International Journal of Engineering & Technology, 7 (4.6) (2018) 332-338

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cryptanalysis of Critical Security Mechanism designed for Hierarchical Multi-medical Server in TMIS Environment

Dr. B Rama Subba Reddy[1]*, A V L N SUJITH[2]

[1] Professor and HOD in CSE, SV College of Engineering for Women, Tirupati
[2] Assistant Professor in CSE, SV college of Engineering, Tirupathi
**Corresponding author E-mail: rsreddyphd@gmail.com*

Abstract

The rapid advancement of pervasive computing, nano-technology and wearable systems, given rise to low-power internet based systems in elimination of distance complications by application of 'The telecare medicine information system (TMIS)', which consists of sensor, medical server and physician servers to sense human biological readings and monitor the health condition of the patients. Due to the association of patient crucial data, and transferring it over an insecure and public communication channel, there is a critical prerequisite for patient authentication, data integrity and data privacy. In this context many researchers had proposed various schemes for user authentication and secure data transmission over TMIS. Recently A.K.Das et al proposed a three-factor user authentication and key agreement protocol for TMIS and claimed that the proposed protocol is efficient, secure and lightweight. We review their scheme for resistance to well-known cryptographic attacks. Though A.K.Das et al scheme resists major cryptographic attacks, after in-depth analysis, we demonstrate that their scheme has security pitfalls such as failure to resist replay attack, known session-specific temporary information attack,and failure to resist stolen-verifier attack.

Keywords: *Telecare medicine information systems, Authentication, Biometrics, Smart cards, Healthcare, Privacy, Key agreement, Multi-medical servers*

1. Introduction

The rapid advancement of networking, Radio frequency identification (RFID)and communication technologies resulted in an evolution of mobile health-care paradigm in which low-power sensors fixed on human body accrue both physical and body movement related data and communicate over networked systems i.e. Telecare Medicine Information Systems (TMIS) or Wireless medical sensor networks (WMSNs)' or Wireless body area network (WBANs) [1,2,3,4-10,20-21]. In TMIS, the patients can access health related information remotely. It also provides a platform of interaction between the patients at home and medical professionals at clinic center via public channel. Adopting TMIS for medical applications has been receiving a lot of attention in recent years due to their essential advantages over wired BANs such as reduced administrative cost, immediate quality of health care, precise record keeping, effective continuation and preventive care, and improve the comfort of the patients etc. [2,11-30].

In TMIS, irrespective of the patient's and medical professional location, the implanted sensors are scattered over a patient body and each of the distributed sensor nodes has the competence to collect patient's critical information like heart beat rate, sugar glucose level, blood pressure, respiration rate and electrocardiogram etc. [3,18] which are used for checking patient health condition as well as a patient can direct these health records to intermingle with doctors virtually and also use diverse health care related services without going anywhere and transfer these patient specific data via other sensor nodes to the base station or GateWayNode (GWN)through a multi-hop wireless communication. The doctor or laboratory etc. can login into to WMSN using any of wireless transmission devices like bluetooth, Wi-Fi etc. which uses radio waves for communication.

However, in TMIS, as the patient physiological information are transferred via radiowaves in an open public environment i.e. internet, the attacker may eavesdrop, delete, modify, rerouted the medical data from the public channel. This may result in serious privacy and security issues such as user impersonation attack, the medical server spoofing attack and modifying the exchanged sensitive patient medical information, which can be very costly for both patient and healthcare professional [1,2,11-14,18-21].

Consequently, the patient substantiation in addition to privacy is accordingly maintained in the TMIS. Patient anonymity is one of the vital requirement of TMIS since the patient might suffer with few isolated diseases that includes leprosy, HIV, etc. [1,2,313,15,19,20,17]. Therefore, an critical authentication scheme is desirable for TMIS, so as to use medical services securely and certainly by the legal users

TMIS Framework and its benefits in healthcare Services:

The framework of the TMIS is represented in Fig. 1. It includes four communicating entities that are involved in the user authentication protocol make use of TMIS as illustrated as follows:

1. Patient / User: The person who is a registered user and who is under the real-time observance of medical professional by means of distributed medical sensors (MS) for treatment.

2. Medical professionals: Doctors, nurses and lab professional who are thoroughly monitoring and observing into patient's information through TMIS.

3. MRS: A gate way node which is a resource heavy master node that takes the responsibility of the registering authority (for user, MS, PS) as well as acts as an interface between the medical server and the user.
4. MS: Medical server is the control authority of physical servers. The PSk enables services scheduled on demand to the endorsed users/patients Pi all the way through a medical server MSj.

