Journal of Medical Systems (2019) 43: 133
https://doi.org/10.1007/s10916-019-1251-3

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare

Km. Renuka[1] · Saru Kumari[1] · Xiong Li[2]

Received: 24 November 2018 / Accepted: 15 March 2019 / Published online: 3 April 2019

Abstract
Now-a-days, the society is witnessing a keen urge to enhance the quality of healthcare services with the intervention of technology in the health sector. The main focus in transforming traditional healthcare to smart healthcare is on facilitating the patients as well as medical professionals. However, this changover is not easy due to various issues of security and integrity associated with it. Security of patients's personal health record and privacy can be handled well by permitting only authorized access to the confidential health-data via suitably designed authentication scheme. In pursuit to contribute in this direction, we came across the role of Universal Serial Bus (USB), the most widely accepted interface, in enabling communication between peripheral devices and a host controller like laptop, personal computer, smart phone, tablet etc. In the process, we analysed a recently proposed a three-factor authentication scheme for consumer USB Mass Storage Devices (MSD) by He et al. In this paper, we demonstrate that He et al.'s scheme is vulnerable to leakage of temporary but session specific information attacks, late detection of message replay, forward secrecy attacks, and backward secrecy attacks. Then motivated with the benefits of USB, we propose a secure three-factor authentication scheme for smart healthcare.

Keywords Universal serial bus · Three-factor authentication · Mass storage device · Message replay · Forward/ backward secrecy

Introduction

Smart healthcare is a set of digitally working systems to provide online healthcare services to the patients securely and efficiently. Patient receiving medical prescription, doctor's advice and treatment of disease at home; patient or medical professional uploading/accessing health-data in cloud databases from their respective places; physicians monitoring vital health parameters of patients at far-off distances enabled by means of sensor technology wherein tiny sensors are implanted on patients's body to collect health-data; prompt and hassle-free solutions of patient's ailments are few instances of smart healthcare approach. But all these boons turn to curses if the system fails to maintain the confidentiality and privacy of patient's private health information and credentials. This problem has attracted a wide range of research community of which one branch is aimed at architecting efficient authentication schemes for regulating authorized access to the confidential health-data.

USB is considered these days the de facto standard for data transfer between devices (e.g. between personal computers and laptops) [1], partly due to its capability to provide fast, reliable and cost effective data transfer services [2], as well as charging of devices (e.g. charging of a mobile device via a USB port on board in an aircraft and on other vehicles). An USB drive is useful device to read/write the data within pendrive by inserting the USB drive into the USB port available in the system. Due to portability, support for electrical power, playing role of connecting device, ease of usability, and goodness of storing large data files efficiently & accessing the stored data anywhere, USBs have become quite popular.

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Xiong Li
lixiongzhq@163.com

Km. Renuka
baliyanrenuka@gmail.com

Saru Kumari
saryusiirohi@gmail.com

[1] Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India

[2] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China

In online medical scenario, various types of patient data such as moving medical images, videos depicting usual/unusual activity of some internal organ, highly detailed patient's personal information, patient X-rays in high definition etc., is generated at varied locations. Such data can be downloaded onto the USB device and instantaneously delivered for reference and assessment. In this way, USB plays important role in increasing the quality of online healthcare services with decreased cost by avoiding cumbersome network file transfer mechanisms.

Nevertheless, the transfer of data through the USB devices and interfaces may be vulnerable to a number of attacks as data is transferred in plaintext over an open channel. In other words, anyone can delete, modify or eavesdrop on the (plaintext) data. To conduct such an attack, an attacker can insert or install a malicious USB interface (that is under his/her control) at any location and any device plugged into this malicious interface (e.g. charging of mobile phone) will be at risk. It is not realistic to be able to secure each USB transfer or interface for a typical user to identify a malicious USB interface. On the other hand, if one encrypts the data using the same key over and over again, leakage of this particular key will lead to the compromise of all past and future data (i.e. loss of forward and backward secrecy). Thus, there is a need to strengthen the security wherever we decide to adopt USB in mass storage devices (MSD). Any type of theft or disclosure of patient's data can be misused and may prove to be detrimental for both patient as well as healthcare organizations. Thus, due to sensitive health data stored in USB drive, only authorized user should be able to access it. For this purpose, these days biometrics USB drives are commonly used that operate with biometrics of the owner to identify the owner and allow authorized access to it.

Authentication and key establishment schemes [3–27] are a viable option for regulating authorized access in any online service. Several authentication and key agreement schemes [3–14, 23–27] for healthcare applications have been proposed using various techniques and taking various factors in consideration. Mishra et al. [3] and Moon et al. [4] presented a biometrics based authentication scheme for telecare medicine information systems (TMIS). Khan et al. [5] proposed a dynamic id-based authentication scheme for TMIS. Hou et al. [6] utilized RSA cryptosystem to design an authentication scheme for IoT based healthcare systems. Lu et al. [7] adopted biometrics and ECC to construct an authentication scheme for TMIS. He et al. [8] used symmetric algorithms and hash functions to present a lightweight authentication scheme for healthcare applications. However, the scheme in [8] was found vulnerable to the off-line guessing attack, the user impersonation attack, and the sensor node capture attack [9]. Amin et al. [10] proposed an anonymous authentication scheme for E-health care systems. However, it was found vulnerable to denial of service attack [11]. Li et al. [12] used chaotic maps to design authentication and key-agreement scheme for e-healthcare systems. Irshad et al. [13] presented an authenticated key agreement scheme for TMIS in multi-server environment. Li et al. [14] proposed chaotic map based authentication scheme for TMIS. Recently, two survey papers [28, 29] came in the literature on authentication schemes for TMIS. Masdari and Ahmadzadeh concluded by their survey work [28] that most of the schemes lack user anonymity and fail to resist key security attacks. Aslam et al. [29] surveyed each family (one-factor, two-factor, and three-factor) of authentication schemes for TMIS. They displayed through their study that most of the proposed schemes were later found to be insecure. Further, they found the three-factor schemes to be more robust as compared to the other two families. The outcomes of the study in [28, 29] pave way for scope of improvement in authentication mechanisms for healthcare applications. In 2017, Li et al. proposed an anonymous authentication scheme for wireless body area networks [15]. Recently, [16, 17] proposed two authentication schemes for personalized healthcare systems using wireless medical sensor networks and smart healthcare systems under global mobility networks, respectively.

