International Journal of Security and Its Applications
Vol. 11, No. 3 (2017), pp.71-80
http://dx.doi.org/10.14257/ijsia.2017.11.3.07

An Efficient Cloud-Assisted Message Authentication Scheme in Wireless Body Area Network

Huaijin Liu[1] and Yonghong Chen[1]

[1]*Department of Computer Science and Technology, Huaqiao University，Xiamen Fujian 361021, China*
[1]*lhjhqdx@163.com;* [2]*djandcyh@163.com*

Abstract

In the telemedicine system, a major challenge is how to ensure the patient's personal health information security and privacy. Although recent related research has solved various security problems, there are few people concerned about the communication overhead and energy consumption. In order to solve these problems, this paper proposes an efficient cloud-assisted message authentication scheme. In our scheme, the cloud server is responsible for storing the patient's encrypted data and transmission to the doctor for diagnosis and treatment, and then return the treatment results to the cloud server to save. Through security analysis and performance evaluation, our scheme not only ensures the patient's identity and data privacy, but also reduces the energy consumption, computation and communication overhead.

Keywords*: Authentication; Efficient; Security and privacy; Wireless body area network*

1. Introduction

As a promising application of the Internet and wireless scenarios, the development of wireless body area network (WBAN) in the field of telemedicine has received more and more attention [1-2]. Because of the limited computing power and storage capacity of the WBAN, a cloud-assisted WBAN can provide more timely and intelligent medical services to the patients. In recent years, the cloud assisted wireless body area network security and privacy protection in [3-7], most of the research work is mainly focused on how to resist various attacks, and in the communication overhead and energy consumption but little attention. In this paper, we propose an efficient cloud-assisted message authentication scheme. The scheme uses the anonymous mechanism to protect the patient's identity privacy will not be exposed and uses the timestamp mechanism to resist replay attacks. In the patient's data upload process, through the bilinear pairings to encrypt the patient’s data and stored in the cloud server, resist the man-in-middle attack and impersonation attack, ensure the security of the storage data. By comparing the proposed scheme with the recently related schemes, the experimental results show that the proposed scheme significantly reduces the communication overhead and energy consumption, and increases the network lifetime.

2. Network Architecture

The system model of cloud-assisted WBANs is shown in Figure 1. The system model is composed of four parts: trusted authority (TA), wireless body area network (WBAN), cloud server (CS) and doctor (D). The trusted authority TA is responsible for the system initialization settings, generates public parameters and the master key before the network deployment, and calculates an independent private key for each participant; WBAN consists of many physiolo- gical sensors and a mobile device (such as PDA) components. Physiological sensors are deployed in the patient's body to perceive the patient's personal

ISSN: 1738-9976 IJSIA

health items (such as ECG), and sent to PDA through the wireless way. PDA to the patient's data aggregation, and then in the form of ciphertext transmitted to the cloud server CS through the base station BS; The cloud server CS stores the received message and forwarded to the doctor D; The doctor D promptly treated the patient's symptoms and returned the treatment results to CS for subsequent analysis and diagnosis. The format of patient's personal health items is shown in Tables 1.

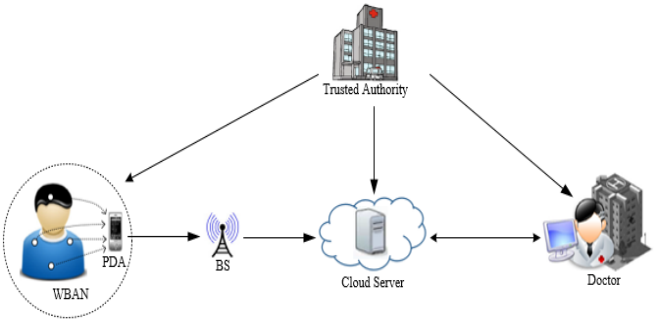

Figure 1. The Network Architecture of Cloud-assisted Wireless Body Area Network

Table 1. The Patient's Personal Health Items

Item	Content
ID	The patient's identity
data1	Electroencephalography(EEG)
data2	Electrocardiography(ECG)
data3	Electromyography
data4	Pulse oximetry(SpO2)
data5	Body pressure
data6	Heartbeat

3. Preliminaries

In this section, we briefly introduce the proposed scheme employs two encryption methods and theorems, namely bilinear pairing and hash function, this explanation is as follows.

