Wireless Pers Commun (2015) 85:241–261
DOI 10.1007/s11277-015-2736-0

A Dynamic-Identity Based Multimedia Server Client Authentication Scheme for Tele-Care Multimedia Medical Information System

Deebak Bakkiam David[1] · Muthaiah Rajappa[1] · Thenmozhi Karupuswamy[2] · Swaminathan Pitchai Iyer[1]

Published online: 19 May 2015

Abstract Recently, several biometric and tele-care based user authentication schemes have been proposed to enhance the safe and security of the systems. In 2013, the authors, namely Das et al. improved the authentication scheme of Chang et al. to overcome the severe security flaws, such as failed to protect man-in-the-middle attack, failed to provide the reliable authentication and flaws in client login-phase. Besides, the authors evaluated the authentication in the simulation tool of AVISPA. In the same year, the authors, namely Khurram et al. proposed an improved the authentication scheme of Youngwa An to eradicate the security flaws, like impersonation attack, mutual authentication and user anonymity. The authors, like Das et al. and Khurram et al. have had their own strategies to mitigate the security flaws, though they are still not able to evaluate their schemes in the real time medical information systems. Besides, both authors fail to prove the privacy preservation to the user systems. Thus, this paper proposes a dynamic-identity based multimedia server client authentication scheme to resolve the major security threats of Das et al. and Khurran et al. We prove that our proposed scheme is secure and efficient in comparison with the authentication schemes, namely Youngwa An, Khurram et al., Das et al. and Chang et al. We also depict that our proposed scheme can offer the features like privacy preservation and service scalability reliably for the user systems. Eventually, we design an develop a real time testbed of multimedia medical information system to cross-examine the authentication schemes. In the cross-examination, our authentication scheme

✉ Deebak Bakkiam David
bddeebak@sastra.ac.in

Muthaiah Rajappa
sjamuthaiah@core.sastra.edu

Thenmozhi Karupuswamy
thenmozhik@ece.sastra.edu

Swaminathan Pitchai Iyer
deanpsw@sastra.edu

[1] School of Computing, SASTRA University, Thanjavur, Tamil Nadu 613401, India

[2] School of Electrical and Electronics, SASTRA University, Thanjavur, Tamil Nadu 13401, India

shows the most achievable results for the metrics like call setup time, signal congestion and bandwidth consumption in relation to the other authentication schemes, such as Youngwa An, Khurram et al., Das et al. and Chang et al.

Keywords Biometric · Tele-care · User authentication scheme · Real time testbed of multimedia medical information system · Security threats · Call setup time · Bandwidth consumption and Signal congestion

1 Introduction

As the wireless multimedia communications and Internet technologies have been proliferating all the corners of the world, thus the tools of which the former and latter technologies have been incorporated, are necessitated to verify the legitimacy of remote-user logon request. In the remote-user logon-cum-authentication process, a remote-server should be able to authenticate a registered user/client related to his/her confidential data. Nowadays, the development tools such as the Internet and multimedia become continuous and moreover its related services such as health/tele-care medical information system personal business-activities, administrative document-activities and social activities can be served through the source of Internet. Since the devices/technologies of telecommunication have been able to reside in any place, the medical devices, such as tele-medicine system can be brought into the home of the patient, by which the doctor and patient can directly be connected through the tele-care machine to ensure the current condition of the patient's health.

As a consequence, the tele-care machine, like Tele-care Medical Information System (TMIS) should ensure the authentication key factors, such as data-integrity, confidentiality, privacy, mutual authenticity, less computation, communication and execution cost for the sake of sever client security efficiency. The authentication key factors are necessitated to place the limit on the access of server resources, and thus guarantee that the server resources can't be available to the ill-legitimate users. On the other hand, in the process of server client authentication, the systems like server and client should use the session key to guarantee that the systems are established the connection over a secure channel. Thus, the ill-legitimate users can't access the server resources. For the ease of security, many researchers have proposed the password schemes of authentication [1–21] and in which the smart card system has been used as common.

Besides, the researchers are used to define the users' identities as static as to all the service session transactions and it may provide some information leak to the ill-legitimate users to initiate a threat of identity (ID) theft. To address the issue of ID-theft, the authors of Das et al. [2] proposed a dynamic authentication scheme for the ID-based systems. The authors of Wang et al. [3] proven that the scheme of Das et al. [2] is totally unsecured for the support of password independence. Moreover, it does not offer the security feature of mutual authentication and suffer from the fake-server attack. In the scheme of Wang et al., the ID-based scheme was developed as dynamic, and thus it can be more secure and efficient than the scheme of Wang et al. The author of Khan et al. [5] projected out the practical difficulties of Wang et al., and so the scheme of Wang et al. is not suited for the real-time analysis.

Subsequently, the Khan et al. presented an extended version of authentication scheme to mitigate the computational complexities of smart card systems. Besides, the Khan et al. scheme offers some special provisional features, such as lost/stolen smart card revocation and expiry time-checkup for the authentication. But, the author of Chen et al. [6] showed off that the scheme of Khan et al. [5] does not provide the client-anonymity feature, and hence it is susceptible to the insider attack since all the legal systems share the common session key. So, the authors of Chen et al. proposed an efficient dynamic ID-based authentication scheme and it was validated under the system of TMIS. The scheme of Chen et al. was also provided a unique feature of client anonymity with un-traceability. To provide the distinguished feature, the authors of Chen et al. utilized the cipher block chaining (CBC) mode while the symmetric-encryption was applied in the TMIS system.

Later on, the authors of Kumari et al. [12] proved that the attacks, like password-guessing, user-key impersonation and denial-of-service (DoS) and key disclosure (session) are probable in the authentication scheme of Jiang et al. [8]. To resolve the issue of attack weaknesses, the authors of Kumari et al. developed an improved authentication scheme. The authors of Li and Hwang [13] presented an efficient authentication scheme and it relates to the biometric verification systems, smart card devices and hashing functions, but then the author of Das et al. [14] told that the scheme of Li and Hwang acquires several security flaws. To address the security flaws, the authors of Das et al. developed an extended authentication protocol version. Besides, the authors of Li et al. [15] pointed that the scheme of Das et al. does not provide the security reliably,and hence they proposed an improved authentication version over the Das et al. scheme's.

Table 1 Important notation and description

Notations	Description
MC_i	Multimedia client
MS_j	Multimedia server
H_{SS}	Home subscriber server
m_k	Master key
s_k	Session key
sip_{uri}	SIP uniform resource identifier
Re_{alm}	Network domain
$secret_{key}$	Secret key
x	Random number
P_i	Proxy server's identity
S_i	Serving server's identity
I_i	Interrogating server's identity
S_{ID_j}	Server's identity
C_{ID_i}	Client's identity
N_{once_i}	Identity of user
N_{once_j}	Identity of server
SIP	Session Initiation Protocol
CSCF	Call Session Control Function
PCSCF	Proxy Call Session Control Function
SCSCF	Serving Call Session Control Function
ICSCF	Interrogating Call Session Control Function

The authors of Chang et al. [16] incorporated the features of uniqueness and anonymity preservation for the healthcare connection systems through the remote-user authentication scheme. The scheme of Chang et al. uses the users/clients identities to authenticate the users' biometric system and it verifies its authentication using the Bio-hashing function. Besides, this scheme has one-way hashing and exclusive-or (X-OR) for the efficient usage, though in the recent authentication scheme of Das et al. [17], the authors of Das et al. projected several authentication weaknesses, such as flaws in design (logon, mutual authentication and password update) and privilege insider-attack for the scheme of Chang et al. Furthermore, the authors of Das et al. presented an authentication mechanism to resolve the design flaws of the scheme of Chang et al. Also, the authors of Das et al. validated their proposed scheme in the popular tool of AVISPA (Automated Validation of Internet Security Protocols and Applications) tool and the tool was used to ensure the security against the attacks, like active and passive.