2. Literature Survey

This section summarizes few authentication mechanisms were proposed to secure health care sensor networks. Over the past few years, several researchers [1-31] had proposed authentication schemes to build up the security and data integrity of Telecare medicine information systems.
In turn to devise an authentication protocol, the researchers employ several methods like ECC-RSA cryptosystem[3,6,12], cryptographic one-way hash function[1], Chaotic maps[2], and light weight cryptographic operations like XOR, concatenate[12] etc.
In 2012, Wu et al. [1] proposed an authentication scheme for TMIS built on complexity of solving the Discrete Logarithm Problem (DLP) and claimed that their TMIS scheme resistances all the key cryptographic attacks. However, He et al [8] on complete analysis, cryptanalyzed Wu etal [1] scheme and discovered that Wu et al scheme fails to accomplish user anonymity. In adding to that, He et al. [8] validated that Wu et al.'s scheme [1] is vulnerable to user impersonation attack, privileged insider attacks.Lee et al.[9] proposed a chaotic mapsbased authentication and key agreement scheme for TMIS, in which the session key is based on chaotic maps. Recently, Jiang et al [10]proposed a chaotic map based remote user authentication scheme for TMIS. Their scheme has the merits of low cost and session key agreement using Chaos theory. Mishra et al [11] analyzed Jiang et al [10] scheme and shown that their scheme is insecure against denial of service attack, and has security flaws in password change phase.
In order to facilitate multi medical server access with single registration, Amin et al [12] proposed a novel multi-medical servers architecture and secure user authentication with key agreement protocol for TMIS. Amin et al [12]scheme facilitates secure user authentication and key agreement protocol for accessing multiple physicians through physician servers. Recently, Ravanbakhsh et al [14], demonstrated that Amin et al [12] scheme is vulnerable to replay attack, privileged-insider attack, session key disclosure attack, fails to provide patient intractability and backward secrecy and proposed an efficient remote mutual authentication scheme on ECC and Fuzzy Extractor. Li et al [17]proposed an (a,k)-anonymity model based privacy protection scheme for data collection through IoT devices attached to patient body, and devised a novel anonymity aware privacy-preserving data collection (PPDC) method for healthcare services. On client-side, Li et al [17] utilize (a,k)-anonymity notion in order to produce anonymous tuples which can stand firm from possible attacks on server-side. Furthermore, they make use of the communication technology to reduce communication cost.
Recently, Amin et al [3] proposed a smart card based security protocol for TMIS system using the cryptographic one-way hash function and bio hashing function, and claimed that their scheme is resistant to major cryptographic attacks. Later, A.K.Das et al[5]proven that Amin et al [3] scheme suffers from various security pitfalls such as (1) failure to resists privileged-insider attack, (2) failure to resist strong replay attack, (3) failure to resists strong man-in-the-middle attack etc. Having shown the pitfalls in Amin et al [3]scheme, to strengthen the security pitfalls, A.K.Das et al [5], devised a robust user authentication mechanism for hierarchical multi-medical server framework in TMIS with key agreement scheme. A.K.Das et al [3] claimed that their authentication scheme resists eaves-dropping, unauthorized use of handheld devices by health professionals and restricts the unauthorized access to the patient's health care privacy data and furthermore it resists all major cryptographic attacks.

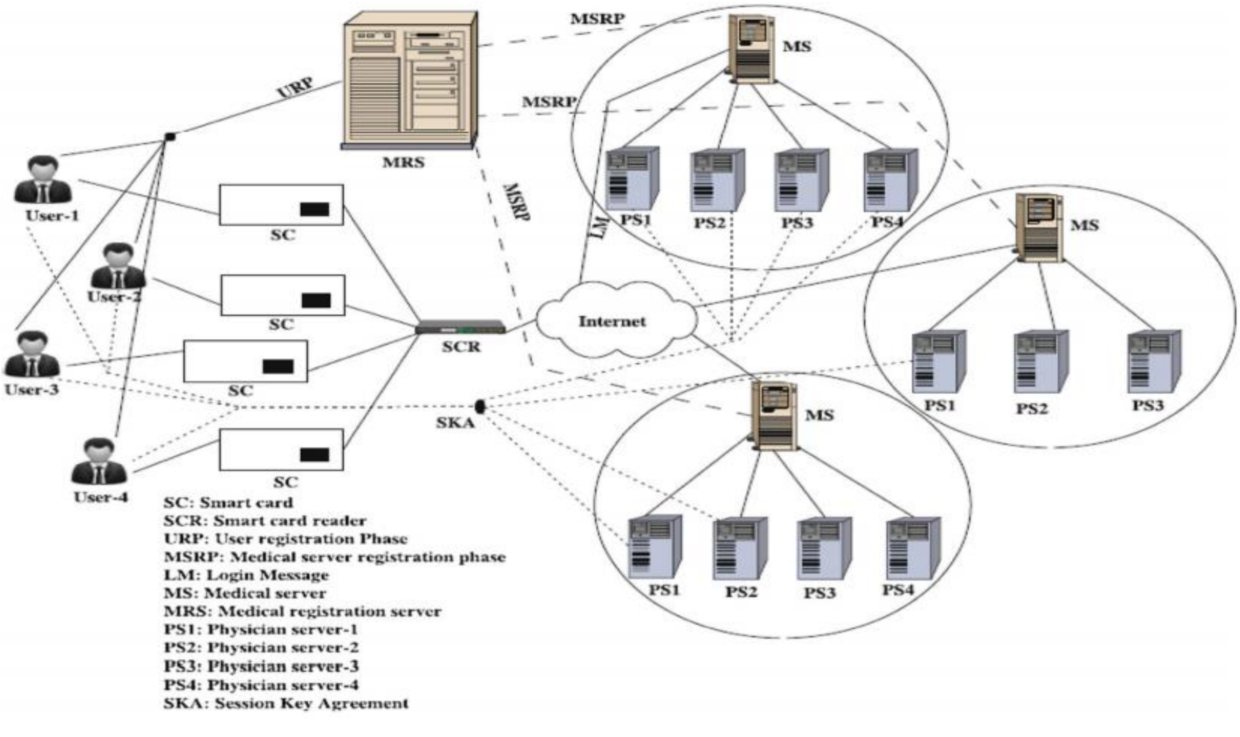

Fig. 1. Framework to access Hierarchical multi-medical server considered in Amin et al scheme (Source: [1])