3.1. Bilinear Pairings

Set $\mathbb{G}_0$ and $\mathbb{G}_1$ be two multiplicative cyclic groups of order P. Set g be a generator of $\mathbb{G}_0$ and e be a bilinear map, namely e: $\mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$. For any $\mathrm{i,j,k} \in \mathbb{G}_0$ and $a, \mathrm{b} \in \mathbb{Z}_p$, this bilinear pair e has the following three properties:

- Bilinear: $\mathrm{e}(i^a, j^b) = e(i,j)^{ab}$.
- Non-degenerate: $\mathrm{e(i,j)} \neq 1$.
- Polymerizability: $\mathrm{e(i \cdot j,k)} = \mathrm{e(i,k)} \times \mathrm{e(j,k)}$.

3.2. Hash Function

Hash function is a mapping of cryptography, it satisfies $\mathrm{H}: \{0,1\}^* \to \{0,1\}^n$. In which $\{0,1\}^*$ represents the bit string set of arbitrary length, the $\{0,1\}^n$ represents the bit string set of length n. Simply put, the hash function is the input of arbitrary length, through the

hash algorithm, compressed into a fixed length of the output, the value of the output is called the message digest. The hash function has the following three properties:

- One way: For any given output y, to find an input x, making $\mathrm{h}(x) = \mathrm{y}$ in the calculation is not feasible.
- Weak impact resistance: For any given input x, to find a different input x', making $\mathrm{h}(x) = \mathrm{h}(x')$ in the calculation is not feasible.
- Strong impact resistance: Find two different input x and x', making $\mathrm{h}(x) = \mathrm{h}(x')$ in the calculation is not feasible.

4. The Proposed Scheme

In this section, we will give a detailed introduction of the proposed scheme. This scheme involves four phases: system initialization phase, participant registration phase, patient health items upload phase and doctor treatment phase. The symbols used in this article are summarized in Table 2.

Table 2. Notations Used in the Paper

Symbol	Description
ID_{P}	The identity of entity P.
T_{P_n}	The *n*th timestamp of P.
$\Delta\mathrm{T}$	The valid transmission time interval.
m_{BS}	The patient's personal health items.
m_{treat}	The patient's treatment results.
SK_{P}	P's secret key.
k	A temporary key.
k_{ij}	Entity i and j's shared key.
H()	A Hash function.
$E_k()$	A encryption function with the key k.

4.1. System Initialization Phase

Healthcare system needs to be initialized before deployment. The trusted authority TA first generates and distributes the public parameters to all the entities in the system. TA perform steps are as follows:

Step 1 Randomly select three security parameters k, n_1, n_2, TA by running the generator Gen(k) to generate a five tuple $(\mathrm{q}, \mathbb{G}_0, \mathbb{G}_1, e, P)$.

Step 2 TA selects a random number $\mathrm{s} \in Z_q$ as the master key, and computes the public key $\mathrm{PK} = \mathrm{s}P$.

Step 3 TA selects three one-way hash functions H, H_1, H_2, where H: $\{0,1\}^* \rightarrow \mathbb{G}_0$, H_1: $\mathbb{G}_1 \rightarrow \{0,1\}^{n_1}$ and H_2: $\{0,1\}^* \times \mathbb{G}_1 \rightarrow \{0,1\}^{n_1}$.

Step 4 TA selects a symmetric encryption algorithm $E_k()$.

Step 5 TA publishes the public parameters $(\mathrm{q}, \mathbb{G}_0, \mathbb{G}_1, e, P, \mathrm{PK}, H, H_1, H_2, E_k())$ to all entities and save the master key s.

