MOBILE & WIRELESS HEALTH

Analysis of Security Protocols for Mobile Healthcare

Mohammad Wazid[1] · Sherali Zeadally[2] · Ashok Kumar Das[1] · Vanga Odelu[3]

Received: 30 June 2016 / Accepted: 5 September 2016 / Published online: 17 September 2016

Abstract Mobile Healthcare (mHealth) continues to improve because of significant improvements and the decreasing costs of Information Communication Technologies (ICTs). mHealth is a medical and public health practice, which is supported by mobile devices (for example, smartphones) and, patient monitoring devices (for example, various types of wearable sensors, etc.). An mHealth system enables healthcare experts and professionals to have ubiquitous access to a patient's health data along with providing any ongoing medical treatment at any time, any place, and from any device. It also helps the patient requiring continuous medical monitoring to stay in touch with the appropriate medical staff and healthcare experts remotely. Thus, mHealth has become a major driving force in improving the health of citizens today. First, we discuss the security requirements, issues and threats to the mHealth system. We then present a taxonomy of recently proposed security protocols for mHealth system based on features supported and possible attacks, computation cost and communication cost. Our detailed taxonomy demonstrates the strength and weaknesses of recently proposed security protocols for the mHealth system. Finally, we identify some of the challenges in the area of security protocols for mHealth systems that still need to be addressed in the future to enable cost-effective, secure and robust mHealth systems.

Keywords Attack · Communication cost · Computation cost · Mobile healthcare · Mobile device · Protocol · Security · Threat

Introduction

In the last two decades, we have seen remarkable advances in the capabilities and performance of Information Communication Technologies (ICTs). The decreasing costs of ICTs have also led to their wide proliferation and ubiquitous use in various sectors including, health, transportation, finance, education, entertainment, tourism, commerce, agriculture, food, etc. In fact today, ICTs have become an integral part of our daily lives in practically everything we do and they have transformed the way we communicate and stay in touch with each other. Today, ICTs enable a wide range of services, higher efficiency/productivity, and increased convenience through the emergence of all kinds of mobile devices (smartphones, tablets, etc.). These mobile devices

This article is part of the Topical Collection on *Mobile & Wireless Health*

✉ Ashok Kumar Das
iitkgp.akdas@gmail.com; ashok.das@iiit.ac.in

Mohammad Wazid
mohammad.wazid@research.iiit.ac.in

Sherali Zeadally
szeadally@uky.edu

Vanga Odelu
odelu.vanga@gmail.com; odelu.vanga@iiits.in

[1] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India

[2] College of Communication and Information, University of Kentucky, Lexington, KY 405 06, USA

[3] Department of Computer Science and Engineering, Indian Institute of Information Technology, Sri City, Chittoor 517 588, Andhra Pradesh, India

are playing a fundamental role in mHealth which aims to improve healthcare quality, make healthcare access more convenient, and reduce healthcare costs [2, 3].

Significant improvements in the performance and capabilities of mobile devices in recent years have made them suitable for: real-time monitoring of a patient's vital signs, collecting the patient's health data (such as patient's pulse rate, temperature, respiration rate, blood glucose level, blood pressure, etc.) using different types of wearable sensors, transmitting the health data to a medical server, providing remote prescriptions to patients, delivering healthcare information to doctors, researchers, and other healthcare professionals. According to a recent report [4], the mobile healthcare industry is projected to reach 26 billion dollar industry by 2017. Over 97,000 health and fitness related mobile applications are currently available on Google Play and Apple App from which 4 million downloads occur every day [4].

Architecture of mHealth system

The architecture of a typical mHealth system is shown in Fig. 1 (adapted from [1]). In this system there are various types of users of medical data and they include patients (as well as their relatives), doctors, nursing staff and medical researchers. Different types of wearable sensors on the patient are used for monitoring blood glucose level, blood pressure, pulse rate, electromyography (EMG), electrocardiogram (ECG), etc. After the sensed medical data is processed it is transmitted to some medical data server using the patient's mobile device (such as a smartphone). The health of a patient is monitored in real-time by healthcare experts (for example, doctor) remotely. Doctors can take decisions and issue prescriptions to the nursing staff based on the remote diagnosis and the health data received from the patient. Medical data researchers are also interested in accessing the health data of patient. For example, if a patient suffers from blood cancer, the medical researcher can analyze and compare the results of the current chemotherapy treatment with those of the previous chemotherapy treatment that was given to the patient. The researcher can also set some chemotherapy medicine markers on the basis of the analysis performed, which will be helpful in future blood cancer treatments [5–9].

Applications of mobile healthcare

The various types of mobile healthcare applications can be broadly classified as follows [2, 3, 10, 11]:

- Remote monitoring of patient's health by healthcare experts as well as by the relatives of the patient.
- Doctors use the health data transmitted from the patient's monitoring devices to provide remote consultations.
- Medical prescriptions issued by doctors are accessed and used by nursing staff and pharmacies for dispensing the required medicine.
- Medical data researchers use health data in their research and development works.
- The mHealth system's data is used in medical education and training.
- The mHealth system is also used for managing various tasks such as scheduling appointments of patients with doctors, and scheduling the meetings of healthcare experts, etc.

Our contributions

The contributions of this paper include:

- We first discuss the security requirements, issues and threats to the mHealth system.

