Mehran University Research Journal of Engineering and Technology
Vol. 39, No. 2, 287- 309, April 2020
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.2002.07

SIP Issues and Challenges – A Scalable Three Factor Authentication Scheme

Saeed Ullah Jan[1a], Fawad Qayum[1b], Ajab Khan[1c]

RECEIVED ON 24.02.2019, ACCEPTED ON 30.01.2020

ABSTRACT

The SIP (Session Initiation Protocol) is an application and presentation layer signaling protocol used for initiating, continuing and terminating multimedia session for the end user. It gains much attention of the researchers because it is exposed to several threats and noticed challenging vulnerabilities from time to time. Consequently, the security of SIP is a crucial task and many efforts have been made by different researchers and tried to divert the attention towards its solution. But still, no one claims with conviction about a foolproof secure mechanism for SIP. As users extensively use SIP services, the mutual authentication and key agreement among the participants is an important issue. So, robust authentication and key agreement scheme are mandatory for enhancing security, legitimacy and better complexities. Therefore, we present an improved three-factor authentication scheme that caters all the weakness and known attacks in Mishra et al. scheme. The proposed scheme not only guarantees for security but performance can also be made lightweight. As performance and security contradict each other, the change in one inversely affects the other. The proposed scheme has been analyzed both formally using BAN (Burrows-Abadi-Needham) logic and ProVerif1.93 software verification toolkit, and informally using assumptions which show a delicate balance of security with performance.

Key Words: **Cryptography, Session Initiation Protocol, Verification, Performance, Signature, Authentication.**

1. INTRODUCTION

VoIP (Voice over Internet Protocol) is considered to be an alternate of traditional PSTN (Public Switched Telephone Network). VoIP is used for transmitting audio, video and multimedia message over IP network. For relaying over IP network, a flexible, reliable and efficient scheme is needed to handle the audio, video and multimedia session. SIP is a text-based application layer signaling protocol built on the basis of HTTP (Hyper Text Transfer Protocol) or SMPT (Simple Mail Transfer Protocol). The connection between sender and receiver is peer-to-peer including request and response messages. IP is standardized by the IETF (Internet Engineering Task Force), and it is used as a signaling protocol to control communications on the internet for establishing, maintaining and terminating an interactive multimedia session among participants.

SIP is not limited to Voice over IP or Telephony over IP and instant messaging, but it can be used by various applications such as online game as well [1]. Fig. 1 shows SIP message structure while Fig. 2 indicates a flow chart for a simple SIP callee who uses SIP services.

The security system of SIP has three major portions i.e. authentication, communication, and trust. SIP authenticates peers, then develops session and finally guarantees the confidentiality and integrity of data. When a new user desires to avail the services of SIP,

[1] Department of Computer Science and IT, University of Malakand, Chakdara, 18800, Pakistan
Email: [a]saeedullah@uom.edu.pk (Corresponding author), [b]fawadqayum@uom.edu.pk, [c]ajabkhan@uom.edu.pk

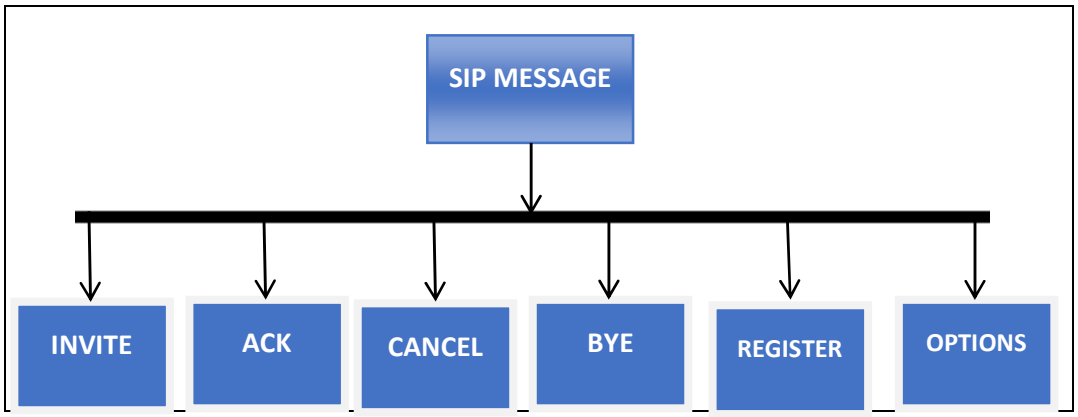


FIG. 1. SIP MESSAGE STRUCTURE

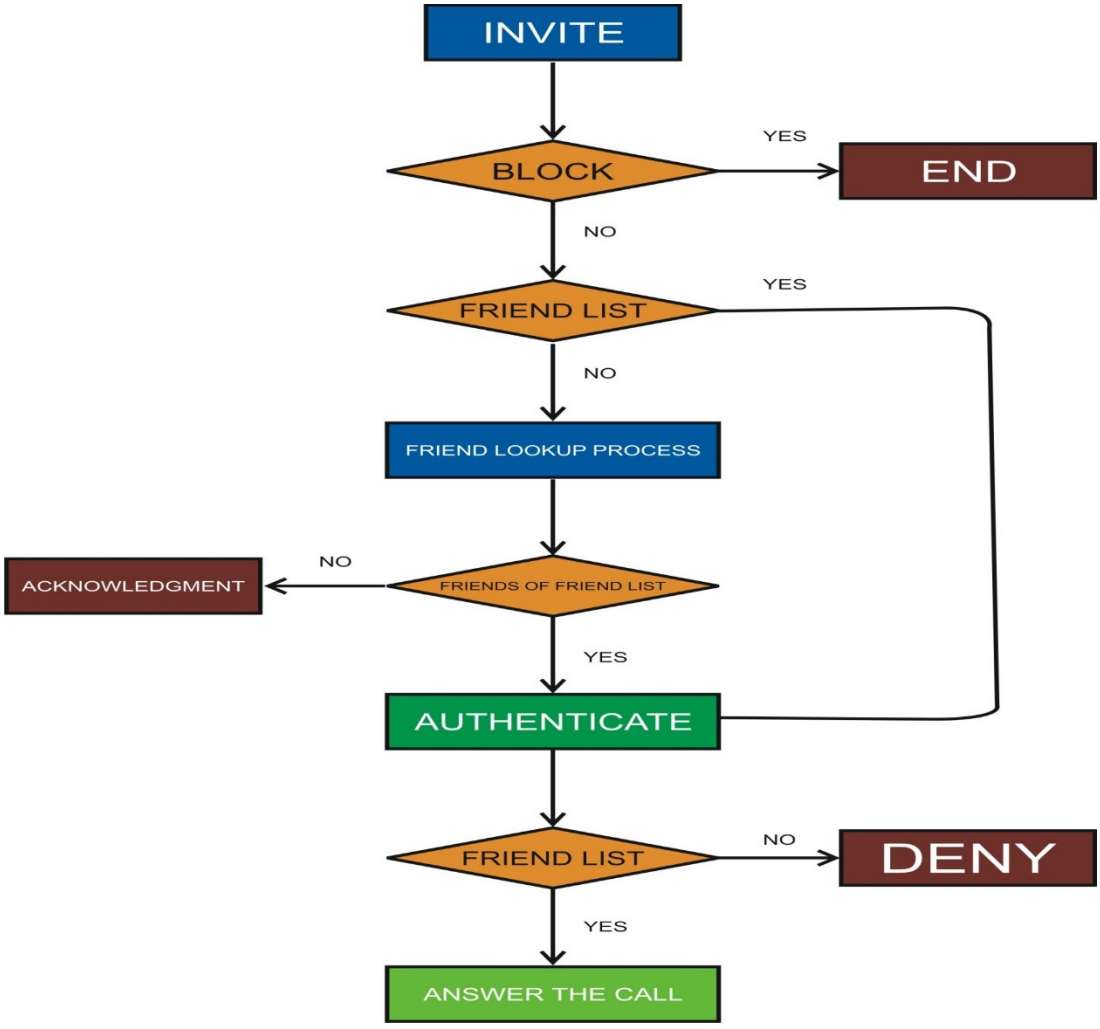


FIG. 2. WORKING PROCEDURE FLOW CHART OF SIP CALLEE

he/she has to enroll first by providing all necessary credentials, overlay algorithm, addresses and stored XML (Extensible Markup Language) file etc. and then bootstrap peer network securely transmits data among them.

1.1 Working Procedure of SIP

Let Alice desires to call Bob; these steps will be taken using SIP-based VoIP authentication protocol.

Step-1: Alice sends a request message from her terminal, the terminal send INVITE message to the Proxy Server and Proxy Server is trying a message to Alice.

Step-2: DNS (Domain Name System) server processes the query of the already connected proxy server and gives a response to it.

Step-3: The proxy server now sends an invitation message to the proxy server nearly connects Bob and exchange trying message to the proxy server connect Alice.

Step-4: Meanwhile the DNS server attached to the proxy server that nearly connects Bob can process the query and transmit a response message.

Step-5: The proxy server that nearly connects Bob can send an INVITE message to Bob's terminal, where sends a ringing tone to the nearly proxy server.

Step-6: The nearest proxy server to Bob relays ringing message towards the nearest proxy server of Alice and finally to Alice.

Step-7: Similarly, The nearest proxy server to Bob sends an OK message to Bob and then to the proxy server near to Alice and finally to the Alice.

Step-8: So, both the peers securely verify each other and communication among them become established, as shown in Fig. 3.

1.2 Preliminaries and Definitions

Protocol: A set of rules defines for sharing information remotely between peers.

Authentication: The legality of peers is termed as authentication.

Hash Function: A technique through which data of arbitrary size is converted into fixed length value, but will never reverse to its original format.

Cryptography: The art of protecting data.

Symmetric Cryptography: A technique used for secure communication using the same key at both ends for encryption/decryption purposes.

Asymmetric Cryptography: A technique used for secure communication using different keys at both ends for encryption/decryption purposes.

Elliptic Curve Cryptography: An Asymmetric lightweight cryptographic technique for protecting information based on the principle of the algebraic structure of elliptic curves over a finite field.

Cryptanalysis: The art of breaking a cryptographic protocol or breaching of cryptographic security principle and achieves access to the hidden contents of a message.

1.3 Designing Ingredients for SIP

Before designing SIP authentication scheme, the following features should be crucial for such an environment.

