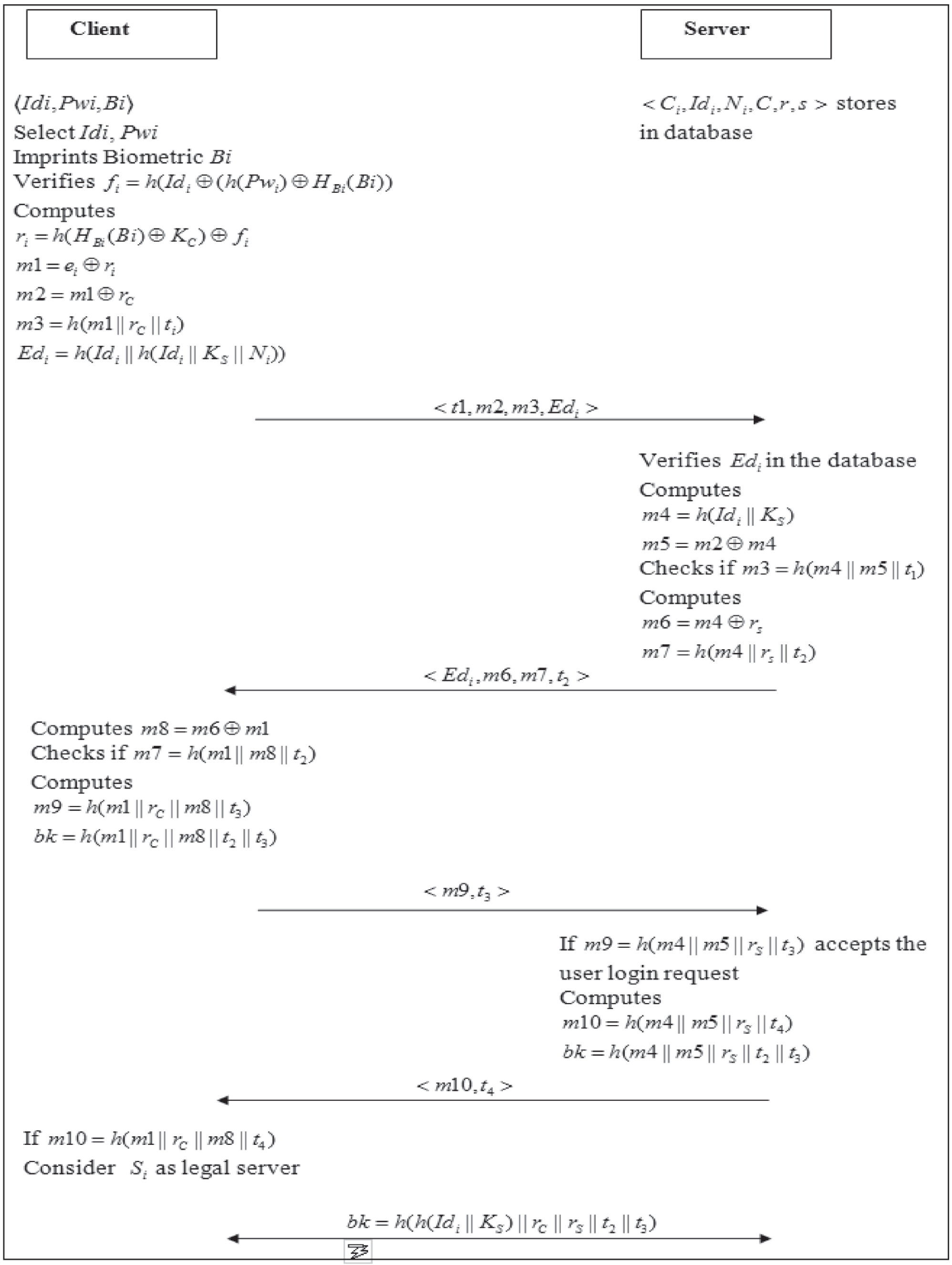

Fig. 3. Login and authentication phase

Then C_i computes the values of r_i, m1, m2, m3, Ed_i as follows:

- $r_i = h(H_{Bi}(Bi) \oplus K_C) \oplus f_i$,
- $m1 = e_i \oplus r_i$ and $m2 = m1 \oplus r_C$,
- $m3 = h(m1 \| r_C \| t_i)$,
- $Ed_i = h(Id_i \| h(Id_i \| K_s \| N_i)$.