4.2. Participant Registration Phase

In order to protect the security of the healthcare system, all participants, including patients, doctors and cloud servers must be registered to TA, so as to obtain their own private key. TA will perform the following steps.

Step 1 Detecting the patient P's identity ID_p and compute the pseudo identity $PID_P = E_s(ID_P)$ by the master key s.

Step 2 Compute the patient P's secret key $SK_P = sH(PID_P)$, the cloud server CS's secret key $SK_P = sH(PID_P)$ and the doctor D's secret key $SK_D = sH(ID_D)$.

Step 3 Send (PID_P, SK_P, ID_D) to the patient P, (SK_{CS}, PID_P) to the cloud server CS and (SK_D, PID_P) to the doctor D.

After registration is completed, based on the properties of bilinear pairing, the shared key k_{P-CS} between the patient P and the cloud server CS, the shared key k_{CS-D} between the cloud server CS and the doctor D, and the shared key k_{P-D} between the patient P and the doctor D can be computed as follows:

$$k_{P-CS} = e\big(SK_P, H(ID_{CS})\big) = e(H(PID_P), SK_{CS}) \quad (1)$$

$$k_{CS-D} = e\big(SK_{CS}, H(ID_D)\big) = e(H(PID_{CS}), SK_D) \quad (2)$$

$$k_{P-D} = e\big(SK_P, H(ID_D)\big) = e(H(PID_P), SK_D) \quad (3)$$

With the establishment of the shared key, the secure communication between entities can be realized through a symmetric encryption algorithm.

4.3. Patient Health Items Upload Phase

In WBAN, physiological sensors to measure the patient's data and sends to the nearby PDA. PDA collects the measured health items m_{BS}, where $m_{BS} = (ID_P, data_1, data_2, \dots, data_6)$. Then performs an encryption function $E_k()$ to get the ciphertext C and uploads to the cloud server CS through the public channel. The specific steps are as follows:

Step 1 Obtain the current timestamp T_{P_1}.

Step 2 Compute a temporary key $k = H_1(k_{P-D})$, where k_{P-D} is the share key between the patient P and the doctor D.

Step 3 Compute $E_k(m_{BS})$ and $H_2(E_k(m_{BS}), k_{P-D})$.

Step 4 Compute $H_2(M, k_{P-CS})$, where $M = E_k(m_{BS})||H_2(E_k(m_{BS}), k_{P-D})$ and k_{P-CS} is the share key between the patient P and the cloud server CS.

Step 5 Upload the ciphertext $C = \{PID_P, M, H_2(M, k_{P-CS}), T_{P_1}\}$ to the cloud server CS.

Upon receiving the ciphertext C, the cloud server CS runs the following steps to verify the validity and integrity of the message M. If the validation is successful, CS forwards the message $\{PID_p, ID_{CS}, M, T_{CS_1}\}$ to the doctor D. Otherwise, discard the message M.

Step 1 Obtain the current timestamp T_{CS_1}.

Step 2 Check if the timestamp T_{P_1} is valid. If $T_{CS_1} - T_{P_1} \leq \Delta T$, perform the following steps, otherwise return $\perp$.

Step 3 Compute the shared key $k'_{P-CS} = e(H(PID_P), SK_{CS})$, where SK_{CS} is the cloud server CS's secret key.

Step 4 Check if the equation $H_2(M, k'_{P-C}) = H_2(M, k_{P-C})$ is equal. If equal, return M, otherwise return $\perp$.

4.4. Doctor Treatment Phase

When the doctor D receives the message $\{PID_p, ID_{CS}, M, T_{CS_1}\}$ sent by the cloud server CS, the doctor D first to verify the validity and integrity of the message M. If the validation is successful, D tries to recover the patient's message. Otherwise, discard the received message. The specific steps are as follows:

Step 1 Obtain the current timestamp T_{D_1}.

Step 2 Check if the timestamp T_{CS_1} is valid. If $T_{D_1} - T_{CS_1} \leq \Delta T$, perform the following steps, otherwise return $\perp$.

