Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems

Mohamed Mohammedi[1], Mawloud Omar[1]*, Wassila Aitabdelmalek[1], Abla Mansouri[1], and Abdelmadjid Bouabdallah[2]
[1] Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes,
Université de Bejaia, 06000 Bejaia, Algérie.
[2] Sorbonne universités, Université de technologie de Compiègne,
CNRS, Heudiasyc UMR 7253, CS 60 319, 60 203 Compiègne cedex, France.
E-mail: * mawloud.omar@gmail.com

***Abstract*—Recently, the home healthcare system has emerged as one of the most useful technology for e-healthcare. Contrary to classical recording methods of patient's medical data, which are, based on paper documents, nowadays all this sensitive data can be managed and forwarded through digital systems. These make possible for both patients and healthcare workers to access medical data or receive remote medical treatment using wireless interfaces whenever and wherever. However, simplifying access to these sensitive and private data can directly put patient's health and life in danger. In this paper, we propose a secure and lightweight biometric-based remote patient authentication scheme using elliptic curve encryption through which two mobile healthcare system communication parties could authenticate each other in public mobile healthcare environments. The security and performance analysis demonstrate that our proposal achieves better security than other concurrent schemes, with lower storage, communication and computation costs.**

***Index Terms*—Security, Biometric, Remote authentication, Healthcare system.**

I. Introduction

The recent technological advances in wireless communications, low-power microelectronics integration, miniaturized sensors, and the Internet are revolutionizing the healthcare domain [21]. They provide relatively low cost and power wearable solutions to enable e-healthcare users to have flexibility and mobility [19]. These make possible to provide healthcare and patient monitoring at anytime and anywhere [2] [19]. Nowadays, mobile healthcare system has emerged as one of the most useful technologies for e-healthcare. From this system, patients can receive medical service they usually need in their homes without going physically to be treated face-to-face in the hospital [11]. Through Wireless Body Area Networks (WBANs) [2], patient's vital signs, such as blood sugar, pulse oximeter, heart rate, and blood pressure, etc., are constantly measured. These vital signs must be monitored remotely in real-time by a doctor via a Graphical User Interface (GUI), then processed and forwarded to medical databases on hospital server [17] [18]. Afterwards, this sensitive and private data can be accessed by different authorized users, including healthcare staff, researchers, and government agencies; to provide immediate medical assistance in case of emergency or in situations representing a danger to the patient's life [9] [13] [18]. Nevertheless, the accessibility to this medical data of a particular registered patient must not be allowed for all the users. For instance, clinicians are only permitted to access the medical data related to their patients but, they do not have the right to access other patients' medical data [9] [18]. The communication of patient's medical data through wireless networks between the patient's mobile device and remote server plays a censorious role in remote medical diagnosis. Indeed, wrong or unauthenticated medical data may put the patient's life in danger. Therefore, a secure authentication may help to ensure the security of the exchanged medical data between patient's mobile device and remote server to protect patient's privacy. In order to provide a greater security of the system and overcome security flaws, some user authentication schemes using passwords and smart cards have been proposed [3] [14] [16]. However, passwords are not only difficult to remember in case of emergencies, but also ineffective in deterring guessing attacks [11], and smart cards might be shared, lost, stolen [3], misplaced, or willingly given to an unauthorized user [8]. Contrary to classical authentication methods, biometrics-based authentication schemes have no such drawbacks [3], and can offer higher security and reliability for user authentication [12] [23]. The reason for this, is biometric systems frees the user to remember something or keep a physical object in their possession [20]. In addition, biometric features do not change over the time [12], are hard to share or forge, and might not be lost or forgotten [15]. In the literature, some biometric-based remote user authentication schemes have been proposed [1] [22]. In [8], Awasthi and Srivastava have proposed a biometric based remote user authentication scheme for telecare medicine information systems. The authors have claimed that their scheme is able to provide higher security and be practical. However, in [6], Mishra et al. have demonstrated that this scheme is vulnerable to password guessing attack, and it does not provide efficient password change. In the same year, in [7], Tan, showed that Awasthi and Srivastava's scheme

