Data Mining based Soft Computing Skills towards Prevention of Cyber Crimes on the Web

[1]Sayyada Sara Banu , [2]Dr.Perumal Uma , [3]Mohammed Waseem Ashfaque ,
[4]Quadri N.Naveed, [5]Quadri S.S Ali Ahmed.

[1] . College of computer science and information system,J azan university,Saudi Arabia
email:- sayyada.sara@gmail.com
[2].College of computer science and information system, Jazan university,Saudi Arabia.
email: prmluma@gmail.com
[3]. Department of Computer Science & IT, College of Management and Computer Technology, Aurangabad, India
email: waseem2000in@gmail.com
[4]Department of Computer Science & IT, King Khalid University, Abha,Saudi Arabia
email:- navqua@gmail.com
[5].Department of Computer Science & IT, College of Management and Computer Technology, Aurangabad, India.
email:- aliahmedquadri@yahoo.co.in

Abstract: Internet is the vital resource of Information technology through which the source of Information can be transfer from one machine to anther machine ,information can be receive from one machine and it can be processed and send to another one in this sense it become a great hub distribution of information resources. Now that information can be utilized for educational, for commercial, for personal, by means of that has a various shapes and structure of its necessity. And this results into the traffic over the Internet. Therefore a robust and ideal methodology need to produced for tracing and detecting terror based activities by using traffic content as the auditing of information is being shown These methodologies read and detect the Abnormal and typical behavior of terrorist by using and applying various algorithms of Data Mining and the textual content of terror related web sites and finally profile is give and used by the system to take a real action in the form of tracing and detecting of such suspected person which are evolves in terror activities. As a modern term of computer science its combines with neural networks, artificial intelligence and advanced information technology in the terms of Web or Internet, no doubt Data mining also has a wide scope and verities of large range of web based Applications, with reference to the soft computing Technology which combines with Fuzzy Logic, Artificial Intelligence, Neural networks, and genetic Algorithm in the proposed computing. In this paper the various approaches of soft computing is discussed.

Keywords: *Data Mining, User Modeling; Terrorist Trend Detection, Anomaly Detection, Activity Monitoring, Fuzzy Logic, Genetic Algorithm, Cyber crime.*

*****

1. Introduction

Terrorist cells are using the Internet infrastructure to exchange information and recruit new members and supporters [1]. For example, high-speed Internet connections were used intensively by members of the infamous ‘Hamburg Cell’ that was largely responsible for the preparation of the September 11 attacks against the United States, One way to detect terrorist activity on the Web is to eavesdrop on all traffic of Web sites associated with terrorist organizations in order to detect the accessing users based on their IP address. Unfortunately it is difficult to monitor terrorist sites (such as ‘Azzam Publications’ [2]. This is one reason for the major effort made by law enforcement agencies around the world in gathering information from the Web about terror-related activities. It is believed that the detection of terrorists on the Web might prevent further terrorist attacks [3]. The geographical locations of Web servers hosting those sites also change frequently in order to prevent successful eavesdropping. To overcome this problem, law enforcement agencies are trying to detect terrorists by monitoring all ISPs traffic [4], though privacy issues raised still prevent relevant laws from being enforced. Data mining has useful business applications such as finding useful hidden information from databases, predicting future trends, and making good business decisions [5,6,7]. Soft computing techniques such as fuzzy logic, genetic algorithm and neural networks are useful in data mining [8,9]. Web intelligence, a term that was coined in the late 1999’s, concerns about research and application of machine learning and information technology with a specific focus on the Web platforms. Typical Web Intelligence applications include but not limited to online text classification, Web document clustering, Web recommender for e-commerce, Web usage profiling and similar knowledge discovery tasks are drawing attention from communities of global researchers. The data, in the context of data that are originated from the Web, called Web Intelligence data pose certain challenges to knowledge discovery tasks and Web mining. WI (Web Intelligence) is studied carefully from different aspects [10]. WI exploits Artificial Intelligence (AI) and advanced Information Technology (IT) on the Web and Internet [10]. Computational Web Intelligence (CWI) is a hybrid technology of Computational Intelligence (CI) and Web

