JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
31st December 2017, Volume 2, Issue 3, JSEIS, CAOMEI Copyright © 2016-2017
www.jseis.org

An improved lightweight privacy preserving authentication scheme for SIP-based-VOIP using smart card

[1]Saeed Ullah Jan, [2]Fawad Qayum, [3]Sohail Abbas, [4]Ghulam Murtaza Khan, [5]Ajab Khan, [6]Siffat Ullah Khan
[1,2,3,5,6] Department of Computer Science & IT, University of Malakand, Khyber Pakhtunkhwa, Pakistan
[4]Department of Computer Science Shaheed Benazir Bhutto University Sheringal, Khyber Pakhtunkhwa, Pakistan
Email: [1]saeedullah@uom.edu.pk, [2]fawadqayum@uom.edu.pk, [3]sabbas@uom.edu.pk, [4]ghulam.murtaza@iiu.edu.pk, [5]ajabkhan@uom.edu.pk, [6]siffatullah@uom.edu.pk

ABSTRACT

Secure information sharing has become very popular in immigration, military applications, healthcare, education and foreign affairs for the past few years. The security and privacy of such type of information cannot easily be compromised because the secure communication utilizes both wireless and wired communication media for exchanging sensitive information. Voice over IP (VoIP) offers many unique capabilities to its users. An important robust dynamism behind the use of IP telephony is cost savings, especially for businesses with large data networks. By transporting voice traffic over IP-based networks, businesses can decrease or abolish the toll charges related to carrying calls over the Public Switched Telephone Network (PSTN). Session Initiation Protocol (SIP) promises simple and efficient management of multimedia sessions amongst several users. To improve the security, integrity, authenticity and privacy issues while sharing sensitive information, numerous authentication schemes or set-of-rules have been recommended by different researchers in recent times. These authentication schemes are vulnerable to prospective security flaws e.g. replay attack, masquerading, insider attack, impersonation, password guessing, server spoofing, Denning Sacco and denial-of-service (DoS). Further, these schemes also fail to deliver mutual authentication. Almost, no researcher claims with conviction about a foolproof secure authentication scheme. This research mainly focuses on designing VoIP system based on SIP scheme that caters all the weaknesses in these schemes having low computation costs and low communication complexity and low storage overhead and shows a significant balance between performance and security. The proposed protocol also offers mutual authentication and reliable information delivery between user and server. A provable formal security analysis for the scheme will also be established mathematically, using BAN logic of authentication.

Keywords: biohashing; transmission latency; π-calculus; public-key-infrastructure; discrete-logarithmic-function; big numeral-factorization-complication;

1. INTRODUCTION

In network communication (Internet), a major issue is the exchange of information confirmation of indigenous and foreigner consumer in the insecure distributed environment. Categorically, authentic users have extra control over the attackers. An authentic user retains information in the internal system that is not accessible to the attacker. Therefore, several remote user authentication schemes are proposed for the exchange information. These protocols claimed that they are more powerful against different attacks, but these schemes still pose weakness [1-3].

Furthermore, application programs are also developed in this regard to monitors task scheduling fragment of each part, authenticate the user recorded data and post a message to the remote server platforms for communication. The user interfaces part of that application program specially designed for end users to operate, understand and mainly communicate with a remote server for different activities like posting text, audio, video, graphics and animated data. Afterward, the server gets demands from clients, accomplishes record repossession, renews and regulates data integrity and finally posts replies to the clients. The server works like a software powerhouse that controls software, provides database facilities, controls printing devices, monitor communication line and enhance the performance of the high powered processor (CPU). The key aim of the server is to complete the back-end responsibilities that are mutual to related applications and users. Network Operating System installed in the server facilitates service areas, such as direction-finding, delivery, messaging, communication supervision services, and guidelines for different tasks [4]. Subsequently, the somatic link is identified and transfer control protocol (TCP) is carefully chosen for mutual authentication between the server and the client. Therefore, a strong authentication protocol becomes mandatory for distributed computation prior to the client gets the benefit of the network facilities. So that to provide a straightforward application for usage, neither in isolation nor a monolithic system and must not be a complicated and must support the latest technology – a centralized control model [4].

The authentication protocols presented so for, to preserve the security of the exchanged information, are classified as: 1) user has a secure PIN code for authenticity called one factor authentication protocol [5] in which the encryption and decryption of PIN code are done by some complex cryptographic algorithms; 2) smart card is used as a second factor together with the PIN code for the authentication of exchanging information called two factor authentication protocol [6]; 3) biometrics in addition to PIN code and smart card used to ensure the communication among the users called three factors authentication protocol [7] that is more secure as of 1) and 2) above.

1.1 Voice-over internet protocol

In past few years, the popularity of voice-over internet protocol (VoIP) facilities has increased because numerous Web and VoIP applications depend on huge and extremely distributed infrastructures to process requests from millions of users in an appropriate manner. Due to their excessive requests, these large-scale internet applications frequently compromise security for other purposes such as performance, scalability, and availability [9]. As a result of these applications characteristically prefer weaker but well-organized security mechanisms in their foundations. Voice-over-IP (VoIP) method has spread in the markets due to low cost and more flexible implementation as compared to Public Switched Telephone Network (PSTN) [10].

1.2 Session initiation protocol

In last few years, many well-organized, extensible and riskless signalized schemes have been suggested to improve the applications usefulness and fast progression of Voice-over-IP. Among these signalized protocols, the Session Initiation Protocol (SIP) is commonly used because of its flexibility and significantly accessible designs and lightweight features. Session Initiation Protocol (SIP) is a presentation and application layers protocol which initiates, modifies and terminates IP-based multimedia intervals. Implementing SIP for secure communications has been a subject of study for the past few years and several proposals are available in the research domain [8]. However, security aspects are not addressed in most of these proposals because SIP is exposed to several threats and faces security issues at these layers like registration hijacking, impersonating a server, message tampering, session tear down, Denial of Service (DoS) and session-key agreement protocol.

However, designing a good authentic key-agreement scheme for Session Initiation Protocol (SIP) is still a challenging task from the performance and security perspectives. Both the performance and security features are the critical factors stimulating SIP applications and these also always appear contradictory. The authentication scheme can secure against different attacks and transport many characteristics to achieve the security needs of IP "Internet Protocol" based communications. Alternatively, the algorithm inserted in authentication portion of IP must not contain complex or heavy computations in clients and SIP servers because VoIP network communications are more delicate to transmission latency [9].

1.3 Smart card

In recent years, the smart-cards have acquired an increasing acceptance as an authoritative contrivance for security, authenticity, authorization, identification, and validation. The term smart-card generally alludes to a flexible card having memory-chip, a microchip, and a complex instruction cycle processing mechanism which is not only capable of storing data but also does the process, computer, manage and perform high cryptographic algorithmic operations. Moreover, smart cards associated communications typically engage five entities namely company, software installer, card issuer, card-holder/data-owner and terminal. Typically, the uses of smart-card are health-care, employee ID, calling cards, ATM cards, government Identification (ID) Cards, SIM cards for telecommunication, transportation services control cards, electronic passports for immigration and foreign travel, voting system in advanced countries, campus cards, satellite TV cards and information security [11].

