IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

SPECIAL SECTION ON SECURITY, PRIVACY, AND TRUST MANAGEMENT IN SMART CITIES

Received February 25, 2019, accepted March 15, 2019, date of publication April 9, 2019, date of current version April 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909556

Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment

SHAHEENA KHATOON[1], (Student Member, IEEE),
SK MD MIZANUR RAHMAN[2], (Member, IEEE),
MAJED ALRUBAIAN[3], (Member, IEEE),
AND ATIF ALAMRI[4], (Member, IEEE)
[1]School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur 492010, India
[2]Centennial College, Toronto, ON M1G 3T8, Canada
[3]Research Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[4]Research Chair of Pervasive and Mobile Computing, Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding authors: Shaheena Khatoon (shaheenataj.28@gmail.com), Sk Md Mizanur Rahman (srahman@centennialcollege.ca), and Atif Alamri (atif@ksu.edu.sa)

This work was supported in part by the King Saud University, Deanship of Scientific Research, Research Chair of Pervasive and Mobile Computing, and in part by the Department of Science and Technology (DST), Government of India under Women Scientist Scheme A (WOS-A) under Grant SR/WOS-A/PM-10/2018(G).

ABSTRACT Smart home systems can provide health care services for people with special needs in their own homes. Briefly defined, such a smart home has special electronics to enable the remote control of automated devices specifically designed for remote health care to ensure the safety of the patient at home and the supervision of their health status. These sensors are linked to a local intelligence unit responsible for analyzing sensor data, detecting emergency situations, and interfacing between the patient at home and a set of people involved in their health care, such as doctors, nurses, emergency services, and paramedics. Smart homes can improve the patient's quality of life and safety through the innovative use of advanced technologies. Telemedicine and telecare are driving forces behind the adoption of smart homes. The telecare medicine information system (TMIS) has drawn worldwide attention for the past 20 years, as modern technologies have made remote delivery of healthcare a reality. TMIS using multidisciplinary research and application involves advanced technologies in information processing, telecommunications, bio-sensing, and artificial intelligence including smart technologies. TMIS leverages the latest mobile and wireless communication technologies and widely available internet infrastructure to deliver quality services to home patients enabling them to remotely access information about their health and obtain telemedical services. TMIS delivers capabilities to remotely provide 24 × 7 health care facilities to patients. Its purpose is to provide patients with convenient and expedited remote health care services, greatly improving the quality and efficiency of health care services. However, the open and insecure nature of the internet poses a number of security threats to patient secrecy and privacy. Security design for TMIS is not trivial. Essential security and privacy are provided by mutual authentication and key agreement protocols. This paper proposes an efficient and secure, bilinear pairing-based, unlink-able, mutual authentication and key agreement protocol for TMIS. The proposed protocol adopts a fuzzy extractor for the identification of patients using the biometric data. The security of the proposed protocol is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP) and elliptic curve computational Diffie–Hellman problem (ECCDHP) to preserve the privacy of the user. The detailed security analysis is discussed, and the results of comparison are provided.

INDEX TERMS Smart city, telecare medicine information systems (TMIS), mutual authentication, key agreement protocol, bilinear pairing, fuzzy extractor.

I. INTRODUCTION

The concept of smart homes in a smart city emerged from a combination of three research areas: medicine, domotics (home-based automation and remote-controlled devices) and information systems. Smart homes are one of the most promising ways to develop patient-centered telemedicine and telecare services. The smart room concept developed earlier in the domains of domotics [2], [3], robotics and artificial intelligence [4] was later extended to the fields of telemedicine and telecare.

Recent advances in networking and wireless technologies and the growing prevalence of smart devices along with access to social networks and cloud computing have significantly changed all spheres of life. The medical field is no exception. Such technologies are rapidly gaining popularity in the medical sector to improve and facilitate the delivery of health care services. The telecare medicine information system (TMIS) is an important example of a rapidly growing medical service. TMIS provides various health-care facilities and treatments to patients via the internet, enabling patients to remotely access information about their health and obtain tele-medical services. TMIS delivers capabilities to remotely provide 24 × 7 health care facilities to patients [16], [31], [40] greatly improving the quality and efficiency of health care services. However, the open and insecure nature of the internet poses various security threats to patient secrecy and privacy.

Essential security and privacy in an open network are provided by mutual authentication and key agreement protocols. Mutual authentication protocols ensure that only authorized entities have access to health data. Key agreement protocols ensure the confidentiality and integrity of the information in transit. Furthermore, given frequent identity attacks, such as identity stealing and tracing, secure authentication and key agreement protocols are desirable to protect the security, integrity and authenticity of patient records. Therefore, it is necessary to design an anonymous and unlink-able mutual authentication and key agreement protocol for TMIS. Initially, two-factor authentication schemes received much attention with numerous schemes proposed. Several weaknesses of two-factor schemes have been identified; passwords are easy to break through simple dictionary attacks and smart cards can be misappropriated and are also subject to differential power attacks. Consequently, biometric-based user authentications protocols have been introduced and are considered better and more reliable alternatives than traditional password-based authentication schemes. Biometric methods are unique and quantifiable methods for recognizing a human being. Biometric information is prone to various noise during data acquisition and the reproduction of actual biometric data is hard in common practice. To avoid these problems a fuzzy extractor [19] is used, Fuzzy extractors generate strong keys from biometric and other noisy data. It involves a two-step method:-

- The generation process (Gen)is a probabilistic production process that takes as input the users biometric information Bio and gives as output a secret value O_i and a random ancillary parameter par_i.
- The reproduction process (Rep)is a deterministic production process that takes as input the users biometric information Bio and the corresponding random ancillary parameter par_i and gives a secret value O_i as the output.

A number of biometric-based mutual authentication and key agreement protocols for TMIS have been proposed but they have either been proven insecure against various attacks or offer security solutions involving modular exponentiation. To this end bilinear pairing can be put forward as an efficient and secure mechanism for a mutual authentication and key agreement protocol for TMIS.