Technology (WT) dedicating to increasing quality of intelligence of e-Business applications on the Internet and wireless networks [11]. CWI uses Computational Intelligence (CI) and Web Technology (WT) to make intelligent e- Business applications on the Internet and wireless networks. Support Vector Machine (SVM) proposed by Vapnik is a newly developed technique which based on statistical learning theory [12,13], it adopts Structure Risk Minimization principle which avoids local minimum and effective solves the over learning and assures good generalization ability and better classify accuracy. Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact. Compared to traditional binary sets (where variables may take on true or false values) fuzzy logic variables may have a truth value that ranges in degree between 0 and 1. A genetic algorithm (GA) is a search heuristic that mimics the process of natural selection. This heuristic (also sometimes called a met heuristic) is routinely used to generate useful solutions to optimization and search problems. Artificial neural systems, or neural networks, are physical cellular systems which can acquire, store, and utilize experiential knowledge.

1.1 Various Approaches of Data mining techniques

- **Artificial neural networks**

Non-linear predictive models that learn through training and resemble biological neural networks in structure. Warren McCulloch and Walter Pitts [14] (1943) created a computational model for neural networks based on mathematics and algorithms. They called this model threshold logic. Neural network is used in data mining for pattern recognition.

- **Role of Decision trees**

Tree-shaped structures that represent sets of decisions. These decisions generate rules for the classification of a dataset. Although decision trees have been in development and use for over 60 years (one of the earliest uses of decision trees was in the study of television broadcasting by Belson in 1956).Decision tree is used in data mining for the classification[15].

- A decision tree consists of 3 types of nodes:

1.1.1 Role of Decision nodes

Commonly represented by squares.

1.1.2 Role of End nodes

Represented by triangles.

- Rule induction - The extraction of useful if-the rules from data based on statistical significance. The rule induction algorithm was first used by Hunt in his CLS system in 1962.

- **Genetic algorithms**

Optimization techniques based on the concepts of genetic combination, mutation, and natural selection. It was introduced by John Holland in 1975.In 1989, Excel is, Inc. released Evolver, the world's first commercial GA product for desktop computers.[15]

- **Nearest neighbor**

A classification technique that classifies each record based on the records most similar to it in an historical database. Donald Knuth in vol. 3 of The Art of Computer Programming (1973) called it the post office problem, referring to an application of assigning to a residence the nearest post office. Nearest is used in data mining for clustering. This paper is organized as follows. Section II describes about data mining, soft computing and web intelligence. Section

1.1.3 Shows various applications of WI. Data mining based soft computing approaches for WI discussed in Section IV. Finally, concluding in Section V.

1.2 World Wide Web

(Abbreviated as WWW or W3, commonly known as the web) is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks. On March 12, 1989, Tim Berners-Lee, a British computer scientist and former CERN(European Organization for Nuclear Research) employee, wrote a proposal for what would eventually become the World Wide Web.[16][17].

1.3 Intrusion Detection System

An Intrusion Detection System (IDS) constantly monitors actions in a certain environment and decides whether they are part of a possible hostile attack or a legitimate use of the environment [18][19]. The environment may be a computer, several computers connected in a network or the network itself. The IDS analyzes various kinds of information about actions emanating from the environment and evaluates the probability that they are symptoms of intrusions. Such information includes, for example, configuration information about the current state of the system, audit information describing the events that occur in the system (e.g., event log in Windows XP), or network traffic.

1.4 Vector-Space Model

One major issue in this research is the representation of textual content of Web pages. More specifically, there is a need to represent the content of terror-related pages as against the content of a currently accessed page in order to efficiently compute the similarity between them. This study will use the vector-space model commonly used in Information Retrieval applications [20] for representing terrorists' interests and each accessed Web page. In the vector-space model, a document d is represented by an n-dimensional vector d = (v1,v2,…..,vn), where vi represents the frequency-based weight of term i in document d. The similarity between two documents represented as vectors may be computed by using one of the known vector distance measuring methods such as Euclidian distance or Cosine [21]. In this study each Web page in considered as a document and is represented as a vector. The terrorists' interests are represented by several vectors where each vector relates to a different topic of interest. The cosine similarity measure is commonly used to estimate the similarity between an accessed Web page and a given set of terrorists' topics of interests.

