Journal of Computer Science, 9 (5): 558-565, 2013
ISSN 1549-3636
© 2013 Science Publications
doi:10.3844/jcssp.2013.558.565 Published Online 9 (5) 2013 (http://www.thescipub.com/jcs.toc)

Fuzzy System to Authenticate Assisted Living Patients in Their Home Environment

[1]Mohanavalli Seetha Subramanian and [2]Sheila Anand

[1]Department of Electronics and Communication Engineering,
Faculty of Electronics and Communication Engineering, Tagore Engineering College, Chennai, India
[2]Faculty of Computer Studies, Rajalakshmi Engineering College, Chennai, India

Received 2012-12-08, Revised 2012-12-21; Accepted 2013-05-18

ABSTRACT

Patient identity verification is a critical requirement for a remote patient monitoring environment. The health of the patient is monitored and crucial medical decisions are taken based on the physiological data collected from the patient using sensors and sent to distant health care centers or hospitals for real-time monitoring. Therefore it is of utmost importance to associate the received data with the correct patient as false verification of the patient's identity could lead to a wrong diagnosis and have serious repercussions leading even to the loss of a patient's life. In this study we propose a simple and robust remote authentication system for verifying the identity of assisted living patients being monitored in their home environment. We propose a biometric authentication that is based on the Electrocardiogram (ECG) data collected from the patient. It is a well established fact that ECG can be used to authenticate people. Moreover ECG data serves to not only monitor the health of the patient but also provides for continuous patient verification which is a very essential requirement for the security of the remote health monitoring system. We have implemented and tested the proposed fuzzy authentication scheme using the Mamdani model and present the results.

Keywords: Authentication, Remote Monitoring, Biometric Features, Fuzzy Logic

1. INTRODUCTION

Assisted living applications enable individuals to receive high quality medical care within the comforts of their home (Kounga *et al*., 2010). Assisted living is for patients who do not require hospitalization but require constant monitoring of their health. Patients are remotely monitored to ensure their health, safety and well-being. Assisted Living Facilities (ALF) provides a suitable alternative to traditional nursing homes and patients can be monitored either within the ALF or in their home environment. It can be used to monitor post-operative patients as well as senior citizens.

Wireless Body Area Networks (WBAN) can be successfully deployed to remotely monitor the patients. Patients are made to wear jackets such as LifeGuard (Mundt *et al*., 2005) or Smart Vest (Pandian *et al*., 2008) fitted with sensors or the sensors can be surgically implanted in the patient's body. These sensors periodically measure the patient's vital parameters and transmit them to hospitals/health care centres for continuous medical evaluation by the health care providers. The advantage of such a system is that while it enables the patient to receive continuous medical care, it does not restrict the patient's mobility or freedom to carry on their day-to-day activities. This not only ensures their physical well being but also their mental health as assisted living applications can be used to deliver health care to patients in the comfort of their homes (Wang *et al*., 2006; Loyouni *et al*., 2009; Mohanavalli and Sheila, 2011).

Corresponding Author: Mohanavalli Seetha Subramanian, Department of Electronics and Communication Engineering,
Faculty of Electronics and Communication Engineering, Tagore Engineering College, Chennai, India

In such remote monitoring scenarios, patient authentication is a prime requirement, as the hospital has to ensure that the received medical data is associated with the correct patient. This is extremely important, as medical decisions which could be life critical are being made on basis of the data received from the patient. Therefore the dependability of a remote health monitoring system largely rests on its ability to correctly authenticate a person so that appropriate medical care can be delivered to the patients. An authentication system performs two different functions, a person is either identified or an identity claim of a person is verified. This can be done by using conventional authentication methods like username and password, or by using the biometric trait of a person. Several physical or behavioral features like voice, retina, fingerprint may be used to provide an automated recognition of the person. All these features and the password method provide a one-time authentication mechanism, which has the risk of an unauthorized person wearing the sensors forcibly from a patient after authentication is done (Sriram *et al*., 2009). Therefore in a remote monitoring environment it is advantageous to have an authentication scheme that will continuously verify the person's identity. In a health monitoring application, it would be cumbersome if the patient is frequently asked to authenticate himself by using the above mentioned biometrics.