II. CONTRIBUTIONS

This paper proposes an efficient and secure bilinear pairing-based, unlink-able, mutual authentication and key agreement protocol for TMIS. The proposed protocol adopts a fuzzy extractor for the identification of patient's using biometric data. Further, the security of the proposed protocol is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP) and elliptic curve computational Diffie Hellman problem (ECCDHP). Our major contributions are as follows:

- a mutual authentication and key agreement protocol for TMIS;
- computational costs distributed between the TMIS server and the patient to lower computation requirements;
- using the elliptic curve discrete logarithm problem (ECDLP) and elliptic curve computational Diffie Hellman problem (ECCDHP) to provide security against known attacks;
- formally analyzing the security of the proposed scheme using the real-or-random (R-OR) model;
- comparing the proposed protocol favorably to other related and existing protocols in terms of the communication and computational costs across the various phases; and
- demonstrating the higher security and efficiency of the proposed protocol compared to other related and existing schemes which make it more appropriate for practical applications.

Organization of the Paper: The next section describes a TMIS architecture and its benefits in the medical field. Section IV briefly reviews the existing protocols for TMIS, and Section V describes preliminaries to enable better understanding of the proposed protocol. The proposed protocol is detailed in Section VI. A formal security analysis of the proposed protocol using the random oracle model is presented in Section VII and Section VIII further analyzes the

---

The associate editor coordinating the review of this manuscript and approving it for publication was Mehedi Masud.

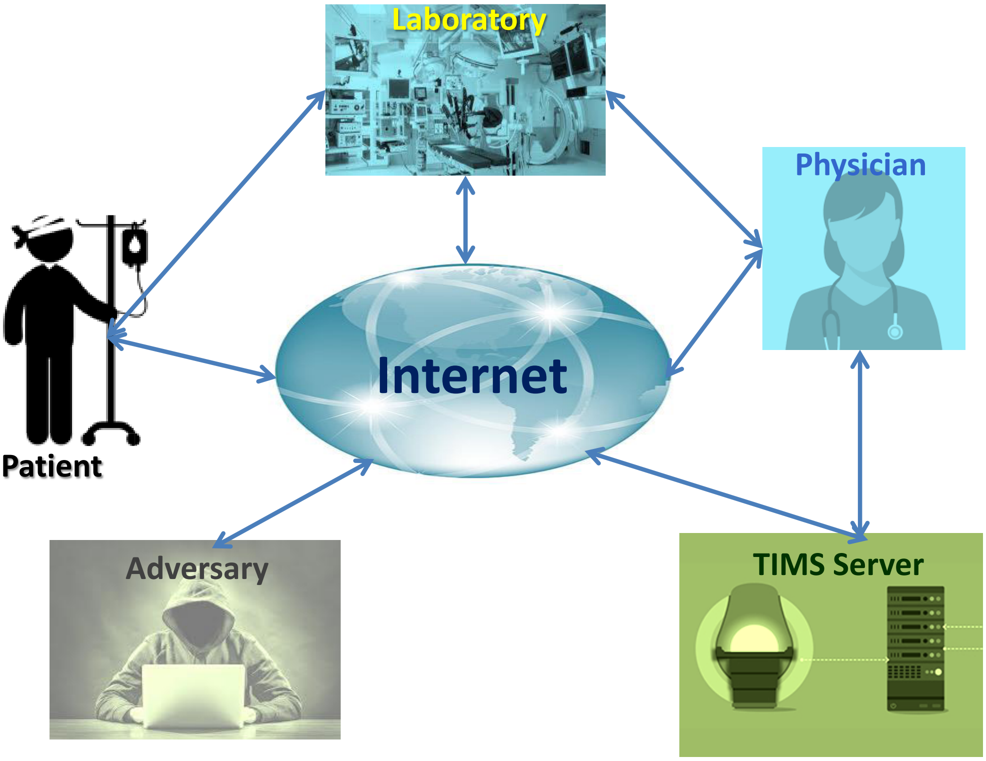

FIGURE 1. A typical model for TMIS system network in a smart city environment.

security of the proposed protocol, while Section IX analyzes its performance compared to other existing protocols. Finally, Section X concludes.

III. A TMIS ARCHITECTURE AND ITS BENEFITS IN THE MEDICAL FIELD

Figure 1 depicts a typical TMIS architecture. TMIS provides communication platform to different parties i.e. the physician, patient, laboratory and medical server. They are connected with each other and are willing to share information related to patient's treatments, medications and test results over an internet. Whenever a patient needs health care services, he/she needs to log into the medical server. On getting a request from a patient, the medical server first verifies the legitimacy of the patient. If the patient is legitimate, then the medical server contacts the physicians to provide health care consultation to the patient. To access these health care services remotely, a user is first required to register with the TMIS server. The server registers patients and acts as an interface between patients and physicians.

As TMIS is provided over the internet, the internets open structure renders a number of security threats. As shown in Figure 1, an adversary can acquire confidential patient information by apprehending messages exchanged between a patient and the medical server. The adversary can also alter messages exchanged between patient and physician. This breaches the privacy of the patient and can also result in irreparable injury. Hence, a secure mechanism for authentication and key agreement should be employed to restrict unauthorized accesses to medical information stored on the medical servers and exchanged between users (physicians and patients) and medical servers. Some of the important benefits of TMIS include the following:

- It provides remote health and medical services.
- It improves patients quality of life.
- It provides accurate diagnosis and treatment to patients, as all medical records are stored on the TMIS server.
- It saves human labor, time and money.

A. SECURITY REQUIREMENTS OF TMIS

TMIS should meet the following essential security criteria:

- It should provide an efficient and secure mutual authentication and key agreement protocol to enable secure communication over an insecure network.
- The mutual authentication and key agreement protocol should provide patients with anonymity and unlink-ability.
- Session key authentication should be used to prevent various possible attacks such as key impersonation and privileged-insider.
- Due to limited resources such as battery, memory, communications bandwidth and computational capabilities, the computational and communication costs of the TMIS should be kept low.

IV. RELATED WORK

This section briefly reviews existing protocols proposed for TMIS. Numerous password-based and biometric-based

TABLE 1. Related protocol for TMIS.