Step 3 According to the patient's pseudo identity PID_P, compute the shared keys $k'_{P-D} = e(H(PID_P), SK_D)$, where SK_D is D's secret key.

Step 4 Check if the equation $H_2(E_k(m_{BS}), k'_{P-D}) = H_2(E_k(m_{BS}), k_{P-D})$ is equal. If equal, perform the following steps, otherwise return $\perp$.

Step 5 Compute the temporary key $k' = H_1(k'_{P-D})$ and recover m_{BS} by decryption $D_{k'}(E_k(m_{BS}))$.

Step 6 Output the patient's personal health items m_{BS}.

After obtaining the patient's personal health items m_{BS}, the doctor to diagnose the patient's symptoms and return the treatment results $\mathrm{m_{treat}}$ to the cloud server CS to store, so that subsequent diagnosis and analysis. The specific steps are as follows:

Step 1 Obtain the current timestamp T_{D_2}.

Step 2 Compute $T_t = H_2(m_{treat}||PID_P||ID_D, k_{CS-D})$ and $C_{treat} = E_{k_{CS-D}}(m_{treat}, ID_D, PID_P, ID_D, T_t)$, where k_{CS-D} is the share key between the doctor D and the cloud server CS.

Step 3 Upload $\{C_{treat}, T_{D_2}\}$ to CS.

5. Security and Performance Analysis

5.1. Security Analysis

In this section, we examine the security strength of the proposed scheme by analyzing its main attack.

5.1.1. Identity Privacy

In order to protect the patient's real identity is not known to others, our scheme uses an anonymous mechanism. In the anonymous communication process, the patient with pseudo identity instead of real identity to communication, the receiver can only know the patient's pseudo identity and no way to know the real identity, so as to well protect the privacy of the patient's identity.

5.1.2. Man-in-middle Attack

In this attack, we assume that the attacker intercepts the patient's message and will modify the message transmission to the participants of the system. In our scheme, the patient P uses the temporary key $k = H_1(k_{P-D})$ to encrypt the message, which involves the computation of the shared key $k_{P-D} = e(H(PID_P), SK_D)$. Because the shared key only the patient P and the doctor D know that the attacker cannot modify P's message and send to D, so the attacker cannot achieve the main-in-middle attack.

5.1.3. Forgery/Modification Attack

In this attack, the attacker attempts to modify, delete or forge the existing messages. In our scheme, when the patient P sends a message m_{BS} to the doctor D, it calculates a hash value $H_2(m_{BS}, k_{P-D})$ by the shared key k_{P-D} to attach to the message m_{BS}. According to the one-way hash function, the doctor D can verify the integrity of the received message. Therefore, our scheme can defend against fabrication/alteration attack.

5.1.4. Impersonation Attack

In this attack, the attacker may disguised as a legal user to attack the system. In our scheme, all participants must register to TA before the network deployment, thereby obtaining their respective secret key. If the attacker pretends to be a legal user, it is necessary to form a correct secret key $SK = sH(PID)$. However, it is difficult for an attacker to pretend to be a legal user, because it does not know the random number s. Therefore, our scheme can defend against impersonation attack.

5.1.5. Replaying Attack

In this attack, the attacker could eavesdrop the message flow and repeat the same message to the system participants. In order to avoid the repeated attack, we used the timestamp mechanism. The sender sends a message to the receiver with a timestamp T, the receiver accepts the message to check whether the timestamp T is valid, if beyond the specified transmission time interval ΔT, the message is discarded. Therefore, our scheme can defend against replaying attack.

5.2. Performance Analysis

In this section, we make a comprehensive comparative analysis of our scheme and the related literature [6] and [7]. For the convenience of description, we referred to the literature [6] as SMDEP, literature [7] as SCAMS. Our experimental equipment for Intel i5-4200U 2.30GHz processor, 4G memory, 64 bits Windows 7 operating system. The experimental environment is constructed on the Oracle VM Virtual BOX 5.0.4 of Ubuntu 14.04.1, with 2G of memory allocation.

