ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/2332
DOI URL: http://dx.doi.org/10.21474/IJAR01/2332

RESEARCH ARTICLE

ENFORCING PATIENT PRIVACY ASSURANCE POLICY: A PRIVACY VIOLATION DETECTION AND RESPONSE SYSTEM.

SofienneMansouri[1] and Bel G Raggad[2].

1. The Higher Institute of Medical Technologies of Tunis, University of Tunis El-Manar, Laboratory of Biophysics and Medical Technology, Tunisia.
2. Seidenberg School of CS & IS, Pace University, Pleasantville, NY 10570.

……………………………………………………………………………………………………....

Manuscript Info

……………………….

Manuscript History

Received: 30 September 2016
Final Accepted: 30 October 2016
Published: November 2016

Key words:-
Telemedicine, Privacy, HIPAA, Privacy Assurance Policy, Privacy Violation Detection Systems.

Abstract

………………………………………………………………

We discuss the design of a patient privacy assurance system through the development of a privacy violation detection and response system (pvdrs) generator. This design collects evidence on patient privacy violations throughout an e-health environment and involves a belief fuser, a classifier, and a memoryless fuzzy incident responder. The telemedicine system’s privacy assurance policy, its current risk profile, and training data constitute input streams feeding the pvdrs. The system is designed to produce an incident response that health providers feasibly adopt to improve the e-health system's risk position as indicated in the system’s privacy assurance policy. We do not present a prototype for the pvdrs generator but we provide sufficient details on the credal and pignistic schemes for the fuser and the classifier, needed to develop the pvdrs generator.

……………………………………………………………………………………………………....

Introduction:-

Great attention was paid to privacy [19, 24]. Despite the varied definitions the literature has given to privacy, this term remains complex and difficult to delineate [20, 21]. Often, the meaning of this term will depend on the context and also on subjects, whether they are politicians, health providers, or human resources [7, 20]. Sometimes, privacy is employed to mean confidentiality, or security. In this study, we use the term privacy in relation to the assembly, storage, and use of patient’s personal information. This definition is concerned with the conditions of data collection, its purpose of use, and patient’s consent: Has the patient authorized the specific processing conditions of his/her personal information [19, 26]?

For example, the privacy protection requirement prevents e-doctors from disclosing information shared with them by an e-patient in the course of an e-consultation. Unauthorized, even accidental, disclosures of data gained as part of an e-consultation, while the e-doctor and his/her e-patient are at a distance, are breaches of privacy [23, 26]. At the same time, privacy is also concerned with all the procedural and technical measures required to prevent unauthorized access, modification, use, and dissemination of patient’s personal data stored or processed in health providers’ computers and networking devices [7, 24, 20].

Privacy protection is an important capability in e-healthcare. Any e-health system remains partial without the support of this capability. Telemedicine systems will need massive data processing to provide for privacy protection,

Corresponding Author:-SofienneMansouri.
Address:-The Higher Institute of Medical Technologies of Tunis, University of Tunis El-Manar, Laboratory of Biophysics and Medical Technology, Tunisia.

and unless an efficient privacy protection system is in place, violations of patient privacy may remain undetected and risks may raise beyond repair. It will be just too late to devise an incident response mechanism that works.

The HIPAA act imposes many requirements on HIPAA-covered entities to protect the health information of patients, and to monitor the sources' disclosure of patient information and the recipients. The Department of Health and Human Services' Office for Civil Rights (OCR) has the power to issue financial penalties to those HIPAA-covered entities that fail to comply with HIPAA Rules. Financial penalties for HIPAA violations get updated in a continuous manner and have recently (March 2013) introduced the Omnibus Rule that introduced charges in line with the Health Information Technology for Economic and Clinical Health Act [23].

The Omnibus Rule applies penalties for HIPAA violations against healthcare providers, health plans, healthcare clearinghouses and all other HIPAA-covered entities that are found to have violated HIPAA Rules [23]. The need for protecting the privacy of patients and confidentiality of health data imposes financial penalties for the purpose of deterring violators and for enforcing the accountability of HIPAA-covered entities. The penalty structure is organized in terms of the extent of knowledge the covered entity has when executing the violation, bearing in mind that ignorance of HIPAA Rules cannot be used as an excuse for a rule violation.