Protocol	year	Major attacks
Chen et al.[17]	2012	dictionary attack and password guessing attack
Wu et al.[42]	2012	masquerade attack, off-line password guessing attack and internal or insider attacks
He et al.[20]	2012	off-line password guessing attack
Wei et al.[43]	2012	off-line password guessing attack
Zhu et al. [48]	2012	impersonation attacks, off-line password guessing attacks and denial-of-service attacks
Jian et al. [28]	2013	patient anonymity violation, spoofing and off-line password guessing attacks
Lin et al. [32]	2013	denial of service attack
Cao and Zhai [18]	2013	denial of service attack
Xie et al. [47]	2013	denial of service attack
Xu et al. [46]	2013	protocol is not efficient and robust, it fails to achieve strong authentication in login and authentication phases and fails to update the password correctly in the password change phase
Awasthi et al. [6]	2013	off-line password guessing attack, reflection attack and inappropriate password changing phase
Jiang et al. [29]	2014	scheme is vulnerable to denial of service attack and error in password change phase
Mishra et al. [35]	2014	Proposed a chaotic maps based user authentication and key agreement protocol for TMIS
Khan et al.s [30]	2013	user impersonation attacks, violates user anonymity and denial of service attacks
Bin Muhaya [15]	2015	off-line password guessing attacks and does not provide perfect forward secrecy
Mir et al. [38]	2015	scheme does not support efficient login phase
Wen and Guo [44]	2015	Analyzed the Wu et al.[42] protocol it and improved it.
Arshad et al. [9]	2016	scheme does not support efficient login phase
Mishra et al.[36]	2014	proposed a computationally efficient biometric based authentication scheme for TMIS
Tan et al. [41]	2014	denial of service attack
Arshad and Nikooghadam [7]	2014	off-line password guessing and patient impersonation attacks
Siddiqui et al. [39]	2014	proposed a biometric-based remote user authentication scheme in TMIS, their protocol is suitable for the cloud-based environment also
Mir and Nikooghadam [37]	2015	denial of service attack
Lu et al. [34]	2015	do-not provide patient anonymity, Patient and the server impersonation attack and protocol do not provide patient untraceability
Das [22]	2015	proposed a robust user authenticated key agreement protocol to eliminate the weaknesses of Mir and Nikooghadam protocol
David [23]	2016	proposed an efficient Mutual Authentication Scheme (MAS) using bilinear-pairing system for TMIS. But, their scheme has many drawbacks such as impersonation attack, replay attack, user anonymity, no efficient password and biometric update phase.

authentication and key agreement schemes have been proposed but all are either prone to different attacks or do not provide desirable features like user anonymity and privacy. In 2012, Chen *et al.* [17] proposed a dynamic ID-based authentication scheme for TMIS which protects user anonymity. Cao and Zhai [18], Lin [32], and Xie *et al.* [47] demonstrated the weaknesses of the Chen et al. protocol and presenting independent improved protocols for TMIS. Later, their protocols were shown to lack the input-verifying condition, which leads to denial of service; if an authorized user mistakenly enters incorrect input in the password change phase the user can never again use the smart card to login to the server.

Wu *et al.* [42] also proposed an authentication protocol for TMIS, but Debiao *et al.* [20] demonstrated that this protocol is prone to various attacks. He et al. then proposed a new protocol to prevent the identified attacks. Later, Wei *et al.* [43] showed that the He et al. protocol is also insecure against password guessing attacks and proposed a new protocol. Zhu [48] showed that the Wei et al. protocol is insecure and Jiang *et al.* [28] soon showed that even the Zhu et al. protocol is insecure.

Over the years several weaknesses of two-factor schemes have been identified, as passwords are easy to break by simple dictionary attacks. Similarly, smart cards can be misappropriated and are also subject to differential power attack. Consequently, biometric-based user authentication protocols have been introduced and are considered better and more reliable alternatives than traditional password-based authentication schemes. Abundant biometric-based protocols have been presented. In 2013, Awasthi and Srivastava [6] proposed a biometric authentication scheme for TMIS. Over the subsequent years Mishra *et al.* [36] and [41] demonstrated that the Awasthi et al. protocol suffers from many drawbacks; offline password guessing and reflection attacks and an inappropriate password changing phase. Therefore, Tan et al. proposed an enhanced three-factor authentication scheme which was later proven prone to replay and denial of service attacks by Arshad and Nikooghadam [7]. Later, Lu *et al.* [34] proved the Arshad and Nikooghadam protocol insecure against off-line password guessing and patient impersonation attacks. They presented a new protocol but the Lu et al. protocol is also vulnerable to numerous attacks, such as the patient anonymity violation attack, patient impersonation attack, and the TMIS server impersonation attack, and the protocol does not provide patient untrace-ability.

Table 1 comprehensively overviews work on the telecare medical information system (TMIS).

V. PRELIMINARIES

The present section elaborates the notation table and briefly discusses fundamental concepts relating to an elliptic curve cryptosystem (ECC) and bilinear pairing.

A. ELLIPTIC CURVE CRYPTOSYSTEM (ECC)

An elliptic curve cryptosystem [25] involves the equation $E_p(a, b) : y^2 = x^3 + ax + bmodp$, where p is a large prime number, $p \geq 160$bits. The integers $a, b \in Z_q^*$ define the

TABLE 2. **Basic notation.**

Notations	Description
q	A large prime.
e	A bilinear map $e : G_1 \times G_1 \rightarrow G_2$.
P	The generator of G_1.
ID_i, PW_i, B_i	Patient i's identity, password and biometric information.
S	TMIS server.
s	Master private key $s \in Z_q^*$ of S.
P_{pub}	Public key $P_{pub} = sP$ of S.
h	A hash function, $h : \{0,1\}^* \rightarrow Z_q$.
H	A hash function, $H_1 : \{0,1\}^* \rightarrow G_1$.
E_{k_i}	Encryption with symmetric key k_i.
T_s, T_i	Time stamp of U_i and S.

curve such that $4a^3 + 27b^2 \neq 0 (mod p)$. The curve is defined as $E_p = \{\{(x, y)\} : E_p(x, y) = 0 \cup \{0\}\}$, where $\{0\}$ is the point at infinity is considered an identity element. Below, we define the following two hard computational problems pertaining to ECC security:

1) The Elliptic Curve Discrete Logarithm Problem (ECDLP) can be defined as follows: given two points P and Q over an elliptic curve $E_p(a, b)$ it is computationally hard to find an integer x such that $P = xQ$ in polynomial time.
2) The Elliptic Curve Computational Diffie Hellman Problem (ECCDHP) can be defined as follows: given three points Q, aQ and bQ over an elliptic curve $E_p(a, b)$ it is computationally hard to find abQ in polynomial time.

B. BILINEAR PAIRING

Let $\langle G_1, + \rangle$ be a cyclic additive group generated by P, whose order is a large prime p and let $\langle G_2, . \rangle$ be a cyclic multiplicative group of the same order p. A bilinear pairing e is a map defined by $e : G_1 \times G_2 \rightarrow G_2$ with the following properties.