In the recent study, the authors, like Younghwa An and Khurram et al. [22, 23] proposed the biometric-based authentication schemes to resolve the security flaws, such as client anonymity,un-traceability, masquerade attack, password guessing and insider attack, but they failed to evaluate the schemes in the real time system tools. Besides, the authors, like Younghwa An and Khurram et al. failed to mention about the nature of user entities, that is, whether static or dynamic. Importantly, the authors have not shown any real time experimental analysis of the safe and secure for the schemes. Thus, we aim to design a mechanism of dynamic-identity based multimedia server client authentication scheme to prevent various attacks and mitigate the computational and communication overheads. Then, We design, develop and integrate the proposed and some recent existing mechanisms, such as Younghwa An, Khurram et al., Das et al. and Chang et al. in the real time tele-care multimedia medical server client system (RTT-MMSCS) to cross-examine some conditional metrics of the systems, such as call setup time, bandwidth consumption and signal congestion. Table 1 illustrates the important notation and description.

The remaining sections are devised as follows. Section 2 demonstrates the real time testbed of tele-care multimedia medical server client systems. Section 3 presents the scheme of dynamic-identity based multimedia server client authentication scheme. Section 4 discusses the comparison and computation efficiencies of secure authentication schemes, namely Younghwa An, Khurram et al., Das et al., Chang et al. and proposed scheme. Section 5 shows the real time multimedia medical information system to probe the metrics, like call setup time, signal congestion and bandwidth consumption. Section 6 concludes the research work.

2 Related Works

Wu et al. [29] presented a two-factor mutual authentication scheme for the Telecare Medicine Information System (TMIS). Debiao et al. [30] determined that the scheme of Wu et al. cannot be resilient to the attacks, such as insider and key-impersonation. In addition, the authors of Debiao et al. improved the earlier version of two-factor authentication scheme using smart-card device. But, Wei et al. [31] found that the schemes, namely Wu et al. and Debiao et al. cannot prevent the attack of offline-password guessing, and thus the authors of Wei et al. presented an authentication scheme to overcome the pitfalls of [29, 30]. In 2012, Wu et al. [32] developed a novel two-factor authentication scheme for the integration of electronic-patient record systems; though the authors of Islam

and Biswas [33] analyzed and found that the scheme of Wu et al. cannot withstand for the attacks, namely offline-password guessing, lost-smartcard, privileged-insider and secret-leakage.

Moreover, the scheme of Wu et al. have not had any proviso for the attacks, like lost (revocation) of smartcard and users'-anonymity. The phase of the password update of Wu et al. cannot update the users' password until the server is permitted to do so. Therefore, it has more computation to be performed to execute the phase of password update. To mitigate the computation and communication overheads, the authors of Pu et al. [34] introduced a novel two-factor authentication scheme using elliptic-curve cryptography (ECC). On the other hand, the authors of Chen et al. [6] presented a dynamic ID-based authentication scheme for the system of TMIS.

In 2013, the authors of Jiang et al. [8] analyzed and found that the scheme of Chen et al. cannot offer a feature of user/client anonymity, and thus the authors of Jiang et al. presented an enhanced authentication scheme based on the symmetric cryptographic technique with mode of cipher-block chaining. But, the authors of Kumari et al. [12] proved that the scheme of Jiang et al. cannot be resilient to the attacks, such as password-guessing, key-impersonation and denial of service (DoS). Since the adversary can compromise the secret-key values which is shared between the users and server for the sake of connection

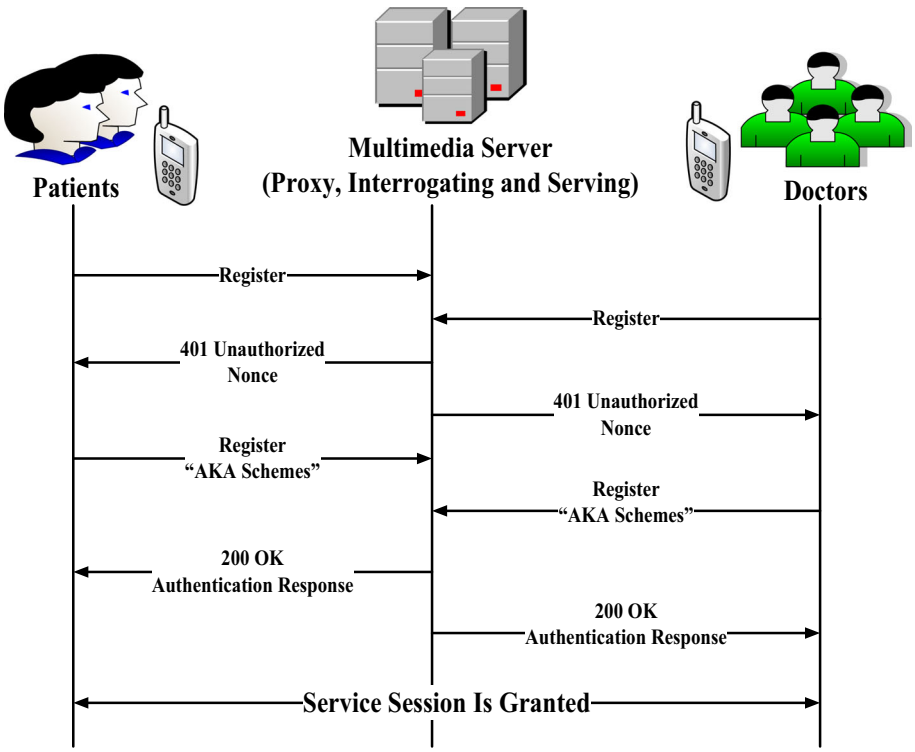

Fig. 1 Real time tele-care multimedia medical information systems

establishment sessions, the protocol scheme of Jiang et al. cannot achieve a true mutual authentication service.

3 Real Time Tele-Care Multimedia Medical Server Client System

Session Initiation Protocol (SIP) [24] is used as a standard signaling protocol for the management of multimedia server and client sessions. The key features are scalability and textual-based structure. The former feature provides a capability of new service integration to the developers, whereas the latter feature provides a suitability of service time sensitivity. Figure 1 demonstrates the real time tele-care multimedia medical information systems. The multimedia server [27] issues the pseudonyms to recognize the legitimate multimedia user [28]. It can be either SIP URI private identity or public identity. The identities namely public and private SIP URI are used to provide user identification and authentication. As and when the user wants the access of multimedia service, he/she should handshake with the proxy call session control function (PCSCF). It declares that he/she is an authorized user and also it makes his/her credential as public as on the networks.

After user credentials being available on the public networks, the interrogating call session control function (ICSCF) raises a query to the home subscriber server (HSS) and that provides an appropriate serving call session control function (SCSCF) to execute the rest of the user authentication procedure. Then, the PCSCF challenges the user devices with a SIP response of '401 Unauthorized Nonce' which includes some random numbers such as N_{once_i} and N_{once_j} for the user device authentication. Upon receiving the SIP challenge response, the user device sends its private identity along with the authentication scheme to the server component of SCSCF. If the user authentication is successful, then the multimedia server responses back with '200 OK'. We should note that the user devices send the authentication procedure as in the form of clear-text. So any snooper may tamper the user credentials to behave as a legitimate user and he/she may use such credentials to spoil the integrity of the server system.