3. Our Contribution

The contribution of the paper is twofold. Firstly, it consists of a brief discussion on A.K.Das et al [3]Hierarchical Multi-medical Server based on authentication mechanism for TMIS. Secondly, we show that A.K.Das et al [3] scheme is susceptible to following attacks. (1) Stolen-verifier attack leading to framing of session key and login request message by an attacker. (2) Replay attack (3) Known session-specific temporary information attack leading to medical server bye pass attack, and fails to preserve patient identity.

The roadmap of this paper is drafted as follows. In Section IV, presents a brief discussion on the A.K.Das et al scheme [3]. Furthermore, it is proved that A.K.Das et al.'s scheme is unsecuered against four malicious attacks specified in Section V. Finally, the conclusion of paper is included in Section VII.

4. Review of A.K. Das et al.'s Scheme

In this section, we describe the various phases of A.K.Das et al [3] mechanism, that are (i) registration phase of medical server, (ii) registration phase for user, (iii) login phase, (iv) authentication and session key agreement phase. The notations used ate providedin Table 1.

Table 1: Notations and their meanings

Symbol	*Description*
Pi	i^{th} user/patient
MRS	Medical registration server
MSj	j^{th} medical server $(1 \le j \le m)$
PSk	k^{th} physician server $(1 \le k \le p)$
PPIDi	Identity of Pi
PPWi	Password of Pi
MSIDj	MSj Identity
PBi	Pi is the personal biometric information
KMRS	Privacy key for MRS
PSIDk	PSk Identity
KMSj	Privacy key for MSj
KPMjk	Shared secret key in between PSk and MSj
RPi	Pi based Random nonce
KPMjk	Shared secret key in between PSk and MSj
RMSj	MSj based Random nonce
RPSk	PSk based Random nonce
TMSj	Recent time-stamp produced by MSj
TPSk	Recent time-stamp produced by PSk
Δt	utmost transmission delay,
TPi	Recent time-stamp produced by Pi
H (·)	Bio-hashing function [27, 35]
h(·)	Collision-less single-way hash function
Rep(·)	Fuzzy based reproduction algorithm
Gen(·)	Fuzzy based generation algorithm
τi	Biometric parameter of Pi
σi	Biometric key of Pi
$P \oplus Q$	Bitwise XOR of data P with data Q
εt	Error tolerance threshold
P||Q	Data P concatenates with data Q

The proposed scheme consists of six phases: (i) pre deployment phase, (ii) registration phase, (iii) login phase,(iv) key agreement and authentication phase, (v) password modification phase (vi) dynamic node addition phase.

Medical Server Registration Phase:

Let us assume that 'ms' denotes the count of medical servers MSj, $(1 \le j \le ms)$ that are to be installed initially within the network. We further assume that ms* additional number of medical servers MSj,$(ms + 1 \le j \le ms + ms^*)$ may be further added in the network, where ms*<< ms. For instance, initially ms = 200 medical servers that may be installed and in a while we may include ms* = 20 additional medical servers after initial employment in the network, based on the demand and the need of health care services depending on the additional users accessibility ratio. In this context, a medical server MSj, $(1 \le j \le ms)$, was initiated to enable the medical services to the remotly located patients, where they need to go for a unique identity MSIDj as well as send it to the MRS. MRS calculate the secret key Xj = h(MSIDj||KMRS) after analysing MSIDj, where KMRS is devised as 1024-bit secret key for the MRS in the context of security reasons, and revert it back to MSj through a secure channel. Thus, every MSj keeps (MSIDj, Xj). For ms^* additional medical servers MSp, $(ms + 1 \le p \le ms + ms^*)$, the MRS itself select a distinctive identity MSIDj in addition it also calculate the privacy key Xq = h(MSIDj||KMRS). The computed (MSIDj, Xq) are set aside to the MRS further it will be used afterwards during the user registration phase along with dynamic medical server enumeration phase.

User Registration Phase

Initially within this phase, a legal patient Pi have to register with the MRS to access the health care services from the selected physician server PSk under a medical server MSj within the network.

Steps in the User registration phase are enumerated as follows :

Step R1: Pi initially inputs his/her preferred identity PPIDi, password PPWi, as well as trace the personal biometrics PBi at the sensor of a specific device. Further Pi produces a 1024-bit random number K, which is maintained confidentially to Pi only. Pi subsequently apply the fuzzy extractor based generation function Gen(·) on the input PBi consecutively to generate the biometric based data key σi along with the public parameter τi as Gen(Bi) = (σi, τi). Note that σi id maintained confidentially with respect to Pi only.