1.4 Biometrics

Biometrics is a term used for body measurements and a calculation which also refers to metrics those are relevant to human characteristics. In computer science, biometrics is used as a form of identification, authorization, and observations. The benefits of biometric verification are presented to basic cryptographic key supervisory systems for the purpose to enhance security and performance [12-13].

The paper is organized such as the part-2 gives some popular existing authentication schemes, part-3 gives detail about the proposed solution and part-4 gives the detail about the research methodology such as the robustness and security analysis of the authentication protocol by using BAN logic and an automated software toolkit ProVerif0.92. Finally, the performance of the scheme is compared with some recent popular authentication schemes, their computation cost, their communication cost and storage overhead.

2. LITERATURE REVIEW

Since the first authentication scheme was presented by Lamport in 1981 [1] using a simple PIN code or a simple password for remote user authentication, later on, considerable attention has been focused on this important research area.

So far Liao et al.'s [2] presented dynamic ID-based remote user authentication scheme using lightweight cryptography functions such as bit-wise X-OR operation and a single-way digital hash function to deliver mutual authentication and session key arrangement. In addition, Liao et al.'s [2] protocol are based on 2-factor and the idea of 'nonce' which guaranteed computation effectiveness and individual anonymity. Hsiang et al.'s [3] proved that Liao et al.'s protocol is defenseless and shows inconsistency of impersonation, insider and server spoofing attacks and might not deliver mutual authentication. Then they presented a medication which is designed to restore the security weaknesses and succeeded a similar level of computation effectiveness by applying a single-way digital hash function and XOR-operation in it. Next, Sood et al.'s [4] used a two-server model design in which different points of confidence are allocated to the main services provider computer and the client's authentic information is spread among a couple of servers called the services supplier and controller server. However, the flaws of the researchers [5-10] were demonstrated by researchers [11-13] correspondingly exposed to impersonation, replay, stolen smart card and leak of verifier attacks could not be delivered.

Later, Lee et al.'s [5] demonstrated a single-sign-in-based authentication scheme for shared networks. The idea of single-sign-in can permit legitimate users to use a unary symbol to access distributed service providers. The client-server architecture is assumed in the Lee scheme and heavyweight exponential computation is implemented to convey the tough security density of their protocol. Based on Lee et al.'s scheme, the security parameters and their protocol appeared prima facie to be properly robust. However, the researchers in [6-8] found two flaws in Lee scheme such as user impersonation and credential recovery attacks. Another scheme was presented by Juang et al.'s [14] based on Elliptic Curve Cryptography (ECC) and symmetric cryptographic functions using a smart card for remote user authentication. They claimed that their protocol might gain identity protection, session key agreement, conflict to low communication, computation cost and insider attack. But, all these announcements couldn't be completed by the researcher [8, 11].

Tsai et al.'s [8] suggest that Li et al.'s [11] protocol is weaker to de-synchronization attack. The personal sensitive data about a user "update mechanism" in Li protocol is not properly addressed and has also no effective registration database. So, Tsai et al.'s [8] validated an anonymous authentication protocol that doesn't need a registration record to preserve privacy for its clients and also creates the protocol for an appropriate distributed system. Wang et al.'s [14] offered a remarkable learning to examine the confidence among smart cards and terminal; that is, whenever an attacker gets a lost smart card, the chance of user's information being compromised. Based on Common Adversary Model (CAM) containing three types of attackers and four important points are presented as: (a) a private key based schemes are secure against the type I and II (updating useful information and masquerading) attackers but not against a type III (Spoofing and password guessing) attacker, (b) a public key schemes are secure against type I, II and III attackers, (c) a public key Rivest–Shamir–Adleman (RSA) schemes are secure against type I and II attackers, but not against the type III attacker and (d) a public key based RSA-based (Rivest–Shamir–Adleman) schemes are secure against type I, II and III attackers. Then, Wang found that the scheme has many practical drawbacks and the protocol is defenseless in the type III attacker. Moreover, Wang et al.'s [15-16] also examined many password-based authentication schemes and offered 12 estimation principles for it.

Wang et al.'s [17-18] also presented the security of two authentication protocols of Leu et al.'s [19] and found that their scheme is defenseless to offline and online dictionary attacks. Further, he proposed a comparative study of "two-factor authentication schemes using smart cards" and "common-memory device-based two-factor schemes" under two self-defined adversary models. Huan et al.'s [20] acknowledged two detailed security setups for password-based authentication using a smart card in the distributed environment: (1) attackers having similar data recorded in smart card and (2) attackers having different data recorded in the smart card. Then two medications were presented for the employment of two authentication schemes which are difficult and consistent counter-measures problem. In another scheme, Wang et al.'s [18] examined the probability of designing an anonymous two-factor authentication scheme with the concept of "Madhusudhan Mittal' Evaluation Set. They presented the characteristics of local user password change and resistance to smart card loss attack which are tough to realize simultaneously. Later, Wang et al.'s [17] investigated the weaknesses between system efficiency and user anonymity and examined significant results of Public Key Infrastructure (PKI) technique and strong user anonymity. Moreover, Wang et al.'s confirmed that a password-based user authentication scheme of Li et al.'s

[11] doesn't resist Denial-of-Service (DoS) and offline password guessing attacks and therefore failed to provide strong user anonymity as well as forward secrecy.

3. PROPOSED SOLUTION

The existing authentication schemes based on symmetric key primitives have many weaknesses. In this paper, all the existing weaknesses have been catered. The enhanced scheme consists of biometric characteristics and smart card – that has the capability to check the uniqueness of the biometric data because a pre-defined template will be stored before purchasing a smart card. Due to using the BioHashing technique if the smart card is stolen or misplaced, no one can extract the Biometrics from it [38].

When the user desires to get a smart card, the buyer asks for iris scan to generate seller Biometric characteristics; the computations between user Biometrics and other necessary parameters will be as: HB=H(BTia) and HB/=H(BTia*) Where BTia represents Biometric Template and BTia* represents newly extracted biometrics. Mainly three entities are used such as password, biometrics, and smart card and are divided into three phases: registration, login and authentication and password change phase. Each of which is briefly described under the following headings.

Symbols and their description

U_{ia}	User's A	S_{ia}	Server's A
ID_{ia}	User's A Identity	PW_{ia}	User's A Password
BT_{ia}	User's A Biometrics	BT_{ia}^{*}	User's A input Biometric
Δ	Matching Algorithm	h(.)	Secure Hash Algorithm
S	Private key of S_{ia}	HB	BioHashing
sk	Shared Session Key	$\|\|$	Concatenation function
$\oplus$	X-OR symbol	t	Timestamp

Notations Used

3.1 Registration phase of the proposed scheme

When an authentic user U_{ia} desires to register into a remote server S_{ia}, the following computation with the server will be performed in this phase.