Moreover, the snoopers may conjoin the user credentials with some other social networks to misuse the real identity of the server system. To stop such illegal activity, Dynamic-Identity Based Multimedia Server Client Authentication Scheme is proposed. It is designed and integrated in the form of 3GPP (Third Generation Partnership Project) [25, 26] in the real time multimedia medical information system. As like, to show the significances like call setup time, signal congestion and bandwidth consumption, the schemes such as Younghwa An [22], Khurram et al. [23], Das et al. [17] and Chang et al. [16] are integrated in the same real time multimedia medical information system. Since our proposed protocol is based on the random nonce strategy, it will definitely yield better results in comparison with the existing authentication schemes. The details of such results are elaborately discussed in Sect. 5.

4 Dynamic-Identity Based Multimedia Server Client Authentication Scheme

The proposed scheme of dynamic-identity based multimedia server client authentication scheme is composed of four phases: client registration phase, client login phase, server client verification phase and session key update phase. The phases involve three major entities, such as multimedia client (MC_i), multimedia server (MS_j) and home subscriber

server center (H_{SS}). H_{SS} selects the master-key m_k and session key s_k to determine $h(m_k \parallel s_k)$ and $h(s_k)$. Then, it shares them with MS_j over a secure channel. Only H_{SS} is aware of master-key m_k and secret key s_k.

4.1 Client registration phase

When any multimedia client (MC_i) wishes to access the (MS_j) system, then he/she has to enter credentials, such as sip_{uri}, Re_{alm} and $secret_{key}$ to H_{SS}. The steps of client registration phase are as follows:

Step 1: $MC_i \Rightarrow H_{SS} : sip_{uri}, H\left(x \oplus secret_{key}\right)$. MC_i may freely opt his/her credentials, such as sip_{uri} and $secret_{key}$ to determine $H\left(x \oplus secret_{key_i}\right)$, where x is a random integer given by MC_i. Later, MC_i sends sip_{uri} and $H\left(x \oplus secret_{key_i}\right)$ to the H_{SS} to register over a secure channel.

Step 2: Then, H_{ss} determines:

$$P_i = H(sip_{uri} \parallel m_k)$$

$$S_i = TS_i \oplus H\left(sip_{uri} \parallel H\left(x \oplus secret_{key_i}\right)\right)$$

$$I_i = H\left(H\left(x \oplus secret_{key_i}\right) \parallel H(m_k \parallel s_k)\right)$$

$$h_i = H(TS_i)$$

Step 3: $H_{SS} \Rightarrow MC_i$: H_{SS} runs the multimedia server MS_j components (proxy, serving and interrogating) and the server components comprises of $\{P_i, S_i, I_i, h_i, H(.), H(s_k)\}$.

Step 4: MC_i enters the credentials x into the multimedia system MS_j, then the multimedia server MS_j contains $\{P_i, S_i, I_i, h_i, x, H(.), H(s_k)\}$.

4.2 Client Login Phase

After execution of multimedia server MS_j components, the multimedia clients MC_i can log on to MS_j to access the services, like voice and data. The steps of multimedia client login are as follows:

Step 1: MC_i runs the application software on the Linux platform and then it enters the input credentials, such as $sip_{uri}$and $secret_{key}$ in the running application. After that, the multimedia server MS_j determines $P_i = S_i \oplus H\left(sip_{uri} \parallel H\left(x \oplus secret_{key_i}\right)\right)$ and $h_i^* = H(T_i)$ and then, MS_j verifies whether h_i^* is as same as h_i or not. If they are found as same, then MC_i continue to the next step. Otherwise, MS_j rejects the MC_i logon request.

Step 2: After the successful verification, MS_i starts to generate a nonce N_{once_i} and determines

$$F_i = H(P_i \parallel H(s_k) \parallel N_{once_i})$$

$$C_{ID_i} = H\left(x \oplus secret_{key_i}\right) \oplus H(P_i \parallel F_i \parallel N_{once_i})$$

$$G_{ij} = P_i \oplus H\left(H(s_k) \parallel N_{once_i} \parallel S_{ID_j}\right)$$

$$E_i = H(I_i \parallel F_i \parallel N_{once_i})$$

Step 3: $MC_i \rightarrow MS_j : C_{ID_i}, G_{ij}, E_i, N_{once_i}$

4.3 Server and Client Authentication Phase

When MS_j receives the MC_i logon request, MS_j executes the following steps to validate the client's logon request. The execution steps are as follows:

Step 1: After receiving the logon-request: $\{C_{ID_i}, G_{ij}, E_i, N_{once_i}\}$ MS_j determines $P_i = G_{ij} \oplus H\big(H(s_k) \parallel N_{once_i} \parallel S_{ID_j}\big)$, $F_i = H(P_i \parallel H(s_k) \parallel N_{once_i})$, $H\big(x \oplus secret_{key_i}\big) = C_{ID_i} \oplus H(P_i \parallel F_i \parallel N_{once_i})$ and $I_i = H\big(H\big(x \oplus secret_{key_i}\big) \parallel h(s_k \parallel m_k)\big)$ from the received logon-request message $C_{ID_i}, G_{ij}, N_{once_i}\}$, $H(s_k)$ and $h(s_k \parallel m_k)$.

Step 2: MS_j determines $H(I_i \parallel F_i \parallel N_{once_i})$ and then, it verifies it with E_i. If they are not equal, then MS_j rejects the client logon-request and terminate the session. Otherwise, MS_j accepts the client logon-request and determine a nonce N_{once_j} to compute $MS_{ij}^{'} = H\big(I_i \parallel N_{once_i} \parallel F_i \parallel S_{ID_j}\big)$. Lastly, MS_j sends the server-response message $\left\{MS_{ij}', N_{once_j}\right\}$ to the client MC_i.

Step 3: After receiving the server-response message $\left\{MS_{ij}^{'}, N_{once_j}\right\}$ from MS_j, MC_i determines $H\big(I_i \parallel N_{once_i} \parallel F_i \parallel S_{ID_j}\big)$ and then, it checks whether it is as same as the server-response message or not. If they are not same, then MC_i rejects the server-response message and terminate the session with the server MS_j. Otherwise, MC_i successfully authenticates the server MS_j and determines $MS_{ij}'' = H\big(I_i \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\big)$. Lastly, MC_i sends back the client-response message $\{MS_{ij}^{''}\}$ to MS_j.

Step 4: Upon receiving the client-response message $\{MS_{ij}^{''}\}$, MS_j determines $H\big(I_i \parallel N_{once_i} \parallel F_i \parallel S_{ID_j}\big)$ and verifies whether it is as same as the client-response message or not. If they are same, then MS_j successfully authenticates MC_i. After the completion of verification phase, MC_i and MS_j may compute a common session key $CS_{key} = H\big(I_i \parallel N_{once_i} \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\big)$ to secure the communication of multimedia server and client systems.

4.4 Session Key Update Phase

In this phase, MC_i may change his/her secret key as and when he/she desires the change. The steps of session key update are as follows:

Step 1: MC_i enters his/her credentials such as $sip_{uri}$and$secret_{key}$ into the multimedia system MS_j.