1) Bilinear: For given $(P, Q) \in G_1$, $e(aP, bQ) = e(P, Q)^{ab}$ for any $a, b \in Z_p*$.
2) Non-degenerate: There exists $(P, Q) \in G_1$ such that $e(P, Q) \neq 1$, where 1 is the identity of G_2.
3) Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $(P, Q) \in G_1$.

The discrete logarithm problem (DLP) is hard in both G_1 and G_2. Weil pairing, modified Weil pairing and Tate pairing are all cryptographically secure pairings.

VI. THE PROPOSED SCHEME

This section presents a new biometric-based, anonymous and unlink-able mutual authentication and key agreement phase for TMIS using bilinear pairing. The security of the proposed scheme is based on the hardness of the ECDLP and ECCDH problems. The proposed scheme has three phases: (1) initialization; (2) registration; (3) login, authentication, and key agreement; and (4) password changing. For clarity, the notations in Table 2 are used throughout the paper.

1) Initialization: TMIS server S sets up its parameters. S chooses the public parameters $\{q, G_1, G_2, e, P, h, H\}$ generates its master private key $MPK = s \in Z_q^*$ computes its master public key as $P_{pub} = sP$ and publishes the system parameters as $Param = \{q, G_1, G_2, e, P, h, H, P_{pub}\}$.
2) Registration: This phase is initiated by a remote user U_i who selects an identity ID_i, password PW_i, imprints its biometric B_i and computes $C_i = PW^i \oplus H_B(B_i)$. U_i sends $\{C_i, ID_i\}$ to the server S. S checks ID_i in its database. If it is new S records $N = 0$; otherwise, S records $N = N+1$. Then it computes $V_i = h(ID_i||C_i)$ and $W_i = C_i \oplus h(ID_i||s)$. Then S customizes a smart card SC_i with $\{V_i, W_i, P_pub, h, H, H_B\}$ and sends it securely to the patient U_i.
3) Login, authentication, and key agreement: User U_i inserts their smart card SC_i into the card reader inputting their identity ID_i and password PW_i and imprinting B_i. The SC_i computes $h(ID_i||PW_i \oplus H_B(B_i))$ and checks its equivalence with the stored V_i. If invalid SC_i aborts the session. Otherwise, SC_i generates a random number $r_i \in Z_q^*$ and fresh time stamp T_i and computes $Q_i = H(ID_i)$, $Q_s = H(ID_s)$, $R_i = r_i Q_i$, $K_i = e(P_pub, r_i Q_s)$ and $Auth_i = E_{(}k_i)(ID_i||T_i||r_i)$ and sends the login request $LR_i = R_i, T_i, Auth_i$ to S.
   Upon receiving the login request LR_i, server S checks the time validity $\Delta T \leq T_s - T_i$ if valid it proceeds to calculate $K_s = e(s, R_i P)$, decrypt $Auth_i$ to obtain $(ID_i||T_i||r_i)$ compute $Q_i = H(ID_i)$ and check $R_i = r_i Q_i$. If it holds, S also generates a random number r_s computes $Q_s = H(ID_s)$, $R_s = r_s Q_i$, $L_s = r_s R_i$, $Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_s)$ and the session key $SK_s = h(T_i||R_i||T_s||R_s||L_s)$ sending the mutual authentication message $MA = (R_s, T_s, Auth_s)$ to the user U_i.
   Upon receiving MA, U_i verifies, $\Delta T \leq T_s - T_i$ if valid, the user calculates $L_i = r_i R_s$ and verifies the equation $Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_i)$. If the equation holds the user computes the common session key as $SK_i = h(T_i||R_i||T_s||R_s||L_s)$.
4) Password changing: Any user can change their password without the involvement of the server S. To do so, user U_i inserts the smart card SC_i enters their identity password and imprints the biometric information. Then SC_i computes $C_i = PW^i \oplus H_B(B_i)4$ and checks its equivalence with the stored C_i. If valid, SC_i asks for the new password. U_i enters the new password PW_i^{new} and computes $C_i = PW_i^{new} \oplus H_B(B_i)$, $V_i^{new} = h(ID_i||C_i^{new})$ and $W_i^{new} = W_i \oplus C_i \oplus C_i^{new}$. Finally, SC_i assigns V_i^{new} to V_i and W_i^{new} to W_i.

The registration and login, authentication and key agreement phases are depicted in Table 3, whereas the password changing phase in depicted in Table 4.

VII. SECURITY ANALYSIS USING RANDOM ORACLE MODEL

This section formally analyzes the security of the proposed scheme using the real-or-random (R-OR) model given by Abdalla *et al.* [5], which assimilates the Bellare and Rogaway [10]–[12] model for key distribution and the Bellare *et al.* [13] model for password-based

TABLE 3. Phases of the proposed protocol.

Registration Phase	
Patient U_i	TMIS server S
Computes $C_i = PW^i \oplus H_B(B_i)$	
Sends $\langle C_i, ID_i \rangle$ to S	
	S checks the ID_i in its database
	If new, S records $N = 0$
	otherwise, S record $N = N + 1$
	compute, $V_i = h(ID_i \vert\vert C_i)$ and $W_i = C_i \oplus h(ID_i \vert\vert s)$
	Customizes SC_i with $\langle V_i, W_i, P_{pub}, h, H, H_B \rangle$
	send its securely to U_i

