Industrial Engineering Journal
ISSN: 0970-2555
Volume : 49, Issue 6, No. 1, June : 2020

A Trustworthy and Reliable User Authenticated Key Agreement Scheme for the Hierarchical Multi-medical Server Environment in the TMIS

P. HIMABINDU
Assistant Professor
Himabindu5808@gmail.com

Y. HARINATH
Assistant professor
Harinath5404@gmail.com

B. VANITHA
Assistant Professor
Vanitha.alts@gmail.com

***Abstract*—The telecare medicine information system (TMIS), which consists of a sensor, medical server, and physician servers to sense human biological readings and monitor the health condition of the patients, has been developed as a result of the rapid advancement of pervasive computing, nanotechnology, and wearable systems. This has allowed for the development of low-power internet-based systems that eliminate distance-related complications. Patient authentication, data integrity, and data privacy are essential requirements due to the association of sensitive patient data and its transmission across an unsecure and public communication channel. Many researchers have put forward different user authentication and safe data transfer via TMIS techniques in this area. A three-factor user authentication and key agreement mechanism for TMIS was recently presented by A.K. Das et al. They said that the proposed protocol is effective, secure, and lightweight. We assess their plan's defense against well-known cryptographic assaults. Even while the A.K.Das et al. method is resistant to significant cryptographic attacks, our in-depth examination shows that it has security flaws, including the inability to withstand replay attacks, known session-specific temporary information attacks, and stolen-verifier attacks.**

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

I. INTRODUCTION

The rapid development of networking, radio frequency identification (RFID), and communication technologies led to the evolution of the mobile health-care paradigm, in which low-power sensors fixed to the human body collect information about the body's motion and physical state and communicate over networked systems, such as Telecare Medicine Information Systems (TMIS) or Wireless medical sensor networks (WMSNs) [1, 2, 3, 4–10, 20–21]. Patients may remotely access health-related information using TMIS. Additionally, it offers a platform for communication between patients at home and medical staff at the clinic via a public channel. Due to its significant advantages over wired BANs, such as lower administrative costs, instant quality of healthcare, accurate record keeping, efficient continuation and preventative treatment, improved patient comfort, etc., TMIS have attracted a lot of interest in recent years. [2,11-30].

The implanted sensors in TMIS are dispersed throughout the body of the patient, regardless of the patient's or doctor's location, and each of the distributed sensor nodes is capable of gathering the patient's vital statistics, including heart rate, blood pressure, glucose level, respiration rate, and electrocardiogram, among others [3,18]. The patient can send these health-related data and communicate with the doctor via video chat. Any wireless transmission device that employs radio waves for communication, such as Bluetooth, Wi-Fi, etc., may be used by the doctor or laboratory, among others, to log into WMSN.

However, since TMIS uses radio waves to transmit patient physiological data in a public setting (the internet), an attacker may eavesdrop on, alter, or redirect the medical data from the open channel. Serious privacy and security problems could result from this, including user impersonation attacks, medical server spoofing attacks, and the modification of exchanged sensitive patient medical information. These problems could be very expensive for both patients and healthcare professionals [1,2,11-14,18-21].

As a result, the TMIS must preserve patient identification and privacy. Because patients may have isolated illnesses like leprosy, HIV, etc., patient confidentiality is another essential necessity of TMIS [1,2,313,15,19,20,17]. Therefore, TMIS needs a secure authentication system so that authorized users may receive medical services with confidence and security..

