CRYPTANALYSIS AND ENHANCEMENT OF MULTI FACTOR REMOTE USER AUTHENTICATION SCHEME BASED ON SIGNCRYPTION

VANI RAJASEKAR*
Department of CSE
Kongu Engineering College
Erode, India

PREMALATHA JAYAPUL AND SATHYA KRISHNAMOORTHI
Department IT and Department of CT-UG
Kongu Engineering College
Erode, India

(Communicated by Daniele Bartoli)

Abstract. The major need of remote user authentication is to verify the authenticity of the user through insecure channel. Till today enormous remote user authentication schemes have been proposed but still some security flaws remains. Some of them are vulnerable to password guessing attack, Id guessing attack, client and server impersonation attack, replay attack, Denial of Service (DoS) attack etc. Besides the security issues many such schemes are supposed to have higher computational and communication cost. To overcome these challenges a lightweight cryptographic scheme called signcryption has evolved. Signcryption is a logical combination of encryption and digital signature in single step. Thereby it provides necessary security features in less computational cost of 0.97 ms and communication cost of 824 bits. The proposed research work outlines the weakness in Dharminder 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 a secure multifactor authentication scheme using signcryption based on Hyper Elliptic Curve Cryptography (HECC) and Bio-hash function. The formal security analysis of proposed scheme is done using Burrows-Abadi-Needham logic. The analysis reveals that the proposed scheme is computational and communication efficient and satisfies all the needed security goals. The scheme is also been formally verified using AVISPA tool that confirms that it is resilient to security attacks.

1. Introduction

Swift advancement of wireless technologies has lead to massive growth in day to day internet activities. These activities can be easily compromised because it is open access to all the users [23] hence there is a possibility for an attacker to steal the secure information and services. All these components demand remote user authentication in order to safely transmit the message through communication channel. It has been identified that authentication scheme based on signcryption [21] provides...
less computational and communicational cost. There are different types of signcryption techniques proposed so for which are based on RSA, El-Gamal, Schnorr, Elliptic curve cryptography for encryption [29], Elliptic curve cryptosystem [13] and SHA, Keccak Hashing to generate digital signature. The proposed signcryption scheme based on Hyper Elliptic Curve Cryptography (HECC) for encryption and Bio-hash function to generate digital signature plays a major role in cryptographic primitives because of its lesser key size compared to that of other cryptographic algorithms and their efficiency in terms of communicational and computational cost.

Traditional authentication scheme was password based and single factor authentication schemes. It has been realized soon that they are prone to major threats. The authentication schemes have been further classified into three major categories as knowledge based, object based [14] and biometric based. Each category has its own pros and cons. Knowledge based authentication schemes are known for their simplicity, efficiency and easier to use, but it is prone to malicious attackers due to the password adoption. Object based authentication uses smart card technology which contains cryptographic information [28] 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 [9]. Biometric based authentication has become the focal point for many researchers because the biometric traits of the users such as fingerprint, facial features, palm prints, iris features, 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 elegant security and to protect against different attacks. The proposed will find its major application in the field of wireless medical sensor networks to monitor the patient health remotely, cloud IoT based application, Random number generation [22] and remote user authentication systems.

The main contribution of the paper is as follows: Section 2 briefly describes the related works carried out in the authentication, proposed light weight cryptographic method signcryption and hash function. Section 3 briefly describes the proposed multifactor authentication technique based on signcryption with HECC and Bio-hash function. Section 4 is mainly devoted for the informal security analysis, formal security analysis on the proposed scheme using Burrow-Abadhi-Needham (BAN) logic and formal security analysis using AVISPA security tool. Section 5 describes the conclusion and future work.

2. Related works

Chaturvedi [6] developed a remote user authentication scheme based on key agreement. From their result analysis it has been identified that their schemes reduce computational and communicational cost by 25 percentage but they fail to provide the necessary security features such as non-repudiation, forward secrecy and they do not protect against password guessing attack, dictionary attack and impersonation attack. Limbasiya et al [16] developed a remote user authentication technique and made cryptanalysis on Nikooghadam et al [17] method. They found that Nikooghadam et al scheme is vulnerable to password guessing attack, insider attack, and replay attack. Similarly Choi and Lee [7] have developed an enhanced multi factor authentication based on bio-hash function. From the literature study it has been identified that their scheme is prone to Biometric recognition fault with 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 compared to that of existing schemes. The result analysis also reveals that proposed scheme is computational and communicational efficient. Lidong et al [12] had proposed an efficient and secure three factor based authenticated key exchange scheme using elliptic curve cryptosystem. Although this scheme uses three factor secure authentication strategy, it fails to avoid biometric recognition error, masquerading attack and mutual authentication.

Chandrakar et al [5] proposed a two factor remote user authentication technique based on rabin cryptosystem. Rabin cryptosystem is based on integer factorization and result analysis shows that their scheme provides considerable security. Kamran et al [24] 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 can be presented to the system. 3. Feature extraction process can be circumventing by malicious codes that may replace the legitimate features of user to fraudulent features. 4. Fusion level or score level can be modified by the intruder results in the increasing False Acceptance Rate (FAR), False Rejection Rate (FRR) thereby reducing the efficiency of the biometric system. Wang et al [27] identified an enhanced group based proofs of storage. The author here shows that their scheme is suitable for IoT based cloud. Several applications have been proposed on remote user authentication technique, some of which are utilized for real time applications such as IoT [10]. Teh et al [26] proposed an authentication technique for IoT that uses Lockitron. The Lockitron is used to lock and unlock the doors remotely using smartphone.