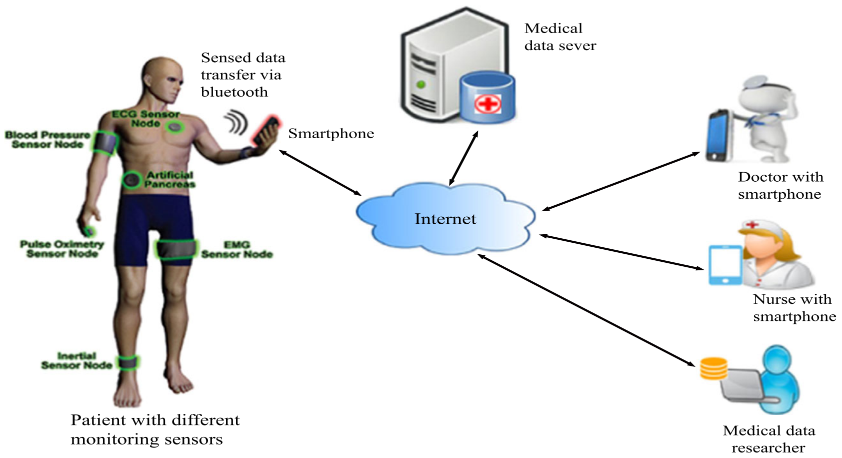

Fig. 1 Architecture of mHealth system (Adapted from [1])

- We then present a taxonomy of recently proposed security protocols for mHealth system based on the features they support and possible attacks, computation cost and communication cost. The detailed taxonomy demonstrates the strength and weaknesses of recently proposed security protocols for the mHealth system.
- We also identify some of the challenges in the area of security protocols for mHealth systems that still need to be addressed in the future to enable secure and efficient mHealth systems.

The rest of the paper is organized as follows. We discuss various security issues with mobile healthcare in the next section. This is followed by a section on the taxonomy of recently proposed security protocols for mHealth. In the following section, we discuss some future challenges that still need to be addressed in the area of security protocols for mHealth systems. Finally, we make some concluding remarks in the last section.

Mathematical preliminaries

In this section, we briefly discuss the following cryptographic primitives needed for analyzing several security protocols for mobile healthcare applications.

Elliptic curve and its properties

Let a and $b \in Z_p$, where $Z_p = \{0, 1, \ldots, p-1\}$ and $p > 3$ be a prime, such that $4a^3 + 27b^2 \neq 0 \pmod p$. A non-singular elliptic curve $y^2 = x^3 + ax + b$ over the finite field $GF(p)$ is the set $E_p(a, b)$ of solutions $(x, y) \in Z_p \times Z_p$ to the congruence

$$y^2 = x^3 + ax + b \pmod p,$$

where a and $b \in Z_p$ are constants such that $4a^3 + 27b^2 \neq 0 \pmod p$, together with a special point $\mathcal{O}$ called the point at infinity or zero point.

The condition $4a^3 + 27b^2 \neq 0 \pmod p$ is necessary and sufficient to ensure that the equation $x^3 + ax + b = 0$ has a non-singular solution [12]. Otherwise, if $4a^3 + 27b^2 = 0 \pmod p$, then the corresponding elliptic curve is called a singular elliptic curve. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points in $E_p(a, b)$. Then $P + Q = \mathcal{O}$ implies that $x_Q = x_P$ and $y_Q = -y_P$. We have $P + \mathcal{O} = \mathcal{O} + P = P$, for all $P \in E_p(a, b)$. In addition, $E_p(a, b)$ forms an abelian or commutative group under an addition modulo p operation.

If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are two points on elliptic curve $y^2 = x^3 + ax + b \pmod p$, $R = (x_R, y_R) = P + Q$ is computed as follows ([13, 14]):

$$x_R = (\lambda^2 - x_P - x_Q) \pmod p,$$
$$y_R = (\lambda(x_P - x_R) - y_P) \pmod p,$$
$$\text{where } \lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} \pmod p, \text{ if } P \neq Q \\ \frac{3x_P{}^2 + a}{2y_P} \pmod p, \text{ if } P = Q. \end{cases}$$

In elliptic curve cryptography, multiplication is defined as repeated additions. For example, if $P \in E_p(a, b)$, then $5P$ is computed as $5P = P + P + P + P + P \pmod p$.

Bilinear pairing

Let q be a large prime and p be a prime such that $q \mid p - 1$. Let G_1 and G_2 be two cyclic groups of prime order q, where G_1 is an additive cyclic group over an elliptic curve $E_p(a, b)$ and G_2 a multiplicative cyclic group over a finite field Z_p.

A bilinear map $e : G_1 \times G_1 \rightarrow G_2$ is a function with the following desirable properties:

Bilinearity: Let $P, Q, R \in G_1$ and $a, b \in Z_p^*$. Then,

$$\begin{aligned} e(P + Q, R) &= e(P, R).e(Q, R), \\ e(P, Q + R) &= e(P, Q).e(P, R), \\ e(aP, bQ) &= e(bP, aQ) \\ &= e(P, Q)^{ab}. \end{aligned}$$

Non-degeneracy Let P be a generator in the group G_1. Then, $e(P, P)$ becomes a generator in the group G_2 such that $e(P, P) \neq 1$.

Computability There exists an efficient algorithm to compute $e(P, Q) \in G_2$ in polynomial time for all $P, Q \in G_1$.

One-way hash function

A cryptographic hash function is an algorithm which accepts a variable length block of data as input and produces a fixed-size bit string known as a hash value or a hash digest. Mathematically, a one-way hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^l$ takes an arbitrary-length input $x \in \{0, 1\}^*$, and produces a fixed-length (say, l-bits) output $h(x) \in \{0, 1\}^l$, called the message digest or hash value. The hash function may be the fingerprint of a file, a message, or other data blocks, and has the following attributes [14].