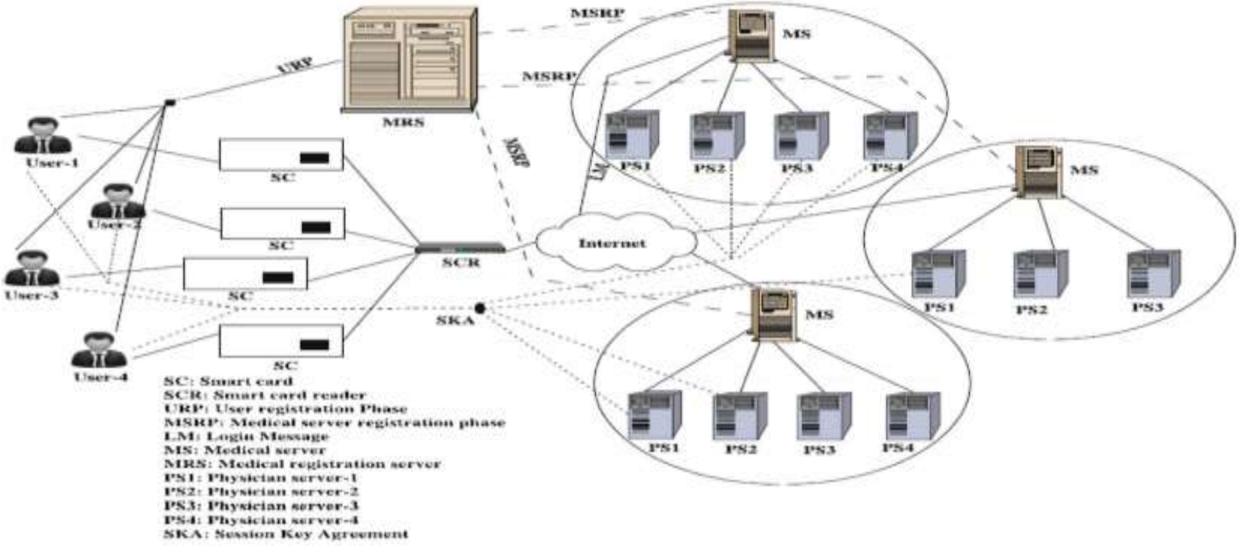

Fig. 1. Architecture for accessing multi-medical server system in Amin et al scheme (Source: [1])

Architecture of TMISand its benefits in healthcare Services:

Fig. 1 shows the TMIS's architectural layout. The user authentication process using TMIS involves four communicating entities, which are listed below:

1. Patient / User: A registered user who is receiving therapy while being monitored in real time by a medical expert using distributed medical sensors (MS).
2. Medical personnel that closely monitor and observe patient physiological data using TMIS include doctors, nurses, and lab workers.

3. MRS: A resource-intensive master node that serves as the user, MS, and PS registration authority and serves as a conduit between the user and the medical server.
4. MS: The physical servers' controlling authority is the medical server. Through a medical server MSj, the PSk offers services on demand to the approved registered users/patients Pi.

II. LITERATURE SURVEY

A few authentication methods that have been suggested to protect healthcare sensor networks are summarized in this section. To improve the security and data integrity of Telecare medical information systems, several researchers [1-31] have put forward authentication approaches throughout the years.

The researchers use a variety of techniques, including the cryptographic one-way hash function[1], ECC-RSA cryptosystem[3,6,12], chaotic maps[2], and light weight cryptographic operations like XOR, concatenate[12], among others, to build an authentication protocol.

Wu et al. [1] suggested an authentication technique for TMIS in 2012 and claimed that it was resistant to all significant cryptographic attacks since it was based on the difficulty of solving the Discrete Logarithm Problem (DLP). Wu et al's approach fails to achieve user anonymity, according to He et al's [8] thorough review of their cryptanalysis of Wu et al's [1] scheme. Additionally, He et al. [8] confirmed that Wu et alsystem .'s [1] is susceptible to insider attacks and user impersonation assaults. The session key in the authentication and key agreement technique Lee et al.[9] developed for TMIS is based on chaotic maps. The chaotic map-based remote user authentication approach for TMIS was recently suggested by Jiang et al [10]. Their approach benefits from minimal costs and Chaos theory-based session key agreement. Jiang et al[10] .'s method was examined by Mishra et al. [11], who found that it was vulnerable to denial-of-service attacks and had security issues during the password changing phase.