R1: $U_{ia} \Rightarrow S_{ia}$:(HB, ID_{ia}, N)

The user U_{ia} selects his/her identity (ID_{ia}), password (PW_{ia}) and confirms an iris scan as biometrics to generate biometric template BT_{ia}. The BioHashing technique HB is applied to keep it secret $HB=H(BT_{ia})$, At the same time chooses an integer number of high entropy 'q' and one-way hash function 'h (.)' that is $\{0, 1\}^{*} \rightarrow \{0, 1\}^{k}$, $M=HB \oplus q$, $N=PW_{ia} \oplus ID_{ia} \oplus M$ and $O=h(M \oplus PW_{ia} \oplus ID_{ia}) \oplus q$ and conveys {HB, N, ID_{ia}} parameters to the remote server over a secure channel ($\Rightarrow$).

R2: $S_{ia} \rightarrow U_{ia}$:(A, F)

The remote server chooses a secret key 'S' and encrypts the ID_{ia} that is $A=E_S(ID_{ia}||t_0)$. Also encrypt ID_{ia} along with the bitwise XOR of the server secret key 'S' such as $B=E_S(ID_i \oplus S)$, here using N to encrypt B which is $F=E_N(B)$ and submit {A, F} to the memory of a smart card for future usage.

R3:

After applying a one-way hash function to the parameter N such as P=h(N), the pre-stored values {O, N} and received parameters from the server {A, F}: the memory of smart card finally consists of {O, P, A, F} parameters.

Legal User		SIP Server
Choose ID_{ia}, PW_{ia}, q, h(.) Produce Iris Scan for Biometrics that is BT_{ia} $HB=H(BT_{ia})$ And calculates $M=HB \oplus q$ $N=PW_{ia} \oplus ID_{ia} \oplus M$ $O=h(PW_{ia} \oplus ID_{ia} \oplus M) \oplus q$	$\{HB, N, ID_{ia}\}$ ⟶	Selects key S And calculates $A=E_S(ID_{ia}\|\|t_0)$ $B=E_S(ID_{ia} \oplus S)$ $F=E_N(B)$

		{A, F}
P=h(N)	←	
Finally store {A, F, O and P} into Smart Card		

Phase – 1: Registration Phase

3.2 Login and authentication phase

In this phase, the following computations are performed that as:

LA1: The legal user (U_{ia}) inserts his/her smart card into the machine, input ID_{ia}, PW_{ia}, and Iris scan to produce Biometrics BT_{ia}^{*}. BioHashing technique is applied to secure the biometrics $HB^{/}=H(BT_{ia}^{*})$. The smart card generates a random number of high entropy 'q' from the stored values in 'O'. The U_{ia} then computes $N^{/}=PW_{ia}\oplus ID_{ia}\oplus HB^{/}\oplus q$ to confirm the calculation $P?=h(N^{/})$, if becomes matched on both entities (smart card and biometric) decrypts F using $N^{/}$ i.e. $B=D_{N/}(F)$ and if doesn't matche computation ended and the processes terminated. Meanwhile, timestamp t_1 is extracted from the machine and concatenated with the other parameters like $R_1=h(B||ID_{ia}||t_1)$ and $R_2=E_B(P||ID_{ia}||R1||t_1)$. Finally, the terminal submits (A, R_1, R_2, t_1) called "*MESSAGE1*" towards the server through a public channel (→).

User		Server
Introduce smart card and enter ID_{ia} and PW_{ia}, and choose p		
Iris scan to obtain BT_{ia}^{*}		
Extract q from O		
Calculate $HB^{/} = H(BT_{ia}^{*})$		
Compute $N^{/} = PW_{ia}\oplus ID_{ia}\oplus HB^{/}\oplus q$		
Check P ?=$h(N^{/})$		
$B = D_{N'}(F)$		
Calculate $R_1 = h(B\|\|ID_{ia}\|\|t_0)$ and		
$R_2 = E_B(P\|\|ID_{ia}\|\|R_1\|\| t_1)$		
	MESSAGE1 {A, R_1, R_2, t_1} →	
		Comparing ($t_1^{/}$ - t_1) against Δt
		Decrypt *A* for ID_{ia} and check in the Identity table
		$ID_{ia}\|\|t_{s0} = D_S(A)$
		Calculate $B= E_s(ID_{ia}\oplus S)$
		Check R_1 ?= $h(B\|\|ID_{ia}\|\|t_1)$
		Decrypt R_2 by using B and select n
		$(P\|\|ID_{ia}\|\|R_1\|\|t_1)=D_B(R_2)$
		Calculate sk = $h(p\oplus n)$
		$R_3 = E_B(n\|\|sk\|\|t_{s1})$
		$A_n = E_s(ID_{ia}\|\|t_{s1})$
	← MESSAGE2 {R_3, A_n, t_{s1}}	
Comparing ($t_2^{/}$ - t_{s1}) against Δt		
Decrypt R_3 by using B i.e. $n\|\|sk^{/} = D_B(R_3)$ and compute		
$sk^{/} = h(p\oplus n)$		
Check $sk^{/}$?= sk if true keep sk as shared secrete key		

Phase – 2: Login and Authentication Phases

LA2: The server deducts the received time from the current and compares it with the predefined threshold time of the server, also decrypts the user identity using secret key 'S' and verifying ID_{ia} in its database table, if doesn't exist the processing terminated otherwise calculates $B=E_S(ID_{ia}\oplus S)$ and checks $R_1?=h(B||ID_{ia}||t_1)$, if found equal, the processes of decryption is proceeded in R_2 using 'B' and selects a shared session key $sk=h(p\oplus n)$ and compute $R_3=E_B(n||sk||t_{s1})$ and $A_n=E_S(ID_{ia}||t_{s1})$. At the end the SIP server transmit parameters (R_3, A_n, t_{s1}) called "*MESSAGE2*" towards the user U_{ia} over a public channel.

LA3: After receiving the MESSAGE2 message, U_{ia} checks the received time from the server time with the terminal time t_2 and matches with the pre-defined threshold time in the user smart card, for the purpose of knowing that whether the value is received from the server is within the limit of threshold timing or not. If it is not, shall be considered as wrong and the computation session be terminated suddenly and "*Access is Denied*" message be shown on the screen of the terminal. Otherwise, the user U_{ia} decrypts R_3 using B and put a session key $sk^{/}=h(p\oplus n)$ and checks that $sk^{/}$?=sk if found true, the user keeps sk is a shared session key and starts communication with the server securely and anonymously.