Step 3: C_i sends the login request message $< t_1, m2, m3, Ed_i >$ to S_i. Once the login message is received from the client, S_i executes the authentication phase as follows.

Step 4: S_i checks for originality of Ed_i from the stored values in its database.

Step 5: If Ed_i is verified correctly, S_i computes m4 and m5 and verifies those against m3 as follows:

- $m4 = h(Id_i \| K_s)$,
- $m5 = m2 \oplus m4$ and $m3 = h(m4 \| m5 \| t_1)$.

Step 6: If the value of m3 is accurate, S_i calculates the current timestamp t_2 and then calculates m6 and m7. Then S_i sends the message $< Ed_i, m6, m7, t_2 >$ to C_i

- $m6 = m4 \oplus r_S$,
- $m7 = h(m4 \| r_S \| t_2)$.

Step 7: C_i computes $m8 = m6 \oplus m1$ and verifies with $m7 = h(m1 \| m8 \| t_2)$ or not. If it is verified, C_i generates time stamp value as t_3 and computes m9. C_i computes bk as follows:

- $m9 = h(m1 \| r_C \| m8 \| t_3)$,
- $bk = h(m1 \| r_C \| m8 \| t_2 \| t_3)$,

C_i sends $< m9,\ t_3 >$ to server S_i.

Step 8: On receiving the value of $< m9 >$, S_i verifies the value $m9 = h(m4 \| m5 \| r_S \| t_3)$ and if it is correct, user login request will be accepted. S_i computes m10, bk and sends $< m10, t_4 >$ to C_i

- $m10 = h(m4 \| m5 \| r_S \| t_4)$,
- $bk = h(m4 \| m5 \| r_S \| t_2 \| t_3)$.

Step 9: On receiving $< m10, t_4 >$, C_i will be checking that $m10 = h(m1 \| r_C \| m8 \| t_4)$ and will declare S_i as a legitimate server to communicate.

Step 10: Hence S_i and C_i shares the same session key for all the phases.

- $bk = h(h(Id_i \| K_S) \| r_C \| r_S \| t_2 \| t_3)$.

6. Result analysis on proposed scheme

Wang et al. [14–16] have proposed multiple methods based on smart card based authentication and introduced a secure scheme to prevent offline attacks. In the proposed scheme, secure authentication is established based on the bio-hash function, which is to resistant major attacks. Security of the proposed scheme is confirmed by various security analyses, formal verification and efficiency computation. The proposed scheme follows a well-defined security notation with stronger secret values (Bi, x). The secret values contain high entropy so that these values can never be guessed by the attacker in polynomial time.

A. Security analysis on proposed scheme

Security analysis of the proposed authentication scheme with other authentication schemes is defined in Table 2.

1. Server masquerading attack

Let us suppose that an attacker tries to masquerade a legitimate server. In order to do so, he must send a login request. Let us consider if C_i sends $< m9, t_3 >$ to the attacker, he must calculate $< m10, t_4 >$ to look like a legitimate server; whereas if an attacker needs to calculate $< m10, t_4 >$ from $< m9, t_3 >$, he must know r_C and $h(Id_i \| K_S)$. It is not possible for the attacker to find as it is stored in the database. Hence it is infeasible for the attacker to masquerade the legitimate server.

2. Replay attack

Let us suppose in the proposed scheme that an intruder intercepts the communicational messages $< t_1, m2, m3, Ed_i >$ and $< m9, t_3 >$ between C_i and S_i and replays the message $< t_1, m2, m3, Ed_i >$ to S_i. It is infeasible for the attacker to communicate with S_i within the timestamp t_1 as even if an attacker manages to pass timestamp t_1, he will not be able to generate response messages $< t_2, m6, m7, Ed_i >$. This is because the attacker knows the previous $< m9, t_3 >$, which will never be appropriate to calculate the response for the message $< t_2, m6, m7, Ed_i >$. Furthermore, the intruder needs to know r_C and $h(Id_i \| K_S)$, which is not possible for the attacker to find as it is stored in the database. Hence it is infeasible for the attacker to succeed in a replay attack.