Login, Authentication and Key Agreement Phase	
Patient U_i	TMIS server S
U_i insert his smart card SC_i in card reader	
Inputs ID_i, PW_i and imprints B_i	
The SC_i computes $h(ID_i \vert\vert PW_i \oplus H_B(B_i))$	
Checks $h(ID_i \vert\vert PW_i \oplus H_B(B_i))$ = V_i	
If invalid SC_i, aborts the session	
Otherwise,	
Selects $r_i \in Z_q$ and fresh T_i	
Compute $Q_i = H(ID_i), Q_s = H(ID_s)$	
$R_i = r_i Q_i, K_i = e(P_{pub}, r_i Q_s)$	
$Auth_i = E_{k_i}(ID_i \vert\vert T_i \vert\vert r_i$	
and $LR_i = \{R_i, T_i, Auth_i\}$ to S	
	Upon receiving LR_i, S checks
	$\Delta T \leq T_s - T_i$ if valid it proceed
	And calculate $K_s = e(s, R_i P)$
	decrypt $Auth_i$ to obtain $(ID_i \vert\vert T_i \vert\vert r_i)$
	Computes $Q_i = H(ID_i)$
	checks $R_i = r_i Q_i$. If valid
	Then S generates a random number r_s
	Computes $Q_s = H(ID_s), R_s = r_s Q_i, L_s = r_s R_i$
	$Auth_s = h(T_i \vert\vert R_i \vert\vert T_s \vert\vert R_s \vert\vert L_s \vert\vert K_s)$
	$SK_s = h(T_i \vert\vert R_i \vert\vert T_s \vert\vert R_s \vert\vert L_s)$
	Send $MA = (R_s, T_s, Auth_s)$ to U_i
Upon receiving MA, U_i verifies, $\Delta T \leq T_s - T_i$	
If valid	
Computes $L_i = r_i R_s$	
verifies $Auth_s = h(T_i \vert\vert R_i \vert\vert T_s \vert\vert R_s \vert\vert L_s \vert\vert K_i)$	
And computes $SK_i = h(T_i \vert\vert R_i \vert\vert T_s \vert\vert R_s \vert\vert L_s)$	

TABLE 4. Password changing phase of the proposed protocol.

Password Changing Phase
U_i, inserts the smart card SC_i, enters his identity password and imprints the biometric
Then SC_i computes $C_i = PW^i \oplus H_B(B_i)$
Checks its equivalence with stored C_i, if valid
SC_i ask for new password
U_i enter new password PW_i^{new}
SC_i computes $C_i = PW_i^{new} \oplus H_B(B_i)$, $V_i^{new} = h(ID_i \vert\vert C_i^{new})$
$W_i^{new} = W_i \oplus C_i \oplus C_i^{new}$
Finally, SC_i assigns V_i^{new} to V_i and W_i^{new} to W_i

authenticated key exchange. We briefly describe the R-OR model details can be found in [5]. The scheme involves two participants, a user U_i and a TMIS server S.

- Instance: $\prod_S^t$ and $\prod_{U_i}^u$ denote the instance t of S and instance u of U_i. These instances are called oracles.
- SID: The SID (session identifier) of any oracle is defined as the concatenation of all the message sent and received by that oracle.
- Open Oracle: If an oracle $\prod_S^t$ reveals the accepted session key in any state then oracle is considered opened in that state.
- Partner Oracle: Two oracles $\prod_S^t$ and $\prod_{U_i}^u$ are called partners if they have the same SID.
- Fresh Oracle: An oracle $\prod_S^t$ is unfresh if it is opened or its partner oracle $\prod_S^{t'}$ is opened or corrupted; otherwise, it is fresh oracle.
- Adversary: In the R-OR model, the adversary A has the ability to control all communications and can make the following queries:
  - Execute($\prod^t$, $\prod^u$): This query models the eavesdropping attack by trying to obtain a message sent between two honest communication participants.
  - Send($\prod^t$, m): An active attack is launched by this query. A communicate a message m to a participant instance $\prod^t$ and records the response.
  - CorruptSC($\prod_{U_i}^t$): This query launches a smart card lost attack revealing the details stored in the smart card.

  - Test($\prod^t$): The semantic security of the session key SK is modeled by this query and follows the R-OR model's indistinguishability [5]. A can make a test query to any fresh oracle at any time. At the beginning of the experiment a fair unbiased coin c is flipped. If answer is 1 the output is a randomly chosen session key. Otherwise, the output is the agreed session key of the test oracle.
- Semantic security of the session key: In the R-OR model, adversary A challenges the experiment to distinguish between the real session key SK of the instance and the random session key. A can execute a number of Test queries to either the user instance or the server instance. The result of the Test query must be consistent with respect to random bit c. At the end of the experiment, A returns a bit c'. If $c' = c$, A wins the game. Let $Succ$ denote the event that A wins the game. The advantage of A in breaking the semantic security of the protocol is $Adv_P^{ake} = 2|Pr[Succ] - 1|$. Therefore, if $Adv_P^{ake} \le \eta$, for any sufficiently small $\eta > 0$, P is a secure authentication protocol in the R-OR sense.
- Random oracle: In this paper, all participants and the adversary A use a one-way hash function $h(.)$ modeled as a Hash oracle.

The following difference lemma will be used in the formal security proof.

Lemma 1 (Difference Lemma): [33]: Let $Succ_1$, $Succ_2$ and $Succ_3$ denote the events defined in some probability distribution. Let $Succ_1 \wedge Succ_3 \Longleftrightarrow ?Succ_2 \wedge ?Succ_3$. Then, we have

$$|Pr[Succ_1] - Pr[Succ_2]| \le Pr[Succ_3].$$

The following theorem will establish the semantic security of the session key.

Theorem 2: Assume that adversary A is operating within polynomial time t for the proposed protocol P in a random oracle. Assume D represents uniformly distributed password dictionary and l denotes bit size of the biometrics key O_i. The probability of that the security of the session key of P is broken by A is as follows:

$$Adv_P^{ake} \le \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^{l-1}.|D|} + 2Adv^{ECCDHP}(t),$$

where q_h, $|HASH|$, q_{send}, $|D|$, and$Adv^{ECCDHP}(t)$ denote the number of Hash queries, the range space of the one-way hash function, the number of Send queries, the size of D, and the advantage of A in breaking the ECCDHP, respectively.

Proof 3: We define a sequence of games $G_i, 0 \le i \le 4$. Let $Succ_i$ denote success of A in guessing the bit c in the game G_i. The proposed protocol runs from game G_0 to game G_4 and the conclusion of the proof will show that A has a negligible advantage to break session key (SK)-security of P.

