Middle-East Journal of Scientific Research 24 (2): 227-233, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.02.22926

Robust Bio-Key Management Scheme for Telemedicine Applications in Body Area Networks

[1]K. Kalaivani and [2]Dr. R. Sivakumar

[1]Department of EIE, Easwari Engineering College, Chennai, India
[2]Department of ECE, RMK Engineering College, Chennai, India

Abstract: Medical sensor networks play a vital role for real-time healthcare monitoring of telemedicine based applications. Telemedicine provides specialized healthcare consultation to patients in remote locations. We use electronic information and communication technologies to provide and support healthcare when the distance separate the participants. In order to make sure the privacy and security of patient's critical health information, it is essential to provide efficient cryptography scheme. This paper presents a novel Mamdani based Bio-Key Management (MBKM) technique, which assures real time health care monitoring without any overhead. We present the simulation results to show that the proposed MBKM scheme can achieve greater security in terms of performance metrics such as False Match Rate (FMR), False Non Match Rate (FNMR) and Genuine Acceptance Rate (GAR) than other recent existing approaches.

Key words: Healthcare · Security · Medical sensor networks · Key Management

INTRODUCTION

Advances in telecommunication and information technologies, for instance, implantable and deployable medical sensors, besides with contemporary developments in the embedded processing area are enabling the plan, improvement and realization of medical sensor networks. This kind of networks provides the direction for exploitation of inventive healthcare monitoring applications. In the preceding few years, a great deal of the research in medical sensor networks has paid attention to subjects related to the design of medical sensors, minimization of the sensor size, sensor circuit with low power consumption, signal processing and communications protocols. In this paper, we propose a novel Mamdani based Bio-Key Management (MBKM), which assures secure and authenticated real time health care monitoring with less overhead for telemedicine applications. Telemedicine means the remote medical expertise at the point of need or medicine at a distance. Telemedicine technology is mainly required for the people living in rural areas, aged people and disabled people [1]. We emphasize some of the design issues and open concerns that will make medical sensor networks extremely everywhere.

The development of telemedicine based healthcare applications presents various novel challenges like reliable real time data transfer, timeliness, Energy and Power management for a lot of applications [2]. Further applying new technologies in telemedicine applications without considering security aspects like privacy, authentication, confidentiality and integrity as susceptible [3]. For example, the patient's health information is delicate and leakage of patient's personal data could make him uncomfortable. Furthermore sometimes exposing health information may result in a person losing his job or make it impracticable to get insurance protection [4].

Fig. 1 explains the risks to patient security in Body Area Network (BAN). Here various sensors, implanted in the human body to measure the vital signs like ECG, EEG, EMG, Blood pressure, glucose level, etc., connected to other sensors or to the control nodes. Further sensors send the patient information to a medical expertise using wired or wireless technology. Now the intruder may watch the patient data and he can alter or may post the data in social sites, which pose risks to patient's security.

More importantly, Healthcare provider must follow HIPAA (Health Insurance Portability and Accountability Act) rules. Otherwise provider is subjected to punishment [5]. So a patient security is a most important anxiety in telemedicine based healthcare applications.

Corresponding Author: K. Kalaivani, Department of EIE, Easwari Engineering College, Chennai, India.