Sensitivity: The scheme should detect all kinds of active attacks like modification and manipulate of message contents.

Robustness: The authentication scheme should have an algorithm that has the ability to tolerate message content and preserving its manipulation.

Localization: The designed scheme must have the ability to locate the message from where it generates.

Recovery: Recovery of any modified, temper message and identification of the region from where it is tempered is also being a feature in an authentication scheme.

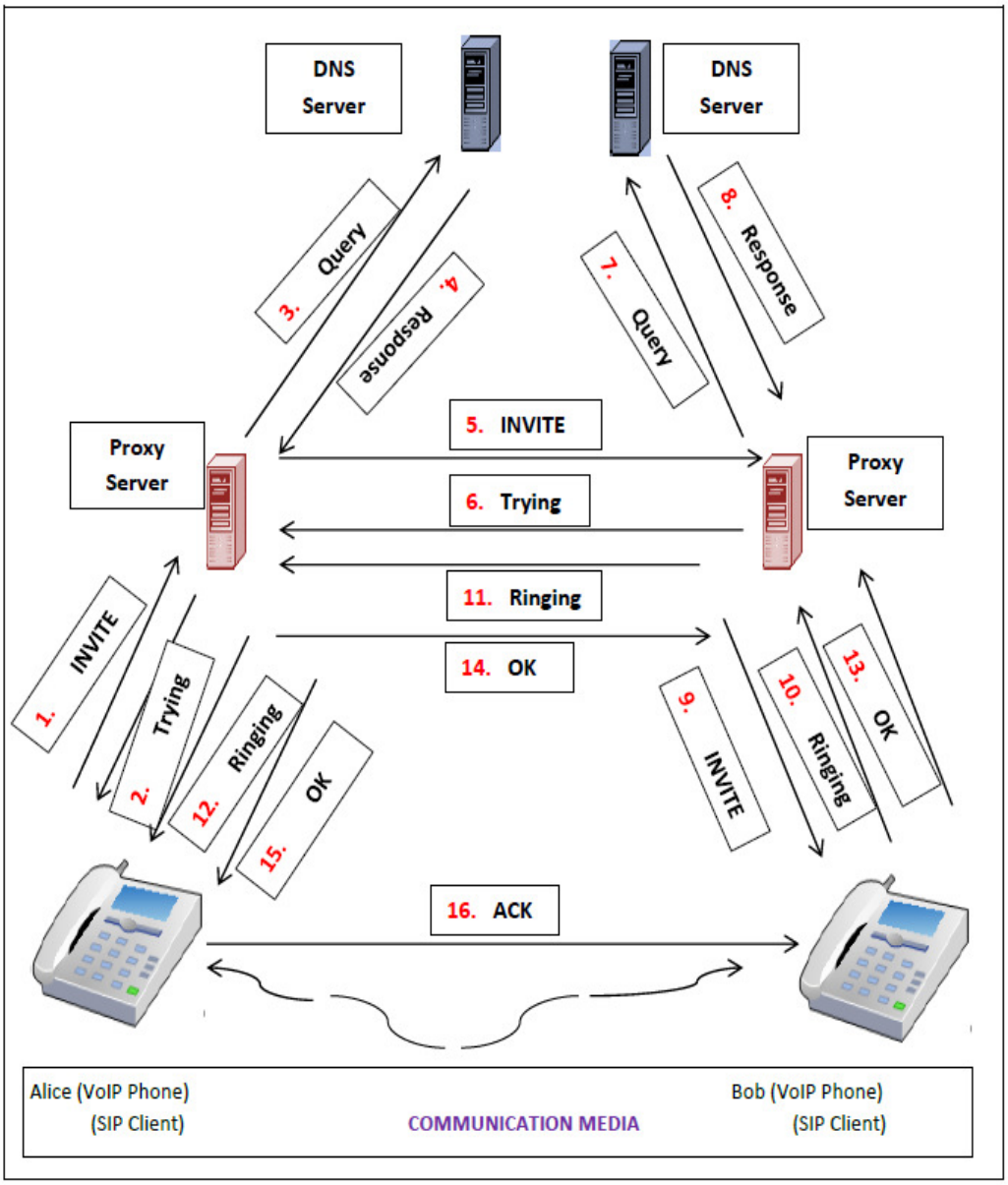


FIG. 3. WORKING SCENARIO FOR SIP CALLER [26]

Security: Protecting the message from any unauthorized access is also an ability that exist an authentication scheme.

Portability: Conveying of a digital signature with the original message during the communication process and other necessary operations are also features that might exist in an authentication scheme.

Complexity: Actually, the applied algorithm used by an authentication system is neither complex nor slow means effective (secure and fast).

1.4 Common Security Flaws in SIP

As SIP expose to several attacks and catch much attention of the researchers for making it secures, yet no one claim with conviction about a foolproof secure SIP-Based-VoIP authentication protocol. Common threats of SIP are as under:

(a) **Sybil Attack:** A type of attack that controls part of the overlay network.

(b) **Partition attack:** The bootstrap provides false information to the legal peers and prohibited the normal initialization of the session.
(c) **Eavesdropping:** A third party shows as legal peer to the joining peers, or record the session of one peer, later on, show as legal peer to the other peer.
(d) **Eclipse Attack:** The third party control and hijack the overall session of legal peers.
(e) **Impersonation**: The third party change, temper and misroute the session transmission of data of legal peers.
(f) **DOS (Denial of Service) Attack:** An attacker may bombard the server with many false requests that would affect its routine operations or hanged the associated peripherals.
(g) **Replay Attack:** If an attacker sends an older message and struggle by changing the new message for disturbing the communication session of legal peers.
(h) **Spam (Special Processed American Meat):** Here exists a chance of ringing false tone on android where many applications use SIP; like Skype, IMO, Viber, Google voice and WhatsApp etc.

1.5 Cryptographic Primitives for SIP

Designing an authentication scheme/protocol by using cryptographic primitives is challenging job from the perspective of performance and security. As both are contradicting features, the change in one inversely affects others. Therefore, hundreds of techniques were used by different researchers for designing schemes. But two methods that we are discussing here have a great extent in the recent technological era, because attackers become stronger for browsing illegal information in both active and passive manner.

Asymmetric Technique: Asymmetric cryptography is a vast field for crypto purposes. Here a simple approach for the popular asymmetric technique has explained along with a suitable example in the following steps:

Method – 1: RSA Method [27]

(i) In the first step two large prime numbers, p and q be chosen.
(ii) In the second step, the value of n which is equal to p×q can be calculated using "Euler's Totient Function" i.e. n= where $\Phi(n)=(p-1)\times(q-1)$.
(iii) Assume "e" chooses for encryption so that gcd(e, $\Phi(n)$}=1, where gcd means greatest common divisor.
(iv) Assume "d" chooses for decryption, so that d×e mod $\Phi(n)$=1, then public key is equal to {e, n} and private key be {d, n}.
(v) For encryption $C=M^e$ mode n formula be used, where C=Cipher text
(vi) And for decryption $M=C^d$ mode n will be used, where M=Plain text

Example:

- Let suppose two random prime number p=5 and q=7 are chosen
- The values of n is p×q which is 5×7=35 and

$\Phi(n)=(p-1)\times q-1)$
$=(5-1)\times(7-1) = 4\times6 =24$
Let suppose, e=5

Then gcd(e, $\Phi(n)$)=1
=gcd(5, 24) =1
So, e=5
And d×e mod n = d×5mod 24
=5
Therefore, d=5
From these results Public Key={e, n}={5, 35}
And Private key={d, n}={5,35}
Now, let message M=3 is taken on sender-side which is less than n because M must be less than that of n. So, we know that $C=M^e$ mod n
$= 3^5$ mod 35
=243 mod 35
= 33
While $M=C^d$ mod n
$=33^5$ mod 35
=39135393 mod 35
=3 we get M=3 on the receiver side. It means that 3 is secretly passed from sender to received.

Method – II: Digital Signature Algorithm (DSA)

This is another asymmetric cryptographic technique uses two sub-techniques to be proved. The DSA (**Digital Signature Algorithm**) using the RSA approach is given below with suitable example:

SENDER	RECEIVER
Let Message M is sent by a sender First, one-way hash function be applied, then Private Key will add with the hash code, and Concatenated with the hash code along with the original message Then encryption is done And sent over a public channel	
	Here a one-way hash function to the received message be performed decryption of the received encrypted message will perform both hash code and received the decrypted message will match for authentication, if not equal the process terminates else secure communication will be established and transmission session starts securely.

The whole procedure of DSA using RSA approach can also be cleared diagrammatically in Fig. 4.

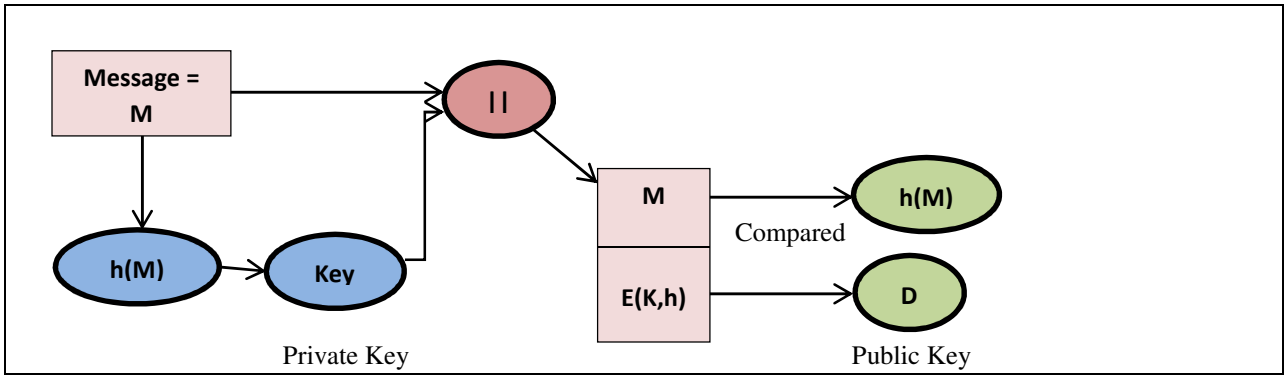


FIG. 4. DIGITAL SIGNATURE USING RSA

Method – III: Digital Signature Standard (DSS):
The DSA is a bit weaker methodology, to make it stronger a DSS approach is used for ensuring information security. The DSS approach used in DSA consists of global parameters that couldn't calculated easily by an attacker. The methodology used in this approach is given below:

(a) First of all, chooses two prime numbers p and q, the prime number p lies between $q^{L-1}<p<q^{L}$ and L is an integer number of 64 bits and q is the prime divisor of (p-1).Now $g=h^{(p-1)/q}$ mod p where h is not representing the one-way hash code actually it is an arbitrary another integer value.