2. Literature Review

2.1 Definition of Data Mining

The phenomenon of extracting required and needed data (knowledge), like patterns, association, changes, and significant structures a data base which is in the large form

2.2 Areas and fields

- Emerging data mining applications in bioinformatics, engineering, and medicine
- Image analysis [22].
- Noise detection and cleansing in large, distributed data environments
- Ontology-based information extraction and knowledge discovery
- Pattern discovery in data streams
- Pattern matching and mining

2.3 Approaches of Clustering Techniques

Cluster analysis is the process of partitioning data objects (records, documents, etc.) into meaningful groups or clusters so that objects within a cluster have similar characteristics but are dissimilar to objects in other clusters [23], Clustering can be viewed as unsupervised classification of unlabelled patterns (observations, data items or feature vectors), since no pre-defined category labels are associated with the objects in the training set. Clustering results in a compact representation of large data sets (e.g, collections of visited Web pages) by a small number of cluster centroids. Applications of clustering include data mining, document retrieval, image segmentation, and pattern classification [24]. Thus, clustering of Web documents viewed by Internet users can reveal collections of documents belonging to the same topic. As shown by [25] clustering can also be used for anomaly detection: normality of a new object can be evaluated by its distance from the most similar cluster under the assumption that all clusters are based on ‘normal’ data only. In this study clustering of Web pages retrieved from terrorist-related sites is used to find collections of Web pages belonging to the same terrorists’ topic of interest. For each collection a centroid is computed and represented by the vector space model.

2.4 Approaches of Soft Computing

Soft computing is an emerging approach to computing which parallels remarkable ability of human mind to reason and learn in an environment of uncertainty and imprecision[26].Soft Computing consists of several computing paradigms like Neural Networks, Fuzzy Logic, and Genetic algorithms. Soft Computing uses hybridization of these techniques. A hybrid technique would inherit all the advantages of constituent techniques. Thus the components of Soft Computing are Complementary, not competitive, offering their own advantages and techniques to partnerships to allow solutions to otherwise unsolvable problems [27].

2.5 Various Methods of Soft Computing

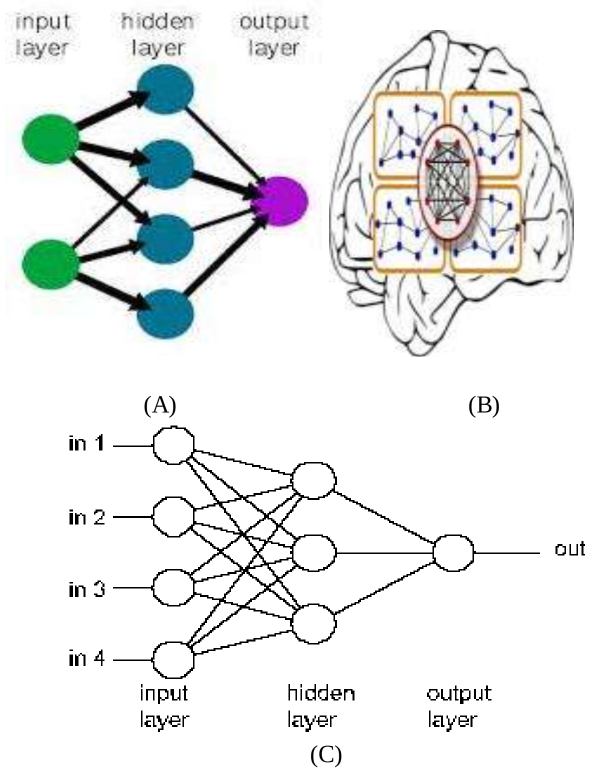
2.5.1 Fuzzy Logic

As one of the principal constituents of soft computing, fuzzy logic is playing a key role in what might be called high MIQ (machine intelligence quotient) systems. Two concepts within fuzzy logic play a central role in its applications. The first is a linguistic variable; that is, a variable whose values are words or sentences in a natural or synthetic language [28]. The other is a fuzzy if-then rule, in which the antecedent and consequents are propositions containing linguistic variables [28]. While variables in mathematics usually take numerical values, in fuzzy logic applications, the non-numeric linguistic variables are often used to facilitate the expression of rules and facts [29]. For example, a simple temperature regulator that uses a fan might look like this:

- IF temperature IS very cold THEN stop fan
- IF temperature IS cold THEN turn down fan

2.5.2 Neural networks

Based on the computational simplicity Artificial Neural Network (ANN) based classifier is used. In this proposed system, a feed forward multilayer network is used. Back propagation (BPN) Algorithm is used for training. There must be input layer, at least one hidden layer and output layer. The hidden and output layer nodes adjust the weights value depending on the error in classification. In BPN the signal flow will be in feed forward direction, but the error is back propagated and weights are up dated to reduce error. The modification of the weights is according to the gradient of the error curve, which points in the direction to the local minimum. Thus making it much reliable in prediction as well as classifying tasks[30].