- **Game** G_0**:** This game is a real attack by the adversary against protocol P in the random oracle. The bit c is chosen at the beginning of this game. By definition, we have:

$$Adv_P^{ake}(A) = 2Pr[Succ_0] - 1 \tag{VII.1}$$

- **Game** G_1**:** This game simulates an eavesdropping attack of an adversary A using the Execute ($\prod^t, \prod^u$) oracle. The attacker also queries the Test oracle and checks whether the result is a real session key SK or some other random value. The session key SK is computed by the server S and user U_i as $SK = h(T_i||R_i||T_s||R_s||L_s)$; the timestamp introduces freshness to the session key. It is hard to compute $L_s = r_i r_s P$ due to the hardness of the ECCDH problem. Further, R_i, R_s cannot be computed due to the hardness of the ECDLP. Thus, the probability of adversary A winning this game through an eavesdropping attack does not increase. Then, G_0 and G_1 have the same probability, so we obtain:

$$Pr[Succ_0] = Pr[Succ_1] \tag{VII.2}$$

- **Game** G_2**:** This game is an extension of G_1, G_2 is simulated by *Send* and *Hash* oracles and Execute ($\prod^t, \prod^u$) and *Test* oracles. An active attack is modeled by adversary A sending fabricated messages to deceive the participants, and A repeatedly generates hash queries to obtain collisions. The login request $LR_i = \{R_i, T_i, Auth_i\}$ and the mutual authentication message $MA = (R_s, T_s, Auth_s)$ are associated with random numbers $r_i$andr_s and time stamps $t_i$andt_s. Therefore, the messages are guaranteed to be random and hence no collision will be obtained in querying the Send oracle. Using the birthday paradox [14] we obtain,

$$|Pr[Succ_1] = Pr[Succ_2]| \le \frac{q_h^2}{2|Hash|} \tag{VII.3}$$

- **Game** G_3**:** The CorruptSC oracle is simulated by this game and a lost smart card attack is launched. Adversary A can attempt a dictionary attack using the information from a smart card attempting to obtain password PW_i and biometric key O_i. A strong fuzzy extractor is used in the suggested protocol. Therefore, the probability that A can guess the biometric key O_i is approximately $\frac{1}{2^l}$ [45]. Since the system controls the number of wrong password inputs, we obtain the following:

$$|Pr[Succ_2] = Pr[Succ_3]| \le \frac{q_{send}}{2^l|D|} \tag{VII.4}$$

- **Game** G_4**:**In this game, adversary A tries to acquire session key SK through eavesdropping on the login request $LR_i = \{R_i, T_i, Auth_i\}$ and the mutual authentication message $MA = (R_s, T_s, Auth_s)$. As mentioned for G_1, it is hard to compute $L_s = r_i r_s P$ due to the hardness of the ECCDH problem. Further, r_i, r_s cannot be computed from the values R_i, R_s due to the hardness of the ECDLP. Thus, we obtain,

$$|Pr[Succ_3] = Pr[Succ_4]| \le Adv^{ECCDHP}(t) \tag{VII.5}$$

TABLE 5. **Definition and conversion of various operation units.**

Notations	Definition and conversion
T_{ML}	Time complexity for executing the modular multiplication.
T_{EX}	Time complexity for executing the modular exponentiation, $1T_{EX} \sim 240T_{ML}$.
T_{EM}	Time complexity for executing the elliptic curve scalar point multiplication, $1T_{EM} \sim 29T_{ML}$.
T_{BP}	Time complexity for executing the bilinear pairing operation, $1T_{BP} \sim 87T_{ML}$.
T_{EA}	Time complexity for executing the addition of two elliptic curve points, $1T_{EA} \sim 0.12T_{ML}$.
T_{IN}	Time complexity for executing the modular inversion operation, $1T_{IN} \sim 11.6T_{ML}$.
T_H	Time complexity for executing the simple hash function, which is negligible.
T_{FE}	Time complexity for executing the fuzzy extractor, which is negligible.
T_S	Time complexity for executing symmetric key encryption and decryption, which is negligible.

TABLE 6. **Computational overhead comparison.**

Protocols	Registration	Login, Authentication and Key Agreement Phase	Password Changing Phase	Total
Irshad et al.[27]	$4T_H + 1T_{EM} + 1T_S + 1T_{FE}$	$17T_H + 11T_{EM} + 4T_S + 1T_{FE}$	$8T_H + 1T_{EM} + 1T_{FE}$	$29T_H + 13T_{EM} + 5T_S$ $+3T_{FE} \sim 377T_{ML}$
Giri et al. [24]	$3T_H + 1T_{EX}$	$9T_H + 1T_{EX}$	$5T_H + 1T_{EX}$	$17T_H + 3T_{EX} \sim 720T_{ML}$
Amin and Biswas [8]	$5T_H$	$13T_H + 2T_{EX}$	$8T_H$	$26T_H + 2T_{EX} \sim 480T_{ML}$
Proposed	$2T_H + 1T_{FE}$	$9T_H + 5T_{EM} + 2T_S + 2T_{BP}$	$1T_H + 1T_{FE}$	$12T_H + 5T_{EM} + 2T_S$ $+2T_{FE} + 2T_{BP} \sim 319T_{ML}$

All session keys are random and independent and the c value is not exposed to Adversary A. Therefore, it is clear that

$$Pr[Succ_4] = \frac{1}{2} \tag{VII.6}$$

Combining the above equations and Lemma 1, we obtain the desired result as follows:

$$Adv_P^{ake} \le \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^{l-1}.|D|} + 2Adv^{ECCDHP}(t)$$

VIII. FURTHER SECURITY ANALYSIS

This section proves that the proposed protocol not only withstands various attacks but also satisfies the basic security requirement mentioned in prior studies.

A. PROVIDES PATIENT ANONYMITY

Patient anonymity means that nobody can obtain the real identity ID_i of any patient except the TMIS server. In the proposed protocol ID_i is concealed in $Auth_i = E_{k_i}(ID_i||T_i||r_i$. To get ID_i the adversary has to compute $K_i = e(P_{pub}, r_iQ_s)$. Without knowledge of r_i the adversary is unable to compute K_i with P_{pub} and Q_s in polynomial time. Therefore, the adversary cannot obtain the identity of any patient. That is, the proposed protocol provides patient anonymity.

B. PROVIDES PATIENT UNLINK-ABILITY

Patient unlink-ability means any adversary is unable to link two past authentication sessions by the same user. In each run protocol, the login request $LR_i = \{R_i, T_i, Auth_i\}$ and mutual authentication message $MA = (R_s, T_s, Auth_s)$ are different since r_i and r_s are different in each session. Hence, $Auth_i$ and $Auth_s$ will also be different between each session. Thus, an adversary cannot link two past authentication sessions by the same user. That is, the proposed protocol provides patient unlink-ability.

C. PROVIDES MUTUAL AUTHENTICATION

In the login and authentication phase of the proposed protocol U_i and S authenticate each other through the following verification processes. First, S verifies the login request $LR_i = \{R_i, T_i, Auth_i\}$ by checking whether $R_i = r_iQ_i$, and U_i verifies the mutual authentication message $MA = (R_s, T_s, Auth_s)$ by checking $Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_i)$. Hence, the proposed protocol provides mutual authentication.