(b) A large integer number x chooses called private key whose values lies between p and q.

(c) The public key $y=g^{x}$ mod p by adding k an integer number. Therefore, p, q, y, g are public parameters while x and k are privately used for signature function as shown in Fig. 5.

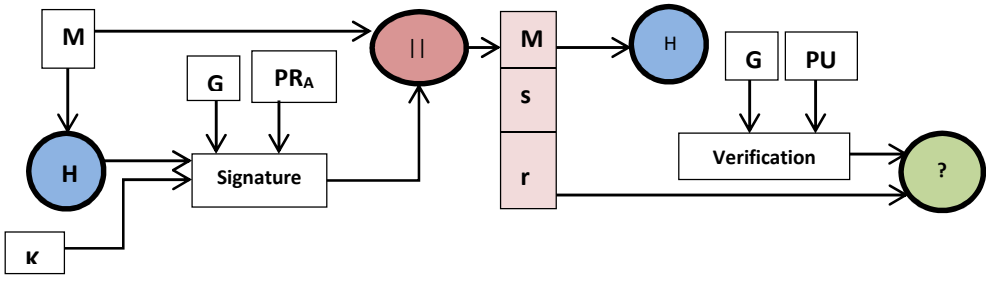


FIG. 5: DIGITAL SIGNATURE USING DSS

The necessary calculations in this approach are as under:

$r=(g^x \bmod p) \bmod q$
$s=[k^{-1}(h(M)+x.r] \bmod q$
Verifying function
$v=[(g^{u1}, y^{u2}) \bmod p] \bmod q$
$u1=[h(M^{/})w] \bmod q$
$u2=[(r\}^{/}w] \bmod q$
where $w=(s^{/})^{-1} \bmod q$
$(M^{/}, r^{/}, s^{/})$

And compare v with r i.e. $v?=r^{/}$

PS: G=Global Elements, PR_A=Private Key, PU_A=Public Key and H=Hash Function which is Secure Hash Algorithm or Message Digest (SHA-254 or MD5). In this approach two functions are used, one is a signature function in the sender side while the other is verification function on the receiving side.

1.6 Our Main Contribution

1. We present a feasible and secure SIP-based-VoIP system. A SIP callee using VoIP key agreements scheme to secure voice packets.

2. Legitimate users can avail our SIP services and associated resources; we propose an efficient and secure authentication mechanism in SIP registration process.

3. A lightweight authentication scheme with provable security analysis is presented in this paper which shows a gentle balance between security and performance.

4. The proposed scheme has the ability to resists all know attacks. This is verified in the informal security analysis section of the paper.

5. SIP background and cryptographic primitives have presented for the very beginners in this work which shows the importance of SIP using VoIP.

2. LITERATURE REVIEW

The security of VoIP authentication scheme like SIP is a challenging task and many researchers proposed different mechanism for protecting the said signaling protocol from common flaws. In this regard, Hsieh and Leu [2] proposed Diffie-Hellman key exchange technique in which two parties set secret session by using cyclic Group-G of order n and the random selection of a big prime number using ECC (*Elliptic Curve Cryptography)* values in different curves. But failed due to high computation and communication cost. Meanwhile, Sureshkumar *et al.* [3] cryptanalyze the Leu *et al.* [2] scheme by highlighting some loopholes including impersonation and replay attacks; and they demonstrated an improved technique based on ECC. Then, Kumari *et al.* [4] highlighted anonymity and mutual authentication issues in Lu *et al.* [2] scheme and presented another ECC based improved technique that guaranteed for anonymity and mutual authentication. But Kumrari *et al*. scheme cryptanalyze by Qiu et al. [5] and supposed that their scheme has failed to provide perfect forward secrecy due to lacks of the pre-verification of smart card. Moreover, the scheme of Qiu *et al.* [5] failed to resist desynchronization attack and also completed in two to three round trips.

The prominent asymmetric cryptographic technique (ECC) has the ability to guarantee security as like that of RSA technique, smaller key size, and lightweight in nature. In this way, Chaudhry *et al.* [6] proposed an authentication scheme for SIP using ECC cryptographic technique. They highlighted all the weakness of Tu *et. al.* [7] and Farash *et al.* [8] schemes, that these schemes are suffering from impersonation, no anonymity, and DOS attacks. Also vulnerable to masquerade and replay attacks. After it, Kumari *et al.* [9] cryptanalyses of Farash *et al.* [8] scheme and proposed an improved version of it. They said that an adversary can easily intercept and inject false information over an open network channel. They also claim that the using Elliptic Curve Discrete Logarithmic Problem [10] and Elliptic Curve Computation Diffie-Hellman technique [11], it is not possible for anyone to break the internal credentials of the session shared key and injects false information.

Since, authentication schemes are widely deployed for mobility, access control and transmission of a secret over a communication channel. The SIP is much attractive widely used among several authentication schemes. Recently, Farash [12] proposed a multifactor

authentication scheme for SIP without a verification table in the server. He breaks Zheng *et al.* [13] scheme and claim that their scheme couldn't resist masquerade attack and the session key is not secure among different peers. He then proposed a robust scheme based on ECC by keeping a point at infinity on the curve so that an attacker cannot challenge the legitimacy of the peers.

Furthermore, Azrour *et al.* [14] worked on solving the DOS attack in the SIP-based-VoIP authentication scheme of Farash et. al. work. While Cao *et al.* [15] explains SIP architecture, different security threat and necessary steps to be taken in near future for protecting information using SIP. Similarly, [16] recommended that SIP has to be designed in a way that shows strong resistance to un-traceability, masquerading and password guessing attacks. And Mishra *et al.* [17] suggested a threat model to guarantee the legitimacy of the peers. Our next portion will focus on the review analysis of Mishra *et al.* [17] scheme.

2.1 Review Analysis of Scheme [17]

In this section, the review analysis of scheme [17] is presented in detail. Scheme [17] consists of initialization, registration, login, authentication/key agreement and password/biometric change/update phases. These phases are described one by one under the following headings:

Initialization Phase: The initialization phase of scheme [17], S first chooses an arbitrary unique master key mk, a big prime number P, nonce N and $h(\cdot)$ a one-way hash function. Then S calculates the public key mkP and lastly, S sorts mkP with $h(\cdot)$ to keep mk a master secret key.

Registration Phase: In the registration phase of scheme [17], U_i first selects his/her identity username in S and receive a personalized smart card from the owner. The following set of computations is performed in this phase:

S1: U_i chooses his/her identity username and password PW_i, a random number r and calculate the pseudo-password $RPW_i=h(r||PW_i||username)$. The registration demand {username, RPW_i} is put towards S through a private communication line.

S2: After receiving {username, RPW_i} message, the S first verifies the parameters of username and authenticates whether username exists in its record database or not, if found, S request another identity, else S uses mk and calculate $X_i=h(mk||username||N)$ and $Y_{ia}=X_i \oplus RPW_i$,

S3: Meanwhile, U_i also generates biometrics Bi and calculates $V=h(username||PW_i||H(B_i))$ and $R=r \oplus H(B_i)$, and keep R and V in the memory of smart card as shown in Module 1.

User(U_i)	Secure Channel	Server (S)
Select r, username and PW_i		
Compute $RPW_i = h(r\|\|PW_i\|\|username)$		
	{username, RPW_i} →	
		Compute $X_i = h(mk\|\|username\|\|N)$, $Y_i = X_i \oplus RPW_i$, mkP
	← {Y_i, mkP, h()}	
Compute $V = h(username\|\|PW_i\|\|H(B_i))$, $R = r \oplus H(B_i)$. Store V and R into the smart card		

MODULE 1. REGISTRATION PHASE OF SCHEME [17]

Login Phase: In this phase of scheme [17], U_i desires ton login to S. He/She provides his/her identity username, password PW_i and generates biometrics Bi. Smart Card checks these parameters and puts a login request by performing the following commutations steps:

S1: Upon receiving the inputs {username, PW_i, B_i}, authenticates the currently computed V

with stored V?=h(username||PW_i||$H(B_i)$). If not holds, the process will terminate, else, these computations will perform $r=R\oplus H(B_i)$, $RPW_i=h(r||PW_i||username)$ and $X_i=Y_{ia}\oplus RPW_i$.

S2: A random number u and big numerical number P that was previously stored by the server in smart card memory will initialize uP, u.mkP and $D_1=h(username||Xi||(u.mkP)_x||(uP)_x||T_1)$, $DID_i=username\oplus h((u.mkP)_x)$, and sends $\{DID_i, D_1, uP, T_1\}$ message to S through an open network channel as shown in Module 2.

Authentication & Key Agreement Phase: In this activity of the scheme [17], when S receive $\{DID_i, D_1, uP, T_1\}$ message from U_i, the S first checks the originality of the received message. If not validate the user's message, further computations stop and the process terminates, else, the following set of computation proceeds.

S1: The server S compare the timestamp T_1 with the server time T_2 i.e. $T_2-T_1=\Delta T$ if not lies in the time threshold, the server discard, else, S calculates $(mk.uP)_x$, and recovers identity username by calculating $DID_i\oplus h((mkuP)_x)$. The S also computes h(mk||username||N) and authenticate D_1?=h(username||X_i||$(mk.uP)_x$||$(uP)_x$||T_1) with the received D_1. If the authenticity of D_1 does not hold, S rejects the whole message else, S agrees to take the message.

S2: Next, S calculates the secrete session key $sk=h(username||X_i||(mk.uP)_x||T_1||T_3)$, $D_2=h(sk||T_1||T_3||(mk.uP)_x)$ and relays {realm, D_2, T_3} message towards Ui through an open communication channel.

S3: The U_i first checks the validity of the message by applying the condition $T_4-T3\leq\Delta T$. If verification is ok, U_i calculates the secret session key $sk=h(username||X_i||(mk.uP)_x||T_2||T_3)$, $D_2=h(sk||T_1||T_3||(u.mkP)_x)$ and keep sk is the authentic shared session key and both the peers authenticate each other as shown in Module 3.