3.3 Password change phase

In this phase of the proposed scheme, the legitimate user (U_{ia}) can change his/her password easily and securely. Also, the user (U_{ia}) doesn't need to interact with the server, all the processes are completed between the terminal and smart card. The following steps are performed in this phase:

User	Smart Card
Provide ID_{ia}, PW_{ia} and biometric BT_{ia}^*	
$HB=H(BT_{ia}^*)$	
$\{ID_{ia}, PW_{ia}, HB\}$ →	
	Abstract q from O and
	$q=O \oplus h(PW_{ia} \oplus ID_{ia} \oplus HB^/)$
	Calculate $HB^/ = BT_{ia}^* \oplus q$ and compare Δ (HB, $HB^/$)
	If similarity were found between the values
← {*Request for a new Password*}	
Input another password PW_{ia}^*	
$\{PW_{ia}^*\}$ →	
	Calculate $O^*=h(PW_{ia}^* \oplus ID_{ia}) \oplus q$
	$F^*=E_{S \oplus PWia \oplus HB \oplus IDia}(PW_{ia}^* \oplus HB \oplus ID_{ia})$
	Update (O, F) with (O^*, F^*)

Phase – 3: Password Change Phase

PC1: If the owner of a smart card desires to change his/her password at any time and at any stage, he/she first inserts his/her smart card into the terminal and makes an iris scan to generate a biometric template BT_{ia*}, provides ID_{ia} and password PW_{ia}. The smart card memory has these parameters $\{ID_{ia}, PW_{ia}, BT_{ia*}\}$ in its memory are transmitted to the terminal. It has the following computations:

PC2: The smart card CPU and EEPROM generates a random number of high entropy say 'q' from its stored values $O \oplus h(PW_{ia} \oplus ID_{ia} \oplus HB^/)$, calculates $HB^/=BT_{ia*} \oplus q$ and associates with the stored template BT_{ia}, that is $HB=BT_{ia} \oplus q$. If equal by using matching algorithm $\Delta(HB, HB^/)$ the smart card conveys a message {*demand for new password*} to the user, and if the value doesn't match in the matching algorithm the process is definitely terminated.

PC3: After getting {*request a new password*} message from the smart card, user inputs the new values PW_{ia*} and directs to the smart card.

PC4: The smart card calculates $O^*=h(ID_{ia} \oplus PW_{ia}^*) \oplus q$ and $F^*=E_{S \oplus HB \oplus IDia \oplus PWia}(HB \oplus ID_{ia} \oplus PW_{ia}^*)$ separately, the value at the smart card {O, F} change with {O^*, F^*}, and new password overlap over the old.

4. SECURITY ANALYSIS

To scrutinize the information of protocol's participants and adversaries thoughtful ideas of cryptographic functions have to be needed. For this purpose, upon receiving a message by the participants, these questions must be given values:

i. Does he/she know who sent it?
ii. Does he/she know that the message is fresh?
iii. Does he/she know that it is never just a repetition from the past message?
iv. Does network investigator know who is talking to whom?

These questions can be covered here both formally and informally in the security analysis part of the paper that is described under the following headings:

4.1 BAN – Logic

A formal-method for expressing and investigating an authentication protocol was first recommended in the late 1980's by three popular mathematician names Burrows Abadi and Needham and is called BAN Logic [31-32]. It is the first in a family of ep-onymous authentication logics – a logic of belief. The intended use of BAN is to analyze a protocol by deriving the security and authenticity of its authentic principles. When the protocol become executed as the BAN principles correctly executing a protocol or not and can come to produce a verifiable result. BAN has been highly successful in divulge protocol flaws. BAN needed ASSUMPTIONS and it is comparatively easy to use. BAN method used to prove that the above scheme accomplishes mutual authentication, resists all known attacks and realize preferred characteristics.

Table. 1 BAN definitions and their descriptions

Protocol Steps	Description
$P \longrightarrow Q: message$	P sends message to Q
A⟶B: {A, Kab} Kbs	B know K_{bs} and K_{ab} another key to transfer with A.
$A \longrightarrow B: \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$	Tells B, recognizes key K_{bs} and K_{ab} is another key to transfer with A.
$B \lhd \{A \overset{K_{ab}}{\longleftrightarrow} B\}_{K_{bs}}$	B sees the communication of A and b via K_{ab} and K_{bs} is another key to transfer with A
$A \mid \equiv A \overset{K}{\leftrightarrow} B$, $B \mid \equiv A \overset{K}{\leftrightarrow} B$	Confirmation is ok among A and B using K
$A \mid \equiv B \mid \equiv A \overset{K}{\leftrightarrow} B, B \mid \equiv A \mid \equiv A \overset{K}{\leftrightarrow} B$	A believes B believes that A transfer data to B using K and vice versa.
$A \mid \equiv \overset{K}{\rightarrow} B$	A believes communication to B over a public key K
$A \mid \equiv A \underset{\rightleftharpoons}{N_a} B$	A and B might share some private secrets

The proposed scheme can be shown using BAN logic is summarized as follows:

a. BAN goals for the proposed scheme

Goal1: user |≡ Server$\overset{sk}{\longleftrightarrow}$ user
Goal2: Server |≡ user |≡ Server$\overset{sk}{\longleftrightarrow}$ user
Goal3: user |≡ Server $\overset{sk}{\longleftrightarrow}$ user
Goal4: user |≡ Server |≡ Server $\overset{sk}{\longleftrightarrow}$ user

b. BAN idealized form for the proposed scheme

Idealization is used in BAN logic to show the central information regarding the beliefs of the receiving party in each step of the protocol. In the proposed procedure idealized form is as follows:

Msg_1: user⟶ Server: A, R_1, R_2, t_1: $\{A, ID_{ia}, R_1, R_2, t_1\}_B$
Msg_2: Server⟶ user: R_3, A_n, t_{s1}: $\{R_3, A_n \| t_{s1}\}_B$

c. BAN assumptions for the proposed scheme

i. A1: User |≡ # (t_1)
ii. A2: Server |≡ # (p, n, t_{s1})
iii. A3: User |≡ Server $\overset{B}{\longleftrightarrow}$User
iv. A4: Server |≡ Server $\overset{B}{\longleftrightarrow}$User
v. A5: User |≡ Server $\overset{sk = h(p \oplus n)}{\longleftrightarrow}$User
vi. A6: Server |≡ Server $\overset{sk = h(p \oplus n)}{\longleftrightarrow}$User
vii. A7: User |≡ Server ⇒ (R_4, p)
viii. A8: Server |≡ User ⇒ (t_1)

Next, take Msg_1 and Msg_3 as,

A) Msg_1: user⟶ Server: A, R_1, R_2, t_1: $\{A, ID_{ia}, R_1, R_2, t_1\}_B$

By applying seeing rule,

B) S1: Server ⊲ A, R_1, R_2, t_1: $\{A, ID_{ia}, R_1, R_2, t_1\}_B$

According to S1, A3 and R1,

C) S2: Server |≡ user~ (A, ID_{ia}, R_1, R_2, t_1)

According to A1, S2, R_4, and R_2

D) S3: Server |≡ user |≡ (A, ID_{ia}, R_1, R_2, t_1); where t_1 is the timestamp used by the user.

