An improved Authentication Protocol for SIP-based VoIP

Husnain Naqvi, Shehzad Ashraf Chaudhry, Khalid Mahmood,
Department of Computer Science and Software Engineering
International Islamic University
Islamabad, Pakistan
husnain.naqvi@iiu.edu.pk, shahzad@iiu.edu.pk, khalid.phdcs74@iiu.edu.pk

***Abstract*—The SIP being an application layer protocol for signaling has been considered as the most appropriate one for multimedia applications. In order to detect some collisions and replay attacks, the SIP offers built-in authentication mechanism as per its specification, designated as HTTP digest based authentication, but study reveals that it is vulnerably susceptible to heterogeneous security issues such as impersonation attacks, man-in-the-middle attacks (MITM), server spoofing and password guessing attacks. Very recently Zhang et al. proposed symmetric key based anonymous authentication scheme for SIP. They claimed the scheme to provide privacy and anonymity, but the analysis in this paper expose that Zhang et al.'s scheme does not provide dynamic identity hence it is not anonymous. Furthermore, we proposed an improved anonymous authentication scheme for SIP. The scheme is more secure as compared with Zhang et al.'s scheme.**

I. Introduction

Voice over Internet Protocol (VoIP) offer audio, video and multimedia services over IP networks. The rapid spread, utilization and success of VoIP is hidden in its flexible implementation and cost effectiveness. To maintain this rapid spread and success of VoIP, many flexible, efficient and secure signaling protocols have been proposed. As the IP Multimedia Subsystem (IMS) has also implemented SIP in its architectural framework to provide IP based multimedia services. The Session Initiation Protocol (SIP) is therefore most widely used among other protocols due to its lightweight scalable and flexible nature. It is text based application-layer control protocol and is utilized to create, manage and terminate sessions among participants. No doubt SIP is an attractive package for authentication along with its impressive features but it is somehow vulnerable to various kind of security threats, and it is due to direct inheritance from HTTP Digest authentication. In recent years researchers are busy to develop secure authentication protocol for SIP but it proved out to be a challenging task due to two major reasons. One is that it should be secure enough to provide protection for IP based networks against various types of threats and other is that it should not be compute intensive because VoIP systems cannot afford the latency due to intensive computations.

Performance and security are inversely proportional to each other, therefore it is a challenging task to introduce an authentication protocol that provide a trade off between the two. A number of prevailing authentication schemes have been proposed [1]–[36]. The schemes proposed on the notion of public key cryptography [1]–[4], [7]–[9], [13]–[19], [32]–[34] are more expensive in terms of computation and communication cost. Furthermore, such schemes incurs more delay and latency as compared with symmetric key primitive based schemes [20]–[28], [35], [36]. So public key based schemes are not suitable for delay sensitive and resource constrained environments. While the schemes based on symmetric key primitives are more vulnerable to a number of attacks [37]. A number of such schemes are also having correctness issues [38], [39].

Zhang et al. [40] recently presented a lightweight authentication protocol for SIP using biometrics characteristics and claimed that their proposed protocol is an initial step as it completely preserve the privacy of user identity and biometric characteristics. But our analysis reveals that Zhang et al. scheme doesn't provide dynamic ID. An adversary, by just analyzing the channel can easily verify whether two sessions are initiated by the same user.

II. Zhang et al.'s scheme

Recently Zhang et al. proposed a lightweight privacy preserving authenticated key agreement protocol for SIP based VoIP. The scheme comprises of three phases registration phase, authentication phase and password change phase. To easily understand the scheme we have listed the notations used through out the paper in Table I. Zhang et al.'s scheme is shown in Fig. 1 and is elaborated in following subsections:

A. Registration phase

When a user wants to register with SIP server in order to become a new legal user, it performs following steps:

Step 1:

$\mathcal{U}_i$ chooses its user-name ID_i and password PW_i and generates a biometric template BT_i. Then using random integer r it calculates $X = r \oplus BT_i$, $Y = PW_i \oplus X \oplus ID_i$ and $Z = h(PW_i \oplus ID_i) \oplus r$. $\mathcal{U}_i$ sends registration request containing $\{ID_i, Z, h(.)\}$ to server through a secure channel.