User (U_i)	Public Channel	Server (S)
Input username and PW_i, imprint Bi,		
Verify V ?= h(username||PW_i||$H(B_i)$)		
Compute $r = R\oplus H(B_i)$ and $RPW_i = h(r\|\|PW_i\|\|username)$, $X_i = Y_i\oplus RPW_i$		
Generate random number u.		
Computer uP, u.mkP. $D_1 = h(username\|\|X_i\|\|(u.mkP)\|\|(uP)_x\|\|T_1)$		
$DID_i = username\oplus h((u.mkP)_x)$.		
	$\{DID_i, D_1, uP, T_1\}$ →	

MODULE 2. LOGIN PHASE OF SCHEME [17]

User (U_i)	Public Channel	Server (S)
		Verify $T_2 - T_1 \leq \Delta T$. If valid,
		Compute mk.uP, $username=DID_1\oplus h((mk.uP)_x)$,
		$X_i = h(mk\|\|username\|\|N)$.
		Verify D_1?=h(username||$(mk.uP)_x$||$(uP)_x$||T_1).
		If valid, compute $sk=h(username\|\|X_i\|\|(mk.uP)_x\|\|T_1\|\|T_3)$,
		$D_2 = h(sk\|\|T_1\|\|T_3\|\|(mk.uP)_x)$.
	← {realm, D_2, T_3}	
Verify $t_4 - T_3 \leq \Delta T$.		
If valid, compute		
$sk = h(username\|\|X_i\|\|(u.mkP)_x\|\|T_2\|\|T_3)$.		
Verify D_2 ?= $h(sk\|\|T_1\|\|T_3\|u.mkP)_x$).		
If valid, accept sk.		

MODULE 3. AUTHENTICATION & KEY AGREEMENT PHASE OF SCHEME [17]

Password & Biometric Updating Phase: If a user U_i wants to change his/her password or updates his/her biometrics, he/she has to passes from the following steps

S1: Compute $r=R\oplus H(B_i)$, pseudo password $RPW_i = h(r||PW_i||username)$, $X_i=Y_{ia}\oplus RPW_i$, $RPW_i^{new}=h(r||PW_i^{new}||username)$, $Y_{ia}^{new}=X_i\oplus RPW_i^{new}$, $V^{new}=h(username||PW_i^{new}||H(B_i^{new})$ and $R^{new}=r\oplus H(B_i^{new})$.

S3: Interchange Y_{ia} with Y_{ia}^{new}, R with R_{ia}^{new} and V with V^{new}. as shown in **Module 4**.

2.2 Drawbacks of Scheme [17]

In this section, different security weaknesses of the scheme [17] will be discussed in detail. A through careful analysis, the following flaws are noted; details of these weaknesses are as under:

Denial-of-Service Attack: The first weak point is that any unauthorized user can straightforwardly launch Denial-of-Service attack with fake authentication requests such as $\{DID_i, D_1, uP, T_1\}$ with fresh timestamp T. The server will first check the timestamp's validity which might pass easily. But, further computations by the server could take time for searching the corresponding contents on the stored database. After so many calculations it will find that the request is invalid. This is a serious demerit of the scheme. Because a hacker sends a fake message towards server which it processed its computations as usual. Similarly, the server checks thoroughly the whole message but in the end, it finds that it is from a hacker. The server immediately discards it but at the same time received another message. Nevertheless, it is a serious issue or problem where the hacker bombards the main server. In this way, the utility of the server is effected which need to be resolved.

Un-Traceability Attack: Secondly, the Mishra's scheme does not provide un-traceability to the user as there is u parameter that remains constant in every session. Such a parameter could be used to trace a particular user's location. At least it exposes the protocol as far as privacy is concerned, as an attacker could easily analyze that any two sessions recorded in different time periods were launched by the same person. In this way, the user can be identified easily. Not only the user, but its location, address and the sensitive information too can be traced. It is because through this way a single user from a single ID in multiple attempts can initiate the session which can help trace a legitimate user. Therefore, it does not provide privacy of the subscriber.

Online Password Guessing Attack: Thirdly, even if a service provider receives an authentication request from a legitimate user, the Mishra's scheme does not illustrate that how the server would find the related user's parameters {u, uP, mk.uP} from the repository, as there may be hundreds of subscribers registered on that server also the user is not submitting its identity in authentication request in any form that could enable the service provider to search its related parameters from the database. If we suppose that server would find those parameters on the basis of mk then what if the subscriber modified its password. Because any password modification upgrades r factor and ultimately N is also upgraded.

User(U_{ia})	**Smart Car**
Input username, PW_i and B_i. Verify $V = h(username||PW_i||H(B_i))$.	
	If verification holds, proceed.
	nput PW_i^{new} and B_i^{new}
	Compute $r = R\oplus H(B_i)$
	$RPW_i = h(r||PW_i||username)$,
	$X_i = Y_i \oplus RPW_i$,
	$RPW_i^{new} = h(r||PW_i^{new}||username)$,
	$V^{new} = h(username||PW_i^{new}||H(B_i^{new}))$,
	$R^{new}= r \oplus H(B_i^{new})$,
	$Y_i^{new} = X_i \oplus RPW_i^{new}$
	Replace Y_i, R and V with Y_i^{new}, R^{new} and V^{new}, respectively

MODULE 4. PASSWORD AND BIOMETRIC UPDATE PHASE OF SCHEME [17]

De-Synchronization Attack: The scheme presented by [17] is suffering from de-synchronization attack in which the shared secrets from synchronous storage might lead the unavailability of service. An adversary interferes the integrity of sensitive information which might lead failure of the synchronous storage area. The adversary overpowering a fake message between server and remote user due to which the protocol couldn't communicate and no longer possible for it to ensure security. Thus scheme [17] is suffering from a de-synchronization attack.

If U_i begins a new session using the random integer values u, S_i should discard the session due to which the server S find that the message is illegal. The issue in these {DID_i, D_1, uP, T_1}, {realm, D_2, T_3} messages is that every time it changes its parameters in the login, authentication and key agreement phases of the scheme. If someone disturbed the normal session, the S_i alter the legitimate user's credentials in its database while the U_{ia} does not change the entire corresponding values, therefore, de-synchronization attack will take place in the next login. Similarly, N is requiring more bit space than identity ID_i or mk. Then how XOR operations in Mishra's protocol could take place for (ID_i, N), (X_i, mkP and Y_i) and mk.uP operations.

3. PROPOSED SOLUTION

In this section, the proposed scheme will be designed, consists of four phases including Registration Phase, Login & Authentication Phase, Password Change Phase, and Card Revocation Phase. Different notations used for the proposed scheme are shown in Table 1.

3.1 Registration. Login & Authentication Phases

Registration: In this phase of the scheme, U_{ia} first registers with his/her identity id to the S_{ia}. The below steps will perform:

S1: U_{ia} first selects his/her identity id, PW_{ia}, a large number r and imprints biometrics B_{ia}. The user biometrics is first XOR with the random number r and then applying a hash function called BioHashing $HB=B_{ia}\oplus r$ and $O=h(HB)$. The pseudo password $PPW_{ia}=r||PW_{ia}||id$, $Q=h(PPW_{ia})$ and relay {id, Q} message through a secure channel to the server.

S2: After obtaining the registration request, S_{ia} authenticates the parameters of U_{ia} and checks whether id exists or not in its database. If id exists, S_{ia} asks for a new identity, else, S_{ia} uses its own master key mk, large prime number P, nonce N and computes $J=mk||id||N$), $X_{ia}=h(J)$ and $M=X_{ia}\oplus Q$ along with server master key mk and large prime number P i.e. mkP and submit {M, mkP and hash code h(.)} towards the server S_{ia}.

S3: The sender means user U_{ia}, $V=h(id||PW_{ia}||O)$ and stores V and O in the memory of smart card for future usage.

Login: The legitimate user U_{ia} if desires to login the remote server S_{ia}, he/she has to provide id, PW_{ia} and generate biometric B_{ia}^* using a sensor. U_{ia} authenticate the originality of biometrics B_{ia}^* with B_{ia} by extracting biometrics in raw data form, passes from an image processing system, important features will extract and BioHashing function will be applied and then the decision made using matching algorithm Δ, $HB^*=B_{ia}^*\oplus u$, $O^*=h(HB^*)$. If the decision is Yes, pass else deny and the process will terminate.

TABLE 1. NOTATIONS & ITS COMPLETE DESCRIPTION

Symbol	Description	Symbol	Description
U_{ia}	User	S_{ia}	Server
id	Identity of user Uia	PW_{ia}	Password of user U_{ia}
B_{ia}	Biometric information of U_{ia}	mk	Master key of S_{ia}
P	A large prime of 512 bits	u	Random Number
$H(\cdot)$	Secure BioHashing function	$h(\cdot)$	collision-free hash function
ΔT	Time Threshold	T	Timestamp

S4: Next, the remaining credentials should also matched i.e. V with V^* by performing this computation step. $V^*=h(id||PW_{ia}||O^*)$). If $V^*?=V$ verify, and onward computation $r=Q\oplus O^*$, $PPW_{ia}=h(r||PW_{ia}||id)$ and $X_{ia}=Y_{ia}\oplus PPW_{ia}$, whereas PPW_{ia} is a pseudo password.

S5: Chose a number u, and compute uP, u.mkP and $D_1=h(id||X_{ia}||(u.mkP)_x||(uP)_x||T_1)$. The dynamic identity $DID_{ia}=id\oplus h((u.mkP)_x)$ will calculate and transmit $\{DID_{ia}, D_1, uP, T_1\}$ message towards server S_{ia} through an open network channel as shown in Figure 10.

Authentication: In this phase of the proposed scheme, the following computations will perform:

S6: When the server receives $\{DID_{ia}, D_1, uP, T_1\}$ message from U_{ia}, S_{ia} check the time threshold
with the next time $T_2-T_1=\Delta T$. If comes under the jurisdiction of the predefined time threshold, S_{ia} calculates $(mk.uP)_x$, and check the id from this equation $DID_i\oplus h((mkuP)_x)$. S_{ia} computes $h(mk||id||N)$, and authenticate the condition $D_1?=h(id||X_{ia}||(mk.uP)_x||(uP)_x||T_1)$, if authentication result becomes successful, further login request will proceed, else deny and the process will terminate.