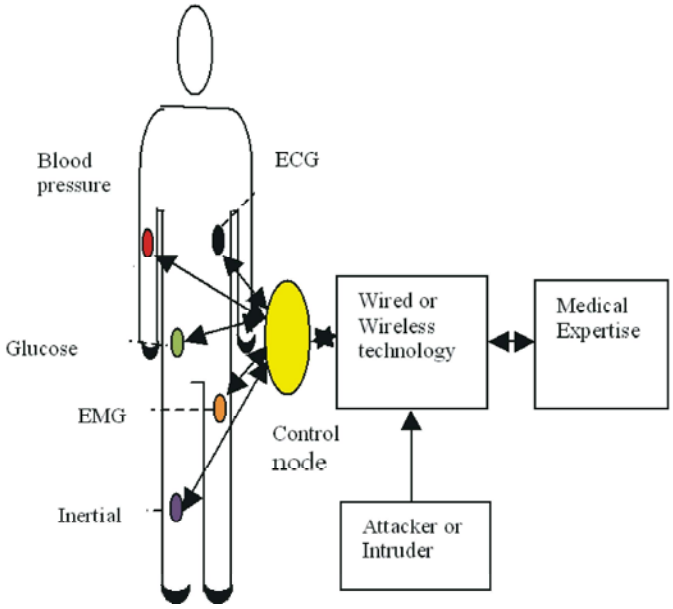

Fig. 1: Risks to patient security

Related Works: With the improvement of advanced technology, invasive computing is observed as a key technology to assist streaming medical data communication for telemedicine based applications with the help of deploying sensors [6, 7].Several solutions for medical information security have been proposed to protect the Body area network security. ECC (Elliptic curve cryptography), hardware encryption, TinySec and biometric methods are the kinds of solutions discussed in [8]. Link layer encryption is achieved in the body area network by TinySec approach [9]. If one medical sensor releases the key or it acts as an attacker, all the information in the Body area network will be released. Elliptic curve cryptography (ECC) has been used in the wireless sensor networks [10, 11]. This public key cryptographic technique requires more energy compared to symmetric key cryptographic techniques.

Biometrics obtained from the human body to secure the key is proposed in [12]. Compared with cryptographic techniques, this technique reduces computation and communication cost. Electro cardiogram (ECG) and Photo plethysmograph (PPG) signals are used as excellent biometric features to secure the data in body area network [13, 14].

The fuzzy vault scheme has been predominantly used for biometric authentication, such as fingerprints and iris image recognition [15-17]. Fuzzy vault scheme plays a major role to solve the problem of security in telemedicine based applications. The Fuzzy vault scheme is used in Physiological Signal based Key Agreement (PSKA) to establish secured pairwise key agreement between the nodes in Body area networks [18], which solves mainly the synchronization problem and issues in feature reordering [19].

The biometric Encryption scheme is a cryptography scheme which is used to maintain the security of biometrics and generate a strong key from biometrics [20]. In this scheme, the chaff points are not necessary to be added to transmit, so the delay time and energy consumption are reduced.

In [21], the author proposes a new idea for a message and user authentication. This scheme compares the present ECG signal with the previously recorded ECG template to verify the identity. Since the template is static, this method provides poor performance. The authors of the paper [22] propose ECG-IJS scheme to improve authentication of streaming medical information. The author used features of ECG signal to key generation for secure real-time medical data communication.

System Design: Mamdani based Bio-Key Management (MBKM) scheme is proposed based on the earlier discussion on ECG-IJS scheme. MBKM scheme is introduced to ensure the security for streaming medical data communication in Telemedicine based applications. The proposed MBKM scheme is shown in Figure 2.

A novel proposed MBKM scheme is shown in Figure 2 which uses body area networks to give an alert to the hospital, even before the patient has critical problems like heart attack, glucose level through

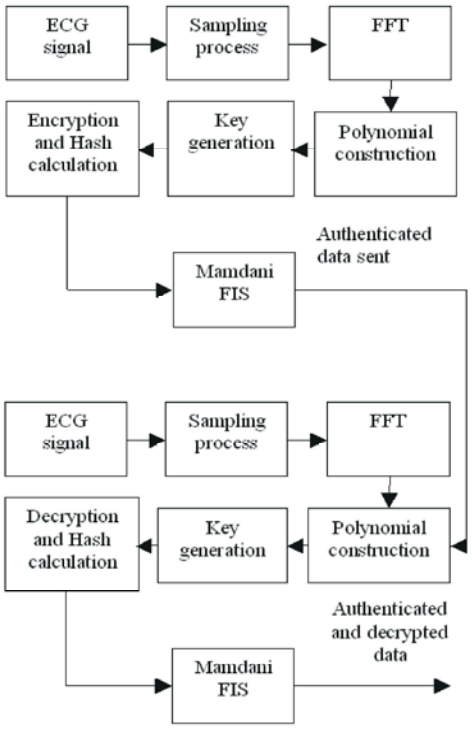

Fig. 2: MBKM scheme

measuring changes in their crucial signs as a temperature of the patient, pulse rate, glucose level, blood pressure and respiratory rate. Sensors, which are implanted in the patient's body measure the level of crucial signs and transmit the parameter values towards the medical expert working in the intensive carrier unit of the hospital to take necessary actions to save the life of a patient.

Intensive care units are equipped with multi-modal monitors, which are able to simultaneously measure and display the health status of the patient. In such case, this crucial real-time medical information must be well sheltered against attackers and security aspects must be satisfied [23]. Health care units with poor security implementation procedures for telemedicine may lead to wrong diagnosis and treatment for the patient.