2.1. Bio hash function. Generally hash function is referred to as one way transformation function in which it takes input of any size and produces output with fixed size. It can be used in various user authentication and verification problems because of the peculiarity and unique nature of user’s biometric traits. The major advantage of using biometric traits is that a single change in the biometric data will cause enormous hash value change. This is due to the intrinsic change in the biometric features of user’s. From the study it is identified that general hash function sometimes results in the recognition error and slight changes result in large differences in hash value. To resolve this problem a new technique called bio hash function is proposed and studied. From the various analyses on bio hashing system it is identified that all bio hash function system should follow the technical characteristics mentioned as follows:

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

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 more advantageous than the traditional way of hash function.
2.2. SIGNCRYPTION. The proposed signcryption scheme is based on hyper elliptic curve cryptography with bio hash function to generate digital signature. The hyper elliptic curve [4] over genus curve is given by the 1
\[
y^2 + h(x)y = f(x) \mod q
\]
Where \( h(x) \) is polynomial of is polynomial where the degree of \( h(x) \leq g \) and \( f(x) \in F(X) \) is a polynomial which is known as 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 the 2.
\[
D = (a(x), b(x)) = \left\{ \sum_{i=0}^{g} x^i a_i, \sum_{i=0}^{g-1} x^i b_i \right\} \in j_c(F_q)
\]
A. Signcryption based on HECC and Bio-hashing

The steps involved in the signcryption process are given as follows:
- Choose a large prime number \( q \) where \( q > 2^{80} \)
- Consider \( C \) be the Hyper elliptic curve defined over prime field is specified as \( F_q \)
- Choose a divisor \( D \) of large prime order \( n \) where \( n \geq 2^{80} \)
- Let \( d_a \) be the private key of the sender where \( d_a \in 0, 1, 2, ..p - 1 \)
- Calculate public key of the sender as \( p_a = d_aD \)
- Let \( d_b \) be the receiver’s private key where \( d_b \in 0, 1, 2, ..p - 1 \)
- Calculate public key of the receiver as \( p_b = d_bD \)
- Consider \( m \) be the secret message to be sent to receiver
- Let \( E_k \) and \( D_k \) denotes the encryption and decryption
- Let the signcrypted tuple be \((C, r, S)\)
- Let \( H_{B_i}(.) \) represents the Bio hash function

B. UnSigncryption based on HECC and Bio-hashing

The steps involved in unsigncryption are given as follows:
- Select a random number \( k \) where \( k = 1, 2, 3, ..n - 1 \)
- Calculate \( K1 = H(kD) \)
- Calculate \( k2 = H(kp_b) \)
- Let cipher text \( C = E_{k2}(m) \)
- Let \( R \) is calculated by \( R = H_{B_i}(m||k2) \)
- Calculate \( S = (k/(R + d_a)) \mod n \)
- Compute \( r = RD \)
- Finally the signcrypted tuple after this process is \((C, r, S)\)
smaller key size and it is more secure by providing forward secrecy [21] and all necessary security requirements.

2.3. Security requirements. Following are the security features needed for real time wireless applications

1. Confidentiality: Only the legitimate users can able to decrypt the encrypted communication occurs through secure channel.

2. Mutual authentication: In this case both the communicating parties have to involve in authentication. The mechanism should also ensures that it protect against all type of spoofing attacks.

3. Availability: All the requested data must be available on demand to the legitimate users.

4. Key freshness: Each communication session should include the fresh session key. This will ensure confidentiality even if the previous communication session key was stolen by the attacker.

5. Forward secrecy: It is impossible for the attacker to trace the communication information in past session with the help of current session communication being stolen. It also ensures that even if the secret keys are stolen by the attacker he cannot be able to trace the communication information.

6. User anonymity: This is to ensure that no intruder can able to trace the communication information occurs between the legitimate users. It is the key requirement to protect against the malicious attack.

3. Multi factor authentication scheme based on signcryption

The proposed method includes 3 phases such as 1. Registration phase 2. Password change phase 3. Login and Authentication phase. The notation used in the proposed approach is specified in Table1.

| S.No | Parameter used | Description          |
|------|----------------|----------------------|
| 1    | $C_i$          | Client/User          |
| 2    | $S_i$          | Server/Receiver      |
| 3    | $B_i$          | Biometric template of Client |
| 4    | $Id_i$         | Client’s Identity    |
| 5    | $Pw_i$         | Client’s password    |
| 6    | $H_{B_i}(.)$   | 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   | ⊕              | Bitwise XOR operation |
| 15   | ||             | Concatenation operator |
| 16   | $(C, r, S)$    | Signcrypted tuple    |
| 17   | $bk$           | Session key used by Client and Server |
3.1. Registration Phase. This phase of $C_i$ with $S_i$ is specified in Fig 1. $C_i$ establishes communication with $S_i$ using the secure channel.