Several physiological characteristics like ECG, EEG, blood pressure are used by physicians for diagnosis, but using medical signals for biometrics is less developed when compared to the most frequently used features like iris, fingerprint, face. Biometrics use anatomical, physiological or behavioral characteristics that is different from person to person (Shen *et al*., 2002). One such biometric signal is the Electrocardiogram (ECG) which varies from person to person due to the physical differences like age, gender, body weight and physiological differences like the position, size and anatomy of the heart (Hoekema *et al*., 2001).

In this study, we propose a simple and robust authentication system that is based on the ECG data that is collected from the patient and sent to the remote health centers/hospitals for health monitoring. The authentication scheme proposed is for patients being monitored within their home environment, where the number of patients being monitored is small and limited to the inmates of the house.

1.1. Related Work

We first briefly explain the ECG wave and then review some of the previous work on authentication of an individual using his/her ECG data.

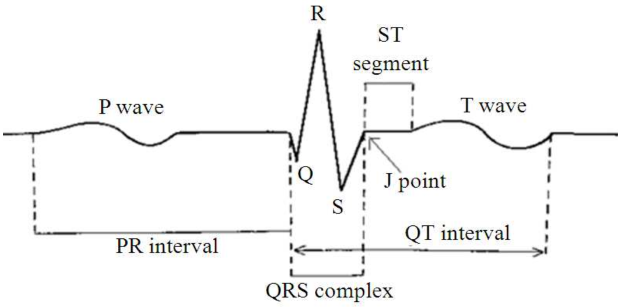

Fig. 1. Electrocardiogram (ECG) wave

The activity of the human heart is powered by electrical simulations inside the heart (Sufi *et al*., 2010). Depolarization of either the atria or the ventricle causes the heart to contract and repolarization results in the relaxation of these chambers. This alternate contraction and relaxation causes changes in the heart's electrical potentials which are measured as the ECG. The ECG wave is made up of the P wave, QRS complex and the T wave as shown in **Fig. 1**. The atrial depolarization is named as the P wave, the QRS complex represents ventricular contraction (depolarization) and the ventricular relaxation or repolarization is seen as the T wave. Though every individual's ECG contains the same major components, the relative position, duration and amplitude of each feature varies from person to person (Biel *et al*., 2001).

As a biometric, ECG data is difficult to disguise or falsely duplicate thereby reducing the possibility of applying false credentials to an authentication system (Shen *et al*., 2002). When compared to conventional biometric features such as the fingerprint, face recognition, palm print, ECG signals are universal, that is, every living human being has a heartbeat. Moreover the ECG trace inherently confirms the "aliveness" of the person and therefore becomes an eligible choice for use as a biometric (Chan *et al*., 2006).

We now look at previous work on using ECG data for authenticating an individual. Israel *et al*. (2005) in their work have extracted fiducial features from the P, R and T complexes, after removing the noise from the ECG signal. These features were identified and digitally extracted and from this data, the stable features that characterized the individual were defined. This technique has a low enrollment rate of 70%. In their work, Irvine *et al*. (2008) have employed the Principal Components Analysis (PCA) for feature extraction and have then performed eigenvector decomposition of the normalized ECG. They state that this approach has a 100% enrollment rate and therefore overcomes the weakness in their previous work.

Biel *et al*. (2001) have used 30 features from the ECG to classify an individual. They have used the SIMCA model based on Principal Component Analysis (PCA).They have showed that the ECG could be used to identify a person from a predetermined group. They have also shown that one lead ECG signal is enough to identify a person. Shen *et al*. (2002) have also used one-lead ECG to identify an individual. They had applied two techniques namely template matching and Decision Based Neural Network (DBNN). They conclude that ECG analysis can be used for identity verification. Chan *et al.* (2006) have used correlation coefficient and the wavelet distance measure for person identification. To detect the PQRST wave they have used the multiplication of backward differences algorithm.