The procedure at the sender side is given as follows: ECG sensor is used to observe the ECG signal from the human body. Nyquist theorem at the rate of 120 Hz is applied to the ECG signal to take samples. 512 points Fast Fourier transform (FFT) is conducted on the sampled ECG data. Since the FFT process is symmetric first 256 coefficients are retained among 512 coefficients. All the peak values of the extracted FFT coefficients are used as features. A polynomial equation with degree N is constructed and the key K is generated. The Patient's data is encrypted with the generated key K and hash value based on the SHA-1 algorithm is calculated. Then the sender sends the envelope contains the encrypted message, a subset of coefficients and hash value to the receiver.

The procedure at the receiver side is described as follows: Similar to the sender, the receiver also repeats the procedure to observe the ECG signal, sample the signal and extract the first 256 Feature coefficients. Then a new polynomial with degree M is constructed using the received coefficients and the polynomial on all points in features to get a set of pairs. The key at the receiver K' is reconstructed from receiving coefficients and the new hash value is calculated. Key K and the hash value are compared with reconstructed key K' and new hash value. If the keys are same, then decrypted data is authenticated data.

Mamdani based Fuzzy inference system plays a major role to ensure security in telemedicine applications. Steps in the design of a fuzzy inference system are explained in the case of polynomial degree 10 as follows: 1) Input variables are identified as I_1, I_2 and the output variable is identified as Y. 2) The Universe of discourse for the input variables are defined in the range [-0.01, $-1e^{-16}$] and the output variable is defined in the range [0, 1]. 3) The Linguistic label assigned for the interval spanned by each input variable into a number of fuzzy subsets are taken as S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9 and S_{10}.The Linguistic label assigned for the interval spanned by each output variables into a number of fuzzy subsets are taken as Y_1, Y_2, Y_3, Y_4, Y_5 Y_6, Y_7, Y_8, Y_9, Y_{10}. 4) The Triangular membership function is assigned for each fuzzy subset. 5) Rule-base is formed by assigning the fuzzy relationship between inputs fuzzy subsets on the one hand and outputs a fuzzy subset on the other hand. If I_1 is S_1 and I_2 is S_1 then Y is Y_1. If I_1 is S_1 and I_2 is S_2 then Y is Y_2. If I_1 is S_1 and I_2 is S_3 then Y is Y_3. If I_1 is S_1 and I_2 is S_4 then Y is Y_4. If I_1 is S_1 and I_2 is S_5 then Y is Y_5. If I_1 is S_1 and I_2 is S_6 then Y is Y_6. If I_1 is S_1 and I_2 is S_7 then Y is Y_7. If I_1 is S_1 and I_2 is S_8 then Y is Y_8. If I_1 is S_1 and I_2 is S_9 then Y is Y_9. If I_1 is S_1 and I_2 is S_{10} then Y is Y_{10}. In a similar way, totally the 100 combinations of rules are formed. 6) Fuzzy outputs recommended by each rule are aggregated. 7) The crisp output is obtained by applying one of the defuzzification techniques called Centroid of area (COA). Then, using this output, parameters like False Match Rate, False Non Match Rate and Genuine Acceptance Rate are calculated.

RESULTS AND DISCUSSION

We validate the MBKM scheme by measuring the parameters like False Match Rate (FMR), False Non Match Rate (FNMR) and Genuine Acceptance Rate (GAR) and Half Total Error Rate (HTER).

