Fuzzy Framework for Preserving Privacy in Neural Networks Classification

Majid Bashir Malik
Deptt. of Computer Sciences, BGSB University, Rajouri, J & K, India

M. Asger
School of Mathematical Sciences & Engg., BGSB University, Rajouri, J & K, India

Rashid Ali
Department of Computer Engineering, Aligarh Muslim University, Aligarh, India

Tasleem Arif
Department of Information Technology, BGSB University, Rajouri, J & K, India

ABSTRACT

Data mining is an automated process of excavating useful information that is previously unknown, from huge and enormous volumes of data. This information is used in banking, agriculture, medical diagnosis, telecommunication, intrusion detection, genetic engineering, education, marketing, investments, weather forecasting etc. Classification is one of the most important data mining techniques. Many real world problems are being solved using this approach. Neural networks, as a classification technique has emerged as an important soft computing based approach in data mining. It is being used widely in healthcare for prediction and analysis. But there are some apprehensions regarding privacy of the individuals to whom the data originally belongs. In this paper, a methodology has been developed to resolve the privacy issue by integrating fuzzy logic in the process of NN classification and at the same time the accuracy of the results of the NN classification has been preserved as in the absence of integrated privacy constraints.

Keywords

Privacy preserving data mining, Soft Computing, Neural Networks, Fuzzy sets, Fuzzy membership function

1. INTRODUCTION

Days are not far when the economy of a country shall be decided by the amount of data it has in its data repositories and the quality of such data. Success of any field that affects human life, may be its business, medical sciences, research, weather forecasting, defense, agriculture, engineering, banking, law, telecommunication, anti-terrorism, cyber crimes or education, now-a-days depends on the quality and amount of data along with the appropriate information discovery mechanism [8]. Appropriate mechanism if applied, it can contribute extensively towards increased revenue, accurate predictions and better decision support system [1-3]. Traditional tools and techniques fail to deliver due to huge volume of data and complexity of the applications. The goal of data mining is to develop efficient, sophisticated, robust and intelligent mechanism for information extraction [1,6,7] from huge volumes of data. The need of data mining has been felt long ago and was being done manually. Simply, it was dependent on the analytical skills of the human experts. With the advent of low cost storage devices and high computational power of the computers the paradigm shifted towards automating the task as the volume of data grew out of the range of human analytical expertise. Although the data mining promises a lot but it has to face some challenges like high dimensionality, non-standardization of data bases, distributed databases, values representing partial truths, ever-changing data and expiry of data [7]. Last but not least is the concern of privacy of the individuals in the process of data mining task.

1.1 Soft Computing

Soft computing technology provides flexible information processing capabilities to handle real-world ambiguous problems [9]. The challenges in developing acceptable and efficient solutions for mining are well being addressed by soft computing techniques [9]. Soft computing is a specialized technique capable of handling partial truth, uncertainty, and imprecision very efficiently [10]. Human brain forms the basis for model of soft computing techniques. The target of soft computing is to achieve solutions with features like robustness, tractability, and at the same time the one which is less expensive in terms of time and space complexity [7]. Systems developed using soft computing techniques have high Machine Intelligence Quotient [7].

Genetic algorithms, Neural networks, Rough sets, and Fuzzy logic are some of the most widely used soft computing techniques. Fuzzy sets specialize in dealing with uncertainty [9-10]. It's a framework that naturally models imprecise but qualitative knowledge for the handling uncertainty and transmission at various stages. It supports reasoning in natural form in a way the humans do. Neural Network is composed of a large number of highly interconnected neurons [19]. Basically neurons are processing elements in an architecture inspired by human brain. Neural Networks are successfully implemented in rule generation and classification. Genetic algorithms are robust and adaptive. They are global search methods suitable for very large search space [9, 19]. Genetic algorithms are used in various search and optimization processes like template selection and optimization of queries [7]. Rough set is a mathematical tool for managing uncertainty because of indiscernibility among objects of a set. It is used for discovering dependencies and redundancies between the given features of a problem during classification of data [6-8].

Soft computing technique is a distinct methodology for addressing problems in its domain that work in cooperative manner rather than in competitive manner. And the result is an intelligent and robust system that is low cost, human interpretable approximate solution in comparison to the solutions developed using conventional techniques of data mining [9].