- h can be applied to a data block of all sizes.

- For any given input x, the message digest $h(x)$ is easy to operate, enabling easy implementation in software and hardware.
- The output length of the message digest $h(x)$ is fixed.
- Deriving the input x from the given hash value $y = h(x)$ and the given hash function $h(\cdot)$ is computationally infeasible. This property is called the *one-way* property.
- For any given input x, finding any other input $y \neq x$ so that $h(y) = h(x)$ is computationally infeasible. This property is referred to as *weak-collision resistant* property.
- Finding a pair of inputs (x, y), with $x \neq y$, so that $h(x) = h(y)$ is computationally infeasible. This property is referred to as *strong-collision resistant* property.

There are many applications of hash functions. For example, in the field of cryptology and information security, notably in digital signatures, Message Authentication Codes (MACs), and other forms of authentication. Thus, a hash function becomes the basis of many cryptographic protocols. One fundamental property of a hash function is that its outputs are very sensitive to small perturbations of its inputs. For example, SHA-1 is a secure hash algorithm [15].

Fuzzy extractor

For biometric authentication, a fuzzy extractor technique is often used. The fuzzy extractor has two procedures: the probabilistic generation function $Gen(\cdot)$ and the deterministic reproduction function $Rep(\cdot)$ [16, 17]. $Gen(\cdot)$ takes the user's personal biometrics Bio_i as input, and then produces a biometric key of length l bits, say $\sigma_i \in \{0, 1\}^l$ and a public reproduction parameter τ_i. $Rep(\cdot)$ takes the biometrics entered by the user, such as Bio' and τ_i as input, provided that the hamming distance $d(Bio'_i, Bio_i) \leq t$, where t is an error tolerance threshold value. The output of $Rep(\cdot)$ is the original biometric key σ_i, that is, $\sigma_i = Rep\left(Bio'_i, \tau_i\right)$.

Biohashing

A bioahshing [18, 19] is used to map a user's biometric features onto user-specific random vectors in order to generate a code, called the biocode and then discretizes the projection coefficients into zero or one. Biocode is as secure as a hashed password.

Chebyshev polynomial and its properties

The Chebyshev polynomial $P_n(x) : [-1, 1] \rightarrow [-1, 1]$ of degree n is defined as

$$P_n(x) = \begin{cases} cos(n \cdot arccos(x)) & \text{if } x \in [-1, 1] \\ cos(n\theta) & \text{if } x = cos\theta, \theta \in [0, \pi]. \end{cases}$$

The Chebyshev polynomial can be also defined recursively as

$$P_n(x) = \begin{cases} 1 & \text{if } n = 0 \\ x & \text{if } n = 1 \\ 2xP_{n-1}(x) - P_{n-2}(x) & \text{if } n \geq 2. \end{cases}$$

The semi-group property of the enhanced Chebyshev polynomial $P_n(x) = 2xP_{n-1}(x) - P_{n-2}(x) \pmod{p}$ holds on the interval $(-\infty, +\infty)$ is as follows [20]:

$$P_r(P_s(x)) \equiv P_{rs}(x) \equiv P_s(P_r(x)) \pmod{p},$$

where $n \geq 2$, $x \in (-\infty, +\infty)$, and p is a large prime number.

Security issues for mobile healthcare

Due to the advancement of wireless and mobile health (mHealth) technologies, it is now possible to perform real-time collection of information in the real-world via wearable sensors. Wearable sensing devices are capable of measuring different health related parameters of a patient, such as blood glucose level, blood pressure, pulse rate, Electromyography (EMG), electrocardiogram (ECG), etc. [8, 21, 22]. Elderly patients often have difficulties moving around as they become old. They can have their health status monitored by wearing sensing devices which can measure various health parameters (as we have mentioned earlier) and send them via the local network and the Internet to some central medical health server for further analysis by healthcare professionals. Currently, several mHealth applications also target healthy people who wear various types of wearable, activity-tracking devices such as "Fitbit One" which monitors their activity/inactivity (for instance, distance traveled, stairs climbed, calories burned, etc.) and transmits the information to an application running on a smartphone [23–25] for further analysis locally or remotely. Although mHealth services provide several health benefits (as we stated earlier) to different people, they also open up a wide range of security and privacy issues that must be addressed by mHealth system designer and implementers [2, 26, 27]. Security in mHealth is vital. This is because many patients have privacy related concerns when it comes to collecting, processing, transmitting, and accessing their personal health data through the mHealth infrastructure that often consists of mobile devices, various network types (Body Area Networks (BANs), Personal Area Networks (PANs), Local Area Networks (LANs), etc.) medical information system, storage, servers, etc. The next section discusses some of the most important security requirements of mHealth.

Security requirements of mHealth

Some of the main security requirements of an mHealth system include [14, 21, 22, 28]:

Confidentiality of mHealth data: This defines how we keep a patient's data private from any unauthorized party. Data of mHealth system can be disclosed by capturing and replaying them, etc. To achieve confidentiality, various data encryption techniques such as Advanced Encryption Standard (AES), RSA, etc. can be used [27, 29].

Integrity of mHealth data: An adversary of mHealth system may attempt to modify the data. Suppose a patient has sent his/her health data to get the required prescription/ treatment from his/her respective doctor(s). If the data is modified by an adversary and a doctor issues a prescription according to the modified data, the patient will not get the required treatment which can further degrade him/her's health condition. This malicious act can be done by the Man-In-The-Middle (MITM) attack. Various data hashing techniques can be used to protect the integrity of the patient's data [15].