S7: Next, the S_{ia} proceed computation process by calculating the session shared key "sk" using server master key, random number of 100 digits and current timestamp T_3 and U_{ia} timestamp T_1 i.e. $sk=h(ide||X_i||(mk.uP)_x||T_1||T_3)$, and then challenge a message {realm, D_2, T_3} towards U_{ia} through public channel, where $D_2=h(sk||T_1||T_3||(mk.uP)_x)$ and realm is message digest MD5 of 512 bits.

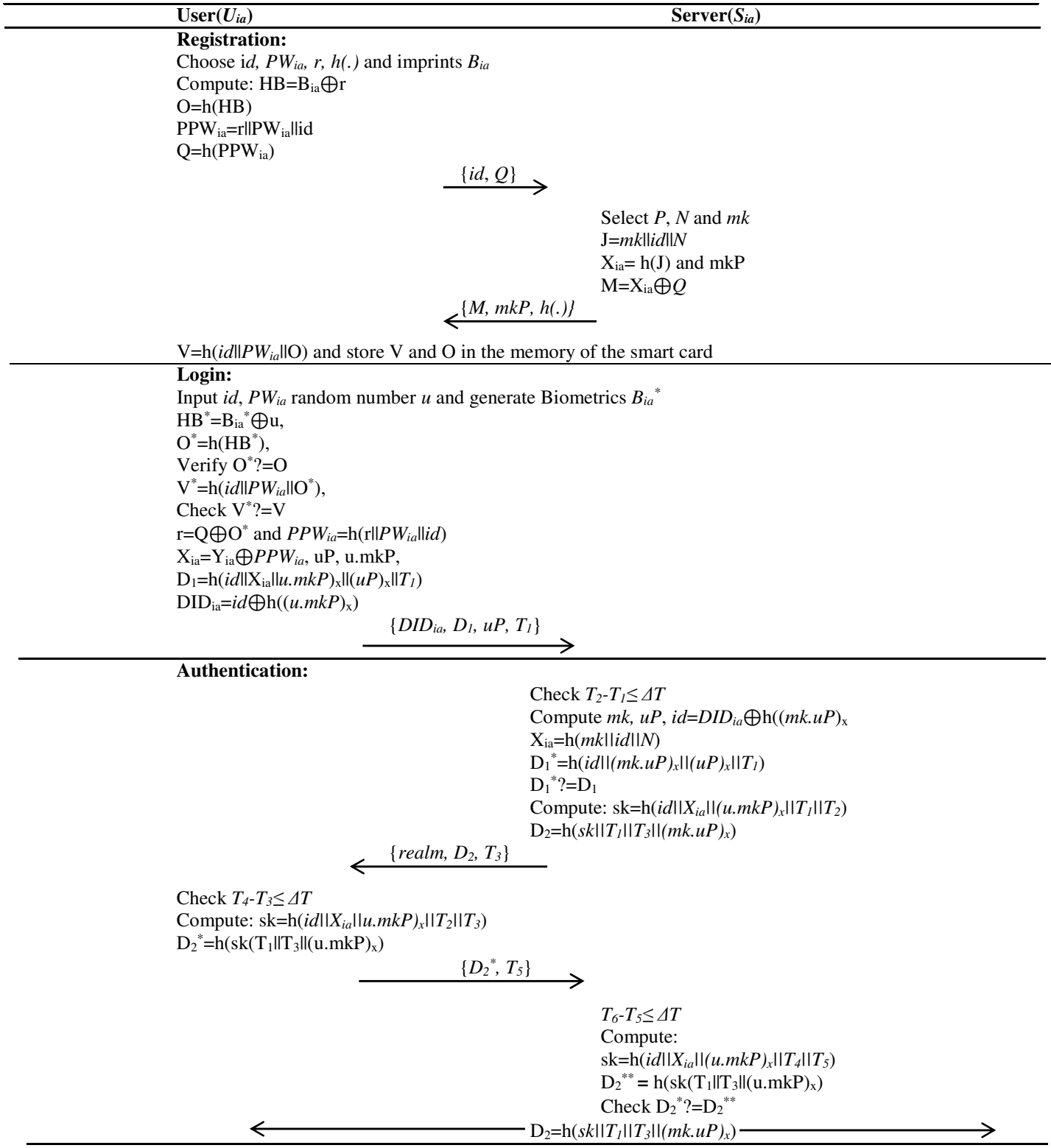
S8: The U_{ia} when receiving {realm, D_2, T_3} message checked with the timestamp of user which is T_4, $T_4-T3\leq\Delta T$. If lies in the jurisdiction of user time threshold, computation proceed else deny and termination takes place. The U_{ia} also calculate the shared session key "sk" i.e. $sk=h(id||X_{ia}||(mk.uP)_x||T_2||T_3)$, and authenticate the condition $D_2=h(sk||T_1||T_3||(u.mkP)_x)$. If not authenticated, the session terminates else U_{ia} send a response message $\{D_2^*, T_5\}$ towards the server to validate and share sk is a valid session key as shown in **Module 5.**

3.2 Password & Biometric Updating Phase

Whenever U_{ia} desires to changes/updates his/her PW_{ia} and the predefined template of biometrics in the storage record of the memory of a smart card, he/she has to insert his/her smart card in the terminal/device and input PW_{ia} and id and generate biometrics using a sensor. The smart card first authenticates the recent credentials by performing some computation $V=h(id||PW_{ia}||H(B_{ia}))$. After the successful authentication of credentials, the user U_{ia} will be asked to provide fresh PW_{ia}^{new} and biometric B_{ia}^{new}, and the smart card recover $r=R\oplus H(B_{ia})$ and compute the pseudo password $PPW_{ia}=h(r||PW_{ia}||id)$ and $X_{ia}=Y_{ia}\oplus PPW_{ia}$. The newly password PW_{ia}^{new} and other computation steps for changing password and updating biometric will be $PPW_{ia}^{new}=h(r||PW_{ia}^{new}||id)$, $Y_{ia}^{new}=X_{ia}\oplus PPW_{ia}^{new}$, $V^{new}=h(id||PW_{ia}^{new}||H(B_{ia}^{new})$ and $R^{new}=r\oplus H(B_{ia}^{new})$. Finally, Y_{ia} replaces by Y_{ia}^{new}, Q by Q_{ia}^{new} and V by V^{new}.

3.3 Card Revocation Phase

If the smart card is stolen or lost, prevention from de-synchronization attack or a legal user desire to leave an organization etc. safely finishing of the session is necessary. To do so, the U_{ia} enter his/her previous id and the new updated PW_{ia}^{new}, the system then computes $h(id||PW_{ia}^{new})$, random number r is calculated $r=Q\oplus H(B_{ia})$, compute $PPW_{ia}=h(r||PW_{ia}||id)$ and transmit $\{id, h(id||PW_{ia}^{new})\}$ towards server S_{ia} through a secure channel. After receiving $\{id, h(id||PW_{ia}^{new})\}$ message, the S_{ia} a big prime number P^*, master key mk^* and compute: uP^*, $u.mk^*P^*$, $id^{new}=DID_{ia}\oplus h((u.mk^*P^*)_x$, $X_{ia}^{new}=h(mk^*||id^{new}||N)$ and $D_1^{new}=h(id^{new}||(u.mk^*P^*)_x||(uP^*)_x||T_1)$. The server swap P and mk with P^*, mk^* in its record for the legal user and inject $\{h(.), D_1^{new}, X_{ia}^{new}, id_{new}\}$ into its database. U_{ia} now computes $O^{new}=h(B_{ia}\oplus r)$ and $V^{new}=h(id^{new}||PW_{ia}^{new}||O^{new})$ and keeps O^{new} and V^{new} instead of O and V.



MODULE 5. REGISTRATION, LOGIN AND AUTHENTICATION PHASES OF THE PROPOSED SCHEME

4. SECURITY ANALYSIS

Security analysis is the most important feature for verifying the strength of a protocol, which means how to analyze and design cryptographic protocols based on the idea of system engineering and trusted. Questions of belief are essential in analyzing protocols for the authentication of principals in distributed computing systems. Therefore, in this section, we present the formal methods for analyzing the proposed scheme by two techniques i.e. BAN logic and verification toolkit ProVerif1.93; and informal methods using assumptions. The analysis shows that the proposed scheme is effective and efficient for SIP-Based-VoIP authenticity and authorization and strongly recommended to be implemented for it. These two methods are described one by one under the following headings:

4.1 Formal Analysis using BAN Logic

The BAN logic was named after its inventors, Mike Burrows, Martin Abadi, and Roger Needham – the logic of competences, belief, and action [18]. BAN logic proofs an authentication scheme that deserves to be treated with grave suspicions and build trust. This is a formal method that mathematical checks the robustness and logic of design of a scheme. So, we have formally validated mutual authentication using the BAN. Different notations used are shown in Table 2.

Further, in BAN logic $\frac{P}{Q}$ means if P is trust then Q is also true. For the proposed authentication scheme, these rules are defined as:

Message Meaning

$\frac{U_{ia}|\equiv U_{ia}\overset{sk}{\longleftrightarrow}S_{ia},\lhd\{M\}_K}{U_{ia}|\equiv S_{ia}|\sim M}$, if U_{ia} believes that Uia and Sia share SK, and sees M encrypted with K, then U_{ia} believes S_{ia} once said M.

$\frac{U_{ia}|\equiv \overset{\overline{SK}}{\longrightarrow}S_{ia},\lhd\{M\}_{K^{-1}}}{U_{ia}|\equiv S_{ia}|\sim M}$, if U_{ia} believes that communication with S_{ia} will be made on SK, and sees M decrypted with K, then U_{ia} believes S_{ia} once said M.

$\frac{U_{ia}|\equiv U_{ia}\overset{SK}{\Rightarrow}S_{ia}\lhd\{M\}_Y}{U_{ia}|\equiv S_{ia}|\sim M}$, if U_{ia} believes that the shared session key among us is SK, and sees M encrypted with key Y, then U_{ia} believes S_{ia} once said M.

$\frac{U_{ia}|\equiv \overset{SK}{\Rightarrow}S_{ia}\lhd\{M\}_{Y^{-1}}}{U_{ia}|\equiv S_{ia}|\sim M}$, if U_{ia} believes that the shared session key SK for sending information with S_{ia}, and sees M decrypted with Y, then U_{ia} believes S_{ia} once said M.