The study by Bousselijot and Kreiseler (1998) does not extract any features from the ECG wave, but uses a pattern comparison method. Here the ECG measured from the patient is compared with the other ECGs. Hoekerd and Delft (2008) have used the eigenPulse and the Percent Residual Distance (PRD) to classify individuals based on their ECG signal. They have used ECG of normal persons as well as patients with myocardial infarctions. They conclude that ECG is a very reliable biometric for identifying individuals, even those with heart diseases. Plataniotis *et al*. (2006) have used the Auto Correlation and Discrete Cosine Transform (AC/DCT) to identify individuals from their ECG. They do not extract any fiducials; instead they use the ECG wave as a whole within a window to perform biometric identification.

Sriram *et al*. (2009) have proposed an authentication system for remote health monitoring which combines the ECG and accelerometer features to authenticate the patient. Their method uses 44 fiducials extracted from the ECG and 6 features obtained from the accelerometer as input to the authentication scheme. They have used both the Bayesian and the K nearest neighbor techniques to authenticate the patient.

Hence, it can be concluded from all of the above mentioned work that ECG has a strong potential to be used as a biometric to identify individuals or verify the identity of an individual. It can also be noted that much of the work necessitates elaborate and complex systems. In this study, we have proposed the use of a fuzzy system for authenticating a patient using ECG for our At-Home Assisted Living architecture. ECG is a general physiological characteristic that is widely and commonly used for remote health monitoring. It provides for continuous patient authentication, an essential security requirement of remote health monitoring systems. To the best of our knowledge there has been no fuzzy based authentication scheme using ECG as the biometric.

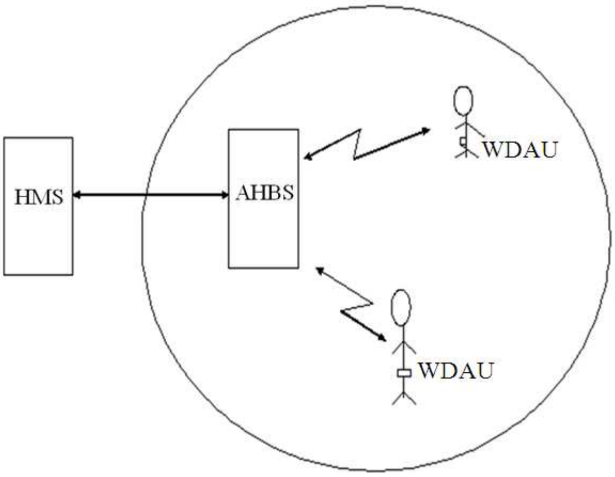

Fig. 2. At-Home Architecture

1.2. Remote Authentication for At-Home Assisted Living Architecture

In our previous work we had proposed a secure architecture for effective remote monitoring of patients within their home environment (Mohanavalli and Sheila, 2011). Such patients could remain in the comforts of their home and be monitored using the architecture shown in **Fig. 2**.

Sensors are used to measure various physiological parameters, like ECG, body temperature, blood pressure. The sensed values are collected and aggregated by a Wearable Data Acquisition Unit (WDAU) worn by the patients. The WDAU transmits the aggregated data to an At-Home Base Station (AHBS) using wireless transmission. If there are more than one patient being monitored at home then, AHBS would collect the data from all WDAU and then transmit the aggregated data to the Hospital Monitoring Station (HMS). In the proposed architecture HMS is placed in a remote hospital or a healthcare centre and is used to receive, process and present the patient data for follow-up action by the medical professionals. A cryptographic solution was presented for the secure transmission of patient data within the home and to/from the hospital to guarantee privacy and confidentiality of the patient's medical data. In this scheme, a unique Patient ID (PID) is used to identify a patient.

We extend our earlier work by proposing an authentication scheme that is based on the Electrocardiogram (ECG) data collected from the patient. The collected ECG data serves to not only monitor the health of the patient but also provides for continuous patient identification. ECG data is difficult to disguise or falsely duplicate and hence provides for a robust authentication system.