Step R2: Pi computes the pseudo-random password PRPWi as PRPWi = h(PPIDi||K||PPWi) and sends the registration request {PPIDi, PRPWi} to the MRS via a privacy channel.

Step R3: After accepting the enrollment ask for from Pi,the MRS keeps on processing RMj = h(PIDi||Xj) $\oplus$PRPWi and RMSj = h(MSIDj ||Xj) $\oplus$PRPWi, for $1 \le j \le ms + ms^*$. At that point the MRS stores the information{{MSIDj , RMj , RMSj|$1 \le j \le m + ms^*$},h(•), Gen(•), Rep(•), t} in a brilliant card, say SCPi andsends it to the patient/client Pi by means of a safe channel, where 'εt' is theerror resistance limit utilized as a part of fluffy extractor.

Step R4: After accepting the savvy card SCi from theMRS, the client Pi registers ei = h(PPIDi||σi) $\oplus$ K andfi = h(PPIDi||PRPWi||σi). Pi at that point stores ei and fi in thesmart card SCPi. At long last, take note of that the brilliant card SCPicontains the data {MSIDj , RMj , RMSj|$1 \le j \le m + m^*$}, ei, fi, h(•), Gen(•), Rep(•), τi,and 'εt'.

Login stage:

In this stage, a lawful client Pi can get to any restorative server MSj for the medicinal administrations from a doctor server PSk under that therapeutic server MSj at whenever from anywhere through his/her issued savvy card PSCi. This stage contains the following advances:

Step L1:Pi first installs his/her astute card PSCi into a smart card per user of a specific terminal, and after that inputs his/her character PPIDi, watchword PPWi, and moreover imprints the singular biometrics PBi at the sensor Step L2: SCi then computesσi* = Rep(Bi, τi),K∗ = h(PPIDi||σi*) ⊕ ei,PRPWi* = h(PPIDi||K∗||PPWi),fi* = h(PPIDi||PRPWi∗ ||σi*).SCi additionally checks the confirmation condition fi*= fi.If it holds, it guarantees that the client Pi passes successfully both secret word and biometric check. Something else, this phase is ended instantly.

Step L3: SCPi further continues to create a random nonce RPi and the present time-stamp TPi. Then SCPi computesM1 = RMj ⊕PRPWi*= h(PPIDi||Xj) ⊕PRPWi ⊕PRPWi*= h(PPIDi||Xj),M2 = RMSj⊕PRPWi*= h(MSIDj ||Xj),M3 = PPIDi⊕ M2,M4 = PPIDi⊕ M1 ⊕RPi,M5 = h(M1||M3||M4||RPi||TPi).SCPi sends the login ask for message {MSIDj, PYIDk, M3,M4, M5, TPi} to the restorative server MSj by means of a public channel, where PYIDk is the character of the doctor server PSk from where Pi needs to get to the medicinal administration.

Session key Agreement and Authentication Phase:

In this stage, a lawful client Pi verifies an accessed physician server PSk and PSk likewise confirms Pi for mutual confirmation reason before they can set up uneven basic session key SKPPS between them for their future secure correspondence. This stage includes the following steps:

Step A1:{MSIDj, PYIDk, M3, M4, M5, TPi}from Pi,MSj confirms the legitimacy of the got time-stamp TPiin the message. Let the login ask for be receivedby MSj at time TPi*. MSj at that point checks the condition|TPi*− TPi|≤ ∆T, where∆T means the maximumtransmission delay. On the off chance that this condition comes up short, thelogin ask for message is rejected and furthermore the session isterminated quickly. Something else, MSj executes thenext step.

Step A2: MSj keeps on registering M6 = h(MSIDj||Xj) utilizing its own character MSIDj and the mystery keyXj , where Xj = h(MSIDj ||Xc) and Xc is the mystery keyof the MRS. MSj then computesM7 = M3 ⊕ M6= PPIDi,M8 = h(M7||Xj)= h(PPIDi||Xj),M9 = M4 ⊕ M7 ⊕ M8= RPi,M10 = h(M8||M3||M4||M9||TPi)= h(h(PPIDi||Xj)||M3||M4||RPi||TPi).MSj additionally checks the condition M10 = M5. In the event that it holds,MSj trusts the validness of the client Pi. Otherwise,MSj ends the session instantly.

On the off chance that the condition M10 =M5 holds, MSj stores the combine (M7, M9) = (PIDi, RPi)in its database. Afterward, when MSj gets the following loginrequest message, say MSIDj, PSIDk, M3*, M4*, M5*,TPi,MSj first checks the legitimacy of the time-stamp TPi. Ifit is legitimate, MSj registers M6* = h(MSIDj ||Xj), M7* =M3*⊕ M6*, M8* = h(M7*||Xj), M9* = M4*⊕ M7*⊕ M8*.After that MSj contrasts M9* and the put away M9 = RPicorresponding to the client Pi's character M7 = PIDi inits database. On the off chance that there is a match, MSj guarantees that thereceived login ask for message {MSIDj, PSIDk, M3*, M4*, M5*,TPi}is a replay message and disposes of this message .Otherwise, MSj replaces M9 with M9* in its database and treats this message as a crisp message.