Availavbility of the various components of an mHealth system: A patient's data should be available to the genuine users of the mHealth system. Different Denial of Service (DoS) attacks can affect the availability of the patient's data stored at the medical data server. Several techniques have been proposed in the literature based on elliptic curve cryptography, hash function, user biometrics verification, etc. that can be used to maintain the available of the system [30–32].

Authenticity of users of mHealth system: The mHealth data should only be accessed by authorized users of the system. Various attacks such as offline/online password guessing [33] can threaten the authentication mechanisms in place. Techniques such as two-factor authentication [30, 34] and three-factor authentication [35, 36] can be used to restrict access of malicious users to the mHealth system.

Security issues of mHealth

The healthcare data contains the personal information of patients, which needs to be protected in order to keep the system safe and secure [28]. The mHealth system needs to efficiently support several security issues such as access, disclosure, modification, disruption, impersonation, and recording and replaying which are discussed further below.

Access: Legitimate users of the mHealth system are patients, doctors, nursing staffs, and researchers and pharmacists (each with his/her own access rights) [1, 5, 7]. Only these people can access the health data stored at the medical server. An adversary of the mHealth system always seeks to access the server illegally so that he/she can steal the data and misuse it to achieve his/her malicious objective. Sometimes adversaries may sell the stolen patient's medical information to third parties (for example healthcare product manufacturer) which results in the patient receiving unwanted solicitations (for instance, emails, phone calls) from that firm to buy their medical products, which are related to their illness or sometime unwanted products too. Strong protocols such as two-factor authentication (smart card and user password as two factors) [30, 34, 40, 41, 47, 48] and three-factor authentication (smart card, user password, and user biometrics as three factors) [35, 36, 39, 44, 49] are required to strengthen the security of the mHealth system [45, 46].

Disclosure: The confidentiality of the health data stored at the medical server is also a major security issue. If the patient's medical record confidentiality is breached, it can have serious ramifications on the life of the patient. Sometimes the medical records that contain the most personal health information of patients can be disclosed to malicious users, who can share such information around without the consent of the patients concerned. Private health information that is disclosed socially can also cause further harm to the patient's reputation and personal life. For example, in a recent case, a woman was sacked from her job after her personal physician (doctor) sent her health records (containing her history of mental health problems) to her employer [50]. To protect the confidentiality of medical data, data encryption techniques such as AES and RSA [27, 29] etc. can be used.

Modification: An adversary of the mHealth system can modify the health data of patients. For instance, the modified data of the patient cannot be used anymore if the patient has a high level of blood glucose value which has been intentionally modified to a low level by an adversary having unauthorized access to the mHealth data. This type of modification affects the patients as the doctor can recommend the medicines based on the low level of blood glucose. Various hashing techniques can be used to protect against patient's data modifications [15].

Medical server disruption: An adversary of the mHealth system can try to disrupt the services of the system by sending bogus request messages to overload the medical server (for example, a DoS attack) to such an extent that it becomes too busy to reply to requests from legitimate users who are denied access to the mHealth system's services. A malicious user can shut off or alter the settings of an insulin pump without the user's (doctor/nurse) knowledge [51]. There are different types of denial of service attack mechanisms [51–53] that can be launched to disrupt the service of the mHealth system. For example, legacy implantable medical devices (IMD) are still in use. They are vulnerable to different attacks. The attacker can take advantage of routine software update capabilities to gain access to the IMD. To mitigate these DoS attacks on the mHealth system, various solutions have been proposed in [31, 32] to protect the mHealth system from disruption attacks. These solutions are based on the efficient cryptographic primitives such as one-way hashing, biohashing and chaotic hashing [54–56].

Impersonation: An adversary of an mHealth system who tries to impersonate the legitimate user (for example, a patient or a doctor) of the system can collect the health data and misguide the other users. Suppose a patient suffers from some disease and is admitted to a hospital. The nursing staff consults with the doctor regarding the medicine that should be given to the patient. If a malicious user impersonates, the actual doctor, he/she can misguide the nursing staff by giving the wrong prescription. Various schemes have been proposed in [31, 35, 36, 43] that can be used to protect against impersonation attacks.

Recording and replaying: An adversary of the mHealth system can intercept and record the exchanged messages, and later replays them back to fool and mislead the legitimate users of the system. By reusing the recorded information, the adversary can later prove his/her identity and authenticity to the other party in order to get information such as the session key that may allow him/her to communicate with the other legitimate users of the mHealth system. Use of both random nonce and current timestamp by both ends of the communicating parties is the best way to protect against replay attacks. Some of these techniques are described in [31, 32, 35, 36].

From the security issues discussed above, various attacks such as stolen smart card/mobile device attack, offline/online password guessing attack, denial-of-service attack, privileged insider attack, user/medical server impersonation attacks, replay attack, man-in-the-middle attack and session key discloser attack are possible on the mHealth system.

Comparative study of security protocols for healthcare applications

In the last decade, several security protocols have been proposed for mobile healthcare applications. We classified the security protocols into three categories, mainly for the Telecare Medical Information System (TMIS), Multimedia Medical Information System (MMIS) and Electronic Patient Record Information System (EPR) that are related to mobile healthcare.