Neural network is mathematical model used for analysis of data in any form, where it is difficult to perform the job using conventional methods or human analysis [19]. Inherently humans have a limitation of handling large volumes of data. Principally neural networks are based on human brain. Neural networks are composed of highly interconnected processing units called neurons. The capability of high processing for handling large volumes of data along with the imitation of human brains, neural network finds itself quite supportive for such operations. Neural networks are mostly used where the solutions are either too complex or it is not possible to develop an algorithm for the solution of a problem [6-7]. It has been found to be very useful in prediction, pattern recognition and classification, decision making, data compression and optimization [7, 19].

1.2 Neural networks in clinical diagnosis

Neural networks are also being applied in medical diagnosis, image analysis and drug development. Some examples to justify the stand are [20]: Pap smears are screened manually to predict/detect cervical cancers by the pathologists. If detected at early stage it can be cured. A neural network based application has been developed that examines Pap smears for the detection of cervical cancer. The application has been found very successful and that too at early stages when it is very difficult to predict manually. Another neural networks application related to cardiology has been developed by research group at University Hospital, Sweden. This application proved to be more successful and effective as compared to some of the senior cardiologists. A neural network program was developed by Andrea Dawson et al for the screening of grade of breast cancer. It was found to be in good agreement with human observers. A lot many, such type of neural network applications have been developed in the field of healthcare.

2. MOTIVATION: PRIVACY AT STAKE

Neural Networks have proved as of great help in various predictive analysis applications, particularly in Medical diagnosis. But little consideration has been given to the privacy of the individuals to whom the data originally belongs [7]. The data is submitted, mostly for record keeping, to various labs, hospitals and research organizations. The data is further shared/sold to various organizations which in turn perform research or generate business out of the data. Very little attention has been given to the individual privacy or to the owners of the data. Even though privacy laws have been enacted and enforced but a complete solution is yet to be developed so as to preserve the privacy of the individuals even in case of honest or semi-honest models.

The benefits of the data mining are too large but as soon as privacy of individuals is attempted to be preserved, the results of data mining get affected adversely [6]. The problem is not with the data mining but with the way it is being done [6]. Now as far as medical diagnosis as a data mining application is concerned, any adversity in the results of the data mining can affect the life of any individual. So a proper technique needs to be developed that preserves the privacy of the individuals whose data is being utilized for analysis purpose and at the same time the result quality of the data mining is not compromised.

The actual process of Neural Network Classification involved in Medical diagnosis is as:

1. Get/Collect data: The data can be requested form a single owner/database/party or from multiple owner/database/party. The data owner/database/party may implement some privacy constraints as per their own policy. Most of them hide Identifier fields as it can disclose the identity of the individuals.

2. Prepare data as per the requirement: Here the data is first prepared to support the application optimally for which it will be used. Normally it includes standardization, normalization, filling the missing values, standardizing outliers, data reduction etc.

3. Train the NN application: The NN application is then trained with the data so produced using some novel NN architecture and topology.

4. Test the results: After training the NN, its performance is tested against certain inputs. The results so generated decide whether to train the NNs further or it is fit for the purpose.

5. Input real time data for results: The application is then used with new real time data.

Basically the problem is to develop a methodology wherein the individual should feel secure about the confidentiality of his/her data. As such the benefits of the data mining need not to be sacrificed if proper privacy preserving algorithms are implemented while performing data mining on the data. But results get affected as soon as privacy needs to be preserved.

So a proper balance is needed to be established where the results of the data mining are least affected and at the same time privacy of the stake holders is also preserved.

Various researchers have proposed techniques to preserve the privacy without affecting the privacy of the individuals. Some of the techniques are Anonymization, Randomized response, Condensation, Cryptography etc. But most of the techniques are either application specific or suffer information loss, or have high computation cost or fail to defend against different attacks on privacy [11-18].

In the process of anonymization to protect privacy the identity of the individuals is kept hidden by removing identifier fields. But still the privacy is at stake when such data, particularily the quasi identifiers are linked to publicly available data [13]. The data in anonymization is dependable but it suffers due to background knowledge and homogeneity attack. Excessive privacy preserving in anonymization process leads to heavy information loss [14].

Original values are replaced by synthetic values in case of perturbation technique to protect privacy in data mining [12]. The data so generated can defend against linkage and homogeneity attacks but reconstruction of original values is not possible and new distribution algorithms are required for various data mining applications like classification, clustering or association rule mining [14].