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 $\langle Id_i, h(Pw_i) \oplus K_C \rangle$ using general hash function. Then by means of bio hash function it computes $\langle H_{Bi} \oplus K_C \rangle$ and sends to $S_i$ using 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 for $C_i$ in database and stores the computed information $\langle C_i, Id_i, N_i, C, r, S \rangle$.

Step 4: $S_i$ also computes the $Ed_i$ as follows and store it in 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 value in the smart card are $\langle h(.), H_{Bi}(.), f_i, e_i, N_i, C, r, S \rangle$

---

**Figure 1. Registration phase**

![Diagram](image-url)
3.2. Password change phase. In the proposed method, this phase will be executed when the legitimate user’s smart card is lost. In need to change the password, the user has to send the old password \( P_{\text{w}i} \) and new password \( P_{\text{w}i,\text{new}} \). The flow of this process is described in Fig 2.

Step 1: \( C_i \) selects \( Id_i, P_{\text{w}i}, P_{\text{w}i,\text{new}} \) and the user imprints the biometric \( B_i \) and generates the new secret key of client as \( K'_C \). It then calculates \( \langle Id_i, h(P_{\text{w}i}) \oplus K'_C \rangle, \langle H_{B_i}(B_i) \oplus K'_C \rangle \), and send this newly calculated values to \( S_i \).

Step 2: After receiving this server the server checks for all the entries of \( C_i \) in the database. It then computes \( v_i' = h(h(P_{\text{w}i}) \oplus H_{B_i}(B_i)) \| K_S) \) 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 \( N_{\text{new}} = N_i + 1 \) and remaining values will be calculated:

- \( f_{\text{new}} = h(Id_i \oplus h(P_{\text{w}i,\text{new}}) \oplus H_{B_i}(B_i)) \)
- \( r_{\text{new}} = h(H_{B_i}(B_i) \oplus K'_C) \oplus f_{\text{new}} \)
- \( e_{\text{new}} = h(Id_i || K_S) \oplus r_{\text{new}} \)

Step 4: \( S_i \) also computes the \( Ed_{\text{new}} \) as follows and stores it in database for the corresponding \( C_i \):

- \( Ed_{\text{new}} = h(Id_i, h(Id_i || K_S) || N_{\text{new}}) \)

Step 5: \( S_i \) sends the new smart card to \( C_i \). The values in the smart card are \( \langle h(\cdot), H_{B_i}(\cdot), f_{\text{new}}, e_{\text{new}}, N_{\text{new}}, C, r, S \rangle \).

---

**Figure 2.** Password change phase
3.3. LOGIN AND AUTHENTICATION PHASE. Fig 3 describes the login and authentication phase of proposed scheme. The following steps are executed when $S_i$ authenticates to server $S_i$. In login phase 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 $Pw_i$ using traditional hash function and computes $H_{Bi}(Bi)$ using Bio-hash function. Then smart card verification will be taken as follows

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

Step 2: If $f_i$ is verified correctly by smart card, $C_i$ generates the value of timestamp as $t_i$ and generates random number as $r_C$. Then $C_i$ computes the values of $m_1, m_2, m_3, Ed_i$ as follows

- $r_i = h(H_{Bi}(Bi) \oplus K_C) \oplus f_i$
- $m_1 = e_i \oplus r_i$
- $m_2 = m_1 \oplus r_e$
- $m_3 = h(m_1||r_C||t_i)$
- $Ed_i = h(Id_i||h(Id_i||K_S||N_i))$

Step 3: $C_i$ sends the login request message $(t_i, m_2, m_3, Ed_i)$ to $S_i$. Once the login message is received from client, $S_i$ executes the authentication phase as follows:

Step 4: $S_i$ checks for the originality of $Ed_i$ from the stored value in database.

Step 5: If $Ed_i$ is verified correctly, $S_i$ computes $m_4, m_5$ and verifies with $m_3$ as follows

- $m_4 = h(Id_i||K_S)$
- $m_5 = m_2 \oplus m_4$
- $m_6 = h(m_4||m_5||t_1)$

Step 6: If the value of $m_3$ is accurate, $S_i$ calculates the current timestamp $t_2$ and then calculates $m_6$ and $m_7$. Then $S_i$ sends the message $(Ed_i, m_6, m_7, t_2)$ to $C_i$

- $m_6 = m_4 \oplus r_S$
- $m_7 = h(m_4||r_S||t_2)$

Step 7: $C_i$ computes $m_8 = m_6 \oplus m_1$ and verifies with $m_7 = h(m_1||m_8||t_2)$ or not. If it is verified, $C_i$ generates timestamp value as $t_3$ and computes $m_9$. The $C_i$ computes $bk$ as follows

- $m_9 = h(m_1||r_C||m_8||t_3)$
- $bk = h(m_1||r_C||m_8||t_2||t_3)$

$C_i$ sends $(m_9, t_3)$ to server $S_i$.