Step 2: MS_j determines $P_i = S_i \oplus H\big(sip_{uri} \parallel H\big(x \oplus secret_{key_i}\big)\big)$ and $h_i^* = H(P_i)$ and then, it verifies whether h_i^* is as same as h_i. If they are equal, then MC_i opts his/her new secret key $secret_{key_{new}}$ and random integer x_{new} to determine $H\big(x_{new} \parallel secret_{key_{new}}\big)$ and $S_{new} = P_i \oplus H\big(sip_{uri} \parallel H\big(x_{new} \parallel secret_{key_{new}}\big)\big)$. Lastly, MC_i and sip_{uri} and $H\big(x_{new} \parallel secret_{key_{new}}\big)$ to H_{SS} over a secure channel.

Step 3: H_{SS} determines $x_{new} = H\big(H\big(x_{new} \parallel secret_{key_{new}}\big) \parallel H(s_k \parallel m_k)\big)$. Then, H_{SS} sends back $\{x_{new}\}$ to MC_i.

Step 4: Lastly, the multimedia server MS_j modifies S_i and I_i with S_{New} and B_{New}.

5 Analysis of Proposed Scheme

In this section, we will discuss the safe and security of our dynamic-identity based authentication mechanism. We model our proposed protocol as a game as between the challenger $\mathfrak{C}$ and adversary $\mathfrak{A}$. The following activities are triggered to the Game-On. At first, the $\mathfrak{C}$ activates the client login phase. Followed by, the $\mathfrak{A}$ who is given of the system (public) parameters, and so has the access to the system oracle model. When we execute the authentication mechanism with the Oracle's authentication, the $\mathfrak{A}$ can raise a query in the form of a polynomial to probe the security parameter s_k. If the random number $y = 0$, then the MC_i randomly compute the session key to send forward to MS_j, whereas if $y = 1$, then it sends forward its own computed session key to MS_j. As like, $\mathfrak{A}$ continuously sends the queries to the oracle; but it does not reveal or corrupt the oracle testing.

Eventually, the output of $\mathfrak{A}$ may assume its guessing as y' for y, if the chances of correct guessing is negligible; then we can also assure that the scheme is safe and secure. The following algorithm will show that the $\mathfrak{A}$ can attack the authentication system of the proposed scheme.

Table 2 Security properties of multimedia authentication schemes

Security properties	Younghwa An [22]	Khurram et al. [23]	Das et al. [17]	Chang et al. [16]	Proposed protocol
Privacy preservation	No	No	No	No	Yes
Hash function collision	No	No	No	No	Yes
Withstand identity (id)-theft attack	No	No	No	No	Yes
Withstand replay attack	No	No	No	No	Yes
Problem of clock un-synchronization	No	No	No	No	Yes
Withstand server client anonymity	No	Yes	No	No	Yes
Withstand session key agreement	No	No	No	No	Yes
Withstand (perfect) forward secrecy	No	No	No	No	Yes
Withstand no-key compromise impersonation	Yes	Yes	No	No	Yes
Withstand no-unknown key-share	No	No	No	No	Yes
Withstand malicious server attack	Yes	No	No	No	Yes
Withstand stolen server component attack	No	No	No	No	Yes
Withstand verifier leakage attack	No	No	No	No	Yes
Withstand mutual authentication (server and client)	Yes	Yes	No	No	Yes
Withstand Denail of Service (dos) attack	No	No	No	No	Yes
Withstand man-in-the-middle attack	No	No	No	No	Yes
Withstand parallel-session attack	No	No	No	No	Yes
Delay transmission	No	No	No	No	Yes
Signal consumption	No	No	No	No	Yes

Algorithm 1
For an adversary $\mathfrak{A}$,

1. Run to execute the $Send(MC_i; MS_j)$ and $Send(MS_j; MC_i)$; and also raise a login query $Login(MC_i; MS_j)$ if it is necessary.
2. Run to $Verify\_Execution(MC_i; MS_j)$ to run the execution process of oracle testing

   Run to execute the $Query\_Test(MC_i)$.
3. Guess to find a bit of y, if y is correct, then the $\mathfrak{A}$ wins the game.

Theorem 1 *The proposed scheme can resist against the hash function collision*

Proof In the login phase, the adversary $\mathfrak{A}$ may trigger some queries, like $Send(MC_i; MS_j)$ and $Send(MS_j; MC_i)$ to infer some system parameters, like $\{P_i, S_i, I_i, h_i, x, H(.), H(s_k)\}$ and $\{P_i, S_i, I_i, h_i, x, H(.), H(s_k)\}$ from the modeling of oracle. Then, the $\mathfrak{A}$ initiates a verifier query $Verify\_Execution(MC_i; MS_j)$ and collects the following parameter information, such as $C_{ID_i} = H(x \oplus secret_{key_i}), P_i, F_i$ and N_{once_i} from the oracle modeling. Before execute a query testing, $\mathfrak{A}$ pre-generate the numerous polynomial queries. At last, $\mathfrak{A}$ executes the $Query\_Test(MC_i)$ to flip the query coin. If the query is coined as 1, then the oracle modeling exhibits a fresh x; otherwise it returns the random string which is equal to the length of y. Then, the $\mathfrak{A}$ should expel one bit to verify the answer with the $Query\_Test$. Since the proposed scheme is bound of secure hash-function $H(x \oplus secret_{key_i}) \oplus H(P_i \parallel F_i \parallel N_{once_i})$, the adversary can't infer the session key from the random generated strings. Thus, the chance of $\mathfrak{A}$'s successful is negligible. Besides, the Theorem 1 is proven. Table 2 summarizes the security properties of multimedia authentication schemes.

5.1 Identity (ID)-Theft Atack

In the phase of proposed server and client authentication, MC_i commonly transfers a value of client-variant ID as C_{ID_i} as to hide its original identity over an insecure communication channel. Since the client-variant ID is chosen randomly, it is certain that the proposed scheme can resist the identity (ID) theft attack and it can also keep the anonymity properties in safe. Younghwa An, Khurram et al., Das et al. and Chang et al.

5.2 Replay Attack and Problem of Clock Un-synchronization

As already mentioned in [20], the authentication mechanism which is based on the timestamp, may seriously suffer from the attack of replay;since the delay transmission is unpredictable in the networks. To avoid such drawback, we change the timestamp based scheme into the nonce based scheme. Thus, our proposed scheme can able to avoid the problem of clock un-synchronization. Besides, in the phase of server client authentication, the adversary $\mathfrak{A}$ may deduce the MC_i previous login-request, and then the $\mathfrak{A}$ may use that information as a new login-request to the MS_j; though in our scheme the C_{ID_i} value is not permitted to be used as session to session. Thus, the $\mathfrak{A}$ can't complete the process of verification at the server system with the legitimate value of previous login-request. Consequently, it is certain that our proposed can resist the replay attack.

5.3 Server Client Anonymity

In our proposed authentication scheme, client/server (MC_i/MS_j) preserves their login-request credentials confidentially; since our scheme shares the credentials of server/client by means of client identity (C_{ID_i})/server identity (S_{ID_i}). We compute the client anonymous identities from $C_{ID_i} = H\left(x \oplus secret_{key_i}\right) \oplus H(P_i \parallel F_i \parallel N_{once_i})$ and the server anonymous identities from $S_{ID_i} = TS_i \oplus H\left(sip_{uri} \parallel H\left(x \oplus secret_{key_i}\right)\right)$. These identities will keep changing for the every attempt of login-request; since the former and latter expressions are calculated from the random integer x. Later, the server and client systems retrieve their identities to share the session keys and to hide their identities during the login-request transmission. So that, we confidently assert that the identity of the client C_{ID_i} Can only be recovered from the server and vice versa. Thus, in the proposed scheme of authentication, no identities can be recovered by any of the adversaries/attackers/intruders.