3. Biometric recognition error

The concept called bio-hash function is introduced in the proposed scheme, which makes it impossible for biometric recognition errors to occur, whereas Cao et al.'s scheme uses the traditional hash function to validate the biometric traits of the user, which makes biometric recognition error occur in their scheme. The main advantage of using the bio-hash function is that it will produce more appropriate output for user biometric value even if the user provides slightly different input hash value.

4. Mutual authentication

This concept involves both the client C_i and server S_i mutually authenticating each other [17]. The proposed scheme enables C_i and S_i to mutually authenticate based on the mutual random number. In this case, only the legitimate C_i and S_i can authenticate because only they know the value of $h(Id_i \| K_S)$. The legitimate server communicates with legitimate

Table 2
Attack resistance of proposed scheme as compared with existing authentication schemes

Various attacks	Hwang et al. [18]	Xiang et al. [19]	Das et al. [20]	Cao et al. [3]	Kumar et al. [21]	Das et al. [22]	Proposed scheme
Server masquerading attack	Yes	Yes	Yes	No	Yes	Yes	No
Replay attack	No	No	No	No	No	No	No
Biometric recognition error	Yes	Yes	Yes	Yes	Yes	Yes	No
Mutual authentication	No	No	No	Yes	Yes	Yes	No
Client impersonation attack	Yes	No	No	Yes	Yes	Yes	No
Offline password guessing attack	Yes	No	No	Yes	Yes	Yes	No
Slow wrong password detection	Yes	Yes	Yes	Yes	No	No	No
Sensitivity to to DoS attack	Yes	Yes	Yes	Yes	Yes	Yes	No
ID guessing attack	Yes	Yes	Yes	Yes	Yes	Yes	No
Lack of session key agreement	Yes	Yes	Yes	Yes	No	No	No

client based on received $< m9, t_3 >$, and here only legitimate C_i can be able to calculate m9 using m6 received from S_i. Similarly, only a legitimate server can be able to calculate m10 from the received $< m9, t_3 >$ because only he knows the value of r_C and $h(Id_i \| K_S)$.

5. Client impersonation attack

To successfully execute a client impersonation attack, the intruder needs to know the value of $h(Id_i \| K_i)$. To compute $h(Id_i \| K_i)$, the attacker needs:

- $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$,
- $r_i = h(H_{Bi}(Bi) \oplus K_C) \oplus f_i$,
- $e_i = h(Id_i \| K_S) \oplus r_i$,

where r_i is protected inside the $h(H_{Bi}(Bi) \oplus K_C)$. From this, the attacker cannot be able to find the value of $H_{Bi}(Bi)$ hence it is infeasible for the attacker to execute a client impersonation attack.

6. Offline password guessing attack

It is possible for an attacker to gain all the information that is stored in the user's smart card by means of executing a side channel attack. In the proposed authentication mechanism the password will always be used with the value of Id_i and biometric traits of the user $H_{Bi}(Bi)$. The user's Id_i is always protected inside the $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$ and $Ed_i = h(Id_i \| h(Id_i \| K_s \| N_i)$ and also the user biometrics Bi has high entropy, which is impossible for the intruder to calculate. Hence from this analysis it is clear that even if the attacker executes a side channel attack to extract f_i, it is impossible for him to calculate Id_i and $H_{Bi}(Bi)$. Therefore with the proposed scheme it is impossible to execute a offline password guessing attack.

7. Slow wrong password detection

Cao et al.'s scheme checks the user password during the login and authentication phase whereas in the proposed scheme when the user is in need to authenticate, he has to give his Id_i, Pw_i, and Bi. With these values the smart card will compute $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$ and verify with f_i stored in the database. In case the user provides the wrong password Pw_i, the calculated f_i will vary from the f_i stored in the database. Hence it is easy for the user to identify the wrong password entry as it takes less time compared to the other authentication schemes.

8. Sensitivity to DoS attack

The time stamp values t_1, t_2, t_3, t_4 in the proposed scheme are used to check the freshness of all messages sent between C_i and S_i. The time stamp values make it difficult for the attacker to establish mutual authentication with the legitimate client and server. C_i and S_i use current time stamp values also in the communication specified as follows:

- $m3 = h(m4 \| m5 \| t_1)$,
- $m7 = h(m4 \| r_S \| t_2)$.