For effective medical services, medical personnel have to promptly go through the complete information of patients for immediate and correct diagnoses so that suitable treatment can be offered to the patients. For practical implementation of this idea, the integrated EPR (Electronic Patient Record) systems [30] have been widely accepted in healthcare industry. EPR systems greatly support patients and medical personnel for accessing health–data. However, web-based nature of EPR systems demands for maintenance of only authorized access to the stored health-data which comprises of private and highly confidential information specific to patient. And none other than a suitably designed authentication scheme with user and server as entities can serve this purpose.

USB-MSD has been used in the design of protocols such as [2, 18, 19]. However, as an attacker can read the information that is stored in plaintext on the USB, it is not possible to utilize these schemes. Yang et al. [2] proposed a secure control protocol for USB-MSD, which was found to be insecure by Chen et al. [18] and by Lee et al. [19]. Unfortunately, the scheme in [19] was found to be insecure by He et al. [20]. He et al. [20] also proposed a biometrics and ECC based authentication scheme using USB-MSD. The scheme being relying on elliptic curve cryptography, the key size is significantly smaller than those of an RSA based cryptosystem. Such a feature is attractive for implementation on USB-MSD.

Our contribution This paper contributes towards analyzing He et al.'s authentication scheme for consumer USB mass storage devices and then proposing a biometrics based authentication scheme for smart healthcare utilizing the benefits of USB. We find that even after comprising substantial features/techniques

such as user's biometrics and elliptic curve cryptography (ECC) in its design, He et al.'s scheme suffers from lack of user anonymity, lack of forward/backward secrecy and session specific temporary attack. It shows lack of optimal use of the deployed features/techniques in He et al.'s scheme. He et al.'s scheme has no provision for users to change their password. As a result, the scheme fails in case user's credential are compromised.

Tele-healthcare facility is the need of today's fast lifestyle. And proper functioning of online healthcare system relies largely on the worthiness of the security and privacy provisions in the authentication/access mechanisms involved. The results of [28, 29] inspired us to present a biometrics based three-factor authentication scheme for smart healthcare. Varied benefits of an USB-MSD along with additional feature of providing only authorized access to the stored data by utilizing user's biometrics motivated us to design a biometric based authentication scheme for smart healthcare utilizing USB-MSD. We structurize an authentication scheme themed on EPR systems for regulating authorized access to sensitive health-data, harnessing the same features/techniques as used in He et al.'s scheme but with their best possible usage. The proposed scheme successfully defies all the problems identified in He et al.'s scheme. Unlike He et al.'s scheme, the password change phase is incorporated in the proposed scheme so that the user can change its password whenever it feels to do so. The scheme is quite efficient as it possesses more attributes and is more secure as compared to the existing related schemes. Important aspect is that we have achieved this without adding any complex operations thereby limiting the time consumption for the computations required in the scheme. All these features of our scheme are shown during performance analysis. In addition to discuss the resistance of the proposed scheme informally, Random Oracle Model has been utilized to justify the security of the scheme.

Organization of the paper In this work, we go through the scheme of He et al. [20] (Section 0) and present our analysis on it (Section 0). We then present a new scheme (Section 0), and demonstrate its security using ROM Model (Section 0). The proposed scheme is examined for its performance (Section 0). The last section (Section 0) is conclusion.

Revisiting the scheme of He et al

The notations given in Table 1, are used in the paper.

Fuzzy extractor used in the scheme [20] to mitigate denial of service attacks is defined below.

Definition 1 Fuzzy extractors is the name given to the methods which reliably extract nearly uniform randomness Ri and an auxiliary string Pi from the biometrics input Bi in an error-tolerant way that Ri will be exactly recovered with the help of auxiliary string Pi even if the biometrics input changes, as long as it remains reasonably close to the original biometrics

Table 1 Notations and Meaning

Symbol	Meaning
F_p	Prime order finite field
AS	Server used for authentication
E_P	Elliptic curve group over a finite field
G	The generator of the group elliptic curve
U	The user
ID_U	The identity of user
B_U	The biometric identity of the user U
$h(\cdot)$	The one-way collision resistant hash function
$E_K(M)/D_K(M)$	Encrypting / Decrypting message M with key K
$D_K(M)$	Decryption of message M under key K
$\|$	Concatenate operation
A	The attacker in system
$H(\cdot)$	The biometric based hash function called Bio-hash
$\oplus$	The X-OR operation
T_h	The execution for time for single $h(\cdot)$ operation
T_H	The execution time for single $H(\cdot)$ function
T_M	The execution time for single modular arithmetic operation in F_p
T_E	The execution time for single exponential operations in F_p
T_F	The time for running a fuzzy extractor operation
T_{sym}	The time for running a symmetric encryption/decryption operation

template. Fuzzy Extractor [31] comprises two procedures namely *Gen* and *Rep*, as follows:

Gen(W): A probabilistic algorithm which takes as input a biometric string distribution W, and outputs $<\sigma,\delta>$where σ is an extracted string and δ is an auxiliary string.
Rep($w^{'},\delta$): A deterministic algorithm, which outputs σ if $w^{'}$ and w (i.e. auxiliary string for W) are within a certain distance t.

Registration phase

When a legitimate user U wishes to register smart card in the system with password pw_i, identity ID_i, biometric B_i, the steps followed are summarized below:

U: Computes $(\sigma_i, \delta_i) = Gen(B_i)$ and submits $\{ID_i, h(pw_i \| \sigma_i)\}$ to AS.
AS: Computes $e_i = h(h(ID_i \| x) \| h(pw_i \| \sigma_i))$ and $s_i = h(ID_i \| x) \oplus h(pw_i \| \sigma_i)$. Here,$x$ is the secret component of AS.
U: Computes $BPW_i = \delta_i \oplus h(pw_i)$. Finally, the storage device stores $\{e_i, s_i, BPW_i\}$.