Step 8: On receiving the value $m_9, S_i$ verifies the value $m_9 = h(m_4||m_5||r_S||t_3)$ and if it is correct, user login request will be accepted. $S_i$ computes $m_10, bk$ and sends $(m_10, t_4)$ to $C_i$

- $m_{10} = h(m_4||m_5||r_S||t_4)$
- $bk = h(m_4||m_5||r_S||t_2||t_3)$

Step 9: On receiving $(m_{10}, t_4)$, $C_i$ will be checking that $m_{10} = h(m_1||r_C||m_8||t_4)$ 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 the all phases

- $bk = h(h(Id_i||K_S)||r_C||r_S||t_2||t_3)$
Figure 3. Password change phase
4. Result analysis on the proposed scheme

This section describes about the security analysis and efficiency analysis of proposed scheme. The efficiency analysis witnessed that the proposed scheme is computationally efficient compared to other state-of-art existing schemes. Security analysis witnessed that the proposed approach is resilient to all major types of attacks.

4.1. Informal security analysis of proposed approach. The comparison of cryptanalysis of various remote user authentication schemes is given in Table 2.

| Remote user authentication schemes | A1   | A2   | A3   | A4   | A5   | A6   | A7   | A8   | A9   | A10  |
|-----------------------------------|------|------|------|------|------|------|------|------|------|------|
| Dharminder et al [11]             | No   | No   | Yes  | No   | No   | No   | Yes  | Yes  | Yes  | Yes  |
| Chaturadevi et al [6]             | Yes  | No   | Yes  | No   | No   | No   | Yes  | Yes  | Yes  | Yes  |
| Nikooghadam et al [17]           | Yes  | No   | Yes  | No   | Yes  | No   | Yes  | Yes  | Yes  | Yes  |
| Chandrakar et al [5]              | No   | Yes  | No   | No   | No   | No   | Yes  | Yes  | Yes  | Yes  |
| Sutrala et al [25]                | Yes  | No   | Yes  | No   | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  |
| Dharminder et al [10]             | No   | Yes  | Yes  | No   | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  |
| Li et al [15]                     | No   | Yes  | No   | No   | No   | Yes  | Yes  | Yes  | Yes  | Yes  |
| Das et al [8]                     | No   | No   | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  |
| Sharma et al [23]                | No   | No   | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  |
| Proposed Scheme                   | No   | No   | No   | No   | No   | No   | No   | No   | No   | No   |

**A1:** Server masquerading attack **A2:** Replay attack **A3:** Biometric recognition error **A4:** Mutual Authentication **A5:** Client Impersonation attack **A6:** Offline password guessing attack **A7:** Slow wrong password detection **A8:** Prone to DoS attack **A9:** Id Guessing attack **A10:** Lack of session key agreement

4.1.1. **Server masquerading attack:** Suppose an attacker tries to masquerade a legitimate server, he must send login request. Let us consider if $C_i$ sends $\langle m_9, t_3 \rangle$ to the attacker he must calculate $\langle m_10, t_4 \rangle$ to look like legitimate server; whereas if an attacker needs to calculate $\langle m_10, t_4 \rangle$ from $\langle m_9, t_3 \rangle$ he must 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 masquerade the legitimate server.

4.1.2. **Replay attack:** Suppose in the proposed scheme if an intruder intercepts the communicational messages $\langle t_1, m_2, m_3, Ed_i \rangle$ and $\langle m_9, t_3 \rangle$ between $C_i$ and $S_i$ and replays the message to $S_i$. It is infeasible for the attacker to communicate with $S_i$ within the timestamp $t_1$ even though if an attacker passes for timestamp $t_1$, he will not be able to generate response messages $\langle t_2, m_6, m_7, Ed_i \rangle$. This is because the attacker knows the previous $\langle m_9, t_3 \rangle$ which will never be appropriate to calculate the response for the message $\langle t_2, m_6, m_7, Ed_i \rangle$. Furthermore 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 replay attack.

4.1.3. **Biometric recognition error:** The concept called Bio hash function is introduced in the proposed scheme which makes it impossible for biometric recognition error whereas most authentication scheme uses the traditional hash function to validate the biometric traits of the user that makes biometric recognition error to occur in their scheme. The main advantage of using 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.

4.1.4. Mutual authentication: This concept involves both the client $C_i$ and $S_i$ server mutually authenticates to each other. 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 they only know the value of $h(Id_i || K_S)$. The legitimate server communicates with legitimate client based on received $\langle m9, t_3 \rangle$ here only legitimate $C_i$ can be able to calculate $m9$ using $m6$ received from $S_i$. Similarly only legitimate server can be able to calculate $m10$ from the received $\langle m9, t_4 \rangle$ because he only knows the value of $r_C$ and $h(Id_i || K_S)$.

4.1.5. Client impersonation attack: To successfully execute client impersonation attack, intruder needs to know the value of $h(Id_i || K_C)$. To compute $h(Id_i || K_C)$ attacker needs to know the following values

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

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

4.1.6. Offline password guessing attack: It is possible for an attacker to gain all the information that is stored in user’s smartcard by means of executing side channel attack. In the proposed authentication mechanism the password will be always used with the value $Id_i$ 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 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 offline password guessing attack.