Table I
Notation Guide

Symbol	Definition
$\mathcal{S}$	SIP server
s	Server's secret key
$\mathcal{U}_i$	The Legal user
ID_i	$\mathcal{U}_i$'s identity
PW_i	$\mathcal{U}_i$'s password
BT_i	$\mathcal{U}_i$'s biometric template stored in smart card
T_{s0}, T_{s1}	Time stamps
$\oplus$	XOR operation
$\|\|$	Concatenation operation
SK	Shared session key

Step 2:

The SIP server $\mathcal{S}$ selects random secret key s, computes $I = E_s(ID_i)$, $J = E_s(ID_i \oplus s)$, $K = (J \oplus Y)$ and $L = E_J(Y)$. $\mathcal{S}$ then maintains a record of $(ID_i, h(.))$ in a specific table known as identity table. The server stores the secure information (I, K, L) in the smart card and issues it to user U_i through secure channel.

Step 3:

On getting the smart card the user $\mathcal{U}_i$ stores $(Z, X, h(.))$ in the smart card secretly. The Smart card finally contains $(I, K, L, X, Z, h(.))$

B. Authentication phase

Authentication phase as shown in Figure 1 involves the following step:

Step 1:

$\mathcal{U}_i$ enters his ID_i and PW_i after inserting the smart card into reader then scan iris of user in order to generate biometric template BT_i^*. $\mathcal{U}_i$ then extract random integer r using ID_i, PW_i and Z the secret information stored in the smart card. Smart card then uses n and BT_i^* to find X'. Then it compares the X and X' and if the match score exceeds a predetermined threshold value the authentication process instantly terminates otherwise the smart card computes J' using X, K, ID_i and PW_i. Then it checks $E_J(PW_i \oplus X \oplus ID_i =^? L)$ and if it holds then server selects a random integer m and computes $R_1 = ((PW_i \oplus X \oplus ID_i)||m)$ and $R_2 = E'_J(K||ID_i||R_1)$. After that user sends a request $REQUEST(I, R_2)$ to server over public channel.

Step 2:

In order to know the ID_i of user the $\mathcal{S}$ decrypts I with its secret key s and checks it in the identity table to ensure that the user ID_i is valid. In case of invalid ID_i the authentication session expires. On the other hand if the ID_i is valid server computes $J = E_s(ID_i \oplus s)$ using ID_i and secret key s. Then it decrypts the R_2 by J to get K, R_1 and ID_i. Then comparison of ID_i in I with ID_i in R_2 is performed by the server. Inequality leads to process termination otherwise it computes $Y = K \oplus J$. Then it is verified whether the equation $PW_i \oplus X \oplus ID_i =^? Y$ holds. If it holds then server chooses two random integers a, b and uses the hash function $h(.)$ to obtain session key and then server sends a challenge message $CHALLANGE(realm, Au_s, a)$ to user.

Step 3:

The user decrypts the Au_s using J' to get R_3 and R_4. Smart card extracts b using R_3, ID_i, PW_i and X. Then the smartcard compute and verify the R_4. It then sets the session key SK' and computes authentication information Au_u. User sends a response message $RESPONSE(realm, Au_u)$ to server.