Similarly, m9 and m10 must also be computed as follows:

- $m9 = h(m1 \| r_C \| m8 \| t_3)$,
- $m10 = h(m4 \| m5 \| r_S \| t_4)$.

Let us consider a situation in which an attacker intercepts and replays the message m3 to S_i. It will check the freshness of the message received from the attacker using the timestamp value t_1, but that will never be equal to the current timestamp. Therefore the intruder can never be able to impersonate the legitimate client and server; hence the proposed scheme is more secure than Cao et al.'s scheme.

9. ID guessing attack

In Cao et al.'s scheme $Ed_i = h(Id_i \| N_i)$ whereas in the proposed scheme $Ed_i = h(Id_i \| h(Id_i \| K_s \| N_i)$. The proposed scheme protects the value of Id_i in EId_i from public communication. Let us consider a situation in which an attacker knows EId_i – he is still not able to identify Id_i from EId_i. Hence an ID guessing attack is not feasible in the proposed scheme.

10. Lack of session key agreement

Cao et al.'s scheme fails to establish the session key agreement between C_i and S_i. Hence there is no possibility for establishing secure communication between the communicating parties. To overcome this technical difficulties, the proposed scheme ensures the secure session key agreement and it is given by $bk = h(m4 \| m5 \| r_S \| t_2 \| t_3)$. All the values in the session key are computed by the legitimate client and server and for each time it is verified with the timestamp value for message freshness.

B. Formal analysis of proposed scheme

BAN logic in the proposed scheme considers A and B for representing principals and Q for representing the statements. BAN logic generally follows four steps in formal analysis.

1. Notations used for BAN logic

$A| \equiv P$: The principal A believes that statement P is true in the current run.

$A \triangleleft P$: The principal A sees the specified statement P which implies that A had received the message that contains P.

$A| \sim P$: The principal A has once said to the statement P which meant $A| \equiv P$ when A sent it.

$A \Rightarrow P$: The defined principal A has more jurisdiction over statement P. This implies that A has full control over the defined formula P.

#(P): Formula P is fresh, which means that P has not been used anywhere before.

$A| \equiv B \overset{k}{\longleftrightarrow} A$: Principal A believes that A and B communicate with each other using shared secret key k.

$A \overset{k}{\longleftrightarrow} B$: Secret key k is known only to A and B and it is used for communication only between A and B.

$\{P\}_k$: Formula P is encrypted with secret key k.

$< P >_k$: Formula P is combined with secret key k.

$(P)_k$: Formula P is hashed with secret key k.

bk: defines the session key of current session.

2. Rules for logical postulates of BAN logic

Belief rule: $\dfrac{A| \equiv P, A| \equiv Q}{A| \equiv (P, Q)}$ defines the assumption that principal A believes P and Q then it believes (P, Q).

Nonce verification rule: $\dfrac{A|\equiv \#(P), A|\equiv B|\sim Q}{A|\equiv B|\equiv P}$ defines the assumption that principal A believes P to be fresh and A also believes that B once said Q, then A believes B believes P.

Message meaning rule: $\dfrac{A|\equiv A \xleftrightarrow{k} B, A \triangleleft (P)_k}{A|\equiv B|\sim P}$ defines that if principal A believes that the secret key will be shared with B, then A will see statement P hashed with k. A believes that B once said P.

Jurisdiction rule: $\dfrac{A|\equiv B| \Rightarrow P, A|\equiv B|\equiv P}{A|\equiv P}$ defines that if principal A believes that B has jurisdiction over P, A believes that principal B believes P hence A believes P.

Freshness conjuncatenation rule: $\dfrac{A|\equiv \#(P)}{A|\equiv \#(P,Q)}$ defines the assumption that principal A believes message P is fresh, then principal A believes that message P, Q are fresh.

3. Goals to be satisfied for BAN logic

- Goal 1: $S_i|\equiv (C_i \xleftrightarrow{bk} S_i)$,
- Goal 2: $C_i|\equiv (C_i \xleftrightarrow{bk} S_i)$,
- Goal 3: $S_i|\equiv C_i|\equiv (C_i \xleftrightarrow{bk} S_i)$,
- Goal 4: $C_i|\equiv S_i|\equiv (C_i \xleftrightarrow{bk} S_i)$.

