ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Adaptive Neuro Fuzzy Inference System For Modeling of Cybercrime control

Anand Kumar Shrivastav[1], Ekata[2]
[1] Department of Computer Science, Mewar University, Chittorgarh, India
[2] Department of Applied Science, Krishna Institute of Engineering & Technology, Ghaziabad, India
shrivastav.anand@gmail.com

Abstract

The prevention of cyber crime is indispensable because a single attack may break the security of computer and network systems. There are certain factors which are responsible for cybercrime and their careful management may substantially reduce cybercrime incidents. The people's liberty, law enforcement cooperation and vulnerability of ICT infrastructure are three such factors. In this paper, we are contemplating the feasibility of an approach based on Adaptive Neuro Fuzzy Inference System (ANFIS) to probe the relationship of factors that are responsible for cyber crime incidents. The results indicate that our approach may help in planning cybercrime prevention strategy.

Keywords: ANFIS, Back-propagation, Cooperation, Cybercrime, Fuzzy logic, ICT, Liberty, Neural Network, Vulnerability

Introduction

Information Technology revolution has transformed the world into a global community. The technological advancement has brought many pleasant changes in the society. But experience shows that such advancement brings with it some unexpected problems also. While the new technology opens new doors of opportunities for the benefit of society, it also gives chance to law breakers to commit the crime with the help of new techniques. The increasing volume of cyber crimes has been one of the serious issues for society, law enforcement agencies and government. The vulnerability in any ICT infrastructure including databases, networks and application software leads to exploitation, compromise and data theft. The literature survey shows that, there are certain factors, which are directly or indirectly responsible for cybercrime. The vulnerability of ICT infrastructure is one such factor. Apart from vulnerability, harmony of laws, technical coordination and treaties between countries, cooperation between public & private entities are other factors which are responsible for cyber crime incidents and making a system or nation vulnerable. We can collectively term this phenomenon as cooperation. The human being is a force directly or indirectly associated with development and use of technology. It is also an active element of cooperation. But cyber security enhancement efforts may adversely affect the people's liberty, a fundamental right. It is assumed that, by balancing vulnerability, cooperation and liberty, the cyber security can be enhanced and cyber crime incidents can be reduced substantially.

In this study, Adaptive Neuro Fuzzy Inference System has been used to model the relationship between vulnerability, cooperation and liberty and their impact on cyber crime incidents. It is assumed that a neural network can provide a considerable improvement in the cybercrime control strategy, though further development work is needed before this becomes a routine tool. The selection of cases used to train the network is crucial to the quality of its performance and there is scope to improve the system further by incorporating other factors that may influence main factors considered herein.

The rest of the paper is organized as follows. In Section 2, we review the factors responsible for cybercrime incidents. Subsequently, we describe the neuro-fuzzy system for cybercrime incidents. In Section 3, we describe the neurofuzzy system for cybercrime incidents, in section 4, we illustrate the simulated adaptive neurofuzzy system for cybercrime incident and show the experimental results. The conclusion and future works are discussed in Section 5.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Factors responsible for cybercrime incidents

Vulnerability

Vulnerability is a weakness that can be exploited to accomplish something that is not authorized to or intended as legitimate use of a network or system. It is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy [1]. A security vulnerability is a flaw in a product that makes it infeasible – even when using the product properly —to prevent an attacker from usurping privileges on the user's system, regulating its operation, compromising data on it, or assuming un-granted trust [2]. When vulnerability is exploited to compromise the security of systems or information on those systems, the result is a security incident. Vulnerabilities may be caused by engineering or design errors, or faulty implementation. The vulnerability may lead to security breach or violation of system's security policy and attacks on cyber infrastructure, their exploitation, computer crime, cyber warfare, espionage etc. that may occur due to flaw in hardware, system design, procedure, internal control and implementation of security procedures. In order to secure a computer system, it is important to understand the vulnerability in the system that can be exploited to compromise its security and for a complete vulnerability assessment all of them should be considered and analyzed.