978-1-5386-4690-8/18/$31.00 2018 IEEE

is vulnerable to other attacks, such as it does not resist to the reflection attacks, it does not achieve three-factor (smart card, password, biometric) security and it is unable to protect users anonymity. To overcome these flaws, an improvement of Awasthi and Srivastava's scheme was proposed by Tan and he has claimed that the improved scheme ensure security against various attacks. However, in [5], Arshad and Nikooghadam have demonstrated that the Tan's scheme is not secure against replay attack and denial-of-service attack. Further, the authors have proposed an improved ECC based scheme overcoming the above-mentioned attacks. They have claimed that their scheme not only withstands various attacks, but also is more efficient than the Tan's scheme and is more suitable for telecare medicine information systems. However, in [4], Lu et al. have demonstrated that their scheme is unable to protect against impersonation attack and off-line password guessing attack. Then, they have proposed an improved scheme overcoming these attacks. The improved scheme provides sufficient security against various attacks. However, it presents some performance limits regarding the storage, computation and communication costs.

In this paper, we propose a new biometric-based authentication scheme for mobile healthcare system using mobile devices, biometric inputs and Elliptic Curve Cryptography (ECC). Our proposal combines the patient's biometric template with ECC technique to generate the key pair, which is computationally derived from that template. When a remote diagnostic is required or an unexpected incident underwent on the health of a given patient, the later can be authenticated by the remote server without requiring to save or communicate the patient's biometric template. The security analysis and simulation results demonstrate that our proposal is appropriated for use in practical healthcare applications.

The remaining of this paper is structured as follows. In Section II, we present a detailed description of our proposed scheme. Then, the security and performance analysis are provided in Section III and IV, respectively. Finally, Section V concludes the paper.

II. The proposed scheme

In this section, we give the detailed description of our biometric-based remote patient authentication scheme between two communication parties, namely (1) the patient P_i's mobile device, which executes all the operations performed by the corresponding patient; and (2) the remote server S of mobile healthcare system in the hospital for collecting and managing the patient's medical information. The proposed scheme consists of three phases, namely the system initialization, the patient registration, and the mutual authentication with a session key agreement, which are described in the following subsections. Before presenting the operations of each phase, some important notations used through this paper are recapitulated in Table I.

TABLE I
Notations

Notation	Description
P_i	The patient i
S	The remote server
ID_i	The patient P_i's identity
$\widehat{K}_S$, K_S	The remote server S's private and public keys
$\widehat{K}_i$, K_i	The patient P_i's private and public keys
$\langle\rangle_{K_j}$	Encryption operation using public key K_j
$E_q(a,b)$	An elliptic curve equation with order n
n	A large number
G	The base point with the order n over $E_q(a,b)$
B_i	The patient P_i's biometric template
M_i	The patient P_i's alert message
SN_i	The patient P_i's mobile device serial number
SK	Session key
H	A collision free one-way secure hash function
$\langle +, -, \cdot \rangle$	Elliptic curve point addition, subtraction and multiplication
$\|\|$	Concatenation operation
$\bigoplus$	Bit-wise exclusive-or (XOR) operation

A. System initialization phase

This process is executed between two communication parties once at the system initialization time, to initialize and select some parameters of the system, and compute ECC key pair, which will be used by both the remote server S and patient P_i's mobile device during the registration and authentication phases. In the server side, S chooses an elliptic curve equation $E_q(a,b)$ [1] with order n, where n is a large number for the security considerations and selects a base point G with order n over $E_q(a,b)$. Afterwards, the remote server S chooses a number $\widehat{K}_S$ as a private key, where $\widehat{K}_S \in [1, n-1]$ and computes its corresponding public key $K_S = \langle Q_S, G \rangle$, where $Q_S = \widehat{K}_S.G$. In the patient side, the patient P_i's mobile device also computes its key pair $\langle \widehat{K}_i, K_i \rangle$ by using the biometric reader. The mobile device extracts the patient P_i's biometric template B_i from which the patient P_i's mobile device computes its own private key $\widehat{K}_i = H(B_i||r_i||SN_i)$, where r_i (such as $r_i \in [1, n-1]$) and SN_i represent a random number and the serial number of the patient P_i's mobile device, respectively. Finally, after generating the private key, the patient's mobile device derives its public key $K_i = \langle Q_i, G \rangle$, where $Q_i = \widehat{K}_i.G$. Note that it is hard to forge the patient P_i's private key $\widehat{K}_i$ from Q_i and G due to the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP).