Step A3: MSj creates an irregular nonce RMSj and the current time-stamp TMSj. MSj figures M11 =h(MSIDj||PSIDk||KPMjk), where 'KPMjk' is the mystery key sharedbetween MSj and PSk. MSj promote computesM12 = PPIDi ⊕ M11,M13 = h(PPIDi||KPMjk) ⊕RMSj,M14 = PPIDi ⊕ M9 ⊕RMSj = PPIDi⊕RPi ⊕RMSj,
M15 = h(PIDi||M11||M12||M13||M14||M9||RMSj||TMSj) MSj at that point sends the confirmation ask for message{MSIDj, PSIDk, M12, M13, M14, M15, TMSj}to thephysician server PSk by means of an open channel.

Step A4: After getting the message in Step A3, PSkchecks the legitimacy of the got time-stamp TMSj inthe message by the condition |TMSj* − TMSj|≤∆T,where TMSj*is the time when the message is gotten byPSk. On the off chance that it is legitimate, PSk additionally proceeds to computeM16 = h(MSIDj||PSIDk||KPMjk),M17 = M12 ⊕ M16= PPIDi,M18 = M13 ⊕ h(M17||KPMjk)= RMSj,M19 = M14 ⊕ M17 ⊕ M18 = RPi, M20 = h(M17||M16||M12||M13||M14||M19||M18||TMSj) = h(PIDi||h(MSIDj||PSIDk||KPMjk)||M12||M13||M14||RPi||RMSj ||TMSj).PSk at that point checks the condition M20 = M15. On the off chance that it doesn't hold, the session is ended by PSk. Something else, PSkbelieves the legitimacy of both MSj and in addition Pi.

Step A5: PSk produces an arbitrary nonce RPSk and thecurrent time-stamp TPSk. PSk likewise computesM21 = h(M17||KPMjk)= h(PPIDi||KPMjk),M22 = M17 ⊕ M19 ⊕RPSk= PPIDi⊕RPi⊕RPSk,M23 = M21 ⊕RPSk= h(PPIDi||KPMjk) ⊕RPSk,SKPPS = h(M17||PSIDk||M19||RPSk||M21||TPSk)= h(PPIDi||PSIDk||RPi ||RPSk||h(PPIDi||KPMjk)||TPSk),M24 = h(SKPPS||M22||M23||M19||RPSk||TPSk).PSk at long last sends the validation answer message {PSIDk,M22, M23, M24,TSk} to the client Pi by means of an open channel.

Step A6: After getting the message in Step A5, the smart card SCi of the client Pi checks the legitimacy of the time-stamp TPSk in the got message by the condition |TPSk* − TPSk|≤T , where TPSk*is the time when the message is gotten by Pi. In the event that it holds, Pi computesM25 = M22 ⊕ (PPIDi⊕RPi)= RPSk,M26 = M23 ⊕ M25= h(PPIDi||Xk),SKPPS* = h(PPIDi||PSIDk||RPi ||M25||M26||TPSk),M27 = h(SKPPS*||M22||M23||RPi ||M25||TPSk).SCPi at that point checks if M27 = M24. On the off chance that it matches, Pi authenticate PSk, and both Pi and PSk regard SKPPS*=SKPPS as the session key shared between them.

5. Cryptanalysis of A.K Das et al’s Scheme

In this section, we show that A.K Das et al.'s authentication scheme is vulnerable to various major cryptographic attacks, which are detailed in the following subsections.
In this section, we crypt analyze A.K.Das et al.’s scheme [3] and demonstrate that their scheme is vulnerable to security attacks. According to the threat model discussed above and depicted in [1,2,15,20,21], an attacker ‘E’ can intercept, eavesdrop and alter

any message transmitted in the public communication channel. As discussed in [1,2,15,18], the attacker by carrying out power consumption analysis, can extract all the parameters stored in the smart card [1,2,11]. Built on these two well accepted assumptions, the A.K.Das et al scheme is susceptible to subsequent cryptographic attacks.

A. Failure to resist Replay attaack

Patient (Pj)	Medical Server (MSj)
Step 1) Login Message 1:{MSIDj, PYIDk, M31, M41, M51, TPi1}, using RPi1 as random number.	Step 1) Stores (PIDi, RPi1) in its database.
Step 2) Attacker intercepts the first login message.	
Step 3) Login Message 2: {MSIDj, PYIDk, M32, M42, M52, TPi2}, using RPi2 as random number.	Step 3) In step A2, MSj compares $M9^*$i.e.RPi2 with M9 i.e.RPi1. As both are different, MSj replaces RPi1 with RPi2. i.e.(PIDi, RPi1) -> (PIDi, RPi2) in its database.
Step 4) Now the Attacker replays the intercepted first login message in step 1 above with in the valid time frame.	Step 4) MSj compares RPi1 with the current entry i.e.RPi2. As both are different, MSj accepts the replayed message as original.