Amin et al [12] introduced a unique multi-medical servers architecture and secure user authentication using key agreement protocol for TMIS in order to enable access to many medical servers with a single registration. Through the utilization of physician servers, Amin et al[12] .'s architecture makes safe user authentication and key agreement protocol possible. The Amin et al. [12] scheme was recently shown to be vulnerable to replay attack, privileged-insider attack, session key disclosure attack, fails to provide patient untraceability, and fails to provide backward secrecy. Ravanbakhsh et al. proposed an effective remote mutual authentication scheme on ECC and Fuzzy Extractor. Li et al. [17] developed a new anonymity-based privacy-preserving data collection (PPDC) technique for healthcare services as well as a (a,k)-anonymity model based privacy protection strategy for data gathering using IoT devices connected to patient bodies. On the client-side, Li et al [17] construct anonymous tuples that can withstand potential attacks using the (a,k)-anonymity idea, and on the server-side, they lowered the communication cost using generalization technology.

Amin et al. [3] recently suggested a smart card-based security protocol for the TMIS system utilizing the cryptographic one-way hash function and the biohashing function, and they asserted that their plan is resistant to significant cryptographic assaults. Later, A.K.Das et al [5] demonstrated that the Amin et al [3] system had a number of security flaws, including a failure to defend against powerful replay attacks, privileged insider attacks, and man-in-the-middle attacks, among others. A.K.Das et al. [5] suggested a strong user authentication with key agreement approach in hierarchical multi-medical server architecture in TMIS after demonstrating the security flaws in Amin et al. [3]'s system. According to A.K.Das et al. [3], their authentication method prevents listening in, unauthorized portable device usage by medical workers, inhibits unauthorized access to patient medical records, and withstands all significant cryptographic assaults.

III. OUR CONTRIBUTION

The contribution of the paper is twofold. First, we briefly discuss A.K.Das et al [3]Hierarchical Multi-medical Server based authentication scheme for TMIS.Second, we demonstrate 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 sketched as follows. In Section IV, we briefly describe the A.K.Das et al scheme [3]. We then show that A.K.Das et al.'s scheme is insecure against four attacks in Section V. Finally, we conclude the paper in Section VII.

IV. REVIEW OF A.K. DAS ET AL.'S SCHEME

In this section, we describe the various phases of A.K.Das et al [3] scheme, which are (i) medical server registration phase, (ii)user registration phase, (iii) login phase, (iv) authenticationand 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
PBi	Personal biometrics of Pi
MSIDj	Identity of MSj
PSIDk	Identity of PSk
KMRS	Secret key of the MRS
KMSj	Secret key of MSj
KPMjk	Shared secret key between PSk and MSj
RPi	Random nonce generated by Pi
RMSj	Random nonce generated by MSj
RPSk	Random nonce generated by PSk
TPi	Current time-stamp generated by Pi
TMSj	Current time-stamp generated by MSj
TPSk	Current time-stamp generated by PSk
Δt	Maximum transmission delay, expected time interval for transmission delay or expected network delay time

$h(\cdot)$	Collision-free one-way hash function
$H(\cdot)$	Biohashing function [27, 35]
$Gen(\cdot)$	Fuzzy extractor generation algorithm
$Rep(\cdot)$	Fuzzy extractor reproduction algorithm
σi	Biometric key of Pi
τi	Biometric public parameter of Pi
εt	Error tolerance threshold
$P \oplus Q$	Bitwise XORed of data P with data Q
$P \| Q$	Data P concatenates with data Q

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

Medical Server Registration Phase:

Suppose ‘m’ number of medical servers MSj, $(1 \leq j \leq m)$ are to be deployed initially in the network. We furtherassume that m* number of additional medical servers MSj,$(m + 1 \leq j \leq m + m^*)$ may be added later in the network,where m*<< m. For example, initially m = 100 medicalservers may be deployed and later we may add m* = 10additional medical servers after initial deployment in thenetwork, if required, based on the demand of the medicalservices when more users want to access the services.For this purpose, a medical server MSj, $(1 \leq j \leq m)$,which wants to provide the medical services to the remoteusers (patients), needs to select a unique identity MSIDjand send it to the MRS. After receiving MSIDj, the MRScomputes the secret key Xj = h(MSIDj|| KMRS), where KMRSis the 1024-bit secret key of the MRS for security reasons,and sends it back to MSj via a secure channel. Thus,each MSj keeps (MSIDj, Xj). For m^* additional medicalservers MSp, $(m + 1 \leq p \leq m + m^*)$, the MRS itselfchooses a unique identity MSIDj and also compute thesecret key Xq = h(MSIDj|| KMRS). Note that these computed(MSIDj, Xq) are kept to the MRS and will be used later duringthe user registration phase and dynamic medical serveraddition phase.