4. Generic types of proposed protocol based on BAN logic

Message 1: $C_i \rightarrow S_i$: $h(Id_i \| h(Id_i \| K_s) \| N_i)$, $h(Id_i \| K_S) \oplus r_C$, $h(h(Id_i \|_S) \| r_C \| t_1)$, t_1.

Message 2: $S_i \rightarrow C_i$: $h(Id_i \| h(Id_i \| K_s) \| N_i)$, $h(Id_i \| K_S) \oplus r_S$, $h(h(Id_i \| K_S) \| r_S \| t_2)$, t_2.

Message 3: $C_i \rightarrow S_i$: $h(h(Id_i \| K_S) \| r_C \| r_S \| t_3)$, t_3.

Message 4: $S_i \rightarrow C_i$: $h(h(Id_i \| K_S) \| r_C \| r_S \| t_4)$, t_4.

5. Idealized form of proposed protocol based on BAN logic

Message 1: $C_i \rightarrow S_i$: $(Id_i, N_i)_{h(Id_i \| K_s)}$, $< r_C >_{h(Id_i \| K_s)}$, $< r_C, t_1 >_{h(Id_i \| K_s)}$, t_1.

Message 2: $S_i \rightarrow C_i$: $(Id_i, N_i)_{h(Id_i \| K_s)}$, $< r_S >_{h(Id_i \| K_s)}$, $< r_S, t_2 >_{h(Id_i \| K_s)}$, t_2.

Message 3: $C_i \rightarrow S_i$: $< r_C, r_S, t_3 >_{h(Id_i \| K_s)}$, t_3, $C_i \xrightarrow{bk} S_i$.

Message 4: $S_i \rightarrow C_i$: $< r_C, r_S, t_4 >_{h(Id_i \| K_s)}$, t_4, $C_i \xrightarrow{bk} S_i$.

6. Initial assumptions of proposed protocol based on BAN logic:

- A1: $C_i|\equiv \#(t_1)$,
- A2: $S_i|\equiv \#(t_2)$,
- A3: $C_i|\equiv \#(t_3)$,
- A4: $S_i|\equiv \#(t_4)$,
- A5: $C_i|\equiv C_i \xrightarrow{h(Id_i \| K_s)} S_i$,
- A6: $S_i|\equiv C_i \xrightarrow{h(Id_i \| K_s)} S_i$,
- A7: $C_i|\equiv S_i \Rightarrow C_i \xrightarrow{bk} S_i$,
- A8: $S_i|\equiv C_i \Rightarrow C_i \xrightarrow{bk} S_i$.

The proof of analysis is specified as follows.

7. Proof of proposed protocol based on BAN logic

Based on message 3, it could be obtained as:

S1: $S_i \triangleleft \left\{(r_C, r_S, t_3)_{h(Id_i \| K_s)},\ t_3, C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption A6 and based on message meaning rule, it could be obtained as:

S2: $S_i|\equiv C_i|\sim \left\{(r_C, r_S, t_3)_{h(Id_i \| K_s)},\ t_3, C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption A3 and based on freshness conjuncatenation meaning rule it could be obtained as:

S3: $S_i|\equiv \# \left\{(r_C, r_S, t_3)_{h(Id_i \| K_s)},\ t_3,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption S2, S3 and based on nonce verification rule, it could be obtained as:

S4: $S_i|\equiv C_i|\equiv \left\{(r_C, r_S, t_3)_{h(Id_i \| K_s)},\ t_3,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on S4, belief rule is obtained as follows:

S5: $S_i|\equiv C_i|\equiv C_i \xrightarrow{bk} S_i$.

Hence Goal 3: $(S_i|\equiv C_i|\equiv C_i \xrightarrow{bk} S_i)$ is satisfied. Based on assumption A8, based on S5 and also based on jurisdiction rule, it is concluded as follows:

S6: $S_i|\equiv C_i \xrightarrow{bk} S_i$.

Hence Goal 1: $(S_i|\equiv C_i \xrightarrow{bk} S_i)$ is satisfied.