The proposed authentication scheme is used at HMS to authenticate the patient. HMS would retrieve the ECG information from the patient data received from AHBS. The ECG signal is first filtered and de-noised and the five fiducial features would be extracted. The extracted values are then compared with the features stored in the hospital database. When a match is found, the PID of the corresponding patient is returned by the fuzzy based system. This PID is verified with the PID present in the packet received from AHBS. If the two values are the same, the patient identity is taken as successfully verified and the data is taken up for further processing at HMS. If the two PIDs do not match, then it is considered as an authentication failure and necessary action can be initiated.

2. MATERIALS AND METHODS

In our proposed scheme, we have chosen the five major and commonly used fiducials, namely, the R peak, QRS interval, P peak, PR interval and QT interval for building the fuzzy authentication system. These fiducials are extracted from the ECG wave and stored in a database at HMS. The proposed scheme does not look for anomalies or variations in the ECG data, the aim is to look for fiducials whose values are consistent to enable authentication.

As stated earlier, several methods are being used for individual authentication like template matching, pattern comparison, decision based neural networks. We propose to use a fuzzy inference system for patient authentication for our proposed At-Home remote monitoring architecture. Fuzzy Logic provides a simple way to make a decision, based on imprecise, ambiguous or vague information. It incorporates a rule based approach to solve problems. Unlike crisp sets which allow either full membership or no membership at all, fuzzy sets allow partial membership. In our approach we have used the fuzzy multiplicative model. Since the ECG features vary within permissible range for the same individual from time to time and as there is no universally acknowledged rule for exactly defining wave boundaries (Plataniotis *et al*., 2006), using a fuzzy based authentication system would provide an opportunity to model conditions that are not precisely defined, thereby accommodating the errors which may occur during fiducial extraction methods.

A Fuzzy Inference System comprises the steps of Fuzzification, Rule Evaluation and Defuzzification to process the system inputs to the appropriate system outputs. Mamdani, Sugeno and Tsukamoto are the three types of Fuzzy Inference Systems (FIS) widely used in various applications (Jang *et al*., 1997). The Sugeno model though computationally more efficient than the Mamdani model works well for a linear system. The Tsukamoto model aggregates the output of each rule by using the weighted average and hence avoids the process of defuzzification. But it is not transparent like the Mamdani or Sugeno model and therefore it is not used often.

Hence, the Mamdani model was chosen for implementation because it is intuitive and can accurately model a real system for which the relation between the inputs and outputs are known. Mamdani system accurately models a crisp system, where the inputs and output are crisp. Crisp inputs are the exact input values measured by a sensor for example like temperature, pressure. In our proposed system, the ECG parameters chosen as input are crisp values and the output is required to identify a single person from the database, which is also a crisp value.

The Fuzzy Inference System using Mamdani model has five layers namely the fuzzy layer, product layer, implication layer, aggregation layer and the defuzzification layer (Guney and Sarikaya, 2009). The FIS architecture for our proposed system using the three inputs; P peak, R peak and the PR interval is given in **Fig. 3**.

The rule base represents the possible combination of inputs and their associated Membership Functions (MF). As there are 3 inputs and each membership function may be named as negative, zero and positive, there are totally 27 rules. The rule set for the Mamdani system may be written as:

$$\begin{gathered}\text{If }\left(\text{R is }M_{1p}\right)\text{AND}\left(\text{P is }M_{2q}\right)\\ \text{AND}\left(\text{PR is }M_{3r}\right)\text{THEN}Y_r\text{is }M_{or}\end{gathered}$$

For p = 1, q = 1, r = 1, 2, 3, the above equation gives the first set of three rules:

- For the next 3 rules, Y_{3+r} ; p = 1, q = 2 and r = 1,2,3
- Y_{6+r}; p = 1, q = 3, r = 1,2,3
- Y_{9+r}; p = 2, q = 1,r = 1,2,3
- Y_{12+r}; p = 2, q = 2, r = 1,2,3
- Y_{15+r}; p = 2,q = 3,r = 1,2,3
- Y_{18+r}; p = 3, q = 1, r = 1, 2, 3
- Y_{21+r}; p = 3, q = 2, r = 1, 2, 3
- Y_{24+r}; p = 3, q = 3, r = 1, 2, 3