User Registration Phase

In this phase, a legal user Pi needs to register with the MRS
for accessing the medical services from a particular physicianserver PSk under a medical server MSj in the network.

This phase has the following steps:

Step R1: Pi first inputs his/her desired identityPPIDi, password PPWi, and then imprints the personalbiometrics PBi at the sensor of a specific device. Pi generatesa 1024-bit random number K, which is kept secretto Pi only. Pi then applies the fuzzy extractor generationfunction $Gen(\cdot)$ on the input

PBi in order to producethe biometric data key σi and the public parameter τi as$Gen(Bi) = (\sigma i, \tau i)$. Note that σi is kept secret to Pi only.

Step R2: Pi computes the pseudo-random passwordPRPWi as$PRPWi = h(PPIDi||K||PPWi)$ and sends the registrationrequest {PPIDi, PRPWi} to the MRS via a securechannel.

Step R3: After receiving the registration request from Pi,the MRS continues to compute $RMj = h(PIDi||Xj) \oplus PRPWi$ and $RMSj = h(MSIDj ||Xj) \oplus PRPWi$, for $1 \leq j \leq m + m^*$. Then the MRS stores the information$\{\{MSIDj , RMj , RMSj|1 \leq j \leq m + m^*\},h(\cdot), Gen(\cdot), Rep(\cdot), t\}$ in a smart card, say SCPi andsends it to the patient/user Pi via a secure channel, where ‘εt’ is theerror tolerance threshold used in fuzzy extractor.

Step R4: After receiving the smart card SCi from theMRS, the user Pi computes $ei = h(PPIDi||\sigma i) \oplus K$ and$fi = h(PPIDi||PRPWi||\sigma i)$. Pi then stores ei and fi in thesmart card SCPi. Finally, note that the smart card SCPicontains the information $\{MSIDj , RMj , RMSj|1 \leq j \leq m + m^*\}$, ei, fi, h(·), Gen(·), Rep(·), τi,and ‘εt’.

Login phase:

In this phase, a legal user Pi can access any medical serverMSj for the medical services from a physician server PSkunder that medical server MSj at anytime from anywherethrough his/her issued smart card PSCi. This phase containsthe following steps:

Step L1: Pi first inserts his/her smart card PSCi into asmart card reader of a specific terminal, and then inputshis/her identity PPIDi, password PPWi, and also imprintsthe personal biometrics PBi at the sensor.

Step L2: SCi then computes$\sigma i^* = Rep(Bi, \tau i)$,$K^* = h(PPIDi|| \sigma i^*) \oplus ei$,$PRPWi^* = h(PPIDi||K^*||PPWi)$,$fi^* = h(PPIDi||PRPWi^* || \sigma i^*)$.SCi further checks the verification condition $fi^*= fi$.If it holds, it ensures that the user Pi passes successfullyboth password and biometric verification. Otherwise, thisphase is terminated immediately.

Step L3:SCPifurther proceeds to generate a randomnonce RPi and the current time-stamp TPi. ThenSCPi computes$M1 = RMj \oplus PRPWi^*= h(PPIDi||Xj) \oplus PRPWi \oplus PRPWi^*= h(PPIDi||Xj)$,$M2 = RMSj \oplus PRPWi^* = h(MSIDj ||Xj)$,$M3 = PPIDi \oplus M2$,$M4 = PPIDi \oplus M1 \oplus RPi$,$M5 = h(M1||M3||M4||RPi ||TPi)$.SCPi sends the login request message {MSIDj, PYIDk, M3,M4, M5, TPi} to the medical server MSj via a publicchannel, where PYIDk is the identity of the physician serverPSk from where Pi wants to access the medical service.