Verification and data encryption phase

In this phase, a legitimate user U and *AS* will authenticate each other and derive session key *sk*.

U: Inserts USB MSD to the USB client with pw_i, ID_i and $B_i^{'}$. Device calculates $\delta_i = BPW_i \oplus h(pw_i), \sigma_i = Rep\left(B_i^{'}, \delta_i\right), w_i = s_i \oplus h(pw_i \| \sigma_i)$. The USB client checks if $e_i = h(w_i \| h(pw_i \| \sigma_i))$ holds. If not, then it rejects; otherwise, selects $a \in_R Z_p$ and computes aG, $\alpha = h(ID_i || aG || F_n \| w_i)$. It sends $\{ID_i, aG, F_n, \alpha\}$ to AS, where F_n is encrypted file.
AS: Checks if ID_i is valid. If not, then it rejects the requests; otherwise, computes $w_i = h(ID_i \| x)$. If $\alpha = h(ID_i || aG || F_n \| w_i)$ holds, then it generates $b \in_R Z_p$. Computes bG, $sk = b(aG) = abG$, $n = h(x \| F_n)$, $\beta = h(\text{"0"} \| ID_i || aG \| F_n || bG \| n || sk \| w_i)$. Finally, AS sends $\{bG, E_{sk}(n), \beta\}$ to U.
U: Computes $sk = a(bG) = abG$ and decrypts$E_{sk}(n)$. Checks whether$\beta = h(\text{"0"} \| ID_i || aG \| F_n || bG \| n || sk \| w_i)$ holds. If not, then terminates the session. Otherwise, it computes $\gamma = h(\text{"1"} \| ID_i || aG \| F_n || bG \| n || sk \| w_i)$ and sends it to AS.
AS: Checks whether $\gamma = h(\text{"1"} \| ID_i || aG \| F_n || bG \| n || sk \| w_i)$ holds. If yes, then authenticated otherwise it terminates the session.

Key agreement phase

Both AS and U agree on the session key, $K = h(ID_i \| n)$, which can be used to secure data-in-transit (e.g. files transferred during the transmission between USB MSD and USB client).

Cryptanalysis of the scheme of He et al

In this section, the security of He et al.'s scheme is analyzed.

The user anonymity attack

As it can be seen, that in He et al.'s scheme, U sends ID_i during the Verification and Data Encryption Phase in the plaintext format. An attacker can easily pick the identity ID_i of the user from the message $\{ID_i, aG, F_n, \alpha\}$ travelling over the network. A user in healthcare application can be a patient or a medical professional such as a doctor, nurse etc. In case the user is a patient and it is patient's identity which is picked by the attacker then it can lead to many unpleasant situations. The attacker can initiate a re-registration request towards the server. Out of success or otherwise, the attacker can impersonate a user. Impersonation by the attacker as a user may lead to false updation of health records thereby causing wrong treatment of patient. On watching the frequency of the messages sent by the user to the server containing identity in plaintext, the attacker can reveal some information such as the disease to which user suffers. If the revealed disease happens to be private, it may lead to an embarrassing situation for the user [32, 33]. Therefore, it is not preferable in sensitive applications such as healthcare. The design of the scheme should be such that the server is able to validate the user without the identity of the user being available in plaintext in any of the messages exchanged over insecure networks.

The session specific temporary information attack

To resist this attack, the scheme should be designed in such a manner that the leakage of any temporary but session specific information (such as the random numbers of that session) should not lead to any security breach of the scheme. In He et al.'s scheme, if the temporary information, i.e., the random numbers a & b, are leaked then the attacker A performs the following steps.

A: It computes $sk = abG$ and decrypts $E_{sk}(n)$ to get n. As ID_i is available from the Verification and Data Encryption Phase, the attacker A can easily compute $K = h(ID_i \| n)$.

Late detection of replay attack

If an attacker A replays $\{ID_i, aG, F_n, \alpha\}$ then AS will not be able to detect it in an immediate step. Although AS will detect it in the final step of the Verification and Data Encryption Phase, which would cost 5 hashing +1 scalar multiplication +1 exponent operation at AS. Thus, overall it costs 24.3 *ms* to detect the replay attack. Also, the attacker A can replay this message at any time in the future. If the attacker continues or simultaneously sends the multiple messages, this would result in levying heavy computational overhead on AS. In the proposed scheme, the timestamp-based notion is used to prevent the replay of a message after certain time.

The forward/backward secrecy attack

To resist this attack, an attacker should fail to get the past or future session key even if the long-term secrets of a user or a server are compromised. In the scheme of He et al., if the secret key x of AS is compromised, then the attacker A does the following.

> **A:** It gets ID_i, F_n from the past sessions of the *Verification and Data Encryption Phase* and calculates $n = h(x\|F_n)$. Finally, it calculates key $K = h(ID_i\|n)$. Same is also true for the future sessions.

The proposed scheme

In this section, we present our scheme for smart healthcare utilizing USB. The user in the scheme is either patient or medical professional. Our scheme has two entities, a user (U) and an authentication server (AS). The user can be a patient seeking treatment, downloading prescription, accessing his own medical history, etc. The user can also be a doctor handling various patients and providing them treatment, prescribing medicines, accessing medical history of a patient or vital health signs of a critical patient, etc. The user can also be a medical professional such as nurse, attendant, dietician, to assist the doctor by providing care instructions to the patients and handling follow-up queries of patients with nominal diseases. The authentication server is the server dedicated to EPR systems maintaining patients' health-data electronically. In order to access health-data, the user in any role will send his request/query to the authentication server installed and maintained in a smart hospital or in community health-centre to facilitate smart healthcare. Then the server will provide the necessary services to the user. For this, each user will first of all regiser itself at the server so that at the time of taking services, the server can check the legitimacy of trhe user. The user and the server agree upon a session key once each one mutually authenticate the other. Using the session key, they can communicate with each other confidentially. Innaddition, the user is able to freely update its password whenever required.

Our scheme is not only secure against the attacks found on He et al.'s scheme, but is also robust against many other attacks. It is noticeable that in the scheme of He et al. there is no phase for the users to change their password. Thus, it fails when the user's credential is compromised. Thus, in the proposed scheme, the password change phase is also incorporated to deal with this issue. The Bio Hash [21] function is used in the proposed scheme which is also used in the research of biometric devices and in the enhanced version of fuzzy extractor.