Cooperation

Due to design of the Internet, the data transfer processes involve more than one country and many hosting services are offered by abroad based companies. While the criminals, who are proactive, creative, flexible and carry out their illicit activities despite of geographical and jurisdictional boundaries, the law enforcement agencies are constrained by jurisdiction issues. The speed and technical complexity of cyber activities requires prearranged, agreed procedures and responses, including both voluntary and legally mandated cooperation in investigation and responding to threats and attacks. The cooperation may be technical and political between countries; between government and private sectors, and, between law enforcement agencies. There may be extradition treaties. Many efforts have been progressed at international forums such as G8, European Union, Council of Europe, Commonwealth, United Nations, BRICS and OECD etc. The member countries have agreed upon some policies and signed the treaties to tackle cyber crime menace. The Convention on Cybercrime proposed by the Council of Europe of 2001 provided a common legal framework on cybercrime. Some international organizations also contributing significantly in technological and law enforcement front to combat cyber crime. The International Telecommunication Union (ITU) provides technical assistance to Member States on cybercrime and Cyber Security. Interpol is a institution promoting cooperation between police forces, plays an important role to counter cybercrime.

Liberty

Liberty implies that an individual is unfettered in any manner to act, with no boundaries to limit human actions. The liberty is the state of being free within society from oppressive restrictions imposed by authority on one's way of life. Liberty is most broadly understood as some 'absence of constraints'. Every infringement upon privacy can potentially result in a infringement of liberty. People have a right to privacy, that is, they have a right to expect that the government will do as little as necessary to intrude upon their rights. Privacy in cyberspace may be intruded by criminals, companies, service providers, financial institutions and government. Privacy is threatened by businesses and other entities that collect and manipulate personal data, criminals who steal such data or stalk people over the Internet, and governments that pursue surveillance or allow intrusive law-enforcement practices. Sophisticated electronic capabilities to collect, analyze, manipulate, and disseminate information, as well as to enable tracking, surveillance, and interference with communications, create unprecedented challenges to privacy [3].

Adaptive Neuro-Fuzzy Inference System (ANFIS)

The concept of fuzzy logic was introduced by Lotif Zadeh [4] in order to represent vagueness in linguistics and to implement human knowledge and inference capability in a natural way. Fuzzy logic starts with the concept of a fuzzy set. A fuzzy set is a set without a crisp, clearly defined boundary. It can contain elements with only a partial degree of membership. A Membership Function (MF) is a curve that defines how each point in the input space is mapped to a membership value (or degree of membership) between 0 and 1. The input space is sometimes referred to as the *universe of discourse*. The fuzzy logic can be considered as superset of standard Boolean logic. Fuzzy logic allows the modelling of uncertainties and the human brain's thinking, reasoning and perception [5]. The Fuzzy modelling [6] has numerous practical application.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The research activity in the area of combined application of intelligent computing technologies was initiated by Zadeh (1994) who first used the term soft computing, which he defined as a "collection of methodologies that aim to exploit the tolerance for imprecision and uncertainty to achieve tractability, robustness, and low solution cost" [7]. Soft computing differs from conventional (hard) computing in that, unlike hard computing, it is tolerant of imprecision, uncertainty, partial truth, and approximation [8]. Fuzzy inference systems, also known as fuzzy rule based systems, fuzzy models, fuzzy associative memory or fuzzy controllers, is composed of five functional blocks: a knowledgebase comprises of rule base and database, a rule base containing a number of fuzzy if-then rules, a database which defines the membership functions of the fuzzy sets used in fuzzy rules, a decision making unit which performs the inference operation on the rules, a fuzzyfier which transforms the crisp inputs into degrees of match with linguistic values, and, a defuzzifier which transform the fuzzy results of the inference into a crisp output. The Artificial neural networks (ANN) have been developed as generalizations of mathematical models of biological nervous systems. The basic processing elements of neural networks are called artificial neurons, or simply neurons or nodes. In a simplified mathematical model of the neuron, the effects of the synapses are represented by connection weights that modulate the effect of the associated input signals, and the nonlinear characteristic exhibited by neurons is represented by a transfer function. The neuron impulse is then computed as the weighted sum of the input signals, transformed by the transfer function. The learning capability of an artificial neuron is achieved by adjusting the weights in accordance to the chosen learning algorithm. The basic architecture consists of three types of neuron layers: input, hidden, and output layers. The back-propagation algorithm uses partial derivative of the error of the network with respect to each weight, and the direction of error of the network is probed. The goal of this exercise is to decrease the error to local minima. It has been proven that back-propagation learning with sufficient hidden layers can approximate any nonlinear function to arbitrary accuracy. Takagi-Sugeno neuro-fuzzy systems make use of a mixture of back-propagation to learn the membership functions and least mean square estimation to determine the coefficients of the linear combinations in the rule's conclusions. Jang proposed ANFIS, which is a fuzzy inference system, implemented in the framework of adaptive systems to facilitate learning and adaptation [10]. An adaptive network is a feed-forward multi-layer Artificial Neural Network (ANN) with; partially or completely, adaptive nodes in which the outputs are predicated on the parameters of the adaptive nodes and the adjustment of parameters due to error term is specified by the learning rules. The Adaptive Neuro Fuzzy Inference System (ANFIS) is the implementation of fuzzy inference system to adaptive networks for developing fuzzy rules with suitable membership functions to have required inputs and outputs. An adaptive neural network is a network structure consisting of a number of nodes connected through directional links. Each node is characterised by a node function with fixed adjustable parameters. Learning or training phase of a neural network is a process to determine parameter values to sufficiently fit the training data. ANFIS are fuzzy Sugeno models put in the framework of adaptive systems to facilitate learning and adaptation.