In randomized the data is scrambled, it treats all the records equal without considering local density [7], due which the outlier records become prone to adversarial attacks [15]. Moreover adding too much of noise leads to the decrease in the utility of the data in data mining task.

Synthetic data is generated from the statistics of the clusters such that each record holds a position in the group having same anonymity level [16]. Although this approach is immune to attacks but suffers heavy information loss [14].

Cryptographic techniques are widely used for transformation of data in case where more than one party is involved in data mining task, so as to avoid disclosure of information. But the privacy of individual in this approach is not taken care of [14]. Moreover very little work has been done in case of malicious models [7].

A model has been proposed in [7], to preserve the privacy of individuals by fuzzifying single attribute. The same work has been extended here in this paper by using some other techniques along with the fuzzification of the data in case of neural network classification.

3. SOLUTION

In the proposed work, an attempt has been made to preserve the privacy of individuals without affecting the final results of the Neural network predictions. An application where NNs are being used in prediction of potential diabetic patients has been studied. The data that is being used here in the present work has already been used in [19] for NN predictions. On the basis of certain parameters like DoB, Sex, Smoking, Drinking, Thirst, Urination, Height, Weight, Fatigue etc, the application predicts the potential diabetic patient.

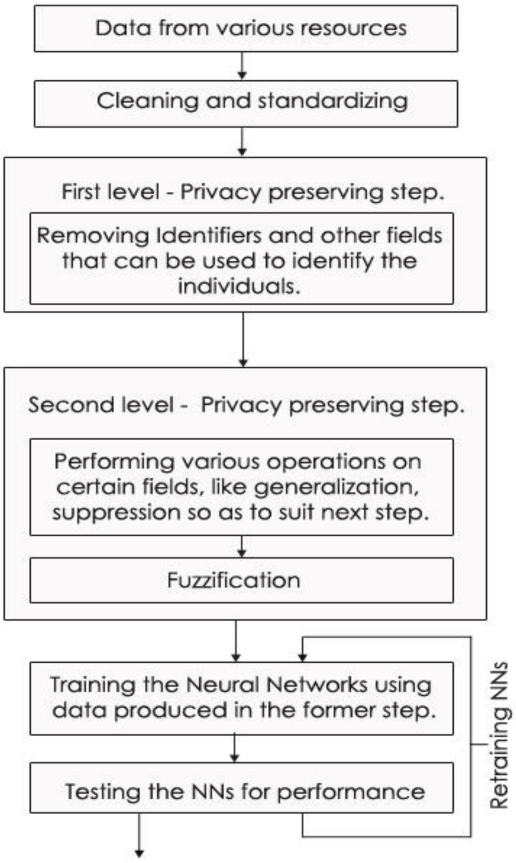
Data from various resources
Cleaning and standardizing
First level - Privacy preserving step.
Removing Identifiers and other fields that can be used to identify the individuals.
Second level - Privacy preserving step.
Performing various operations on certain fields, like generalization, suppression so as to suit next step.
Fuzzification
Training the Neural Networks using data produced in the former step.
Testing the NNs for performance
Retraining NNs

Fig.1: Block Diagram of the proposed solution.

The algorithmic solution/model that has been proposed for the same application where in an attempt has been made to preserve the privacy is as:

1. The data regarding potential diabetic patients has been requested from various diagnostic labs.
2. Identifier fields, like name, address, which can be used to identify the individual have been removed.
3. Some fields have been generalized like DoB.
4. For the purpose of privacy preservation fuzzification of the all fields has been done (except those which take Boolean values) using S-shaped fuzzification membership function.
5. Train the Neural networks using multiple back propagation.
6. Test the results.
7. In case the training is not satisfactory the NNs are further re-trained

For the purpose of study the results so drawn have been compared with the results of that have been drawn in absence of the privacy preservation mechanism. It has been established that the results are in good agreement with each other.