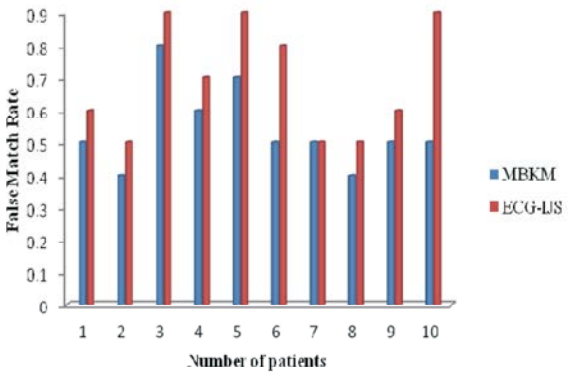

Fig. 3: FMR versus Number of patients

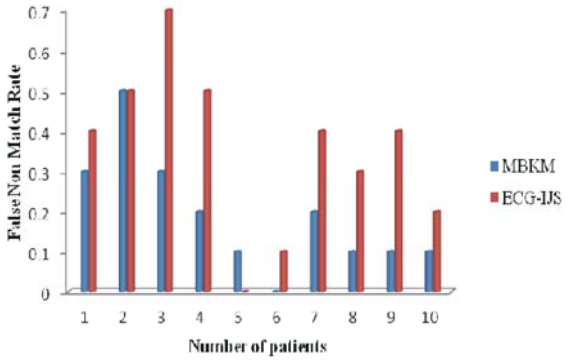

Fig. 4: FNMR versus Number of patients

In this scheme, we downloaded 48 patient's ECG signal for ten seconds from the MIT-BIH Arrhythmia database. We used MATLAB software tool to simulate the proposed MBKM scheme. ECG signals are used for generation of the key and medical information like EEG, EMG, blood glucose level, blood pressure level, etc., can be sent to medical expertise in real time for telemedicine based applications. The performance graph of 10 patients with the Polynomial degree 10 is drawn to study the performance metrics like FMR, FNMR, GAR and HTER.

The performance of FMR versus a number of patients is given in Fig. 3. FMR value represents the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. So FMR value must be low for the stable system. This plot proves that the False Match Rate is lower in the proposed MBKM scheme when compared to ECG-IJS scheme.

The performance of FNMR versus a number of patients is shown in Fig. 4. FNMR value represents the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected. The stable system should yield lower

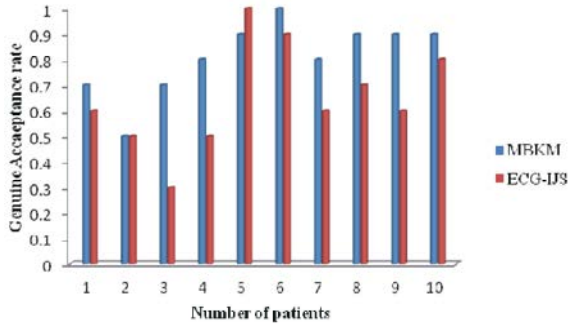

Fig. 5: GAR versus Number of patients

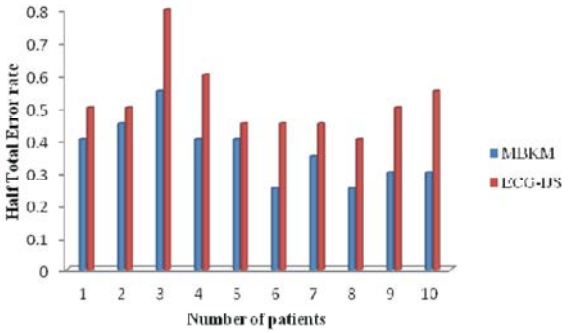

Fig. 6 HTER versus Number of patients

FNMR. This plot proves that the False Non Match Rate is lower in the proposed MBKM scheme when compared to existing ECG-IJS scheme.

The performance of GAR versus a number of patients is present in Fig.5. GAR value represents the fraction of authentication attempts by genuine users that are accepted. The stable system should yield higher GAR. This plot proves that the Genuine Acceptance Rate is higher in the proposed MBKM scheme when compared to the existing ECG-IJS scheme.

The performance of HTER versus a number of patients is present in Fig.6. HTER value represents the average of False Match Rate and False Non Match Rate. The stable system should yield low HTER. This plot proves that HTER is lower in the proposed MBKM scheme when compared to the existing ECG-IJS scheme.

Statistical Analysis: We have attempted to test the average False Non Match Rate (FNMR) of the patient population is less than the test value by conducting one sample T test. The test was conducted in the case of polynomial degree 5 and 10. The null and alternate hypothesis for the polynomial degree 5 can be formulated as given in expression 1. The null and alternate hypothesis for the polynomial degree 10 can be formulated as given in expression 2.