C. Password change phase

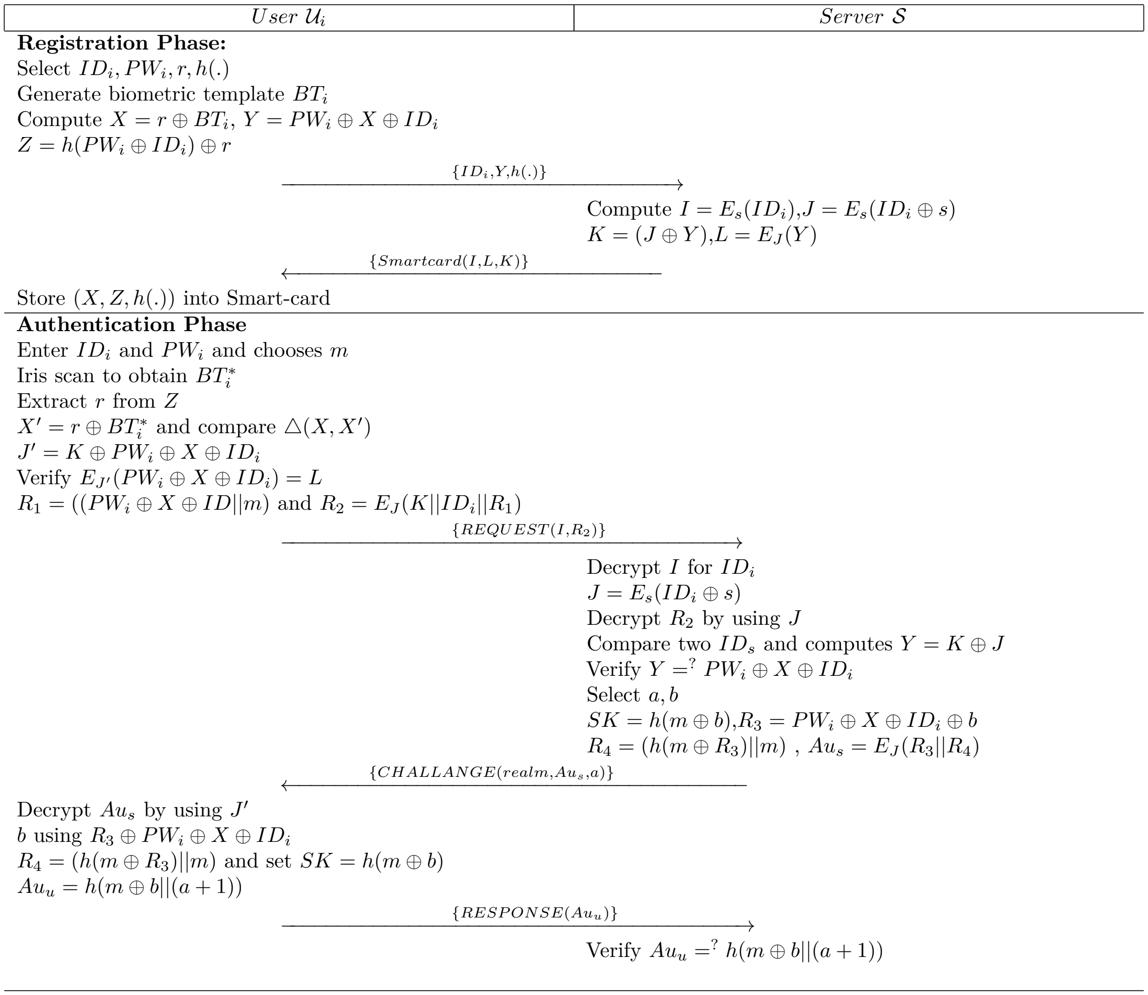
This phase is initiated when user wants to update his password, $\mathcal{U}_i$ insert his smart card and generate biometric template BT_i^*. Then $\mathcal{U}_i$ enters his ID_i and PW_i. The smart card extracts random integer r from Z. Then it computes X' using r and the biometric data BT_i^*. Then it compares X with X' and upon successful verification it sends a request for new password. User enters the new password and sends to smart card. On getting new password it computes Z^* , K^* , L^* respectively and replace old values with these new values.

III. Cryptanalysis of Zhang et al.'s scheme

This section shows that Zhang et al.'s scheme lacks strong anonymity and is vulnerable to replay and denial of services attacks.

A. Lacks Strong Anonymity

Privacy and anonymity protects user's sensitive information from the adversary, the leakage of such information may enables the adversary to analyze victim's lifestyle, preferences, the social circles and so on. Importantly, the expose of such information in wireless environments can help the adversary to track the current location and login history of the target[UFO2F]. To achieve user anonymity, the typical approach is to employ dynamic ID, where the real identity of the user is covered in session related parameters. An authentication scheme is said to preserve anonymity and privacy if it possesses two properties (i) Real identity of user should not revealed to an adversary, (ii) User should have dynamic identity for each session so that adversary cannot distinguish whether two different sessions are initiated by same user. In Zhang et al.'s scheme the server using its secret key encrypts user's real ID and stores it in the smart card. The user sends this encrypted ID in each authentication request, since in each session same ID is used, so Zhang et al.'s scheme does not employ the dynamic ID. The adversary can easily trace whether two different sessions are initiated by same user.