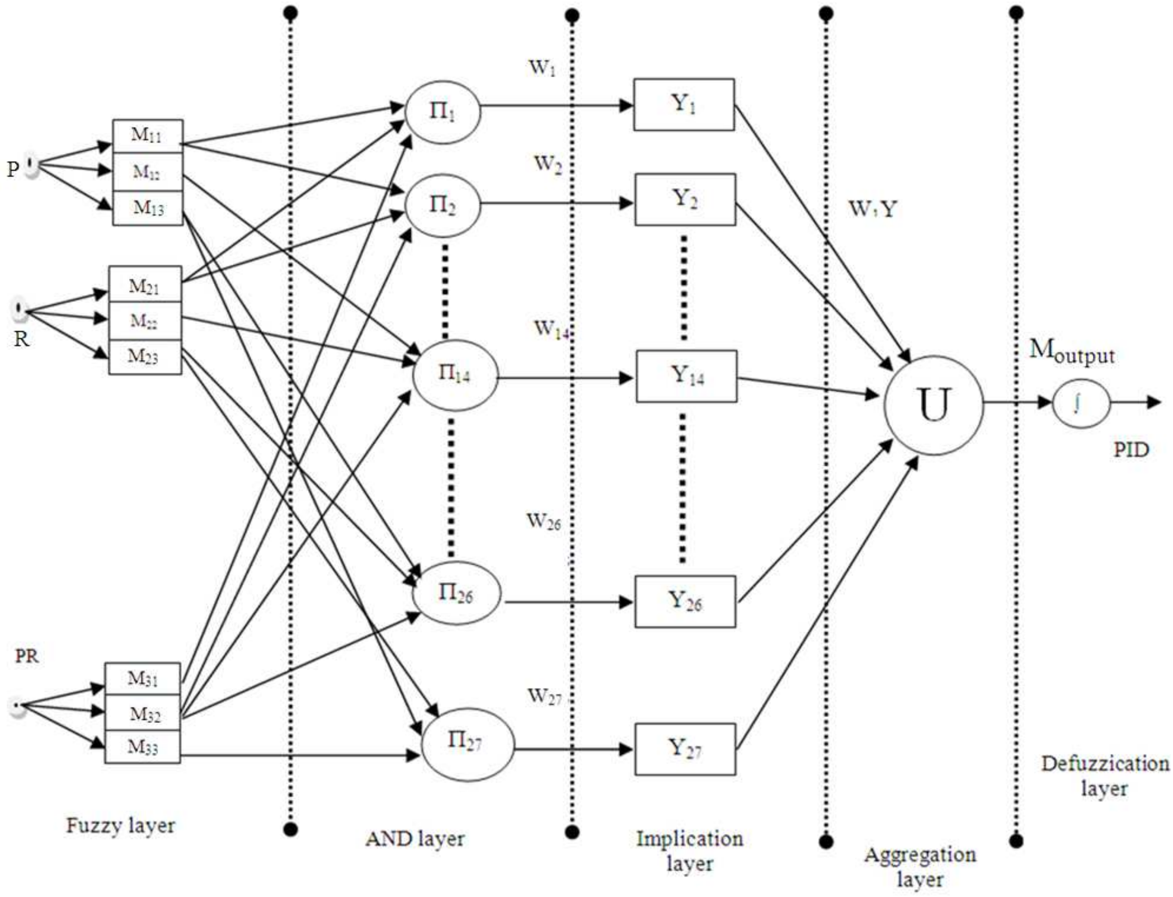

Fig. 3. FIS architecture for 3 parameter authentication system

The above expressions give a total of 27 rules for the FIS. Here R, P and PR are the ECG features taken as input, M_{1p}, M_{2q} and M_{3r} are the input MF.

M_{or} is the output MF.