[1] An elliptic curve $E_q(a,b)$ is defined over a finite field F_q ($q > 3$ and is a large prime number), by the following equation: $y^2 \ mod \ q = x^3 + ax + b \ mod \ q$, where a and b are integers satisfying the following condition: $4a^3 + 27b^2 \ mod \ q \neq 0$. The points of an elliptic curve are therefore (x, y) pairs, with real numbers x and y, which satisfy the following equation: $y^2 \ mod \ q = x^3 + ax + b \ mod \ q$ [10].

B. Patient registration phase

This process is operated when a patient P_i attempts to register itself in the system. Initially, the patient P_i freely chooses his/her identity ID_i. Then, he/she introduces his/her biometrics by using the biometric reader of the mobile device to obtain the template B_i. Afterwards, the patient's mobile device computes $A_i = H(\widehat{K}_i||ID_i)$ and sends the registration request $\langle ID_i, K_i, A_i \rangle_{K_S}$ to the remote server. Upon receiving the P_i's registration request, the remote server S decrypts the registration request message using its own private key $\widehat{K}_S$, and checks the unicity of patient's identity ID_i. If patient's identity ID_i already exists in its database, the remote server S requests the patient P_i for another identity ID_i. Otherwise, the remote server S computes some security parameters as follows: $E_i = H(ID_i||T||\widehat{K}_S)$, and $W_i = E_i \bigoplus A_i = H(ID_i||T||\widehat{K}_S) \bigoplus H(\widehat{K}_i||ID_i)$, where T denotes the current timestamp of the remote server S. Finally, the remote server S saves $\langle ID_i, W_i \rangle$ in its locally for the future authentication and sends $\langle ID_i, A_i, W_i \rangle_{K_i}$ to the patient's mobile device.

C. Mutual authentication

This process is operated when a body medical sensor of a monitored patient detects an abnormal situation in the captured vital signs. Further to an abnormal situation on patient's health, the body medical sensor triggers an alert message M_i. This alert message is automatically communicated to the patient P_i's mobile device. Following this release of alert message, the authentication phase starts. The detailed steps of this phase are presented as follows:

- **Step-1:** Initially, the patient P_i inputs his/her identity ID_i. Then, using an appropriate biometric reader, the patient P_i's introduces his/her biometrics allowing the extraction of the biometric template B_i, from which the patient P_i's mobile device computes its key pair $\langle \widehat{K}_i, K_i \rangle$. Afterwards, the patient's mobile device P_i computes $A'_i = H(\widehat{K}_i||ID_i)$, and verifies whether A'_i is equal to the already stored $A_i = H(\widehat{K}_i||ID_i)$ or not. If the two are not equal, the patient authentication process terminates immediately. Otherwise, the patient's mobile device selects a random number $r_i \in [1, n-1]$ and computes $R_i = r_i.G$, $R'_i = r_i.K_S = r_i.\widehat{K}_S.G$, $E_i = W_i \bigoplus H(\widehat{K}_i||ID_i)$, $PID_i = ID_i \bigoplus H(R'_i)$, $PAM_i = M_i \bigoplus H(R'_i)$, and $\theta = H(ID_i||E_i||R_i||R'_i||M_i||T_i)$, where T_i denotes the current timestamp of the mobile device. Furthermore, the patient's mobile device sends the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$ to the remote server S over an insecure channel. Finally, the patient's mobile device waits for a period of time, which depend of the type of alert message. If it does not receive any acknowledgement from the remote server S, the patient's mobile device sends back the same alert message.
- **Step-2:** After receiving $\langle PID_i, R_i, \theta, PAM_i, T_i \rangle$, the remote server S checks the timestamp validity, such as $T_S - T_i \leq \Delta T$, where T_s and ΔT denote, respectively, the current timestamp of the remote server and the expected valid time interval for a transmission delay. If it is incorrect, S rejects the login request, otherwise, the remote server S computes $R'_i = \widehat{K}_S.R_i$, and then extracts $ID_i = PID_i \bigoplus H(R'_i)$, checks the validity of ID_i. If it is not valid, the remote server S rejects the login request; otherwise, the remote server S extracts the alert message $M_i = PAM_i \bigoplus H(R'_i)$ then checks whether θ and $H(ID_i||E_i||R_i||R'_i||M_i||T_i)$ are equal. If they are not equal, S rejects the login request; otherwise, the remote server S authenticates the patient P_i, and then generates a random number $r_s \in [1, n-1]$, computes $R_s = r_s.G$, $R'_s = r_s.K_i = r_s.\widehat{K}_i.G$, $C_i = M_i \bigoplus H(R'_s)$, and $\gamma = H(ID_i||E_i||R_s||R'_s||M_i||T_s)$, where T_s is the current timestamp of the remote server S. Afterwards, it computes the session key SK to be shared with the patient's mobile device, such as $SK = r_s.R_i = r_s.r_i.G$. Finally, the remote server S computes the response, which is an acknowledgement such as $\langle R_s, R_i, \gamma, C_i, T_s \rangle$, and sends it to the patient's mobile device.
- **Step-3:** After receiving $\langle R_s, R_i, \gamma, C_i, T_s \rangle$, the patient P_i's mobile device checks the validity of the timestamp by $T_i - T_S \leq \Delta T$. If it is incorrect, a replay attack could be suspected and then, the patient P_i's mobile device rejects the login request. Otherwise, the patient's mobile device computes $R'_s = \widehat{K}_i.R_s$, extracts $M_i = C_i \bigoplus H(R'_s)$, and then verifies the validity of alert message M_i. If the alert message verification fails, the patient's mobile device considers the remote server S as illegitimate and the authentication process terminates immediately. Otherwise, the patient P_i's mobile device checks whether γ and $H(ID_i||E_i||R_s||R'_s||M_i||T_s)$ are equal. If they are not equal, the patient P_i's mobile device rejects the login request. Otherwise, the patient P_i authenticates the remote server S and computes the common secret session key SK shared with the remote server S, such as $SK = r_i.R_s = r_i.r_s.G$. Finally, the patient P_i's mobile device computes $\delta = H(ID_i||R_i||R_s||SK)$ and sends $\langle \delta \rangle$ to the remote server S.
- **Step-4:** After receiving $\langle \delta \rangle$ from the patient P_i's mobile device, the remote server S computes $\delta' = H(ID_i||R_i||R_s||SK)$ and verifies whether the computed δ' is equal to the received δ. If the two are not equal, the remote server S rejects the login request; otherwise, the remote server S believes that the patient P_i is an authentic remote party. Finally, mutual authentication process between patient P_i's mobile device and remote server S is completed successfully. Therefore, the computed secret session key SK can be used by the two communication parties for their confidential future communication.

III. Security analysis

In this section, we analyse the security of our proposed scheme by showing its resistance to various malicious attacks as described below.

A. Replay attack

Assume that an adversary intercepts the login request $\langle PID_i, R_i, \theta, PAM_i, T_i\rangle$ sent out from the patient P_i's mobile device to the remote server S and tries to impersonate the legitimate patient P_i. If the adversary replays the same intercepted request, the remote server S could obviously detect the attack by checking the validity of $T_S - T_i \leq \Delta T$. If it is incorrect, the adversary will not be considered as legitimate patient, therefore, the remote server S will reject the login request. Inversely, the adversary cannot impersonate the legitimate remote server S just by replaying the intercepted login request $\langle R_s, R_i, \gamma, C_i, T_s\rangle$ to the patient P_i's mobile device, because the later can easily detect the attack by checking the validity of $T_i - T_S \leq \Delta T$. In addition, the remote server S can easily detect the forged request by checking the correctness of $\delta = H(ID_i||R_i||R_s||SK)$ in the fourth step of the authentication phase since both R_i and R_s will be frequently changed in each session. Therefore, we conclude that our proposed scheme can provide the security against replay attack.