There are then 4 categories for the penalty structure as follows [23]:
Category 1: A violation that the HIPAA-covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
Category 2: A violation that the HIPAA-covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
Category 3: A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation.

Category 4: A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation In the case of unknown violations, where the HIPAA-covered entity could not have been expected to avoid a data breach, it may seem unreasonable for a HIPAA-covered entity to be issued with a fine. The OCR appreciates this, and has the discretion to waive a financial penalty. The penalty cannot be waived if the violation involved willful neglect of Privacy, Security and Breach Notification Rules.

Each category of violation carries a separate HIPAA penalty. It is up to the discretion of the OCR to determine a financial penalty within the appropriate range. The OCR considers a number of factors when determining penalties, such as the length of time a violation was allowed to persist, the number of people affected and the nature of the data exposed. The financial penalties are organized as follows [23]:

Category 1: Minimum fine of $100 per violation up to $50,000
Category 2: Minimum fine of $1,000 per violation up to $50,000
Category 3: Minimum fine of $10,000 per violation up to $50,000
Category 4: Minimum fine of $50,000 per violation

The financial component of patient privacy violations risks may be computed in terms of the financial penalties as documented in the patient privacy and HIPAA literature. The non-financial component is concerned with all other losses that are not financial. This latter component includes, for example, social, ethical/legal, and operational factors related to the enforcement of the privacy assurance policy [23].

Among the nonfinancial penalties, a HIPAA violation can also result in criminal charges being filed against the individual(s) responsible for a breach of protected health information (PHI). Those criminal penalties for HIPAA violations may be of three tiers: Tier 1: Reasonable cause or no knowledge of violation – Up to 1 year in jail, for no knowledge of the violation; Tier 2: Up to 5 years in jail for obtaining PHI under false pretenses; and Tier 3: Up to 10 years in jail for obtaining PHI for personal gain or with malicious intent [23].

This patient privacy violation risk is then computed in terms of the probability of falling in one of the violation categories described above. If the probability distribution is known then we can write tthis risk as the weighted average of resulting losses. For example, we can compute this risk as $p_1L(v_1) + p_2L(v_2) + p_3L(v_3) + p_4L(v_4)$ where v1, v2, v3, and v4 are signals indicating violations of categories 1, 2, 3, and 4 respectively, and L is a loss function.

Unfortunately, such a probability distribution cannot be know given the enormous amount ambiguity linked to the distributed players in the telemedicine environment and the uncertainty associated with the behaviors of various agents handling patients records and electronic interactions with them throughout the distributed environment. Given this type of uncertainty, we later in this paper, model this uncertainty problem using Dempster and Shafer theory that is more suitable to evidence management.

This type of real-time auditing systems often involves combining multiple sources of information which is, despite the profusion of statistical research, still a major and difficult task in the management of uncertainty. But full assurance that privacy is not violated is really impossible to maintain in a well-spread telemedicine environment. Health providers, who may know all possible threats, all possible vulnerabilities, and all available responses, still cannot make an accurate projection of all these factors on their e-health environment, without thorough and costly testing activities. Privacy officers can only develop belief models about the type of violations threatening the e-health system. It is impossible therefore to develop the dual belief model on the non-occurrence of any type of privacy violation, which expresses the amount of ignorance involved in the health providers' evidence structure.

Under these conditions, Dempster and Shafer's theory should apply. We will however assume that we can embed indicators in the distributed telemedicine environment that work independently, which is a very reasonable assumption that can be easily achieved by configuring the e-health reporting system in this manner. In this way, we can then prevent the computing complexity imposed by incidence calculus needed to combine evidence generated by dependent sources.