Authentication and Session key Agreement Phase

In this phase, a legal user Pi authenticates an accessedphysician server PSk and PSk also authenticates Pi formutual authentication purpose before they can establish asymmetric common session key SKPPS between them fortheir future secure communication. This phase involves thefollowing steps:

Step A1:{MSIDj, PYIDk, M3, M4, M5, TPi}from Pi,MSj verifies the validity of the received time-stamp TPiin the message. Let the login request be receivedby MSj at time TPi^*. MSj then checks the condition$|TPi^* - TPi| \leq \Delta T$, where$\Delta T$ denotes the maximumtransmission delay. If this condition fails, thelogin request message is rejected and also the session isterminated immediately. Otherwise, MSj executes thenext step.

Step A2: MSj continues to compute $M6 = h(MSIDj||Xj)$ using its own identity MSIDj and the secret keyXj , where $Xj = h(MSIDj ||Xc)$ and Xc is the secret keyof the MRS. MSj then computes$M7 = M3 \oplus M6 = PPIDi$,$M8 = h(M7||Xj) = h(PPIDi||Xj)$,$M9 = M4 \oplus M7 \oplus M8 = RPi$,$M10 = h(M8||M3||M4||M9||TPi) = h(h(PPIDi||Xj)||M3||M4|| RPi||TPi)$.MSj further checks the condition M10 = M5. If it holds,MSj believes the authenticity of the user Pi. Otherwise,MSj terminates the session immediately.

If the condition M10 =M5 holds, MSj stores the pair (M7, M9) = (PIDi, RPi)in its database. Later, when MSj receives the next loginrequest message, say MSIDj, PSIDk, $M3^*$, $M4^*$, $M5^*$, TPi,MSj first checks the validity of the time-stamp TPi. Ifit is valid, MSj computes $M6^* = h(MSIDj ||Xj)$, $M7^* = M3^* \oplus M6^*$, $M8^* = h(M7^*||Xj)$, $M9^* = M4^* \oplus M7^* \oplus M8^*$.After that MSj compares $M9^*$ with the stored M9 = RPicorresponding to the user Pi's identity M7 = PIDi inits database. If there is a match, MSj ensures that thereceived login request message {MSIDj, PSIDk, $M3^*$, $M4^*$, $M5^*$, TPi }is a replay message and discards this message.Otherwise, MSj replaces M9 with $M9^*$ in its database andtreats this message as a fresh message.

Step A3: MSj generates a random nonce RMSj and thecurrent time-stamp TMSj. MSj computes $M11 = h(MSIDj||PSIDk||KPMjk)$, where 'KPMjk' is the secret key sharedbetween MSj and PSk. MSj further computes$M12 = PPIDi \oplus M11$,$M13 = h(PPIDi|| KPMjk) \oplus RMSj$,$M14 = PPIDi \oplus M9 \oplus RMSj = PPIDi \oplus RPi \oplus RMSj$,$M15 = h(PIDi||M11||M12||M13||M14||M9|| RMSj ||TMSj)$.MSj then sends the authentication request message{MSIDj, PSIDk, M12, M13, M14, M15, TMSj}to thephysician server PSk via a public channel.

Step A4: After receiving the message in Step A3, PSkchecks the validity of the received time-stamp TMSj inthe message by the condition $| TMSj^* - TMSj | \leq \Delta T$,where $TMSj^*$ is the time when the message is received byPSk. If it is valid, PSk further continues to compute$M16 = h(MSIDj||PSIDk || KPMjk)$,$M17 = M12 \oplus M16 = PPIDi$,$M18 = M13 \oplus h(M17|| KPMjk) = RMSj$,$M19 = M14 \oplus M17 \oplus M18 = RPi$,$M20 = h(M17||M16||M12||M13||M14||M19||M18||TMSj) = h(PIDi||h(MSIDj|| PSIDk ||KPMjk)||M12||M13||M14|| RPi ||RMSj ||TMSj)$.PSk then checks the condition M20 = M15. If it does not hold, the session is terminated by PSk. Otherwise, PSkbelieves the authenticity of both MSj as well as Pi.