Based on message 4, it could be obtained as:

S7: $C_i \triangleleft \left\{(r_C, r_S, t_4)_{h(Id_i \| K_s)},\ t_4,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption A5 and message meaning rule, it could be obtained as:

S8: $C_i|\equiv S_i|\sim \left\{(r_C, r_S, t_4)_{h(Id_i \| K_s)},\ t_4,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption A4 and freshness conjuncatenation rule, it could be obtained as:

S9: $C_i|\equiv \# \left\{(r_C, r_S, t_4)_{h(Id_i \| K_s)},\ t_4,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption S8, S9 and nonce verification rule, it could be obtained as:

S10: $C_i|\equiv S_i|\equiv \left\{(r_C, r_S, t_4)_{h(Id_i \| K_s)},\ t_4,\ C_i \xrightarrow{bk} S_i\right\}$.

Based on assumption S10 and belief rule, it could be obtained as:

S11: $C_i|\equiv S_i|\equiv (C_i \xrightarrow{bk} S_i)$.

Hence Goal 4: $(C_i|\equiv S_i|\equiv (C_i \xrightarrow{bk} S_i))$ is satisfied.

Based on assumption A7, S11 and jurisdiction rule, it could be obtained as:

C. Efficiency analysis of proposed scheme

The efficiency of the proposed scheme is analyzed and specified in Table 3. Computational time considered in the proposed scheme is the time taken to compute hash function and time taken to compute XOR operation in a system using 4 GB RAM and a Pentium V 3.2 GHZ processor. The computational time in Table 3 is the time taken to compute the hash function on each authentication scheme and it is specified as milliseconds. The time taken to compute XOR operation is not specified here because it can be neglected when compared to the time taken to compute hash function. The time taken for simulation is specified in Table 4 and it is given in milliseconds. Similarly, the communication cost of the proposed scheme is compared with other existing schemes and it is specified in Table 5. The proposed scheme takes $9T_h$ in total, which is less as compared to other existing schemes. From the efficiency analysis based

Table 3
Computational cost of proposed scheme as compared with existing authentication schemes

Authentication phases	Hwang et al. [18]	Xiang et al. [19]	Das et al. [20]	Cao et al. [3]	Kumar et al. [21]	Das et al. [22]	Proposed scheme
Registration phase	30 ms	30 ms	30 ms	70 ms	50 ms	40 ms	30 ms
Login phase	40 ms	30 ms	20 ms	40 ms	110 ms	40 ms	40 ms
Authentication phase	50 ms	60 ms	80 ms	70 ms	40 ms	130 ms	40 ms

Table 4
Communication cost of proposed scheme as compared with existing authentication schemes

Authentication phases	Hwang et al. [18]	Xiang et al. [19]	Das et al. [20]	Cao et al. [3]	Kumar et al. [21]	Das et al. [22]	Proposed scheme
Registration phase	$4T_h$	$4T_h$	$3T_h$	$6T_h$	$8T_h$	$7T_h$	$3T_h$
Login phase	$4T_h$	$3T_h$	$3T_h$	$4T_h$	$3T_h$	$4T_h$	$2T_h$
Authentication phase	$8T_h$	$8T_h$	$6T_h$	$4T_h$	$5T_h$	$7T_h$	$4T_h$

Table 5
Computational cost of proposed scheme as compared with existing authentication schemes

Authentication schemes		Hwang et al. [18]	Xiang et al. [19]	Das et al. [20]	Cao et al. [3]	Kumar et al. [21]	Das et al. [22]	Proposed scheme
Total No. of bits required for communication	Client	640 bits	620 bits	680 bits	720 bits	1024 bits	820 bits	512 bits
	Server	640 bits	620 bits	680 bits	720 bits	1024bits	820 bits	512 bits

on computational cost (Table 3), simulation time (Table 4) and communication cost (Table 5), it is witnessed that the proposed scheme based on signcryption and the bio-hash function has less simulation time, computational efficiency and communication efficiency as compared to other existing authentication schemes.