Nuorofuzzy system for cybercrime incident

There are factors which influence the occurrence of cyber crime incidents. The literature review reveals that vulnerability of an ICT infrastructure, cooperation (particularly, law enforcement cooperation) and liberty (privacy) of people on Internet have definite role in this. Also there are factors, which contribute to vulnerability, cooperation and liberty. In this study, our effort is to identify these factors, find their mutual relationship and establish their impact on cybercrime incidents. A Neurofuzzy block diagram of cybercrime incidents is shown in Fig.1.

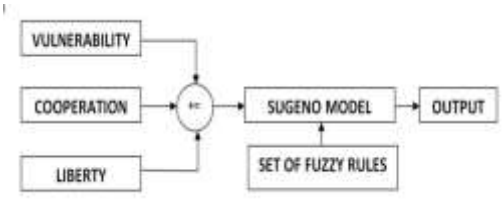

Fig.1: Block diagram of Neurofuzzy system for cybercrime incidents

Some of the causes that amount to vulnerability are, (a) Software vulnerability, which is a deficiency in software that facilitates a malicious entity to weaken the software's security and potentially cause harm; (b) Exploits, that is capable of granting privileges on

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

a computer system in contradiction to system's design; (c) Un-trusted websites, which may contain harmful Spyware or Adware that can be installed automatically on the computer systems; (d) Developer's flabbiness, where programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application. (e) User's laxity, where user uses a weak password, or store it on the system itself, and do not use other security ethics like antivirus, firewall etc; and (f) the Work culture, where the businesses operating in cyber space normally remain reluctant to cooperate in cyber crime suppression efforts to minimize the negative impact on their businesses. They avoid reporting cases of cyber attack to law enforcement agencies due to the reason that information of security breach and vulnerability in their systems would cause them harm if revealed.

Socio economic level of development: The socio economic level of development is a factor which influences vulnerability. The developed countries rely more on automation and use of technology. Even developing countries are also investing heavily on technology and automation now. The services like Internet and mobile banking, online examination and digital database are examples of use of technology. These types of services require participation of large number of users, who, in absence of proper security measure and awareness, may become victim. On the other hand, the ICT infrastructure, application software and network systems, that may have any kind of vulnerability, can be exploited. Thus, the reliance on technology is a reason for vulnerability, which is associated with socio economic level of development. Other reasons, associated with socio-economic development, are, presence of large number of internet service providers (ISPs) and large penetration of internet and mobile telephony. The cooperation, particularly law enforcement cooperation is second factor which affects vulnerability, cyber crime and its prevention efforts. The cooperation between countries and their various agencies in terms of technological cooperation, and treaties; the availability of clear laws, presence of dedicated investigating agency at national and international level, presence of dedicated agency for technical assistance, prevention and cooperation etc. are some other factors that fall under the category of cooperation. The third factor is liberty (or privacy). The civil liberty of people and the liberty on internet are factors that have reciprocal relation with vulnerability and cyber crime. When stringent security of ICT infrastructure is ensured and each transaction, each communication packet is scanned, it adversely affects peoples liberty and privacy. The factors responsible for vulnerability, cooperation and liberty are summarized in Table-1.