5.2.1. Communication Overhead

In our scheme, the patient's message needs to be stored in the cloud server and transmitted to the doctor for diagnosis and treatment. In the patient's health items upload phase, the message size is:

$$|PID_P| + |E_k(m_{BS})| + |\ H_2(E_k(m_{BS}), k_{P-D})| + |H_2(M, k_{P-CS})| + |T_{P_1}| \quad (4)$$

In the doctor treatment phase, the cloud server needs to transmit the patient's message to the doctor to diagnosis and treatment, and then returns the treatment results to the cloud server to store. Thus, the total message size is:

$$|PID_P| + |ID_{CS}| + |E_k(m_{BS})| + |\ H_2(E_k(m_{BS}), k_{P-D})| + |T_{CS_1}| + |C_{treat}| + |T_{D_2}| \quad (5)$$

Table 3 summarizes the communication overhead of our scheme and the other two schemes, there E denote the size of a symmetric encryption ciphertext, E' denote the size of an asymmetric encryption ciphertext, C denote the size of a Chebyshev polynomial, H denote the size of a hash value, ID denote the size of the identity, T denote the size of a timestamp. Figure 2 illustrates the relationship between the communication overhead and the number of message transmissions. Obviously, we can observe our scheme has a low communication overhead compared with the other two schemes.

Table 3. Communication Overhead

Phase	Our scheme	SCAMS	SMDEP
Upload data phase	$1E + 2H + 1ID + 1T$	$1E + 6H + 10ID + 7C + 4T$	$2E + 1E' + 1ID$
Treatment phase	$2E + 2H + 3ID + 2T$	$2E + 2H + 2ID + 3C + 2T$	$3E + 1E' + 1ID$
Total	$3E + 4H + 4ID + 3T$	$3E + 8H + 12ID + 10C + 6T$	$5E + 2E' + 2ID$

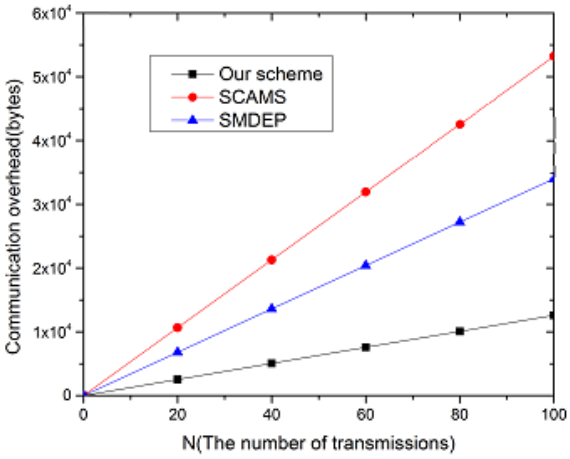

Figure 2. The Relationship between Communication Overhead and the Number of Messages Transmissions

5.2.2. Energy Consumption on Communications

In this subsection, we take the approach proposed by [12] to evaluate the energy consumption of communication. As shown in [13], the wireless communication circuit transmits and receives 1 byte of energy consumption for 59.2uJ and 28.6uJ. Table 4 summarizes our scheme and the other two schemes of the results of the energy consumption. Figure 3 illustrates the relationship between the energy consumption and the number of message transmissions. It is obvious that we can see from the graph that our scheme has a low energy consumption compared with the other two schemes.

Table 4. Energy Consumption on Communications

The schemes	Energy consumption (uJ)
Our scheme	$(3E + 4H + 4ID + 3T) * (28.6 + 59.2)$
SCAMS	$(3E + 8H + 12ID + 10C + 6T) * (28.6 + 59.2)$
SMDEP	$(5E + 2E' + 2ID) * (28.6 + 59.2)$