D. PROTECTS AGAINST AN OFF-LINE GUESSING ATTACK

An attacker can get $\{V_i, W_i, P_{pub}, h_1, h_2, H_B\}$ from a stolen card and can intercept the login request $LR_i = \{R_i, T_i, Auth_i\}$. Any adversary may try to guess the password PW_i by retrieving these attributes. But, without knowledge of ID_i and B_i, the attacker cannot rightly guess PW_i.

E. PREVENTS PATIENT AND SERVER IMPERSONATION ATTACKS

To impersonate as a legitimate patient and cheat the TMIS server S, an attacker must compute a correct value $Auth_i = E_{k_i}(ID_i||T_i||r_i$. But A cannot compute $K_i = e(P_{pub}, r_iQ_s)$ without knowledge of r_i. Similarly, A cannot impersonate S to cheat U_i as A is unable to compute the correct value $Auth_s = h(T_i||R_i||T_s||R_s||L_s||K_s)$ without knowledge of the server private key s.

IX. PERFORMANCE EVALUATION AND COMPARISON

This section evaluates the performance of the proposed protocol compared with the protocols of Amin and Biswas [8], Giri *et al.* [24], and Irshad *et al.* [27] with respect to computational cost during registration, login authentication and key agreement and password changing. Generally, computation cost is examined based on the respective operations in the various phases of the protocol. Table 5 defines various computational complexities and their conversions in terms of T_{ML} as given in [26]. Table 6 summarizes the computation overhead of the proposed protocol and other relevant protocols [8], [24] and [27]. Table 7 also gives a comparative security analysis. Thus, from Tables 6 and 7, we conclude that the proposed protocol is more efficient and secure than existing protocols.

TABLE 7. Security comparison.

Features	Irshad et al.[27]	Giri et al. [24]	Amin and Biswas [8]	Proposed
User anonymity	yes	no	yes	yes
Mutual authentication	yes	yes	yes	yes
Off-line pw guessing attack	yes	no	no	yes
Impersonation Attacks	yes	yes	yes	yes
Replay attack	yes	no	no	yes
Provides formal security	yes	no	yes	yes

X. CONCLUSION

Remote health care for patients has drawn interest from researchers and industry. Remote health care includes services such as remote diagnosis, advice, treatment and assistance implemented mainly using information and communication technologies. As Tang and Venables [1] pointed out, smart homes and telecare are natural companions: smart homes make it possible to provide effective telecare services. The proliferation of telecare medical information system (TMIS) are consistently leading to the development of smart homes. Hence, in this paper, we proposed an efficient and secure, bilinear pairing based, mutual authentication and key agreement protocol for TMIS. The security of the proposed protocol is formally analyzed using the real-or-random (R-OR) model under the assumption of the hardness of the elliptic curve discrete logarithm problem (ECDLP) and elliptic curve computational Diffie Hellman problem (ECCDHP). Further, the protocol is resilient to all known attacks. In terms of computational costs during the various phases, the proposed protocol is also comparable to existing, related protocols.

ACKNOWLEDGEMENT

The research work was supervised by Sk Md Mizanur Rahman during his service in the Research Chair of Pervasive and Mobile Computing, Information Systems Department, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia.

REFERENCES

[1] P. Tang and T. Venables, "'Smart' homes and telecare for independent living," *J. Telemed. Telecare*, vol. 6, no. 1, pp. 8–14, 2000.

[2] A. Dutta-Roy, "Networks for homes," *IEEE Spectrum*, vol. 36, no. 12, pp. 26–33, Dec. 1999.

[3] A. Van Berlo, "A smart model house as research and demonstration tool for telematics developmen," in *Proc. 3rd TIDE Congr. Technol. Inclusive Design Equality Improving Quality Life Eur. Citizen*, Helsinki, Finland, 1998, p. 23.

[4] R. A. Brooks, "The intelligent room project," in *Proc. 2nd Int. Conf. Cogn. Technol. (CT)*, Aug. 1997, pp. 271–277.

[5] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, Jan. 2003, pp. 65–84.

[6] A. K. Awasthi and K. Srivastava, "A biometric authentication scheme for telecare medicine information systems with nonce," *J. Med. Syst.*, vol. 37, p. 9964, Oct. 2013. doi: 10.1007/s10916-013-9964-1.

[7] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 12, p. 136, Dec. 2014.

[8] R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement Protocol usable in TMIS," *J. Med. Syst.*, vol. 39, no. 8, p. 79, 2015.

[9] H. Arshad and M. Nikooghadam, "An efficient and secure authentication and key agreement scheme for session initiation Protocol using ECC," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 181–197, Jan. 2016.

[10] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient Protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, Dec. 1993, pp. 62–73.

[11] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Proc. Annu. Int. Cryptol. Conf.*, 1993, pp. 232–249.

[12] M. Bellare and P. Rogaway, "Provably secure session key distribution: The three party case," in *Proc. STOC*, vol. 95, Jun. 1995, pp. 57–66.

[13] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, May 2000, pp. 139–155.

[14] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-authenticated key exchange using Diffie-Hellman," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2000, pp. 156–171.

[15] F. T. B. Muhaya, "Cryptanalysis and security enhancement of Zhu's authentication scheme for telecare medicine information system," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 149–158, Jan. 2015.

[16] A. T. S. Chan, J. Cao, H. Chan, and G. Young, "A Web-enabled framework for smart card applications in health services," *Commun. ACM.*, vol. 44, no. 9, pp. 76–82, Sep. 2001.

[17] H.-M. Chen, J.-W. Lo, and C.-K. Yeh, "An efficient and secure dynamic Id-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3907–3915, Dec. 2012.

[18] T. Cao and J. Zhai, "Improved dynamic id-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 2, p. 9912, Apr. 2013.

[19] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, May 2004, pp. 523–540.

[20] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1989–1995, Jun. 2012.

[21] A. K. Das, V. Odelu, and A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS," *J. Med. Syst.*, vol. 39, no. 9, p. 92, Sep. 2015.

[22] A. K. Das, "A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems," *J. Med. Syst.*, vol. 39, no. 3, p. 30, Mar. 2015.

[23] D. B. David, "Mutual authentication scheme for multimedia medical information systems," *Multimedia Tools Appl.*, vol. 76, no. 8, pp. 10741–10759, Apr. 2017.