According to A7, S3, and Jurisdiction rule

E) S4: Server $|\equiv$ (A, ID_{ia}, R_1, R_2, t_1)
According to A5, S4, and session key rule

F) S5: Server $|\equiv$ user $|\equiv$ Server $\xleftrightarrow{sk = h(p \oplus n)}$ User Achieved (Goal 2)
According to A7, S5, and R4 rule

G) S6: Server $|\equiv$ Server $\xleftrightarrow{sk = h(p \oplus n)}$ User Achieved (Goal 1)
Taking the second idealized message as:

H) Msg_2: Server→ user: R_3, A_n, T_{s1}: { R_3, $A_n \| t_{s1}$}$_B$

By applying seeing rule,

I) S7: User ◅ Server → user: R_3, A_n, T_{s1}: { R_3, $A_n \| t_{s1}$}$_B$
According to S7, A4 and R1,

J) S8: user $|\equiv$ Server ~ (R_3, $A_n \| t_{s1}$)
According to A2, S8, R4, and R3 rules,

K) S9: user $|\equiv$ Server$|\equiv$ (R_3, $A_n \| t_{s1}$); Where, t_2 is the timestamp produced by the server. so
According to A6, S9, and R4 rule

L) S10: user $|\equiv$ (R_3, $A_n \| t_{s1}$)
According to A4, S10, and session key rule

M) S11: user $|\equiv$ Server $|\equiv$ Server $\xleftrightarrow{sk = h(p \oplus n)}$ User Achieved (Goal 4)
According to A8, S11, and Jurisdiction rule

N) S12: User $|\equiv$ Server $\xleftrightarrow{sk = h(p \oplus n)}$ U_{ia} Achieved (Goal 3)

4.2 ProVerif implementation

It is a software package for automatically investigating the assurance of cryptographic protocols, capable of giving reach-ability materials and is very interactive for zero-knowledge verifications. It also shows us the messages acknowledgment, remarkable similarities, confidentiality, traceability and, verifiability. The verification of a protocol using ProVerif [25-26] is useful for computer security point of view. Whenever a property cannot be verified, this tool restructures and processes the weaknesses and robustness of the protocol. It is a language-based toolkit derived from PROLOG which uses π-calculus. The proposed scheme is formally proved using this toolkit; so that the work will best satisfy the mutual authentication and session key secrecy. This tool supports many cryptographic techniques like private key/public key encryption/decryption, hashing algorithm, Rivest–Shamir–Adleman (RSA) cryptosystem, Diffie-Hellman algorithm, Public-Key-Infrastructure techniques and digital signature.

At the start, two different channels, a private channel ‘SCh’ is taken for the use of protected communication between user and server while public channel ‘PCh’ is used for unprotected communication between user and server.

```
(*---------------- Channels ----------------*)

free SCh:channel [private].   (*Secure Channel*)

free PCh:channel.

(*---------------- Constants & Variables ----------------*)

free IDia:bitstring.

free PWia:bitstring [private].
```

```
free BTia:bitstring [private].

free S:bitstring [private].

(*---------------- Constructor ----------------*)

fun H(bitstring):bitstring.

fun h(bitstring):bitstring.

fun XOR(bitstring,bitstring):bitstring.

fun CONCAT(bitstring,bitstring):bitstring.

fun E(bitstring,bitstring):bitstring.

(*---------------- Destructors & Equations ----------------*)

equation forall a:bitstring,b:bitstring; XOR(XOR(a,b),b)=a.

reduc forall m:bitstring,key:bitstring; D(E(m,key),key)=m.

(*---------------------- Events ----------------------------*)

event beginUserUi(bitstring).

event endUserUi(bitstring).

event beginServerSIP(bitstring).

event endServerSIP(bitstring).

(*---------------------- Queries ----------------------------*)

free SK:bitstring [private].

query attacker(SK).

query id:bitstring; inj-event(endUserUi(id)) ==> inj-
event(beginUserUi(id)) .

query id:bitstring; inj-event(endServerSIP(id)) ==> inj-
event(beginServerSIP(id)) .

(*--------------------- User Ui ---------------------*)

let UserUi=

(*-------------------- Registration -----------------*)

new q:bitstring;

let HB = H(BTia) in

let M = XOR(HB,q) in

let N = XOR(PWia,(IDia,M)) in

let O =XOR(h(XOR(PWia,(IDia,M))),q) in

out(SCh,(HB, N , IDia));

in(SCh,(xA:bitstring, xF:bitstring));

let P =h(N) in
```

```
(*---------------- Login and Authentication ----------------*)
event beginUserUi(IDia);
new IDia':bitstring;
new PWia':bitstring;
new BTia':bitstring;
let HB' = H(BTia') in
let q' = XOR(O,h(XOR(PWia',(IDia',HB')))) in
let N' = XOR(PWia',(IDia',HB',q')) in
let P' =h(N') in
if (P = P') then
let (B:bitstring) = D(xF,N') in
new T1:bitstring;
let R1 = h(CONCAT(B,(IDia',T1))) in
let R2 = E(CONCAT(P',(IDia',R1,T1)),B) in
out(PCh,(xA, R1, R2, T1));
in(PCh,(xR3:bitstring, xAn:bitstring, xTs1:bitstring));
let (xn:bitstring,xSK:bitstring,xTs1:bitstring) = D(xR3,B) in
let SK = h(XOR(P',xn)) in
if(SK = xSK) then
event endUserUi(IDia)
else
0.
(*---------------------- Server SIP ----------------------*)
let ServerSIP=
(*---- Registration ----*)
in(SCh,(xHB:bitstring, xN:bitstring , xIDia:bitstring));
new ts0:bitstring;
let A = E(CONCAT(IDia,ts0),S) in
let B = E(XOR(IDia,S),S) in
let F =E(B,xN) in
out(SCh,(A, F));
(*---- Login and Authentication ----*)
event beginServerSIP(S);
```

```
in(PCh,(xA:bitstring, xR1:bitstring, xR2:bitstring, xT1:bitstring));

let (xIDia:bitstring,xtsU:bitstring) = D(A,S) in

let B' = E(XOR(xIDia,S),S) in

let R1' = h(CONCAT(B',(xIDia,xT1))) in

if (xR1 = R1') then

let (xP:bitstring,xIDia:bitstring,xR1:bitstring,xT1:bitstring)= D(xR2,B')
in

new n:bitstring;

let SK = h(XOR(xP,n)) in

new Ts1:bitstring;

let R3 = E(CONCAT(n,(SK,Ts1)),B') in

let An = E(CONCAT(xIDia,Ts1),S) in

out(PCh,(R3, An, Ts1));

event endServerSIP(S)

else

U.

process

((!UserUi)  | (!ServerSIP) )
```

The above mentioned program has been executed on ProVerif 1.93. The following result has been displayed.

```
-- Query inj-event(endServerSIP(id)) ==> inj-event(beginServerSIP(id))
Completing...
Starting query inj-event(endServerSIP(id)) ==> inj-event(beginServerSIP(id))
RESULT inj-event(endServerSIP(id)) ==> inj-event(beginServerSIP(id)) is true.
-- Query inj-event(endUserUi(id_624)) ==> inj-event(beginUserUi(id_624))
Completing...
Starting query inj-event(endUserUi(id_624)) ==> inj-event(beginUserUi(id_624))
RESULT inj-event(endUserUi(id_624)) ==> inj-event(beginUserUi(id_624)) is true.
-- Query not attacker(SK[])
Completing...
Starting query not attacker(SK[])
RESULT not attacker(SK[]) is true.
```

The above result shows that both the server and user evolvement beginning and ending successfully also confirms that the session key not exposed to an attacker. Therefore, the confidentiality is preserved.