User $\mathcal{U}_i$ | *Server* $\mathcal{S}$

Registration Phase:

Select $ID_i, PW_i, r, h(.)$
Generate biometric template BT_i
Compute $X = r \oplus BT_i$, $Y = PW_i \oplus X \oplus ID_i$
$Z = h(PW_i \oplus ID_i) \oplus r$

$\xrightarrow{\{ID_i,Y,h(.)\}}$

Compute $I = E_s(ID_i)$,$J = E_s(ID_i \oplus s)$
$K = (J \oplus Y)$,$L = E_J(Y)$

$\xleftarrow{\{Smartcard(I,L,K)\}}$

Store $(X, Z, h(.))$ into Smart-card

Authentication Phase

Enter ID_i and PW_i and chooses m
Iris scan to obtain BT_i^*
Extract r from Z
$X' = r \oplus BT_i^*$ and compare $\triangle(X, X')$
$J' = K \oplus PW_i \oplus X \oplus ID_i$
Verify $E_{J'}(PW_i \oplus X \oplus ID_i) = L$
$R_1 = ((PW_i \oplus X \oplus ID||m)$ and $R_2 = E_J(K||ID_i||R_1)$

$\xrightarrow{\{REQUEST(I,R_2)\}}$

Decrypt I for ID_i
$J = E_s(ID_i \oplus s)$
Decrypt R_2 by using J
Compare two ID_s and computes $Y = K \oplus J$
Verify $Y =^? PW_i \oplus X \oplus ID_i$
Select a, b
$SK = h(m \oplus b)$,$R_3 = PW_i \oplus X \oplus ID_i \oplus b$
$R_4 = (h(m \oplus R_3))||m)$, $Au_s = E_J(R_3||R_4)$

$\xleftarrow{\{CHALLANGE(realm,Au_s,a)\}}$

Decrypt Au_s by using J'
b using $R_3 \oplus PW_i \oplus X \oplus ID_i$
$R_4 = (h(m \oplus R_3))||m)$ and set $SK = h(m \oplus b)$
$Au_u = h(m \oplus b||(a + 1))$

$\xrightarrow{\{RESPONSE(Au_u)\}}$

Verify $Au_u =^? h(m \oplus b||(a + 1))$

Figure 1. Zhang et al.'s scheme

B. Replay Attack

The scheme is vulnerable to replay attack. Adversary can intercept the $REQUEST(I, C_2)$ and later replay this $REQUEST(I, C_2)$, of course adversary will not be able to share the session key with server, but server can be overwhelmed by too many authentication requests sent intentionally by the adversary, which may exhaust the computation power of server or the user may face denial of services.

IV. Proposed Scheme

The major problem with the Zhang et al. scheme is that identity of the user remain same for different sessions therefore an adversary can easily guess that the two different sessions are initiated by same user which nullify their claim of user anonymity and privacy. The proposed idea is to keep the user's identity dynamic to make it impossible for the adversary to guess initiation of two session by same user. Note that the password change phase is considered same as discussed in zhang et al.'s scheme but the registration and authentication phase of proposed scheme are as under:

A. Registration phase

For registration a new legal user performs the following steps:

Step 1:
The first step is similar to Zhang et al.'s scheme as described in subsection II-A .

Step 2:
The SIP server selects random secret key, computes $I = E_s(ID_i||t_{s0})$, (Where t_{s0} is the current time stamp), $J = E_s(ID_i \oplus s)$, $K = E_s(J \oplus Y)$ and $L = E_J(Y)$. SIP server then maintains a record of $(ID_i, h(.))$ in a specific table known as identity table. The server stores the secure information (I, K, L) in the smart card and issues it to user U_i through secure channel.

Step 3:
The user U_i stores $(Z, X, h(.))$ in the smart card secretly. The Smart card finally contains $(I, K, L, X, Z, h(.))$.