B. Impersonation attack

Assume that an adversary intercepts a valid login request message sent out from the patient P_i's mobile device $\langle PID_i, R_i, \theta, PAM_i, T_i\rangle$ or from the remote server $\langle R_s, R_i, \gamma, C_i, T_s\rangle$ of previous sessions of the protocol. However, the adversary has no way to create a forged request message for the fresh timestamps T_i and T_S without knowing the patient and server private keys ($\widehat{K}_i$, $\widehat{K}_S$). Conversely, the adversary cannot impersonate both the patient P_i's mobile device and the remote server S without knowing $\widehat{K}_i$ and $\widehat{K}_S$. Therefore, we conclude that our proposed scheme can resist against impersonation attack.

C. Server spoofing attack

Assume that an adversary intercepts the request message $\langle PID_i, R_i, \theta, PAM_i, T_i\rangle$ of a previous sessions of the protocol and attempt to masquerade as the remote server S to discover the patient's long-term secret. However, it is impossible for an adversary to extract the original identity ID_i from PID_i, and the patient P_i's alert message M_i from PAM_i without holding server S's private key $\widehat{K}_S$. In addition, it is also not possible to forge a valid login request message $\langle R_s, R_i, \gamma, C_i, T_s\rangle$ without server S's private key $\widehat{K}_S$ and E_i. Consequently, the adversary cannot get success in Step-2 of the authentication phase. Therefore, we conclude that our proposed scheme has the ability to successfully prevent the server spoofing attack.

D. Privileged insider attack

In our scheme, the patient P_i's registers himself to the remote server S by sending $\langle ID_i, K_i, A_i\rangle_{K_S}$. Since $\langle ID_i, K_i, A_i\rangle$ is encrypted by the server S's private key $\widehat{K}_S$, the privileged-insider is unable to figure out A_i from the bloc $\langle ID_i, K_i, A_i\rangle_{K_S}$ without server S's private key. In addition, he cannot obtain $\widehat{K}_i$ from $A_i = H(\widehat{K}_i||ID_i)$ due to the one-way property of the hash function. Hence, the privileged-insider who is unable to authenticate himself to the remote server S, cannot impersonate the legal patient to access the remote server S without holding patient P_i's private key $\widehat{K}_i$. Therefore, we conclude that our proposed scheme can resist the privileged-insider attack.

E. User anonymity

Assume that an adversary intercepts the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i\rangle$ sent out from the patient P_i to the remote server S. However, the adversary is unable to figure out the original patient's identity ID_i from $PID_i = ID_i \bigoplus H(R'_i)$. For the reason that to extract the original patient's identity ID_i, the adversary has to compute R'_i using R_i and K_S. However, it computationally impossible due to difficulties of the computational Diffie-Hellman problem (CDHP). Therefore, we conclude that our proposed scheme preserves thoroughly the patient anonymity and the original patient's identity ID_i cannot be known anymore.

F. Modification attack

Assume that an adversary intercepts the login request message $\langle PID_i, R_i, \theta, PAM_i, T_i\rangle$ sent out from the patient P_i's mobile device. Then, the adversary modifies the intercepted message and sends it to the remote server S. However, this attack cannot success because the remote server S can easily detect the attack by verifying the correctness of θ. Inversely, the patient P_i's mobile device can detect the attack just by verifying the validity of the communicated messages. Therefore, we conclude that our proposed scheme provides security against modification attack.

G. Man-in-the-Middle attack

Assume that an adversary who is in the middle of patient P_i's mobile device and remote server S attempts to masquerade both mobile device and remote server by creating a fake login request message for authentication. However, the adversary cannot success this type of attack because he/she cannot create a valid login request message without knowing some secret parameters. Therefore, we conclude that our proposed scheme can resist the man-in-the-middle attack.

IV. Performance evaluation

In this section, we provide the simulation results comparing our proposed scheme, with three relevant biometrics-based authentication schemes for tele-care medicine information systems, that is, Tan's scheme [7], Arshad and Nikooghadam's scheme [5], and Lu et al.'s scheme [4].