5. PERFORMANCE AND COMPARATIVE ANALYSIS

In this section the performance of the scheme in terms of attack resistance, functionality, storage-overhead, computation and communication cost is analyzed. As security is inversely proportional to cost and vice versa therefore, in the proposed scheme a delicate balance is shown between security and performance that is discussed one-by-one under the following headings:

5.1 Attack resistance and functionality analysis

The attack resistance and functionality analysis of the proposed authentication scheme are compared with other authentication schemes namely Li *et al.'s* [40], Lue *et al.'s* [41], Zhang *et al.'s* [42], Wu *et al.'s* [43-44] and Kumari *et al.'s* [45] schemes.

The comparison results in Table 2 below determine that the proposed user authentication scheme provide resistance to all known attacks which in terms shows robustness, privacy-preserving authentication scheme.

Table. 2 Performance analysis (comparison)

Schemes ⟶ / **Security Properties** ↓	**[40]**	**[41]**	**[42]**	**[43-44]**	**[45]**	**Proposed**
Resists Denning-Sacco-Attack	Yes	Yes	Yes	Yes	Yes	Yes
Resists Stolen-Verifier Attack	Yes	Yes	Yes	Yes	Yes	Yes
Resists Insider Attack	Yes	No	Yes	Yes	Yes	Yes
Resists Password Disclosure Attack	Yes	Yes	Yes	Yes	No	Yes
Resists Replay Attack	No	No	No	Yes	Yes	Yes
Strong User Anonymity	No	No	No	No	Yes	Yes`
Rests Server Spoofing Attack	Yes	Yes	Yes	Yes	No	Yes
Provides Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes
Provides Certified-Key Guarantee	Yes	Yes	Yes	Yes	Yes	Yes
Resists Impersonation Attack	Yes	No	Yes	Yes	No	Yes

5.2 Computation cost analysis

To scrutinize and evaluate the proposed scheme by comparing computational overhead in the eyes of complexity with six recent schemes e.g. Li *et al.* [40], Lue *et al.*'s [41], Zhang *et al.*'s [42], Wu *et al.*'s [43-44] and Kumari *et al.*'s [45] schemes, the proposed scheme is strong and efficient in terms of computational cost. Table 5 illustrates the comparison in terms of computation cost.

Table. 5 Computational coast analysis of different schemes

Different Schemes		**[40]**	**[41]**	**[42]**	**[43]**	**[44]**	**[45]**	**Proposed**
Phases	**Participant**							
Registration	User	$1t_{\oplus}+1t_h$	$1t_{\oplus}+1t_h$	$5t_{\oplus}+1t_h$	$3t_{\oplus}+1t_h$	$1t_{\oplus}+1t_h$	$2t_{\oplus}+1t_h$	$6t_{\oplus}+3t_h$
	Server	$1t_{\oplus}+5t_h$	$7t_{\oplus}+5t_h$	$2t_{\oplus}+0$	$3t_{\oplus}+3t_h$	$2t_{\oplus}+3t_h$	$3t_{\oplus}+3t_h$	$1t_{\oplus}+0$
Login and Authentication	User	$4t_{\oplus}+9t_h$	$6t_{\oplus}+13t_h$	$13t_{\oplus}+2t_h$	$9t_{\oplus}+7t_h$	$3t_{\oplus}+7t_h$	$10t_{\oplus}+6t_h$	$8t_{\oplus}+5t_h$
	Server	$4t_{\oplus}+9t_h$	$7t_{\oplus}+19t_h$	$9t_{\oplus}+3t_h$	$4t_{\oplus}+8t_h$	$2t_{\oplus}+5t_h$	$3t_{\oplus}+5t_h$	$2t_{\oplus}+2t_h$
Password Change	User	$6t_{\oplus}+7t_h$	$4t_{\oplus}+3t_h$	$7t_{\oplus}+1t_h$	$4t_{\oplus}+5t_h$	$4t_{\oplus}+5t_h$	$7t_{\oplus}+4t_h$	$8t_{\oplus}+3t_h$
	Server	$1\ t_{\oplus}+3t_h$	$2t_{\oplus}+2t_h$	0	$3t_{\oplus}+1t_h$	$3t_{\oplus}+1t_h$	$0+2t_h$	0
Total (Only Login and Authentication phases are considered)		$8t_{\oplus}+18t_h$	$13t_{\oplus}+32t_h$	$22t_{\oplus}+5t_h$	$13t_{\oplus}+15t_h$	$5t_{\oplus}+12t_h$	$13t_{\oplus}+11t_h$	$10t_{\oplus}+7t_h$

Here t_h represents time efficiency of hash-function and $t_{\oplus}$ represents the time efficiency of exclusive-OR operation, then the mentioned table clearly shows the difference among these schemes. Furthermore, the performance analysis of scheme [42] above has reduced the computational cost of one-way hash function time t_h which is considered to be good but its XOR bitwise operation time is much higher than that of the proposed scheme. Also, if any function (either hash or XOR) takes less time for completion it must be higher clock frequency for stored operation. In this way, the computational complexity of the proposed scheme is much better than among all. Therefore, the proposed scheme shows good performance.

5.3 Storage overhead analysis

This is actually the number of parameters stored in the memory of the smart card. The memory of smart card consists of A, F, O, P parameters and "p, q, S, m, n" symmetric key values. Assume that the Symmetric Cryptographic Functions (SHA-1) used in the proposed scheme which can occupy 160 bits key length and the number of parameters in the smart card at registration phase is just 4, so 4 x 160 = 640 bits which are the actual storage cost analysis as shown in Table – 3 below:

Table. 3 Storage overhead analysis

Parameters	Storage Overhead (in bits)
The Parameters of Smart Card {A, F, O, P}	(160+160+160+160)
Total	**640**

5.4 Communication overhead / cost analysis

Power consumption is an attractive topic for research in wireless communication due to either computational overhead or communication determination that can be seen from different angles like its parameters, links, wait time, cryptographic-functions and many more. In fact, the communication cost is higher than computation cost in terms of power consumption. The communication cost is a cycle for the successful communication of messages exchanged between the user and server.

When a legitimate user login into a remote server, it is easy to imagine that the proposed scheme is somewhere same as Li *et al.*'s [40], Lue *et al.*'s [41], Zhang *et al.*'s [42], Wu *et al.*'s [43-44] and Kumari *et al.*'s [45] schemes while somewhere stronger user login and authentication phase.