5.4 Session Key Agreement

In the phase of key authentication, our proposed scheme can provide the session key $CS_{key} = H\left(I_i \parallel N_{once_i} \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\right)$ and it is shared mutually between the server MS_j and client MC_i systems. The value of F_i is determined by $F_i = H(P_i \parallel H(s_k) \parallel N_{once_i})$ and the parameter values, such as $N_{once_i}, N_{once_j}, S_{ID_j}$ are determined in sequence to find a reliable mutual authentication session key. Besides, the value CS_{key} will often change for every login-session, and thus the expired session keys can't be reused for the purpose of re-login. So that, we confidently assert that the anonymous users can't reuse the expired session to the request of re-login. Thus, the proposed scheme holds the property of session-key agreement as safe and secure.

5.5 (Perfect) Forward Secrecy

A protocol can be (perfect) forward secrecy, if the private keys of the participants/clients do not breach the previous session keys securities. It has two notions, such as perfect and master-key forward secrecies. The former secrecy does not harm the previous session-keys, whereas the latter secrecy can be satisfied as and when the master server-key is compromised. Our proposed protocol can be able to satisfy both the former and latter secrecies from the usage of $P_i = G_{ij} \oplus H\left(H(s_k) \parallel N_{once_i} \parallel S_{ID_j}\right)$ and $H\left(x \oplus secret_{key_i}\right) = C_{ID_i} \oplus H(P_i \parallel F_i \parallel N_{once_i})$ to share the common session keys. The adversary may determine the parameter such as s_k, though he/she can't determine the rest of the parameters, like G_{ij}, N_{once_i}, S_{ID_j}, $secret_{key_i}$ and F_i. Thus, the proposed protocol satisfies the secrecies, like perfect and master-key.

5.6 No-Key Compromise Impersonation

Since our proposed protocol often changes the common session key CS_{key} for every login-session request, we thus confidently assert that the adversaries can't infer server/client identities S_{ID_j}/C_{ID_i} neither. So, our proposed protocol holds the property of no-key compromise impersonation.

5.7 No-Unknown Key-Share

A protocol can be unknown key-share, if the adversaries can't be able to determine the secret-key of the client systems. Because the client's secret key can only be determined from the key generation center (KGC). To infer the client's secret key, the adversary should learn some hidden entities, such as $C_{ID_i}, G_{ij}, N_{once_i}, S_{ID_j}, secret_{key_i}$ and F_i. Otherwise, the adversary can't deduce any bit of details to crack the client's secret key. Thus, we assert that our proposed protocol has some hidden parameters of no-unknown key-share.

5.8 Malicious Server Attack

In the malicious server attack, the malicious server $MS_j^{'}$ behaves as a legitimate multimedia server MS_j to monitor and collect some information related to the multimedia client MC_i and it especially occurs during the client login-request process. In the process of client login-request, the malicious server can be able to infer only one parameter of the legitimate client that is s_k. But, it does not determine the values such as $C_{ID_i}, G_{ij}, N_{once_i}, S_{ID_j}, secret_{key_i}$ and F_i to forge the client. Thus, we assert that our proposed withstands for the malicious server attack.

5.9 Stolen Server Component Attack

In the stolen server component attack, the malicious user $MC_i^{'}$ tries to collect the information related to the server components of multimedia server MS_j if he/she steals the component details of multimedia servers. Our proposed protocol has the parameters like P_i, S_i and I_i for all the server components of multimedia server, and thus we confidently assert that the malicious user can't acquire any details of server components unless they exploits their related parameters. Since the server component parameters are closely related to each other, thus the malicious user can't steal their details easily. Hence, our proposed protocol withstands for the stolen server component attack.

5.10 Verifier Leakage Attack

In the verifier leakage attack, the malicious user $MC_i^{'}$ may forge the information related to the server components of multimedia, namely P_i, S_i and I_i in order to behave as a legitimate user. In our proposed protocol, the identities of users change often, and so the malicious user $MC_i^{'}$ can't tamper any details from the previous login-session. Moreover, the related parameters of the server component such as P_i, S_i and I_i can't be inferred to compute the secret session keys of multimedia server client systems. Hence, our proposed protocol withstands for the verifier leakage attack.

5.11 Mutual Authentication (Server and Client)

Our proposed protocol involves of two major entities, namely multimedia client MC_i and server MS_j that mutually authenticate each other before they agree upon a common session key. The common session $CS_{key} = H\left(I_i \parallel N_{once_i} \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\right)$ is derived from the parameters, namely N_{once_i}, N_{once_j} F_i, SID_j and I_i that is later used to authenticate the service sessions of multimedia server and client systems. The multimedia server and client systems validate their related entities from the parameters like C_{ID_i} and S_{ID_j} to authenticate the

request service session of multimedia client MC_i. Hence, we assert that our proposed protocol achieves the mutual authentication for the multimedia server client systems.

5.12 Denail of Service (DoS) attack

In the DoS attack, the malicious user $MC_i^{'}$ may impede the legitimate user from the login-request and it is done to update the password verification to some random values. But, in our proposed protocol even if the malicious client steals some important credentials of multimedia server, he/she is supposed to proceed the process of session key update before he/she starts changing the verification details. First and foremost, the malicious user should guess the prompt info such as P_i, S_i, I_i and x to compute its related expression like $P_i = G_{ij} \oplus H\big(H(s_k) \parallel N_{once_i} \parallel S_{ID_j}\big)$ and $H\big(x \oplus secret_{key_i}\big) = C_{ID_i} \oplus H(P_i \parallel F_i \parallel N_{once_i})$. Then, the expressions which are computer should undergo into the session key update phase to satisfy the verification details. It is practically not possible to speculate the parameters, namely P_i, S_i, I_i and x spontaneously. Hence, we assert that our proposed protocol withstands for the DoS attack.

5.13 Man-in-the-Middle Attack

In the man-in-the-middle attack, the malicious user $MC_i^{'}$ overhears on the communication channel and he/she also seizes the messages of server and client systems to send the messages back. In the seize of server and client communication, the malicious user may behave to the client as a legitimate user/server. In our proposed protocol, the malicious user may try to intercept the communication of multimedia server and client systems, but he/she can infer the common session key $CS_{key} = H\big(I_i \parallel N_{once_i} \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\big)$ since it relies on the N_{once_i}, N_{once_j}, F_i, SID_j and I_i which are chosen to be fresh or each service session. Hence, we assert that our proposed protocol withstands for the man-in-the-middle attack.

5.14 Parallel-Session Attack

In the parallel-session attack, the malicious user $MC_i^{'}$ may establish a parallel-session along with the legitimate multimedia user MC_i to listen, modify and resend the original messages to the legitimate multimedia server MS_j. The malicious activities such as listen, modify and resend are done within the stipulated duration of the frame window. In our proposed protocol, the malicious user $MC_i^{'}$ may try to masquerade as a legitimate multimedia user to resend the session login-request. But, he/she can't compute the common session key $CS_{key} = H\big(I_i \parallel N_{once_i} \parallel N_{once_j} \parallel F_i \parallel S_{ID_j}\big)$ since it is partially related to the random nonce values N_{once_i} and N_{once_j} which are always chosen to be a fresh for each login-session. Hence, we assert that our proposed protocol withstands for the parallel-session attack.