The registration phase

The user U has the identity ID_i, password pw_i and biometric identity B_i. The authentication server AS has the secret parameter x and the public parameter $P_{pub} = xG$. This phase has following steps and its pictorial representation is given in Fig. 1.

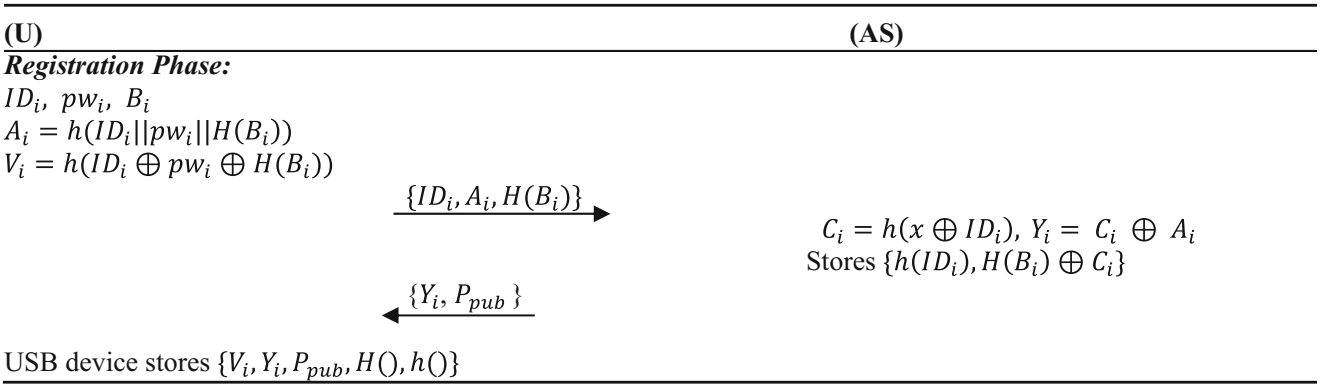

Fig. 1 Registration phase

U: U inputs ID_i, pw_i, B_i, computes $A_i = h(ID_i \| pw_i \| H(B_i))$ and $V_i = h(ID_i \oplus pw_i \oplus H(B_i))$, and then submits $\{ID_i, A_i, H(B_i)\}$ to AS.
AS: AS computes $C_i = h(x \oplus ID_i)$, $Y_i = C_i \oplus A_i$ and stores $\{h(ID_i), H(B_i) \oplus C_i\}$ in a table. Then it sends Y_i and $P_{pub}$to U.
U: Finally, the USB device stores $\{V_i, Y_i, P_{pub}, H(), h()\}$.

The verification and data encryption phase

This phase is required for mutual authentication as well as to send data to the USB MSD. Steps are as follows and its pictorial representation is given in Fig. 2.

U: U inserts USB MSD into the USB port, then inputs ID_i, pw_i, and B_i. The USB device checks if $V_i = h(ID_i \oplus pw_i \oplus H(B_i))$ holds. If so then computes $A_i = h(ID_i || pw_i || H(B_i))$, $C_i = Y_i \oplus A_i$, and randomly selects $r_i \in_R Z_p$. Then it computes $R_i = r_i G$, $E_i = r_i P_{pub}$, $D_i = (ID_i) \oplus h(E_i)$, $F_i = h(C_i \| T_1 \| E_i \| H(B_i))$, where T_1 is the current timestamp. It sends $\{D_i, R_i, F_i, T_1\}$ to AS.
AS: AS Verifies if $T_2 - T_1 < \triangle T$, where T_2 is the received timestamp. It computes $E_i = xR_i = xr_iG$ and $ID_i = D_i \oplus h(E_i)$ and $h(x \oplus ID_i)$. Next it searches for $h(ID_i)$ in the table, obtains the corresponding $H(B_i) \oplus h(x \oplus ID_i)$ and retrieves $H(B_i)$. It verifies if $F_i = ? h(C_i \| T_1 \| E_i \| H(B_i))$. AS generates r_s and computes $R_s = r_sG$, $E_s = r_sR_i = r_sr_iG$, $sk = h(E_s \| H(B_i) || ID_i \| E_i)$, $H_i = h(ID_i \| sk \| T_2 \| R_s)$. Finally, AS sends $\{R_s, H_i, T_2\}$ to U.
U: U verifies if $T_3 - T_2 < \triangle T$. Here T_3 is the received timestamp of message from AS, computes $E_s = r_iR_s = r_ir_sG$ and $sk = h(E_s \| H(B_i) || ID_i \| E_i)$, and *verifies* $H_i = ? h(ID_i \| sk \| T_2 \| R_s)$. If it does not hold, then it rejects it; otherwise AS is authenticated.

Key agreement phase

If mutual authentication succeeds, than U accepts *sk* as the session key for subsequent data transfer, such as $E_{sk}(file)$ and $D_{sk}(file)$ to encrypt and decrypt files transfer.

The password change phase

When U thinks that the password pw_i is compromised then by using this phase, U can change it with a new password pw_{new} as follows and its pictorial representation is given in Fig. 3. U does not require interaction with AS to do this.