User $\mathcal{U}_i$	*Server* $\mathcal{S}$
Registration Phase Select $ID_i, PW_i, r, h(.)$ Generate BT_i Compute $X = r \oplus BT_i$, $Y = PW_i \oplus X \oplus ID_i$, $Z = h(PW_i \oplus ID_i) \oplus r$	
$\xrightarrow{\{ID_i,Y,h(.)\}}$	
	Compute $I = E_s(ID_i\|\|t_{s0})$,$J = E_s(ID_i \oplus s)$ $K = (J \oplus Y)$,$L = E_J(Y)$
$\xleftarrow{\{Smartcard(I,L,K)\}}$	
Store $(X, Z, h(.))$ into Smart-card	
Authentication Phase Enters ID_i and PW_i and chooses m Iris scan to obtain BT_i^* Extract r from Z $X' = r \oplus BT_i^*$ and compare $\triangle(X, X')$ $J' = K \oplus PW_i \oplus X \oplus ID_i$ Verify $E_{J'}(PW_i \oplus X \oplus ID_i) = L$ $R_1 = ((PW_i \oplus X \oplus ID\|\|m)$ and $R_2 = E_J(K\|\|ID_i\|\|R_1\|t_i)$	
$\xrightarrow{\{REQUEST(I,R_2,t_i)\}}$	
	For $t_{sc} - t_i \leq \delta$ Decrypt I for ID_i and finds it in identity table $J = E_s(ID_i \oplus s)$ Decrypt R_2 by using J Compare two ID_s, two time stamps t_i Computes $Y = K \oplus J$ Verify $Y =^? PW_i \oplus X \oplus ID_i$ Select a, b Compute $SK = h(m \oplus b)$,$R_3 = PW_i \oplus X \oplus ID_i \oplus b$ $R_4 = (h(m \oplus R_3)\|\|m)$, $Au_s = E_J(R_3\|\|R_4)$ $I_n = E_s(ID_i\|\|t_{s1})$
$\xleftarrow{\{CHALLANGE(realm,Au_s,a,I_n))\}}$	
Decrypt Au_s by using J' Compute b using $R_3 \oplus PW_i \oplus X \oplus ID_i$ $R_4 = (h(m \oplus R_3)\|\|m)$ and set $SK = h(m \oplus b)$ Compute $Au_u = h(m \oplus b\|\|(a + 1))$ $I = I_n$	

Figure 2. Proposed Scheme

B. Authentication phase

The authentication phase involves the following steps as shown in Figure 2, which are as follows:

Step 1:

$\mathcal{U}_i$ enters his ID_i and PW_i after inserting the smart card into reader then scan iris of user in order to generate biometric template BT_i^*. $\mathcal{U}_i$ then extract random integer r using ID_i, PW_i and Z the secret information stored in the smartcard. Smartcard then uses n and BT_i^* to find X'. Then it compares the X and X' and if the match score exceeds a predetermined threshold value the authentication process instantly terminates otherwise the smart card computes J' using X, K, ID_i and PW_i. Then it checks $E_J(PW_i \oplus X \oplus ID_i =^? L)$ and if it holds then server selects a random integer m and computes $R_1 = ((PW_i \oplus X \oplus ID_i)||m)$ and $R_2 = E'_J(K||ID_i||R_1)$. After that user sends a request $REQUEST(I, R_2)$ to server over public channel.

Step 2:

In order to know the ID_i of user the $\mathcal{S}$ decrypts I with its secret key s and checks it in the identity table to ensure that the user ID_i is valid. In case of invalid ID_i the authentication session expires. On the other hand if the ID_i is valid server computes $J = E_s(ID_i \oplus s)$ using ID_i and secret key s. Then it decrypts the R_2 by J to get K, R_1 and ID_i. Then comparison of ID_i in I with ID_i in R_2 is performed by the server. Inequality leads to process termination otherwise it computes $Y = K \oplus J$. Then it is verified whether the equation $PW_i \oplus X \oplus ID_i =^? Y$ holds. If it holds then server chooses two random integers a, b and uses the hash function $h(.)$ to obtain session key.R_4,Au_s and $I_n = E_s(ID_i||t_s1)$ and are computed, then server sends a challenge message $CHALLANGE(realm, Au_s, a, I_n)$ to user.

Step 3:

$\mathcal{U}_i$ decrypts Au_s using J' to get R_3 and R_4. Smartcard extracts b using R_3, ID_i, PW_i and X. Then the smartcard computes and verifies R_4. It then sets the session key SK' and computes authentication information Au_u. I_n is taken as I. User sends a response message $RESPONSE(realm, Au_u)$ to server.

V. Security comparison

Security of proposed scheme is evaluated with respect to other related protocols of Zhang et al. [40] and Kumari et al. [28]. Stolen-verifier along with insider attack are impossible because our scheme does not store password or maintain table on server. Smart card contain entropy protected biometric template, so even in case of theft or lost it is impossible for the adversary to extract the stored biometric characteristics. Identity of user is not even protected by ciphertext but all it is kept dynamic so that adversary fails to differentiate that the two sessions are initiated by the same user or not. Therefore, our protocol actually provide the user anonymity. While Zhang et al.'s scheme does not provide proper user anonymity and Kumari et al.'s protocol does not resists smart card stolen attack.