D. Entropy of proposed scheme

Entropy of the proposed authentication system is measured in bits. If the entropy of the system is measured in S bits, which means after 2^S possibilities, the system can certainly be broken into by the attacker. The total number of bits used in the proposed authentication technique is 700 bits. For an attacker to compromise this technique, he has to make 2^700 possibilities which is not feasible in nature. Hence it is concluded that the proposed scheme is highly secure as compared to other existing techniques.

E. Demonstration of BAN logic and bio-hash significance in attack phase

The bio-hash function helps the user identify and eradicate an intentional attack. The attack phase is executed in the network with three systems: a) client; b) server and c) attacker with a 4GB RAM Intel i3 processor each. The attacker eavesdrops on the communication messages between the client and server. Among all types of attacks, offline password guessing attacks and biometric recognition errors are demonstrated and their results are given. Fig. 4 depicts that an offline password guessing attack can never be possible on the proposed scheme because of the bio-hash function.

7. Conclusion and future work

To conclude the proposed research, multi-factor authentication based on secure signcryption and bio-hash function will have enhanced security features and will resist against all types of attacks. The proposed research work is compared mainly with Cao et al.'s scheme. It is identified that Cao et al.'s scheme is sensitive to various attacks due to lack of the bio-hash and signcryption functionality, and it has less security features as compared with the multi-factor authentication schemes being proposed. Moreover, from the result analysis it is witnessed that the proposed scheme is computationally and communicationally efficient, and it needs less simulation time as compared with all other existing authentication schemes. Detailed security analysis and formal analysis based on BAN logic has been proposed to demonstrate that the proposed scheme is capable of demonstrating higher security features. Therefore it is concluded from the proposed scheme that, having higher security features, it can

- Consider an adversary got m2 and m3 by eavesdropping the previous communication
- Consider that adversary also acquires h(.), f_i, e_i from stolen smart card
- Suppose adversary knows all formula used in this scheme

$$m1 = e_i \oplus r_i$$
$$m2 = m1 \oplus r_C$$
$$m3 = h(m1 \,||\, r_C \,||\, t_i)$$

- Due to $r_C = m1 \oplus m2$, m3 can also be expressed as $m3 = h(m1 \,||\, m1 \oplus m2 \,||\, t_i)$

$$m3 = h(e_i \oplus r_i \,||\, e_i \oplus r_i \oplus m2 \,||\, t_i)$$

- Due to $r_i = h(HBi\ (Bi) \oplus KC) \oplus fi$, m3 can be expressed as follows

$$m3 = h(e_i \oplus h(H_{Bi}\ (Bi) \oplus K_C) \oplus f_i \,||\, e_i \oplus h(H_{Bi}\ (Bi) \oplus K_C) \oplus f_i \oplus m2 \,||\, t_i)$$

- Even though e_i, r_i, r_C are known by the attacker he cannot be able to identify the $h(H_{Bi}\ (Bi))$ because it needs biometrics of the user.

Hence the system can never be compromised by the attacker because of Bio hash function.

Fig. 4. Demonstration of protection against offline password guessing attack due to bio-hash and BAN logic postulates rules

be used in applications such as border control, banking [23], e-Passport, the military, IoT, health care, e-governance [24] etc. The proposed research work can be further extended to include using fuzzy verifier logic to analyze the bio-hash function. The purpose of the fuzzy verifier concept is to resolve the tradeoff between security and usability.

References

[1] S.D. Kaul and K.A. Awasthi, "Security enhancement of an improved remote user authentication scheme with key agreement", *Wireless Pers. Commun.* 89, 621–637 (2016).

[2] V. Rajasekar, J. Premalatha, and K. Sathya, "An efficient signcryption scheme for secure authentication using hyper elliptic curve cryptography and Keccak hashing", *Int. J. Recent Technol. Eng.* 8 (3), 1593–1598 (2019).

[3] S.-Q. Cao, Q. Sun, and L.-L. Cao, "Security Analysis and Enhancement of A Remote User Authentication Scheme", *Int. J. Inf. Secur.* 21 (4), 661–669 (2019).

[4] R. Amin, H. Islam, M.K. Khan, A. Karati, D. Giri, and S. Kumari, "A Two-Factor RSA based Robust Authenticaton System for Multi Server Environment", *Secur. Commun. Netw*. 2017, 5989151 (2017).