Table 1: Statistical Analysis of FNMR

	Number of Patients	Mean	Standard Deviation	Standard Error Mean	Test value	t	Sig. (2 tailed)	Level of significance
Polynomial degree 5	48	0.1250	0.14947	0.02157	0.08	2.086	0.042	5%
Polynomial degree 10	48	0.5313	0.15181	0.02157	0.05	2.414	0.020	5%

Table 2: Statistical Analysis of FMR

	Number of Patients	Mean	Standard Deviation	Standard Error Mean	Test value	t	Sig. (2 tailed)	Level of significance
Polynomial degree 5	48	0.6021	0.12631	0.01823	0.56	2.308	0.025	5%
Polynomial degree 10	48	0.5313	0.15181	0.01291	0.48	2.339	0.024	5%

Table 3. Statistical Analysis of GAR

	Number of Patients	Mean	Standard Deviation	Standard Error Mean	Test value	t	Sig. (2 tailed)	Level of significance
Polynomial degree 5	48	0.8750	0.14947	0.02157	0.93	-2.549	0.014	5%
Polynomial degree 10	48	0.8979	0.14945	0.02157	0.95	-2.414	0.020	5%

$$H_0: \mu_{FNMR} = 0.08 \quad [1]$$
$$H_1: \mu_{FNMR} < 0.08$$

$$H_0: \mu_{FNMR} = 0.05 \quad [2]$$
$$H_1: \mu_{FNMR} < 0.05$$

Since t value is significant at 5% the null hypothesis can be rejected in both the cases. Hence, alternate hypothesis can be accepted in both the cases. Therefore, average FNMR can be less than 0.08 in the case of polynomial degree 5 and 0.05 in the case of polynomial degree 10. Results show that robustness level is good in both the cases. It is explained in Table 1 that test value is lesser in polynomial degree 10 when compared to polynomial degree 5. This means that when number of mutual elements of the characteristic is required to authenticate, the system may deny the two feature sets that coming from the same person. So FNMR value increases when polynomial degree value increases.

We have attempted to test the average False Match Rate (FMR) of the patient population is less than the test value by conducting one sample T test. The test was conducted in the case of polynomial degree 5 and 10. The null and alternate hypothesis for the polynomial degree 5 can be formulated as given in expression 3. The null and alternate hypothesis for the polynomial degree 10 can be formulated as given in expression 4.

$$H_0: \mu_{FMR} = 0.56 \quad [3]$$
$$H_1: \mu_{FMR} < 0.56$$

$$H_0: \mu_{FMR} = 0.48 \quad [4]$$
$$H_1: \mu_{FMR} < 0.48$$

Since t value is significant at 5% the null hypothesis can be rejected in both the cases. Hence, an alternate hypothesis can be accepted in both the cases. Therefore, average FMR can be less than 0.56 in the case of polynomial degree 5 and 0.48 in the case of polynomial degree 10. Results show that Distinctiveness level is good in both the cases. It is explained in Table 2 that test value is lesser in polynomial degree 10 when compared to polynomial degree 5. This means that when the polynomial degree is high, then a number of shared features must be recovered to find out the hidden information. So FMR value decreases when polynomial degree value increases.

We have attempted to test the average Genuine Acceptance Rate (GAR) of the patient population is less than the test value by conducting one sample T test. The test was conducted in the case of polynomial degree 5 and 10. The null and alternate hypothesis for the polynomial degree 5 can be formulated as given in expression 5. The null and alternate hypothesis for the polynomial degree 10 can be formulated as given in expression 6.

$$H_0: \mu_{GAR} = 0. \quad [5]$$
$$H_1: \mu_{GAR} > 0.93$$

$$H_0: \mu_{GAR} = 0.95 \quad [6]$$
$$H_1: \mu_{GAR} > 0.95$$

Since t value is significant at 5% the null hypothesis can be rejected in both the cases. Hence, an alternate hypothesis can be accepted in both the cases. Therefore, average GAR can be more than 0.93 in the case of polynomial degree 5 and 0.95 in the case of polynomial degree 10. Results show that the Genuine Acceptance Rate is good in both the cases. It is explained in the table that test value is greater in polynomial degree 10 when compared to polynomial degree 5. So GAR value decreases when polynomial degree value increase.

CONCLUSION

Secure communication is robustly required to preserve a patient's health privacy and safety in telemedicine based applications. In this paper, we present an efficient Mamdani based Bio-Key Management (MBKM) scheme for key management based security scheme in telemedicine based applications and its statistical analysis. This scheme makes the system stable system by providing low FNMR, High GAR, low FMR and low HTER. This new scheme is less complex and offers the security in terms of authentication, data confidentiality, data integrity. It remains to be a future work to do energy analysis and implement a neural network approach to secure medical data communication for telemedicine applications.