The first layer is the fuzzy layer, wherein the crisp input values are mapped into fuzzy values by using the Membership Function (MF). The MF used in this work is a triangular membership function Equation (1):

$$f(x,a,b,c) = \max\left[\min\left[\frac{x-a}{b-c},\frac{c-x}{c-b}\right],0\right] \tag{1}$$

where, a and b are the 'feet' of the triangle and b locates the 'peak' of the triangle.

The second layer is the product layer. We have chosen the AND operator because it is desirable for the authentication scheme to include the membership of all the three inputs to compute the firing strength (weight w) of each rule. In other words, all the input parameters are given equal importance in identifying the patient. The weights are determined by applying the AND operator to the membership values of the input. This corresponds to obtaining the product of the input membership values, as in Equatiion 2:

$$\left.\begin{aligned}
W_1 &= M_{11}(R)M_{21}(P)M_{31}(PR)\\
W_2 &= M_{11}(R)M_{21}(P)M_{32}(PR)\\
W_3 &= M_{11}(R)M_{21}(P)M_{33}(PR)\\
W_4 &= M_{11}(R)M_{22}(P)M_{31}(PR)\\
&.\\
&.\\
W_{26} &= M_{13}(R)M_{23}(P)M_{33}(PR)\\
W_{27} &= M_{13}(R)M_{23}(P)M_{33}(PR)
\end{aligned}\right\} \tag{2}$$

The third layer is the implication layer the implication of each output MF is computed by (Guney and Sarikaya, 2009) Equation (3):

$$M_{im,j} = W_j Y_j \forall j = 1,2,3......27 \quad (3)$$

The next layer is the aggregation layer where every implicated membership function is aggregated using the union operator to obtain an overall output given by Equation (4):

$$M_{OUTPUT} = \bigcup_{j=1}^{27} M_{imp,j} \quad (4)$$

The fifth layer is the defuzzification layer**.** In this layer Defuzzification is performed by using the centroid of area method, that is, the fuzzy output is mapped into a crisp output.

As explained earlier, the R peak, P peak and the PR interval values are given as input to the FIS, the PID of the person thus identified is returned by the Fuzzy system as the crisp output. The PID returned is then compared with the PID received along with the patient data. If the PIDs match then authentication is successful and the received data can be processed further at HMS. If the PIDs do not match, then the authentication is unsuccessful and appropriate action can be taken.

In the event that somebody else wears the sensor jacket of the patient either intentionally or otherwise, the ECG parameters of the new person would not be available in the HMS database. So a match would not be found and therefore the system sounds an alert indicating that the authentication procedure was unable to identify the patient. In this case too, appropriate action can be initiated, such as alerting a family member of the patient to check the safety of the patient.

3. RESULTS

The Fuzzy Inference System was implemented in MATLAB using the Fuzzy Logic Toolbox. The ECG waves were taken from the Physio Bank database. Two sets of data were taken for each patient; one set was used in the training phase and the other as the test set. The fiducials extracted from the training set were stored in a database. The fiducials that were extracted from the test set were compared with the fiducials obtained during the training phase. The fuzzy system was implemented for varying number of input parameters, namely single parameter (R peak), two parameters (R peak and P peak), three parameters (R peak, P peak and PR interval), four parameters (R peak, P peak, QRS interval and QT interval) and five parameters (R peak, P peak, QRS interval, QT interval and PR interval).

Totally 50 people's ECG were taken for testing the system. We had also implemented and tested the performance of our system with the K-Nearest Neighbor method used in (Sriram *et al*., 2009) as the authentication scheme has been proposed specifically for a remote health monitoring application. All other methods have proposed an ECG based authentication scheme in general. The comparison of the two schemes is shown in **Table 1**.

It can be noted from the table that when a single input was given to the fuzzy system, less than half the number of persons were correctly identified by our proposed fuzzy system and the accuracy was 40% only. Whereas the K-Nearest Neighbor method achieved 58% accuracy, that is, out of the 50 persons, 29 were correctly identified. For the two input system where the R peak and the P peak were given as input, the K-Nearest Neighbor method once again performed better than our proposed system by achieving 84% accuracy as against the 79% accuracy of our system. However, for three or more inputs, our proposed system is able to achieve 100% accuracy, that is, all 50 people were correctly identified for the 3 input system. The K-Nearest Neighbor method gives 89% accuracy for the three input system but achieves 100% accuracy for four and five input systems. The K-Nearest Neighbor method consistently produces better accuracy with increasing number of parameters, but the Fuzzy Inference System shows significant improvement in accuracy when only 3 parameters are given as input to the system.