The simulations of our proposed scheme and other concurrent ones [7], [5] and [4] are developed on a Samsung Galaxy $S6$ smartphone with the following system configuration of processor speed of 2.1 GHz, RAM rate of 3 Go, capacity of memory card of 32 Go, and a wireless transmission rate of 5.76 Mbps. The smartphone interacts with a remote server machine characterized by a processing rate of 2.3 GHz, a memory of 4 Go, hard-disk capacity of 260 Go, and a wireless

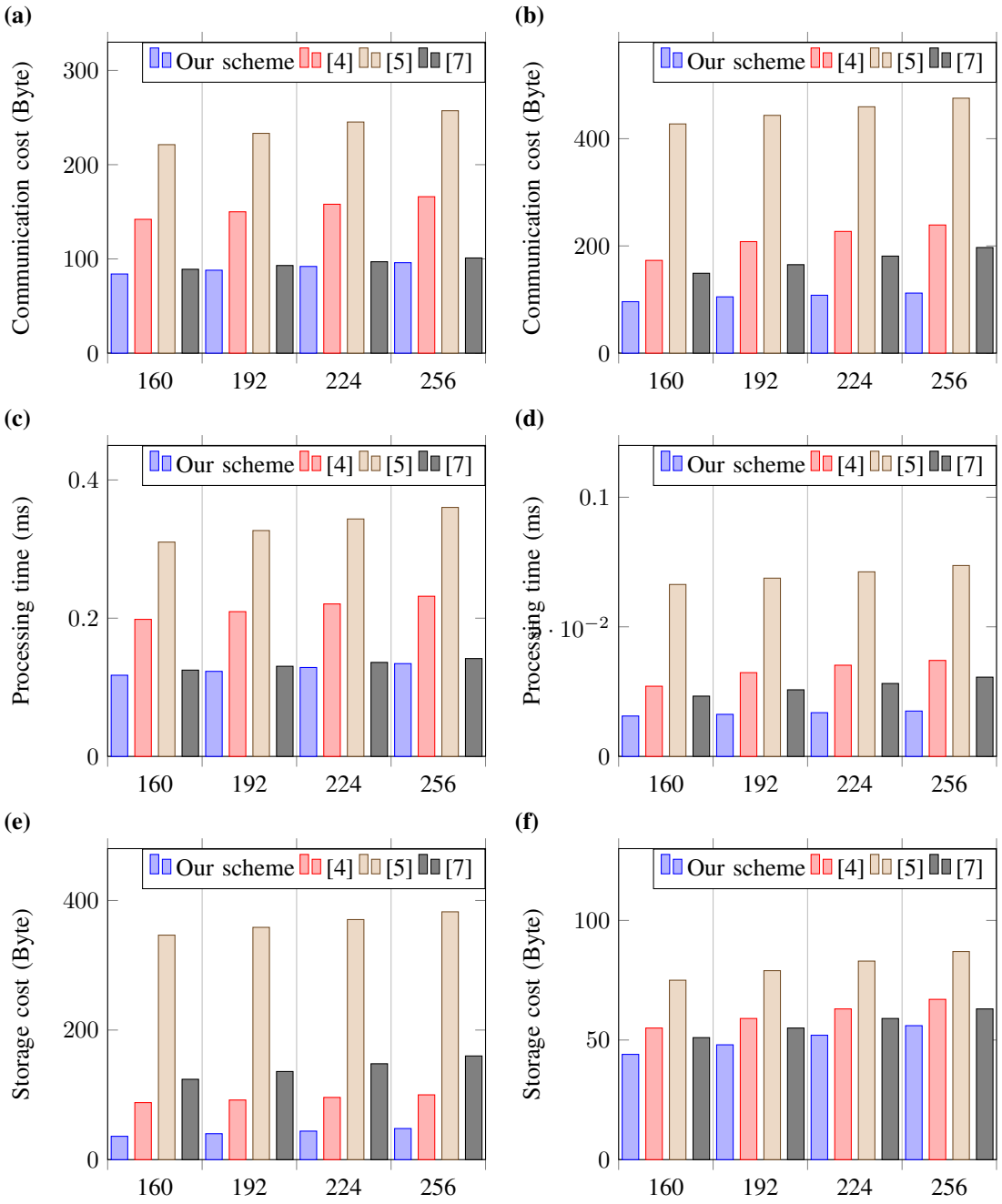

Fig. 1. Communication, processing and storage evaluation in mobile device and remote server sides per session of authentication