Step A5: PSk generates a random nonce RPSk and thecurrent time-stamp TPSk. PSk also computes$M21 = h(M17|| KPMjk) = h(PPIDi|| KPMjk)$,$M22 = M17 \oplus M19 \oplus RPSk = PPIDi \oplus RPi \oplus RPSk$,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 finally sends the authentication reply message {PSIDk,M22, M23, M24,TSk} to the user Pi via a public channel.

Step A6: After receiving the message in Step A5, thesmart card SCi of the user Pi checks the validity of thetime-stamp TPSk in the received message by the condition|$TPSk^*$ − TPSk|≤T , where $TPSk^*$is the time when themessage is received by Pi. If 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 then checks if M27 = M24. If it matches, Pi authenticatesPSk, and both Pi and PSk treat $SKPPS^*$=SKPPS as the session key shared between them.

V. 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 cryptanalyze 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	Step 3) In step A2, MSj compares $M9^*$i.e.RPi2 with M9 i.e.RPi1. As both are different, MSj

random number.	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] scheme they are resisting the replay and MiM attacks based on match between the random number stored in the data base (last successful login message) and the random number used in the current login request. So, the adversary can impersonate as Pi by replaying any of the intercepted login messages from the patient which are framed based on the random number other than the one currently stored in the database as shown in the table above. Hence, we can conclude that A.K Das et al., scheme suffers from replay attack, user impersonation attack.

B. *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.

<table>
<tr><th>User (Pi)</th><th>Medical Server MSj</th><th>Physician Server PSk</th></tr>
<tr>
<td>Inserts SC into a terminal
Inputs PPIDi, PPWi
Step a)
Compute: $\sigma i^* = Rep(Bi, \tau i)$, $K^* = h(PPIDi|| \sigma i^*) \oplus ei$, $PRPWi^* = h(PPIDi||K^*||PPWi)$, $fi^* = h(PPIDi|| PRPWi^*||\sigma i^*)$.
SCi further checks the verification condition
$fi^* = fi$.

Step b)

Generate : RPi
Current time-stamp TPi.
Computes:
$M1 = RMj \oplus PRPWi^* = h(PPIDi||Xj) \oplus PRPWi \oplus PRPWi^* = h(PPIDi||Xj)$
$M2 = RMSj \oplus PRPWi^* = h(MSIDj ||Xj)$
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
→</td>
<td>

Receive:
m1 = {MSIDj, PYIDk, M3, M4, M5, TPi} @ TPi^*
Checks if $| TPi^* - TPi| < \Delta T$
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 }
→</td>
<td>Step a)
PSk checks $|| TMSj^* - TMSj | \le \Delta T$,
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</td>
</tr>
</table>

Receive at $TPSk^*$: Check : $\mid TPSk^* - TPSk \mid \leq T$, If it holds, Computes $M25 = M22 \oplus (PPIDi \oplus RPi) = RPSk$ $M26 = M23 \oplus M25 = h(PPIDi \| KPMjk))$, $SKPPS^* = h(PPIDi\| PSIDk\| RPi \|M25\|M26\| TPSk)$, $M27 = h(SKPPS^*\|M22\|M23\| RPi \|M25\|TPSk)$. 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.	← { PSIDk, M22, M23, M24, TPSk }	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 [] scheme.

C. 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}.

$M3 = PPIDi \oplus M2 = > M2 = M3 \oplus PPIDi$.
$M1 = M4 \oplus PPIDi \oplus RPi$
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 by 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.

VI. ANALYSIS OF WEAKNESS OF DAS ET AL. SCHEME

6.1 Huge Data Storage and Computation Requirement for Generating User Smart Card

In A.K. Das et al. scheme the smart card memory is stored with key-plus-Id combination (Aj,Pj) { $1 \leq j \leq m + m^*$. }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.

6.2Fails 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 notachieved.

VII. CONCLUSION

In this paper, we have first reviewed the recently proposedA.K.Das et al.'sscheme 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.

[21] 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

[22] 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.

[23] 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.

[24] 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.

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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 and Applications, Vol 32, pp: 15-26, Feb 2017.