Table 1. Comparative results for the accuracy of Fuzzy Inference System and KNN method

Number of parameters method	1 parameter FIS (%)	2 parameters FIS (%)	3 parameters FIS (%)	4 parameters FIS (%)	5 parameters FIS (%)
Fuzzy	40	79	100	100	100
KNN method-distance	58	84	89	100	100

Table 2. Performance measures for the Fuzzy based authentication System

Performance Metric	1 parameter FIS	2 parameters FIS	3 parameters FIS	4 parameters FIS	5 parameters FIS
True positive	15.000	30.000	38	38	38
False negative	23.000	8.000	0	0	0
Sensitivity	0.395	0.789	1	1	1
False negative rate	0.605	0.211	0	0	0

4. DISCUSSION

We now evaluate the performance of our proposed system using standard performance measures used for a person identification scheme. Since a one-to-many match is performed, performance metrics such as the count of True Positive, False Negative and Sensitivity have been used. True Positive gives the number of instances when the identification made is accurate. False Positive gives the number of instances when the identification is incorrect. Sensitivity is a measure of the proportion of actual positives which are correctly identified as shown in Equation 5:

$$\text{sensitivity} = \frac{\text{Number of Ture Positives}}{\text{Number of ture positives} + \text{Number of Fals Negatives}} \quad (5)$$

Another parameter which is related to the Sensitivity is the False Negative Rate (FNR) given in Equation 6:

$$\text{FNR} = 1 - \beta \quad (6)$$

where, β is the value of sensitivity calculated using Equation 5. FNR denotes the proportion of events that are being tested for which the yield is a negative outcome. The calculated performance measures are given in **Table 2**.

It can be noted from the table that sensitivity increases as the number of parameters are increased and 100% enrollment is obtained for 3, 4 and 5 parameters.

We were able to achieve 100% accuracy in our proposed system for a lesser number of fiducials as compared to other systems. Therefore, the proposed system is less complex than other systems which use more number of fiducials to achieve the required accuracy.

5. CONCLUSION

Patient authentication is a key element of a remote health monitoring system because it is used to associate the received data with the correct patient. Our proposed scheme uses patient ECG data to authenticate assisted living patients in their home environment. The authentication scheme is capable of uniquely identifying the patient from the patient database maintained at the HMS. The proposed scheme is simple and gives 100% enrollment, with only three fiducial inputs. Moreover the proposed system provides for continuous authentication based on the ECG data collected from the patient at regular intervals. As the range for the values of the ECG fiducials is not exactly defined, using a fuzzy system for patient authentication has helped in exploiting the fuzzy nature of the biometric input. Since the proposed system is not used for remote diagnosis, the authentication scheme does not look to recognize any anomalies in the ECG patterns.

6. REFERENCES

Biel, L., O. Pettersson and P. Wide, 2001. ECG analysis: A new approach in human identification. IEEE Trans. Instrum. Meas., 50: 808-812. DOI: 10.1109/19.930458

Bousselijot, R. and D. Kreiseler, 1998. ECG signal analysis by pattern comparison. Comput. Cardiol., 25: 349-352. DOI: 10.1109/CIC.1998.731806

Chan, A.D.C., M.M. Hamdy, A. Badre and V. Badee, 2006. Person identification using electrocardiograms. Proceedings of the Canadian Conference on Electrical and Computer Engineering, May 7-10, IEEE Xplore Press, Ottawa. pp: 1-4. DOI: 10.1109/CCECE.2006.277291

Guney, K. and N. Sarikaya, 2009. Comparison of mamdani and sugeno fuzzy inference system models for resonant frequency calculation of rectangular microstrip antenna. Prog. Electrom. Res., 12: 81-104. DOI: 10.2528/PIERB08121302

Hoekema, R., G.J.H. Uijen and A.V. Oosterom, 2001. Geometrical aspects of the interindividual variability of multilead ECG recordings. IEEE Transa. Biomed. Eng., 48: 551-559. DOI: 10.1109/10.918594

Hoekerd, P. and B.V. Delft, 2008. Biometric authentication-a heartbeat away.