3.1 Experimental results

The data of various individuals who are suspected to be diabetic by the doctor is being used in the study. The data has already been used in [19] for Neural network classification. Firstly the identifier fields have been removed. DoB attribute has been converted into 'Age'. It is an xls file having 388 records with ten input attributes and one result/class attribute. All the input attributes, except boolean attributes, have been fuzzified using S-shaped fuzzy membership function. The equation for S-shaped fuzzy membership function is as:

$$f(x;a,b) = \left\{\begin{array}{cc} 0, & x \le a \\ 2\left(\frac{x-a}{b-a}\right)^2, & a \le x \le \frac{a+b}{2} \\ 1-2\left(\frac{x-b}{b-a}\right)^2, & \frac{a+b}{2} \le x \le b \\ 1, & x \ge b \end{array}\right\}$$

Eq. 1: S-shaped fuzzy membership function

Where 'x' is the value to be fuzzified

'a' and 'b' are lower and upper limits

Now there are two sets of data

1. Original data and
2. Fuzzified data

Both the datasets original and fuzzified have been used for training the neural network applications using same set of parameters, NN architecture and topology. Standard back propagation based multilayer perceptron (MLP) architecture of ANN has been for training original and fuzzified data so that the results after training the NN by both forms of data can be compared. This architecture is often used for ANN in medical research [19]. It's a directed graph of multiple layers of artificial neurons where each layer is connected to next layer. Back propagation is a gradient descent technique that minimizes the error criteria and it is a simple way to determine the error criteria and it is simple way to determine the error values in hidden layers. The hidden layer allows ANN to develop its representation of input–output mapping. In case of back propagation, the error data at the output layer is propagated back to earlier layers, thereby allowing incoming weights to these layers be updated and adjusted such that the error between the input and desired output is as least as possible [19]. The topology employed is 10 inputs, one hidden layer and one output.

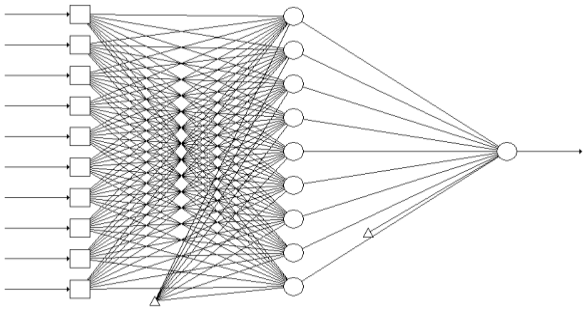

Fig. 2: NN Topology followed in the experiment.

3.2 Performance of ANNs

First the ANNs have been trained and tested by Normal data for 100000 epochs using Multiple Back Propagation version 2.2.4 tool. The number of records for training purpose is 270 and 118 records have been used for testing purpose of the same using the topology as shown in Fig. 2. Thereafter the fuzzified version of the original data that has been fuzzified using S-shaped fuzzy membership function is used to train the ANNs. The number of records in training and testing purpose, number of epochs and even the topology and architecture followed are the same as in the former case. After training and testing the neural networks the results were drawn and compared for both normal and fuzzified data.

The accuracy rate of the ANNs' trained through fuzzified data has been found producing better results as compared to the ANNs' trained through original data. During testing, out of 119, only 20 instances were predicted wrongly in former case as compared to 28 wrongly predicted instances in the later one. Thereby accuracy rate so generated is 85.61% in former and 79.85% in later case.

3.3 Confusion Matrix

A confusion Matrix (proposed by Kohavi and Provost in 1998) represents information in a tabular form regarding predicted and actual classification calculated by the system. This information in the matrix is used to evaluate the performance of systems. The following table shows the confusion matrix for a two class classifier.

Table 1: Confusion Matrix for a two classifier.

		Predicted	
		Negative	**Positive**
Actual	**Negative**	**a**	**b**
	Positive	**c**	**d**

a) *number of correct predictions that an instance is negative,*

b) *number of incorrect predictions that an instance is positive,*

c) *number of incorrect of predictions that an instance negative, and*

d) *number of correct predictions that an instance is positive.*

The parameters calculated on the basis of the results in the above table:

1. Accuracy (AC) is the proportion of the total number of predictions that are correct and is calculated by the equation: AC= (a + d) / (a + b + c + d).
2. True positive rate (TP) is the proportion of positive cases and is calculated by the equation: TP= d / (c + d).
3. False positive rate (FP) is the proportion of negative cases that are incorrectly classified as positive: FP= b / (a + b).
4. True negative rate (TN) is the proportion of negative cases that are classified correctly and is represented by: TN= a / (a + b).
5. False negative rate (FN) is the proportion of positive cases that are incorrectly classified as negative and is represented by: FN= c / (c + d).
6. Precision (P) is the proportion of predicted positive cases that are correct and is represented as: P= d / (b + d).