TMIS helps patients to benefit from the health monitoring while at home and access medical services over the Internet using their mobile devices. MMIS is an information system that provides the multimedia data of a patient's health to the healthcare experts [38]. An integrated EPR information system provides a patient's information to medical institutions for making the correct diagnosis to be used in clinical decisions for the patient [39].

The taxonomy of various existing schemes is shown in Fig. 2. Authentication in TMIS can use either two-factor authentication or three-factor authentication. A two-factor authentication scheme in TMIS requires smart card and user password as two factors for authentication. In contrast, a three-factor authentication scheme in TMIS requires smart card, user password and personal user biometrics as three factors for authentication.

We have compared various recently proposed security schemes for mobile healthcare. The comparisons of the recently proposed security schemes of Arshad et al. [30], Mishra et al. [31], Mir-Nikooghadam [32], Das et al. [35], Siddiqui et al. [42], Das [33], David [37], Moon et al. [57] and Mir et al. [58] are performed based on their functionality features, computation costs and communication costs.

Arshad et al. [30] presented a two-factor authentication and key agreement scheme based on the Elliptic Curve Cryptosystem (ECC). However, their scheme does not support efficient login phase because when the user enters his/her identity and password, they are not locally verified. Mishra et al. [31] proposed a biometric based authentication scheme for TMIS with nonce, which is computationally efficient, and it uses biohashing for biometric verification. Mir and Nikooghadam [32] proposed another biometrics-based authentication and key agreement scheme for TMIS.

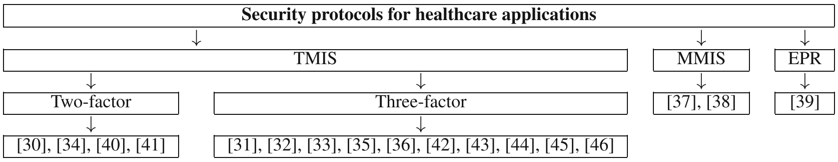

Fig. 2 Taxonomy of security protocols for healthcare applications

Table 1 Different types of computational times

Term	Description of operation	Time taken (in milliseconds)
T_h	one-way cryptographic hash function	0.0001
T_m	elliptic curve point multiplication	0.442
T_a	elliptic curve point addition	0.0018
T_{bh}	biohashing	0.442
T_{fe}	fuzzy extractor used in biometric verification	0.442
T_{bp}	bilinear pairing	4.211
T_{ccm}	Chebyshev polynomial computation	0.0001

However, their scheme suffers from denial of service attack because the user biometrics is directly applied to the one-way hash function. Since the outputs of a hash function are very sensitive to small perturbations of its inputs and user biometrics may sometimes change from time to time, a little variation in current user biometrics from the registered user biometrics may lead to produce a totally different hash output. Mir-Nikooghadam's scheme is not efficient for biometric verification using one-way hash function. Later, Das et al. [35] proposed a robust user authenticated key agreement scheme for the hierarchical multi-server environment, which is suitable for TMIS. Their scheme is based on the cryptographic one-way hash function and fuzzy extractor. As a result, the problem of biometrics verification in Mir-Nikooghadam's scheme is eliminated in Das et al.'s scheme. Siddiqui et al. [42] presented a three-factor remote user authentication scheme in TMIS. Their scheme transforms a smartphone to act as a unique and only identity that is required to access the TMIS system remotely. In addition, their scheme is suitable for the cloud-based environment.

Das [33] pointed out security limitations of the previous authentication schemes proposed in TMIS and then presented a more secure three-factor remote user authentication scheme for TMIS. This scheme preserves the user anonymity property. David [37] then proposed an efficient authentication scheme using bilinear pairing operations for multimedia medical information system. However, this scheme has several weaknesses listed in Table 4. Moon et al. [57] also proposed a two-factor authentication scheme, which is based on user password and smart card as two factors using the chaotic maps. Finally, Mir et al. [58] proposed a user authentication scheme for TMIS. However, their scheme does not support the biometric update phase.

The computation cost is the total execution time needed to execute the various cryptographic primitives for a security protocol. The times taken to compute different cryptographic operations are given in Table 1. These execution times were reported by He et al. [59] who used the hardware platform consisting of an Intel I7-4770 processor with 3.40 GHz clock frequency and 4 gigabytes memory, running Windows 7 operating system. They computed the execution time of various cryptographic operations using multiprecision integer and rational arithmetic cryptographic library (MIRACL), which is a cryptographic library used to implement cryptographic operations in many environments. It is assumed that the time for executing a fuzzy extractor/biohashing is the same as the time for executing an elliptic curve point multiplication at most [60]. In addition, the time taken to compute a Chebyshev polynomial approximates to the time taken for executing a hashing operation [61]. The comparison of computation costs for the login and authentication phases of various schemes is given in Table 2.

The communication cost of a security protocol is the number of bits exchanged for secure communications by the underlying security protocol. The comparison of communication costs for the login and authentication phases of various schemes is presented in Table 3. It is worth noting that we have assumed the following: the identity (ID) is of length 160 bits; a prime p in an elliptic curve is 160 bits assuming that 1024-bit RSA public key security is equivalent to 160-bit Elliptic Curve Cryptography (ECC) security [62], a random nonce/number is 128 bits; the timestamp is 32 bits; the symmetric cryptographic encryption/decryption block is 128 bits (if we apply AES symmetric-key cryptosystem [27]), and the hash digest is 160 bits (if we apply the Secure Hash Algorithm SHA-1 as the one-way hash function [15]). The communication costs for the same security schemes shown in Table 2 are presented in Table 3.