(A) (B)

(C)

Fig:1 Basic Structure of Neural Network(A),(B),(C)

2.6 Content- based detection of terror-related activity

2.6.1 Detection Environment system

This study suggests a new type of knowledge-based detection methodology that uses the content of Web pages browsed by terrorists and their supporters as an input to a detection process. In this study, refers only to the textual content of Web pages, excluding images, music, video clips, and other complex data types. It is assumed that terror-related content usually viewed by terrorists and their supporters can be used as training data for a learning process to obtain a ‘Typical-Terrorist-Behavior’. This typical behavior will be used to detect further terrorists and their supporters. A ‘Terrorist- Typical-Behavior’ is defined as an access to information relevant to terrorists and their supporters. A general description of a system based on the suggested methodology is presented in Figure 1. Each user under surveillance is identified as a ‘user's computer’ having a unique IP address rather than by his or her name. In the case of a real-time alarm, the detected IP can be used to locate the computer and hopefully the suspected terrorist who may still be logged on to the same computer[30][31].

3. Proposed Methodology

3.1 Study and Background of Cyber criminal Behavior

The learning Cyber criminal-Behavior is one of the part of methodology defines and represents the typical behavior of cyber criminal users based on the content of their Web activities. It is assumed that it is possible to collect Web pages from criminals -related sites. The content of the collected pages is the input to the Vector Generator module that converts the pages into vectors of weighted terms (each page is converted to one vector). The vectors are stored for future processing in the Vector of Cyber criminals Transactions DB. The Clustering module accesses the collected vectors and performs unsupervised clustering resulting in n clusters representing the typical topics viewed by cyber criminal users. For each cluster, the Cyber criminal Represent or module computes the centroid vector (denoted by Cvi) which represents a topic typically accessed by cyber criminals. As a result, a set of centroid vectors represent a set of cyber criminals’ interests referred to as the ‘Typical-Cyber criminal-Behavior’. The Typical-Cyber criminal-Behavior is based on a set of Web pages that were downloaded from cyber criminal related sites and is the main input of the detection algorithm. In order to make the detection algorithm more accurate, the process of generating the Typical-Cyber criminal-Behavior has to be repeated periodically due to changes in the content of cyber criminal related site. Typical-Cyber criminal-Behavior depends on the number of clusters. When the number of clusters is higher, the Typical-Cyber criminal-Behavior includes more topics of interest by cyber criminals where each topic is based on fewer pages. It is hard to hypothesize what the optimal number of clusters is. In the case study presented in the next section detection performance for two settings of the number of clusters are presented with the following diagram of Algorithm

STEP1: Acquisition of Criminals related web pages
STEP2: Vector generation
SETP3: Vector data of Criminals transaction DB
STEP4: Applying cluster techniques
STEP5: Cluster vector (1)………. Cluster vector (n)
STEP6: Criminals representation
STEP7: Collecting Criminal behavior