VI. Performance comparison

Performance is compared with respect to two major operations which are symmetric encryption/ decryption (denoted as T_{Sen}) and one way hash function (denoted as T_{Owh}). Proposed scheme just incurs an extra T_{Sen} operation as compared to Zhang et al.'s scheme [40]. While Zhang et al.'s scheme is does not provide user untraceability additionally Kumari et al.'s scheme [40] is more lightweight but it does not resists smart card stolen attack. Performance comparison is solicited in Table II.

VII. Conclusion

In this paper, we have cryptanalyzed a recent authentication scheme. We have proven that Zhang et al.'s scheme does not provide user traceability and is vulnerable to replay attack Furthermore, we proposed an improved biometric based authentication scheme. Proposed scheme is robust against several attacks and provides user untraceability while having slight higher computation cost.

References

[1] Q. Xie, N. Dong, D. S. Wong, B. Hu, Cryptanalysis and security enhancement of a robust two-factor authentication and key agreement protocol, International Journal of Communication Systems (2014) n/a–n/adoi:10.1002/dac.2858.

[2] H. Arshad, M. Nikooghadam, An efficient and secure authentication and key agreement scheme for session initiation protocol using ecc, Multimedia Tools and Applications (2014) 1–17.

[3] A. Irshad, M. Sher, E. Rehman, S. A. Ch, M. U. Hassan, A. Ghani, A single round-trip sip authentication scheme for voice over internet protocol using smart card, Multimedia Tools and Applications (2013) 1–18doi:10.1007/s11042-013-1807-z.

[4] A. Irshad, M. Sher, M. S. Faisal, A. Ghani, M. Ul Hassan, S. A. Ch, A secure authentication scheme for session initiation protocol by using ecc on the basis of the tang and liu scheme, Security and Communication Networks 7 (8). doi:10.1002/sec.834.

[5] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Farash, M. K. Khan, An improved smart card based authentication scheme for session initiation protocol, Peer-to-Peer Networking and Applications (2015) 1–15doi:10.1007/s12083-015-0409-0.

[6] M. S. Farash, S. A. Chaudhry, M. Heydari, S. M. Sajad Sadough, S. Kumari, M. K. Khan, A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security, International Journal of Communication Systems (2015) n/a–n/adoi:10.1002/dac.3019.

[7] R. Amin, G. Biswas, An improved rsa based user authentication and session key agreement protocol usable in tmis, Journal of Medical Systems 39 (8) (2015) 1–14.

[8] R. Amin, G. Biswas, Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment, Wireless Personal Communications (2015) 1–24.

[9] S. A. Chaudhry, H. Naqvi, M. Sher, M. S. Farash, M. u. Hassan, An improved and provably secure privacy preserving authentication protocol for sip, Peer-to-Peer Networking and Applications (2015) 1–14doi:10.1002/ppna.1299.

[10] S. A. Chaudhry, K. Mahmood, H. Naqvi, M. K. Khan, An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography, Journal of Medical Systems (2015) 1–12doi:10.1007/s10916-015-0335-y.

[11] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, M. K. Khan, An enhanced privacy preserving remote user authentication scheme with provable security, SECURITY AND COMMUNICATION NETWORKS (2015) 1–13doi:10.1002/sec.1299.

[12] S. A. Chaudhry, M. Farash, H. Naqvi, M. Sher, A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography, Electronic Commerce Research (2015) 1–27doi:10.1007/s10660-015-9192-5.

[13] L. Zhang, S. Tang, Z. Cai, Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card, International Journal of Communication Systems.

[14] C.-C. Chang, T.-F. Cheng, W.-Y. Hsueh, A robust and efficient dynamic identity-based multi-server authentication scheme using smart cards, International Journal of Communication Systems (2014) n/a–n/adoi:10.1002/dac.2830.

[15] J. Wei, X. Hu, W. Liu, Two-factor authentication scheme using attribute and password, International Journal of Communication Systems (2014) n/a–n/adoi:10.1002/dac.2915.

[16] N. ul Amin, M. Asad, N. Din, S. Ashraf Ch, An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem, in: Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on, IEEE, 2012, pp. 118–121.

[17] S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, M. Farash, Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems, Journal of Medical Systems 39 (6). doi:10.1007/s10916-015-0244-0.

[18] M.-C. Chuang, M. C. Chen, An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, Expert Systems with Applications 41 (4) (2014) 1411–1418.

[19] M. S. Farash, An improved password-based authentication scheme for session initiation protocol using smart cards without verification table, International Journal of Communication Systemsdoi:10.1002/dac.2879.