U: As in the the Verification and Data Encryption Phase, U verifies if $V_i = h(ID_i \oplus pw_i \oplus H(B_i))$. If verification

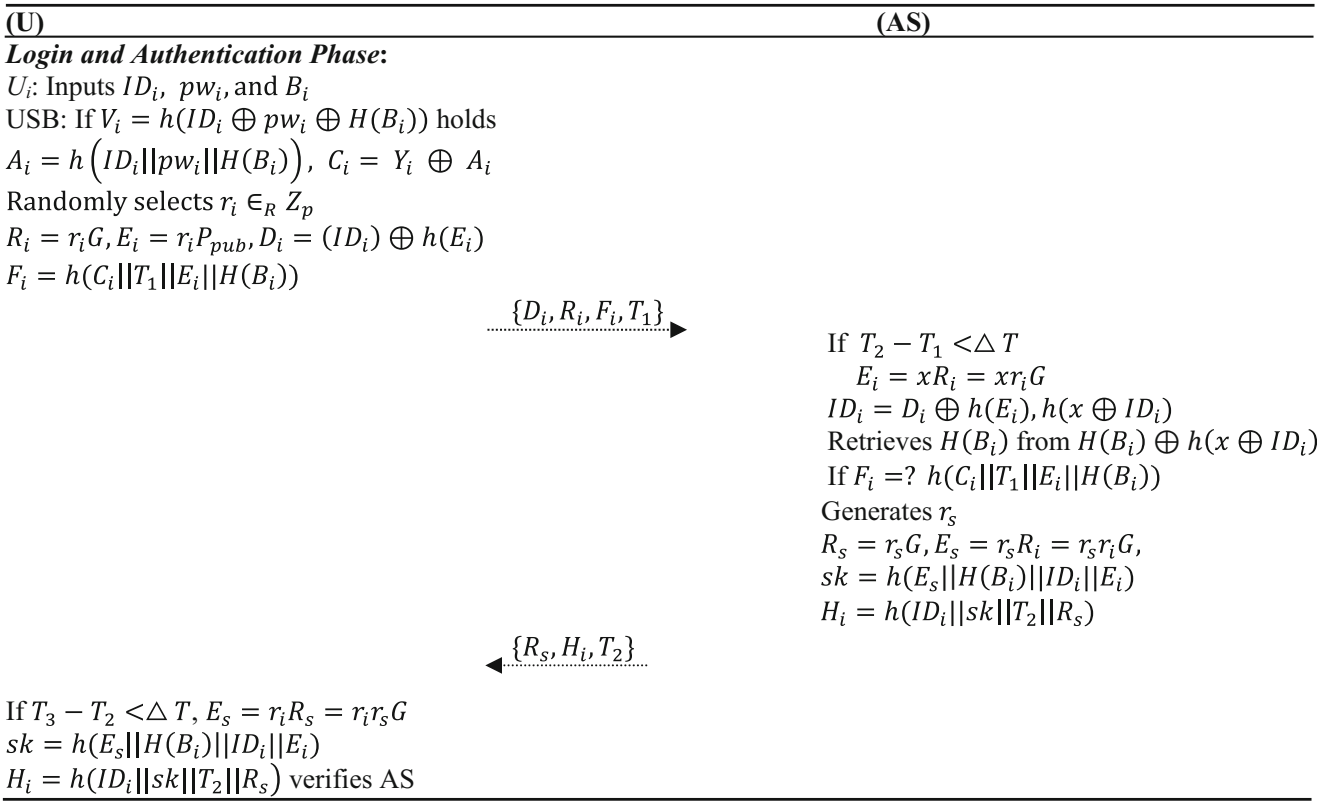

Fig. 2 Verification and Data Encryption Phase

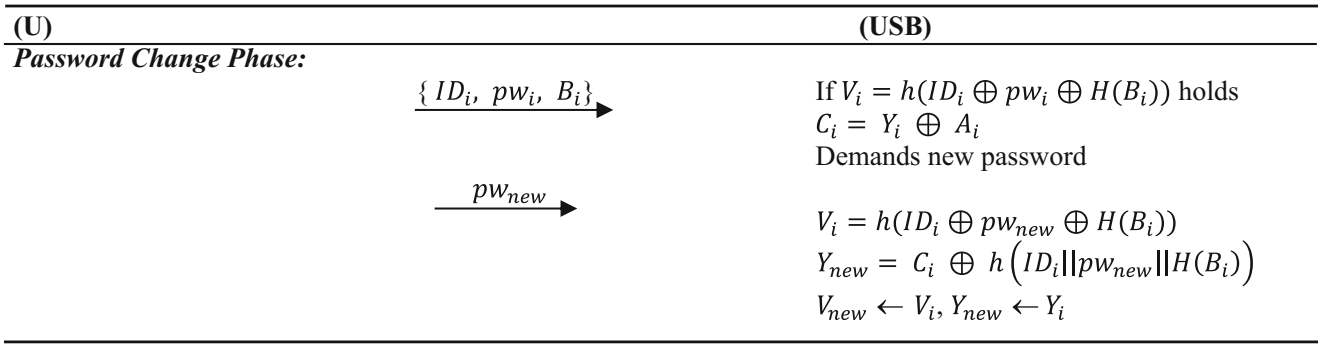

Fig. 3 Password Change Phase

holds, it computes $C_i = Y_i \oplus A_i$. Then asks for new password.

On receiving the new password pw_{new}, USB device computes $V_i = h(ID_i \oplus pw_{new} \oplus H(B_i))$ and $Y_{new} = C_i \oplus h(ID_i \| pw_{new} \| H(B_i))$. Then, it replaces V_i with V_{new} and Y_i with Y_{new}.

Security analysis

Here, first we formaly analyze the security of the proposed scheme based on ROM Model. Then we heuristically explain the robustness of the scheme.

The scheme is secure under rom model

Definition 1 Let *q and rin* Z_p, *a trial* $Exp_G^{cdh}(A)$ calculates *qP and rP, then present qPand rP to A. A trial* $Exp_G^{cdh}(A)$ *outputs 1* if $Z = qrP$ *and 0,* if not. Let $Adv_G^{cdh}(A) = Pr[Exp_G^{cdh}(A) = 1]$ as gain of adversary in breaking EC-CDH assumption. The advantage function of the group is given by $Adv_G^{cdh}(t) = max_A\{Adv_G^{cdh}(A)\}$, where time complexity is at most *t*.

Definition 2 Instances $\prod_S^i$ is believed to be a partner of the instance $\prod_U^i$ provided the following hold:

(1) *Both* $\prod_S^i$ *and* $\prod_U^i$ *agree;*
(2) $\prod_S^i$ *and* $\prod_U^i$ *split the common session identifications (sid);*
(3) Identification of partner for $\prod_S^i$ *and* $\prod_U^i$ and vice-versa.