In A.K.das et al [5] plot they are opposing the replay and MiM assaults in light of match between the irregular number put away in the information base (last effective login message) and the arbitrary number utilized as a part of the current login ask. In this way, the foe can mimic as Pi by replaying any of the blocked login messages from the patient which are encircled in light of the arbitrary number other than the one as of now put away in the database as appeared in the table above. Henceforth, we can presume that A.K Das et al., plot experiences replay assault, client pantomime assault. Known session-specific temporary information attack

The compromise or leakage of a short-term secret (session specific random values) information shouldnot compromise the generated session key [20, 21, 22, 23,29]. However, in
A.K.Das et al scheme, if session specific random numbers i.e.RPi, RMSj and RPSk are compromised,then the adversarycan compute the session key SKPPS as follows:
E can intercept and record the transmitted messages {PSIDk, M22, M23, M24,TSk}and{MSIDj, PYIDk, M3,M4, M5, TPi}.
With these messages in hand the adversary can frame the session key as follows:
Compute:
$M23 = M21 \oplus RPSk \Rightarrow M21 = M23 \oplus RPSk = h(PPIDi||KPMjk)$.
$M22 = PPIDi \oplus RPi \oplus RPSk \Rightarrow M22 \oplus RPi \oplus RPSk = PPIDi$
With these values, the adversary can compute the session key $SKPPS = h(PPIDi||PSIDk||RPi||RPSk||h(PPIDi||KPMjk)||TPSk)$.
Therefore, A.K.Das et al scheme is vulnerable to Known session-specific temporary information attack in which the compromise of RPi, RPSk, RMSj results in framing of session key by an attacker.

User (Pi)	Medical Server MSj	Physician Server PSk
Inserts SC into a terminal Inputs PPIDi, PPWi Step a) Compute: σi* = Rep(Bi, τi), K* = h(PPIDi|| σi*) ⊕ ei, PRPWi* = h(PPIDi||K*||PPWi), fi* = h(PPIDi|| PRPWi*||σi*). SCi further checks the verification condition fi* = fi. Step b) Generate : RPi Current time-stamp TPi. Computes: M1 = RMj ⊕PRPWi* = h(PPIDi||Xj) ⊕ PRPWi ⊕ PRPWi* = h(PPIDi||Xj) M2 = RMSj ⊕ PRPWi* = h(MSIDj||Xj) M3 = PPIDi ⊕ M2 M4 = PPIDi ⊕ M1 ⊕ RPi M5 = h(M1|| M3 || M4|| RPi ||TPi). SCPi sends the login request message {MSIDj, PYIDk, M3, M4, M5, TPi} to MSj → Receive at TPSk*: Check : | TPSk* – TPSk | ≤ T , If it holds, Computes M25 = M22 ⊕ (PPIDi ⊕ RPi) = RPSk M26 = M23 ⊕ M25 = h(PPIDi|| KPMjk)), SKPPS* = h(PPIDi|| PSIDk|| RPi ||M25||M26|| TPSk), M27 = h(SKPPS*||M22||M23|| RPi ||M25||TPSk). SCi then checks if M27 = M24. If it matches, Pi authenticates PSk, and both Pi and PSk treat SKPPS* = SKPPS as the session key shared between them.	Receive: m1 = {MSIDj, PYIDk, M3, M4, M5, TPi} @ TPi* Checks if | TPi* - TPi| < ΔT MSj continues: Compute M6 = h(MSIDj||Xj). M7 = M3 ⊕ M6 = PPIDi M8 = h(M7||Xj) = h(PPIDi||Xj) M9 = M4 ⊕ M7 ⊕ M8 = RPi M10 = h(M8||M3||M4||M9|| TPi) = h(h(PPIDi|| Xj)|| M3||M4|| RPi ||TPi). MSj further checks the condition M10 = M5. Generates a random nonce RMSj, TMSj. MSj computes M11 = h(MSIDj || PSIDk || KPMjk). M12 = PPIDi ⊕ M11, M13 = h(PPIDi|| KPMjk) ⊕ RMSj, M14 = PPIDi⊕M9⊕ RMSj = PIDi ⊕ RPi ⊕ RMSj, M15 = h(PPIDi||M11||M12||M13||M14||M9|| RMSj || TMSj). sends the authentication request message {MSIDj, PSIDk, M12, M13, M14, M15, TMSj } → ← { PSIDk, M22, M23, M24, TPSk }	Step a) PSk checks || TMSj* – TMSj | ≤ ΔT, where TMSj* is the time when the message is received by PSk. Compute M16 = h(MSIDj ||IDk|| KPMjk), M17 = M12 ⊕ M16 = PPIDi, M18 = M13 ⊕ h(M17|| KPMjk) = RMSj, M19 = M14 ⊕ M17 ⊕ M18 = RPi, M20 = h(M17||M16||M12||M13|| M14 || M19|| M18||TSms) = h(PIDi ||h(MSIDj|| PSIDk || Xk)|| M12||M13||M14 || RPi || RMSj || TMSj). PSk then checks the condition M20 = M15. Step b) PSk generates : RPSk, TPSk. M21 = h(M17||KPMjk) = h(PPIDi|| KPMjk), M22 = M17 ⊕ M19 ⊕RPSk = PPIDi ⊕ RPi ⊕RPSk. M23 = M21 ⊕RPSk = h(PPIDi||KPMjk) ⊕RPSk SKPPS = h(M17||PSIDk||M19|| RPSk ||M21|| TPSk) = h(PPIDi||PSIDk|| RPi || RPSk||h(PIDi|| KPMjk) || TPSk), M24 = h(SKPPS||M22||M23||M19||RPSk || TPSk). PSk sends the authentication reply message {PSIDk, M22, M23, M24, TPSk } to the user Pi via a public channel.