Table 1. Factors responsible for Vulnerability, Cooperation, and Liberty

Vulnerability	Cooperation	Liberty
• Number of ISPs • Level of Internet penetration • Level of economic and industrial development • Reliance on technology • Security measures	• Law enforcement Cooperation • Public-Private cooperation • Designated agency for cooperation • Designated agency for Investigation • Procedural law amended to cater cybercrime	• Civil liberty • Liberty on internet

The vulnerability increases due to reliance on technology, higher internet penetration, lack of legal framework, weak security measures, policy oversight, lack of training and awareness, lack of cooperation among entities and presence of enemy country or groups. The vulnerability decreases due to careful use and of ICT for critical infrastructures, isolation of critical infrastructure, protective

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

approach of cyber security, stringent security measures and encryption, good awareness and training, enhanced cooperation and absence of enemy country or group. The cooperation increases due to legal treaty between nations, technical coordination between organizations and countries and presence of standard legal framework. The cooperation decreases due to absence of treaty among countries, no cooperation state, fearing publicizing of vulnerability, absence of standard rules and policies. The liberty of people increases due to privacy protection, freedom on Internet and protection of civil and political rights. The liberty is decreased due to security breach, intrusive investigation, security measures including Internet banning, and intrusion by government and private agencies.

In order to establish relationship between factors like vulnerability, cooperation and liberty and to see their impact on cyber crime, we have assigned rating to these factors. The rating strategy has been adopted from the rating system used by the Freedom House (www.freedomhouse.org) in its publication 'Freedom in the World', an annual publication comprising of survey ratings of 195 countries and contains comparative assessment of global political rights, civil liberties and liberty on Internet in these countries. We have assigned rating 0-2 to non-vulnerable, 3 to low-vulnerable, 5 to vulnerable and 7 to highly-vulnerable. Similarly, a rating of 1 has been assigned for no-cooperation, 2-3 for limited cooperation, 4-5 for cooperation and 6-7 for full cooperation. The rating for liberty (freedom on net) has been taken from freedom house as 0-30 Free, 31-60 Partly free, and 61-100 Not free.

Proposed ANFIS model

In the proposed model, three feature variable, 'vulnerability', 'cooperation' and 'liberty' are selected as inputs of the ANFIS. Four membership functions each are assigned to vulnerability and cooperation and three membership functions are assigned to liberty. The flow chart for the model is shown in **Fig.-2**. The ANN architecture of the proposed model is shown in **Fig.9**. It shows the fuzzy rule architecture of ANFIS when the triangular membership function is adopted. Each of the three inputs is limited to four, four and three membership functions (MFs) respectively. The parameters are shown in **Table 2**.

Table 2. Cybercrime incident parameter

Input variable	Vulnerability	Cooperation	Liberty
Parameter-1	Not Vulnerable	No Cooperation	Free
Parameter-2	Some Vulnerable	Limited Cooperation	Partly Free
Parameter-3	Vulnerable	Cooperation	Not Free
Parameter-4	Highly Vulnerable	Full Cooperation	

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

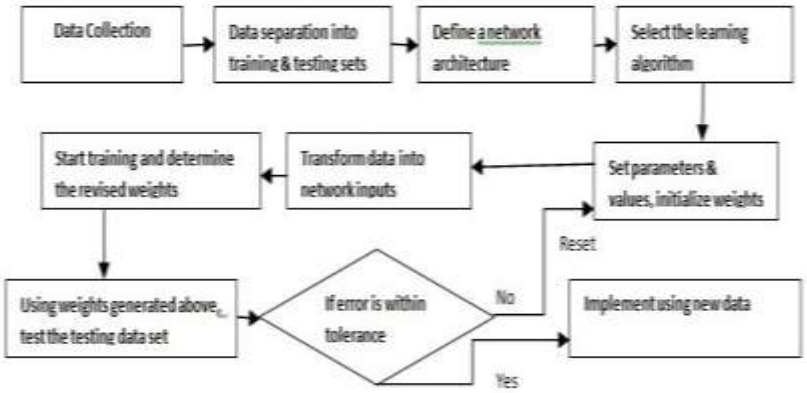

Fig.2:ANFIS Flowchart

Simulated result of Adaptive neurofuzzy system for cybercrime incidents

This section illustrates the adaptive neurofuzzy system for cybercrime incidents. The successful attempt has been made to neurofuzzy integrated system for water quality status, human age group estimation, knowledge management, intrusion detection etc. [11] [12] [13] [14] [15] . This work is an effort to contribute to this field and to explore this important technology in cybercrime control. Depending upon input values to fuzzy inference engine, the output suggests cybercrime incident level. This may help in deciding various strategic decisions and cyber security policies. For cybercrime incident level, we have laid down 48 rules and some of them are listed here:

- If (Vulnerability is Not-Vulnerable) and (Cooperation is No-Cooperation) and (Liberty is Free) then (Cybercrime-incidents is Low
- If (Vulnerability is Not-Vulnerable) and (Cooperation is Limited-Cooperation) and (Liberty is Partly-Free) then (Cybercrime-incidents is Low
- If (Vulnerability is Vulnerable) and (Cooperation is No-Cooperation) and (Liberty is Free) then (Cybercrime-incidents is High
- If (Vulnerability is Vulnerable) and (Cooperation is Cooperation) and (Liberty is Free) then (Cybercrime-incidents is Medium
- If (Vulnerability is High-Vulnerable) and (Cooperation is Limited-Cooperation) and (Liberty is Free) then (Cybercrime-incidents is High
- If (Vulnerability is High-Vulnerable) and (Cooperation is Full-Cooperation) and (Liberty is Not-Free) then (Cybercrime-incidents is Medium

The adaptive neurofuzzy system can be used for cybercrime prevention efforts by fine tuning various responsible parameters.

a. Fuzzy Inference System using Sugeno Method

A Sugeno model (Fig.3) is developed in MATLAB using Fuzzy tool by defining the inputs and output for the system. We have taken 3 inputs for the system which are actually the factors responsible for cyber crime, i.e., Vulnerability, Cooperation and Liberty.

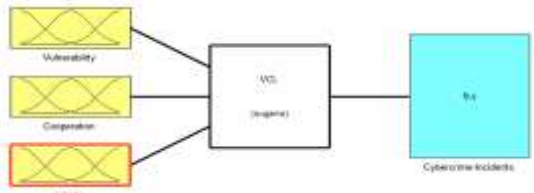

Fig.3:Fuzzy Inference System for Cybercrime incidents

b. Membership Function of factors

The factors are taken as inputs to the system and membership functions for each input have been defined. The Membership Function of Vulnerability' is shown in fig. 4.

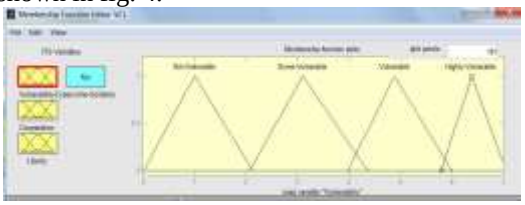

Fig.4: Membership function of Vulnerability

c. Rule Viewer of cybercrime incident:

The fuzziness of a fuzzy membership permits us to handle the problem of a incident prognosis. Various research data have been studied to lay down linguistic fuzzy rules. The rule viewer of cybercrime incidents is shown in fig.5.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

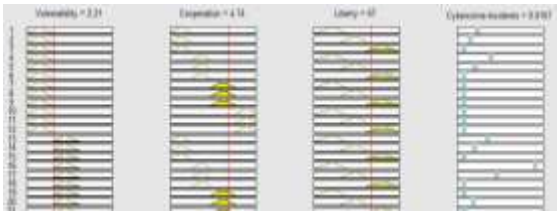

Fig.5: Rule viewer for Cybercrime incidents

d. Training data:

ANFIS modeling process starts by obtaining a data set (input-output data pairs). We have divided the data set into 70-30 ratio (70% for training and 30% for testing). Training data constitutes a set of input and output vectors. The training data used to train the adaptive neurofuzzy system is shown in fig 6.

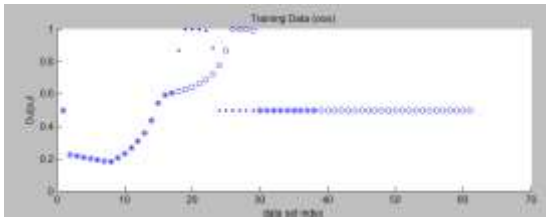

Fig.6: Training data to train the Nerofuzzy System

e. Training error:

At the end of 100 training epochs, the network error (mean square error) convergence course of each ANFIS was derived. From the curve (Fig.7), the final convergence value is .082505.

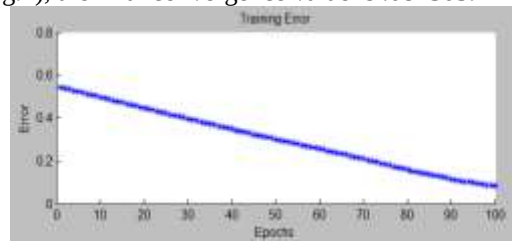

Fig. 7: Training error

f. Surface Plot:

The surface plot of the cybercrime incident is shown in fig.8.