This article discusses the design of a privacy violation detection system equipped with an incident response system (pvdrs). An experimental framework is given in Figure 1.Before we further proceed, let us introduce some notations. Let Ω be our frame of discernment for our indicators' outputs. Also let B be a Boolean algebra of subsets of Ω. The degree of belief held by an indicator i at time t that the actual state ω0 belongs to the set A of states is equal to x, where A is a subset of the frame of discernment Ω and A Ɛ B is:

$\mathrm{Bel}\{\Omega, B, i, t\}[e(i, t)]\ (\omega 0\ Ɛ\ A) = x.$

The belief is based on the evidential corpus e(i, t) held by i at t, where e(i, t) represents all what the indicator i knows at t. Even though this notation is general and allows for a dynamic system, this study will be limited to one instantiation of the indicators' reporting system. The pvdrs generator is hence memoryless, for it does not allow for combining past data with the current indicators' reports. This is not in any way meant to be a statefull inspection system because we do not include the extraction and propagation processes, and limit ourselves to the combination of evidence alone.

We will soon omit some of the subscripts to ease our notation style. Most often, B is actually the Boolean algebra 2^{Ω}, the power set of Ω. When B is not explicitly stated, it means that Bel is defined on 2^{Ω}. Also 'ω0 Ɛ A' is often denoted as simply 'A'. When the missing elements are clearly defined from the context, { Ω , B, i, t} then other parameters will be left out as needed. So $\mathrm{Bel}_{\{\Omega\}}[E]$ (A) will sometimes be simply denoted as Bel(A).

The pvdrs generator's design, depicted in Figure 1, consists mainly of three core components: a fuser F, a classifier C, and an incident response module R. The pvdrs is hence equipped with a fuser F which receives all indicators' messages and processes them to produce a fused message.

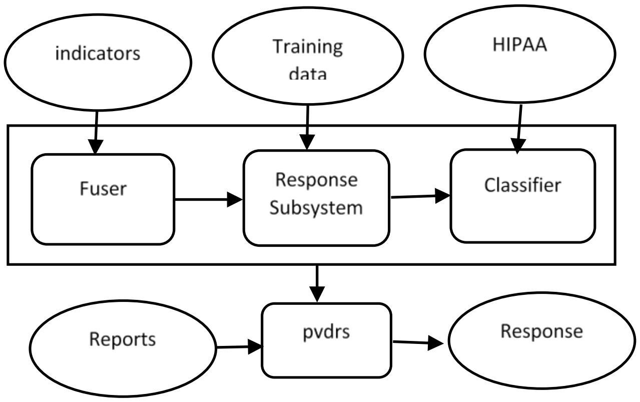


Figure 1:- pvdrs design

Most specifications of the pvdrs generator, are defined in the privacy policy in HIPAA, for privacy violation patterns and privacy controls [17, 18]. All specifications for additional technical requirements should be approved by the health providers before they are added to the design of pvdrs generator.

The fuser:-

The fuser accepts indicators' messages (no extraction or propagation processes are implied, as mentioned earlier), combines them, and produces a fused message that the classifier processes to predict the privacy assurance policy violation type for which the responder produces a set of privacy assurance controls. General design specifications may be discussed in terms of indicators configurations, the fusion process, and the output sent to the classifier. Constraints imposed by indicators configurations and constraints imposed by the classifier's input requirements should be taken into considerations. A fuzzy classifier, for example, requires that the fuser's output be expressed in terms of fuzzy subsets. A possibilistic classifier requires that the fuser' s output expressed in terms of possibilities. Traveling from one computing method to another is a central element of the fuser's design specifications.

This article will however adopt a belief tree classifier. The fuser's output stream should, in this case, be written using a belief structure expressed by its basic belief assignments. That is, the total belief fully committed to a subset E in 2^{Ω}, where Ω is the indicators' frame of discernment, is expressed using bel(E) and pl(E) defining the credibility and the plausibility of E, respectively.

$m: 2\ \Omega \rightarrow [0,1]$
$Bel(E) =: \sum_{F \leq E} m(F)$
$Pl(E)= \sum_{F \wedge E \neq \phi} m(F)$

This section should discuss the Smets' Transferred Belief Model (TBM) [17, 18] design specifications and computations needed to generate the fuser. Remember, we made the assumption that all indicators are configured to produce Shafer's signals expressed in terms of bba's. Without this assumption, extra computation steps and approximations may be needed to bring the data patterns to a belief structure.

In order to ease interpretability in the fuser's belief structure, we adopt the TBM in two steps: the credal model and the pinistic model [17, 18]. The reader may alternatively opt for Shafer's plausibility functions as a substitute to Smets' pignistic probabilities, as both techniques stem from the same belief structure and both add greater interpretability to the TBM.