Fig1 : Login and authentication phases of Amin et al [2] scheme.

Failure to resist stolen-verifier attack

The stolen-verifier attack occurs when an adversary steals the verificationtable from the server and uses it directly to masquerade as a legal user.'E' as an insider can access to MSj database to getall the pairs of (PPIDi, RPi). As the patient identity is stored in plain format without any encryption, the adversary can findout all the identities of the patients. Hence, A.K.Das et al fail to preserve the patient identity PIDiwhich is a critical requirement in TMIS systems. As the communication messages are transmitted over insecure public communication channel, 'E' can intercept all these communication messages exchanged among the communication entities i.e {MSIDj, PYIDk, M3, M4, M5, TPi}.

M3 = PPIDi ⊕ M2 = >M2 = M3⊕PPIDi.
M1 = M4⊕PPIDi⊕RPi
The MSj transfers the message {MSIDj, PSIDk, M12, M13, M14, M15, TMSj}

M11 = M12 ⊕PPIDi, // from M12.
M14 = PPIDi ⊕ M9 ⊕RMSj = PPIDi ⊕RPi ⊕RMSj
RMSj = M14⊕PPIDi ⊕RPi // from M14.
M13 = h(PPIDi||KPMjk) ⊕RMSj
h(PPIDi||KPMjk) = M13 ⊕RMSj // from M13.
Now the adversary can frame the session key and the login request MSj i.e {MSIDj, PSIDk, M12, M13, M14, M15, TMSj}.

Therefore, A.K. das et al scheme is susceptible to stolen verifier attack, once the database or verifier table is stolen by the attacker, the attacker can frame the session key SKPPS and the login request message sent by the MSj to PSk. Hence, we can confirm that A.K.Das et al scheme is susceptible to resist Replay attaack, Known session-specific temporary information attackdf Now the adversary can frame the session key and the login request by MSj i.e. {MSIDj, PSIDk, M12, M13, M14, M15, TMSj}.

Based on the above discussion, we can confirm that, A.K. das et al scheme is susceptible to stolen verifier attack. Once the database or verifier table is stolen by the attacker, the attacker can frame the session key SKPPS and the login request message sent by the MSj to PSk. Hence, we can confirm that A.K.Das et al scheme fails to resist Replay attaack, resist stolen-verifier attack, Known session-specific temporary information attack, medical server bye pass attack, and fails to preserve patient identity.

6. Analysis of Weakness of Das Et Al. Scheme

6.1. Analysis on enormous data storage along with computational requirements to generate user smart cards

In A.K. Das et al. scheme the smart card memory is stored with key-plus-Id combination (Aj,Pj) { $1 \le j \le m + m^*$. }of all the medical servers MSj. Based on the A.K.Das et al. discussion, for a total ofm = 100 and m* = 10, on each user 110 values are stored. If the system contains n users, then a total of (n * 110) hash operations need to be performed to load the smart card memory of corresponding user which requires huge computation cost from the MS. The major issue is that the user may not interested or in need of data from all the medical servers (because a cardiac patient access only the cardiac and related medical servers). Hence storing all the m+m*medical server details is a major drawback in das et al. scheme.If any medical server or patient server structure has been changed, then all thesmart card users data corresponding to that specific server has to be changed, which is a computationally intensive task.

6.2 Fails to achieve mutual authentication among all the communicating entities.

In A.K. Das et al. scheme on receiving the login request from from the medical server MSj, the patient server responds directly to the patient by passing the medical server. Hence, the mutual authentication among the communicating entities is not achieved.

7. Conclusion

In this paper, we have first reviewed the recently proposed A.K.Das et al.'s scheme for TMIS. A.K.Das et al.'s scheme is efficient in resisting most of the cryptographic attacks. Unfortunately, on in-depth analysis, we have verifiedthat their scheme is insecure against several major well knownattacks. Thus, their proposed scheme is not suitable for practical application in TMIS.In future work, we will come up with an improved version of authentication scheme for TMIS which can resist all major cryptographic attacks.

References

[1] Z.Y.Wu, Y.C.Lee, F.Lai, H.C. Lee, and Y.Chung, 'A secure authentication scheme for telecare medicine information systems', springer Journal of Medical Systems, vol 36, pp:1529–1535, 2012.

[2] C.Guo, and C.C.Chang, Chaotic maps-based passwordauthenticated key agreement using smart cards.Elsevier journal of Communications in Nonlinear Science and Numerical Simulation,vol 18, pp:1433–1440, 2013.

[3] R.Amin, and G.P.Biswas, A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usablein TMIS. J. Med. Syst. vol 39,. pp : 1–17, 2015.

[4] R.Amin and G.P.Biswas,A Secure Three-Factor User Authentication and Key Agreement Protocol for TMIS With User Anonymity,J Med Syst, Aug 2015.

[5] A.K.Das, V.Odelu and A.Goswami, A Secure and Robust User Authenticated Key Agreement Scheme for Hierarchical Multi-medical Server Environment in TMIS,J Med Syst, vol 39, 2015.