Definition 3 An event $\prod_U^i$ *is* measured fresh if the below given rules hold:

(i) *It has believed;*
(ii) $\prod_U^i$ *and* $\prod_S^i$ *are locked;*
(iii) *Honest parties holding above instances.*

Definition 4 *The authentication scheme* $\prod$ *exexutes through* A, *where right to use to the Execute, Send, and Test oracles, and requests at most one Test query to the fresh instance of the honest user. Suppose* b^0 is his output, *if* $b^0 = b$, *where b is the hidden bit chosen through Test oracle. Suppose D is the password dictionary of client with size* $|D|$. *Subsequently, advantage of* A *to violate semantic security of the authentication scheme* $\prod$ *is given by:*

$$Adv_{\prod,D}(A) = |2Pr\left[b' = b\right] - 1|$$

Here, $\prod$ is semantically secure *if* $Adv_{\prod,D}(A)$ is insignificantly larger than $O(q_s)/|D|$, *where* q_s denotes number of active sessions.

Theorem Define *D* as the dictionary of uniformly distributed probable passwords of size $|D|$, $\prod$ a proposed authentication scheme and A as the adversary versus the semantic security in time period t. If CDH is satisfied, then:

$$Adv_{\prod,D}(A) = \frac{2q_h^2}{p} + \frac{2q_s}{p} + \frac{(q_s + q_e)^2}{p} + 2q_h Adv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{2q_s^2}{D}$$

where $Adv_G^{cdh}(A)$ denotes the probability of success to solve CDH assumption by A. q_s denotes the frequency of Send queries, q_e denotes the frequency of Execute queries, *and* q_h denotes the frequency of queries raised by random oracle.

Proof Here is described a series of hybrid games, beginning with the actual attack and finishing up in game where A has no gain/advantage. For each game $G_i (0 \le i \le 5)$, we define by $Succ_i$ an event in which A correctly guesses the bit *b* in the test-query.

G_0: It corresponds to actual attack in ROM, where altogether instances of *U* and *AS* are modeled as real-

execution in random oracle. By classification of event $Succ_i$, where A suitably estimates involvement of b within Test-query.

$$Adv_{\prod,D}(A) = 2\left|Pr[Succ_0] - \frac{1}{2}\right| \quad (1)$$

G_1: It is like the last discussed game G_0 with addition of hash oracles h simulation by keeping hash lists $List_h$ with entries of type *(Inp,Out)*. On hash query to the record *(Inp,Out)* in $List_h$, the algorithm returns Out. Else, randomly selects Out $\in \{0,1\}$, sends to A and records new *(Inp,Out)* into $List_h$. The Execute, Reveal, Send, Corrupt, and Test oracles are simulated as in the actual attack where A asks for the simulation of different polynomial number of queries. We find that the game is perfectly indistinguishable from the real attack from the perspective of A. So, it leads to:

$$Pr[Succ_1] = Pr[Succ_0] \quad (2)$$

G_2: Here, simulation of whole oracles is alike to game G_1 excepting game is ended if collision arises in simulation of records $<ID_i \oplus h(E_i),\ R_i,\ h(C_i||T_1||E_i\|H(B_i)),\ T_1>$ and $<R_s,\ h(ID_i\|sk||T_2||R_s),\ T_2>$. As per birthday paradox, the probability of collisions of hash oracles simulation is at most $\frac{q_h^2}{2p}$. Likewise, probability of transcripts simulations collisions is at most $\frac{(q_h+q_e)^2}{2p}$. As C_i was identified uniformly at random, we get:

$$|\Pr[Succ_2] - \Pr[Succ_1]| = \frac{q_h^2}{2p} + \frac{(q_h+q_e)^2}{2p} \quad (3)$$

G_3 Its simulation is similar to preceding game excluding that game will be terminated if A can suitably guess E_i and E_s without enquiring oracle h. It is indistinguishable with the earlier game except instances $\prod_U^i$ and $\prod_{AS}^i$ *which* discard a legal authentication value. Therefore, we get:

$$|\Pr[Succ_3] - \Pr[Succ_2]| = \frac{q_h}{2p} \quad (4)$$

G_4: Here, session key is guessed without requesting corresponding oracle h so that it grows independent of PW and $r_i xG$. We modify the technique with previous game unless A queries h on $h(C_i||T_1||E_i\|H(B_i))$. So, $Adv_G^{cdh}(A) \geq \frac{1}{q_h}|\Pr[Succ_4] - \Pr[Succ_3]| - \frac{1}{p}$, that is, the variance between G_4 and G_3 as:

$$|\Pr[Succ_4] - \Pr[Succ_3]| \leq q_h Adv_G^{cdh}(A) + \frac{q_h}{p} \quad (5)$$

G_5: This game is similar to the game G_4, the only difference is that that in Test query, the game is terminated if A

Table 2 Attack Based Analysis

Scheme Attack	Yang et al. [2]	He et al. [20]	Proposed Scheme
Forward/Backward Secrecy	No	No	Yes
Session Specific Temporary Information	No	No	Yes
User Anonymity	No	No	Yes
DoS	No	Yes	Yes
Mutual authentication	Yes	Yes	Yes
Impersonation	Yes	Yes	Yes
Stolen Verifier	Yes	Yes	Yes
Password Guessing	No	Yes	Yes
Replay	No	No (Partial)	Yes

asks a hash function query with $h(ID_i \| sk \| T_2 \| R_s)$ without asking for corresponding oracle h so as to make it independent of ephemeral key $r_i r_s G$. A gets the session key $sk = h(E_s \| H(B_i) \| IDi \| Ei)$ by hash function query with probability at most $\frac{q_h^2}{2p}$. This gives:

$$|\Pr[Succ_5] - \Pr[Succ_4]| \leq \frac{q_h^2}{2p} \quad (6)$$

In case, A does not make any h query using the correct input, it will have no advantage in making distinction between the actual session key and the random one. Further, if Corrupt(U,2) (the corrupt query) is made then this implies that Corrupt(U,1) (the password corrupt query) is not made. So, the probability of A mounting off-line password guessing attack is $\frac{q_s^2}{D}$.