5.15 Comparative Efficiencies of Authentication Schemes

In the comparative efficiencies, we cross-analyze the proposed authentication scheme by means of its security properties and we examine such properties in one by one with the existing authentication schemes, namely Younghwa An, Khurram et al., Das et al. and Chang et al. Table 2 illustrates the comparative efficiencies of multimedia authentication schemes. We can observe from the Table 2 that our proposed authentication scheme is able to withstand with the most of the attacks, whereas the existing authentication schemes [16,

17, 22, 23] are not able to do such prevention as what the proposed scheme does so. Besides, our proposed scheme is able to offer privacy preservation for both server and client systems, whereas the existing schemes [16, 17, 22, 23] fail to do so.

In addition, the proposed and existing authentication schemes are evaluated using the real time Testbed For Tele-Care Multimedia Medical Information System and the examination results are revealed that the proposed authentication scheme can also mitigate the end-to-end delay, signal congestion and bandwidth consumption to offer a feature of scalability, whereas the existing authentication scheme [16, 17, 22, 23] can't be able to do as such mitigation. Table 3 depicts the compuation efficiencies of multimedia authentication schemes. As we can observe from the Table 3, the proposed scheme is almost carrying the hash function as double as comparing with the existing authentication scheme [16, 17, 22, 23]. To conceal the identities of the server and client systems on the networks, we additionally overload the hash functions, but it achieves the most important feature of privacy preservation.

6 Results and Discussion

To evaluate the major significances such as call setup time, signal congestion and bandwidth consumption of the proposed and existing authentication schemes, the OpenIMSCore server [27] and UCTIMS clients [28] have been utilized. On both the server and client sides, the authentication schemes, namely proposed and existing have been designed and implemented in the form of 3GPP standard. Besides, the server components, namely proxy, interrogating and serving have been modified to make the authentication schemes (proposed and existing) to use the message authentication header of the SIP. Figure 2 depicts the real time testbed for Tele-Care Multimedia Medical Information System. The systems like OpenIMSCore and UCTIMS have been installed in the high-end processor which is capable of Intel i3 core processor with 4 GB RAM and the systems are installed on Linux Mint (version 14) operating system.

For the users such as patient and doctor, we generate the random identities under the modulo inversion of chosen a random prime number. Besides, we monitor the call setup time of server client systems for every login-request over the normal wireless traffic. To provide an authentic login-request, we have collected and fed the private medical hospital information of doctors' and patients' in the database of multimedia (HSS). As for real time

Table 3 Compuation efficiencies of multimedia authentication schemes

Phases	Younghwa An [22]	Khurram et al. [23]	Das et al. [17]	Chang et al. [16]	Proposed protocol
Client registration phase	3 h(.)	4 h(.)	3 h(.)	3 h(.)	4 h(.)
Client login phase	2 h(.)	3 h(.)	2 h(.)	3 h(.)	4 h(.)
Server client authentication phase	5 h(.)	7 h(.)	8 h(.)	6 h(.)	10 h(.)
Session key update phase	Not defined	Not defined	Not defined	Not defined	6 h(.)
Total	8 h(.)	14 h(.)	13 h(.)	12 h(.)	24 h(.)

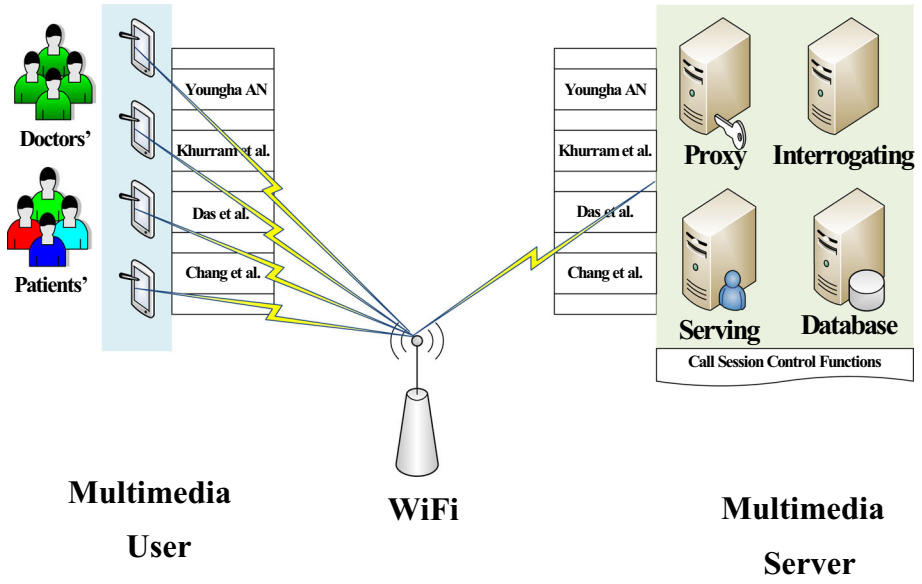

Fig. 2 Real Time testbed for tele-care multimedia medical information system

practice, the laptops (100 Nos') of which we have issued, are installed UCTIMS client and also configured of patients'/doctors' info. To cross-examine the call setup time, the proposed and existing authentication schemes are implemented. The schemes, such as proposed and existing will be authenticated as and when the multimedia server and client are sought for the service connection establishment.

In order to cross-examine the proposed and existing authentication schemes, we execute the authentication schemes, namely Younghwa An, Khurram et al., Das et al. and Chang et al. in parallel between the multimedia server client systems. In the cross-analysis, we have examined the authentication scheme as Server-Client with Youngwa An, Khurram et al., Das et al. Chang et al. and proposed protocol. To realize as a real time processing system, we have utilized the real time components (such as proxy, serving and interrogating) as the integral components of multimedia server.

To conceal the users identity in the public network domain, we have done some important changes in the message header format. The changes are:

1. 'Header': represents that the users are intended to hide the private info and the server components, such as proxy and the home subscriber server are responsible to hide such intentional infos' of users.
2. 'Session': The keys which are generated by the authentication schemes are to be used by the users to hide his/her private infos' included in the Session Description Protocol (SDP) over the public network domain.
3. 'Users': It sends the login-request in which it represents that the network should provide the privacy service since it is incompetent to provide such feature.
4. 'None': Server provides the privacy service to the users, other than that, none of the service like privacy will be appended to the users' message.
5. 'Critical': It represents for the critical situation of privacy function. As if such situation is arisen, then the service will automatically reject the users' service to ensure a feature

of privacy preservation. Besides, it re-run the proxy server to resolve the critical error of the multimedia server.

Though this mechanism is susceptible for the bid-down attack, thus the adversary may be able to strip out the message without the desirable feature of privacy protection. Besides, it does not conceal the private identity in the first hop and thus, it can't conceal the identity of an authentic user in the authorization header. Hence, the server and client systems are required for re-authentication. To strengthen the end-to-end communication, the authentication schemes (proposed and existing) of multimedia client and server systems are configured with a security layer of IPSec (Internet Protocol Security).