transmission rate of 54 Mbps. Before given the simulation results, we firstly start, by specifying the three major metrics that we have considered to be interesting to study: (1) the communication cost, which represents total number of packet sent out from patient's mobile device or remote server machine S per session of authentication, (2) the processing time, which represents the required time involved in the execution of a scheme per session of authentication, and (3) the storage cost, which represents the memory space required for the system parameters, which are required to be stored per session of authentication. We have evaluated these metrics following different ECC key size, namely: 160, 192, 224, and 256 bits.

Figure (a) and (b), show the obtained results for the communication cost, respectively, in mobile device and remote server side. As expected, the communication overhead increases for both our proposal and for all the compared schemes when the ECC key size increases. From the Figure (a) and (b), it is clear that the performance of our proposal is very higher than the other schemes. Indeed, our proposal require 5 message exchanges, while Tan's scheme [7], requires

4 exchanges, achieving better results compared to the schemes of Lu et al. [4], and Arshad and Nikooghadam [5], which require 5 exchanges.

Figure (c) and (d), show the obtained results for the processing time, respectively, in mobile device and remote server side. As expected, the processing time increases for both our proposal and for all the compared schemes when the ECC key size increases. From the Figure (c) and (d), it is clear that the performance of our proposal is very higher than the other schemes. In fact, our scheme performs the mutual authentication process in three rounds of communication. During the registration and authentication phases, both mobile device and remote server perform less number of hash and ECC operations, while the other schemes perform an important number of hash and ECC operations, which are necessarily required to achieve the authentication process.

Figure (e) and (f), show the obtained results for the storage cost, respectively, in mobile device and remote server side. Obviously, when the ECC key size increases, it is expected that the storage cost respectively, in mobile device and remote server side increases for our proposal and for all the compared schemes. The results indicate that the performance of our proposal is very higher than the other schemes. In the case of our scheme, there is one and two cryptographic parameters stored per one patient, respectively, in patient's mobile device and remote server side, and all the other parameters and keys are dynamically computed. In the case of the other schemes, there are many cryptographic parameters, which are required to be stored in both mobile device and remote server side for the future authentication process.

V. Conclusion

Mobile healthcare system provides medical service to patients in their own homes without visiting hospital. This type of system offers great rapidness for clinicians, chemists, nurses, and patient in medical service. However, access to patient's vital signs or receive remote medical treatment using wireless interfaces, can directly put patient's life in danger. Therefore, it is more important to secure these critical data exchanged among the two communication parties. In this paper, we have proposed a secure and lightweight biometric-based remote patient authentication scheme for mobile healthcare systems to ensure the security of the exchanged medical data between the two communication parties. Through security and performance analysis, we have proved that our proposed scheme offers several advantages: it is secure against several malicious attacks, it is efficient in terms of storage, computation and communication costs, it is faster, and it can be easily implemented in a modern smartphone environment. As a result, our proposed scheme is extremely suitable, particularly for practical applications in mobile healthcare environments compared with other concurrent schemes since it provides higher security, reliability, and lower communication and computational costs.

References

[1] Y. Lin, K. Wang, B. Zhang, Y. Liu, and X. Li. "An enhanced biometric-based three factors user authentication scheme for multi-server environments", International Journal of Security and Its Applications, 10 (1), (pp. 315-328), 2016.

[2] M. Aqsa, Q. Junaid, A. Basharat, A.Y. Kok-Lim, and U. Ubaid. "QoS in IEEE 802.11-based wireless networks: A contemporary review", Journal of Network and Computer Applications, 55, (pp. 24-46), 2015.