[6] J.Srinivas, D.Mishra and S.Mukhopadhyay, 'A Mutual Authentication Framework for Wireless Medical Sensor Networks',J Med Syst, pp:41:80, 2017.

[7] S.Challaa,A.K.Das,V.Odelu, N.Kumar,S.Kumari,M.K.Khane and A.V.Vasilakos, 'An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks',Elsevier journal of Computers and Electrical Engineering, pp:1–21,2017.

[8] D.He, J. Chen, and R. Zhang, 'A more secure authentication scheme fortelecare medicine information systems', springer journal of medical systems, vol 36, pp: 1989–1995, 2012.

[9] T.F.Lee, An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems,springer journal of Med Syst, vol 37, 2013.

[10] Jiang, Q., Ma, J., Lu, X., Tian, Y., Robust chaotic map-basedauthentication and key agreement scheme with strong anonymityfor telecare medicine information systems. J. Med. Syst. 2014.

[11] D.Mishra,J.Srinivas and S.Mukhopadhyay,A Secure and Efficient Chaotic Map-Based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems,Journal of Medical Systems, vol 38, Oct 2014.

[12] R.Amin,SK HafizulIslam,G.P.Biswas,M.K.Khan and N.Kumar,A robust and anonymous patient monitoring system using wireless medical sensor networks,Vol 80, Pages 483-495, March 2018.

[13] A.K.Awasthi, and K. Srivastava, 'A biometric authentication scheme for telecare medicine information systems with nonce', springer jurnal of medical systems, vol 37, Oct 2013.

[14] N.Ravanbakhsh and M.Nazari,An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems,Multimedia Tools and Applications,vol 77, pp 55–88,Jan 2018.

[15] Hongtao Li,Feng Guo,Wenyin Zhang,Jie Wang and Jinsheng Xing, (a,k)- Anonymous Scheme for Privacy-Preserving Data Collection in IoT-based Healthcare Services Systems,Journal of Medical Systems,vol 42, 2018.

[16] S.A.Chaudhry, M.T.Khan, M.K.Khan, and T.Shon, 'A Multiserver Biometric Authentication Scheme for TMIS using Elliptic Curve Cryptography',springer Journal of Medical Systems, vol 40, pp: 230-243, Nov 2016.

[17] C.T.Li,C.Y.Weng, and C.C.Lee, 'A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system', springer Journal of Medical Systems, vol 39, pp: 1–8, 2015.

[18] M.Benssalah,M.Djeddou and K.DroPiche, 'Security Analysis and Enhancement of the Most Recent RFID Authentication Protocol for Telecare Medicine Information System', springer journal of Wireless Personal Communications pp: 6221–6238, vol 96, Oct 2017.

[19] H.Lai, M.Luo,Z.Qu,F.Xiao, and M.A.Orgun, 'A Hybrid Quantum Key Distribution Protocol for Tele-care Medicine Information Systems', Volume 98, pp 929–943,Jan 2018.

[20] Xie Q, Tang Z, Chen K. Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks. Comput Electr Eng 2017;59:218–30.

A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," inThird IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2005, pp. 324–328

[21] V.Odelu,A.K.Das, and A.Goswami, 'An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card', Elsevier journal of Journal of Information Security and Applications, vol 21, pp: 1-19, 2015.

[22] N.Druml,M.Menghin,A.Kuleta,C.Steger,R.Weiss,'A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems',17th Euromicro Conference on Digital System Design,2014.Italy.

[23] M.Sarvabhatla,and C.S.Vorugunti, 'A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN',2014 Fourth International Conference of Emerging Applications of Information Technology, ISI-Kolkatta, 2015.

[24] Q.Cheng,X.Zhang and J.Ma, 'ICASME: An Improved Cloud-Based Authentication Scheme for Medical Environment', pp:41-44,March 2017.

[25] S.I. Chu,Y.J.Huang and W.C.Lin, 'Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks',IEEE SYSTEMS JOURNAL, Vol 11, Dec 2017.

[26] S.Kumari,X.Li,F.Wu,A.K.Das,H.Arshad, and M.K.Khan, 'A User Friendly Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks using Chaotic Maps', Vol 63, PP : 56-75, oct 2016.

[27] V.Odelu, S.Banerjee, A.K.Das, S.Chattopadhyay, S.Kumari,X.Li and A.Goswami, 'A Secure Anonymity Preserving Authentication Scheme for Roaming Service in Global Mobility Networks',springe journal of Wireless Personal Communications, vol 96, pp: 2351–2387,sep 2017.

[28] V.C.Sekhar, M.Bharavi, A.Ruhul, P.B.Rakesh, and S.Mrudula, 'Improving Security of Lightweight Authentication Technique for Heterogeneous Wireless Sensor Networks',springer journal of Wireless Personal Communications, pp:1–26,2017.

[29] X.Li,F.Wu,M.K.Khan,L.Xu,J.Shen and M.Jo, 'A Secure Chaotic Map-based Remote Authentication Scheme for Telecare Medicine Information Systems.',elsevier journal of Future Generation Computer Systems, Aug 2017.

[30] A.Chaturvedi, D.Mishra, S.Jangirala and S.Mukhopadhyay, 'A privacy preserving biometric-based threefactor remote user authenticated key agreement scheme.',Elsevier Journal of Information Security.