4.1.7. Slow wrong password detection: Password detection is the major threat in today’s wireless applications. Cao et al’s [2] scheme checks the user password during the login and authentication phase whereas in proposed scheme when user in need to authenticate he has to give his $Id_i, Pw_i, and Bi$. With these values smart card will compute $f_i = h(Id_i \oplus h(Pw_i) \oplus H_{Bi}(Bi))$ and verifies with $f_i$ stored in database. In case if user provides the wrong password $Pw_i$ the calculated $f_i$ will be vary as $f_i$ stored in 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.

4.1.8. Prone to DoS attack. The time stamp values $\langle t_1, t_2, t_3, t_4 \rangle$ in the proposed scheme is used to check the freshness of all messages sent between $C_i$ and $S_i$. The time stamp values make the attacker difficult to establish mutual authentication with legitimate client and server. Also the important part of the proposed scheme is $C_i$ and $S_i$ uses 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 $m10$ also be computed as follows
Consider if an attacker intercepts and replays the message $m_3$ to $S_i$. It will check the freshness of message received from attacker using the timestamp value $t_1$ but that will never be equal to the current timestamp. Therefore the intruders can never be able to forge the legitimate client and server; hence the proposed scheme is more secure than existing remote user authentication schemes.

4.1.9. **ID guessing attack:** In Dharminder et al’s [10] scheme $Ed_i = h(Id_i || N_i)$ whereas in the proposed scheme $Ed_i = h(h(Id_i || N_i || K_S || m_2 || r_S || t_2 || t_3))$. The proposed scheme protects the value of $Id_i$ from public communication. Consider if an attacker knows $Ed_i$ he is not able to identify $Id_i$ from $Ed_i$. Hence ID guessing attack is not feasible in the proposed scheme.

4.1.10. **Lack of session key agreement:** Dharminder et al’s [10] 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 $bk = h(m_4 || m_5 || r_S || t_2 || t_3)$. 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 the message freshness. The proposed scheme changes the session key for each session to protect against the various attacks.

4.2. **Formal analysis on proposed scheme.** (Burrows-Abadi-Needham) BAN logic was first identified by Burrows et al [1]. It has considerably drawn favorable attention of many researchers due to its simplicity to use and efficiency in formal analysis of various authentication schemes. BAN logic in the proposed scheme considers A and B for representing principals; P and Q for representing the statements. BAN logic generally follows four steps in formal analysis.

4.2.1. **Notations used for BAN logic:**

- $A \models B$: The principal A believes that statement P is true in current run.
- $A \triangleleft B$: The principal A sees specified statement P which implies that A had received message that contains P.
- $A \triangleleft B$: The principal A has once said to the statement P which meant A—P when A sent it.
- $A \Rightarrow B$: The defined principal A has more jurisdiction over the 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.
- $A \models B_k$: Principal A believes that A and B communicate with each other using shared secret key k.
- $A_kB$: 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
4.2.2. **Rules for logical postulates of BAN logic:**

- **Belief rule:** \( A \equiv P, A \equiv Q \frac{A \equiv (P \land Q)}{A \equiv (P \lor Q)} \) defines that suppose principal A believes P and Q then it believes \((P \land Q)\).
- **Nonce verification rule:** \( A \equiv P, A \equiv \neg Q \frac{A \equiv (P \lor \neg Q)}{A \equiv B} \) defines that suppose principal A believes as P is fresh and A also believes that the B once said Q, then A believes B believes P.
- **Message meaning rule:** \( A \equiv B, A \equiv (P \land Q) \frac{A \equiv (P \land Q)}{A \equiv B} \) defines that if principal A believes that secret key will be shared with B. A will see statement P hashed with k.
- **Belief over principals:** \( A \equiv B, A \equiv P \) defines that if principal A believes that B once said P, A believes as P is fresh and A also believes that the B once said Q, then A believes B believes P.
- **Jurisdiction rule:** \( A \equiv B, A \equiv P \frac{A \equiv (P \lor \neg Q)}{A \equiv B} \) defines that if principal A believes that B has jurisdiction over P, A believes that principal B believes P hence A believes P.
- **Freshness conjunctaenation rule:** \( A \equiv P, A \equiv Q \frac{A \equiv (P \land Q)}{A \equiv B} \) defines that suppose principal A believes message P is fresh, then principal A believes that message P,Q are fresh.

4.2.3. **Goals to be satisfied for BAN logic:**

- Goal 1: \( S_i \equiv \langle C_i b_k S_i \rangle \)
- Goal 2: \( C_i \equiv \langle C_i b_k S_i \rangle \)
- Goal 3: \( S_i \equiv C_i \equiv \langle C_i b_k S_i \rangle \)
- Goal 4: \( C_i \equiv \langle C_i b_k S_i \rangle \)