[3] D. He, and D. Wang. "Robust biometrics-based authentication scheme for multiserver environment", IEEE Systems Journal, 9 (3), (pp. 816-823), 2015.

[4] Y. Lu, L. Li, H. Peng, and Y. Yang. "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem", Journal of Medical Systems, 39 (3), (pp. 1-8), 2015.

[5] H. Arshad, and M. Nikooghadam. "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems", Journal of Medical Systems, 38 (12), (pp. 1-12), 2014.

[6] D. Mishra, S. Mukhopadhyay, S. Kumari, M.K. Khan, and A. Chaturvedi. "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce", Journal of Medical Systems, 38 (5), (pp. 1-11), 2014.

[7] Z. Tan. "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems", Journal of Medical Systems, 38 (3), (pp. 1-9), 2014.

[8] A.K. Awasthi, and K. Srivastava. "A biometric authentication scheme for telecare medicine information systems with nonce", Journal of Medical Systems, 37 (5), (pp. 1-4), 2013.

[9] S. Chatterjee, A.K. Das, and J.K. Sing. "A novel and efficient user access control scheme for wireless body area sensor networks", Journal of King Saud University Computer and Information Sciences, 26 (2), (pp. 181-201), 2013.

[10] S.K.H. Islam, and G.P. Biswas. "Design of improved password authentication and update scheme based on elliptic curve cryptography", Mathematical and Computer Modelling, 57(11-12), (pp. 2703-2717), 2013.

[11] Q. Jin, W. Jeon, C. Lee, Y. Choi, and D. Won. "Fingerprint-based user authentication scheme for home healthcare system", In: Proceedings of the 5^{th} International Conference on Ubiquitous and Future Networks, (pp. 178-183), 2013.

[12] G.M.A. Sagayee, S. Arumugam, and G.S.A. Mala. "Biometric encryption using enhanced fingerprint image and elliptic curve", International Journal of Computer Science and Network Security, 13 (7), (pp. 106-112), 2013.

[13] K. Elgazzar, M. Aboelfotoh, P. Martin, and H.S. Hassanein. "Ubiquitous health monitoring using mobile web services", In: Proceedings of the 3^{rd} International Conference on Ambient Systems, Networks and Technologies, (pp. 332-339), 2012.

[14] C.T. Li, and C.C. Lee. "A novel user authentication and privacy preserving scheme with smart cards for wireless communications", Mathematical and Computer Modelling, 55 (1–2), (pp. 35-44), 2012.

[15] R. Moganeshwaran, M.K. Hani, and M.A. Suhaini. "Fingerprint-fingervein multimodal biometric authentication system in field programmable gate array", In: Proceedings of the International Conference on Circuits and Systems, (pp. 237-242), 2012.

[16] H. Wang, Y. Zhang, H. Xiong, and B. Qin. "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme", IET Information Security, 6 (1), (pp. 20-27), 2012.

[17] H. Alemdar, and C. Ersoy. "Wireless sensor networks for healthcare: A survey", Computer Networks, 54 (15), (pp. 2688-2710), 2010.

[18] M. Li, W. Lou, and K. Ren. "Data security and privacy in wireless body area networks", IEEE Wireless Communications, 17 (1), (pp. 51-58), 2010.

[19] Y. Ren, R. Werner, N. Pazzi, and A. Boukerche. "Monitoring patients via a secure and mobile healthcare system", IEEE Wireless Communications, 17 (1), (pp. 59-65), 2010.

[20] S. Hidano, T. Ohki, N. Komatsu, and M. Kasahara. "On biometric encryption using fingerprint and it's security evaluation", In: Proceedings of the 10^{th} International Conference on Control, Automation, Robotics and Vision, (pp. 950-956), 2008.

[21] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov. "System architecture of a wireless body area sensor network for ubiquitous health monitoring", Journal of Mobile Multimedia, 1 (4), (pp. 307-326), 2006.

[22] C.H. Lin, and Y.Y. Lai. "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, 27 (1), (pp. 19-23), 2004.

[23] V. Matyas, and Z. Riha. "Toward reliable user authentication through biometrics", IEEE Security and Privacy, 1 (3), (pp. 45-49), 2003.