We utilize 100 users to establish the voice call connection over a single network domain. We interface the multimedia client and server in the wireless access router of 802.11 g and then we initiate the voice call connections between the multimedia clients over a campus wifi network domain. Before the service establishment, we evaluate the authentication schemes to ensure the privacy preservation. To prove the major significances of the proposed protocol, we cross-examine the metrics, like call setup time, signal congestion and bandwidth consumption with the other authentication schemes such as Younghwa An, Khurram et al., Das et al. and Chang et al. for a day. The cross-examination results of which we describe below are the cumulative result of one day.

The multimedia server has been executed in one day in which all the hundred client systems have initiated the service of voice call connection through the exchange of authentication schemes. Figure 3 illustrates Call Setup Time. The inspection results reveal that the proposed protocol is often mitigated the delay transmission at around 0.223 s and thus, it infers minimum delay, whereas the authentication schemes, such as Younghwa An, Khurram et al., Das et al. and Chang et al. are able to stabilize the delay transmission (at around 0.348, 0.341, −.37 and 0.363 s), but then it has higher call setup time in relation to the proposed protocol.

Our proposed protocol conceals the parameter like private key (CID_i/SID_i from the anonymous user so as to avoid the re-authentication when the user experiences timeout. Besides, our proposed curtails the pairing computational time of the multimedia server client systems. This curtailing of computational time stabilizes the message transmission of

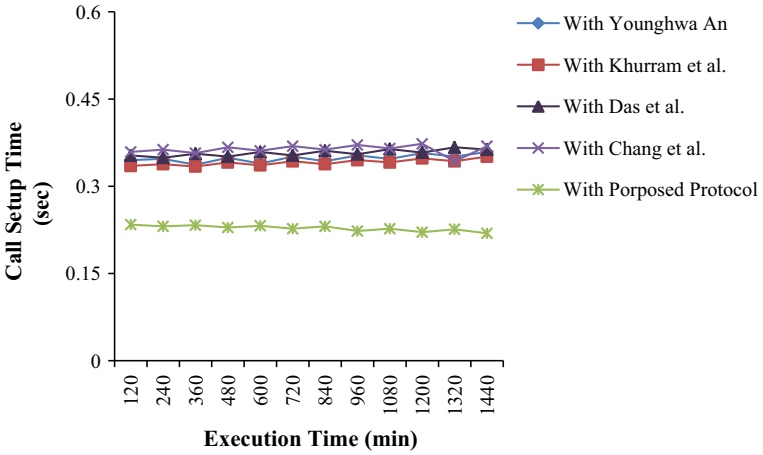

Fig. 3 Call setup time

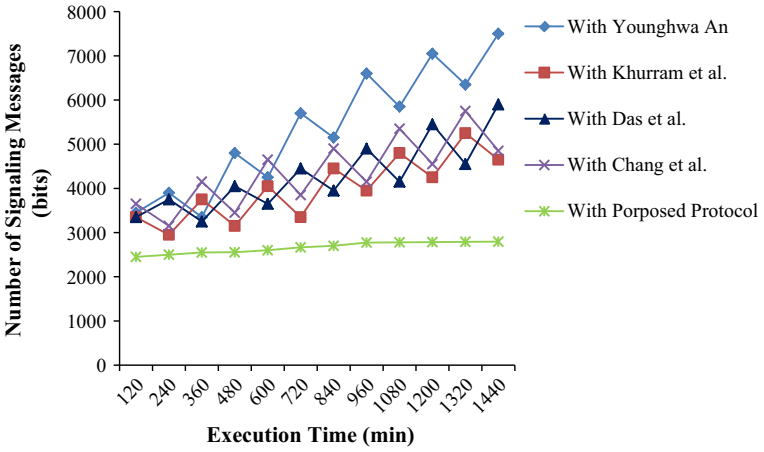

Fig. 4 Signal congestion

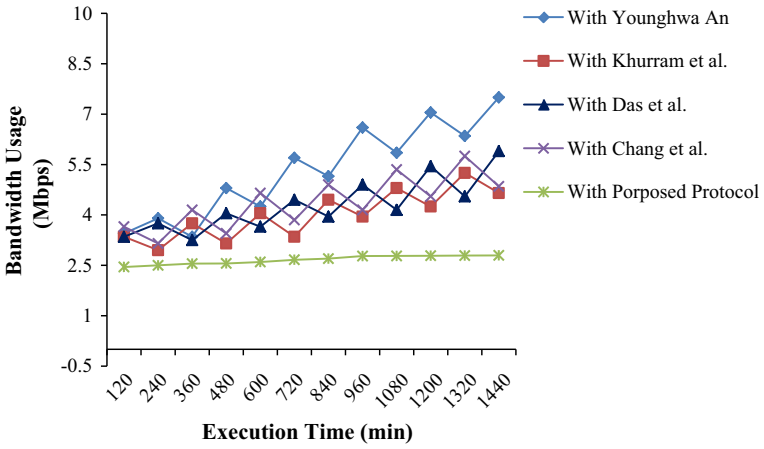

Fig. 5 Bandwidth consumption

the proposed protocol. Hence the computational time of the proposed authentication minimizes the traffic congestion of the multimedia server client systems. Figure 4 illustrates signal congestion. The proposed protocol has much less signal congestion in comparison with the other existing schemes, namely Younghwa An, Khurram et al., Das et al. and Chang et al.

The network capacity is specially classified into two key issues. KeyIssue1 divulges the bandwidth requirement of each user. KeyIssue2 divulges the rate of bandwidth usage. Figure 5 illustrates the bandwidth consumption. To analyze the bandwidth, this research chooses the voice call. To inspect the bandwidth usage, the usage rate is set as $\sim$10 Mbps for the wifi access point. The inspection result is shown that the proposed authentication mechanism has minimize the bandwidth usage, and thus it can be able to offer the feature of service scalability, whereas the other authentication mechanism, such as Younghwa An,

Khurram et al., Das et al. and Chang et al. have arbitrary usage of bandwidth, and so they can't offer the service reliability and scalability as well.

7 Conclusion

This paper proves that the authentication schemes such as Younghwa An, Khurram et al., Das et al. and Chang et al. are susceptible to several major security threats. We prove that the schemes of [16, 17, 22, 23] fails to resist the attacks, like stolen server component attack, mutual authentication, server client anonymity, parallel session and identity theft, verifier leakage, session key agreement and hash function collision. Besides, we also find that the existing schemes [16, 17, 22, 23] fails to offer the significant services, like privacy preservation, Problem of Clock Un-synchronization and service scalability. Thus, we have proposed a reliable dynamic-identity based multimedia server client authentication scheme so as to resolve those major security threats. Moreover, a testbed of multimedia medical information system has been designed and developed to investigate the metrics, such as call setup time, signal congestion and bandwidth consumption as in real time practice. The cross-examination results proves that the proposed authentication scheme is able to mitigate delay transmission, signal congestion and bandwidth consumption notably in comparison with the other authentication schemes [16, 17, 22, 23]. Also, our authentication scheme abides all the security features of 3GPP to achieve the security goals of multimedia medical information system.

Acknowledgments The corresponding author would like to thank SASTRA University and Tata Consultancy Services (TCS) for the financial assistance under the scheme of Research Scholar Program (RSP).