Finally, we present a comparison of the main functionality features of the various security schemes of Arshad et al. [30], Mishra et al. [31], Mir and Nikooghadam [32], Das et al. [35], Siddiqui et al. [42], Das [33], David [37], Moon et al. [57] and Mir et al. [58] given in Table 4. Mir et al.'s

Table 2 Comparison of computation costs

Scheme	[30]	[31]	[32]	[35]	[42]	[33]	[37]	[57]	[58]
Total cost	$12T_h + 6T_m$	$1T_{bh} + 6T_h$	$19T_h$	$18T_h + 1T_{fe}$	$2T_h$	$12T_h + 7T_m + 2T_{fe}$	$4T_m + 6T_h + T_{bp}$	$14T_h + 4T_{ccm}$	$17T_h$
Estimated time (ms)	2.6532	0.4426	0.0019	0.4438	0.0002	3.9792	5.9796	0.0018	0.0017

Table 3 Comparison of communication costs

Scheme	[30]	[31]	[32]	[35]	[42]	[33]	[37]	[57]	[58]
Total number of messages exchanged	3	2	3	3	1	2	3	3	3
Total number of bits exchanged	1312	544	1024	2496	320	1280	1440	1120	864

scheme [58] has low computation and communication costs and also provides additional security and functionality features. From the analysis of the results in Tables 2, 3 and 4, the computation and communication costs of Das et al. [35] and Das [33] schemes are slightly higher but are accepted because they provide additional security and functionality features (AFN_{11}, AFN_{13}, AFN_{14}, AFN_{15}). Siddiqui et al.'s scheme [42] incurs the lowest computation and communication costs among all the schemes. However, it does not satisfy most of the functionality features listed in Table 4. Considering better trade-off among the computation cost, communication cost and functionality features, Mir et al.'s scheme [58] has the best performance and David's scheme [37] has the worst performance among all the schemes considered in our comparisons.

Future challenges of security protocols for mobile healthcare

In this section, we identify some future challenges of security protocols for mobile healthcare.

- The fundamental security requirements of the mHealth system are confidentiality, data integrity, accountability, availability, and access control. For assuring these security requirements, developing efficient key distribution protocols becomes challenging task in the mHealth system.
- Recent studies in the literature [63] have shown that the public key operations (for example, elliptic curve cryptography) are practical in mobile devices. However, the private key operations are expensive because of their computational complexity. Thus, efficiency of private key operations still needs to be explored. Since mobile healthcare applications deal with sensitive patient data, authenticity of the public keys should be efficient and cost effective to protect the data from unauthorized access.
- In contrast to public-key cryptography, symmetric key cryptography is superior and is easier to implement in term of its computational efficiency. However, symmetric key cryptography is not suitable because it relies on distributing the key in the mHealth system to provide a variety of security services, such as credentials privacy,

Table 4 Comparison of functionality features

Functionality feature	[30]	[31]	[32]	[35]	[42]	[33]	[37]	[57]	[58]
AFN_1	yes	yes	yes	yes	yes	yes	no	yes	yes
AFN_2	yes	yes	yes	yes	yes	yes	no	yes	yes
AFN_3	yes	no	no	no	no	no	no	no	yes
AFN_4	no	yes	yes	yes	yes	yes	no	yes	no
AFN_5	yes	yes	yes	yes	yes	yes	yes	yes	yes
AFN_6	yes	yes	yes	yes	yes	yes	yes	yes	yes
AFN_7	yes	yes	yes	yes	no	yes	yes	yes	yes
AFN_8	yes	yes	yes	yes	yes	yes	no	yes	yes
AFN_9	yes	yes	yes	yes	yes	yes	no	no	yes
AFN_{10}	yes	yes	yes	yes	yes	yes	yes	yes	yes
AFN_{11}	yes	no	yes	yes	no	yes	no	yes	yes
AFN_{12}	yes	yes	yes	yes	no	yes	yes	yes	yes
AFN_{13}	yes	no	yes	yes	no	yes	yes	yes	yes
AFN_{14}	no	yes	no	yes	no	yes	N.A.	yes	yes
AFN_{15}	no	no	no	yes	no	yes	no	no	no

AFN_1 : efficient password change phase; AFN_2 : stolen smart card/mobile device attack; AFN_3 : two-factor authentication; AFN_4 : three-factor authentication; AFN_5 : password guessing attack; AFN_6 : denial-of-service attack ; AFN_7 : privileged insider attacker ; AFN_8 : impersonation attack; AFN_9 : replay attack; AFN_{10} : man-in-the-middle attack ; AFN_{11} : user anonymity preserving; AFN_{12} : mutual authentication; AFN_{13} : session key agreement; AFN_{14} : efficient login phase; AFN_{15} : efficient biometric update phase; yes: the protocol protects against that attack or provides that feature; no: the protocol does not protect against that attack or does not provide that feature. N.A. : not applicable mutual authentication, and session key security. Hence, designing efficient and flexible key distribution protocols for mobile healthcare applications needs to be addressed in the future.

- Obtaining passwords from unconscious patients may not be possible. In such cases, biometric methods may be used for authentication. However, the biometric methods that work with unique biometric features from unconscious patients for identification purposes still needs further research attention in order to correctly authenticate an unconscious patient.
- The mHealth system also includes different types of wearable sensors deployed in a patient's body. The privacy of the information stored in these sensors must be guaranteed. In this case, designing lightweight, efficient, and robust privacy enhancing techniques for the wearable sensors remains an area of future research.
- Meeting the quality-of-service (QoS) requirements along with security requirements simultaneously remains a challenge for the mHealth system, which includes different types of wearable sensors deployed in a patient's body for monitoring vital parameters. Thus, the security and QoS requirements need to be evaluated jointly in such systems.