The fuser combines indicator' signals and produces the fused Shafer's signal m as a one fused bba. In order to grant better interpretability we suggest the credal model made of the fused belief structure be transformed into a pignistic model. Alternatively, health providers can request Shafer's plausibility functions. The plausibility function is computed as Shafer's belief of the subset minus Shafer's belief of its complementary. At this point, Dempster's rule for combining evidence should apply. The health provider's privacy assurance policy should describe how the pvidrs components are configured.

The credal model:-

The design of the creedal step of the pvidrs generator may be set to fully asserted evidence or discounted evidence. The case of fully asserted evidence does not discount the evidence induced from indicators' messages. This means that the basic belief assignment expressing the uncertainty associated with the indicator's evidence remains fully asserted. That is:

For any E in Ω, the indicator's frame of discernment, we have:

$m: 2\Omega \rightarrow [0,1]$
$m(\Omega)=l;\ \sum E \leq \Omega\ m(E)=1$

Since this indicator's evidence is fully asserted, then Shafer's discount factor equals zero, and the sensor's reliability may be expressed using a belief structure as follows:

m(indicator reliability)=l; m(indicator non-reliability)=0.

In case of one indicator, then the discounted evidence imposes a Shafer's discount factor of 1-δ where δ expresses the indicator's reliability. The reliability belief structure is as follows:

m(indicator reliability)= δ
m(indicator non-reliability)= 1- δ.

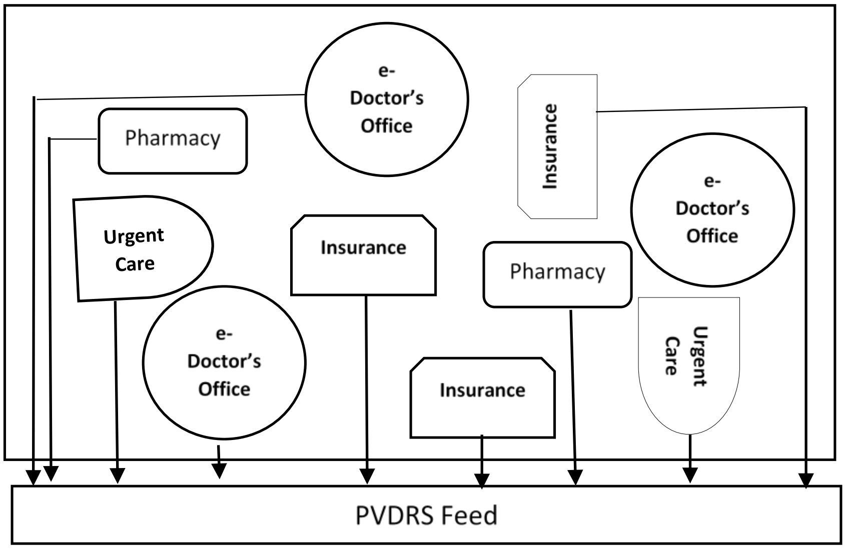
The belief structure is defined as follows:

$m: 2\Omega \rightarrow [0,1]$
$m(\Omega)=l;$
$\sum E \leq \Omega \qquad m(E)=1$

For any E in Ω,
$m_{\delta}(E) = \delta m(E)$, and
$m_{\delta}(\Omega) = (l - \delta) m(\Omega)$

In the general case of N indicators we will have the following:

For any E in Ω,
$m_{\delta}(E) = m_{1,\delta 1}(E) \oplus \ldots \oplus m_{N,\delta N}$
$=[\ \sum_{E1\Lambda \ldots \Lambda EN=E} \prod i=1,N\ \ m_{i,\delta i}(Ei)]/[1-\sum_{E1\ \Lambda\ \ldots\ \Lambda\ EN}=\varnothing \prod i=1,N\ \ m_{i,\delta i}(Ei)]$
$=[\ \sum_{E1\Lambda \ldots \Lambda EN=E} \{(\prod i=1,N\ \ \delta i)\ (\prod i=1,N\ \ mi\ (Ei))\}/[1-\{(\prod i=1,N\ \ \delta i\ )\ (\sum_{E1\ \Lambda\ \ldots\ \Lambda\ EN=\varnothing} \prod i=1,N\ \ mi\ (Ei))\}]$