Let suppose the length of each parameter in the proposed scheme is 160 bits because of using SHA – 1, the one-way hash function values are 256 bits and the operation performing by XOR value always yields zero which can be neglected, therefore, the proposed scheme is relatively small compared to Li *et al.* [40], Lue *et al.*'s [41], Zhang *et al.*'s [42], Wu *et al.*'s [43-44] and Kumari *et al.*'s [45] schemes, because in communication cost when using SHA-1 of key size is 160 bit which is for the proposed scheme is the number of transmitting and receiving bits of each entity. U_{ia} transmits 4 x 160 = 640 bits and receives 3 x 160 = 480 bits; the total communication cost at U_{ia} is 1120 bits. Similarly, the server receives 4 x 160 = 640 bits and transmits 3 x 160 = 480 bits, the total communication cost at server side is also 1120 bits; the total communicational cost of the scheme is 2240 bits, as shown in Table 4 below:

Table. 4 Communication cost analysis

Transmitting/Receiving bits			Messages
U_{ia}:	640+480	1120	1
S_{ia}:	480+640	1120	1
Total:		**2240 bits**	**2**

6. CONCLUSION AND FUTURE WORK

Internet systems such as VoIP and Web applications are growing rapidly in size and complexity to support a large number of users. Mobile platforms such as smartphones and Internet of Things (IoT) are becoming the main medium to access the Internet content. Users will be generating more requests to Internet applications. The entire request load generated by applications needs to be properly handled. The result of which threat level against Internet application is increased and the powerful attackers struggle to compromise these systems. Therefore, more robust security mechanisms are needed. The already designed and implemented practical authentication protocols which guarantee for security which also satisfy the performance and scalability constraints of large-scale VoIP and Web applications than currently deployed protocols based on symmetric cryptographic algorithms. A biometric cryptosystem was also offered in the aforementioned protocol which is a sign of robustness. To extend this three-factor security authentication scheme, one can also use Elliptic Curve Cryptography (ECC), Public Key Infrastructure (PKI) and Discrete Logarithmic Function (DLF) methodologies or else can use big numeral factorization complication. It is mandatory for every researcher to identify the knowledge or experiences that are required for finding out attack(s) on a protocol.

ACKNOWLEDGEMENT

Special thanks to Faculty of Basic & Applied Sciences International Islamic University Islamabad, Pakistan for providing resources to carry out this research. Moreover, special thanks to Dr. Shahzad Ashraf Chaudhry for his kind support in completion of this research.

REFERENCES

1. Lamport, L., *Password Authentication with Insecure Communication, ACM Communications*, 1981. 24(11):p.770-772.
2. Laio Xiong., Jianwei Niu., Saru Kumari., SK Hafizul Islam., Fan Wu., Muhammad Khurram Khan., and Ashok Kumar Das., *A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security*, *Wireless Personal Communications, 2016.* p.1-29.
3. Hsiang, C. and Shih, W.K., *Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces*, 2009. 31(6):p.1118-1123.
4. Sood, S. K., Sarje, A. K., Singh, K., *A secure dynamic identity based authentication protocol for multi-server architecture*, *Journal of Network and Computer Applications*, 2011. 34(2):p.609-618.
5. Chang, C.C., Lee, C.Y., *A secure single sign-on mechanism for distributed computer networks*, *IEEE Trans. on Industrial Electronics*, 2012. 59(1):p.629-637.
6. G.Yang., D. S. Wong., H. Wang, X. Deng., *Two-factor mutual authentication based on smart cards and passwords*, *Journal of Computer and System Sciences*, 2008. vol 74:p.1160-1172.
7. Tsai, J.L., Lo, N.W., Wu, T.C., *Novel anonymous authentication scheme using smart cards*, *IEEE Trans. On Industrial Informatics*, 2013. 9(4):p.2004-2013.
8. Yeh, Hsiu-Lien., Tien-Ho Chen., and Wei-Kuan Shih., *Robust smart card secured authentication scheme on SIP using elliptic curve cryptography*. *Computer Standards & Interfaces* 36, no. 2, 2014. p.397-402.
9. Zhang Liping., Shanyu Tang and Shaohui Zhu., *An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. Journal of Network and Computer Applications* 59, 2016. p.126-133.
10. Zhang Liping., Shanyu Tang., and Shaohui Zhu., *A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP*. *Peer-to-Peer Networking and Applications* 9, no. 1, 2016. p.108-126.
11. Lue, X., Qiu, W., Zheng, D., Chen, K., Li, J., *Anonymity enhancement on robust and efficient password authenticated key agreement using smart cards*, *IEEE Trans. on Industrial Electronics*, 2010. 57(2):p.793-800.
12. Juang, W.S., Chen, S.T., Liaw, H.T., *Robust and efficient password-authenticated key agreement using smart cards*, *IEEE Trans. Industrial Electronics*, 2008. 55(6):p.2551-2556.
13. Wang, D., Ma, C., *Cryptanalysis and security enhancement of a remote user authentication scheme using smart cards*, *The Journal of China Universities of Posts and Telecommunications*, 2012. 19(5):p.104-114.
14. Wang, D., Ma, C., Wang, P., Chen, Z., *iPass: Privacy preserving two-factor authentication scheme against smart card loss problem*, *Journal of Computer and System Sciences* (In press), 2012. p.1-14.
15. Wang, D., Ma, C., Wang, P., *Secure password-based remote user authentication scheme with non-tamper resistant smart cards*, *26th Ann. IFIP Conf. on Data and Applications Security and Privacy*, 2012. p.114-121.
16. Wang, D., Wang, P., *Offline dictionary attack on password authentication schemes using smart cards*, 16th Information Security Conference, 2013. pp.1-14.
17. Wang, Y., *Password protected smart card and memory stick authentication against off-Line dictionary attacks*, 27th IFIP TC 11 Information Security and Privacy Conference, 2012. p.489-500.
18. Wang, D., Wang, P., *On the anonymity of two-factor authentication schemes for wireless sensor networks*: *attacks, principle and solutions*, *Computer Networks*, 2014. 73:41-57.
19. Hsieh, W., Leu, J., *Exploiting hash functions to intensify the remote user authentication scheme*, *Computers & Security*, 31(6), 2012. p.791-798.
20. Huan, X., Chen, X., Li, J., Xiang, Y., Xu, L., *Further observations on smart-card-based password authenticated key agreement in distributed systems*, *IEEE Trans. on Parallel and Distributed Systems*, 25(7), 2013. p.1767-1775.
21. Eric Bach., *Discrete logrithms and factoring. Techinical Report UCB/CSD84/186, Computer Science Division (EECS), University of California, Berkeley, June*, **1984**.
22. Arshad Hamed and Morteza Nikooghadam., *An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. Multimedia Tools and Applications* 75, no. 1, 2016.:p.181-197.
23. Sun, D.Z., Huai, J.P., Sun, J.Z., Zhang, J.W., Feng, Z.Y., *Improvements of Juang et al.'s password authenticated key agreement scheme using smart cards*, *IEEE Trans. on Industrial Electronics*, 2009. 56(6):p.2284-2291.