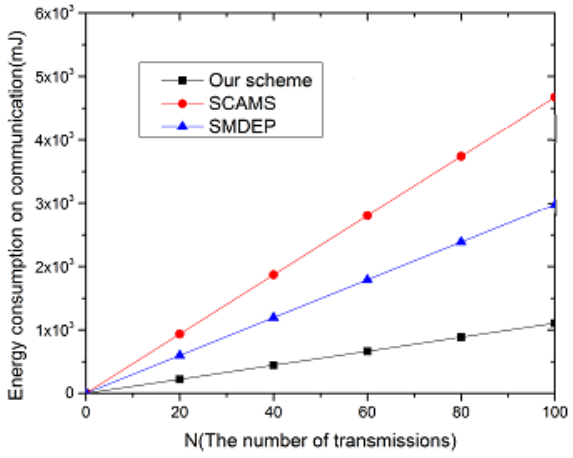

Figure 3. The Relationship between Energy Consumption and the Number of Message Transmissions

5.2.3. Computation Overhead

In this subsection, we compare our scheme and the other two schemes in terms of computation overhead. The comparison results are shown in Table 5, where T_{sig} means the time of execute a signature operation, T_{ver} means the time of verify a signature operation, T_m means the time of execute a multiplication operation, T_b means the time of execute a pairing operation, T_h means the time of execute a hashing function operation, T_c means the time of execute a Chebyshev polynomial operation, T_{sym} means the time of execute a symmetric encryption/decryption operation and T_{asym} means the time of execute an asymmetric encryption/decryption operation. In our evaluation, the bilinear map e uses the Tate pairing, in which the elliptic curve E is defined over F_p, p is a 512 bits prime and the order q is a subgroup of 160 bits prime. According to [10], the average cost of computing a Tate pairing on the 32 bits Intel PXA255 processor is 62.06ms. For the Chebyshev polynomial, it takes 70ms to compute a Chebyshev polynomial in the Intel 1.7 GHz, 512 MB RAM processor, where N and P are 1024 bits long [11]. Figure 4 illustrates the relationship between the computation overhead and the number of message transmissions. As can be seen from the graph, the computation overhead of SMDEP is minimum, and the computation overhead of SCAMS is maximum. Although our scheme has a slightly larger computation overhead compared with SMDEP, the communication overhead and energy consumption are minimal.

Table 5. Computation Overhead

Entity	Our scheme	SCAMS	SMDEP
Patient	$5T_h + 2T_b + 1T_{sym} + 3T_{asym}$	$4T_h + 2T_c + 1T_{sym}$	$1T_m + 1T_b + 1T_h + 2T_{sym} +$
Cloud	$3T_h + 2T_b$	$6T_h + 4T_c + 1T_{sig} + 3T_{sym}$	$1T_m + 1T_b + 1T_h + 1T_{sig} + 1T_{ver} + 3T_{smy} + 1T_{asmy}$
Doctor	$5T_h + 2T_b + 2T_{sym} + 2T_{asym}$	$6T_h + 2T_c + 2T_{sym}$	$2T_b + 2T_h + 5T_{sym} +$
Total	$13T_h + 6T_b + 3T_{sym}$	$16T_h + 8T_c + 1T_{sig} + 6T_{sym}$	$2T_m + 4T_b + 4T_h + 1T_{sig} + 1T_{ver} + 10T_{smy} + 6T_{asmy}$

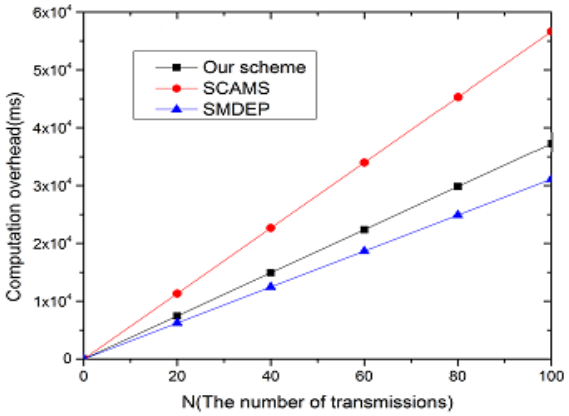

Figure 4. The Relationship between Communication Overhead and the Number of Messages Transmissions

6. Conclusion

Due to the limited resources of WBANs, the design of the scheme should not only secure the patient's identity and data privacy, but also improve the transmission efficiency and reduce the energy consumption when uploading physiological data to doctors for diagnosis and treatment. In this paper, we propose a new efficient cloud-assisted message authentication scheme. The scheme not only to protect the patient's identity and data privacy through anonymous mechanisms and bilinear pairings, but also can resist various main attack models. Through performance evaluation, our scheme has lower computation and communication overhead compared with other schemes.