Conclusion

In this paper, we have discussed the security requirements, issues and threats to the mHealth system. We have presented the taxonomy of recently proposed security protocols of the mHealth system. We have also identified some of the future challenges that need to be addressed for security protocols used by mHealth system. Security and privacy will continue to play a vital role in mHealth systems in protecting the personal medical information of patients and medical data held by healthcare organizations.

Acknowledgments We thank the anonymous reviewers for their valuable feedback on the paper which helped us to improve its quality and presentation.

Compliance with Ethical Standards

Conflict of interests The authors declare that they have no conflict of interest.

References

1. Asare, P.: Emerging health monitoring systems. https://pages.shanti.virginia.edu/Science_Straight_Up. Accessed on June 2016.
2. Boukerche, A., and Ren, Y., A secure mobile healthcare system using trust-based multicast scheme. *IEEE J. Selected Areas Commun.* 27(4):387–399, 2009.
3. Arora, S., Yttri, J., and Nilsen, W., Privacy and security in mobile health (mHealth) research. *Alcohol Res. Current Rev.* 36(1):143, 2014.
4. Is Mobile Healthcare the Future. http://www.greatcall.com/greatcall/lp/is-mobile-healthcare-the-future-infographic.aspx. Accessed on June 2016.
5. Wu, L., Li, J. Y., and Fu, C. Y., The adoption of mobile healthcare by hospital's professionals: an integrative perspective. *Decis. Support Syst.* 51(3):587–596, 2011.
6. Kamel Boulos, M. N., Wheeler, S., Tavares, C., and Jones, R., How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *BioMed. Eng. OnLine* 10(24):1–14, 2011.
7. Ren, Y., Werner, R., Pazzi, N., and Boukerche, A., Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Commun.* 17(1):59–65, 2010.
8. Ren, Y., Chen, Y., Chuah, M. C., and Yang, J., User verification leveraging gait recognition for Smartphone enabled mobile healthcare systems. *IEEE Trans. Mobile Comput.* 14(9):1961–1974, 2015.
9. National Cancer Institute, Chemotherapy. http://www.cancer.gov/about-cancer/treatment/types/chemotherapy. Accessed on June 2016.
10. Diana, A.: Securing Mobile Healthcare Devices: Best Practices. http://www.informationweek.com/healthcare/security-and-privacy/securing-mobile-healthcare-devices-best-practices/d/d-id/1269357. Accessed on June 2016.
11. He, D., and Zeadally, S., Authentication protocol for an ambient assisted living system. *IEEE Commun. Mag.* 53(1):71–77, 2015.
12. Odelu, V., Das, A. K., and Goswami, A., An effective and secure key-management scheme for hierarchical access control in e-medicine system. *J. Med. Syst.* 37(2):1–18, 2013.
13. Koblitz, N., Elliptic curves cryptosystems. *Math. Comput.* 48:203–209, 1987.
14. Stallings, W.: *Cryptography and Network Security: Principles and Practices*, 3rd edn. Prentice Hall, 2003.
15. Secure Hash Standard: FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 1995.
16. Dodis, Y., Reyzin, L., and Smith, A., Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Advances in Cryptology-Eurocrypt 2004, pp. 523–540. Interlaken: Springer, 2004.
17. Odelu, V., Das, A. K., and Goswami, A., A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Trans. Inf. Forens. Secur.* 10(9):1953–1966, 2015.
18. Jina, A. T. B., Linga, D. N. C., and Goh, A., Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recog.* 37(11):2245–2255, 2004.
19. Lumini, A., and Nanni, L., An improved BioHashing for human authentication. *Pattern Recog.* 40(3):1057–1065, 2007.
20. Zhang, L., Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons and Fractals* 50(1):669–674, 2008.
21. HIT Consultant, 5 Best Practices for Mobile Device Security in Healthcare. https://www.hitconsultant.net/2015/11/03/5-best-practices-for-mobile-device-security-in-healthcare/. Accessed on June 2016.
22. Pittman, D.: 5 Problems With Mobile Health App Security. https://www.theguardian.com/society/2000/jun/25/futureofthenhs.health. Accessed on June 2016.
23. Nelson, E. C., Verhagen, T., and Noordzij, M. L., Health empowerment through activity trackers: an empirical smart wristband study. *Comput. Human Behav.* 62:364–374, 2016.
24. Phang, T. C., Mokhtar, M. H., Mokhtar, M. N., and Rokhani, F. Z., Time-division multiple access based intra-body communication for wearable health tracker. In: 17th International Symposium

on Quality Electronic Design (ISQED), pp. 468–472. USA: Santa Clara, 2016.