Table 2: Confusion Matrix of Normal Data Training

		Predicted	
		0	**1**
Actual	**0**	190	0
	1	3	56

AC=	(190 + 56) / (190 + 3 + 0 + 56)	=0.98795
TP=	56 / (3 + 56)	=0.94915
FP=	0 / (190 + 0)	=0
TN=	190 / (190 + 0)	=1.0
FN=	3 / (3 + 56)	=0.05084
P=	56 / (0 +56)	=1.0

Table 3: Confusion Matrix of Fuzzified Data Training

		Predicted	
		0	**1**
Actual	**0**	189	01
	1	01	58

AC=	(189 + 58) / (189 + 1 + 1 + 58)	=0.99196
TP=	58 / (1 + 58)	=0.98305
FP=	1 / (189 + 1)	=0.00526
TN=	189 / (189 + 1)	=0.99473
FN=	1 / (1 + 58)	=0.01694
P=	58 / (1 + 58)	=0.98305

Table 4: Confusion Matrix of Normal Data Testing.

		Predicted	
		0	**1**
Actual	**0**	03	0
	1	28	108

AC=	(3 + 108) / (3 + 0 + 28 + 108)	=0.79856
TP=	108 / (28 + 108)	=0.79411

FP=	0 / (3 + 0)	=0
TN=	3 / (3 + 0)	=1.0
FN=	28 / (28 + 108)	=0.20588
P=	108 / (0 + 108)	=1

Table 5: Confusion Matrix of Fuzzified Data Testing.

		Predicted	
		0	**1**
Actual	**0**	3	0
	1	20	116

AC=	(3 + 116) / (3 + 0 + 20 + 116)	=0.85611
TP=	(116) / (20 + 116)	=0.85294
FP=	0 / (3 + 0)	=0
TN=	3 / (3 + 0)	=1.0
FN=	20 / (20 + 116)	=0.14705
P=	116 / (0 + 116)	=1.0

Table 6: Comparative results of normal and fuzzified training and normal and fuzzified testing on the basis of various parameters calculated through Confusion Matrix.

	Data Training		Data Testing	
	Normal	**Fuzzified**	**Normal**	**Fuzzified**
AC	0.98795	0.99196	0.79856	0.85611
TP	0.94915	0.98305	0.79411	0.85294
FP	0.0	0.00526	0.0	0.0
TN	1.0	0.99473	1.0	1.0
FN	0.05084	0.01694	0.20588	0.14705
P	1.0	0.98305	1.0	1.0

Bar Chart representation of the results shown in the table 6:

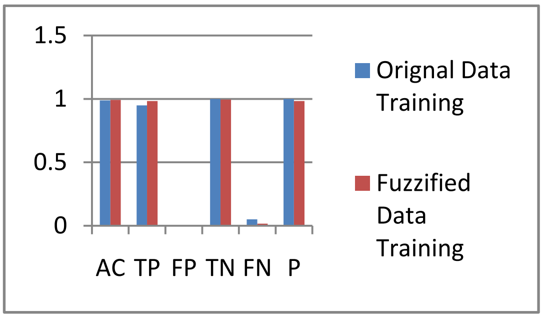

Fig.: 3: Bar Chart representation of the results of Normal Data Training and Fuzzified data training.

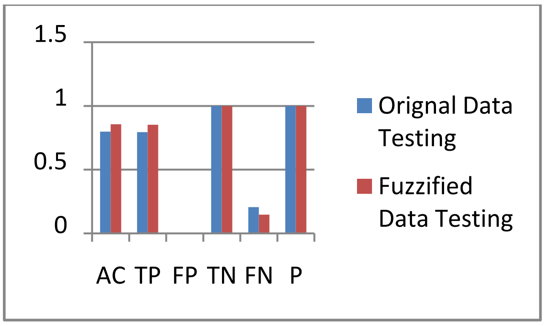

Fig.: 4: Bar Chart representation of the results of Normal Data Testing and Fuzzified data testing

4. CONCLUSION

Privacy in data mining has evolved as a research field of great interest and need. Lots of research is being done in order to preserve the privacy of the individuals without sacrificing the quality of data and adding to the complexity in the data mining process. But most of them suffer from information loss or computational complexity. In this paper it is demonstrated how to preserve privacy during data analysis without effecting the quality of results. Results so generated are almost same and even better accuracy is being delivered when fuzzified data is being used instead of the normal one. Various parameters calculated through confusion matrix as represented in table 7, Fig. 3 and Fig. 4 prove the efficiency of the proposed model.