Acknowledgements

Above work is supported by National Natural Science Foundation (NSF) of China under grant Nos. 61370007, 61572206, U1405254, Huaqiao University graduate research innovation ability cultivation project of China under grant No. 1511314006, Fujian Provincial Natural Science Foundation of China under grant No. 2013J01241, and Program for New Century Excellent Talents of Fujian Provincial under grant No. 2014FJ-NCET-ZR06.

References

[1] G. Fortino, M. Pathan and G. Di Fatta, “BodyCloud: Integration of Cloud Computing and body sensor networks”, IEEE International Conference on Cloud Computing Technology and Science, **(2012)**, pp: 851-856.
[2] G. Fortino, M. Pathan and G. Di Fatta, “BodyCloud: Integration of Cloud Computing and body sensor networks”, IEEE International Conference on Cloud Computing Technology and Science, **(2012)**, pp: 851-856.
[3] M. Al Ameen, J. Liu and K. Kwak, “Security and privacy issues in wireless sensor networks for healthcare applications”, Journal of medical systems, vol. 36, no. 1, **(2012)**, pp. 93-101.
[4] H. M. Chen, J. W. Lo and C. K. Yeh, “An efficient and secure dynamic id-based authentication scheme for telecare medical information systems”, Journal of medical systems, vol. 36, no. 6, **(2012)**, pp. 3907-3915.
[5] Z. Y. Wu, Y. C. Lee, F. Lai, H. C. Lee and Y. Chung, “A secure authentication scheme for telecare medicine information systems”, Journal of medical systems, vol. 36, no. 3, **(2012)**, pp. 1529-1535.
[6] Q. Jiang, J. Ma, Z. Ma and G. Li, “A privacy enhanced authentication scheme for telecare medical information systems”, Journal of medical systems, vol. 37, no. 1, **(2013)**, pp. 1-8.
[7] C. L. Chen, T. T. Yang and T. F. Shih, “A secure medical data exchange protocol based on cloud environment”, Journal of medical systems, vol. 38, no. 9, **(2014)**, pp. 1-12.
[8] C. T. Li, C. C. Lee and C. Y. Weng, “A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System”, Journal of medical systems, vol. 40, no. 5, **(2016)**, pp. 1-15.

[9] Q. Wang, C. Wang, K. Ren, “Enabling public auditability and data dynamics for storage security in cloud computing”, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, **(2011)**, pp. 847-859.
[10] J. Guo, T. Peyrin and A. Poschmann, “The PHOTON family of lightweight hash functions”, Annual Cryptology Conference. Springer Berlin Heidelberg, **(2011)**, pp. 222-239.
[11] C. Arene, T. Lange, M. Naehrig and C. Ritzenrhaler, “Faster computation of the Tate pairing”, Journal of number theory, vol. 131, no. 5, **(2011)**, pp. 842-857.
[12] Q. Xie, J. Zhao and X. Yu, “Chaotic maps-based three-party password-authenticated key agreement scheme”, Journal of Nonlinear Dynamics, vol. 74, no. 4, **(2013)**, pp. 1021-1027.
[13] K. A. Shim, Y. R. Lee and C. M. Park, “EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks", Journal of Ad Hoc Networks, vol. 11, no. 1, **(2013)**, pp. 182-189.
[14] Z. Noroozi and J. Kadivar, “Energy analysis for wireless sensor networks”, IEEE International Conference on Mechanical and Electronics Engineering, **(2010)**, 2: V2-382-V2-386.