REFERENCES

1. Yasumitsu Tomaika, Isao Nakajima, Hiroshi Juzoji and Toshihikonkitano, 2008. Patent Issues on Telemedicine in eHealth, IEEE International conference on e-Health Networking, Applications and Service, pp: 187-193.
2. kumar Pardeep and Hoon Jay-Lee, 2012. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, Sensors, pp: 55-91.
3. Dimitriou, T. and K. Loannis, 2008. Security Issues in Biomedical Wireless Sensor Networks, In Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL'08), Aalborg, Denmark.
4. Meingast, M., T. Roosta and S. Sastry, 2006. Security and Privacy Issues with Healthcare Information Technology, In Proceedings of the 28th IEEE EMBS Annual International Conference, New York, NY, USA, pp: 5453-5458.
5. Office for Civil Rights United State Department of Health and Human Services. Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. Available online: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.
6. Woods, J., 2006. The five styles of sensory applications, Gartner Research.
7. Amer, M.M.M.B. and M.I.M. Izraiq, 2007. System with intelligent cable-less transducers for monitoring and analyzing biosignals, European Patent Application.
8. Mana, M., M. Feham and B.A. Bensaber, 2011. Trust key management scheme for wireless body area networks, International Journal of Network Security, 12(2): 61-69.
9. Karlof, C., N. Sastry and D. Wagner, 2004. TinySec: a link layer security architecture for wireless sensor networks, in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, (SenSys '04), 162-175, Baltimore, Md, USA.
10. Guennoun, M., M. Zandi and K. El-Khatib, 2008. On the use of biometrics to secure wireless biosensor networks, in Proceedings of the 3rd International Conference on Informationand Communication Technologies: From Theory to Applications, (ICTTA '08), Damascus, Syria, pp: 1-5.
11. Szczechowiak, P., L.B. Oliveira, M. Scott, M. Collier and R. Dahab, 2008. NanoECC: testing the limits of elliptic curve cryptography in sensor networks, in Proceedings of the 5th European Conference on Wireless Sensor Networks, Bologna, Italy, pp: 305-320.
12. Cherukuri, S., K.K. Venkatasubramanian and S.K.S. Gupta, 2003. BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, in Proceedings of the International Conferenceon Parallel Processing Workshops, Kaohsiung, Taiwan, pp: 432-439.
13. Poon, C.C.Y., Y.T. Zhang and S.D. Bao, 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Communications Magazine, 44(4): 73-81.
14. Bao, S.D., C.C.Y. Poon, L.F. Shen and Y.T. Zhang, 2008. Using the timing information of heartbeats as an entity identifier to secure body sensor network IEEE Transactions on Information Technology in Biomedicine, 12(6): 772-779.

15. Uludag, U., S. Pankanti and A.K. Jain, 2005. Fuzzy vault for fingerprints, in Proceedings of the Audio-and Video-Based Biometric Person Authentication (AVBPA '05), Hilton Rye Town, NY, USA, 3546: 310-319.
16. Reddy, E.S. and I.R. Babu, 2008. Authentication using fuzzy vault based on iris textures, in Proceedings of the 2nd Asia International Conference on Modelling and Simulation, (AMS '08), Kuala Lumpur, Malaysia, pp: 361-368.
17. Juels, A. and M. Sudan, 2006. A fuzzy vault scheme, in Proceedings of the International Symposium on Information Theory,, Seattle,Wash, USA, 38: 237-257.
18. Venkatasubramanian, K.K., A. Banerjee and S.K.S. Gupta, 2010. PSKA: usable and secure key agreement scheme for body area networks, IEEE Transactions on Information Technology in Biomedicine, 14(1): 60-68.
19. Bui, F.M. and D. Hatzinakos, 2008. Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling, EURASIPJournal on Advances in Signal Processing, Article ID 529879, pp: 16.
20. Jain, A.K., K. Nandakumar and A. Nagar, 2008. Biometric template security, EURASIP Journal on Advances in Signal Processing, Article ID 579416, pp: 17.
21. Biel, L., O. Pettersson, L. Philipson and P. Wide, 2001. ECG Analysis: A new approach in human identification, IEEE Trans. Instrum. Meas, pp: 808-812.
22. zhang Zhaoyang, Honggangwang, Athanasios V. Vasilokas and Hua Fang, 2012. ECG-Cryptography and Authentication in Body Area Networks, IEEE Transactions on Information Technology in Biomedicine, pp: 1070-1078.
23. Wang, H., D. Peng, W. Wang, H. Sharif, H. Hwa Chen and A. Khoynezhad, 2010. Resource-aware secure ECG health care monitoring through body sensor networks, IEEE Wireless Communications, 17(1): 12-19.