5. REFERENCES

[1] A. Ahmad, and L. Dey, "A k-mean clustering algorithm for mixed numeric and categorical data," Data & Knowledge Engineering, vol. 63, no. 2, pp. 503-527, 2007.

[2] Zhihua, X. "Statistics and Data Mining", Department of Information System and Computer Science, National University of Singapore, 1998.

[3] Tsantis L & Castellani J. "Enhancing Learning Environment Solution-based knowledge Discovery Tools: Forecasting for Self-perpetuating Systematic Reform", JSET Journal, 2001

[4] Luan, J. "Data Mining Application in Higher education", SPSS Executive Report. Retrieved from http://www.crisp-dm.org/CRISPWP.pdf, 2002

[5] N Matatov, L Rokach, O Maimon, "Privacy Preserving Data Mining: A feature set partitioning approach", Elsevier, March 2010.

[6] M. B. Malik, M. A. Ghazi, R. Ali, "Privacy preserving data mining techniques: Current Scenario and future prospects", Third International Conference on Computer and Communication Technology, 2012.

[7] M B Malik, M Asger, R Ali, A Sarvar, "A Model for Privacy Preserving in Data Mining using Soft Computing Techniques", INDIACom 2015, International Conference on Computing for Sustainable Global Development, PP 181-186, March 2015.

[8] M B Malik, M Asger, R Ali, T Arif, "Privacy preserving data mining using fuzzy based approach", Commune 2015, International conference on Advances in Computers, Communication and Electronic Engineering, PP 336-338, March 2015.

[9] Sushmita Mitra, Sankar K. Pal and Pabitra Mitra, "Data Mining in Soft Computing Framework: A Survey", IEEE Transactions on Neural Networks, Vol 13, No. 1, 2002.

[10] L. A. Zadeh, "Fuzzy Logic, Neural Networks, and Soft Computing." *Communications of the ACM*, vol. 37, no. 3, pp: 77-84, March 1994.

[11] Benjamin C M Fung, Ke Wang, Rui Chen, Philip S Yu, "Privacy Preserving Data Publishing: A Survey of recent developments", ACM Computing Surveys, Vol. 42, No. 4, Article 14, June 2010.

[12] B. Karthikeyan, G Manikandan, V. Vathiyanathan, "A fuzzy based approach for privacy preserving clustering", Journal of Theoretical and Applied Information technology", Vol. 32, No. 2, Oct. 2011

[13] Sweeney L, "Achieving k-Anonymity privacy protection using generalization and suppression" International journal of Uncertainty, Fuzziness and Knowledge based systems, 10(5), 571-588, 2002.

[14] Gayatri Nayak, Swagatika Devi, "A survey on Privacy Preserving Data Mining: Approaches and Techniques", International Journal of Engineering Science and Technology, Vol. 3 No. 3, 2127-2133, 2011.

[15] Y. Lindell and B. Pinkas, "Privacy Preserving Data Mining", Journal of Cryptology, 15(3), pp.36-54, 2000.

[16] Aggarwal C, Philip S Yu, "A condensation approach to privacy preserving data mining", EDBT, 183-199, 2004.

[17] Aggarwal C, Philip S Yu, "A General Survey of Privacy-Preserving Data Mining Models and Algorithms", Springer Magazine, XXII, 11-52, 2008.

[18] Clifton C, Kantarcioglu M, Vaidya J, Xiaodong L, Michael Y, "Tools for Privacy Preserving Distributed Data mining", SIGKDD Explorations letters Vol. 4, Issue 2, December 2002.

[19] Abid Sarvar, Vinod Sharma, "Comparative analysis of machine learning techniques in prognosis of type II diabetes", AI and Society, Journal of Knowledge, Culture and Communication, Vol. 29, No. I, 2014.

[20] Margarta Sordo, "Introduction to Neural Networks in Healthcare", Open Clinical Knowledge Management for Medical Care, October 2002.