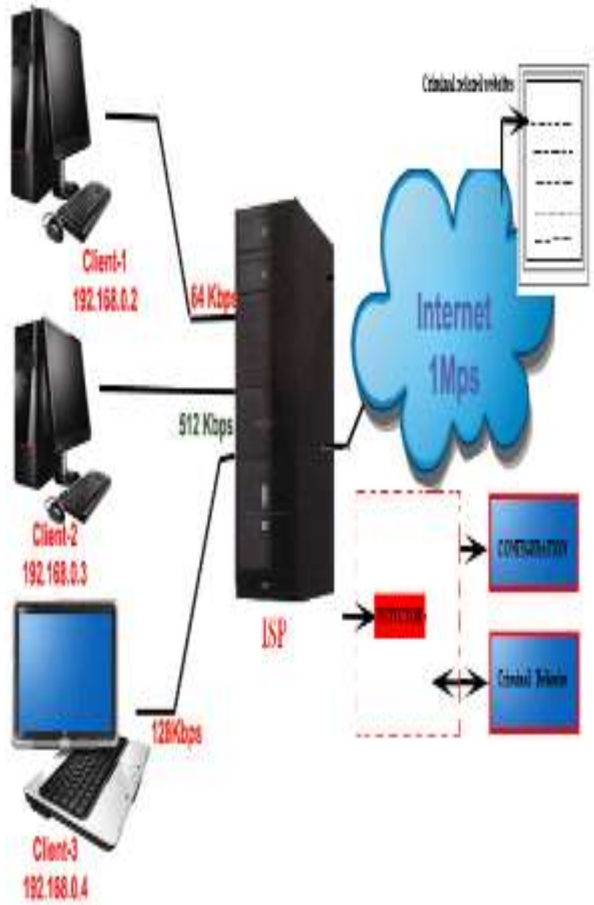


Fig:2 Detection Architecture of Cyber criminal Behavior

3.2 Typical Criminal Behavior Detection

In the Monitoring module the Vector-Generator converts the content of each page accessed by a user into a vector representation (referred to as the ‘access vector’). The Detector uses the access vector and the criminal Behavior and tries to determine whether the access vector belongs to criminal groups. This is done by computing similarity between the access vector and all centroid vectors of the criminal Behavior. The cosine measure is used to compute the similarity. The detector issues an alarm when the similarity between the access vector and the nearest centroid is higher than the predefined threshold denoted by following expression Xr:

$$Max\left(\frac{\sum_{i=1}^{p}(xCv_{n}\text{-}xBv_{1})}{\sqrt{\sum_{i=1}^{p}xCv^{2}{}_{n}\text{-}\sum_{i=1}^{p}xBv^{2}{}_{1}}}\cdots\frac{\sum_{i=1}^{p}(xCv_{p1}\text{-}xBv_{1})}{\sqrt{\sum_{i=1}^{p}xCv^{2}{}_{p}\text{-}\sum_{i=1}^{p}xBv^{2}{}_{1}}}\right)>Xr$$

3.2.1. Terms used in the expression:

i Cv is the ith centroid vector, *Bv* - the access vector, *i*1 *xCv* - the ith term in the vector *i Cv* , *i xBv* - the ith term in the vector *Bv* , and p - the number of unique terms in each vector. The threshold parameter Xr controls the sensitivity of the detection. Higher value of Xr will decrease the sensitivity of the detection process, decrease the number of alarms, increase the accuracy and decrease the number of false alarms. Lower value of Xr will increase the detection process sensitivity, increase the number of alarms and false alarms and decrease the accuracy. The optimal value of Xr depends on the preferences of the system user. In the next section, the feasibility of the new methodology is explored using a case study

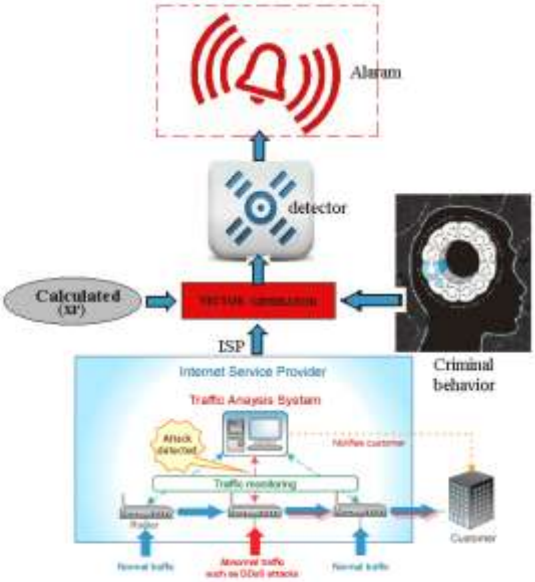


Fig:3 Detection of Cyber criminal Module

3.3 Experimental Approach

An initial evaluation of the proposed knowledge-based detection methodology is conducted through a prototype system. The experimental environment included a small network of ten computers, each computer having a constant IP address and a proxy server through which all the computers accessed the Web. In the experiment, the proxy server represented an ISP. Eight students in information systems engineering were instructed to access Web sites related to general topics and generated about 800 transactions. Several other users were requested to access Criminals related information (mainly the 'Azzam Publications' sites visited by one of the September 11 criminals) and generated about 214 transactions. In this experiment, the users accessed only pages in English, though the methodology is readily applicable to other languages as well. The Vector Generator, Clustering and Detector modules described above were implemented and installed inside the server. Vcluster program from the Cluto Clustering Tool is used to implement the clustering module where the clustering algorithm used was 'k-way' and the similarity between the objects computed using the cosine measure The 'k-way' clustering algorithm is a variation of the popular K-Means clustering algorithm. One problem with these algorithms is that it is hard to find the optimal k (number of clusters) that will achieve the best clustering performance. The experiments were done with different k's and compared results.