25. Sullivan, D.: My life with the Fitbvit One activity tracker. http://www.cnet.com/news/my-life-with-the-fitbit-one-activity-tracker. Accessed on June 2016.
26. Fortino, G., and Pathan, M., Integration of cloud computing and body sensor networks. *Future Gen. Comput. Syst.* 35:57–61, 2014.
27. Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Accessed on June 2016.
28. Baig, M. M., GholamHosseini, H., and Connolly, M. J., Mobile healthcare applications: system design review, critical issues and challenges. *Aust. Phys. Eng. Sci. Med.* 38(1):23–38, 2015.
29. Rivest, R. L., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21(2):120–126, 1978.
30. Arshad, H., Teymoori, V., Nikooghadam, M., and Abbassi, H., On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 39(8):1–10, 2015.
31. 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. *J. Med. Syst.* 38(5):1–11, 2014.
32. Mir, O., and Nikooghadam, M., A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services. *Wireless Person. Commun.* 83(4):2439–2461, 2015.
33. Das, A. K., A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems. *J. Med. Syst.* 39(3):1–20, 2015.
34. Liu, C. H., and Chung, Y. F.: Secure user authentication scheme for wireless healthcare sensor networks. *Computers & Electrical Engineering*. doi:10.1016/j.compeleceng.2016.01.002, 2016.
35. Das, A. K., Odelu, V., and Goswami, A., A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS. *J. Med. Syst.* 39(9):1–24, 2015.
36. Wazid, M., Das, A. K., Kumari, S., Li, X., and Wu, F., Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Secur. Commun. Netw.* 9(13):1983–2001, 2016.
37. David, D. B., Mutual authentication scheme for multimedia medical information systems. *Multimed. Tools Appl.* 1–19, 2016.
38. David, D. B., Rajappa, M., Karupuswamy, T., and Iyer, S. P., A dynamic-identity based multimedia server client authentication scheme for tele-care multimedia medical information system. *Wireless Person. Commun.* 85(1):241–261, 2015.
39. Li, C. T., Weng, C. Y., Lee, C. C., and Wang, C. C., A hash based remote user authentication and authenticated key agreement scheme for the integrated EPR information system. *J. Med. Syst.* 39(11):1–11, 2015.
40. Das, M. L., Two-factor user authentication in wireless sensor networks. *IEEE Trans. Wireless Commun.* 8(3):1086–1090, 2009.
41. Sutrala, A. K., Das, A. K., Odelu, V., Wazid, M., and Kumari, S., Secure anonymity-preserving password-based user authentication and session key agreement protocol for telecare medicine information systems. *Comput. Methods Programs Biomed.* 135:167–185, 2016.
42. Siddiqui, Z., Abdullah, A. H., Khan, M. K., and Alghamdi, A. S., Smart environment as a service: three factor cloud based user authentication for telecare medical information system. *J. Med. Syst.* 38(1):1–14, 2013.
43. Jiang, Q., Khan, M. K., Lu, X., Ma, J., and He, D., A privacy preserving three-factor authentication protocol for e-Health clouds. *J. Supercomput.* 1–24, 2016.
44. Zhang, L., Zhu, S., and Tang, S.: Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. *IEEE Journal of Biomedical and Health Informatics*. doi:10.1109/JBHI.2016.2517146, 2016.
45. Das, A. K., Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Inf. Secur.* 5(3):145–151, 2011.
46. Li, C. T., and Hwang, M. S., An efficient biometric-based remote user authentication scheme using smart cards. *J. Netw. Comput. Appl.* 33:1–5, 2010.
47. Li, X., Niu, J., Liao, J., and Liang, W., Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. *Int. J. Commun. Syst.* 28(2):374–382, 2015.
48. Li, X., Niu, J., Kumari, S., Liao, J., and Liang, W., An enhancement of a smart card authentication scheme for multi-server architecture. *Wireless Person. Commun.* 80(1):175–192, 2015.
49. Li, X., Niu, J., Wang, Z., and Chen, C., Applying biometrics to design three-factor remote user authentication scheme with key agreement. *Secur. Commun. Netw.* 7(10):1488–1497, 2014.
50. Browne, A.: Lives ruined as NHS leaks patients' notes. http://www.medpagetoday.com/practicemanagement/informationtechnology/44161. Accessed on June 2016.
51. Ohri, A.: Denial of service attacks against hospitals and emergency rooms. https://decisionstats.com/2011/09/21/denial-of-service-attacks-against-hospitals-and-emergency-rooms. Accessed on June 2016.
52. White, J.: How hospitals can fight back against new hacker attacks. http://www.healthcarebusinesstech.com/ddos-attacks-hospitals. Accessed on June 2016.
53. Ouellette, P.: DDoS attack considerations for healthcare organizations. http://healthitsecurity.com/news/ddos-attack-considerations-for-healthcare-organizations. Accessed on June 2016.
54. Jina, A. T. B., Linga, D. N. C., and Goh, A., Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recog.* 37(11):2245–2255, 2004.
55. Lumini, A., and Nanni, L., An improved BioHashing for human authentication. *Pattern Recog.* 40(3):1057–1065, 2007.
56. Xiao, D., Liao, X., and Deng, S., One-way hash function construction based on the chaotic map with changeable-parameter. *Chaos, Solitons & Fractals* 24(1):65–71, 2005.
57. 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. *J. Med. Syst.* 40(3):1–11, 2016.
58. Mir, O., van der Weide, T., and Lee, C. C., A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems. *J. Med. Syst.* 39(9):1–16, 2015.
59. He, D., Zeadally, S., Xu, B., and Huang, X., An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forens. Secur.* 10(12):2681–2691, 2015.
60. He, D., Kumar, N., Lee, J. H., and Sherratt, R. S., Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Trans. Consum. Electron.* 60(1):30–37, 2014.
61. Lee, T. F.: Provably secure anonymous single-sign-on authentication mechanisms using extended Chebyshev chaotic maps for distributed computer networks. IEEE Syst. J., 2015.
62. Vanstone, S., Responses to NIST's proposal. *Commun. ACM* 35(7):50–52, 1992.
63. Lauter, K., The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless Commun.* 11(1):62–67, 2004.