Message Integrity

$\frac{U_{ia}|\equiv \#(M),S_{ia}|\sim M}{U_{ia}|\equiv S_{ia}|\equiv M}$, if U_{ia} believes that the freshness of M and that S_{ia} once said M, then U_{ia} believes that S_{ia} trusts M.

$\frac{U_{ia}|\equiv \#(M)}{S_{ia}|\equiv\#(M)}$, if U_{ia} believes on the freshness of M, then S_{ia} also believes on the freshness of message M.

TABLE 2. BAN NOTATIONS AND ITS DESCRIPTION

Notations	Description
$\|\equiv$	Believes For example, P|≡X means P believes message X
$\|\sim$	Once Said For example, P|∼X means P sends a message where exists X
$\lhd$	Sees For example, P⊲X means P sees/understandings X
$\overset{K}{\longleftrightarrow}$	Shared key For example, $P\overset{SK}{\longleftrightarrow}X$ means P and X using K key for mutual information sharing
$\|\Rightarrow$	Jurisdiction For example, P|⇒X means P has jurisdiction on X
#	Fresh For example, P#X means that message X is fresh for P
< >	Combines For example, $\langle X\rangle_Y$, X is combined with Y

Jurisdictional Rule

$\frac{U_{ia}|\equiv S_{ia}|\Rightarrow(M),U_{ia}|\equiv S_{ia}|\equiv X}{U_{ia}|\equiv X}$, if U_{ia} believes that S_{ia} has full controls over M, because it lies in the jurisdiction of both peers; and U_{ia} believes that S_{ia} believes M, then U_{ia} believes M.

Security Goals

So for, we define goals for the proposed authentications scheme first, which are as under:

Goal1: $U_{ia} \equiv S_{ia} \overset{sk}{\longleftrightarrow} U_{ia}$

Goal2: $U_{ia} \equiv S_{ia} \equiv S \overset{sk}{\longleftrightarrow} U_{ia}$

Goal3: $S \equiv S_{ia} \overset{sk}{\longleftrightarrow} U_{ia}$

Goal4: $S \equiv U_{ia} \equiv S_{ia} \overset{sk}{\longleftrightarrow} U_{ia}$

Idealized Scheme

The idealized form shall be defined for the scheme which are:

Message 1: $U_{ia} \rightarrow S_{ia}$:{ DID_{ia}, D_1, uP, T_1}$_x$

Message 2: $S_{ia} \rightarrow U_{ia}$:{realm, D_2, T_3}$_x$

Message 3: $U_{ia} \rightarrow S_{ia}$:{$D_2^*$, T_5}$_x$

Setting of Assumptions

The different assumptions for our scheme are:

Assumption1: $U_{ia} \equiv \#$ (T)

Assumption2: $S \equiv \#$ (r, u, mk, P, Timestamp)

Assumption3: $U_{ia} \equiv S_{ia} \overset{x}{\longleftrightarrow} U_{ia}$

Assumption4: $S_{ia} \equiv S_{ia} \overset{x}{\longleftrightarrow} U_{ia}$

Assumption5: $U_{ia} \equiv S_{ia} \overset{sk= h(id||Xia||(u.mkP)x||T1||T2)}{\longleftrightarrow} U_{ia}$

Assumption6: $S_{ia} \equiv S_{ia} \overset{sk=h(id||Xia||u.mkP)x||T3|T4)}{\longleftrightarrow} U_{ia}$

Assumption7: $U_{ia} \equiv U_{ia} \overset{sk=h(id||Xia||u.mkP)x||T4||T5)}{\longleftrightarrow} S_{ia}$

Assumption8: $U_{ia} \equiv S_{ia} \Rightarrow (D_2^*, T_5)$

Assumption9: $S_{ia} \equiv U_{ia} \Rightarrow$ (Timestamp)

We now use BAN-Logic postulates and rules to prove that user U_{ia} and server S_{ia} can successfully establish the same session key SK as follows. In the first phase, we take Message1 and Message2 for analyzing the scheme:

Message 1: $U_{ia} \rightarrow S_{ia}$:(DID_{ia}, D_1, uP, T_1):{(DID_{ia}, D_1, uP, T_1)}$_x$

By applying the seeing rule:

Seeing S1: $S_{ia} \triangleleft$(DID_{ia}, D_1, uP, T_1):{(DID_{ia}, D_1, uP, T_1)}$_x$

According to Asumption1, Assumption3, and V_{ia}, it is stated that:

Seeing S2: $S_{ia} \equiv U_{ia}$~(DID_{ia}, D_1, uP, T_1)

According to Assumption1, SeeingS2, r, and D_2

Seeing S3: $S_{ia} \equiv U_{ia} \equiv$(realm, D_2, T_3)

where T' is the user's side timestamp

According to Assumption7, SeeingS3, and Jurisdictional rules

Seeing S4: $S_{ia} \equiv$(realm, D_2, T_3)

Seeing S5: $U_{ia} \equiv$(D_2^*, T_5)

According to Assumption5, SeeingS4, and sk

Seeing S5: $U_{ia} \equiv S_{ia} \overset{h(sk(T1||T3||(u.mkP)x)}{\longleftrightarrow} U_{ia}$

Realized (Goal1)

According to A_7, S_5, and R_4 rule

Seeing S6: $U_{ia} \equiv S_{ia} \equiv S_{ia} \overset{h(sk(T1||T3||(u.mkP)x)}{\longleftrightarrow} U_{ia}$

Realized (Goal2)

Now, for the second message in the network transmission channel, the following steps will perform for the proposed scheme:

Message 2: $S \rightarrow U_{ia}$: (realm, D_2, T_3): {(realm, D_2, T_3)}$_x$

By applying seeing rules to message2,

Seeing S7: $U_{ia} \triangleleft S_{ia} \rightarrow U_{ia}$: (realm, D_2, T_3): {(realm, D_2, T_3)}$_x$

According to SeeingS7, Assumption4, and D_2

Seeing S8: $U_{ia} \equiv S_{ia}$~h(sk(T_1||T_3||(u.mkP)$_x$)

According to Assumption2, SeeingS8, b, and C_3, the following steps will be obtained:

Seeing S9: $U_{ia} \equiv S_{ia} \equiv$ h(sk(T_1||T_3||(u.mkP)$_x$)

T_2, T_3, and T_4 are the times added to the message in user/server-sides computations, so

According to Assumption6, SeeingS9, and D_2

Message 3: $U_{ia} \rightarrow S_{ia}$:{$D_2^*$, T_5}$_x$

By applying seeing rules

Seeing S10: $U_{ia} \equiv D_2^*$, T_5

According to Assumption4, SeeingS10, and sk (Shared session Key)

SeeingS11: $S_{ia} \equiv S_{ia} \overset{h(sk(T1||T3||(u.mkP)x)}{\longleftrightarrow} U_{ia}$

Realized (Goal3)

According to Assumption8, SeeingS11, and Jurisdictional rules

Seeing S12: $S_{ia} \models U_{ia} \models U_{ia} \xleftrightarrow{h(sk(T1||T3||(u.mkP)x)} S_{ia}$
Realized (Goal4)

From this proof, it has been cleared that both server and end user authenticate mutually and not compromise the shared session key.

4.2 Formal Analysis using ProVerif1.93

By using verification toolkit called ProVerif1.93 [19] for formal verifying and confirming the security and robustness of any authentication scheme is mandatory. So, the code for the authentication scheme using ProVerif1.93 is given below:

```
(*----AS THE SCHEME HAS TWO CHANNELS, PRIVATE AND PUBLIC----*)
free SecCh:   channel [private].
free UnsecCh: channel.

(*--- THE CONSTANT AND VARIABLES USED FOR DESIGNING THE SCHEME ARE---*)
free r: bitstring. (* declaration of prime number r*)
free IDs: bitstring.
free idi: bitstring.
free Bia:bitstring. (* deceleration of user's biometrics*)
free PWia:bitstring [private].

(*.....................CONSTRUCTOR.....................*)
fun h(bitstring):bitstring.                (* one way hash function*)
fun Inverse(bitstring):bitstring. (* as Enc=1/Dec inverse to each other *)
fun CONCAT(bitstring,bitstring):bitstring. (*Concatenate function*)
fun XOR(bitstring,bitstring):bitstring.(*Bit-wise XOR Operation function*)
fun ENC(bitstring,bitstring): bitstring. (*Encryption Function*)
fun DEC(bitstring,bitstring): bitstring. (*Decryption Function*)
fun Mult(bitstring,bitstring): bitstring.

(*.....................DIFFERENT EQUATIONS.....................*)
equation forall a:bitstring; Inverse(Inverse(a))=a.
equation forall x:bitstring, y:bitstring; XOR(XOR(x,y),y)=x.
equation forall x:bitstring, y:bitstring; DEC(ENC(x,y),y)=x.
equation forall x:bitstring, y:bitstring; ENC(DEC(x,y),y)=x.

(*.....................EVENTS.....................*)
event start_Ui(bitstring).
event end_Ui(bitstring).
event start_S(bitstring).
event end_S(bitstring).

(*.....................QUERIES.....................*)
free sk:bitstring [private].
query attacker(sk).
query id:bitstring; inj-event(end_Ui(id)) ==> inj-event(start_Ui(id)).
query id:bitstring; inj-event(end_S(id)) ==> inj-event(start_S(id)).
(*……USER……*)
let pUi=
(*……REGISTRATION……*)
let HB = XOR(Bia,r) in
let O = h(XOR(Bia,r)) in
let PPWia = CONCAT(idi,(PWia,r)) in
let Q = h(CONCAT(idi,(PPWia,r))) in
let V = h(CONCAT(idi,(PPWia,O) ))in
out(SecCh,(Q,idi));
```

```
(*……LOGIN & AUTHENTICATION……*)
event start_Ui(idi);
new Biastr: bitstring;
new u: bitstring;
new T: bitstring;
new P: bitstring;
new mk: bitstring;
let HBstr = h(XOR(Biastr, u)) in
let Ostr = XOR(idi,PWia)  in
let Vstr = h(CONCAT(idi,(PWia,Ostr))) in
let PPWia' = h(CONCAT(r,(idi,PWia))) in
let D1 = ENC(Mult(u,P),(Mult(u,mk),T)) in
let DIDia = XOR(idi, (Mult(u,Mult(mk,P)))) in
out(UnsecCh,(DIDia, D1,T));
new T1:bitstring;
new T2:bitstring;
new T3:bitstring;
new T4:bitstring;
let Sk = h(CONCAT(idi, (Mult(u,P),T2,T3))) in
let D2str = CONCAT(Sk,(T1,T3,(Mult(u, P)))) in
event end_Ui(idi)
else
0.

(*……SERVER……*)
let pS =
(*……REGISTRATION……*)
in(SecCh,(Xia:bitstring,Q:bitstring,P:bitstring,mk:bitstring,u:bitstring));
new N:bitstring;
let J = XOR(mk,(CONCAT(idi,N)) )in
let M = XOR(Xia,Q) in
out(SecCh,(M,mk));
(*……LOGIN & AUTHENTICATION……*)
event start_S(IDs);
new T2:bitstring;
new T3:bitstring;
in(UnsecCh,(DIDia:bitstring, D1:bitstring, uP:bitstring, T1:bitstring,mkP:bitstring));
let id' =CONCAT(DIDia,(h(Mult(mk,P)))) in
let Xia' = h(CONCAT(mk,(idi,N))) in
let D1str = h(CONCAT(idi,(Mult(u,P),(Mult(u,P),T1))) )in
if D1 = D1str then
let Sk' = h(CONCAT(idi,(Xia,(Mult(u,mkP)),T1,T2))) in
let D2 = h(CONCAT(sk,(T1,T3,(Mult(u,mkP))))) in
new realm:bitstring;
out(UnsecCh,(realm,D2,T3));
event end_S(IDs)
else
0.
process ((!pS) | (!pUi) )
```