Irvine, J.M., S.A. Israel, W.T. Scruggs and W.J. Worek, 2008. Eigenpulse: Robust human identification from cardiovascular function. Patt. Recog., 41: 3427-3435. DOI: 10.1016/j.patcog.2008.04.015

Israel, S.A., J.M. Irvine, A. Cheng, M.D. Wiederhold and B.K. Wiederhold, 2005. ECG to identify individuals. Patt. Recog., 38: 133-142. DOI: 10.1016/j.patcog.2004.05.014

Jang, J.S.R., C.T. Sun and E. Mizutani, 1997. Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence. 1 Edn., Prentice Hall, Upper Saddle River, ISBN-10: 0132610663, pp: 614.

Kounga, G., M.C. Mont and P. Bramhall, 2010. Privacy-preserving management of personal data for assisted-living applications. Proceedings of the 1st International Workshop on the Security of the Internet of Things (SIT '10), Tokyo.

Loyouni, M., K. Verslype, M.T. Sandikkaya, B. Decker and H. Vangheluwe, 2009. Privacy-preserving telemonitoring for ehealth. Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, (WCDAS '09), Springer-Verlag Berlin, Heidelberg, pp: 95-110. DOI: 10.1007/978-3-642-03007-9_7

Mohanavalli, S.S. and A. Sheila, 2011. Security architecture for at-home medical care using body sensor network. Int. J. AdHoc, Sensor Ubiquitous Comput., 2: 60-69.

Mundt, C.W., K.N. Montgomery, U.E. Udoh, V.N. Barker and G.C. Thonier, 2005. A multiparameter wearable physiologic monitoring system for space and terrestrial applications. IEEE Trans. Inform. Technol. Biomed., 9: 382-391. DOI: 10.1109/TITB.2005.854509

Pandian, P.S., K. Mohanavelu, K.P. Safeer, T.M. Kotresh and D.T. Shakunthala *et al*., 2008. Smart Vest: Wearable multi-parameter remote physiological monitoring system. Med. Eng. Phys., 30: 466-477. DOI: 10.1016/j.medengphy.2007.05.014

Plataniotis, K.N., D. Hatzinakos and J.K.M. Lee, 2006. ECG biometric recognition without fiducial detection. Proceedings of the Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, Sept. 19-Aug. 21, IEEE Xplore Press, Baltimore, MD., pp: 1-6. DOI: 10.1109/BCC.2006.4341628

Shen, T.W., W.J. Tompkins and Y.H. Hu, 2002. One-lead ECG for identity verification. Proceedings of the 2nd Joint Engineering in Medicine and Biology, 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society EMBS/BMES Conference, Oct. 23-26, IEEE Xplore Press, pp: 62-63. DOI: 10.1109/IEMBS.2002.1134388

Sriram, J.C., M. Shin, T. Choudhury and D. Kotz, 2009. Activity-aware ECG-based patient authentication for remote health monitoring. Proceedings of the 2009 International Conference on Multimodal Interfaces, (MI '09), ACM Press, New York, USA., pp: 297-304. DOI: 10.1145/1647314.1647378

Sufi, F., I. Khalil and J. Hu, 2010. ECG-based Authentication. In: Handbook of Information and Communication Security, Stavroulakis, P. and M. Stamp, (Eds.), Springer, New York, ISBN-10: 3642041175, pp: 309-331.

Wang, Q., W. Shin, X. Liu, Z. Zeng and C. Oh *et al*., 2006. I-living: An open system architecture for assisted living. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Oct. 8-11, IEEE Xplore Press, Taipei, pp: 4268-4275. DOI: 10.1109/ICSMC.2006.384805