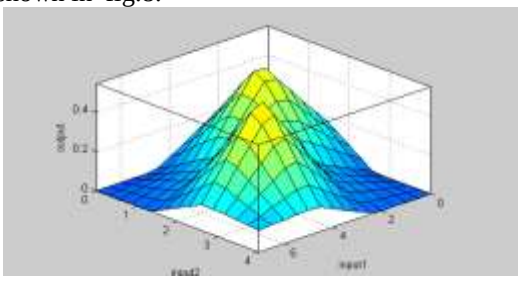

Fig.8: Cybercrime incidents with Vulnerability and Cooperation

g. Neurofuzzy architecture for cybercrime incidents:

The adaptive neurofuzzy architecture for cybercrime incident is shown in Fig.9.

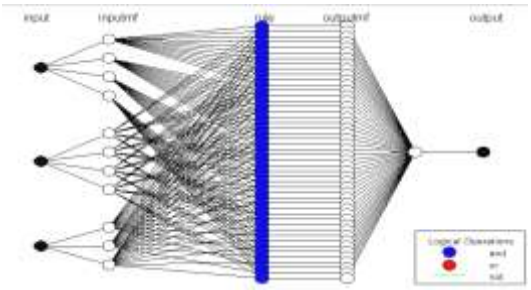

Fig.-9: ANFIS structure for research model

Conclusion

The cybercrime prevention is crucial for safety of vital infrastructures. The vulnerability, cooperation and liberty are factors that contribute to cybercrime incidents. In this paper, an adaptive neurofuzzy inference system (ANFIS) is used to successfully estimate the vulnerability-cooperation-liberty relationship. The accuracy of the rules inferred make them usable in practical setting. Future work can be focused on analyzing the cofactors affecting vulnerability, cooperation and liberty. We emphasize that this model can easily be applied to other cybercrime related areas.

References

1. *Internet Engineering Task Force RFC 2828 Internet Security Glossary; http://tools.ietf.org/html/rfc2828*
2. *http://technet.microsoft.com/en-us/library/cc751383.aspx*
3. *Ekaterina A. Drozdova, "Civil Liberties and Security in Cyberspace", CISAC Report, August 2000*
4. *Zadeh LA (1965) Fuzzy Sets, Information and Control 8: 338-353*
5. *Abraham, A. (2005), "Rule-based expert systems", Sydenham PH, Thorn R Handbook of measuring system design, Wiley, New York.*
6. *Takagi T & Sugeno M, "Fuzzy identification of systems and its applications to modelling and control", IEEE Trans Syst Man Cybernet, SMC-15(1) (1985) 116-132.*
7. *Zadeh LA (1994), "Soft computing and fuzzy logic", IEEE Software, Nov.: 48-58*
8. *Zadeh L.A., "Fuzzy Logic, Neural Networks, and Software Computing", Communications of the ACM, 37 (3), 77, March 1994*
9. *Sugeno M & Kang G T, "Structure identification of fuzzy model", Fuzzy Sets Syst, 28 (1988) 15-33*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

10. *Roger Jang J S & Sun C T, "Neuro Fuzzy modelling and control", Proc IEEE 83, (1995) 378-404*
11. *Han Yan, Zhihong Zou, Huiwen Wang; "Adaptive neuro fuzzy inference system for classification of water quality status"; Journal of Environmental Sciences 2010, 22(12) 1891–1896;www.jesc.ac.cn*
12. *H M Fard, S Khanmohammadi, S Ghaemi and F Samadi; "Human Age Group Estimation Based on ANFIS using the HOG and LBP Features"; Electrical and Electronics Engineering: An International Journal (ELELIJ) Vol 2, No 1, February 2013*
13. *S. Petrovic-Lazarevic, K. Coghill, A. Abraham; "Neuro-fuzzy modelling in support of knowledge management in social regulation of access to cigarettes by minors"; Knowledge-Based Systems 17 (2004) 57–60; www.elsevier.com/locate/knosys*
14. *A.N. Toosi, M. Kahani; "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers"; Computer Communications 30 (2007) 2201–2212; www.elsevier.com/locate/comcom*
15. *M Nilashi, M Fathian, M R Gholamian, O Ibrahim & A Khoshraftar; "The Identification Level of Security, Usability and Transparency Effects on Trust in B2C Commercial Websites Using Adaptive Neuro Fuzzy Inference System (ANFIS)"; International Journal of Artificial Intelligence And Expert Systems (IJAE), Volume (2) : Issue (3) : 2011, pp 126-149*
16. *www.freedomhouse.org*