Conflict of interest All the authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Lambrinoudakis, C., & Gritzalis, S. (2000). Managing medical and insurance information through a smart-card-based information system. *Journal of Medical Systems, 24*(4), 213–234.
2. Das, M. L., Saxena, A., & Gulati, V. P. (2004). A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics, 50*(2), 629–631.
3. Wang, Y. Y., Kiu, J. Y., Xiao, F. X., & Dan, J. (2009). A more scheme, secure dynamic ID-based remote user authentication. *Computer Communications, 32*(4), 583–585.
4. Tsai, J.-L., Wu, T.-C., & Tsai, K.-Y. (2010). New dynamic ID authentication scheme using smart cards. *International Journal of Communication Systems, 23*, 1449–1462.
5. Khan, M. K., Kim, S. K., & Alghathbar, K. (2010). Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme. *Computer Communications, 34*(3), 305–309.
6. Chen, H. M., Lo, J. W., & Yeh, C. K. (2012). An efficient secure dynamic id-based authentication scheme for telecare medical information systems. *Journal of Medical Systems, 36*(6), 3907–3915.
7. Ma, C.-G., Wang, D., & Zhao, S.-D. (2012). Security flaws in two improved remote user authentication schemes using smart cards. *International Journal of Communication Systems,*. doi:10.1002/dac.2468.
8. Jiang, Q., Ma, J., Ma, Z., & Li, G. (2013). A privacy enhanced authentication scheme for telecare medical information systems. *Journal of Medical Systems,*. doi:10.1007/s10916-012-9897-0.
9. Kumari, S., & Khan, M. K. (2013). Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems,*. doi:10.1002/dac.2590.

10. Jiang, Q., Ma, J., Li, G., & Li, X. (2013). Improvement of robust smart-card-based password authentication scheme. *International of Communication Systems,*. doi:10.1002/dac.2644.
11. Li, X., Niu, J., Liao, J., & Liang, W. (2013). Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. *International Journal of Communication Systems,*. doi:10.1002/dac.2676.
12. Kumari, S., Khan, M. K., & Kumar, R. (2013). Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems. *Journal of Medical Systems,*. doi:10.1007/s10916-013-9952-5.
13. Li, C. T., & Hwang, M. S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications, 33*(1), 1–5.
14. Das, A. K. (2011). Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Information Security, 5*(3), 145–151.
15. Li, X., Niu, J.-W., Ma, J., Wang, W.-D., & Liu, C.-L. (2011). Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications, 34*(1), 73–79.
16. Chang, Y.-F., Yu, S.-H., & Shiao, D.-R. (2013). An uniqueness-and -anonymity-preserving remote user authentication scheme for connected health care. *Journal of Medical Systems,*. doi:10.1007/s10916-012-9902-7.
17. Das, A. K., & Goswami, A. (2013). A secure efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *Journal of Medical Systems,*. doi:10.1007/s10916-013-9948-1.
18. Islam, S., & Biswas, G. (2011). A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. *Journal of Systems and Software, 84*(11), 1892–1898. doi:10.1016/j.jss.2011.06.061.
19. Bellare, M., Pointcheval, D., & Rogaway, P. (2000). Authenticated key exchange secure against dictionary attacks. In: Advances in Cryptograhy-EUROCRYPT 2000, Lecture Notes in Computer Science. Berlin: Springer. doi:10.1007/3-540-45539-6_11.
20. Katz, J., & Yung, M. (2007). Scalable protocols for authenticated group key exchange. *Journal of Cryptology, 20*(1), 85–113. doi:10.1007/s00145-006-0361-5.
21. Tseng, Y. (2007). A communication-efficient and fault-tolerant conference-key agreement protocol with forward secrecy. *Journal of Systems and Software, 80*(7), 1091–1101. doi:10.1016/j.jss.2006.10.053.
22. Younghwa An. (2012). Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. *Journal of Biomedicine and Biotechnology*, Article ID 519723, 6 pages. doi:10.1155/2012/519723.
23. Khan, M. K., & Kumari, S. (2013). An improved biometrics-based remote user authentication scheme with user anonymity. *BioMed Research International*, Article ID 491289, 9 pages. doi:10.1155/2013/491289.
24. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., & Sparks, R. (2002). SIP: Session initiation protocol, IETF: RFC 3261.
25. GPP. 2011. TS 23.228: IP Multimedia Subsystems (IMS), third generation partnership project, technical specification group services and system aspects.
26. GPP. 2010. TS 33.203: 3G security; access security for IP-based services (release 10), third generation partnership project, technical specification group services and system aspects.
27. Fraunhofer FOKUS;OpenIMSCore; www.openimscore.org.
28. BerliOS; UCTIMS Client; www.uctimsclient.berlios.de.
29. Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C., & Chung, Y. (2010). A secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems, 36*(3), 1529–1535.
30. He, D., Chen, J., & Zhang, R. (2012). A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems, 36*(3), 1989–1995.
31. Wei, J., Hu, X., & Liu, W. (2012). An improved authentication scheme for telecare medicine information systems. *Journal of Medical Systems, 36*(6), 3597–3604.
32. Wu, Z.-Y., Chung, Y., Lai, F., & Chen, T.-S. (2012). A password-based user authentication scheme for the integrated EPR information system. *Journal of Medical Systems, 36*(2), 631–638.
33. Islam, S. H., & Biswas, G. P. (2015). Cryptanalysis and improvement of a password-based user authentication scheme for integrated EPR information system. *Journal of King Saud University Computer and Information Sciences, 27*(2), 211–221.
34. Pu, Q., Wang, J., & Zhao, R. (2012). Strong authentication scheme for telecare medicine information systems. *Journal of Medical Systems, 36*(4), 2609–2619.

Deebak Bakkiam David obtained the degree of B.Tech (Information Technology) at Anna University, Chennai, India in 2007. He obtained the degree of M.E. (Embedded System and Computing) at RTM Nagpur University, Nagpur, INDIA in 2009. Since July 2011, he has been pursuing the degree of Ph.D. (Wireless Multimedia Communication Networking) at SASTRA University, Thanjavur, INDIA. He has had 6 months of experience in industry sector and 2.5 years of experience in academic sector. He worked as Lecturer for 1.8 years at KITS-RANTEK, India and then he worked as Assistant Professor for 1 year at Sundharsan Engineering College, Pudukottai, INDIA. He has so far had 7 International Journals papers and 6 International Conferences papers. He is an active member of IE. His research interest includes Computer Networks, Wireless Networks and Network Security, Multimedia Communication and Protocols.

Muthaiah Rajappa obtained the degree of B.E. (Electronic and Instrumentation) at Annamalai University, Chidambaram, India in 1989. He obtained the degree of M.E. (Power Electronics and Industrial Drives) at Bharathidasan University, Thiruchupalli, INDIA in 1996. And then, he obtained the degree Ph.D. (Digital Image Compression) at SASTRA University, Thanjavur, INDIA in 2009. He has had 3 years of experience in industry sector and 21 years of experience in academic sector. He worked as Lecturer for 12 years and Associate Professor for 2 years at SASTRA University, Thanjavur, INDIA. Since April 2013, he has been working as Professor at the same University. He has so far had 28 International Journals papers and 5 International Conferences papers. He is being a member of IE and AECE. His research interest includes Image Processing, VLSI and Speech Recognition.

Thenmozhi Karuppusamy obtained Ph.D. degree from SASTRA University in 2008. Currently, he is working as Associate Dean in School of Electrical and Electronics Engineering at SASTRA University. Her research interest includes Networking and Wireless Communication.

Swaminathan Pitchai Iyer obtained Doctorate Degree in Electronics and Communication Engineering. Currently, he is working as Dean in School of Computing at SASTRA University. His research interest includes Embedded Systems, Software Engineering and Expert Systems.