Now, merging the eq. 1, 2, 3, 4, 5 and 6, we get:

$$Adv_{\prod,D}(A) = \frac{2q_h^2}{p} + \frac{2q_s}{p} + \frac{(q_s + q_e)^2}{p} + 2q_h Adv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{2q_s^2}{D}$$

Informal security assessment

Password guessing

The scheme is said to withstands this attack if attacker A fails to guess the password using MSD. Let it be said, A gets A_i, C_i from the USB MSD. However, to verify a guessed password $pw_i^{'}$, A requires ID_i and B_i which is not possible as B_i is biometrics. Thus, the proposed protocol is resists the password guessing attack.

The DoS attack

The scheme is vulnerable to this attack if a legal user is denied access to the entitled services due to matching problem of its own biometrics. As in the proposed protocol, the specific hash function called BioHash has been used, which takes care of the input biometric of the same person even though it is not exact. So, the proposed protocol is secure against the DoS attack.

The replay attack

Let us assume that the attacker replays $\{D_i, E_i, F_i, T_1\}$. However, as the proposed protocol uses the timestamp-based technique for the message interaction, the attacker A is not able to fool the opposite entity after a specified time limit ΔT. Further, AS can detect the replay with 1 hashing and 1 exponent only, which is much less as compared to He et al.'s scheme. So, the proposed protocol is secure against the reply attack.

The stolen verifier

The scheme is said to be free from this attack, if compromised table stored at AS does not leads to the compromised of user's identity or previous sessions keys. As the stored values are $h(ID_i)$ & $H(B_i) \oplus h(x \oplus ID_i)\}$, the attacker cannot retrieve ID_i, B_i due to the one-way flow of hash function and unavailability of the secret x of AS. Also, the attacker doesn't get the key K as it requires r_i, r_s too along with (B_i) and ID_i. Thus, the proposed protocol withstands the stolen verifier attack.

The impersonation attack

The scheme is vulnerable to this attack when an attacker A can pretend to be a valid user to AS. One can see that the attacker A requires to know the details ID_i, pw_i, B_i of the user's, which is not possible. We have already discussed that the replay of the message $\{D_i, E_i, F_i, T_1\}$ is either not possible or early detectable. Moreover, using the lesser communication, AS can detect it. Thus, the proposed protocol is free from impersonation attack.

The mutual authentication

The scheme is said to achieve the mutual authentication if AS and U mutually authenticate each other. AS verifies the system

Table 3 Timing analysis

Task	Time (in milliseconds)
T_h	0.32
T_H	0.01
T_M	17.1
T_E	19.2
T_F	17
T_{sym}	5.6

Table 4 Timing (in ms) Analysis

Scheme	User	Authentication Server	Total
[2]	83.36	121.4	204.8
[19]	41.4	41.08	82.4
[20]	58.5	41.08	99.5
This Work	54.2	69.68	123.88

Table 5 Performance Analysis

Scheme	User	Authentication Server	Total
[2]	$4T_E + 3T_h + 1T_{sym}$	$6T_E + 2T_h + 1T_{sym}$	$10T_E + 5T_h + 2T_{sym}$
[19]	$2T_E + 5T_h + 1T_{sym}$	$2T_E + 4T_h + 1T_{sym}$	$4T_E + 9T_h + 2T_{sym}$
[20]	$2T_E + 5T_h + 1T_{sym} + 1T_{FE}$	$2T_E + 4T_h + 1T_{sym}$	$4T_E + 9T_h + 2T_{sym} + 2T_{FE}$
This Work	$9T_h + 2T_H + 3T_M$	$4T_h + 4T_M$	$13T_h + 2T_H + 7T_M$

user by $F_i = h((h(ID_i) \oplus x)||T_1||R_i||H(B_i))$ and the same way U can verify the AS by $H_i = h(ID_i||sk||T_2||R_s)$. Also, the key on the user side is also verified in this process. It is clear that He et al.'s scheme fails to verify the generated key at the user side. Thus, the proposed protocol is providing mutual authentication.

The user anonymity

Scheme is achieving this if identity of the user is not sent in the plaintext via public channel. As one can see that U and AS both are using ID_i of U protected by the one-way flow of hash function in the messages communicated over public channel. Thus, the attacker A fails to identitfy the user and thus the scheme is providing the user anonymity.

Session specific temporary information

The scheme withstands this attack if compromise of short term secrets (i.e. generated during session) fails to compromise the session key. As it can be seen, even if the random values r_s & r_i are leaked, they do not allow the attacker to compute the session key sk as we also require $H(B_i)$. $H(B_i)$ is unique to the user and can be generated by the user only or can be retrieved by the AS. Thus, the proposed protocol withstands this attack.

The forward/backward secrecy

If compromise of the secrets of entities does not leads to the compromise the previous or future session keys, then the scheme is said to withstand this attack. As it can be seen the key sk is computed on r_s, r_i and $H(B_i)$, thus compromise of ID_i, pw_i and x does not compromise the sk. So, the proposed protocol is secure against this attack.

Performance analysis

In this section, the analysis of the proposed scheme against He et al.'s [20], Lee et al.'s [19] and Yang et al.'s [2] schemes is given. For notations, refer to Table 1.

In the Table 2, the exhaustive survey of the existing and the proposed scheme is given based on various attacks. The "YES" in the table shows that the scheme withstands attack, while "NO" says that the scheme fails to withstand the attack.

Refer to Table 3 for the execution time of each operation. The time for T_H is taken from [19, 21].

In Table 4, the timing analysis is given.

In Table 5, the endurance of the proposed scheme towards previous competing schemes based on the various phases is given.

It is evident from Table 4 that our scheme is less time consuming at the user side and more time consuming at the AS side as compared to that of He et al's scheme. It is visible from Table 2 that our scheme withstands all the attacks which have adverse effect on the functionality of He et al.'s and Yang et al.'s schemes. This clearly justifies the superiority of our proposed scheme over the two aforementioned schemes.

Conclusion

In this paper, we revealed a previously unknown design flaw in the scheme of He et al. meant for USB MSD implementation. We have shown that the user is not anonymous in their scheme. We have also explained the vulnerability of He et al.'s scheme to session specific temporary information attack, forward/backward secrecy attack and late detection of replay attack. We then presented our new scheme themed on EPR systems for smart healthcare defying the weakness identified in He et al.'s scheme, and demonstrated its excellent security charcteristics through heuristic arguments and security proofs using ROM model. We have also comparatively evaluated the performance of the proposed scheme with some contemporary schemes, to demonstrate that harnassing the benefits of USB MSD it is suitable for implementation in smart healthcare environment.