The illustration in Tables 1 and 2 shows that we received 5 signals from the telemedicine environment on privacy violations. Given that we only allowed 4 types of violations v1, v2, v3, and v4, each signal is expressed by a belief structure on the frame of discernment $\Omega= \{v_1, v_2, v_3, v_4\}$. Table 1 provides the belief structures of the 5 signals received. We then combined the belief structure using Dempster's rule of combination of evidence as shown in Table 2.

Table 1: Belief structure for indicators' reports

	v_1	v_2	v_3	v4	$\{v_2, v_3\}$	Ω	
s_1		x				x	m_1 :(v_2 :.3 ; Ω :.7)
s_2	x					x	m_2 :(v_1 :.2 ; Ω :.8)
s_3			x			x	m_3 :(v_3 :.4 ; Ω :.6)
s_4						x	m_4 :(Ω :.7)
s_5		x	x			x	m_5 :({v_2, v_3}:.2 ; Ω :.8)

Table 2: Fusing the bba's from various sources of privacy violations

Subsets	∅	Ω	v_1	v_2	v_3	v4	$\{v_1, v_2\}$	$\{v_1, v_3\}$	$\{v_2, v_3\}$
Fused m	.0	.34	.09	.17	.27	.0	.0	.0	.09

The pignistic model:-

Even though we herein demonstrate the pignistic model, the interested reader may alternatively choose to compute Shafer's plausibility functions as a substitute to the pignistic probabilities. Smets' pignistic probabilities may be induced from the above belief function as follows: For any V in E:

For any V is Ω,
$P(V) = \sum E \leq \Omega\ m_\delta(E)|V \Lambda E|/|E|$.

We just showed how to use the TBM to travel from the initial specifications defined in the corporate privacy policy to the design of a pvdrs generator's fuser capable of incorporating major indicators while incorporating Shafer's evidence discounts expressing sources' reliability conditions. The final fused message produced by the fuser will be transferred to the pvdrs generator's classifier.

The example in Figure 2 considers a telemedicine environment consisting of some e-doctor's offices, some urgent care centers, some insurance agencies, and some pharmacies. They all part of the patient privacy assurance requirements as enforced in HIPAA and in other corporate privacy assurance policies [17, 18].

We can then compute the pignistic probabilities as in the equation p(V) above. Once these numbers are obtained the risk is then computed as the expected value of losses givens the pignistic probabilities and the losses given the types of violations.

The classifier:-

The corporate privacy policy should impose the design of the privacy violations detection and response system. Some health providers do not allow unsupervised learning because they do not allow simulation techniques including random sampling used in machine learning and in the statistics community. Other health providers may not approve supervised learning when they are not sure of the quality of the training data sets. Anyway, classifiers may be designed to provide supervised learning provided that there are sufficient cases for training and also sufficient cases for testing and for preventing over fitting. The classifier should not violate any privacy rules established in HIPAA of the corporate privacy assurance policies [17, 18].

Diverse classification models have been proposed in the literature [14, 15]. Decision trees are attractive for their intuitive representation, easy assimilation, their cost-effectiveness [12], and their precision superiority [8, 11]. Within the area of decision tree classification, there are many algorithms to construct decision trees; you may just choose one of your choices to incorporate in the pvdsr generator.

The responder:-

The responder, as shown in Figure 5, fits the specifications of a Mamdani's fuzzy rule base system (MFRBS), for the fuser, and produces a basic belief assignment that can be easily transformed into a fuzzy subset [5]. In fact, you also can skip the computation of pignistic probabilities and of Shafer's plausibility functions, as the privacy officer may not need to interpret the classifier output but instead wait for the recommendations generated by the responder.

In order to produce a highly descriptive model of the telemedicine environment, and achieve easy interpretability of the responder output, a MFRBS will produce rules defining system behavior as a conjunction of linguistic terms and their labels. This will allow for a more global and an easier interpretation of system statements detailed in the corporate privacy policy.