[20] J.-S. Leu, W.-B. Hsieh, Efficient and secure dynamic id-based remote user authentication scheme for distributed systems using smart cards, Information Security, IET 8 (2) (2014) 104–113.

[21] C.-T. Chen, C.-C. Lee, A two-factor authentication scheme with anonymity for multi-server environments, Security and Communication Networks (2014) n/a–n/adoi:10.1002/sec.1109. URL `http://dx.doi.org/10.1002/sec.1109`

[22] X. Li, J. Ma, W. Wang, Y. Xiong, J. Zhang, A novel smart card and dynamic id based remote user authentication scheme for multi-server environments, Mathematical and Computer Modelling 58 (1) (2013) 85–95.

[23] C.-C. Lee, T.-H. Lin, R.-X. Chang, A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards, Expert Systems with Applications 38 (11) (2011) 13863–13870.

Table II
Computation Cost Analysis

Scheme→	Our	[40]	[28]
Registration	$3T_{Sen} + 1T_{Owh}$	$3TSenc + 1T_{Owh}$	$4T_{Owh}$
Login and Authentication	$7T_{Sen} + 6T_{Owh}$	$6T_{Sen} + 6T_{Owh}$	$11T_{Owh}$

[24] D. Mishra, A. K. Das, S. Mukhopadhyay, A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards, Expert Systems with Applications 41 (18) (2014) 8129–8143.

[25] Y.-y. Wang, J.-y. Liu, F.-x. Xiao, J. Dan, A more efficient and secure dynamic id-based remote user authentication scheme, Computer communications 32 (4) (2009) 583–585.

[26] M. L. Das, A. Saxena, V. P. Gulati, A dynamic id-based remote user authentication scheme, Consumer Electronics, IEEE Transactions on 50 (2) (2004) 629–631.

[27] Y.-F. Chang, W.-L. Tai, H.-C. Chang, Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update, International Journal of Communication Systems 27 (11) (2014) 3430–3440.

[28] S. Kumari, M. K. Khan, X. Li, An improved remote user authentication scheme with key agreement, Computers & Electrical Engineering 40 (6) (2014) 1997–2012.

[29] S. A. Ch, N. uddin, M. Sher, A. Ghani, H. Naqvi, A. Irshad, An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography, Multimedia Tools and Applications (2014) 1–13doi:10.1007/s11042-014-2283-9.

[30] S. Ch, W. Nasar, Q. Javaid, et al., Efficient signcryption schemes based on hyperelliptic curve cryptosystem, in: Emerging Technologies (ICET), 2011 7th International Conference on, IEEE, 2011, pp. 1–4.

[31] R. Amin, G. Biswas, A novel user authentication and key agreement protocol for accessing multi-medical server usable in tmis, Journal of medical systems 39 (3) (2015) 1–17.

[32] R. Amin, G. Biswas, A secure three-factor user authentication and key agreement protocol for tmis with user anonymity, Journal of medical systems 39 (8) (2015) 1–19.

[33] D. Giri, T. Maitra, R. Amin, P. Srivastava, An efficient and robust rsa-based remote user authentication for telecare medical information systems, Journal of medical systems 39 (1) (2015) 1–9.

[34] Z. Mehmood, N. Nizamuddin, S. Ch, W. Nasar, A. Ghani, An efficient key agreement with rekeying for secured body sensor networks, in: Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on, IEEE, 2012, pp. 164–167.

[35] S. Kumari, M. K. Khan, More secure smart card-based remote user password authentication scheme with user anonymity, Security and Communication Networks 7 (11) (2014) 2039–2053.

[36] S. Kumari, M. K. Khan, M. Atiquzzaman, User authentication schemes for wireless sensor networks: A review, Ad Hoc Networks.

[37] D. Wang, P. Wang, On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions, Computer Networks 73 (2014) 41–57.

[38] D. Wang, D. He, P. Wang, C. Chu, Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment, Dependable and Secure Computing, IEEE Transactions on PP (99) (2014) 1–1. doi:10.1109/TDSC.2014.2355850.

[39] S. A. Chaudhry, Comment on 'robust and efficient password authenticated key agreement with user anonymity for session initiation protocol-based communications', IET Communications 9 (2015) 1034–1034(1).

[40] L. Zhang, S. Tang, S. Zhu, A lightweight privacy preserving authenticated key agreement protocol for sip-based voip, Peer-to-Peer Networking and Applications (2014) 1–19doi:10.1007/s12083-014-0317-8.