[5] B. Huang, and M.K. Khan, "An Efficient Remote User Authentication with Key Agreement Scheme using Elliptic Curve Cryptography", *Wireless Pers. Commun.* 85, 225–240 (2015).

[6] B. Zhang, Z. Jia, and C. Zhao, "An efficient Certificateless generalized Signcryption scheme", *Secur. Commun. Netw.* 2018, 3578942 (2018).

[7] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using Elliptic curve cryptography", *Int. J. Dist. Network* 9 (4), (2013), doi: 10.1155/2013/730831.

[8] Y. Choi, Y. Lee, J. Moon, and D. Won, "Security enhanced multi-factor biometric authentication scheme using bio-hash function", *PLOS ONE* 12 (5), e0176250 (2017), doi: 10.1371/journal.pone.0176250.

[9] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem", *J. Med. Syst*. 39, 32 (2015), doi: 10.1007/s10916-015-0221-7.

[10] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for Telecare medicine information systems", *J. Med. Syst.* 38 (5), 1–11 (2015), doi: 10.1007/s10916-014-0136-8.

[11] L. Han, X. Tan, S. Wang, and X. Liang, "An efficient and secure three factor based authenticated key exchange scheme using elliptic curve cryptosystems", *Peer Peer. Netw. Appl.* 11, 63–73 (2017).

[12] K. Siddique, Z. Akhtar, and Y. Kim, "Biometric vs Passwords: a modern version of tortoise and the hare", *Comput. Fraud. Secur*. 2017 (1), 13–17 (2017).

[13] M. Burrows, M. Abadi, and R.M. Needham, "A logic of authentication", *P. Roy. Soc. A-Math. Phy.* 8 (1), 233–271, 1989.

[14] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment", *IEEE. Syst. J*. 9 (3), 816–823 (2015), doi: 10.1109/JSYST.2014.2301517.

[15] D. Wang , C.G. Ma, and P.Wu, "Secure password-based remote user authentication scheme with nontamper resistant smart cards", in *IFIP Annual Conference on Data and Applications Security and Privacy*, Springer Berlin Heidelberg, 2012.

[16] C.G. Ma, D. Wang, and S.D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards", *Int. J. Comun. Syst*. 27 (10) 2215–2227 (2014). doi: 10.1002/dac.2468.

[17] D. Otway and O. Rees, "Efficient and timely mutual authentication", *SIGOPS Oper. Syst. Rev*. 21 (1), 8–10 (1987), doi: 10.1145/24592.24594.

[18] M.-S. Hwang, E.F. Cahyadi, C.-Y. Yang, and S.-F. Chiou, "An Improvement of the Remote Authentication Scheme for Anonymous Users Using an Elliptic Curve Cryptosystem", in *2018 IEEE 4th International Conference on Computer and Communications* (ICCC), 2018, pp. 1872–1877, doi: 10.1109/CompComm.2018.8780891.

[19] Li Xiong, Jianwei Niu, M. Karuppiah, Kumari Saru, and Fan Wu, "Secure and efficient two factor authentication scheme with user anonymity for network based E-health care applications", *J. Med. Syst*. 40, 268 (2016), doi: 10.1007/s10916-016-0629-8.

[20] A.K. Das and A. Gowsami, "A Robust anonymous biometric based remote user authentication scheme using smart cards", *Comput. Inf. Sci*. 27 (2), 193–210 (2015).

[21] S. Kumar, V. Singh, and V. Sharma, "Advance remote user authentication scheme using smart card", *Telcom. Radio. Engg*. 78 (11), 957–971 (2019), doi: 10.1615/TelecomRadEng.v78.i11.40.

[22] A.K. Das, A.K. Sutrala, O.Vanga, and A. Goswami, "A secure smartcard based anonymous user authentication scheme for health care applications using wireless medical sensor networks", *Wireless Pers. Commun*. 94, 1899–1933 (2016).

[23] A. Sharma and S.K. Lenka, "Analysis of QKD multifactor authentication in online banking systems", *Bull. Pol. Ac.: Tech*. 63 (2), 545–548 (2015).

[24] G. Sharma and A.S. Kalr, "A Secure remote user authentication scheme for smart cities e-governance applications", *J. Reliable Intell. Environment* 3, 177–188 (2018).