Running the code using ProVerif1.93, the following result is displayed which shows that no attacker breaks the scheme. Also, verify the authenticity and reachability. The ProVerif1.93 [19] verification results are as shown in Fig. 6**.**

```
Completing equations...
Completing equations...
-- Query not attacker(sk[])
Completing...
Starting query not attacker(sk[])
RESULT not attacker(sk[]) is true.
-- Query inj-event(end_Ui(id)) ==> inj-event(start_Ui(id))
Completing...
Starting query inj-event(end_Ui(id)) ==> inj-event(start_Ui(id))
goal reachable: begin(start_Ui(idi[]), @sid_876 = endsid_3030, @occ27 = @occ_cst) -> end(endsid_3030,end_Ui(idi[]))
RESULT inj-event(end_Ui(id)) ==> inj-event(start_Ui(id)) is true.
-- Query inj-event(end_S(id_57)) ==> inj-event(start_S(id_57))
Completing...
Starting query inj-event(end_S(id_57)) ==> inj-event(start_S(id_57))
RESULT inj-event(end_S(id_57)) ==> inj-event(start_S(id_57)) is true.
```

FIG. 6. PROVERIF RESULT GENERATED

The result indicates that the attacker couldn't enter at any phase during communication and cannot expose the secrets among U_{ia} and S_{ia}. The session key did not compromise at any phase during communication. Similarly, if an adversary struggles for injecting any false information, would be denied due to strong mutual authentication among peers.

4.3 Informal Analysis

Let suppose an attacker intercepts a communication line that actively changes, sees, copy and modify the message and its contents. Therefore, the informal security analysis of the proposed authentication scheme is discussed here in this part by mentioning the following important attacks.

Insider Attack: If an attacker could extract the user's identity, due to timestamp which makes it DID_{ia}, he/she cannot launch an attack. Also, due to lack of physical database in the server, an attacker cannot match user's identity. Therefore, the proposed scheme resists an insider attack.

Mutual Authentication: The proposed authentication scheme, both the server and user share session key sk in all the three round trips which guarantees for mutual authentication.

Password Disclosure Attack: Before starting any session by a legal user, he/she has to send id, Q messages towards the server which consists of high entropy random integer number r, user's password, and biometrics. Here the adversary has no chance to find out user's password, because of missing with r and B_{ia}. Therefore, the proposed scheme resists password disclosure attack due to no opportunity for anyone to extract the password from the line.

Denning-Sacco Attack: The attacker couldn't record session shared key, because it created from high random number P, server master key mk and high entropy random number u. The attacker if extract password from the session key, he/she will be denied by the server due to random key x. Therefore, the proposed scheme resists denning-Sacco attack.

Biometrics Security: Due to BioHashing function, $HB^{*}=h(B_{ia} \oplus u)$, the user's biometrics is secure. Before, entering to the authentication process, the user's put his/her thumb on the sensor, the raw data extracted will pass from an image processing system, from where the important feature will extract and BioHashing function will convert it to a fixed length hash code [20]. The whole scenario is shown in Fig. 8. Therefore, the proposed scheme will provide guarantees for a user's biometrics.

Stolen-Verifier Attack: The S_{ia} has no database for password, if an attacker could guess or extract the user's password, he/she cannot verify it from the physical database. Therefore, the proposed scheme resists stolen-verifier attack.

Resists to De-Synchronization Attack: This attack is applicable only when S_{ia} matches the message of U_{ia} and vice versa. Matching is not possible in the proposed authentication scheme, because each time the server chooses a new large prime number P, and the U_{ia} also start computation by choosing a new random number u in each session. If an attacker copies the message from the line and sent towards either

server or user, which consists of old values, so the message will immediately be discarded by these pairs. Therefore, a desynchronization attack is not possible in the proposed authentication scheme.

Provides Un-traceability: If an attacker desires to trace the location, identity and other useful credential of a legal user then he/she has to capture all the login and response credentials that relays over a public channel to server i.e. $\{DID_{ia}, D_1, uP, T_1\}$, $\{D_2^*, T_5\}$, where $D_1=h(id||X_{ia}||u.mkP)_x||(uP)_x||T_1)$, $D_2^*=h(sk(T_1||T_3||(u.mkP)_x)$ and $DID_{ia}=id\oplus h((u.mkP)_x)$. Each time the value(s) in login and response stages will be different therefore, the attacker cannot extract useful information about a legal user due to random number u and private key x. Moreover, in the response message the D_2^* values contain 100 bits of random number P and server master key mk , Therefore, the attacker fails to break un-traceability property.

Resists Reply Attack: Each time the random numbers (u, P, mk, x) is generated freshly, the parameters in the communication line are different in each session. If an adversary copy $\{DID_{ia}, D_1, uP, T_1\}$ message and launch attack by sending it towards the server, {realm, D_2, T_3} will never authenticate in the user side because U_{ia} compute $D_2^*=h(sk(T_1||T_3||(u.mkP)_x)$ contains timestamp information and master key values u.mkP so, couldn't verify $D_2?=D_2^*$. Therefore, the proposed scheme strongly resists a replay attack.

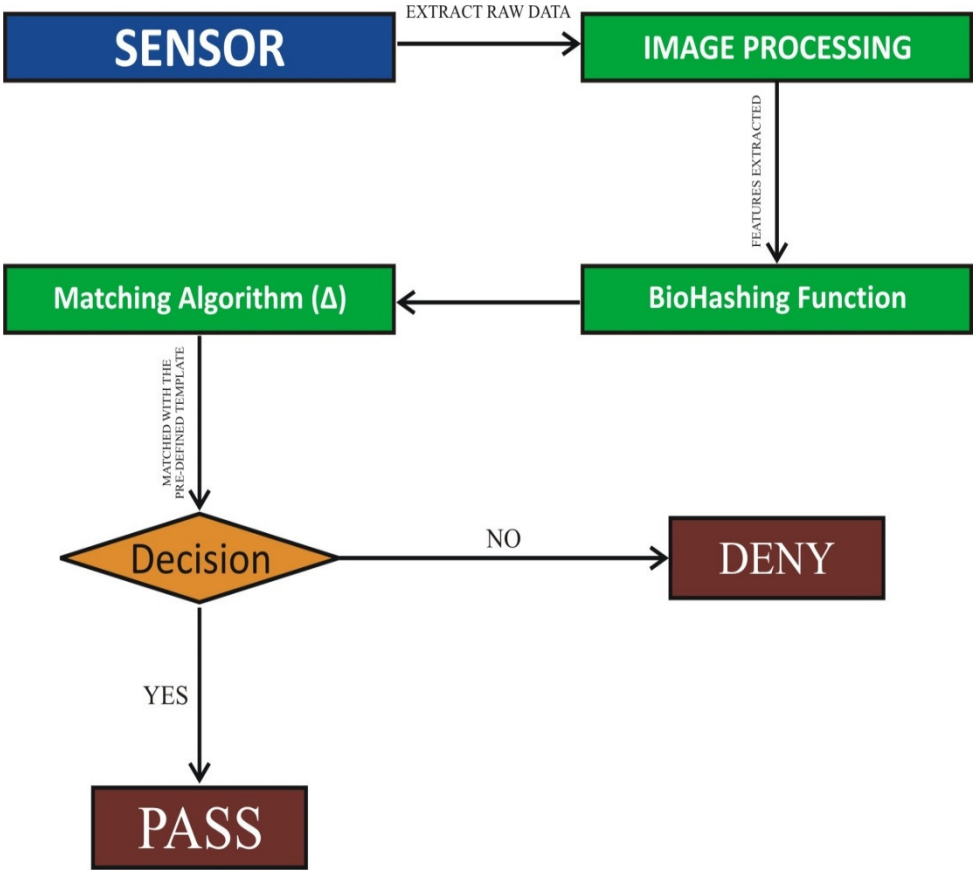


FIG. 7. BIOMETRIC EXTRACTION PROCESS

5. PERFORMANCE ANALYSIS

In this section of the paper, performance analysis of the proposed authentication scheme will be presented in terms of storage, communication and computation costs, because the performance of any cryptographic protocol is a very crucial task [21], so, must be carefully evaluated.

5.1 Storage Overhead Analysis

In order to have a clear understanding of the overhead, all the experiments were performed with RSA keys which are an important feature of networking revealed the surplus or indirect access of memory, bandwidth or associated peripherals needed for performing a specified function (MD5, realm) [22]. In this feature of the authentication scheme, we will check how many arguments have been stored in the memory of the smart card and how much bandwidth occupied by these parameters during initiation of the session among peers. So, in the proposed registration phase of our scheme, the memory occupied by XOR bitwise operation is negligible equal to zero while for one-way hash function, mkP is the combination two big prime numbers mk and P of 512-bit space, identity, nonce and other parameters like u, r, are occupying 64 bits space and biometrics stored in 60 bits. The total storage overhead for the proposed scheme is shown in Table 3.