In future, we will focus on enforcing on demand security with the inclusion of risk based authentication (RBA), without hindering the easy-going authentication set-up under routine circumstances. It will put a check on impersonation problems and data theft. Surely, this add-on will highly benefit the healthcare industry.

Compliance with ethical standards

Conflict of interest All the authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Al-Zarouni, M., The reality of risks from consented use of USB devices. in Proc. 4th in Proc. 4th Australian Information Security Management Conference, pp. 312–317, 2006.
2. Yang, F. Y., Wu, T. D., and Chiu, S. H., A secure control protocol for USB mass storage devices. IEEE Transactions on Consumer Electronics. 56(4):2239–2243, 2010.
3. Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M. K., and Chaturvedi, A., Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. Journal of medical systems. 38(5): 41, 2014.
4. Moon, J., Choi, Y., Kim, J., and Won, D., An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. Journal of medical systems. 40(3):70, 2016.
5. Khan, M. K., and Kumari, S., Cryptanalysis and improvement of "an efficient and secure dynamic ID-based authentication scheme for telecare medical information systems". Security and Communication Networks. 7(2):399–408, 2014.
6. Hou, J. L., and Yeh, K. H., Novel authentication schemes for IoT based healthcare systems. International Journal of Distributed Sensor Networks. 11(11):183659, 2015.
7. Lu, Y., Li, L., Peng, H., and Yang, Y., An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. Journal of medical systems. 39(3):32, 2015.
8. He, D., Kumar, N., Chen, J., Lee, C. C., Chilamkurti, N., and Yeo, S. S., Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems. 21(1):49–60, 2015.
9. Wu, F., Xu, L., Kumari, S., and Li, X., An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Systems. 23(2):195–205, 2017.
10. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., and Li, X., Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems. Journal of medical systems. 39(11):140, 2015.
11. Li, X., Niu, J., Karuppiah, M., Kumari, S., and Wu, F., Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications. Journal of medical systems. 40(12):268, 2016.
12. Li, C. T., Lee, C. C., Weng, C. Y., and Chen, S. J., A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. Journal of medical systems. 40(11):233, 2016.
13. Irshad, A., Sher, M., Nawaz, O., Chaudhry, S. A., Khan, I., and Kumari, S., A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme. Multimedia Tools and Applications. 76(15):16463–16489, 2017.
14. Li, X., Wu, F., Khan, M. K., Xu, L., Shen, J., and Jo, M., A secure chaotic map-based remote authentication scheme for telecare medicine information systems. Future Generation Computer Systems. 84:149–159, 2018.
15. Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V., and Choo, K. K., Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 129:429–443, 2017.
16. Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., and Shen, J., A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 82:727–737, 2018.
17. Wu, F., Li, X., Xu, L., Kumari, S., and Sangaiah, A. K., A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. Computers & Electrical Engineering. 68:107–118, 2018.
18. Chen, B., QIN, C., YU, L., and JIANG, P., A secure access authentication scheme for removable storage media. Journal of information & Computational Science. 9(15):4353–4363, 2012.
19. Lee, C. C., Chen, C. T., Wu, P. H., and Chen, T. Y., Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices. IET Computers & Digital Techniques. 7(1):48–55, 2013.
20. He, D., Kumar, N., Lee, J. H., and Sherratt, R. S., Enhanced three-factor security protocol for consumer USB mass storage devices. IEEE Transactions on Consumer Electronics. 60(1):30–37, 2014.
21. Li, C. T., and Hwang, M. S., An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and computer applications. 33(1):1–5, 2010.
22. Li, X., Peng, J., Niu, J., Wu, F., Liao, J., and Choo, K. R., A robust and energy efficient authentication protocol for industrial internet of things. IEEE Internet of Things Journal. 5(3):1606–1615, 2018.
23. Amin, R., Islam, S. H., Gope, P., Choo, K.-K. R., and Tapas, N., Anonymity preserving and lightweight multi-medical server authentication protocol for telecare medical information system. *IEEE Journal of Biomedical and Health Informatics* In press, 2018. https://doi.org/10.1109/JBHI.2018.2870319.
24. J. Holdsworth, W.B. Glisson and K-K R. Choo, Medical device vulnerability mitigation effort gap analysis taxonomy. Smart Health, In press, https://doi.org/10.1016/j.smhl.2017.12.001, 2017.
25. Chen, L., Lee, W. K., Chang, C. C., Choo, K.-K. R., and Zhang, N., Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems 95:420–429, 2019.
26. Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., and Vasilakos, A. V., An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Computers and Electrical Engineering 69:534–554, 2018.
27. S. F. Aghili, H. Mala, M. Shojafar, P. Peris-Lopez, LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT, Future Generation Computer Systems, Elsevier, In press, doi: https://doi.org/10.1016/j.future.2019.02.020, 2019.
28. Masdari, M., and Ahmadzadeh, S., A survey and taxonomy of the authentication schemes in telecare medicine information systems. Journal of Network and Computer Applications. 87:1–9, 2017.
29. Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., and Aslam, B., A survey of authentication schemes in telecare medicine information systems. Journal of medical systems. 41(1):14, 2017.

30. Chen, T. L., Chung, Y. F., and Lin, F. Y., A study on agent-based secure scheme for electronic medical record system. Journal of medical systems. 36(3):1345–1357, 2012.
31. Dodis, Y., Reyzin, L., and Smith, A., Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: InInternational conference on the theory and applications of cryptographic techniques 2004 may 2. Berlin, Heidelberg: Springer, 523–540.
32. Zhang, S., Li, X., Tan, Z., Peng, T., and Wang, G., A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. Future Generation Computer Systems. 94:40–50, 2019.
33. Zhang, S., Choo, K. R., Liu, Q., and Wang, G., Enhancing privacy through uniform grid and caching in location-based services. Future Generation Computer Systems. 86:881–892, 2018.