The literature contains a decent amount of studies on FRBSs [1, 2, 3, 4, 6, 10]. The closest to what we are doing here will be Duns [1, 6] and Chiu [2] who applied fuzzy clustering techniques that derive partitions of the input and output fuzzy variables needed to produce fuzzy rules. Their learning process generates fuzzy rules using cluster centers. Herrera et al. [10] and Herrera [3, 4] have adopted genetic learning for approximative FRBS where the learning process uses an optimization problem to search for the best individual rules that optimize a prescribed objective function. In our case, the best responses are the ones that minimize the patient privacy assurance policy violation risk, as defined very early in this article. The best responses will then be risk-driven conditional actions in terms of the fuzzy rule produced by the system.

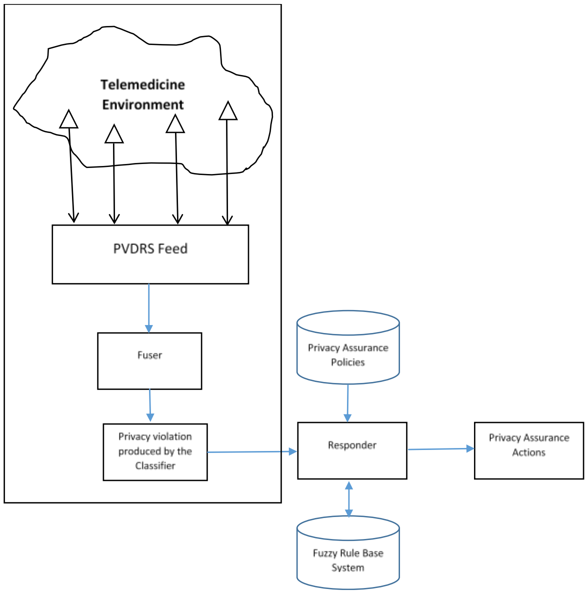

Telemedicine Environment
PVDRS Feed
Fuser
Privacy violation produced by the Classifier
Privacy Assurance Policies
Responder
Privacy Assurance Actions
Fuzzy Rule Base System

Figure 3:- Response subsystem

Even though privacy assurance solutions can take different approaches, they all aim at identifying events of unauthorized access to patient information and violation of the corporate privacy assurance policies. The bottom line should be the detection of all violations of the corporate privacy policy. In fact, for the pvdrs rule base, there is not really any difference between the requirements of privacy assurances rules, as long as the privacy assurance rule is fully specified. Once the privacy violation is detected, it is classified, and the pvdrs starts searching for the most appropriate privacy assurance actions to undertake. A privacy assurance control may consist of any action, device, procedure, technique, or other measure that reduces the vulnerability of a component of the telemedicine environment.

Conclusion:-

This article discussed the design of a patient privacy detection and response system generator. The design of the pvdrs generator included an evidence fuser, a classifier, and an incident responder. This system was designed to accept three main input streams: the firm's privacy assurance policy, its current risk profile, and training data sets, and to produce an incident response in terms of managerial, technical, and operational privacy assurance controls that security health providers feasibly adopt to improve the health provider's risk position as indicated in the corporate polices. This article did not present a prototype of the pvdrs generator but demonstrated sufficient details about the use of the Transferred Belief Model in both the fuser and the classifier supported by Smets' pignistic probabilities.

A possible extension of this article is the intelligent development of a pvdrs that integrates both privacy assurance policies and the corporate security policy since security breaches of any kind can put the patient privacy in real danger and also the pvdrs itself.