4.2.4. **Generic types of proposed protocol based on BAN logic:**

- **Message 1:** \( C_i \rightarrow S_i : h(Id_i || h(Id_i || K_S)) || N_i, h(Id_i || K_S) \oplus r_C, h(h(Id_i || K_S)) || r_C || t_1 \)
- **Message 2:** \( S_i \rightarrow C_i : h(Id_i || h(Id_i || K_S)) || N_i, h(Id_i || K_S) \oplus r_S, h(h(Id_i || K_S)) || r_S || t_2 \)
- **Message 3:** \( C_i \rightarrow S_i : h(h(Id_i || K_S)) || r_C, r_S, t_3, t_3 \)
- **Message 4:** \( S_i \rightarrow C_i : h(h(Id_i || K_S)) || r_C, r_S, t_4, t_4 \)

4.2.5. **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:** \( C_i \rightarrow S_i : < r_C, r_S, t_3 > h(Id_i || K_S), t_3, C_i b_k S_i \)
- **Message 4:** \( S_i \rightarrow C_i : < r_C, r_S, t_4 > h(Id_i || K_S), t_4, C_i b_k S_i \)

4.2.6. **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: \( C_i \equiv C_i h(Id_i || K_S) S_i \)
- A6: \( S_i \equiv C_i h(Id_i || K_S) S_i \)
- A7: \( C_i \equiv S_i \Rightarrow C_i b_k S_i \)
- A8: \( S_i \equiv C_i \Rightarrow C_i b_k S_i \)

The proof of analysis is specified as follows.
4.2.7. Proof of proposed protocol based on BAN logic.

- Based on message 3, it could be obtained as
  \( S_1 : S_i \equiv \{ < r_C, r_S, t_3 >_{h(I_d || |K_s)} t_3, C_i \}$
- Based on assumption A6 and based on message meaning rule it could be obtained as
  \( S_2 : S_i |\equiv C_i |\{ < r_C, r_S, t_3 >_{h(I_d || |K_s)} t_3, C_i \}$
- Based on assumption A3 and based on freshness conjunctenation meaning rule it could be obtained as
  \( S_3 : S_i |\equiv \# < r_C, r_S, t_3 >_{h(I_d || |K_s)} t_3, C_i \)$
- Based on assumption S2, S3 and based on Nonce verification rule it could be obtained as
  \( S_4 : S_i |\equiv C_i |\equiv < r_C, r_S, t_3 >_{h(I_d || |K_s)} t_3, C_i \)$
- Based on S4, belief rule is obtained as follows
  \( S_5 : S_i |\equiv C_i |\equiv C_i \)$

Hence Goal 3: \( S_i |\equiv C_i |\equiv C_i \) is satisfied.

- Based on assumption A8, based on S5 and also based on jurisdiction rule it is concluded as follows
  \( S_6 : S_i |\equiv C_i \)$

Hence Goal 1: \( S_i |\equiv C_i \) is satisfied.

- Based on message 4, it could be obtained as
  \( S_7 : C_i \equiv \{ < r_C, r_S, t_4 >_{h(I_d || |K_s)} t_4, C_i \}$
- Based on assumption A5 and message meaning rule it could be obtained as
  \( S_8 : C_i |\equiv S_i |\{ < r_C, r_S, t_4 >_{h(I_d || |K_s)} t_4, C_i \}$
- Based on assumption A4 and freshness conjunctenation rule it could be obtained as
  \( S_9 : C_i |\equiv S_9 |\equiv < r_C, r_S, t_4 >_{h(I_d || |K_s)} t_4, C_i \)$
- Based on assumption S8, S9 and nonce verification rule it could be obtained as
  \( S_10 : C_i |\equiv S_i |\equiv < r_C, r_S, t_4 >_{h(I_d || |K_s)} t_4, C_i \)$
- Based on assumption S10 and belief rule it could be obtained as
  \( S_11 : C_i |\equiv S_i |\equiv C_i \)$

Hence Goal 4: \( (C_i \equiv S_i \equiv C_i) \) is satisfied

- Based on assumption A7, S11 and jurisdiction rule it could be obtained as
  \( S_12 : C_i |\equiv C_i \)$

Hence Goal 2: \( (C_i \equiv C_i) \) is satisfied.

| Table 3. Cryptanalysis on various authentication schemes |
|----------------------------------------------------------|
| **Remote user authentication schemes**                  |
| **Registration phase**                                  |
| **Password change phase**                               |
| **Login and Authentication phase**                      |
| Dharminder et al [11]                                   |
| 2T_{su} + 1T_h                                         |
| 2T_{bk} + 1T_h                                         |
| 3T_{su} + 2T_h + 1T_{bk}                               |
| Chaturadevi et al [6]                                   |
| 3T_h                                                    |
| 2T_{bk} + 2T_h                                         |
| 6T_{su} + 2T_h + 3T_{bk}                                |
| Nikooghadam et al [17]                                  |
| 5T_h                                                    |
| 2T_{bk} + 3T_h                                         |
| 5T_{su} + 3T_h + 2T_{bk}                                |
| Chandrakar et al [5]                                    |
| 5T_h                                                    |
| 2T_{bk} + 6T_h                                         |
| 5T_{su} + 6T_h + 2T_{bk}                                |
| Sutrala et al [25]                                      |
| 5T_h + 2T_{su}                                          |
| 3T_{bk} + 4T_h                                         |
| 6T_{su} + 4T_h + 1T_{bk}                                |
| Dharminder et al [10]                                   |
| 2T_h + 1T_{su}                                          |
| 1T_{bk} + 4T_h                                         |
| 6T_{su} + 4T_h + 1T_{bk}                                |
| Li et al [15]                                           |
| 5T_h                                                    |
| 2T_{bk} + 3T_{hk}                                      |
| 4T_{su} + 2T_h + 1T_{bk}                                |
| Das et al [8]                                           |
| 3T_h + 2T_{su}                                          |
| 2T_{bk} + 2T_{h}                                       |
| 3T_{su} + 2T_h + 1T_{bk}                                |
| Sharma et al [23]                                      |
| 3T_h + 2T_{su}                                          |
| 2T_{bk} + 2T_{h}                                       |
| 6T_{su} + 2T_h + 3T_{bk}                                |
| Proposed Scheme                                         |
| 1T_h + 1T_{su}                                          |
| 1T_{hk} + 1T_{hk}                                      |
| 1T_{su} + 1T_{hk}                                      |