5.2 Computation Cost Analysis

The computation cost analysis means the time required for the completion of the computations in the process for resource constraint wearable devices [23]. In Table 4, t_h and $t_\oplus$ the time efficiency for one-way hash function and bitwise XOR operation respectively. Therefore, for the proposed scheme the computation cost is shown in Table 4. It is clear from the analysis that our proposed scheme is slightly efficient in terms of computation cost. Here the time efficiency for one-way hash function (t_h) is slightly greater than that of Mishra et al. scheme because our protocol provides more unique features. In addition, the proposed protocol can resist various attacks and provide more attractive security features, so the proposed protocol is a successful authenticated key agreement protocol for SIP from the viewpoint of both performance and security.

TABLE 3. STORAGE OVERHEAD ANALYSIS

Proposed Scheme		Mishra et. al. Scheme [17]	
Different Parameters	Space Occupied in Bits	Different Parameters	Space Occupied in Bits
h(.), mkP	512x3 = 1536	h(.), mkP	512x3 = 1536
Identity(Id)	64x1= 64	username	64x1= 64
Biometrics	60x1=60	Biometrics	60x1=60
Password	64x1 = 64	Password	64x1 = 64
r, R, N	64x3 = 192	r, R, N, u	64x4 = 256
Total Storage	1916 bits	Total Storage	1980 bits

TABLE 4. COMPUTATION COST ANALYSIS

Phases	Participant	Mishra et. al. Scheme [17]	Proposed Scheme
Registration	User	$1t_\oplus+3t_h$	$1t_\oplus+3t_h$
	Server	$1t_\oplus+1t_h$	$1t_\oplus+1t_h$
Login & Authentication	User	$4t_\oplus+7t_h$	$3t_\oplus+7t_h$
	Server	$1t_\oplus+7t_h$	$1t_\oplus+5t_h$
Password Change	User	$4t_\oplus+3t_h$	$4t_\oplus+3t_h$
	Server	0	0
Card Revocation	User	$4t_\oplus+3t_h$	$4t_\oplus+3t_h$
	Server	0	0
Computation Cost(s) taken only for Login and Authentication phase		$5t_\oplus+14t_h$	$4t_\oplus+12t_h$

5.3 Communication Cost Analysis

The communication between peers by taking into consideration hardware resources, services, software, power, and data is termed as communication cost. So, communication cost for the proposed authentication scheme means the exchange of three messages between the server and end user. Let suppose looking into [24-25s], MD5 and realm Message Digest h(.) is 512 bits, identity 64 bits, random numbers 160 bits, realm and timestamp is 60 bits. Therefore, the communication cost for messages (U_{ia} to S_{ia}), (S_{ia} to U_{ia}) and (U_{ia} to S_{ia}) is shown in Table 5**.**

TABLE 5. COMMUNICATION COST COMPARISON ANALYSIS

No.	Message Exchanges	Parameters	Cost(s) in Bits
1.	User → Server	DID_{ia}, D_1, uP, T_1	64+512+512+ 64= 1152 bits
2.	Server → User	realm, D_2, T_3	512+512+64=1 088 bits
3.	User → Server	realm, D_2^*, T_4	512+512+64 =1088 bits

6. CONCLUSION

In this paper, we describe how to design an authentication scheme for SIP signaling protocol, because the IP Telephony based on SIP technology has been gaining attention for its innovative approach in providing VoIP service. At the same time, it has raised many new research topics, particularly around the area of security. We have described three important asymmetric methods namely RSA, DSA and DSS in detail along with the solution of example for each method. The new proposed three-factor authentication scheme in this paper is scalable and generic for providing secure services to its end user. We have demonstrated that the proposed scheme can guarantees against many potential known attacks along with the attacks identified in Mishra's scheme. We also have developed a formal security analysis using logic proposed by Burrows-Abadi-Needham to resilient the extensiveness of our scheme. The scheme formally verified using automated verification software toolkit ProVerif1.93 which shows that it can easily be implemented for a real-world environment. We have compared the performance with other related scheme and showed that the proposed scheme possesses more security features and fast for communication.

ACKNOWLEDGMENT:

Special thanks to the administration of Higher Education, Achieves & Libraries Department Government of Khyber Pakhtunkhwa, Pakistan for issuing NOC to pursue PhD in Computer Science from University of Malakand, and awarded "**Best Teacher Award**" Khyber Pakhtunkhwa, for the year 2018-2019.

REFERENCES

[1] Peterson, J., C. Jennings, E. Rescorla, and C. Wendt., "Authenticated Identity Management in the Session Initiation Protocol (SIP)", Internet Engineering Task Force, No. RFC 8224, pp. 1-46, 2018.

[2] Wen-Bin, H., and Jenq-Shiou, L., "Implementing a Secure VoIP Communication Over SIP-Based Networks", Wireless Networks, Volume 24, No. 8, pp. 2915-2926, 2018.

[3] Suresh kumar, Venkatasamy, Amin R., and Anitha R., "A robust mutual authentication scheme for session initiation protocol with key establishment", Peer-to-Peer Networking and Applications, Volume 11, No. 1, pp. 900–916, 2017.

[4] Kumari S., Karuppiah M., Das A. K,, Xiong Li, Fan Wu, and Gupta V., "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography", Journal of Ambient Intelligence and Humanized Computing, Volume 9, No. 3, pp. 643-653, 2018.

[5] Qiu S., Xu G., Ahmad H., and Guo Y., "An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy", PloS one, Volume 13, No. 3, pp. 172-194, 2018.

[6] Chaudhry S. A., Naqvi H., Sher M., Farash M. S., and Hassan M., "An improved and provably secure privacy preserving

authentication protocol for SIP", Peer-to-Peer Networking and Applications, Volume 10, No. 1, pp. 1-15, 2017.

[7] Tu H., Kumar N., Chilamkurti N., and Rho S., "An improved authentication protocol for session initiation protocol using smart card", Peer-to-Peer Networking and Applications, Volume 8, No. 5, pp. 903-910, 2015.

[8] Farash M. S., "Security analysis and enhancements of an improved authentication for session initiation protocol with provable security", Peer-to-Peer Networking and Applications, Volume 9, No. 1, pp. 82-91, 2016.

[9] Kumari S., Chaudhry S. A., Wu F., Xiong Li, Farash M.S., and Khurram M. K., "An improved smart card based authentication scheme for session initiation protocol", Peer-to-Peer Networking and Applications Volume 10, No. 1, pp. 92-105, 2017.

[10] Tsaur, and Woei-Jiunn, "Several security schemes constructed using ECC-based self-certified public key cryptosystems", Applied Mathematics and Computation, Volume 168, No. 1, pp. 447-464, 2015.

[11] Varma C., "A Study of the ECC, RSA and the Diffie-Hellman Algorithms in Network Security", International Conference on Current Trends towards Converging Technologies (ICCTCT), pp. 1-4, IEEE, 2018.

[12] Farash M. S., "An improved password-based authentication scheme for session initiation protocol using smart cards without verification table", International Journal of Communication Systems, Voume. 30, No. 1, pp. 2879, 2017.

[13] Zhang L., Tang S., and Cai Z., "Cryptanalysis and improvement of password authenticated key agreement for session initiation protocol using smart cards", Security and Communication Networks, Volume 7, No. 12, pp.2405-2411, 2014.

[14] Azrour, Mourade, Yousef F., and Ouanan M., "Cryptanalysis of Farash et al.'s SIP authentication protocol", International Journal of Dynamical Systems and Differential Equations, Volume 8, No. 1, pp. 77-94, 2018.

[15] Cao, Feng, David A., Bryan, Bruce B., and Lowekamp, "Providing secure services in peer-to-peer communications networks with central security servers", In Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06), pp. 105-105, IEEE, 2006.

[16] Lu, Yanrong, Lixiang Li, Haipeng Peng, and Yixian Yang, "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography", Multimedia Tools and Applications, Voume 76, No. 2, pp. 1801-1815, 2017.

[17] Mishra, Dheerendra, Das A. K., and Mukhopadhyay S., "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using a smart card", Peer-to-Peer Networking and Applications, Volume 9, No. 1, pp.171-192, 2016.

[18] Burrows M., Abadi M., and Needham R., "A logic of authentication", ACM Transactions on Computer Systems, Volume 8, No. 1, pp. 18–36, 1990.

[19] Bruno B., Smyth B., and Cheval V., "ProVerif 1.93: Automatic cryptographic protocol verifier, user manual and tutorial", Available from: https://www. bensmyth. com/publications/2010-ProVerif-manualversion-1.93 (2016). url: https://bensmyth.com/files/ProVerif-manual-version-1.93.pdf

[20] Najam, S., Shaikh, A., and Naqvi, S., "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition", Mehran University Research Journal of Engineering and Technology, Volume 37, No. 1, pp. 10, 2018.

[21] Khan, H., and Chowdhry, M., "Performance Enhancement of Low Voltage Distribution Network in Developing Countries using Hybrid Rehabilitation Technique", Mehran University Research Journal of Engineering

and Technology, Volume 37, No. 3, pp. 493-512, 2018.

[22] Maliberan, E. V., Sison, A. M., and Medina, R. P., "A New Approach in Expanding the Hash Size of MD5", International Journal of Communication Networks and Information Security, Volume 10, No. 2, pp. 374-379, 2018.

[23] Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., and Gupta, V., "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography", Journal of Ambient Intelligence and Humanized Computing, Volume 9, No. 3, pp. 643-653, 2018.

[24] Akhter F., Memon A., and Shaikh N., "A Proposed Supergrid Model for National Transmission Network of Pakistan", Mehran University Research Journal of Engineering and Technology, Volume 36, No. 1, pp.149-158, 2017.

[25] PUB F., "Secure hash standard", Public Law, pp.100-235, 1995.

[26] William Stalling., "Data and computer communications", 10th edition, Prentice Hall Press, Upper Saddle River, NJ, USA, 2013.

[27] Rivest R. L., Shamir, A. and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Volume 21. No. 2, pp.120-126, 1978.