References:-

1. Bezdek, J.C. (1981).Pattern Recognition WithFuzz.V Objective Function Algorithms, Plenum Press.
2. Chiu, S.L. (1994) Fuzzy Model Identification Based On Cluster Estimation, Journal of Intelligent and Fuzzy Systems 2:267-278.
3. Cordon, O. and F. Herrera, (1997) A Three-Stage Evolutionary Process For Learning Descriptive And Approximate Fuzzy Logic Controller Knowledge Bases From Examples, Int. Journal of Approximate Reasoning 17(4): 369-407.
4. Cordon, O. and F. Herrera, (1999) HybridisingGenetic Algorithms With Sharing Scheme And Evolution Strategies For Designing Approximate Fuzzy Rule-Based Systems, Fuzzy Sets and Systems.
5. 11
6. Cordon, O., Herrera, F., Magdalena, L. and P. Villar. (2001) A Genetic Leaming Process for the Scaling Factors, Granularity and Contexts of the Fuzzy Rule-Based System Data Base. Information Science 136 85-107.
7. Dunn, J.C. (1974) A fuzzy relative of the ISODATA Process And Its Use In Detecting Compact Well Separated Clusters, Journal Cybernetics 3:3, 32-57.
8. Goozner, M..2015 National Action Needed to AdvanceTelemedicine. Modern Healthcare.
9. Hand. D.J. (1997) Construction and Assessment ofClassifi-cation Rules, Wiley Press.
10. Herrera, F., M. Lozano, M. and J.L. Verdegay, (1995) Generating Fuzzy Rules From Examples using Genetic Algorithms, Fuzzy Logic and Soft Computing (B. Bouchon-Meunier, B., Yager, R.R., and LA Zadeh, Eds.), World Scientific, 1995.
11. Herrera, F. M. Lozano, M. and J.L. Verdegay, (1998) A Learning Process For Fuzzy Control Rules Using Genetic Algorithms, Fuzzy Sets and Systems 100 143-158.
12. Lim, T.S. W.-Y. Loh, W.Y. and Y.-S. Shih. (1997) An Empirical Comparison Of Decision Trees And Other Classification Methods. TR 979, Department of Statistics, UW Madison.
13. LohW.Y. and N. Vanichsetakul. (1996) Tree-Structured Classification Via Generalized Disriminant Analysis. Journal of the American Statistical Association, 83:715-728.
14. Mehta, M. R. Agrawal, R. and J. Rissanen. (1996) SLIQ: A Fast Scalable Classifier For Data Mining. In Proc. of EDBT.
    Michie, D. Spiegelhalter, D.J. and C.C. Taylor,(1994) Machine Learning, Neural and Statistical Classification.
15. Smets, P. and R. Kennes, (1994). The Transferable Belief Model. Artificial Intelligence, 66, 191-234.
16. Smets, P. (1998). TheTransferable Belief Model For Quantified Belief Representation. In Gabbay D.M. & P. Smets (Eds.), Handbook of defeasible reasoning and uncertainty management systems, vol. 1 (pp. 267-301). Doordrecht, The Netherlands: Kluwer.
17. Warkentin, M., Johnson, A.C. and Adams, A.C. (2006) 'User interaction with healthcare information systems: Do healthcare professionals want to comply with HIPAA?', Proceedings of the 12th Americas Conference on Information Systems, Acapulco, Mexico, pp.2682–2691.
18. Wen, K.W. and Zhang, Y.J. (2002) 'Research issues on medical information systems facing the implementation of HIPAA', International Journal of Healthcare Technology and Management, Vol. 4, Nos. 1–2, pp.93–105.
19. Weddle M, Kokotailo P. (2005) Confidentiality and Consent In Adolescent Substance Abuse: An Update. Virtual Mentor, American Medical Association Journal of Ethics.
20. Weiss S.M. and C.A. Kulikowski. (1991) Computer Systems that Learn: Classification and Prediction Methods from Statistics, Neural Nets, Machine Learning, and Expert Systems.
21. Wentland EJ. (1993) Survey responses: An evaluation of theirvalidity, AcademicPress, San Diego, CA.
22. Westin A. Science, (1966) Privacy and Freedom, Columbia Law Review;66(7):1205–1253.
23. What Are The Penalties For Hipaa Violations?, HIPAA Requirements, HIPAA Journal, http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.
24. Whiddett R, Hunter I, Engelbrecht J, and J.Handy, (2006) Patients' Attitudes Towards Sharing TheirHealth Information. International Journal of Medical Informatics;75(7):530–541.
25. Woolley M, and S.M. Propst(2005) Public Attitudes And Perceptions About HealthRelatedResearch. JAMA. 2005;294:1380–1384
26. Xu, R. (2014) "The Doctor Will See You Onscreen." The NewYorker. March 10, 2014.