4.3. Computational and Communicational cost analysis. The efficacy of the proposed scheme is analyzed with existing schemes and specified in Table 3.
The proposed approach is experimented in Anaconda tool using Python programming language in a system having 4 GB RAM and Pentium V 3.2 GHZ processor. The computational cost of proposed scheme is analyzed using $T_{su}, T_h, T_{bk}$ which denotes time taken to compute signcryption and unsigncryption, hash function and session key computation respectively. The total execution time of proposed scheme is denoted in Fig 4. The time taken to compute XOR operation is neglected here because it takes lesser time compared to other operations. The computational cost of proposed scheme is analyzed by considering total number of bits taken for communication as given in Fig 5. The result analysis witnessed that the proposed scheme based on signcryption and bio hash function is both computationally and communication efficient compared to that of other existing schemes.

![Computational time analysis](image)

**Figure 4.** Computational time analysis on various schemes

4.4. **Formal security verification using AVISPA.** The game between attacker and challenger is verified and proposed here. This section uses formal security verification tool Automated Validation of Internet Security Protocol Applications (AVISPA) [18] to prove the security of the proposed approach by demonstrating man in the middle and replay attack. These protocols are verified and coded using High Level Protocol Specification Language (HLPSL). It is a power security tool for defining security protocols and model the communication. It consists of HLPSL 2IF translator which is used to translate HLPSL protocols to intermediate communication. This is then given as input to one of four back ends to generate output format. They are
The proposed approach uses two basic roles one for user and another for server. The roles have to be defined with all instances. The roles consist of compositions and global constants. The authentication and secrecy goals are maintained by HLPSL. The proposed approach uses five secrecy goals and four authentication goals. The output format of AVISPA contains “Summary” which has three notations SAFE, UNSAFE or INCONCLUSIVE. The simulation result SAFE indicates that the proposed protocol is secure against all types of major attacks. The “Detail” section denotes that under what condition the proposed protocol is declared as safe. The “Protocol” section denotes the name of protocol. The “Goal” section denotes the main objective of proposed analysis scheme. The “Backend” section denotes the name of backend used. The “Statistics” shows the time required to execute the protocol. The “Attack race” used to identify the display the identified attack in standard Alice-Bob format. The output of AVISPA tool is specified in Fig 6.
In this paper, an enhanced secure multi factor authentication scheme was introduced. It is identified that most of the existing authentication schemes are prone to various attacks due to lack of bio hash [19] and signcryption functionality and has less security features compared to proposed multifactor authentication schemes. Moreover from the result analysis it is witnessed that the proposed scheme is computational efficient, communication efficient and has less simulation time compared to all other existing authentication schemes. Detailed security analysis was done with well known AVISPA security tool and formal analysis was done based on BAN logic. Because of this efficacy it can be used in applications such as Border control, E-Passport, Military, IoT, Health care [20] etc. The proposed research work can be further intended to extend it studies on fuzzy verifier logic to analyze the bio hash function. The purpose of fuzzy verifier concept is to resolve the tradeoff between security and usability.

6. Declarations

1. Data Availability Statement
The data supporting the results reported in this work are generated in our simulation environment. No external data set repository is used for this experimental analysis.

2. Conflicts of Interest
The authors declare here that they have no conflict of interest.
3. **Funding Statement**

The authors declare here that they got no funding for this research work.

**ACKNOWLEDGMENTS**

The authors would like to thank Sihem Mesnager and the anonymous reviewers for their detailed technical and editorial comments that significantly improved the quality of the paper.

**REFERENCES**

[1] M. Burrows, M. Abadi and R. M. Needham, *A logic of authentication*, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 426 (1989), 233–271.

[2] S. Q. Cao, Q. Sun and L. Cao, *Security analysis and enhancements of a remote user authentication scheme*, IJ Network Security, 21 (2019), 661–669.

[3] S. A. Ch, M. Sher, A. Ghani, H. Naqvi and A. Irshad, An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, Multimedia Tools and Applications, 74 (2015), 1711–1723.

[4] S. A. Ch and M. Sher, Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem, in *International Conference on Information Systems, Technology and Management*, (Springer, Berlin, Heidelberg), (2012), 135–142.