[24] D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, "An efficient and robust RSA-based remote user authentication for telecare medical information systems," *J. Med. Syst.*, vol. 39, no. 1, p. 145, Jan. 2015. doi: 10.1007/s10916-014-0145-7.

[25] D. Hankerson, S. Vanstone, and A. Menezes, "Elliptic curve arithmetic," in *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004, pp. 75–152.

[26] S. K. H. Islam and G. P. Biswas, "A pairing-free identity-based authenticated group key agreement Protocol for imbalanced mobile networks," *Ann. Telecommun.*, vol. 67, nos. 11–12, pp. 558–574, Dec. 2012.

[27] A. Irshad, M. Sher, O. Nawaz, S. A. Chaudhry, I. Khan, and S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin *et al.* scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16463–16489, Aug. 2017.

[28] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A privacy enhanced authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 1, p. 9897, 2013.

[29] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 2, p. 12, Feb. 2014.

[30] M. K. Khan and S. Kumari, "An authentication scheme for secure access to healthcare services," *J. Med. Syst.*, vol. 37, no. 4, p. 9954, Aug. 2013.

[31] S.-H. Li, C.-Y. Wang, W.-H. Lu, Y.-Y. Lin, and D. C. Yen, "Design and implementation of a telecare information platform," *J. Med. Syst.*, vol. 36, no. 3, pp. 1629–1650, Jun. 2012.

[32] H. Y. Lin, "On the security of a dynamic ID-based authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 2, p. 9929–9934, Jan. 2013.

[33] T.-F. Lee, "Provably secure anonymous single-sign-on authentication mechanisms using extended Chebyshev chaotic maps for distributed computer networks," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1499–1505, Jun. 2018.

[34] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 39, no. 3, p. 32, Mar. 2015.

[35] D. Mishra, J. Srinivas, and S. Mukhopadhyay, "A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 10, p. 120, Oct. 2014.

[36] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. K. Khan, "Cryptanalysis and improvement of Yan *et al.*'s biometric-based authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 6, p. 24, Jun. 2014.

[37] O. Mir and M. Nikooghadam, "A secure biometrics based authentication with key agreement scheme in telemedicine networks for E-health services," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 2439–2461, Aug. 2015.

[38] O. Mir, T. van der Weide, and C.-C. Lee, "A secure user anonymity and authentication scheme using AVISPA for telecare medical information systems," *J. Med. Syst.*, vol. 39, no. 9, p. 89, Sep. 2015.

[39] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: Three factor cloud based user authentication for telecare medical information system," *J. Med. Syst.*, vol. 38, p. 9997, Jan. 2014. doi: 10.1007/s10916-013-9997-5.

[40] H. Takeda, Y. Matsumura, S. Kuwata, H. Nakano, N. Sakamoto, and R. Yamamoto, "Architecture for networked electronic patient record systems," *Int. J. Med. Inform.*, vol. 60, no. 2, pp. 161–167, Nov. 2000.

[41] Z. Tan, "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 3, p. 16, Mar. 2014.

[42] Z.-Y. Wu, Y.-C. Lee, F. Lai, H.-C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 3, pp. 1529–1535, Jun. 2012.

[43] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3597–3604, Dec. 2012.

[44] F. Wen and D. Guo, "An improved anonymous authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 38, no. 5, p. 26, May 2014.

[45] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu, "Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1983–2001, Sep. 2016.

[46] X. Xu, P. Zhu, Q. Wen, Z. Jin, H. Zhang, and L. He, "A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 1, p. 9994, 2013.

[47] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems," *J. Med. Syst.*, vol. 37, no. 2, p. 9911, 2013.

[48] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *J. Med. Syst.*, vol. 36, no. 6, pp. 3833–3838, Dec. 2012.

SHAHEENA KHATOON received the B.Sc., M.Sc. (Hons.), and MPhil. degrees in mathematics from Pt. Ravishankar Shukla University, India, in 2005, 2007, and 2009, respectively. She joined Pt. Ravishankar Shukla University for her research work, where she is currently a full-time Research Scholar. Her research interests include public key cryptography, information security, and applied mathematics. She is a Life Member of the Cryptology Research Society of India and a Student Member of the IEEE.

SK MD MIZANUR RAHMAN received the Ph.D. degree in engineering (major in cybersecurity risk engineering) from the Laboratory of Cryptography and Information Security, Department of Risk Engineering, University of Tsukuba, Japan, in 2007. He was an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences, King Saud University, for five years. He also worked for several years in cryptography and security engineering in the high-tech industry in Ottawa, ON, Canada. He was a Postdoctoral Researcher with the University of Ottawa, the University of Ontario Institute of Technology (UOIT), and the University of Guelph, Canada, for several years. He is currently a full-time Professor with the Department of Information and Communication Engineering Technology, School of Engineering Technology and Applied Science, Centennial College. He has published approximately 100 peer-reviewed journal and conference research articles. He has a granted industrial patent (U.S. Patent) on cryptographic key generation and protection. His primary research interests include cryptographic protocol design, software and network security, reverse engineering and ethical hacking, privacy enhancing technology, machine learning for information security, sensor and mobile ad hoc network security, cloud and the Internet of Things (IoT) security, block chain, and cryptocurrency. He received the Digital Courier Funai Young researcher Encouragement Award for his excellent contributions to IT security research from the Information Processing Society Japan (IPSJ). He received a Gold Medal for distinction in his undergraduate and graduate programs.

MAJED ALRUBAIAN received the Ph.D. degree from the Department of Information Systems, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, in 2017. He has published several papers in refereed journals, including the IEEE, ACM, Springer, and Wiley. His research interests include social media analysis and mining data, information credibility, security informatics, and machine learning. He received the Best Ph.D. Thesis Award from CCIS, KSU, in 2017.

ATIF ALAMRI received the Ph.D. degree in computer science from the School of Information Technology and Engineering, University of Ottawa, Canada, in 2010. He is currently a Full Professor with the Software Engineering Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. He is one of the founding members of the Chair of Pervasive and Mobile Computing (CPMC), CCIS, KSU, successfully managing its research program, which transformed the chair as one of the best chairs of research excellence in the college. His research interests include multimedia-assisted health systems, ambient intelligence, service-oriented architecture, multimedia cloud, sensor cloud, the Internet of Things, big data, mobile cloud, social networks, and recommender systems.