24. Li, C.T., Lee, C.C., Liu, C.J., Lee, C.W., *A robust remote user authentication scheme against smart card security breach*, 25th Annual IFIP WG 11.3 Conference, 2011. p.231-238.
25. Blanche, Bruno., Ben Smyth and Vincent Cheval, *ProVerif 1.90: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial. URL: http://prosecco. gforge. inria. fr/personal/bblanche/proverif/manual. pdf*, **2015**.
26. Blanchet Bruno., Ben Smyth and Vincent Cheval., *ProVerif 1.88: automatic cryptographic protocol verifier, user manual and tutorial, INRIA Paris-Rocquencourt, LSV, ENS Cachan & CNRS & INRIA Saclay II le-de-France, Paris, Franc*, **2013**.
27. Muir Paul., Shantao Li., Shaoke Lou., Daifeng Wang., Daniel J. Spakowicz., Leonidas Salichos., Jing Zhang et al., *The real cost of sequencing: scaling computation to keep pace with data generation. Genome biology* 17, no. 1. **2016**.
28. Braverman Mark and David P. Woodruff., *Guest Editorial for Information Complexity and Applications. Algorithmica* 76, no. 3, 2016. p.595-596.
29. Hakke Sachin R., and Manohar S. Chaudhari., *Attribute based encryption of data stored in Clouds with Anonymous Authentication. International Journal* 4, no. 3, **2016**.
30. Lu Yanrong., Lixiang Li., Haipeng Peng and Yixian Yang., *A secure and efficient mutual authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications* 9, no. 2, 2016. p.449-459.
31. Burrows M., Abadi M., Needham R., *A logic of authentication, ACM Trans Comput Syst* Vol. 08,p.108-126.
32. Mart´ın Abadi and Andrew D. Gordon., A calculus for cryptographic protocols: *The pi calculus Information and Computation, January 1999*. 148(1):1–70. *An extended version appeared as Digital Equipment Corporation Systems Research Center* report no. 149, January 1998.
33. Benjamin C. Pierce and David N. Turner. Pict: *A programming language based on the pi-calculus. In Gordon Plotkin, Colin Stirling, and Mads Tofte, editors*, Proof, Language and Interaction: *Essays in Honour of Robin Milner, Foundations of Computing.* MIT Press, May **2000**.
34. Blanchet Bruno., Ben Smyth and Vincent Cheval. ProVerif 1.90: Automatic Cryptographic Protocol Verifier, User Manual and Tutorial, 2015.
35. Stallings, W., Cryptography and network security: principles and practices, 3th edition: Prentice Hall, 2003.
36. Gong L., Needham R., Yahalom R., Reasoning about belief in cryptographic protocols, *Proceedings of IEEE Computer Society Symp. Research in Security and Privacy, Oakland*, CA, 7–9 May, 1990. p.234–248.
37. Jin, Andrew Teoh Beng., David Ngo Chek Ling and Alwyn Goh. *Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition* 37, no. 11, 2004. p.2245-2255.
38. Eric Bach., *Discrete logrithms and factoring. Techinical Report UCB/CSD84/186, Computer Science Division (EECS), University of California, Berkeley*, June, 1984.
39. Lee Cheng-Chi., Tsung-Hung Lin and Rui-Xiang Chang., *A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. Expert Systems with Applications* 38, no. 11m. 2011. p.13863-13870.
40. Li, X., Xiong, Y., Ma, J., Wang, W., *An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards, Journal of Network and Computer Applications*, 2012. 35(2):p.763-769.
41. Leu Jenq-Shiou and Wen-Bin Hsieh., *Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. Information Security, IET* 8, no. 2, 2014. p.104-113.
42. Zhang Liping., Shanyu Tang., and Shaohui Zhu., *A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP*. *Peer-to-Peer Networking and Applications* 9, no. 1, 2016. p.108-126.
43. Wu F., Xu L., Kumari S., Li X., *A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks, 2015.* Comput Electr Eng. doi:10.1016/ j.compeleceng.
44. Wu Fan., Lili Xu., Saru Kumari., Xiong Li and Abdulhameed Alelaiwi. *A new authenticated key agreement scheme based on smart cards providing user anonymity with formal proof. Security and Communication Networks* 8, no. 18, 2015. p.3847-3863.
45. Kumari Saru., Muhammad Khurram Khan and Xiong Li., *An improved remote user authentication scheme with key agreement.* Computers & Electrical Engineering, Vol. 40, no 6, 2014. pp 1997-2012.

AUTHORS PROFILE

SAEED ULLAH JAN received the MPhil degree in network security from University of Malakand in 2016. He is working as a Lecturer in Computer Science at Higher Education, Achieves & Libraries Department Govt of Khyber Pakhtunkhwa – Pakistan. His research interests include Information Security, VoIP and SIP Authentication. Saeed Ullah Jan also working as BS – Coordinator at Govt College Wari (Dir Upper) and has started 09 BS Disciplines in the far-flung remote area of the province where most of the youngers have no access to Universities for higher education. Currently, he is PhD scholar in the Department of Computer Science & IT – University of Malakand.

FAWAD QAYUM received PhD Degree from University of Leicester, U.K in 2012. He is working as In-charge Department of Software Engineering University of Malakand, Pakistan. His research Interests includes: Model-driven software evolution and re-engineering. Quality-Controlled Refactoring at Model Level Using Graphs and Search-Based Refactoring using Graph Transformation Systems.

SOHAIL ABBAS received the PhD Degree from Liverpool John Moores University, Liverpool UK, in 2011. His research interest includes Cooperation Enforcement in Adhoc Networks, Reputation and Trust based schemes, detection of identity based Attacks, selfish or misbehavior node detection in routing and in MAC 802.11 protocols in static and mobile adhoc networks, as well as in Internet of Things (IoT) environments.

GHULAM MURTAZA KHAN received the MS degree in Software Engineering from International Islamic University Islamabad in 2012. Currently he is working as Lecturer in Computer Science at Shaheed BB University Sheringal Pakistan. His research interest includes; Software Engineering, GSD, GSE, Agile computing, Green computing, Cloud computing and Mobile/Ubiquitous computing. Currently, he is PhD scholar in the Department of Computer Science & IT – University of Malakand.

AJAB KHAN received the PhD Degree from University of Leicester, U.K in 2011. Currently he is working as In-charge Department of Computer Science & IT, University of Malakand. His research interest includes; Stochastic Simulation of P2P VoIP Network Reconfiguration Using Graph Transformation, Modeling Skype like VoIP protocol and graph transformation based modeling.

SIFFAT ULLAH KHAN received the Ph.D. degree in computer science from Keele University, U.K. He is currently an Assistant Professor in the Department of Computer Science & IT, University of Malakand. He has authored over 110 articles, so far, in well reputed international conferences and journals. His research interest includes software outsourcing, empirical software engineering, agile software development, systematic literature review, and software metrics, cloud computing, requirements engineering, and green computing/IT.