[5] P. Chandrakar and H. Om, An efficient two-factor remote user authentication and session key agreement scheme using rabin cryptosystem, Arabian Journal for Science and Engineering, 43 (2018), 661–673.

[6] A. Chaturvedi, D. Mishra, S. Jangirala and S. Mukhopadhyay, A privacy preserving biometric–based three–factor remote user authenticated key agreement scheme, Information Security and Applications, 32 (2017), 15–16.

[7] Y. Choi, Y. Lee, J. Moon and D. Won, Security enhanced multi–factor biometric authentication scheme using bio–hash function, PloS One, 12 (2017), e0176250.

[8] A. K. Das and A. Goswami, A robust anonymous biometric–based remote user authentication scheme using smart cards, Journal of King Saud University–Computer and Information Sciences, 27 (2015), 193–210.

[9] A. K. Das, A. K. Sutrula, V. Odela and A. Goswami, A secure smartcard–based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks, Wireless Personal Communications, 94 (2017), 1899–1933.

[10] D. Dharminnder, D. Mishra, J. J. Rodrigues, R. de AL Rabelo and K. Saleem, PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments, Software: Practice and Experience, (2020), 1–12.

[11] D. Dharminnder, M. Obaidat, D. Mishra and A. K. Das, FEEC: Provably secure signcryption–based big data security framework for energy–efficient computing environment, IEEE Systems Journal, (2020).

[12] 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–to–peer Networking and Applications, 11 (2018), 63–73.

[13] M. S. Hwang, E. Cahyadi, C. 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), IEEE, (2018), 1872–1877.

[14] S. Kumar, V. Singh, V. Sharma and V. P. Singh, Advance remote user authentication using smart card, Telecommunications and Radio Engineering, 78 (2019), 8–10.

[15] C. T. Li, C. C. Lee, C. Y. Weng and S. J. Chen, A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e–healthcare systems, Journal of Medical Systems, 40 (2016), 233.

[16] T. Limbasiya, M. Soni and S. K. Mishra, Advanced formal authentication protocol using smart cards for network applicants, Computers and Electrical Engineering, 66 (2018), 50–63.

[17] M. Nikooghadam, R. Jahantigh and H. Arshad, A lightweight authentication and key agreement protocol preserving user anonymity, Multimedia Tools and Applications, 76 (2017), 13401–13423.
[18] V. Odelu, A. K. Das and A. Goswami, A secure effective key management scheme for dynamic access control in a large leaf class hierarchy, *Information Sciences*, 269 (2014), 270–285.

[19] D. Otway and O. Rees, Efficient and timely mutual authentication, *ACM SIGOPS Operating Systems Review*, 1 (1987), 8–10.

[20] J. Premalatha, R. Vani and K. Sathya, Biometric signcryption using hyperelliptic curve and cryptographically secure random number, *Asian Journal of Research in Social Sciences and Humanities*, 6 (2016), 462–472.

[21] V. Rajasekar, J. Premalatha and K. Sathya, An efficient signcryption scheme for secure authentication using hyper elliptic curve cryptography and Keccak hashing, *International Journal of Recent technology and Engineering*, 8 (2019), 1593–1598.

[22] K. Sathya, J. Premalatha and V. Rajasekar, Sensor–seeded cryptographically secure random number generation, *Indian Journal of Science*, (2019).

[23] G. Sharma and S. Kalra, Advanced lightweight multi–factor remote user authentication scheme for cloud–IoT applications, *Journal of Ambient Intelligence and Humanized Computing*, 11 (2020), 1771–1794.

[24] K. Siddique, Z. Akhtar and Y. Kim, Biometrics vs passwords: A modern version of the tortoise and the hare, *Computer Fraud and Security*, 1 (2017), 13–17.

[25] A. K. Sutrala, A. KDas, V. Odelu, M. Wazid and S. Kumari, Secure anonymity–preserving password–based user authentication and session key agreement scheme for telecare medicine information systems, *Computer Methods and Programs in Biomedicine*, 135 (2016), 167–185.

[26] T. Y. Teh, Y. S. Lee, Z. Y. Cheah and J. J. Chin, IBI–Mobile Authentication: A prototype to facilitate access control using identity–based identification on mobile smart devices, *Wireless Personal Communications*, 94 (2017), 127–144.

[27] X. A. Wang, Y. Liu, J. Zhang, X. Yang and M. Zhang, Improved group–oriented proofs of cloud storage in IoT setting, *Concurrency and Computation: Practice and Experience*, 30 (2018), e4781.

[28] K. Xue and P. Hong, Security improvement on an anonymous key agreement protocol based on chaotic maps, *Communications in Nonlinear Science and Numerical Simulation*, 17 (2012), 2969–2977.

[29] B. Ying and A. Nayak, Lightweight remote user authentication protocol for multi–server 5G networks using self–certified public key cryptography, *journal of Network and Computer Applications*, 131 (2019), 66–74.

Received December 2019; revised May 2020.

*E-mail address*: vanikecit@gmail.com  
*E-mail address*: jprem@kongu.ac.in  
*E-mail address*: pearlhoods@gmail.com