3.4 Measurements

- **Detection Rate(DR)**

the percentage of criminals pages receiving a rating above the threshold (referred to as Xr in the model). In the experiments, Criminals' pages will be obtained from the users simulating criminals

- **Non-detection Rate (NDR)**

the percentage of regular Internet access pages that the system incorrectly determined as related to criminals activities, i.e., the percentage of non-criminals pages receiving a rating above threshold and suspected falsely as criminals.

- **Measurement Accuracy**

percentage of alarms related to criminals behavior out of the total number of alarms.

Table 1: Result and Measurements for 10 clusters

DR	NDR	Threshold	Accuracy Of Measurements
0.1	0.025	0	0.05
0.225	0.923	0.05	0.945
0.324	0.456	0.1	0.889
0.567	0.874	0.12	0.763
0.564	0.763	0.13	0.824
0.723	0.678	0.14	0.762
0.132	0.638	0.15	0.627
0.342	0.789	0.16	0.888
0.512	0.982	0.17	0.873
0.321	0.881	0.18	0.998
0.381	0.872	0.19	0.891
0.120	0.822	0.2	0.907

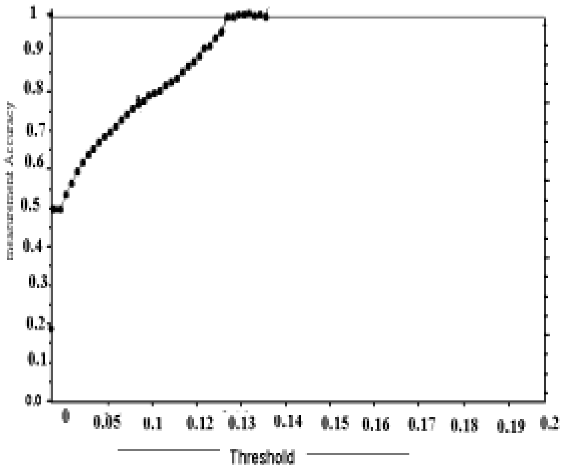


Fig:4 Measurements of Accuracy of threshold value

4. Conclusion

This paper represents the various data miming based approaches and skills in terms of soft computing which is used to prevent and attack of Cyber crimes on the web. The outcome of the results and the methodology of the study directs towards robust detection and prevention skills against the cyber crimes on the web.

References

[1]. Lemos, R. (2002) What are the real risks of cyberterrorism?, ZDNet, URL: http://zdnet.com.com/2100-1105-955293.html

[2]. Corbin, J. (2002) Al-Qaeda: In Search of the Terror Network that Threatens the World, Thunder's Mouth Press / Nation Books, New York

[3]. Kelley, J. (2002) Terror Groups behind Web encryption, USA Today, URL: http://www.apfn.org/apfn/WTC_why.htm

[4]. Ingram, M. (2001) Internet privacy threatened following terrorist attacks on US, URL: http://www.wsws.org/articles/2001/sep2001/isps24.shtml

[5]. K. Cios, W. Pedrycz, and R. Swiniarski, Data Miming methodr for Knowledge Discovery, Kluwer AcademicPublishers, 1998.

[6]. K. Thearling, “Increasing customer value by integrating Data Mining and Campaign Management SoAware,” Direct Marketing Magazine, February 1999.

[7]. C. Westpbal and T. Blaxton, Data Mining Solulions -Methods and Tools for Solving Real- World Problems,John Wiley \& Sons, 1998.E. Gelenbe, Y. Feng, K.R.R. Krishnan, Neural Network Methods for Volumetric Magnetic Resonance Imaging of the Human Skin, Proc.IEEE, 84, 1996: pp.1488–1496.

[8]. Meijuan Gao, Jingwen Tian, and Shiru Zhou ,”Research of Web Classification Mining Based on Classify Support Vector Machine” 2009 ISECS International Colloquium on Computing, Communication, Control, and Management

[9]. J.Weston and C. Watkins, Support vector machines for multi-class pattern recognition, In Proceeding of the 6th European symposium on Artificial Neural Network (ESANN), 1999

[10]. Y.Y. Yao, Zhong, N., Liu, J. and Ohsuga, S., “Web Intelligence (WO:Research challenges and trends in the new information age”, Proc. Of WI2001, pp. 1-17, Springer, 2001.

[11]. Y.-Q. Zhang and T.Y. Lin, “Computational Web Intelligence (CWI): Synergy of Computational Intelligence and Web Technology,” Proc. of FUZZIEEE2002 of World Congress on Computational Intelligence 2002: Special Session on Computational Web Intelligence, pp.1104-1107, May 2002.

[12]. V.Vapnik, Statistical Learning Theory, Wiley, 1998.

[13]. J.Weston and C. Watkins, Support vector machines for multi-class pattern recognition, In Proceeding of the 6th European symposium on Artificial Neural Network (ESANN), 1999.

[14]. McCulloch, Warren; Walter Pitts (1943). "A Logical Calculus of Ideas Immanent in Nervous Activity". Bulletin of Mathematical Biophysics 5 (4): 115–133. doi:10.1007/BF02478259.

[15]. Markoff, John (29 August 1990). "What's the Best Answer? It's Survival of the Fittest". New York Times. Retrieve 9 August 2009.

[16]. "World Wide Web Consortium". "The World Wide Web Consortium (W3C)..."

[17]. Zhong, Ning; Liu Yao, Jiming; Yao, Y.Y.; Ohsuga, S. (2000), "Web Intelligence (WI)", Web Intelligence, Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International, p. 469, doi:10.1109/CMPSAC.2000.884768, ISBN 0-7695-0792-1.

[18]. Y.Elovici1, A.Kandel2, M.Last1, B.Shapira1, O. Zaafrany1,” Using Data Mining Techniques for Detecting Terror-Related Activities on the Web”

[19]. Debar, H., Dacier, H., Dacier, M., Wespi, A. (1999) Towards a taxonomy of intrusion-detection systems, *Computer Networks*, **31**, pp. 805–822

[20]. Salton, G. (1989) *Automatic Text Processing: the Transformation, Analysis, and Retrieval of Information by Computer*, Addison-Wesley, Reading.

[21]. Boger, Z., Kuflik, T., Shoval, P., Shapira, B.(2001) Automatic keyword identification by artificial neural networks compared to manual identification by users of filtering systems, Information Processing and Management, 37:187-198.

[22]. Richards, K. (1999) Network Based Intrusion Detection: A Review of Technologies, Computers & Security, 18:671-682.

[23]. Han, J., Kamber, M. (2001) Data Mining: Concepts and Techniques, Morgan Kaufmann

[24]. Jain, A.K., Murty, M.N., Flynn, P.J. (1999) Data Clustering: A Review, ACM Computing Surveys, 31, 3:264-323.

[25]. Sequeira, K., Zaki, M. (2002) ADMIT: Anomaly-based Data Mining for Intrusions, Proceedings of SIGKDD 02, pp. 386-395, ACM.

[26]. J. S. R. Jang, C. T. Sun and E. Mizutani, Neuro-Fuzzy and Soft Computing :A Computational Approach to Learning & Machine Intelligence, Prentice Hall, Saddle River, New Jersey, 1997.

[27]. S.N. Sivanandam, S.N. Deepa, Principles of Soft Computing, Wiley India (P) Ltd, 2007.

[28]. L.A. Zadeh, “Outline of a New Approach to the Analysis of Complex Systems and Dccision Processes,” IEEE Trans. Systems, Man and Cybmzetics, pp. 28-44.

[29]. Zadeh, L. A. et al. 1996 Fuzzy Sets, Fuzzy Logic, Fuzzy Systems, World Scientific Press, ISBN 981-02-2421-4.

[30]. Zhong, Ning; Liu Yao, Jiming; Yao, Y.Y.; Ohsuga, S. (2000), "Web Intelligence (WI)", Web Intelligence, Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International, p. 469, doi:10.1109/CMPSAC.2000.884768, ISBN 0-7695-0792-1.

[31] 1Mohammed Waseem Ashfaque;2Abdul Samad Shaikh; 3Sumegh Tharewal; 4Sayyada Sara Banu; 5Mohammed Ali Sohail, Challenges of Interactive Multimedia Data Mining in Social and Behavioral Studies for latest Computing &Communication of an Ideal Applications, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VII (Nov – Dec. 2014), PP 21-31